Darstellungstheorie

Vorlesung im Sommersemester 1993,
Wintersemester 1993/94
und Sommersemester 1994

B. Külshammer

Ausarbeitung:
Markus Deiml

Inhaltsverzeichnis

KAPITEL 1

Darstellungen

Sei G endliche Gruppe und K ein (stets kommutativer) Körper.

1.1. Definition. Eine *(lineare) Darstellung* Δ von G auf einen K-Vektorraum V ist ein Homomorphismus von G in die allgemeine lineare Gruppe $\mathrm{GL}(V)$ aller Bijektionen $V \to V$. Man nennt $\deg(\Delta) := \dim(V)$ den *Grad* von Δ und $\mathrm{Ker}(\Delta) := \{g \in G : \Delta(g) = \mathrm{id}_V\}$ den *Kern* von Δ. Im Fall $\mathrm{Ker}(\Delta) = 1$ nennt man Δ *treu.*

Beispiel.

(i) Die *triviale Darstellung* von G ist die Abbildung $\Delta : G \to \mathrm{GL}(K),\ g \mapsto \mathrm{id}_K$. Diese Darstellung hat Grad 1 und Kern G.

(ii) Gegeben sei eine Operation Von G auf einer endlichen Menge Ω, d.h. eine Abbildung $G \times \Omega \to \Omega,\ (g,\omega) \mapsto {}^g\omega$ mit ${}^1\omega = \omega$ und ${}^g({}^h\omega) = {}^{gh}\omega$ für alle $\omega \in \Omega,\ g,h \in G$. Mit $K\Omega$ bezeichnen wir den K-Vektorraum aller Abbildungen $f : \Omega \to K$ mit punktweise definierten Verknüpfungen. Für $g \in G$ und $f \in K\Omega$ sei ${}^gf \in K\Omega$ definiert durch $({}^gf)(\omega) := f({}^{g^{-1}}\omega)$ für $\omega \in \Omega$. Dann ist ${}^1f = f$ und

$$({}^g({}^hf))(\omega) = ({}^hf)({}^{g^{-1}}\omega) = f({}^{h^{-1}}({}^{g^{-1}}\omega)) = f({}^{h^{-1}g^{-1}}\omega) = f({}^{(gh)^{-1}}\omega) = ({}^{gh}f)(\omega)$$

für alle $g,h \in G,\ f \in K\Omega,\ \omega \in \Omega$. Daher ist auch die Abbildung $G \times K\Omega \to K\Omega,\ (g,f) \mapsto {}^gf$ eine Gruppenoperation. Diese ist linear, d.h. es ist ${}^g(\alpha f + \alpha' f') = \alpha({}^gf) + \alpha'({}^gf')$ für $g \in G,\ \alpha,\alpha' \in K,\ f,f' \in K\Omega$. Definiert man also $\Delta(g) \in \mathrm{GL}(K\Omega)$ für $g \in G$ druch $(\Delta(g))(f) := {}^gf$ für $f \in K\Omega$, so erhält man eine Darstellung $\Delta : G \to \mathrm{GL}(K\Omega)$. Es ist $\deg(\Delta) = \dim K\Omega = |\Omega|$; definiert man nämlich für $\omega \in \Omega$ ein Element $\hat\omega \in K\Omega$ durch $\hat\omega(\psi) := 0$ für $\psi \in \Omega \setminus \{\omega\}$ und $\hat\omega(\omega) = 1$, so bilden die Elemente $\hat\omega$ $(\omega \in \Omega)$ eine Basis von $K\Omega$. Für $g \in G$ und $\omega,\psi \in \Omega$ ist

$$({}^g\hat\omega)({}^g\psi) = \hat\omega({}^{g^{-1}}({}^g\psi)) = \hat\omega({}^{g^{-1}g}\psi) = \hat\omega(\psi) = \begin{cases} 1 & \text{für } \omega = \psi \\ 0 & \text{sonst} \end{cases},$$

d.h. ${}^g\hat\omega = \widehat{{}^g\omega}$. Ist also $g \in G,\ f \in K\Omega,\ f = \sum_{\omega\in\Omega} \alpha_\omega\hat\omega$ mit $\alpha_\omega \in K$ für $\omega \in \Omega$, so ist

$$(\Delta(g))(f) = \sum_{\omega\in\Omega} \alpha_\omega(\Delta(g))(\hat\omega) = \sum_{\omega\in\Omega} \alpha_\omega\, {}^g\hat\omega = \sum_{\omega\in\Omega} \alpha_\omega \widehat{{}^g\omega}.$$

Häufig identifiziert man jedes Element $\omega \in \Omega$ mit $\hat\omega$. Dann ist Ω Basis von $K\Omega$. Jedes Element in $K\Omega$ läßt sich also in der Form $f = \sum_{\omega\in\Omega} \alpha_\omega\omega$ mit $\alpha_\omega \in K$ für $\omega \in \Omega$ schreiben. Für $g \in G$ ist dann $(\Delta(g))(f) = \sum_{\omega\in\Omega} \alpha_\omega\, {}^g\omega$.

(iii) G operiert auf sich selbst durch Linksmultiplikation: $(g,h) \mapsto gh$. Wie in (ii) erhält man also eine Darstellung $\Delta : G \to \mathrm{GL}(KG)$. Ist $f = \sum_{h\in G} \alpha_h h$ mit $\alpha_h \in K$ für $h \in G$, so ist $(\Delta(g))(f) = \sum_{h\in G} \alpha_h gh$. Man nennt Δ die *reguläre Darstellung* von G über K.

(iv) Sei N ein elementarabelscher p-Normalteiler von G für eine Primzahl p. Bekanntlich kann man N auffassen als Vektorraum über dem Körper $\mathbb{Z}/p\mathbb{Z}$: $(k + p\mathbb{Z})x := x^k$ für $x \in N,\ k \in \mathbb{Z}$. Für $g \in G$ ist dann die Abbildung $\Delta(g) : N \to N,\ x \mapsto gxg^{-1}$ linear und bijektiv, und man erhält so eine Darstellung $\Delta : G \to \mathrm{GL}(N)$. Diese Darstellung hat als Kern $\{g \in G : gxg^{-1} = x$ für alle $x \in N\} = C_G(N)$ den Zentralisator von N in G.

Bemerkung.

(i) Wir verabreden, daß unsere Gruppen stets endlich und unsere Vektorräume stets endlich-dimensional sind, auch wenn wir das nicht explizit erwähnen. Ausnahmen von dieser Regel werden wir betonen, es sei denn, sie sind offensichtlich wie etwa im Fall der Gruppe $\mathrm{GL}(V)$, falls $|V| = \infty$ ist.

(ii) Ist $\Delta : G \to \mathrm{GL}(V)$ eine Darstellung, H eine Gruppe und $f : H \to G$ ein Homomorphismus, so ist auch $\Delta \circ f : H \to \mathrm{GL}(V)$ eine Darstellung. Statt $\Delta \circ f$ schreibt man auch $\mathrm{Res}_f(\Delta)$ und nennt dies die *Einschränkung* oder *Restriktion* von Δ mittels f. Ist H eine Untergruppe von G und $f : H \to G,\ h \mapsto h$ die Inklusionsabbildung, so nennt man $\mathrm{Res}_H^G(\Delta) := \mathrm{Res}_f(\Delta)$ die Einschränkung oder Restriktion von G auf H. Ist $G = H/N$ für einen Normalteiler N von H und $f : H \to G,\ h \mapsto hN$ der kanonische Epimorphismus, so nennt man $\mathrm{Inf}_N^H(\Delta) := \mathrm{Res}_f(\Delta)$ die *Inflation* von Δ zu H. Sind G und H Untergruppen einer Gruppe X und f ist die Einschränkung eines Automorphismus α von X, so schreibt man auch ${}^{\alpha^{-1}}\Delta$ statt $\Delta \circ f$. Ist $x \in X$ und $\alpha(y) := xyx^{-1}$ für alle $y \in X$, so schreibt man ${}^{x^{-1}}\Delta$. Es ist also $({}^{x^{-1}}\Delta)(h) = \Delta(xhx^{-1})$ für $h \in H$.

(iii) Sind $\Delta_1 : G \to \mathrm{GL}(V_1), \ldots, \Delta_n : G \to \mathrm{GL}(V_n)$ Darstellungen, so auch ihre *direkte Summe* $\Delta_1 \oplus \ldots \oplus \Delta_n : G \to \mathrm{GL}(V_1 \times \ldots \times V_n),\ g \mapsto \Delta_1(g) \oplus \ldots \oplus \Delta_n(g)$; dabei ist $(\Delta_1(g) \oplus \ldots \oplus \Delta_n(g))(v_1, \ldots, v_n) := ((\Delta_1(g))(v_1), \ldots, (\Delta_n(g))(v_n))$ für $v_1 \in V_1, \ldots, v_n \in V_n$.

(iv) Seien $V_1, \ldots, V_n$ K-Vekträume und $V_1 \otimes \ldots \otimes V_n = V_1 \otimes_K \ldots \otimes_K V_n$ ihr Tensorprodukt. Das bedeutet, daß $V_1 \otimes \ldots \otimes V_n$ ein K-Vektorraum mit einer multilinearen Abbildung $\mu : V_1 \times \ldots \times V_n \to V_1 \otimes \ldots \otimes V_n,\ (v_1, \ldots, v_n) \mapsto v_1 \otimes \ldots \otimes v_n$ und der folgenden *universellen Eigenschaft* ist: Ist W ein K-Vektorraum und $f : V_1 \times \ldots \times V_n \to W$ multilinear, so existiert genau eine lineare Abbildung $F : V_1 \otimes \ldots \otimes V_n \to W$ mit $f = F \circ \mu$.

$$
\begin{tikzcd}
V_1 \times \ldots \times V_n \arrow[rr, "\mu"] \arrow[dr, "f"'] & & V_1 \otimes \ldots \otimes V_n \arrow[dl, dotted, "F"] \\
& W &
\end{tikzcd}
$$

Nach Aufgabe 2 ist $\dim V_1 \otimes \ldots \otimes V_n = (\dim V_1) \ldots (\dim V_n)$. Sind $\Delta_1 : G_1 \to \mathrm{GL}(V_1), \ldots, \Delta_n : G_n \to \mathrm{GL}(V_n)$ Darstellungen, so auch ihr *(äußeres) Tensorprodukt* $\Delta_1 \otimes \ldots \otimes \Delta_n : G_1 \times \ldots \times G_n \to \mathrm{GL}(V_1 \otimes \ldots \otimes V_n),\ (g_1, \ldots, g_n) \mapsto \Delta_1(g_1) \otimes \ldots \otimes \Delta_n(g_n)$; dabei ist $(\Delta_1(g_1) \otimes \ldots \otimes \Delta_n(g_n))(v_1 \otimes \ldots \otimes v_n) = (\Delta_1(g_1))(v_1) \otimes \ldots \otimes (\Delta_n(g_n))(v_n)$ für $v_1 \in V_1, \ldots, v_n \in V_n$ (vgl. Aufgabe 3).

(v) Sind $\Delta_1 : G \to \mathrm{GL}(V_1), \ldots, \Delta_n : G \to \mathrm{GL}(V_n)$ Darstellungen, so auch ihr *(inneres) Tensorprodukt* $\Delta_1 \otimes \ldots \otimes \Delta_n : G \to \mathrm{GL}(V_1 \otimes \ldots \otimes V_n),\ g \mapsto \Delta_1(g) \otimes \ldots \otimes \Delta_n(g)$. Dieses entsteht aus dem äußeren Tensorprodukt $G \times \ldots \times G \to \mathrm{GL}(V_1 \otimes \ldots \otimes V_n)$ durch Komposition mit dem Homomorphismus $\delta : G \to G \times \ldots \times G,\ g \mapsto (g, \ldots, g)$ gemäß (ii).

(vi) Sind $\Gamma : G \to \mathrm{GL}(V),\ \Delta : H \to \mathrm{GL}(W)$ Darstellungen, so auch $\Theta : G \times H \to \mathrm{GL}(\mathrm{Hom}(V, W))$, wobei $(\Theta(g, h))(f) := \Delta(h) \circ f \circ \Gamma(g^{-1})$ für $g \in G,\ h \in H,\ f \in \mathrm{Hom}(V, W)$ ist. Statt Θ schreibt man auch $\mathrm{Hom}(\Gamma, \Delta)$.

(vii) Sind $\Gamma : G \to \mathrm{GL}(V),\ \Delta : G \to \mathrm{GL}(W)$ Darstellungen, so kann man die Darstellung $\mathrm{Hom}(\Gamma, \Delta) : G \times G \to \mathrm{GL}(\mathrm{Hom}(V, W))$ aus (vi) mit dem Homomorphismus $\delta : G \times G \to G,\ g \mapsto (g, g)$ zusammensetzen und erhält so eine Darstellung $\Theta : G \to \mathrm{GL}(\mathrm{Hom}(V, W))$ mit $(\Theta(g))(f) = \Delta(g) \circ f \circ \Gamma(g^{-1})$ für $g \in G,\ f \in \mathrm{Hom}(V, W)$. Diese bezeichnet man auch mit $\mathrm{Hom}(\Gamma, \Delta)$.

(viii) Nimmt man in (vii) $W := K$, so ist $\mathrm{Hom}(V, W) = V^*$ der Dualraum von V. Nimmt man für Δ die triviale Darstellung, so erhält man die zu Γ *duale Darstellung* $\Gamma^* : G \to \mathrm{GL}(V^*)$ mit $(\Gamma^*(g))(f) = f \circ \Gamma(g^{-1})$ für $g \in G,\ f \in V^*$. Daher ist $\Gamma^*(g) : V^* \to V^*$ für $g \in G$ die duale Abbildung zur linearen Abbildung $\Gamma(g^{-1}) : V \to V$.

(ix) Sei V ein K-Vektorraum und L ein Teilkörper von K mit $[K : L] = \dim_L K < \infty$. Wir können V auch als L-Vektorraum ansehen und schreiben dann V_L statt V. Bekanntlich ist $\dim_L V_L = [K : L] \dim_K V$. Da jede K-lineare Abbildung auch L-linear ist, ist $\mathrm{GL}(V) \subseteq \mathrm{GL}(V_L)$. Jede

Darstellung $\Delta : G \to \mathrm{GL}(V)$ liefert also eine Darstellung $\Delta_L = \mathrm{Res}_L^K(\Delta) : G \to \mathrm{GL}(V_L)$ mit $\deg(\Delta_L) = [K : L] \deg(\Delta)$.

1.2. Definition. Eine *Matrixdarstellung* von G des Grades n über K ist ein Homomorphismus Λ von G in die allgemeine lineare Gruppe $\mathrm{GL}(n, K)$ aller invertierbaren $n \times n$-Matrizen mit Koeffizienten in K.

Bemerkung.

(i) Ist Δ eine Darstellung von G auf den K-Vektorraum V und $b_1, \ldots, b_n$ eine Basis von V, so erhält man eine Matrixdarstellung $\Lambda : G \to \mathrm{GL}(n, K)$, indem man jedem $g \in G$ die Matrix $\Lambda(g)$ von $\Delta(g) \in \mathrm{GL}(V)$ bzgl. $b_1, \ldots, b_n$ zuordnet. Ist also $(\Delta(g))(b_j) = \sum_{i=1}^n \lambda_{ij}(g) b_i$ mit $\lambda_{ij} \in K$ für $i, j = 1, \ldots, n$, so ist $\Lambda(g) = (\lambda_{ij}(g))$.

(ii) Ist umgekehrt $\Lambda : G \to \mathrm{GL}(n, K)$ eine Matrixdarstellung, so erhält man eine Darstellung Δ von G auf den K-Vektorraum $V = K^{n \times 1} = \mathrm{Mat}(n, 1, K)$, indem man jedem $g \in G$ die Abbildung $\Delta(g) : V \to V,\ v \mapsto \Lambda(g) v$ zuordnet.
Lineare Darstellungen und Matrixdarstellungen entsprechen sich also wie lineare Abbildungen und Matrizen. Begriffe wie „Kern", „treu", usw. übertragen sich daher auf Matrixdarstellungen.

(iii) Sei $\Lambda : G \to \mathrm{GL}(n, K)$ eine Matrixdarstellung und $\alpha : K \to L$ ein Homomorphismus von Körpern. Dann ist $\mathrm{GL}(n, K) \to \mathrm{GL}(n, L),\ (\kappa_{ij}) \mapsto (\alpha(\kappa_{ij}))$ ein Homomorphismus von Gruppen, den wir wieder mit α bezeichnen. Wir erhalten so eine neue Matrixdarstellung $\alpha \circ \Lambda : G \to \mathrm{GL}(n, K) \to \mathrm{GL}(n, L)$. Ist K ein Teilkörper von L und $\alpha : K \to L$ die Inklusionsabbildung, so schreibt man Λ^L statt $\alpha \circ \Lambda$ und sagt: Λ^L entsteht durch *Skalarerweiterung* aus Λ. Ist $K = L$ und α ein Körperautomorphismus, so schreibt man ${}^\alpha\Lambda$ statt $\alpha \circ \Lambda$ und nennt ${}^\alpha\Lambda$ *algebraisch konjugiert* zu Λ.

Beispiel. Gegeben sei eine Operation von G auf einer endlichen Menge Ω und die entsprechende Darstellung $\Delta : G \to \mathrm{GL}(K\Omega)$. Wir haben gesehen, daß man Ω als Basis von $K\Omega$ auffassen kann. Bzgl. dieser Basis wird jedes $\Delta(g)$ durch eine Permutationsmatrix $\Lambda(g)$ beschrieben, d.h. in jeder Zeile und Spalte von $\Lambda(g)$ steht genau eine 1 und sonst lauter Nullen.

1.3. Definition.

(i) Darstellungen Γ, Δ von G auf den K-Vektorräumen V, W nennt man *ähnlich* ($\Gamma \sim \Delta$), falls eine lineare Bijektion $f : V \to W$ existiert mit $f \circ \Gamma(g) = \Delta(g) \circ f$ für alle $g \in G$.

$$\begin{tikzcd} V \arrow[r, "\Gamma(g)"] \arrow[d, "f"'] & V \arrow[d, "f"] \\ W \arrow[r, "\Delta(g)"] & W \end{tikzcd}$$

(ii) Matrixdarstellungen $\Theta : G \to \mathrm{GL}(m, K),\ \Lambda : G \to \mathrm{GL}(n, K)$ nennt man *ähnlich* ($\Theta \sim \Lambda$), falls $m = n$ ist und ein $A \in \mathrm{GL}(n, K)$ existiert mit $A\Theta(g) = \Lambda(g) A$ für alle $g \in G$.

Bemerkung.

(i) $\sim$ ist eine Äquivalenzrelation.

(ii) Wie man sich in der Gruppentheorie in der Regel für Gruppen nur bis auf Isomorphie interessiert, so interessiert man sich in der Darstellungstheorie für Darstellungen nur bis auf Ähnlichkeit.

(iii) Sind $\Gamma : G \to \mathrm{GL}(V)$ und $\Delta : G \to \mathrm{GL}(W)$ ähnliche Darstellungen und sind $b_1, \ldots, b_n$ und $c_1, \ldots, c_n$ Basen von V bzw. W, so sind die entsprechenden Matrixdarstellungen Θ und Λ ähnlich; ist nämlich $f : V \to W$ eine lineare Bijektion und $f \circ \Gamma(g) = \Delta(g) \circ f$ für alle $g \in G$, und ist A die Matrix von f bzgl. $b_1, \ldots, b_n$ und $c_1, \ldots, c_n$, so ist $A\Theta(g) = \Lambda(g) A$ für alle $g \in G$. Insbesondere sind je zwei Matrixdarstellungen zu einer festen Darstellung aber zu verschiedenen Basen ähnlich.

(iv) Umgekehrt sind für ähnliche Matrixdarstellungen $\Theta, \Lambda : G \to \mathrm{GL}(n, K)$ die entsprechenden Darstellungen $\Gamma, \Delta : G \to \mathrm{GL}(K^{n \times 1})$ ähnlich. Ähnlichkeitsklassen von Darstellungen und Ähnlichkeitsklassen von Matrixdarstellungen entsprechen sich also.

1.4. Definition. Sei Δ eine Darstellung der Gruppe G auf einem K-Vektorraum V. Einen Untervektorraum U von V nennt man *Δ-invariant*, falls $(\Delta(g))(u) \in U$ für alle $g \in G,\ u \in U$.

Bemerkung. Man erhält dann Darstellungen $\Gamma : G \to \mathrm{GL}(U)$, $\Theta : G \to \mathrm{GL}(V/U)$, indem man jedem $g \in G$ die Einschränkung $\Gamma(g) : U \to U$ von $\Delta(g)$ bzw. die durch $\Delta(g)$ induzierte Abbildung $\Theta(g) : V/U \to V/U,\ v + U \mapsto (\Delta(g))(v) + U$ zuordnet. Man nennt Γ eine *Teildarstellung* und Θ eine *Faktordarstellung* von Δ. Wählt man eine Basis $b_1, \dots, b_m$ von U und ergänzt man diese zu einer Basis $b_1, \dots, b_n$ von V, so gilt für die entsprechende Matrixdarstellung $\tilde{\Delta}$ von G

$$\tilde{\Delta}(g) = \begin{pmatrix} \tilde{\Gamma}(g) & * \\ 0 & \tilde{\Theta}(g) \end{pmatrix}$$

für $g \in G$; dabei ist $\tilde{\Gamma}$ die Matrixdarstellung zu Γ und $b_1, \dots, b_m$ und $\tilde{\Theta}$ die Matrxdarstellung von Θ bzgl. der Basis $b_{m+1} + U, \dots, b_n + U$ von V/U.

Beispiel. Operiert G auf einer endlichen Menge Ω und ist $\Delta : G \to \mathrm{GL}(K\Omega)$ die entsprechende Darstellung, so ist der von $b := \sum_{\omega \in \Omega} \omega$ aufgespannte Untervektorraum U von $K\Omega$ Δ-invariant, und die entsprechende Teildarstellung $\Gamma : G \to \mathrm{GL}(U)$ ist zur trivialen Darstellung ähnlich; denn für $g \in G$ ist $(\Delta(g))(b) = \sum_{\omega \in \Omega} {}^g\omega = b$.

1.5. Satz (Maschke). *Sei* $\mathrm{char}(K) \nmid |G|$ *(z.B.* $\mathrm{char}(K) = 0$*),* Δ *eine Darstellung von* G *auf einen* K*-Vektorraum* V *und* U *ein* Δ*-invarianter Untervektorraum von* V*. Dann existiert ein* Δ*-invarianter Untervektorraum* W *von* V *mit* $V = U \oplus W$*.*

Beweis. Wir wählen zunächst einen beliebigen Untervektorraum X von V mit $V = U \oplus X$ und bezeichnen mit $h : V \to V$ die entsprechenden Projektion auf U. Dann setzen wir

$$g := \frac{1}{|G|} \sum_{x \in G} \Delta(x^{-1}) \circ h \circ \Delta(x)$$

und $W := \mathrm{Ker}(g)$. Für $u \in U$ ist also

$$g(u) = \frac{1}{|G|} \sum_{x \in G} (\Delta(x^{-1}) \circ h \circ \Delta(x))(u) = \frac{1}{|G|} \sum_{g \in G} \underbrace{(\Delta(x^{-1}) \circ \Delta(x))}_{=\Delta(x^{-1}x)=\Delta(1)=\mathrm{id}_V} (u) = u.$$

Insbesondere ist $U \cap W = 0$. Für $v \in V$ ist $g(v) \in U$, also

$$g(v - g(v)) = g(v) - g(g(v)) = g(v) - g(v) = 0,$$

d.h. $v - g(v) \in W$ und $v = g(v) + (v - g(v)) \in U + W$. Folglich ist $V = U \oplus W$. Für $w \in W$ und $y \in G$ ist

$$\begin{aligned} (g \circ \Delta(y))(w) &= \left(\frac{1}{|G|} \sum_{x \in G} \Delta(x^{-1}) \circ h \circ \Delta(xy) \right)(w) \\ &= \left(\Delta(y) \circ \underbrace{\left(\frac{1}{|G|} \sum_{x \in G} \Delta(y^{-1}x^{-1}) \circ h \circ \Delta(xy) \right)}_{=g} \right)(w) \\ &= (\Delta(xy) \circ g)(w) \ = \ (\Delta(y))(0) \ = \ 0, \end{aligned}$$

also $(\Delta(y))(w) \in \mathrm{Ker}(g) = W$. Folglich ist W Δ-invariant. $\square$

Bemerkung. Wählt man eine Basis $b_1, \dots, b_m$ von U und eine Basis $d_1, \dots, d_n$ von W, so gilt für die Matrixdarstellung $\tilde{\Delta}$ bzgl. der Basis $b_1, \dots, b_m, d_1, \dots, d_n$ von V:

$$\tilde{\Delta}(g) = \begin{pmatrix} \tilde{\Gamma}(g) & 0 \\ 0 & \tilde{\Theta}(g) \end{pmatrix}$$

für $g \in G$; dabei sind Γ und Θ die entsprechenden Teildarstellungen zu U bzw. W und $\tilde{\Gamma}$ und $\tilde{\Theta}$ die zugehörigen Matrixdarstellungen. Folglich gilt $\Delta \sim \Gamma \oplus \Theta$.

1.6. Definition. Eine Darstellung Δ von G auf einen K-Vektorraum $V \neq 0$ nennt man *irreduzibel*, falls außer 0 und V keine Δ-invarianten Untervektorräume existieren.

Bemerkung. Der Satz von Maschke besagt, daß im Fall $\operatorname{char} K \not| \, |G|$ jede Darstellung von G zu einer direkten Summe irreduzibler Darstellungen ähnlich ist. Man kennt also alle Darstellungen von G, wenn man nur die irreduziblen Darstellungen kennt.

Beispiel. Darstellungen vom Grad 1 sind immer irreduzibel.

1.7. Satz (Schurs Lemma). *Seien $\Gamma : G \to \mathrm{GL}(V)$, $\Delta : G \to \mathrm{GL}(W)$ irreduzible Darstellungen und $f : V \to W$ linear mit $\Delta(g) \circ f = f \circ \Gamma(g)$ für alle $g \in G$. Ist $f \neq 0$, so ist f bijektiv.*

Beweis. Für $g \in G$ und $x \in \mathrm{Ker}(f)$ ist

$$(f \circ \Gamma(g))(x) = (\Delta(g) \circ f)(x) = (\Delta(g))(0) = 0,$$

also $(\Gamma(g))(x) \in \mathrm{Ker}(f)$. Daher ist $\mathrm{Ker}(f)$ ein Γ-invarianter Untervektorraum von V. Analog ist $\mathrm{Bild}(f)$ ein Δ-invarianter Untervektorraum von W. Ist $f \neq 0$, so ist also $\mathrm{Ker}(f) = 0$ und $\mathrm{Bild}(f) = W$ wegen der Irreduzibilität von Γ und Δ. $\square$

Bemerkung. Unter den gegebenen Voraussetzungen ist also $\Gamma \sim \Delta$.

1.8. Definition. Für jede Darstellung $\Delta : G \to \mathrm{GL}(V)$ setzt man

$$C(\Delta) := \{f \in \mathrm{End}(V) : \Delta(g) \circ f = f \circ \Delta(g) \text{ für alle } g \in G\}.$$

Für jede Matrixdarstellung $\Lambda : G \to \mathrm{GL}(n, K)$ setzt man analog

$$C(\Lambda) := \{A \in \mathrm{Mat}(n, K) : \Lambda(g) \circ A = A \circ \Lambda(g) \text{ für alle } g \in G\}.$$

Bemerkung.

(i) Ist Λ eine Matrixdarstellung zu Δ und einer Basis $b_1, \dots, b_n$ von V, so besteht $C(\Lambda)$ aus den Matrizen der Elemente in $C(\Delta)$ bzgl. $b_1, \dots, b_n$.
(ii) $C(\Delta), C(\Lambda)$ sind K-Vektorräume und Ringe.
(iii) Falls Δ und Λ irreduzibel sind, so sind $C(\Delta)$ und $C(\Lambda)$ nach Schurs Lemma Schiefkörper.
(iv) Ist $L \supseteq K$ Körpererweiterung, so ist $C(\Lambda) = C(\Lambda^L) \cap \mathrm{Mat}(n, K)$ und $\dim_L C(\Lambda^L) = \dim_K C(\Lambda)$; denn man kann $C(\Lambda)$ als K-Lösungsraum des linearen homogenen Gleichungssystems $\Lambda(g)X - X\Lambda(g) = 0$ $(g \in G)$ ansehen, und $C(\Lambda^L)$ ist dann der L-Lösungsraum des gleichen Gleichungssystems.

Satz. *Sei $\mathrm{char}(K) \not| \, |G|$, Δ eine Darstellung von G auf einen K-Vektorraum V und $C(\Delta)$ Schiefkörper. Dann ist Δ irreduzibel.*

Beweis. Ist Δ reduzibel, so existieren nach Maschke Δ-invariante Untervektorräume $U \neq 0, W \neq 0$ von V mit $V = U \oplus W$. Die Projektionen auf U bzw. W liegen dann in $C(\Delta)$, sind aber nicht invertierbar. $\square$

Beispiel. Ist K algebraisch abgeschlossen und Δ irreduzibel, so ist $C(\Delta) = K \,\mathrm{id}_V$. Ist nämlich $f \in C(\Delta)$ beliebig und $\lambda \in K$ Eigenwert von f, so ist auch $f - \lambda \,\mathrm{id}_V \in C(\Delta)$, aber $f - \lambda \,\mathrm{id}_V$ nicht invertierbar. Nach Bemerkung (iii) ist also $f - \lambda \,\mathrm{id}_V = 0$, d.h. $f = \lambda \,\mathrm{id}_V \in K \,\mathrm{id}_V$.

KAPITEL 2

Zerfällungskörper

Sei G Gruppe und K Körper.

2.1. Bemerkung. Sei $L \supseteq K$ eine Körpererweiterung. Es kann vorkommen, daß eine Matrixdarstellung $\Delta : G \to \mathrm{GL}(n,K)$ irreduzibel ist, aber nicht $\Delta^L : G \to \mathrm{GL}(n,K) \to \mathrm{GL}(n,L)$ (vgl. Aufgabe 5).

Definition. Eine Matrixdarstellung $\Delta : G \to \mathrm{GL}(n,K)$ heißt *absolut irreduzibel*, falls Δ^L für jede Körpererweiterung $L \supseteq K$ irreduzibel ist.

Satz. *Ist die Matrixdarstellung $\Delta : G \to \mathrm{GL}(n,K)$ absolut irreduzibel, so ist $C(\Delta) = K1_n$. Im Fall $\operatorname{char} K \nmid |G|$ gilt auch die Umkehrung.*

Beweis. Sei Δ absolut irreduzibel und $\overline{K}$ der algebraische Abschluß von K. Dann ist $\Delta^{\overline{K}}$ irreduzibel, also $C(\Delta^{\overline{K}}) = \overline{K}1_n$ nach Beispiel 1.8. Folglich ist $C(\Delta) = C(\Delta^{\overline{K}}) \cap \mathrm{Mat}(n,K) = K1_n$.
Sei umgekehrt $\operatorname{char} K \nmid |G|$, $C(\Delta) = K1_n$ und $L \supseteq K$ eine Körpererweiterung. Dann ist $\dim_L C(\Delta^L) = \dim_K C(\Delta) = 1$. Wegen $L1_n \subseteq C(\Delta^L)$ ist $C(\Delta^L) = L1_n \cong L$. Nach Satz 1.8 ist Δ^L irreduzibel. □

2.2. Satz. *Für jede irreduzible Darstellung Δ von G über K gilt:*

(i) *Ist Δ treu, so ist $Z(G)$ zyklisch.*
(ii) *Ist G abelsch und Δ absolut irreduzibel, so ist* $\deg(\Delta) = 1$.

Beweis.

(i) Wegen $Z(G) \cong \Delta(Z(G)) \subseteq C(\Delta)$ erzeugen die Elemente $\Delta(g)$ $(g \in Z(G))$ eine endliche Körpererweiterung $L \supseteq K\,\mathrm{id}_V \cong K$. Als endliche Untergruppe von $L^\times$ ist dann $\Delta(Z(G))$ zyklisch.
(ii) Für $g \in G$ ist $\Delta(g) \in C(\Delta) = K\,\mathrm{id}_V$. Da Δ irreduzibel ist, folgt $\deg(\Delta) = 1$. □

2.3. Definition. Man nennt K einen *Zerfällungskörper* für G, falls jede irreduzible Matrixdarstellung von G über K absolut irreduzibel ist.

Bemerkung. Im Fall $\operatorname{char} K \nmid |G|$ bedeutet das: $C(\Delta) = K1_n$ für jede irreduzible Matrixdarstellung $\Delta : G \to \mathrm{GL}(n,K)$. (Dies gilt auch im Fall $\operatorname{char} K \mid |G|$, wird aber anders bewiesen.)

Beispiel. Algebraisch abgeschlossene Körper K mit $\operatorname{char} K \nmid |G|$ sind stets Zerfällungskörper. Wichtigstes Beispiel ist $\mathbb{C}$. Häufig interessiert man sich für „kleinere“ Zerfällungskörper.

2.4. Satz. *Seien $\Lambda : G \to \mathrm{GL}(m,K)$, $\Theta : G \to \mathrm{GL}(n,K)$ irreduzible Matrixdarstellungen und $\Lambda(g) = (\lambda_{ij}(g))$, $\Theta(g) = (\vartheta_{ij}(g))$ für $g \in G$. Dann gilt für alle i,j,k,l:*

(i) *Sind Λ und Θ nicht ähnlich, so ist*

$$\sum_{g \in G} \lambda_{ij}(g)\vartheta_{kl}(g^{-1}) = 0.$$

(ii) *Ist Λ absolut irreduzibel und* $\operatorname{char} K \nmid |G|$, *so ist* $\operatorname{char} K \nmid m$ *und*

$$\sum_{g \in G} \lambda_{ij}(g)\lambda_{kl}(g^{-1}) = \frac{|G|}{m}\delta_{il}\delta_{jk}.$$

Beweis. Sei $E_{jk} \in \mathrm{Mat}(m,n,K)$ die Matrix, die an der Stelle (j,k) eine 1 und sonst lauter Nullen enthält, und sei

$$F_{jk} := \sum_{g \in G} \Lambda(g) E_{jk} \Theta(g^{-1}) = \left(\sum_{g \in G} \lambda_{ij}(g) \vartheta_{kl}(g^{-1}) : i,j = 1, \dots, m,\ l = 1, \dots, n \right).$$

Für $h \in G$ ist dann $\Lambda(h) F_{jk} \Theta(h^{-1}) = F_{jk}$, d.h. $\Lambda(h) F_{jk} = F_{jk} \Theta(h)$. Sind Λ und Θ nicht ähnlich, so ist $F_{jk} = 0$ nach Schur, und (i) ist bewiesen.
Sei also $\Lambda = \Theta$ absolut irreduzibel. Dann ist $F_{jk} \in C(\Lambda) = K1_m$, also $F_{jk} = \alpha_{jk} 1_m$ für ein $\alpha_{jk} \in K$. Folglich gilt für $i, l = 1, \dots, n$:

$$\begin{aligned} \alpha_{jk}\delta_{il} &= \sum_{g \in G} \lambda_{ij}(g) \lambda_{kl}(g^{-1}) = \sum_{h \in G} \lambda_{ij}(h^{-1}) \lambda_{kl}(h) \\ &= \sum_{h \in G} \lambda_{kl}(h) \lambda_{ij}(h^{-1}) = \alpha_{li} \delta_{kj}. \end{aligned}$$

Daher ist $\alpha_{li} = 0$ für $i \neq l$ und $\alpha_{jj} = \alpha_{ii}$ für alle i,j. Mit $\alpha := \alpha_{11}$ ist $\alpha_{jk} = \alpha \delta_{jk}$. Für $i = 1, \dots, m$ ist ferner

$$m\alpha = \sum_{j=1}^{m} \sum_{g \in G} \lambda_{ij}(g) \lambda_{ji}(g^{-1}) = \sum_{g \in G} 1_K = |G| 1_K$$

wegen $\Lambda(g)\Lambda(g^{-1}) = 1_m$ für $g \in G$. Daher ist $\operatorname{char} K \not| \, m$ und $\alpha = \frac{|G|}{m}$. □

2.5. Bemerkung. Für jede Körpererweiterung $L \supseteq K$ bilden die Funktionen $G \to L$ einen L-Vektorraum $F(G,L)$ der Dimension $|G|$.

Satz. *Seien $\Lambda_1 : G \to \mathrm{GL}(d_1, K), \dots, \Lambda_r : G \to \mathrm{GL}(d_r, K)$ paarweise nichtähnliche absolut irreduzible Matrixdarstellungen von G, sei $\operatorname{char} K \not| \, |G|$ und $\Lambda_s(g) = (\lambda_{ij}^s(g))$ für $s = 1, \dots, r$ und $g \in G$. Für jeden Erweiterungskörper $L \supseteq K$ sind dann die Funktionen $\lambda_{ij}^s : G \to L$ $(i,j = 1, \dots, d_s,\ s = 1, \dots, r)$ linear unabhängig über L; insbesondere ist $\sum_{s=1}^{r} d_i^2 \leq |G|$. Daher gibt es bis auf Ähnlichkeit nur endlich viele absolut irreduzible Matrixdarstellungen von G über K.*

Beweis. Gegeben seien Elemente $\alpha_{ij}^s \in L$ mit $\sum_{s=1}^{r} \sum_{i,j=1}^{d_s} \alpha_{ij}^s \lambda_{ij}^s = 0$. Für $g \in G,\ k,l = 1, \dots, d_t,\ t = 1, \dots, r$ gilt dann nach 2.4:

$$0 = \sum_{g \in G} \sum_{s=1}^{r} \sum_{i,j=1}^{d_s} \alpha_{ij}^s \lambda_{ij}^s(g) \lambda_{kl}^t(g^{-1}) = \sum_{i,j=1}^{d_t} \sum_{g \in G} \alpha_{ij}^t \lambda_{ij}^t(g) \lambda_{kl}^t(g^{-1}) = \alpha_{lk}^t \frac{|G|}{d_t}.$$

□

2.6. Definition. Sei $\Lambda : G \to \mathrm{GL}(n,K)$ eine Matrixdarstellung und $L \subseteq K$ ein Teilkörper. Man nennt Λ *realisierbar* über L, falls es eine Darstellung $\Theta : G \to \mathrm{GL}(n,L)$ gibt mit $\Lambda \sim \Theta^K$.

Satz. *Sei K ein Zerfällungskörper für G mit $\operatorname{char} K \not| \, |G|$ und $L \subseteq K$ ein Teilkörper. Läßt sich jede irreduzible Matrixdarstellung $\Lambda : G \to \mathrm{GL}(n,K)$ über L realisieren, so ist auch L ein Zerfällungskörper für G.*

Beweis. Seien $\Theta_1 : G \to \mathrm{GL}(d_1, L), \dots, \Theta_r : G \to \mathrm{GL}(d_r, L)$ Matrixdarstellungen mit der Eigenschaft, daß $\Theta_1^K, \dots, \Theta_r^K$ bis auf Ähnlichkeit alle irreduziblen Matrixdarstellungen von G über K sind. Für $s = 1, \dots, r$ und $g \in G$ sei $\Theta_s(g) = (\vartheta_{ij}^s(g))$. Dann ist $C(\Theta_s) = C(\Theta_s^K) \cap \mathrm{Mat}(n,L) = K1_{d_s} \cap \mathrm{Mat}(n,L) = L1_{d_s}$, also Θ_s absolut irreduzibel. Sei $\Theta : G \to \mathrm{GL}(n,L)$ eine beliebige irreduzible Matrixdarstellung, und sei $\Theta(g) = (\vartheta_{ij}(g))$ für $g \in G$. Da Θ^K zu einer direkten Summe von einigen Θ_s^K ähnlich ist, ist ϑ_{11} eine K-Linearkombination der Funktionen ϑ_{ij}^s $(i,j = 1, \dots, d_s,\ s = 1, \dots, r)$. Nach 2.4(i) ist also Θ zu einer der Darstellungen $\Theta_1, \dots, \Theta_r$ ähnlich. □

2.7. Satz. *Im Fall $\operatorname{char} K \not| \, |G|$ existiert eine endliche Körpererweiterung L von K, so daß L ein Zerfällungskörper für G ist.*

Beweis. Sei $\overline{K}$ algebraischer Abschluß von K, und seien $\Lambda_1 : G \to \mathrm{GL}(d_1, \overline{K}), \dots, \Lambda_r : G \to \mathrm{GL}(d_r, \overline{K})$ bis auf Ähnlichkeit alle irreduziblen Matrixdarstellungen von G über $\overline{K}$. Für $s = 1, \dots, r$, $g \in G$ sei $\Lambda_s(g) = (\lambda_{ij}^s(g))$. Dann ist $L := K(\lambda_{ij}^s(g) : i, j = 1, \dots, d_s,\ s = 1, \dots, r,\ g \in G)$ eine endliche Körpererweiterung von K. Mit $\overline{K}$ ist auch L nach 2.6 ein Zerfällungskörper für G. □

Bemerkung. Wir werden später beweisen, daß $\mathbb{Q}(e^{2\pi i/|G|})$ Zerfällungskörper für G ist.

2.8. Satz. *Sei* $\operatorname{char} K \nmid |G|$, $g \in G$ *und* $\Delta : G \to \mathrm{GL}(n, K)$ *eine Matrixdarstellung. Dann existiert eine endliche Körpererweiterung L von K, so daß $\Delta^L(g)$ zu einer Diagonalmatrix ähnlich ist.*

Beweis. O.B.d.A. sei $G = \langle g \rangle$. Nach 2.7 existiert eine endliche Körpererweiterung $L \supseteq K$, so daß L Zerfällungskörper für G ist. Nach 2.2 haben alle irreduziblen Matrixdarstellungen von G über L den Grad 1. □

KAPITEL 3

Charaktere

Sei G Gruppe und K Körper mit $\operatorname{char} K = 0$, also o.B.d.A. $\mathbb{Q} \subseteq K$.

3.1. Definition. Für jede Matrixdarstellung $\Delta : G \to \mathrm{GL}(n, K)$ bezeichnet man die Abbildung $\chi_\Delta : G \to K,\ g \mapsto \operatorname{spur}(\Delta(g))$ als *Charakter* von Δ.

Bemerkung. Da ähnliche Matrizen die gleiche Spur haben, haben ähnliche Matrixdarstellungen den gleichen Charakter. Daher kann man auch jeder Darstellung von G einen Charakter zuordnen. Ähnliche Darstellungen haben dann den gleichen Charakter.

Satz. *Für jede Matrixdarstellung $\Delta : G \to \mathrm{GL}(n, K)$ gilt:*

(i) $\chi_\Delta(1) = \deg(\Delta)$.
(ii) *Für $g \in G$ ist $\chi_\Delta(g)$ eine Summe von $|G|$-ten Einheitswurzeln über K.*
(iii) *Im Fall $K \subseteq \mathbb{C}$ ist $\chi_\Delta(g^{-1}) = \overline{\chi_\Delta(g)}$ für $g \in G$.*

Beweis.

(i) Trivial.
(ii) Sei $g \in G$. Nach 2.8 existiert eine endliche Körpererweiterung L von K, so daß $\Delta^L(g)$ zu einer Diagonalmatrix D ähnlich ist. Nach Fermat ist $\Delta^L(g)^{|G|} = \Delta^L(g^{|G|}) = \Delta^L(1) = 1_n$, also auch $D^{|G|} = 1_n$. Daher sind die Diagonalelemente in D alle $|G|$-te Einheitswurzeln.
(iii) Im Fall $K \subseteq \mathbb{C}$ kann man auch $L \subseteq \mathbb{C}$ annehmen. Für jede Einheitswurzel $\zeta \in \mathbb{C}$ ist aber $\zeta^{-1} = \overline{\zeta}$. Folglich ist
$$\chi_\Delta(g^{-1}) = \operatorname{spur}(\Delta^L(g^{-1})) = \operatorname{spur}(D^{-1}) = \overline{\operatorname{spur}(D)} = \overline{\operatorname{spur}(\Delta^L(g))} = \overline{\chi_\Delta(g)}.$$

$\square$

Beispiel.

(i) Für Matrixdarstellungen $\Delta_1 : G \to \mathrm{GL}(d_1, K), \ldots, \Delta_n : G \to \mathrm{GL}(d_n, K)$ ist $\chi_{\Delta_1 \oplus \ldots \oplus \Delta_n} = \chi_{\Delta_1} + \ldots + \chi_{\Delta_n}$.
(ii) Für Matrixdarstellungen $\Delta_1 : G_1 \to \mathrm{GL}(d_1, K), \ldots, \Delta_n : G_n \to \mathrm{GL}(d_n, K)$ und Elemente $g_1 \in G_1, \ldots, g_n \in G_n$ ist $\chi_{\Delta_1 \otimes \ldots \otimes \Delta_n}(g_1, \ldots, g_n) = \chi_{\Delta_1}(g_1) \ldots \chi_{\Delta_n}(g_n)$ (vgl. Aufgabe 6). Daher schreibt man auch $\chi_{\Delta_1 \otimes \ldots \otimes \Delta_n} = \chi_{\Delta_1} \cdots \chi_{\Delta_n}$.
(iii) Für jede Darstellung Δ von G mit Charakter χ hat die duale Darstellung Δ^* den *dualen Charakter* $\chi^* : G \to K,\ g \mapsto \chi(g^{-1})$; denn bekanntlich entspricht der dualen Abbildung die transponierte Matrix.
(iv) Zur trivialen Matrixdarstellung $\Delta : G \to \mathrm{GL}(1, K)$ gehört der *triviale Charakter* $\chi_\Delta = 1_G : G \to K,\ g \mapsto 1$.
(v) G operiere auf einer endlichen Menge Ω, und $\Delta : G \to \mathrm{GL}(K\Omega)$ sei die entsprechende Darstellung. Für $g \in G$ ist die Matrix von $\Delta(g)$ bzgl. Ω als Basis eine Permutationsmatrix. Die Einträge 1 auf der Hauptdiagonalen entsprechen dabei den Elementen $\omega \in \Omega$ mit ${}^g\omega = \omega$, d.h. den Fixpunkten von g auf Ω. Daher ist $\chi_\Delta(g) = |\{\omega \in \Omega : {}^g\omega = \omega\}|$. Man nennt χ_Δ den *Permutationscharakter* dieser Gruppenoperation.
(vi) Bei der regulären Darstellung operiert G auf sich selbst durch Linksmultiplikation. Für $g \in G \setminus \{1\}$ und $h \in G$ ist aber $gh \neq h$, also $\chi_\Delta(g) = 0$. Außerdem ist $\chi_\Delta(1) = |G|$. Man nennt $\chi_\Delta = \rho_G$ den *regulären Charakter* von G.

3.2. Definition. Eine Abbildung $f : G \to K$, die konstant auf den Konjugationsklassen von G ist, nennt man eine *Klassenfunktion.*

Bemerkung. Dies bedeutet: $f(ghg^{-1}) = f(h)$ für alle $g, h \in G$. Die Klassenfunktionen $G \to K$ bilden einen K-Vektorraum $\mathrm{CF}(G, K)$, dessen Dimension die Anzahl der Konjugationsklassen von G ist.

Beispiel. Für jede Matrixdarstellung $\Delta : G \to \mathrm{GL}(n, K)$ und $g, h \in G$ ist $\Delta(ghg^{-1}) = \Delta(g)\Delta(h)\Delta(g)^{-1}$ und

$$\chi_\Delta(ghg^{-1}) = \mathrm{spur}(\Delta(ghg^{-1})) = \mathrm{spur}(\Delta(g)\Delta(h)\Delta(h)^{-1}) = \mathrm{spur}(\Delta(h)) = \chi_\Delta(h).$$

Daher ist jeder Charakter eine Klassenfunktion.

3.3. Definition. Für $\varphi, \psi \in \mathrm{CF}(G, K)$ setzt man

$$(\varphi|\psi)_G := \frac{1}{|G|} \sum_{g \in G} \varphi(g)\psi(g^{-1}).$$

Bemerkung. Dann ist die Abbildung $\mathrm{CF}(G, K) \times \mathrm{CF}(G, K) \to K,\ (\varphi, \psi) \mapsto (\varphi|\psi)_G$ eine nichtausgeartete symmetrische Bilinearform.

Satz. *Für irreduzible Matrixdarstellungen Λ, Θ von G gilt:*
(i) $\Lambda \not\sim \Theta \ \Rightarrow\ (\chi_\Lambda|\chi_\Theta)_G = 0$.
(ii) Λ *absolut irreduzibel* $\Rightarrow\ (\chi_\Lambda|\chi_\Lambda)_G = 1$.

Beweis. Für $g \in G$ sei $\Lambda(g) = (\lambda_{ij}(g)),\ \Theta(g) = (\vartheta_{ij}(g))$, also $\chi_\Lambda(g) = \sum_i \lambda_{ii}(g),\ \chi_\Theta(g) = \sum_j \vartheta_{jj}(g)$. Nach 2.4 gilt also im Fall (i):

$$(\chi_\Lambda|\chi_\Theta)_G = \frac{1}{|G|} \sum_{g \in G} \sum_{i,j} \lambda_{ii}(g)\vartheta_{jj}(g^{-1}) = 0.$$

Im Fall (ii) gilt analog mit $n := \deg(\Lambda)$:

$$(\chi_\Lambda|\chi_\Lambda)_G = \frac{1}{|G|} \sum_{i,j} \sum_{g \in G} \lambda_{ii}(g)\lambda_{jj}(g^{-1}) = \frac{n}{|G|} \cdot \frac{|G|}{n} = 1.$$

□

3.4. Satz. *Sei $\Lambda : G \to \mathrm{GL}(n, K)$ eine Matrixdarstellung, und sei $\Lambda \sim \Lambda_1 \oplus \ldots \oplus \Lambda_k$ mit (nicht notwendig verschiedenen) irreduziblen Matrixdarstellungen $\Lambda_1, \ldots, \Lambda_k$ von G. Mit $m := |\{i : 1 \le i \le k,\ \Lambda_i \sim \Lambda_1\}|$ gilt dann:*

$$(\chi_\Lambda|\chi_{\Lambda_1})_G = m(\chi_{\Lambda_1}|\chi_{\Lambda_1})_G.$$

Beweis. Beispiel 3.1 und Satz 3.3. □

Bemerkung. Stets ist $(\chi_{\Lambda_1}|\chi_{\Lambda_1})_G \neq 0$; dies folgt z.B. aus 3.3 nach Übergang zum algebraischen Abschluß $\overline{K}$ von K. Daher kann man den Satz auch in der Form $m = \frac{(\chi_\Lambda|\chi_{\Lambda_1})_G}{(\chi_{\Lambda_1}|\chi_{\Lambda_1})_G}$ schreiben. Die Anzahl m der zu Λ_1 ähnlichen *irreduziblen Bestandteile* Λ_1 von Λ ist also durch χ_Λ bestimmt; insbesondere hängt m nicht von der Wahl der Zerlegung $\Lambda \sim \Lambda_1 \oplus \ldots \oplus \Lambda_k$ ab. Man nennt m die *Vielfachheit* des irreduziblen Bestandteils Λ_1 von Λ.

Beispiel. G operiere auf einer endlichen Menge Ω mit Permutationscharakter π. In der Gruppentheorie haben wir bewiesen, daß für die Anzahl n der Bahnen gilt: $n = \frac{1}{|G|} \sum_{g \in G} \pi(g)$. Dies kann man auch in der Form $n = (\pi|1_G)_G$ schreiben. Daher ist n die Anzahl der trivialen irreduziblen Bestandteile der Darstellung zu π.

3.5. Satz. *Zwei Darstellungen von G über K sind genau dann ähnlich, wenn sie den gleichen Charakter haben.*

Beweis. Dies folgt aus der obigen Bemerkung. □

Bemerkung. Der Satz bedeutet, daß Charaktere Darstellungen bis auf Ähnlichkeit charakterisieren. Daher verliert man in der Regel nicht viel, wenn man mit Charakteren statt mit Darstellungen rechnet. Dies werden wir häufig tun. Begriffe wie „treu“, „irreduzibel“, „Kern“ übertragen sich also von Darstellungen auf Charaktere.

3.6. Satz. *Für den regulären Charakter ρ und jeden Charakter χ von G gilt: $(\chi|\rho)_G = \chi(1)$.*

Beweis.

$$(\chi|\rho)_G = \frac{1}{|G|}\sum_{g\in G}\chi(g)\rho(g^{-1}) = \frac{1}{|G|}\chi(1)|G| = \chi(1).$$

□

Bemerkung. Jede irreduzible Darstellung Δ kommt also in der regulären Darstellung von G vor und zwar mit Vielfachheit $\frac{\chi_\Delta(1)}{(\chi_\Delta|\chi_\Delta)}$. Ist K Zerfällungskörper von G, so ist diese Vielfachheit gleich $\chi_\Delta(1)$.

3.7. Satz. *Sei K Zerfällungskörper von G und $L \supseteq K$ eine Körpererweiterung. Zu jeder Matrixdarstellung Δ von G über L existiert dann eine Matrixdarstellung Γ von G über K mit $\Delta \sim \Gamma^L$; insbesondere ist L Zerfällungskörper für G.*

Beweis. Seien $\Delta_1, \ldots, \Delta_r$ bis auf Ähnlichkeit alle irreduzible Matrixdarstellungen von G über K. Dann sind $\Delta_1^L, \ldots, \Delta_r^L$ irreduzibel. Nach 3.6 ist die reguläre Matrixdarstellung von G über K zu

$$\underbrace{\Delta_1 \oplus \ldots \oplus \Delta_1}_{\deg(\Delta_1)} \oplus \ldots \oplus \underbrace{\Delta_r \oplus \ldots \oplus \Delta_r}_{\deg(\Delta_r)}$$

ähnlich. Daher ist die reguläre Matrixdarstellung von G über L zu

$$\underbrace{\Delta_1^L \oplus \ldots \oplus \Delta_1^L}_{\deg(\Delta_1)} \oplus \ldots \oplus \underbrace{\Delta_r^L \oplus \ldots \oplus \Delta_r^L}_{\deg(\Delta_r)}$$

ähnlich. Nach 3.6 ist also jede irreduzible Matrixdarstellung von G über L zu einer der Matrixdarstellungen $\Delta_1^L, \ldots, \Delta_r^L$ ähnlich. □

Bemerkung. Darstellungen über Zerfällungskörper der Charakteristik 0 hängen also nicht wesentlich von der Wahl des Zerfällungskörper ab. Wir können und werden daher oft $K \subseteq \mathbb{C}$ annehmen.

3.8. Satz. *Sei K Zerfällungskörper für G, seien $\chi_1, \ldots, \chi_k$ die irreduziblen Charaktere von G, und sei ρ der reguläre Charakter von G. Dann gilt:*

(i) $(\chi_i|\chi_j)_G = \Delta_{ij}$ *für $i, j = 1, \ldots, k$.*
(ii) $\sum_{g\in G}\chi_i(g) = \begin{cases} |G| & \textit{falls } \chi_i = 1_G \\ 0 & \textit{sonst} \end{cases}$.
(iii) *Ist ϑ ein beliebiger Charakter von G und $\vartheta = \sum_{i=1}^k a_i\chi_i$ mit $a_i \in \mathbb{N}_0$ für $i = 1, \ldots, k$, so ist $(\vartheta|\chi_i)_G = a_i$ für $i = 1, \ldots, k$ und $(\vartheta|\vartheta)_G = \sum_{i=1}^k a_i^2$.*
(iv) *Jeder Charakter ϑ von G mit $(\vartheta|\vartheta)_G = 1$ ist irreduzibel.*
(v) $\rho = \sum_{i=1}^k \chi_i(1)\chi_i$.
(vi) $\sum_{i=1}^k \chi_i(1)^2 = |G|$.

Beweis.

(i) 3.3.
(ii) folgt aus (i) mit $\chi_j = 1_G$.
(iii) folgt aus (i).
(iv) folgt aus (iii).
(v) folgt aus 3.6.
(vi) Nach 3.6 und (iii) gilt: $|G| = \rho(1) = (\rho|\rho)_G = \sum_{i=1}^k \chi_i(1)^2$. □

Beispiel. G operiere transitiv auf einer endlichen Menge Ω mit Permutationscharakter π. Sei $\omega \in \Omega$ fest und $H := \mathrm{Stb}_G(\omega)$. In der Gruppentheorie haben wir gezeigt, daß für die Anzahl n der Bahnen von H auf Ω gilt: $n = \frac{1}{|G|}\sum_{g\in G}\pi(g)^2$. Dies können wir jetzt auch in der Form $n = (\pi|\pi)_G$ schreiben. Für G sind also äquivalent:

(1) G operiert 2-transitiv auf Ω.
(2) $n = 2$.
(3) $\pi = 1_G + \chi$ für einen irreduziblen Charakter $\chi \neq 1_G$ von G.

Auf diese Weise können wir manchmal irreduzible Charaktere konstruieren.

3.9. Satz. *Sei K ein Zerfällungskörper für G, seien $\Lambda_1, \dots, \Lambda_k$ bis auf Ähnlichkeit alle irreduziblen Matrixdarstellungen von G, und sei $\Lambda_l(g) = (\lambda^l_{ij}(g))$ für $l = 1, \dots, k$, $g \in G$. Dann bilden die Funktionen λ^l_{ij} $(i, j = 1, \dots, \deg(\Lambda_l),\ l = 1, \dots, k)$ eine Basis von $F(G, K)$.*

Beweis. Nach 3.8(vi) gibt es genau $\sum_{l=1}^k \deg(\Lambda_l)^2 = |G|$ Funktionen der Form λ^l_{ij}, und nach 2.5 sind diese linear unabhängig. □

KAPITEL 4

Konjugationsklassen

Sei G Gruppe, K Zerfällungskörper der Charakteristik 0 für G (also o.B.d.A. $\mathbb{Q} \subseteq K$), $\mathrm{Cl}(G)$ die Menge der Konjugationsklassen von G und $\mathrm{Irr}(G)$ die Menge der irreduziblen Charaktere von G über K.

4.1. Definition. Für $C \in \mathrm{Cl}(G)$ und jede Darstellung Δ von G mit Charakter χ setzt man

$$\omega_\Delta(C) := \omega_\chi(C) := \frac{|C|}{\chi(1)}\chi(g),$$

wobei $g \in C$ beliebig ist.

Satz. *Für $C \in \mathrm{Cl}(G)$ und jede irreduzible Matrixdarstellung $\Delta : G \to \mathrm{GL}(n, K)$ ist*

$$\sum_{g \in C} \Delta(g) = \omega_\Delta(C) 1_n.$$

Beweis. Mit $S := \sum_{g \in C} \Delta(g)$ ist $\Delta(h) S \Delta(h)^{-1} = S$ für $h \in G$, d.h. $S \in C(\Delta) = K 1_n$, etwa $S = s 1_n$ mit $s \in K$. Folglich ist $s \cdot \chi_\Delta(1) = \mathrm{spur}(S) = |C| \chi_\Delta(g)$ für $g \in C$. □

4.2. Bemerkung. Für $C, D, E \in \mathrm{Cl}(G)$ und $x, y \in E$ ist $|\{(c,d) \in C \times D : cd = x\}| = |\{(c,d) \in C \times D : cd = y\}|$; ist nämlich $h \in G$ mit $y = hxh^{-1}$, so liefert die Abbildung $(c,d) \mapsto (hch^{-1}, hdh^{-1})$ eine Bijektion zwischen diesen beiden Mengen. Wir setzen

$$a_{CDE} := |\{(c,d) \in C \times D : cd = x\}| \qquad \text{für } x \in E.$$

Im Fall $E = \{1\}$ ist also

$$a_{CDE} = \begin{cases} 0 & \text{falls } D \neq C^{-1} \\ |C| & \text{falls } D = C^{-1} \end{cases}.$$

Satz. *Mit den obigen Bezeichnungen gilt für jede irreduzible Darstellung Δ von G über K:*

$$\omega_\Delta(C)\, \omega_\Delta(D) = \sum_{E \in \mathrm{Cl}(G)} a_{CDE} \omega_\Delta(E).$$

Beweis. Nach 4.1 ist

$$\omega_\Delta(C)\, \omega_\Delta(D) 1_n = \left(\sum_{c \in C} \Delta(c) \right) \left(\sum_{d \in D} \Delta(d) \right) = \sum_{\substack{c \in C \\ d \in D}} \Delta(cd) = \sum_{E \in \mathrm{Cl}(G)} \Bigg(a_{CDE} \underbrace{\sum_{e \in E} \Delta(e)}_{= \omega_\Delta(E) \cdot 1_n} \Bigg).$$

□

4.3. Satz (Zweite Orthogonalitätsrelation)**.** *Für $g, h \in G$ gilt:*

$$\sum_{\chi \in \mathrm{Irr}(G)} \chi(g) \chi(h^{-1}) = \begin{cases} 0 & \text{, falls } g, h \text{ nicht konjugiert in } G \\ |C_G(g)| & \text{, sonst} \end{cases}.$$

Beweis. Seien C, D die Konjugationsklassen von g bzw. h^{-1}. Für $\chi \in \mathrm{Irr}(G)$ gilt dann nach 4.2:

$$\left(\frac{|C|}{\chi(1)} \chi(g) \right) \left(\frac{|D|}{\chi(1)} \chi(h^{-1}) \right) = \sum_{E \in \mathrm{Cl}(G)} a_{CDE} \frac{1}{\chi(1)} \sum_{e \in E} \chi(e).$$

Wir multiplizieren mit $\chi(1)^2$, summieren über $\mathrm{Irr}(G)$ und erhalten:

$$|C||D| \sum_{\chi\in\mathrm{Irr}(G)} \chi(g)\chi(h^{-1}) = \sum_{E\in\mathrm{Cl}(G)} a_{CDE} \sum_{e\in E} \rho_G(e) = |G|a_{CD\{1\}} = |G||C|\delta_{CD^{-1}}.$$

Benutze $\frac{|G|}{|C_G(g)|} = |C|$ $(= |D|$, falls $C = D^{-1})$. □

Bemerkung. Die *erste Orthogonalitätsrelation* ist die zu 3.8(i) äquivalente Gleichung:

$$\frac{1}{|G|} \sum_{g\in G} \chi(g)\psi(g^{-1}) = \begin{cases} 1 & \text{für } \chi = \psi \\ 0 & \text{sonst} \end{cases} \qquad \text{für alle } \chi,\psi \in \mathrm{Irr}(G).$$

4.4. Satz. $\mathrm{Irr}(G)$ *ist eine Basis für* $\mathrm{CF}(G,K)$*; insbesondere ist* $|\mathrm{Irr}(G)| = |\mathrm{Cl}(G)|$.

Beweis. Nach 3.8(i) ist $\mathrm{Irr}(G)$ ein lineare unabhängige Teilmenge von $\mathrm{CF}(G,K)$; insbesondere ist $|\mathrm{Irr}(G)| \leq \dim \mathrm{CF}(G,K) = |\mathrm{Cl}(G)|$. Nach 4.3 ist andererseits

$$\frac{1}{|C_G(h)|} \sum_{\chi\in\mathrm{Irr}(G)} \chi(h^{-1})\chi$$

für $h \in G$ die charakteristische Funktion auf der Konjugationsklasse von h. Folglich ist $|\mathrm{Irr}(G)| \geq |\mathrm{Cl}(G)|$. □

Bemerkung. $\mathrm{Irr}(G)$ ist also eine Orthonormalbasis von $\mathrm{CF}(G,K)$ bzgl. $(\cdot|\cdot)_G$.

4.5. Bemerkung. Ein Element $\alpha \in K$ nennt man *ganz-algebraisch*, falls α Nullstelle eines normierten Polynoms mit Koeffizienten in $\mathbb{Z}$ ist. In der Algebra lernt man, daß die ganz-algebraischen Elemente einen Teilring R von K bilden mit $R \cap \mathbb{Q} = \mathbb{Z}$.

Beispiel. Jede n-te Einheitswurzel $\zeta \in K$ ist wegen $\zeta^n - 1 = 0$ ganz-algebraisch. Daher ist für $\chi \in \mathrm{Irr}(G)$ und $g \in G$ auch $\chi(g)$ ganz-algebraisch.

Satz. *Sei* $\mathrm{Cl}(G) = \{C_1,\ldots,C_k\}$ *und* $c_i \in C_i$ *für* $i = 1,\ldots,k$. *Für* $i,s,t = 1,\ldots,k$ *sei* $a_{ist} := |\{(g,h) \in C_i \times C_s : gh = c_t\}|$ *und* $A_i := (a_{ist})_{s,t=1}^k$. *Für* $i = 1,\ldots,k$ *und* $\chi \in \mathrm{Irr}(G)$ *ist* $\omega_\chi(c_i)$ *Eigenwert von* A_i*; insbesondere ist* $\omega_\chi(c_i)$ *ganz-algebraisch.*

Beweis. Nach 4.2 gilt für $i,j = 1,\ldots,k,\ \chi \in \mathrm{Irr}(G)$:

$$\sum_{s=1}^k (a_{ijs} - \omega_\chi(c_i)\delta_{js})\,\omega_\chi(c_s) = 0.$$

Daher ist für festes i der Vektor $(\omega_\chi(c_1),\ldots,\omega_\chi(c_k))$ Lösung des homogenen linearen Gleichungssystems mit Koeffizientenmatrix $(a_{ijs} - \omega_\chi(c_i)\delta_{js})_{js}$. Wegen $\omega_\chi(1) = 1 \neq 0$ ist diese Lösung nichttrivial. Also ist $\det(A_i - \omega_\chi(c_i)1_k) = 0$. □

4.6. Satz. *Für* $\chi \in \mathrm{Irr}(G)$ *gilt:* $\chi(1) \mid |G|$.

Beweis. Sei $\mathrm{Cl}(G) = \{C_1,\ldots,C_k\}$ und $c_i \in C_i$ für $i = 1,\ldots,k$. Dann ist

$$\frac{|G|}{\chi(1)} = \frac{1}{\chi(1)} \sum_{g\in G} \chi(g)\chi(g^{-1}) = \frac{1}{\chi(1)} \sum_{i=1}^k |C_i|\,\chi(c_i)\chi(c_i^{-1}) = \sum_{i=1}^k \omega_\chi(c_i)\chi(c_i^{-1})$$

ganz-algebraisch und in $\mathbb{Q}$, also in $\mathbb{Z}$. □

4.7. Definition. Sei $\mathrm{Irr}(G) = \{\chi_1,\ldots,\chi_k\}$, $\mathrm{Cl}(G) = \{C_1,\ldots,C_k\}$ und $g_i \in C_i$ für $i = 1,\ldots,n$. Dann nennt man die Matrix $(\chi_i(g_j))_{i,j=1}^k$ die *Charaktertafel* von G.

Bemerkung.

(i) Die Charaktertafel hängt natürlich ab von der Reihenfolge von $\chi_1,\ldots,\chi_k$ und $C_1,\ldots,C_k$.

(ii) Die Charaktertafel einer abelschen Gruppe G ist leicht zu bestimmen. Es ist $|\operatorname{Irr}(G)| = |\operatorname{Cl}(G)| = |G|$. Jeder irreduzible Charakter hat Grad 1, und jedes $\chi \in \operatorname{Irr}(G)$ ist ein Homomorphismus $G \to K^\times$.

Beispiel.

(i) $G = \langle g \rangle$ zyklisch der Ordnung 2.

	1	g
χ_1	1	1
χ_2	1	-1

(ii) $G = \langle g \rangle$ zyklisch der Ordnung 3.

	1	g	g^2
χ_1	1	1	1
χ_2	1	ζ	ζ^2
χ_3	1	ζ^2	ζ

Dabei ist $\zeta \in K$ mit $\zeta^3 = 1 \neq \zeta$, also z.B. $\zeta = e^{2\pi i/3} = -\frac{1}{2} + \frac{1}{3}\sqrt{-3} \in \mathbb{C}$.

(iii) $G = \langle g \rangle$ zyklisch der Ordnung 4.

	1	g	g^2	g^3
χ_1	1	1	1	1
χ_2	1	-1	1	-1
χ_3	1	i	-1	$-i$
χ_4	1	$-i$	-1	i

(iv) $G = \langle g, h \rangle$ Kleinsche Vierergruppe.

	1	g	h	gh
χ_1	1	1	1	1
χ_2	1	1	-1	-1
χ_3	1	-1	1	-1
χ_4	1	-1	-1	1

4.8. Bemerkung. Elemente der Form $[x, y] := xyx^{-1}y^{-1}$ nennt man *Kommutatoren*. Die von allen Kommutatoren erzeugte Untergruppe G' von G ist ein Normalteiler in G mit abelscher Faktorgruppe G/G'. Man nennt G' die *Kommutatorgruppe* von G.

Satz. *G besitzt genau $|G/G'|$ Charaktere vom Grad 1. Diese sind genau die Inflationen der irreduziblen Charaktere von G/G'.*

Beweis. Da $\operatorname{GL}(1, K) \cong K^\times$ abelsch ist, ist $\Delta(xyx^{-1}y^{-1}) = \Delta(x)\Delta(y)\Delta(x)^{-1}\Delta(y)^{-1} = 1$ für $x, y \in G$ und jede Matrixdarstellung Δ vom Grad 1. Also ist $G' \subseteq \operatorname{Ker}(\Delta)$, und Δ induziert eine Matrixdarstellung $\overline{\Delta} : G/G' \to \operatorname{GL}(1, K)$, $gG' \mapsto \Delta(g)$. Umgekehrt liefert jede irreduzible Matrixdarstellung von G/G' nach Komposition mit dem natürlichen Epimorphismus $G \to G/G'$ eine irreduzible Matrixdarstellung von G. $\square$

Beispiel.

(i) Die symmetrische Gruppe $\operatorname{Sym}(3)$ der Ordnung 6 hat genau 3 Konjugationsklassen. Diese werden z.B. repräsentiert durch die Elemente $(1), (1,2), (1,2,3)$. Bekanntlich ist $G' = \langle (1,2,3) \rangle$, also $|G/G'| = 2$. Dies liefert den folgenden Teil der Charaktertafel:

	(1)	$(1,2)$	$(1,2,3)$
χ_1	1	1	1
χ_2	1	-1	1
χ_3			

Aus der Formel $\sum_{i=1}^{3}\chi_i(1)^2 = |G| = 6$ ergibt sich $\chi_3(1) = 2$. Wegen $0 = \sum_{i=1}^{3}\chi_i(1)\chi_i(1,2)$ ist $\chi_3(1,2) = 0$. Wegen $0 = \sum_{i=1}^{3}\chi_i(1)\chi_i(1,2,3)$ ist $\chi_3(1,2,3) = -1$. Insgesamt ergibt sich:

	(1)	$(1,2)$	$(1,2,3)$
χ_1	1	1	1
χ_2	1	-1	1
χ_3	2	0	-1

(ii) Die alternierende Gruppe $G = \mathrm{Alt}(4)$ der Ordnung 12 hat genau 4 Konjugationsklassen. Diese werden z.B. repräsentiert durch $(1),(1,2,3),(1,3,2),(1,2)(3,4)$. Bekanntlich hat $G' = \langle(1,2)(3,4),(1,3)(2,4)\rangle$ Ordnung 4, also $|G/G'| = 3$. Wie in (i) erhält man den Rest der Charaktertafel:

	(1)	$(1,2,3)$	$(1,3,2)$	$(1,2)(3,4)$
χ_1	1	1	1	1
χ_2	1	ζ	ζ^2	1
χ_3	1	ζ^2	ζ	1
χ_4	3	0	0	-1

4.9. Bemerkung. Für Homomorphismen $\lambda,\mu : G \to K^\times$ ist auch $\lambda\mu : G \to K^\times,\ g \mapsto \lambda(g)\mu(g)$ ein Homomorphismus. Daher bilden die Homomorphismen $G \to K^\times$ eine abelsche Gruppe $\hat{G}$. Für $\chi,\psi \in \mathrm{Irr}(G)$ ist $\chi\psi$ ein Charakter von G nach Beispiel 3.1, aber nicht unbedingt irreduzibel. Für $\lambda \in \hat{G}$ ist jedoch $\lambda\chi$ irreduzibel wegen

$$(\lambda\chi|\lambda\chi)_G = \frac{1}{|G|}\sum_{g\in G}\lambda(g)\chi(g)\lambda(g^{-1})\chi(g^{-1}) = \frac{1}{|G|}\sum_{g\in G}\chi(g)\chi(g^{-1}) = (\chi|\chi)_G = 1.$$

Daher operiert $\hat{G}$ auf $\mathrm{Irr}(G)$ durch Multiplikation.

Beispiel. Die symmetrische Gruppe $\mathrm{Sym}(4)$ der Ordnung 24 hat 5 Konjugationsklassen. Diese werden z.B. repräsentiert durch $(1),(1,2),(1,2,3),(1,2,3,4),(1,2)(3,4)$. Bekanntlich besitzt G einen Normalteiler V_4 der Ordnung 4, nämlich $V_4 = \langle(1,2)(3,4),(1,3)(2,4)\rangle$, und $G/V_4 \cong \mathrm{Sym}(3)$. Jeder irreduzible Charakter von $\mathrm{Sym}(3)$ liefert durch Inflation einen irreduziblen Charakter von $\mathrm{Sym}(4)$. Dies ergibt den folgenden Teil der Charaktertafel:

	(1)	$(1,2)$	$(1,2,3)$	$(1,2,3,4)$	$(1,2)(3,4)$
χ_1	1	1	1	1	1
χ_2	1	-1	1	-1	1
χ_3	2	0	-1	0	2
χ_4					
χ_5					

Zur Berechnung weiterer irreduzibler Charakter ziehen wir den Permutationscharakter π zur natürlichen Operation von G auf $\{1,2,3,4\}$ heran. Die Werte von π sind $4,2,1,0,0$. Wir wissen bereits, daß π nicht irreduzibel ist, sondern einen trivialen Bestandteil hat (Beispiel 1.4). Daher ist $\pi - 1_G$ wieder ein Charakter mit Werten $3,1,0,-1,-1$. Da G 2-transitiv auf $\{1,2,3,4\}$ operiert, ist $\pi - 1_G$ nach 3.8 irreduzibel; dies bestätigt auch die Rechnung:

$$(\pi - 1_G|\pi - 1_G)_G = \frac{1}{24}(9 + 6\cdot 1 + 6\cdot 1 + 3\cdot 1) = 1.$$

Wir setzen $\chi_4 := \pi - 1_G$. Dann ist $\chi_5 := \chi_2\chi_4$ ein weiterer irreduzibler Charakter (, den man auch mit früheren Methoden erhalten kann). Insgesamt ergibt sich:

	(1)	$(1,2)$	$(1,2,3)$	$(1,2,3,4)$	$(1,2)(3,4)$
χ_1	1	1	1	1	1
χ_2	1	-1	1	-1	1
χ_3	2	0	-1	0	2
χ_4	3	1	0	-1	-1
χ_5	3	-1	0	1	-1

4.10. Satz. *Sei* $\mathrm{Cl}(G) = \{C_1, \dots, C_k\}$ *und* $x_i \in C_i$ *für* $i = 1, \dots, k$. *Dann gilt für* $h, i, j = 1, \dots, k$:

$$a_{hij} := |\{(c,d) \in C_h \times C_i : cd = x_j\}| = \frac{|C_h| \cdot |C_i|}{|G|} \sum_{\chi \in \mathrm{Irr}(G)} \frac{\chi(x_h)\chi(x_i)\chi(x_j^{-1})}{\chi(1)}.$$

Beweis. Nach 4.2 ist

$$\frac{|C_h|\chi(x_h)}{\chi(1)} \frac{|C_i|\chi(x_i)}{\chi(1)} = \sum_{r=1}^{k} a_{hir} \frac{|C_r|\chi(x_r)}{\chi(1)}$$

für $\chi \in \mathrm{Irr}(G)$. Diese Gleichung multiplizieren wir mit $\chi(x_j^{-1})$ und summieren über alle $\chi \in \mathrm{Irr}(G)$. Aus der zweiten Orthogonalitätsrelation ergibt sich die Behauptung. $\square$

KAPITEL 5

Kern und Zentrum

Sei G Gruppe und K Zerfällungskörper der Charakteristik 0 für G (z.B. $K = \mathbb{C}$).

5.1. Satz. *Sei $K \subseteq \mathbb{C}$, Δ Darstellung von G mit Charakter χ und $g \in G$. Dann gilt:*

(i) $|\chi(g)| \le \chi(1)$.
(ii) $|\chi(g)| = \chi(1) \iff \Delta(g) \in K^\times \operatorname{id}$.
(iii) $\chi(g) = \chi(1) \iff g \in \operatorname{Ker}(\Delta)$.

Beweis. Die Eigenwerte von $\Delta(g)$ sind Einheitswurzeln $\varepsilon_1, \ldots, \varepsilon_n \in \mathbb{C}$, wobei $n = \chi(1)$. Daher ist

$$|\chi(g)| = |\varepsilon_1 + \ldots + \varepsilon_n| \le |\varepsilon_1| + \ldots + |\varepsilon_n| = n = \chi(1).$$

Im Fall $|\chi(g)| = \chi(1)$ ergibt sich $\varepsilon_1 = \ldots = \varepsilon_n$. Folglich ist $\Delta(g) = \varepsilon_1 \operatorname{id}$. Im Fall $\chi(g) = \chi(1)$ folgt $\varepsilon_1 = 1$, also $\Delta(g) = \operatorname{id}$. $\square$

Definition. Man nennt $Z(\Delta) := Z(\chi) := \{g \in G : |\chi(g)| = \chi(1)\}$ das *Zentrum* von Δ bzw. χ.

Bemerkung. Bekanntlich ist $K^\times \operatorname{id} = Z(\operatorname{GL}(V)) \trianglelefteq \operatorname{GL}(V)$ für den entsprechenden K-Vektorraum V. Daher ist $Z(\chi) = \Delta^{-1}(K^\times \operatorname{id}) \trianglelefteq G$ und $\operatorname{Ker}(\chi) \subseteq Z(\chi)$. Ferner ist $Z(\chi)/\operatorname{Ker}(\chi)$ zu einer Untergruppe von $K^\times$ isomorph, also zyklisch, und $Z(\chi)/\operatorname{Ker}(\chi) \subseteq Z(G/\operatorname{Ker}(\chi))$. Ist χ irreduzibel, so ist umgekehrt $Z(G/\operatorname{Ker}(\chi)) \subseteq Z(\chi)/\operatorname{Ker}(\chi)$. Auf diese Weise kann man häufig Normalteiler konstruieren.

5.2. Satz. *Sei $\chi \in \operatorname{Irr}(G)$, $C \in \operatorname{Cl}(G)$ und $g \in C$ mit $\operatorname{ggT}(\chi(1), |C|) = 1$. Dann ist $g \in Z(\chi)$ oder $\chi(g) = 0$.*

Beweis. Sei $n := |G|$, L der Zerfällungskörper des Polynoms $X^n - 1$ über $\mathbb{Q}$, $\Gamma := \operatorname{Gal}(L|\mathbb{Q})$, o.B.d.A. $K \subseteq \mathbb{C}$ und $\alpha := \frac{\chi(g)}{\chi(1)}$, also $\alpha \in L$. Wegen $\operatorname{ggT}(\chi(1), |C|) = 1$ existieren $u, v \in \mathbb{Z}$ mit $u\chi(1) + v|C| = 1$. Mit $\omega_\chi(C)$ und $\chi(g)$ sind auch

$$\alpha - u\chi(g) = \frac{\chi(g)}{\chi(1)}(1 - u\chi(1)) = v\frac{|C|\chi(g)}{\chi(1)} = v\omega_\chi(C)$$

und α ganz-algebraisch. Mit α ist auch $\sigma(\alpha)$ ganz-algebraisch für $\sigma \in \Gamma$. Daher ist auch $\beta := \prod_{\sigma \in \Gamma} \sigma(\alpha)$ ganz-algebraisch. Wegen $\sigma(\beta) = \beta$ für $\beta \in \Gamma$ ist $\beta \in \mathbb{Q}$ (Galoistheorie). Also ist $\beta \in \mathbb{Z}$. Im Fall $g \notin Z(\chi)$ ist $|\alpha| < 1$. Mit $\chi(g)$ ist auch $\sigma(\chi(g))$ eine Summe von $\chi(1)$ n-ten Einheitswurzeln in L. Daher ist $|\sigma(\chi(g))| \le \chi(1)$ und $|\sigma(\alpha)| \le 1$ für $\sigma \in \Gamma$. Folglich ist $|\beta| < 1$, d.h. $\beta = 0$. Also ist $\alpha = 0$ und $\chi(g) = 0$. $\square$

5.3. Satz. *Sei G einfach und nichtabelsch, $C \in \operatorname{Cl}(G)$ und $|C|$ Potenz einer Primzahl p. Dann ist $C = \{1\}$.*

Beweis. Wir nehmen $C \neq \{1\}$ an und wählen $g \in C \setminus \{1\}$, $\chi \in \operatorname{Irr}(G) \setminus \{1_G\}$. Da G einfach ist, ist $\operatorname{Ker}(\chi) = 1$. Da G nichtabelsch ist, ist auch $Z(\chi) = 1$. Im Fall $p \nmid \chi(1)$ ist also $\chi(g) = 0$ nach 5.2. Daher ist

$$0 = \sum_{\chi \in \operatorname{Irr}(G)} \chi(1)\chi(g) = 1 + p\alpha \qquad \text{mit } \alpha = \sum_{\substack{\chi \in \operatorname{Irr}(G) \\ p \mid \chi(1)}} \frac{\chi(1)}{p}\chi(g).$$

Dann ist $\alpha = -\frac{1}{p} \in \mathbb{Q} \setminus \mathbb{Z}$ ganz-algebraisch. Widerspruch. $\square$

5.4. Satz (Burnside). *Sei* $|G| = p^a q^b$ *mit Primzahlen* p, q *und* $a, b \in \mathbb{N}_0$. *Dann ist* G *auflösbar.*

Beweis. (Induktion nach $|G|$) O.B.d.A. sei $G \neq 1$. Sei N maximaler Normalteiler von G. Ist $N \neq 1$, so sind N und G/N nach Induktion auflösbar, also auch G. Daher sei $N = 1$, d.h. G ist einfach und o.B.d.A. nichtabelsch. Sei $P \neq 1$ eine Sylowgruppe von G, $g \in Z(P) \setminus \{1\}$ und C die Konjugationsklasse von g. Dann ist $|C| = |G : C_G(g)|$ Primzahlpotenz. Nach 5.3 ist $C = \{1\}$. Widerspruch. □

5.5. Satz. *Sei* G *einfach,* $\chi \in \mathrm{Irr}(G)$ *und* $\chi(1) = p$ *Primzahl. Dann hat jede* p*-Sylowgruppe* P *von* G *die Ordnung* p.

Beweis. Da G einfach ist, ist $\mathrm{Ker}(\chi) = 1$.
Annahme: P ist nichtabelsch, d.h. $P' \neq 1$. Wegen $P' \not\subseteq \mathrm{Ker}(\chi)$ kann die Einschränkung von χ auf P keine Summe von lauter Charakteren vom Grad 1 sein. Da die Grade der irreduziblen Charaktere von P Potenzen von p sind, muß also diese Einschränkung irreduzibel sein, und $1 \neq Z(P) \subseteq Z(\chi) \trianglelefteq G$. Widerspruch.
Also ist P abelsch. Für $g \in P \setminus \{1\}$ ist daher $\mathrm{ggT}(\chi(1), |G : C_G(g)|) = 1$. Folglich ist $g \in Z(\chi)$ oder $\chi(g) = 0$ nach 5.3. Da G einfach ist, folgt $\chi(g) = 0$. Daher ist die Einschränkung von χ auf P ein Vielfaches des regulären Charakters ρ_P. Insbesondere ist $|P| = \rho_P(1) \mid \chi(1)$. □

Bemerkung. Der Fall $p = 2$ kann hier nicht auftreten, da es keine nichtabelschen einfachen endlichen Gruppen mit einer 2-Sylowgruppe der Ordnung 2 gibt (Gruppentheorie).

5.6. Satz. *Für Gruppen* G, H *ist stets* $\mathrm{Irr}(G \times H) = \{\chi\psi : \chi \in \mathrm{Irr}(G),\ \psi \in \mathrm{Irr}(H)\}$.

Beweis. Für $\chi, \chi' \in \mathrm{Irr}(G),\ \psi, \psi' \in \mathrm{Irr}(H)$ sind $\chi\psi, \chi'\psi'$ Charaktere von $G \times H$ mit

$$(\chi\psi|\chi'\psi')_{G\times H} = \frac{1}{|G \times H|}\chi(g)\psi(h)\chi'(g^{-1})\psi'(h^{-1}) = (\chi|\chi')_G(\psi|\psi')_H = \delta_{\chi\chi'}\delta_{\psi\psi'}.$$

Auf diese Weise erhält man $|\mathrm{Irr}(G)| \cdot |\mathrm{Irr}(H)|$ verschiedene irreduzible Charaktere von $G \times H$. Wegen

$$\sum_{\substack{\chi\in\mathrm{Irr}(G)\\ \psi\in\mathrm{Irr}(H)}} \chi(1)^2\psi(1)^2 = |G| \cdot |H| = |G \times H|$$

gibt es keine weiteren. □

Bemerkung. Man kann 5.6 natürlich auf direkte Produkte endlich vieler Gruppen verallgemeinern.

5.7. Satz. *Für* $\chi \in \mathrm{Irr}(G)$ *ist* $\chi(1) \mid |G : Z(\chi)|$.

Beweis. Sei $\Delta : G \to \mathrm{GL}(n, K)$ eine irreduzible Matrixdarstellung mit Charakter χ und o.B.d.A. treu. Wir müssen $n \mid |G : Z(G)|$ zeigen. Für $z \in Z(G)$ ist $\Delta(z) \in C(\Delta) = K1_n$, also $\Delta(z) = \lambda(z)1_n$ für ein $\lambda(z) \in K^\times$. Auf diese Weise erhält man einen Homomorphismus $\lambda : Z(G) \to K^\times$. Für $m \in \mathbb{N}$ ist

$$\Delta_m := \underbrace{\Delta \oplus \ldots \oplus \Delta}_{m}$$

eine irreduzible Darstellung von G^m nach 5.6. Für $z_1, \ldots, z_m \in Z(G)$ ist dabei $\Delta_m(z_1, \ldots, z_m) = \lambda(z_1 \ldots z_m)1_{n^m}$. Offenbar ist $H := \{(z_1, \ldots, z_m) \in Z(G)^m : z_1 \ldots z_m = 1\} \trianglelefteq G^m$, $|H| = |Z(G)|^{m-1}$ und $H \subseteq \mathrm{Ker}(\Delta_m)$. Man kann also Δ_m als irreduzible Darstellung von G^m/H auffassen. Nach 4.6 ist

$$n^m \mid |G^m/H| = \frac{|G|^m}{|Z(G)|^{m-1}}.$$

Folglich ist

$$\left(\frac{|G : Z(G)|}{n}\right)^m \in \frac{1}{|Z(G)|}\mathbb{Z} \qquad \text{für alle } m \in \mathbb{N},$$

also $\frac{|G:Z(G)|}{n} \in \mathbb{Z}$. □

5.8. Satz. *Sei ϑ ein treuer Charakter von G, der genau r verschiedene Werte $a_1, \ldots, a_r$ annimmt. Dann tritt unter den irreduziblen Bestandteilen von $\vartheta^0 = 1_G, \vartheta, \vartheta^2, \ldots, \vartheta^{r-1}$ jeder irreduzible Charakter von G auf.*

Beweis. Sei $\chi \in \mathrm{Irr}(G)$ kein irreduzibler Bestandteil von $\vartheta^0, \vartheta, \ldots, \vartheta^{r-1}$, und sei $A_j := \{g \in G : \vartheta(g) = a_j\}$ für $j = 1, \ldots, r$. Dann ist

$$0 = |G|(\vartheta^s|\chi)_G = \sum_{g\in G} \vartheta^s(g)\chi(g^{-1}) = \sum_{j=1}^{r} a_j^s \sum_{g\in A_j} \chi(g^{-1})$$

für $s = 0, \ldots, r-1$. Daher ist $\left(\sum_{g\in A_1} \chi(g^{-1}), \ldots, \sum_{g\in A_r} \chi(g^{-1})\right)$ Lösung des homogenen Gleichungssystems mit der Koeffizientenmatrix

$$\begin{pmatrix} 1 & 1 & \cdots & 1 \\ a_1 & a_2 & \cdots & a_r \\ \vdots & \vdots & \ddots & \vdots \\ a_1^{r-1} & a_2^{r-1} & \cdots & a_r^{r-1} \end{pmatrix}.$$

Matrizen dieser Form (Vandermonde-Matrix) sind bekanntlich invertierbar. Folglich ist $\sum_{g\in A_j} \chi(g^{-1}) = 0$ für $j = 1, \ldots, r$. Sei $j \in \{1, \ldots, r\}$ mit $1 \in A_j$, also $a_j = \vartheta(1)$. Da ϑ treu ist, ist $A_j = \{1\}$, und man hat den Widerspruch $\chi(1) = 0$. $\square$

KAPITEL 6

Restriktion und Induktion

Sei K Zerfällungskörper der Charakteristik 0 für die im folgenden auftretenden Gruppen, sei G Gruppe und $H \leq G$.

6.1. Bemerkung. Für $\vartheta \in \mathrm{CF}(G, K)$ ist die *Einschränkung* oder *Restriktion* $\mathrm{Res}_H^G(\vartheta) : H \to K,\ g \mapsto \vartheta(g)$ eine Klassenfunktion auf H. Wir werden im folgenden umgekehrt zu jedem $\eta \in \mathrm{CF}(H, K)$ eine Klassenfunktion auf G definieren.

Satz. *Für $\eta \in \mathrm{CF}(H, K)$ ist die lineare Abbildung*

$$\mathrm{Ind}_H^G(\eta) : G \to K,\ x \mapsto \frac{1}{|H|} \sum_{\substack{y \in G \\ yxy^{-1} \in H}} \eta(yxy^{-1})$$

eine Klassenfunktion auf G.

Beweis. Für $x, y \in G$ ist

$$\sum_{\substack{y \in G \\ ygxg^{-1}y^{-1} \in H}} \eta(ygxg^{-1}y^{-1}) = \sum_{\substack{z \in G \\ zxz^{-1} \in H}} \eta(zxz^{-1}).$$

□

Definition. Man nennt $\mathrm{Ind}_H^G(\eta)$ die *Induktion* von η zu G.

6.2. Satz.

(i) *Für jede Untergruppe I von H und $\iota \in \mathrm{CF}(I, K)$ ist*

$$\mathrm{Ind}_H^G(\mathrm{Ind}_I^H(\iota)) = \mathrm{Ind}_I^G(\iota).$$

(ii) *Für $\vartheta \in \mathrm{CF}(G, K)$ und $\eta \in \mathrm{CF}(H, K)$ ist*

$$\vartheta \,\mathrm{Ind}_H^G(\eta) = \mathrm{Ind}_H^G(\mathrm{Res}_H^G(\vartheta)\eta).$$

(iii) *Für jede Untergruppe I von G und $\eta \in CF(H, K)$ ist*

$$\mathrm{Res}_I^G(\mathrm{Ind}_H^G(\eta)) = \sum_{IgH \in I\backslash G/H} \mathrm{Ind}_{I \cap {}^gH}^I(\mathrm{Res}_{I \cap {}^gH}^{{}^gH}({}^g\eta));$$

dabei ist $I \backslash G/H$ die Menge der Doppelnebenklassen IgH, und für $g \in G$ ist ${}^g\eta \in \mathrm{CF}({}^gH, K)$ definiert durch $({}^g\eta)({}^gh) = \eta(h)$ für $h \in H$.

Bemerkung. (ii) nennt man Frobenius-Formel und (iii) die Mackey-Formel.

Beweis.

(i) Für $x \in G$ ist

$$\begin{aligned}
(\mathrm{Ind}_H^G(\mathrm{Ind}_I^H(\iota)))(x) &= \frac{1}{|H|} \sum_{\substack{y \in G \\ yxy^{-1} \in H}} (\mathrm{Ind}_I^H(\iota))(yxy^{-1}) \\
&= \frac{1}{|H|}\frac{1}{|I|} \sum_{\substack{y \in G \\ yxy^{-1} \in H}} \sum_{\substack{z \in H \\ zyxy^{-1}z^{-1} \in I}} \iota(zyxy^{-1}z^{-1}) \\
&= \frac{1}{|H|}\frac{1}{|I|} \sum_{\substack{y \in G, z \in H \\ zyxy^{-1}z^{-1} \in I}} \iota(zyxy^{-1}z^{-1}) \\
&= \frac{1}{|H|}\frac{1}{|I|} \sum_{z \in H} \sum_{\substack{y \in G \\ zyxy^{-1}z^{-1} \in I}} \iota(zyxy^{-1}z^{-1}) \\
&= \frac{1}{|H|}\frac{1}{|I|} \sum_{z \in H} \sum_{\substack{w \in G \\ wxw^{-1} \in I}} \iota(wxw^{-1}) \\
&= \frac{1}{|I|} \sum_{\substack{w \in G \\ wxw^{-1} \in I}} \iota(wxw^{-1}) \\
&= (\mathrm{Ind}_I^G(\iota))(x).
\end{aligned}$$

(ii) Für $x \in G$ ist

$$\vartheta(x)\frac{1}{|H|} \sum_{\substack{y \in G \\ yxy^{-1} \in H}} \eta(yxy^{-1}) = \frac{1}{|H|} \sum_{\substack{y \in G \\ yxy^{-1} \in H}} \vartheta(yxy^{-1})\eta(yxy^{-1}).$$

(iii) Ist R ein Repräsentantensystem für $I\backslash G/H$ und S_r ein Repräsentantensystem für $I/I \cap^r H$ für $r \in R$, so ist

$$G = \dot{\bigcup_{r \in R}} \dot{\bigcup_{s \in S_r}} srH.$$

Folglich gilt für $x \in I$:

$$\begin{aligned}
(\mathrm{Ind}_H^G(\eta))(x) &= \frac{1}{|H|} \sum_{r \in R} \sum_{s \in S_r} \sum_{\substack{h \in H \\ h^{-1}r^{-1}s^{-1}xsrh \in H}} \eta(h^{-1}r^{-1}s^{-1}xsrh) \\
&= \sum_{r \in R} \sum_{\substack{s \in S_r \\ r^{-1}s^{-1}xsr \in H}} \eta(r^{-1}s^{-1}xsr) \\
&= \sum_{r \in R} \frac{1}{|I \cap^r H|} \sum_{\substack{s \in I \\ s^{-1}xs \in I \cap^r H}} {}^r\eta(s^{-1}xs) \\
&= \sum_{r \in R} \mathrm{Ind}_{I \cap^r H}^I(\mathrm{Res}_{I \cap^r H}^{^rH}({}^r\eta))(x).
\end{aligned}$$

$\square$

6.3. Bemerkung. Offenbar sind die Abbildungen $\mathrm{Res}_H^G : \mathrm{CF}(G, K) \to \mathrm{CF}(H, K)$ und $\mathrm{Ind}_H^G : \mathrm{CF}(H, K) \to \mathrm{CF}(G, K)$ linear. Der folgende Satz zeigt, daß Res_H^G und Ind_H^G zueinander adjungiert sind bzgl. der Bilinearform $(\cdot\,|\,\cdot)_G$ und $(\cdot\,|\,\cdot)_H$.

Satz (Frobenius-Reziprozität). *Für $\vartheta \in \mathrm{CF}(G,K)$ und $\eta \in \mathrm{CF}(H,K)$ ist $(\vartheta|\operatorname{Ind}_H^G(\eta))_G = (\operatorname{Res}_H^G(\vartheta)|\eta)_H$.*

Beweis.

$$\begin{aligned}(\vartheta|\operatorname{Ind}_H^G(\eta))_G &= \frac{1}{|G|}\frac{1}{|H|}\sum_{\substack{g\in G, h\in G\\ hg^{-1}h^{-1}\in H}} \vartheta(g)\eta(hg^{-1}h^{-1})\\ &= \frac{1}{|G|}\frac{1}{|H|}\sum_{\substack{g,h\in G\\ hg^{-1}h^{-1}\in H}} \vartheta(hgh^{-1})\eta(hg^{-1}h^{-1})\\ &= \frac{1}{|H|}\sum_{x\in H}\vartheta(x)\eta(x^{-1})\\ &= (\operatorname{Res}_H^G(\vartheta)|\eta)_H.\end{aligned}$$

□

6.4. Satz. *Für $\chi \in \operatorname{Irr}(G)$ sei*

$$\operatorname{Res}_H^G(\chi) = \sum_{\psi\in\operatorname{Irr}(H)} a_{\chi\psi}\psi$$

mit $a_{\chi\psi} \in \mathbb{N}_0$ für $\psi \in \operatorname{Irr}(H)$, und für $\psi \in \operatorname{Irr}(H)$ sei

$$\operatorname{Ind}_H^G(\psi) = \sum_{\chi\in\operatorname{Irr}(G)} b_{\chi\psi}\chi$$

mit $b_{\chi\psi} \in K$ für $\chi \in \operatorname{Irr}(G)$. Dann ist $b_{\chi\psi} = a_{\chi\psi} \in \mathbb{N}_0$ für $\chi \in \operatorname{Irr}(G), \psi \in \operatorname{Irr}(H)$.

Beweis. $b_{\chi\psi} = (\chi|\operatorname{Ind}_H^G(\psi))_G = (\operatorname{Res}_H^G(\chi)|\psi)_H = a_{\chi\psi}$. □

Bemerkung. Für jeden (irreduziblen) Charakter ψ von H ist also $\operatorname{Ind}_H^G(\psi)$ ein Charakter von G. In den Übungen werden wir sehen, wie man aus einer Darstellung Δ von H mit Charakter ψ eine Darstellung $\operatorname{Ind}_H^G(\Delta)$ von G mit Charakter $\operatorname{Ind}_H^G(\psi)$ macht. Man beachte: $(\operatorname{Ind}_H^G(\psi))(1) = |G:H|\psi(1)$.

Beispiel. $\operatorname{Ind}_H^G(1_H)$ ist der Permutationscharakter zur Operation von G auf G/H durch Linksmultiplikation. Für $x \in G$ ist nämlich

$$\begin{aligned}(\operatorname{Ind}_H^G(1_H))(x) &= \frac{1}{|H|}\sum_{\substack{y\in G\\ y^{-1}xy\in H}} 1_H(y^{-1}xy) = \frac{1}{|H|}|\{y\in G : y^{-1}xy \in H\}|\\ &= |\{yH \in G/H : xyH = yH\}|.\end{aligned}$$

Insbesondere ist also $\operatorname{Ind}_1^G(1)$ der reguläre Charakter von G.

6.5. Bemerkung. Für Untergruppen H, I von G, $\eta \in \mathrm{CF}(H,K)$ und $\iota \in \mathrm{CF}(I,K)$ ist

$$\begin{aligned}(\operatorname{Ind}_H^G(\eta)|\operatorname{Ind}_I^G(\iota))_G &= (\operatorname{Res}_I^G(\operatorname{Ind}_H^G(\eta))|\iota)_I\\ &= \sum_{IgH\in I\backslash G/H} (\operatorname{Ind}_{I\cap {}^gH}^I(\operatorname{Res}_{I\cap {}^gH}^{{}^gH}({}^g\eta))|\iota)_I\\ &= \sum_{IgH\in I\backslash G/H} (\operatorname{Res}_{I\cap {}^gH}^{{}^gH}({}^g\eta)|\operatorname{Res}_{I\cap {}^gH}^I(\iota))_{I\cap {}^gH}.\end{aligned}$$

Satz. *Für $\psi \in \operatorname{Irr}(H)$ gilt:*
$\operatorname{Ind}_H^G(\psi)$ ist irreduzibel $\iff$ Für alle $g \in G\setminus H$ ist $(\operatorname{Res}_{H\cap {}^gH}^{{}^gH}({}^g\psi)|\operatorname{Res}_{H\cap {}^gH}^H(\psi))_{H\cap {}^gH} = 0$.

Beweis. $\operatorname{Ind}_H^G(\psi)$ ist genau dann irreduzibel, wenn $(\operatorname{Ind}_H^G(\psi)|\operatorname{Ind}_H^G(\psi)) = 1$ ist. Der Summand oben für $g = 1$ ist $(\psi|\psi) = 1$. Also müssen alle anderen Summanden verschwinden. □

Beispiel. Für $H \trianglelefteq G$ und $\psi \in \mathrm{Irr}(H)$ gilt: $\mathrm{Ind}_H^G(\psi)$ irreduzibel $\iff$ $({}^g\psi|\psi)_H = 0$ für alle $g \in G\backslash H$ $\iff$ ${}^g\psi \neq \psi$ für alle $g \in G \setminus H$; denn mit ψ ist auch ${}^g\psi \in \mathrm{Irr}(H)$. Diese Aussage werden wir im folgenden verallgemeinern.

6.6. Bemerkung. Im Fall $H \trianglelefteq G$ ist die Abbildung $G \times \mathrm{Irr}(H) \to \mathrm{Irr}(H),\ (g,\psi) \mapsto {}^g\psi$ eine Gruppenoperation. Da Charaktere Klassenfunktionen sind, operiert dabei H trivial. (Folglich operiert G/H auf $\mathrm{Irr}(H)$ durch ${}^{gH}\psi := {}^g\psi$ für $g \in G$.) Den Stabilisator $\mathrm{Stb}_G(\psi)$ eines $\psi \in \mathrm{Irr}(H)$ bezeichnet man auch als *Trägheitsgruppe* von ψ in G. Offenbar ist $H \leq \mathrm{Stb}_G(\psi) \leq G$ und

$$\mathrm{Res}_H^G(\mathrm{Ind}_H^G(\psi)) = \sum_{gH \in G/H} {}^g\psi$$

nach Mackey. Bezeichnet R ein Repräsentantensystem für $G/\mathrm{Stb}_G(\psi)$, so kann man diese Gleichung auch in der Form

$$\mathrm{Res}_H^G(\mathrm{Ind}_H^G(\psi)) = |\mathrm{Stb}_G(\psi) : H| \sum_{g \in R} {}^g\psi$$

schreiben.

Satz. *Seien $H \trianglelefteq G$, $\chi \in \mathrm{Irr}(G)$ und $\psi \in \mathrm{Irr}(H)$ mit $e := (\mathrm{Res}_H^G(\chi)|\psi)_H \neq 0$. Dann ist*

$$\mathrm{Res}_H^G(\chi) \;=\; e \sum_{g\,\mathrm{Stb}_G(\psi) \in G/\mathrm{Stb}_G(\psi)} {}^g\psi.$$

Beweis. Wegen $0 \neq (\mathrm{Res}_H^G(\chi)|\psi)_H = (\chi|\mathrm{Ind}_H^G(\psi))_G$ bilden die irreduziblen Bestandteile von $\mathrm{Res}_H^G(\chi)$ eine Teilmenge der irreduziblen Bestandteile von $\mathrm{Res}_H^G(\mathrm{Ind}_H^G(\psi))$. Nach der obigen Bemerkung sind diese irreduziblen Bestandteile alle von der Form ${}^g\psi$ für ein $g \in G$. Für $g \in G$ ist aber offenbar $e := (\mathrm{Res}_H^G(\chi)|\psi)_H = (\mathrm{Res}_H^G(\chi)|{}^g\psi)_H$. □

Definition. Man nennt e den *Verzweigungsindex* von χ bzgl. H. Man kann zeigen, daß e stets ein Teiler von $|G : H|$ ist.

6.7. Definition. Für $\psi \in \mathrm{Irr}(H)$ setzt man $\mathrm{Irr}(G|\psi) := \{\chi \in \mathrm{Irr}(G) : (\mathrm{Res}_H^G(\chi)|\psi) \neq 0\}$.

Satz (Clifford). *Seien $H \trianglelefteq G$, $\psi \in \mathrm{Irr}(H)$ und $I := \mathrm{Stb}_G(\psi)$. Dann gilt:*

(i) *Für $\iota \in \mathrm{Irr}(I|\psi)$ ist $\mathrm{Ind}_I^G(\iota) \in \mathrm{Irr}(G|\psi)$.*
(ii) *Für $\chi \in \mathrm{Irr}(G|\psi)$ existiert genau ein $\iota \in \mathrm{Irr}(I|\psi)$ mit $(\mathrm{Res}_I^G(\chi)|\iota)_I \neq 0$.*
(iii) *Die Abbildungen in (i) und (ii) induzieren zueinander inverse Bijektionen zwischen $\mathrm{Irr}(I|\psi)$ und $\mathrm{Irr}(G|\psi)$; diese erhalten den Verzweigungsindex.*

Beweis.

(i) Für $\iota \in \mathrm{Irr}(I|\psi)$ existiert nach 6.6 ein $e \in \mathbb{N}$ mit $\mathrm{Res}_H^I(\iota) = e\psi$. Sei $\chi \in \mathrm{Irr}(G)$ mit $0 \neq (\chi|\mathrm{Ind}_I^G(\iota))_G = (\mathrm{Res}_I^G(\chi)|\iota)_I$. Dann ist also $(\mathrm{Res}_H^G(\chi)|\psi)_H \geq (\mathrm{Res}_H^I(\iota)|\psi)_H = e$. Für $g \in G$ ist also auch $(\mathrm{Res}_H^G(\chi)|{}^g\psi)_H \geq e$. Daher ist
$$\chi(1) \geq e \sum_{gI \in G/I} ({}^g\psi)(1) = e|G:I|\psi(1) = |G:I|\iota(1) = (\mathrm{Ind}_I^G(\iota))(1) \geq \chi(1).$$
Folglich ist $\mathrm{Ind}_I^G(\iota) = \chi \in \mathrm{Irr}(G|\psi)$ und $\mathrm{Res}_H^G(\chi) = e\sum_{gI \in G/I} {}^g\psi$.
(ii) Sei $\chi \in \mathrm{Irr}(G|\psi)$, also $\mathrm{Res}_H^G(\chi) = e\sum_{gI \in G/I} {}^g\psi$ für ein $e \in \mathbb{N}$. Dann existiert ein $\iota \in \mathrm{Irr}(I|\psi)$ mit $0 \neq (\mathrm{Res}_I^G(\chi)|\iota)_I = (\chi|\mathrm{Ind}_I^G(\iota))_G$. Nach (i) ist $\chi = \mathrm{Ind}_I^G(\iota)$ und $\mathrm{Res}_H^I(\iota) = e\psi$. Wegen $\mathrm{Res}_H^G(\chi) = e\sum_{gI \in G/I} {}^g\psi$ ist ι eindeutig bestimmt.
(iii) folgt aus den Beweisen von (i) und (ii). □

Bemerkung. Der obige Satz liefert ein Beispiel für ein sogenannte *Charakter-Korrespondenz*. Dabei geht es allgemein darum, gewisse irreduzible Charaktere einer Gruppe G zu gewissen irreduziblen Charakteren einer (i.a. kleineren) Gruppe H in Beziehung zu setzen. Ziel ist es, Aussagen über die beteiligten irreduziblen Charaktere von G auf Aussagen über die entsprechenden Charaktere von H zurückzuführen. Solche Charakter-Korrespondenzen spielen eine große Rolle in der Darstellungstheorie.

6.8. Definition. Einen irreduziblen Charakter χ von G nennt man *primitiv*, falls es keine echte Untergruppe H von G und keinen (irreduziblen) Charakter ψ von H mit $\chi = \mathrm{Ind}_H^G(\psi)$ gibt.

Satz. *Sei $\chi \in \mathrm{Irr}(G)$ treu und primitiv und A ein abelscher Normalteiler von G. Dann ist $A \subseteq Z(G)$.*

Beweis. Sei $\psi \in \mathrm{Irr}(A)$ mit $(\mathrm{Res}_A^G(\chi)|\psi)_A \neq 0$, d.h. $\chi \in \mathrm{Irr}(G|\psi)$, und sei $I := \mathrm{Stb}_G(\psi)$. Nach 6.7 existiert ein $\iota \in \mathrm{Irr}(I|\psi)$ mit $\chi = \mathrm{Ind}_I^G(\iota)$. Da χ primitiv ist, folgt $I = G$. Nach 6.6 ist also $\mathrm{Res}_A^G(\chi) = e\psi$ für ein $e \in \mathbb{N}$. Da A abelsch ist, ist $\psi(1) = 1$. Für $a \in A$ ist also $|\chi(a)| = e|\psi(a)| = e = \chi(1)$. Folglich ist $A \subseteq Z(\chi)$. Da χ treu ist, ist $Z(\chi) = Z(G)$. □

6.9. Satz. *Ist G nilpotent und $\chi \in \mathrm{Irr}(G)$, so existiert eine Untergruppe H von G und ein $\lambda \in \mathrm{Irr}(H)$ mit $\lambda(1) = 1$ und $\chi = \mathrm{Ind}_H^G(\lambda)$.*

Beweis. Sei G Gegenbeispiel minimaler Ordnung. Ist $N := \mathrm{Ker}(\chi) \neq 1$, so existiert genau ein $\overline{\chi} \in \mathrm{Irr}(G/N)$ mit $\chi = \mathrm{Inf}_N^G(\overline{\chi})$. Da G/N kein Gegenbeispiel ist, existiert eine Untergruppe H/N von G/N und ein $\overline{\lambda} \in \mathrm{Irr}(H/N)$ mit $\overline{\lambda}(1) = 1$ und $\overline{\chi} = \mathrm{Ind}_{H/N}^{G/N}(\overline{\lambda})$. Mit $\lambda := \mathrm{Inf}_N^H(\overline{\lambda})$ ist dann $\lambda(1) = 1$ und $\chi = \mathrm{Ind}_H^G(\lambda)$, und man hat einen Widerspruch.
Also ist χ treu. Ist χ nicht primitiv, so existiert eine echte Untergruppe U von G und ein $\varphi \in \mathrm{Irr}(U)$ mit $\chi = \mathrm{Ind}_U^G(\varphi)$. Da U kein Gegenbeispiel ist, existiert eine Untergruppe H von U und ein $\lambda \in \mathrm{Irr}(H)$ mit $\lambda(1) = 1$ und $\varphi = \mathrm{Ind}_H^U(\lambda)$. Dann ist aber auch $\chi = \mathrm{Ind}_H^G(\lambda)$, und wir haben einen Widerspruch.
Also ist χ primitiv. In der Gruppentheorie haben wir bewiesen, daß G einen Normalteiler A mit $C_G(A) = A$ enthält; insbesondere ist A abelsch. Nach 6.8 ist $G \subseteq C_G(A) = A$, also G abelsch und $\chi(1) = 1$. Widerspruch. □

KAPITEL 7

Induktionssätze

Sei G Gruppe. Wir betrachten Darstellungen über $\mathbb{C}$.

7.1. Bemerkung. G operiere auf der Menge Ω mit Permutationscharakter π. Seien $\Omega_1, \ldots, \Omega_n$ die Bahnen von G auf Ω, und für $i = 1, \ldots, n$ sei $\omega_i \in \Omega_i$ und $H_i := \mathrm{Stb}_G(\omega_i)$. Nach Beispiel 6.4 ist $\pi = \sum_{i=1}^n \mathrm{Ind}_{H_i}^G(1_{H_i})$.

Definition. Wir setzen $\mathrm{Per}(G) := \{\sum_{H \leq G} a_H \mathrm{Ind}_H^G(1_H) : a_H \in \mathbb{Z} \text{ für } H \leq G\}$.

Satz. $\mathrm{Per}(G)$ *ist ein Teilring von* $\mathrm{CF}(G, \mathbb{C})$ *mit* $1_G \in \mathrm{Per}(G)$.

Beweis. Offenbar ist $1_G \in \mathrm{Per}(G)$, und für $\varphi, \psi \in \mathrm{Per}(G)$ ist auch $\varphi \pm \psi \in \mathrm{Per}(G)$. Für Untergruppen H, I von G ist außerdem

$$\begin{aligned} \mathrm{Ind}_H^G(1_H)\,\mathrm{Ind}_I^G(1_I) &= \mathrm{Ind}_I^G(\mathrm{Res}_I^G(\mathrm{Ind}_H^G(1_H))1_I) \\ &= \mathrm{Ind}_I^G\Big(\sum_{IgH \in I\backslash G/H} \mathrm{Ind}_{I\cap gHg^{-1}}^I(\mathrm{Res}_{I\cap gHg^{-1}}^{gHg^{-1}}(1_{gHg^{-1}}))\Big) \\ &= \sum_{IgH \in I\backslash G/H} \mathrm{Ind}_{I\cap gHg^{-1}}^G(1_{I\cap gHg^{-1}}) \in \mathrm{Per}(G). \end{aligned}$$

□

7.2. Definition. Eine Gruppe H nennt man *p-quasielementar* für eine Primzahl p, falls H einen zyklischen Normalteiler N mit $p \nmid |N|$ besitzt, so daß H/N eine p-Gruppe ist. Man nennt H *quasielementar*, falls H p-quasielementar für eine Primzahl p ist.

Bemerkung. Man rechnet leicht nach, daß Untergruppen und Faktorgruppen von (p-)quasielementaren Gruppen wieder (p-)quasielementar sind.

Satz. *Zu jeder Primzahl p und jedem $x \in G$ existiert eine p-quasielementare Untergruppe H von G mit* $p \nmid (\mathrm{Ind}_H^G(1_H))(x)$.

Beweis. Wir schreiben $\langle x \rangle = P \times C$, wobei P die p-Sylowgruppe von $\langle x \rangle$ und C das eindeutig bestimmte Komplement von P in $\langle x \rangle$ ist. Dann ist $\langle x \rangle \subseteq N := N_G(C)$, und $\langle x \rangle / C$ ist eine p-Untergruppe von N/C. Wir wählen eine p-Sylowgruppe H/C von N/C. Dann ist H p-quasielementar, und $(\mathrm{Ind}_H^G(1_H))(x) = |\{gH \in G/H : xgH = gH\}|$. Ist $g \in G$ mit $xgH = gH$, so ist $g^{-1}xg \in H$ und daher $g^{-1}Cg \subseteq H$. Da H/C eine p-Gruppe ist, folgt daraus $g^{-1}Cg \subseteq C$, also $g \in N$. Daher ist $(\mathrm{Ind}_H^G(1_H))(x) = |\{gH \in N/H : xgH = gH\}|$. Für $g \in N$ ist aber $CgH = gCH = gH$. Daher operiert die Untergruppe C von $\langle x \rangle$ trivial durch Multiplikation auf N/H. Da $\langle x \rangle / C$ eine p-Gruppe ist, folgt

$$|\{gH \in N/H : xgH = gH\}| \equiv |N : H| \not\equiv 0 \pmod p.$$

□

7.3. Satz (L. Solomon)**.** *Es existieren ganze Zahlen b_H mit*

$$1_G = \sum_{\substack{H \leq G \\ H \text{ quasiel.}}} b_H \,\mathrm{Ind}_H^G(1_H).$$

Beweis. Analog zum Beweis von 7.1 zeigt man, daß

$$\operatorname{Per}'(G) := \{ \sum_{\substack{H \le G \\ H \text{ quasiel.}}} c_H \operatorname{Ind}_H^G(1_H) : c_H \in \mathbb{Z} \text{ für alle } H\}$$

Ideal in $\operatorname{Per}(G)$ ist. Für $x \in G$ ist daher $U_x := \{\pi(x) : \pi \in \operatorname{Per}'(G)\}$ eine Untergruppe von $(\mathbb{Z}, +)$. Nach 7.2 ist $U_x \nsubseteq p\mathbb{Z}$ für jede Primzahl p. Für $x \in G$ ist also $U_x = \mathbb{Z}$, d.h. es existiert ein $\pi_x \in \operatorname{Per}'(G)$ mit $\pi_x(x) = 1$. Dann ist $(1_G - \pi_x)(x) = 0$. Folglich ist $\prod_{x \in G}(1_G - \pi_x) = 0$. Nach Ausmultiplizieren erhält man eine Gleichung der gewünschten Form. □

7.4. Definition. Eine Gruppe H nennt man *p-elementar* für eine Primzahl p, falls sie direktes Produkt einer p-Gruppe mit einer zyklischen Gruppe ist. Ist H p-elementar für eine Primzahl p, so nennt man H *elementar*.

Bemerkung. Man unterscheide p-elementare Gruppen und elementarabelsche p-Gruppen! Offenbar sind Untergruppen und Faktorgruppen von (p-)elementaren Gruppen wieder (p-)elementar. Ferner sind elementare Gruppen stets nilpotent.

Satz. *Zu jedem $\chi \in \operatorname{Irr}(G)$ existieren ganze Zahlen $c_{H,\psi}$ mit*

$$\chi = \sum_{\substack{H \le G \\ H \text{ elem.}}} \sum_{\psi \in \operatorname{Irr}(H)} c_{H,\psi} \operatorname{Ind}_H^G(\psi).$$

Beweis. Sei G ein Gegenbeispiel minimaler Ordnung. Offenbar kann man $\chi = 1_G$ annehmen; denn eine Gleichung der gewünschten Form für 1_G liefert nach Multiplikation mit χ eine für χ. Nach 7.3 ist o.B.d.A. G p-quasielementar für eine Primzahl p. Es existiert also ein zyklischer Normalteiler C von G mit $p \nmid |C|$, so daß G/C eine p-Gruppe ist. Sei P eine p-Sylowgruppe von G, also $G = PC$ und $C \cap P = 1$. Offenbar ist G nicht elementar, also $Z := C_C(P) < C$ und $E := PZ < G$. Wegen $(\operatorname{Ind}_E^G(1_E)|1_G)_G = (1_E|1_E)_E = 1$ ist $\xi := \operatorname{Ind}_E^G(1_E) - 1_G$ ein Charakter von G. Nach Wahl von G besitzt ξ einen primitiven irreduziblen Bestandteil χ. Nach Mackey ist $1_C + \operatorname{Res}_C^G(\xi) = \operatorname{Res}_C^G(\operatorname{Ind}_E^G(1_E)) = \operatorname{Ind}_Z^C(1_Z)$. Daher ist

$$(1_C + \operatorname{Res}_C^G(\xi)|1_C)_C = (\operatorname{Ind}_Z^C(1_Z)|1_C)_C = (1_Z|1_Z)_Z = 1,$$

also $(\operatorname{Res}_C^G(\xi)|1_C)_C = 0$ und $(\operatorname{Res}_C^G(\chi)|1_C)_C = 0$. Sei $\lambda \in \operatorname{Irr}(C)$ mit $(\operatorname{Res}_C^G(\chi)|\lambda)_C \neq 0$, also $\lambda \neq 1_C$. Wegen $Z \trianglelefteq G$ ist $Z \subseteq \operatorname{Ker}(\operatorname{Ind}_E^G(1_E)) \subseteq \operatorname{Ker}(\chi)$ nach Mackey. Folglich ist $Z \subseteq N := \operatorname{Ker}(\lambda)$. Da χ primitiv ist, ist $\operatorname{Stb}_G(\lambda) = G$ nach Clifford. Offenbar ist λ konstant auf Nebenklassen von N. Da $\lambda : C \to \mathbb{C}^\times$ ein Homomorphismus ist, nimmt λ auf verschiedenen Nebenklassen nach N verschiedene Werte an. Für $x \in C$ und $y \in P$ ist aber $\lambda(y^{-1}xy) = \lambda(x)$, also $y^{-1}xy \in xN$. Folglich operiert P durch Konjugation auf xN. Wegen

$$|xN \cap C_C(P)| \equiv |xN| = |N| \not\equiv 0 \pmod p$$

ist $\emptyset \neq xN \cap Z \subseteq xN \cap N$, also $x \in N$. Folglich ist $C = N$ im Widerspruch zu $\lambda \neq 1_C$. □

7.5. Definition. Für jeden Teilring R von $\mathbb{C}$ setzen wir $R\operatorname{Irr}(G) := \{\sum_{\chi \in \operatorname{Irr}(G)} a_\chi \chi : a_\chi \in R \text{ für } \chi \in \operatorname{Irr}(G)\}$.

Bemerkung. $R\operatorname{Irr}(G)$ ist ein Teilring von $\operatorname{CF}(G, \mathbb{C})$.

Satz (R. Brauer). *Für ein Element $\varphi \in \operatorname{CF}(G, \mathbb{C})$ und einen Teilring R von $\mathbb{C}$ sind äquivalent:*

(1) *Es existieren Elemente $a_{H,\psi} \in R$ mit*

$$\varphi = \sum_{\substack{H \le G \\ H \text{ elem.}}} \sum_{\psi \in \operatorname{Irr}(H)} a_{H,\psi} \operatorname{Ind}_H^G(\psi).$$

(2) *Es existieren Elemente $b_{H,\lambda} \in R$ mit*

$$\varphi = \sum_{\substack{H \le G \\ H \text{ elem.}}} \sum_{\substack{\lambda \in \operatorname{Irr}(H) \\ \lambda(1) = 1}} b_{H,\lambda} \operatorname{Ind}_H^G(\lambda).$$

(3) $\varphi \in R\,\mathrm{Irr}(G)$.
(4) *Für jede elementare Untergruppe H von G ist* $\mathrm{Res}_H^G(\varphi) \in R\,\mathrm{Irr}(H)$.

Beweis.
(1)⇒(2): 6.9.
(2)⇒(3): Trivial.
(3)⇒(4): Trivial.
(4)⇒(1): Die Elemente $\vartheta \in \mathrm{CF}(G,\mathbb{C})$ mit $\mathrm{Res}_H^G(\vartheta) \in R\,\mathrm{Irr}(H)$ für jede elementare Untergruppe H von G bilden einen Teilring T von $\mathrm{CF}(G,\mathbb{C})$, und die Elemente der Form in (1) bilden ein Ideal I in T. Nach 7.4 ist $1_G \in I$, also $I = T$. □

7.6. Satz. *Eine Klassenfunktion χ auf G ist genau dann ein irreduzibler Charakter von G, wenn gilt:*
(i) $\mathrm{Res}_H^G(\chi) \in \mathbb{Z}\,\mathrm{Irr}(H)$ *für jede elementare Untergruppe H von G.*
(ii) $(\chi|\chi)_G = 1$.
(iii) $\chi(1) > 0$.

Beweis.
⇒: Klar.
⇐: $\chi \in \mathrm{CF}(G,\mathbb{C})$ erfülle (i), (ii) und (iii). Nach 7.5 und (i) ist $\chi \in \mathbb{Z}\,\mathrm{Irr}(G)$. Mit (ii) ergibt sich dann $\pm\chi \in \mathrm{Irr}(G)$, und aus (iii) folgt $\chi \in \mathrm{Irr}(G)$. □

Bemerkung. Mit diesem Kriterium werden wir häufig irreduzible Charaktere konstruieren.

Definition. Man nennt $\mathbb{Z}\,\mathrm{Irr}(G)$ den *Charakterring* von G und seine Elemente *verallgemeinerte* oder *virtuelle Charaktere.*

7.7. Satz. *Sei $\chi \in \mathrm{Irr}(G)$ und p Primzahl mit $p \nmid \frac{|G|}{\chi(1)}$. Dann ist $\chi(g) = 0$ für alle $g \in G$ mit $p \mid |\langle g\rangle|$.*

Beweis. Wir definieren eine Klassenfunktion ϑ auf G durch
$$\vartheta(g) := \begin{cases} \chi(g) & \text{im Fall } p \nmid |\langle g\rangle| \\ 0 & \text{sonst} \end{cases}.$$
Wir zeigen zunächst, daß ϑ ein verallgemeinerter Charakter ist. Dazu sei E eine elementare Untergruppe von G. Wir schreiben $E = P \times Q$, wobei P die p-Sylowgruppe von E ist. Jedes $x \in E$ mit $p \nmid |\langle x\rangle|$ liegt in Q. Daher ist $\vartheta(x) = 0$ für alle $x \in E \setminus Q$ und $\vartheta(x) = \chi(x)$ für $x \in Q$. Für $\psi \in \mathrm{Irr}(E)$ ist also
$$|E|(\mathrm{Res}_E^G(\vartheta)|\psi)_E = \sum_{x\in Q} \chi(x)\psi(x^{-1}) = |Q|(\mathrm{Res}_Q^G(\chi)|\,\mathrm{Res}_Q^E(\psi))_Q.$$
Daher ist $|P|(\mathrm{Res}_E^G(\vartheta)|\psi)_E \in \mathbb{Z}$. Sei $\omega = \omega_\chi$, $g \in G$, K die Konjugationsklasse von g in G und $\omega(g) := \omega(K) = \frac{|K|\chi(g)}{\chi(1)}$. Dann ist
$$\chi(g) = \frac{\omega(g)\chi(1)}{|K|} = \frac{\omega(g)\chi(1)|C_G(g)|}{|G|}.$$
Folglich ist
$$|E|(\mathrm{Res}_E^G(\vartheta)|\psi)_E = \sum_{x\in Q} \chi(x)\psi(x^{-1}) = \frac{\chi(1)}{|G|}\sum_{x\in Q}\omega(x)\psi(x^{-1})|C_G(x)|.$$
Für $x \in Q$ ist $P \subseteq C_G(x)$. Daher ist
$$\frac{|G|\cdot|Q|}{\chi(1)}(\mathrm{Res}_E^G(\vartheta)|\psi)_E = \sum_{x\in Q}\omega(x)\psi(x^{-1})|C_G(x):P|$$
eine ganz-algebraische Zahl in $\mathbb{Q}$. Folglich ist
$$\frac{|G|\cdot|Q|}{\chi(1)}(\mathrm{Res}_E^G(\vartheta)|\psi)_E \in \mathbb{Z}.$$

Wegen $\frac{|G|\cdot|Q|}{\chi(1)} \in \mathbb{Z}$ und $\mathrm{ggT}(\frac{|G|\cdot|Q|}{\chi(1)}, |P|) = 1$ ist auch $(\mathrm{Res}^G_E(\vartheta)|\psi)_E \in \mathbb{Z}$. Dies zeigt, daß $\mathrm{Res}^G_E(\vartheta)$ ein verallgemeinerter Charakter von E für jede elementare Untergruppe E von G ist. Nach Brauer ist $\vartheta \in \mathbb{Z}\,\mathrm{Irr}(G)$; insbesondere ist $(\vartheta|\chi)_G \in \mathbb{Z}$. Andererseits ist

$$0 < \frac{1}{|G|} \sum_{\substack{g\in G\\ p\nmid|\langle g\rangle|}} \chi(g)\overline{\chi(g))} = (\vartheta|\chi)_G \leq (\chi|\chi)_G = 1.$$

Daher ist $(\vartheta|\chi)_G = (\chi|\chi)_G = 1$ und

$$0 = (\chi - \vartheta|\chi)_G = \frac{1}{|G|} \sum_{\substack{g\in G\\ p||\langle g\rangle|}} \chi(g)\overline{\chi(g))},$$

d.h. $\chi(g) = 0$ für alle $g \in G$ mit $p \mid |\langle g\rangle|$. □

Definition. Für $\chi \in \mathrm{Irr}(G)$ und jede Primzahl p nennt man

$$\max\{a \in \mathbb{N}_0 : p^a \mid \frac{|G|}{\chi(1)}\}$$

den *p-Defekt* von χ.

Bemerkung. Der Satz betrifft also irreduzible Charaktere von p-Defekt 0. Es gibt eine Reihe offener Vermutungen über solche Charaktere. Zum Beispiel sagt eine Vermutung von Alperin-Knörr-Robinson, daß ihre Anzahl für jede Gruppe G gleich

$$\sum_{n\geq 0}(-1)^n \sum_{\substack{Q_1,\ldots,Q_n \ p\text{-Ugr. von } G\\ 1<Q_1<\ldots<Q_n}} \frac{|\,\mathrm{Irr}(N_G(Q_1)\cap\ldots\cap N_G(Q_n))|}{|G : N_G(Q_1)\cap\ldots\cap N_G(Q_n)|}$$

ist.

Beispiel. Sei $G = \mathrm{Sym}(3)$, also $|G| = 2\cdot 3$ und $\mathrm{Irr}(G) = \{\chi_1, \chi_2, \chi_3\}$ mit $\chi_1(1) = \chi_2(1) = 1$, $\chi_3(1) = 2$. Es gibt also genau einen irreduziblen Charakter mit 2-Defekt 0. Wir betrachten Ketten $1 < Q_1 < \ldots < Q_n$, ihre Normalisatoren und die entsprechenden Terme in der obigen Summe:

$n = 0:$	1	G	$\frac{3}{1}$
$n = 1:$	$1 < \langle(1,2)\rangle$	$\langle(1,2)\rangle$	$\frac{2}{3}$
	$1 < \langle(1,3)\rangle$	$\langle(1,3)\rangle$	$\frac{2}{3}$
	$1 < \langle(2,3)\rangle$	$\langle(2,3)\rangle$	$\frac{2}{3}$

Die Summe wird also zu $\frac{3}{1} - (\frac{2}{3} + \frac{2}{3} + \frac{2}{3}) = 3 - 2 = 1$.

7.8. Satz (R. Brauer). *Sei $n := \exp(G)$ und ζ eine primitive n-te Einheitswurzel in $\mathbb{C}$. Dann ist $\mathbb{Q}(\zeta)$ Zerfällungskörper für G.*

Beweis. Sei $\Lambda : G \to \mathrm{GL}(d, \mathbb{C})$ eine irreduzible Matrixdarstellung mit Charakter χ. Nach 2.6 genügt es zu zeigen, daß sich Λ über $F := \mathbb{Q}(\zeta)$ realisieren läßt. Nach 7.5 existieren Untergruppen $H_1, \ldots, H_k$ von G, $a_1, \ldots, a_k \in \{\pm 1\}$ und $\lambda_1 \in \mathrm{Irr}(H_1), \ldots, \lambda_k \in \mathrm{Irr}(H_k)$ mit $\lambda_1(1) = \ldots = \lambda_k(1) = 1$ und $\chi = \sum_{i=1}^k a_i \,\mathrm{Ind}^G_{H_i}(\lambda_i)$. Sei o.B.d.A. $a_1 = \ldots = a_l = 1$, $a_{l+1} = \ldots = a_k = -1$, also

$$\chi + \sum_{i=l+1}^k \mathrm{Ind}^G_{H_i}(\lambda_i) = \sum_{i=1}^l \mathrm{Ind}^G_{H_i}(\lambda_i).$$

Offenbar sind $\lambda_1, \ldots, \lambda_k$ über F realisierbar. In den Übungen haben wir gesehen, daß dann auch $\mathrm{Ind}^G_{H_1}(\lambda_1), \ldots, \mathrm{Ind}^G_{H_k}(\lambda_k)$ über F realisierbar sind. Es existieren also Matrixdarstellungen $\Delta_1 : G \to \mathrm{GL}(d_1, F)$, $\Delta_2 : G \to \mathrm{GL}(d_2, F)$ mit $\Lambda \oplus \Delta_1^{\mathbb{C}} \sim \Delta_2^{\mathbb{C}}$. Wir wählen dabei Δ_1, Δ_2 so, daß $\deg(\Delta_1)$ möglichst klein ist. Im Fall $\deg(\Delta_1) = 0$ sind wir fertig. Sei also $\deg(\Delta_1) > 0$ und Θ ein irreduzibler Bestandteil von Δ_1, etwa $\Delta_1 \sim \Theta \oplus \Delta_1'$. Dann ist

$$(\chi_{\Delta_2}|\chi_\Theta)_G \geq (\chi_{\Delta_1}|\chi_\Theta)_G > 0.$$

Daher ist Θ auch irreduzibler Bestandteil von Δ_2, etwa $\Delta_2 \sim \Theta \oplus \Delta_2'$. Aus 3.4 folgt dann $\Lambda \oplus {\Delta_1'}^{\mathbb{C}} \sim {\Delta_2'}^{\mathbb{C}}$ im Widerspruch zur Wahl von Δ_1. $\square$

KAPITEL 8

Normale Komplemente

Sei G Gruppe und K Zerfällungskörper der Charakteristik 0 für die im folgenden auftretenden Gruppen (z.B. $K = \mathbb{C}$).

8.1. Satz (Brauer-Dade). *Sei $N \trianglelefteq H \leq G$ und π eine Primzahlmenge mit folgenden Eigenschaften:*

(i) *H/N ist π-Gruppe.*
(ii) *$|G : H|$ ist durch keine Primzahl in π teilbar.*
(iii) *Sind $x, y \in H$ konjugiert in G, so sind xN, yN konjugiert in H/N.*
(iv) *Ist h ein π-Element in $H \setminus N$ und P eine p-Sylowgruppe von $C_G(h)$ für eine Primzahl $p \in \pi$ mit $p \not| \, |\langle h \rangle|$, so ist $\langle h \rangle P$ zu einer Untergruppe von H konjugiert.*

Dann existiert ein Normalteiler M von G mit $G = HM$ und $H \cap M = N$.

Definition. Man nennt M ein *(relatives) normales Komplement* zu H/N in G.

Bemerkung. Hat man die Existenz von M bereits bewiesen, so kann man $\mathrm{Irr}(G/M)$ aus $\mathrm{Irr}(H/N)$ und dem Isomorphismus $G/M = HM/M \cong H/H \cap M = H/N$ konstruieren. Im Beweis von 8.1 geht man umgekehrt vor und konstruiert zunächst die Inflation der Charaktere in $\mathrm{Irr}(G/M)$ und erhält M als Durchschnitt der Kerne dieser Charaktere.

Beweis. Sei $\mathrm{Cl}(H/N) = \{C_1, \ldots, C_k\}$ und $C_1 = \{1\}$. Für $i = 1, \ldots, k$ sei

$$B_i := \{h \in H : hN \in C_i\},$$

also $B_1 = N$ und $H = \bigcup_{i=1}^k B_i$. Jedes $g \in G$ hat eine eindeutige Zerlegung $g = g_\pi g_{\pi'} = g_{\pi'} g_\pi$, wobei g_π ein π-Element und $g_{\pi'}$ ein π'-Element ist. (Mit π' bezeichnen wir die Menge aller Primzahlen außerhalb von π.) Für $i = 2, \ldots, k$ sei

$$A_i := \{g \in G : g_\pi \text{ konjugiert zu einem Element in } B_i\}.$$

Mit $A_1 := G \setminus \bigcup_{i=2}^k A_i$ ist also $G = \bigcup_{i=1}^k A_i$.
Für $i = 1, \ldots, k$ ist A_i eine Vereinigung von Konjugationsklassen in G. Für $i \neq j$ ist dabei $A_i \cap A_j = \emptyset$: Sei nämlich $g \in A_i \cap A_j$ und o.B.d.A. $i \neq 1 \neq j$, dann ist g_π zu einem Element $h_i \in B_i$ und einem Element $h_j \in B_j$ konjugiert. Folglich existiert ein $x \in G$ mit $x h_i x^{-1} = h_j$. Wegen (iii) sind dann $h_i N$ und $h_j N$ in H/N konjugiert, d.h. $i = j$.
Für $i = 2, \ldots, k$ ist $B_i = A_i \cap H$: Ist nämlich $h = h_\pi h_{\pi'} \in B_i$, so ist $h_{\pi'} \in N$ nach (i), also $hN = h_\pi N$ und damit $h_\pi \in B_i$ und $h \in A_i \cap H$. Ist umgekehrt $h \in A_i \cap H$, so ist h_π konjugiert zu einem Element in B_i. Folglich ist $hN = h_\pi N \in C_i$ wegen (iii) und damit $h \in B_i$. Nach Definition ist $A_1 \cap H = H \setminus \bigcup_{i=2}^k (A_i \cap H) = H \setminus \bigcup_{i=2}^k B_i = B_1$. Also ist $A_i \cap H = B_i$ für $i = 1, \ldots, k$.
Für $p \in \pi$ enthält H wegen (ii) eine p-Sylowgruppe von G. Daher ist jedes p-Element $x \in G$ zu einem Element $y \in H$ konjugiert. Wir sagen, daß x im Fall $y \in H \setminus N$ vom Typ I und im Fall $y \in N$ vom Typ II ist. Nach (iii) ist x entweder vom Typ I oder vom Typ II, aber nicht beides. Für jedes $g \in G$ schreiben wir $g_\pi = \prod_{p \in \pi} g_p$, wobei g_p für $p \in \pi$ der p-Faktor von g ist, und setzen

$$\alpha(g) := \prod_{\substack{p \in \pi \\ g_p \text{ vom Typ I}}} g_p \qquad \text{und} \qquad \beta(g) := \prod_{\substack{p \in \pi \\ g_p \text{ vom Typ II}}} g_p.$$

Dann ist $g = \alpha(g)\beta(g)g_{\pi'}$.

Beh.: Für jedes $g \in G$ mit $\alpha(g) \neq 1$ ist g_π zu einem Element in $H \setminus N$ konjugiert.
Bew.: Ist g_π ein p-Element für eine Primzahl p, so ist g_π vom Typ I wegen $\alpha(g) \neq 1$, und wir sind fertig. Ist g_π kein p-Element, so wählen wir einen Primteiler p von $|\langle g_\pi \rangle|$ und schreiben $g_\pi = x g_p$ mit $x := g_{\pi \setminus \{p\}}$; wegen $\alpha(g) \neq 1$ können wir annehmen, daß g_q vom Typ I ist für ein $q \in \pi \setminus \{p\}$. Das bedeutet $\alpha(x) \neq 1$. Argumentieren wir durch Induktion nach der Anzahl der verschiedenen Primfaktoren von g_π, so können wir annehmen, daß x zu einem Element in $H \setminus N$ konjugiert ist. Indem wir g durch ein Konjugiertes ersetzen, können wir sogar $x \in H \setminus N$ annehmen. Sei P eine p-Sylowgruppe von $C_G(x)$ mit $g_p \in P$. Nach (iv) ist $\langle x \rangle P$ zu einer Untergruppe von H konjugiert; insbesondere ist $g_\pi = x g_p$ zu einem Element $h \in H$ konjugiert. Im Fall $h \in N$ wäre $h_q \in N$ für jeden Primteiler q von $|\langle h \rangle| = |\langle g_\pi \rangle|$. Dann wäre aber g_q vom Typ II für jedes solche q im Widerspruch zu $\alpha(g) \neq 1$. Also ist $h \notin N$, und die Behauptung ist bewiesen.
Es ist $A_1 = \{g \in G : \alpha(g) = 1\}$: Ist nämlich $g \in G$ mit $\alpha(g) \neq 1$, so ist $g \in A_i$ für ein $i \in \{2, \ldots, k\}$ nach der obigen Behauptung. Ist umgekehrt $g \in A_i$ für ein $i \in \{2, \ldots, k\}$, so ist g_π zu einem Element $h \in B_i$ konjugiert. Folglich ist $\alpha(g)$ zu $\alpha(h)$ und $\beta(g)$ zu $\beta(h)$ konjugiert. Jeder p-Faktor y von $\beta(h)$ liegt also in H und ist zu einem Element in N konjugiert. Nach (iii) ist also $y \in N$. Dies zeigt: $\beta(h) \in N$. Folglich ist $\alpha(h)N = \alpha(h)\beta(h)N = hN \in C_i$ und damit $\alpha(h) \in B_i$; insbesondere ist $\alpha(h) \neq 1$ und $\alpha(g) \neq 1$.
Ist $g \in A_i$ für ein $i \in \{2, \ldots, k\}$, so ist wieder $\alpha(g)$ konjugiert zu einem Element $\alpha(h) \in B_i \subseteq A_i$, also auch $\alpha(g) \in A_i$. Ist $g \in A_1$, so ist $\alpha(g) = 1 \in B_1 \subseteq A_1$. Damit haben wir gezeigt: Mit g liegt auch $\alpha(g)$ in A_i für $i = 1, \ldots, k$. Nach Definition von A_i ist in diesem Fall auch g_π in A_i. Für $g \in A_1$ ist $\alpha(g) = 1$. Für $n \in \mathbb{N}$ ist dann auch $\alpha(g^n) = 1$. Folglich liegt mit g auch g^n in A_1 für $n \in \mathbb{N}$. Wegen $A_1 = \{g \in G : \alpha(g) = 1\}$ liegen außerdem alle π'-Elemente in A_1.
Beh.: Ist $E = U \times Q$ eine π-Untergruppe von G, wobei $U = \langle u \rangle$ zyklisch mit $\alpha(u) \neq 1$ und Q eine p-Gruppe für eine Primzahl $p \in \pi$ mit $p \nmid |U|$ ist, so ist E zu einer Untergruppe von H konjugiert.
Bew.: Wegen $\alpha(u) \neq 1$ ist $u = u_\pi$ zu einem Element in $H \setminus N$ konjugiert. Indem wir E durch ein Konjugiertes ersetzen, können wir also $u \in H \setminus N$ annehmen. Dann folgt die Behauptung aus (iv).
Sei $\operatorname{Irr}(H/N) = \{\psi_1, \ldots, \psi_k\}$ und $\psi_1 = 1_{H/N}$. Für $i = 1, \ldots, k$ ist dann $\varphi_i := \operatorname{Inf}_N^H(\psi_i)$ konstant auf jedem B_i und besitzt genau eine Fortsetzung zu einer Klassenfunktion χ_i auf G, die konstant auf jedem A_j ist. Wir werden zeigen, daß χ_i ein verallgemeinerter Charakter ist.
Dazu sei E eine elementare Untergruppe von G. Wir müssen zeigen, daß $\operatorname{Res}_E^G(\chi_i)$ ein verallgemeinerter Charakter ist. Da E nilpotent ist, können wir $E = E_\pi \times E_{\pi'}$ schreiben, wobei E_π eine π-Gruppe und $E_{\pi'}$ eine π'-Gruppe ist. Für $x \in E$ ist $x_\pi \in E_\pi$ und $\chi_i(x) = \chi_i(x_\pi)$; denn x und x_π liegen im gleichen A_j. Daher ist $\operatorname{Res}_E^G(\chi_i) = \operatorname{Res}_{E_\pi}^G(\chi_i) \circ \rho$, wobei $\rho : E \to E_\pi$ die entsprechende Projektion bezeichnet. Daher genügt es zu zeigen, daß $\operatorname{Res}_{E_\pi}^G(\chi_i)$ ein verallgemeinerter Charakter ist.
Als Untergruppe von E ist E_π elementar. Wir schreiben $E_\pi = U \times Q$, wobei $U = \langle u \rangle$ zyklisch und Q eine p-Gruppe für eine Primzahl $p \in \pi$ ist, o.B.d.A. $p \nmid |\langle u \rangle|$. Im Fall $\alpha(u) \neq 1$ können wir E_π durch ein Konjugiertes ersetzen und $E_\pi \subseteq H$ annehmen. Dann ist aber $\operatorname{Res}_{E_\pi}^G(\chi_i) = \operatorname{Res}_{E_\pi}^H(\varphi_i)$ ein Charakter von E_π. Sei also $\alpha(u) = 1$, d.h. $u \in A_1$. Für $m \in \mathbb{N}$ ist dann auch $u^m \in A_1$, d.h. $\alpha(u^m) = 1$. Bezeichnet σ die Projektion von $E_\pi = U \times Q$ auf Q, so ist also $\alpha(x) = \alpha(\sigma(x))$ für $x \in E_\pi$. Wegen $\chi_i(x) = \chi_i(\alpha(x)) = \chi_i(\alpha(\sigma(x))) = \chi_i(\sigma(x))$ für $x \in E_\pi$ ist daher $\operatorname{Res}_{E_\pi}^G(\chi_i) = \operatorname{Res}_Q^G(\chi_i) \circ \sigma$. Folglich genügt es zu zeigen, daß $\operatorname{Res}_Q^G(\chi_i)$ ein verallgemeinerter Charakter ist.
Nach Sylow können wir o.B.d.A. $Q \subseteq H$ annehmen. Dann ist aber $\operatorname{Res}_Q^G(\chi_i) = \operatorname{Res}_Q^H(\varphi_i)$ ein Charakter von Q. Damit haben wir bewiesen, daß χ_i ein verallgemeinerter Charakter ist.
Für $i = 1, \ldots, k$ wählen wir $b_i \in B_i$ und setzen $\vartheta_i := \sum_{j=1}^k \varphi_j(b_i^{-1})\chi_j$. Nach den Orthogonalitätsrelationen ist dann

$$\begin{aligned}
(\vartheta_i|1_G)_G &= \frac{1}{|G|}\sum_{g\in G}\vartheta_i(g) = \frac{1}{|G|}\sum_{j=1}^k \varphi_j(b_i^{-1})\sum_{r=1}^k |A_r|\varphi_j(b_r) \\
&= \frac{|A_i|}{|G|}\,|C_{H/N}(b_iN)| = \frac{|A_i|}{|G|}\,\frac{|H:N|}{|C_i|} \\
&= \frac{|A_i|}{|G:H|\cdot|B_i|} \in \mathbb{Q}.
\end{aligned}$$

Andererseits ist $(\vartheta_i|1_G)_G$ eine ganz-algebraische Zahl. Also ist $\frac{|A_i|}{|G:H|\cdot|B_i|} \in \mathbb{N}$. Insbesondere ist $|A_i| \geq |G : H| \cdot |B_i|$. Daher ist

$$|G| = \sum_{i=1}^{k} |A_i| \geq |G : H| \sum_{i=1}^{k} |B_i| = |G : H| \cdot |H| = |G|.$$

Für $i = 1, \ldots, k$ ist also $|A_i| = |G : H| \cdot |B_i|$. Folglich ist

$$\begin{aligned}(\chi_i|\chi_i)_G &= \frac{1}{|G|} \sum_{g \in G} \chi_i(g)\chi(g^{-1}) \\ &= \frac{1}{|G|} \sum_{j=1}^{k} |A_j| \varphi_i(b_j)\varphi(b_j^{-1}) \\ &= \frac{1}{|H|} \sum_{j=1}^{k} |B_j| \varphi_i(b_j)\varphi(b_j^{-1}) \\ &= (\varphi_i|\varphi_i)_H \ = \ 1.\end{aligned}$$

Wegen $\chi_i(1) = \varphi(1)_i > 0$ ist also $\chi_i \in \mathrm{Irr}(G)$. Wegen $B_1 = N = \bigcap_{i=1}^{k} \mathrm{Ker}(\varphi_i)$ ist $A_1 = \bigcap_{i=1}^{k} \mathrm{Ker}(\chi_i) \trianglelefteq G$ mit $A_1 \cap H = B_1 = N$. Wegen $|A_1| = |G : H| \cdot |B_1| = |G : H| \cdot |N|$ ist $|A_1 H| = \frac{|A_1|\cdot|H|}{|A_1 \cap H|} = \frac{|G|\cdot|N|}{|N|} = |G|$, also $A_1 H = G$, und wir sind fertig. □

8.2. Satz (Dade)**.** *Sei $N \trianglelefteq H \leq G$ und π eine Primzahlmenge mit folgenden Eigenschaften:*

(i) *H/N ist π-Gruppe.*
(ii) *Sind $x, y \in H$ konjugiert in G, so sind xN, yN konjugiert in H/N.*
(iii) *Jede elementare π-Untergruppe von G ist zu einer Untergruppe von H konjugiert.*

Dann existiert ein Normalteiler M von G mit $G = HM$ und $H \cap M = N$.

Beweis. Sei $p \in \pi$ und P eine p-Sylowgruppe von G. Da P elementar ist, ist P zu einer Untergruppe von H konjugiert, also $p \nmid |G : H|$. Damit erfüllt G die Voraussetzungen von 8.1, und wir sind fertig. □

Bemerkung. Einen direkten Beweis von 8.2 findet man z.B. bei Suzuki II, p. 227.

8.3. Satz (Brauer-Suzuki)**.** *Sei π eine Primzahlmenge und H eine π-Untergruppe von G mit folgenden Eigenschaften:*

(i) *Sind $x, y \in H$ konjugiert in G, so auch in H.*
(ii) *Jede elementare π-Untergruppe von G ist zu einer Untergruppe von H konjugiert.*

Dann existiert ein Normalteiler M von G mit $G = HM$ und $H \cap M = 1$.

Beweis. 8.2 mit $N := 1$. □

Bemerkung.

(i) Man nennt M ein *normales Komplement* von H in G.
(ii) Der Beweis von 8.2 zeigt, daß H unter den gegebenen Voraussetzungen eine π-Hallgruppe in G ist, d.h. kein Primteiler von $|G : H|$ liegt in π.
(iii) Man vergleiche 8.3 und die folgenden Sätze mit ähnlichen Resultaten aus der Gruppentheorie.

8.4. Satz. *Sei p Primzahl und P eine p-Sylowgruppe von G. Sind je zwei Elemente in P, die in G konjugiert sind, auch schon in P konjugiert, so besitzt P ein normales Komplement in G.*

Beweis. 8.3. □

8.5. Satz (Wielandt)**.** *Sei $N \trianglelefteq H \leq G$. Ferner sei $H \cap xHx^{-1} \subseteq N$ für alle $x \in G \setminus H$. Dann existiert ein Normalteiler M von G mit $G = HM$ und $H \cap M = N$.*

Beweis. Bezeichnet man mit π die Menge der Primteiler von $|H/N|$, so ist 8.1(i) erfüllt.
Sei $p \in \pi$, Q eine p-Sylowgruppe von H und P eine p-Sylowgruppe von G mit $Q \subseteq P$. Bekanntlich ist QN/N eine p-Sylowgruppe von H/N, also $QN/N \neq 1$ wegen $p \bigm| |H/N|$. Folglich ist $Q \not\subseteq N$. Für $g \in N_P(Q)$ ist $Q = gQg^{-1} \subseteq H \cap gHg^{-1}$. Wegen $Q \not\subseteq N$ folgt $g \in H$. Daher ist $N_P(Q) \subseteq H \cap P = Q$ und damit $P = Q$. Folglich ist $p \not| |G : H|$, und 8.1(ii) ist erfüllt.
Seien $x, y \in H$ und $g \in G$ mit $y = gxg^{-1}$. Im Fall $g \in H$ ist $yN = (gN)(xN)(gN)^{-1}$. Sei also $g \notin H$. Dann ist $y = gxg^{-1} \in H \cap gHg^{-1} \subseteq N$ und analog $x \in N$, also $yN = 1 = xN$ in H/N. Damit ist 8.1(iii) erfüllt.
Sei schließlich $x \in H \setminus N$ und $g \in C_G(x)$. Dann ist $x = gxg^{-1} \in H \cap gHg^{-1}$, also $g \in H$. Folglich ist $C_G(x) \subseteq H$. Damit sind die Voraussetzungen von 8.1 erfüllt, und die Behauptung folgt. □

8.6. Satz (Frobenius)**.** *Sei $H \leq G$ mit $H \cap gHg^{-1} = 1$ für alle $g \in G \setminus H$. Dann existiert ein Normalteiler F von G mit $G = HF$ und $H \cap F = 1$.*

Beweis. 8.5 mit $N := 1$. □

Definition. Sind die Voraussetzungen von 8.6 erfüllt und ist $1 < H < G$, so nennt man G *Frobeniusgruppe* mit *Frobeniuskern* F und *Frobeniuskomplement* H.

KAPITEL 9

Frobeniusgruppen

Sei G Gruppe.

9.1. Definition. Man nennt G *p-nilpotent* für eine Primzahl p, falls G einen Normalteiler N mit $p \nmid |N|$ besitzt, so daß G/N eine p-Gruppe ist.

Bemerkung.

(i) Untergruppen und Faktorgruppen von p-nilpotenten Gruppen sind wieder p-nilpotent.
(ii) In der Gruppentheorie haben wir bewiesen (Satz von Frobenius), daß eine Gruppe G genau dann p-nilpotent ist, wenn $N_G(Q)$ für jede p-Untergruppe $Q \neq 1$ von G p-nilpotent ist.

9.2. Definition. Sei p eine Primzahl, P eine p-Gruppe,

$$d(P) := \min\{d : P \text{ wird von } d \text{ Elementen erzeugt}\},$$
$$m(P) := \max\{d(A) : A \text{ abelsche Untergruppe von } P\}.$$

Dann nennt man

$$J(P) := \langle A : A \text{ abelsche Untergruppe von } P \text{ mit } d(A) = m(P)\}\rangle$$

die *Thompsonuntergruppe* von P.

Bemerkung. Ist $J(P) \subseteq Q \subseteq P$, so ist $J(P) = J(Q)$. Ferner ist $J(P)$ charakteristisch in P.

Satz (Thompson)**.** *Sei p eine ungerade Primzahl und P eine p-Sylowgruppe von G. Sind $C_G(Z(P))$ und $N_G(J(P))$ p-nilpotent, so auch G.*

Beweis. Sei G ein Gegenbeispiel minimaler Ordnung. Offenbar erfüllt jede echte Untergruppe von G, die P enthält, auch die Voraussetzungen des Satzes und ist damit p-nilpotent.
Annahme: G enthält einen Normalteiler $T \neq 1$ mit $p \nmid |T|$.
Offenbar ist $PT/T \cong P/P\cap T = P/1 \cong P$ eine p-Sylowgruppe von G/T und $J(PT/T) = J(P)T/T$. Nach dem Frattini-Argument ist also $N_{G/T}(J(PT/T)) = N_{G/T}(J(P)T/T) = N_G(J(P)T)/T = N_G(J(P))T/T \cong N_G(J(P))/N_G(J(P)) \cap T$ p-nilpotent. Analog ist $Z(PT/T) = Z(P)T/T$ und $C_{G/T}(Z(PT/T)) = C_{G/T}(Z(P)T/T) = C_G(Z(P)T)/T \cong C_G(Z(P))/C_G(Z(P)) \cap T$ p-nilpotent. Nach Wahl von G ist also G/T p-nilpotent. Dann ist aber auch G p-nilpotent. Widerspruch.
Nach Frobenius ist $\mathcal{X} := \{H : 1 \neq H$ p-Untergruppe von G, $N_G(H)$ nicht p-nilpotent$\} \neq \emptyset$. Wir bezeichnen mit r das Maximum der Ordungen der p-Sylowgruppen von $N_G(H)$ für Gruppen $H \in \mathcal{X}$ und setzen $\mathcal{Y} := \{H \in \mathcal{X} : N_G(H)$ hat eine p-Sylowgruppe der Ordnung $r\}$. Dann ist $\mathcal{Y} \neq \emptyset$, und wir wählen $H \in \mathcal{Y}$ mit maximaler Ordnung.
Wegen $N_G(P) \subseteq N_G(J(P))$ ist $N_G(P)$ p-nilpotent, also $P \notin \mathcal{X}$; insbesondere ist $1 < |H| < |P|$. Sei $N := N_G(H)$ und P_0 eine p-Sylowgruppe von N, also $|P_0| = r$ und $H \subseteq P_0$. Indem wir P durch ein Konjugiertes ersetzen, können wir $P_0 \subseteq P$ annehmen. Wegen $H < P$ ist $H < N_P(H) = P_0$, also $1 \neq J(P_0/H) =: P_1/H$. Daher ist $H < P_1$ und $P_0 \subseteq N_G(P_1)$; insbesondere haben die p-Sylowgruppen von $N_G(P_1)$ mindestens Ordnung r. Wäre $P_1 \in \mathcal{X}$, so wäre sogar $P_1 \in \mathcal{Y}$ im Widerspruch zur Wahl von H. Also ist $P_1 \notin \mathcal{X}$, d.h. $N_G(P_1)$ ist p-nilpotent. Wegen $N_{N/H}(P_1/H) = N_N(P_1)/H$ ist $N_{N/H}(P_1/H)$ p-nilpotent. Analog zeigt man, daß $C_{N/H}(Z(P_0/H))$ p-nilpotent ist. Nach Wahl von G ist also N/H p-nilpotent.
Wegen $H \subseteq P$ ist $Z(P) \subseteq N_P(H) = P_0$, also $Z(P) \subseteq Z(P_0)$. Wegen $C_N(Z(P_0)) \subseteq C_G(Z(P))$ ist daher $C_N(Z(P_0))$ p-nilpotent.

Annahme: $N_G(J(P_0))$ ist nicht p-nilpotent, d.h. $J(P_0) \in \mathcal{X}$.
Da $N_G(J(P))$ p-nilpotent ist, ist $P_0 < P$, also auch $P_0 < P^* := N_P(P_0)$. Dann ist aber $P^* \subseteq N_G(J(P_0))$ im Widerspruch zur Definition von r.
Also sind $N_G(J(P_0))$ und $N_N(J(P_0))$ p-nilpotent. Daher ist auch N ein Gegenbeispiel zur Behauptung. Nach Wahl von G ist also $G = N$; insbesondere ist $H \trianglelefteq G$, $P_0 = P$ und G/H p-nilpotent. Daher enthält G/H einen Normalteiler K/H mit $p \not| \, |K/H|$, so daß $G/K \cong (G/H)/(K/H)$ eine p-Gruppe ist. Nach Schur-Zassenhaus existiert eine Untergruppe S von K mit $K = HS$ und $H \cap S = 1$.
Annahme: Es existiert ein p-Normalteiler H_1 von G mit $H < H_1$. Da $G = N_G(H_1)$ nicht p-nilpotent ist, ist $H_1 \in \mathcal{X}$, also sogar $H_1 \in \mathcal{Y}$ im Widerspruch zur Wahl von H.
Also ist H der größte p-Normalteiler von G. Sei L/H ein minimaler Normalteiler von G/H mit $L/H \subseteq K/H$. Dann ist $L = L \cap K = L \cap SH = (L \cap S)H$ mit $1 < L \cap S \leq S$.
Annahme: $L \cap S < S$.
Dann ist $PL = P(L \cap S)H = P(L \cap S) < G$. Folglich ist PL p-nilpotent; insbesondere ist $L \cap S \trianglelefteq PL$, also auch $L \cap S \trianglelefteq PLS = PK = G$ im Widerspruch zu $p \not| \, |L \cap S|$.
Also ist $L \cap S = S$ und $L = (L \cap S)H = SH = K$. Daher ist K/H minimaler Normalteiler von G/H; insbesondere ist K/H charakteristisch einfach.
Sei q Primteiler von $|S|$ und Q q-Sylowgruppe von S, also auch von $SH = K$. Nach dem Frattini-Argument ist $G = KN_G(Q) = SHN_G(Q)$. Folglich enthält $HN_G(Q)$ eine p-Sylowgruppe von G.
Annahme: $HN_G(Q) < G$.
Dann ist $HN_G(Q)$ p-nilpotent; insbesondere ist $[H, Q] = 1$. Für $s \in S$ ist also $sQs^{-1} \subseteq C_G(sHs^{-1}) = C_G(H)$. Da $S \cong K/H$ charakteristisch einfach ist, ist $S = \langle sQs^{-1} : s \in S \rangle \subseteq C_G(H)$. Folglich ist $K = HS = H \times S$ und $S \trianglelefteq G$ im Widerspruch zu $p \not| \, |S|$.
Also haben wir $G = N_G(Q)$; insbesondere ist $HQ \trianglelefteq G$ und $HQ \leq HS = K$. Da K/H minimaler Normalteiler von G/H ist, folgt $K = HQ$; insbesondere ist $Q = S$ eine elementarabelsche q-Gruppe. Daher ist $1 < H < K = HQ < G$ eine Normalreihe von G; insbesondere ist G auflösbar und $G = HQP = QP$.
Annahme: Es existiert eine Untergruppe U von G mit $P < U < G$.
Dann ist $U = G \cap U = PQ \cap U = P(Q \cap U)$ mit $Q \cap U \neq 1$. Offenbar wird $H(Q \cap U) = HQ \cap U$ von Q und U normalisiert, also auch von $\langle Q, U \rangle = G$. Damit ist $H(Q \cap U) = K = HQ$, $Q = Q \cap U \subseteq U$ und $G = PQ \subseteq U$. Widerspruch.
Dies zeigt, daß P maximale Untergruppe von G ist; insbesondere ist $P = C_G(Z(P)) = N_G(J(P))$. Im Fall $J(P) \subseteq H$ wäre $J(P) = J(H)$ und daher $G = N_G(H) = N_G(J(H)) = N_G(J(P))$ p-nilpotent. Also ist $J(P) \not\subseteq H$. Daher existiert eine abelsche Untergruppe A von P mit $d(A) = m(P) =: m$ und $A \not\subseteq H$. Wir wählen A möglichst klein mit diesen Eigenschaften und schreiben $\exp(A) = p^n$. Im Fall $n > 1$ ist $B := \{a \in A : a^{p^{n-1}} = 1\} < A$ und $d(B) = d(A)$, also $B \subseteq H$ nach Wahl von A. Auf jeden Fall ist $A/A \cap H$ elemantarabelsch.
Offenbar ist $H = F(G)$, also $C_G(H) \subseteq H$ wegen der Auflösbarkeit von G. Da H der größte p-Normalteiler in G ist, ist $K/H = F(G/H)$, also analog $C_{G/H}(K/H) = K/H$. Für Elemente und Untergruppen von G bezeichnen wir ihre Bilder in G/H mit einem Querstrich. Insbesondere ist $\overline{G} = G/H$ und $\overline{A} = AH/H \cong A/A \cap H$ elementarabelsch.
In der Gruppentheorie haben wir gezeigt: $\overline{Q} = \overline{Q_1} \times \overline{Q_2}$ mit $\overline{Q_1} := \overline{Q} \cap Z(\overline{QA})$ und $\overline{Q_2} := [\overline{Q}, \overline{A}]$. Im Fall $\overline{Q_2} = 1$ wäre $\overline{A} \subseteq C_{\overline{G}}(\overline{Q}) = \overline{Q}$, was nicht geht. Also ist $\overline{Q_2} \neq 1$. Wir schreiben $\overline{Q_2} = Q_2H/H$ mit einer Untergruppe Q_2 on Q. Dann ist auch $Q_2 \neq 1$. Ferner ist $I := HQ_2A \leq G$, und HA ist p-Sylowgruppe von I mit $A \subseteq J(AH)$. Wir schreiben $N_I(J(AH)) = Q_2^*HA$ mit einer Untergruppe Q_2^* von Q_2. Wegen $HQ_2 \trianglelefteq HQA$ ist dann $[Q_2^*, A] \subseteq J(AH) \cap HQ_2 \subseteq H$. Folglich ist $\overline{Q_2^*} \subseteq \overline{Q_1} \cap \overline{Q_2} = 1$. Damit ist $N_I(J(AH)) = HA$ p-Gruppe, also insbesondere p-nilpotent. Wegen $Z(P) \subseteq C_G(H) \subseteq H \subseteq HA$ ist $Z(P) \subseteq Z(HA)$ und $C_G(Z(HA)) \subseteq C_G(Z(P))$; insbesondere ist $C_I(Z(HA))$ p-nilpotent.
Annahme: $I < G$.
Dann ist I p-nilpotent nach Wahl von G; insbesondere ist $Q_2 \trianglelefteq I$. Dann ist aber $[Q_2, H] \subseteq Q_2 \cap H = 1$, also $Q_2 \subseteq C_G(H) \subseteq H$, und man hat den Widerspruch $Q_2 = 1$.
Also ist $G = I = HQ_2A$; insbesondere ist $Q_2 = Q$, $\overline{Q} = \overline{Q_2} = [\overline{Q}, \overline{A}]$ und $\overline{Q} \cap Z(\overline{QA}) = \overline{Q_1} = 1$. Nun ist $\overline{Q}$ minimaler Normalteiler von $\overline{G} = \overline{QA}$ mit $C_{\overline{G}}(\overline{Q}) = \overline{Q}$. In der Gruppentheorie haben wir

bewiesen, daß daraus folgt, daß $\overline{A}$ zyklisch ist. Da $\overline{A}$ andererseits elementarabelsch ist, folgt $|\overline{A}| = p$. Wegen $\overline{A} = AH/H \cong A/A \cap H$ ergibt sich daraus $d(A \cap H) \geq m - 1$.
Wegen $Z(P) \subseteq C_G(H) = Z(H) \trianglelefteq G$ ist auch $W : \langle gZ(P)g^{-1} : g \in G \rangle \subseteq Z(H)$. Daher ist W ein abelscher p-Normalteiler von G, insbesondere von WQ. Wie in der Gruppentheorie gezeigt, ist also $W = [W, Q] \times (W \cap Z(WQ))$. Wegen $Q \not\subseteq P = C_G(Z(P))$ ist $Q \not\subseteq C_G(W)$, also $1 \neq W_1 := [W, Q]$. Wegen $W \subseteq Z(H)$ ist $W_1 = [W, HQ] \trianglelefteq G$, also auch $1 \neq V := \{w \in W_1 : w^p = 1\} \trianglelefteq G$. Da V elementarabelscher p-Normalteiler von VQ ist, hat man $V = [V, Q] \times (V \cap Z(VQ))$ und $V \cap Z(VQ) \subseteq W_1 \cap Z(WQ) = 1$. Folglich ist $V = [V, Q]$. Offenbar ist $V_0 := V \cap A = V \cap H \cap A = V \cap A_0$ mit $A_0 := A \cap H$. Wegen $V \subseteq W \subseteq Z(H)$ und $A_0 \subseteq H$ ist $\langle A_0, V \rangle$ abelsch. Da V elementarabelsch ist, ist $d(\langle A_0, V \rangle) = d(A_0) + d(V/V_0)$. Andererseits ist $d(\langle A_0, V \rangle) \leq m \leq d(A_0) + 1$, also $d(V/V_0) \leq 1$.
Wir schreiben $A = \langle A_0, a \rangle$. Dann ist $C_V(a) \geq A \cap V = V_0$, also $|V : C_V(a)| \leq p$. Wegen $P = HA = \langle H, a \rangle \ntrianglelefteq G$ existiert ein $x \in G$ mit $xax^{-1} \notin P$. Wegen $xVx^{-1} = V$ erhalten wir $|V : C_V(xax^{-1})| \leq p$, d.h. $|V : C_V(a, xax^{-1})| \leq p^2$. Wegen der Maximalität von P ist $G = \langle P, xax^{-1} \rangle = \langle H, a, xax^{-1} \rangle$. Wegen $V \subseteq W \subseteq Z(H)$ ist also $C_V(a, xax^{-1}) \subseteq V \cap Z(G) \subseteq V \cap Z(VQ) = 1$, d.h. $|V| \leq p^2$ und $H \subseteq C_G(V) \trianglelefteq G$.
Annahme: $H < C_G(V)$.
Dann ist $C_G(V)$ keine p-Gruppe, also $Q \cap C_G(V) \neq 1$. Da $\overline{Q}$ ein minimaler Normalteiler in $\overline{G}$ ist, folgt $Q = Q \cap C_G(V) \subseteq C_G(V)$. Folglich hat man den Widerspruch $1 = [V, Q] = V$.
Also ist $H = C_G(V)$. Wäre $|V| = p$, so wäre $G/H = G/C_G(V)$ zyklisch von zu p teilerfremder Ordnung. Also ist $|V| = p^2$, und $\overline{G}$ ist zu einer Untergruppe von $\mathrm{GL}(2, \mathbb{F}_p)$ isomorph. Nun ist $\mathrm{SL}(2, \mathbb{F}_p) \trianglelefteq \mathrm{GL}(2, \mathbb{F}_p)$ und $|\mathrm{GL}(2, \mathbb{F}_p) : \mathrm{SL}(2, \mathbb{F}_p)| = p - 1$. Also liegen alle p-Elemente von $\mathrm{GL}(2, \mathbb{F}_p)$ in $\mathrm{SL}(2, \mathbb{F}_p)$. Da $\overline{P}$ eine maximale Untergruppe von $\overline{G}$ ist, wird $\overline{G}$ von seinen p-Elementen erzeugt. Daher ist $\overline{G}$ zu einer Untergruppe von $\mathrm{SL}(2, \mathbb{F}_p)$ isomorph. Bekanntlich ist $|\mathrm{SL}(2, \mathbb{F}_p)| = p(p-1)(p+1)$; insbesondere ist $q \mid |\overline{Q}| \mid (p+1)(p-1)$.
Annahme: $q \neq 2$.
Dann kann q nicht gleichzeitig $p - 1$ und $p + 1$ teilen. Die Gruppe $\overline{A}$ der Ordnung p operiert in Bahnen der Länge p auf $\overline{Q} \setminus \{1\}$. Daher ist $p \mid |\overline{Q}| - 1 = |Q| - 1$. Also ist $|Q| \geq p + 1$ und damit $|Q| = p + 1$. Da p ungerade ist (das haben wir noch nicht benutzt), ist $p + 1$ gerade, und wir haben einen Widerspruch.
Also ist $q = 2$. In den Übungen wird gezeigt, daß $\mathrm{SL}(2, \mathbb{F}_p)$ genau ein Element der Ordnung 2 enthält, nämlich -1. Also ist $|Q| = 2$ und $\overline{Q} \subseteq Z(\overline{G})$, was nicht geht. Damit ist der Satz bewiesen. □

9.3. Definition. Ein Automorphismus α von G mit $\{g \in G : \alpha(g) = g\} = 1$ nennt man *fixpunktfrei*.

Satz. *Ist α ein fixpunktfreier Automorphismus der Ordnung n von G, so gilt:*
(i) *Die Abbildung $G \to G,\ g \mapsto \alpha(g)^{-1}g$ ist bijektiv.*
(ii) *Sind g und $\alpha(g)$ in G konjugiert, so ist $g = 1$.*
(iii) *Für $g \in G$ ist $g\alpha(g)\alpha^2(g)\dots\alpha^{n-1}(g) = 1$.*
(iv) *Für jede Primzahl p existiert eine p-Sylowgruppe P von G mit $\alpha(P) = P$.*
(v) *Für jeden Normalteiler N von G mit $\alpha(N) = N$ ist die Abbildung $G/N \to G/N,\ gN \mapsto \alpha(g)N$ ein fixpunktfreier Automorphismus von G/N.*

Beweis. Aufgabe 16. □

Beispiel. Sei G Frobeniusgruppe mit Frobeniuskomplement H und Frobeniuskern F. Für $h \in H \setminus \{1\}$ ist dann die Abbildung $F \to F,\ x \mapsto hxh^{-1}$ nach Aufgabe 23 ein fixpunktfreier Automorphismus von F.

9.4. Satz. *Sei A abelsche Gruppe, $H \leq \mathrm{Aut}(A)$, $H = M\langle\sigma\rangle$, $M \trianglelefteq H$, $M \cap \langle\sigma\rangle = 1$ und $\mathrm{ggT}(|A|, |M|) = 1$. Ist $\beta \circ \sigma$ fixpunktfrei der Primzahlordnung p für jedes $\beta \in M$, so ist $M = 1$.*

Beweis. Für $a \in A$ und $\beta \in M$ ist $\prod_{i=0}^{p-1} (\beta \circ \sigma)^i(a) = 1$ nach 9.3. Daher ist
$$1 = \prod_{\beta \in M} \prod_{i=0}^{p-1} (\beta \circ \sigma)^i(a) = a^{|M|} \prod_{i=1}^{p-1} \prod_{\beta \in M} (\beta \circ \sigma)^i(a).$$
Seien $\beta_1, \beta_2 \in M$ und $i \in \{1, \dots, p-1\}$ mit $(\beta_1 \circ \sigma)^i = (\beta_2 \circ \sigma)^i$. Dann ist $\langle \beta_1 \circ \sigma \rangle = \langle (\beta_1 \circ \sigma)^i \rangle = \langle (\beta_2 \circ \sigma)^i \rangle = \langle \beta_2 \circ \sigma \rangle$, also $\beta_1 \circ \sigma = (\beta_2 \circ \sigma)^j$ für ein $j \in \{1, \dots, p-1\}$. Wegen $M\sigma = M\beta_1\sigma = M(\beta_2\sigma)^j = M\sigma^j$ folgt

$j = 1$ und $\beta_1 = \beta_2$. Dies zeigt: $\{(\beta \circ \sigma)^i : \beta \in M\} = \{\beta \circ \sigma^i : \beta \in M\}$. Folglich ist

$$a^{-|M|} = \prod_{i=1}^{p-1} \prod_{\beta \in M} (\beta \circ \sigma^i)(a).$$

Für $\alpha \in M$ und $a \in A$ ist also $\alpha(a^{-|M|}) = a^{-|M|}$. Wegen $\mathrm{ggT}(|A|, |M|) = 1$ ist daher $\alpha(a) = a$ für $\alpha \in M$ und $a \in A$. Folglich ist $M = 1$. □

9.5. Satz (Thompson). *Hat G einen fixpunktfreien Automorphismus α der Primzahlordnung p, so ist G nilpotent.*

Beweis. Sei G ein Gegenbeispiel minimaler Ordnung. Nach 9.3 ist die Abbildung $\beta : G/Z(G) \to G/Z(G)$, $gZ(G) \mapsto \alpha(g)Z(G)$ ein fixpunktfreier Autmorphismus von $G/Z(G)$. Wegen $G/Z(G) \neq 1$ hat β auch Ordnung p. Da $G/Z(G)$ nicht nilpotent ist, ist auch $G/Z(G)$ ein Gegenbeispiel zu unserer Behauptung. Nach Wahl von G ist also $Z(G) = 1$. Wir unterscheiden zwei Fälle:
Fall 1: G auflösbar.
Sei A ein möglichst kleiner nichttrivialer Normalteiler von G mit $\alpha(A) = A$. Dann ist A charakteristisch einfach, also eine elementarabelsche q-Gruppe für eine Primzahl q. Da G nicht nilpotent ist, ist G keine q-Gruppe. Sei r Primteiler von $|G|$ mit $r \neq q$. Nach 9.3 enthält G eine r-Sylowgruppe R mit $\alpha(R) = R$. Offenbar ist $r \neq p$; denn sonst hätte α nach der Klassengleichung einen nichttrivialen Fixpunkt auf R. Ist $AR \neq G$, so ist AR nilpotent nach Wahl von G, also $R \subseteq C_G(A)$. Dies gilt für jeden Primteiler r von $|G|$ mit $r \neq q$. Daher ist $G/C_G(A)$ eine q-Gruppe. Nach der Klassengleichung wäre dann aber $A \cap Z(G) \neq 1$, was nicht geht.
Also ist $AR = G$. Wir bezeichnen mit σ die Einschränkung von α auf A und mit M die Gruppe der von den Elementen in R induzierten Automorphismen von A. Dann ist $H := \langle M, \sigma \rangle$ mit $M \trianglelefteq H$. Wir zeigen, daß die Voraussetzungen von 9.4 erfüllt sind. Sei $g \in R$ und γ der von g induzierte Automorphismus von A. Es genügt zu zeigen, daß $\gamma \circ \sigma$ in $\mathrm{Aut}(A)$ zu σ konjugiert ist. Da mit α auch α^{-1} fixpunktfrei ist, existiert nach 9.3 ein $r \in R$ mit $\alpha^{-1}(g) = \alpha^{-1}(r)r^{-1}$, d.h. $g = r\alpha(r^{-1})$. Wir bezeichnen mit ρ den von r induzierten Automorphismus von A. Für $a \in A$ ist

$$\gamma(\sigma(a)) = g\sigma(a)g^{-1} = r\alpha(r^{-1})\alpha(a)\alpha(r)r^{-1} = r\alpha(r^{-1}ar)r^{-1} = (\rho \circ \rho^{-1})(a).$$

Damit können wir 9.4 anwenden und erhalten $M = 1$, d.h. $R \subseteq C_G(A)$. Folglich ist G nilpotent.
Fall 2: G nicht auflösbar.
Sei q ein ungerader Primteiler von $|G|$ und Q eine q-Sylowgruppe von G mit $\alpha(Q) = Q$. Dann ist $\alpha(J(Q)) = J(Q)$ und $\alpha(N_G(J(Q))) = N_G(J(Q))$. Im Fall $J(Q) \trianglelefteq G$ könnte man wie oben argumentieren und erhalten, daß $G/J(Q)$ nilpotent ist. Dann wäre aber G auflösbar, und wir wären im Fall 1.
Also ist $N_G(J(Q)) < G$. Nach Wahl von G ist also $N_G(J(Q))$ nilpotent. Analog zeigt man, daß $C_G(Z(Q))$ nilpotent ist. Nach Thompson ist G q-nilpotent; insbesondere besitzt G einen Normalteiler K mit $q \nmid |K|$, so daß G/K eine q-Gruppe ist. Offenbar ist $\alpha(K) = K$. Nach Wahl von G ist K nilpotent. Damit ist wieder G auflösbar, und wir sind im Fall 1. □

9.6. Satz (Thompson). *Sei G eine Frobeniusgruppe mit Frobeniuskern F und Frobeniuskomplement H. Dann ist F nilpotent.*

Beweis. Jedes $h \in H \setminus \{1\}$ induziert nach Beispiel 9.3 einen fixpunktfreien Automorphismus von F. Die Behauptung folgt aus 9.5. □

Bemerkung. Sei G eine Frobeniusgruppe mit Frobeniuskern F und Frobeniuskomplement H. Aus dem obigen Satz folgt leicht, daß F die Fittunggruppe von G ist; insbesondere ist F eindeutig durch G bestimmt. Nach Aufgabe 24 sind F und H Hallgruppen von G. Nach Schur-Zassenhaus ist H eindeutig bis auf Konjugation in G.

9.7. Satz (Brauers Permutationslemma). *Gegeben seien Gruppen G und F und Operationen von G auf $\mathrm{Cl}(F)$ und $\mathrm{Irr}(F)$ mit der Eigenschaft, daß für alle $g \in G$, $C \in \mathrm{Cl}(F)$ und $\chi \in \mathrm{Irr}(F)$ der Wert von ${}^g\chi$ auf C mit dem Wert von χ auf ${}^gC$ übereinstimmt. Dann gilt für $g \in G$: $|\{\chi \in \mathrm{Irr}(F) : {}^g\chi = \chi\}| = |\{C \in \mathrm{Cl}(F) : {}^gC = C\}|$.*

Beweis. Sei $\mathrm{Irr}(F) = \{\chi_1, \dots, \chi_k\}$, $\mathrm{Cl}(F) = \{C_1, \dots, C_k\}$ und $X := (x(\chi_i, C_j))$ die Charaktertafel von F, d.h. für $i, j = 1, \dots, k$ ist $x(\chi_i, C_j)$ der Wert von χ_i auf C_j. Für $g \in G$ entstehen $(x({}^g\chi_i, C_j))$ und $(x(\chi_i, {}^gC_j))$ aus X durch Permutation der Zeilen bzw. der Spalten. Daher existieren Permutationsmatrizen Φ, Ψ mit $\Phi X = (x({}^g\chi_i, C_j))$ und $(x(\chi_i, {}^gC_j)) = X\Psi$. Nach Voraussetzung ist $\Phi X = X\Psi$, also $\Phi = X\Psi X^{-1}$ wegen der Invertierbarkeit von X. Daher ist $|\{\chi \in \mathrm{Irr}(F) : {}^g\chi = \chi\}| = \mathrm{spur}(\Phi) = \mathrm{spur}(\Psi) = |\{C \in \mathrm{Cl}(F) : {}^gC = C\}|$. ☐

Bemerkung. Wir haben früher gesehen, daß $\frac{1}{|G|}\sum_{g\in G} |\{\chi \in \mathrm{Irr}(F) : {}^g\chi = \chi\}|$ und $\frac{1}{|G|}\sum_{g\in} |\{C \in \mathrm{Cl}(F) : {}^gC = C\}|$ die Anzahl der Bahnen von G auf $\mathrm{Irr}(F)$ bzw. $\mathrm{Cl}(F)$ sind. In der obigen Situation stimmen diese also überein. Es ist jedoch keineswegs gesagt, daß $\mathrm{Irr}(F)$ und $\mathrm{Cl}(F)$ als G-Mengen isomorph sind.

9.8. Satz. *Sei G Frobeniusgruppe mit Frobeniuskomplement H und Frobeniuskern F, und sei X ein Repräsentantensystem für die Bahnen von G auf $\mathrm{Irr}(F) \setminus \{1_F\}$. Dann ist*

$$\mathrm{Irr}(G) = \{\mathrm{Inf}_F^G(\lambda) : \lambda \in \mathrm{Irr}(G/F)\} \,\dot\cup\, \{\mathrm{Ind}_F^G(\psi) : \psi \in X\}.$$

Beweis. Offenbar operiert H durch Konjugation auf $\mathrm{Cl}(F)$ und $\mathrm{Irr}(F)$. Nach 9.3 hat jedes $h \in H \setminus \{1\}$ genau einen Fixpunkt auf $\mathrm{Cl}(F)$, nämlich $\{1\}$. Nach 9.7 hat also jedes $h \in H \setminus \{1\}$ genau einen Fixpunkt auf $\mathrm{Irr}(F)$, nämlich $\{1_F\}$. Daher hat jedes Element $\psi \in \mathrm{Irr}(F) \setminus \{1_F\}$ Trägheitsgruppe F. Für $\psi \in \mathrm{Irr}(F) \setminus \{1_F\}$ ist also $\mathrm{Ind}_F^G(\psi) \in \mathrm{Irr}(G)$ und $\mathrm{Res}_F^G(\mathrm{Ind}_F^G(\psi)) = \sum_{gF\in G/F} {}^g\psi$. Daher sind die Charaktere $\mathrm{Ind}_F^G(\psi)$ $(\psi \in X)$ paarweise verschieden. Offenbar sind auch die Charaktere $\mathrm{Inf}_F^G(\lambda)$ $(\lambda \in \mathrm{Irr}(G/F))$ paarweise verschieden mit $\mathrm{Res}_F^G(\mathrm{Inf}_F^G(\lambda)) = \lambda(1)1_F$. Die Behauptung folgt wegen

$$\begin{aligned}
&\sum_{\psi\in X} (\mathrm{Ind}_F^G(\psi))(1)^2 + \sum_{\lambda\in\mathrm{Irr}(G/F)} (\mathrm{Inf}_F^G(\lambda))(1)^2 \\
&= |G:F|^2 \sum_{\psi\in X} \psi(1)^2 + \sum_{\lambda\in\mathrm{Irr}(G/F)} \lambda(1)^2 \\
&= |G:F| \sum_{\psi\in\mathrm{Irr}(F)\setminus\{1_F\}} \psi(1)^2 + |G:F| \\
&= |G:F|(|F|-1) + |G:F| \;=\; |G:F|\cdot|F| \;=\; |G|.
\end{aligned}$$

☐

9.9. Satz. *Seien K Körper, V ein Vektorraum und A eine Untergruppe der Ordnung pq von $\mathrm{GL}(V)$, wobei p und q nicht notwendig verschiedene Primzahlen sind. Gilt $a(v) \neq v$ für alle $a \in A \setminus \{1\}$ und alle $\in V \setminus \{0\}$, so ist A zyklisch.*

Beweis. Wir nehmen das Gegenteil an. Im Fall $p = q$ besitzt A genau $p + 1$ Untergruppen $A_0, \dots, A_p$ der Ordnung p. Im Fall $p > q$ besitzt A genau eine p-Sylowgruppe A_0 und p q-Sylowgruppen $A_1, \dots, A_p$. In jedem Fall gilt für $i = 0, \dots, p$, $a \in A_i \setminus \{1\}$ und $v \in V \setminus \{0\}$:

$$a(\sum_{b\in A_i} b(v)) = \sum_{b\in A_i} (ab)(v) = \sum_{b\in A_i} b(v),$$

also $\sum_{b\in A_i} b(v) = 0$. Analog ist $\sum_{b\in A} b(v) = 0$. Folglich ist

$$0 = \sum_{i=0}^{p} \sum_{b\in A_i} b(v) = pv + \sum_{b\in A} b(v) = pv.$$

Daher ist $\mathrm{char}(K) = p$, und für jedes Element x der Ordnung p in A ist $0 = (x^p - 1)(v) = (x-1)^p(v)$. Folglich existiert ein $i \in \{0, \dots, p-1\}$ mit $w := (x-1)^i(v) \neq 0 = (x-1)^{i+1}(v)$, d.h. wir haben den Widerspruch $x(w) = w$. ☐

Bemerkung. Sei G Frobeniusgruppe mit Frobeniuskern F und Frobeniuskomplement H. Ist A eine Untergruppe der Ordnung pq von H, wobei p und q nicht notwendig verschiedene Primzahlen sind, so existiert wegen der Nilpotenz von F eine A-invariante elementar-abelsche Untergruppe $V \neq 1$ von F. Nach

9.3 erfüllen A und V die Voraussetzungen von 9.9. Daher ist A zyklisch. Insbesondere ist jede Untergruppe der Ordnung p^2 von H zyklisch. Wie in der Gruppentheorie gezeigt, folgt daraus, daß für $p \neq 2$ die p-Sylowgruppen von H zyklisch und daß die 2-Sylowgruppen zyklisch oder Quaternionengruppen sind (vgl. Aufgabe 8).

KAPITEL 10

TI-Mengen

Sei G Gruppe.

10.1. Definition. Eine Teilmenge D von G mit $D \cap gDg^{-1} \subseteq \{1\}$ für alle $g \in G \setminus N_G(D)$ nennt man eine *TI-Menge* in G (TI = trivial intersection).

Satz. *Sei D eine TI-Menge in G und $H := N_G(D)$. Dann gilt:*

(i) *Sind Teilmengen X, Y von D in G konjugiert, so auch in H.*
(ii) *Für jede Teilmenge X in D mit $X \not\subseteq \{1\}$ ist $N_G(X) \subseteq H$.*
(iii) $D \subseteq H$.
(iv) *Für jede Klassenfunktion ϑ auf H mit $\vartheta(x) = 0$ für alle $x \in H \setminus D$ und für jedes $d \in D \setminus \{1\}$ ist* $(\operatorname{Ind}_H^G \vartheta)(d) = \vartheta(d)$.
(v) *Sind ϑ, η Klassenfunktionen auf H mit $\vartheta(x) = 0 = \eta(x)$ für alle $x \in H \setminus D$ und ist $\vartheta(1) = 0$, so ist* $(\operatorname{Ind}_H^G \vartheta | \operatorname{Ind}_H^G \eta)_G = (\vartheta|\eta)_H$.

Beweis. Aufgabe 18. □

Beispiel. In jeder Frobeniusgruppe G ist das Frobeniuskomplement H eine TI-Menge mit $N_G(H) = H$.

10.2. Bemerkung. Sei $n := |G|$, ζ eine primitive n-te Einheitswurzel in $\mathbb{C}$ und $K := \mathbb{Q}(\zeta)$. Bekanntlich ist $K|\mathbb{Q}$ eine Galoiserweiterung mit Galoisgruppe $\mathcal{G} \cong (\mathbb{Z}/n\mathbb{Z})^\times$; dabei entspricht einem Element $i + n\mathbb{Z} \in (\mathbb{Z}/n\mathbb{Z})^\times$ das Element $\sigma_{i+n\mathbf{Z}} = \sigma_i \in \mathcal{G}$ mit $\sigma_i(\zeta) = \zeta^i$. Nach Brauer ist K ein Zerfällungskörper für G. Sei $\Lambda : G \to \mathrm{GL}(n, K)$ eine irreduzible Matrixdarstellung von G und $\Lambda(g) = (\lambda_{ij}(g))$ für $g \in G$. Für $\sigma \in \mathcal{G}$ ist dann auch ${}^\sigma\Lambda$ eine irreduzible Matrixdarstellung; dabei ist $({}^\sigma\Lambda)(g) = (\sigma(\lambda_{ij}(g)))$ für $g \in G$. Ist χ der Charakter von Λ, so ist ${}^\sigma\chi = \sigma \circ \chi$ der Charakter von ${}^\sigma\Lambda$. Für $g \in G$ ist K auch Zerfällungskörper für $\langle g \rangle$. Man kann also $\Lambda(g)$ diagonalisieren. Insbesondere sind die Eigenwerte von $\Lambda(g)$ n-te Einheitswurzeln $\zeta_1, \ldots, \zeta_d$. Für $i \in \mathbb{Z}$ sind dann $\zeta_1^i, \ldots, \zeta_d^i$ die Eigenwerte von $\Lambda(g)^i = \Lambda(g^i)$. Im Fall $i + n\mathbb{Z} \in (\mathbb{Z}/n\mathbb{Z})^\times$ erhalten wir

$$\chi(g^i) = \zeta_1^i + \ldots + \zeta_d^i = \sigma_i(\zeta_1 + \ldots + \zeta_d) = \sigma_i(\chi(g)).$$

Die Gruppe $(\mathbb{Z}/n\mathbb{Z})^\times$ operiert auf der Menge G durch ${}^{i+n\mathbf{Z}}g := g^i$ für $i + n\mathbb{Z} \in (\mathbb{Z}/n\mathbb{Z})^\times$, $g \in G$. Sind g, h in G konjugiert, so auch g^i, h^i für $i \in \mathbb{Z}$. Damit operiert $(\mathbb{Z}/n\mathbb{Z})^\times$ auch auf $\mathrm{Cl}(G)$. Der Isomorphismus $\mathcal{G} \cong (\mathbb{Z}/n\mathbb{Z})^\times$ induziert daher eine Operation von $\mathcal{G}$ auf G und auf $\mathrm{Cl}(G)$. Die obige Gleichung zeigt: $\chi({}^\sigma g) = ({}^\sigma\chi)(g)$ für alle $\chi \in \mathrm{Irr}(G)$, $\sigma \in \mathcal{G}$, $g \in G$. Nach Brauers Permutationslemma stimmt dann für jedes $\sigma \in \mathcal{G}$ die Anzahl der Fixpunkte von σ auf $\mathrm{Irr}(G)$ mit der Anzahl der Fixpunkte von σ auf $\mathrm{Cl}(G)$ überein. Dies kann man bei der Berechnung von Charaktertafeln benutzen: Ein Element $\chi \in \mathrm{Irr}(G)$ ist offenbar genau dann Fixpunkt unter einem Element $\sigma \in \mathcal{G}$, wenn $\chi(g)$ für alle $g \in G$ im Fixkörper von σ liegt. Aus Brauers Permutationslemma folgt auch, daß für jede Untergruppe $\mathcal{H}$ von $\mathcal{G}$ die Anzahl der Bahnen von $\mathcal{H}$ auf $\mathrm{Irr}(G)$ mit der Anzahl der Bahnen von $\mathcal{H}$ auf $\mathrm{Cl}(G)$ übereinstimmt. Diese Anzahl stimmt natürlich auch mit der Anzahl der Bahnen von $\mathcal{H} \times G$ auf G überein, wobei $\mathcal{H} \times G$ auf G operiert durch ${}^{(\sigma,x)}g := {}^\sigma(xgx^{-1}) = x\,{}^\sigma g x^{-1}$ für $\sigma \in \mathcal{H}$, $g, x \in G$.

Beispiel. Das Element $-1 + n\mathbb{Z} \in (\mathbb{Z}/n\mathbb{Z})^\times$ entspricht dem Element $\iota \in \mathcal{G}$ mit $\iota(\zeta) = \zeta^{-1} = \overline{\zeta}$, d.h. der komplexen Konjugation. Ein Element $\chi \in \mathrm{Irr}(G)$ ist genau dann Fixpunkt unter ι, wenn $\chi(g) \in \mathbb{R}$ für alle $g \in G$ ist. Die Anzahl der reellwertigen irreduziblen Charaktere von G stimmt also überein mit der Anzahl der Konjugationsklassen C von G mit $C = C^{-1}$ (jedes Element ist zu seinem Inversen konjugiert). Solche Konjugationsklassen und ihre Elemente nennt man *reell.*

10.3. Bemerkung. Für $n \in \mathbb{N}$ mit $n \geq 3$ nennt man eine Gruppe P, die von einem Element a der Ordnung 2^{n-1} und einem Element b der Ordnung 4 mit $b^2 = a^{2^{n-2}}$ und $bab^{-1} = a^{-1}$ erzeugt wird, eine *Quaternionengruppe* (vgl. Aufgabe 8). Man rechnet leicht nach, daß P die Ordnung 2^n hat und genau eine Involution enthält (nämlich $b^2 = a^{2^{n-2}}$). Jede Untergruppe von P ist nach einem Satz der Gruppentheorie entweder zyklisch oder selbst eine Quaternionengruppe.

Satz (Brauer-Suzuki)**.** *Hat G eine Quaternionengruppe P als 2-Sylowgruppe und ist t die einzige Involution in P, so ist $G = C_G(t)O(G)$; insbesondere ist G nicht einfach.*

Beweis. Sei G ein Gegenbeispiel minimaler Ordnung. Dann erfüllt auch $G/O(G)$ die Voraussetzungen des Satzes, und es ist $O(G/O(G)) = 1$. Im Fall $O(G) \neq 1$ wäre also $G/O(G) = C_{G/O(G)}(tO(G)) = C_G(t)O(G)/O(G)$, und man hätte $G = C_G(t)O(G)$. Folglich ist $O(G) = 1$. Besitzt G einen echten Normalteiler $M \neq 1$, so ist $|M|$ gerade und $O(M) \subseteq O(G) = 1$. Ferner ist die 2-Sylowgruppe $P \cap M$ von M entweder zyklisch oder eine Quaternionengruppe. Nach einem Satz der Gruppentheorie oder wegen der Minimalität von G ist also $M = C_M(t)$; insbesondere ist t die einzige Involution in M. Folglich ist $G = C_G(t)$, und wir sind fertig. Daher können wir im folgenden annehmen, daß G einfach ist. Wie in 10.3 schreiben wir $P = \langle a, b\rangle$, wobei $a^{2^{n-1}} = 1,\ b^2 = a^{2^{n-2}},\ bab^{-1} = a^{-1}$ und $|P| = 2^n$ ist.
Fall 1: $n \geq 4$.
Sei U die Untergruppe der Ordnung 4 in $\langle a\rangle$, $N := N_G(U)$ und $C := C_G(U)$. Dann ist $b \in N \setminus C$, also $|N : C| = 2$. Wegen $\langle a\rangle \subseteq C$ ist daher $\langle a\rangle$ eine 2-Sylowgruppe von C. Wie in der Gruppentheorie gezeigt, ist also $C = \langle a\rangle B$ mit $B := O(C)$. Folglich ist $N = PC = PB$. Wir setzen $T := \langle a^{2^{n-2}}\rangle = \langle t\rangle$ und $D := C \setminus TB$. Offenbar ist $D = \{c \in C : U \subseteq \langle c\rangle\}$. Sind $d \in D$ und $g \in G$ mit $gdg^{-1} \in D$, so ist auch $g \in N_G(U)$. Umgekehrt ist $N_G(U) \subseteq N_G(D)$. Folglich ist D eine TI-Menge in G und $N_G(D) = N$.
Wegen $C/B \cong \langle a\rangle$ existiert ein $\mu \in \mathrm{Irr}(C)$ mit $\mathrm{Ker}(\mu) = TB$; insbesondere ist $\mu(1) = 1$. Setzt man $\lambda := 1_C - \mu$, so verschwindet $\mathrm{Ind}_C^N(\lambda)$ auf $N \setminus C$ wegen $C \trianglelefteq N$, und wegen $TB \subseteq \mathrm{Ker}(\mu)$ verschwindet $\mathrm{Ind}_C^N(\lambda)$ auf TB. Insgesamt verschwindet $\mathrm{Ind}_C^N(\lambda)$ also auf $N \setminus D$. Offenbar ist

$$(\mathrm{Ind}_C^N 1_C | \mathrm{Ind}_C^N 1_C)_N = (1_C | \mathrm{Res}_C^N \mathrm{Ind}_C^N 1_C)_C = (1_C | 2 \cdot 1_C)_C = 2$$

und

$$(\mathrm{Ind}_C^N 1_C | 1_N)_N = (1_C | 1_C)_C = 1,$$

also $\mathrm{Ind}_C^N 1_C = 1_N + \vartheta$ für ein $\vartheta \in \mathrm{Irr}(N) \setminus \{1_N\}$. Wegen $n \geq 4$ ist $\mathrm{Stb}_N(\mu) = C$, d.h. $\mathrm{Ind}_C^N(\mu) \in \mathrm{Irr}(N)$, $\mathrm{Ind}_C^N(\lambda) = 1_N + \vartheta - \mathrm{Ind}_C^N(\mu)$ und $(\mathrm{Ind}_C^N \lambda | \mathrm{Ind}_C^N \lambda)_N = 3$. Nach 10.1 ist also $(\mathrm{Ind}_C^G \lambda | \mathrm{Ind}_C^G \lambda)_G = 3$, und nach Frobenius $(\mathrm{Ind}_C^G \lambda | 1_G) = (\lambda | 1_C) = 1$, also $\mathrm{Ind}_C^G \lambda = 1_G + \varepsilon_1 \chi_1 + \varepsilon_2 \chi_2$ mit verschiedenen $\chi_1, \chi_2 \in \mathrm{Irr}(G) \setminus \{1_G\}$ und $\varepsilon_1, \varepsilon_2 \in \{\pm 1\}$. Für $i = 1, 2$ sei $n_i := \chi_i(1)$ und $x_i := \chi_i(t)$. Da 1 und t nicht zu Elementen in D konjugiert sind, haben wir $0 = (\mathrm{Ind}_C^G \lambda)(1) = 1 + \varepsilon_1 n_1 + \varepsilon_2 n_2$ und $0 = (\mathrm{Ind}_C^G \lambda)(t) = 1 + \varepsilon_1 x_1 + \varepsilon_2 x_2$. Aus der ersten Gleichung folgt $\varepsilon_1 \neq \varepsilon_2$. Daher können wir $\varepsilon_1 = 1,\ \varepsilon_2 = -1$ annehmen. Dann ist $\mathrm{Ind}_C^G \lambda = 1_G + \chi_1 - \chi_2$ und $1 + n_1 - n_2 = 0 = 1 + x_1 - x_2$. Wir bezeichnen mit I die Konjugationsklasse von t in G.
Annahme: Es existieren $u, v \in I,\ w \in D$ mit $uv = w$.
Dann ist $w^{-1} = v^{-1}u^{-1} = vu^{-1} = u(uv)u^{-1} = uwu^{-1}$. Folglich ist $\langle U, u\rangle$ eine Untergruppe der Ordnung 8 in G, aber weder zyklisch noch eine Quaternionengruppe. Widerspruch.
Für jede Konjugationsklasse E von G mit $E \cap D \neq \emptyset$ und jedes $e \in E \cap D$ ist also

$$0 = a_{IIE} = |\{(u,v) \in I \times I : uv = e\}| = \frac{|I|^2}{|G|} \sum_{\chi \in \mathrm{Irr}(G)} \frac{\chi(t)^2 \chi(e^{-1})}{\chi(1)}$$

nach 4.10. Wegen $D = D^{-1}$ verschwindet daher $\varphi := \sum_{\chi\in\mathrm{Irr}(G)} \frac{\chi(t)^2}{\chi(1)}\chi$ auf der Vereinigung V aller Konjugierten von D. Da $\mathrm{Ind}_C^G \lambda$ außerhalb von V verschwindet, erhalten wir:

$$\begin{aligned}
0 &= (\mathrm{Ind}_C^G \lambda|\varphi)_G = (1_G + \chi_1 - \chi_2| \sum_{\chi\in\mathrm{Irr}(G)} \frac{\chi(t)^2}{\chi(1)}\chi)_G \\
&= 1 + \frac{x_1^2}{n_1} - \frac{x_2^2}{n_2} = 1 + \frac{x_1^2}{n_1} - \frac{(1+x_1)^2}{1+n_1} \\
&= \frac{n_1 + n_1^2 + x_1^2 + n_1x_1^2 - n_1 - 2n_1x_1 - n_1x_1^2}{n_1(1-n_1)} = \frac{(n_1-x_1)^2}{n_1(1-n_1)}.
\end{aligned}$$

Folglich ist $\chi_1(t) = x_1 = n_1 = \chi_1(1)$, also $t \in \mathrm{Ker}(\chi_1)$ im Widerspruch zur Einfachheit von G.
Fall 2: $n = 3$.
In diesem Fall wird P von Elementen a, b der Ordnung 4 erzeugt. Wir verwenden zunächst die Verlagerung $V := V^G_{P/\langle a\rangle}$. Bekanntlich ist $V(b) = \prod_{i=1}^t x_i b^{r_i} x_i^{-1}\langle a\rangle$ mit Elementen $x_1, \dots, x_t \in G$ und $r_1, \dots, r_t \in \mathbb{N}$, wobei $x_1b^{r_1}x_1^{-1}, \dots, x_tb^{r_t}x_t^{-1} \in P$ und $r_1 + \dots + r_t = |G : P|$ ist. Wäre $x_ib^{r_i}x_i^{-1} \equiv b^{r_i} \pmod{\langle a\rangle}$ für $i = 1, \dots, t$, so ergäbe die Einfachheit von G den Widerspruch $1 = V(b) = b^{|G:P|}\langle a\rangle = b\langle a\rangle$. Also existiert ein $i \in \{1, \dots, t\}$ mit $x_ib^{r_i}x_i^{-1} \not\equiv b^{r_i} \pmod{\langle a\rangle}$. Dann ist r_i ungerade und $b^{r_i}\langle a\rangle = b\langle a\rangle \neq 1$, also $x_ib^{r_i}x_i^{-1} \in \langle a\rangle$. Folglich ist $x_ib^{r_i}x_i^{-1} \in \{a, a^{-1}\}$; insbesondere sind a und b in G konjugiert. Analog zeigt man, daß a und ab in G konjugiert sind. Daher sind alle Elemente der Ordnung 4 in G konjugiert. und natürlich sind alle Elemente der Ordnung 2 in G konjugiert.
Wir setzen $N := N_G(\langle a\rangle)$ und $C := C_G(\langle a\rangle)$. Dann ist P eine 2-Sylowgruppe von N und $P\cap C$ eine 2-Sylowgruppe von C. Wie in Fall 1 ist also $C = \langle a\rangle \times B$ mit $B := O(C)$. Wegen $|N : C| = 2$ ist daher $N = PC = PB$. Wir setzen $D := aB \cup a^{-1}B$. Wegen $\langle D\rangle = c$ ist $N_G(D) = N_G(C) = N$. Für $g \in G\setminus N$ ist andrerseits $D \cap gDg^{-1} = \emptyset$. Daher ist D eine TI-Menge in G und $N_G(D) = N$.
Wegen $|C/\langle a^2\rangle \times B| = 2$ existiert ein $\mu \in \mathrm{Irr}(C)$ mit $\mu(y) = 1$ für alle $y \in \langle a^2\rangle \times B$ und $\mu(y) = -1$ für alle $y \in D$. Mit $\lambda := 1_C - \mu$ ist also $\lambda(y) = 2$ für alle $y \in D$ und $\lambda(y) = 0$ für alle $y \in C\setminus D$. Für alle $y \in D$ ist also

$$(\mathrm{Ind}_C^N \lambda)(y) = \frac{1}{|C|}\sum_{g\in N}\lambda(gyg^{-1}) = \frac{|N|}{|C|}2 = 4.$$

Für alle $y \in C\setminus D$ ist analog $(\mathrm{Ind}_C^N \lambda)(y) = 0$, und für alle $y \in N\setminus C$ ist natürlich $(\mathrm{Ind}_C^N \lambda)(y) = 0$. Nach 10.1 ist

$$(\mathrm{Ind}_C^G \lambda|\,\mathrm{Ind}_C^G \lambda) = (\mathrm{Ind}_C^N \lambda|\,\mathrm{Ind}_C^N \lambda) = \frac{1}{|N|}\sum_{y\in N}(\mathrm{Ind}_C^N \lambda)(y)(\mathrm{Ind}_C^N \lambda)(y^{-1}) = \frac{|D|}{|N|}16 = 4,$$

und nach Frobenius ist $(\mathrm{Ind}_C^G \lambda|1_G) = (\lambda|1_C) = 1$. Daher existieren paarweise verschiedene $\chi_1, \chi_2, \chi_3 \in \mathrm{Irr}(G)\setminus\{1_G\}$ und $\varepsilon_1, \varepsilon_2, \varepsilon_3 \in \{\pm1\}$ mit $\mathrm{Ind}_C^G \lambda = 1_G + \varepsilon_1\chi_1 + \varepsilon_2\chi_2 + \varepsilon_3\chi_3$. Wir bezeichnen mit D^G die Menge aller Elemente $g \in G$, die zu einem Element in D konjugiert sind. Offenbar ist $(\mathrm{Ind}_C^G \lambda)(y) = 0$ für alle $y \in G\setminus D^G$, und nach 10.1 ist $(\mathrm{Ind}_C^G \lambda)(y) = (\mathrm{Ind}_C^N \lambda)(y) = 4$ für $y \in D$. Wir bezeichnen mit I die Konjugationsklasse von t in G.
Annahme: $II \cap D^G \neq \emptyset$.
Dann existieren $u, v \in I$, $w \in D$ mit $uv = w$. Ist $w = az$ mit $z \in B$, so ist $a^{-1}z^{-1} = w^{-1} = (uv)^{-1} = u(uv)u^{-1} = uwu^{-1} = uazu^{-1}$, also auch $uau^{-1} = a$. Folglich ist $\langle a, u\rangle$ eine 2-Sylowgruppe von G, aber keine Quaternionengruppe. Analog erhält man einen Widerspruch im Fall $w = a^{-1}z$ für ein $z \in B$.
Also ist $II \cap D^G = \emptyset$. Wir setzen $\varphi := \sum_{\chi\in\mathrm{Irr}(G)} \frac{\chi(t)^2}{\chi(1)}\chi$ und erhalten wie in Fall 1 $\varphi(y) = 0$ für alle $y \in D^G$. Da $\mathrm{Ind}_C^G \lambda$ auf $G\setminus D^G$ verschwindet, ist also

$$0 = (\mathrm{Ind}_C^G \lambda|\varphi) = (1_G + \varepsilon_1\chi_1 + \varepsilon_2\chi_2 + \varepsilon_3\chi_3|\sum_{\chi\in\mathrm{Irr}(G)}\frac{\chi(t)^2}{\chi(1)}) = 1 + \sum_{i=1}^3 \varepsilon_i\frac{\chi_i(t)^2}{\chi_i(1)}.$$

Für $i = 1,2,3$ setzen wir $n_i := \chi_i(1),\ x_i := \chi_i(t),\ y_i := n_i - x_i$. Sei $i \in \{1,2,3\}$ und Δ eine Darstellung von G mit Charakter χ_i. Die Eigenwerte von $\Delta(a)$ sind vierte Einheitswurzeln. Seien $\alpha, \beta, \gamma, \delta$ die Vielfachheiten von $1, -1, i, -i$ als Eigenwerte von $\Delta(a)$. Da a und a^{-1} in G konjugiert sind, ist $\gamma = \delta$. Ferner hat $\Delta(a^2)$ die Eigenwerte $1, -1$ mit Vielfachheiten $\alpha + \beta$ bzw. 2γ. Folglich ist $n_i := \chi_i(1) = \alpha + \beta + 2\gamma$ und $x_i := \chi_i(a^2) = \alpha + \beta - 2\gamma$, also $y_i = n_i - x_i = 4\gamma \equiv 0 \pmod 4$. Im Fall $x_i = n_i$ wäre $t \in \mathrm{Ker}(\chi_i)$ im Widerspruch zur Einfachheit von G. Also ist $x_i < n_i$ und $y_i \in \mathbb{N}$. Wegen $(\mathrm{Ind}_C^G \lambda)(y) = 0$ für alle $y \in G \setminus D^G$ ist $1 + \varepsilon_1 n_1 + \varepsilon_2 n_2 + \varepsilon_3 n_3 = 0 = 1 + \varepsilon_1 x_1 + \varepsilon_2 x_2 + \varepsilon_3 x_3$. Von oben erhalten wir außerdem

$$0 = 1 + \frac{\varepsilon_1 x_1^2}{n_1} + \frac{\varepsilon_2 x_2^2}{n_2} + \frac{\varepsilon_3 x_3^2}{n_3}.$$

Folglich ist $0 = \varepsilon_1 y_1 + \varepsilon_2 y_2 + \varepsilon_3 y_3$ und

$$\begin{aligned}
&\frac{\varepsilon_1 y_1^2}{n_1} + \frac{\varepsilon_2 y_2^2}{n_2} + \frac{\varepsilon_3 y_3^2}{n_3} \\
&= \ \varepsilon_1 n_1 + \varepsilon_2 n_2 + \varepsilon_3 n_3 - 2(\varepsilon_1 x_1 + \varepsilon_2 x_2 + \varepsilon_3 x_3) + \frac{\varepsilon_1 x_1^2}{n_1} + \frac{\varepsilon_2 x_2^2}{n_2} + \frac{\varepsilon_3 x_3^2}{n_3} \\
&= \ -1 + 2 - 1 \ = \ 0.
\end{aligned}$$

Mit a und a^{-1} sind auch aB und $a^{-1}B$ in N konjugiert. Für jeden verallgemeinerten Charakter χ von G ist daher

$$\begin{aligned}
(\chi | \mathrm{Ind}_C^G \lambda)_G &= (\mathrm{Res}_C^G \chi | \lambda)_C = \frac{1}{|C|} \sum_{y \in C} \chi(y)\lambda(y^{-1}) \\
&= \frac{2}{|C|} \sum_{y \in D} \chi(y) = \frac{1}{2|B|} \left(\sum_{y \in aB} \chi(y) + \sum_{y \in a^{-1}B} \chi(y) \right) \\
&= \frac{1}{|B|} \sum_{y \in aB} \chi(y).
\end{aligned}$$

Sei ζ eine primitive $|G|$-te Einheitswurzel in $\mathbb{C}$ und $\mathcal{G} := \mathrm{Gal}(\mathbb{Q}(\zeta)|\mathbb{Q})$. Da $\mathrm{Ind}_C^G \lambda$ nur Werte in $\mathbb{Q}$ hat, gilt für alle $\sigma \in \mathcal{G}$:

$$\mathrm{Ind}_C^G \lambda = {}^\sigma(\mathrm{Ind}_C^G \lambda) = {}^\sigma(1_G + \varepsilon_1 \chi_1 + \varepsilon_2 \chi_2 + \varepsilon_3 \chi_3) = 1_G + \varepsilon_1 {}^\sigma\chi_1 + \varepsilon_2 {}^\sigma\chi_2 + \varepsilon_3 {}^\sigma\chi_3.$$

Annahme: ${}^\sigma\chi_1 = \chi_2$.
Dann ist $\varepsilon_1 = \varepsilon_2,\ x_2 = \chi_2(t) = \sigma(\chi_1(t)) = \sigma(x_1) = x_1,\ n_2 = \chi_2(1) = \sigma(\chi_1(1)) = \sigma(n_1) = n_1$ und $y_2 = y_1$. Folglich ist

$$\begin{aligned}
&\varepsilon_3 n_3 = -1 - \varepsilon_1 n_1 - \varepsilon_2 n_2 = -1 - 2\varepsilon_1 n_1, \\
&\varepsilon_3 y_3 = -\varepsilon_1 y_1 - \varepsilon_2 y_2 = -2\varepsilon_1 y_1, \\
&0 = \frac{\varepsilon_1 y_1^2}{n_1} + \frac{\varepsilon_2 y_2^2}{n_2} + \frac{\varepsilon_3 y_3^2}{n_3} = 2\frac{\varepsilon_1 y_1^2}{n_1} + \frac{4y_1^2}{-1 - 2\varepsilon_1 n_1} = y_1^2 \frac{-2\varepsilon_1 - 4n_1 + 4n_1}{n_1(-1 - 2\varepsilon_1 n_1)}.
\end{aligned}$$

Damit haben wir den Widerspruch $y_1 = 0$.
Aus Symmetriegründen ist also ${}^\sigma\chi_i = \chi_i$ für alle $\sigma \in \mathcal{G}$ und $i = 1,2,3$. Daher ist $\chi_i(g) \in \mathbb{Z}$ für $g \in G,\ i = 1,2,3$. Nach dem Chinesischen Restsatz existiert ein $m \in \mathbb{Z}$ mit $m \equiv 1 \pmod 4$ und $m \equiv -1 \pmod{\frac{|G|}{8}}$. Daher existiert ein $\sigma \in \mathcal{G}$ mit $\sigma(i) = i$ und $\sigma(\zeta^{|G|/8}) = \zeta^{-|G|/8}$. Für $i = 1,2,3$ und $z \in B$ ist also $\chi_i(az) = ({}^\sigma\chi_i)(az) = \chi_i(az^{-1})$. Wir wählen eine Teilmenge B_1 von B mit $B_1 \dot\cup B_1^{-1} = B \setminus \{1\}$. Dann ist

$$\varepsilon_i = (\chi_i | \mathrm{Ind}_C^G \lambda) = \frac{1}{|B|} \sum_{z \in B} \chi_i(az) = \frac{1}{|B|} \left(\chi_i(a) + 2 \sum_{z \in B_1} \chi_i(az) \right),$$

also $\chi_i(a) + 2\sum_{z \in B_1} \chi_i(az) = |B|\varepsilon_i$ ungerade; insbesondere ist $\chi_i(a)$ ungerade. Folglich ist auch

$$|B|(\chi_i^2 | \mathrm{Ind}_C^G \lambda) = \sum_{z \in B} \chi_i^2(az) = \chi_i^2(a) + 2 \sum_{z \in B_1} \chi_i^2(az)$$

ungerade.
Annahme: $\chi_i(a) \neq \varepsilon_i$ für ein $i \in \{1,2,3\}$.
Dann ist $|\chi_i(a)| > 1$ oder $\chi_i(a) = -\varepsilon_i$. In beiden Fällen ist $\chi_i(a)^2 > \varepsilon_i\chi_i(a)$. Wegen $\chi_i(y) \in \mathbb{Z}$ ist $\chi_i(y)^2 \geq \varepsilon_i\chi_i(y)$ für alle $y \in G$. Folglich ist

$$(\chi_i^2 | \operatorname{Ind}_C^G \lambda) = \frac{1}{|B|}\sum_{z\in B}\chi_i^2(az) > \frac{1}{|B|}\sum_{z\in B}\varepsilon_i\chi_i(az) = \varepsilon_i(\chi_i|\operatorname{Ind}_C^G \lambda) = \varepsilon_i^2 = 1.$$

Da $(\chi_i^2|\operatorname{Ind}_C^G\lambda)$ ungerade ist, folgt $(\chi_i^2|\operatorname{Ind}_C^G\lambda) \geq 3$. Wegen $0 = |G|(\chi_i|1_G) = \sum_{y\in G}\chi_i(y) = \sum_{y\in D^G}\chi_i(y) + \sum_{g\in G\setminus D^G}\chi_i(y)$ und $\chi_i(1) > -\varepsilon_i\chi_i(1)$ ist

$$\begin{aligned}\sum_{y\in G\setminus D^G}\chi_i(y)^2 \quad &> \sum_{y\in G\setminus D^G} -\varepsilon_i\chi_i(y) \;=\; \frac{1}{4}\sum_{y\in G}\varepsilon_i\chi_i(y)((\operatorname{Ind}_C^G\lambda)(y^{-1}))\\ &= \frac{\varepsilon_i|G|}{4}(\chi_i|\operatorname{Ind}_C^G\lambda) \;=\; \frac{|G|}{4}.\end{aligned}$$

Man erhält so den Widerspruch

$$\begin{aligned}|G| &= |G|(\chi_i|\chi_i) = \sum_{y\in G}\chi_i(y)^2\\ &> \frac{|G|}{4} + \frac{1}{4}\sum_{y\in G}\chi_i^2(y)((\operatorname{Ind}_C^G\lambda)(y^{-1}))\\ &= \frac{|G|}{4} + \frac{|G|}{4}(\chi_i^2|\operatorname{Ind}_C^G\lambda) \;\geq\; \frac{|G|}{4} + \frac{3|G|}{4} \;=\; |G|.\end{aligned}$$

Für $i = 1,2,3$ ist also $\chi_i(a) = \varepsilon_i$. Folglich ist

$$8(\operatorname{Res}_P^G\chi_i|1_P) = \sum_{y\in P}\chi_i(y) = n_i + x_i + 6\varepsilon_i;$$

insbesondere ist $n_i + x_i + 6\varepsilon_i \equiv 0 \pmod 8$ oder $2(n_i - \varepsilon_i) - y_i \equiv 0 \pmod 8$. Wegen $4 \mid y_i$ ist $n_i - \varepsilon_i$ gerade und n_i ungerade. Sei 2^k die größte Potenz von 2, die $\operatorname{ggT}(y_1,y_2,y_3)$ teilt, also $k \geq 2$. Wir setzen $m_i := \frac{y_i}{2^k}$ für $i = 1,2,3$. Wegen $0 = \frac{\varepsilon_1 y_1^2}{n_1} + \frac{\varepsilon_2 y_2^2}{n_2} + \frac{\varepsilon_3 y_3^2}{n_3}$ ist

$$0 = \varepsilon_1 n_2 n_3 m_1^2 + \varepsilon_2 n_1 n_3 m_2^2 + \varepsilon_3 n_1 n_2 m_3^2.$$

Da $\varepsilon_1,\varepsilon_2,\varepsilon_3,n_1,n_2,n_3$ ungerade sind, ist eine der Zahlen m_1,m_2,m_3 gerade, o.B.d.A. m_1. Da eine der beiden Zahlen m_2,m_3 ungerade ist, müssen m_2,m_3 beide ungerade sein. Folglich ist

$$0 \equiv \varepsilon_2 n_1 n_3 m_2^2 + \varepsilon_3 n_1 n_2 m_3^2 \equiv \varepsilon_2 n_1 n_3 + \varepsilon_3 n_1 n_2 \equiv \varepsilon_2\varepsilon_3 n_1(\varepsilon_3 n_3 + \varepsilon_2 n_2) \pmod 4,$$

also

$$4 \mid \varepsilon_2 n_2 + \varepsilon_3 n_3 = -1 - \varepsilon_1 n_1 = -\varepsilon_1(n_1 + \varepsilon_1)$$

und $4 \mid n_1 + \varepsilon_1$. Wegen $8 \mid y_1$ und $8 \mid 2(n_1 - \varepsilon_1) - y_1$ ist andererseits $4 \mid n_1 - \varepsilon_1$. Damit hat man den Widerspruch $4 \mid n_1 + \varepsilon_1 - n_1 + \varepsilon_1 = 2\varepsilon_1$. □

Bemerkung. G. Glauberman hat die folgende Verallgemeinerung des obigen Satzes bewiesen (Z^*-Satz): Sei P eine 2-Sylowgruppe von G und $t \in P$ ein Element der Ordnung 2. Gibt es kein Element $g \in G$ mit $gtg^{-1} \in P \setminus \{t\}$, so ist $G = C_G(t)O(G)$.
Darauf werden wir im nächsten Semester im Rahmen der modularen Darstellungstheorie zurückkommen. Eine entsprechende Aussage gilt auch für ungerade Primzahlen; ein Beweis ohne Verwendung der Klassifikation der endlichen einfachen Gruppen ist jedoch bis heute nicht bekannt.

KAPITEL 11

CN-Gruppen

11.1. Definition. Eine Gruppe G nennt man eine *CN-Gruppe*, falls $C_G(g)$ für jedes $g \in G\setminus\{1\}$ nilpotent ist.

Bemerkung. Wir werden beweisen, daß CN-Gruppen ungerader Ordnung auflösbar sind. Dies war der zweite von insgesamt drei Schritten auf dem Weg zum Beweis der Auflösbarkeit von Gruppen ungerader Ordnung. Der erste Schritt war M. Suzikis Beweis der Auflösbarkeit von Gruppen ungerader Ordnung mit der Eigenschaft, daß $C_G(g)$ für jede $g \in G \setminus \{1\}$ abelsch ist (CA-Gruppen). Der vorliegende zweite Schritt stammt von W. Feit, M. Hall und J. Thompson. Der dritte Schritt ist bekanntlich ein Satz von W. Feit und J. Thompson.

Satz. *Sei G eine CN-Gruppe, seien p, q verschiedene Primteiler von $|G|$, sei P eine p-Sylowgruppe und Q eine q-Sylowgruppe von G, und seien $x \in P \setminus \{1\}$, $y \in Q \setminus \{1\}$. Gilt $xy = yx$, so gilt auch $ab = ba$ für alle $a \in P$, $b \in Q$.*

Beweis. Aus $xy = yx$ folgt $C_G(x) \geq \langle Z(P), y\rangle$. Da $C_G(x)$ nilpotent ist, ist $Z(P) \subseteq C_G(y)$. Bekanntlich ist $Z(P) \neq 1$. Für $x' \in Z(P) \setminus \{1\}$ ist $C_G(x') \geq \langle y, P\rangle$. Da $C_G(x')$ nilpotent ist, folgt $P \subseteq C_G(y)$, d.h. $\langle P, Z(Q)\rangle \subseteq C_G(y)$. Da $C_G(y)$ nilpotent ist, ergibt sich $P \subseteq C_G(Z(Q))$. Wegen $Z(Q) \neq 1$ existiert ein Element $y' \in Z(Q)\setminus\{1\}$. Dann ist $\langle P, Q\rangle \subseteq C_G(y')$. Da $C_G(y')$ nilpotent ist, erhalten wir $P \subseteq C_G(Q)$. □

11.2. Bemerkung. Offenbar sind Untergruppen von CN-Gruppen wieder CN-Gruppen.

Satz. *Für jeden Normalteiler H einer CN-Gruppe G ist auch G/H wieder eine CN-Gruppe.*

Beweis. Wir nehmen an, daß der Satz falsch ist und wählen ein Gegenbeispiel (G, H) mit möglichst kleinem $|G| + |H|$. Dann folgt leicht, daß H eine elementarabelsche p-Gruppe für eine Primzahl p ist. Sei $g \in G \setminus H$ so, daß $C_{G/H}(gH)$ nicht nilpotent ist. Schreibt man $C_{G/H}(gH) = C/H$, so ist auch (C, H) ein Gegenbeispiel. Nach Wahl von (G, H) ist also $C = G$, d.h. $gH \in Z(G/H)$. Indem wir das Element g notfalls durch eine geeignete Potenz von g ersetzen, können wir annehmen, daß die Ordnung von gH eine Primzahl q ist.
Im Fall $q \neq p$ könnte man sogar annehmen, daß g die Ordnung q hat. Nach einem Satz der Gruppentheorie wäre dann aber $G/H = C_{G/H}(gH) = C_G(g)H/H \cong C_G(g)/C_G(g) \cap H$ nilpotent. Widerspruch.
Folglich ist $q = p$. Dann ist $A := \langle H, g\rangle$ ein p-Normalteiler in G. Sei y ein Element der Primzahlordnung $r \neq p$ in G. Wegen $ygy^{-1}H = gH$ operiert $\langle y\rangle$ auf gH durch Konjugation. Wegen $|gH| = |H|$ besitzt $\langle y\rangle$ einen Fixpunkt $x \in gH$. Also ist $y \in C_G(x)$, und nach 11.1 ist also $G = C_G(A)P$ mit einer p-Sylowgruppe P von G. Bekanntlich ist $B := A \cap Z(P) \neq 1$, und $G = C_G(B)$ ist nilpotent. Widerspruch. □

11.3. Bemerkung. Sei p Primzahl und G Gruppe. Mit p' bezeichnen wir die Menge aller von p verschiedenen Primzahlen, mit $O_p(G)$ den größten p-Normalteiler und mit $O_{p'}(G)$ den größten p'-Normalteiler von G. Ferner definieren wir Normalteiler $O_{pp'}(G)$, $O_{pp'p}(G)$, $\ldots$ von G durch $O_{pp'}(G)/O_p(G) = O_{p'}(G/O_p(G))$, $O_{pp'p}(G)/O_{pp'}(G) = O_p(G/O_{pp'}(G))$, $\ldots$.

Satz. *Für jede auflösbare CN-Gruppe G tritt einer der folgenden Fälle auf:*

(I) *G ist nilpotent.*

(II) *G ist Frobeniusgruppe, und jedes Frobeniuskomplement von G ist entweder zyklisch oder das direkte Produkt einer zyklischen Gruppe ungerader Ordnung mit einer Quaternionengruppe.*

(III) *Es existiert eine Primzahl p mit $G = O_{pp'p}(G) \neq O_{pp'}(G)$, $O_{pp'}(G)$ und $G/O_p(G)$ sind Frobeniusgruppen mit Frobeniuskern $O_p(G)$ bzw. $O_{pp'}(G)/O_p(G)$, und $O_{pp'}(G)/O_p(G)$ ist zyklisch von ungerader Ordnung.*

Beweis. O.B.d.A. sei $G \neq F(G) =: F$. Bekanntlich ist $C_G(F) \subseteq F \neq 1$. Sei π die Menge der Primteiler von $|F|$ und A eine π'-Hallgruppe von G.
Annahme: Es existieren $p \in \pi$, $q \in \pi'$, ein p-Element $x \in F \setminus \{1\}$ und ein q-Element $y \in A \setminus \{1\}$ mit $xy = yx$.
Nach 11.1 zentralisiert y eine p-Sylowgruppe von G und insbesondere $O_p(G)$. Daher ist $\langle y, O_{p'}(F)\rangle \subseteq C_G(x)$. Da $C_G(x)$ nilpotent ist, wird $F = O_p(G)O_{p'}(F)$ von y zentralisiert im Widerspruch zu $C_G(F) \subseteq F$. Nach Aufgabe 23 ist also FA eine Frobeniusgruppe mit Frobeniuskern F (oder es ist $FA = F$), und nach 9.9 sind alle Sylowgruppen von A zyklisch oder Quaternionengruppen.
Annahme: A ist nicht nilpotent; insbesondere ist $A \neq 1$ und $B := F(A) \neq 1$.
Die Sylowgruppen von B sind zyklisch oder Quaternionengruppen. Sei r der kleinste Primteiler von $|B|$ und R die einzige Untergruppe der Ordnung r in B. Dann ist $R \trianglelefteq A$ und $B \subseteq C_A(R) \trianglelefteq A$. Da $C_A(R)$ nilpotent ist, folgt $B = C_A(R)$ und $|A/B| = |A/C_A(R)| \mid |\mathrm{Aut}(R)| = r - 1$; insbesondere ist B eine Hallgruppe von A. Da A eine CN-Gruppe ist, zeigt der erste Teil des Beweises, daß A selbst eine Frobeniusgruppe mit Frobeniuskern B ist. Sei s ein Primteiler von $|A/B|$ und $z \in A$ mit $|\langle z\rangle| = s$. Nach 9.9 ist $\langle R, z\rangle$ zyklisch und wir haben den Widerspruch $z \in C_A(R) = B$.
Folglich ist A nilpotent, und wir können annehmen, daß $FA \neq G$ (sonst liegt Fall (II) vor).
Annahme: Es existieren verschiedene $p, q \in \pi$.
Sei P eine p-Sylowgruppe und Q eine q-Sylowgruppe von G. Dann ist $P \cap F$ die p-Sylowgruppe und $Q \cap F$ die q-Sylowgruppe von F. Nach 11.1 ist $P \subseteq C_G(Q) \subseteq C_G(Q \cap F) \trianglelefteq G$. Da $C_G(Q \cap F)$ nilpotent ist, folgt $P \trianglelefteq G$ und damit $P \subseteq F$. Dies zeigt, daß F eine Hallgruppe von G ist, und wir haben den Widerspruch $G = FA$.
Also ist $\pi = \{p\}$ für eine Primzahl p, und für jede p-Sylowgruppe P von G ist $G = PA$. Nach 11.2 ist G/F eine auflösbare CN-Gruppe. Jeder minimale Normalteiler R/F von G/F ist wegen $O_p(G/F) = 1$ eine elementarabelsche q-Gruppe für eine Primzahl $q \neq p$. Da AF/F eine p'-Hallgruppe von G/F ist, folgt $R/F \subseteq AF/F$. Da die Sylowgruppen von $AF/F \cong A$ zyklisch oder Quaternionengruppen sind, ergibt sich $|R/F| = q$. Da AF/F nilpotent ist, folgt $AF/F \subseteq C_{G/F}(R/F)$. Da $C_{G/F}(R/F)$ ein nilpotenter Normalteiler von G/F ist, folgt $C_{G/F}(R/F) \subseteq F(G/F)$. Wegen $p \nmid |F(G/F)|$ ist also $AF/F = C_{G/F}(R(F) = F(G/F)$. Der erste Teil des Beweises zeigt nun, daß G/F eine Frobeniusgruppe mit Frobeniuskern $F(G/F) = AF/F$ und Frobeniuskomplement P/F ist. Insbesondere induziert jedes Element in $P/F \setminus \{1\}$ eine fixpunktfreien Automorphismus auf AF/F. Daher ist $2 \nmid |AF/FA|$; denn sonst enthielte AF/F genau eine Involution, und diese wäre natürlich ein Fixpunkt unter P/F. Damit ist G vom Typ (III). $\square$

11.4. Bemerkung. Ist G vom Typ (III) in 11.3, so ist $N_{\overline{G}}(V)$ eine p-Gruppe für jede p-Untergruppe $V \neq 1$ der Frobeniusgruppe $\overline{G} := G/O_p(G)$. Daher ist $N_G(U)$ eine p-Gruppe für jede p-Untergruppe U von G mit $U \not\subseteq O_p(G)$. Analog ist $C_G(U)$ eine p-Gruppe für jede Untergruppe $U \neq 1$ von $O_p(G)$.

Satz. *Sei G eine einfache CN-Gruppe ungerader Ordnung, in der jede echte Untergruppe auflösbar ist, und sei P eine p-Sylowgruppe von G für eine Primzahl p. Dann ist P eine TI-Menge in G.*

Beweis. Wir nehmen an, daß der Satz falsch ist. Sei $\tilde{P} \neq P$ eine p-Sylowgruppe von G mit $P \cap \tilde{P} \neq 1$. Wir wählen eine p-Sylowgruppe $\hat{P} \neq P$ von G so, daß $U := P \cap \hat{P}$ möglichst groß und $P \cap \tilde{P} \subseteq U$ ist.
Annahme: $N_G(U)$ enthält eine normale p-Sylowgruppe Q.
Sei R eine p-Sylowgruppe von G mit $Q \subseteq R$. Wegen $U < N_P(U) \subseteq P \cap Q \subseteq P \cap R$ ist dann $R = P$, und wir haben den Widerspruch $U < N_{\hat{P}}(U) \subseteq \hat{P} \cap Q \subseteq \hat{P} \cap R = \hat{P} \cap P = U$.
Also enthält $N_G(U)$ keine normale p-Sylowgruppe. Wegen $O_p(N_G(U)) \geq U \neq 1$ ist $N_G(U)$ also vom Typ (III) in 11.3. Wir wählen eine möglichst große Untergruppe M von G mit $N_G(U) \subseteq M$ und $O_p(M) \neq 1$. Dann enthält auch M keine normale p-Sylowgruppe. Folglich ist auch M vom Typ (III) in 11.3.
Sei P^* eine p-Sylowgruppe von M mit $N_P(U) \subseteq P^*$. Nach der Vorbemerkung ist $C_M(Z(P^*)) = P^*$. Da M nicht p-nilpotent ist, ist nach Thompson $N_M(J(P^*))$ nicht p-nilpotent. Aus der Vorbemerkung folgt

also $J(P^*) \subseteq O_p(M)$. Folglich ist $J(P^*) = J(O_p(M)) \trianglelefteq M$, d.h. $M \subseteq N_G(J(P^*))$. Nach Wahl von M ist also $M = N_G(J(P^*))$.
Sei S eine p-Sylowgruppe von G mit $P^* \subseteq S$. Dann ist $P^* \subseteq N_S(P^*) \subseteq N_G(J(P^*)) = M$. Daher ist $P^* = N_S(P^*)$, d.h. $P^* = S$ ist eine p-Sylowgruppe von G. Wegen $P \cap P^* \supseteq N_G(U) > U$ ist $P^* = P$ nach der Wahl von $\hat{P}$. Da $N_G(U) = N_M(U)$ keine p-Gruppe ist, folgt $U \subseteq O_p(G)$ aus der Vorbemerkung. Daher ist $P \cap \tilde{P} \subseteq U \subseteq O_p(M) = O_p(N_G(J(P)))$. Wir haben also gezeigt: Für jede p-Sylowgruppe $P_1 \neq P$ von G ist $P \cap P_1 \subseteq O_p(N_G(J(P))) = O_p(M) =: X$.
Seien $x, y \in P$ und $g \in G$ mit $y = gxg^{-1}$. Wir zeigen, daß xX und yX in P/X konjugiert sind. Dies ist klar im Fall $g \in P$. Sei also $g \notin P$. Nach der Vorbemerkung ist $P = N_M(P) = N_G(P)$, d.h. $g \notin N_G(P)$. Dann ist aber $y = gxg^{-1} \in P \cap gPg^{-1} \subseteq X$, und analog ist $x \in X$, also $xX = 1 = yX$. Wir können also 8.2 anwenden und erhalten einen Normalteiler N von G mit $G = PN$ und $P \cap N = X$ im Widerspruch zur Einfachheit von G. □

11.5. Satz. *Sei G eine einfache nichtabelsche CN-Gruppe ungerader Ordnung, in der jede echte Untergruppe auflösbar ist, und sei H eine maximale nilpotente Untergruppe von G. Dann ist H eine TI-Hallgruppe in G, und $N_G(H)$ ist eine Frobeniusgruppe mit Frobeniuskern H.*

Beweis. Sei p ein Primteiler von $|H|$, Q eine p-Sylowgruppe von H und P eine p-Sylowgruppe von G mit $Q \subseteq P$. Bekanntlich ist $Q \cap Z(N_P(Q)) \neq 1$, etwa $1 \neq x \in Q \cap Z(N_P(Q))$. Dann ist $H \leq \langle H, N_P(Q) \rangle \leq C_G(x)$. Da $C_G(x)$ nilpotent ist, folgt $H = C_G(x)$. Daher ist $Q \subseteq N_P(Q) \subseteq H$, also $Q = N_P(Q)$ und damit $Q = P$. Dies zeigt, daß H eine Hallgruppe von G ist.
Sei $g \in G$ mit $1 \neq H \cap gHg^{-1}$, sei p ein Primteiler von $|H \cap gHg^{-1}|$, und sei u ein Element der Ordnung p in $H \cap gHg^{-1}$. Dann ist u in der einzigen p-Sylowgruppe P von H und in der einzigen p-Sylowgruppe gPg^{-1} von gHg^{-1} enthalten; insbesondere ist $P \cap gPg^{-1} \neq 1$, also $g \in N_G(P)$ nach 11.4. Im Fall $H = P$ ist H eine TI-Gruppe nach 11.4. Sei also $H \neq P$, d.h. $1 \neq O_{p'}(H) \subseteq C_G(u)$ und $gO_{p'}(H)g^{-1} = O_{p'}(gHg^{-1}) \subseteq C_G(u)$. Da $C_G(u)$ nilpotent und $O_{p'}(H)$ eine Hallgruppe von G und $C_G(u)$ ist, ist $gO_{p'}(H)g^{-1} = O_{p'}(H)$. Wegen $H = PO_{p'}(H)$ ist also $g \in N_G(H)$, d.h. H ist eine TI-Gruppe.
Im Fall $H = N_G(H)$ hätte H ein normales Komplement in G nach Frobenius im Widerspruch zur Einfachheit von G. Also ist $H < N_G(H)$. Nach Aufgabe 23 genügt es zu zeigen: $C_G(x) \subseteq H$ für alle $x \in H \setminus \{1\}$. Wegen $C_G(x) \subseteq C_G(x^i)$ für $i \in \mathbb{N}$ kann man annehmen, daß $|\langle x \rangle|$ eine Primzahl p ist. Ferner genügt es zu zeigen, daß jedes Element $y \in C_G(x)$, dessen Ordnung Potenz einer Primzahl q ist, in H liegt. Wegen $1 \neq x = yxy^{-1} \in H \cap yHy^{-1}$ ist $yHy^{-1} = H$ und $yPy^{-1} = P$. Im Fall $q = p$ ist $\langle P, y \rangle = P\langle y \rangle$ eine p-Gruppe und folglich $y \in P \subseteq H$. Sei also $q \neq p$. Nach 11.1 ist dann $y \in C_G(P) \subseteq C_G(Z(P))$. Offenbar ist $C_G(Z(P))$ nilpotent und $H \subseteq C_G(Z(P))$, also $C_G(Z(P)) = H$ nach Wahl von H und damit $y \in H$. □

11.6. Satz. *Sei G eine einfache nichtabelsche CN-Gruppe ungerader Ordnung, in der jede echte Untergruppe auflösbar ist, und seien $H_1, \dots, H_k$ Repräsentanten für die Konjugationsklassen maximaler nilpotenter Untergruppen von G. Dann gilt:*

(i) *Für $i \neq j$ ist* $\operatorname{ggT}(|H_i|, |H_j|) = 1$.
(ii) $|G| = |H_1| \dots |H_k|$.
(iii) *Zu jedem $g \in G$ existiert ein $i \in \{1, \dots, k\}$, so daß g zu einem Element in H_i konjugiert ist.*

Beweis.

(i) Seien $i, j \in \{1, \dots, k\}$ mit $\operatorname{ggT}(|H_i|, |H_j|) \neq 1$, sei p ein Primteiler von $\operatorname{ggT}(|H_i|, |H_j|)$, und sei P eine p-Sylowgruppe von H_i, also auch von G nach 11.5. Nach 11.5 existiert ein $y \in G$ mit $P \subseteq yH_jy^{-1}$. Indem wir H_j durch yH_jy^{-1} ersetzen, können wir $P \subseteq H_j$ annehmen. Für $1 \neq x \in Z(P)$ ist $H_i \subseteq C_G(x)$. Da $C_G(x)$ nilpotent ist, folgt $H_i \subseteq C_G(x)$ wegen der Maximalität von H_i. Analog ist $H_j = C_G(x)$, also $H_i = H_j$ und $i = j$.
(ii) folgt aus (i), da jede Sylowgruppe nilpotent ist.
(iii) Sei $g \in G \setminus \{1\}$. Dann hat $h := g^n$ Primzahlordnung für ein $n \in \mathbb{N}$. Wegen (ii) ist h zu einem Element in H_i für ein $i \in \{1, \dots, k\}$ konjugiert, o.B.d.A. $h \in H_i$ nach geeigneter Konjugation. Da H_i nach 11.5 eine TI-Untergruppe von G ist, ist $C_G(h) \subseteq N_G(H_i)$. Da $N_G(H_i)$ nach 11.5 eine

Frobeniusgruppe mit Frobeniuskern H_i ist, folgt $C_G(h) \subseteq H_i$ nach Aufgabe 23; insbesondere ist $g \in C_G(h) \subseteq H_i$.

□

Bemerkung. Nach 11.5 enthalten für $i = 1, \dots, k$ die Konjugierten von H_i genau $|G : N_G(H_i)| \big(|H_i|-1\big)$ von 1 verschiedene Elemente. Wegen (i) und (iii) ist also

$$|G| = 1 + \sum_{i=1}^{k} |G : N_G(H_i)| \big(|H_i| - 1\big),$$

d.h.

$$1 = \frac{1}{|G|} + \sum_{i=1}^{k} \frac{|H_i| - 1}{|N_G(H_i)|}.$$

11.7. Satz. *Sei $n \in \mathbb{N}$, $n \geq 2$, sei $\vartheta_{ij} \in \mathbb{Z}\operatorname{Irr}(G)$ mit $\vartheta_{ij}(1) = 0$ für $i, j = 1, \dots, n$, und sei $(\vartheta_{ij}|\vartheta_{st}) = \delta_{is} - \delta_{js} - \delta_{it} + \delta_{jt}$ für alle $i, j, s, t = 1, \dots, n$. Dann existieren ein $\varepsilon \in \{\pm 1\}$ und paarweise verschiedene $\chi_1, \dots, \chi_n \in \operatorname{Irr}(G)$ mit $\vartheta_{ij} = \varepsilon(\chi_i - \chi_j)$ für alle $i, j = 1, \dots, n$.*

Beweis. Für $i = 1, \dots, n$ ist $(\vartheta_{ii}|\vartheta_{ii}) = 0$, also $\vartheta_{ii} = 0$. Für $i, j \in \{1, \dots, n\}$ mit $i \neq j$ ist $(\vartheta_{ij}|\vartheta_{ij}) = 2$. Wegen $\vartheta_{ij}(1) = 0$ ist ϑ_{ij} die Differenz von zwei irreduziblen Charakteren von G. Wegen $(\vartheta_{ij}|\vartheta_{ji}) = -2$ ist $\vartheta_{ji} = -\vartheta_{ij}$. Im Fall $n = 2$ sind wir also fertig. Sei daher $n \geq 3$. Wegen $(\vartheta_{12}|\vartheta_{13}) = 1$ existieren ein $\varepsilon \in \{\pm 1\}$ und paarweise verschiedene $\chi_1, \chi_2, \chi_3 \in \operatorname{Irr}(G)$ mit $\vartheta_{12} = \varepsilon(\chi_1 - \chi_2)$, $\vartheta_{13} = \varepsilon(\chi_1 - \chi_3)$.
Annahme: Es existiert ein $j \in \{4, \dots, n\}$ mit $(\chi_1|\vartheta_{1j}) = 0$.
Dann ist $(\chi_2|\vartheta_{1j}) = -\varepsilon(\vartheta_{12}|\vartheta_{1j}) = -\varepsilon$ und analog ist $(\chi_3|\vartheta_{1j}) = -\varepsilon$. Folglich ist $\vartheta_{1j} = -\varepsilon(\chi_2 + \chi_3)$ im Widerspruch zu $\vartheta_{ij}(1) = 0$.
Für $j = 4, \dots, n$ ist also $\vartheta_{1j} = \varepsilon_j(\chi_1 - \chi_j)$ mit $\varepsilon_j \in \{\pm 1\}$, $\chi_j \in \operatorname{Irr}(G) \setminus \{\chi_1\}$. Wegen

$$1 = (\vartheta_{12}|\vartheta_{1j}) = \varepsilon\varepsilon_j(\chi_1 - \chi_2|\chi_1 - \chi_j) \geq 0$$

ist $\varepsilon = \varepsilon_j$. Für $j, t \in \{2, \dots, n\}$ mit $j \neq t$ ist

$$1 = (\vartheta_{1j}|\vartheta_{1t}) = (\chi_1 - \chi_j|\chi_1 - \chi_t),$$

also $\chi_j \neq \chi_t$. Ferner ist

$$\begin{aligned}
&(\vartheta_{jt} - \vartheta_{1t} + \vartheta_{1j}|\vartheta_{jt} - \vartheta_{1t} + \vartheta_{1j}) \\
&\quad = (\vartheta_{jt}|\vartheta_{jt}) + (\vartheta_{1t}|\vartheta_{1t}) + (\vartheta_{1j}|\vartheta_{1j}) - 2(\vartheta_{jt}|\vartheta_{1t}) + 2(\vartheta_{jt}|\vartheta_{1j}) - 2(\vartheta_{1t}|\vartheta_{1j}) \\
&\quad = (2 - 2\delta_{jt}) + 2 + 2 - 2(1 - \delta_{jt}) + 2(\delta_{jt} - 1) - 2(1 + \delta_{jz}) \\
&\quad = 0,
\end{aligned}$$

also $\vartheta_{jt} = \vartheta_{1t} - \vartheta_{1j} = \varepsilon(\chi_j - \chi_t)$. □

11.8. Satz (W. Feit, M. Hall, J. Thompson)**.** *CN-Gruppen ungerader Ordnung sind auflösbar.*

Beweis. Sei G ein Gegenbeispiel minimaler Ordnung. Sei N ein maximaler Normalteiler von G. Dann ist N auch eine CN-Gruppe ungerader Ordnung, also auflösbar nach Wahl von G. Nach 11.2 ist dann G/N eine CN-Gruppe ungerader Ordnung, aber nicht auflösbar. Nach Wahl von G ist daher $N = 1$ und G einfach. Ferner ist jede echte Untergruppe von G auflösbar.
Seien $H_1, \dots, H_k$ Repräsentanten für die Konjugationsklassen maximaler nilpotenter Untergruppen von G. Für $i = 1, \dots, k$ sei $M_i := N_G(H_i)$, $h_i := |H_i|$, $e_i := |M_i : H_i|$ und $Z_i := \{\zeta \in \operatorname{Irr}(M_i) : H_i \not\subseteq \operatorname{Ker}(\zeta)\}$. Für $\zeta \in Z_i$ existiert nach 9.8 ein $\psi \in \operatorname{Irr}(H_i)$ mit $\zeta = \operatorname{Ind}_{H_i}^{M_i}(\psi)$; insbesondere ist $e_i \mid \zeta(1)$. Wir bezeichnen die Charaktergrade der Elemente in Z_i mit $e_i d_{i1} < e_i d_{i2} < \dots$ und setzen $Z_{is} := \{\zeta \in Z_i : \zeta(1) = e_i d_{is}\} = \{\zeta_{is1}, \dots, \zeta_{isw_{is}}\}$ für $s = 1, 2, \dots$. Nach Aufgabe 17 ist 1_{M_i} der einzige reellwertige irreduzible Charakter vn M_i. Folglich ist w_{is} gerade für alle s. Da H_i nilpotent ist, ist außerdem $d_{i1} = 1$ und $w_{i1} = \big(|H_i : H_i'|-1\big)/e_i$. Wir numerieren $H_1, \dots, H_k$ so, daß $e_1 \leq \dots \leq e_k$ und $w_{11} = \max\{w_{i1} : i = 1, \dots, k,\ e_i = e_1\}$.

Für $i = 1, \dots, k,\ s = 1, 2, \dots,$ und $t, u = 1, \dots, w_{is}$ sei $\alpha_{istu} := \zeta_{ist} - \zeta_{isu}$ und $\vartheta_{istu} := \mathrm{Ind}_{M_i}^G(\alpha_{istu})$. Dann verschwindet α_{istu} auf $M_i \setminus H_i$ und auf $\{1\}$. Für $t', u' = 1, \dots, s$ gilt nach 10.1:

$$\vartheta_{istu}|\vartheta_{ist'u'})_G = (\alpha_{istu}|\alpha_{ist'u'})_{M_i} = \delta_{tt'} - \delta_{tu'} - \delta_{t'u} + \delta_{t'u'}.$$

Nach 11.7 existieren also $\varepsilon_{is} \in \{\pm 1\}$ und paarweise verschiedene $\chi_{is1}, \dots, \chi_{isw_{is}} \in \mathrm{Irr}(G)$ mit $\vartheta_{istu} = \varepsilon_{is}(\chi_{ist} - \chi_{isu})$ für $t, u = 1, \dots, s$. Sei $X_{is} := \{\chi_{is1}, \dots, \chi_{isw_{is}}\}$, ω eine primitive $|G|$-te Einheitswurzel in $\mathbb{C}$ und $\mathcal{G} := \mathrm{Gal}(\mathbb{Q}(\omega)|\mathbb{Q})$. Für $\sigma \in \mathcal{G}$ und $t = 1, \dots, w_{is}$ ist $\sigma \circ \zeta_{ist} \in Z_{is}$. Wir schreiben $\sigma \circ \zeta_{ist} = \zeta_{is\sigma(t)}$. Für $t, u = 1, \dots, s$ gilt dann:

$$\begin{aligned}
\sigma \circ \chi_{ist} - \sigma \circ \chi_{isu} &= \sigma \circ (\chi_{ist} - \chi_{isu}) \\
&= \sigma \circ (\varepsilon_{is} \mathrm{Ind}_{M_i}^G(\zeta_{ist} - \zeta_{isu})) \\
&= \varepsilon_{is} \mathrm{Ind}_{M_i}^G(\sigma \circ \zeta_{ist} - \sigma \circ \zeta_{isu}) \\
&= \varepsilon_{is} \mathrm{Ind}_{M_i}^G(\zeta_{is\sigma(t)} - \zeta_{is\sigma(u)}) \\
&= \chi_{is\sigma(t)} - \chi_{is\sigma(u)}.
\end{aligned}$$

Folglich ist $\sigma \circ \chi_{ist} = \chi_{is\sigma(t)}$. Für $j \neq i$ ist $\mathrm{ggT}(|H_i|, |H_j|) = 1$. Daher verschwindet

$$\sigma \circ \chi_{ist} - \chi_{ist} = \chi_{is\sigma(t)} - \chi_{ist} = \varepsilon_{is} \mathrm{Ind}_{M_i}^G(\zeta_{is\sigma(t)} - \zeta_{ist})$$

auf H_j. Für $h \in H_j$ ist also $(\sigma \circ \chi_{ist})(h) = \chi_{ist}(h)$, d.h. $\chi_{ist}(h) \in \mathbb{Z}$.
Behauptung: $\mathrm{Irr}(G) = \{1_G\} \mathbin{\dot\cup} \dot{\bigcup}_{i=1}^k \dot{\bigcup}_s X_{is}$.
Beweis: Für alle i, s, t, u ist $(1_G|\vartheta_{istu})_G = (1_{M_i}|\alpha_{istu})_{M_i} = 0$. Daher ist $\chi_{ist} \neq 1_G$. Sei also $\chi_{ist} = \chi_{i's't'}$ für gewisse i, i', s, s', t, t'. Im Fall $i \neq i'$ hätte χ_{ist} nach 11.6 nur Werte in $\mathbb{Z}$. Da $|G|$ ungerade ist, geht das nach Aufgabe 17 nicht. Also ist $i = i'$ und

$$(\zeta_{ist} - \overline{\zeta_{ist}}|\zeta_{is't'} - \overline{\zeta_{is't'}})_{M_i} = (\chi_{ist} - \overline{\chi_{ist}}|\chi_{is't'} - \overline{\chi_{is't'}})_G = 2$$

nach 10.1. Daher ist $\zeta_{ist} = \zeta_{is't'}$ und $s = s',\ t = t'$. Für jedes i ist

$$\sum_s |X_{is}| = \sum_s w_i s = |\mathrm{Irr}(M_i)| - |\mathrm{Irr}(M_i/H_i)| = |\mathrm{Cl}(M_i)| - |\mathrm{Cl}(M_i/H_i)|$$

die Anzahl der Konjugationsklassen von M_i, die in $H_i \setminus \{1\}$ liegen. Nach 11.6 ist also $\sum_{i=1}^k \sum_s |X_{is}|$ die Anzahl der von $\{1\}$ verschiedenen Konjugationsklassen von G.
Wir setzen $M := M_1,\ H := H_1,\ h := h_1,\ e := e_1,\ w := w_1 1,\ \zeta_t := \zeta_{11t}$ und $\chi_t := \chi_{11t}$ für $t = 1, \dots, w$. Ferner setzen wir $\delta := \sum_{t=1}^w \chi_t$. Dann ist $\sigma \circ \delta = \delta$ für alle $\sigma \in \mathcal{G}$, d.h. alle Werte von δ liegen in $\mathbb{Z}$. Für $t = 1, \dots, w$ existiert ein $\varphi_t \in \mathrm{Irr}(H) \setminus \{1_H\}$ mit $\varphi_t(1) = 1$ und $\zeta_t = \mathrm{Ind}_H^M(\varphi_t)$. Dann verschwindet $\beta := \mathrm{Ind}_H^G(1_H - \varphi_1)$ auf Elementen, die nicht zu Elementen in H konjugiert sind. Für $i \neq 1$ und alle s, t verschwindet andererseits $\chi_{ist} - \overline{\chi_{ist}}$ auf Konjugierten von H. Daher ist $(\beta|\chi_{ist} - \overline{\chi_{ist}}) = 0$. Außerdem gilt nach 10.1:

$$\begin{aligned}
(\beta|\beta)_G &= (\mathrm{Ind}_H^G(1_H - \varphi_1)|\,\mathrm{Ind}_H^G(1_H - \varphi_1))_G \\
&= (\mathrm{Ind}_H^M(1_H - \varphi_1)|\,\mathrm{Ind}_H^M(1_H - \varphi_1))_M \ = \ e + 1
\end{aligned}$$

und

$$(\beta|\chi_{1st} - \chi_{1st'})_G = (\mathrm{Ind}_H^M(1_H - \varphi_1)|\varepsilon_{is}(\zeta_{1st} - \zeta_{1st'}))_M = \varepsilon_{is}\delta_{1s}(\delta_{1t'} - \delta_{1t})$$

für alle t, t', und

$$(\beta|1_G) = (1_H - \varphi_1|1_H) = 1.$$

Daher existieren $a \in \mathbb{Z}$ und ein reellwertiger Charakter χ von G mit

$$\beta = 1_G - \varepsilon_{11}\chi_1 + a\delta + \gamma$$

und $(\gamma|1_G) = 0,\ (\gamma|\delta) = 0,\ (\gamma|\gamma) \leq e - 1$. Wir setzen $A := \{j : 2 \leq j \leq k$ und $(\chi_{ist}|\beta) = 0$ für alle $s, t\}$ und $B := \{2, \dots, k\} \setminus A$. Für $j \in B$ existieren s, t mit $(\chi_{ist}|\gamma) \neq 0 \neq (\overline{\chi_{ist}}|\gamma)$. Wegen $(\gamma|\gamma) \leq e - 1$ ist also $|B| \leq \frac{e-1}{2}$. Ferner ist $\frac{h_j-1}{h_j e_j} \leq \frac{1}{e_j} \leq \frac{1}{e_2}$ für alle $j \in B$ und damit

$$\sum_{j \in B} \frac{h_j - 1}{h_j e_j} \leq \frac{e-1}{2e_2}.$$

Seien $j \in A$, $h \in H_j$ und $\chi \in \operatorname{Irr}(G)$ mit $(\chi|\beta) \neq 0$. Dann ist $\chi(h) \in \mathbb{Z}$; insbesondere ist $\chi(h) = \overline{\chi}(h)$. Da γ und δ reellwertig sind, müssen $\gamma(h)$ und $\delta(h)$ gerade sein. Daher ist

$$0 = \beta(h) \equiv 1 - \varepsilon_{11}\chi_1(h) \pmod 2;$$

insbesondere ist $\chi_1(h) \neq 0$. Wegen $\chi_1(h) \in \mathbb{Z}$ folgt $|\chi_1(h)| \geq 1$. Für $t = 1, \dots, w$ verschwindet $\chi_1 - \chi_t$ auf H_j. Daher ist $|\delta(h)| = w|\chi_1(h)| \geq w$.
Sei $G_0 := \{g \in G : g$ konjugiert zu einem Element in $H_j \setminus \{1\}$ für ein $j \in A\}$. Dann ist

$$|G_0| := \sum_{j \in A} |G : M_j| \big(|H_j| - 1\big) = |G| \sum_{j \in A} \frac{h_j - 1}{h_j e_j}.$$

Folglich ist

$$w = (\delta|\delta)_G \geq \frac{1}{|G|} \sum_{g \in G_0} |\delta(g)|^2 \geq w^2 \frac{|G_0|}{|G|} = w^2 \sum_{j \in A} \frac{h_j - 1}{h_j e_j}$$

und

$$\sum_{j \in A} \frac{h_j - 1}{h_j e_j} \leq \frac{1}{w}.$$

Mit Bemerkung 11.6 ergibt sich

$$1 = \frac{1}{|G|} + \sum_{i=1}^{k} \frac{h_i - 1}{h_i e_i} \leq \frac{1}{|G|} + \frac{h-1}{he} + \frac{1}{w} + \frac{e-1}{2e_2}.$$

Annahme: $w > 2$, also $w \geq 4$.
Wegen $e_2 \geq e \geq 3$ erhält man

$$1 \leq \frac{1}{|G|} + \frac{1}{e} + \frac{1}{4} + \frac{1}{2} - \frac{1}{2e} = \frac{1}{|G|} + \frac{3}{4} + \frac{1}{2e} \leq \frac{1}{|G|} + \frac{3}{4} + \frac{1}{6} = \frac{1}{|G|} + \frac{11}{12}.$$

Daher ist $\frac{1}{12} \leq \frac{1}{|G|}$ und $|G| \leq 12$. Widerspruch.
Also ist $w = 2$. Nach Wahl der Numerierung von $H_1, \dots, H_k$ ist dann $e_2 > e$. Da e_2 und e ungerade sind, folgt $e_2 \geq e + 2$. Daher ist

$$\frac{1}{2} \leq \frac{1}{|G|} + \frac{h-1}{he} + \frac{e-1}{2(e+2)} = \frac{1}{|G|} + \frac{1}{e} - \frac{1}{he} + \frac{1}{2} - \frac{3}{2(e+2)}.$$

Folglich ist

$$0 \leq \frac{1}{|G|} - \frac{1}{he} + \frac{4-e}{2e(e+2)}.$$

Im Fall $e \geq 5$ wäre $0 < \frac{1}{|G|} - \frac{1}{he}$, und man hätte den Widerspruch $|G| < he$. Also ist $e < 5$. Da e ungerade ist, folgt $e = 3$. Daher ist $|H : H'| = we + 1 = 7$; insbesondere ist H/H' zyklisch. Da H nilpotent ist, ist auch H zyklisch. Folglich ist $|H| = 7$, und wir erhalten

$$0 \leq \frac{1}{|G|} - \frac{1}{21} + \frac{1}{30} = \frac{1}{|G|} + \frac{7-10}{210} = \frac{1}{|G|} - \frac{1}{70}.$$

Dies liefert den Widerspruch $|G| \leq 70$. $\square$

KAPITEL 12

Projektive Darstellungen

12.1. Definition. Für $n \in \mathbb{N}$ und jeden Körper K bezeichnet man $\mathrm{PGL}(n,K) := \mathrm{GL}(n,K)/Z(\mathrm{GL}(n,K))$ als *projektive allgemeine lineare Gruppe* des Grades n über K. Für jeden K-Vektorraum $V \neq 0$ bezeichnet man analog $\mathrm{PGL}(V) := \mathrm{GL}(V)/Z(\mathrm{GL}(V))$ als *projektive allgemeine lineare Gruppe* von V.

Bemerkung. Bekanntlich ist $Z(\mathrm{GL}(n,K)) = \{\alpha 1_n : \alpha \in K^\times\}$ und $Z(\mathrm{GL}(V)) = \{\alpha\,\mathrm{id}_V : \alpha \in K^\times\}$.

12.2. Definition. Eine *projektive Darstellung* einer Gruppe G auf einem Vektorraum $V \neq 0$ über einem Körper K ist ein Homomorphismus $\Pi : G \to \mathrm{PGL}(V)$. Man nennt $\deg \Pi := \dim V$ den *Grad* von Π. Analog definiert man projektive Matrixdarstellungen.

Bemerkung. Für $g \in G$ wählen wir ein $\Psi(g) \in \mathrm{GL}(V)$ mit $\Pi(g) = \Psi(g)Z(\mathrm{GL}(V))$. Für $g,h \in G$ ist dann $\Psi(g)\Psi(h)Z(\mathrm{GL}(V)) = \Pi(g)\Pi(h) = \Pi(gh) = \Psi(gh)Z(\mathrm{GL}(V))$, d.h. $\Psi(g)\Psi(h) = \alpha(g,h)\Psi(gh)$ für ein eindeutig bestimmtes $\alpha(g,h) \in K^\times$. Für $g,h,k \in G$ gilt dabei:

$$\big(\Psi(g)\Psi(h)\big)\Psi(k) = \alpha(g,h)\Psi(gh)\Psi(k) = \alpha(g,h)\alpha(gh,k)\Psi(ghk)$$

und

$$\Psi(g)\big(\Psi(h)\Psi(k)\big) = \Psi(g)\alpha(h,k)\Psi(hk) = \alpha(h,k)\alpha(g,hk)\Psi(ghk),$$

also $\alpha(g,h)\alpha(gh,k) = \alpha(h,k)\alpha(g,hk)$.

12.3. Definition. Sei G eine beliebige und A eine (nicht notwendige endliche) abelsche Gruppe. Eine Abbildung $\alpha : G \times G \to A$ mit

$$\alpha(g,h)\alpha(gh,k) = \alpha(h,k)\alpha(g,hk)$$

für alle $g,h,k \in G$ nennt man ein *Faktorensystem* von G mit Werten in A. Die Menge dieser Faktorensysteme bezeichnen wir mit $Z^2(G,A)$.

Bemerkung. Man sieht leicht, daß $Z^2(G,A)$ eine Untergruppe der abelschen Gruppe $C^2(G,A)$ aller Abbildungen $G \times G \to A$ ist; dabei ist $\alpha\beta$ für $\alpha,\beta \in C^2(G,A)$ definiert durch $(\alpha\beta)(g,h) := \alpha(g,h)\beta(g,h)$ für $g,h \in G$. Analog bilden die Abbildungen $\varphi : G \to A$ eine abelsche Gruppe $C^1(G,A)$.

Beispiel. Wie in der Gruppentheorie gezeigt, ist für $\varphi \in C^1(G,A)$ die Abbildung $\partial\varphi : G \times G \to A,\ (g,h) \mapsto \varphi(g)\varphi(h)\varphi(gh)^{-1}$ ein Faktorensystem, und die Abbildung $\partial : C^1(G,A) \to C^2(G,A),\ \varphi \mapsto \partial\varphi$ ist ein Homomorphismus, dessen Bild eine Untergruppe $B^2(G,A)$ von $Z^2(G,A)$ ist. Wir bezeichnen die Elemente in $B^2(G,A)$ als *prinzipale Faktorensysteme* und nennen die Faktorgruppe $Z^2(G,A)/B^2(G,A) =: H^2(G,A)$ die *zweite Kohomologiegruppe* von G mit Werten in A. In der Gruppentheorie haben wir gezeigt, daß $x^{|G|} = 1$ für alle $x \in H^2(G,A)$ ist.

12.4. Bemerkung. Sei G ein beliebige Gruppe, A eine abelsche Gruppe, U eine Untergruppe von G und $n := |G:U|$. In der Gruppentheorie haben wir gezeigt, daß die Einschränkung einen Homomorphismus $\mathrm{Res}^G_U : H^2(G,A) \to H^2(U,A)$ induziert. Ist dabei $x \in H^2(G,A)$ mit $\mathrm{Res}^G_U(x) = 1$, so ist $x^n = 1$. Für beliebige $x \in H^2(G,A)$ gilt also: Existiert zu jedem Primteiler p von $|G|$ eine p-Sylowgruppe P von G mit $\mathrm{Res}^G_P(x) = 1$, so ist $x = 1$.

12.5. Bemerkung. Sei G Gruppe, $V \neq 0$ ein Vektorraum über dem Körper K und $\Pi : G \to \mathrm{PGL}(V)$ eine projektive Darstellung. Wie in 12.2 wählen wir Elemente $\Psi(g) \in \mathrm{GL}(V)$, $\alpha(g,h) \in K^\times$ mit $\Psi(g)Z(\mathrm{GL}(V)) = \Pi(g)$ und $\Psi(g)\Psi(h) = \alpha(g,h)\Psi(gh)$ für $g,h \in G$. Man nennt dann auch $\Psi : G \to \mathrm{GL}(V)$

eine *projektive Darstellung* von G zum Faktorensystem α. Für $g \in G$ ist $\Psi(g)$ durch $\Pi(g)$ nur bis auf Skalare eindeutig bestimmt. Ist $\Psi'(g) = \varphi(g)\Psi(g)$ mit $\varphi(g) \in K^\times$, so ist

$$\begin{aligned}\Psi'(g)\Psi'(h) &= \varphi(g)\Psi(g)\varphi(h)\Psi(h) = \varphi(g)\varphi(h)\alpha(g,h)\Psi(gh) \\ &= \varphi(g)\varphi(h)\alpha(g,h)\varphi(gh)^{-1}\Psi'(gh) = \alpha(g,h)\varphi(g)\varphi(h)\varphi(gh)^{-1}\Psi'(gh)\end{aligned}$$

für $g, h \in G$, d.h. zu der projektiven Darstellung $\Psi' : G \to \mathrm{GL}(V)$ gehört das Faktorensystem $\alpha \cdot \partial\varphi$. Dies zeigt, daß jede projektive Darstellung $\Pi : G \to \mathrm{PGL}(V)$ genau ein Element $\overline{\alpha} \in H^2(G, K^\times)$ bestimmt.

Satz. *Sei $\Pi : G \to \mathrm{PGL}(n, K)$ eine projektive Matrixdarstellung und $\overline{\alpha}$ das entsprechende Element in $H^2(G, K^\times)$. Dann ist $\overline{\alpha}^n = 1$.*

Beweis. Wir wählen Elemente $\Psi(g)$, $\alpha(g,h)$ wie oben. Für $g, h \in G$ ist dann $\Psi(g)\Psi(h) = \alpha(g,h)\Psi(gh)$, d.h. $\det(\Psi(g))\det(\Psi(h)) = \alpha(g,h)^n \det(\Psi(gh))$. Folglich ist $\alpha^n = \partial(\det \circ \Psi) \in B^2(G, K^\times)$, d.h. $\overline{\alpha}^n = 1$. □

12.6. Satz. *Sei G eine Gruppe, K ein algebraisch abgeschlossener Körper, $x \in H^2(G, K^\times)$ und $n := |\langle x \rangle|$. Dann gilt:*

(i) *Es existiert ein $\alpha \in Z^2(G, K^\times)$ mit $x = \alpha B^2(G, K^\times)$ und $|\langle \alpha \rangle| = n$.*
(ii) *$|H^2(G, K^\times)| < \infty$ und $p := \mathrm{char}(K) \nmid |H^2(G, K^\times)|$.*
(iii) *Ist G zyklisch, so ist $H^2(G, K^\times) = 1$.*

Beweis.

(i) Sei $\beta \in Z^2(G, K^\times)$ mit $x = \beta B^2(G, K^\times)$. Wegen $x^n = 1$ ist dann $\beta^n \in B^2(G, K^\times)$. Daher existiert ein $\varphi \in C^1(G, K^\times)$ mit $\beta(g,h)^n = \varphi(g)\varphi(h)\varphi(gh)^{-1}$ für alle $g, h \in G$. Da K algebraisch abgeschlossen ist, existiert für $g \in G$ ein $\psi(g) \in K^\times$ mit $\varphi(g) = \psi(g)^n$. Setzt man $\alpha := \beta(\partial\psi^{-1})$, so ist $\alpha(g,h)^n = 1$ für alle $g, h \in G$ und $x = \alpha B^2(G, K^\times)$.
(ii) Da K nur endlich viele $|G|$-te Einheitswurzeln enthält, folgt $|H^2(G, K^\times)| < \infty$ aus (i) und Beispiel 12.3. Hat x die Ordnung $n = p = \mathrm{char}(K)$, so ergibt sich mit den Bezeichnungen aus (i): $\beta(g,h)^p = (\psi(g)\psi(h)\psi(gh)^{-1})^p$, also auch $\beta(g,h) = \psi(g)\psi(h)\psi(gh)^{-1}$ für alle $g, h \in G$. Folglich ist $\beta = \partial\psi \in B^2(G, K^\times)$ und $x = \beta B^2(G, K^\times) = 1$. Widerspruch.
(iii) In den Übungen zur Gruppentheorie haben wir gesehen, daß für jede zyklische Gruppe G und jede abelsche Gruppe A gilt: $H^2(G, A) \cong A/\{a^{|G|} : a \in A\}$. Da jedes Element in $K^\times$ eine $|G|$-te Wurzel besitzt, folgt $H^2(G, A) = 1$.

□

12.7. Definition. Eine *Gruppenerweiterung* ist ein 5-Tupel $(Z, H, G, \varepsilon, \nu)$, das aus Gruppen Z, H, G, einem Monomorphismus $\varepsilon : Z \to H$ und einem Epimorphismus $\nu : H \to G$ mit $\mathrm{Ker}(\nu) = \varepsilon(Z)$ besteht. Man schreibt diese Gruppenerweiterung meist in der Form $Z \xrightarrow{\varepsilon} H \xrightarrow{\nu} G$. Im Fall $\varepsilon(Z) \subseteq Z(H)$ nennt man die Gruppenerweiterung *zentral*.

Bemerkung. Sei $Z \xrightarrow{\varepsilon} H \xrightarrow{\nu} G$ eine zentrale Gruppenerweiterung. Für $x \in G$ wählen wir $h_x \in H$ mit $\nu(h_x) = x$. Wie in der Gruppentheorie gezeigt, existiert dann für $x, y \in G$ genau ein Element $\zeta(x,y) \in Z$ mit $h_x h_y = \varepsilon(\zeta(x,y))h_{xy}$, und die so definierte Abbildung $\zeta : G \times G \to Z$ ist ein Faktorensystem. Ferner hängt das Element $\zeta B^2(G, Z) \in H^2(G, Z)$ nicht von der Wahl der Elemente h_x ab, d.h. jede zentrale Gruppenerweiterung $Z \xrightarrow{\varepsilon} H \xrightarrow{\nu} G$ bestimmt genau ein Element in $H^2(G, Z)$.
Sei K ein Körper und $\lambda : Z \to K^\times$ ein Homomorphismus. Man rechnet leicht nach, daß $\alpha := \lambda \circ \zeta : G \times G \to K^\times$ ein Faktorensystem ist, und daß $\alpha B^2(G, K^\times)$ unabhängig von der Wahl der Element h_x ist. Daher bestimmen jede Gruppenerweiterung und jeder Homomorphismus $\lambda : Z \to K^\times$ genau ein Element $\overline{\alpha} \in H^2(G, K^\times)$.
Ist $\Delta : H \to \mathrm{GL}(n, K)$ eine lineare Matrixdarstellung mit $\mathrm{Res}_\varepsilon\, \Delta \sim (\deg \Delta) \cdot \lambda = \lambda \oplus \ldots \oplus \lambda$, so ist die Abbildung $\Psi : G \to \mathrm{GL}(n, K)$, $x \mapsto \Delta(h_x)$ eine projektive Matrixdarstellung mit Faktorensystem α; für

$x, y \in G$ gilt nämlich:

$$\begin{aligned}\Psi(x)\Psi(y) &= \Delta(h_x)\Delta(h_y) \;=\; \Delta(h_x h_y)\\ &= \Delta(\varepsilon(\zeta(x,y))h_{xy} \;=\; \Delta(\varepsilon(\zeta(x,y)))\Delta(h_{xy})\\ &= \lambda(\zeta(x,y))\Psi(xy) \;=\; \alpha(x,y)\Psi(xy).\end{aligned}$$

Ist umgekehrt $\Psi : G \to \mathrm{GL}(n,K)$ eine projektive Matrixdarstellung zum Faktorensystem α, so ist die Abbildung $\Delta : H \to \mathrm{GL}(n,K),\ \varepsilon(z)h_x \mapsto \lambda(z)\Psi(x)$ eine lineare Matrixdarstellung mit $\mathrm{Res}_\varepsilon\,\Delta \sim n\lambda$; denn jedes Element in H läßt sich in der Form $\varepsilon(z)h_x$ mit eindeutig bestimmten $z \in Z,\ x \in G$ schreiben, und für $z, z' \in Z,\ x, y \in G$ gilt:

$$\begin{aligned}\Delta(\varepsilon(z)h_x)\Delta(\varepsilon(z')h_y) &= \lambda(z)\Psi(x = \lambda(z')\Psi(y)\\ &= \lambda(z)\lambda(z')\alpha(x,y)\Psi(xy)\\ &= \lambda(zz'\zeta(x,y))\Psi(xy)\\ &= \Delta(\varepsilon(zz'\zeta(x,y))h_{xy})\\ &= \Delta(\varepsilon(z)\varepsilon(z')\varepsilon(\zeta(x,y))h_{xy})\\ &= \Delta(\varepsilon(z)h_x\varepsilon(z')h_y).\end{aligned}$$

Dies zeigt, daß sich lineare Matrixdarstellungen $\Delta : H \to \mathrm{GL}(n,K)$ mit $\mathrm{Res}_\varepsilon \sim n\lambda$ und projektive Matrixdarstellungen $\Psi : G \to \mathrm{GL}(n,K)$ zum Faktorensystem α entsprechen.

$$\begin{tikzcd} Z(\mathrm{GL}(n,K)) \arrow[r] & \mathrm{GL}(n,K) \arrow[r] & \mathrm{PGL}(n,K) \\ Z \arrow[u, "\lambda"'] \arrow[r] & H \arrow[u, "\Delta"'] \arrow[r] & G \arrow[u, "\Pi"'] \end{tikzcd}$$

Man sagt, daß die projektive Darstellung $\Pi : G \to \mathrm{PGL}(n,K)$ zu einer linearen Darstellung $\Delta : H \to \mathrm{GL}(n,K)$ *gehoben* werden kann.

12.8. Bemerkung. Sei G ein beliebige, A eine (nicht notwendig endliche) abelsche Gruppe und $\alpha \in Z^2(G,A)$, so ist nach der Gruppentheorie $\alpha(1,g) = \alpha(1,1) = \alpha(g,1)$ für alle $g \in G$.

Satz. *Seien G Gruppe, K algebraisch abgeschlossener Körper und $\overline{\alpha}$ ein Element der Ordnung m in $H^2(G,K^\times)$. Dann existiert eine zentrale Gruppenerweiterung $Z \xrightarrow{\varepsilon} H \xrightarrow{\nu} G$, wobei Z eine zyklische Gruppe der Ordnung m ist, und ein Monomorphismus $\lambda : Z \to K^\times$, wodurch wie in Bemerkung 12.7 das Element $\overline{\alpha}$ bestimmt wird.*

Beweis. Aus 12.6 folgt, daß ein Element α der Ordnung m in $Z^2(G,K^\times)$ existiert mit $\overline{\alpha} = \alpha B^2(G,K^\times)$. Sei Z die Gruppe der m-ten Einheitswurzeln in $K^\times$, d.h. Z ist zyklisch der Ordnung m mit $\alpha(g,h) \in Z$ für alle $g, h \in G$. Nach der Gruppentheorie ist $H := Z \times G$ eine Gruppe bzgl. der durch

$$(a,x)\cdot(b,y) := (ab\alpha(x,y), xy)$$

definierten Multiplikation, die Abbildung $\varepsilon : Z \to H,\ a \mapsto (\alpha(1,1)^{-1}a, 1)$ ist ein Monomorphismus, die Abbildung $\nu : H \to G,\ (a,x) \mapsto x$ ist ein Epimorphismus, und $Z \xrightarrow{\varepsilon} H \xrightarrow{\nu} G$ ist eine Gruppenerweiterung. Für $a \in Z,\ (b,y) \in H$ gilt nach der Vorbemerkung:

$$\begin{aligned}\varepsilon(a)\cdot(b,y) &= (\alpha(1,1)^{-1}a, 1)\cdot(b,y)\\ &= (\alpha(1,1)^{-1}aba\alpha(1,y), 1\cdot y)\\ &= (b\cdot\alpha(1,1)^{-1}a\cdot\alpha(y,1), y\cdot 1)\\ &= (b,y)\cdot(\alpha(1,1)^{-1}a, 1)\\ &= (b,y)\cdot\varepsilon(a),\end{aligned}$$

also $\varepsilon(Z) \subseteq Z(H)$. Nach der Gruppentheorie bestimmt $Z \xrightarrow{\varepsilon} H \xrightarrow{\nu} G$ das Faktorensystem $\alpha : G \times G \to Z$. Komposition mit der Inklusionsabbildung $\lambda : Z \to K^\times$ liefert also das Faktorensystem $\alpha : G \to K^\times$. ∎

12.9. Definition. Seien G_1, G_2 beliebige Gruppen, A eine (nicht notwendig endliche) abelsche Gruppe. Eine Abbildung $\beta : G_1 \times G_2 \to A$ mit

$$\beta(x_1y_1, x_2) = \beta(x_1, x_2) \cdot \beta(y_1, x_2) \text{ und } \beta(x_1, x_2y_2) = \beta(x_1, x_2) \cdot \beta(x_1, y_2)$$

für alle $x_1, y_1 \in G_1,\ x_2, y_2 \in G_2$ heißt *Paarung*. Die Menge aller Paarungen bezeichnet man mit $\mathrm{Prg}(G_1, G_2; A)$.

Bemerkung. $\mathrm{Prg}(G_1, G_2; A)$ ist abelsche Gruppe, und dabei definiert man $(\beta\gamma)(x, y) := \beta(x, y) \cdot \gamma(x, y)$.

Satz (Künneth)**.** *Für beliebige Gruppen G_1, G_2 und jede (nicht notwendig endliche) abelsche Gruppe A ist*

$$H^2(G_1 \times G_2, A) = H^2(G_1, A) \times H^2(G_2, A) \times \mathrm{Prg}(G_1, G_2; A).$$

Beweis. Sei $G := G_1 \times G_2$ und fasse G_1, G_2 als Untergruppen von G auf. Für jedes Faktorensystem $\alpha : G \times G \to A$ definiert man eine Abbildung $\beta_\alpha : G_1 \times G_2 \to A$ durch $\beta_\alpha(x_1, x_2) := \alpha(x_1, x_2)\alpha(x_2, x_1)^{-1}$. Dann gilt für $x_1, y_1 \in G_1,\ x_2, y_2 \in G_2$:

$$\begin{aligned} \beta_\alpha(x_1y_1, x_2) &= \alpha(x_1y_1, x_2)\alpha(x_2, x_1y_1)^{-1} \\ &= \beta_\alpha(y_1, x_2)^{-1}\alpha(x_2, y_1)\alpha(x_1, y_1x_2)\alpha(x_2x_1, y_1)^{-1}\beta_\alpha(x_1, x_2)\alpha(x_1, x_2)^{-1} \\ &= \beta_\alpha(x_1, x_2)\beta_\alpha(y_1, x_2) \end{aligned}$$

und analog $\beta_\alpha(x_1, x_2y_2) = \beta_\alpha(x_1, x_2)\beta_\alpha(x_1, y_2)$. Also ist $\beta_\alpha \in \mathrm{Prg}(G_1, G_2; A)$. Offenbar ist die Abbildung $F_3 := Z^2(G, A) \to \mathrm{Prg}(G_1, G_2; A),\ \alpha \mapsto \beta_\alpha$ ein Homomorphismus, und für $\varphi \in C^1(G, A),\ x_1 \in G_1,\ x_2 \in G_2$ ist

$$\begin{aligned} (\beta_{\partial\varphi}(x_1, x_2) &= (\partial\varphi)(x_1, x_2) \cdot (\partial\varphi)(x_2, x_1)^{-1} \\ &= \varphi(x_1)\varphi(x_2)\varphi(x_1x_2)^{-1}\varphi(x_2)^{-1}\varphi(x_1)^{-1}\varphi(x_1x_2) \\ &= 1. \end{aligned}$$

Also induziert F_3 einen Homomorphismus $H^2(G, A) \to \mathrm{Prg}(G_1, G_2; A)$, den man auch mit F_3 bezeichnet. Dies liefert insgesamt einen Homomorphismus

$$\begin{aligned} F : H^2(G, A) &\to H^2(G_1, A) \times H^2(G_2, A) \times \mathrm{Prg}(G_1, G_2; A), \\ x &\mapsto (\mathrm{Res}^G_{G_1}(x), \mathrm{Res}^G_{G_2}(x), F_3(x)). \end{aligned}$$

Surjektivität von F: Sei $\alpha_1 \in Z^2(G_1, A),\ \alpha_2 \in H^2(G_2, A),\ \alpha_3 \in \mathrm{Prg}(G_1, G_2; A)$ und definiere $\alpha : G \times G \to A$ durch $\alpha(x_1x_2, y_1y_2) := \alpha_1(x_1, y_1)\alpha_2(x_2, y_2)\alpha_3(x_1, y_2)$. Dann ist

$$\begin{aligned} &\alpha(x_1x_2, y_1y_2)\alpha(x_1x_2 \cdot y_1y_2, z_1z_2) \\ &= \alpha_1(x_1, y_1)\alpha_2(x_2, y_2)\alpha_3(x_1, y_2)\alpha_1(x_1y_1, z_1)\alpha_2(x_2y_2, z_2)\alpha_3(x_1y_1, z_2) \\ &= \alpha_1(x_1, y_1z_1)\alpha_1(y_1, z_1)\alpha_2(x_2, y_2z_2)\alpha_2(y_2, z_2)\alpha_3(x_1, y_2)\alpha_3(x_1, z_2)\alpha_3(y_1, z_2) \\ &= \alpha(x_1x_2, y_1y_1 \cdot z_1z_2)\alpha(y_1y_2, z_1z_2). \end{aligned}$$

Also ist $\alpha \in Z^2(G, A)$, und weiter gilt:

$$\begin{aligned} \beta_\alpha(x_1, x_2) &= \alpha(x_1, x_2)\alpha(x_2, x_1)^{-1} \\ &= \alpha_1(x_1, 1)\alpha_2(1, x_2)\alpha_3(x_1, x_2)\alpha_1(1, x_1)^{-1}\alpha_2(x_2, 1)^{-1}\alpha_3(1, 1)^{-1} \\ &= \alpha_3(x_1, x_2), \end{aligned}$$

d.h. $\beta_\alpha = \alpha_3$. Weiter ist

$$\alpha(x_1, y_1) = \alpha_1(x_1, y_1)\alpha_2(1, 1)\alpha_3(x_1, 1) = \alpha_1(x_1, y_1)\alpha_2(1, 1),$$

also $(\mathrm{Res}^G_{G_1} \alpha)B^2(G_1, A) = \alpha_1 B^2(G_1, A)$ und analog $(\mathrm{Res}^G_{G_2} \alpha)B^2(G_2, A) = \alpha_2 B^2(G_2, A)$. Also ist F surjektiv.

Injektivität von F: Sei $\alpha \in Z^2(G, A)$ mit $\alpha_i := \mathrm{Res}^G_{G_i} \alpha \in B^2(G_i, A)$ für $i = 1, 2$ und $\beta_\alpha = 1$. Für $i = 1, 2$ sei $\varphi_i \in C^1(G_i, A)$ mit $\alpha_i = \partial\varphi$. Definiere die Abbildung $\varphi : G \to A$ durch

$$\varphi(x_1, x_2) := \varphi_1(x_1)\varphi_2(x_2)\alpha(x_1, x_2)^{-1},$$

so gilt für $x_1, y_1 \in G_1,\ x_2, y_2 \in G_2$:

$$(\partial\varphi)(x_1x_2, y_1y_2) \quad =$$

`[hier fehlt noch was]` Somit ist F injektiv. $\square$

12.10. Bemerkung. Seien $G_1, \dots, G_n$ beliebige Gruppen und A eine (nicht notwendig endliche) abelsche Gruppe. Dann ist

$$\mathrm{Prg}(G_1 \times G_2, G_3; A) \cong \mathrm{Prg}(G_1, G_3; A) \times \mathrm{Prg}(G_2, G_3; A)$$

und durch Induktion erhält man aus 12.9:

$$H^2(\prod_{i=1}^n G_i, A) \cong \prod_{i=1}^n H^2(G_i, A) \times \prod_{1 \le i < j \le n} \mathrm{Prg}(G_i, G_j; A).$$

Sind $G_1, \dots, G_n$ zyklisch, so gilt nach der Gruppentheorie:

$$H^2(G_i, A) \cong A/\{a^{|G_i|} : a \in A\}.$$

Insbesondere ist $H^2(G_i, \mathbb{C}^\times) = 1$ für $i = 1, \dots, n$ nach 12.6, also

$$H^2(\prod_{i=1}^n G_i, \mathbb{C}^\times) \cong \prod_{1 \le i < j \le n} \mathrm{Prg}(G_i, G_j; \mathbb{C}^\times).$$

Seien $i, j \in \{1, \dots, n\},\ G_i = \langle g \rangle,\ G_j = \langle h \rangle$ und $\beta \in \mathrm{Prg}(G_i, G_j; \mathbb{C}^\times)$. Für $k, l \in \mathbb{Z}$ ist dann $\beta(g^k, h^l) = \beta(g, h)^{kl}$, d.h. β ist durch $\zeta := \beta(g, h)$ eindeutig bestimmt. Für $g^k = 1$ ist $\zeta^k = \beta(g, h)^k = \beta(g^k, h) = \beta(1, h) = 1$ und analog $\zeta^l = 1$ für $h^l = 1$. Also ist ζ eine $\mathrm{ggT}(|G_i|, |G_j|)$-te Einheitswurzel in $\mathbb{C}$. Umgekehrt liefert jede solche Einheitswurzel ein Element in $\mathrm{Prg}(G_i, G_j; \mathbb{C}^\times)$. Daher ist $\mathrm{Prg}(G_i, G_j; \mathbb{C}^\times)$ eine zyklische Gruppe der Ordnung $\mathrm{ggT}(|G_i|, |G_j|)$, und für beliebige zyklische Gruppen $G_1, \dots, G_n$ gilt:

$$H^2(\prod_{i=1}^n G_i, \mathbb{C}^\times) \cong \prod_{1 \le i < j \le n} \mathbb{Z}/\,\mathrm{ggT}(|G_i|, |G_j|)\mathbb{Z}.$$

Beispiel. Für die Kleinsche Vierergruppe $G = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ ist $|H^2(G, \mathbb{C}^\times)| = 2$.

KAPITEL 13

Das Tensorprodukt von Moduln

Sei R ein Ring (stets assoziativ mit 1, aber i.a. nicht kommutativ).

13.1. Bemerkung. Für jeden R-Rechtsmodul M und jeden R-Linksmodul N ist die Menge F aller Abbildungen $\varphi : M \times N \to \mathbb{Z}$ mit $|\{(m,n) \in M \times N : \varphi(m,n) \neq 0\}| < \infty$ eine abelsche Gruppe mit $(\varphi + \psi)(m,n) := \varphi(m,n) + \psi(m,n)$ für $\varphi, \psi \in F,\ m \in M,\ n \in N$. Für $m \in M,\ n \in N$ sei $[m,n] \in F$ definiert durch

$$[m,n](m',n') := \begin{cases} 1 & \text{falls } (m,n) = (m',n') \\ 0 & \text{sonst} \end{cases} .$$

Dann ist $\varphi = \sum_{m\in M, n\in N} \varphi(m,n)[m,n]$. (Die Summe ist nach Definition von F endlich.) Folglich wird F von den Elementen $[m,n]$ mit $m \in M,\ n \in N$ erzeugt. Diese Elemente sind auch linear unabhängig über $\mathbb{Z}$; denn ist $\sum_{m\in M, n\in N} z_{mn}[m,n] = 0$ mit Elementen $z_{mn} \in \mathbb{Z}$, von denen nur endlich viele von 0 verschieden sind, so ist

$$0 = \Bigg(\sum_{m\in M, n\in N} z_{mn}[m,n]\Bigg)(m',n') = \sum_{m\in M, n\in N} z_{mn}[m,n](m',n') = z_{m'n'}$$

für $m' \in M,\ n' \in N$. Daher ist F eine freie abelsche Gruppe mit Basis $\{[m,n] : m \in M,\ n \in N\}$. Jedes Element in F läßt sich also in der Form $\sum_{m\in M, n\in N} z_{mn}[m,n]$ mit eindeutig bestimmten $z_{mn} \in \mathbb{Z}$, von denen nur endliche viele von 0 verschieden sind, schreiben.
Wir bezeichnen mit U die von allen Elementen der Formen

$$\left.\begin{array}{l} [m+m',n] - [m,n] - [m',n] \\ [m,n+n'] - [m,n] - [m,n'] \\ [mr,n] - [m,rn] \end{array}\right\} m,m' \in M,\ n,n' \in N,\ r \in R$$

erzeugte Untergruppe von F und nennen $M \otimes_R N := F/U$ das *Tensorprodukt* von M und N. Dies ist eine abelsche Gruppe (i.a. kein R-Modul) und wird von den Elementen $m \otimes n := [m,n] + U$ mit $m \in M,\ n \in N$ erzeugt. Wegen

$$\begin{aligned} (m+m') \otimes n &= m \otimes n + m' \otimes n, \\ m \otimes (n+n') &= m \otimes n + m \otimes n', \\ mr \otimes n &= m \otimes rn \end{aligned}$$

für $m,m' \in M,\ n,n' \in N,\ r \in R$ ist $0 \otimes n = 0 = m \otimes 0$ und $(-m) \otimes n = -(m \otimes n) = m \otimes (-n)$ für $m \in M,\ n \in N$. Daher kann man jedes Element in $M \otimes_R N$ in der Form $\sum_{i=1}^k m_i \otimes n_i$ mit $m_1, \ldots, m_k \in M,\ n_1, \ldots, n_k \in N$ schreiben. Diese Schreibweise ist jedoch i.a. nicht eindeutig. Auch ist i.a. nicht jedes Element in $M \otimes_R N$ von der Form $m \otimes n$ mit $m \in M,\ n \in N$.

13.2. Definition. Seien M ein R-Rechtsmodul, N ein R-Linksmodul und A eine abelsche Gruppe. Eine Abbildung $f : M \times N \to A$ mit

$$\begin{aligned} f(m+m',n) &= f(m,n) + f(m',n), \\ f(m,n+n') &= f(m,n) + f(m,n'), \\ f(mr,n) &= f(m,rn) \end{aligned}$$

nennt man *(R-)ausgeglichen*.

Beispiel. Die Abbildung $M \times N \to M \otimes_R N,\ (m,n) \mapsto m \otimes n$ aus 13.1 ist ausgeglichen. Wir nennen sie die *kanonische* Abbildung von $M \times N$ in $M \otimes_R N$.

Satz (Universelle Eigenschaft des Tensorprodukts)**.** *Zu jedem R-Rechtsmodul M, jedem R-Linksmodul N, jeder abelschen Gruppe A und jeder ausgeglichenen Abbildung $f : M \times N \to A$ existiert genau ein Homomorphismus $f' : M \otimes_R N \to A$ mit $f'(m \otimes N) = f(m,n)$ für $m \in M,\ n \in N$.*

$$\begin{tikzcd} M \times N \arrow[rr] \arrow[dr, "f"'] & & M \otimes_R N \arrow[dl, dotted, "f'"] \\ & A & \end{tikzcd}$$

Beweis. Mit den Bezeichnungen aus 13.1 definieren wir eine Abbildung $h : F \to A$ durch

$$h\Bigg(\sum_{m \in M, n \in N} z_{mn}[m,n]\Bigg) := \sum_{m \in M, n \in N} z_{mn} f(m,n)$$

für beliebige Elemente $z_{mn} \in \mathbb{Z}$, von denen nur endliche viele von 0 verschieden sind. Da $\{[m,n] : m \in M,\ n \in N\}$ eine $\mathbb{Z}$-Basis von F ist, ist h wohldefiniert und ein Homomorphismus mit

$$\begin{aligned} h([m+m',n]-[m,n]-[m',n]) &= h([m+m',n]) - h([m,n]) - h([m',n]) \\ &= f(m+m',n) - f(m,n) - f(m',n) \ = \ 0, \\ h([m,n+n'] - [m,n] - [m,n']) &= \ \ldots \ = \ 0, \\ h([mr,n] - [m,rn]) &= \ \ldots \ = \ 0. \end{aligned}$$

für $m, m' \in M,\ n, n' \in N,\ r \in R$. Daher ist $h(U) = 0$. Folglich ist die Abbildung $f' : M \otimes_R N = F/U \to A,\ x + U \mapsto h(x)$ wohldefiniert und ein Homomorphismus mit $f'(m \otimes n) = f'([m,n] + U) = h([m,n]) = f(m,n)$ für $m \in M,\ n \in N$. Ist auch $f'' : M \otimes_R N \to A$ ein Homomorphismus mit $f''(m \otimes n) = f(m,n)$ für $m \in M,\ n \in N$, so ist $f''(m \otimes n) = f'(m \otimes n)$ für $m \in M,\ n \in N$, also $f'' = f'$. $\square$

Bemerkung. Wir werden diesen Satz häufig dazu benutzen, um Abbildungen auf dem Tensorprodukt zu definieren.

13.3. Satz (Universelle Charakterisierung des Tensorprodukts)**.** *Sei M ein R-Rechtsmodul, N ein R-Linksmodul, T_1, T_2 abelsche Gruppen und $t_1 : M \times N \to T_1,\ t_2 : M \times N \to T_2$ ausgeglichenen Abbildungen. Für $i = 1,2$, jede abelsche Gruppe A und jede ausgeglichene Abbildung $f : M \times N \to A$ existiere genau ein Homomorphismus $f_i : T_i \to A$ mit $f_i \circ t_i = f$.*

$$\begin{tikzcd} M \times N \arrow[rr, "t_i"] \arrow[dr, "f"'] & & T_i \arrow[dl, dotted, "f_i"] \\ & A & \end{tikzcd}$$

Dann ist der Homomorphismus $f_1 : T_1 \to T_2$ mit $f_1 \circ t_1 = t_2$ ein Isomorphismus.

Beweis. Nach Voraussetzung existieren eindeutig bestimmte Homomorphismen $f_1 : T_1 \to T_2,\ f_2 : T_2 \to T_1$ mit $f_1 \circ t_1 = t_2,\ f_2 \circ t_2 = t_1$:

$$\begin{tikzcd}
M \times N \arrow[rr, "t_1"] \arrow[dr, "t_2"'] & & T_1 \arrow[dl, dotted, "f_1"] \\
& T_2 &
\end{tikzcd}
\qquad
\begin{tikzcd}
M \times N \arrow[rr, "t_2"] \arrow[dr, "t_1"'] & & T_2 \arrow[dl, dotted, "f_2"] \\
& T_1 &
\end{tikzcd}$$

Dann ist $f_2 \circ f_1 \circ t_1 = f_2 \circ t_2 = t_1 = \mathrm{id}_{T_1} \circ t_1$ und $f_1 \circ f_2 \circ t_2 = f_1 \circ t_1 = t_2 = \mathrm{id}_{T_2} \circ t_2$:

$$\begin{tikzcd}
M \times N \arrow[rr, "t_1"] \arrow[dr, "t_1"'] & & T_1 \arrow[dl, shift right, "\mathrm{id}_{T_1}"'] \arrow[dl, shift left, "f_2 \circ f_1"] \\
& T_1 &
\end{tikzcd}
\qquad
\begin{tikzcd}
M \times N \arrow[rr, "t_2"] \arrow[dr, "t_2"'] & & T_2 \arrow[dl, shift right, "\mathrm{id}_{T_2}"'] \arrow[dl, shift left, "f_1 \circ f_2"] \\
& T_2 &
\end{tikzcd}$$

Folglich ist $\mathrm{id}_{T_1} = f_2 \circ f_1$ und $\mathrm{id}_{T_2} = f_1 \circ f_2$, d.h. f_1 und f_2 sind bijektiv. $\square$

Bemerkung. Aus dem Satz folgt insbesondere, daß das Tensorprodukt durch seine universelle Eigenschaft bis auf Isomorphie eindeutig bestimmt ist. Mit seiner Hilfe kann man manchmal den Isomorphietyp von $M \otimes_R N$ bestimmen.

13.4. Satz. *Für jedes Linksideal J in R und jeden R-Rechtsmodul M ist die Abbildung $\iota : M/MJ \to M \otimes_R (R/J),\ m + MJ \mapsto m \otimes (1 + J)$ ein Gruppenisomorphismus; dabei ist MJ die von allen Elementen der Form mj mit $m \in M,\ j \in J$ erzeugte Untergruppen von M.*

Beweis. Offenbar ist die Abbildung $\varphi : M \to M \otimes_R (R/J),\ m \mapsto m \otimes (1+J)$ ein Gruppenhomomorphismus mit

$$\varphi(mj) = mj \otimes (1 + J) = m \otimes j(1 + J) = m \otimes 0 = 0$$

für $m \in M,\ j \in J$. Daher ist $\varphi(MJ) = 0$. Folglich ist ι wohldefiniert und ein Homomorphismus. Andererseits ist die Abbildung $M \times (R/J) \to M/MJ,\ (m, r + J) \mapsto mr + MJ$ wohldefiniert und ausgeglichen, induziert also einen Gruppenhomomorphismus $\kappa : M \otimes_R (R/J) \to M/MJ$ mit $\kappa(m \otimes (r + J)) = mr + MJ$ für $m \in M,\ r \in R$. Offenbar ist $\kappa \circ \iota = \mathrm{id}$ und $\iota \circ \kappa = \mathrm{id}$, d.h. ι und κ sind bijektiv. $\square$

Bemerkung. Analog ist für jedes Rechtsideal I von R und jeden R-Linksmodul N die Abbildung $N/IN \to (R/I) \otimes_R N,\ n + IN \mapsto (1 + I) \otimes n$ ein Gruppenisomorphismus. Insbesondere erhält man also auf diese Weise Gruppenisomorphismen $M \to M \otimes_R R,\ m \mapsto m \otimes 1$ und $N \to R \otimes_R N,\ n \mapsto 1 \otimes n$. Wir nennen die so definierten Isomorphismen und ihre Umkehrabbildungen *kanonisch*.

Beispiel. Für $m, n \in \mathbb{N}$ ist

$$\begin{aligned}
(\mathbb{Z}/m\mathbb{Z}) \otimes_{\mathbf{Z}} (\mathbb{Z}/n\mathbb{Z}) &\simeq (\mathbb{Z}/n\mathbb{Z})/m(\mathbb{Z}/n\mathbb{Z}) = (\mathbb{Z}/n\mathbb{Z})/(m\mathbb{Z} + n\mathbb{Z}/n\mathbb{Z}) \\
&\simeq \mathbb{Z}/m\mathbb{Z} + n\mathbb{Z} \simeq \mathbb{Z}/\operatorname{ggT}(m,n)\mathbb{Z}.
\end{aligned}$$

13.5. Bemerkung. Mit R^o bezeichnen wir den zu R *entgegengesetzten Ring*, d.h. als abelsche Gruppe ist $R^o = R$, aber die Multiplikation $\circ$ in R^o wird definiert durch $r \circ s := sr$ für $r, s \in R$. Jeder R-Rechtsmodul M wird dann zu einem R^o-Linksmodul M^o, wenn man $r \circ m := mr$ für $r \in R,\ m \in M$ definiert. Analog wird jeder R-Linksmodul N zu einem R^o-Rechtsmodul N^o mit $n \circ r := rn$ für $r \in R,\ n \in N$.

Satz (Kommutativität des Tensorprodukts). *Mit den obigen Bezeichnungen gibt es genau einen Gruppenisomorphismus $\iota : M \otimes_R N \to N^o \otimes_{R^o} M^o$ mit $\iota(m \otimes n) = n \otimes m$ für $m \in M,\ n \in N$.*

Beweis. Die Abbildung $M \times N \to N^o \otimes_{R^o} M^o,\ (m,n) \mapsto n \otimes m$ ist offenbar ausgeglichen. Daher existiert genau ein Gruppenhomomorphismus $\iota : M \otimes_R N \to N^o \otimes_{R^o} M^o$ mit $\iota(m \otimes n) = n \otimes m$ für $m \in M,\ n \in N$. Analog existiert genau ein Gruppenhomomorphismus $\kappa : N^o \otimes_{R^o} M^o \to M \otimes_R N$ mit $\kappa(n \otimes m) = m \otimes n$ für $m \in M,\ n \in N$. Also ist $\iota \circ \kappa = \mathrm{id}$ und $\kappa \circ \iota = \mathrm{id}$; insbesondere sind ι und κ bijektiv. □

Beispiel. Ist R kommutativ, so ist $R = R^o$, und jeder R-Rechtsmodul wird auf die oben beschrieben Weise (automatisch) zu einem R-Linksmodul (und umgekehrt). Der Satz besagt dann (in etwas ungenauer Schreibweise): $M \otimes_R N \simeq N \otimes_R M$.

13.6. Bemerkung. Seien R, S Ringe und $\rho : S \to R$ ein Ringhomomorphismus. (Wir verlangen nicht $\rho(1_S) = 1_R$. Für jeden R-Rechtsmodul M ist $\mathrm{Res}_\rho\, M := M\rho(1_S)$ ein S-Rechtsmodul mit $xs := x\rho(s)$ für $x \in \mathrm{Res}_\rho\, M,\ s \in S$. Wir bezeichnen $\mathrm{Res}_\rho\, M$ als *Restriktion* von M bzgl. ρ. Für R-Rechtsmoduln M, M' und jeden R-Homomorphismus $\varphi : M \to M'$ ist $\mathrm{Res}_\rho\, \varphi : \mathrm{Res}_\rho\, M \to \mathrm{Res}_\rho\, M'$ ein S-Homomorphismus. Wir bezeichnen wir als *Restriktion* von φ bzgl. ρ. Für R-Rechtsmoduln M, M', M'' und R-Homomorphismen $\varphi : M \to M',\ \varphi' : M' \to M''$ ist $\mathrm{Res}_\rho(\varphi' \circ \varphi) = (\mathrm{Res}_\rho\, \varphi') \circ (\mathrm{Res}_\rho\, \varphi)$ und $\mathrm{Res}_\rho\, \mathrm{id}_M = \mathrm{id}_{\mathrm{Res}_\rho\, M}$. Für Ringe R, S, T und Ringhomomorphismen $\rho : S \to R,\ \sigma : T \to S$ ist ferner

$$\mathrm{Res}_\sigma(\mathrm{Res}_\rho\, M) = (M\rho(1_S))\sigma(1_T) = M\rho(1_S)\rho(\sigma(1_T)) = M\rho(\sigma(1_T)) = \mathrm{Res}_{\rho\circ\sigma}\, M$$

und analog $\mathrm{Res}_\sigma(\mathrm{Res}_\rho\, \varphi) = \mathrm{Res}_{\rho\circ\sigma}\, \varphi$.
Ist S ein Teilring von R (nicht unbedingt $1_R = 1_S$) und $\rho : S \to R$ die Inklusionsabbildung, so schreiben wir Res_S^R statt Res_ρ. Ist $R = S/I$ für ein Ideal I von S und $\rho : S \to R$ der kanonische Epimorphismus, so schreiben wir Inf_I^S und sprechen von der *Inflation*. Ähnlich können wir mit Linksmoduln vorgehen.

13.7. Bemerkung. Seien R, S Ringe, $\rho : S \to R$ ein Ringhomomorphismus, M ein R-Rechtsmodul und N ein R-Linksmodul. Dann ist die Abbildung $\mathrm{Res}_\rho\, M \times \mathrm{Res}_\rho\, N \to M \otimes_R N,\ (m,n) \mapsto m \otimes n$ ausgeglichen, induziert also einen $\mathbb{Z}$-Homomorphismus $\gamma : \mathrm{Res}_\rho\, M \otimes_S \mathrm{Res}_\rho\, N \to M \otimes_R N$ mit $\gamma(m \otimes n) = m \otimes n$ für $m \in M,\ n \in N$. Wir bezeichnen γ als *kanonisch*. Ist ρ unitär (d.h. $\rho(1_S) = 1_R$), so ist γ surjektiv wegen $\mathrm{Res}_\rho\, M = M$ und $\mathrm{Res}_\rho\, N = N$, aber i.a. nicht injektiv.

Satz. *Mit den obigen Bezeichnungen gilt: Ist ρ surjektiv, so ist γ ein Isomorphismus.*

Beweis. Ist ρ surjektiv, so ist auch die Abbildung $M \times N \to M \otimes_S N,\ (m,n) \mapsto m \otimes n$ ausgeglichen, induziert also einen Homomorphismus $\delta : M \otimes_R N \to M \otimes_S N$ mit $\delta(m \otimes n) = m \otimes n$ für $m \in M,\ n \in N$. Offenbar ist $\delta \circ \gamma = \mathrm{id}$ und $\gamma \circ \delta = \mathrm{id}$; insbesondere ist γ bijektiv. □

Beispiel. Für jedes Ideal I von S (und $R = S/I$) ist also $\mathrm{Inf}_I^S\, M \otimes_S \mathrm{Inf}_I^S\, N \simeq M \otimes_{S/I} N$.

KAPITEL 14

Das Tensorprodukt von Homomorphismen

Sei R ein Ring.

14.1. Satz. *Seien M, M' R-Rechtsmoduln, N, N' R-Linksmoduln und $\varphi : M \to M'$, $\psi : N \to N'$ R-Homomorphismen. Dann existiert genau ein $\mathbb{Z}$-Homomorphismus $\pi : M \otimes_R N \to M' \otimes_R N'$ mit $\pi(m \otimes n) = \varphi(m) \otimes \psi(n)$ für $m \in M,\ n \in N$.*

Definition. Wir nennen π das *Tensorprodukt* von φ und ψ und schreiben $\pi = \varphi \otimes \psi$.

Beweis. Die Aussage folgt aus 13.2, da die Abbildung $M \times N \to M' \otimes_R N',\ (m,n) \mapsto \varphi(m) \otimes \psi(n)$ offenbar ausgeglichen ist. □

Bemerkung. Für jeden R-Rechtsmodul M'', jeden R-Linksmodul N'' und R-Homomorphismen $\varphi' : M' \to M'',\ \psi' : N' \to N''$ ist $(\varphi' \otimes \psi') \circ (\varphi \otimes \psi) = (\varphi' \circ \varphi) \otimes (\psi' \circ \psi)$ wegen

$$\begin{aligned}(\varphi' \otimes \psi')((\varphi \otimes \psi)(m \otimes n)) &= (\varphi' \otimes \psi')(\varphi(m) \otimes \psi(n))\\ &= \varphi'(\varphi(m)) \otimes \psi'(\psi(n))\\ &= ((\varphi' \circ \varphi) \otimes (\psi' \circ \psi))(m \otimes n)\end{aligned}$$

für $m \in M,\ n \in N$. Analog ist

$$\begin{aligned}\mathrm{id}_M \otimes \mathrm{id}_N &= \mathrm{id}_{M \otimes_R N},\\ (\varphi_1 + \varphi_1) \otimes \psi &= \varphi_1 \otimes \psi + \varphi_2 \otimes \psi,\\ \varphi \otimes (\psi_1 + \psi_2) &= \varphi \otimes \psi_1 + \varphi \otimes \psi_2\end{aligned}$$

für R-Homomorphismen $\varphi_1, \varphi_2 : M \to M',\ \psi_1, \psi_2 : N \to N'$. Das bedeutet, daß die Abbildung

$$\mathrm{Hom}_R(M, M') \times \mathrm{Hom}_R(N, N') \to \mathrm{Hom}_{\mathbf{Z}}(M \otimes_R N, M' \otimes_R N'),\ (\varphi, \psi) \mapsto \varphi \otimes \psi$$

eine ausgeglichene Abbildung von $\mathbb{Z}$-Moduln ist. Mit 13.2 erhalten wir einen $\mathbb{Z}$-Homomorphismus

$$\Phi : \mathrm{Hom}_R(M, M') \otimes_{\mathbf{Z}} \mathrm{Hom}_R(N, N') \to \mathrm{Hom}_{\mathbf{Z}}(M \otimes_R N, M' \otimes_R N')$$

mit $\Phi(\varphi \otimes \psi) = \varphi \otimes \psi$ für $\varphi \in \mathrm{Hom}_R(M, M'),\ \psi \in \mathrm{Hom}_R(N, N')$. Wir bezeichnen Φ als *kanonisch.* I.a. ist Φ weder injektiv noch surjektiv. Die gleiche Bezeichnung $\varphi \otimes \psi$ für verschiedene Elemente in beiden Mengen ist also irreführend.

14.2. Bemerkung. Seien $(M_i)_{i \in I}$ eine Familie von R-Rechtsmoduln und $(N_j)_{j \in J}$ eine Familie von R-Linksmoduln. Für $k \in I,\ l \in J$ bezeichnen wir mit $\pi_k : \prod_{i \in I} M_i \to M_k,\ \rho_l : \prod_{j \in J} N_j \to N_l$ die entsprechenden Projektionen. Dann ist $\pi_k \otimes \rho_l : (\prod_{i \in I} M_i) \otimes_R (\prod_{j \in J} N_j) \to M_k \otimes_R N_l$ ein $\mathbb{Z}$-Homomorphismus. Folglich ist auch die Abbildung

$$\sigma : \left(\prod_{i \in I} M_i\right) \otimes_R \left(\prod_{j \in J} N_j\right) \to \prod_{k \in I, l \in J} (M_k \otimes_R N_l),\ x \mapsto \big((\pi_k \otimes \rho_l)(x)\big)_{k \in I, l \in J}$$

ein $\mathbb{Z}$-Homomorphismus. Wir bezeichnen ihn als *kanonisch.* I.a. ist er weder injektiv noch surjektiv. Für $m = (m_i)_{i \in I} \in \prod_{i \in I} M_i$ und $n = (n_j)_{j \in J} \in \prod_{j \in J} N_j$ ist explizit $\sigma(m \otimes n) = (m_k \otimes n_l)_{k \in I, l \in J}$. Im Fall $m \in \coprod_{i \in I} M_i,\ n \in \coprod_{j \in J} \mathbb{N}_j$ ist also $\sigma(m \otimes n) \in \coprod_{k \in I, l \in J} M_k \otimes_R N_l$. Wir erhalten also einen $\mathbb{Z}$-Homomorphismus

$$\tau : \left(\coprod_{i \in I} M_i\right) \otimes_R \left(\coprod_{j \in J} N_j\right) \to \coprod_{k \in I, l \in J} (M_k \otimes_R N_l)$$

mit $\tau(m \otimes n) = (m_k \otimes n_l)_{k\in I, l\in J}$ für $m = (m_i)_{i\in I} \in \coprod_{i\in I} M_i,\ n = (n_j)_{j\in J} \in \coprod_{j\in J} N_j$. Wir bezeichnen τ als *kanonisch.*

Satz (Distributivität des Tensorprodukts). *Mit den obigen Bezeichnungen ist τ ein Isomorphismus.*

Beweis. Für $k \in I,\ l \in J$ seien $\iota_k : M_k \to \coprod_{i\in I} M_i,\ \kappa_l : N_l \to \coprod_{j\in J} N_j$ die entsprechenden Injektionen. Dann ist $\iota_k \otimes \kappa_l : M_k \otimes_R N_l \to (\coprod_{i\in I} M_i) \otimes (\coprod_{j\in J} N_j)$ ein $\mathbb{Z}$-Homomorphismus. Zusammen ergibt das einen $\mathbb{Z}$-Homomorphismus

$$\begin{aligned}\lambda : \coprod_{k\in I, l\in J} (M_k \otimes_R N_l) &\to \left(\coprod_{i\in I} M_i\right) \otimes_R \left(\coprod_{j\in J} N_j\right),\\ (x_{kl})_{k\in I, l\in J} &\mapsto \sum_{k\in I, l\in J} (\iota_k \otimes \kappa_k)(x_{kl});\end{aligned}$$

insbesondere gilt dann für $(m_k)_{k\in I} \in \coprod_{i\in I} M_i,\ (n_l)_{l\in J} \in \coprod_{j\in J} N_j$:

$$\begin{aligned}\lambda((m_k \otimes n_l)_{k\in I, l\in J}) &= \sum_{k\in I, l\in J} \iota_k(m_k) \otimes \kappa_l(n_l)\\ &= \left(\sum_{k\in I} \iota_k(m_k)\right) \otimes \left(\sum_{l\in J} \kappa_l(n_l)\right)\\ &= (m_k)_{k\in I} \otimes (n_l)_{l\in J}\end{aligned}$$

und

$$\tau(\lambda((m_k \otimes n_l)_{k\in I, l\in J})) = (m_k \otimes n_l)_{k\in I, l\in J}.$$

Folglich ist $\tau \circ \lambda = \mathrm{id}$, und analog ist $\lambda \circ \tau = \mathrm{id}$. □

14.3. Satz. *Seien M ein freier R-Rechtsmodul mit Basis B und N ein R-Linksmodul. Dann läßt sich jedes Element in $M \otimes_R N$ in der Form $\sum_{b\in B} b \otimes n_b$ mit eindeutig bestimmten $n_b \in N$ beschreiben, von denen nur endlich viele von 0 verschieden sind; insbesondere ist $M \otimes_R N \simeq \coprod_{b\in B} N$.*

Beweis. Die Abbildung $\iota : \coprod_{b\in B} R \to M,\ (r_b)_{b\in B} \mapsto \sum_{b\in B} br_b$ ist ein R-Isomorphismus. Daher ist $\iota \otimes \mathrm{id}_N : (\coprod_{b\in B} R) \otimes_R N \to M \otimes_R N$ ein Gruppenisomorphismus. Nach 14.2 hat man einen $\mathbb{Z}$-Isomorphismus $\tau : (\coprod_{b\in B} R) \otimes_R N \to \coprod_{b\in B} (R \otimes_R N)$ mit $\tau((r_b)_{b\in B} \otimes n) = (r_b \otimes n)_{b\in B}$ für $(r_b)_{b\in B} \in \coprod_{b\in B} R,\ n \in N$. Nach 13.4 ist außerdem $\mu : N \to R \otimes_R N,\ n \mapsto 1 \otimes n$ ein $\mathbb{Z}$-Isomorphismus. Insgesamt erhalten wir also einen $\mathbb{Z}$-Homomorphismus $\varphi : \coprod_{b\in B} N \to M \otimes_R N$ mit $\varphi((n_b)_{b\in B}) = \sum_{b\in B} b \otimes n_b$ für $(n_b)_{b\in B} \in \coprod_{b\in B} N$. □

14.4. Satz. *Für jede exakte Folge $M \xrightarrow{\varphi} M' \xrightarrow{\varphi'} M'' \longrightarrow 0$ von R-Rechtsmoduln und jede exakte Folge $N \xrightarrow{\psi} N' \xrightarrow{\psi'} N'' \longrightarrow 0$ von R-Linksmoduln ist die folgende Sequenz von abelschen Gruppen exakt:*

$$0 \longrightarrow \mathrm{Bild}(\varphi \otimes \mathrm{id}_{N'}) + \mathrm{Bild}(\mathrm{id}_{M'} \otimes \psi) \xrightarrow{\alpha} M' \otimes_R N' \xrightarrow{\varphi' \otimes \psi'} M'' \otimes_R N'' \longrightarrow 0;$$

dabei ist α die entsprechende Inklusionsabbildung.

Beweis. Mit φ' und ψ' ist auch $\varphi' \otimes \psi'$ surjektiv. Wegen $(\varphi' \otimes \psi') \circ (\varphi \otimes \mathrm{id}_{N'}) = (\varphi' \circ \varphi) \otimes \psi' = 0 \otimes \psi' = 0$ ist $\mathrm{Bild}(\varphi \otimes \mathrm{id}_{N'}) \subseteq \mathrm{Ker}(\varphi' \otimes \psi') =: K$. Analog ist $\mathrm{Bild}(\mathrm{id}_{M'} \otimes \psi) \subseteq K$, also $B := \mathrm{Bild}(\varphi \otimes \mathrm{id}_{N'}) + \mathrm{Bild}(\mathrm{id}_{M'} \otimes \psi) \subseteq K$. Daher ist die Abbildung

$$\beta : M' \otimes_R N'/B \to M'' \otimes_R N'',\ x + B \mapsto (\varphi' \otimes \psi')(x)$$

wohldefiniert und ein Gruppenhomomorphismus. Umgekehrt definieren wir eine Abbildung $\gamma : M'' \times N'' \to M' \otimes_R N'/B$ durch $\gamma(\varphi'(m'), \psi'(n')) = m' \otimes n' + B$ für $m' \in M',\ n' \in N'$. Dies ist wohldefiniert; ist nämlich $m_1' \in M'$ mit $\varphi'(m') = \varphi'(m_1')$, so ist $m_1' - m' \in \mathrm{Ker}(\varphi') = \mathrm{Bild}(\varphi)$, also $m_1' - m' = \varphi(m)$ für ein $m \in M$ und daher

$$m_1' \otimes n' + B = m' \otimes n' + \varphi(m) \otimes n' + B = m' \otimes n' + B.$$

Offenbar ist γ ausgeglichen, induziert also einen $\mathbb{Z}$-Homomorphismus $\delta : M'' \otimes_R N'' \to M' \otimes_R N'/B$ mit $\delta(\varphi'(m') \otimes \psi'(n')) = m' \otimes n' + B$ für $m' \in M',\ n' \in N'$. Wegen

$$\delta(\beta(m' \otimes n' + B)) = \delta((\varphi' \otimes \psi')(m' \otimes n')) = \delta(\varphi'(m') \otimes \psi'(n')) = m' \otimes n' + B$$

für $m' \in M',\ n' \in N'$ ist $\delta \circ \beta = \mathrm{id}$; insbesondere ist β injektiv. Für $k \in K$ ist $\beta(k+B) = (\varphi' \otimes \psi')(k) = 0$, also $k + B = 0$ und $k \in B$. Dies zeigt: $B = K$. □

Bemerkung.

(i) Für jede exakte Folge $M \xrightarrow{\varphi} M' \xrightarrow{\varphi'} M'' \longrightarrow 0$ von R-Rechtsmoduln und jeden R-Linksmodul N ist also wegen der Exaktheit von $0 \longrightarrow N \xrightarrow{\mathrm{id}_N} N \longrightarrow 0$ die Folge $M \otimes_R N \xrightarrow{\varphi \otimes \mathrm{id}_N} M' \otimes_R N \xrightarrow{\varphi' \otimes \mathrm{id}_N} M'' \otimes_R N \longrightarrow 0$ exakt.

(ii) Analog ist für jeden R-Rechtsmodul M und jede exakte Folge $N \xrightarrow{\psi} N' \xrightarrow{\psi'} N'' \longrightarrow 0$ von R-Linksmoduln die folgende Sequenz exakt: $M \otimes_R N \xrightarrow{\mathrm{id}_M \otimes \psi} M \otimes_R N' \xrightarrow{\mathrm{id}_M \otimes \psi'} M \otimes_R N'' \longrightarrow 0$.

(iii) Jedoch folgt aus der Exaktheit von $0 \longrightarrow M \xrightarrow{\varphi} M'$ (bzw. $0 \longrightarrow N \xrightarrow{\psi} N'$) i.a. nicht die Exaktheit von $0 \longrightarrow M \otimes_R N \xrightarrow{\varphi \otimes \mathrm{id}_N} M' \otimes_R N$ (bzw. $0 \longrightarrow M \otimes_R N \xrightarrow{\mathrm{id}_M \otimes \psi} M \otimes_R N'$).

(iv) Seien M, N Untermoduln von M', N' und $\varphi : M \to M',\ \psi : N \to N'$ die entsprechenden Inklusionsabbildungen. Auch in diesem Fall ist i.a. die *kanonische* Abbildung $\varphi \otimes \psi : M \otimes_R N \to M' \otimes_R N'$ nicht injektiv. Für Elemente $m \in M,\ n \in N$ muß man also zwischen dem Element $m \otimes n$ in $M \otimes_R N$ und dem Element $m \otimes n = (\varphi \otimes \psi)(m \otimes n)$ in $M' \otimes_R N'$ unterscheiden.

(v) Sind $0 \longrightarrow M \xrightarrow{\varphi} M'$ und $0 \longrightarrow N \xrightarrow{\psi} N'$ exakt und zerfallend, so auch $0 \longrightarrow M \otimes_R N \xrightarrow{\varphi \otimes \psi} M' \otimes_R N'$; denn sind $\varphi' : M' \to M,\ \psi' : N' \to N$ R-Homomorphismen mit $\varphi' \circ \varphi = \mathrm{id}_M,\ \psi' \circ \psi = \mathrm{id}_N$, so ist $\varphi' \otimes \psi' : M' \otimes_R N' \to M \otimes_R N$ ein $\mathbb{Z}$-Homomorphismus mit

$$(\varphi' \otimes \psi') \circ (\varphi \otimes \psi) = (\varphi' \circ \varphi) \otimes (\psi' \circ \psi) = \mathrm{id}_M \otimes \mathrm{id}_N = \mathrm{id}_{M \otimes_R N}\,.$$

Definition. Man nennt einen R-Linksmodul N *flach*, falls $\varphi \otimes \mathrm{id}_N : M \otimes_R N \to M' \otimes_R N$ für jeden R-Monomorphismus $\varphi : M \to M'$ injektiv ist. Analog definiert man flache R-Rechtsmoduln.

Beispiel. Als R-Linksmodul (und analog als R-Rechtsmodul) ist R selbst flach; denn ist $\varphi : M \to M'$ ein R-Monomorphismus und bezeichnen $\iota : M \otimes_R R \to M,\ \iota' : M' \otimes_R R \to M'$ die kanonischen Isomorphismen aus 13.4, so gilt für $m \in M,\ r \in R$:

$$\iota'((\varphi \otimes \mathrm{id}_R)(m \otimes r)) = \iota'(\varphi(m) \otimes r) = \varphi(m)r = \varphi(mr) = \varphi(\iota(m \otimes r)).$$

Folglich ist $\iota' \circ (\varphi \otimes \mathrm{id}_R) = \varphi \circ \iota$.

$$\begin{tikzcd}
M \otimes_R R \arrow[r, "\varphi \otimes \mathrm{id}_R"] \arrow[d, "\iota"] & M' \otimes_R R \arrow[d, "\iota'"] \\
M \arrow[r, "\varphi"] & M'
\end{tikzcd}$$

Mit φ ist also auch $\varphi \otimes \mathrm{id}_R$ injektiv.

14.5. Satz. *Direkte Summen und direkte Summanden von flachen R-Linksmoduln (R-Rechtsmoduln) sind wieder flach. Insbesondere sind freie und allgemeiner projektive R-Linksmoduln (R-Rechtsmoduln) flach.*

Beweis. Seien $\varphi : M \to M'$ ein R-Monomorphismus, $(N_i)_{i \in I}$ eine Familie von R-Linksmoduln, $N := \coprod_{i \in I} N_i$, $\tau : M \otimes_R (\coprod_{i \in I} N_i) \to \coprod_{i \in I} (M \otimes_R N_i)$ und $\tau' : M' \otimes_R (\coprod_{i \in I} N_i) \to \coprod_{i \in I} (M' \otimes_R N_i)$ die kanonischen Isomorphismen aus 14.2 und $\coprod_{i \in I} (\varphi \otimes \mathrm{id}_{N_i}) : \coprod_{i \in I} (M \otimes_R N_i) \to \coprod_{i \in I} (M' \otimes_R N_i),\ (x_i)_{i \in I} \mapsto$

$((\varphi \otimes \mathrm{id}_{N_i})(x_i))_{i\in I}$.

$$\begin{tikzcd}
M \otimes_R \left(\coprod_{i\in I} N_i\right) \arrow[r, "\varphi\otimes\mathrm{id}_N"] \arrow[d, "\tau"'] & M' \otimes_R \left(\coprod_{i\in I} N_i\right) \arrow[d, "\tau'"] \\
\coprod_{i\in I}(M \otimes_R N_i) \arrow[r, "\coprod_{i\in I}(\varphi\otimes\mathrm{id}_{N_i})"] & \coprod_{i\in I}(M' \otimes_R N_i)
\end{tikzcd}$$

Für $m \in M$ und $n = (n_i)_{i\in I}$ ist dann

$$\begin{aligned}
\tau'((\varphi \otimes \mathrm{id}_N)(m \otimes n)) &= \tau'(\varphi(m) \otimes n) \;=\; (\varphi(m) \otimes n_i)_{i\in I} \\
&= \left(\coprod_{i\in I}(\varphi \otimes \mathrm{id}_{N_i})\right)((m \otimes n_i)_{i\in I}) \\
&= \left(\coprod_{i\in I}(\varphi \otimes \mathrm{id}_{N_i})\right)(\tau(m \otimes n)).
\end{aligned}$$

Folglich ist $\tau' \circ (\varphi \otimes \mathrm{id}_N) = (\coprod_{i\in I}(\varphi \otimes \mathrm{id}_{N_i})) \circ \tau$. Es gilt also: $\varphi \otimes \mathrm{id}_N$ injektiv $\iff$ $\coprod_{i\in I}(\varphi \otimes \mathrm{id}_{N_i})$ injektiv $\iff$ $\forall i \in I : \varphi \otimes \mathrm{id}_{N_i}$ injektiv. Damit ist die erste Aussage bewiesen. Da R selbst flach ist, ist auch $\coprod_{i\in I} R$ flach und jeder direkte Summand hiervon. $\square$

Bemerkung. Für einen flachen R-Linksmodul N, einen R-Rechtsmodul M' und einen Untermodul M von M' ist die kanonische Abbildung $\lambda : M \otimes_R N \to M' \otimes_R N$ injektiv. Wir können (und werden) also $M \otimes_R N$ mit $\lambda(M \otimes_R N)$ identifizieren und so als Untergruppe von $M' \otimes_R N$ auffassen.

KAPITEL 15

Bimoduln

15.1. Definition. Seien R, S Ringe. Ein *R-S-Bimodul* ist eine Menge M mit Verknüpfungen

$$\begin{array}{ll} M \times M \to M, & (m,n) \mapsto m+n, \\ R \times M \to M, & (r,m) \mapsto rm, \\ M \times S \to M, & (m,s) \mapsto ms, \end{array}$$

so daß M ein R-Linksmodul und ein S-Rechtsmodul mit $(rm)s = r(ms)$ für $r \in R,\ m \in M,\ s \in S$ ist.

Beispiel. Jedes Ideal in R ist ein R-R-Bimodul; insbesondere ist R selbst ein R-R-Bimodul.

Bemerkung. Es ist klar, daß sich viele Aussagen und Begriffe von Moduln auf Bimoduln übertragen. Dies werden wir jeweils stillschweigend tun.

Satz. *Seien R, S Ringe, M ein R-Rechtsmodul und N ein R-S-Bimodul. Dann existiert eine Verknüpfung $(M \otimes_R N) \times S \to M \otimes_R N,\ (x,s) = xs$, so daß $M \otimes_R N$ ein S-Rechtsmodul mit $(m \otimes n)s = m \otimes ns$ für $m \in M,\ n \in N,\ s \in S$ wird.*

Beweis. Für $s \in S$ ist die Abbildung $M \times N \to M \otimes_R N,\ (m,n) \mapsto m \otimes ns$ ausgeglichen, induziert also einen $\mathbb{Z}$-Homomorphismus $\mu_s : M \otimes_R N \to M \otimes_R N$ mit $\mu_s : (m \otimes n) = m \otimes ns$ für $m \in M,\ n \in N$. Wir definieren die gesuchte Verknüpfung durch $xs := \mu_s(x)$ für $x \in M \otimes_R N,\ s \in S$. Dann ist

$$\begin{aligned} (x+y)s &= \mu_s(x+y) = \mu_s(x) + \mu_s(y) = xs + ys, \\ (m \otimes n)s &= \mu_s(m \otimes n) = m \otimes ns \end{aligned}$$

für $x, y \in M \otimes_R N,\ s \in S,\ m \in M,\ n \in N$. Sind $s, t \in S,\ x \in M \otimes_R N$ und $m_1, \ldots, m_k \in M,\ n_1, \ldots, n_k \in N$ mit $x = \sum_{i=1}^k m_i \otimes n_i$, so ist:

$$\begin{aligned} x(s+t) &= \mu_{s+t}(x) \ = \ \sum_{i=1}^k \mu_{s+t}(m_i \otimes n_i) \ = \ \sum_{i=1}^k m_i \otimes n_i(s+t) \\ &= \sum_{i=1}^k m_i \otimes (n_i s + n_i t) \ = \ \sum_{i=1}^k m_i \otimes n_i s + m_i \otimes n_i t \\ &= \sum_{i=1}^k \mu_s(m_i \otimes n_i) + \sum_{i=1}^k \mu_t(m_i \otimes n_i) \ = \ \mu_s(x) + \mu_t(x) \\ &= xs + xt, \\ x(st) &= \mu_{st}(x) \ = \ \sum_{i=1}^k \mu_{st}(m_i \otimes n_i) \ = \ \sum_{i=1}^k m_i \otimes n_i(st) \\ &= \sum_{i=1}^k m_i \otimes (n_i s)t \ = \ \sum_{i=1}^k \mu_t(\mu_s(m_i \otimes n_i)) \\ &= \mu_t(\mu_s(x)) \ = \ (xs)t, \\ x1_S &= \mu_1(x) \ = \ \sum_{i=1}^k \mu_1(m_i \otimes n_i) \ = \ \sum_{i=1}^k m_i \otimes n_i 1 \ = \ \sum_{i=1}^k m_i \otimes n_i \ = \ x. \end{aligned}$$

□

15.2. Bemerkung. Seien R, S Ringe, M ein R-Rechtsmodul, N ein R-S-Bimodul, A ein S-Rechtsmodul und $f : M \times N \to A$ eine ausgeglichene Abbildung mit $f(m, ns) = f(m, n)s$ für $m \in M,\ n \in N,\ s \in S$. Dann ist der nach 13.2 eindeutig bestimmte $\mathbb{Z}$-Homomorphismus $f' : M \otimes_R N \to A$ mit $f'(m \otimes n) = f(m, n)$ für $m \in M,\ n \in N$ ein S-Homomorphismus; denn für $s \in S,\ x \in M \otimes_R N$ und $m_1, \ldots, m_k \in M,\ n_1, \ldots, n_k \in N$ mit $x = \sum_{i=1}^k m_i \otimes n_i$ gilt:

$$\begin{aligned} f'(xs) &= f'\left(\sum_{i=1}^k m_i \otimes n_i s\right) = \sum_{i=1}^k f(m_i, n_i s) = \sum_{i=1}^k f(m_i, n_i)s \\ &= \sum_{i=1}^k f'(m_i \otimes n_i)s = f'(x)s. \end{aligned}$$

Daher sind viele der in Kapitel 13 und 14 konstruierten Gruppenhomomorphismen zwischen Tensorprodukten sogar S-Homomorphismen, wenn die beteiligten R-Linksmoduln sogar R-S-Bimoduln sind. Ausführlich gehen wir darauf nicht ein. Z.B. ist der kanonische Isomorphismus $M \otimes_R R \to M$ ein R-Isomorphismus, und für jeden R-Homomorphismus $\varphi : M \to M'$ und jeden R-S-Homomorphismus $\psi : N \to N'$ ist $\varphi \otimes \psi : M \otimes_R N \to M' \otimes_R N'$ ein S-Homomorphismus. Entsprechende Aussagen gelten natürlich auch auf der anderen Seite. Ist Q ein weiterer Ring, M ein Q-R-Bimodul und N ein R-S-Bimodul, so ist $M \otimes_R N$ ein Q-S-Bimodul, denn für $q \in Q,\ s \in S,\ x \in M \otimes_R N$ und $m_1, \ldots, m_k \in M,\ n_1, \ldots, n_k \in N$ mit $x = \sum_{i=1}^k m_i \otimes n_i$ ist:

$$q(xs) = q\sum_{i=1}^k m_i \otimes n_i s = \sum_{i=1}^k q m_i \otimes n_i s = \left(\sum_{i=1}^k q m_i \otimes n_i\right)s = (qx)s.$$

15.3. Satz (Assoziativität des Tensorprodukts)**.** *Seien R, S Ringe, L ein R-Rechtsmodul, M ein R-S-Bimodul und N ein S-Linksmodul. Dann existiert genau ein $\mathbb{Z}$-Isomorphismus $\psi : (L \otimes_R M) \otimes_S N \to L \otimes_R (M \otimes_S N)$ mit $\psi((l \otimes m) \otimes n) = l \otimes (m \otimes n)$ für $l \in L,\ m \in M,\ n \in N$.*

Beweis. Für $n \in N$ ist die Abbildung $L \times M \to L \otimes_R (M \otimes_S N),\ (l, m) \mapsto l \otimes (m \otimes n)$ ausgeglichen, induziert also einen $\mathbb{Z}$-Homomorphismus $\varphi_n : L \otimes_R M \to L \otimes_R (M \otimes_S N)$ mit $\varphi_n(l \otimes m) = l \otimes (m \otimes n)$ für $l \in L,\ m \in M$. Für $n, n' \in N,\ s \in S,\ x \in L \otimes_R M$ und $l_1, \ldots, l_k \in L,\ m_1, \ldots, m_k \in M$ mit $x = \sum_{i=1}^k l_i \otimes m_i$ ist

$$\begin{aligned} \varphi_n(xs) &= \varphi_n\left(\sum_{i=1}^k l_i \otimes m_i s\right) = \sum_{i=1}^k l_i \otimes (m_i s \otimes n) \\ &= \sum_{i=1}^k l_i \otimes (m_i \otimes sn) = \sum_{i=1}^k \varphi_{sn}(l_i \otimes m_i) \\ &= \varphi_{sn}(x), \\ \varphi_{n+n'}(x) &= \sum_{i=1}^k \varphi_{n+n'}(l_i \otimes m_i) = \sum_{i=1}^k l_i \otimes (m_i \otimes (n + n')) \\ &= \sum_{i=1}^k l_i \otimes (m_i \otimes n) + l_i \otimes (m_i \otimes n') \\ &= \sum_{i=1}^k l_i \otimes (m_i \otimes n) + \sum_{i=1}^k l_i \otimes (m_i \otimes n') \\ &= \varphi_n(x) + \varphi_{n'}(x). \end{aligned}$$

Daher ist die Abbildung $(L \otimes_R M) \times N \to L \otimes_R (M \otimes_S N),\ (x, n) \mapsto \varphi_n(x)$ ausgeglichen, induziert also einen $\mathbb{Z}$-Homomorphismus $\psi : (L \otimes_R M) \otimes_S N \to L \otimes_R (M \otimes_S N)$ mit $\psi(x \otimes n) = \varphi_n(x)$ für $x \in L \otimes_R M,\ n \in N$, d.h.

$$\psi((l \otimes m) \otimes n) = \varphi_n(l \otimes m) = l \otimes (m \otimes n)$$

für $l \in L,\ m \in M,\ n \in N$. Analog existiert ein $\mathbb{Z}$-Homomorphismus $\omega : L \otimes_R (M \otimes_S N) \to (L \otimes_R M) \otimes_S N$ mit $\omega(l \otimes (m \otimes n)) = (l \otimes m) \otimes n$ für $l \in L,\ m \in M,\ n \in N$. Dann ist $\psi \circ \omega = \mathrm{id}$ und $\omega \circ \psi = \mathrm{id}$; insbesondere ist ψ bijektiv. Ferner ist ψ eindeutig bestimmt. □

Bemerkung. Sind auch Q, T Ringe, ist L ein Q-R-Bimodul und N ein S-T-Bimodul, so ist ψ ein Q-T-Isomorphismus, wie man leicht nachrechnet.

15.4. Bemerkung. Seien R, S Ringe und $\rho : S \to R$ ein Ringhomomorphismus. Dann ist $R\rho(1_S)$ ein R-S-Bimodul mit $xs = x\rho(s)$ für $x \in R\rho(1_S),\ s \in S$. Für jeden S-Linksmodul M ist also $\mathrm{Ind}_\rho M := R\rho(1_S) \otimes_S M$ ein R-Linksmodul. Wir bezeichnen ihn als *Induktion* von M bzgl. ρ. Für S-Linksmoduln M, M' und jeden S-Homomorphismus $\varphi : M \to M'$ ist $\mathrm{Ind}_\rho \varphi := \mathrm{id}_{R\rho(1_S)} \otimes \varphi : \mathrm{Ind}_\rho M \to \mathrm{Ind}_\rho M'$ ein R-Homomorphismus. Wir bezeichnen ihn als *Induktion* von φ bzgl. ρ.
Für S-Linksmoduln M, M', M'' und S-Homomorphismen $\varphi : M \to M',\ \varphi' : M' \to M''$ ist $\mathrm{Ind}_\rho(\varphi' \circ \varphi) = \mathrm{Ind}_\rho \varphi' \circ \mathrm{Ind}_\rho \varphi$ und $\mathrm{Ind}_\rho \mathrm{id}_M = \mathrm{id}_{\mathrm{Ind}_\rho M}$. Für Ringe R, S, T, Ringhomomorphismen $\rho : S \to T,\ \sigma : T \to S$ und jeden T-Linksmodul N ist ferner

$$\begin{aligned}
\mathrm{Ind}_\rho(\mathrm{Ind}_\sigma N) &= R\rho(1_S) \otimes_S (S\sigma(1_T) \otimes_T N) \\
&\simeq (R\rho(1_S) \otimes_S S\sigma(1_T)) \otimes_T N \\
&\simeq (R\rho(1_S) \otimes_S S/S(1_S - \sigma(1_T))) \otimes_T N \\
&\simeq (R\rho(1_S)/R\rho(1_S) \cdot S(1_S - \sigma(1_T))) \otimes_T N \\
&= (R\rho(1_S)/R(\rho(1_S) - \rho(\sigma(1_T)))) \otimes_T N \\
&\simeq R\rho(\sigma(1_T)) \otimes_T N \\
&= \mathrm{Ind}_{\rho\circ\sigma} N;
\end{aligned}$$

denn es ist $S = S\sigma(1_T) \oplus S(1_S - \sigma(1_T))$ und $R\rho(1_S) = R\rho(\sigma(1_T)) \oplus R(\rho(1_S) - \rho(\sigma(1_T)))$, wie man leicht nachrechnet.
Ist S ein Teilring von R und $\rho : S \to R$ die Inklusionsabbildung, so schreiben wir Ind_S^R statt Ind_ρ. Ist S ein unitärer Teilring von R und N frei über S mit Basis B, so ist $\mathrm{Ind}_S^R N$ frei über R mit Basis $\{1_R \otimes b : b \in B\}$. Auf diese Weise wird z.B. aus jedem reellem Vektorraum ein komplexer Vektorraum gleicher Dimension konstruiert. Ähnlich kann man für Rechtsmoduln vorgehen.

Satz. *Für jeden Ring R, jeden inneren Automorphismus α von R und jeden R-Linksmodul M ist* $\mathrm{Res}_\alpha M \simeq M \simeq \mathrm{Ind}_\alpha M$.

Beweis. Sei $u \in R^\times$ mit $\alpha(r) = u^{-1}ru$ für $r \in R$. Dann ist $\varphi : \mathrm{Res}_\alpha M \to M,\ m \mapsto um$ ein $\mathbb{Z}$-Isomorphismus mit

$$r\varphi(m) = rum = u(u^{-1}ru)m = \varphi(\alpha(r)m)$$

für $r \in R,\ m \in M$, d.h. φ ist R-Homomorphismus.
Die Abbildung $\omega : R \times M \to M,\ (r, m) \mapsto ru^{-1}m$ induziert wegen

$$\omega(r\alpha(s), m) = ru^{-1}suu^{-1}m = ru^{-1}sm = \omega(r, sm)$$

für $r, s \in R,\ m \in M$ einen $\mathbb{Z}$-Homomorphismus $\psi : \mathrm{Ind}_\alpha M \to M$ mit $\psi(r \otimes m = ru^{-1}m$ für $r \in R,\ m \in M$. Andererseits ist $\chi : M \to \mathrm{Ind}_\alpha M,\ m \mapsto u \otimes m$ ein $\mathbb{Z}$-Homomorphismus mit $\chi \circ \varphi = \mathrm{id}$ und $\psi \circ \chi = \mathrm{id}$. Wegen

$$\chi(rm) = u \otimes rm = u\alpha(r) \otimes m = ru \otimes m = r(u \otimes m) = r\chi(m)$$

für $r \in R,\ m \in M$ ist χ ein R-Homomorphismus. □

15.5. Bemerkung. Seien R, S Ringe, $\rho : S \to R$ ein Ringhomomorphismus und M ein R-Linksmodul. Dann ist $\rho(1_S)R$ ein S-R-Bimodul mit

$$\rho(1_S)R \otimes_R M \simeq R/(1_R - \rho(1_S))R \otimes_R M \simeq M/(1_R - \rho(1_S))M \simeq \rho(1_S)M = \mathrm{Res}_\rho M.$$

Daher kann man auch die Restriktion von Moduln als Tensorprodukt auffassen.

15.6. Bemerkung. Ist R ein kommutativer Ring, so kann man jeden R-Rechtsmodul nach 13.5 auch also R-Linksmodul auffassen. Auf diese Weise wird M wegen

$$r(ms) = (ms)r = m(sr) = m(rs) = (mr)s = (rm)s$$

für $r, s \in R,\ m \in M$ zu einem R-R-Bimodul. Analog ist jeder R-Linksmodul N ein R-R-Bimodul. Nach 15.2 ist also $M \otimes_R N$ ein R-R-Bimodul, und für $r \in R,\ x \in M \otimes_R N$ und $m_1, \ldots, m_k \in M,\ n_1, \ldots, n_k \in N$ ist

$$rx = \sum_{i=1}^{k} rm_i \otimes n_i = \sum_{i=1}^{k} m_i r \otimes n_i = \sum_{i=1}^{k} m_i \otimes rn_i = \sum_{i=1}^{k} m_i \otimes n_i r = xr.$$

Für R-Linksmoduln M, N ist also $M \otimes_R N$ ein R-Linksmodul und für R-Homomorphismen $\varphi : M \to M',\ \psi : N \to N'$ ist $\varphi \otimes \psi : M \otimes_R N \to M' \otimes_R N'$ ein R-Homomorphismus.
Ist M frei mit Basis $\{b_i : i \in I\}$ und N frei über R mit Basis $\{c_j : j \in J\}$, so ist $M \otimes_R N$ frei mit Basis $\{b_i \otimes c_j : i \in I,\ j \in J\}$.

KAPITEL 16

Morita-Theorie

16.1. Definition. Ein *Morita-Kontext* ist ein 6-Tupel, das aus Ringen R, S, einem S-R-Bimodul M, einem R-S-Bimodul N, einem S-S-Homomorphismus $\Phi : M \otimes_R N \to S$ und einem R-R-Homomorphismus $\Psi : N \otimes_S M \to R$ mit

$$\Phi(m \otimes n)m' = m\Psi(n \otimes m') \quad \text{und} \quad n\Phi(m \otimes n') = \Psi(n \otimes m)n'$$

für $m, m' \in M,\ n, n' \in N$ besteht.

Beispiel. Seien R Ring, M ein R-Rechtsmodul, $S := \mathrm{End}_R(M)$ und $N := \mathrm{Hom}_R(M, R)$. Dann wird M zu einem S-Linksmodul mit $\varphi m := \varphi(m)$ für $\varphi \in S,\ m \in M$. Wegen

$$(\varphi m)r = \varphi(m)r = \varphi(mr) = \varphi \cdot (mr)$$

für $\varphi \in S,\ m \in M,\ r \in R$ ist M sogar ein S-R-Bimodul. Ferner ist N ein S-Rechtsmodul mit $\lambda\varphi := \lambda \circ \varphi$ für $\lambda \in N,\ \varphi \in S$. Nach Aufgabe 4 ist N auch ein R-Linksmodul mit $(r\lambda)(m) := r\lambda(m)$ für $r \in R,\ \lambda \in N,\ m \in M$. Wegen

$$((r\lambda)\varphi)(m) = (r\lambda)(\varphi(m)) = r\lambda(\varphi(m)) = r(\lambda \circ \varphi)(m) = (r(\lambda(\varphi))(m)$$

für $m \in M$ ist $(r\lambda)\varphi = r(\lambda\varphi)$ für $r \in R,\ \lambda \in N,\ \varphi \in S$, d.h. N ist ein R-S-Bimodul.
Für $m \in M,\ \lambda \in N$ ist die Abbildung $\Phi_{m,\lambda} : M \to M,\ x \mapsto m\lambda(x)$ ein R-Homomorphismus. Wir erhalten also eine, wie man leicht nachrechnet, ausgeglichene Abbildung $M \times N \to S,\ (m, \lambda) \mapsto \Phi_{m,\lambda}$. Daher existiert genau ein $\mathbb{Z}$-Homomorphismus $\Phi : M \otimes_R N \to S$ mit $\Phi(m \otimes \lambda) = \Phi_{m,\lambda}$ für $m \in M,\ \lambda \in N$. Man rechnet leicht nach, daß Φ ein S-S-Homomorphismus ist.
Offenbar ist die Abbildung $N \times M \to R,\ (\lambda, m) \mapsto \lambda(m)$ ebenfalls ausgeglichen, induziert also einen $\mathbb{Z}$-Homomorphismus $\Psi : N \otimes_S M \to R$ mit $\Psi(\lambda \otimes m) = \lambda(m)$ für $\lambda \in N,\ m \in M$. Man rechnet leicht nach, daß Ψ ein R-R-Homomorphismus ist und so ein Morita-Kontext entsteht.

Bemerkung. Wir sind hauptsächlich an der Situation aus dem Beispiel interessiert; aber die Einführung eines Morita-Kontextes macht die Sache symmetrisch in R und S, M und N.

16.2. Definition. Sei R ein Ring. Ein R-Rechtsmodul (R-Linksmodul) M heißt *(R-)Generator*, falls jeder R-Rechtsmodul (R-Linksomdul) zu einem Faktormodul einer direkten Summe von Kopien von M isomorph ist.

Beispiel.
- (i) R ist ein R-Generator.
- (ii) Ist M^k ein R-Generator für ein $k \in \mathbb{N}$, so auch M.
- (iii) Sind L, M R-Rechtsmoduln und ist $\varphi : L \to M$ ein R-Epimorphismus, so ist mit M auch L ein R-Generator.

Satz. *Sei (R, S, M, N, Φ, Ψ) ein Morita-Kontext. Ist Φ surjektiv, so gilt:*
- (i) *Φ ist bijektiv.*
- (ii) *M und N sind endlich erzeugt und projektiv als R-Moduln.*
- (iii) *M und N sind S-Generatoren.*
- (iv) *Die Abbildung $N \to \mathrm{Hom}_R(M, R)$, die jedem $n \in N$ die Abbildung $M \to R,\ m \mapsto \Phi(n \otimes m)$ zuordnet, ist ein R-S-Isomorphismus. Die Abbildung $M \to \mathrm{Hom}_R(N, R)$, die jedem $m \in M$ die Abbildung $N \to R,\ n \mapsto \Psi(n \otimes m)$ zuordnet, ist ein S-R-Isomorphismus.*

(v) *Die Abbildung* $S \to \mathrm{End}_R(M)$*, die jedem Element* $s \in S$ *die Abbildung* $M \to M,\ m \mapsto sm$ *zuordnet, ist ein Ringhomomorphismus. Die Abbildung* $S^o \to \mathrm{End}_R(N)$*, die jedem* $s \in S$ *die Abbildung* $N \to N,\ n \mapsto ns$ *zuordnet, ist ein Ringhomomorphismus.*

Beweis. Seien $m_1, \dots, m_k \in M,\ n_1, \dots, n_k \in N$ mit $\Phi(\sum_{i=1}^k m_i \otimes n_i) = 1_S$.

(i) Sind $x_1, \dots, x_l \in M,\ y_1, \dots, y_l \in N$ mit $\Phi(\sum_{j=1}^l x_j \otimes y_j) = 0$, so ist

$$\begin{aligned}\sum_{j=1}^{l} x_j \otimes y_j &= \sum_{i,j} x_j \otimes y_j \Phi(m_i \otimes n_i) = \sum_{i,j} x_j \otimes \Psi(y_j \otimes m_i) n_i \\ &= \sum_{i,j} x_j \Psi(y_j \otimes m_i) \otimes n_i = \sum_{i,j} \Phi(x_j \otimes y_j) m_i \otimes n_i = 0.\end{aligned}$$

Daher ist Φ auch injektiv.

(ii) Die Abbildungen $f : R^k \to M,\ (r_1, \dots, r_k) \mapsto \sum_{i=1}^k m_i r_i$ und $g : M \to R^k,\ m \mapsto (\Psi(n_1 \otimes m), \dots, \Psi(n_k \otimes m))$ sind R-Homomorphismen mit

$$f(g(m)) = \sum_{i=1}^{k} m_i \Psi(n_i \otimes m) = \sum_{i=1}^{k} \Phi(m_i \otimes n_i) m = m$$

für $m \in M$, d.h. $0 \longrightarrow \mathrm{Ker}(f) \longrightarrow R^k \xrightarrow{f} M \longrightarrow 0$ ist eine zerfallende exakte Folge. Daher ist M ein endlich erzeugter projektiver R-Rechtsmodul, und N ist analog ein endlich erzeugter projektiver R-Linksmodul.

(iii) Die Abbildung $h : M^k \to S,\ (x_1, \dots, x_k) \mapsto \Phi(\sum_{i=1}^k x_i \otimes n_i)$ ist ein S-Homomorphismus und surjektiv wegen $h(m_1, \dots, m_k) = 1_S$. Analog für N.

(iv) Man rechnet leicht nach, daß die angegebene Abbildung $N \to \mathrm{Hom}_R(M, R)$ wohldefiniert und ein R-S-Homomorphismus ist. Ist $n \in N$ mit $\Psi(n \otimes m) = 0$ für $m \in M$, so ist

$$n = \sum_{i=1}^{k} n \Phi(m_i \otimes n_i) = \sum_{i=1}^{k} \Psi(n \otimes m_i) n_i = 0.$$

Für $\lambda \in \mathrm{Hom}_R(M, R)$ und $m \in M$ gilt:

$$\begin{aligned}\lambda(m) &= \sum_{i=1}^{k} \lambda(\Phi(m_i \otimes n_i) m) = \sum_{i=1}^{k} \lambda(m_i \Psi(n_i \otimes m)) \\ &= \sum_{i=1}^{k} \lambda(m_i) \Psi(n_i \otimes m) = \sum_{i=1}^{k} \Psi(\lambda(m_i) n_i \otimes m).\end{aligned}$$

Folglich ist λ das Bild von $\sum_{i=1}^k \lambda(m_i) n_i$ unter der angegebenen Abbildung $N \to \mathrm{Hom}_R(M, R)$. Analog behandelt man den zweiten Teil.

(v) Man rechnet leicht nach, daß die angegebene Abbildung $S \to \mathrm{End}_R(M)$ wohldefiniert und ein Ringhomomorphismus ist. Ist $s \in S$ mit $sM = 0$, so ist

$$s = s\Phi\left(\sum_{i=1}^{k} m_i \otimes n_i\right) = \sum_{i=1}^{k} \Phi(s m_i \otimes n_i) = 0.$$

Für $\varphi \in \mathrm{End}_R(M)$ und $m \in M$ ist

$$\begin{aligned}\varphi(m) &= \sum_{i=1}^{k} \varphi(\Phi(m_i \otimes n_i) m) = \sum_{i=1}^{k} \varphi(m_i \Psi(n_i \otimes m)) \\ &= \sum_{i=1}^{k} \varphi(m_i) \Psi(n_i \otimes m) = \sum_{i=1}^{k} \Phi(\varphi(m_i) \otimes n_i) m,\end{aligned}$$

d.h. φ ist das Bild von $\sum_{i=1}^k \Phi(\varphi(m_i) \otimes n_i)$ unter der angegebenen Abbildung. Den zweiten Teil behandelt man analog.

□

Bemerkung. Entsprechende Aussagen gelten natürlich auch, falls Ψ surjektiv ist.

16.3. Satz. *Seien R ein Ring, M ein R-Rechtsmodul und (R, S, M, N, Φ, Ψ) der zugehörige Morita-Kontext aus Beispiel 16.1. Dann gilt:*

(i) *Ist M endlich erzeugt und projektiv über R, so ist Φ surjektiv.*
(ii) *Ist M ein R-Generator, so ist Ψ surjektiv.*

Beweis.

(i) Ist M endlich erzeugt, so existiert ein $k \in \mathbb{N}$ und eine exakte Folge von R-Rechtsmoduln $0 \longrightarrow K \longrightarrow R^k \xrightarrow{f} M \longrightarrow 0$. Ist M projektiv, so existiert ein R-Homomorphismus $g : M \to R^k$ mit $f \circ g = \mathrm{id}_M$. Mit $e_1, \dots, e_k$ bezeichnen wir die kanonische Basis von R^k und mit $p_i : R^k \to R$ für $i = 1, \dots, k$ die entsprechenden Projektionen. Für $x \in R^k$ ist dann $x = \sum_{i=1}^k e_i p_i(x)$. Für $x \in M$ ist also
$$m = f(g(m)) = \sum_{i=1}^k f(e_i p_i(g(m))) = \sum_{i=1}^k \underbrace{f(e_i)}_{m_i} \underbrace{p_i(g(m))}_{\lambda_i(m)},$$
wobei $m_i := f(e_i) \in M$ und $\lambda_i := p_i \circ g \in N$ für $i = 1, \dots, k$ ist. Folglich ist $1_S = \mathrm{id}_M = \Phi(\sum_{i=1}^k m_i \otimes \lambda_i) \in \Phi(M \otimes_R N)$, d.h. Φ ist surjektiv.

(ii) Seien I eine Menge, $f : \bigoplus_{i \in I} M \to R$ ein R-Epimorphismus und $(m_i)_{i \in I} \in \bigoplus_{i \in I} M$ mit $f((m_i)_{i \in I}) = 1_R$. Die Injektionen $M \to \bigoplus_{i \in I} M$ bezeichnen wir mit g_i $(i \in I)$ und setzen $I_0 := \{i \in I : m_i \neq 0\}$. Dann ist I_0 endlich, $(m_i)_{i \in I_0} = \sum_{i \in I_0} g_i(m_i)$ und
$$1_R = \sum_{i \in I_0} f(g_i(m_i)) = \Psi\Bigg(\sum_{i \in I_0} (f \circ g_i) \otimes m_i) \in \Psi(N \otimes_R M).$$
Folglich ist Ψ surjektiv.

□

Definition. Ist M endlich erzeugt, projektiv und ein R-Generator, so nennt man M einen *(R-)Progenerator.*

Beispiel. Für $n \in \mathbb{N}$ ist R^n ein R-Progenerator.

16.4. Definition. Man nennt Ringe R, S *Morita-äquivalent* und schreibt $R \sim S$, falls ein Morita-Kontext $R, S, M, N, \Phi, \Psi)$ mit surjektiven Φ, Ψ existiert,

Bemerkung. In den Übungen rechnen wir nach, daß $\sim$ eine Äquivalenzrelation ist, und daß isomorphe Ringe stets Morita-äquivalent sind. Nach den vorangegangenen Sätzen sind zwei Ringe R, S genau dann Morita-äquivalent, wenn S zum Endomorphismenring eines R-Progenerators isomorph ist.

Beispiel. Für $n \in \mathbb{N}$ ist jeder Ring R zu $\mathrm{End}_R(R^n) \cong \mathrm{Mat}(n, R)$ Morita-äquivalent.

16.5. Bemerkung. Sei (R, S, M, N, Φ, Ψ) ein Morita-Kontext mit surjektiven Φ, Ψ. Für jeden R-Linksmodul P ist dann $M \otimes_R P$ ein S-Linksmodul, und für jeden S-Linksmodul Q ist $N \otimes_S Q$ ein R-Linksmodul. Ferner ist
$$N \otimes_S (M \otimes_R P) \simeq (N \otimes_S M) \otimes_R P \simeq R \otimes_R P \simeq P$$
und
$$M \otimes_R (N \otimes_S Q) \simeq (M \otimes_R N) \otimes_S Q \simeq S \otimes_S Q \simeq Q.$$

Die entsprechenden Isomorphismen $f_P : N \otimes_S (M \otimes_R P) \to P$ und $g_Q : M \otimes_R (N \otimes_S Q) \to Q$ erfüllen

$$\begin{aligned} f_P(n \otimes (m \otimes p)) &= \Psi(n \otimes m)p, \\ g_Q(m \otimes (n \otimes q)) &= \Phi(m \otimes n)q \end{aligned}$$

für $m \in M,\ n \in N,\ p \in P,\ q \in Q$. Daher sind für R-Linksmoduln P, P', S-Linksomoduln Q, Q', $\alpha \in \mathrm{Hom}_R(P, P'),\ \beta \in \mathrm{Hom}_S(Q, Q')$ die folgenden Diagramme kommtativ:

$$\begin{tikzcd} N \otimes S(M \otimes_R P) \arrow[r, "f_P"] \arrow[d, "\mathrm{id}_N \otimes (\mathrm{id}_M \otimes \alpha)"'] & P \arrow[d, "\alpha"] \\ N \otimes_S (M \otimes_R P') \arrow[r, "f_{P'}"] & P' \end{tikzcd} \qquad \begin{tikzcd} M \otimes R(N \otimes_S Q) \arrow[r, "g_Q"] \arrow[d, "\mathrm{id}_M \otimes (\mathrm{id}_N \otimes \beta)"'] & P \arrow[d, "\beta"] \\ M \otimes_R (N \otimes_S Q') \arrow[r, "g_{Q'}"] & Q' \end{tikzcd}$$

Folglich sind $F_{PP'} : \mathrm{Hom}_R(P, P') \to \mathrm{Hom}_S(M \otimes_R P, M \otimes_R P'),\ \alpha \mapsto \mathrm{id}_M \otimes \alpha$ und $G_{QQ'} : \mathrm{Hom}_S(Q, Q') \to \mathrm{Hom}_R(N \otimes_S Q, N \otimes_S Q'),\ \beta \mapsto \mathrm{id}_N \otimes \beta$ $\mathbb{Z}$-Homomorphismen mit

$$\begin{aligned} H_{PP'} \circ G_{M \otimes_R P, M \otimes_R P'} \circ F_{PP'} &= \mathrm{id}, \\ K_{QQ'} \circ F_{N \otimes_S Q, N \otimes_S Q'} \circ G_{QQ'} &= \mathrm{id}; \end{aligned}$$

dabei sind

$$\begin{aligned} H_{PP'} : \mathrm{Hom}_R(N \otimes_S (M \otimes_R P), N \otimes_S (M \otimes_R P')) &\to \mathrm{Hom}_R(P, P'), \\ \gamma &\mapsto f_{P'} \circ \gamma \circ f_P^{-1} \end{aligned}$$

und

$$\begin{aligned} K_{QQ'} : \mathrm{Hom}_S(M \otimes_R (N \otimes_S Q), M \otimes_R (N \otimes_S Q')) &\to \mathrm{Hom}_S(Q, Q'), \\ \delta &\mapsto g_{Q'} \circ \delta \circ g_Q^{-1} \end{aligned}$$

$\mathbb{Z}$-Isomorphismen. Folglich sind $F_{PP'}, G_{QQ'}$ injektiv und $G_{M \otimes_R P, M \otimes_R P'}, F_{N \otimes_S Q, N \otimes_S Q'}$ surjektiv. Also sind $G_{M \otimes_R P, M \otimes_R P'}, F_{N \otimes_S Q, N \otimes_S Q'}$ bijektiv, und damit auch $F_{PP'}, G_{QQ'}$. (Offenbar sind $F_{PP'}, G_{QQ'}$ sogar Ringisomorphismen.) Ist $\alpha : P \to P'$ ein R-Isomorphismus, so ist $\mathrm{id}_M \otimes \alpha$ ein S-Isomorphismus; denn die Umkehrabbildung ist $\mathrm{id}_M \otimes \alpha^{-1}$. Ist umgekehrt $\mathrm{id}_M \otimes \alpha$ ein S-Isomorphismus, so ist analog $\mathrm{id}_N \otimes (\mathrm{id}_M \otimes \alpha)$ ein R-Isomorphismus, also auch $f_{P'} \circ (\mathrm{id}_N \otimes (\mathrm{id}_M \otimes \alpha)) \circ f_P^{-1} = \alpha$. Daher erhält man durch $P \mapsto M \otimes_R P$ und $Q \mapsto N \otimes_S Q$ zueinander inverse Bijektionen zwischen der Gesamtheit der Isomorphieklassen von R-Linksmoduln und der Gesamtheit der Isomorphieklassen von S-Linksmoduln.
Sei P ein Untermodul eines R-Linksmoduls P' und $\alpha : P \to P'$ die Inklusionsabbildung. Da M R-flach ist, ist $\mathrm{id}_M \otimes \alpha : M \otimes_R P \to M \otimes_R P'$ injektiv, d.h. man kann $M \otimes_R P$ mit seinem Bild unter $\mathrm{id}_M \otimes \alpha$, der von allen Elementen der Form $m \otimes p$ $(m \in M,\ p \in P)$ erzeugten Untergruppe von $M \otimes_R P'$, identifizieren. Auf diese Weise wird $M \otimes_R P$ zu einem S-Untermodul von $M \otimes_R P'$. Analog kann man $N \otimes_S Q$ für jeden Untermodul Q eines S-Linksmoduls Q' als R-Untermodul von $N \otimes_S Q'$ ansehen. Insbesondere wird $N \otimes_S (M \otimes_R P)$ auf diese Weise zu einem R-Untermodul von $N \otimes_S (M \otimes_R P')$, der unter $f_{P'}$ auf P abgebildet wird. Für jeden R-Linksmodul P' erhält man also durch $P \mapsto M \otimes_R P$ eine Bijektion zwischen der Menge der R-Untermoduln von P' und der Menge der S-Untermoduln von $M \otimes_R P'$. Analog erhält man für jeden S-Linksmodul Q' durch $Q \mapsto N \otimes_S Q$ eine Bijektion zwischen der Menge der S-Untermoduln von Q' und der Menge der R-Untermoduln von $N \otimes_S Q'$. Diese Bijektionen erhalten Inklusionen zwischen Untermoduln und damit Summe und Durchschnitt von Untermoduln. Insbesondere ist P' genau dann ein einfacher (bzw. halbeinfacher, unzerlegbarer) R-Linksmodul, wenn $M \otimes_R P'$ ein einfacher (bzw. halbeinfacher, unzerlegbarer) S-Linksmodul ist.
Im Fall $P' = R$ hat man einen kanonischen Isomorphismus ι zwischen $M \otimes_R P'$ und M mit $\iota(m \otimes r) = mr$ für $m \in M,\ r \in R$. Daher erhält man durch $P \mapsto MP$ eine Bijektion zwischen der Menge der Linksideale in R und der Menge der S-Untermoduln von M. Analog erhält man durch $Q \mapsto NQ$ eine Bijektion zwischen der Menge der Linksideale in S und der Menge der R-Untermoduln von N.

Es ist leicht zu sehen, daß bei diesen Bijektionen die zweiseitigen Ideale in R (bzw. S) genau den S-R-Untermoduln von M (bzw. R-S-Untermoduln von N) entsprechen. Aus Symmetriegründen hat man ebenfalls Bijektionen $P \mapsto PN$ (bzw. $Q \mapsto QM$) zwischen der Menge der zweiseitigen Ideale in R (bzw. S) und der Menge der R-S-Untermoduln von N (bzw. S-R-Untermoduln von M). Insgesamt erhält man also eine inklusionserhaltende Bijektion zwischen der Menge der zweiseitigen Ideale in R und S.

16.6. Satz. *Morita-äquivalente Ringe haben isomorphe Zentren.*

Beweis. Sei (R, S, M, N, Φ, Ψ) ein Morita-Kontext mit surjektiven Φ und Ψ. Für $r \in Z(R)$ ist die Abbildung $\rho_r : M \to M,\ m \mapsto mr$ ein R-Homomorphismus mit

$$\varphi(\rho_r(m)) = \varphi(mr) = \varphi(m)r = \rho_r(\varphi(m))$$

für $\varphi \in \mathrm{End}_R(M),\ m \in M$. Folglich ist $\rho_r \in Z(\mathrm{End}_R(M))$. Nach 16.2 existiert also genau ein $\zeta(r) \in Z(S)$ mit $\zeta(r)m = \rho_r(m) = mr$ für $m \in M$. Analog existiert zu jedem $s \in Z(S)$ genau ein $\eta(s) \in Z(R)$ mit $m\eta(s) = sm$ für $m \in M$. Für $r \in Z(R)$ und $m \in M$ ist dann $mr = m\eta(\zeta(r))$ für $m \in M$, also $M(r - \eta(\zeta(r))) = 0$. Da M ein R-Generator ist, folgt $R(r - \eta(\zeta(r))) = 0$, also $\eta(\zeta(r)) = r$. Analog ist $\zeta(\eta(s)) = s$ für $s \in Z(S)$. Daher sind $\zeta : Z(R) \to Z(S)$ und $\eta : Z(S) \to Z(R)$ zueinander inverse Abbildungen. Offenbar sind ζ und η Ringhomomorphismen. $\square$

KAPITEL 17

Das Tensorprodukt von Algebren

17.1. Definition. Eine *R-Algebra* ist eine Menge A mit Verknüpfungen

$$\begin{array}{ll} A \times A \to A, & (a,b) \mapsto a+b, \\ A \times A \to A, & (a,b) \mapsto ab, \\ R \times A \to A, & (r,a) \mapsto ra, \end{array}$$

so daß A ein Ring und ein R-Linksmodul mit $r(ab) = (ra)b = a(rb)$ für $r \in R,\ a, b \in A$ ist.

Beispiel.

(i) 0 und R sind R-Algebren.

(ii) Für jede Familie $(A_i)_{i \in I}$ von R-Algebren ist auch das *direkte Produkt* $\prod_{i \in I} A_i = \bigtimes_{i \in I} A_i$ eine R-Algebra. Im Fall $I = \{1, \ldots, n\}$ ür ein $n \in \mathbb{N}$ schreiben wir $A_1 \times \ldots \times A_n$ statt $\prod_{i \in I} A_i$.

(iii) Für jede R-Algebra A ist auch A^o eine R-Algebra, die zu A *entgegengesetzte* R-Algebra.

(iv) Für jede R-Algebra A und $n \in \mathbb{N}$ ist auch $\mathrm{Mat}(n, A)$ eine R-Algebra, die *volle Matrixalgebra des Grades n* über A.

(v) Der Polynomring $R[X]$ in einer Variablen X (oder mehreren) ist eine R-Algebra.

(vi) Für jeden R-Linksmodul M ist $\mathrm{End}_R(M)$ eine R-Algebra.

(vii) Jeden Ring kann man als $\mathbb{Z}$-Algebra auffassen.

Satz. *Für R-Algebren A, B existiert stets eine Verknüpfung $(A \otimes_R B) \times (A \otimes_R B) \to A \otimes_R B,\ (c, d) \mapsto cd$, so daß $A \otimes_R B$ eine R-Algebra mit $(a \otimes b)(a' \otimes b') = aa' \otimes bb'$ für $a, a' \in A,\ b, b' \in B$ wird.*

Beweis. Für $a \in A,\ b \in B$ sind $\mu_a : A \to A,\ x \mapsto ax$ und $\mu_b : B \to B,\ y \mapsto by$ R-Homomorphismen. Daher ist auch $\mu_a \otimes \mu_b : A \otimes_R B \to A \otimes_R B$ ein R-Homomorphismus. Wegen $\mu_{a+a'} = \mu_a + \mu_{a'},\ \mu_{b+b'} = \mu_b + \mu_{b'},\ \mu_{ra} = r\mu_a$ und $\mu_{rb} = r\mu_b$ für $a, a' \in A,\ b, b' \in B,\ r \in R$ ist die Abbildung $A \times B \to \mathrm{End}_R(A \otimes_R B),\ (a, b) \mapsto \mu_a \otimes \mu_b$ ausgeglichen, induziert also einen R-Homomorphismus $\Phi : A \otimes_R B \to \mathrm{End}_R(A \otimes_R B)$ mit $\Phi(a \otimes b) = \mu_a \otimes \mu_b$ für $a \in A,\ b \in B$. Wir definieren die Multiplikation auf $A \otimes_R B$ durch $cd := (\Phi(c))(d)$ für $c, d \in A \otimes_R B$. Dann ist

$$\begin{array}{rcl} (c+c')d &=& (\Phi(c+c'))(d) \ = \ (\Phi(c) + \Phi(c'))(d) \ = \ (\Phi(c))(d) + (\Phi(c'))(d) \ = \ cd + c'd, \\ c(d+d') &=& (\Phi(c))(d+d') \ = \ (\Phi(c))(d) + (\Phi(c))(d') \ = \ cd + cd', \\ r(cd) &=& r(\Phi(c))(d) \ = \ (\Phi(c))(rd) \ = \ c(rd), \\ r(cd) &=& r(\Phi(c))(d) \ = \ (r\Phi(c))(d) \ = \ (\Phi(rc))(d) \ = \ (rc)d \end{array}$$

für $r \in R,\ c, c', d, d' \in A \otimes_R B$ und

$$(a \otimes b)(a' \otimes b') = (\Phi(a \otimes b))(a' \otimes b') = (\mu_a \otimes \mu_b)(a' \otimes b') = \mu_a(a') \otimes \mu_b(b') = aa' \otimes bb'$$

für $a, a' \in A,\ b, b' \in B$. Daher ist

$$\begin{array}{rcl} ((a \otimes b)(a' \otimes b'))(a'' \otimes b'') &=& (aa' \otimes bb')(a'' \otimes b'') \ = \ (aa')a'' \otimes (bb')b'' \\ &=& a(a'a'') \otimes b(b'b'') \ = \ (a \otimes b)(a'a'' \otimes b'b'') \\ &=& (a \otimes b)((a' \otimes b')(a'' \otimes b'')) \end{array}$$

für $a, a', a'' \in A,\ b, b', b'' \in B$, woraus leicht die Assoziativität der Multiplikation folgt. Analog zeigt man, daß $1_A \otimes 1_B$ Einselement in $A \otimes_R B$ ist. $\square$

Bemerkung. Es ist klar, wie man Homomorphismen, Isomorphismen, usw. zwischen R-Algebren definiert. Offenbar sind $\kappa_A : A \to A \otimes_R B,\ a \mapsto a \otimes 1$ und $\kappa_B : B \to A \otimes_R B,\ b \mapsto 1 \otimes b$ unitäre Homomorphismen. Wir bezeichnen sie als *kanonisch*. I.a. sind sie nicht injektiv. Für $a \in A,\ b \in B$ gilt:

$$\kappa_A(a)\kappa_B(b) = (a \otimes 1)(1 \otimes b) = a \otimes b = (1 \otimes b)(a \otimes 1) = \kappa_B(b)\kappa_A(a).$$

17.2. Satz (Universelle Eigenschaft des Tensorprodukts von Algebren)**.**
Seien A, B, C R-Algebren und $\alpha : A \to C,\ \beta : B \to C$ Homomorphismen mit $\alpha(a)\beta(b) = \beta(b)\alpha(a)$ für $a \in A,\ b \in B$. Dann existiert genau ein Homomorphismus $\gamma : A \otimes_R B \to C$ mit $\gamma(a \otimes b) = \alpha(a)\beta(b)$ für $a \in A,\ b \in B$.

Beweis. Die Abbildung $A \times B \to C,\ (a, b) \mapsto \alpha(a)\beta(b)$ ist ausgeglichen, induziert also einen R-Homomorphismus $\gamma : A \otimes_R B \to C$ mit $\gamma(a \otimes b) = \alpha(a)\beta(b)$ für $a \in A,\ b \in B$. Wegen

$$\begin{aligned}\gamma((a \otimes b)(a' \otimes b')) &= \gamma(aa' \otimes bb') = \alpha(aa')\beta(bb') = \alpha(a)\alpha(a')\beta(b)\beta(b') \\ &= \alpha(a)\beta(b)\alpha(a')\beta(b') = \gamma(a \otimes b)\gamma(a' \otimes b')\end{aligned}$$

für $a, a' \in A,\ b, b' \in B$ folgt leicht, daß γ ein Homomorphismus von R-Algebren ist. □

Bemerkung. Für R-Algebren A, B, C gilt:

$$\begin{aligned} A \otimes_R R &\cong A, \\ A \otimes_R B &\cong B \otimes_R A, \\ (A \otimes_R B) \otimes_R C &\cong A \otimes_R (B \otimes_R C). \end{aligned}$$

Zum Beweis prüft man nach, daß die entsprechenden kanonischen Isomorphismen Homomorphismen von R-Algebren sind. Für endliche Familien von R-Algebren $(A_i)_{i \in I},\ (B_j)_{j \in J}$ gilt analog:

$$\left(\prod_{i \in I} A_i\right) \otimes_R \left(\prod_{j \in J} B_j\right) \cong \prod_{i \in I, j \in J} (A_i \otimes_R B_j),$$

und für A, A', B, B' und Homomorphismen $\varphi : A \to A',\ \psi : B \to B'$ ist auch $\varphi \otimes \psi : A \otimes_R B \to A' \otimes_R B'$ ein Homomorphismus.

17.3. Satz. *Für $m, n \in \mathbb{N}$ und jede R-Algebra A ist $\mathrm{Mat}(m, R) \otimes_R \mathrm{Mat}(n, R) \cong \mathrm{Mat}(mn, R)$ und $\mathrm{Mat}(m, R) \otimes_R A \cong \mathrm{Mat}(m, A)$.*

Beweis. Für $i, j = 1, \ldots, m$ sei $e_{ij} \in \mathrm{Mat}(m, R)$ die Matrix mit 1 an der Position (i, j) und 0 sonst. Diese Elemente bilden eine R-Basis von $\mathrm{Mat}(m, R)$ mit $e_{ij}e_{kl} = \delta_{jk}e_{il}$ für $i, j, k, l = 1, \ldots, m$. Entsprechend hat man für $i, j = 1 \ldots, n$ Elemente f_{ij} in $\mathrm{Mat}(n, R)$ und für $i, j = 1, \ldots, mn$ Elemente $g_{ij} \in \mathrm{Mat}(mn, R)$. Aus 14.3 folgt, daß die Elemente $e_{ij} \otimes f_{kl}$ $(i, j = 1, \ldots, m,\ k, l = 1, \ldots, n)$ eine R-Basis von $\mathrm{Mat}(m, R) \otimes_R \mathrm{Mat}(n, R)$ bilden. Daher existiert genau ein R-Isomorphismus $\varphi : \mathrm{Mat}(m, R) \otimes_R \mathrm{Mat}(n, R) \to \mathrm{Mat}(mn, R)$ mit $\varphi(e_{ij} \otimes f_{kl}) = g_{(i-1)n+k,(j-1)n+l}$ für $i, j = 1, \ldots, m,\ k, l = 1, \ldots, n$. Wegen

$$\begin{aligned}\varphi(e_{ij} \otimes f_{jk})\varphi(e_{rs} \otimes f_{tu}) &= g_{(i-1)n+k,(j-1)n+l}\,g_{(r-1)n+t,(s-1)n+u} \\ &= \delta_{jr}\delta_{lt}\,g_{(i-1)n+k,(s-1)n+u} \\ &= \delta_{jr}\delta_{lt}\,\varphi(e_{is} \otimes f_{ku}) \\ &= \varphi(e_{ij}e_{rs} \otimes f_{kl}f_{tu}) \\ &= \varphi((e_{ij} \otimes f_{kl})(e_{rs} \otimes f_{tu}))\end{aligned}$$

fü $i, j, r, s = 1, \ldots, m,\ k, l, t, u = 1, \ldots, n$ ist φ ein Homomorphismus von Algebren.
Jedes Element in $\mathrm{Mat}(m, R) \otimes_R A$ hat nach 14.3 die Form $\sum_{i,j=1}^{m} e_{ij} \otimes a_{ij}$ mit eindeutig bestimmten

$a_{ij} \in A$. Daher ist $\psi : \mathrm{Mat}(m, A) \to \mathrm{Mat}(m, R) \otimes_R A,\ (a_{ij}) \mapsto \sum_{i,j=1}^m e_{ij} \otimes a_{ij}$ ein R-Isomorphismus mit

$$\begin{aligned}
\psi((a_{ij}))\psi((b_{kl})) &= \sum_{i,j,k,l=1}^{m} (e_{ij} \otimes a_{ij})(e_{kl} \otimes b_{kl}) \\
&= \sum_{i,j,k,l=1}^{m} e_{ij}e_{kl} \otimes a_{ij}b_{kl} \;=\; \sum_{i,j,l=1}^{m} e_{il} \otimes a_{ij}b_{jl} \\
&= \psi\left(\left(\sum_{j=1}^{m} a_{ij}b_{jl}\right)\right) \;=\; \psi((a_{ij})(b_{kl}))
\end{aligned}$$

für $(a_{ij}), (b_{kl}) \in \mathrm{Mat}(m, A)$. □

17.4. Bemerkung. Sei G ein Monoid und F die Menge aller Abbildungen $\varphi : G \to R$ mit $|\{g \in G : \varphi(g) \neq 0\}| < \infty$. Dann ist F ein R-Linksmodul mit $(\varphi + \psi)(g) = \varphi(g) + \psi(g)$ und $(r\varphi)(g) = r\varphi(g)$ für $\varphi, \psi \in F,\ g \in G,\ r \in R$. Für $g \in G$ sei $\hat{g} \in F$ definiert durch

$$\hat{g}(h) := \begin{cases} 1 & \text{falls } g = h \\ 0 & \text{sonst} \end{cases} .$$

Dann bilden die Elemente $\hat{g}$ $(g \in G)$ eine R-Basis von F. Jedes Element in F läßt sich also in der Form $\sum_{g \in G} r_g \hat{g}$ mit eindeutig bestimmten Elementen $r_g \in R$ schreiben, von denen nur endlich viele von 0 verschieden sind. Wir definieren eine Multiplikation auf F durch

$$\left(\sum_{g \in G} r_g \hat{g}\right)\left(\sum_{h \in G} s_h \hat{h}\right) := \sum_{g,h \in G} r_g s_h \widehat{gh}$$

für Elemente $r_g, s_h \in R$ für $g, h \in G$. Man rechnet leicht nach, daß F so zu einer R-Algebra mit $\hat{g}\hat{h} = \widehat{gh}$ für $g, h \in G$ wird. Wir können also jedes Element $g \in G$ mit dem entsprechenden Element $\hat{g} \in F$ identifizieren. Dann wird G zu einer Teilmenge von F, jedes Element in F hat die Form $\sum_{g \in G} r_g g$ mit eindeutig bestimmten Elementen $r_g \in R$, von denen nur endlich viele von 0 verschieden sind, und die Multiplikation von F setzt die Multiplikation auf G fort. Wir nennen F die *Monoidalgebra* von G über R und bezeichnen sie mit RG. Ist G eine Gruppe, so sprechen wir von der *Gruppenalgebra*.

Beispiel. Nimmt man für G das Monoid aller Wörter über dem einelementigen Alphabet $\{X\}$, so ist die Monoidalgebra RG zur Polynomalgebra $R[X]$ isomorph. Man kann also Monoidalgebren als Verallgemeinerung von Polynomalgebren ansehen.

Satz (Universelle Eigenschaft von Monoidalgebren)**.** *Sei G ein Monoid, A eine R-Algebra und $\varphi : G \to A$ mit $\varphi(gh) = \varphi(g)\varphi(h)$ für $g, h \in G$ (d.h. φ ist ein Homomorphismus von Monoiden). Dann kann man φ zu einem Homomorphismus von Algebren $RG \to A$ fortsetzen.*

Beweis. Da die Elemente $g \in G$ eine R-Basis von RG bilden, kann man φ sicher zu einem R-Homomorphismus $RG \to A$ fortsetzen. Wegen $\varphi(gh) = \varphi(g)\varphi(h)$ für $g, h \in G$ ist diese Fortsetzung ein Homomorphismus von Algebren. □

17.5. Beispiel. Ist G ein Monoid, so gibt es genau einen Homomorphismus $\nu : RG \to R$ mit $\nu(g) = 1$ für $g \in G$. Man nennt ν die *Augmentationsabbildung* von RG. Explizit ist also $\nu(\sum_{g \in G} r_g g) = \sum_{g \in G} r_g$ für Elemente $r_g \in R$ $(g \in G)$. Allgemeiner läßt sich jeder Homomorphismus von Monoiden $\varphi : G \to H$ zu einem Homomorphismus der Monoidalgebren $RG \to RH$ fortsetzen, den wir i.a. wieder mit φ bezeichnen.

Bemerkung. Im folgenden behandeln wir meist Gruppenalgebren, obwohl vieles auch für Monoidalgebren zutrifft.

Satz. *Sind G, H Gruppen, so existiert genau ein Isomorphismus $\alpha : R[G \times H] \to RG \otimes_R RH$ mit $\alpha(g, h) = g \otimes h$ für $g \in G,\ h \in H$.*

Beweis. Die Gruppenhomomorphismen $\varphi : G \to G \times H,\ g \mapsto (g, 1)$ und $\psi : H \to G \times H,\ h \mapsto (1, h)$ lassen sich zu Homomorphismen $RG \to R[G \times H],\ RH \to R[G \times H]$ fortsetzen, die wir wieder mit φ bzw. ψ bezeichnen. Wegen

$$\varphi(g)\psi(h) = (g, 1)(1, h) = (g, h) = (1, h)(g, 1) = \psi(h)\varphi(g)$$

für $g \in G,\ h \in H$ ist auch $\varphi(a)\psi(b) = \psi(b)\varphi(a)$ für $a \in RG,\ b \in RH$. Daher existiert genau ein Homomorphismus von Algebren $\omega : RG \otimes_R RH \to R[G \times H]$ mit $\omega(a \otimes b) = \varphi(a)\psi(b)$ für $a \in RG,\ b \in RH$, d.h. $\omega(g \otimes h) = \varphi(g)\psi(h) = (g, h)$ für $g \in G,\ h \in H$. Umgekehrt ist $\alpha : G \times H \to RG \otimes_R RH,\ (g, h) \mapsto g \otimes h$ eine Abbildung mit

$$\alpha(g, h)\alpha(g', h') = (g \otimes h)(g' \otimes h') = gg' \otimes hh' = \alpha(gg', hh') = \alpha((g, h)(g', h'))$$

für $g, g' \in G,\ h, h' \in H$, läßt sich also zu einem Homomorphismus $R[G \times H] \to RG \otimes_R RH$ fortsetzen, den wir auch mit α bezeichnen. Offenbar ist $\alpha(\omega(g \otimes h)) = g \otimes h$ und $\omega(\alpha(g, h)) = (g, h)$ für $g \in G,\ h \in H$. Da $\{g \otimes h : g \in G,\ h \in H\}$ nach 14.3 eine R-Basis von $RG \otimes_R RH$ und $\{(g, h) : g \in G,\ h \in H\}$ eine R-Basis von $R[G \times H]$ ist, folgt: $\alpha \circ \omega = \mathrm{id}$ und $\omega \circ \alpha = \mathrm{id}$. □

17.6. Bemerkung. Seien G eine Gruppe, $H \leq G$ und $\varphi : H \to G$ die Inklusionsabbildung. Nach 17.4 läßt sich φ zu einem Homomorphismus $RH \to RG$ fortsetzen. Diese Fortsetzung ist injektiv. Wir können und werden also RH als unitäre R-Unteralgebra von RG auffassen.

KAPITEL 18

Moduln, Darstellungen und Matrixdarstellungen

Sei R ein kommutativer Ring.

18.1. Bemerkung. Sind A, B R-Algebren, so kann man jeden A-Linksmodul (bzw. B-Rechtsmodul) M auch als R-Linksmodul (bzw. als B-Rechtsmodul) mit $rm := (r1_A)m$ (bzw. $mr := m(1_B r)$) für $r \in R,\ m \in M$ ansehen. Ist M ein A-B-Bimodul mit $rm = mr$ für $r \in R,\ m \in M$, so nennt man M einen A-B-Bimodul *über* R. In diesem Fall wird M, wie man leicht nachrechnet, zu einem $A \otimes_R B^o$-Linksmodul (bzw. $A^o \otimes_R B$-Rechtsmodul) mit $(a \otimes b)m = amb$ (bzw. $m(a \otimes b) = amb$) für $a \in A,\ b \in B,\ m \in M$. Ferner entstehen auf diese Weise alle $A \otimes_R B^o$-Linksmoduln (bzw. $A^o \otimes_R B$-Rechtsmoduln). Kurz gesagt: $\{A$-B-Bimoduln über $R\}$=$\{A \otimes_R B^o$-Linksmoduln $\}$=$\{A^o \otimes_R B$-Rechtsmoduln$\}$.

18.2. Satz. *Seien A, B R-Algebren, M ein A-Linksmodul und N ein B-Linksmodul. Dann existiert eine Verknüpfung $(A \otimes_R B) \times (M \otimes_R N) \to M \otimes_R N,\ (c, d) \mapsto cd$, so daß $M \otimes_R N$ ein $A \otimes_R B$-Linksmodul mit $(a \otimes b)(m \otimes n) = am \otimes bn$ für $a \in A,\ b \in B,\ m \in M,\ n \in N$ wird.*

Beweis. Mit 18.1 oder analog zu 17.1. □

Bemerkung. Analoges gilt auch für Rechtsmoduln.

18.3. Bemerkung. Für Gruppen G, H existieren nach 17.5 ein Isomorphismus $\alpha : R[G \times H] \to RG \otimes_R RH$ mit $\alpha(g, h) = g \otimes h$ für $g \in G,\ h \in H$. Für jeden RG-Linksmodul M und jeden RH-Linksmodul N ist also $\mathrm{Res}_\alpha(M \otimes_R N)$ ein $R[G \times H]$-Linksmodul mit $(g, h)(m \otimes n) = gm \otimes hn$ für $g \in G,\ h \in H,\ m \in M,\ n \in N$. Man nennt ihn das *(äußere) Tensorprodukt* von M und N und bezeichnet ihn mit $M \#_R N$ oder wieder mit $M \otimes_R N$. Weiterhin läßt sich der Homomorphismus $G \to G \times G,\ g \mapsto (g, g)$ zu einem Homomorphismus $\delta : RG \to R[G \times G]$ fortsetzen. Für RG-Linksmoduln M, N ist daher $\mathrm{Res}_\delta(M \#_R N)$ ein RG-Linksmodul mit $g(m \otimes n) = gm \otimes gn$ für $g \in G,\ m \in M,\ n \in N$. Man nennt ihn das *(innere) Tensorprodukt* von M und N und schreibt wieder $M \otimes_R N$. Man beachte aber, daß nicht stets $a(m \otimes n) = am \otimes an$ für $a \in RG,\ m \in M,\ n \in N$ ist. Daher läßt sich diese Konstruktion auch nicht von Gruppenalgebren auf beliebige Algebren verallgemeinern.

18.4. Bemerkung. Für $i = 1, 2$ seien A_i, B_i R-Algebren, N_i ein B_i-Linksmodul und M_i ein A_i-B_i-Bimodul über R. Dann ist $M_i \otimes_{B_i} N_i$ ein A_i-Linksmodul, also $(M_1 \otimes_{B_1} N_1) \otimes_R (M_2 \otimes_{B_2} N_2)$ ein $A_1 \otimes_R A_2$-Linksmodul. Andererseits ist $N_1 \otimes_R N_2$ ein $B_1 \otimes_R B_2$-Linksmodul und $M_1 \otimes_R M_2$ ein $A_1 \otimes_R A_2$-$B_1 \otimes_R B_2$-Bimodul über R, wie man leicht sieht. Daher ist $(M_1 \otimes_R M_2) \otimes_{B_1 \otimes_R B_2} (N_1 \otimes_R N_2)$ ein $A_1 \otimes_R A_2$-Linksmodul.

Satz. *In der obigen Situation existiert genau ein $A_1 \otimes_R A_2$-Isomorphismus*

$$\gamma : (M_1 \otimes_{B_1} N_1) \otimes_R (M_2 \otimes_{B_2} N_2) \to (M_1 \otimes_R M_2) \otimes_{B_1 \otimes_R B_2} (N_1 \otimes_R N_2)$$

mit $\gamma((m_1 \otimes n_1) \otimes (m_2 \otimes n_2)) = (m_1 \otimes m_2) \otimes (n_1 \otimes n_2)$ für $m_i \in M_i,\ n_i \in N_i,\ i = 1, 2$.

Definition. Wir bezeichnen γ als *kanonisch*.

Beweis. Für $m_1 \in M_1,\ n_1 \in N_1$ ist die Abbildung

$$\begin{aligned} M_2 \times N_2 &\to (M_1 \otimes_R M_2) \otimes_{B_1 \otimes_R B_2} (N_1 \otimes_R N_2), \\ (m_2, n_2) &\mapsto (m_1 \otimes m_2) \otimes (n_1 \otimes n_2) \end{aligned}$$

ausgeglichen, induziert also einen $\mathbb{Z}$-Homomorphismus

$$\alpha_{m_1, n_1} : M_2 \otimes_{B_2} N_2 \to (M_1 \otimes_R M_2) \otimes_{B_1 \otimes_R B_2} (N_1 \otimes_R N_2)$$

mit $\alpha_{m_1,n_1}(m_2 \otimes n_2) = (m_1 \otimes m_2) \otimes (n_1 \otimes n_2)$ für $m_2 \in M_2,\ n_2 \in N_2$. Man rechnet leicht nach, daß α_{m_1,n_1} ein R-Homomorphismus ist und

$$\begin{aligned} \alpha_{m_1+m_1',n_1} &= \alpha_{m_1,n_1} + \alpha_{m_1',n_1}, \\ \alpha_{m_1,n_1+n_1'} &= \alpha_{m_1,n_1} + \alpha_{m_1,n_1'}, \\ \alpha_{m_1 b_1,n_1} &= \alpha_{m_1,b_1 n_1} \end{aligned}$$

für $m_1, m_1' \in M_1,\ n_1, n_1' \in N_1,\ b_1 \in B_1$ ist. Daher ist die Abbildung

$$\begin{aligned} M_1 \times N_1 &\to \operatorname{Hom}_R(M_2 \otimes_{B_2} N_2, (M_1 \otimes_R M_2) \otimes_{B_1 \otimes_R B_2} (N_1 \otimes_R N_2)), \\ (m_1, n_1) &\mapsto \alpha_{m_1,n_1} \end{aligned}$$

ausgeglichen, induziert also einen $\mathbb{Z}$-Homomorphismus

$$\beta : M_1 \otimes_{B_1} N_1 \to \operatorname{Hom}_R(M_2 \otimes_{B_2} N_2, (M_1 \otimes_R M_2) \otimes_{B_1 \otimes_R B_2} (N_1 \otimes_R N_2))$$

mit $\beta(m_1 \otimes n_1) = \alpha_{m_1,n_1}$ für $m_1 \in M_1,\ n_1 \in N_1$. Man rechnet leicht nach, daß β ein R-Homomorphismus ist. Daher ist die Abbildung

$$\begin{aligned} (M_1 \otimes_{B_1} N_1) \times (M_2 \otimes_{B_2} N_2) &\to (M_1 \otimes_R M_2) \otimes_{B_1 \otimes_R B_2} (N_1 \otimes_R N_2), \\ (x, y) &\mapsto (\beta(x))(y) \end{aligned}$$

ausgeglichen, induziert also einen $\mathbb{Z}$-Homomorphismus

$$\gamma : (M_1 \otimes_{B_1} N_1) \otimes_R (M_2 \otimes_{B_2} N_2) \to (M_1 \otimes_R M_2) \otimes_{B_1 \otimes_R B_2} (N_1 \otimes_R N_2)$$

mit $\gamma(x \otimes y) = (\beta(x))(y)$ für $x \in M_1 \otimes_{B_1} N_1,\ y \in M_2 \otimes_{B_2} N_2$; insbesondere ist

$$\begin{aligned} \gamma((m_1 \otimes n_1) \otimes (m_2 \otimes n_2)) &= (\beta(m_1 \otimes n_1))(m_2 \otimes n_2) \ = \ \alpha_{m_1,n_1}(m_2 \otimes n_2) \\ &= (m_1 \otimes n_1) \otimes (n_1 \otimes n_2) \end{aligned}$$

für $m_i \in M_i,\ n_i \in N_i,\ i = 1, 2$. Analog konstruiert man einen $\mathbb{Z}$-Homomorphismus

$$\delta : (M_1 \otimes_R M_2) \otimes_{B_1 \otimes_R B_2} (N_1 \otimes_R N_2) \to (M_1 \otimes_{B_1} N_1) \otimes_R (M_2 \otimes_{B_2} N_2)$$

mit $\delta((m_1 \otimes m_2) \otimes (n_1 \otimes n_2)) = (m_1 \otimes n_1) \otimes (m_2 \otimes n_2)$ für $m_i \in M_i,\ n_i \in N_i,\ i = 1, 2$. Dann ist $\gamma \circ \delta = \mathrm{id}$ und $\delta \circ \gamma = \mathrm{id}$; insbesondere ist γ bijektiv. Ferner ist γ eindeutig bestimmt. Wegen

$$\begin{aligned} (a_1 \otimes a_2)\gamma((m_1 \otimes n_1) \otimes (m_2 \otimes n_2)) &= (a_1 \otimes a_2)((m_1 \otimes m_2) \otimes (n_1 \otimes n_2)) \\ &= (a_1 \otimes a_2)(m_1 \otimes m_2) \otimes (n_1 \otimes n_2) \\ &= (a_1 m_1 \otimes a_2 m_2) \otimes (n_1 \otimes n_2) \\ &= \gamma((a_1 m_1 \otimes n_1) \otimes (a_2 m_2 \otimes n_2)) \\ &= \gamma(a_1(m_1 \otimes n_1) \otimes a_2(m_2 \otimes n_2)) \\ &= \gamma((a_1 \otimes a_2)((m_1 \otimes n_1) \otimes (m_2 \otimes n_2))) \end{aligned}$$

für $a_i \in A_i,\ m_i \in M_i,\ n_i \in N_i,\ i = 1, 2$ folgt leicht, daß γ ein $A_1 \otimes_R A_2$-Isomorphismus ist. □

18.5. Bemerkung. Für $i = 1, 2$ seien A_i, B_i R-Algebren, $\rho_i : B_i \to A_i$ ein Homomorphismus und N_i ein B_i-Linksmodul, also $\operatorname{Ind}_{\rho_i} N_i = A_i \rho_i(1_{B_i}) \otimes_{B_i} N_i$ ein A_i-Linksmodul. Dann ist

$$\operatorname{Ind}_{\rho_1} N_1 \otimes_R \operatorname{Ind}_{\rho_2} N_2 = (A_1 \rho_1(1_{B_1}) \otimes_{B_1} N_1) \otimes_R (A_2 \rho_2(1_{B_2}) \otimes_{B_2} N_2)$$

ein $A_1 \otimes_R A_2$-Linksmodul, der nach 18.4 isomorph ist zu

$$\begin{aligned} &(A_1 \rho_1(1_{B_1}) \otimes_R A_2 \rho_2(1_{B_2})) \otimes_{B_1 \otimes_R B_2} (N_1 \otimes_R N_2) \\ \simeq\ &(A_1 \otimes_R A_2)(\rho_1(1 B_1) \otimes \rho_2(1_{B_2})) \otimes_{B_1 \otimes_R B_2} (N_1 \otimes_R N_2) \\ \simeq\ &(A_1 \otimes_R A_2)((\rho_1 \otimes \rho_2)(1_{B_1} \otimes 1_{B_2})) \otimes_{B_1 \otimes_R B_2} (N_1 \otimes_R N_2) \\ =\ &\operatorname{Ind}_{\rho_1 \otimes \rho_2}(N_1 \otimes_R N_2). \end{aligned}$$

Also ist $\operatorname{Ind}_{\rho_1} N_1 \otimes_R \operatorname{Ind}_{\rho_2} N_2 \simeq \operatorname{Ind}_{\rho_1 \otimes \rho_2}(N_1 \otimes_R N_2)$, und analog ist $\operatorname{Res}_{\rho_1} M_1 \otimes_R \operatorname{Res}_{\rho_2} M_2 \simeq \operatorname{Res}_{\rho_1 \otimes \rho_2}(M_1 \otimes_R M_2)$ für A_i-Linksmoduln M_i, $i = 1, 2$.

18.6. Definition. Eine *Darstellung* einer R-Algebra A ist ein unitärer Homomorphismus von R-Algebren $\Delta : A \to \mathrm{End}_R(M)$, wobei M ein R-Linksmodul ist.

Bemerkung. In diesem Fall wird M, wie man leicht sieht, zu einem A-Linksmodul, wenn man $am := (\Delta(a))(m)$ für $a \in A,\ m \in M$ definiert. Umgekehrt liefert jeder A-Linksmodul M, wie man leicht nachrechnet, eine Darstellung $\Delta : A \to \mathrm{End}_R(M)$ mit $(\Delta(a))(m) = am$ für $a \in A,\ m \in M$. Daher entsprechen sich Darstellungen von A und A-Linksmoduln.

Beispiel. Eine *Darstellung* einer Gruppe über R ist ein Homomorphismus von Gruppen $\Delta : G \to \mathrm{Aut}_R(M)$, wobei M ein R-Linksmodul ist. Jede solche Darstellung von G läßt sich nach 17.4 zu einem unitären Homomorphismus von Algebren $RG \to \mathrm{End}_R(M)$, d.h. zu einer Darstellung von RG fortsetzen. Umgekehrt liefert jede Darstellung $\Delta : RG \to \mathrm{End}_R(M)$ von RG durch Einschränkung eine Darstellung $G \to \mathrm{Aut}_R(M)$ von G. Daher entsprechen sich Darstellungen von G über R und Darstellungen von RG.

18.7. Definition. Darstellungen $\Delta_1 : A \to \mathrm{End}_R(M_1),\ \Delta_2 : A \to \mathrm{End}_R(M_2)$ einer R-Algebra A nennt man *ähnlich* oder *äquivalent*, falls ein R-Isomorphismus $f : M_1 \to M_2$ existiert mit $\Delta_2(a) \circ f = f \circ \Delta_1(a)$ für $a \in A$.

Bemerkung. In diesem Fall ist f ein Isomorphismus zwischen den durch 18.6 definierten A-Linksmoduln M_1, M_2, wie man leicht sieht. Umgekehrt sind für isomorphe A-Linksmoduln M_1, M_2 die durch 18.6 definierten Darstellungen $\Delta_1 : A \to \mathrm{End}_R(M_1),\ \Delta_2 : A \to \mathrm{End}_R(M_2)$ äquivalent. Daher entsprechen sich Äquivalenzklassen von Darstellungen von A und Isomorphieklassen von A-Linksmoduln.

Beispiel. Darstellungen $\Delta_1 : G \to \mathrm{Aut}_R(M_1),\ \Delta_2 : G \to \mathrm{Aut}_R(M_2)$ einer Gruppe G über R nennt man *ähnlich* oder *äquivalent*, falls ein R-Isomorphismus $f : M_1 \to M_2$ existiert mit $\Delta_2(g) \circ f = f \circ \Delta_1(g)$ für $g \in G$. In diesem Fall sind auch die durch 18.6 definierten Darstellungen $RG \to \mathrm{End}_R(M_1),\ RG \to \mathrm{End}_R(M_2)$ äquivalent. Umgekehrt liefern äquivalente Darstellungen von RG nach Einschränkung äquivalente Darstellungen von G über R. Daher entsprechen sich Äquivalenzklassen von Darstellungen von RG und Äquivalenzklassen von Darstellungen von G über R.

18.8. Definition. Eine *Matrixdarstellung* das *Grades* n einer R-Algebra A ist ein unitärer Homomorphismus $\Lambda : A \to \mathrm{Mat}(n, R)$.

Bemerkung. In diesem Fall wird der freie R-Linksmodul $R^{n\times 1}$ zu einem A-Linksmodul mit $ax := \Lambda(a)x$ für $a \in A,\ x \in R^{n\times 1}$. Ist umgekehrt M ein A-Linksmodul, der als R-Linksmodul frei von endlichem Rang mit Basis $b_1, \dots, b_n$ ist, und schreibt man $ab_j = \sum_{i=1}^n \lambda_{ij}(a)b_j$ mit $\lambda_{ij}(a) \in R$ für $a \in A,\ i, j = 1, \dots, n$, so ist die Abbildung $\Lambda : A \to \mathrm{Mat}(n, R),\ a \mapsto (\lambda_{ij}(a))$ eine Matrixdarstellung des Grades n von A, wie man leicht nachrechnet.

Beispiel. Eine *Matrixdarstellung* des *Grades* n über R einer Gruppe G ist ein Homomorphismus $\Lambda : G \to \mathrm{GL}(n, R)$. Jede solche können wir nach 17.4 zu einem unitären Homomorphismus $RG \to \mathrm{Mat}(n, R)$, d.h. zu einer Matrixdarstellung von RG, fortsetzen. Umgekehrt liefert jede Matrixdarstellung $\Lambda : RG \to \mathrm{Mat}(n, R)$ durch Einschränkung eine Matrixdarstellung $G \to \mathrm{GL}(n, R)$ von G über R. Daher entsprechen sich Matrixdarstellungen von RG und Matrxdarstellungen von G über R.

18.9. Definition. Matrixdarstellungen $\Lambda_1, \Lambda_2 : A \to \mathrm{Mat}(n, R)$ des gleichen Grades n einer R-Algebra A nennt man *ähnlich* oder *äquivalent*, falls ein $P \in \mathrm{GL}(n, R)$ existiert mit $\Lambda_2(a)P = P\Lambda_1(a)$ für $a \in A$.

Bemerkung. In diesem Fall ist die Abbildung $R^{n\times 1} \to R^{n\times 1},\ x \to Px$ ein Isomorphismus zwischen den durch Λ_1 und Λ_2 definierten A-Linksmodulstrukturen auf $R^{n\times 1}$. Umgekehrt seien M, N isomorphe A-Linksmoduln, die als R-Linksmoduln frei von endlichem Rang sind, mit Basen $b_1, \dots, b_n$ bzw. $c_1, \dots, c_n$, und sei $f : M \to N$ ein A-Isomorphismus mit Matrix P bzgl. $b_1, \dots, b_n$ bzw. $c_1, \dots, c_n$. Sind Λ_1, Λ_2 die durch M und $b_1, \dots, b_n$ bzw. N und $c_1, \dots, c_n$ definierten Matrixdarstellungen von A, so ist $\Lambda_2(a)P = P\Lambda_1(a)$ für $a \in A$, d.h. Λ_1 und Λ_2 sind äquivalent.

Beispiel. Matrixdarstellungen $\Lambda_1, \Lambda_2 : G \to \mathrm{GL}(n, R)$ einer Gruppe G über R nennt man *ähnlich* oder *äquivalent*, falls ein $P \in \mathrm{GL}(n, R)$ existiert mit $\Lambda_2(g)P = P\Lambda_1(g)$ für $g \in G$. In diesem Fall sind auch die Fortsetzugen $RG \to \mathrm{Mat}(n, R)$ von Λ_1, Λ_2 als Matrixdarstellungen von RG äquivalent. Umgekehrt liefern äquivalente Matrixdarstellungen $\Lambda_1, \Lambda_2 : RG \to \mathrm{Mat}(n, R)$ von RG durch Einschränkung äquivalente Matrixdarstellungen von G über R. Daher entsprechen sich Äquivalenzklassen von Matrixdarstellungen von RG und Äquivalenzklassen von Matrixdarstellungen von G über R.

KAPITEL 19

Skalarerweiterungen

19.1. Bemerkung. Für jeden kommutativen Ring R und eine R-Algebra S erhält man durch $r \mapsto r1_S$ einen unitären Homomorphismus von Ringen $R \to Z(S)$. Ist umgekehrt R ein kommutativer Ring, S ein beliebiger Ring und $\rho : R \to Z(S)$ ein unitärer Homomorphismus von Ringen, so wird S, wie man leicht nachrechnet, zu einer R-Algebra durch $rs := \rho(r)s$ für $r \in R,\ s \in S$. Daher kann man für jeden kommutativen Ring R R-Algebren mit Paaren (S, ρ) identifizieren, wobei S ein Ring und $\rho : R \to Z(S)$ ein unitärer Ringhomomorphismus ist.

19.2. Bemerkung. Seien R, S kommutative Ringe, $\rho : R \to S$ ein unitärer Homomorphismus und A eine R-Algebra. Nach 19.1 kann man S als R-Algebra ansehen. Daher wird $S \otimes_R A$ nach 17.1 zu einer R-Algebra mit $(s \otimes a)(t \otimes b) = st \otimes ab$ für $s, t \in S,\ a, b \in A$. Andererseits ist $S \otimes_R A = \mathrm{Ind}_\rho A$ nach 15.4 ein S-Linksmodul mit $s(t \otimes a) = st \otimes a$ für $s, t \in S,\ a \in A$. Wegen

$$\begin{aligned}
s((t \otimes a)(u \otimes b)) &= s(tu \otimes ab) \ = \ stu \otimes ab \\
&= (st \otimes a)(u \otimes b) \ = \ (s(t \otimes a))(u \otimes b), \\
s((t \otimes a)(u \otimes b)) &= stu \otimes ab \ = \ tsu \otimes ab \\
&= (t \otimes a)(su \otimes b) \ = \ (t \otimes a)(s(u \otimes b))
\end{aligned}$$

für $s, t, u \in S,\ a, b \in A$ folgt $s(xy) = (sx)y = x(sy)$ für $s \in S,\ x, y \in S \otimes_R A$. Wir können also $\mathrm{Ind}_\rho A = S \otimes_R A$ als S-Algebra auffassen. Man sagt, daß $S \otimes_R A$ durch *Skalarerweiterung* aus A entsteht. Ist ρ aus dem Zusammenhang klar, so schreiben wir auch $\mathrm{Ind}_R^S A$ statt $\mathrm{Ind}_\rho A$. Es ist klar, daß viele in den vorangegangenen Kapiteln konstruierten kanonischen Homomorphismen und Isomorphismen in unserer Situation zu Homomorphismen und Isomorphismen von S-Algebren werden. Im einzelnen gehen wir darauf nicht ein.

Satz. *Für jeden kommutativen Ring R, jede kommutative R-Algebra S und jede Gruppe existiert genau ein Isomorphismus von S-Algebren $\varphi : S \otimes_R RG \to SG$ mit $\varphi(s \otimes x) = sx$ für $s \in S,\ x \in RG$.*

Beweis. Die Abbildungen $\alpha : S \to SG,\ s \mapsto s1_G$ und $\beta : RG \to SG,\ x \mapsto x$ sind Homomorphismen von R-Algebren mit $\alpha(s)\beta(x) = \beta(x)\alpha(s)$ für $s \in S,\ x \in RG$, induzieren also einen Homomorphismus von R-Algebren $\varphi : S \otimes_R RG \to SG$ mit $\varphi(s \otimes x) = \alpha(s)\beta(x) = sx$ für $s \in S,\ x \in RG$. Man rechnet leicht nach, daß φ Homomorphismus von S-Algebren ist.
Andererseits ist $\psi : G \to S \otimes_R RG,\ g \mapsto 1 \otimes g$ eine Abbildung mit $\psi(g)\psi(h) = \psi(gh)$ für $g, h \in G$, läßt sich also fortsetzen zu einem Homomorphismus von S-Algebren $SG \to S \otimes_R RG$, den wir wieder mit ψ bezeichnen. Dann ist $\psi(\varphi(1 \otimes g)) = 1 \otimes g$ und $\varphi(\psi(g)) = g$ für $g \in G$. Da SG und $S \otimes_R RG$ von den Elementen $g \in G$ bzw. $1 \otimes g,\ g \in G$, erzeugt werden, folgt: $\varphi \circ \psi = \mathrm{id}$ und $\psi \circ \varphi = \mathrm{id}$. $\square$

19.3. Bemerkung. Für jeden kommutativen Ring R, jede kommutative R-Algebra S und beliebige R-Algebren A, B konstruiert man leicht Isomorphismen von S-Algebren

$$\begin{aligned}
S \otimes_R (A \times B) &\cong (S \otimes_R A) \times (S \otimes_R B), \\
S \otimes_R (A \otimes_R B) &\cong (S \otimes_R A) \otimes_S (S \otimes_R B).
\end{aligned}$$

Ferner kann man jede kommutative S-Algebra T auch als R-Algebra auffassen mit $rt := (r1_S)t$ für $r \in R,\ t \in T$, und man konstruiert leicht einen Isomorphismus von T-Algebren

$$T \otimes_S (S \otimes_R A) \ \cong \ T \otimes_R A.$$

19.4. Bemerkung. Seien R ein kommutativer Ring, S eine kommutative R-Algebra, A eine beliebige R-Algebra und M ein A-Linksmodul. Fassen wir S als S-Linksmodul auf, so wird $S \otimes_R M$ nach 18.2 zu einem Linksmodul über der R-Algebra $S \otimes_R A$. Daher können wir $S \otimes_R M$ auch als Linksmodul über der S-Algebra $S \otimes_R A$ ansehen. Man sagt, daß $S \otimes_R M$ durch *Skalarerweiterung* aus M entsteht. Man zeigt, daß zu 19.3 analoge Rechenregeln gelten.

19.5. Bemerkung. Seien R ein kommutativer Ring, S eine kommutative R-Algebra und B eine beliebige S-Algebra. Dann kann man B auch als R-Algebra ansehen mit $rb := (r1_S)b$ für $r \in R,\ b \in B$. Man sagt, daß diese R-Algebra $Res_R^S B$ durch *Skalarrestriktion* aus B entsteht. Näher gehen wir darauf nicht ein.

KAPITEL 20

Endlich-dimensionale Algebren und das Radikal

Sei F ein algebraisch abgeschlossener Körper.

20.1. Bemerkung. Im folgenden betrachten wir endlich-dimensionale Algebren über F. Wichtige Beispiele sind die volle Matrixalgebra $\mathrm{Mat}(n, F)$ und die Gruppenalgebra FG einer endlichen Gruppe G über F. Die Voraussetzung, daß F algebraisch abgeschlossen ist, dient nur unserer Bequemlichkeit. Viele unserer Sätze lassen sich auf beliebige Körper verallgemeinern. Die Voraussetzung endlicher Dimension sichert, daß unsere Algebren rechts- und linksartinsch sind; denn alle Rechts- und Linksideale von A sind automatisch F-Untervektorräume. Wir können also die entsprechenden Sätze aus der Algebra anwenden. Für eine endlich-dimensionale F-Algebra A bezeichnen wir mit $J(A) = JA$ das *Radikal* von A, d.h. den Durchschnitt aller maximalen Linksideale von A. Aus der Algebra wissen wir, daß JA auch der Durchschnitt aller maximalen Rechtsideale von A und ein nilpotentes Ideal in A ist (d.h. es existiert ein $n \in \mathbb{N}$ mit $x_1 \dots x_n = 0$ für alle $x_1, \dots, x_n \in JA$). Ferner enthält JA jedes Linksideal (Rechtsideal) von A, das aus lauter nilpotenten Elementen besteht (d.h. Elemente x mit $x^n = 0$ für ein $n \in \mathbb{N}$). Für jedes Ideal I von A gilt bekanntlich $JA + I/I \subseteq J(A/I)$, und im Fall $I \subseteq JA$ gilt sogar $J(A/I) = JA/I$; insbesondere ist $J(A/JA) = JA/JA = 0$.

Satz. *Für endlich-dimensionale F-Algebren A, B ist $J(A \times B) = JA \times JB$.*

Beweis. Offenbar ist $JA \times JB$ ein nilpotentes Ideal in $A \times B$, also $JA \times JB \subseteq J(A \times B)$. Bezeichnet $\pi : A \times B \to A$ die Projektion, so ist andrerseits $\pi(J(A \times B))$ ein nilpotentes Ideal in A, also $\pi(J(A \times B)) \subseteq JA$. Analog ist $\rho(J(A \times B)) \subseteq JB$ für die Projektion $\rho : A \times B \to B$. Daher ist $J(A \times B) \subseteq \pi(J(A \times B)) \times \rho(J(A \times B)) \subseteq JA \times JB$. □

20.2. Bemerkung. Seien A eine endlich-dimensionale F-Algebra und B ein Unteralgebra von A. Dann ist $B \cap JA$ ein nilpotentes Ideal in B, also $B \cap JA \subseteq JB$. I.a. ist $B \cap JA \neq JB$.

Beispiel. Für $z \in JZA := J(Z(A))$ ist $zA = Az$, also $(zA)^n = z^n A$ für $n \in \mathbb{N}$. Daher ist zA ein nilpotentes Ideal in A, d.h. $z \in zA \subseteq JA$. Folglich ist $JZA \subseteq JA \cap ZA$, also $JZA = JA \cap ZA$.

20.3. Bemerkung. Seien A eine endlich-dimensionale F-Algebra und $e \in A$ mit $e^2 = e$. (Man nennt e *idempotent* oder ein *Idempotent*.) Dann ist $eAe := \{eae : a \in A\}$ eine Unteralgebra von A mit Einselement $1_{eAe} = e$. Nach 20.2 ist $JA \cap eAe \subseteq J(eAe)$. Für jedes Ideal I in eAe ist andrerseits $AIA := \{\sum_{i=1}^n a_i x_i b_i : a_i, b_i \in A,\ x_i \in I,\ i = 1, \dots, n,\ n \in \mathbb{N}_0\}$ ein Ideal in A, und für Ideale I, I' ist

$$(AIA)(AI'A) = AIAI'A = AIeAeI'A = AII'A.$$

Daher ist $(AIA)^n = AI^n A$ für $n \in \mathbb{N}$. Mit I ist also auch AIA nilpotent; insbesondere ist $AJ(eAe)A$ ein nilpotentes Ideal in A, d.h. $AJ(eAe)A \subseteq JA$. Folglich ist $J(eAe) \subseteq JA \cap eAe$, also $J(eAe) = JA \cap eAe = eJAe$.

20.4. Bemerkung. Ein Linksmodul M über einer endlich-dimensionalen F-Algebra A heißt *halbeinfach*, falls er eine (direkte) Summe von einfachen A-Linksmoduln ist. Man nennt A eine *halbeinfache* F-Algebra, wenn A als A-Linksmodul halbeinfach ist. Bekanntlich ist dies genau dann der Fall, wenn A als A-Rechtsmodul halbeinfach ist. Ferner ist diese Bedingung äquivalent zu $JA = 0$. Der Satz von Wedderburn aus der Algebra besagt, daß A genau dann halbeinfach ist, wenn A zu einem direkten Produkt von endlich vielen vollen Matrixalgebren über Schiefkörpern isomorph ist. In unserer Situation ist jeder dabei auftretende Schiefkörper D selbst eine endlich-dimensionale F-Algebra. Für $d \in D$ bilden also die F-Linearkombinationen der Elemente $1_D, d, d^2, d^3, \dots$ einen Erweiterungskörper E endlichen Grades des zu F isomorphen Körpers $F1_D$. Da F und $F1_D$ algebraisch abgeschlossen sind, folgt $E = F1_D$, also $D = F1_D \cong F$. Es gilt also:

Satz (Wedderburn). *Eine endlich-dimensionale F-Algebra A ist genau dann halbeinfach, wenn A zu einem direkten Produkt von endlich vielen vollen Matrixalgebren über F isomorph ist.*

Beispiel. Für eine beliebige endlich-dimensionale F-Algebra A ist A/JA nach 20.1 halbeinfach, also $A/JA \cong \prod_{i=1}^n \mathrm{Mat}(d_i, F)$ mit Zahlen $n \in \mathbb{N}_0,\ d_1, \ldots, d_n \in \mathbb{N}$, die, wie in der Algebra gezeigt wird, eindeutig bestimmt sind.

20.5. Satz. *Für endlich-dimensionale halbeinfache F-Algebren A, B sind auch $A \times B$ und $A \otimes_F B$ halbeinfach.*

Beweis. Ist $A \cong \prod_{i=1}^m \mathrm{Mat}(d_i, F)$ und $B \cong \prod_{j=1}^n \mathrm{Mat}(e_j, F)$ mit $m, n \in \mathbb{N}_0,\ d_1, \ldots, d_m,\ e_1, \ldots, e_n \in \mathbb{N}$, so ist

$$A \times B \ \cong\ \prod_{i=1}^m \mathrm{Mat}(D_i, F) \times \prod_{j=1}^n \mathrm{Mat}(e_j, F)$$

und

$$A \otimes_F B \ \cong\ \prod_{i,j} \mathrm{Mat}(d_i, F) \otimes_F \mathrm{Mat}(e_j, F) \ \cong\ \prod_{i,j} \mathrm{Mat}(d_i e_j, F).$$

□

20.6. Satz. *Seien A eine endlich-dimensionale F-Algebra und I ein nilpotentes Ideal in A. Ist A/I halbeinfach, so ist $I = JA$.*

Beweis. Da I nilpotent ist, ist $I \subseteq JA$. Ist A/I halbeinfach, so ist $0 = J(A/I) = JA/I$, d.h. $JA = I$. □

Bemerkung. Für endlich-dimensionale F-Algebren A, B ist $JA \otimes_F B$ ein nilpotentes Ideal in $A \otimes_F B$, also $JA \otimes_F B \subseteq J(A \otimes_F B)$ und analog $A \otimes_F JB \subseteq J(A \otimes_F B)$. Daher ist $I := JA \otimes_F B + A \otimes_F JB$ ein nilpotentes Ideal in $A \otimes_F B$. Nach 14.4 gibt es einen Isomorphismus von F-Algebren $\varphi : (A \otimes_F B)/I \to A/JA \otimes_F B/JB$. Mit A/JA und B/JB ist nach 20.5 auch $A/JA \otimes_F B/JB$ und $(A \otimes_F B)/I$ halbeinfach. Nach dem obigen Satz ist also $J(A \otimes_F B) = I = JA \otimes_F B + A \otimes_F JB$.

20.7. Bemerkung. Sind $A_1, \ldots, A_n$ F-Algebren und ist I_j ein Ideal in A_j für $j = 1, \ldots, n$, so ist offenbar $I_1 \times \ldots \times I_n$ ein Ideal in $A_1 \times \ldots \times A_n$. Man zeigt leicht, daß umgekehrt jedes Ideal in $A_1 \times \ldots \times A_n$ so entsteht. Ist $A_i = \mathrm{Mat}(d_i, F)$ mit $d_i \in \mathbb{N}$ für $i = 1, \ldots, n$, so ist $I_i \in \{0, A_i\}$ wegen der Einfachheit von A_i für $i = 1, \ldots, n$. Daher ist

$$(A_1 \times \ldots \times A_n) \ / \ (I_1 \times \ldots \times I_n) \cong (A_1/I_1) \times \ldots \times (A_n/I_n) \cong \prod_{i: I_i = 0} A_i$$

halbeinfach. Dies zeigt, daß jeder Restklassenring einer halbeinfachen F-Algebra halbeinfach ist.

Satz. *Für jede endlich-dimensionale F-Algebra A und jedes Ideal I in A ist $J(A/I) = JA + I/I$.*

Beweis. Offenbar ist $JA + I/I$ ein nilpotentes Ideal in A/I, und

$$(A/I) \ / \ (JA + I/I) \cong A/JA + I \cong (A/JA) \ / \ (JA + I/JA)$$

ist halbeinfach. Mit 20.6 folgt die Behauptung. □

20.8. Satz. *Ist A eine endlich-dimensionale F-Algebra und B eine Unteralgebra von A mit $A = B + (JA)^2$, so ist $A = B$.*

Beweis. Aus $A = B + (JA)^2$ folgt $JA = (B \cap JA) + (JA)^2$ nach Dedekind. Daher ist $(JA)^n = (B \cap JA)^n + (JA)^{n+1}$ für $n \in \mathbb{N}$. Folglich ist

$$\begin{aligned} A &= B + (JA)^2 = B + (B \cap JA)^2 + (JA)^3 \\ &= B + (JA)^3 = B + (B \cap JA)^3 + (JA)^4 \\ &= B + (JA)^4 = \ldots = B. \end{aligned}$$

$\square$

20.9. Bemerkung. Sei G eine endliche Gruppe und $\operatorname{char} F \nmid |G|$ (z.B. $\operatorname{char} F = 0$). Der Satz von Maschke aus der Darstellungstheorie I besagt, daß in diesem Fall jede Matrixdarstellung von G über F zu einer direkten Summe von irreduziblen Matrixdarstellungen ähnlich ist. Dies bedeutet, daß jeder endlich-dimensionale FG-Modul halbeinfach ist. Insbesondere ist im Fall $\operatorname{char} F \nmid |G|$ die Gruppenalgebra FG halbeinfach.

20.10. Bemerkung. Sei G eine endliche Gruppe und $p := \operatorname{char} F \mid |G|$. Für jede endliche Teilmenge X von FG setzen wir $X^+ := \sum_{x \in X} x \in FG$. Für $h \in G$ ist dann $hG^+ = \sum_{g \in G} hg = \sum_{k \in G} k = G^+$, also $(G^+)^2 = |G|G^+ = 0$. Daher ist $F \cdot G^+$ ein nilpotentes Ideal in FG, also $JFG \neq 0$. Es ist i.a. schwierig, JFG genau zu berechnen.

KAPITEL 21

Kommutatoren

Seien F ein algebraisch abgeschlossener Körper und $p := \operatorname{char} F$.

21.1. Definition. Für jede Teilmenge X einer endlich-dimensionalen F-Algebra A bezeichnen wir mit FX den von X aufgespannten F-Untervektorraum von A. Für $a, b \in A$ nennen wir $[a, b] := ab - ba$ den *Kommutator* von a und b. Für $U, V \subseteq A$ nennen wir $[U, V] := F\{[u, v] : u \in U,\ v \in V\}$ den *Kommutator* von U und V. Ferner nennen wir $[A, A] =: K(A) = KA$ den *Kommutatorraum* von A.

Bemerkung. Man rechnet leicht nach, daß für $a, b, c \in A,\ \alpha \in F$ gilt:
(i) $\alpha[a, b] = [\alpha a, b]$.
(ii) $[a + b, c] = [a, c] + [b, c]$.
(iii) $[b, a] = -[a, b]$.
(iv) $[a, [b, c]] + [b, [c, a]] + [c, [a, b]] = 0$ (Jacobi-Identität).

Satz.
(i) *Für jede endlich-dimensionale F-Algebra A ist KA ein ZA-Untermodul von A.*
(ii) *Für jedes Ideal I von A ist $K(A/I) = KA + I/I$.*
(iii) *Für endlich-dimensionale F-Algebren $A_1, \dots, A_n$ ist $K(A_1 \times \dots \times A_n) = KA_1 \times \dots \times KA_n$.*
(iv) *Für endlich-dimensionale F-Algebren A, B ist $K(A \otimes_F B) = KA \otimes_F B + A \otimes_F KB$.*

Beweis.
(i) Für $a, b \in A$ und $z \in ZA$ ist

$$z[a, b] = z(ab - ba) = zab - zba = za \cdot b - b \cdot za = [za, b].$$

(ii),(iii) Trivial.
(iv) Für $a, a' \in A,\ b \in B$ ist

$$\begin{aligned} [a, a'] \otimes b &= (aa' - a'a) \otimes b = aa' \otimes b - a'a \otimes b \\ &= (a \otimes b)(a' \otimes 1) - (a' \otimes 1)(a \otimes b) \ \in\ K(A \otimes_F B). \end{aligned}$$

Daher ist $KA \otimes_F B \subseteq K(A \otimes_F B)$ und analog $A \otimes_F KB \subseteq K(A \otimes_F B)$. Andererseits ist $K(A \otimes_F B) = F\{[a \otimes b, a' \otimes b'] : a, a' \in A,\ b, b' \in B\}$, und für $a, a' \in A,\ b, b' \in B$ gilt:

$$\begin{aligned} [a \otimes b, a' \otimes b'] &= (a \otimes b)(a' \otimes b') - (a' \otimes b')(a \otimes b) \\ &= aa' \otimes bb' - a'a \otimes b'b \\ &= aa' \otimes bb' - a'a \otimes bb' + a'a \otimes bb' - a'a \otimes b'b \\ &= (aa' - a'a) \otimes bb' + a'a \otimes (bb' - b'b) \\ &= [a, a'] \otimes bb' - a'a \otimes [b, b'] \ \in\ KA \otimes_F B + A \otimes_F KB. \end{aligned}$$

□

21.2. Satz. *Für $n \in \mathbb{N}$ ist $K(\operatorname{Mat}(n, F))$ der Kern der Spurabbildung.*

Beweis. Für $a, b \in A := \operatorname{Mat}(n, F)$ ist

$$\operatorname{spur}([a, b]) = \operatorname{spur}(ab - ba) = \operatorname{spur}(ab) - \operatorname{spur}(ba) = 0.$$

Daher ist $KA \subseteq \mathrm{Ker(spur)}$. Ist $\{e_{ij} : i,j = 1,\dots,n\}$ die Standardbasis von A, so bilden die Elemente e_{ij} $(i \neq j)$ zusammen mit den Elementen $e_{ii} - e_{11}$ $(i = 2,\dots,n)$ eine Basis von $\mathrm{Ker(spur)}$. Für $i \neq j$ ist

$$e_{ij} = e_{ii}e_{ij} - e_{ij}e_{ii} = [e_{ii}, e_{ij}] \in KA,$$

und für $i = 2,\dots,n$ ist

$$e_{ii} - e_{11} = e_{i1}e_{1i} - e_{1i}e_{i1} = [e_{i1}, e_{1i}] \in KA.$$

Daher ist $\mathrm{Ker(spur)} \subseteq KA$. □

21.3. Bemerkung. Für jede Gruppe G bezeichnen wir mit $\mathrm{Cl}(G)$ die Menge der Konjugationsklassen von G.

Satz. *Ist G eine endliche Gruppe, $a \in FG$ und $a = \sum_{g\in G} \alpha_g g$ mit $\alpha_g \in F$ für $g \in G$, so gilt:*

$$a \in KFG \iff \sum_{g\in C} \alpha_g = 0 \text{ für } C \in \mathrm{Cl}(G).$$

Insbesondere ist $\dim FG/KFG = |\,\mathrm{Cl}(G)|$.

Beweis. Offenbar ist $KFG = F\{[g,h] : g,h \in G\}$, und für $g,h \in G$ ist

$$[g,h] = gh - hg = gh - h(gh)h^{-1}.$$

Daraus folgt leicht, daß jedes Element $a \in KFG$ die Bedingungen auf der rechten Seite erfüllt.
Sei umgekehrt $a = \sum_{g\in G} \alpha_g g \in FG$ mit $\sum_{g\in C} \alpha_g = 0$ für $C \in \mathrm{Cl}(G)$, und sei $g_C \in C$ für $C \in Cl(G)$. Wegen

$$xyx^{-1} - y = x \cdot yx^{-1} - yx^{-1} \cdot x = [x, yx^{-1}] \in KFG$$

für $x,y \in G$ ist $g - g_C \in KFG$ für $C \in \mathrm{Cl}(G)$ und $g \in C$, also

$$a = \sum_{C\in\mathrm{Cl}(G)} \sum_{g\in C} \alpha_g g \equiv \sum_{C\in\mathrm{Cl}(G)} \Big(\sum_{g\in C} \alpha_g\Big) g_C = 0 \pmod{KFG},$$

d.h. $a \in KFG$. □

21.4. Satz. *Seien A eine endlich-dimensionale F-Algebra und $A/JA \cong \prod_{i=1}^n \mathrm{Mat}(d_i, F)$ mit $n \in \mathbb{N}_0$, $d_1,\dots,d_n \in \mathbb{N}$. Dann ist $n = \dim A/JA + KA$.*

Beweis. Wir setzen $B := A/JA$ und $B_i := \mathrm{Mat}(d_i, F)$ für $i = 1,\dots,n$. Dann ist

$$\begin{aligned}
\dim A/JA + KA &= \dim(A/JA) \;/\; (JA + KA/JA)\\
&= \dim(A/JA) \;/\; K(A/JA) \;=\; \dim B/KB\\
&= \dim(B_1 \times \dots \times B_n) \;/\; (KB_1 \times \dots \times KB_n)\\
&= \dim B_1/KB_1 \times \dots \times B_n/KB_n \;=\; n
\end{aligned}$$

nach 21.2. □

Bemerkung. Aus der Algebra wissen wir, daß JA alle einfachen A-Moduln annulliert. Daher kann man die einfachen A-Moduln mit den einfachen A/JA-Moduln identifizieren. Aus der Algebra wissen wir auch, daß n die Anzahl der Isomorphieklassen einfacher A/JA-Moduln ist und damit auch die Anzahl der Isomorphieklassen einfacher A-Moduln.

21.5. Satz. *Seien $p > 0$, A eine endlich-dimensionale F-Algebra, $a,b \in A$ und $k \in KA$. Dann ist*

$$(a+b)^p \equiv a^p + b^p \pmod{KA}$$

und $k^p \in KA$.

Beweis. Multiplizieren wir $(a+b)^p$ aus, so erhalten wir eine Summe von 2^p Termen der Form $c_1 \dots c_p$ mit $c_1, \dots, c_p \in \{a,b\}$. Wegen $c_1 \dots c_p - c_i \dots c_p c_1 \dots c_{i-1} \in KA$ für $i = 2, \dots, p$ ist

$$c_1 \dots c_p + c_2 \dots c_p c_1 + \dots + c_p c_1 \dots c_{p-1} \equiv p c_1 \dots c_p \equiv 0 \pmod{KA}.$$

Daher ist $(a+b)^p \equiv a^p + b^p \pmod{KA}$. Für $x, y \in A$ ist

$$(xy - yx)^p \equiv (xy)^p - (yx)^p = (xy)^{p-1}x \cdot y - y \cdot (xy)^{p-1}x \equiv 0 \pmod{KA}.$$

Daher ist auch $k^p \in KA$ für $k \in KA$. □

Bemerkung. Aus dem Satz folgt leicht, daß die Abbildung $A/KA \to A/KA,\ a + KA \mapsto a^p + KA$ wohldefiniert und additiv ist. Wir schreiben auch $(a+KA)^p$ statt $a^p + KA$.

21.6. Satz. *Sei $p > 0$ und A eine endlich-dimensionale F-Algebra. Dann ist*

$$JA + KA = \{x \in A : x^{p^n} \in KA \text{ für ein } n \in \mathbb{N}\}.$$

Beweis. Sind $x, y \in A$ und $m, n \in \mathbb{N}$ mit $x^{p^m}, y^{p^n} \in KA$, so liegen nach 21.5 auch $x^{p^{m+n}}, y^{p^{m+n}}, (x+y)^{p^{m+n}} \in KA$. Daher ist die rechte Seite der obigen Gleichung ein F-Untervektorraum TA von A, der KA enthält. Da die Elemente in JA nilpotent sind, ist außerdem $JA \subseteq TA$. Daher genügt es zu zeigen, daß $TA \subseteq JA + KA$.
Sei $x \in TA$, und sei $n \in \mathbb{N}$ mit $x^{p^n} \in KA$. Dann ist

$$(x + JA)^{p^n} = x^{p^n} + JA \in KA + JA/JA = K(A/JA),$$

also $x + JA \in T(A/JA)$. Daher ist $TA/JA \subseteq T(A/JA)$, und es genügt zu zeigen: $T(A/JA) \subseteq K(A/JA)$. Sei $B := A/JA$, also $B \cong \prod_{i=1}^{k} \mathrm{Mat}(d_i, F)$ mit $k \in \mathbb{N}_0,\ d_1, \dots, d_k \in \mathbb{N}$. Wir setzen $B_i := \mathrm{Mat}(d_i, F)$ für $i = 1, \dots, k$ und können $B = B_1 \times \dots \times B_k$ annehmen. Wegen $KB = KB_1 \times \dots \times KB_k$ folgt leicht, daß $TB = TB_1 \times \dots \times TB_k$. Daher genügt es zu zeigen: $T(\mathrm{Mat}(d,F)) = K(\mathrm{Mat}(d,F))$ für $d \in \mathbb{N}$.
Wir wissen $K(\mathrm{Mat}(d,F)) \subseteq T(\mathrm{Mat}(d,F)) \subseteq \mathrm{Mat}(d,F)$ und $\dim \mathrm{Mat}(d,F)/K(\mathrm{Mat}(d,F)) = 1$. Sei $\{e_{ij} : i,j = 1, \dots, n\}$ die Standardbasis von $\mathrm{Mat}(d,F)$. Wegen $\mathrm{spur}(e_{11}) = 1$ ist $e_{11} \notin K(\mathrm{Mat}(d,F))$. Wegen $e_{11}^2 = e_{11}$ ist also auch $e_{11} \notin T(\mathrm{Mat}(d,F))$. Daher ist $T(\mathrm{Mat}(d,F)) \neq \mathrm{Mat}(d,F)$, also $T(\mathrm{Mat}(d,F)) = K(\mathrm{Mat}(d,F))$. □

21.7. Bemerkung. Seien G eine endliche Gruppe und p eine Primzahl. Ein Element $g \in G$ nennt man ein *p-Element* (bzw. *p'-Element*), falls seine Ordnung eine Potenz von p (bzw. zu p teilerfremd) ist. Die Menge aller p-Elemente (bzw. p'-Elemente) in G bezeichnen wir mit G_p (bzw. $G_{p'}$). I.a. sind G_p und $G_{p'}$ keine Untergruppen von G. Stets ist $G_p \cap G_{p'} = \{1\}$, aber i.a. ist $G_p \cup G_{p'} \neq G$. Zu jedem Element $g \in G$ existieren eindeutig bestimmte Elemente $g_p \in G_p,\ g_{p'} \in G_{p'}$ mit $g = g_p g_{p'} = g_{p'} g_p$. Wir nennen g_p den *p-Faktor* und $g_{p'}$ den *p'-Faktor* von g.
Sind $g, h \in G$ konjugiert, so schreiben wir $g \sim h$ oder genauer $g \sim_G h$. Sind $g, h \in G$ mit konjugierten p-Faktoren (bzw. p'-Faktoren), so schreiben wir $g \sim_p h$ (bzw. $g \sim_{p'} h$). Dann sind $\sim_p, \sim_{p'}$ Äquivalenzrelationen auf G, und die entsprechenden Äquivalenzklassen bezeichnet man als *p-Sektionen* (bzw. *p'-Sektionen*) von G.
Da konjugierte Elemente konjugierte p-Faktoren und konjugierte p'-Faktoren haben, ist jede p-Sektion und jede p'-Sektion Vereinigung von Konjugationsklassen. Dagegen brauchen zwei Elemente, die sowohl in der gleichen p-Sektion als auch in der gleichen p'-Sektion von G liegen, nicht konjugiert zu sein. Mit $\mathrm{Sec}_p(G)$ (bzw. $\mathrm{Sec}_{p'}(G)$) bezeichnen wir die Menge der p-Sektionen (bzw. p'-Sektionen) von G.
Offenbar enthält jede p-Sektion genau eine *p-Konjugationsklasse*, d.h. eine Konjugationsklasse, die aus lauter p-Elementen besteht. Analog enthält jede p'-Sektion genau eine p'-Konjugationsklasse, d.h. eine Konjugationsklasse, die aus lauter p'-Elementen besteht. Insbesondere ist $|\mathrm{Sec}_p(G)|$ die Anzahl der p-Konjugationsklassen von G und $|\mathrm{Sec}_{p'}(G)|$ die Anzahl der p'-Konjugationsklassen von G.
Mit $\exp(G)$ bezeichnen wir den *Exponenten* von G, d.h. die kleinste natürliche Zahl n mit $g^n = 1$ für $g \in G$. Mit $\exp_p(G)$ bezeichnen wir den Exponenten einer p-Sylowgruppe von G, d.h. die kleinste natürliche Zahl n mit $g^n = 1$ für $g \in G_p$.

Satz. *Für eine endliche Gruppe G, eine Primzahl p und Elemente $g, h \in G$ sind äquivalent:*

(1) $g \sim_{p'} h$.
(2) $g^{\exp_p(G)} \sim h^{\exp_p(G)}$.
(3) $\exists n \in \mathbb{N} : g^{p^n} \sim h^{p^n}$.

Beweis.

(1)⇒(2): Sei $x \in G$ mit $xg_{p'}x^{-1} = h_{p'}$ und $e := \exp_p(G)$. Dann ist $xg^e x^{-1} = x(g_p g_{p'})^e x^{-1} = xg_p^e g_{p'}^e x^{-1} = xg_{p'}^e x^{-1} = (xg_{p'}x^{-1})^e = h_{p'}^e = h_p^e h_{p'}^e = h^e$.

(2)⇒(3): Trivial.

(3)⇒(1): Sei $n \in \mathbb{N}$ mit $g^{p^n} \sim h^{p^n}$, und sei $|G| = p^a b$ mit $a, b \in \mathbb{N}_0$, $p \nmid b$. Wir können annehmen: $n \geq a$ und $p^n \equiv 1 \pmod b$. Dann ist $g^{p^n} = g_p^{p^n} g_{p'}^{p^n} = g_{p'}^{p^n} = g_{p'}$ und analog $h^{p^n} = h_{p'}$.

□

21.8. Satz. *Ist $p > 0$, G eine endliche Gruppe, $a \in FG$ und $a = \sum_{g \in G} \alpha_g g$ mit $\alpha_g \in F$ für $g \in G$, so gilt:*

$$a \in JFG + KFG \iff \sum_{g \in S} \alpha_g = 0 \textit{ für } S \in \mathrm{Sec}_{p'}(G).$$

Insbesondere ist $\dim FG/JFG + KFG = |\operatorname{Sec}_{p'}(G)|$.

Beweis.

⇒: Sei $a \in JFG + KFG$. Dann existiert ein $n \in \mathbb{N}$ mit $a^{p^n} \in KFG$, d.h.

$$0 = a^{p^n} \equiv \sum_{g \in G} \alpha_g^{p^n} g^{p^n} \pmod{KFG}.$$

Für $C \in \mathrm{Cl}(G)$ ist also

$$0 = \sum_{\substack{g \in G \\ g^{p^n} \in C}} \alpha_g^{p^n} = \Bigg(\sum_{\substack{g \in G \\ g^{p^n} \in C}} \alpha_g \Bigg)^{p^n}, \text{ d.h.} \quad 0 = \sum_{\substack{g \in G \\ g^{p^n} \in C}} \alpha_g.$$

Folglich ist $\sum_{g \in S} \alpha_g = 0$ für $S \in \mathrm{Sec}_{p'}(G)$.

⇐: Sei $\sum_{g \in S} \alpha_g = 0$ und $g_S \in S$ für $S \in \mathrm{Sec}_{p'}(G)$. Für $e := \exp_p(G)$, $S \in \mathrm{Sec}_{p'}(G)$ und $g \in S$ ist dann $g^e \sim g_S^e$, also $(g - g_S)^e \equiv g^e - g_S^e \equiv 0 \pmod{KFG}$ nach 21.3. Daher ist $g - g_S \in JFG + KFG$ und

$$a = \sum_{S \in \mathrm{Sec}_{p'}(G)} \sum_{g \in S} \alpha_g g \equiv \sum_{S \in \mathrm{Sec}_{p'}(G)} \Bigg(\sum_{g \in S} \alpha_g \Bigg) g_S = 0 \pmod{JFG + KFG},$$

d.h. $a \in JFG + KFG$.

□

Bemerkung. Nach 21.4 ist also $|\operatorname{Sec}_{p'}(G)|$ die Anzahl der Isomorphieklassen einfacher FG-Moduln, und nach 21.7 ist $|\operatorname{Sec}_{p'}(G)|$ auch die Anzahl der p'-Konjugationsklassen von G.

Beispiel. Für jede endliche Gruppe G wird F zu einem FG-Modul mit $g\alpha = \alpha$ für $g \in G$, $\alpha \in F$. Man nennt $F = F_G$ den *trivialen* FG-Modul. Ist G eine endliche p-Gruppe, so ist $|\operatorname{Sec}_{p'}(G)| = 1$, d.h. F_G ist bis auf Isomorphie der einzige einfache FG-Modul.

21.9. Bemerkung. Sei $p > 0$ und A eine endlich-dimensionale F-Algebra. Für $n \in \mathbb{N}_0$ ist dann $T_n A := \{x \in A : x^{p^n} \in KA\}$ nach 21.5 ein ZA-Untermodul von A, und es gilt: $KA = T_0 A \subseteq T_1 A \subseteq T_2 A \subseteq \dots$ und $JA + KA = \bigcup_{n \in \mathbb{N}} T_n A$. Wegen der endlichen Dimension von A existiert ein $N \in \mathbb{N}$ mit $T_N A = JA + KA$. Wir interessieren uns für das kleinste N mit dieser Eigenschaft.

Satz. *Seien* $p > 0$, G *eine endliche Gruppe,* $n \in \mathbb{N}_0$, $a \in FG$ *und* $a = \sum_{g \in G} \alpha_g g$ *mit* $\alpha_g \in F$ *für* $g \in G$. *Dann gilt:*

$$a \in T_n FG \iff \sum_{g \in C^{p^{-n}}} \alpha_g = 0 \text{ für } C \in \mathrm{Cl}(G);$$

dabei ist $C^{p^{-n}} := \{x \in G : x^{p^n} \in C\}$ *für* $C \in \mathrm{Cl}(G)$.

Beweis. Analog zu 21.8. □

21.10. Satz. *Seien* $p > 0$ *und* G *eine endliche Gruppe. Dann ist* $\exp_p(G) = \min\{p^n : n \in \mathbb{N}_0,\ x^{p^n} \in KFG$ *für* $x \in JFG\}$.

Beweis. Seien $\exp_p(G) = p^e$, $x \in JFG$ mit $x = \sum_{g \in G} \xi_g g$ mit $\xi_g \in F$ für $g \in G$. Nach 21.8 ist $\sum_{g \in S} \xi_g = 0$ für $S \in \mathrm{Sec}_{p'}(G)$. Für $C \in \mathrm{Cl}(G)$ ist $C^{p^{-e}}$ nach 21.7 entweder leer oder eine p'-Sektion. Daher ist auch $\sum_{g \in C^{p^{-e}}} \xi_g = 0$ für $C \in \mathrm{Cl}(G)$. Folglich ist $x \in T_e FG$ nach 21.9, d.h. $x^{p^e} \in KFG$.
Sei nun $n \in \mathbb{N}_0$ mit $p^n < \exp_p(G)$, und sei $g \in G_p$ mit $g^{p^n} \neq 1$. Dann ist $(g-1)^{p^e} = g^{p^e} - 1^{p^e} = 1 - 1 = 0 \in KFG$, also $g - 1 \in JFG + KFG$, etwa $g - 1 = x + y$ mit $x \in JFG$, $y \in KFG$. Folglich ist

$$x^{p^n} \equiv x^{p^n} + y^{p^n} = (x+y)^{p^n} = (g-1)^{p^n} = g^{p^n} - 1 \neq 0 \pmod{KFG}.$$

□

Beispiel. Hat G eine zyklische p-Sylowgruppe der Ordnung p^n, so existiert ein Element $x \in JFG$ mit $x^{p^{n-1}} \notin KFG$. Daher ist $x^{p^{n-1}} \neq 0$ und $(JFG)^{p^{n-1}} \neq 0$. Auf diese Weise erhält man Aussagen darüber, wie nilpotent JFG ist.

KAPITEL 22

Idempotente

Sei F ein algebraisch abgeschlossener Körper.

22.1. Satz. *Seien A eine endlich-dimensionale F-Algebra, I ein nilpotentes Ideal in A und $f^2 = f \in A/I$. Dann existiert ein Idempotent $e \in A$ mit $f = e + I$.*

Bemerkung. Man sagt, daß man das Idempotent f in A/I zu dem Idempotent e in A *heben* oder *liften* kann.

Beweis. Wir schreiben $f = a + I$ mit $a \in A$. Wegen $f^2 = f$ ist $a^2 - a \in I$. Wir setzen $b := 3a^2 - 2a^3$. Dann ist

$$b + I = 3a^2 - 2a^3 + I = 3f^2 - 2f^3 = f$$

und

$$\begin{aligned} b^2 - b + I &= (3a^2 - 2a^3)^2 - (3a^2 - 2a^3) + I^2 \\ &= 9a^4 - 12a^5 + 4a^6 - 3a^2 + 2a^3 + I^2 \\ &= 4(a^2 - a)^3 - 3(a^2 - a)^2 + I^2 \;=\; 0. \end{aligned}$$

Daher ist $g := b + I^2$ ein Idempotent in A/I^2. Da I nilpotent ist, ist $I^2 < I$ (oder $I = 0$). Schließt man durch Induktion nach $\dim I$, so existiert also ein Idempotent e in A mit $e + I^2 = g = b + I^2$, also $e + I = b + I = f$. □

22.2. Definition. Eine endlich-dimensionale F-Algebra $A \neq 0$ heißt *lokal*, wenn gilt: $a, b \in A \setminus A^\times \implies a + b \in A \setminus A^\times$.

Bemerkung. In der Algebra haben wir gesehen, daß für jede lokale endlich-dimensionale F-Algebra A gilt: $M := A \setminus A^\times$ ist ein maximales Ideal, und A/M ist ein Schiefkörper, in unserer Situation also $A/M \cong F$. Insbesondere ist $0 = J(A/M) = JA + M/M$, d.h. $JA \subseteq M$. Der Beweis des folgenden Satzes wird zeigen: $JA = M$.

Satz. *Für eine endlich-dimensionale F-Algebra A sind äquivalent:*

(1) *A ist lokal.*
(2) *0 und 1 sind die einzigen Idempotente in A.*
(3) *0 und 1 sind die einzigen Idempotente in A/JA.*
(4) *$A/JA \cong F$.*

Beweis.

(1)⇒(2): Sei A lokal und $e = e^2 \in A$. Wegen $e + (1-e) = 1 \in A^\times$ ist $e \in A^\times$ oder $1 - e \in A^\times$. Wegen $e(1-e) = e - e^2 = 0$ ist also $e = 0$ oder $1 - e = 0$.

(2)⇒(3): Sei (2) erfüllt und $f^2 = f \in A/JA$. Nach 22.1 existiert ein Idempotent e in A mit $e + JA = f$. Wegen (2) ist $e \in \{0, 1\}$, also $f \in \{0, 1\}$.

(3)⇒(4): Sei (3) erfüllt, $A/JA \cong \prod_{i=1}^{d} \mathrm{Mat}(d_i, F) =: B$ mit $n \in \mathbb{N}_0$, $d_1, \ldots, d_n \in \mathbb{N}$, und sei $\{e_{ij} : i, j = 1, \ldots, d_1\}$ die Standardbasis von $\mathrm{Mat}(d_1, F)$. Dann ist $(e_{11}, 0, \ldots, 0)$ ein von 0 verschiedenes Idempotent in B, also $(e_{11}, 0, \ldots, 0) = 1$. Folglich ist $n = 1$ und $d_1 = 1$, also $A/JA \cong F$.

(4)⇒(1): Sei $A/JA \cong F$. Für $A \setminus JA$ ist dann $a + JA \neq 0$, also $1 = (a + JA)(b + JA) = ab + JA$ für ein $b \in A$, d.h. $ab = 1 - x$ für ein $x \in JA$. Sei $n \in \mathbb{N}$ mit $(JA)^n = 0$. Dann ist

$$(1 - x)(1 + x + x^2 + \ldots + x^{n-1}) = 1 - x^n = 1,$$

also $ac = 1$ für ein $c \in A$. Analog ist $da = 1$ für ein $d \in A$, also $a \in A^\times$. Dies zeigt: $A \setminus A^\times \subseteq JA$. Andererseits ist $JA \subseteq A \setminus A^\times$, also $JA = A \setminus A^\times$. Folglich ist A lokal.

□

22.3. Bemerkung. Aus 22.2 folgt, daß jede von 0 verschiedene Unteralgebra und jede von 0 verschiedene Restklassenalgebra einer endlich-dimensionalen lokalen F-Algebra A wieder lokal ist (verwende (2) bzw. (4)).

Definition. Idempotente e, f einer endlich-dimensionalen F-Algebra A mit $ef = 0 = fe$ nennt man *orthogonal*. Ein Idempotent $g \neq 0$ in A nennt man *primitiv* (in A), falls keine orthogonalen Idempotente e, f in A existieren mit $g = e + f$ und $e \neq 0 \neq f$.

Satz. *Ein Idempotent e in einer endlich-dimensionalen F-Algebra A ist genau dann primitiv in A, wenn eAe lokal ist.*

Beweis.

$\Rightarrow$: Sei e primitiv in A, also $e \neq 0$ und $eAe \neq 0$. Ist f ein Idempotent in eAe, so ist $e = f + (e - f)$ mit $f(e - f) = fe - f^2 = f - f = 0$, $(e - f)f = 0$ und $(e - f)^2 = e(e - f) - f(e - f) = e - f$. Da e primitiv ist, folgt $f = 0$ oder $e - f = 0$, d.h. $f = 0$ oder $f = e = 1_{eAe}$. Folglich ist eAe lokal.

$\Leftarrow$: Sei eAe lokal, also $e \neq 0$. Ist $e = f + g$ mit von 0 verschiedenen orthogonalen Idempotenten f, g in A, so ist $fe = f(f + g) = f^2 + fg = f$ und analog $ef = f$, also $f = efe \in eAe$. Da eAe lokal ist, folgt $f = 0$ oder $f = 1_{eAe} = e$, d.h. $f = 0$ oder $g = 0$. Folglich ist e primitiv in A.

□

22.4. Satz. *Sei A eine endlich-dimensionale F-Algebra, I ein Ideal in A und e ein primitives Idempotent in A mit $e \notin I$. Dann ist $e + I$ primitiv in A/I.*

Beweis. Nach 22.3 ist $(e + I)(A/I)(e + I) = eAe + I/I \cong eAe/eAe \cap I$ lokal. □

22.5. Bemerkung. Sei A eine endlich-dimensionale F-Algebra, sei $A = P_1 \oplus \ldots \oplus P_r$ mit A-Linksmoduln $P_1, \ldots, P_r$, und sei $1_A = e_1 + \ldots + e_r$ mit $e_1 \in P_1, \ldots, e_r \in P_r$. Für $i = 1, \ldots, r$ und $a_i \in P_i$ ist $a_i = a_i 1_A = a_i e_1 + \ldots + a_i e_r$ mit $a_i e_1 \in P_1, \ldots, a_i e_r \in P_r$. Daher ist $a_i e_j = 0$ für $j \neq i$ und $a_i e_i = a_i$. Insbesondere ist $P_i = Ae_i$, $e_i^2 = e_i$ und $e_i e_j = 0$ für $j \neq i$. Daher sind $e_1, \ldots, e_r$ paarweise orthogonale Idempotente mit $P_i = Ae_i$ für $i = 1, \ldots, r$.
Sind umgekehrt $f_1, \ldots, f_s$ paarweise orthogonale Idempotente in A mit $f_1 + \ldots + f_s = 1_A$, so ist $a = a1_A = af_1 + \ldots + af_s$ für $a \in A$, also $A = Af_1 + \ldots Af_s$. Wegen $a = af_1 = 0$ für $a \in Af_1 \cap (Af_2 + \ldots Af_s)$ ist $Af_1 \cap (Af_2 + \ldots + Af_s) = 0$, also $A = Af_1 \oplus \ldots \oplus Af_s$.
Dies zeigt, daß sich Zerlegungen von 1_A in paarweise orthogonale Idempotente und (direkte) Zerlegungen von A in Untermoduln entsprechen. Es ist leicht zu sehen, daß sich dabei Zerlegungen von A in unzerlegbare Untermoduln und Zerlegungen von 1_A in primitive paarweise orthogonale Idempotente entsprechen. Insbesondere besitzt 1_A eine Zerlegung in primitive paarweise orthogonale Idempotente.

Satz (Rosenbergs Lemma)**.** *Seien A eine endlich-dimensionale F-Algebra, $I_1, \ldots, I_n$ Ideale von A und e ein primitives Idempotent in A mit $e \in I_1 + \ldots + I_n$. Dann ist $e \in I_j$ für ein $j \in \{1, \ldots, n\}$.*

Beweis. Offenbar sind $eI_1e, \ldots, eI_ne$ Ideale in der lokale F-Algebra eAe mit $e = e^3 \in eI_1e + \ldots + eI_ne$. Insbesondere ist $eI_je \not\subseteq J(eAe)$ für ein $j \in \{1, \ldots, n\}$, sonst wäre $e \in J(eAe)$. Da eAe lokal ist, folgt $eI_je = eAe$, also $e \in eAe = eI_je \subseteq I_j$. □

22.6. Definition. Sei A eine endlich-dimensionale F-Algebra. Die in ZA primitiven Idempotente von A bezeichnet man als *Blockidempotente* von A.

Bemerkung. Nach 22.5 kann man $1_A = e_1 + \ldots + e_r$ mit paarweise orthogonalen Blockidempotenten $e_1, \ldots, e_r$ in A schreiben. Dann ist $A = Ae_1 \oplus \ldots \oplus Ae_r$, und für $i = 1, \ldots, r$ ist $Ae_i = e_iA$ ein Ideal in A. Analog ist $ZA = ZAe_1 \oplus \ldots \oplus ZAe_r$ mit Idealen $ZAe_1, \ldots, ZAe_r$ in ZA. Nach Rosenbergs Lemma existiert zu jedem Blockidempotent e in A ein $i \in \{1, \ldots, r\}$ mit $e \in ZAe_i$. Da $ZAe_i = e_iZAe_i$ eine lokale F-Algebra ist, folgt $e = e_i$. Daher sind $e_1, \ldots, e_r$ die einzigen Blockidempotente in A; insbesondere

sind je zwei verschiedene Blockidempotente orthogonal. Man bezeichnet die Ideale $B_i := Ae_i = e_iA$ als *Blöcke* von A. Jeder Block B_i ist wegen $B_i = e_iAe_i$ auch eine F-Unteralgebra von A mit Einselement e_i. Block und Blockidempotent bestimmen sich also gegenseitig.
Wegen $A = B_1 \oplus \ldots \oplus B_r$ und $B_iB_j = Ae_ie_jA = 0$ für $i \neq j$ ist die Abbildung $B_1 \times \ldots \times B_r \to A$, $(b_1, \ldots, b_r) \mapsto b_1 + \ldots + b_r$ ein Isomorphismus von Algebren. Die Struktur einer endlich-dimensionalen F-Algebra ist also durch die Struktur ihrer Blöcke eindeutig bestimmt. Im weiteren Verlauf der Vorlesung werden wir uns häufig mit Blöcken von Gruppenalgebren beschäftigen.
Wegen $Z(B_1 \times \ldots \times B_r) = ZB_1 \times \ldots \times ZB_r$ ist $ZA = ZB_1 \oplus \ldots \oplus ZB_r$, also $ZB_i = ZAe_i$ für $i = 1, \ldots, r$. Analog ist $JA = JB_1 \oplus \ldots \oplus JB_r$ und $JB_i = JAe_i$ für $i = 1, \ldots, r$, und in gleicher Weise ist $JZA = JZB_1 \oplus \ldots \oplus JZB_r$ und $JZB_i = JZAe_i$ für $i = 1, \ldots, r$.

22.7. Definition. Für jede endlich-dimensionale F-Algebra A setzen wir $E(A) := F\{e : e^2 = e \in A\} + KA$.

Bemerkung. Ist A kommutativ, so ist $E(A) = F\{e : e^2 = e \in A\}$.

Satz. *Sei A eine endlich-dimensionale F-Algebra und $1_A = e_1 + \ldots + e_r$ mit Blockidempotenten $e_1, \ldots, e_r$ in A. Dann ist $E(ZA) = Fe_1 \oplus \ldots \oplus Fe_r$ eine Unteralgebra von ZA mit $ZA = E(ZA) \oplus JZA$.*

Beweis. Für ein beliebiges Idempotent e in ZA ist $e = e1_A = ee_1 + \ldots + ee_r$. Für $i = 1, \ldots, r$ ist dabei ee_i ein Idempotent in der lokalen F-Algebra ZAe_i, also $ee_i \in \{0, e_i\}$. Folglich ist $e \in Fe_1 + \ldots + Fe_r$. Da $e_1, \ldots, e_r$ paarweise orthogonal sind, ist $E(ZA) = Fe_1 + \ldots + Fe_r = Fe_1 \oplus \ldots \oplus Fe_r$. Für $i = 1, \ldots, r$ ist $ZAe_i = Fe_i \oplus J(ZAe_i)$, also $ZA = ZAe_1 + \ldots + ZAe_r = Fe_1 + J(ZAe_1) \oplus \ldots \oplus Fe_r + J(ZAe_r) = E(ZA) \oplus JZA$. Offenbar ist $E(ZA)$ eine Unteralgebra von ZA. ☐

22.8. Satz. *Sei A eine endlich-dimensionale F-Algebra, I ein Ideal in A mit $I \subseteq (JA)^2$ und e ein Blockidempotent in A. Dann ist $e + I$ ein Blockidempotent in A/I.*

Bemerkung. Dies folgt nicht unmittelbar aus 22.4; denn i.a. ist $ZA + I/I < Z(A/I)$.

Beweis. Sei $e + I = f_1 + f_2$ mit orthogonalen Idempotenten f_1, f_2 in $Z(A/I)$. Nach 22.1 existiert ein Idempotent e_1 in A mit $f_1 = e_1 + I$. Da wir e_1 notfalls durch ee_1 ersetzen können, können wir $ee_1 = e_1$ annehmen. Wegen

$$\begin{aligned} e_1A(1-e_1) + I/I &= (e_1 + I)(A/I)(1 - e_1 + I) = f_1(A/I)(1 - f_1) \\ &= f_1(1 - f_1)(A/I) = 0 \end{aligned}$$

ist $e_1A(1 - e_1) \subseteq I$ und analog $(1 - e_1)Ae_1 \subseteq I$. Daher ist

$$\begin{aligned} A &= 1_AA1_A = (e_1 + 1 - e_1)A(e_1 + 1 - e_1) \\ &= e_1Ae_1 + e_1A(1 - e_1) + (1 - e_1)Ae_1 + (1 - e_1)A(1 - e_1) \\ &= B + I, \end{aligned}$$

wobei $B := e_1Ae_1 + (1 - e_1)A(1 - e_1)$ eine Unteralgebra von A ist. Nach 20.8 ist $A = B$. Für $x \in e_1Ae_1$ ist aber $e_1x = x = xe_1$, und für $x \in (1 - e_1)A(1 - e_1)$ ist $e_1x = 0 = xe_1$. Daher ist $e_1 \in ZA$. Wegen $e_1e = e_1$ ist sogar $e_1 \in ZAe$. Da ZAe lokal ist, folgt: $e_1 = 0$ oder $e_1 = e$. Daher ist $f_1 = 0$ oder $f_1 = e + I$, d.h. $f_1 = 0$ oder $f_2 = 0$. ☐

22.9. Satz. *Seien A eine endlich-dimensionale F-Algebra, I ein Ideal in A mit $I \subseteq (JZA)A$ und e ein Blockidempotent in A. Dann ist $e + I$ ein Blockidempotent in A/I.*

Bemerkung. Hierbei bezeichnet $(JZA)A = A(JZA)$ das von JZA erzeugte Ideal in A. Offensichtlich ist $(JZA)A \subseteq JA$.

Beweis. Sei $e + I = f_1 + f_2$ mit orthogonalen Idempotenten $f_1, f_2 \in Z(A/I)$. Nach 22.1 existiert ein Idempotent $e_1 \in A$ mit $f_1 = e_1 + I$, o.B.d.A. $ee_1 = e_1$. Wie im Beweis von 22.8 ist dann $e_1A(1 - e_1) \subseteq I \subseteq (JZA)A$, also

$$\begin{aligned} e_1A(1 - e_1) &= e(JZA)A(1 - e_1) = (JZA)e_1A(1 - e_1) \\ &= (JZA)^2e_1A(1 - e_1) = \ldots = 0. \end{aligned}$$

Analog ist $(1-e_1)Ae_1 = 0$. Daher ist

$$\begin{aligned} A &= 1_A A 1_A \; = \; e_1Ae_1 + e_1A(1-e_1) + (1-e_1)Ae_1 + (1-e_1)A(1-e_1) \\ &= e_1Ae_1 + (1-e_1)A(1-e_1), \end{aligned}$$

und man kann wie im Beweis von 22.8 argumentieren. □

KAPITEL 23

Frobeniusalgebren

Sei F ein algebraisch abgeschlossener Körper und $p := \mathrm{char}(F)$.

23.1. Definition. Eine Bilinearform β auf einer endlich-dimensionalen F-Algebra A mit $\beta(ab, c) = \beta(a, bc)$ für $a, b, c \in A$ nennt man *assoziativ.*

Bemerkung. In diesem Fall ist $\beta(a, b) = \beta(1a, b) = \beta(1, ab)$ für $a, b \in A$. Die Abbildung $\lambda : A \to F,\ a \mapsto \beta(1, a)$ ist also eine Linearform auf A mit $\beta(a, b) = \lambda(ab)$ für $a, b \in A$. Umgekehrt ist für jede Linearform $\lambda : A \to F$ die Abbildung $\beta : A \times A \to F,\ (a, b) \mapsto \lambda(ab)$ eine assoziative Bilinearform auf A. Auf diese Weise entsprechen sich assoziative Bilinearformen und Linearformen auf A. Dabei gilt:

$$\begin{aligned}
\beta \text{ nicht ausgeartet} \quad &\iff \quad (\forall a \in A : \beta(a, A) = 0 \ \Rightarrow\ a = 0)\\
&\iff \quad (\forall a \in A : \lambda(aA) = 0 \ \Rightarrow\ a = 0)\\
&\iff \quad \mathrm{Ker}(\lambda) \text{ enthält kein Rechtsideal von } A \text{ außer } 0.
\end{aligned}$$

Analog gilt: β nicht ausgeartet $\iff$ $\mathrm{Ker}(\lambda)$ enthält kein Linksideal von A außer 0.

23.2. Definition. Eine endliche-dimensionale F-Algebra A nennt man eine *Frobeniusalgebra*, falls auf A eine nichtausgeartete assoziative Bilinearform β existiert. Manchmal nennt man dann auch das Paar (A, β) eine Frobeniusalgebra.

Bemerkung. Nach 23.1 ist eine endlich-dimensionale F-Algebra A genau dann eine Frobeniusalgebra, wenn auf A eine Bilnearform λ existiert, deren Kern kein Rechtsideal (Linksideal) von A außer 0 enthält. Manchmal nennt man dann auch das Paar (A, λ) eine Frobeniusalgebra.
Ist (A, β) eine Frobeniusalgebra über F, so ist die Abbildung $\Phi : A \to \mathrm{Hom}_F(A, F)$, die jedem $a \in A$ die Abbildung $\Phi(a) : A \to F,\ b \mapsto \beta(a, b)$ zuordnet, eine lineare Bijektion. Analog ist die Abbildung $\Psi : A \to \mathrm{Hom}_F(A, F)$, die jedem $a \in A$ die Abbildung $\Psi(a) : A \to F,\ b \mapsto \beta(b, a)$ zuordnet, eine lineare Bijektion. Folglich ist $\Lambda := \Psi^{-1} \circ \Phi : A \to A$ eine lineare Bijektion mit $\Psi(\Lambda(a)) = \Phi(a)$ für $a \in A$, d.h. $\beta(b, \Lambda(a)) = \beta(a, b)$ für $a, b \in A$. Wegen

$$\begin{aligned}
\beta(b, \Lambda(aa') - \Lambda(a)\Lambda(a')) &= \beta(b, \Lambda(aa')) - \beta(b, \Lambda(a)\Lambda(a'))\\
&= \beta(aa', b) - \beta(b\Lambda(a), \Lambda(a'))\\
&= \beta(a, a'b) - \beta(a', b\Lambda(a))\\
&= \beta(a'b, \Lambda(a)) - \beta(a'b, \Lambda(a))\\
&= 0
\end{aligned}$$

für $b \in A$ ist $\Lambda(aa') = \Lambda(a)\Lambda(a')$ für $a, a' \in A$, d.h. Λ ist ein Automorphismus der F-Algebra A. Man nennt Λ den *Nakayama-Automorphismus* von (A, β).

Beispiel.

(i) Für $n \in \mathbb{N}$ wird $A := \mathrm{Mat}(n, F)$ mit der Spurabbildung $\lambda : A \to F$ zu einer Frobeniusalgebra. Ist nämlich $x \in A$ mit $\lambda(xA) = 0$, so ist $0 = \lambda(xab) = \lambda(axb)$ für $a, b \in A$, also $\lambda(AxA) = 0$. Da A einfach und $\lambda(A) \neq 0$ ist, folgt $AxA = 0$, d.h. $x = 0$.

(ii) Für jede Gruppe wird FG zu einer Frobeniusalgebra mit der Linearform λ, die jedem Element der Form $a = \sum_{g \in G} \alpha_g g \in FG$ mit $\alpha_g \in F$ für $g \in G$ das Element $\lambda(a) := \alpha_1$ zuordnet. Ist nämlich $\lambda(aA) = 0$, so ist $0 = \lambda(ah^{-1}) = \lambda(\sum_{g \in G} \alpha_g gh^{-1}) = \alpha_h$ für $h \in G$, d.h. $a = 0$.

(iii) Sind (A,β) und (B,γ) Frobeniusalgebren, so ist $A\times B$ eine Frobeniusalgebra bzgl. der Bilinearform $\delta:(A\times B)\times(A\times B)\to F,\ ((a,b),(a',b'))\mapsto\beta(a,a')+\gamma(b,b')$; ist nämlich X (bzw. Y) die Matrix von β (bzw. γ) bzgl. einer Basis von A (bzw. B), so ist $\left(\begin{smallmatrix}X&0\\0&Y\end{smallmatrix}\right)$ die Matrix von δ bzgl. der Basis von $A\times B$.

(iv) Aus (iii) folgt, daß jede halbeinfache F-Algebra eine Frobeniusalgebra ist.

23.3. Satz. *Seien (A,λ) und $(A/I,\mu)$ Frobeniusalgebren über F für ein Ideal I von A und Linearformen $\lambda:A\to F$, $\mu:A/I\to F$, Dann existiert ein Element $x\in A$ mit $\mu(a+I)=\lambda(ax)$ für $a\in A$ und $I=\{a\in A:ax=0\}$.*

Beweis. Die Abbildung $A\to F,\ a\mapsto\mu(a+I)$ ist linear. Nach 23.2 existiert ein Element $x\in A$ mit $\mu(a+I)=\lambda(ax)$ für $a\in A$. Wegen $0=\mu(0)=\mu(a+I)=\lambda(ax)$ für $a\in I$ ist $\lambda(Ix)=0$. Da $\mathrm{Ker}(\lambda)$ keine Linksideale außer 0 enthält, folgt $Ix=0$. Ist umgekehrt $a\in A$ mit $ax=0$, so ist $\mu(ba+I)=\lambda(bax)=0$ für $b\in A$, also $\mu((A/I)(a+I))=0$. Da $\mathrm{Ker}(\mu)$ keine Linksideale außer 0 enthält, folgt $a+I=0$, d.h. $a\in I$. □

Bemerkung. Analog existiert natürlich ein $y\in A$ mit $\mu(a+I)=\lambda(ya)$ für $a\in A$ und $I=\{a\in A:ya=0\}$. Offenbar ist $x=\Lambda(y)$, wobei Λ der entprechende Nakayama-Automorphismus ist.

Beispiel. Im Fall $I=0$ kann man A/I mit A identifizieren. Dann hat man Linearformen λ,μ auf A, die beide A zu einer Frobeniusalgebra machen. Nach dem Satz existiert ein Element $x\in A$ mit $\mu(a)=\lambda(ax)$ für $a\in A$. Analog existiert ein $x'\in A$ mit $\lambda(a)=\mu(ax')$ für $a\in A$. Dann ist

$$\lambda(a(x'x-1))=\lambda(ax'x)-\lambda(a)=\mu(ax')-\mu(ax')=0$$

für $a\in A$, also $x'x-1=0$, d.h. $x'x=1$. Analog ist $xx'=1$, d.h. $x\in A^\times$.

23.4. Bemerkung. Sei (A,β) eine Frobeniusalgebra über F, wobei $\beta:A\times A\to F$ bilinear ist. Für jede Teilmenge X von A sind dann $X^\perp:=\{a\in A:\beta(X,a)=0\}$ und ${}^\perp X:=\{a\in A:\beta(a,X)=0\}$ Untervektorräume von A, und für Untervektorräume X,Y von A gilt:

(i) $\dim X^\perp=\dim A-\dim X=\dim{}^\perp X$.

(ii) ${}^\perp(X^\perp)=X=({}^\perp X)^\perp$.

(iii) $(X\cap Y)^\perp=X^\perp+Y^\perp,\ {}^\perp(X\cap Y)={}^\perp X+{}^\perp Y$,
$(X+Y)^\perp=X^\perp\cap Y^\perp,\ {}^\perp(X+Y)={}^\perp X\cap{}^\perp Y$.

Definition. Seien A eine F-Algebra und $X\subseteq A$. Dann bezeichnet man $\mathrm{RAn}(X):=\{a\in A:Xa=0\}$ als *Rechtsannullator* und $\mathrm{LAn}(X):=\{a\in A:aX=0\}$ als *Linksannullator* von X in A.

23.5. Bemerkung. Sei (A,β) eine Frobeniusalgebra über F, wobei $\beta:A\times A\to F$ bilinear ist. Für $X\subseteq A$ ist $\mathrm{RAn}(X)$ ein Rechtsideal in A, und für $a\in\mathrm{RAn}(X)$ ist $\beta(X,a)=\beta(1,Xa)=\beta(1,0)=0$. Daher ist $\mathrm{RAn}(X)\subseteq X^\perp$. Ist R ein beliebiges Rechtsideal in A mit $R\subseteq X^\perp$, so ist $\beta(Xa,A)=\beta(X,aA)\subseteq\beta(X,X^\perp)=0$ für $a\in R$, also $Xa=0$ für $a\in R$. Daher ist $\mathrm{RAn}(X)$ das größte Rechtsideal in A, das in $X^\perp$ enthalten ist. Analog ist $\mathrm{LAn}(X)$ das größte Linksideal in A, das in ${}^\perp X$ enthalten ist.
Ist X selbst ein Linksideal in A, so gilt für $a\in A$:

$$a\in X^\perp\iff\beta(X,a)=0\iff\beta(AX,a)=0\iff\beta(A,Xa)=0\iff Xa=0.$$

Für jedes Linksideal X in A ist also $X^\perp=\mathrm{RAn}(X)$ ein Rechtsideal in A, und analog ist ${}^\perp Y=\mathrm{LAn}(Y)$ ein Linksideal in A für jedes Rechtsideal Y in A.

Satz. *Für jede Frobeniusalgebra (A,β) über F und jedes Element $x\in A$ ist $\dim Ax=\dim xA$. Ist xA ein Ideal in A, so ist $xA=Ax$.*

Beweis. Die Abbildung $A\to Ax,\ a\mapsto ax$ ist linear mit Kern $\mathrm{LAn}(\{x\})=\mathrm{LAn}(xA)={}^\perp(xA)$. Folglich ist $\dim Ax=\dim A-\dim{}^\perp(xA)=\dim xA$. □

Beispiel. Für jedes Idempotent e in A und beliebiges $a\in A$ gilt:

$$a\in(Ae)^\perp\iff Aea=0\iff ea=0\iff(1-e)a=a\iff a\in(1-e)A.$$

Daher ist $(Ae)^\perp=(1-e)A$.

23.6. Satz. *Für $k \in \mathbb{N}$ und jede Frobeniusalgebra (A, β) ist* $\mathrm{RAn}((JA)^k) = \mathrm{LAn}((JA)^k)$.

Beweis. Wir schreiben $J := JA = \cap_{i=1}^n M_i$ mit maximalen Linksidealen $M_1, \ldots, M_n$ von A. Dann ist $J^\perp = (\cap_{i=1}^n M_i)^\perp = \sum_{i=1}^n M_i^\perp$ mit minimalen Rechtsidealen $M_1^\perp, \ldots, M_n^\perp$ von A. Insbesondere ist $J^\perp$ ein halbeinfacher A-Rechtsmodul. Folglich ist $J^\perp \cdot J = 0$, also $\mathrm{RAn}(J) = J^\perp \subseteq \mathrm{LAn}(J)$, und analog ist $\mathrm{LAn}(J) \subseteq \mathrm{RAn}(J)$.
Sei nun $k \in \mathbb{N}$ mit $\mathrm{LAn}(J^k) = \mathrm{RAn}(J^k)$. Wegen $\mathrm{LAn}(J^{k+1})J^{k+1} = 0$ ist $\mathrm{LAn}(J^{k+1})J \subseteq \mathrm{LAn}(J^k) = \mathrm{RAn}(J^k)$, also $J^k\,\mathrm{LAn}(J^{k+1})J = 0$. Daher ist $J^k\,\mathrm{LAn}(J^{k+1}) \subseteq \mathrm{LAn}(J) = \mathrm{RAn}(J)$, also $0 = J \cdot J^k\,\mathrm{LAn}(J^{k+1})$. Folglich ist $\mathrm{LAn}(J^{k+1}) \subseteq \mathrm{RAn}(J^{k+1})$, und analog ist $\mathrm{RAn}(J^{k+1}) \subseteq \mathrm{LAn}(J^{k+1})$. □

23.7. Bemerkung. Sei (A, β) eine Frobeniusalgebra über F, wobei $\beta : A \times A \to F$ bilinear ist. Zu jeder F-Basis $a_1, \ldots, a_n$ von A existiert bekanntlich eine F-Basis $b_1, \ldots, b_n$ von A mit $\beta(a_i, b_j) = \delta_{ij}$ für $i, j = 1, \ldots, n$. (Umgekehrt existiert zu jeder F-Basis $b_1, \ldots, b_n$ von A genau eine F-Basis $a_1, \ldots, a_n$ von A mit dieser Eigenschaft.) Man nennt $\big(\{a_1, \ldots, a_n, \}, \{b_1, \ldots, b_n\}\big)$ ein Paar von *Dualbasen* von (A, β). Für $x \in A$ ist bekanntlich

$$x = \sum_{i=1}^n \beta(x, b_i)a_i = \sum_{j=1}^n \beta(a_j, x)b_j.$$

Wir setzen $\Gamma(x) := \sum_{i=1}^n b_i x a_i$. Ist $\big(\{a_1', \ldots, a_n'\}, \{b_1', \ldots, b_n'\}\big)$ ein weiteres Paar von Dualbasen von (A, β), so ist

$$\sum_{i=1}^n b_i' x a_i' = \sum_{i,j=1}^n \beta(a_j, b_i')b_j x a_i' = \sum_{i,j=1}^n b_j x \beta(a_j, b_i')a_i' = \sum_{j=1}^n b_j x a_j.$$

Daher hängt Γ nicht von der Wahl des Paares von Dualbasen ab (wohl aber von β). Ferner gilt für $x, y \in A$:

$$\Gamma(x)y = \sum_{i,j=1}^n b_i x \beta(a_i y, b_j)a_j = \sum_{i,j=1}^n \beta(a_i, y b_j) b_i x a_j = \sum_{i,j=1}^n y b_j x a_j = y\Gamma(x).$$

Wir erhalten also eine lineare Abbildung $\Gamma : A \to ZA$, die *Gaschütz-Abbildung* von (A, β). Wegen $\Gamma(zx) = z\Gamma(x)$ für $z \in ZA$, $x \in A$ ist $\Gamma(A)$ ein Ideal in ZA. Man nennt $\Gamma(A)$ das *Higman-Ideal* von ZA.
Ist auch $\beta' : A \times A \to F$ bilinear und (A, β') eine Frobeniusalgebra über F, so existiert ein Element $y \in A^\times$ mit $\beta'(1, a) = \beta(1, ay)$ für $a \in A$, d.h. $\beta'(a, b) = \beta'(1, ab) = \beta(1, aby) = \beta(a, by)$ für $a, b \in A$. Daher ist $\big(\{a_1, \ldots, a_n\}, \{b_1 y^{-1}, \ldots, b_n y^{-1}\}\big)$ ein Paar von Dualbasen von (A, β'). Bezeichnet man die Gaschütz-Abbildung von (A, β') mit Γ', so ist also

$$\Gamma'(x) = \sum_{i=1}^n b_i y^{-1} x a_i = \Gamma(y^{-1}x)$$

für $a \in A$; insbesondere ist $\Gamma'(A) = \Gamma(A)$. Folglich hängt das Higman-Ideal nur von A, nicht aber von β ab.
Ist $k \in \mathbb{N}_0$ und $a_1, \ldots, a_l$ eine F-Basis von $(JA)^k$, so liegen $b_{l+1}, \ldots, b_n$ wegen $\beta(a_i, b_j) = 0$ für $i = 1, \ldots, l$, $j = l{+}1, \ldots, n$ in $((JA)^k)^\perp$. Wegen $\dim((JA)^k)^\perp = \dim A - \dim(JA)^k = n - l$ bilden $b_{l+1}, \ldots, b_n$ sogar eine F-Basis von $((JA)^k)^\perp$. Wir betrachten die Reihe von Untervektorräumen $A \supseteq JA \supseteq (JA)^2 \supseteq \ldots \supseteq (JA)^t = 0$ und wählen die Basis $a_1, \ldots, a_n$ von A entsprechend. Für $x \in JA$, $i = 1, \ldots, n$ und $k \in \mathbb{N}$ mit $a_i \in (JA)^k$ ist $x a_i \in (JA)^{k+1} = F\{a_1, \ldots, a_j\}$ für ein $j < i$, also $b_i \in ((JA)^{k+1})^\perp$ und damit $b_i x a_i = 0$. Folglich ist $\Gamma(JA) = 0$ und analog $\Gamma(A)JA = 0$.
Offenbar sind die Blöcke $B_1, \ldots, B_r$ von A Frobeniusalgebren über F bzgl. der entsprechenden Einschränkungen $\beta_1, \ldots, \beta_r$ von β. Wie man leicht nachrechnet, ist auch $\Gamma(A) = \Gamma(B_1) \oplus \ldots \oplus \Gamma(B_r)$. Sei $i \in \{1, \ldots, r\}$ und $B := B_i$. Ist $JB \neq 0$, so ist $1_B \notin \Gamma(B)$ wegen $\Gamma(B)JB = 0$. Da ZB lokal ist, folgt $\Gamma(B) \subseteq JZB$, und damit $\Gamma(B)^2 \subseteq \Gamma(B)JZB \subseteq \Gamma(B)JB = 0$. Ist $JB = 0$, so ist $B \cong \mathrm{Mat}(d, F)$ für ein $d \in \mathbb{N}$. Dual zu der Standardbasis $\{e_{ij} : i, j = 1, \ldots, n\}$ von $\mathrm{Mat}(d, F)$ bzgl. der durch die Spur gegebenen

Bilinearform ist die Basis $\{e_{ji} : i,j = 1,\dots,n\}$. Für die Gaschützabbildung Γ_d von $\mathrm{Mat}(d,F)$ gilt also:

$$\Gamma_d(e_{11}) = \sum_{i,j=1}^{n} e_{ji}e_{11}e_{ij} = \sum_{j=1}^{n} e_{jj} = 1_n.$$

Daher ist $\Gamma(B) = ZB$ und $\Gamma(B)^2 = ZB$. Damit haben wir insgesamt:

$$\Gamma(A)^2 = \bigoplus_{\substack{i=1\\ JB_i=0}}^{r} ZB_i;$$

Insbesondere ist $\dim \Gamma(A)^2$ die Anzahl der Blöcke von A, die einfache Algebren sind.

Beispiel. Seien G eine endliche Gruppe und λ die früher definierte Linearform, die FG zu einer Frobeniusalgebra macht. Dual zu der Basis $\{g : g \in G\}$ von (FG,λ) ist die Basis $\{g^{-1} : g \in G\}$. Für $x \in FG$ ist also $\Gamma(x) = \sum_{g\in G} g^{-1}xg$. Für $x \in G$ ist insbesondere $\Gamma(x) = |C_G(x)|C_x^+$, wobei C_x die Konjugationsklasse von x in G ist.
Im Fall $\mathrm{char}(F) = 0$ ist also $\Gamma(FG) = ZFG$ in Übereinstimmung mit der obigen Bemerkung, und im Fall $\mathrm{char}(F) = p > 0$ bilden die Klassensummen der Elemente $x \in G$ mit $p \nmid |C_G(x)|$ eine Basis von $\Gamma(FG)$. Wegen $\langle x\rangle \le C_G(x)$ liegt jedes solche x in G'_p.

23.8. Bemerkung. Für jede endliche Gruppe G bezeichnen wir mit $\beta_0(FG)$ die Anzahl der Blöcke von FG, die einfache Algebren sind. Nach 23.7 ist $\beta_0(FG) = \dim\Gamma(FG)^2$. Eine wichtige unbewiesene Vermutung von Alperin besagt, daß im Fall $\mathrm{char}(F) = p > 0$ für jedes Repräsentantensystem $\mathcal{Q}$ für die Konjugationsklassen von p-Untergruppen von G gilt:

$$|\operatorname{Sec}_{p'}(G)| = \sum_{Q\in\mathcal{Q}} \beta_0(F[N_G(Q)/Q]).$$

23.9. Satz. *Sind A und B Frobeniusalgebren über F, so auch $A \otimes_F B$.*

Beweis. Sind λ,μ Linearformen, so daß $(A,\lambda),(B,\mu)$ Frobeniusalgebren über F sind. Dann ist $\lambda\otimes\mu : A\otimes_F B \to F\otimes_F F \cong F$ eine Linearform. Sind $\big(\{a_1,\dots,a_m\},\{a'_1,\dots,a'_m\}\big)$ und $\big(\{b_1,\dots,b_n\},\{b'_1,\dots,b'_n\}\big)$ Paare von Dualbasen von (A,λ) bzw. (B,μ), so ist offenbar $\big(\{a_i\otimes b_j : i = 1,\dots,m,\ j = 1,\dots,n\},\{a'_i\otimes b'_j : i = 1,\dots,m,\ j = 1,\dots,n\}\big)$ ein Paar von Dualbasen bzgl. der durch $\lambda\otimes\mu$ definierten Bilinearform. $\square$

KAPITEL 24

Symmetrische Algebren

Sei F ein algebraisch abgeschlossener Körper und $p := \mathrm{char}(F)$.

24.1. Definition. Eine endlich-dimensionale F-Algebra A nennt man *symmetrisch*, falls auf A eine nichtausgeartete assoziative symmetrische Bilinearform β existiert. Manchmal nennt man dann auch das Paar (A, β) eine symmetrische F-Algebra.

Bemerkung. In diesem Fall erfüllt die Linearform $\lambda : A \to F,\ a \mapsto \beta(1, a)$ die Bedingung

$$\lambda(ab - ba) = \lambda(ab) - \lambda(ba) = \beta(1, ab) - \beta(1, ba) = \beta(a, b) - \beta(b, a) = 0$$

für $a, b \in A$, d.h. es ist $KA \subseteq \mathrm{Ker}(\lambda)$. Umgekehrt liefert jede Linearform $\lambda : A \to F$, deren Kern KA, aber kein Rechtsideal (Linksideal) außer 0 enthält, eine nichtausgeartete assoziative symmetrische Bilinearform $\beta : A \times A \to F,\ (a, b) \mapsto \lambda(ab)$, die (A, λ) zu einer symmetrischen F-Algebra macht. Manchmal nennt man auch das Paar (A, λ) eine symmetrische F-Algebra.

Satz. *Seien A eine endliche-dimensionale F-Algebra und $\lambda : A \to F$ eine Linearform, deren Kern KA, aber kein Ideal außer 0 enthält. Dann ist (A, λ) eine symmetrische F-Algebra.*

Beweis. Ist $x \in A$ mit $\lambda(xA) = 0$, so ist $\lambda(axb) = \lambda(xba) = 0$ für $a, b \in A$, also $\lambda(AxA) = 0$. □

Beispiel.

(i) Für $d \in \mathbb{N}$ ist $(\mathrm{Mat}(d, F), \mathrm{spur})$ symmetrisch wegen $\mathrm{spur}(KA) = 0$.

(ii) Für symmetrische F-Algebren $A_1, \ldots, A_n$ ist auch $A_1 \times \ldots \times A_n$ symmetrisch, wie man leicht nachrechnet. Insbesondere ist jede halbeinfache F-Algebra symmetrisch.

(iii) Für symmetrische F-Algebren A, B ist auch $A \otimes_F B$ symmetrisch, wie man leicht nachrechnet.

(iv) Ist (A, λ) eine symmetrische F-Algebra, wobei $\lambda : A \to F$ linear ist, so ist eAe für jedes Idempotent e in A symmetrisch bzgl. der Einschränkung μ von λ; ist nämlich $x \in eAe$ mit $0 = \mu(xeAe) = \lambda(exeA) = \lambda(xA)$, so ist $x = 0$.

(v) Für jede endliche Gruppe G ist FG symmetrisch bzgl. der früher definierten Linearform λ; für $g, h \in G$ ist nämlich $\lambda(gh) = \lambda(hg)$ wegen $gh = 1 \iff h(gh)h^{-1} = 1 \iff hg = 1$.

24.2. Satz. *Seien (A, λ) und $(A/I, \mu)$ symmetrische F-Algebren, wobei I ein Ideal in A ist und $\lambda : A \to F,\ \mu : A/I \to F$ linear sind. Dann existiert ein Element $z \in ZA$ mit $\mu(a + I) = \lambda(az)$ und $I = \{a \in A : az = 0\}$.*

Beweis. Nach 23.3 existiert ein $z \in A$ mit den gewünschten Eigenschaften. Wegen

$$\lambda(a(bz - zb)) = \lambda(abz) - \lambda(azb) = \mu(ab + I) - \lambda(baz) = \mu(ba + I) - \mu(ba + I) = 0$$

für $a, b \in A$ ist $bz - zb = 0$ für $b \in A$, also $z \in ZA$. □

Beispiel. Im Fall $I = 0$ kann man A/I und A identifizieren. Dann hat man Linearformen λ, μ auf A, die A zu einer symmetrischen F-Algebra machen. Nach dem obigen Satz existiert ein $z \in ZA$ mit $\mu(a) = \lambda(az)$ für $a \in A$. Wie in 23.3 ist $z \in (ZA)^\times$.

24.3. Bemerkung. Sei (A, β) eine symmetrische F-Algebra. Für $X \subseteq A$ ist dann $X^\perp = {}^\perp X$. Für jedes Ideal I in A ist also $\mathrm{LAn}(I) = {}^\perp I = I^\perp = \mathrm{RAn}(I)$.

Satz. *Sei (A, λ) eine symmetrische F-Algebra, wobei $\lambda : A \to F$ linear ist. Dann ist $(ZA)^\perp = KA$; insbesondere ist $\dim A/KA = \dim ZA$.*

Beweis. Für $a, b, c \in A$ ist

$$\lambda((ab - ba)c) = \lambda(abc) - \lambda(bac) = \lambda(bca) - \lambda(bac) = \lambda(b(ca - ac)).$$

Daher gilt: $c \in (KA)^\perp \iff ca - ac = 0$ für alle $a \in A \iff c \in ZA$. $\square$

24.4. Satz (Nakayama). *Sei (A, λ) eine symmetrische F-Algebra, wobei $\lambda : A \to F$ linear ist. Dann ist $(JA)^\perp = sA$ für ein $s \in ZA$.*

Beweis. Nach 24.1 ist A/JA symmetrisch. Nach 24.2 existiert also ein $s \in ZA$ mit

$$JA = \{a \in A : as = 0\} = \{a \in A : asA = 0\} = \mathrm{LAn}(sA) = (sA)^\perp.$$

Daher ist $(JA)^\perp = sA$. $\square$

Bemerkung. Offenbar ist $s \in (JA)^\perp \cap ZA = (JA)^\perp \cap (KA)^\perp = (JA + KA)^\perp$. Für jeden ZA-Untermodul U von A ist auch $U^\perp$ ein ZA-Untermodul von A wegen $\lambda(U \cdot ZA \cdot U^\perp) \subseteq \lambda(UU^\perp) = 0$, d.h. $ZA \cdot U^\perp \subseteq U^\perp$. Daher ist insbesondere $(JA + KA)^\perp$ ein ZA-Untermodul von A. Wegen $(JA + KA)^\perp \subseteq (KA)^\perp = ZA$ ist also $(JA + KA)^\perp$ ein Ideal in ZA. Man nennt $(JA + KA)^\perp$ das *Reynolds-Ideal* von ZA. Offenbar ist $(JA)^\perp = (JA + KA)^\perp A$ und $JA = \{x \in A : x(JA + KA)^\perp = 0\}$. Wegen $\Gamma(A)JA = 0$ ist $\Gamma(A) \subseteq (JA)^\perp \cap ZA = (JA + KA)^\perp$, d.h. das Higman-Ideal ist stets im Reynolds-Ideal enthalten.
Sind $B_1, \ldots, B_r$ die Blöcke von A, so ist, wie man leicht nachrechnet, $(JA + KA)^\perp = \bigoplus_{i=1}^r (JB_i + KB_i)^\perp$. Sei $i \in \{1, \ldots, r\}$ und $B := B_i$. Ist $JB \neq 0$, so ist $1_B \notin (JB + KB)^\perp$ wegen $(JB + KB)^\perp JB = 0$. Da ZB lokal ist, folgt $(JB + KB)^\perp \subseteq JZB \subseteq JB$ und damit $((JB + KB)^\perp)^2 \subseteq (JB)^\perp JB = 0$. Ist $JB = 0$, so ist $(JB + KB)^\perp = (KB)^\perp = ZB$ und $((JB + KB)^\perp)^2 = ZB$. Wie beim Higman-Ideal gilt also:

$$((JB + KB)^\perp)^2 = \bigoplus_{\substack{i=1 \\ JB_i = 0}}^{r} ZB_i;$$

insbesondere ist $\dim((JA + KA)^\perp)^2$ die Anzahl der Blöcke von A, die einfache Algebren sind.

Beispiel. Seien $p > 0$, G eine endliche Gruppe und $\lambda : FG \to F$ die früher definierte Linearform, die FG zu einer symmetrischen F-Algebra macht. Für jede Teilmenge X von G und jedes Element $a \in FG$ der Form $a = \sum_{g \in G} \alpha_g g$ mit $\alpha_g \in F$ für $g \in G$ gilt:

$$\lambda(aX^+) = \sum_{g \in X^{-1}} \alpha_g;$$

dabei ist $X^{-1} := \{x^{-1} : x \in X\}$. Da mit S auch S^{-1} eine p'-Sektion von G ist, folgt aus 21.8:

$$JFG + KFG = \left(F\{S^+ : S \in \mathrm{Sec}_{p'}(G)\}\right)^\perp,$$

also $(JFG + KFG)^\perp = F\{S^+ : S \in \mathrm{Sec}_{p'}(G)\}$. Auf diese Weise hatte Reynolds sein Ideal ursprünglich definiert.

24.5. Satz (Brauer-Tsushima). *Im Fall $p > 0$ gilt für jede endliche Gruppe G:*

$$JFG = \{x \in FG : xS^+ = 0 \text{ für } S \in \mathrm{Sec}_{p'}(G)\}.$$

Beweis. 24.4. $\square$

24.6. Satz. *Sei (A, β) eine symmetrische F-Algebra, wobei $\beta : A \times A \to F$ bilinear ist. Dann gilt:*

(i) *Für Idempotente e, f in A ist* $\dim eAf = \dim fAe$.

(ii) *Für jedes Ideal $I \neq 0$ in A ist $I \cap ZA \neq 0$.*

Beweis.

(i) Die Einschränkung von β liefert eine Bilinearform $\beta' : eAf \times fAe \to F$. Ist $x \in eAf$ mit

$$0 = \beta'(x, fAe) = \beta(xfA, e) = \beta(xA, e) = \beta(e, xA) = \beta(ex, A) = \beta(x, A),$$

so ist $x = 0$. Ein analoges Argument zeigt, daß β' nicht ausgeartet ist. Daher ist $\dim eAf = \dim fAe$.

(ii) Aus $I \cap ZA = 0$ folgt

$$A = 0^\perp = (I \cap ZA)^\perp = I^\perp + (ZA)^\perp = I^\perp + KA,$$

also

$$A/I^\perp = KA + I^\perp/I^\perp = K(A/I^\perp) = J(A/I^\perp) + K(A/I^\perp).$$

Nach 21.4 ist $A/I^\perp = 0$, d.h. $A = I^\perp$ und $I = A^\perp = 0$.

□

24.7. Bemerkung. Seien $p > 0$ und (A, β) eine symmetrische F-Algebra, wobei $\beta : A \times A \to F$ bilinear ist. Wegen $(ZA)^\perp = KA$ ist die Abbildung $\overline{\beta} : A/KA \times ZA \to F$, $(a + KA, z) \mapsto \beta(a, z)$ wohldefiniert, bilinear und nichtausgeartet. Außerdem ist $\overline{\beta}$ assoziativ in dem Sinne, daß $\overline{\beta}(x, yz) = \overline{\beta}(xy, z)$ für $x \in A/KA$, $y, z \in ZA$; dabei fassen wir A/KA als ZA-Modul auf. Für $n \in \mathbb{N}_0$ hatten wir eine additive Abbildung $A/KA \to A/KA$, $x \mapsto x^{p^n}$ konstruiert. Für $z \in ZA$ ist also auch die Abbildung $\varphi : A/KA \to F$, $x \mapsto \overline{\beta}(x^{p^n}, z)$ additiv. Ferner ist

$$\varphi(\alpha x) = \overline{\beta}((\alpha x)^{p^n}, z) = \overline{\beta}(\alpha^{p^n} x^{p^n}, z) = \alpha^{p^n}\overline{\beta}(x^{p^n}, z) = \alpha^{p^n}\varphi(x)$$

für $\alpha \in F$, $x \in A/KA$. Bekanntlich ist die Abbildung $F \to F$, $\alpha \mapsto \alpha^{p^n}$ ein Körperautomorphismus. Seine Umkehrabbildung schreiben wir in der Form $\alpha \mapsto \alpha^{p^{-n}}$. Dann ist die Abbildung $A/KA \to F$, $x \mapsto \overline{\beta}(x^{p^n}, z)^{p^{-n}}$ F-linear. Da $\overline{\beta}$ eine lineare Bijektion $ZA \to \mathrm{Hom}_F(A/KA, F)$ induziert, existiert also genau ein Element $\zeta_n(z) \in ZA$ mit $\overline{\beta}(x^{p^n}, z)^{p^{-n}} = \overline{\beta}(x, \zeta_n(z))$ für $x \in A/KA$. Wir erhalten so eine Abbildung $\zeta_n : ZA \to ZA$, die wir als „dual" oder „adjungiert" zu der Abbildung $A/KA \to A/KA$, $x \mapsto x^{p^n}$ ansehen.

Definition. Im Fall $p > 0$ definieren wir für $n \in \mathbb{N}_0$ und jede endlich-dimensionale F-Algebra A: $P_n A := F\{x^{p^n} : x \in A\} + KA$.

Satz. *Mit den obigen Bezeichnungen gilt:*
(i) *Für $y, z \in ZA$ ist $\zeta_n(y + z) = \zeta_n(y) + \zeta_n(z)$ und $\zeta_n(y^{p^n} z) = y\zeta_n(z)$.*
(ii) *Für $m, n \in \mathbb{N}_0$ ist $\zeta_m \circ \zeta_n = \zeta_{m+n}$.*
(iii) *Bild*$(\zeta_n) = (T_n A)^\perp$ *und* $\mathrm{Ker}(\zeta_n) = (P_n A)^\perp$.

Beweis.
(i) Für $x \in A/KA$ ist

$$\begin{aligned}
\overline{\beta}(x, \zeta_n(y + z)) &= \overline{\beta}(x^{p^n}, y + z)^{p^{-n}} = \overline{\beta}(x^{p^n}, y)^{p^{-n}} + \overline{\beta}(x^{p^n}, z)^{p^{-n}} \\
&= \overline{\beta}(x, \zeta_n(y)) + \overline{\beta}(x, \zeta_n(z)) = \overline{\beta}(x, \zeta_n(y) + \zeta_n(z)). \\
\overline{\beta}(x, \zeta_n(y^{p^n} z)) &= \overline{\beta}(x^{p^n}, y^{p^n} z)^{p^{-n}} = \overline{\beta}(x^{p^n} y^{p^n}, z)^{p^{-n}} \\
&= \overline{\beta}((xy)^{p^n}, z)^{p^{-n}} = \overline{\beta}(xy, \zeta_n(z)) = \overline{\beta}(x, y\zeta_n(z)).
\end{aligned}$$

(ii) Für $x \in A/KA$ und $z \in ZA$ ist

$$\begin{aligned}
\overline{\beta}(x, \zeta_{m+n}(z)) &= \overline{\beta}(x^{p^{m+n}}, z)^{p^{-m-n}} = (\overline{\beta}((x^{p^m})^{p^n}, z)^{p^{-n}})^{p^{-m}} \\
&= \overline{\beta}(x^{p^m}, \zeta_n(z))^{p^{-m}} = \overline{\beta}(x, \zeta_m(\zeta_n(z))).
\end{aligned}$$

(iii) Für $x \in A/KA$ gilt:

$$\begin{aligned}
x \in \mathrm{Bild}(\zeta_n)^\perp &\iff \overline{\beta}(x, \zeta_n(z)) = 0 \text{ für } z \in ZA \\
&\iff \overline{\beta}(x^{p^n}, z)^{p^{-n}} = 0 \text{ für } z \in ZA \\
&\iff x^{p^n} = 0 \\
&\iff x \in T_n(A/KA).
\end{aligned}$$

Für $z \in ZA$ gilt:

$$\begin{aligned} z \in \operatorname{Ker}(\zeta_n) &\iff \zeta_n(z) = 0 \\ &\iff \overline{\beta}(x, \zeta_n(z)) = 0 \text{ für } x \in A/KA \\ &\iff \overline{\beta}(x^{p^n}, z)^{p^{-n}} = 0 \text{ für } x \in A/KA \\ &\iff \overline{\beta}(x^{p^n}, z) = 0 \text{ für } x \in A/KA \\ &\iff z \in (P_n A)^{\perp}. \end{aligned}$$

□

Beispiel. Seien $p > 0$, $n \in \mathbb{N}_0$, G eine endliche Gruppe und $\lambda : FG \to F$ wie früher. Für $C \in \operatorname{Cl}(G)$ ist dann $\zeta_n(C^+) = (C^{p^{-n}})^+$; denn für $g \in G$ ist

$$\lambda(g\zeta_n(C^+)) = \lambda(g^{p^n} C^+)^{p^{-n}} = \begin{cases} 1 & \text{falls } g^{p^n} \in C^{-1} \\ 0 & \text{sonst} \end{cases},$$

d.h. $\lambda(g\zeta_n(C^+)) = \lambda(g(C^{p^{-n}})^+)$.

24.8. Bemerkung. Seien $p > 0$, (A, β) eine symmetrische F-Algebra, wobei $\beta : A \times A \to F$ bilinear ist, und $\overline{\beta} : A/KA \times ZA \to F$ wie oben. Dann ist auch die Abbildung $\psi : ZA \to ZA,\ z \mapsto z^{p^n}$ additiv mit $\psi(\alpha z) = \alpha^{p^n}\psi(z)$ für $\alpha \in F,\ z \in ZA$. Daher existiert analog zu jedem Element $x \in A/KA$ genau ein Element $\kappa_n(x) \in A/KA$ mit $\overline{\beta}(\kappa_n(x), z) = \overline{\beta}(x, z^{p^n})^{p^{-n}}$ für $z \in ZA$. Auf diese Weise erhalten wir eine Abbildung $\kappa_n : A/KA \to A/KA$.

Satz. *Mit den obigen Bezeichnungen gilt:*

(i) *Für $x, y \in A/KA$ ist $\kappa_n(x + y) = \kappa_n(x) + \kappa_n(y)$.*
(ii) *Für $x \in A/KA$ und $y \in ZA$ ist $\kappa_n(xy^{p^n}) = \kappa_n(x)y$ und $\kappa_n(x^{p^n}y) = x\zeta_n(y)$.*
(iii) *Für $m, n \in \mathbb{N}_0$ ist $\kappa_m \circ \kappa_n = \kappa_{m+n}$.*
(iv) $\operatorname{Bild}(\kappa_n) = (T_n ZA)^{\perp}/KA$ *und* $\operatorname{Ker}(\kappa_n) = (P_n ZA)^{\perp}/KA$.

Beweis. Für $x \in A/KA,\ y, z \in ZA$ ist

$$\begin{aligned} \overline{\beta}(\kappa_n(x^{p^n}y), z) &= \overline{\beta}(x^{p^n}y, z^{p^n})^{p^{-n}} = \overline{\beta}(x^{p^n}, yz^{p^n})^{p^{-n}} \\ &= \overline{\beta}(x, \zeta_n(yz^{p^n}))^{p^{-n}} = \overline{\beta}(x, \zeta_n(y)z)^{p^{-n}} \\ &= \overline{\beta}(x\zeta_n(y), z). \end{aligned}$$

Der Rest geht analog zum Beweis von 24.7. □

Beispiel. Wir werden κ_n für Gruppenalgebren im folgenden Kapitel auf einem kleinen Umweg berechnen.

KAPITEL 25

Das Zentrum der Gruppenalgebra

Sei F ein algebraisch abgeschlossener Körper der Charakteristik $p > 0$.

25.1. Bemerkung. Für jede endliche Gruppe G und jede Teilmenge X von G sei $\mathrm{Pr}_X = \mathrm{Pr}_X^G : FG \to FG$ die lineare Abbildung mit

$$\mathrm{Pr}_X^G(g) := \begin{cases} g & \text{für } g \in X, \\ 0 & \text{sonst.} \end{cases}$$

Für $g, x \in G$ ist dann $\mathrm{Pr}_{xX}^G(xg) = x\,\mathrm{Pr}_X^G(g)$, $\mathrm{Pr}_{Xx}^G(gx) = \mathrm{Pr}_X^G(g)x$ und $\mathrm{Pr}_{xXx^{-1}}^G(xgx^{-1}) = x\,\mathrm{Pr}_X^G(g)x^{-1}$.

Satz. *Für jede endliche Gruppe G und jede p-Untergruppe Q von G ist die Abbildung*

$$\mathrm{Br}_Q^G = \mathrm{Br}_Q : ZFG \to ZFC_G(Q),\ z \mapsto \mathrm{Pr}_{C_G(Q)}^G(z)$$

ein Homomorphismus von Algebren mit $\mathrm{Br}_Q(K^+) = (K \cap C_G(Q))^+$ *für* $K \in \mathrm{Cl}(G)$.

Definition. Man nennt Br_Q den *Brauer-Homomorphismus* bzgl. Q.

Beweis. Zu zeigen ist $\mathrm{Br}_Q(K^+L^+) = \mathrm{Br}_Q(K^+)\,\mathrm{Br}_Q(L^+)$ für $K, L \in \mathrm{Cl}(G)$. Offenbar ist $K^+L^+ = \sum_{g\in G} \alpha_g g$ mit $\alpha_g = |\{(k,l) \in K \times L : kl = g\}|1_F$ für $g \in G$, also $\mathrm{Br}_Q(K^+L^+) = \sum_{g \in C_G(Q)} \alpha_g g$. Andererseits ist $\mathrm{Br}_Q(K^+)\,\mathrm{Br}_Q(L^+) = (K \cap C_G(Q))^+(L \cap C_G(Q))^+ = \sum_{g\in C_G(Q)} \alpha'_g g$ mit $\alpha'_g = |\{(k,l) \in (K \cap C_G(Q)) \times (L \cap C_G(Q)) : kl = g\}|1_F$. Für $g \in C_G(Q)$ operiert Q auf $\{(k,l) \in K \times L : kl = g\}$ durch Konjugation, und $\{(k,l) \in (K \cap C_G(Q)) \times (L \cap C_G(Q)) : kl = g\}$ ist die Menge der entsprechenden Fixpunkte. Da Q eine p-Gruppe ist, folgt

$$|\{(k,l) \in K \times L : kl = g\}| \equiv |\{(k,l) \in (K \cap C_G(Q)) \times (L \cap C_G(Q)) : kl = g\}| \pmod p,$$

d.h. $\alpha_g = \alpha'_g$. □

25.2. Satz. *Seien G eine endliche Gruppe, $g \in G$ mit p-Faktor u und p'-Faktor s, $K \in \mathrm{Cl}(G)$ und $n \in \mathbb{N}_0$. Dann ist*

$$\kappa_n(K^+g + KFG) = \big((Ku)^{p^{-n}}\big)^+ s^{p^{-n}} + KFG;$$

dabei ist $(Ku)^{p^{-n}} := \{x \in G : x^{p^n} \in Ku\}$, und $s^{p^{-n}}$ das eindeutig bestimmte Element $y \in G_{p'}$ mit $y^{p^n} = s$. Insbesondere ist $\kappa_n(g + KFG) = \big(\{u\}^{p^{-n}}\big)^+ s^{p^{-n}} + KFG$.

Beweis. Für $z \in ZFG$ gilt mit den üblichen Bezeichnungen:

$$\begin{aligned}
\overline{\beta}(\kappa_n(K^+g + KFG), z) &= \overline{\beta}(K^+g + KFG, z^{p^n})^{p^{-n}} = \beta(K^+g, z^{p^n})^{p^{-n}} \\
&= \lambda(K^+gz^{p^n})^{p^{-n}} = \lambda(\mathrm{Pr}_{C_G(u)}(gK^+z^{p^n}))^{p^{-n}} \\
&= \lambda(g\,\mathrm{Pr}_{C_G(u)}(K^+z^{p^n}))^{p^{-n}} \\
&= \lambda(su\,\mathrm{Br}_{\langle u\rangle}(K^+)\,\mathrm{Br}_{\langle u\rangle}(z)^{p^n})^{p^{-n}} \\
&= \lambda(y^{p^n}\,\mathrm{Br}_{\langle u\rangle}(z)^{p^n}\,\mathrm{Br}_{\langle u\rangle}(K^+)u)^{p^{-n}} \\
&= \overline{\beta}_{C_G(u)}((y\,\mathrm{Br}_{\langle u\rangle}(z) + KFC_G(u))^{p^n}, (K \cap C_G(u))^+u)^{p^{-n}} \\
&= \overline{\beta}_{C_G(u)}(y\,\mathrm{Br}_{\langle u\rangle}(z) + KFC_G(u), \zeta_n^{C_G(u)}((Ku \cap C_G(u))^+)) \\
&= \beta_{C_G(u)}(y\,\mathrm{Br}_{\langle u\rangle}(z), \{h \in C_G(u) : h^{p^n} \in Ku \cap C_G(u)\}^+) \\
&= \lambda(y\{h \in C_G(u) : h^{p^n} \in Ku\}^+\,\mathrm{Br}_{\langle u\rangle}(z)) \\
&= \lambda(y\{h \in C_G(u) : h^{p^n} \in Ku\}^+z) \\
&= \overline{\beta}(y\{h \in C_G(u) : h^{p^n} \in Ku\}^+ + KFG, z).
\end{aligned}$$

Nun operiert $\langle u\rangle$ auf $X := \{h \in G : h^{p^n} \in Ku\}$ durch Konjugation, und $\{h \in C_G(u) : h^{p^n} \in Ku\}$ ist die Menge der Fixpunkte. Für $x \in X$ ist aber $y \cdot uxu^{-1} = uyxu^{-1} \equiv yx \pmod{KFG}$. Daher ist $\kappa_n(K^+g + KFG) = yX^+ + KFG$. □

Beispiel. Im Fall $p^n \geq \exp_p(G)$ ist

$$\{u\}^{p^{-n}} = \begin{cases} \emptyset & \text{falls } u \neq 1, \\ G_p & \text{falls } u = 1. \end{cases}$$

Folglich ist in diesem Fall

$$\kappa_n(g + KFG) = \begin{cases} G_p^+ g^{p^{-n}} + KFG & \text{falls } g \in G_{p'}, \\ 0 & \text{sonst.} \end{cases}$$

25.3. Satz. *Für jede endliche Gruppe G und $n \in \mathbb{N}_0$ ist $\{z \in ZFG : z^{p^n} = 0\} = T_nZFG = \{z \in ZFG : z(\{u\}^{p^{-n}})^+ \in F[G \setminus C_G(u)_{p'}]$ für $u \in G_{p'}\}$.*

Beweis. Für $z \in ZFG$ gilt mit den üblichen Bezeichnungen:

$$\begin{aligned}
z \in T_nZFG &\iff 0 = \beta((T_nZFG)^\perp, z) \\
&\iff 0 = \overline{\beta}((T_nZFG)^\perp/KFG, z) \\
&\iff 0 = \overline{\beta}(\kappa_n(FG/KFG), z).
\end{aligned}$$

Nach 25.2 ist

$$\kappa_n(FG/KFG) = F\{(\{u\}^{p^{-n}})^+s + KFG : u \in G_{p'},\ s \in C_G(u)_{p'}\}.$$

Daher gilt:

$$\begin{aligned}
z \in T_nZFG \iff 0 &= \overline{\beta}((\{u\}^{p^{-n}})^+s + KFG, z) \\
&= \beta(s, \{u\}^{p^{-n}}z) \\
&= \lambda(s\{u\}^{p^{-n}}z) \text{ für } u \in G_{p'},\ s \in C_G(u)_{p'}.
\end{aligned}$$

□

Beispiel. Im Fall $p^n \geq \exp_p(G)$ gilt also für $z \in ZFG$:

$$z^{p^n} = 0 \iff zG_{p'}^+ \in F[G \setminus G_{p'}].$$

Wegen $G_p \in \mathrm{Sec}_{p'}(G)$ ist $G_p^+ \in (JFG + KFG)^\perp$ und $zG_p^+ \in (JFG + KFG)^\perp$, also

$$zG_p^+ = \sum_{S \in \mathrm{Sec}_{p'}(G)} \alpha_S S^+$$

mit $\alpha_S \in F$ für $S \in \mathrm{Sec}_{p'}(G)$. Da jede p'-Sektion auch p'-Elemente enthält, gilt:

$$zG_p^+ \in F[G \setminus G_{p'}] \iff zG_p^+ = 0.$$

Damit erhalten wir im Fall $p^n \geq \exp_p(G)$ für $z \in ZFG$: $z^{p^n} = 0 \iff zG_p^+ = 0$.

25.4. Satz (Iizuka-Watanabe)**.** *Für jede endliche Gruppe G und jedes $z \in ZFG$ gilt:*

$$z \in JZFG \iff zG_p^+ = 0 \iff z^{\exp_p(G)} = 0.$$

25.5. Satz. *Seien G eine endliche Gruppe, $N \trianglelefteq G$ und $\nu_N : FG \to F[G/N]$ kanonisch. Dann ist $\mathrm{Ker}(\nu_N) = (\Omega FN)FG = FG(\Omega FN)$.*

Beweis. Sei $x \in \Omega FN$ und $x = \sum_{n \in N} \xi_n n$ mit $\xi_n \in F$ für $n \in N$. Dann ist $\nu_N(x) = \sum_{n \in N} \xi_n nN = 0$. Daher ist $FG(\Omega FN) \subseteq \mathrm{Ker}(\nu_N)$. Sei umgekehrt $x \in \mathrm{Ker}(\nu_N)$ und T ein Repräsentantensystem für G/N. Wir schreiben $x = \sum_{t \in T} \sum_{n \in N} \xi_{tn} tn$ mit $\xi_{tn} \in F$ für $t \in T$, $n \in N$. Dann ist $0 = \nu_N(x) = \sum_{t \in T} (\sum_{n \in N} \xi_{tn}) tN$, also $\sum_{n \in N} \xi_{tn} = 0$ für $t \in T$. Daher ist $x \in FG(\Omega FN)$. Folglich ist $\mathrm{Ker}(\nu_N) = FG(\Omega FN)$, und analog ist $\mathrm{Ker}(\nu_N) = (\Omega FN)FG$. □

25.6. Satz (Okuyama)**.** *Für jede endliche Gruppe G, jede p-Sylowgruppe P von G und $q := |P|$ ist $(JZFG)^{q-1} \subseteq (JFG)^\perp$; insbesondere ist $(JZFG)^q = 0$.*

Beweis. Sei G ein Gegenbeispiel minimaler Ordnung, also $G \neq 1$. Mit den üblichen Bezeichnungen ist dann $0 \neq \beta((JZFG)^{q-1}, JFG) \subseteq \beta((JZFG)^{q-1}, JFG + KFG)$. Wir wählen $x \in JFG + KFG$, $z \in (JZFG)^{q-1}$ mit $\beta(z, x) \neq 0$ und schreiben $x = \sum_{g \in G} \xi_g g$ mit $\xi_g \in F$ für $g \in G$. Dann ist also $0 \neq \beta(z, \sum_{g \in S} \xi_g g)$ für ein $S \in \mathrm{Sec}_{p'}(G)$. Sei $s \in S \cap G_{p'}$. Dann ist $\sum_{g \in S} \xi_g g = \sum_{g \in S} \xi_g (g - s)$, also $0 \neq \beta(z, g - s)$ für ein $g \in S$. Sei $h \in G$ mit $hg_{p'}h^{-1} = s$. Dann ist

$$0 \neq \beta(z, \underbrace{g - hgh^{-1}}_{\in KFG} + hgh^{-1} - s) = \beta(z, hgh^{-1} - s).$$

Jetzt ist s der p'-Faktor von hgh^{-1}, und $u := hg_ph^{-1}$ ist der p-Faktor von hgh^{-1}. Daher ist

$$0 \neq \lambda(z(us - s)) = \lambda(\mathrm{Pr}_{C_G(u)}(z(us - s))) = \lambda(\mathrm{Br}_{\langle u \rangle}(z)(us - s));$$

insbesondere ist $\mathrm{Br}_{\langle u \rangle}(z)(u - 1) \neq 0$. Dabei ist $\mathrm{Br}_{\langle u \rangle}(z) \in (JZFC_G(u))^{q-1}$ und $u - 1 \in JZFC_G(u)$. Daher ist $(JZFC_G(u))^q \neq 0$. Insbesondere ist $C_G(u)$ auch ein Gegenbeispiel zur Behauptung. Nach Wahl von G ist also $G = C_G(u)$ und $(JZFG)^q \neq 0$. Daher ist $N := \langle u \rangle \trianglelefteq G$ und $|G/N| < |G|$. Nach Wahl von G ist also $(JZF[G/N])^{q/|N|} = 0$. Ist $\nu_N : FG \to F[G/N]$ kanonisch, so ist auch $\nu_N((JZFG)^{q/|N|}) = 0$. Folglich ist $(JZFG)^{q/|N|} \subseteq \mathrm{Ker}(\nu_N) = FG(\Omega FN)$. Wegen $(\Omega FN)^{|N|} = (JFN)^{|N|} = 0$ ist also $(JZFG)^q \subseteq FG(\Omega FN)^{|N|} = 0$. Widerspruch. □

25.7. Satz. *Sei G eine endliche Gruppe, $K \in \mathrm{Cl}(G)$, $z \in ZFG$, $n \in \mathbb{N}_0$ und $K^+ z^{p^n} = \sum_{g \in G} \alpha_g g$ mit $\alpha_g \in F$ für $g \in G$. Ist $g \in G$ mit $\alpha_g \neq 0$, so ist $(Kg_p^{-1})^{p^{-n}} \cap C_G(Q) \neq \emptyset$ für jede p-Sylowgruppe Q von $C_G(g)$.*

Beweis. Mit den üblichen Bezeichnungen ist

$$\begin{aligned} 0 \neq \alpha_g &= \beta\big(g^{-1}, K^+ z^{p^n}\big) = \beta\big(g^{-1}K^+, z^{p^n}\big) \\ &= \overline{\beta}\big(K^+ g^{-1} + KFG, z^{p^n}\big) = \overline{\beta}(\kappa_n(K^+ g^{-1} + KFG), z)^{p^{-n}} \\ &= \overline{\beta}\big(((Kg_p^{-1})^{p^{-n}})^+ g_{p'}^{p^{-n}} + KFG, z\big)^{p^{-n}}, \end{aligned}$$

also $((Kg_p^{-1})^{p^{-n}})^+ g_{p'}^{p^{-n}} \notin KFG$. Jede p-Sylowgruppe Q von $C_G(g)$ operiert durch Konjugation auf $(Kg_p^{-1})^{p^{-n}} g_{p'}^{p^{-n}}$, und Elemente in der gleichen Bahn liegen in der gleichen Nebenklasse nach KFG. Daher ist

$$\begin{aligned} 0 &\not\equiv \left((Kg_p^{-1})^{p^{-n}}\right)^+ g_{p'}^{p^{-n}} \\ &\equiv \left((Kg_p^{-1})^{p^{-n}} g_{p'}^{p^{-n}} \cap C_G(Q)\right)^+ \\ &= \left((Kg_p^{-1})^{p^{-n}} \cap C_G(Q)\right)^+ g_{p'}^{p^{-n}} \pmod{KFG}; \end{aligned}$$

insbesondere ist $(Kg_p^{-1})^{p^{-n}} \cap C_G(Q) \neq \emptyset$. □

Bemerkung. Im Fall $p^n \geq \exp_p(G)$ ist $z^{p^n} = 0$ für $z \in JZFG$. Wegen $ZFG = EZFG \oplus JZFG$ ist also $P_n ZFG = EZFG$. Für $h \in (Kg_p^{-1})^{p^{-n}} \cap C_G(Q)$ ist außerdem $h^{p^n} \in C_G(Q)_{p'} \subseteq C_G(g_p)_{p'}$ und $h^{p^n} \in Kg_p^{-1}$, also $h^{p^n} g_p \in K$. Dies zeigt, daß K und g_p in der gleichen p-Sektion von G liegen. Wir haben damit bewiesen:

25.8. Satz (Iizuka-Osima). *Für jede endliche Gruppe G und $U \in \mathrm{Sec}_p(G)$ ist*

$$(ZFG \cap FU)EZFG \subseteq ZFG \cap FU;$$

insbesondere ist $EZFG \subseteq FG_{p'}$.

Bemerkung. $ZFG \cap FU$ ist also ein $EZFG$-Untermodul von ZFG für $U \in \mathrm{Sec}_p(G)$. Wegen

$$ZFG = \bigoplus_{U \in \mathrm{Sec}_p(G)} ZFG \cap FU$$

ist also für $U \in \mathrm{Sec}_p(G)$ die Einschränkung von Pr_U auf ZFG ein $EZFG$-Homomorphismus. Offenbar bilden für $U \in \mathrm{Sec}_p(G)$ die Klassensummen der Konjugationsklassen K von G mit $K \subseteq U$ eine F-Basis von $ZFG \cap FU$.

25.9. Satz. *Seien G eine endliche Gruppe, $U \in \mathrm{Sec}_p(G)$ und $u \in U \cap G_p$.*

(i) *Für $K \in \mathrm{Cl}(G)$ mit $K \subseteq U$ ist $K' := \{g \in K : g_p = u\} \in \mathrm{Cl}(C_G(u))$.*
(ii) *Auf diese Weise erhält man eine Bijektion zwischen der Menge aller Konjugationsklassen von G in U und der Menge aller Konjugationsklassen von $C_G(u)$ in der p-Sektion U' von u in $C_G(u)$.*
(iii) *Für $K \in \mathrm{Cl}(G)$ mit $K \subseteq U$ ist außerdem $K' = S \cap U'$, wobei S die p'-Sektion von $C_G(u)$ mit $K' \subseteq S$ ist.*

Beweis.

(i) Sei $K \in \mathrm{Cl}(G)$ mit $K \subseteq U$ und $K' := \{g \in K : g_p = u\}$. Offenbar ist $K' \neq \emptyset$. Sind $g, h \in K'$ und $x \in G$ mit $xgx^{-1} = h$, so ist $xux^{-1} = xg_px^{-1} = h_p = u$, d.h. $x \in C_G(u)$. Daher sind g und h auch in $C_G(u)$ konjugiert. Für $g \in K'$ und $y \in C_G(u)$ hat andererseits ygy^{-1} den p-Faktor $yg_py^{-1} = yuy^{-1} = u$. Daher ist auch $ygy^{-1} \in K'$.
(ii) Für $K \in \mathrm{Cl}(G)$ mit $K \subseteq U$ ist $\emptyset \neq K' \subseteq K$. Daher ist die Abbildung $\{K \in \mathrm{Cl}(G) : K \subseteq U\} \to \{L \in \mathrm{Cl}(C_G(u)) : L \subseteq U'\}$, $K \mapsto K'$ injektiv. Wegen $u \in Z(C_G(u))$ haben alle Elemente in U' p-Faktor u. Ist also $L \in \mathrm{Cl}(C_G(u))$ mit $L \subseteq U'$ und ist $K \in \mathrm{Cl}(G)$ mit $L \subseteq K$, so ist $K \subseteq U$ und $L \subseteq K'$, also $L = K'$ nach (i).
(iii) Sei $K \in \mathrm{Cl}(G)$ mit $K \subseteq U$, und sei S die p'-Sektion von $C_G(u)$ mit $K' \subseteq S$. Dann ist natürlich $K' \subseteq S \cap U'$. Umgekehrt hat jedes Element $g \in S \cap U'$ p-Faktor $g_p = u$, und der p'-Faktor $g_{p'}$ von g ist in $C_G(u)$ zu dem p'-Faktor $h_{p'}$ eines Elementes $h \in K'$ konjugiert. Sei $x \in C_G(u)$ mit $xg_{p'}x^{-1} = h_{p'}$. Dann ist $xgx^{-1} = xg_pg_{p'}x^{-1} = xug_{p'}x^{-1} = uxg_{p'}x^{-1} = uh_{p'} = h_ph_{p'} = h$, also $g \in K'$ nach (i).

□

Bemerkung. Mit den obigen Bezeichnungen ist $U' = uC_G(u)_{p'}$. Die Abbildung $C_G(u)_{p'} \to U'$, $s \mapsto us$ ist also bijektiv und verträglich mit der Konjugation in $C_G(u)$. Daher stehen die Konjugationsklassen von

G in U ebenfalls in Bijektion zu den p'-Konjugationsklassen von $C_G(u)$. Für jedes Repräsentantensystem $\mathcal{U}$ für die Konjugationsklassen von p-Elementen in G ist also $|\operatorname{Cl}(G)| = \sum_{u\in\mathcal{U}} |\operatorname{Sec}_{p'}(C_G(u))|$.

KAPITEL 26

Blöcke von Gruppenalgebren

Sei F ein algebraisch abgeschlossener Körper der Charakteristik $p > 0$.

26.1. Bemerkung. Wir beschäftigen uns zunächst mit der Zerlegung $ZFG = EZFG \oplus JZFG$ und der entsprechenden Projektion $\varepsilon = \varepsilon_G : ZFG \to EZFG$ für eine endliche Gruppe G.

Satz. *Für jede endliche Gruppe G, jede p-Untergruppe Q von G und für $z \in ZFG$ ist* $\mathrm{Br}_Q(\varepsilon_G(z)) = \varepsilon_{C_G(Q)}(\mathrm{Br}_Q(z))$.

Beweis. Wir schreiben $z = x + y$ mit $x \in EZFG,\ y \in JZFG$. Dann ist $\mathrm{Br}_Q(y)$ nilpotent, also $\mathrm{Br}_Q(y) \in JZFC_G(Q)$. Wegen $\mathrm{Br}_Q(e)^2 = \mathrm{Br}_Q(e^2) = \mathrm{Br}_Q(e)$ für jedes Idempotent $e \in ZFG$ ist analog $\mathrm{Br}_Q(x) \in EZFC_G(Q)$. Daher ist $\varepsilon_{C_G(Q)}(\mathrm{Br}_Q(z)) = \varepsilon_{C_G(Q)}(\mathrm{Br}_Q(x) + \mathrm{Br}_Q(y)) = \mathrm{Br}_Q(x) = \mathrm{Br}_Q(\varepsilon_G(z))$. □

26.2. Satz. *Seien G eine endliche Gruppe, $z \in ZFG$, $K \in \mathrm{Cl}(G)$, $U \in \mathrm{Sec}_p(G)$ mit $K \subseteq U$, $u \in U \cap G_p$, $U' := uC_G(u)_{p'}$ (d.h. U' ist die p'-Sektion von u in $C_G(u)$) und $S \in \mathrm{Sec}_{p'}(C_G(u))$ mit $K' \cap U' \subseteq S$. Dann ist $\mathrm{Pr}^G_{U'}(\varepsilon(z)K^+) = \mathrm{Pr}^G_{U'}(zS^+)$.*

Bemerkung. Nach 25.8 ist $\varepsilon(z)K^+ \in ZFG \cap FU$, und nach 25.9 ist die Einschränkung von $\mathrm{Pr}^G_{U'}$ eine lineare Bijektion zwischen $ZFG \cap U$ und $ZFC_G(u) \cap FU'$. Man kann also den obigen Satz dazu benutzen, um $\varepsilon(z)K^+$ zu berechnen.

Beispiel. Im Spezialfall $K = \{1\}$ ergibt sich mit 25.8 insbesondere: $\varepsilon(z) = \mathrm{Pr}^G_{G_{p'}}(zG_p^+)$.

Beweis.

$$\begin{aligned}
\mathrm{Pr}^G_{U'}(\varepsilon(z)K^+) &= \mathrm{Pr}^{C_G(u)}_{U'}(\mathrm{Br}_{\langle u\rangle}(\varepsilon(z)K^+)) \\
&= \mathrm{Pr}^{C_G(u)}_{U'}(\mathrm{Br}_{\langle u\rangle}(\varepsilon(z))\,\mathrm{Br}_{\langle u\rangle}(K^+)) \\
&= \mathrm{Pr}^{C_G(u)}_{U'}(\varepsilon_{C_G(u)}(\mathrm{Br}_{\langle u\rangle}(z))\,\mathrm{Br}_{\langle u\rangle}(K^+)) \\
&= \varepsilon_{C_G(u)}(\mathrm{Br}_{\langle u\rangle}(z))\,\mathrm{Pr}^{C_G(u)}_{U'}(\mathrm{Br}_{\langle u\rangle}(K^+)) \\
&= \varepsilon_{C_G(u)}(\mathrm{Br}_{\langle u\rangle}(z))(K \cap U')^+ \\
&= \varepsilon_{C_G(u)}(\mathrm{Br}_{\langle u\rangle}(z))(S \cap U')^+ \\
&= \varepsilon_{C_G(u)}(\mathrm{Br}_{\langle u\rangle}(z))\,\mathrm{Pr}^{C_G(u)}_{U'}(S^+) \\
&= \mathrm{Pr}^{C_G(u)}_{U'}(\varepsilon_{C_G(u)}(\mathrm{Br}_{\langle u\rangle}(z))S^+) \\
&= \mathrm{Pr}^{C_G(u)}_{U'}(\mathrm{Br}_{\langle u\rangle}(z)S^+) \\
&= \mathrm{Pr}^G_{U'}(zS^+).
\end{aligned}$$

□

26.3. Bemerkung. Seien G eine endliche Gruppe, $\nu = \nu_G : FG \to F$ die Augmentationsabbildung und $e_1, \ldots, e_r$ die Blockidempotente von FG. Wegen $1 = \nu(1) = \nu(e_1 + \ldots + e_r) = \nu(e_1) + \ldots + \nu(e_r)$ ist $\nu(e_i) \neq 0$ für ein $i \in \{1, \ldots, r\}$. Für $j \neq i$ ist $\nu(e_j)\nu(e_i) = \nu(e_j e_i) = \nu(0) = 0$, also $\nu(e_j) = 0$. Daher ist e_i das einzige Blockidempotent von FG mit $\nu(e_i) \neq 0$. Folglich ist $\nu(e_i) = 1$. Man nennt e_i das *Hauptblockidempotent* und $B := FGe_i$ den *Hauptblock* von FG. Wir schreiben $e_i := e_0(FG)$ und $B_i := B_0(FG)$. Für viele Anwendungen ist dies der wichtigste Block von FG.

Satz (Osima). *Für jede endliche Gruppe G und $U \in \mathrm{Sec}_p(G)$ ist $U^+ \in B_0(FG) \cap ZFG = ZB_0(FG)$.*

Beweis. Sei $x \in FG$ und $x = \sum_{g\in G} \xi_g g$ mit $\xi_g \in F$ für $g \in G$. Dann ist

$$xG^+ = \sum_{g\in G} \xi_g gG^+ = \sum_{g\in G} \xi_g G^+ = \nu(x)G^+;$$

insbesondere ist $e_0(FG)G^+ = \nu(e_0(FG))G^+ = G^+$. Folglich ist

$$U^+ = \mathrm{Pr}_U^G(G^+) = \mathrm{Pr}_U^G(e_0(FG)G^+) = e_0(FG)\,\mathrm{Pr}_U^G(G^+) = e_0(FG)U^+ \in B_0(FG).$$

□

26.4. Satz. *Für jede endliche Gruppe G ist $p \nmid |G_{p'}|$.*

Beweis. Jede p-Sylowgruppe P von G operiert auf $G_{p'}$ durch Konjugation. Daher ist $|G_{p'}| \equiv |C_G(P)_{p'}| \pmod p$. Nach Schur-Zassenhaus besitzt P ein Komplement K in $PC_G(P)$. Wegen $p \nmid |K|$ ist $K \subseteq C_G(P)$, also $C_G(P) = C_G(P) \cap PK = (C_G(P) \cap P)K = Z(P)K = Z(P) \times K$. Folglich ist $C_G(P)_{p'} = K$ und $p \nmid |G_{p'}|$. □

Bemerkung. Ist $\nu : FG \to G$ die Augmentationsabbildung, so ist also $\nu(G_{p'}^+) = |G_{p'}|\,1_F \neq 0$. Daher ist $G_{p'}^+$ nicht nilpotent. Nach 26.3 ist also $G_{p'}^+ \in ZB_0(FG) \setminus JZB_0(FG)$.

26.5. Satz. *Für jede endliche Gruppe G ist $e_0(FG) = \sum_{g\in G_{p'}} \alpha_g g$ mit*

$$|G_{p'}|\,\alpha_g = |\{(s,u) : G_{p'} \times G_p : su = g\}|\,1_F$$

für $g \in G_{p'}$.

Beweis. Wegen $ZB_0(FG) = Fe_0(FG) \oplus JZB_0(FG)$ ist $G_{p'}^+ = \alpha e_0(FG) + x$ mit $\alpha \in F^\times$, $x \in JZB_0(FG)$. Ist $\nu : FG \to F$ die Augmentationsabbildung, so ist $\nu(x) = 0$, also $|G_{p'}|\,1_F = \nu(G_{p'}^+) = \alpha$. Folglich ist $\varepsilon(G_{p'}^+) = \alpha e_0(FG) = |G_{p'}|\,e_0(FG)$. Nach 26.2 ist andererseits $\varepsilon(G_{p'}^+) = \mathrm{Pr}_{G_{p'}}^G(G_{p'}^+ G_p^+) = \sum_{g\in G_{p'}} |\{(s,u) \in G_{p'} \times G_p : su = g\}|\,g$. □

Beispiel.
(i) Für jede endliche p-Gruppe G ist $e_0(FG) = 1$.
(ii) Für jede endliche p'-Gruppe G ist $e_0(FG) = \frac{1}{|G|}\sum_{g\in G} g$.

26.6. Satz (Brauers III. Hauptsatz)**.** *Für jede endliche Gruppe G und jede p-Untergruppe Q von G ist $\mathrm{Br}_Q(e_0(FG)) = e_0(FC_G(Q))$.*

Beweis. Nach 26.5 ist $\mathrm{Br}_Q(e_0(FG)) = \sum_{g\in C_G(Q)_{p'}} \alpha_g g$ und $e_0(FC_G(Q)) = \sum_{g\in C_G(Q)_{p'}} \alpha'_g g$ mit

$$|G_{p'}|\,\alpha_g = |\{(s,u) \in G_{p'} \times G_p : su = g\}|\,1_F$$

und

$$|C_G(Q)_{p'}|\,\alpha'_g = |\{(s,u) \in C_G(Q)_{p'} \times C_G(Q)_p : su = g\}|\,1_F$$

für $g \in C_G(Q)_{p'}$. Offenbar operiert Q durch Konjugation auf $G_{p'}$, und $C_G(Q)_{p'}$ ist die Menge der entsprechenden Fixpunkte. Daher ist $|G_{p'}| \equiv |C_G(Q)_{p'}| \pmod p$. Analog ist $|\{(s,u) \in G_{p'} \times G_p : su = g\}| \equiv |\{(s,u) \in C_G(Q)_{p'} \times C_G(Q)_p : su = g\}| \pmod p$. Folglich ist $\alpha_g = \alpha'_g$ für $g \in C_G(Q)_{p'}$. □

26.7. Satz. *Für jede endliche Gruppe G und jeden Normalteiler N von G ist $|G_{p'}|\,\mathrm{Pr}_N^G(e_0(FG)) = |N_{p'}|e_0(FN)$.*

Beweis. Nach 26.5 ist $|G_{p'}|\,\mathrm{Pr}_N^G(e_0(FG)) = \sum_{g\in N_{p'}} \xi_g g$ und $|N_{p'}|e_0(FN) = \sum_{g\in N_{p'}} \xi'_g g$ mit

$$\xi_g = |\{(s,u) \in G_{p'} \times G_p : su = g\}|\,1_F$$

und

$$\xi'_g = |\{(s,u) \in N_{p'} \times N_p : su = g\}|\,1_F$$

für $g \in N_{p'}$. Für $g \in N$, $s \in G_{p'}$, $u \in G_p$ mit $su = g$ ist aber $(sN)(uN) = gN = 1$, also $sN = (uN)^{-1} \in (G/N)_{p'} \cap (G/N)_p = 1$, d.h. $s \in N$ und $u \in N$. Dies zeigt: $\xi_g = \xi'_g$ für $g \in N_{p'}$. □

26.8. Definition. Für jede endliche Gruppe G, $K \in \mathrm{Cl}(G)$ und $g \in K$ nennt man jede p-Sylowgruppe von $C_G(g)$ eine *(p-)Defektgruppe* von K. Wir bezeichnen die Menge aller p-Defektgruppen von K mit $\mathrm{Def}_p(K)$.

Bemerkung. $\mathrm{Def}_p(K)$ ist eine Konjugationsklasse von p-Untergruppen von G. Ist $D \in \mathrm{Def}_p(K)$ und $|D| = p^d$, so nennt man d den *(p-)Defekt* von K.

26.9. Definition. Seien G eine endliche Gruppe und $H, K \leq G$. Wir schreiben $H \leq_G K$, falls ein Element $g \in G$ existiert mit $gHg^{-1} \leq K$. Im Fall $gHg^{-1} = K$ für ein $g \in G$ schreiben wir $H \sim_G K$.

Bemerkung. Die Relation $\leq_G$ ist offenbar reflexiv und transitiv (aber nicht antisymmetrisch). Solche Relationen bezeichnet man als *Quasi-Ordnungen*. Offenbar ist $H \sim_G K$ äquivalent zu $H \leq_G K$ und $K \leq_G H$.

Satz. *Für jede endliche Gruppe G und jede p-Untergruppe Q von G ist*

$$I_Q(FG) := F\{K^+ : K \in \mathrm{Cl}(G),\ R \leq_G Q \textit{ für } R \in \mathrm{Def}_p(K)\}$$

ein Ideal in ZFG.

Beweis. Seien $K, L \in \mathrm{Cl}(G)$, $R \in \mathrm{Def}_p(K)$, $S \in \mathrm{Def}_p(L)$ und $K^+L^+ = \sum_{g \in G} \alpha_g g$ mit $\alpha_g \in F$ für $g \in G$. Dann ist $\alpha_g = |\{(k,l) \in K \times L : kl = g\}|\,1_F$ für $g \in G$. Sei $g \in G$ mit $\alpha_g \neq 0$. Jede p-Sylowgruppe T von $C_G(g)$ operiert auf $\{(k,l) \in K \times L : kl = g\}$ durch Konjugation. Daher ist $0 \neq \alpha_g = |\{(k,l) \in (K \cap C_G(T)) \times (L \cap C_G(T)) : kl = g\}|\,1_F$. Insbesondere ist $K \cap C_G(T) \neq \emptyset \neq L \cap C_G(T)$. Folglich ist $T \leq_G R$ und $T \leq_G S$. □

KAPITEL 27

Defektgruppen von Blöcken

Sei F ein algebraisch abgeschlossener Körper der Charakteristik $p \neq 0$.

27.1. Bemerkung. Seien G eine endliche Gruppe und Q, R p-Untergruppen von G. Dann gilt für die in 26.9 definierten Ideale: $Q \leq_G R \implies I_Q(FG) \subseteq I_R(FG)$. Insbesondere ist $I_Q(FG) = I_R(FG)$ im Fall $Q \sim_G R$. Für jede p-Sylowgruppe P von G ist $I_P(FG) = ZFG$, und $I_1(FG)$ ist das Higman-Ideal $\Gamma(FG)$.

Definition. Seien G eine endliche Gruppe, B ein Block von FG mit Blockidempotent $e = 1_B$ und Q eine p-Untergruppe von G. Man nennt Q eine *Defektgruppe* von B, falls $e \in I_Q(FG)$, aber $e \notin I_R(FG)$ für $R < Q$ ist. Mit $\mathrm{Def}(B)$ bezeichnen wir die Menge aller Defektgruppen von B.

Satz. *Seien G eine endliche Gruppe, B ein Block von FG mit Blockidempotent e, $D \in \mathrm{Def}(B)$ und Q eine p-Untergruppe von G. Dann gilt: $e \in I_Q(FG) \iff D \leq_G Q$. Insbesondere sind je zwei Defektgruppen von B in G konjugiert.*

Beweis.

$\Leftarrow$: Trivial.

$\Rightarrow$: Wegen $e \in I_D(FG)$ ist e eine F-Linearkombination der Element K^+, wobei K alle Konjugationsklassen von G durchläuft, deren Defektgruppen zu Untergruppen von D konjugiert sind. Wegen $e \notin I_R(FG)$ für jede echte Untergruppe R von D ist auch $e \notin \sum_{R<D} I_R(FG)$ nach Rosenbergs Lemma. Schreibt man also $e = \sum_{K \in \mathrm{Cl}(G)} \alpha_K K^+$ mit $\alpha_K \in F$ für $K \in \mathrm{Cl}(G)$, so ist $\alpha_K \neq 0$ für ein $K \in \mathrm{Cl}(G)$ mit Defektgruppe D. Im Fall $e \in I_Q(FG)$ ist also $D \leq_G Q$.

□

27.2. Definition. Für jede endliche Gruppe G und jede p-Untergruppe Q von G setzen wir $I_{<Q} := \sum_{R<Q} I_R(FG)$.

Bemerkung. $I_{<Q}(FG)$ ist ein Ideal in ZFG mit $I_{<Q}(FG) \subseteq I_Q(FG)$. Ist D Defektgruppe eines Blocks B von FG mit Blockidempotent e, so zeigt der Beweis von 27.1: $e \notin I_{<D}(FG)$. Ist $|D| = p^d$, so nennt man d den *Defekt* von B.

Beispiel. Schreibt man $e_0(FG) = \sum_{g \in G} \alpha_g g$ mit $\alpha_g \in F$ für $g \in G$, so ist

$$|G_{p'}|\alpha_1 1_F = |G_{p'}| \, \mathrm{Pr}_1^G(e_0(FG)) = e_0(F1) = 1$$

nach 26.7. Da die p-Defektgruppen der trivialen Konjugationsklasse genau die p-Sylowgruppen von G sind, hat $B_0(FG)$ die p-Sylowgruppen von G als Defektgruppen.

Satz. *Seien G eine endliche Gruppe, Q eine p-Untergruppe von G, $n \in \mathbb{N}_0$ mit $p^n \geq \exp(Q)$ und $x \in JFG + KFG$. Dann ist $x^{p^n} \in I_Q(FG)^\perp$.*

Beweis. Andernfalls gilt mit den üblichen Bezeichnungen:

$$\begin{aligned} 0 \;\neq\; \beta(x^{p^n}, K^+) &= \overline{\beta}(x^{p^n} + KFG, K^+) \\ &= \overline{\beta}(x + KFG, \zeta_n(K^+))^{p^n} = \beta(x, (K^{p^{-n}})^+)^{p^n} \end{aligned}$$

für ein $K \in \mathrm{Cl}(G)$ und ein $R \in \mathrm{Def}_p(K)$ mit $R \leq Q$; insbesondere ist $K^{p^{-n}} \neq \emptyset$. Sei $g \in K^{p^{-n}}$, also $g^{p^n} \in K$. Wegen $g_p \in C_G(g^{p^n})$ ist $g^{p^n} = g_p^{p^n} g_{p'}^{p^n} = g_{p'}^{p^n} \in G_{p'}$, also $K \subseteq G_{p'}$. Sei $S \in \mathrm{Sec}_{p'}(G)$ mit $g_{p'} \in S$.

Für $h \in K^{p^{-n}}$ ist $h^{p^n} \in K$, also $h^{p^n} \sim_G g^{p^n} = g_{p'}^{p^n}$. Daher ist auch $h \in S$. Für $h \in S$ ist umgekehrt $h_{p'} \sim_G g_{p'}$, also $h_p \in C_G(h_{p'}) \sim_G C_G(g_{p'}) = C_G(g_{p'}^{p^n}) = C_G(g^{p^n})$ und damit $h^{p^n} = h_p^{p^n} h_{p'}^{p^n} = h_{p'}^{p^n} \sim_G g_{p'}^{p^n} = g^{p^n} \in K$, also $h \in K^{p^{-n}}$. Dies zeigt: $K^{p^{-n}} = S$. Insbesondere ist $(K^{p^{-n}})^+ \in (JFG + KFG)^\perp$ im Widerspruch zu $\beta(x, (K^{p^{-n}})^+) \neq 0$. $\square$

27.3. Satz. *Seien G eine endliche Gruppe, B ein Block von FG und $D \in \mathrm{Def}(B)$. Dann ist*

$$\exp(D) = \min\{p^n : n \in \mathbb{N},\ x^{p^n} \in KB \text{ für } x \in JB\}.$$

Beispiel. Ist B ein Block von FG mit zyklischer Defektgruppe $D \neq 1$ der Ordnung p^n, so existiert ein $x \in JB$ mit $x^{p^{n-1}} \notin KB$; insbesondere ist $x^{p^{n-1}} \neq 0$ und $(JB)^{p^{n-1}} \neq 0$.

Beweis. Für $x \in JB$ ist $x^{\exp(D)} \in I_D(FG)^\perp$ nach 27.2. Insbesondere gilt für das Blockidempotent e von B mit den üblichen Bezeichnungen:

$$0 = \beta(x^{\exp(D)}, ez) = \beta(x^{\exp(D)}e, z) = \beta(x^{\exp(D)}, z)$$

für $z \in ZFG$. Daher ist $x^{\exp(D)} \in (ZFG)^\perp = KFG$. Wegen $x = xe$ folgt $x^{\exp(D)} \in KFGe = KB$.
Sei also $n \in \mathbb{N}_0$ mit $p^n < \exp(D)$, und sei $e = \sum_{g \in G} \alpha_g g$ mit $\alpha_g \in F$ für $g \in G$. Nach Bemerkung 27.2 existiert also ein $g \in C_G(D)$ mit $\alpha_g \neq 0$. Nach Iizuka-Osima ist $g \in G_{p'}$. Wir wählen ein Element d maximaler Ordnung in D und setzen $h := (g^{-1})^{p^{-n}} \in C_G(D)_{p'}$. Da $d - 1$ nilpotent ist und mit h kommutiert, ist $(d-1)he \in JB + KB$, etwa $(d-1)he = a + b$ mit $a \in JB$ und $b \in KB$. Andererseits ist

$$((d-1)he)^{p^n} = d^{p^n} h^{p^n} e - h^{p^n} e = d^{p^n} g^{-1} e - g^{-1} e = \sum_{y \in G} \alpha_y (d^{p^n} g^{-1} y - g^{-1} y).$$

Im Fall $\alpha_y \neq 0$ ist $y \in G_{p'}$ und $d^{p^n} g^{-1} \in G_{p'}$, also $\beta(\alpha_y, d^{p^n} g^{-1} y, 1) = 0$. Daher ist $0 \neq -\alpha_g = \beta(((d-1)he)^{p^n}, 1)$, also $((d-1)he)^{p^n} \notin KFG$ und

$$a^{p^n} \equiv a^{p^n} + b^{p^n} \equiv (a+b)^{p^n} = ((d-1)he)^{p^n} \not\equiv 0 \pmod{KB},$$

d.h. $a^{p^n} \notin KB$. $\square$

27.4. Satz (R. Brauer)**.** *Seien G eine endliche Gruppe und B ein Block von FG. Dann gilt: B hat Defekt $0 \iff B$ ist eine einfache Algebra.*

Beweis.

$\Rightarrow$: B habe Defekt 0, d.h. Defektgruppe 1. Nach 27.3 ist $JB \subseteq KB$. Daher ist $1_B \in ZB = (KB)^\perp \subseteq (JB)^\perp$, also $(JB)^\perp = B$ und $JB = 0$.

$\Leftarrow$: Ist B einfach, so ist 1 das Minimum in 27.3, d.h. B hat die triviale Defektgruppe 1.

$\square$

27.5. Satz (Tsushima)**.** *Seien G eine endliche Gruppe, $B_1, \ldots, B_r$ die Blöcke vom Defekt 0 in FG und $e_1, \ldots, e_r$ die entsprechenden Blockidempotente. Dann ist $(G_p^+)^2 = e_1 + \ldots + e_r$.*

Beweis. Wegen $G_p \in \mathrm{Sec}_{p'}(G)$ ist $G_p^+ \in (JFG + KFG)^\perp$ und $(G_p^+)^2 \in ((JFG + KFG)^\perp)^2 = B_1 \oplus \ldots \oplus B_r$, also $(G_p^+)^2 = \sum_{i=1}^r (G_p^+)^2 e_i$. Für $i = 1, \ldots, r$ und $K \in \mathrm{Cl}(G)$ ist aber $K^+ e_i \in I_1(FG) \in FG_{p'}$. Andererseits ist $K^+ e_i$ eine F-Linearkombination von Elementen in der gleichen p-Sektion wie K. Daher ist $K^+ e_i = 0$ im Fall $K \subseteq G_p$, ausgenommen den Fall $K = \{1\}$. Folglich ist $G_p^+ e_i = 1 e_i = e_i$ und $(G_p^+)^2 e_i = e_i$. $\square$

27.6. Bemerkung. Seien G eine endliche Gruppe, $K \in \mathrm{Cl}(G)$, $Q \in \mathrm{Def}_p(K)$ und $g \in K$ mit $Q \in C_G(g)$. Sei ferner $N \trianglelefteq G$, $\nu_N : FG \to F[G/N]$ kanonisch und $\overline{K} \in \mathrm{Cl}(G/N)$ mit $gN \in \overline{K}$. Dann ist $\nu_N(K^+) = n\overline{K}^+$ mit

$$\begin{aligned} n \ &= \ \frac{|K|}{|\overline{K}|} = \frac{|G : C_G(g)|}{|G/N : C_{G/N}(gN)|} = \frac{|N| \cdot |C_{G/N}(gN)|}{C_G(g)} \\ &= \ \frac{|N : Q \cap N| \cdot |C_{G/N}(gN) : QN/N|}{|C_G(g) : Q|}. \end{aligned}$$

Wegen $p \nmid |C_G(g) : Q|$ gilt also im Fall $\nu_N(K^+) \neq 0$: $p \nmid |N : Q \cap N|$ und $QN/N \in \mathrm{Def}_p(\overline{K})$. Insbesondere ist also $\nu_N(I_D(FG)) \subseteq I_{DN/N}(F[G/N])$ für jede p-Untergruppe D von G, und $\nu_N(I_D(FG)) = 0$ im Fall $p \mid |N : D \cap N|$.

27.7. Bemerkung. Seien G eine endliche Gruppe, B ein Block von FG mit Blockidempotent e und $D \in \mathrm{Def}(B)$. Seien ferner $N \trianglelefteq G$ und $\nu_N : FG \to F[G/N]$ kanonisch. Dann ist $\nu_N(e)$ ein Idempotent in $ZF[G/N]$, aber nicht unbedingt ein Blockidempotent. Daher ist $\nu_N(e) = e_1 + \ldots + e_r$ mit Blockidempotenten $e_1, \ldots, e_r$ in $F[G/N]$.

Satz. *Mit den obigen Bezeichnungen gilt im Fall $\nu_N(e) \neq 0$:*

(i) *$D \cap N$ ist eine p-Sylowgruppe von N.*
(ii) *Für $i = 1, \ldots, r$ enthält DN/N eine Defektgruppe des Blocks $B_i := F[G/N]e_i$.*
(iii) *Es existiert ein $i \in \{1, \ldots, r\}$ mit $DN/N \in \mathrm{Def}(B_i)$.*

Beweis.

(i) Wegen $\nu_N(e) \neq 0$ ist $\nu_N(I_D(FG)) \neq 0$, also $p \nmid |N : D \cap N|$ nach 27.6.
(ii) Wegen $e \in I_D(FG)$ ist $\nu_N(e) \in \nu_N(I_D(FG)) \subseteq I_{DN/N}(F[G/N])$ nach 27.6, also auch $e_i = e_i\nu_N(e) \in I_{DN/N}(F[G/N])$ für $i = 1, \ldots, r$.
(iii) Ist (iii) nicht erfüllt, so ist $\nu_N(e) \in \nu_N(I_{<D}(FG))$, also $e \in \mathrm{Ker}(\nu_N|ZFG) + I_{<D}(FG)$. Nach Rosenbergs Lemma ist daher $e \in \mathrm{Ker}(\nu_N)$ oder $e \in I_{<D}(FG)$. Widerspruch.

□

27.8. Satz. *Seien G eine endliche Gruppe, Q ein p-Normalteiler von G und B ein Block von FG mit Defektgruppe D. Dann ist $Q \subseteq D$.*

Beweis. Nach Aufgabe 26 liegt das Blockidempotent e von B in $FC_G(Q)$. □

27.9. Satz (Okuyama)**.** *Seien G eine endliche Gruppe, B ein Block von FG und $D \in \mathrm{Def}(B)$. Dann ist $(JZB)^{|D|-1} \subseteq (JFG)^{\perp}$; insbesondere ist $(JZB)^{|D|} = 0$.*

Beweis. Sei G ein Gegenbeispiel minimaler Ordnung. Mit den üblichen Bezeichnungen existieren dann Elemente $x \in JFG$, $z \in (JZB)^{|D|-1}$ mit $0 \neq \beta(x, z)$. Offenbar ist $JFG + KFG = F\{g - gh : g \in G_{p'},\ h \in C_G(g)_p\} + KFG$. Daher existieren Elemente $g \in G_{p'}$, $h \in C_G(g)_p$ mit

$$0 \neq \beta(g - gh, z) = \lambda((g - gh)z) = \lambda(\mathrm{Pr}^G_{C_G(h)}((g - gh)z)) = \lambda((g - gh)\,\mathrm{Br}_{\langle h\rangle}(z)).$$

Bezeichnet man das Blockidempotent von B mit e, so ist $\mathrm{Br}_{\langle h\rangle}(e)$ ein Idempotent in $ZFC_G(h)$, und es existieren Untergruppen $D_1, \ldots, D_r$ von $C_G(h)$ mit $D_i \leq_G D$ für $i = 1, \ldots, r$ und $\mathrm{Br}_{\langle h\rangle}(e) = I_{D_1}(FC_G(h)) + \ldots + I_{D_r}(FC_G(h))$. Wir schreiben $\mathrm{Br}_{\langle h\rangle}(e) = e_1 + \ldots + e_n$ mit Blockidempotenten $e_1, \ldots, e_n$ von $FC_G(h)$. Dann ist $0 \neq (1-h)\,\mathrm{Br}_{\langle h\rangle}(z)e_i$ für ein $i \in \{1, \ldots, n\}$. Der Block $B_i := FC_G(h)e_i$ hat nach Rosenbergs Lemma eine Defektgruppe Q mit $Q \leq_G D$. Ferner ist $\mathrm{Br}_{\langle h\rangle}(z)e_i \in (JZB_i)^{|D|-1}$ und $(1-h)e_i \in JZB_i$. Daher ist auch $C_G(h)$ ein Gegenbeispiel zu unserer Behauptung. Nach Wahl von G ist also $G = C_G(h)$, $B = B_i$, $e = e_i$ und $D = Q$. Jetzt ist $1 \neq N := \langle h\rangle \subseteq Z(G)$, also $N \subseteq D$ nach 27.8. Sei $\nu_N : FG \to F[G/N]$ kanonisch. Dann ist $\mathrm{Ker}(\nu_N) = (\Omega FN)FG = (JFN)FG \subseteq (JZFG)FG$. Daher ist $\nu_N(e)$ ein Blockidempotent in $F[G/N]$, und der Block $F[G/N]\nu_N(e) = \nu_N(B)$ hat nach 27.7 Defektgruppe D/N. Wegen $|G/N| < |G|$ ist $(JZ\nu_N(B))^{|D/N|} = 0$, also auch $\nu_N(JZB)^{|D/N|} = 0$. Folglich ist $(JZB)^{|D/N|} \subseteq \mathrm{Ker}(\nu_N) = (JFN)FG = FG(JFN)$ und $(JZB)^{|D|} = 0$. Widerspruch. □

KAPITEL 28

Blockanzahlen

Sei F ein algebraisch abgeschlossener Körper der Charakteristik $p \neq 0$.

28.1. Satz. *Seien G eine endliche Gruppe und D eine p-Untergruppe von G.*

(i) *Für $K \in \mathrm{Cl}(G)$ mit $D \in \mathrm{Def}_p(K)$ ist dann $K \cap C_G(D) \in \mathrm{Cl}(N_G(D))$ und $D \in \mathrm{Def}_p(K \cap C_G(D))$.*

(ii) *Auf diese Weise erhält man eine Bijektion zwischen der Menge aller Konjugationsklassen von G mit p-Defektgruppe D und der Menge aller Konjugationsklassen von $N_G(D)$ mit p-Defektgruppe D.*

Beweis.

(i) Sei $K \in \mathrm{Cl}(G)$ mit $D \in \mathrm{Def}_p(K)$ und $x \in K$ mit $D \subseteq C_G(x)$, also $x \in K \cap C_G(D)$. Insbesondere ist $K \cap C_G(D) \neq \emptyset$. Ist auch $y \in K \cap C_G(D)$, so existiert ein $g \in G$ mit $gxg^{-1} = y$. Folglich ist gDg^{-1} eine p-Sylowgruppe von $gC_G(x)g^{-1} = C_G(gxg^{-1}) = C_G(y)$. Wegen $D \subseteq C_G(y)$ existiert ein $h \in C_G(y)$ mit $hgDg^{-1}h^{-1} = D$. Dann ist $hg \in N_G(D)$ und $y = hyh^{-1} = hgxg^{-1}h^{-1}$.
Für $z \in N_G(D)$ ist andererseits $zxz^{-1} \in K \cap C_G(D)$, d.h. $K \cap C_G(D) \in \mathrm{Cl}(N_G(D))$ und $D \in \mathrm{Def}_p(K \cap C_G(D))$.

(ii) Sei umgekehrt $L \in \mathrm{Cl}(N_G(D))$ und $D \in \mathrm{Def}_p(L)$. Nach (i) ist $L \cap C_G(D) \in \mathrm{Cl}(N_G(D))$, also $L = L \cap C_G(D) \subseteq C_G(D)$. Für $x \in L$ ist D eine p-Sylowgruppe von $C_G(x) \cap N_G(D) = N_{C_G(x)}(D)$, also auch von $C_G(x)$ (Gruppentheorie). Ist $K \in \mathrm{Cl}(G)$ mit $L \subseteq K$, so ist also $D \in \mathrm{Def}_p(K)$. Nach (i) ist $L = K \cap C_G(D)$.

□

28.2. Satz (Brauers I. Hauptsatz)**.** *Seien G eine endliche Gruppe und D eine p-Untergruppe von G.*

(i) *Für jeden Block B von FG mit Blockidempotent e und Defektgruppe D ist $f := \mathrm{Br}_D(e)$ ein Blockidempotent in $FN_G(D)$, und der Block $FN_G(D)f$ hat auch Defektgruppe D.*

(ii) *Auf diese Weise erhält man eine Bijektion zwischen der Menge aller Blöcke von FG mit Defektgruppe D und der Menge aller Blöcke von $FN_G(D)$ mit Defektgruppe D.*

Beweis.

(ii) Sei b ein Block von $FN_G(D)$ mit Blockidempotent f und Defektgruppe D. Nach Aufgabe 26 ist $f \in FC_G(D)$. Daher ist f eine F-Linearkombination von Klassensummen von Konjugationsklassen in $N_G(D)$ mit Defektgruppe D. Nach `[fehlt noch]`

(i) Sei umgekehrt B ein Block von FG mit Defektgruppe D und Blockidempotent e. Dann ist $\mathrm{Br}_D(e)$ ein Idempotent in $ZFN_G(D)$ mit $\mathrm{Br}_D(e) \in I_D(FN_G(D))$. Nach 28.1 ist $\mathrm{Br}_D(e) \neq 0$. Wir schreiben $\mathrm{Br}_D(e) = f_1 + \ldots + f_r$ mit verschiedenen Blockidempotenten $f_1, \ldots, f_r$ in $FN_G(D)$. Für $i = 1, \ldots, r$ hat der Block $b_i := FN_G(D)f_i$ wegen $f_i \in I_D(FN_G(D))$ eine Untergruppe von D als Defektgruppe. Wegen $D \trianglelefteq N_G(D)$ haben $b_1, \ldots, b_r$ alle Defektgruppe D. Nach dem ersten Teil des Beweises existiert ein Block B_i von FG mit Defektgruppe D und Blockidempotent e_i, so daß $f_i = \mathrm{Br}_D(e_i)$ ist. Wegen $\mathrm{Br}_D(ee_i) = \mathrm{Br}_D(e)\,\mathrm{Br}_D(e_i) = \mathrm{Br}_D(e)f_i = f_i \neq 0$ ist $ee_i \neq 0$, also $e = e_i$. Daher ist $r = 1$, d.h. $\mathrm{Br}_D(e) = f_1$ ist ein Blockidempotent in $FN_G(D)$, und der entsprechende Block b_1 hat Defektgruppe D.
Sei B' ein weiterer Block von FG mit Defektgruppe D und Blockidempotent e'. Im Fall $\mathrm{Br}_D(e) = \mathrm{Br}_D(e')$ ist $0 \neq \mathrm{Br}_D(e)\,\mathrm{Br}_D(e') = \mathrm{Br}_D(ee')$, also $ee' \neq 0$ und damit $e = e'$.

□

Definition. Die oben definierte Bijektion nennt man *Brauer-Korrespondenz.*

Bemerkung. Broué vermutet, daß ein Block B von FG mit abelscher Defektgruppe D und sein Brauer-Korrespondent b in $FN_G(D)$ die gleiche Anzahl einfacher Moduln haben, und daß $ZB \cong Zb$ gilt.

28.3. Satz (Willems). *Seien G eine endliche Gruppe, $N \trianglelefteq G$ und D eine p-Untergruppe von G mit der Eigenschaft, daß $D \cap N$ eine p-Sylowgruppe von N und $C_G(D \cap N) \subseteq N$ ist. Dann stimmt die Anzahl der Blöcke von FG mit Defektgruppe D mit der Anzahl der in N enthaltenen p'-Konjugationsklassen von G mit Defektgruppe D überein.*

Beweis. Nach 28.2 stimmt die Anzahl der Blöcke von FG mit Defektgruppe D mit der Anzahl der Blöcke von $FN_G(D)$ mit Defektgruppe D überein. Nach 28.1 erhält man andererseits durch $K \mapsto K \cap C_G(D)$ eine Bijektion zwischen der Menge der (p'-)Konjugationsklassen von G mit Defektgruppe D und der Menge der (p'-)Konjugationsklassen von $N_G(D)$ mit Defektgruppe D. Dabei gilt offenbar: $K \subseteq N \iff K \cap C_G(D) \subseteq N \cap N_G(D)$. Ferner ist $N \cap N_G(D) \trianglelefteq N_G(D)$, D ist eine p-Untergruppe von $N_G(D)$, $D \cap N \cap N_G(D) = D \cap N$ ist eine p-Sylowgruppe von $N \cap N_G(D)$ und $C_{N_G(D)}(D \cap N) \subseteq N \cap N_G(D)$. Daher kann man G durch $N_G(D)$ ersetzen und damit $D \trianglelefteq G$ annehmen.
Nach Aufgabe 26 liegen dann die Blockidempotente von FG in $FC_G(D) \subseteq FC_G(D \cap N) \subseteq FN$ und damit in $FC_N(D)$. Offensichtlich ist D eine p-Sylowgruppe von $DC_N(D)$, also $DC_N(D) = D \times S$ mit $S := O_{p'}(C_N(D)) \trianglelefteq G$ nach Schur-Zassenhaus. Daher liegen die Blockidempotente von FG mit Defektgruppe D in $I_D(FG) \cap FS$ nach Iizuka-Osima. Für die Anzahl r dieser Blockidempotente gilt also: $r \leq \dim I_D(FG) \cap FS$.
Jede in N enthaltene p'-Konjugationsklasse von G mit Defektgruppe D liegt offenbar in S. Umgekehrt ist jede in S enthaltene Konjugationsklasse von G mit p-Defektgruppe $Q \leq_G D$ eine p'-Konjugationsklasse mit Defektgruppe D. Daher bilden die Klassensummen von p'-Konjugationsklassen von G in N mit p-Defektgruppe D eine Basis von $I_D(FG) \cap FS$. Insbesondere stimmt $\dim I_D(FG) \cap FS$ mit der Anzahl dieser Konjugationsklassen überein. Wegen $p \not| \, |S|$ sind FS und ZFS halbeinfache Algebren. Daher sind auch die Unteralgebra $ZFG \cap FS$ und das Ideal $I_D(FG) \cap FS$ halbeinfache Algebren. Folglich ist $I_D(FG) \cap FS = Fe_1 \oplus \ldots \oplus Fe_s$ mit paarweise orthogonalen Idempotenten $e_1, \ldots, e_s$. Daher enthält $I_D(FG)$ mindestens s verschiedene Blockidempotente von FG. Die entsprechenden Blöcke haben alle Defektgruppe D. Daher ist $s \leq r$. $\square$

28.4. Satz (Brauer-Nesbitt). *Seien G eine endliche Gruppe und D eine p-Sylowgruppe von G. Dann stimmt die Anzahl der Blöcke von FG mit Defektgruppe D mit der Anzahl der p'-Konjugationsklassen mit p-Defektgruppe D überein.*

Beweis. Setze $N := G$ in 28.3. $\square$

Bemerkung. Man sagt, die obigen Blöcke haben *vollen* oder *maximalen* Defekt.

28.5. Satz. *Für jede endliche Gruppe G und jede p-Untergruppe D von G ist $\varepsilon_G(I_D(FG)) = \sum_e Fe$, wobei e die Blockidempotente von FG durchläuft, für die der Block FGe eine Untergruppe von D als Defektgruppe hat.*

Beweis. Offenbar ist $I_D(FG) = I_D(FG)1 = \sum_e I_D(FG)e$, wobei e alle Idempotente von FG durchläuft. Hat der Block FGe eine Defektgruppe Q mit $Q \not\leq_G D$, so ist $e \notin I_D(FG)$. Daher ist $I_D(FG)e$ ein echtes Ideal in der lokalen Algebra $ZFGe$, also $I_D(FG)e \subseteq JZFGe$ und damit $\varepsilon_G(I_D(FG)e) = 0$. Hat der Block FGe eine Defektgruppe Q mit $Q \leq_G D$, so ist $e \in I_D(FG)$, also $e = \varepsilon_G(e) \in \varepsilon_G(I_D(FG)e)$. Andererseits ist $\varepsilon_G(I_D(FG)e) \subseteq \varepsilon_G(ZFG)\varepsilon_G(e) = \varepsilon_G(ZFG)e = Fe$. $\square$

Bemerkung. Es ist also $\varepsilon_G(I_D(FG)) + I_{<D}(FG)/I_{<D}(FG) = \sum_e F(e + I_{<D}(FG))$, wobei e alle Blockidempotente von FG durchläuft, für die FGe Defektgruppe D hat. Da diese Blockidempotente paarweise orthogonal sind, sind ihre Bilder in $ZFG/I_{<D}(FG)$ linear unabhängig über F. Daher ist $\dim \varepsilon_G(I_D(FG)) + I_{<D}(FG)/I_{<D}(FG)$ die Anzahl der Blöcke von FG mit Defektgruppe D. Wegen $\varepsilon_G(I_D(FG)) \subseteq I_{<D}(FG)$ ist ferner $\varepsilon_G(I_D(FG)) + I_{<D}(FG)/I_{<D}(FG) = \varepsilon_G(V_D(FG)) + I_{<D}(FG)/I_{<D}(FG)$, wobei $V_D(FG)$ den von allen Klassensummen von p'-Konjugationsklassen von G mit Defektgruppe D aufgespannten F-Vektorraum bezeichnet.

Im folgenden werden wir $\varepsilon_G(V_D(FG)) + I_{<D}(FG)/I_{<D}(FG)$ explizit berechnen und so eine Formel für die Anzahl der Blöcke von FG mit Defektgruppe D erhalten.

28.6. Definition. Für jede endliche Gruppe G bezeichnen wir mit $\mathrm{Syl}_p(G)$ die Menge der p-Sylowgruppen von G.

Satz. *Für jede endliche Gruppe G und jede p-Untergruppe Q von G ist $|\{P \in \mathrm{Syl}_p(G) : Q \subseteq P\}| \equiv 1 \pmod p$.*

Beweis. Q operiert auf $\mathrm{Syl}_p(G)$ durch Konjugation. Nach Sylow gilt also:

$$1 \equiv |\mathrm{Syl}_p(G)| \equiv |\{P \in \mathrm{Syl}_p(G) : Q \subseteq N_G(P)\}| \equiv |\{P \in \mathrm{Syl}_p(G) : Q \subseteq P\}| \pmod p.$$

□

Bemerkung. Es ist also $G_p^+ = \sum_{P \in \mathrm{Syl}_p(G)} P^+$; denn in der Summe kommt jedes $u \in G_p$ mit Vielfachheit $|\{P \in \mathrm{Syl}_p(G) : u \in P\}| \equiv 1 \pmod p$ vor.

28.7. Satz. *Seien G eine endliche Gruppe, $K \in \mathrm{Cl}(G)$, $P \in \mathrm{Syl}_p(G)$ und $K^+G_p^+ = \sum_{C \in \mathrm{Cl}(G)} \alpha_C C^+$ mit $\alpha_C \in F$ für $C \in \mathrm{Cl}(G)$. Dann ist $\alpha_C = n_C 1_F$ mit*

$$n_C = \frac{|\mathrm{Syl}_p(G)|}{|C|} |\{(c,k) \in C \times K : c^{-1}k \in P\}| \in \mathbb{N}_0$$

für $C \in \mathrm{Cl}(G)$.

Beweis. Für $C \in \mathrm{Cl}(G)$ und $c_0 \in C$ gilt nach 28.6: $\alpha_C = n_C 1_F$ mit

$$\begin{aligned} n_C &= |\{(k,Q,u) : k \in K,\ Q \in \mathrm{Syl}_p(G),\ u \in Q,\ ku = c_0\}| \\ &= \frac{1}{|C|} |\{(k,Q,u) : k \in K,\ Q \in \mathrm{Syl}_p(G),\ u \in Q,\ ku \in C\}| \\ &= \frac{1}{|C|} |\{(c,k,Q) : c \in C,\ k \in K,\ Q \in \mathrm{Syl}_p(G),\ c^{-1}k \in Q\}| \\ &= \frac{|\mathrm{Syl}_p(G)|}{|C|} |\{(c,k) \in C \times K : c^{-1}k \in P\}| \end{aligned}$$

□

Bemerkung. Für $n \in \mathbb{N}$ bezeichnen wir mit n_p die höchste p-Potenz, die n teilt, und setzen $n_{p'} := n/n_p$.

28.8. Satz. *Seien G eine endliche Gruppe, $K \in \mathrm{Cl}(G)$, $D \in \mathrm{Def}_p(G)$, $P \in \mathrm{Syl}_p(G)$ und $K^+G_p^+ = \sum_{C \in \mathrm{Cl}(G)} \alpha_C C^+$ mit $\alpha_C \in F$ für $C \in \mathrm{Cl}(G)$. Dann ist*

$$|C|_{p'}\, \alpha_C = \sum_{PgP \in P\backslash G/P} n(g,C)n(g,K)1_F$$

für $C \in \mathrm{Cl}(G)$ mit $D \in \mathrm{Def}_p(G)$, wobei $n(g,C) := |\{c \in gP \cap C : P \cap gPg^{-1} \in \mathrm{Syl}_p(C_G(c))\}|$ für $g \in G$ ist.

Beweis. Sei $C \in \mathrm{Cl}(G)$ mit $D \in \mathrm{Def}_p(C)$. Dann ist

$$\{(c,k) \in C \times K : c^{-1}k \in P\} = \dot{\bigcup_{gP \in G/P}} (C \cap gP) \times (K \cap gP).$$

Für $u \in P$ ist dabei $|C \cap ugP| = |C \cap ugPu^{-1}| = |u(C \cap gP)u^{-1}| = |C \cap gP|$. Daher ist

$$|\{(c,k) \in C \times K : c^{-1}k \in P\}| = \sum_{PgP \in P\backslash G/P} |P : P \cap gPg^{-1}| \cdot |C \cap gP| \cdot |K \cap gP|.$$

Sei $g \in G$. Wegen $(gPg^{-1})(gP)P = gP$ operiert $P \cap gPg^{-1}$ durch Konjugation auf $C \cap gP$. Die Bahn eines Elementes $c \in C \cap gP$ hat dabei wegen $P \cap gPg^{-1} \cap C_G(c) = C_P(c) \cap cPc^{-1} = C_P(c)$ die Länge $|P \cap gPg^{-1} : C_P(c)|$. Nun ist aber $|P : P \cap gPg^{-1}| \cdot |P \cap gPg^{-1} : C_P(c)| \cdot |P \cap gPg^{-1} : C_P(k)|$ durch eine höhere p-Potenz teilbar als $|C|_p$ außer im Fall $C_P(c) \in \mathrm{Syl}_p(C_G(c))$ und $P \cap gPg^{-1} = C_P(k)$. In diesem Fall ist aber

$$|P \cap gPg^{-1}| = |C_P(k)| \leq |D| = |C_P(c)| \leq |P \cap gPg^{-1}|$$

und damit $P \cap gPg^{-1} = C_P(c) \in \mathrm{Syl}_p(C_G(c))$ und $P \cap gPg^{-1} = C_P(k) \in \mathrm{Syl}_p(C_G(k))$. Nach 28.7 ist also

$$\begin{aligned} |C|_{p'}\alpha_C \quad &= \sum_{PgP \in P\backslash G/P} |\{(c,k) \in (C \cap gP) \times (K \cap gP) : \\ &\qquad P \cap gPg^{-1} \in \mathrm{Syl}_p(C_G(c)) \cap \mathrm{Syl}_p(C_G(k))\}| \, 1_F. \end{aligned}$$

□

Bemerkung. Für jede p'-Konjugationsklasse K von G und $D \in \mathrm{Def}_p(K)$ ist

$$\varepsilon_G(K^+) = \mathrm{Pr}_{G_{p'}}(K^+G_P^+) \equiv \sum_{\substack{C \in \mathrm{Cl}(G),\ C \subseteq G_{p'} \\ D \in \mathrm{Def}_p(C)}} \alpha_C C^+ \pmod{I_{<D}(FG)}$$

mit den oben berechneten α_C. Da die entsprechenden Elemente $C^+ + I_{<D}(FG)$ linear unabhängig über F sind, erhalten wir:

28.9. Satz (Robinson)**.** *Seien G eine endliche Gruppe, D eine p-Untergruppe von G, $P \in \mathrm{Syl}_p(G)$, $K_1, \ldots, K_r$ die p'-Konjugationsklassen von G mit Defektgruppe D und $g_1, \ldots, g_s$ ein Repräsentantensystem für $P\backslash G/P$. Ferner sei $N = (n_{ij})$ mit*

$$n_{ij} := |\{k \in K_i \cap g_jP : P \cap g_jPg_j^{-1} \in \mathrm{Syl}_p(C_G(k))\}| \, 1_F$$

für $i = 1, \ldots, r,\ j = 1, \ldots, s$. Dann ist der Rang von NN^T die Anzahl der Blöcke von FG mit Defektgruppe D.

28.10. Satz (Green)**.** *Seien G eine endliche Gruppe, B ein Block von FG und $D \in \mathrm{Def}_p(B)$. Dann existiert ein Element $c \in C_G(D)_{p'}$ und eine p-Sylowgruppe P von G mit $D = P \cap cPc^{-1}$.*

Beweis. Die Matrix N aus 28.9 kann nicht 0 sein. Es existiert also ein Element x in einer p'-Konjugationsklasse von G mit Defektgruppe D, so daß $P \cap xPx^{-1} \in \mathrm{Syl}_p(C_G(x))$ ist. Für ein $y \in G$ ist also

$$D = y(P \cap xPx^{-1})y^{-1} = yPy^{-1} \cap yxy^{-1} \cdot yPy^{-1} \cdot yx^{-1}y^{-1} \in \mathrm{Syl}_p(C_G(yxy^{-1})).$$

□

KAPITEL 29

Graduierte Algebren

Sei F ein algebraisch abgeschlossener Körper.

29.1. Definition. Sei G eine Gruppe. Eine *G-graduierte F-Algebra* ist ein Paar $(A, (A_g)_{g\in G})$, das aus einer endlich-dimensionalen F-Algebra A und einer Familie $(A_g)_{g\in G}$ von F-Untervektorräumen A_g von A mit $A = \bigoplus_{g\in G} A_g$ und $A_g A_h \subseteq A_{gh}$ für $g, h \in G$ besteht. Dabei ist $A_g A_h := F\{a_g b_h : a_g \in A_g,\ b_h \in A_h\}$. Statt $(A, (A_g)_{g\in G})$ schreiben wir meist $A = \bigoplus_{g\in G} A_g$. Für $g \in G$ nennt man A_g die *g-Komponente* von A.

Beispiel. Die Gruppenalgebra $A = FG$ ist eine G-graduierte F-Algebra mit $A_g = Fg$ für $g \in G$. Allgemeiner ist $A = FG$ für jeden Normalteiler N von G eine G/N-graduierte F-Algebra mit $A_{gN} = FNg$ für $g \in G$.

Bemerkung. Jedes Element a in einer G-graduierten F-Algebra $A = \bigoplus_{g\in G} A_g$ läßt sich in der Form $a = \sum_{g\in G} a_g$ mit eindeutig bestimmten Elementen $a_g \in A_g$ schreiben. Für $g \in G$ bezeichnen wir a_g als *g-Komponente* von a. Wir nennen a *graduiert* oder *homogen*, falls $a \in A_g$ für ein $g \in G$ ist.

Satz. *Für jede endliche Gruppe G und jede G-graduierte F-Algebra $A = \bigoplus_{g\in G} A_g$ ist A_1 eine unitäre Teilalgebra von A.*

Beweis. Wegen $A_1 A_1 \subseteq A_{1\cdot 1}$ genügt es zu zeigen, daß $1_A \in A_1$. Dazu schreiben wir $1_A = \sum_{g\in G} e_g$ mit $e_g \in A_g$ für $g \in G$. Für $h \in G$ und $x \in A_h$ ist dann $x = 1_A x = \sum_{g\in G} e_g x$ mit $e_g x \in A_g A_h \subseteq A_{gh}$ für $g \in G$. Daher ist $x = e_1 x$. Wegen $A = \bigoplus_{h\in G} A_h$ ist also $e_1 a = a$ für $a \in A$. Analog ist $a e_1 = a$ für $a \in A$, also $1_A = e_1 \in A_1$. □

29.2. Satz. *Seien G eine endliche Gruppe und $A = \bigoplus_{g\in G} A_g$ eine G-graduierte F-Algebra. Für einen Untervektorraum V von A sind dann äquivalent:*

(1) $V = \bigoplus_{g\in G}(V \cap A_g)$.
(2) *Für $v \in V$ und $g \in G$ gehört auch die g-Komponente von v zu V.*
(3) *V wird von homogenen Elementen aufgespannt.*

Beweis.

(1)⇒(2): Sei $V = \bigoplus_{g\in G}(V \cap A_g)$ und $v \in V$. Dann ist $v = \sum_{g\in G} v_g$ mit $v_g \in V \cap A_g$ für $g \in G$. Da v_g für $g \in G$ die g-Komponente von v ist, gilt (2).

(2)⇒(3): Sei (2) erfüllt, so wird V offenbar von allen homogenen Elementen in V aufgespannt.

(3)⇒(1): Sei S die Menge homogener Elemente in A, die V aufspannt, sei $v \in V$, und sei $v = \sum_{s\in S} \alpha_s s$ mit $\alpha_s \in F$ für $s \in S$. Für $g \in G$ ist dann $v_g := \sum_{s\in S\cap A_g} \alpha_s s$ die g-Komponente von v, und diese liegt offenbar in $V \cap A_g$. Daher ist $V \subseteq \bigoplus_{g\in G}(V \cap A_g)$, und die andere Inklusion ist trivial.

□

Bemerkung. Gegebenenfalls nennt man V einen *(G-)graduierten* oder *homogenen* Untervektorraum von A. Auf diese Weise sind z.B. G-graduierte Unteralgebren und G-graduierte Ideale von A definiert. Jede G-graduierte Unteralgebra B von $A = \bigoplus_{g\in G} A_g$ kann man offenbar selbst als G-graduierte Algebra mit g-Komponente $B_g := B \cap A_g$ für $g \in G$ auffassen. Analog wird für jedes G-graduierte Ideal I von A die Restklassenalgebra A/I zu einer G-graduierten F-Algebra mit g-Komponente $(A/I)_g := A_g + I/I$ für

$g \in G$; ist nämlich $\sum_{g\in G} a_g + I = 0$ mit $a_g \in A_g$ für $g \in G$, so ist $\sum_{g\in G} a_g \in I$, also auch $a_g \in I$, d.h. $a_g + I = 0$ für $g \in G$.

Beispiel.

(i) Für jedes Idempotent e in A_1 ist $eAe = \bigoplus_{g\in G} eA_ge$ eine graduierte Unteralgebra von A; denn für $g \in G$ ist $eA_ge \subseteq A_1A_gA_1 \subseteq A_g$ und daher $eA_ge = A_g \cap eAe$.

(ii) Für jede Teilmenge X von A_1 ist $C_A(X) = \bigoplus_{g\in G} C_{A_g}(X)$ eine graduierte unitäre Unteralgebra von A; ist nämlich $c \in C_A(X)$ und $c = \sum_{g\in G} c_g$ mit $c_g \in A_g$ für $g \in G$, so ist $\sum_{g\in G} c_gx = cx = xc = \sum_{g\in G} xc_g$ mit $c_gx, xc_g \in A_g$ für $g \in G$, $x \in X$. Daher ist $c_gx = xc_g$ für $x \in X$, $g \in G$, also $c_g \in C_A(x) \cap A_g := C_{A_g}(X)$ für $g \in G$. Insbesondere ist also $C_A(A_1)$ eine G-graduierte F-Algebra mit 1-Komponente $C_A(A_1) \cap A_1 = ZA_1$.

29.3. Satz. *Seien G eine endliche Gruppe, $A = \bigoplus_{g\in G} A_g$ eine G-graduierte F-Algebra, $h \in G$ und $u \in A_h \cap UA$. Dann ist $u^{-1} \in A_{h^{-1}}$.*

Beweis. Sei $u^{-1} = \sum_{g\in G} v_g$ mit $v_g \in A_g$ für $g \in G$. Dann ist $1 = uu^{-1} = \sum_{g\in G} uv_g$ mit $uv_g \in A_hA_g \subseteq A_{hg}$ für $g \in G$. Wegen $1 \in A_1$ ist also $1 = uv_{h^{-1}}$ und analog $v_{h^{-1}}u = 1$. Daher ist $u^{-1} = v_{h^{-1}} \in A_{h^{-1}}$. □

Bemerkung. Die graduierten Einheiten von A bilden also eine Untergruppe $U_G(A)$ von UA.

29.4. Definition. Seien G eine endliche Gruppe und $A = \bigoplus_{g\in G} A_g$ eine G-graduierte F-Algebra. Enthält jede g-Komponente A_g von A eine graduierte Einheit u_g, so nennt man $A = \bigoplus_{g\in G} A_g$ ein *verschränktes Produkt* (von G mit A_1).

Bemerkung. Gegebenenfalls ist $A_g = A_gu_g^{-1}u_g \subseteq A_1u_g \subseteq A_g$ nach 29.3, also $A_g = A_1u_g$ und analog $A_g = u_gA_1$ für $g \in G$; insbesondere ist $A_{gh} = A_1u_gu_h \subseteq A_gA_h \subseteq A_{gh}$, also $A_gA_h = A_{gh}$ für $g, h \in G$.

Beispiel. Für jeden Normalteiler N von G ist FG ein verschränktes Produkt von G/N mit FN.

29.5. Definition. Seien G eine endliche Gruppe und $A = \bigoplus_{g\in G} A_g$ ein verschränktes Produkt mit $\dim A_g = 1$ für $g \in G$. Dann nennt man $A = \bigoplus_{g\in G} A_g$ eine *verschränkte Gruppenalgebra* von G über F.

Beispiel. Die Gruppenalgebra FG kann man auch als verschränkte Gruppenalgebra von G über F auffassen.

Bemerkung. Seien G eine endliche Gruppe, $A = \bigoplus_{g\in G} A_g$ eine verschränkte Gruppenalgebra von G über F und $u_g \in A_g \cap UA$ für $g \in G$. Für $g, h \in G$ ist dann $u_gu_h \in Fu_{gh}$, also $u_gu_h = \alpha(g,h)u_{gh}$ für ein $\alpha(g,h) \in F^\times$. Wegen

$$u_gu_hu_k = \alpha(g,h)u_{gh}u_k = \alpha(g,h)\alpha(gh,k)u_{ghk}$$

und

$$u_gu_hu_k = u_g\alpha(h,k)u_{hk} = \alpha(h,k)\alpha(g,hk)u_{ghk}$$

ist

$$\alpha(g,h)\alpha(gh,k) = \alpha(h,k)\alpha(g,hk)$$

für $g, h, k \in G$. Daher ist die Abbildung $G \times G \to F^\times$, $(g,h) \mapsto \alpha(g,h)$ ein Faktorensystem (vgl. Darstellungstheorie I), d.h. $\alpha \in Z^2(G, F^\times)$. Für jedes $\varphi(g) \in F^\times$ ist $v_g := \varphi(g)u_g \in A_g \cap UA$ für $g \in G$ (und jede graduierte Einheit v_g von A in A_g entsteht so). Dann ist

$$v_gv_h = \varphi(g)u_g\varphi(h)u_h = \varphi(g)\varphi(h)\alpha(g,h)u_{gh} = \varphi(g)\varphi(h)\alpha(g,h)\varphi(gh)^{-1}v_{gh}$$

für $g, h \in G$, d.h. man erhält ein Faktorensystem, das sich von α durch ein prinzipales Faktorensystem unterscheidet. Daher bestimmt jede verschränkte Gruppenalgebra $A = \bigoplus_{g\in G} A_g$ genau ein Element $\overline{\alpha} = \alpha B^2(G, F^\times) \in H^2(G, F^\times)$.

29.6. Definition. Seien G eine endliche Gruppe, $A = \bigoplus_{g\in G} A_g$, $B = \bigoplus_{g\in G} B_g$ G-graduierte F-Algebren und $\varphi : A \to B$ ein Homomorphismus von Algebren mit $\varphi(A_g) \subseteq B_g$ für $g \in G$. Dann nennt man φ *(G-)graduiert* oder *homogen*.

Satz. *Für eine endliche Gruppe G und eine verschränkte Gruppenalgebra $A = \bigoplus_{g\in G} A_g$ von G über F sind äquivalent:*

(1) *A ist isomorph zu FG als G-graduierte F-Algebra.*
(2) *A ist isomorph zu FG als abstrakte F-Algebra.*
(3) *Das durch A bestimmte Element $\overline{\alpha}$ in $H^2(G, F^\times)$ verschwindet.*

Beweis. Seien $u_g \in A_g \cap UA$ für $g \in G$ und $\alpha(g,h) \in F^\times$ mit $u_g u_h = \alpha(g,h)u_{gh}$ für $g,h \in G$.

(1)⇒(2): Trivial.

(2)⇒(3): Sei $\Phi : A \to FG$ ein Isomorphismus von F-Algebren und $\nu : FG \to F$ die Augmentationsabbildung. Dann ist

$$\nu(\Phi(u_g)) \cdot \nu(\Phi(u_h)) = \alpha(g,h)\nu(\Phi(u_{gh}))$$

für $g,h \in G$. Folglich ist α ein prinzipales Faktorensystem.

(3)⇒(1): Sei $\varphi(g) \in F^\times$ mit $\alpha(g,h) = \varphi(g)\varphi(h)\varphi(gh)^{-1}$ für $g,h \in G$. Dann ist $v_g = \varphi(g)^{-1}u_g \in A_g \cap UA$ und $v_g v_h = v_{gh}$ für $g,h \in G$. Wegen $a = \bigoplus_{g\in G} Fv_g$ gibt es einen graduierten Isomorphismus $\Phi : FG \to A$ mit $\Phi(g) = v_g$ für $g \in G$.

□

Bemerkung. Man kann zeigen, daß die in der Darstellungtheorie I betrachteten projektiven Darstellungen den Darstellungen von verschränkten Gruppenalgebren ebenso entsprechen wie lineare Darstellungen den Darstellungen von (gewöhnlichen) Gruppenalgebren. Näher gehen wir darauf nicht ein.

29.7. Satz (Green). *Seien* $\operatorname{char} F = p > 0$*, G eine endliche p-Gruppe und $A = \bigoplus_{g\in G} A_g$ ein verschränktes Produkt. Ist A_1 eine lokale Algebra, so auch A.*

Beweis. Für $g \in G$ und $u_g \in A_g \cap UA$ ist die Abbildung $A_1 \to A_1,\ x \mapsto u_g x u_g^{-1}$ ein Automorphismus von A_1. Daher ist $u_g J(A_1) u_g^{-1} = J(A_1)$, d.h. $u_g J(A_1) = J(A_1)u_g$. Folglich ist $AJ(A_1) = J(A_1)A$ ein nilpotentes Ideal in A. Wegen

$$J(A_1)A = \bigoplus_{g\in G} J(A_1)u_g \subseteq \bigoplus_{g\in G}(J(A_1)A \cap A_g) \subseteq J(A_1)A$$

ist $J(A_1)A$ ein graduiertes Ideal in A, d.h. $A/J(A_1)A$ ist eine G-graduierte F-Algebra mit g-Komponente $A_g + J(A_1)A/J(A_1)A$ für $g \in G$. Offenbar ist $A/J(A_1)A$ auch ein verschränktes Produkt, und es ist $A_1 + J(A_1)A/J(A_1)A \cong A_1/A_1 \cap J(A_1)A = A_1/J(A_1) \cong F$. Es genügt zu zeigen, daß $A/J(A_1)A$ lokal ist. Daher können wir A durch $A/J(A_1)A$ ersetzen und folglich $A_1 \cong F$ annehmen. Für $g \in G$ ist dann $A_g = A_1 u_g = F1u_g = Fu_g$, d.h. A ist eine verschränkte Gruppenalgebra von G über F. Nach 12.6 ist $H^2(G, F^\times) = 1$. Nach 29.6 ist also $A \cong FG$. Damit ist A lokal. □

29.8. Satz. *Seien G eine endliche Gruppe und $A = \bigoplus_{g\in G} A_g$ ein verschränktes Produkt. Ist A_1 eine einfache F-Algebra, so existiert ein Isomorphismus*

$$\Phi : C_A(A_1) \otimes_F A_1 \to A$$

mit $\Phi(c \otimes x) = cx$ für $c \in C_A(A_1),\ x \in A_1$, und $C_A(A_1)$ ist eine verschränkte Gruppenalgebra von G über F.

Beweis. Die erste Aussage folgt aus Aufgabe 22, und nach 29.2 ist $C_A(A_1)$ eine graduierte Unteralgebra von A. Für $g \in G$ und $u_g \in A_g \cap UA$ ist die Abbildung $A_1 \to A_1,\ x \mapsto u_g x u_g^{-1}$ ein Automorphismus von A_1. Nach Aufgabe 27 ist dies ein innerer Automorphismus von A_1, d.h. es existiert ein Element $a_g \in U(A_1)$ mit $u_g x u_g^{-1} = a_g x a_g^{-1}$ für $x \in A_1$. Dann ist $v_g := a_g^{-1}u_g \in A_g \cap UA \cap C_A(A_1)$. Folglich ist $C_A(A_1)$ ein verschränktes Produkt mit 1-Komponente $ZA_1 \cong F$. Daher ist $C_A(A_1) = \bigoplus_{g\in G} ZA_1 v_g = \bigoplus_{g\in G} Fv_g$ eine verschränkte Gruppenalgebra von G über F. □

Bemerkung. Viele Aussagen über Gruppenalgebren lassen sich (in geeignet modifizierter Form) auf verschränkte Gruppenalgebren, verschränkte Produkte oder sogar graduierte Algebren verallgemeinern. Darauf können wir hier nicht eingehen. Wir benutzen die Begriffe nur dazu, eine Gruppenalgebra selbst besser zu verstehen.

29.9. Satz. *Seien* $\operatorname{char} F = p > 0$, D *eine endliche* p*-Gruppe und* G *eine* p'*-Untergruppe von* $\operatorname{Aut}(D)$. *Ferner sei* $A = \bigoplus_{g\in G} A_g$ *ein verschränktes Produkt mit* $A_1 = FD$. *Schließlich existiere zu jedem* $g \in G$ *ein* $u_g \in A_g \cap UA$ *mit* $u_g d u_g^{-1} = g(d)$. *Dann ist* A *zu einer verschränkten Gruppenalgebra des semidirekten Produkts von* G *mit* D *isomorph.*

Beweis. Für $g \in G$ ist $\gamma(g,h) := u_g u_h u_{gh}^{-1} \in UA_1 = UFD$, und für $d \in D$ ist

$$\gamma(g,h)d\gamma(g,h)^{-1} = u_g u_h u_{gh}^{-1} d u_{gh} u_h^{-1} u_g^{-1} = g(h((g\circ h)^{-1}(d))) = d,$$

also $\gamma(g,h) \in UFD \cap ZFD = UZFD$. Für $g,h,k \in G$ ist

$$\begin{aligned}
\gamma(g,h)\gamma(gh,k) &= u_g u_h u_{gh}^{-1} u_{gh} u_k u_{ghk}^{-1} \\
&= u_g u_h u_k u_{ghk}^{-1} \\
&= u_g \gamma(h,k) u_{hk} u_{ghk}^{-1} \\
&= g(\gamma(h,k)) u_g u_{hk} u_{ghk}^{-1} \\
&= g(\gamma(h,k))\gamma(g,hk).
\end{aligned}$$

Mit $\rho(g) := \prod_{k\in G} \gamma(g,k) \in UZFD$ ist also

$$\gamma(g,h)^{|G|} = g(\rho(h))\rho(g)\rho(g,h)^{-1}$$

für $g,h \in G$. Da FD lokal ist, ist $UZFD = F^\times(1 + JZFD)$, und für $j \in JZFD$ ist $j^{|D|} = 0$, d.h. $(1+j)^{|D|} = 1$. Wir wählen $r,s \in \mathbb{Z}$ mit $-1 = |G|r + |D|s$. Dann ist

$$\gamma(g,h)^{-1} = \gamma(g,h)^{|G|r}\gamma(g,h)^{|D|s} = g(\rho(h))^r \rho(g)^r \rho(gh)^{-r} \delta(g,h)^{-1}$$

mit $delta(g,h) := \gamma(g,h)^{-|D|s} \in F^\times 1_D$ für $g,h \in G$. Setzt man $v_g := \rho(g)^r u_g$ für $g \in G$, so ist

$$A = \bigoplus_{g\in G} A_1 v_g = \bigoplus_{g\in G, d\in D} F d v_g.$$

Für $g,h \in G,\ c,d \in D$ gilt dabei:

$$\begin{aligned}
(cv_g)(dv_h) &= c\rho(g)^r u_g d \rho(h)^r u_h \\
&= c\rho(g)^r g(d) g(\rho(h)^r) u_g u_h \\
&= cg(d)\rho(g)^r g(\rho(h)^r)\gamma(g,h) u_{gh} \\
&= cg(d)\rho(gh)^r \delta(g,h) u_{gh} \\
&= \delta(g,h) c g(d) v_{gh}.
\end{aligned}$$

Damit ist die Behauptung bewiesen. □

KAPITEL 30

Blöcke und Faktorgruppen

Sei F ein algebraisch abgeschlossener Körper.

30.1. Bemerkung. Zunächst verallgemeinern wir unsere Kenntnisse über das Heben von Idempotenten.

Satz (Wedderburn-Malcev). *Seien S eine halbeinfache, A eine beliebige endlich-dimensionale F-Algebra und I ein nilpotentes Ideal in A.*

(i) *Zu jedem Homomorphismus $\varphi : S \to A/I$ existiert dann ein Homomorphismus $\psi : S \to A$ mit $\psi(s) + I = \varphi(s)$ für $s \in S$.*
(ii) *Sind $\varphi, \varphi' : S \to A$ Homomorphismen mit $\varphi(s) + I = \varphi'(s) + I$ für $s \in S$, so existiert ein $x \in I$ mit $\varphi'(s) = (1-x)^{-1}\varphi(s)(1-x)$ für $s \in S$.*

Beweis. Nach 24.1 existiert eine bilineare Abbildung $\beta : S \times S \to F$, die S zu einer symmetrischen F-Algebra macht. Seien $(\{a_1, \ldots, a_n\}, \{b_1, \ldots, b_n\})$ ein Paar von Dualbasen und Γ die Gaschütz-Abbildung von (S, β). Wegen $\Gamma(S) = ZS$ existiert ein $c \in S$ mit $\sum_{i=1}^n b_i c a_i = \Gamma(c) = 1_S$.

(i) Das Idempotent $\varphi(1)$ in A/I läßt sich nach 22.1 zu einem Idempotent e in A heben. Wegen

$$\begin{aligned} \varphi(S) &= \varphi(1S1) = \varphi(1)\varphi(S)\varphi(1) \subseteq (e+I)(A/I)(e+I) \\ &= eAe + I/I \cong eAe/eAe \cap I = eAe/eIe \end{aligned}$$

induziert φ einen unitären Homomorphismus $\tilde{\varphi} : S \to eAe/eIe$. Ist $\tilde{\varphi} : S \to eAe$ ein Homomorphismus mit $\tilde{\varphi}(s) + eIe = \tilde{\varphi}(s)$ für $s \in S$,, so ist $\psi : S \xrightarrow{\tilde{\varphi}} eAe \hookrightarrow A$ ein Homomorphismus mit $\psi(s) + I = \tilde{\varphi}(s) + I = \varphi(s)$ für $s \in S$. Daher können wir annehmen, daß φ unitär ist.

Sicher existiert eine F-lineare Abbildung $\eta : S \to A$ mit $\eta(s) + I = \varphi(s)$ für $s \in S$. Dann ist $\gamma(s,t) := \eta(st) - \eta(s)\eta(t) \in I$ und

$$\begin{aligned} \gamma(s,t)\eta(u) + \gamma(st,u) &= \eta(st)\eta(u) - \eta(s)\eta(t)\eta(u) + \eta(stu) - \eta(st)\eta(u) \\ &= \gamma(s,tu) + \eta(s)\eta(tu) - \eta(s)\eta(t)\eta(u) \\ &= \gamma(s,tu) + \eta(s)\gamma(t,u) \end{aligned}$$

für $s, t, u \in S$. Setzt man

$$\varphi'(s) := \eta(s) + \sum_{i=1}^n \gamma(s, b_i c)\eta(a_i)$$

für $s \in S$, so gilt für $s, t \in S$:

$$\begin{aligned}
\varphi'(st) - \varphi'(s)\varphi'(t) &\equiv \eta(st) + \sum_{i=1}^{n} \gamma(st, b_i c)\eta(a_i) - \eta(s)\eta(t) \\
&\quad - \sum_{i=1}^{n} \eta(s)\gamma(t, b_i c)\eta(a_i) - \sum_{i=1}^{n} \gamma(s, b_i c)\eta(a_i)\eta(t) \\
&\equiv \gamma(s,t) + \sum_{i=1}^{n} \gamma(s, tb_i c)\eta(a_i) - \sum_{i=1}^{n} \gamma(s,t)\eta(b_i c)\eta(a_i) \\
&\quad - \sum_{i=1}^{n} \gamma(s, b_i c)\eta(a_i t) \\
&\equiv \gamma(s,t) + \sum_{i,j=1}^{n} \gamma(s, \beta(a_j, tb_i)b_j c)\eta(a_i) - \sum_{i=1}^{n} \gamma(s,t)\eta(b_i c a_i) \\
&\quad - \sum_{i,j=1}^{n} \gamma(s, b_i c)\eta(\beta(a_i t, b_j)a_j) \\
&\equiv 0 \pmod{I^2}.
\end{aligned}$$

Folglich ist die Abbildung $S \to A/I^2,\ s \mapsto \varphi'(s) + I^2$ ein Homomorphismus mit $\varphi'(s) + I = \varphi(s)$ für $s \in S$. Da I nilpotent ist, erhält man die Behauptung durch Induktion nach $\dim I$.

(ii) Offenbar sind $\varphi(1), \varphi'(1)$ Idempotente in A mit $\varphi(1) + I = \varphi'(1) + I$. Nach Aufgabe 24 existiert ein Element $y \in I$ mit $(1-y)^{-1}\varphi(1)(1-y) = \varphi'(1)$. Daher kann man $\varphi(1) = \varphi'(1) =: e$ annehmen. Dann induzieren φ, φ' Homomorphismen $\psi, \psi' : S \to eAe$ mit $\psi(s) + eIe = \psi'(s) + eIe$ für $s \in S$ wegen $eAe + I/I \cong eAe/eAe \cap I = eAe/eIe$. Daher kann man annehmen, daß φ, φ' unitär sind. Dann ist $\eta(s) := \varphi(s) - \varphi'(s) \in I$, $\eta(1) = 0$ und

$$\eta(st) = \varphi(s)(\varphi(t) - \varphi'(t)) + (\varphi(s) - \varphi'(s))\varphi'(t) = \varphi(s)\eta(t) + \eta(s)\varphi'(t)$$

für $s, t \in S$. Folglich ist

$$x := \sum_{i=1}^{n} \varphi(b_i c)\eta(a_i) \in I$$

und

$$\begin{aligned}
\varphi(s)x - x\varphi'(s) &= \sum_{i=1}^{n} \varphi(sb_i c)\eta(a_i) - \sum_{i=1}^{n} \varphi(b_i c)\eta(a_i)\varphi'(s) \\
&= \sum_{i,j=1}^{n} \varphi(\beta(a_j, sb_i)b_j c)\eta(a_i) - \sum_{i=1}^{n} \eta(b_i c a_i)\varphi'(s) \\
&\quad + \sum_{i=1}^{n} \eta(b_i c)\varphi'(a_i)\varphi'(s) \\
&= \sum_{i,j=1}^{n} \varphi(b_j c)\eta(\beta(a_j s, b_i)a_i) + \sum_{i=1}^{n} \eta(b_i c)\varphi'(a_i s) \\
&= \sum_{j=1}^{n} \varphi(b_j c)\eta(a_j s) + \sum_{i=1}^{n} \eta(b_i c)\varphi'(a_i s) \\
&= \sum_{i=1}^{n} \eta(b_i c a_i s) \;=\; \eta(s) \;=\; \varphi(s) - \varphi'(s),
\end{aligned}$$

d.h. $\varphi(s)(1-x) = (1-x)\varphi'(s)$ für $s \in S$, und die Behauptung folgt.

$\square$

30.2. Satz. *Zu jeder endlich-dimensionalen F-Algebra A existiert eine unitäre Unteralgebra T mit $A = T \oplus JA$. Ist T' eine weitere unitäre Unteralgebra mit $A = T' \oplus JA$, so existiert ein $x \in JA$ mit $(1-x)^{-1}T(1-x) = T'$.*

Beweis. Zu der endlich-dimensionalen F-Algebra $S := A/JA$ und dem Homomorphismus $\mathrm{id}_S : S \to A/JA$ existiert nach 30.1 ein Homomorphismus $\psi : S \to A$ mit $\psi(s) + JA = s$ für $s \in S$, d.h. $\psi(a + JA) + JA = a + JA$ und $a - \psi(a + JA) \in JA$ für $a \in A$. Folglich ist $A = T + JA$, wobei $T := \psi(A/JA)$ eine halbeinfache Unteralgebra von A ist. Insbesondere ist $T \cap JA \subseteq JT = 0$, also $A = T \oplus JA$. Folglich ist $1_T + JA = 1_{A/JA} = 1_A + JA$. Nach Aufgabe 24 sind also 1_T und 1_A konjugiert. Daher ist $1_T = 1_A$. Sei auch T' eine unitäre Unteralgebra von A mit $A = T' \oplus JA$. Dann sind $\tau : T \to A/JA,\ t \mapsto t + JA$ und $\tau' : T' \to A/JA,\ t' \mapsto t' + JA$ Isomorphismen. Folglich sind $\varphi : S \xrightarrow{\tau^{-1}} T \hookrightarrow A,\ \varphi' : S \xrightarrow{\tau'^{-1}} T' \hookrightarrow A$ Homomorphismen mit $\varphi(s) + JA = \varphi'(s) + JA$ für $s \in S$. Nach 30.1 existiert also ein $x \in JA$ mit $\varphi'(s) = (1-x)^{-1}\varphi(s)(1-x)$ für $s \in S$. Insbesondere ist $T' = \varphi'(S) = (1-x)^{-1}T(1-x)$. $\square$

30.3. Bemerkung. Seien G eine endliche Gruppe, $N \trianglelefteq G$, $\nu : FG \to F[G/N]$ kanonisch, $B_0 := B_0(FN)$ und $e_0 := e_0(FN)$. Für $g \in G$ ist dann

$$\nu(ge_0g^{-1}) = \nu(g)\nu(e_0)\nu(g)^{-1} = \nu(g)1\nu(g)^{-1} = 1.$$

Da ge_0g^{-1} auch ein Blockidempotent in FN ist, folgt $ge_0g^{-1} = e_0$. Folglich ist $e_0 \in ZFG$.
Wir betrachten im folgenden $A := FG$ als G/N-graduierte F-Algebra mit gN-Komponente $A_{gN} = FNg$ für $g \in G$. Dann ist auch $A_0 := e_0FGe_0 = FGe_0 = e_0FG$ eine G/N-graduierte F-Algebra mit gN-Komponente $(A_0)_{gN} = e_0FNg = B_0g$ für $g \in G$. Offenbar sind A und A_0 sogar verschränkte Produkte. Nach 29.2 sind auch $C_{FG}(N) = \bigoplus_{gN \in G/N} C_{FNg}(N)$ und $C_0 := C_{A_0}(B_0)$ G/N-graduierte F-Algebren, aber i.a. keine verschränkten Produkte. Für $g \in G$ ist dann $(C_0)_{gN} = C_{B_0g}(B_0)$; insbesondere hat C_0 die 1-Komponente ZB_0.
Sei nun $p := \operatorname{char} F > 0$ und $Q \in \mathrm{Syl}_p(N)$. Nach dem Frattini-Argument der Gruppentheorie ist dann $G = N \cdot N_G(Q)$. Wir setzen im folgenden $G = N \cdot C_G(Q)$ voraus und zeigen, daß dann C_0 ein verschränktes Produkt ist.
Sei also $gN \in G/N$, o.B.d.A. $g \in C_G(Q)$. Wir lassen dann N auf G durch Konjugation operieren. Die Bahn K von g enthält dann genau $|N : C_N(g)|$ Elemente. Wegen $Q \subseteq C_N(g)$ ist $p \nmid |N : C_N(g)|$. Wegen $K \subseteq NgN = gN$ ist also $\nu(K^+) = |K|gN \neq 0$. Offenbar ist $K^+ \subseteq C_{FG}(N)$, also $K^+e_0 \in C_{FG}(N)e_0 = C_0$. Wegen $K^+e_0 = e_0K^+ \in e_0FNg$ liegt e_0K^+ in der gN-Komponente von C_0. Folglich liegt $(K^+e_0)^{|G|}$ in der 1-Komponente ZB_0 von C_0. Wegen $\nu((K^+e_0)^{|G|}) = \nu(K^+)^{|G|}\nu(e_0) = |K|^{|G|}1 \neq 0$ ist $(K^+e_0)^{|G|}$ nicht nilpotent. Da ZB_0 lokal ist, ist $(K^+e_0)^{|G|}$ invertierbar in ZB_0 und C_0. Daher ist auch K^+e_0 invertierbar in C_0. Folglich ist $u_{gN} := |K|^{-1}K^+e_0$ eine graduierte Einheit in C_0 mit $\nu(u_{gN}) = gN$. Dies zeigt, daß C_0 ein verschränktes Produkt ist. Daher ist $C_0 = \bigoplus_{gN \in G/N} ZB_0u_{gN}$ ein freier ZB_0-Modul vom Rang $|G/N|$.
Für $g \in G$ ist u_{gN} auch eine graduierte Einheit in A_0. Daher ist analog $A_0 = \bigoplus_{gN \in G/N} B_0u_{gN}$ ein freier B_0-Modul vom Rang $|G/N|$. Insbesondere ist $A_0 = B_0C_0$ und $ZB_0 \subseteq ZA_0$. Wir können also A_0, B_0, C_0 als ZB_0-Algebren auffassen. Die Inklusionsabbildungen $B_0 \hookrightarrow A_0$ und $C_0 \hookrightarrow A_0$ induzieren also einen Epimorphismus von ZB_0-Algebren $\Phi : B_0 \otimes_{ZB_0} C_0 \to A_0$ mit $\Phi(x \otimes y) = xy$ für $x \in B_0,\ y \in C_0$. Offenbar ist $\dim_F B_0 \otimes_{ZB_0} C_0 = (\dim_F B_0)|G/N| = \dim_F A_0$, d.h. Φ ist ein Isomorphismus.
Das nilpotente Ideal $(JZB_0)B_0 \otimes C_0 + B_0 \otimes (JZB_0)C_0$ von $B_0 \otimes_{ZB_0} C_0$ wird unter Φ auf $(JZB_0)B_0C_0 + B_0(JZB_0)C_0 = (JZB_0)A_0$ abgebildet. Daher induziert Φ einen Isomorphismus

$$\overline{\Phi} : B_0/(JZB_0)B_0 \otimes_{ZB_0} C_0/(JZB_0)C_0 = B_0/(JZB_0)B_0 \otimes_F C_0/(JZB_0)C_0 \to A_0/(JZB_0)A_0$$

mit

$$\overline{\Phi}((x + (JZB_0)B_0) \otimes (y + (JZB_0)C_0)) = xy + (JZB_0)A_0$$

für $x \in B_0,\ y \in C_0$.

Offenbar ist $(JZB_0)C_0 = \bigoplus_{gN\in G/N}(JZB_0)u_{gN}$, also $\dim C_0/(JZB_0)C_0 = |G/N|$. Durch Einschränkung von ν erhält man einen Epimorphismus $C_0 \to F[G/N]$, dessen Kern $(JZB_0)C_0$ enthält. Folglich ist $C_0 \cap \mathrm{Ker}(\nu) = (JZB_0)C_0$, und ν induziert einen Isomorphismus $C_0/(JZB_0)C_0 \to F[G/N]$. Daher ist

$$A_0/(JZB_0)A_0 \cong B_0/(JZB_0)B_0 \otimes_F F[G/N]$$

und

$$A/JA_0 \cong B_0/JB_0 \otimes_F F[G/N]/JF[G/N].$$

Wegen $A_0 = B_0C_{A_0}(B_0)$ ist $ZA_0 = ZC_{A_0}(B_0)$. Die Blockidempotente von A_0 sind also genau die Blockidempotente von $C_{A_0}(B_0) = C_0$. Diese entsprechen unter ν bijektiv den Blockidempotenten von $F[G/N]$. Daher ist die Abbildung $e \mapsto \nu(e)$ eine Bijektion zwischen der Menge der Blockidempotente von A_0 und der Menge der Blockidempotente von $F[G/N]$. Nach 27.7 ist DN/N für jede Defektgruppe D des Blocks $A_0e = FGe_0e = FGe$ eine Defektgruppe des Blocks $F[G/N]\nu(e) = \nu(FGe)$. Aus den Eigenschaften des Tensorproduktes folgt, daß die obigen Isomorphismen Block für Block gelten. Wir fassen zusammen:

Satz. *Seien $p := \mathrm{char}\, F > 0$, G eine endliche Gruppe, $N \trianglelefteq G$, $Q \in \mathrm{Syl}_p(N)$ und $G = NC_G(Q)$.*

(i) *Dann induziert die kanonische Abbildung $\nu : FG \to F[G/N]$ eine Bijektion zwischen der Menge der Blöcke B von FG mit $BB_0(FN) \neq 0$ und der Menge der Blöcke von $F[G/N]$. Für $D \in \mathrm{Def}(B)$ ist dabei $D \cap N \in \mathrm{Syl}_p(N)$ und $DN/N \in \mathrm{Def}(\nu(B))$.*

(ii) *Ist $B_0 := B_0(FN)$ und B ein Block von FG mit $BB_0 \neq 0$, so ist*

$$\begin{aligned} B &\cong B_0 \otimes_{ZB_0} C_B(B_0), \\ B/(JZB_0)B &\cong B_0/(JZB_0)B_0 \otimes_F \nu(B), \\ B/JB &\cong B_0/JB_0 \otimes_F \nu(B)/J\nu(B), \\ \nu(B) &\cong C_B(B_0)/(JZB_0)C_B(B_0). \end{aligned}$$

30.4. Satz. *Seien $p := \mathrm{char}\, F > 0$, G eine endliche Gruppe, $N \trianglelefteq G$, $B_0 := B_0(FN)$, $Q \in \mathrm{Syl}_p(N)$ und $G = NC_G(Q)$. Ist B ein Block von FG mit $BB_0 \neq 0$ und Defektgruppe $D \subseteq N$, so ist $\nu(B)$ eine einfache F-Algebra und $B \cong B_0 \otimes_F \nu(B) \cong \mathrm{Mat}(n, B_0)$ für ein $n \in \mathbb{N}$.*

Beweis. Nach 30.3 ist $\nu(B)$ ein Block von $F[G/N]$ mit Defektgruppe $DN/N = 1$, d.h. $\nu(B)$ ist eine einfache F-Algebra. Nach 30.2 existiert eine unitäre Unteralgebra S von $C_B(B_0)$ mit $C_B(B_0) = S \oplus JC_B(B_0)$. Nach 30.3 ist $JC_B(B_0) = (JZB_0)C_B(B_0)$, also

$$C_B(B_0) = S \oplus (JZB_0)C_B(B_0) = (ZB_0)S + (JZB_0)C_B(B_0) = (ZB_0)S$$

nach Nakayamas Lemma. Nach 30.3 ist daher $B = B_0C_B(B_0) = B_0S$. Wir erhalten also einen Epimorphismus $\Psi : B_0 \otimes_F S \to B$ mit $\Psi(x \otimes y) = xy$ für $x \in B_0$, $y \in S$. Offenbar ist $Z(B_0 \otimes_F S) = ZB_0 \otimes_F ZS = ZB_0 \otimes_F e_0$, und für $z \in ZB_0$ ist $\Psi(z \otimes e_0) = ze_0 = z$. Daher ist $Z(B_0 \otimes_F S) \cap \mathrm{Ker}(\Psi) = 0$. Da $B_0 \otimes_F S$ eine symmetrische F-Algebra ist, folgt $\mathrm{Ker}(\Psi) = 0$ mit 24.6. □

30.5. Satz (Alperin-Dade). *Seien $p := \mathrm{char}\, F > 0$, G eine endliche Gruppe, $N \trianglelefteq G$, $Q \in \mathrm{Syl}_p(N)$, $G = NC_G(Q)$ und $p \nmid |G/N|$. Dann ist $B_0(FG) \cong B_0(FN)$.*

Beweis. Nach 26.7 ist $e_0(FG)e_0(FN) \neq 0$, also $B_0(FG)B_0(FN) \neq 0$. Die Defektgruppen von $B_0(FG)$ sind die p-Sylowgruppen von G, also auch die von N wegen $p \nmid |G : N|$. Nach 30.3 ist $\nu(e_0(FG))$ ein Blockidempotent in $F[G/N]$. Da $\nu(e_0(FG))$ und $e_0(F[G/N])$ die gleiche Augmentation 1 haben, ist $\nu(e_0(FG)) = e_0(F[G/N]) = \frac{1}{|G/N|}(G/N)^+$ wegen $p \nmid |G/N|$. Daher ist $\nu(B_0(FG)) = F[G/N]\nu(e_0(FG)) = Fe_0(F[G/N]) \cong F$. Nach 30.4 ist also $B_0(FG) \cong B_0(FN) \otimes_F F \cong B_0(FN)$. □

30.6. Satz (Brauer-Reynolds). *Sei $p := \mathrm{char}\, F > 0$, G eine endliche Gruppe, D ein p-Normalteiler von G mit $G = DC_G(D)$ und B ein Block von FG mit Defektgruppe D. Dann ist $B \cong \mathrm{Mat}(n, FD)$ für ein $n \in \mathbb{N}$.*

Beweis. Wir wenden 30.4 mit $N = D = Q$ an. Dann ist $B_0(FN) = FD$, also $BB_0(FN) \neq 0$ für jeden Block B von FG. □

Bemerkung. Eine unbewiesene Vermutung von P. Donovan besagt, daß zu jeder endlichen p-Gruppe D nur endliche viele Morita-Äquivalenzklassen von Blöcken mit zu D isomorpher Defektgruppe existieren.

30.7. Satz (Brauer). *Seien $p := \operatorname{char} F > 0$, G eine endliche Gruppe und Q ein p-Normalteiler von G mit $G = QC_G(Q)$. Für jeden Block B von FG ist dann das Bild $\overline{B}$ von B in $F[G/Q]$ ein Block von $F[G/Q]$, und auf diese Weise erhält man eine Bijektion zwischen der Menge der Blöcke von FG und der Menge der Blöcke von $F[G/Q]$. Ist $D \in \operatorname{Def}(B)$, so ist $Q \subseteq D$ und $D/Q \in \operatorname{Def}(\overline{B})$.*

Beweis. 30.3. □

30.8. Satz. *Seien $p := \operatorname{char} F > 0$, G eine endliche Gruppe und N ein p'-Normalteiler von G. Dann ist $FGe_0(FN) \cong F[G/N]$.*

Beweis. Wegen $p \nmid |N|$ ist $e_0(FN) = \frac{1}{|N|}N^+$ und $B_0(FN) = FNe_0(FN) = Fe_0(FN) \cong F$; insbesondere ist $JZB_0(FN) = 0$. Der Isomorphismus $\overline{\Phi}$ aus Bemerkung 30.3 wird also zu einem Isomorphismus zwischen $F \otimes_F F[G/N]$ und $A_0 = FGe_0(FN)$. □

KAPITEL 31

Blöcke und Normalteiler

Sei F ein algebraisch abgeschlossener Körper der Charakteristik $p \neq 0$.

31.1. Definition. Seien G eine endliche Gruppe, $H \trianglelefteq G$, A ein Block von FG und B ein Block von FH. Man sagt, daß B von A *überdeckt* wird, falls $AB \neq 0$.

Bemerkung. Sind e und f die Blockidempotente von A bzw. B, so ist $AB \neq 0$ äquivalent zu $ef \neq 0$.

Satz. *Seien G eine endliche Gruppe und $H \trianglelefteq G$. Dann überdeckt jeder Block von FG mindestens einen Block von FH, und jeder Block von FH wird von mindestens einem Block von FG überdeckt.*

Beweis. Seien $e_1, \ldots, e_r$ die Blockidempotente von FG und $f_1, \ldots, f_s$ die von FH. Für $i = 1, \ldots, r$ ist dann $e_i = e_i 1 = e_i(f_1 + \ldots + f_s) = e_i f_1 + \ldots + e_i f_s$, also $e_i f_j \neq 0$ für ein $j \in \{1, \ldots, s\}$. Für $j = 1, \ldots, s$ ist analog $f_j = 1 f_j = (e_1 + \ldots + e_r) f_j = e_1 f_j + \ldots + e_r f_j$, also $e_i f_j \neq 0$ für ein $i \in \{1, \ldots, r\}$. $\square$

31.2. Bemerkung. Seien G eine endliche Gruppe und $H \trianglelefteq G$. Für jeden Block B von FH mit Blockidempotent f und jedes $g \in G$ ist gBg^{-1} ein Block von FH mit Blockidempotent gfg^{-1}. Auf diese Weise operiert G durch Konjugation auf der Menge der Blöcke und der Menge der Blockidempotente von FH. Sind $f_1 = f, f_2, \ldots, f_s$ die verschiedenen Konjugierten von f unter G, so ist also $f^G := f_1 + \ldots + f_s$ ein Idempotent in $ZFH \cap ZFG$.

Satz. *Seien G eine endliche Gruppe und $H \trianglelefteq G$. Für Blockidempotente e, f von FG bzw. FH gilt dann: $ef \neq 0 \iff ef^G = e$. Insbesondere überdeckt jeder Block von FG genau eine Konjugationsklasse von Blöcken in FH.*

Beweis.

$\Rightarrow$: Aus $0 \neq ef = ef^G f$ folgt $ef^G \neq 0$, also $ef^G = e$ wegen $f^G \in ZFG$.

$\Leftarrow$: Aus $ef^G = e \neq 0$ folgt $0 \neq egfg^{-1} = gefg^{-1}$ für ein $g \in G$, also $ef \neq 0$.

Ist $ef \neq 0$, so ist $0 \neq egfg^{-1} = gefg^{-1}$ für $g \in G$. Ist umgekehrt $\tilde{f}$ ein Blockidempotent von FH mit $e\tilde{f} \neq 0$, so ist $e\tilde{f}^G f = ef \neq 0$, d.h. $g\tilde{f}g^{-1} f \neq 0$ für ein $g \in G$, also $g\tilde{f}g^{-1} = f$. $\square$

31.3. Bemerkung. Seien G eine endliche Gruppe, $H \trianglelefteq G$ und B ein Block von FH mit Blockidempotent f. Dann ist $I := \mathrm{Stb}_G(B) = \mathrm{Stb}_G(f)$ eine Untergruppe von G mit $H \leq I \leq G$ und $f \in ZFI$. Sind $x, y \in G$ mit $xI \neq yI$, so sind xfx^{-1}, yfy^{-1} verschiedene Blockidempotente in FH, also $xfx^{-1}yfy^{-1} = 0$. Insbesondere ist $fzfz^{-1} = 0$, also $fzf = 0$ für $z \in G \setminus I$. Daher ist $fFGf = fFIf = FIf = fFI$. Sei $t_1 = 1, t_2, \ldots, t_s$ ein Repräsentantensystem für G/I. Dann sind $t_1 f t_1^{-1}, \ldots, t_s f t_s^{-1}$ die verschiedenen Konjugierten von f unter G. Wie in 31.2 ist also $f^G = t_1 f t_1^{-1} + \ldots + t_s f t_s^{-1}$ ein Idempotent in $ZFH \cap ZFG$ mit $f^G \in FGfFG$, also $FGf^G \subseteq FGfFG$. Andererseits ist $ff^G = f$, also $FGfFG = FGff^GFG = FGfFGf^G \subseteq FGf^G$. Daher ist $FGfFG = FGf^G = f^GFG$.

Satz. *Mit den obigen Bezeichnungen gilt:*

(i) *Die Abbildungen*

$$\mathrm{Mat}(s, FIf) \to FGf^G, \ (a_{ij}) \mapsto \sum_{i,j=1}^{s} t_i a_{ij} t_j^{-1}$$

und

$$FGf^G \to \mathrm{Mat}(s, FIf), \ x \mapsto (f t_i^{-1} x t_j f)_{i,j=1}^{s}$$

sind zueinander inverse Isomorphismen.

(ii) *Die Abbildungen*

$$Z(FIf) \to Z(FGf^G),\ z \mapsto \sum_{i=1}^{s} t_i z t_i^{-1}$$

und

$$Z(FGf^G) \to Z(FIf),\ y \mapsto yf$$

sind zueinander inverse Isomorphismen.

Beweis.

(i) Nach der Vorbemerkung sind die Abbildungen wohldefiniert und offenbar linear. Für Elemente $a_{ij}, b_{ij} \in FIf$ $(i, j = 1, \ldots, s)$ hat man

$$\begin{aligned}\sum_{i,j,k,l=1}^{s} t_i a_{ij} t_j^{-1} \cdot t_k b_{kl} t_l^{-1} &= \sum_{i,j,k,l=1}^{s} t_i a_{ij} t_j^{-1}(t_j f t_j^{-1})(t_k f t_k^{-1}) t_k b_{kl} t_l^{-1} \\ &= \sum_{i,j,l=1}^{s} t_i a_{ij} t_j^{-1}(t_j f t_j^{-1}) t_j b_{jl} t_l^{-1} \\ &= \sum_{i,j,l=1}^{s} t_i a_{ij} b_{jl} t_l^{-1}.\end{aligned}$$

Daher ist die erste Abbildung ein Homomorphismus. Für $m, n \in \{1, \ldots, s\}$ ist außerdem

$$\begin{aligned} f t_m^{-1} \sum_{i,j=1}^{s} t_i a_{ij} t_j^{-1} \cdot t_n f &= \sum_{i,j=1}^{s} t_m^{-1}(t_m f t_m^{-1})(t_i f t_i^{-1}) t_i a_{ij} t_j^{-1}(t_j f t_j^{-1})(t_n f t_n^{-1}) t_n \\ &= t_m^{-1}(t_m f t_m^{-1}) t_m a_{mn} t_n^{-1}(t_n f t_n^{-1}) t_n \ = \ a_{mn}.\end{aligned}$$

Für $x \in FGf^G$ gilt umgekehrt:

$$\sum_{i,j=1}^{s} t_i f t_i^{-1} x t_j f t_j^{-1} = f^G x f^G = x.$$

Daraus folgt die Behauptung.

(ii) Nach (i) ist $Z(FIf) \cong Z(\mathrm{Mat}(s, FIf)) \cong Z(FGf^G)$, und die angegebene Abbildung $Z(FIf) \to Z(FGf^G)$ ist ein entsprechender Isomorphismus. Die zweite Abbildung ist dazu invers; denn für $z \in Z(FIf)$ gilt:

$$\left(\sum_{i,j=1}^{s} t_i z t_i^{-1}\right) = \sum_{i=1}^{s} t_i z t_i^{-1}(t_i f t_i^{-1}) f = zf = z.$$

$\square$

31.4. Bemerkung. Seien G eine endliche Gruppe, $H \trianglelefteq G$, B ein Block von FH mit Blockidempotent f und $I := \mathrm{Stb}_G(B)$. Durch 31.3 erhält man eine Bijektion zwischen der Menge aller Blöcke von FGf^G und der Menge aller Blöcke von FIf. Diese bezeichnet man als *Clifford-Korrespondenz* oder *Fong-Korrespondenz.*

Wegen $FG = FGf^G \oplus FG(1 - f^G)$ und $f^G \in ZFG$ ist jeder Block A von FGf^G auch einer von FG, und für das Blockidempotent e von A ist $ef^G = e$. Folglich wird B von A überdeckt. Ist umgekehrt A ein Block von FG mit Blockidempotent e, der B überdeckt, so ist $ef^G = e$, also $FGf^G = FGe \oplus FG(f^G - e)$. Folglich ist $A = FGe$ ein Block von FGf^G. Die Blöcke von FGf^G sind also genau die Blöcke von FG, die B überdecken, und analog sind die Blöcke von FIf genau die Blöcke von FI, die B überdecken. Ist A ein Block von FG, der B überdeckt, mit Blockidempotent e und ist C der entsprechende Block von

FI (der *Clifford-Korrespondent* von A bzgl. B), so ist ef nach 31.3 das Blockidempotent von C, und es gilt:

$$A \cong \mathrm{Mat}(|G:I|, C) \qquad \text{und} \qquad ZA \cong ZC.$$

Im folgenden werden wir das Verhalten von Defektgruppen unter der Clifford-Korrespondenz untersuchen. Dabei ist es nützlich, Defektgruppen in etwas größerer Allgemeinheit als bisher zu betrachten.

31.5. Bemerkung. Sei G eine endliche Gruppe. Jede Untergruppe H von G operiert auf G durch Konjugation, und die entsprechende Bahnen bezeichnen wir mit *H-Konjugationsklassen* von G. Die entsprechenden *H-Klassensummen* bilden eine F-Basis von $C_{FG}(H)$. Für jede H-Konjugationsklasse K von G und jedes Element $g \in K$ bezeichnet man jede p-Sylowgruppe Q von $C_H(g)$ als *p-Defektgruppe* von K (in H). Je zwei p-Defektgruppen von K in H sind also in H konjugiert. Wie ein zu 26.9 analoger Beweis zeigt, ist K^+L^+ für jede H-Konjugationsklasse L von G eine F-Linearkombination von H-Klassensummen M^+, wobei M die H-Konjugationsklassen von G durchläuft, deren p-Defektgruppen in H zu Untergruppen von Q konjugiert sind. Daher bilden für jede p-Untergruppe R von H die H-Klassensummen M^+, wobei M die H-Konjugationsklassen von G durchläuft, deren p-Defektgruppen in H zu Untergruppen von R konjugiert sind, eine Basis eines Ideals $I_R^H(FG)$ von $C_{FG}(H)$.

Satz. *Seien G eine endliche Gruppe, $H \trianglelefteq G$, A ein Block von FG, B ein von A überdeckter Block von FH, $I := \mathrm{Stb}_G(B)$ und C der Clifford-Korrespondent von A bzgl. B. Dann ist jede Defektgruppe D von C auch eine von A.*

Bemerkung. Man beachte jedoch, daß alle Konjugierten von D in G auch Defektgruppen von A, während die Defektgruppen von C lediglich die Konjugierten von D in I sind.

Beweis. Seien e, f die Blockidempotente von A bzw. B. Dann ist ef das Blockidempotent von C. Nach Definition ist ef eine F-Linearkombination von Klassensummen L^+, wobei L die Konjugationsklassen von I mit einer Untergruppe von D als Defektgruppe durchläuft. Für jedes Repräsentantensystem $t_1 = 1, t_2, \ldots, t_s$ für G/I ist $e = \sum_{i=1}^s t_i e f t_i^{-1}$.
Sei L eine Konjugationsklasse von I mit einer Untergruppe Q von D als Defektgruppe, sei $x \in L$, und sei K die Konjugationsklasse von x in G. Dann ist $\sum_{i=1}^s t_i L^+ t_i^{-1} = nK^+$ mit $n = |C_G(x) : C_I(x)|$. Im Fall $p \mid n$ ist also $\sum_{i=1}^s t_i L^+ t_i^{-1} = 0$. Dies zeigt, daß e eine F-Linearkombination von Klassensummen K^+ ist, wobei K die Konjugationsklassen von G mit einer Untergruppe von D als Defektgruppe durchläuft. Mit anderen Worten: $e \in I_D(FG)$. Folglich hat A eine Defektgruppe $E \leq D$. Daher ist e eine F-Linearkombination von Klassensummen K^+, wobei K die Konjugationsklassen von G mit einer Untergruppe von E als Defektgruppe durchläuft. Folglich ist e auch eine F-Linearkombination von I-Klassensummen L^+, wobei L die I-Konjugationsklassen von G durchläuft, deren p-Defektgruppe nicht größer als der Defekt von A ist. Nach der Vorbemerkung ist auch ef eine F-Linearkombination dieser Form. Also ist $|D| \leq |E|$, und wir sind fertig. □

31.6. Bemerkung. Seien wieder G eine endliche Gruppe, $H \trianglelefteq G$, A ein Block von FG, B ein von A überdeckter Block von FH und $I := \mathrm{Stb}_G(B)$. Die vorangegangenen Sätze liefern eine Reduktion auf den Fall $G = I$. In diesem Fall nennen wir B *G-stabil*. Die Struktur von A in diesem Fall ist komplizierter zu beschreiben und auch nur in Spezialfällen bekannt. Man bezeichnet diesen Fall auch als *stabile Clifford-Theorie.*

Satz (Dade)**.** *Seien G eine endliche Gruppe, $H \trianglelefteq G$, A ein Block von FG mit Defektgruppe D und B ein von A überdeckter G-stabiler Block von FH. Dann ist $D \cap H \in \mathrm{Def}(B)$.*

Beweis. Seien e, f Blockidempotente von A bzw. B. Dann ist $f \in ZFG$ und $ef = e$. Wir schreiben $e = \sum_{K \in \mathrm{Cl}(G)} \alpha_K K^+$ mit $\alpha_K \in F$ für $K \in \mathrm{Cl}(G)$. Wegen $e = e^2 = \sum_{K \in \mathrm{Cl}(G)} \alpha_K K^+ e$ ist $K^+ e \notin JZFG$ für ein $K \in \mathrm{Cl}(G)$ mit $\alpha_K \neq 0$. Wegen $I_{<D}(FG)e \subseteq JZFG$ ist $D \in \mathrm{Def}_p(K)$. Sei $g \in K$ mit $D \in \mathrm{Syl}_p(C_G(g))$, und sei L die H-Konjugationsklasse vpn g. Dann ist auch K die disjunkte Vereinigung der verschiedenen Konjugierten von L unter G.
Wäre $L^+ f \in JC_{FG}(H)$, so wäre auch $K^+ f \in JC_{FG}(H)$, d.h. $K^+ f$ und $K^+ e = K^+ fe$ wären nilpotent, was nicht der Fall ist. Daher ist $L^+ f \notin JC_{FG}(H)$.

$C_{FG}(H)f$ ist eine G/H-graduierte F-Algebra mit 1-Komponente $ZFHf = ZB$. Wegen $L \subseteq HgH = Hg$ ist $L^+f = fL^+ \in FHg$, d.h. L^+f liegt in der gH-Komponente von $C_{FG}(H)f$. Daher ist $L^+fg^{-1} \in FH$ und $L^+f \cdot C_{FG}(H)f = L^+fg^{-1}C_{FG}(H)gf = C_{FG}(H) \cdot L^+fg^{-1}gf = C_{FG}(H)fL^+f$ ist ein Ideal in $C_{FG}(H)f$, das nicht nilpotent ist. Daher sind auch $(L^+f \cdot C_{FG}(H)f)^{|G|} = (L^+f)^{|G|}C_{FG}(H)f$ und $(L^+f)^{|G|}$ nicht nilpotent. Andererseits liegt $(L^+f)^{|G|}$ in der 1-Komponente $ZFHf$ von $C_{FG}(H)f$. Da $ZFHf$ lokal ist, ist $(L^+f)^{|G|}$ invertierbar, also auch L^+f selbst. Sei $z \in C_{FG}(H)f \subseteq C_{FG}(H)$ mit $L^+fz = f$. Da L p-Defektgruppe $D \cap H$ hat, ist f eine Linearkombination von H-Klassensummen M^+, wobei M die H-Konjugationsklassen von G mit einer Untergruppe von $D \cap H$ als Defektgruppe durchläuft. Wegen $f \in FH$ ist also $f \in I_{D\cap H}(FH)$, d.h. B hat eine Defektgruppe $E \leq D \cap H$. Wir schreiben $f = \sum_{h\in H} \beta_h h$ mit $\beta_h \in F$ für $h \in H$. Ist $h \in H$ mit $\beta_h \neq 0$ und ist $P \in \mathrm{Syl}_p(C_G(h))$, so ist $P \cap H \in \mathrm{Syl}_p(C_H(h))$, also $P \cap H \leq_H E$. Daher ist $f \in \sum_P I_P(FG)$, wobei P alle p-Untergruppen von G mit $P \cap H \leq_H E$ durchläuft. Wegen $ef = e$ liegt auch e in diesem Ideal von ZFG. Daher existiert eine p-Untergruppe P von G mit $P \cap H \leq_H E$ und $D \leq_G P$ nach Rosenbergs Lemma, d.h. $D \cap H \leq_G P \cap H \leq_H E$. Folglich ist $D \cap H = E$, und wir sind fertig. □

31.7. Satz. *Seien G eine endliche Gruppe, $H \trianglelefteq G$ und B ein G-stabiler Block von FH. Dann existiert stets ein Block A von FG, der B überdeckt mit $p \nmid |G : DH|$ für ein $D \in \mathrm{Def}(A)$.*

Beweis. Sei f das Blockidempotent von B. Wegen $f \in ZFG$ kann man $f = \sum_{K\in\mathrm{Cl}(G)} \alpha_K K^+$ mit $\alpha_K \in F$ für $K \in \mathrm{Cl}(G)$ schreiben. Wegen $f = f^2 = \sum_{K\in\mathrm{Cl}(G)} \alpha_K K^+ f$ existiert ein $K \in \mathrm{Cl}(G)$ mit $\alpha_K \neq 0$ und $K^+f \notin JZFG$. Offenbar ist $K \subseteq H$ und $K^+f \in JZFH$. Seien $h \in K$ und L die Konjugationsklasse von h in H. Dann ist K die disjunkte Vereinigung von

$$\frac{|K|}{|L|} = \frac{|G : C_G(h)|}{|H : C_H(h)|} = \frac{|G| \cdot |H \cap C_G(h)|}{|H| \cdot |C_G(h)|} = \frac{|G|}{|HC_G(h)|}$$

Konjugierten von L. Sei $\alpha \in F$ mit $L^+f \equiv \alpha f \pmod{JZFHf}$. Dann ist

$$0 \not\equiv K^+f \equiv |G : HC_G(h)|\, \alpha f \pmod{JZFHf};$$

insbesondere ist $p \nmid |G : HC_G(h)|$, also auch $p \nmid |G : QH|$ für $Q \in \mathrm{Syl}_p(C_G(h))$. Wegen $\alpha_K \neq 0$ existiert ein Block A von FG, der B überdeckt und eine Defektgruppe D von A mit $Q \subseteq D$ besitzt. Folglich ist auch $p \nmid |G : DH|$. □

31.8. Satz. *Seien G eine endliche p-nilpotente Gruppe (d.h. $G/O_{p'}(G)$ ist eine p-Gruppe) und A ein Block von FG mit Defektgruppe D. Dann ist $A \cong \mathrm{Mat}(n, FD)$ für ein $n \in \mathbb{N}$.*

Beweis. Seien $H := O_{p'}(G)$, B ein von A überdeckter Block von FH, f das Blockidempotent von B, $I := \mathrm{Stb}_G(B)$ und C der Clifford-Korrespondent von A bzgl. B. Nach 31.5 hat C eine zu D konjugierte Defektgruppe, und nach 31.4 ist $A \cong \mathrm{Mat}(|G : I|, C)$. Da auch I p-nilpotent ist, können wir G durch I ersetzen und folglich annehmen, daß B G-stabil ist. Dann ist $fFGf = fFG = FGf$ wie früher eine G/H-graduierte F-Algebra mit 1-Komponente $fFHf = FHf = B$. Offenbar ist FGf sogar ein verschränktes Produkt. Wegen $p \nmid |H|$ ist B eine einfache F-Algebra, also $B \cong \mathrm{Mat}(n, F)$ für ein $n \in \mathbb{N}$. Nach 29.8 ist also $FGf \cong B \otimes_F C_{FGf}(B)$, und $C_{FGf}(B)$ ist eine verschränkte Gruppenalgebra von G/H über F. Da G/H eine p-Gruppe ist, ist $H^2(G/H, F^\times) = 1$ nach 12.6. Daher ist $C_{FGf}(B) \cong F[G/H]$ nach 29.6. Folglich ist

$$FGf \cong B \otimes_F F[G/H] \cong \mathrm{Mat}(n, F[G/H]);$$

insbesondere ist $Z(FGf) \cong Z(F[G/H])$ lokal, da G/H eine p-Gruppe ist. Das bedeutet, daß FGf genau einen Block besitzt, nämlich A, d.h. $A = FGf$. Da A der einzige Block von FG ist, der B überdeckt, folgt $p \nmid |G : DH|$ aus 31.7. Da G p-nilpotent ist, ist andererseits $|G : DH|$ eine Potenz von p, also $|G : DH| = 1$. Daher ist $G = DH$. Wegen $D \cap H = 1$ ist damit $G/H = DH/H \cong D/D \cap H \cong D$, und wir sind fertig. □

31.9. Bemerkung. Seien G eine endliche Gruppe, D ein p-Normalteiler von G und A ein Block von FG mit Defektgruppe D. Ferner sei B ein von A überdeckter Block von $FDC_G(D)$. Dann ist D auch eine Defektgruppe von B.

Wir nehmen o.B.d.A. an, daß B G-stabil ist. Das Blockidempotent f von B liegt dann in ZFG, und das Blockidempotent e von A in $FC_G(D) \subseteq FDC_G(D)$. Daher ist $e = ef = f$. Folglich ist A der einzige Block von FG, der B überdeckt.
Nach 31.7 ist $p \nmid |G : DC_G(D)|$. Daher ist $DC_G(D)/C_G(D) \cong D/D \cap C_G(D) = D/Z(D)$ eine normale p-Sylowgruppe von $G/C_G(D)$, besitzt nach Schur-Zassenhaus also ein Komplement K in $G/C_G(D)$. Dann ist K eine zu $G/DC_G(D)$ isomorphe p'-Gruppe, die wir mit einer Untergruppe von $\mathrm{Aut}(D)$ identifizieren können. Nach 30.6 ist $B \cong FD \otimes_F S$ für eine einfache F-Algebra $S \cong \mathrm{Mat}(n, F)$. Wie der Beweis von 30.4 zeigt, können wir $S \subseteq C_B(D)$ annehmen und den Isomorphismus $\Phi : FD \otimes_F S \to B$ so wählen, daß $\Phi(x \otimes s) = xs$ für $x \in FD,\ s \in S$ ist.
Wegen $G/DC_G(D) \cong K$ können wir $A = FGe = FGf = fFG = fFGf$ als K-graduierte F-Algebra ansehen mit 1-Komponente $FDC_G(D)f = B$. Wegen $S \subseteq B$ ist also $C_A(S)$ eine K-graduierte Unteralgebra von A mit 1-Komponente $C_B(S) \cong FD$. Jedes $g \in G$ operiert auf B durch Konjugation. Wegen $C_B(D) = S \oplus JC_B(D)$ (vgl. 30.4) ist auch $C_B(D) = {}^gS \oplus JC_B(D)$. Nach Wedderburn-Malcev existiert eine Einheit x in $C_B(D)$ mit ${}^{xg}S = S$. Die Abbildung $S \to S,\ s \mapsto xgsg^{-1}x^{-1}$ ist also ein Automorphismus von S. Wegen $\mathrm{Out}(S) = 1$ existiert eine Einheit y in S mit $yxgsg^{-1}x^{-1}y^{-1} = s$. Dann ist $yxg \in Bg$ eine graduierte Einheit in $C_A(S)$, und für $d \in D$ ist $yxgdg^{-1}x^{-1}y^{-1} = gdg^{-1}$. Daher ist $C_A(S)$ ein verschränktes Produkt, das die Voraussetzungen von 29.9 erfüllt. Folglich ist $C_A(S)$ eine verschränkte Gruppenalgebra des semidirekten Produkts L von D und K über F. Nach Aufgabe 32 ist dann $A \cong S \otimes_F C_A(S) \cong \mathrm{Mat}(n, C_A(S))$.
Wir haben also bewiesen:

Satz (Reynolds)**.** *Seien G eine endliche Gruppe, D ein p-Normalteiler von G und A ein Block von FG mit Defektgruppe D. Ferner sei B ein von A überdeckter Block von $FDC_G(D)$ und $I := \mathrm{Stb}_G(B)$. Dann ist $A \cong \mathrm{Mat}(n, C)$ für ein $n \in \mathbb{N}$ mit einer verschränkten Gruppenalgebra C einer Gruppe L über F, die das semidirekte Produkt von D und einer zu $I/DC_G(D)$ isomorphen p'-Untergruppe von $\mathrm{Aut}(D)$ ist.*

KAPITEL 32

Projektive Moduln und Cartaninvarianten

Sei F ein algebraisch abgeschlossener Körper.

32.1. Bemerkung. Im folgenden betrachten wir einen (stets endlich erzeugten) unzerlegbaren projektiven Linksmodul P über einer endlich-dimensionalen F-Algebra A. Nach Definition ist P zu einem unzerlegbaren direkten Summanden von A^n für ein $n \in \mathbb{N}$ isomorph. Nach Krull-Schmidt ist P also zu einem unzerlegbaren direkten Summanden von A isomorph. Nach 22.5 ist daher $P \simeq Ae$ für ein primitives Idempotent e in A. Wie in der Algebra gezeigt, ist dann $\mathrm{Rad}(P) = \mathrm{Rad}(A)P \simeq JAe$.

Satz. *Sei A eine endlich-dimensionale F-Algebra.*

(i) *Für jeden unzerlegbaren projektiven A-Linksmodul P ist $P/\mathrm{Rad}(P)$ ein einfacher A-Linksmodul.*

(ii) *Auf diese Weise erhält man eine Bijektion zwischen der Menge der Isomorphieklassen unzerlegbarer projektiver A-Linksmoduln und der Menge der Isomorphieklassen einfacher A-Linksmoduln.*

Beweis.

(i) Für $\varphi \in E := \mathrm{End}_A(P)$ ist $\varphi(\mathrm{Rad}(P)) \subseteq \mathrm{Rad}(P)$, wie aus der Algebra bekannt. Daher ist die Abbildung $\overline{\varphi} : \overline{P} := P/\mathrm{Rad}(P) \to \overline{P}$, $x + \mathrm{Rad}(P) \mapsto \varphi(x) + \mathrm{Rad}(P)$ wohldefiniert und ein A-Endomorphismus on $\overline{P}$. Auf diese Weise erhält man, wie man leicht nachrechnet, einen Homomorphismus von F-Algebren $\Phi : E \to \overline{E} := \mathrm{End}_A(\overline{P})$, $\varphi \mapsto \overline{\varphi}$. Offenbar ist Φ surjektiv; ist nämlich $\psi \in \overline{E}$ und $\nu : P \to \overline{P}$ kanonisch, so existiert wegen der Projektivität von P ein A-Endomorphismus φ von P, so daß folgendes Diagramm kommutiert:

$$\begin{tikzcd} P \arrow[r, "\nu"] \arrow[d, dotted, "\varphi"'] & \overline{P} \arrow[d, "\psi"] & \\ P \arrow[r, "\nu"] & \overline{P} \arrow[r] & 0 \end{tikzcd}$$

Folglich ist $\psi = \overline{\varphi} = \Phi(\varphi)$. Wegen der Unzerlegbarkeit von P ist E lokal, also auch $E/\mathrm{Ker}(\Phi) \cong \overline{E}$. Daher ist $\overline{P}$ unzerlegbar. Andererseits ist $\overline{P}$ halbeinfach, wie in der Algebra gezeigt. Insgesamt ist $\overline{P}$ also einfach.

(ii) Sei Q ein weiterer unzerlegbarer projektiver A-Linksmodul und $\overline{Q} := Q/\mathrm{Rad}(Q)$. Im Fall $P \simeq Q$ ist natürlich $\overline{P} \simeq \overline{Q}$. Sei umgekehrt $\overline{P} \simeq \overline{Q}$ und $\rho : \overline{P} \to \overline{Q}$ ein A-Isomorphismus. Wegen der Projektivität von P existiert ein A-Homomorphismus $\sigma : P \to Q$, so daß folgendes Diagramm kommutiert:

$$\begin{tikzcd} P \arrow[r, "\nu"] \arrow[d, dotted, "\sigma"'] & \overline{P} \arrow[d, "\rho"] & \\ Q \arrow[r, "\mu"] & \overline{Q} \arrow[r] & 0 \end{tikzcd}$$

Dabei ist $\mu : Q \to \overline{Q}$ kanonisch und $\mu \circ \sigma = \rho \circ \nu$ surjektiv; insbesondere ist $\mu \circ \sigma \neq 0$, d.h. $\sigma(P) \nsubseteq \mathrm{Ker}(\mu) = \mathrm{Rad}(Q)$. Da $\mathrm{Rad}(Q)$ nach (i) der einzige maximale Untermodul von Q ist, folgt $\sigma(P) = Q$. Daher ist die Sequenz $\mathcal{E} : 0 \longrightarrow \mathrm{Ker}(\sigma) \hookrightarrow P \xrightarrow{\sigma} Q \longrightarrow 0$ exakt. Wegen der Projektivität von Q zerfällt $\mathcal{E}$, d.h. $P \simeq \mathrm{Ker}(\sigma) \oplus Q$. Da P unzerlegbar ist, folgt $\mathrm{Ker}(\sigma) = 0$; insbesondere ist $P \simeq Q$.

Schließlich sei S ein beliebiger einfacher A-Linksmodul. Wie in der Algebra gezeigt, existiert ein

A-Epimorphismus $\alpha : A \to S$. Schreibt man $A = P_1 \oplus \ldots \oplus P_r$ mit unzerlegbaren (projektiven) A-Linksmoduln $P_1, \ldots, P_r$, so ist $\alpha(P_i) \neq 0$ für ein $i \in \{1, \ldots, r\}$. Die Einschränkung von α ist also wegen der Einfachheit von S ein A-Epimorphismus $\alpha_i : P_i \to S$. Nach dem Homomorphiesatz ist $\operatorname{Ker}(\alpha_i)$ ein maximaler Untermodul von P_i, also $\operatorname{Ker}(\alpha_i) = \operatorname{Rad}(P_i)$ nach (i). Folglich ist $S \simeq P_i/\operatorname{Ker}(\alpha_i) = P_i/\operatorname{Rad}(P_i) = \overline{P_i}$.

□

32.2. Satz. *Seien A eine endlich-dimensionale F-Algebra, P ein unzerlegbarer A-Linksmodul, $S := P/\operatorname{Rad}(P)$ und M ein beliebiger endlich erzeugter A-Linksmodul. Dann ist $\dim_F \operatorname{Hom}_A(P, M)$ die Anzahl der zu S isomorphen Kompositionsfaktoren von M.*

Beweis. (Induktion nach der Kompostionslänge l von M) Im Fall $l = 0$ ist $M = 0$ und die Behauptung ist trivial. Sei also $l > 0$ und N ein maximaler Untermodul von M. Dann ist M/N einfach, und N hat Kompositionslänge $l - 1$. Seien $\varphi \in \operatorname{Hom}_A(P, M)$ und $\nu : M \to M/N$ kanonisch. Dann ist $P/\operatorname{Ker}(\nu \circ \varphi) \simeq \nu\varphi(P)) \subseteq M/N$ halbeinfach, also $\operatorname{Rad}(P) \subseteq \operatorname{Ker}(\nu \circ \varphi)$. Im Fall $M/N \not\simeq S$ ist $\nu \circ \varphi = 0$, d.h. $\varphi(P) \subseteq \operatorname{Ker}(\nu) = N$. Folglich ist $\dim_F \operatorname{Hom}_A(P, M) = \dim_F \operatorname{Hom}_A(P, N)$. Andererseits besitzen M und N die gleiche Anzahl zu S isomorpher Kompositionsfaktoren. Die Behauptung folgt also in diesem Fall aus der Induktionsvoraussetzung.
Sei daher $M/N \simeq S$ und $\pi : P \to M/N$ ein A-Epimorphismus. Da P projektiv ist, existiert ein A-Homomorphismus $\psi : P \to M$, so daß folgendes Diagramm kommutiert:

$$\begin{tikzcd}
& P \arrow[d, "\pi"] \arrow[dl, dotted, "\psi"'] & \\
M \arrow[r, "\nu"] & M/N \arrow[r] & 0
\end{tikzcd}$$

Wegen $\nu \circ \psi = \pi \neq 0$ ist $\psi(P) \not\subseteq \operatorname{Ker}(\nu) = N$, also $\dim_F \operatorname{Hom}_A(P, M) > \dim_F \operatorname{Hom}_A(P, N) =: n$. Nach Induktion ist n die Anzahl der zu S isomorphen Kompositionsfaktoren von N. Daher ist $\dim_F \operatorname{Hom}_A(P, M) \geq n + 1$, und $n + 1$ ist die Anzahl der zu S isomorphen Kompositionsfaktoren von M. Folglich genügt es zu zeigen: $\dim_F \operatorname{Hom}_A(P, M) \leq n + 1$.
Sei $\varphi \in \operatorname{Hom}_A(P, M)$ beliebig. Dann ist $\varphi(\operatorname{Rad}(P)) \subseteq \operatorname{Rad}(M) \subseteq N$, d.h. φ induziert einen A-Homomorphismus $\overline{\varphi} : P/\operatorname{Rad}(P) \to M/N$. Insbesondere induziert ψ einen A-Homomorphismus $\overline{\psi} \neq 0$. Nach Schurs Lemma ist $\operatorname{Hom}_A(P/\operatorname{Rad}(P), M/N) \cong \operatorname{End}_A(S) \cong F$. Folglich ist $\overline{\varphi} = \alpha\overline{\psi}$ für ein $\alpha \in F$. Dies bedeutet: $\varphi(x) - \alpha\psi(x) \in N$ für $x \in P$, d.h. $\operatorname{Bild}(\varphi - \alpha\psi) \subseteq N$. Man kann also $\varphi - \alpha\psi$ als Element in $\operatorname{Hom}_A(P, N)$ auffassen. Dies zeigt: $\dim_F \operatorname{Hom}_A(P, M) \leq \dim_F \operatorname{Hom}_A(P, N) + 1 = n + 1$, und wir sind fertig. □

Definition. Seien A eine endlich-dimensionale F-Algebra und $S_1, \ldots, S_l$ ein Repräsentantensystem für die Isomorphieklassen einfacher A-Linksmoduln. Für $i = 1, \ldots, l$ sei P_i ein unzerlegbarer projektiver A-Linksmodul mit $P_i/\operatorname{Rad}(P_i) \simeq S_i$, und für $i, j = 1, \ldots, l$ sei c_{ij} die Anzahl der zu S_j isomorphen Kompositionsfaktoren von P_i. Dann nennt man $C = (c_{ij}) \in \operatorname{Mat}(l, \mathbb{Z})$ die *Cartanmatrix* und ihre Einträge c_{ij} die *Cartaninvarianten* von A.

Bemerkung.
(i) C hängt – wenn auch nur unwesentlich – von der Numerierung der Moduln $S_1, \ldots, S_l$ ab.
(ii) Nach dem obigen Satz ist $c_{ij} = \dim_F \operatorname{Hom}_A(P_j, P_i)$ für $i, j = 1, \ldots, l$.

32.3. Satz. *Seien A eine endlich-dimensionale F-Algebra, e ein Idempotent in A und M ein endlich erzeugter A-Linksmodul. Dann ist die Abbildung $\Phi : \operatorname{Hom}_A(Ae, M) \to eM$, $\varphi \mapsto \varphi(e)$ eine lineare Bijektion; insbesondere ist $\dim_F \operatorname{Hom}_A(Ae, M) = \dim_F eM$.*

Beweis. Für $\varphi \in \operatorname{Hom}_A(Ae, M)$ ist $\varphi(e) = \varphi(e^2) = e\varphi(e) \in eM$, Daher ist Φ wohldefiniert. Offenbar ist Φ linear. Im Fall $0 = \Phi(\varphi) = \varphi(e)$ ist $\varphi(ae) = a\varphi(e) = 0$ für $a \in A$, also $\varphi = 0$. Daher ist Φ injektiv. Für $m \in M$ existiert umgekehrt ein A-Homomorphismus $\psi : A \to M$ mit $\psi(a) = am$. Durch Einschränkung wird aus ψ ein A-Homomorphismus $\varphi : Ae \to M$ mit $\varphi(e) = em = m$, d.h. $\Phi(\varphi) = m$. Also ist Φ auch surjektiv. □

Bemerkung. Sei wieder $S_1, \ldots, S_l$ ein Repräsentantensystem für die Isomorphieklassen einfacher A-Linksmoduln und $C = (c_{ij})$ die entsprechende Cartanmatrix. Für $i = 1, \ldots, l$ sei P_i ein unzerlegbarer projektiver A-Linksmodul mit $P_i/\operatorname{Rad}(P_i) \simeq S_i$. Nach 22.5 kann man $P_i = Ae_i$ für ein primitives Idempotent e_i in A annehmen. Nach dem obigen Satz ist $c_{ij} = \dim_F(Ae_j, Ae_i) = \dim_F e_j A e_i$ für $i, j = 1, \ldots, l$.

32.4. Satz. *Jede symmetrische F-Algebra besitzt eine symmetrische Cartanmatrix.*

Beweis. Bemerkung 32.3 und Satz 24.6. □

Bemerkung. Insbesondere ist also die Cartanmatrix C jeder Gruppenalgebra symmetrisch. Wir werden im nächsten Semester segen, daß in diesem Fall C stets positiv definit und daß $\det(C)$ stets eine Potenz von $p := \operatorname{char}(F)$ ist.

32.5. Satz. *Seien A eine endlich-dimensionale F-Algebra und e, f Idempotente in A. Genau dann sind die A-Linksmoduln Ae und Af isomorph, wenn eine Einheit u in A existiert mit $u^{-1}eu = f$.*

Beweis.

- $\Rightarrow$: Nach 22.5 ist $Ae \oplus A(1-e) = A = Af \oplus A(1-f)$. Sind Ae und Af isomorph, so auch $A(1-e)$ und $A(1-f)$ nach Krull-Schmidt. Es existiert also ein A-Automorphismus φ von A mit $\varphi(Ae) = Af$ und $\varphi(A(1-e)) = A(1-f)$. Mit $u := \varphi(1)$ ist also $\varphi(a) = \varphi(a \cdot 1) = au$ für $a \in A$. Analog ist $\varphi^{-1}(a) = av$ für $a \in A$ mit $v := \varphi^{-1}(1)$. Also ist $1 = \varphi(\varphi^{-1}(1)) = \varphi(v) = vu$ und analog $1 = uv$, d.h. $u \in UA$ und $v = u^{-1}$. Wegen $Af = \varphi(Ae) = A\varphi(e) = Aeu = Au^{-1}eu$ und $A(1-f) = \varphi(A(1-e)) = A\varphi(1-e) = A(1-e)u = Au^{-1}(1-e)u$ folgt $f = u^{-1}eu$ aus 22.5.
- $\Leftarrow$: Ist $u \in UA$ mit $u^{-1}eu = f$, so ist die Abbildung $Ae \to Aeu = Au^{-1}eu = Af$, $x \mapsto xu$ ein A-Isomorphismus.

□

Bemerkung. Durch $e \mapsto Ae$ erhält man also eine Bijektion zwischen der Menge der Konjugationsklassen primitiver Idempotente in A und der Menge der Isomorphieklassen unzerlegbarer projektiver A-Linksmoduln.

32.6. Bemerkung. Seien A eine endlich-dimensionale F-Algebra und M ein endlich erzeugter A-Linksmodul. Nach Aufgabe 46 ist dann $M^* := \operatorname{Hom}_F(M, F)$ ein endlich erzeugter A-Rechtsmodul, und die Abbildung $U \mapsto U^\perp := \{f \in M^* : f(U) = 0\}$ ist eine Bijektion zwischen der Menge aller Untermoduln von M und der Menge der Untermoduln von M^*. Dabei drehen sich die Inklusionen um: $U \subseteq V \iff V^\perp \subseteq U^\perp$. Man nennt M^* den zu M *dualen* A-Modul.
Nach Aufgabe 46 ist M genau dann projektiv (injektiv), wenn M^* injektiv (projektiv) ist. Außerdem ist mit M uach M^* unzerlegbar und umgekehrt. Da jeder unzerlegbare projektive A-Linksmodul P genau einen maximalen Untermodul, nämlich $\operatorname{Rad}(P)$, hat, hat der entsprechende unzerlegbare injektive A-Rechtsmodul P^* genau einen minimalen Untermodul, nämlich $\operatorname{Soc}(P^*)$ (vgl. Aufgabe 43), und es ist $\operatorname{Soc}(P^*) \simeq (P/\operatorname{Rad}(P))^*$; hier kann man natürlich auch „links“ und „rechts“ vertauschen.
Jede Frobeniusalgebra A über F ist nach Aufgabe 46 zu A^* als A-Linksmodul isomorph; insbesondere ist A als A-Linksmodul injektiv. Daher ist auch jeder endlich erzeugte freie und jeder endlich erzeugte projektive A-Linksmodul injektiv. Analog ist in diesem Fall auch jeder endlich erzeugte projektive A-Rechtsmodul injektiv. Ein endlich erzeugter A-Linksmodul (A-Rechtsmodul) über einer Frobeniusalgebra A ist also genau dann projektiv, wenn er injektiv ist. Insbesondere hat jeder unzerlegbare projektive A-Linksmodul (A-Rechtsmodul) P über einer Frobeniusalgebra A genau einen minimalen Untermodul, nämlich $\operatorname{Soc}(P)$, und genau einen maximalen Untermodul, nämlich $\operatorname{Rad}(P)$.

Satz. *Seien (A, β) eine Frobeniusalgebra über F mit Nakayama-Automorphismus Λ und $e = e^2 \in A$. Dann ist $(eA)^* \simeq A\Lambda(e)$.*

Beweis. Durch Einschränkung von β erhalten wir eine Bilinearform $\beta' : eA \times A\Lambda(e) \to F$. Wegen $A\Lambda(e) = \Lambda(A)\Lambda(e) = \Lambda(Ae)$ ist $\dim A\Lambda(e) = \dim \Lambda(Ae) = \dim Ae = \dim eA$. Ist $y \in Ae$ mit $0 = \beta(eA, \Lambda(y)) =$

$\beta(y, eA) = \beta(ye, A) = \beta(y, A)$, so ist $y = 0$. Daher ist β' nicht ausgeartet. Wir erhalten also eine lineare Bijektion $\Phi : A\Lambda(e) \to (eA)^*$ mit $(\Phi(\Lambda(x)))(y) := \beta(y, \Lambda(x)) = \beta(x, y)$ für $x \in Ae,\ y \in eA$. Wegen

$$\begin{aligned}(a\Phi(\Lambda(x)))(y) &= (\Phi(\Lambda(x)))(ya) \;=\; \beta(x, ya) \;=\; \beta(xy, a)\\ &= \beta(xy, \Lambda(\Lambda^{-1}(a))) \;=\; \beta(\Lambda^{-1}(a), xy)\\ &= \beta(\Lambda^{-1}(a)x, y) \;=\; (\Phi(\Lambda(\Lambda^{-1}(a)x)))(y)\\ &= (\Phi(a\Lambda(x)))(y)\end{aligned}$$

für $a \in A,\ x \in Ae,\ y \in eA$ ist Φ ein A-Isomorphismus. □

Beispiel. Ist A sogar symmetrisch, so ist $\Lambda = \mathrm{id}_A$ und daher $(eA)^* \simeq Ae$.

32.7. Satz. *Seien (A, β) eine Frobeniusalgebra über F mit Nakayama-Automorphismus Λ und $e = e^2 \in A$. Dann ist $\mathrm{Soc}(A\Lambda(e)) \simeq Ae/JAe$.*

Beweis. Nach 32.6 ist $\mathrm{Soc}(A\Lambda(e)) \simeq \mathrm{Soc}((eA)^*) \simeq (eA/eJA)^*$ als A-Linksmodul und als A/JA-Linksmodul. Nun ist aber $eA/eJA = eA/eA \cap JA \simeq eA + JA/JA = (e + JA)(A/JA)$ also A/JA-Rechtsmodul. Da A/JA symmetrisch ist, folgt $((e + JA)(A/JA))^* \simeq (A/JA)(e + JA)$ nach Beispiel 32.6. Daher ist $\mathrm{Soc}(A\Lambda(e)) \simeq (A/JA)(e + JA) \simeq Ae/JAe$ als A/JA-Linksmodul und als A-Linksmodul. □

Beispiel. Ist A symmetrisch, so ist also stets $\mathrm{Soc}(Ae) \simeq Ae/JAe$. Dies trifft insbesondere auf Gruppenalgebren zu.

32.8. Satz. *Seien A eine endlich-dimensionale F-Algebra und $A = P_1 \oplus \ldots \oplus P_r$ mit unzerlegbaren (projektiven) A-Linksmoduln $P_1, \ldots, P_r$. Für $i = 1, \ldots, r$ ist dann $|\{j : 1 \leq j \leq r,\ P_j \simeq P_i\}| = \dim_F P_i/(JA)P_i$.*

Beweis. Wegen $JA = (JA)P_1 \oplus \ldots \oplus (JA)P_r$ ist $A/JA \simeq P_1/(JA)P_1 \oplus \ldots \oplus P_r/(JA)P_r$. Wegen $P_k \simeq P_l \iff P_k/(JA)P_k \simeq P_l/(JA)P_l$ kann man A durch A/JA ersetzen und daher annehmen, daß A halbeinfach ist. Dann ist $A = A_1 \oplus \ldots \oplus A_n$ und $A_i \simeq \mathrm{Mat}(d_i, F)$ mit $d_i \in \mathbb{N}$ für $i = 1, \ldots, n$. Der einzige einfache A_i-Modul S_i hat Dimension d_i, d.h. es ist $A_i \simeq S_i^{d_i}$. Folglich ist $A = S_1^{d_1} \oplus \ldots \oplus S_n^{d_n}$, und für $i \neq j$ ist $S_i \not\simeq S_j$ wegen $A_i S_j = 0 \neq A_i S_i$. □

KAPITEL 33

Bewertungsringe

33.1. Definition. Eine *Bewertung* eines Körpers K ist eine Abbildung $\varphi : K \to \mathbb{R}$ mit folgenden Eingenschaften:

(i) Für $a, b \in K$ ist $\varphi(a) > 0$, $\varphi(ab) = \varphi(a)\varphi(b)$ und $\varphi(a+b) \leq \varphi(a) + \varphi(b)$ (Dreiecksungleichung).
(ii) Für $a \in K$ gilt: $\varphi(a) \Longleftrightarrow a = 0$.

Beispiel.

(i) Der Absolutbetrag ist eine Bewertung in jedem Teilkörper von $\mathbb{C}$.
(ii) Für jeden Körper K hat man die *triviale* Bewertung, definiert durch

$$\varphi(a) := \begin{cases} 1 & \text{für } a \neq 0 \\ 0 & \text{für } a = 0 \end{cases} .$$

(iii) Seien R ein faktorieller Ring mit Quotientenkörper K, p ein Primelement in R und $\gamma \in \mathbb{R}$ mit $0 < \gamma < 1$. Jedes Element x in $K \setminus \{0\}$ kann man in der Form $x = p^a \frac{b}{c}$ mit $a \in \mathbb{Z}$, $b, c \in R \setminus (p)$ schreiben. Setzt man $\varphi(x) := \gamma^a$ und $\varphi(0) := 0$, so erhält man auf diese Weise eine Bewertung von K. Insbesondere liefert dies zu jeder Primzahl p eine Bewertung φ_p von $\mathbb{Q}$, die *p-adische* Bewertung von $\mathbb{Q}$; dabei wählt man i.a. $\gamma = \frac{1}{p}$.

Bemerkung.

(i) Für jede Bewertung φ eines Körpers K und für beliebige Elemente $a, b \in K$ ist $\varphi(a-b) \geq |\varphi(a) - \varphi(b)|$ und $\varphi(-a) = \varphi(a)$. Außerdem ist $\varphi(\zeta) = 1$ für jede Einheitswurzel ζ in K; insbesondere ist $\varphi(1) = 1$.
(ii) Jede Bewertung φ eines Körpers K liefert durch Einschränkung einen Homomorphismus von Gruppen $K^\times \to \mathbb{R}^\times$. Man nennt $\varphi(K^\times)$ *Wertegruppe* von φ. Ist $\varphi(K^\times)$ eine unendliche zyklische Gruppe, so nennt man die Bewertung *diskret*. Ein Beispiel dafür ist die p-adische Bewertung von $\mathbb{Q}$ für jede Primzahl p.
(iii) Für jede Bewertung φ eines Körpers K ist die Abbildung $d : K \times K \to \mathbb{R}$, $(a, b) \mapsto \varphi(a-b)$ eine Metrik. Wir können also Begriffe aus der Analysis verwenden. Zum Beispiel nennt man die Bewertung φ *vollständig*, wenn in (K, d) jede Cauchy-Folge konvergiert.

33.2. Satz. *Für jede diskrete Bewertung φ eines Körpers K gilt:*

(i) *Für $a, b \in K$ ist $\varphi(a+b) \leq \max\{\varphi(a), \varphi(b)\}$. Im Fall $\varphi(a) \neq \varphi(b)$ gilt sogar $\varphi(a+b) = \max\{\varphi(a), \varphi(b)\}$.*
(ii) *$R := \{a \in K : \varphi(a) \leq 1\}$ ist ein Teilring von K und ein lokaler Hauptidealring.*
(iii) *$M := \{a \in K : \varphi(a) < 1\}$ ist das einzige maximale Ideal von R; insbesondere ist $M = \mathrm{Rad}(R)$. Die von 0 verschiedenen Ideale sind also alle von der Form M^i für ein $i \in \mathbb{N}_0$.*
(iv) *$R^\times = \{a \in K : \varphi(a) = 1\}$.*
(v) *Für $a \in K \setminus R$ ist $\frac{1}{a} \in R$. Insbesondere ist K (isomorph zum) Quotientenkörper von R.*

Beweis. Algebra. □

Bemerkung. Es ist $M = pR$ für ein Primelement p in R. Jedes weitere Primelement in R ist zu p assoziiert. Jedes Element x in $R \setminus \{0\}$ hat die Form $x = up^i$ mit $u \in R^\times$ und $i \in \mathbb{N}_0$, und jedes Element x in $K \setminus \{0\}$ hat die Form $x = up^i$ mit $u \in R^\times$ und $i \in \mathbb{Z}$.

Definition. Man nennt R den *Bewertingsring*, M das *Bewertungsideal* und R/M den *Restklassenkörper*.

33.3. Definition. Seien φ eine Bewertung eines Körpers K und L ein Erweiterungskörper von K. Eine *Fortsetzung* von φ auf L ist eine Bewertung ψ von L mit der Eigenschaft $\psi|_K = \varphi$.

Satz. *Zu jeder Bewertung φ eines Körpers K existiert ein Erweiterungskörper $\hat{K}$ und eine Fortsetzung $\hat{\varphi}$ von φ auf $\hat{K}$ mit der Eigenschaft, daß $\hat{K}$ vollständig bzgl. $\hat{\varphi}$ und K dicht in $\hat{K}$ ist.*

Beweis. Algebra. □

Bemerkung. Im wesentlichen sind $\hat{K}$ und $\hat{\varphi}$ eindeutig bestimmt. Man nennt $\hat{K}$ die *Vervollständigung* oder *Komplettierung* von K bzgl. φ. Ist φ diskret, so auch $\hat{\varphi}$, und es ist $\hat{\varphi}(\hat{K} = \varphi(K)$ in diesem Fall. Für die Bewertungsringe R und $\hat{R}$ von φ bzw. $\hat{\varphi}$ und ihre Bewertungsideale M und $\hat{M}$ gilt $\hat{R} = R + \hat{M}$ und $R \cap \hat{M} = M$. Insbesondere ist die Abbildung $R/M \to \hat{R}/\hat{M},\ a + M \mapsto a + \hat{M}$ ein Isomorphismus der Restklassenkörper.

Beispiel. Im Fall $K = \mathbb{Q}$ und $\varphi = \varphi_p$ für eine Primzahl p setzt man $\mathbb{Q}_p := \hat{K}$ und $\mathbb{Z}_p := \hat{R}$. Die Elemente in $\mathbb{Q}_p$ nennt man *p-adische Zahlen* und die in $\mathbb{Z}_p$ *ganze p-adische Zahlen*. Der Restklassenkörper ist in diesem Fall zu $\mathbb{Z}/p\mathbb{Z}$ isomorph.

33.4. Satz (Hensels Lemma)**.** *Sei φ eine vollständige diskrete Bewertung eines Körpers K mit Bewertungsring R und Restklassenkörper $F := R/\operatorname{Rad}(R)$. Seien $f \in R[X]$ und $\overline{f}$ das Bild von f unter der kanonischen Abbildung $R[X] \to F[X]$. Ist $\deg(\overline{f}) = \deg(f)$ und $\overline{f} = \gamma\eta$ mit teilerfremden $\gamma, \eta \in F[X]$, so existieren (teilerfremde) $g, h \in R[X]$ mit $\overline{g} = \gamma,\ \overline{h} = \eta,\ \deg(g) = \deg(\gamma),\ \deg(h) = \deg(\eta)$ und $f = gh$. Ist γ normiert, so kann man auch g normiert wählen.*

Beweis. Sei p ein Primelement in R, also $\operatorname{Rad}(R) = pR$ und $\varphi(o) < 1$. Sei $m := \deg(\gamma)$ und $n := \deg(\eta)$, also $m + n = \deg(\gamma\eta) = \deg(\overline{f}) = \deg(f)$. Wir werden Folgen $(g_k)_{k\in\mathbb{N}_0},\ (h_k)_{k\in\mathbb{N}_0}$ von Polynomen $g_k, h_k \in R[X]$ mit folgenden Eigenschaften konstruieren:

(i) $\deg(g_k) = m,\ \deg(h_k) = n$ für alle k.
(ii) Die Koeffizienten von $f - g_k h_k$ sind durch p^{k+1} teilbar.
(iii) Die Koeffizienten von $g_k - g_{k-1}$ und $h_k - h_{k-1}$ sind durch p^k teilbar.
(iv) Ist γ normiert, so auch g_k für alle k.

Zur Konstruktion dieser Folgen wählen wir zunächst ein beliebiges Polynom $g_0 \in R[X]$ mit $\deg(g_0) = m$ und $\overline{g_0} = \gamma$. (Ist γ normiert, so wählen wir auch g_0 normiert.) Analog wählen wir ein $h_0 \in R[X]$ mit $\deg(h_0) = n$ und $\overline{h_0} = \eta$. Dann gilt (i)–(iv) für $k = 0$. Sei also $k \in \mathbb{N}_0$, und es seien g_k, h_k mit den gewünschten Eigenschaften bereits konstruiert. Dann ist $c_k := (f - g_k h_k)/p^{k+1} \in R[X]$. Da γ und η teilerfremd sind, existieren Polynome α_k, β_k in $F[X]$ mit $-\overline{c_k} = \alpha_k\eta + \beta_k\gamma$. Dabei kann man $\deg(\alpha_k) < m$ annehmen. (Notfalls ersetzt man α_k durch seinen Rest bei der Division durch γ.) Dann ist $\deg(\beta_k) \le n$. Wir wählen Polynome $a_k, b_k \in R[X]$ mit $\deg(a_k) = \deg(\alpha_k),\ \deg(b_k) = \deg(\beta_k),\ \overline{a_k} = \alpha_k,\ \overline{b_k} = \beta_k$. Dann sind die Koeffizienten von $c_k + a_k h_k + b_k g_k$ durch p teilbar. (Tatsächlich sind nämlich $\overline{g_k} = \gamma$ und $\overline{h_k} = \eta$.) Setzt man $g_{k+1} := g_k - a_k p^{k+1}$ und $h_{k+1} := h_k - b_k p^{k+1}$, so sind, wie man leicht nachrechnet, die Bedingungen (i)–(iv) für $k + 1$ erfüllt. Wegen (iii) sind $(g_k)_{k\in\mathbb{N}}$ und $(h_k)_{k\in\mathbb{N}}$ Cauchy-Folgen (d.h. Koeffizienz für Koeffizient), konvergieren also gegen Polynome $g, h \in R[X]$. Da Addition und Multiplikation in R stetig sind, ist $gh = f$ wegen (ii). Aus (iii) folgt $\overline{g} = \overline{g_0} = \gamma,\ \overline{h} = \overline{h_0} = \eta$, und aus (i) folgt $\deg(g) = m,\ \deg(h) = n$. Schließlich folgt aus (iv), daß mit γ auch g normiert ist. □

33.5. Satz. *Sei φ eine vollständige diskrete Bewertung eines Körpers K mit Bewertungsring R und Restklassenkörper $F := R/\operatorname{Rad}(R)$. Dann gilt für jedes irreduzible Polynom $f = \alpha_0 X^n + \alpha_1 X^{n-1} + \ldots + \alpha_n \in K[X]$ und $i = 0, \ldots, n$: $\varphi(\alpha_i) \le \max\{\varphi(\alpha_0), \varphi(\alpha_n)\}$.*

Beweis. Wir nehmen $t := \max\{\varphi(\alpha_0), \ldots, \varphi(\alpha_n)\} > \max\{\varphi(\alpha_0), \varphi(\alpha_n)\}$ an und setzen $r := \max\{i : 0 \le i \le n,\ \varphi(\alpha_i) = t\}$. Dann ist $0 < r < n,\ g := \alpha_r^{-1} f = \beta_0 X^n + \beta_1 X^{n-1} + \ldots + \beta_n \in R[X],\ \beta_r = 1$ und $\beta_{r+1}, \ldots, \beta_n \in \operatorname{Rad}(R)$. Also ist $\overline{g} = X^{n-1}(\overline{\beta_0} X^r + \ldots + \overline{\beta_{r-1}} X + 1)$ das Produkt von zwei teilerfremden, nichtkonstanten Polynomen in $F[X]$. Nach Hensels Lemma ist daher auch g das Produkt von zwei teilerfremdem, nichtkonstanten Polynomen in $R[X]$. Folglich ist g reduzibel, und damit auch f. Widerspruch. □

33.6. Satz. *Sei φ eine vollständige diskrete Bewertung eines Körpers K mit Bewertungsring R, und sei $L|K$ eine endliche Körpererweiterung. Ein Element $a \in L$ ist genau dann ganz über R, wenn $N_K^L(a) \in R$ ist.*

Beweis.

$\Rightarrow$: Algebra.

$\Leftarrow$: Sei $a \in L$ mit $N_K^L(a) \in R$, und sei $f = X^n + \alpha_1 X^{n-1} + \ldots + \alpha_n$ das Minimalpolynom von a über K. Da $\pm N_K^L(a)$ eine Potenz von α_n ist, folgt $\alpha_n \in R$. Wegen 33.5 ist also $\varphi(a_i) \leq \max\{\varphi(1), \varphi(\alpha_n)\} = 1$, d.h. $\alpha_i \in R$ für alle $i = 1, \ldots, n$. Daher ist $f \in R[X]$ und a ganz über R.

□

33.7. Satz. *Sei φ eine vollständige diskrete Bewertung eines Körpers K, sei ψ eine Fortsetzung von φ auf einen Erweiterungskörper L von K, seien $b_1, \ldots, b_m$ über K linear unabhängige Elemente in L, sei $(x_k)_{k\in\mathbb{N}}$ eine Folge von Elementen in L, und sei $x_k = \sum_{i=1}^m \xi_{ik} b_i$ mit $\xi_{ik} \in K$ für $k \in \mathbb{N}$ und $i = 1, \ldots, m$. Dann gilt: $(x_k)_{k\in\mathbb{N}}$ ist eine Cauchy-Folge in L $\iff$ $(\xi_{ik})_{k\in\mathbb{N}}$ ist eine Cauchy-Folge in K für $i = 1, \ldots, m$.*

Beweis.

$\Leftarrow$: Klar.

$\Rightarrow$: (Induktion nach m) Im Fall $m = 1$ ist $x_k = \xi_{1k} b_1$ für $k \in \mathbb{N}$, und die Behauptung ist trivial. Sei also $m > 1$ und $(x_k)_{k\in\mathbb{N}}$ eine Cauchy-Folge in L. Wir nehmen an, daß $(\xi_{mk})_{k\in\mathbb{N}}$ keine Cauchy-Folge ist. Dann existieren $\varepsilon > 0$ und $p_1, p_2, \ldots, q_1, q_2, \ldots \in \mathbb{N}$ mit $p_1 < p_2 < \ldots$, $q_1 < q_2 < \ldots$ und $\varphi(\xi_{mp_k} - \xi_{mq_k}) > \varepsilon$ für alle $k \in \mathbb{N}$. Setzt man

$$y_k := \frac{x_{p_k} - x_{q_k}}{\xi_{mp_k} - \xi_{mq_k}}$$

für $k \in \mathbb{N}$, so ist $(y_k)_{k\in\mathbb{N}}$ eine Nullfolge. Ferner ist $z_k := y_k - b_m = \sum_{i=1}^{m-1} \zeta_{ik} b_i$ mit $\zeta_{ik} \in K$ für $k \in \mathbb{N}$, $i = 1, \ldots, m-1$, und die Folge $(z_k)_{k\in\mathbb{N}}$ konvergiert gegen $-b_m$, ist also insbesondere eine Cauchy-Folge. Für $i = 1, \ldots, m-1$ ist daher $(\zeta_{ik})_{k\in\mathbb{N}}$ nach Induktionsvoraussetzung eine Cauchy-Folge; insbesondere existiert $\lim_{k\to\infty} \zeta_{ik} =: \zeta_i$. Dann ist

$$\sum_{i=1}^{m-1} \zeta_i b_i + b_m = \lim_{k\to\infty} \sum_{i=1}^{m-1} \zeta_{ik} b_i + b_m = \lim_{k\to\infty} z_k + b_m = 0$$

im Widerspruch zur linearen Unabhängigkeit von $b_1, \ldots, b_m$.

□

Bemerkung.

(i) Ist $(x_k)_{k\in\mathbb{N}}$ sogar eine Nullfolge, so ist auch $(\xi_{ik})_{k\in\mathbb{N}}$ für $i = 1, \ldots, m$ eine Nullfolge (und auch umgekehrt); denn mit $(x_k)_{k\in\mathbb{N}}$ ist auch $(\xi_{ik})_{k\in\mathbb{N}}$ für $i = 1, \ldots, m$ eine Cauchy-Folge, also konvergent. Ist $\xi_i := \lim_{k\to\infty} \xi_{ik}$ für $i = 1, \ldots, m$, so ist

$$0 = \lim_{k\to\infty} x_k = \lim_{k\to\infty} \sum_{i=1}^{m} \xi_{ik} b_i = \sum_{i=1}^{m} \xi_i b_i,$$

also $\xi_1 = \ldots = \xi_m = 0$.

(ii) Ist $[L : K] < \infty$, so ist L vollständig bzgl. ψ; in diesem Fall kann man nämlich $b_1, \ldots, b_m$ als K-Basis von L wählen. Ist $(x_k)_{k\in\mathbb{N}}$ eine Cauchy-Folge in L, so ist nach dem Satz $(\xi_{ik})_{k\in\mathbb{N}}$ für $i = 1, \ldots, m$ eine Cauchy-Folge in K, d.h. $\xi_i := \lim_{k\to\infty} \xi_{ik}$ existiert für $i = 1, \ldots, m$. Daher ist aber $\sum_{i=1}^m \xi_i b_i = \lim_{k\to\infty} \sum_{i=1}^m \xi_{ik} b_i = \lim_{k\to\infty} x_k$.

33.8. Satz. *Seien φ eine vollstänfige diskrete Bewertung eines Körpers K mit Bewertungsring R und L eine Körpererweiterung endlichen Grades m von K. Dann existiert genau eine Fortsetzung ψ von φ auf L. Diese ist diskret, vollständig und wird gegeben durch*

$$\psi(a) := \varphi\Big(N_K^L(a)\Big)^{1/m}$$

für $a \in L^\times$.

Beweis. Seien ψ, ψ' zwei Fortsetzungen von φ zu Bewertungen von L. Nach 33.7 stimmen die Nullfolgen bzgl. ψ und die bzgl. ψ' überein. Daher sind ψ und ψ' äquivalent im Sinne der Algebra. Folglich existiert ein $\rho \in \mathbb{R}$ mit $\rho > 0$ und $\psi'(a) = \psi(a)^\rho$ für alle $a \in L$. Ist p ein Primelement in R, so ist also $1 \neq \varphi(p) = \psi'(p) = \psi(p)^\rho = \varphi(p)^\rho$, d.h. $rho = 1$. Folglich ist $\psi' = \psi$.
Umgekehrt definieren wir ψ durch $\psi(a) := \varphi(N_K^L(a))^{1/m}$ für $a \in L^\times$ und $\psi(0) := 0$. Dann ist $\psi(a) \geq 0$ für $a \in L$, $\psi(a) = 0 \Leftrightarrow a = 0$, $\psi(ab) = \psi(a)\psi(b)$ für $a, b \in L$, und schließlich gilt sogar $\psi(a + b) \leq \max\{\psi(a), \psi(b)\}$; denn zum Beweis hiervon ist o.B.d.A. $a = 1$ und $\psi(b) \leq 1$ (notfalls dividieren oder vertauschen wir). Dann ist $N_K^L(b) \in R$, d.h. b und $1 + b$ sind ganz über R. Folglich ist $N_K^L(1 + b) \in R$ und $\psi(1 + b) = \varphi(N_K^L(1 + b))^{1/m} \leq 1 = \max\{\psi(1), \psi(b)\}$. Dies zeigt, daß ψ eine Bewertung ist.
Für $a \in K^\times$ ist $\psi(a) = \varphi(N_K^L(a))^{1/m} = \varphi(a^m)^{1/m} = \varphi(a)$. Schreibt man $\varphi(K^\times) = \langle\gamma\rangle$ mit $\gamma \in \mathbb{R}$, so ist $\psi(L^\times)$ eine Untergruppe von $\langle\gamma^{1/m}\rangle$, also insbesondere zyklisch. Die Vollständigkeit von ψ folgt aus Bemerkung 33.7(ii). □

Bemerkung. In der obigen Situation hat $\varphi(K^\times)$ endlichen Index in $\psi(L^\times)$. Man nennt $e_{L|K} := |\psi(L^\times) : \varphi(K^\times)|$ den *Verzweigungsindex* der Körpererweiterung $L|K$. Im Fall $e_{L|K} = 1$ nennt man $L|K$ *unverzweigt*. Für die Bewertungsringe R und S und die Bewertungsideale P und Q von φ und ψ gilt: $R \cap Q = P$. Daher ist die Abbildung $F := R/P \to S/Q =: E$, $r + P \mapsto r + Q$ ein Monomorphismus von Körpern. Wir werden ihn benutzen, um F als Teilkörper von E aufzufassen, und nennen $[E : F] =: f_{L|K}$ den *Trägheitsgrad* der Erweiterung $L|K$.

33.9. Satz. *Seien φ eine vollständige diskrete Bewertung eines Körpers K, L ein Erweiterungkörper des endlichen Grades n von K und ψ die Fortsetzung von φ zu einer Bewertung von L. Dann gilt: $n = e_{L|K} f_{L|K}$.*

Beweis. Seien R und S die Bewertungsringe von φ und ψ, P, Q die entsprechenden Bewertungsideale und F, E die entsprechenden Restklassenkörper. Seien $a_1, \ldots, a_s \in S$ mit der Eigenschaft, daß $a_1 + Q, \ldots, a_s + Q$ linear unabhängig über F sind. Ferner seien $b_1, \ldots, b_t \in L^\times$ mit der Eigenschaft, daß $\psi(b_1), \ldots, \psi(b_t)$ in verschiedenen Nebenklassen nach $\varphi(K^\times)$ liegen. Wir werden zunächst zeigen, daß die Elemente $a_i b_j \in L$ $(i = 1, \ldots, s,\ j = 1, \ldots, t)$ linear unabhängig über K sind. Sei also $0 = \sum_{i=1}^s \sum_{j=1}^t \alpha_{ij} a_i b_j$ mit $\alpha_{ij} \in K$ für $i = 1, \ldots, s,\ j = 1, \ldots, t$. Wir können annehmen, daß für $j = 1, \ldots, t$ ein $i \in \{1, \ldots, s\}$ mit $\alpha_{ij} \neq 0$ existiert und suchen einen Widerspruch.
Für $j = 1, \ldots, t$ sei $\mu_j \in \{\alpha_{1j}, \ldots, \alpha_{sj}\}$ so ausgewählt, daß $\varphi(\mu_j)$ möglichst groß ist. Dann ist $0 = \sum_{i=1}^s \sum_{j=1}^t \frac{\alpha_{ij}}{\mu_j} a_i(\mu_j b_i)$. Wir können also $b_1, \ldots, b_t$ durch $\mu_1 b_1, \ldots, \mu_t b_t$ ersetzen und daher annehmen, daß $\alpha_{ij} \in R$ für $i = 1, \ldots, s,\ j = 1, \ldots, t$ ist. Nach passender Umnumerierung können wir ferner $\psi(b_1) > \ldots > \psi(b_t)$ und $\alpha_{11} \notin P$ annehmen. Dann ist $\sum_{i=1}^s \sum_{j=1}^t \alpha_{ij} a_i \frac{b_j}{b_1} = 0$ und $\frac{b_2}{b_1}, \ldots, \frac{b_t}{b_1} \in Q$. Folglich ist $0 = \sum_{i=1}^s (\alpha_{i1} + P)(a_i + Q)$ im Widerspruch zur linearen Unabhängigkeit von $a_1 + Q, \ldots, a_s + Q$. Dies zeigt $e_{L|K} f_{L|K} \leq n$.
Zum Beweis der Gleichheit wählen wir $a_1, \ldots, a_f \in S$ so, daß $a_1 + Q, \ldots, a_f + Q$ eine F-Basis von E bilden. Außerdem wählen wir Primelemente $p \in R$ und $q \in S$. Dann ist $\varphi(K^\times) = \langle\varphi(p)\rangle$ und $\psi(L^\times) = \langle\psi(q)\rangle$. Wegen $|\psi(L^\times) : \varphi(K^\times)| = e_{L|K} =: e$ bilden die Elemente $1, \psi(q), \ldots, \psi(q^{e-1})$ ein Repräsentantensystem für $\psi(L^\times)/\varphi(K^\times)$. Nach dem ersten Teil des Beweises sind die Elemente $a_i q^j$ $(i = 1, \ldots, f,\ j = 0, \ldots, e-1)$ linear unabhängig über K. Es genügt also zu zeigen, daß diese Elemente den K-Vektorraum L erzeugen. Sei also $x \in L$ und o.B.d.A. $x \neq 0$. Dann ist $\psi(x) = \varphi(p)^k \psi(q)^j$ für ein $k \in \mathbb{Z}$ und ein $j \in \{0, \ldots, e-1\}$. Daher ist $\frac{x}{p^k q^j} \in S$. Folglich existieren $r_1, \ldots, r_f \in R$ und $z \in Q$ mit $\frac{x}{p^k q^j} = \sum_{i=1}^f r_i a_i + z$, d.h. $x = \sum_{i=1}^f r_i a_i p^k q^j + y$ mit $\psi(y) < \psi(x)$. Dann wiederholen wir das Verfahren mit y statt x. Auf diese Weise erhalten wir eine Darstellung

$$x = \sum_{i=1}^{t} \sum_{j=0}^{e-1} \left(\sum_{k=k_0}^{\infty} r_{ijk} p^k \right) a_i q^j$$

mit konvergierenden Reihen $\sum_{k=k_0}^\infty r_{ijk} p^k$ für $i = 1, \ldots, f,\ j = 0, \ldots, e-1$. Also ist $x = \sum_{i=1}^f \sum_{j=0}^{e-1} s_{ij} a_i q^j$ mit $s_{ij} \in K$ für $i = 1, \ldots, f,\ j = 0, \ldots, e-1$. □

Bemerkung. Ist M ein endlicher Erweiterungskörper von L, so gilt bekanntlich $[M:K] = [M:L][L:K]$. Man überlegt sich leicht, daß auch $e_{M|K} = e_{M|L}e_{L|K}$ und $f_{M|K} = f_{M|L}f_{L|K}$ gilt.

33.10. Satz. *Sei φ eine vollständige diskrete Bewertung des Körpers K mit Bewertungsring R und endlichem Restklassenkörper F. Für $n \in \mathbb{N}$ existiert dann eine unverzweigte Körpererweiterung L des Grades n von K.*

Beweis. Bekanntlich besitzt F einen Erweiterungskörper E des Grades n. Wir schreiben $E = F(y)$ für ein $y \in E$ und bezeichnen mit f das Minimalploynom von y über F. Dann ist $\deg(f) = n$. Wir wählen ein normiertes Polynom $g \in R[X]$ mit $\deg(g) = n$ und $\overline{g} = f$. Dann ist g irreduzibel in $R[X]$ und $K[X]$. Sei x Nullstelle von g über K und $L := K(x)$, also $[L:K] = n$. Sei ψ die Fortsetzung von φ auf L und S der Bewertungsring von ψ. Dann ist $x \in S$ und $x + \mathrm{Rad}(S)$ liegt im Restklassenkörper von ψ. Daher ist $n \leq [S/\mathrm{Rad}(S) : F] \leq [L:K] = n$. Nach 33.9 ist also $e_{L|K} = 1$. □

33.11. Satz. *Sei φ eine vollständige diskrete Bewertung eines Körpers K mit Bewertungsring R und endlichem Restklassenkörper F, und sei ψ eine unverzweigte Fortsetzung von φ auf eine endliche Körpererweiterung L von K. Dann ist der Restklassenkörper E von ψ auch endlich, und L ist der Zerfällungskörper von $X^{|E|-1} - 1$ über K.*

Beweis. Nach 33.9 ist $[E:F] = [L:K] < \infty$, also $q := |E| < \infty$. Bekanntlich zerfällt $X^{q-1} - 1$ in $E[X]$ in paarweise verschiedene Linearfaktoren. Nach Hensels Lemma zerfällt $X^{q-1} - 1$ also auch in $L[X]$ in paarweise verschiedene Linearfaktoren. Folglich enthält L eine primitive $(q-1)$-te Einheitswurzel ζ. Dann ist $\psi|K(\zeta)$ eine vollständige diskrete Bewertung mit zu E isomorphem Restklassenkörper. Nach 33.9 ist $[L:K] \geq [K(\zeta):K] \geq [E:F] = [L:K]$, also $L = K(\zeta)$. □

33.12. Bemerkung. Sei φ eine vollständige diskrete Bewertung eines Körpers K mit endlichem Restklassenkörper F der Ordnung q, und sei $\tilde{K}$ ein algebraischer Abschluß von K. Für $n \in \mathbb{N}$ enthält $\tilde{K}$ nach 33.10 und 33.11 genau eine unverzweigte Körpererweiterung K_n des Grades n von K, nämlich den Zerfällungskörper des Polynoms $X^{q^n-1} - 1$ über K. Im Fall $m \mid n$ ist dabei $K_m \subseteq K_n$. Daher ist

$$L := \bigcup_{n\in\mathbb{N}} K_n$$

ein Teilkörper von $\tilde{K}$, und die Bewertung φ von K kann man in eindeutiger Weise zu einer Bewertung ψ von L fortsetzen. Der Restklassenkörper von ψ ist der algebraische Abschluß von F. Die Bewertung ψ von L ist diskret mit $\psi(L^\times) = \varphi(K^\times)$, aber i.a. nicht vollständig. Wenn man jedoch will, kann man L nich vervollständigen (ohne den Restklassenkörper und die Wertegruppe zu verändern). Mann kann aber φ nicht zu einer diskreten Bewertung von $\tilde{K}$ fortsetzen.

KAPITEL 34

Ordnungen

Sei φ eine vollständige diskrete Bewertung eines Körpers K der Charakteristik 0 mit Bewertungsring R, Bewertungsideal $\operatorname{Rad}(R) = \pi R$ und algebraisch abgeschlossenem Restklassenkörper $F = R/\pi R$ der Charakteristik $p > 0$.

34.1. Bemerkung. Seien M ein endlich erzeugter freier R-Modul und $b_1, \dots, b_d$ eine R-Basis von M. Wir definieren eine Abbildung $M \to \mathbb{R}$, $m \mapsto \|m\|$ durch $\|0\| := 0$ und $\|m\| := \varphi(\pi)^n$, falls $m \in \pi^n M \setminus \pi^{n+1} M$; wegen $\bigcap_{n \in \mathbb{N}} \pi^n M = 0$ ist dies wohldefiniert, und es gilt:

(i) $\|m\| \geq 0$ für $m \in M$.
(ii) $\|m\| = 0 \iff m = 0$.
(iii) $\|rm\| = \varphi(r)\|m\|$ für $r \in R$, $m \in M$.
(iv) $\|m + m'\| \leq \max\{\|m\|, \|m'\|\}$ für $m, m' \in M$.

Daher ist die Abbildung $d : M \times M \to \mathbb{R}$, $(m, m') \mapsto \|m - m'\|$ eine Metrik auf M. Analytische Begriffe beziehen sich im folgenden stets auf diese Metrik. Aus den obigen Eigenschaften folgt leicht, daß Addition und Multiplikation mit Skalaren stetige Abbildungen sind. Da R ein Hauptidealring ist, sind Untermoduln von M wieder frei und abgeschlossene Teilmengen von M.
Sei $(m_n)_{n \in \mathbb{N}}$ eine Folge von Elementen in M, und sei $m_n = \sum_{i=1}^d r_{ni} b_i$ mit $r_{ni} \in R$ für $n \in \mathbb{N}$, $i = 1, \dots, d$. Ist $(m_n)_{n \in \mathbb{N}}$ eine Cauchy-Folge in M, so ist $(r_{ni})_{n \in \mathbb{N}}$ für $i = 1, \dots, d$ eine Cauchy-Folge in R, konvergiert also gegen ein Element $r_i \in R$. Daher konvergiert $(m_n)_{n \in \mathbb{N}}$ gegen $\sum_{i=1}^d r_i b_i$. Dies zeigt, daß M ein vollständiger metrischer Raum ist.
Ferner kann man $M/\pi M$ als Modul über $R/\pi R = F$, d.h. als F-Vektorraum auffassen; dabei ist $\dim_F M/\pi M = \operatorname{rk}_R M$. Den Übergang von M zu $M/\pi M$ nennt man *Reduktion modulo* π.

34.2. Definition. Eine *R-Ordnung* ist eine R-Algebra Λ, die als R-Modul endlich erzeugt und frei ist.

Beispiel.

(i) Die Gruppenalgebra RG einer endlichen Gruppe G ist stets eine R-Ordnung.
(ii) Für $n \in \mathbb{N}$ ist $\operatorname{Mat}(n, R)$ eine R-Ordnung.
(iii) Jede Unteralgebra einer R-Ordnung ist wieder eine R-Ordnung.
(iv) Für R-Ordnungen Λ, Λ' sind auch $\Lambda \times \Lambda'$ und $\Lambda \otimes_R \Lambda'$ R-Ordnungen.

Bemerkung. Für Elemente a, b einer R-Ordnung Λ ist stets $\|ab\| \leq \|a\| \cdot \|b\|$. Daher ist auch die Multiplikation in Λ eine stetige Abbildung.

Satz. *Sei Λ eine R-Ordnung. Dann ist $\pi\Lambda \subseteq \operatorname{Rad}(\Lambda)$ und $\operatorname{Rad}(\Lambda)^n \subseteq \pi\Lambda$ für ein $n \in \mathbb{N}$.*

Beweis. Sei M ein einfacher Λ-Modul. Da πM ein Λ-Untermodul vn M ist, folgt $\pi M \in \{0, M\}$. Nach Nakayamas Lemma ist $\pi M \neq M$, also $\pi M = 0$. Folglich ist $\pi 1 \in \operatorname{Rad}(\Lambda)$ und $\pi\Lambda \in \operatorname{Rad}(\Lambda)$. Offenbar ist $A := \Lambda/\pi\Lambda$ eine endlich-dimensionale F-Algebra mit $JA = \operatorname{Rad}(A) = \operatorname{Rad}(\Lambda)/\pi\Lambda$. Daher existiert ein $n \in \mathbb{N}$ mit $0 = (JA)^n = \operatorname{Rad}(\Lambda)^n + \pi\Lambda/\pi\Lambda$, d.h. $\operatorname{Rad}(\Lambda)^n \subseteq \pi\Lambda$. $\square$

34.3. Satz. *Seien Λ eine R-Ordnung und f ein Idempotent in der endlich-dimensionalen F-Algebra $\Lambda/\pi\Lambda$. Dann existiert ein Idempotent e in Λ mit $f = e + \pi\Lambda$.*

Bemerkung. Man sagt, daß man Idempotente *heben* oder *liften* kann.

Beweis. Sei $e_0 \in \Lambda$ beliebig mit $e_0 + \pi\Lambda = f$. Dann ist $e_0^2 - e_0 \in \pi\Lambda$. Sei $n \in \mathbb{N}$ und bereits $e_{n-1}^2 - e_{n-1} \in \pi^{2^{n-1}}\Lambda$ gezeigt. Setzt man $e_n := 3e_{n-1}^2 - 2e_{n-1}^3$, so gilt:

$$\begin{aligned} e_n^2 - e_n &= 9e_{n-1}^4 - 12e_{n-1}^5 + 4e_{n-1}^6 - 3e_{n-1}^2 + 2e_{n-1}^3 \\ &= 4(e_{n-1}^2 - e_{n-1})^3 - 3(e_{n-1}^2 - e_{n-1})^2 \\ &\in (\pi^{2^{n-1}}\Lambda)^3 + (\pi^{2^{n-1}}\Lambda)^2 \subseteq \pi^{2^n}\Lambda. \end{aligned}$$

Ferner ist $e_n - e_{n-1} = (1 - 2e_{n-1})(e_{n-1}^2 - e_{n-1}) \in \pi^{2^{n-1}}\Lambda$. Daraus folgt, daß $(e_n)_{n\in\mathbb{N}}$ eine Cauchy-Folge ist. Diese konvergiert gegen ein Element $e \in \Lambda$ mit $e^2 - e = \lim_{n\to\infty} e_n^2 - e_n = 0$. Wegen $e_n - e_0 \in \pi\Lambda$ für alle $n \in \mathbb{N}$ ist auch $e - e_0 \in \pi\Lambda$, d.h. $e + \pi\Lambda = e_0 + \pi\Lambda = f$. □

34.4. Satz. *Seien Λ eine R-Ordnung und $u \in \Lambda$. Dann gilt: $u \in \Lambda^\times \iff u + \pi\Lambda \in (\Lambda/\pi\Lambda)^\times$.*

Beweis.

$\Rightarrow$: Trivial.

$\Leftarrow$: Sei $u + \pi\Lambda \in (\Lambda/\pi\Lambda)^\times$, also $uv + \pi\Lambda = 1 + \pi\Lambda$ für ein $v \in \Lambda$. Dann ist $y := 1 - uv \in \pi\Lambda$. Daher konvergiert die Reihe $\sum_{n=0}^\infty y^n$ in Λ, und es ist $\sum_{n=0}^\infty y^n = (1-y)\sum_{n=0}^\infty y^n = 1$. Folglich ist u rechtsinvertierbar, und analog ist u linksinvertierbar.

□

34.5. Satz. *Für eine R-Ordnung $\Lambda \neq 0$ sind äquivalent:*

(1) *Λ ist ein lokaler Ring.*
(2) *$\Lambda/\pi\Lambda$ ist ein lokaler Ring.*
(3) *0 und 1 sind die einzigen Idempotente in $\Lambda/\pi\Lambda$.*
(4) *0 und 1 sind die einzigen Idempotente in Λ.*

Beweis.

(1)$\Leftrightarrow$(2): 34.4.
(2)$\Leftrightarrow$(3): 22.2.
(3)$\Leftrightarrow$(4): 34.3.

□

34.6. Satz. *Seien Λ eine R-Ordnung und e, f Idempotente in Λ mit $e + \pi\Lambda = f + \pi\Lambda$. Dann existiert eine Einheit u in Λ mit $ueu^{-1} = f$.*

Beweis. Wir setzen $u := 1 - e - f + 2fe$. Wegen $u + \pi\Lambda = 1$ ist $u \in \Lambda^\times$ nach 34.4. Wegen $ue = fe = fu$ folgt die Behauptung. □

34.7. Definition. Idempotente e, f in einer R-Ordnung Λ mit $ef = 0 = fe$ nennt man *orthogonal*. Ein Idempotent g in Λ nennt man *primitiv*, wenn keine orthogonalen Idempotente e, f in Λ existieren mit $g = e + f$ und $e \neq 0 \neq f$.

Bemerkung. Wie in 22.3 zeigt man, daß ein Idempotent g in Λ genau dann primitiv ist, wenn $g\Lambda g$ ein lokaler Ring ist. Daraus folgt leicht, daß ein Idempotent g in Λ genau dann primitiv ist, wenn $g + \pi\Lambda$ ein primitives Idempotent in der endlich-dimensionalen F-Algebra $\Lambda/\pi\Lambda$ ist. Ferner ergibt sich wie in 22.5:

Satz (Rosenbergs Lemma). *Seien Λ eine R-Ordnung, $I_1, \ldots, I_n$ Ideale in Λ und e ein primitives Idempotent in Λ mit $e \in I_1 + \ldots + I_n$. Dann ist $e \in I_j$ für ein $j \in \{1, \ldots, n\}$.*

34.8. Definition. Sei Λ eine R-Ordnung. Die in $Z(\Lambda)$ primitiven Idempotente bezeichnet man als *Blockidempotente* von Λ, und die von den Blockidempotenten erzeugten Ideale nennt man die *Blöcke* von Λ.

Bemerkung. Wie in 22.6 zeigt man, daß Λ nur endlich viele Blockidempotente $e_1, \ldots, e_r$ enthält. Diese sind paarweise orthogonal mit $e_1 + \ldots + e_r = 1$. Daraus folgt, daß $\Lambda = \Lambda e_1 \oplus \ldots \oplus \Lambda e_r$ mit $(\Lambda e_i)(\Lambda e_r) = 0$ für $i \neq j$ ist. Jeder Block Λe_i ist selbst eine R-Ordnung mit Einselement e_i. Blöcke und Blockidempotente von Λ bestimmen sich also gegenseitig. Ferner ist $\Lambda \cong \Lambda e_1 \times \ldots \times \Lambda e_r$. Wie in 22.9 zeigt man, daß für jedes Blockidempotent e in Λ das Idempotent $e + \pi\Lambda$ ein Blockidempotent in der endlich-dimensionalen F-Algebra $\Lambda/\pi\Lambda$ ist. Daher entsprechen sich Blöcke in Λ und Blöcke in $\Lambda/\pi\Lambda$.

KAPITEL 35

Gitter

Sei φ eine vollständige diskrete Bewertung eines Körpers K der Charakteristik 0 mit Bewertungsring R, Bewertungsideal $\mathrm{Rad}(R) = \pi R$ und algebraisch abgeschlossenem Restklassenkörper $F = R/\pi R$ der Charakteristik $p > 0$.

35.1. Definition. Seien Λ eine R-Ordnung und L ein Λ-Modul, der als R-Modul endlich erzeugt und frei ist. Dann nennt man L ein Λ-*Gitter*.

Bemerkung. Untermoduln, direkte Produkte und Tensorprodukte (soweit sinnvoll) von Gittern sind wieder Gitter. Dagegen sind Faktormoduln von Gittern in der Regel keine Gitter. Für jedes Λ-Gitter L ist $L/\pi L$ ein (endlich-dimensionaler) Modul über der endlich-dimensionalen F-Algebra $\Lambda/\pi\Lambda$. Man sagt, daß $L/\pi L$ entsteht durch *Reduktion modulo* π aus L.

Satz. *Für jede R-Ordnung Λ und jedes Λ-Gitter L ist $\mathrm{End}_\Lambda(L)$ wieder eine R-Ordnung.*

Beweis. $\mathrm{End}_\Lambda(L)$ ist eine Unteralgebra von $\mathrm{End}_R(L)$, und $\mathrm{End}_R(L) \cong \mathrm{Mat}(n, R)$, wobei $n = \mathrm{rk}_R L$ ist. □

35.2. Satz. *Sei Λ eine R-Ordnung. Ein Λ-Gitter L ist genau dann unzerlegbar, wenn $\mathrm{End}_\Lambda(L)$ ein lokaler Ring ist.*

Beweis.

$\Rightarrow$: Sei L ein unzerlegbarer Λ-Gitter. Dann sind 0 und 1 die einzigen Idempotente in der R-Ordnung $\mathrm{End}_\Lambda(L)$. Nach 34.5 ist $\mathrm{End}_\Lambda(L)$ ein lokaler Ring.

$\Leftarrow$: Algebra.

□

Bemerkung. Wie in der Algebra gezeigt, folgt aus diesem Satz, daß für Λ-Gitter stets der Satz von Krull-Schmidt gilt, d.h., ist L ein Λ-Gitter und ist $L = M_1 \oplus \ldots \oplus M_m = N_1 \oplus \ldots \oplus N_n$ mit unzerlegbaren Λ-Gittern $M_1, \ldots, M_m, N_1, \ldots, N_n$, so ist $m = n$ und $M_i \simeq N_i$ für $i = 1, \ldots, n$ bei geeigneter Numerierung. Ferner besitzt jedes Λ-Gitter eine Zerlegung in endlich viele unzerlegbare Λ-Gitter.

35.3. Bemerkung. Im folgenden betrachten wir Gitter über der R-Ordnung RG, wobei G eine endliche Gruppe ist. Diese Gitter kann man wie üblich auf Gruppenalgebren von Untergruppen von G einschränken und zu Gruppenalgebren von endlichen Obergruppen von G induzieren. Dabei gelten die gewöhnlichen Rechenregeln wie z.B. die Formeln von Mackey und Frobenius (vgl. Vorlesung „Geordnete Mengen II"). Außerdem vertauschen Restriktion und Induktion mit der Reduktion modulo π, wie der folgende Satz zeigt:

Satz. *Sei G eine endliche Gruppe und H eine Untergruppe von G.*

(i) *Für jedes RG-Gitter L ist $\mathrm{Res}^G_H(L)/\pi\,\mathrm{Res}^G_H(L) \simeq \mathrm{Res}^G_H(L/\pi L)$.*

(ii) *Für jedes RH-Gitter M ist $\mathrm{Ind}^G_H(M)/\pi\,\mathrm{Ind}^G_H(M) \simeq \mathrm{Ind}^G_H(M/\pi M)$.*

Dabei sollte man jeweils $RG/\pi RG$ und FG identifizieren.

Beweis.

(i) Trivial.

(ii) Einfach.

□

35.4. Definition. Seien L, M Gitter über der R-Ordnung Λ. Wir schreiben $M \mid L$, falls ein Λ-Gitter N existiert mit $M \oplus N \simeq L$.

Satz. *Seien G eine endliche Gruppe, H eine Untergruppe von G und L ein RG-Gitter. Dann sind äquivalent:*

(1) $L \mid \mathrm{Ind}_H^G(\mathrm{Res}_H^G(L))$.

(2) $L \mid \mathrm{Ind}_H^G(M)$ *für ein RH-Gitter M.*

(3) *Ist $A \xrightarrow{\alpha} B \longrightarrow 0$ eine exakte Folge von RG-Gittern und sind $f \in \mathrm{Hom}_{RG}(L, B)$, $g \in \mathrm{Hom}_{RH}(L, A)$ mit $\alpha \circ g = f$, so existiert ein $g' \in \mathrm{Hom}_{RG}(L, A)$ mit $\alpha \circ g' = f$.*

$$\begin{tikzcd} & L \arrow[d, "f"] \arrow[dl, dotted, "g'"'] & \\ A \arrow[r, "\alpha"] & B \arrow[r] & 0 \end{tikzcd}$$

(4) *Ist $\mathcal{E} : 0 \to N \to M \to L \to 0$ eine kurze exakte Folge von RG-Gittern mit der Eigenschaft, daß $\mathrm{Res}_H^G(\mathcal{E}) := 0 \to \mathrm{Res}_H^G(N) \to \mathrm{Res}_H^G(M) \to \mathrm{Res}_H^G(L) \to 0$ zerfällt, so zerfällt auch $\mathcal{E}$.*

Beweis. Vgl. Vorlesung „Geordnete Mengen II". □

35.5. Definition. Seien G eine endliche Gruppe und H eine Untergruppe von G. Man nennt ein RG-Gitter L *H-projektiv*, falls L die äquivalenten Bedingungen aus 35.4 erfüllt.

Bemerkung. Offenbar sind Summen und direkte Summanden von H-projektiven RG-Gittern wieder H-projektiv. Ferner sind (wie in der Vorlesung „Geordnete Mengen II") Tensorprodukte mit H-projektiven RG-Gittern stets H-projektiv. Jedes H-projektive RG-Gitter ist auch gHg^{-1}-projektiv für $g \in G$ und I-projektiv für jede Untergruppe I von G mit $H \leq I$. Außerdem ist ein RG-Gitter L genau dann 1-projektiv, wenn L ein projektiver RG-Modul ist. Für jedes H-projektive RG-Gitter L ist ferner $L/\pi L$ ein H-projektiver FG-Modul.

35.6. Bemerkung. Seien G eine endliche Gruppe und L ein unzerlegbares RG-Gitter, das H-projektiv für eine Untergruppe H von G ist. Wie in der Vorlesung „Geordnete Mengen II" existiert dann ein unzerlegbares RH-Gitter M mit $M \mid \mathrm{Res}_H^G(L)$ und $L \mid \mathrm{Ind}_H^G(M)$.

Definition. Seien G eine endliche Gruppe und L ein unzerlegbares RG-Gitter. Eine Untergruppe Q von G nennt man einen *Vertex* von L, falls L Q-projektiv, aber für keine echte Untergruppe P von Q P-projektiv ist. In diesem Fall nennt man jedes unzerlegbare RQ-Gitter M mit $M \mid \mathrm{Res}_Q^G(L)$ und $L \mid \mathrm{Ind}_Q^G(M)$ eine *Quelle* (source) von L bzgl. Q. Mit $\mathrm{Vtx}(L)$ bezeichnen wir die Menge aller Vertizes von L und mit $\mathrm{Sce}_Q(L)$ die Gesamtheit aller RQ-Gitter, die Quellen von L sind.

Satz. *Seien G eine endliche Gruppe und L ein unzerlegbares RG-Gitter mit Vertex Q und Quelle M bzgl. Q. Ist L H-projektiv für eine Untergruppe H von G und ist $L \mid \mathrm{Ind}_H^G(N)$ für ein unzerlegbares RH-Gitter N, so existiert ein Element $g \in G$ mit $gQg^{-1} \subseteq H$ und ${}^gM \mid \mathrm{Res}^H_{gQg^{-1}}(N)$; dabei ist ${}^gM$ die Restriktion von M bzgl. der Abbildung $gQg^{-1} \to Q$, $x \mapsto g^{-1}xg$. Insbesondere sind alle Vertizes von L in G konjugiert, und alle RQ-Gitter, die Quellen von L sind, sind (bis auf Isomorphie) „konjugiert" in $N_G(Q)$.*

Beweis. Vorlesung „Geordnete Mengen II". □

Beispiel. Wie dort zeigt man, daß Vertizes unzerlegbarer RG-Gitter stets p-Untergruppen von G sind.

35.7. Bemerkung. Seien G eine endliche Gruppe, L ein unzerlegbares RG-Gitter, Q ein Vertex von L und M eine Quelle von L bzgl. Q. Wie in der Vorlesung „Geordnete Mengen II" ist Q dann auch Vertex von M.

Definition. Seien G eine endliche Gruppe und $H, I \leq G$. Wir schreiben $H \leq_G I$, falls $gHg^{-1} \subseteq I$ für ein $g \in G$ ist. Wir schreiben $H \sim_G I$, falls H und I in G konjugiert sind.

Satz. *Seien G eine endliche Gruppe, L ein unzerlegbares RG-Gitter mit Vertex Q, H eine Untergruppe von G und $\mathrm{Res}_H^G(L) = M_1 \oplus \ldots \oplus M_r$ mit unzerlegbaren RH-Gittern $M_1, \ldots, M_r$. Für $i = 1, \ldots, r$ und jeden Vertex R_i von M_i ist $R_i \leq_G Q$, und im Fall $Q \leq H$ ist $R_i \sim Q$ für ein $i \in \{1, \ldots, r\}$.*

Beweis. Vgl. Vorlesung „Geordnete Mengen II“. □

Beispiel. Für jede endliche Gruppe G hat das triviale RG-Gitter R die p-Sylowgruppen von G als Vertizes; ist nämlich R H-projektiv für eine Untergruppe H von G, so ist der triviale FG-Modul $F = R/\pi R$ ebenfalls H-projektiv. Wie in der Vorlesung „Geordnete Mengen II“ gezeigt, enthält H also eine p-Sylowgruppe von G.

35.8. Definition. Seien G eine endliche Gruppe, $\mathcal{X}$ eine Menge von Untergruppen von G und L ein RG-Gitter. Wir nennen L *$\mathcal{X}$-projektiv*, falls eine Zerlegung $L = L_1 \oplus \ldots \oplus L_n$ existiert, wobei L_i für $i = 1, \ldots, n$ ein X_i-projektives RG-Gitter für ein $X_i \in \mathcal{X}$ ist.

Satz (Green-Korrespondenz). *Seien G eine endliche Gruppe, Q eine p-Untergruppe von G, H eine Untergruppe von G mit $N_G(Q) \leq H$, $\mathcal{X} := \{gQg^{-1} \cap Q : g \in G \setminus H\}$ und $\mathcal{Y} := \{gQg^{-1} \cap Q : g \in G \setminus H\}$. Dann gilt*

(i) *Ist L ein unzerlegbares RG-Gitter mit Vertex Q, so ist $\mathrm{Res}_H^G(L) \simeq M \oplus Y$, wobei M ein unzerlegbares RH-Gitter mit Vertex Q und Y ein $\mathcal{Y}$-projektives RH-Gitter ist.*

(ii) *Ist M ein unzerlegbares RH-Gitter mit Vertex Q, so ist $\mathrm{Ind}_H^G(L) \simeq L \oplus X$, wobei L ein unzerlegbares RG-Gitter mit Vertex Q und X ein $\mathcal{X}$-projektives RG-Gitter ist.*

(iii) *Durch (i) und (ii) erhält man zueinander inverse Bijektionen zwischen der Menge der Isomorphieklassen unzerlegbarer RG-Gitter mit Vertex Q und der Menge der Isomorphieklassen unzerlegbarer RH-Gitter mit Vertex Q.*

Beweis. Vgl. Vorlesung „Geordnete Mengen II“. □

Bemerkung. Wie dort zeigt man, daß ein unzerlegbares RG-Gitter nicht gleichzeitig Vertex Q haben und $\mathcal{X}$-projektiv sein kann. Analog kann ein unzerlegbares RH-Gitter nicht gleichzeitig Vertex Q haben und $\mathcal{Y}$-projektiv sein.

35.9. Bemerkung. Seien G eine endliche Gruppe, N ein Normalteiler in G und L ein $R[G/N]$-Gitter. Dann wird L zu einem RG-Gitter, wenn man $gx := (gN)x$ für $g \in G$, $x \in L$ definiert. Das so entstehende RG-Gitter nennt man die *Inflation* von L zu G und bezeichnet es mit $\mathrm{Inf}_N^G(L)$. Wie in der Vorlesung „Geordnete Mengen II“ beweist man:

Satz. *Seien G eine endliche Gruppe, P ein p-Normalteiler von G und L ein unzerlegbares $R[G/P]$-Gitter mit Vertex Q/P. Dann ist $\mathrm{Inf}_P^G(L)$ ein unzerlegbares RG-Gitter mit Vertex Q.*

KAPITEL 36

Moduln in Blöcken

Sei φ eine vollständige diskrete Bewertung eines Körpers K der Charakteristik 0 mit Bewertungsring R, Bewertungsideal $\mathrm{Rad}(R) = \pi R$ und algebraisch abgeschlossenem Restklassenkörper $F = R/\pi R$ der Charakteristik $p > 0$.

36.1. Bemerkung. Seien G eine endliche Gruppe, H, I Untergruppen von G mit $I \leq H \leq G$, T ein Repräsentantensystem für H/I und L ein RG-Gitter. Wir setzen $L^H := \{x \in L : hx = x \text{ für } h \in H\}$ und definieren eine Abbildung $\mathrm{Tr}_I^H : L^I \to L^H$ durch $\sum_{t \in T} tx$ für $x \in L^I$. Wie in der Vorlesung „Geordnete Mengen II“ zeigt man, daß dies wohldefiniert ist und eine von T unabhängige Abbildung liefert. Man nennt Tr_I^H *relative Spur*, *Verlagerung* oder *Korestriktion*. Es gelten die üblichen Eigenschaften wie z.B. die Mackey-Formel.

Beispiel. Für RG-Gitter L, M wird auch $\mathrm{Hom}_R(L, M)$ zu einem RG-Gitter, wenn man ${}^g f$ für $g \in G$ und $f \in \mathrm{Hom}_R(L, M)$ durch $({}^g f)(x) := gf(g^{-1}x)$ für $x \in L$ definiert. Für jede Untergruppe H von G ist dabei $\mathrm{Hom}_R(L, M)^H = \mathrm{Hom}_{RH}(L, M)$.

Satz (Higmans Kriterium)**.** *Seien G eine endliche Gruppe, H eine Untergruppe von G und L ein RG-Gitter. Genau dann ist L H-projektiv, wenn $\mathrm{id}_L \in \mathrm{Tr}_H^G(\mathrm{Hom}_{RH}(L, L))$ ist.*

Beweis.

$\Rightarrow$: Ist L H-projektiv, so existiert ein RH-Gitter M und ein RG-Gitter N mit $\mathrm{Ind}_H^G(M) = L \oplus N$. Seien $i : L \to \mathrm{Ind}_H^G(M)$ die Injektion und $j : \mathrm{Ind}_H^G(M) \to L$ die entsprechende Projektion. Außerdem sei $f \in \mathrm{Hom}_{RH}(\mathrm{Ind}_H^G(M), \mathrm{Ind}_H^G(M))$ die Projektion mit Bild $1 \otimes M$ zur Zerlegung

$$\mathrm{Ind}_H^G(M) = (1 \otimes M) \oplus \bigoplus_{\substack{gH \in G/H \\ g \notin H}} g \otimes M.$$

Dann ist $\mathrm{Tr}_H^G(f) = \mathrm{id}_{\mathrm{Ind}_H^G(M)}$, also $j \circ f \circ i \in \mathrm{Hom}_{RH}(L, L)$ mit

$$\mathrm{Tr}_H^G(j \circ f \circ i) = j \circ \mathrm{Tr}_H^G(f) \circ i = j \circ \mathrm{id}_{\mathrm{Ind}_H^G(M)} \circ i = j \circ i = \mathrm{id}_L .$$

$\Leftarrow$: Sei $f \in \mathrm{Hom}_{RH}(L, L)$ mit $\mathrm{id}_L = \mathrm{Tr}_H^G(f)$, sei $\alpha : M \to N$ ein Epimorphismus von RG-Gittern, sei $\beta : L \to N$ ein RG-Homomorphismus, und sei $\gamma : L \to M$ ein RH-Homomorphismus mit $\alpha \circ \gamma = \beta$. Dann ist

$$\alpha \circ \mathrm{Tr}_H^G(\gamma \circ f) = \mathrm{Tr}_H^G(\alpha \circ \gamma \circ f) = \mathrm{Tr}_H^G(\beta \circ f) = \beta \circ \mathrm{Tr}_H^G(f) = \beta \circ \mathrm{id}_L = \beta.$$

$$\begin{tikzcd} & L \arrow[dl, dotted, "\gamma"'] \arrow[d, "\beta"] & \\ M \arrow[r, "\alpha"] & N \arrow[r] & 0 \end{tikzcd}$$

□

36.2. Bemerkung. Seien Λ eine R-Ordnung und $\Lambda = B_1 \oplus \ldots \oplus B_r$ die Zerlegung von Λ in Blöcke. Für jedes Λ-Gitter L ist dann $L = \Lambda L = B_1 L + \ldots + B_r L$. Diese Zerlegung ist direkt; denn ist e_1 das Blockidempotent von B_1, so ist $e_1 x = x$ für $x \in B_1 L$ und $e_1 x = 0$ für $x \in B_2 l + \ldots + B_r L$. Daher ist $L = B_1 L \oplus \ldots \oplus B_r L$ mit Λ-Gittern $B_1 L, \ldots, B_r L$. Im Fall $L = B_1 L$ (d.h. $B_i L = 0$ für $i = 2, \ldots, r$) sagt

man, daß L zum Block B_1 *gehört* oder im Block B_1 *liegt*. In diesem Fall kann man L auch als B_1-Gitter auffassen. Insbesondere gehört jedes unzerlegbare Λ-Gitter zu genau einem Block von Λ. Auf diese Weise kann man die unzerlegbaren Λ-Gitter auf die Blöcke von L verteilen.
Im Fall $\Lambda = RG$ für eine endliche Gruppe G werden wir im folgenden den Zusammenhang zwischen Defektgruppen und Vertizes untersuchen. Für jeden Block B von RG bezeichnen wir dabei die Defektgruppen des entsprechenden Blocks von $RG/\pi RG = FG$ als Defektgruppen von B. Ihre Gesamtheit bezeichnen wir mit $\mathrm{Def}(B)$.

Satz. *Seien G eine endliche Gruppe, L ein unzerlegbares RG-Gitter, B der Block von RG, in dem L liegt, und D eine Defektgruppe von B. Dann ist L D-projektiv, d.h. D enthält einen Vertex von L.*

Beweis. Seien $K_1, \dots, K_r$ die Konjugationsklassen von G mit einer Untergruppe von D als Defektgruppe. Dann existieren $\alpha_1, \dots, \alpha_r \in R$ und $z \in ZRG$ mit $e = \sum_{i=1}^r \alpha_i K_i^+ + \pi z$; dabei ist e das Blockidempotent von B. Für $i = 1, \dots, r$ ist die Multiplikation mit K_i^+ ein RG-Endomorphismus von L, und analog ist die Multiplikation mit z ein RG-Endomorphismus von L. Die Multiplikation mit e ist die Identität auf L. Da $\mathrm{End}_{RG}(L)$ ein lokaler Ring ist, existiert also ein $i \in \{1, \dots, r\}$ mit der Eigenschaft, daß die Multiplikation mit K_i^+ ein RG-Automorphismus f von L ist. Für $x \in K_i$ ist die Multiplikation mit x ein $RC_G(x)$-Endomorphismus g von L mit $f = \mathrm{Tr}_{C_G(x)}^G(g)$, d.h. $\mathrm{id}_L = \mathrm{Tr}_{C_G(x)}^G(g) \circ f^{-1} = \mathrm{Tr}_{C_G(x)}^G(g \circ f^{-1})$. Nach Higman ist also L $C_G(x)$-projektiv. Für jede p-Sylowgruppe Q von $C_G(x)$ ist L dann auch Q-projektiv. Da Q bis auf Konjugation in D enthalten ist, ist damit L auch D-projektiv. □

36.3. Bemerkung. Als nächstes untersuchen wir den Zusammenhang zwischen der Brauer-Korrespondenz und der Green-Korrespondenz. Dazu sei G eine endliche Gruppe, B ein Block von RG mit Blockidempotent e und $\overline{e}$ das Bild von e in $RG/\pi RG = FG$. Für jede p-Untergruppe Q von G hat man den Brauer-Homomorphismus $\mathrm{Br}_Q : ZFG \to ZFC_G(Q)$. I.a. kennt man keinen entsprechenden Homomorphismus $ZRG \to ZRC_G(Q)$. Dennoch existiert natürlich genau ein Idempotent f in $ZRC_G(Q)$ mit $\mathrm{Br}_Q(\overline{e}) = \overline{f}$.

Satz (Nagao)**.** *Seien G eine endliche Gruppe, B ein Block von RG mit Blockidempotent e, sei Q eine p-Untergruppe von G, H eine Untergruppe von G mit $QC_G(Q) \subseteq H \subseteq N_G(Q)$ und f das eindeutig bestimmte Idempotent in ZRH mit $\overline{f} = \mathrm{Br}_Q(\overline{e})$. Für jedes RG-Gitter L in B ist dann $\mathrm{Res}_H^G(L) = fL \oplus M$, wobei M $\mathcal{H}$-projektiv zur Menge $\mathcal{H}$ aller p-Untergruppen P von H mit $Q \not\leq P$ ist.*

Beweis. Offenbar ist $eL = L = fL \oplus (1-f)L$. Daher genügt es zu zeigen, daß $(1-f)L = (1-f)eL = (e-fe)L = (e-f)eL = (e-f)L$ $\mathcal{H}$-projektiv ist. Wegen $\overline{f} = \mathrm{Br}_Q(\overline{e})$ ist $\overline{e} - \overline{f}$ eine F-Linearkombination von H-Klassensummen K^+, wobei K die H-Konjugationsklassen von G mit $K \not\subseteq C_G(Q)$ durchläuft. Jede solche H-Konjugationsklasse K hat eine Defektgruppe P mit $Q \not\leq P$; denn sonst wäre $K \subseteq C_G(P) \subseteq C_G(Q)$. Seien $K_1, \dots, K_r$ die H-Konjugationsklassen von G, deren Defektgruppen Q nicht enthalten. Dann ist $e - f = \sum_{i=1}^r \alpha_i K_i^+ + \pi z$ mit Elementen $\alpha_1, \dots, \alpha_r \in R$ und $z \in C_{RG}(H)$. Für jeden unzerlegbaren direkten Summanden U des RH-Gitters $(e-f)L$ ist die Multiplikation mit $e-f$ die Identität auf U, und für $i = 1, \dots, r$ ist die Multiplikation mit K_i^+ ein RH-Endomorphismus von U. Da $\mathrm{End}_{RH}(U)$ lokal ist, existiert ein $i \in \{1, \dots, r\}$ mit der Eigenschaft, daß die Multiplikation mit K_i^+ ein RH-Automorphismus von U ist. Für $x \in K_i$ ist also U wie im Beweis des vorigen Satzes $C_H(x)$-projektiv und P-projektiv für jede p-Sylowgruppe P von $C_H(x)$. □

36.4. Satz. *Seien G eine endliche Gruppe, B ein Block von RG mit Blockidempotent e, L ein unzerlegbares RG-Gitter in B mit Vertex Q, M der Green-Korrespondent von L in $N_G(Q)$ und f das eindeutig bestimmte Idempotent in $ZRN_G(Q)$ mit $\mathrm{Br}_Q(\overline{e}) = \overline{f}$. Dann ist $M = fM$.*

Beweis. Nach Nagao ist $\mathrm{Res}_{N_G(Q)}^G(L) = fL \oplus L'$, wobei die unzerlegbaren direkten Summanden von L' Vertizes haben, die Q nicht enthalten. Da M ein direkter Summand von L mit Vertex Q ist, folgt $M \mid fL$, d.h. $M = fM$. □

36.5. Satz. *Seien G eine endliche Gruppe, B ein Block von RG mit Defektgruppe D und L ein unzerlegbares RG-Gitter in B mit Vertex D. Dann gehört der Green-Korrespondent M von L in $N_G(D)$ zum Brauer-Korrespondenten b von B in $N_G(D)$.*

Beweis. 36.4. $\square$

36.6. Satz. *Seien G eine endliche Gruppe und B ein Block von RG mit Defektgruppe D. Dann enthält B einen unzerlegbaren RG-Modul mit Vertex D.*

Beweis. Sei b der Brauer-Korrespondent von B in $N_G(D)$, also ein Block von $RN_G(D)$ mit Defektgruppe D, und sei M ein einfacher $FN_G(D)$-Modul in dem entsprechenden Block $\overline{b}$ von $FN_G(D)$. Bekanntlich operiert D trivial auf M, d.h. man kann M auch als einfachen $F[N_G(D)/D]$-Modul auffassen. Sei P ein unzerlegbarer projektiver $F[N_G(D)/D]$-Modul mit $P/\operatorname{Rad}(P) \simeq M$. Dann ist $P \simeq F[N_G(D)/D]f$ für ein primitives Idempotent in $F[N_G(D)/D]$. Bekanntlich existiert ein primitives Idempotent in $R[N_G(D)/D]$ mit $f = \overline{e}$. Dann ist $R[N_G(D)/D]e$ ein unzerlegbarer $R[N_G(D)/D]$-Modul. Diesen fassen wir nach Inflation als unzerlegbaren $RN_G(D)$-Modul U auf. Sei b_1 der Block von $RN_G(D)$, der U enthält, und sei e_1 das Blockidempotent von b_1. Dann operiert e_1 als Identität auf U, auf $F[N_G(D)/D]f$, auf P und auf M. Daher gehört M auch zu b_1, d.h. $b = b_1$. Da $R[N_G(D)/D]e$ als $R[N_G(D)/D]$-Gitter projektiv ist, hat U den Vertex D. Der Green-Korrespondent L von U hat dann auch Vertex D. Nach 36.4 gehört L zum Brauer-Korrespondenten B von b in G. $\square$

KAPITEL 37

Induzierte Moduln

Sei φ eine vollständige diskrete Bewertung eines Körpers K der Charakteristik 0 mit Bewertungsring R, Bewertungsideal $\mathrm{Rad}(R) = \pi R$ und algebraisch abgeschlossenem Restklassenkörper $F = R/\pi R$ der Charakteristik $p > 0$.

37.1. Definition. Seien G eine endliche Gruppe, $H \trianglelefteq G$ und M ein RH-Gitter. Dann nennt man $T_G(M) := \{g \in G : {}^gM \simeq M\}$ die *Trägheitsgruppe* von M in G. Im Fall $T_G(M) = G$ nennt man M *G-invariant* oder *G-stabil*.

Bemerkung. In der obigen Definition ist ${}^gM = \mathrm{Res}_{\alpha_g}(M)$, wobei $\alpha_g : H \to H,\ h \mapsto g^{-1}hg$ ist. Für $m \in {}^gM = M$ und $h \in H$ ist das Produkt $h * m$ in ${}^gM$ genau das Produkt $(g^{-1}hg) \cdot m$ in M. Offenbar ist ${}^gM$ zu dem Teilgitter $g \otimes M$ von $RG \otimes_{RH} M$ isomorph; denn für $h \in H$ und $m \in M$ ist

$$h(g \otimes m) = hg \otimes m = g(g^{-1}hg) \otimes m = g \otimes (g^{-1}hg)m.$$

Offenbar operiert G auf der Menge der Isomorphieklassen $[M]$ von RH-Gittern M durch ${}^g[M] := [{}^gM]$ für $g \in G$, und $T_G(M)$ ist der Stabilisator von $[M]$ unter dieser Operation; insbesondere ist $T_G(M) \leq G$. Für $h \in H$ ist bekanntlich ${}^hM \simeq M$, d.h. $H \leq T_G(M) \leq G$.

Satz. *Seien G eine endliche Gruppe, $H \trianglelefteq G$, M ein unzerlegbares RH-Gitter, $I := T_G(M)$ und $\mathrm{Ind}_H^I(M) = N_1 \oplus \ldots \oplus N_r$ mit unzerlegbaren RI-Gittern $N_1, \ldots, N_r$. Dann ist $\mathrm{Ind}_H^G(M) = \mathrm{Ind}_I^G(N_1) \oplus \ldots \oplus \mathrm{Ind}_I^G(N_r)$ mit unzerlegbaren RG-Gittern $\mathrm{Ind}_I^G(N_1), \ldots, \mathrm{Ind}_I^G(N_r)$. Ferner gilt für $i, j = 1, \ldots, r$: $N_i \simeq N_j \iff \mathrm{Ind}_I^G(N_i) \simeq \mathrm{Ind}_I^G(N_j)$.*

Beweis. Sei T ein Repräsentantensystem für G/I, und sei S ein Repräsentantensystem für I/H. Dann ist

$$\mathrm{Res}_H^I(\mathrm{Ind}_H^I(M)) = \bigoplus_{s \in S} s \otimes M \simeq M^{|I:H|}.$$

Nach Krull-Schmidt existiert also für $i = 1, \ldots, r$ ein $n_i \in \mathbb{N}$ mit $\mathrm{Res}_H^I(N_i) \simeq M^{n_i}$. Wegen $N_i \mid \mathrm{Res}_I^G(\mathrm{Ind}_I^G(N_i))$ existiert ein unzerlegbarer direkter Summand L_i von $\mathrm{Ind}_I^G(N_i)$ mit $N_i \mid \mathrm{Res}_I^G(L_i)$. Dann ist $M^{n_i} \mid \mathrm{Res}_H^G(L_i)$. Für $t \in T$ ist also

$$({}^tM)^{n_i} \mid {}^t(\mathrm{Res}_H^G(L_i) = \mathrm{Res}_H^G({}^tL_i) = \mathrm{Res}_H^G(L_i).$$

Folglich ist auch $\bigoplus_{t \in T}({}^tM)^{n_i} \mid \mathrm{Res}_H^G(L_i)$, also

$$\mathrm{rk}_R\, L_i \geq |G : I| n_i \,\mathrm{rk}_R\, M = |G : I| \,\mathrm{rk}_R\, N_i = \mathrm{rk}_R\, \mathrm{Ind}_I^G(N_i) \geq \mathrm{rk}_R\, L_i.$$

Daher ist $\mathrm{Ind}_I^G(N_i) = L_i$ unzerlegbar.
Wir nehmen an, daß $i, j \in \{1, \ldots, r\}$ existieren mit $N_i \not\simeq N_j$, aber $\mathrm{Ind}_I^G(N_i) \simeq \mathrm{Ind}_I^G(N_i) \simeq \mathrm{Ind}_I^G(N_j)$. Wegen $N_i \mid \mathrm{Res}_I^G(\mathrm{Ind}_I^G(N_i))$ und $N_j \mid \mathrm{Res}_I^G(\mathrm{Ind}_I^G(N_j))$ ist dann $N_i \oplus N_j \mid \mathrm{Res}_I^G(\mathrm{Ind}_I^G(N_i))$, also

$$M^{n_i+n_j} \mid \mathrm{Res}_H^G(\mathrm{Ind}_I^G(N_i)) = \mathrm{Res}_H^G(L_i) = \bigoplus_{t \in T}({}^tM)^{n_i}.$$

Widerspruch. $\square$

37.2. Definition. Sei G eine endliche Gruppe. Eine *G-graduierte R-Ordnung* ist eine R-Ordnung Λ mit einer festen Zerlegung $\Lambda = \bigoplus_{g \in G} \Lambda_g$ in R-Untermoduln Λ_g mit $\Lambda_g \Lambda_h \subseteq \Lambda_{gh}$ für $g, h \in G$. Enthält Λ_g für jedes $g \in G$ eine Einheit in Λ, so nennt man $\Lambda = \bigoplus_{g \in G} \Lambda_g$ ein *verschränktes Produkt*.

Bemerkung. Die in der Darstellungstheorie II über graduierte Algebren bewiesenen elementaren Tatsachen übertragen sich ohne Schwierigkeit auf graduierte Ordnungen. Näher gehen wir darauf nicht ein.

Satz. *Seien G eine endliche Gruppe, $H \trianglelefteq G$, M ein RH-Gitter, $E := \mathrm{End}_{RG}(\mathrm{Ind}_H^G(M))$ und $E_{gH} := \{f \in E : f(1 \otimes M) \subseteq g^{-1} \otimes M\}$ für $g \in G$. Dann ist $E = \bigoplus_{gH \in G/H} E_{gH}$ eine G/H-graduierte R-Ordnung mit $E_1 \cong \mathrm{End}_{RH}(M)$. Ist M G-invariant, so ist E ein verschränktes Produkt.*

Beweis. Offenbar hängt die Definition von E_{gH} nicht von G, sondern nur von gH ab. Sei T ein Repräsentantensystem für G/H. Dann ist $\mathrm{Ind}_H^G(M) = \bigoplus_{t \in T} t \otimes M$. Für $t \in T$ sei $\pi_t : \mathrm{Ind}_H^G(M) \to \mathrm{Ind}_H^G(M)$ die entsprechende Projektion mit Bild $t \otimes M$. Dann ist also $\sum_{t \in T} \pi_t = \mathrm{id}_{\mathrm{Ind}_H^G(M)}$.
Sei $f \in E$ und $g_t : 1 \otimes M \to t \otimes M \subseteq \mathrm{Ind}_H^G(M)$ für $t \in T$ die Einschränkung von $\pi_t \circ f$ auf $1 \otimes M$. Dann ist g_t ein RH-Homomorphismus, und es existiert genau ein RG-Homomorphismus $f_t : RG \otimes_{RH} M \to RG \otimes_{RH} M$ mit $f_t(x \otimes m) = xg_t(1 \otimes m)$ für $x \in RG$ und $m \in M$. Wegen $f_t(1 \otimes M) = g_t(1 \otimes M) \subseteq t \otimes M$ ist $f_t \subseteq E_{t^{-1}H}$. Für $m \in M$ ist

$$\sum_{t \in T} f_t(1 \otimes m) = \sum_{t \in T} g_t(1 \otimes m) = \sum_{t \in T} \pi_t(f(1 \otimes m)) = f(1 \otimes m).$$

Daher ist $f = \sum_{t \in T} f_t$.
Sei nun $f_t \in E_{t^{-1}H}$ für $t \in T$ mit $\sum_{t \in T} f_t = 0$. Für $m \in M$ ist dann $0 = \sum_{t \in T} f_t(1 \otimes m)$ mit $f_t(1 \otimes m) \in t \otimes M$ für $t \in T$. Daher ist $f_t(1 \otimes m) = 0$ für $t \in T$, $m \in M$, d.h. $f_t = 0$ für $t \in T$. Dies zeigt: $e = \bigoplus_{t \in T} E_{tH}$.
Für $x, y \in G$, $f \in E_{xH}$, $g \in E_{yH}$ ist $f(1 \otimes M) \subseteq x^{-1} \otimes M$, $g(1 \otimes M) \subseteq y^{-1} \otimes M$, also

$$(f \circ g)(1 \otimes M) \subseteq f(y^{-1} \otimes M) = y^{-1} f(1 \otimes M) = y^{-1}x^{-1} \otimes M = (xy)^{-1} \otimes M.$$

Folglich ist $f \circ g \in E_{xyH}$. Damit ist E eine G/H-graduierte R-Ordnung.
Offenbar ist die Abbildung $\mathrm{End}_{RH}(M) \to \mathrm{End}_{RG}(RG \otimes_{RH} M)$, $f \mapsto \mathrm{id}_{RG} \circ f$ ein Monomorphismus von R-Ordnungen, dessen Bild in E_1 enthalten ist. Sei umgekehrt $g \in E_1$, also $g(1 \otimes M) \subseteq 1 \otimes M$. Dann existiert genau ein RH-Endomorphismus f von M mit $g(1 \otimes m) = 1 \otimes f(m)$ für $m \in M$. Folglich ist $g = \mathrm{id}_{RG} \otimes f$. Dies zeigt: $E_1 \cong \mathrm{End}_{RH}(M)$.
Ist M G-invariant, so existiert für $t \in T$ ein RH-Isomorphismus $g_t : 1 \otimes M \to t \otimes M$. Wie oben exisiert dazu genau ein RG-Homomorphismus $f_t : RG \otimes_{RH} M \to RG \otimes_{RH} M$ mit $f_t(x \otimes m) = xg_t(1 \otimes m)$ für $x \in RG$, $m \in M$. Offenbar ist f_t ein RG-Isomorphismus, d.h. f_t ist eine Einheit von E mit $f_t \in E_{t^{-1}H}$. Folglich ist E ein verschränktes Produkt. □

37.3. Satz (Green)**.** *Seien G eine endliche Gruppe, $H \trianglelefteq G$ und M ein unzerlegbares RH-Gitter. Ist G/H eine p-Gruppe, so ist $\mathrm{Ind}_H^G(M)$ ein unzerlegbares RG-Gitter.*

Beweis. Wir argumentieren durch Induktion nach $|G : H|$ und können daher annehmen, daß $|G : H| = p$ ist. Im Fall $T_G(M) = H$ folgt aus 37.1, daß $\mathrm{Ind}_H^G(M)$ unzerlegbar ist. Wir können also auch annehmen, daß M G-invariant ist. Nach 37.2 ist $E := \mathrm{End}_{RG}(\mathrm{Ind}_H^G(M))$ eine G/H-graduierte R-Ordnung mit $E_1 \cong \mathrm{End}_{RH}(M)$; insbesondere ist E_1 eine lokale R-Ordnung. Es folgt leicht, daß $\overline{E} := E/\pi E$ eine G/H-graduierte F-Algebra mit $\overline{E_1} \cong E_1/\pi E_1$ ist; insbesondere ist $\overline{E_1}$ eine lokale F-Algebra. Da M G-invariant ist, sind E und $\overline{E}$ verschränkte Produkte. Nach 29.7 ist $\overline{E}$ eine lokale F-Algebra. Daher ist E eine lokale Ordnung. Folglich ist $\mathrm{Ind}_H^G(M)$ unzerlegbar. □

37.4. Bemerkung. Seien Λ eine R-Ordnung und L ein Λ-Gitter. Für $a \in \Lambda$ sei $\chi_L(a)$ die Spur der linearen Abbildung $L \to L$, $x \mapsto ax$. Dann nennt man die Abbildung $\chi_L : \Lambda \to R$, $a \mapsto \chi_L(a)$ den *Charakter* von L. Wie üblich ist $\chi_L(ab) = \chi_L(ba)$ für $a, b \in \Lambda$. Ist $x_1, \dots, x_n$ eine R-Basis von L und $\Delta : \Lambda \to \mathrm{Mat}(n, R)$ die entsprechende Matrixdarstellung, so ist $\chi_L(a) = \mathrm{spur}(\Delta(a))$ für $a \in \Lambda$.

Satz. *Seien G eine endliche Gruppe und L ein unzerlegbares RG-Gitter mit Vertex Q. Ist g ein Element in G mit der Eigenschaft, daß der p-Faktor g_p von g nicht zu einem Element in Q konjugiert ist, so ist $\chi_L(g) = 0$.*

Beweis. Seien $A := \langle g\rangle$, $B := \langle g^p\rangle$ und $\mathrm{Res}_A^G(L) = M_1 \oplus \ldots \oplus M_r$ mit unzerlegbaren RA-Gittern $M_1, \ldots, M_r$. Für $i = 1, \ldots, r$ sei $P_i \in \mathrm{Vtx}(M_i)$. Dann ist $P_i \leq_G Q$ und $g_p \notin P_i$, also $P_i \subseteq B$. Insbesondere ist M_i B-projektiv. Es existiert also ein unzerlegbares RB-Gitter N_i mit $M_i \mid \mathrm{Ind}_B^A(N_i)$. Nach Green ist $\mathrm{Ind}_B^A(N_i)$ unzerlegbar, also $M_i \simeq \mathrm{Ind}_B^A(N_i)$. Daher ist $\chi_{M_i} = \mathrm{Ind}_B^A(\chi_{N_i})$, also $\chi_{M_i}(g) = 0$. Folglich ist $\chi_L(g) = \chi_{M_1}(g) + \ldots + \chi_{M_r}(g) = 0$. □

37.5. Satz. *Seien G eine endliche Gruppe, L ein unzerlegbares RG-Gitter mit Vertex Q und S eune p-Sylowgruppe von G mit $Q \subseteq S$. Dann ist $|S : Q| \mid \mathrm{rk}_R L$.*

Beweis. Wegen $L \mid \mathrm{Ind}_Q^G(\mathrm{Res}_Q^G(L))$ ist

$$\begin{aligned}
\mathrm{Res}_S^G(K) \mid \mathrm{Res}_S^G(\mathrm{Ind}_Q^G(\mathrm{Res}_Q^G(L))) &= \bigoplus_{SgQ \in S\backslash G/Q} \mathrm{Ind}_{S\cap gQg^{-1}}^S(\mathrm{Res}_{S\cap gQg^{-1}}^{gQg^{-1}}({}^g\mathrm{Res}_Q^G(L))) \\
&= \bigoplus_{SgQ \in S\backslash G/Q} \mathrm{Ind}_{S\cap gQg^{-1}}^S(\mathrm{Res}_{S\cap gQg^{-1}}^{gQg^{-1}}(\mathrm{Res}_{gQg^{-1}}^G({}^gL))) \\
&= \bigoplus_{SgQ \in S\backslash G/Q} \mathrm{Ind}_{S\cap gQg^{-1}}^S(\mathrm{Res}_{S\cap gQg^{-1}}^G(L)).
\end{aligned}$$

Für jeden unzerlegbaren direkten Summanden M von $\mathrm{Res}_{S\cap gQg^{-1}}^G(L)$ ist $\mathrm{Ind}_{S\cap gQg^{-1}}^S(M)$ nach Green unzerlegbar. Zu jedem unzerlegbaren direkten Summanden N von $\mathrm{Res}_S^G(L)$ existiert also ein $g \in G$ mit $|S : S \cap gQg^{-1}| \mid \mathrm{rk}_R N$. Daher ist $|S : Q| \mid \mathrm{rk}_R L$. □

KAPITEL 38

Charaktere in Blöcken

Sei φ eine vollständige diskrete Bewertung eines Körpers K der Charakteristik 0 mit Bewertungsring R, Bewertungsideal $\mathrm{Rad}(R) = \pi R$ und algebraisch abgeschlossenem Restklassenkörper $F = R/\pi R$ der Charakteristik $p > 0$.

38.1. Bemerkung. Für jede R-Ordnung Λ ist $A := K \otimes_R \Lambda$ eine endlich-dimensionale K-Algebra mit $\dim_K A = \mathrm{rk}_R \Lambda$; für jede R-Basis $a_1, \ldots, a_n$ von Λ ist nämlich $1 \otimes a_1, \ldots, 1 \otimes a_n$ eine K-Basis von A. Insbesondere ist die Abbildung $\Lambda \to A,\ a \mapsto 1 \otimes a$ injektiv. Wir werden sie benutzen, um Λ als Unteralgebra von A aufzufassen. Zu jedem Element $x \in A$ existiert dann ein Element $r \in R \setminus \{0\}$ mit $rx \in \Lambda$. Im Fall $\Lambda = RG$ für eine endliche Gruppe G können wir $A = K \otimes_R RG$ mit KG identifizieren.

Satz. *Seien Λ eine R-Ordnung, $A := K \otimes_R \Lambda$ und V ein endlich-dimensionaler A-Modul. Dann existiert eine K-Basis $b_1, \ldots, b_k$ von V mit der Eigenschaft, daß $L := Rb_1 + \ldots + Rb_k$ ein Λ-Gitter ist.*

Beweis. Sei $c_1, \ldots, c_k$ eine beliebige K-Basis von V. Dann ist $L := \Lambda c_1 + \ldots + \Lambda c_k$ ein Λ-Gitter. Jede R-Basis $b_1, \ldots, b_l$ von L ist offenbar auch linear unabhängig über K. Kedes Element $v \in V$ ist eine Linearkombination von $c_1, \ldots, c_k$, also auch von $b_1, \ldots, b_l$. Daher bilden $b_1, \ldots, b_l$ auch eine K-Basis von V; insbesondere ist $k = l$. □

Definition. Man nennt jedes solche L eine *R-Form* von V.

38.2. Bemerkung.

(i) Seien Λ eine R-Ordnung, $A := K \otimes_R \Lambda$ und $\Delta : A \to \mathrm{Mat}(n, K)$ eine Matrixdarstellung. Aus 38.1 folgt dann, daß eine Matrix $T \in \mathrm{GL}(n, K)$ existiert mit $T\Delta(a)T^{-1} \in \mathrm{Mat}(n, R)$ für alle $a \in \Lambda$.
(ii) R-Formen eines A-Moduls sind i.a. nicht eindeutig, auch nicht bis auf Isomorphie.

Definition. Seien Λ eine R-Ordnung, $A := K \otimes_R \Lambda$, V ein A-Modul und B ein Block von Λ mit Blockidempotent e. Man sagt, daß V zum Block B *ghört* oder im Block B *liegt*, falls $ev = v$ für alle $v \in V$ ist.

Satz. *Seien Λ eine R-Ordnung und $A := K \otimes_R \Lambda$. Dann gehört jeder irreduzible A-Modul V zu genau einem Block von Λ.*

Beweis. Seien $B_1, \ldots, B_r$ die Blöcke von Λ und $e_1, \ldots, e_r$ die entsprechenden Blockidempotente. Wegen $1 = e_1 + \ldots + e_r$ ist $V = 1V = e_1V + \ldots + e_rV$. Für $v \in e_1V$ ist $e_1v = v$, und für $v \in e_2V + \ldots + e_rV$ ist $e_1v = 0$. Daher ist $V = e_1V \oplus \ldots \oplus e_rV$ mit A-Untermoduln $e_1V, \ldots, e_rV$ von V; denn $e_1, \ldots, e_r$ liegen in $Z(A)$. Da V irreduzibel ist, existiert genau ein $i \in \{1, \ldots, r\}$ mit $V = e_iV$. Dann gehört V zum Block B_i. □

38.3. Bemerkung. Seien Λ eine R-Ordnung, $A := K \otimes_R \Lambda$ und V ein A-Modul. Wie üblich bezeichnen wir für $a \in A$ die Spur der linearen Abbildung $V \to V,\ v \mapsto av$ mit $\chi_V(a)$. Bekanntlich ist $\chi_V(ab) = \chi_V(ba)$ für $a, b \in A$. Die Abbildung $\chi_V : A \to K,\ a \mapsto \chi_V(a)$ bezeichnet man als *Charakter* von V.
Ist L eine R-Form von V, so ist offenbar $\chi_V(a) = \chi_L(a)$ für $a \in \Lambda$. Liegt V im Block B von Λ und ist e das Blockidempotent von B, so ist $\chi_V(a) = \chi_V(ae)$ für alle $a \in A$. Wir sagen, daß χ_V zum Block B *gehört* oder im Block B *liegt*.

Satz. *Seien Λ eine R-Ordnung, $B_1, \ldots, B_r$ die Blöcke von Λ und $e_1, \ldots, e_r$ die entsprechenden Blockidempotente. Für $i = 1, \ldots, r$ existiert dann genau ein Homomorphismus von R-Algebren $\vartheta_i : Z(\Lambda) \to F$*

mit $\vartheta_i(e_i) = 1$. für $j \neq i$ ist $\vartheta_i(e_j) = 0$. Ferner sind $\vartheta_1, \ldots, \vartheta_r$ die einzigen unitären Homomorphismen von R-Algebren $Z(\Lambda) \to F$.

Beweis. Sei $\vartheta : Z(\Lambda) \to F$ ein beliebiger Homomorphismus von R-Algebren. Dann ist $\vartheta(\pi Z(\Lambda)) = \pi\vartheta(Z(\Lambda)) = 0$, d.h. ϑ induziert einen Homomorphismus von F-Algebren $\overline{\vartheta} : \overline{Z(\Lambda)} := Z(\Lambda)/\pi Z(\Lambda) \to F$. Wir wissen, daß die Bilder $\overline{e_1}, \ldots, \overline{e_r}$ von $e_1, \ldots, e_r$ genau die Blockidempotente von $\overline{Z(\Lambda)}$ sind. Da $J := J(\overline{Z(\Lambda)}) = J(Z(\Lambda))/\pi Z(\Lambda)$ nilpotent ist, ist $\overline{\vartheta}(J) = 0$, d.h. $\vartheta(J(Z(\Lambda))) = 0$. Daher induziert ϑ einen Homomorphismus von F-Algebren $\overline{\overline{\vartheta}} : \overline{\overline{Z(\Lambda)}} := Z(\Lambda)/J(Z(\Lambda)) \to F$. Die Bilder $\overline{\overline{e_1}}, \ldots, \overline{\overline{e_r}}$ von $e_1, \ldots, e_r$ sind genau die Blockidempotente von $\overline{\overline{Z(\Lambda)}}$. Da $\overline{\overline{Z(\Lambda)}}$ eine halbeinfache F-Algebra ist, ist $\overline{\overline{Z(\Lambda)}} = F\overline{\overline{e_1}} \oplus \ldots \oplus F\overline{\overline{e_r}}$, und die Behauptung folgt. □

Definition. Man nennt ϑ_i den *zentralen Charakter* von B_i.

38.4. Bemerkung. Seien K ein Zerfällungskörper für die endliche Gruppe G und $\chi \in \mathrm{Irr}(G)$. Aus 4.2 folgt leicht, daß die lineare Abbildung $\omega_\chi : ZKG \to K$ mit $\omega_\chi(C^+) := \chi(C^+)/\chi(1)$ für $C \in \mathrm{Cl}(G)$ ein Homomorphismus von K-Algebren ist. Nach 4.5 ist $\omega_\chi(C^+)$ für $C \in \mathrm{Cl}(G)$ eine ganz-algebraische Zahl in K; insbesondere ist $\omega_\chi(C^+)$ stets ganz über R. Da R ganz abgeschlossen ist, ist $\omega_c hi(C^+) \in R$ für $C \in \mathrm{Cl}(G)$, d.h. die Einschränkung von ω_χ ist ein Homomorphismus von R-Ordnungen $ZRG \to R$. Diesen verknüpfen wir mit dem natürlichen Epimorphismus $R \to R/\pi R = F$ und erhalten so einen Homomorphismus von R-Algebren $\overline{\omega_\chi} : ZRG \to F$.

Satz. *Seien K ein Zerfällungskörper für die endliche Gruppe G und B ein Block von RG mit Blockidempotent e und zentralem Charakter ϑ. Für jeden irreduziblen Charakter χ von G in B ist dann $\overline{\omega_\chi} = \vartheta$.*

Beweis. Wegen $\omega_\chi(e) = \frac{\chi(e)}{\chi(1)} = \frac{\chi(1)}{\chi(1)} = 1$ ist auch $\overline{\omega_\chi}(e) = 1$, d.h. $\overline{\omega_\chi} = \vartheta$. □

38.5. Satz. *Seien K ein Zerfällungskörper für die endliche Gruppe G und $\chi, \chi' \in \mathrm{Irr}(G)$. Genau dann gehören χ, χ' zum gleichen Block von RG, wenn $\frac{\chi(C^+)}{\chi(1)} \equiv \frac{\chi'(C^+)}{\chi'(1)} \pmod{\pi R}$ für alle $C \in \mathrm{Cl}(G)$ gilt.*

Beweis. Die Bedingung bedeutet $\overline{\omega_\chi} = \overline{\omega_{\chi'}}$. Die Behauptung folgt also aus 38.4. □

Definition. Für jeden Block B von RG bezeichnen wir mit $\mathrm{Irr}(B)$ die Menge der irreduziblen Charaktere von G in B.

Beispiel. Aus der Darstellungstheorie II kennen wir die Augmentationsabbildung $FG \to F$, $\sum_{g \in G} \alpha_g g \mapsto \sum_{g \in G} \alpha_g$, einen Homomorphismus von F-Algebren. Durch Komposition mit dem natürlichen Epimorphismus $RG \to FG$ erhalten wir einen Homomorphismus von R-Algebren $RG \to F$, und durch Einschrämkung erhalten wir einen Homomorphismus von R-Algebren $\vartheta_0 : ZRG \to F$. Sei $e_0 = e_0(RG)$ das Blockidempotent in RG, dessen Bild $\overline{e_0}$ in FG das Hauptblockidempotent von FG ist. Wir bezeichnen e_0 als *Hauptblockidempotent* von RG und den entsprechenden Block $B_0 = B_0(RG) = RGe_0$ als *Hauptblock* von RG. Offenbar ist ϑ_0 der zentrale Charakter von B_0. Ein irreduzibler Charakter von G gehört also genau dann zu B_0, wenn $\frac{\chi(C^+)}{\chi(1)} \equiv |C| \pmod{\pi R}$ für alle $C \in \mathrm{Cl}(G)$ ist. Insbesondere gehört der triviale Charakter von G zu B_0.

38.6. Bemerkung. Sei K ein Zerfällungskörper für die endliche Gruppe G. Dann ist $\mathrm{End}_{KG}(V) \cong K$ für jeden einfachen KG-Modul V. Sind $V_1, \ldots, V_k$ Repräsentanten für die Isomorphieklassen einfacher KG-Moduln, so ist $KG \cong \bigoplus_{i=1}^k V_i^{d_i}$ als KG-Modul mit $d_i := \dim_K V_i$ für $i = 1, \ldots, k$. Wie in der Algebra gezeigt, folgt daraus $KG \cong (KG)^o \cong \bigoplus_{i=1}^k \mathrm{Mat}(d_i, K)$ als K-Algebren. Daher ist $KG = A_1 \oplus \ldots \oplus A_k$ mit Idealen $A_1, \ldots, A_k$, die einfache Algebren sind. Dabei sei die Numerierung so gewählt, daß $A_i V_i = V_i$ und $A_i V_j = 0$ für $i \neq j$ gilt. Für $i = 1, \ldots, k$ ist also $A_i \cong \mathrm{Mat}(d_i, K) \cong \mathrm{End}_K(V_i)$, und die Abbildung $\Phi_i : A_i \to \mathrm{End}_K(V_i)$, die jedem $a \in A_i$ die lineare Abbildung $\Phi_i(a) : V_i \to V_i$, $v \mapsto av$ zuordnet, ist eine lineare Bijektion.

Für beliebige KG-Moduln V, W wird $H := \mathrm{Hom}_K(V, W)$ zu einem $K[G \times G]$-Modul, wenn man ${}^{(x,y)}f \in H$ für $x, y \in G$ und $f \in H$ durch $({}^{(x,y)}f)(v) := xf(y^{-1}v)$ für $v \in V$ definiert. Bilden $v_1, \ldots, v_m$ eine Basis von V und $w_1, \ldots, w_n$ eine Basis von W, so bilden die durch $f_{ij}(v_r) := \delta_{ir} w_j$ für $r = 1, \ldots, m$ definierten

Elemente $f_{ij} \in H$ $(i = 1, \dots, m,\ j = 1, \dots, n)$ eine Basis von H. Schreibt man $xw_i = \sum_{j=1}^{n} \beta_{ij}(x)w_j$ mit $\beta_{ij}(x) \in K$ für $i, j = 1, \dots, n,\ x \in G$ und $yv_i = \sum_{j=1}^{m} \alpha_{ij}(y)v_i$ mit $\alpha_{ij}(y) \in K$ für $i, j = 1, \dots, m,\ y \in G$, so ist

$$\begin{aligned} xf_{ij}(y^{-1}v_r) &= xf_{ij}\left(\sum_{s=1}^{m} \alpha_{rs}(y^{-1})v_s\right) = \sum_{s=1}^{m} \alpha_{rs}(y^{-1})x\delta_{is}w_j \\ &= \alpha_{ri}(y^{-1})xw_j = \alpha_{ri}(y^{-1})\sum_{s=1}^{n} \beta_{js}(x)w_s \\ &= \sum_{s=1}^{n} \alpha_{ri}(y^{-1})\beta_{js}(x)f_{rs}(v_r) = \sum_{s=1}^{n}\sum_{t=1}^{m} \alpha_{ti}(y^{-1})\beta_{js}(x)f_{ts}(v_r) \end{aligned}$$

für $r = 1, \dots, m$, also

$$^{(x,y)}f_{ij} = \sum_{s=1}^{n}\sum_{t=1}^{m} \alpha_{ti}(y^{-1})\beta_{js}(x)f_{ts}$$

für $i = 1, \dots, m,\ j = 1, \dots, n,\ x, y \in G$. Der Charakter χ_H von H wird also gegeben durch $\chi_H(x, y) = \sum_{i=1}^{m}\sum_{j=1}^{n} \alpha_{ii}(y^{-1})\beta_{jj}(x) = \chi_V(y^{-1})\chi_W(x)$ für $x, y \in G$.
Mit den obigen Bezeichnungen ist also $E_i := \mathrm{End}_K(V_i)$ ein $K[G \times G]$-Modul mit Charakter $\chi_{E_i} : G \times G \to K,\ (x, y) \mapsto \chi_{V_i}(x)\chi_{V_i}(y^{-1})$. Die Gruppenalgebra KG ist ebenfalls ein $K[G \times G]$-Modul mit $^{(x,y)}z := xzy^{-1}$ für $x, y, z \in G$. Für $i = 1, \dots, k$ ist A_i ein $K[G \times G]$-Untermodul von KG, und die oben definierte Bijektion $\Phi_i : A_i \to \mathrm{End}_K(V_i)$ ist $K[G \times G]$-linear. Daher ist $\chi_{A_i}(x, y) = \chi_{V_i}(x)\chi_{V_i}(y^{-1})$ für $x, y \in G$.

Satz (Zweite Orthogonalitätsrelation für Blöcke)**.** *Seien K ein Zerfällungskörper für die endliche Gruppe G, B ein Block von RG und x, y Elemente in G, dere p-Faktoren x_p, y_p nicht konjugiert sind. Dann ist*

$$\sum_{\chi \in \mathrm{Irr}(B)} \chi(x)\chi(y^{-1}) = 0.$$

Beweis. Sei e das Blockidempotent von B. Dann ist $RG = eRG \oplus (1-e)RG$ und $KG = eKG \oplus (1-e)KG$. Zerlegt man $KG = A_1 \oplus \ldots \oplus A_k$ wie oben, so ist offenbar eKG die Summe der A_i mit der Eigenschaft, daß V_i zu B gehört. Für $x, y \in G$ ist also

$$\chi_{eKG}(x, y) = \sum_{V_i \text{ in } B} \chi_{A_i}(x, y) = \sum_{V_i \text{ in } B} \chi_{V_i}(x)\chi_{V_i}(y^{-1}) = \sum_{\chi \in \mathrm{Irr}(B)} \chi(x)\chi(y^{-1}).$$

Andererseits ist eRG eine R-Form des $K[G \times G]$-Moduls eKG und ein direkter Summand des $R[G \times G]$-Gitters RG. Wir setzen $\Delta(G) := \{(g, g) : g \in G\} \leq G \times G$. Man rechnet leicht nach, daß die R-lineare Abbildung $\Psi : \mathrm{Ind}_{\Delta(G)}^{G}(R) \to RG$ mit $\Psi((g, 1) \otimes 1) = g$ für $g \in G$ ein Isomorphismus von $R[G \times G]$-Gittern ist. Daher sind die Vertizes der unzerlegbaren direkten Summanden des $R[G \times G]$-Gitters RG zu Untergruppen von $\Delta(G)$ konjugiert. Entsprechendes gilt für die Einschränkung von RG auf die Untergruppe $\langle (x, y) \rangle$ von $G \times G$, x, y wie in der Voraussetzung. Offenbar ist $\langle (x_p, y_p) \rangle$ die einzige p-Sylowgruppe von $\langle (x, y) \rangle$. Gäbe es Elemente $g, h \in G$ mit $(g, h)(x_p, y_p)(g, h)^{-1} \in \Delta(G)$, so wäre $gx_pg^{-1} = hy_ph^{-1}$ und x_p, y_p konjugiert im Widerspruch zur Voraussetzung. Daher sind die Vertizes der unzerlegbaren direkten Summanden des $R\langle [x, y) \rangle$-Gitters RG echte Untergruppen von $\langle (x_p, y_p) \rangle$. Folglich verschwindet ihr Charakter auf (x, y) und es ist $0 = \chi_{eRG}(x, y) = \chi_{eKG}(x, y)$. □

38.7. Bemerkung. Seien K ein Zerfällungskörper für die endliche Gruppe G und $\mathrm{Cf}(G)$ der K-Vektorraum aller Klassenfunktionen $G \to K$. Für jede p-Sektion S von G setzen wir $\mathrm{Cf}(G|S) := \{\varphi \in \mathrm{Cf}(G) : \varphi(g) = 0 \text{ für } g \in G \setminus S\}$. Dann ist

$$\mathrm{Cf}(G) = \bigoplus_{S \in \mathrm{Sec}_p(G)} \mathrm{Cf}(G|S).$$

Für jeden Block von RG setzen wir $\mathrm{Cf}(B) := \sum_{\chi \in \mathrm{Irr}(G)} K\chi$. Bezeichnet man die Menge aller Blöcke von RG mit $\mathrm{Bl}(RG)$, so ist also

$$\mathrm{Cf}(G) = \bigoplus_{B \in \mathrm{Bl}(RG)} \mathrm{Cf}(B).$$

Für $B \in \mathrm{Bl}(RG)$ und $S \in \mathrm{Sec}_p(G)$ setzen wir $\mathrm{Cf}(B|S) := \mathrm{Cf}(G|S) \cap \mathrm{Cf}(B)$.

Satz. *Ist K ein Zerfällungskörper für die endliche Gruppe G, so ist*

$$\mathrm{Cf}(G) = \bigoplus_{B \in \mathrm{Bl}(RG)} \bigoplus_{S \in \mathrm{Sec}_p(G)} \mathrm{Cf}(B|S).$$

Beweis. Für $B \in \mathrm{Bl}(G)$ und $x \in G$ sei $\psi_{x,B} := \sum_{\chi \in \mathrm{Irr}(B)} \chi(x^{-1})\chi$. Ist S die p-Sektion von G mit $x \in S$, so ist $\psi_{x,B} \in \mathrm{Cf}(B|S)$ nach 38.6. Wegen der klassischen zweiten Orthogonalitätsrelation ist

$$\frac{1}{|C_G(x)|} \sum_{B \in \mathrm{Bl}(RG)} \psi_{x,B} = \frac{1}{|C_G(x)|} \sum_{\chi \in \mathrm{Irr}(G)} \chi(x^{-1})\chi$$

die charakteristische Funktion der Konjugationsklasse C von x. Daher ist

$$\mathrm{Cf}(G) = \sum_{B \in \mathrm{Bl}(RG)} \sum_{S \in \mathrm{Sec}_p(G)} \mathrm{Cf}(B|S).$$

Nach der Vorbemerkung ist diese Summe direkt. □

38.8. Definition. Seien K ein Zerfällungskörper für die endliche Gruppe G, $S \in \mathrm{Sec}_p(G)$ und $\psi \in \mathrm{Cf}(G)$. Dann definieren wir $\psi|S \in \mathrm{Cf}(G|S)$ durch $(\psi|S)(x) := \psi(x)$ für $x \in S$ und $(\psi|S)(x) = 0$ für $x \in G \setminus S$.

Satz (Erste Orthogonalitätsrelation für Blöcke)**.** *Seien K ein Zerfällungskörper für die endliche Gruppe G, $S \in \mathrm{Sec}_p(G)$, $B \in \mathrm{Bl}(RG)$ und $\chi \in \mathrm{Irr}(B)$. Dann ist $\chi|S \in \mathrm{Cf}(B|S)$, und für jeden Block $B' \neq B$ von RG und $\chi' \in \mathrm{Irr}(B')$ ist*

$$\sum_{x \in S} \chi(x)\chi'(x^{-1}) = 0.$$

Beweis. Nach 38.7 ist $\chi = \sum_{A \in \mathrm{Bl}(RG)} \sum_{T \in \mathrm{Sec}_p(G)} \psi_{AT}$ mit $\psi_{AT} \in \mathrm{Cf}(A|T)$ für $A \in \mathrm{Bl}(RG)$ und $T \in \mathrm{Sec}_p(G)$. Wegen $\mathrm{Cf}(G) = \bigoplus_{A \in \mathrm{Bl}(RG)} \mathrm{Cf}(A)$ ist $\sum_{T \in \mathrm{Sec}_p(G)} \psi_{AT} = 0$ für jeden Block $A \neq B$ von RG. Daher ist $\chi = \sum_{T \in \mathrm{Sec}_p(G)} \psi_{BT}$, d.h. $\psi_{BT} = \chi|T$ für $T \in \mathrm{Sec}_p(G)$. Insbesondere ist $\chi|S = \psi_{BS} \in \mathrm{Cf}(B|S)$. Für jeden Block $B' \neq B$ von RG und $\chi' \in \mathrm{Irr}(B')$ ist also

$$\frac{1}{|G|} \sum_{x \in S} \chi(x)\chi'(x^{-1}) = \frac{1}{|G|} \sum_{x \in G} (\chi|S)(x)\chi'(x^{-1}) = 0.$$

□

38.9. Satz. *Seien K ein Zerfällungskörper für die endliche Gruppe G und $\chi \in \mathrm{Irr}(G)$. Gehört χ nicht zum Hauptblock von RG, so ist $\sum_{x \in S} \chi(x) = 0$ für $S \in \mathrm{Sec}_p(G)$.*

Beweis. Dies folgt aus 38.8 wegen $1_G \in \mathrm{Irr}(B_0(RG))$. □

KAPITEL 39

Brauers Zweiter Hauptsatz und Anwendungen

Sei φ eine vollständige diskrete Bewertung eines Körpers K der Charakteristik 0 mit Bewertungsring R, Bewertungsideal $\mathrm{Rad}(R) = \pi R$ und algebraisch abgeschlossenem Restklassenkörper $F = R/\pi R$ der Charakteristik $p > 0$. Ferner sei K ein Zerfällungskörper für die endliche Gruppe G.

39.1. Bemerkung. Seien $\chi \in \mathrm{Irr}(G)$ und $u \in G_p$. Dann ist

$$\mathrm{Res}^G_{C_G(u)}(\chi) = \sum_{b \in \mathrm{Bl}(RC_G(u))} \chi_b$$

mit $\chi_b \in \mathrm{Cf}(b)$ für $b \in \mathrm{Bl}(RC_G(u))$. Dabei ist χ_b jeweils eine nichtnegative ganze Linearkombination von $\mathrm{Irr}(b)$.

Satz (Brauers Zweiter Hauptsatz)**.** *Seien $B \in \mathrm{Bl}(RG)$, $\chi \in \mathrm{Irr}(B)$ und $u \in G_p$. Für $s \in \mathbb{C}_G(u)_{p'}$ ist dann*

$$\chi(us) = \sum_{\substack{b \in \mathrm{Bl}(RC_G(u)) \\ \mathrm{Br}_{\langle u \rangle}(\overline{1_B})\overline{1_b} \neq 0}} \chi_b(us).$$

Beweis. Seien V ein irreduzibler KG-Modul mit $\chi_V = \chi$ und L eine R-Form von V, also $\chi_L = \chi_V = \chi$. Sei f das eindeutig bestimmte Idempotent in $ZRC_G(u)$ mit $\mathrm{Br}_{\langle u \rangle}(\overline{1_B}) = \overline{f}$. Nach Nagao ist dann $\mathrm{Res}^G_{C_G(u)}(L) = fL \oplus M$, wobei M $\mathcal{H}$-projektiv zur Menge $\mathcal{H}$ aller p-Untergruppen P von $C_G(u)$ mit $u \notin P$ ist. Die Vertizes der unzerlegbaren direkten Summanden von M enthalten also u nicht. Nach 37.4 ist also $\chi_M(us) = 0$. Daher ist

$$\chi_L(us) = \chi_{fL}(us) = \chi_{fV}(us) = \sum_{\substack{b \in \mathrm{Bl}(RC_G(u)) \\ f1_b \neq 0}} \chi_{1_b V}(us) = \sum_{\substack{b \in \mathrm{Bl}(RC_G(u)) \\ \mathrm{Br}_{\langle u \rangle}(\overline{1_B})\overline{1_b} \neq 0}} \chi_b(us).$$

□

39.2. Satz. *Seien B_0 der Hauptblock von RG, $u \in G_p$ und b_0 der Hauptblock von $RC_G(u)$. Für $\chi \in \mathrm{Irr}(B_0)$ und $s \in C_G(u)_{p'}$ ist dann $\chi(us) = \chi_{b_0}(us)$.*

Beweis. Brauers zweiter und dritter Hauptsatz. □

39.3. Satz. *Sei B_0 der Hauptblock von RG. Dann ist $\bigcap_{\chi \in \mathrm{Irr}(B_0)} \mathrm{Ker}(\chi) = O_{p'}(G)$.*

Beweis. Seien e_0, f_0 die Hauptblockidempotente von RG und $RO_{p'}(G)$. Bekanntlich ist

$$f_0 = \frac{1}{|O_{p'}(G)|} \sum_{g \in O_{p'}(G)} g \in ZRG$$

und $e_0 f_0 \neq 0$, also $e_0 f_0 = e_0$. Für $x \in O_{p'}(G)$ ist $x f_0 = f_0$, also $x e_0 = x f_0 e_0 = f_0 e_0 = e_0$. Für $\chi \in \mathrm{Irr}(B_0)$ ist also $\chi(x) = \chi(x e_0) = \chi(e_0) = \chi(1)$. Daher ist $x \in \mathrm{Ker}(\chi)$. Dies zeigt: $O_{p'}(G) \subseteq \bigcap_{\chi \in \mathrm{Irr}(B_0)} \mathrm{Ker}(\chi)$. Ist der Satz falsch, so enthält also $\bigcap_{\chi \in \mathrm{Irr}(B_0)} \mathrm{Ker}(\chi)$ ein p-Element $u \neq 1$. Nach 38.6 ist dann

$$0 = \sum_{\chi \in \mathrm{Irr}(B_0)} \chi(u)\chi(1) = \sum_{\chi \in \mathrm{Irr}(B_0)} \chi(1)^2.$$

Widerspruch. □

39.4. Satz (Glaubermans Z^*-Satz). *Seien T eine 2-Sylowgruppe von G und i eine Involution in T mit der Eigenschaft, daß $gig^{-1} = i$ für jedes Element $g \in G$ mit $gig^{-1} \in T$ ist. Dann ist $iO_{2'}(G) \in Z(G/O_{2'}(G))$. Im Fall $G \neq \langle i \rangle$ ist also G nicht einfach.*

Beweis. Sei $p = 2$ und G ein Gegenbeispiel minimaler Ordnung. Ist $M \neq 1$ ein Normalteiler in G mit $i \notin M$, so ist iM eine Involution in der 2-Sylowgruppe TM/M von G/M. Ist $gM \in G/M$ mit $TM/M \ni (gM)(iM)(gM)^{-1} = gig^{-1}M$, so ist $gig^{-1} \in TM$, also $mgig^{-1}m^{-1} \in T$ für ein $m \in M$. Nach Voraussetzung ist $mgig^{-1}m^{-1} = i$, also $gig^{-1}M = mgig^{-1}m^{-1}M = iM$. Daher erfüllen $\overline{G} := G/M$, $\overline{T} := TM/M$, $\overline{i} := iM$ die Voraussetzungen des Satzes. Wegen $|\overline{G}| < |G|$ ist also $\overline{i}O_{2'} \in Z(\overline{G}/O_{2'}(\overline{G}))$.
Im Fall $O_{2'}(G) \neq 1$ könnte man diese Überlegung auf $M := O_{2'}(G)$ anwenden. Wegen $O_{2'}(\overline{G}) = 1$ wäre dann $\overline{i} \in Z(\overline{G})$ im Widerspruch zur Wahl von G. Also ist $O_{2'}(G) = 1$.
Ist H eine echte Untergruppe von G mit $i \in H$, S eine 2-Sylowgruppe von H mit $i \in S$ und $x \in G$ mit $xSx^{-1} = T$, so ist $xix^{-1} \in T$, also $xix^{-1} = i$ nach Voraussetzung. Ist $h \in H$ mit $hih^{-1} \in S$, so ist $xhih^{-1}x^{-1} \in T$, also $xhih^{-1}x^{-1} = i = xix^{-1}$ und $hih^{-1} = i$. Daher erfüllen H, S, i die Voraussetzungen des Satzes. Wegen $|H| < |G|$ ist also $iO_{2'}(H) \in Z(H/O_{2'}(H))$.
Wir nehmen an, daß G einen echten Normalteiler N mit $i \in N$ enthält. Dann können wir die obigen Überlegungen auf $H = N$ anwenden. Wegen $O_{2'}(N) \subseteq O_{2'}(G) = 1$ erhalten wir $i \in Z(N)$. Ferner ist $Z(N)$ eine 2-Gruppe, d.h. $Z(N) \subseteq T$. Für $g \in G$ ist also $gig^{-1} \in Z(N) \subseteq T$, d.h. $gig^{-1} = i$. Daher ist $i \in Z(G)$. Dieser Widerspruch zeigt, daß G der einzige Normalteiler von G ist, der i enthält.
Für $t \in T$ ist $tit^{-1} \in T$, also $tit^{-1} = i$ nach Voraussetzung. Daher ist $i \in Z(T)$. Wegen $Q := O_2(G) \subseteq T$ ist also $i \in C_G(T) \subseteq C_G(Q) \trianglelefteq G$. Folglich ist $C_G(Q) = G$ und $Q \subseteq Z(G)$. Schreibt man $O_{2'}(G/Q) = X/Q$ mit einem Normalteiler X von G, so besitzt Q nach Schur-Zassenhaus ein Komplement Y in X. Wegen $Q \subseteq Z(G)$ ist $X = Q \times Y$, also $Y \subseteq O_{2'}(X) \subseteq O_{2'}(G) = 1$. Daher ist $X = Q$ und $O_{2'}(G/Q) = 1$. Wegen $i \notin Z(G)$ ist $i \notin Q$. Im Fall $Q \neq 1$ wäre also, wie zu Beginn des Beweises gezeigt, $iQ \in Z(G/Q)$. Dann wäre aber $\langle i, Q \rangle$ ein 2-Normalteiler von G im Widerspruch zu $Q = O_2(G)$. Daher ist $O_2(G) = Q = 1$.
Wir nehmen an, daß i die einzige Involution in T ist. Wie in der Gruppentheorie gezeigt, ist T dann zyklisch oder eine (verallgemeinerte) Quaternionengruppe. Ist T zyklisch, so ist G 2-nilpotent, wie in der Gruppentheorie gezeigt. Wegen $O_{2'}(G) = 1$ ist dann $G = T$ und $i \in Z(G)$. Ist T eine Quaternionengruppe, so ist G nach dem Satz von Brauer-Suzuki (10) kein Gegenbeispiel.
Sei also j eine Involution in $T \setminus \{i\}$.
Beh.: Für $g \in G$ und $\chi \in \mathrm{Irr}(B_0(RG))$ ist $\chi(i \cdot gjg^{-1}) = \chi(ij)$.
Bew.: Nach Voraussetzung ist $gjg^{-1} \neq i$, also $t := i \cdot gjg^{-1} \neq 1$. Ferner ist $iti^{-1} = gjg^{-1} \cdot i = t^{-1} = (gjg^{-1}) \cdot t \cdot (gjg^{-1})^{-1}$.
Wir betrachten zunächst den Fall, daß t eine Involution ist. Dann ist $i \cdot gjg^{-1} = t = t^{-1} = gjg^{-1} \cdot i$, d.h. $i \in C_G(gjg^{-1})$. Sei $P \in \mathrm{Syl}_2(C_G(gjg^{-1}))$ mit $i \in P$. Wegen $gig^{-1} \in gC_G(j)g^{-1} = C_G(gjg^{-1})$ existiert ein Element $h \in C_G(gjg^{-1})$ mit $hgig^{-1}h^{-1} \in P$. Wie oben gezeigt, ist $hgig^{-1}h^{-1} = i$. Daher ist $i \cdot gjg^{-1} = (hgig^{-1}h^{-1})(hgjg^{-1}h^{-1}) = (hg)ij \cdot (hg)^{-1}$ und $\chi(i \cdot gjg^{-1}) = \chi(ij)$.
Sei also t keine Involution. Für $n \in \mathbb{Z}$ ist $t^n(gjg^{-1})t^{-n} = t^nt^ngjg^{-1} = t^{2n}gjg^{-1}$. Im Fall $2 \nmid |\langle t \rangle|$ könnten wir n so wählen, daß $t^{2n} = t$ ist. Dann wäre aber $t^n(gjg^{-1})t^{-n} = t \cdot gjg^{-1} = i$. Da i und j nicht konjugiert sind, wäre das ein Widerspruch. Daher ist $|\langle t \rangle|$ gerade. Sei z die einzige Involution in $\langle t \rangle$. Dann sind $i, gjg^{-1} \in C_G(z) =: H$. Wegen $O_2(G) = 1$ ist $H < G$, alsi $iO_{2'}(H) \in Z(H/O_{2'}(H))$, wie oben gezeigt. Daher ist $t = i \cdot gjg^{-1} \equiv gjg^{-1} \cdot i = t^{-1} \pmod{O_{2'}(H)}$, also $t^2 \in O_{2'}(H)$. Insbesondere hat t^2 ungerade Ordnung, d.h. $\langle t \rangle = \langle z \rangle \times \langle t^2 \rangle$. Nach 39.2 existieren Zahlen $a_\varphi \in \mathbb{Z}$ mit $\chi(zy) = \sum_{\varphi \in \mathrm{Irr}(B_0(H))} a_\varphi \varphi(zy)$ für alle $y \in H_{2'}$. Schreibt man $t = zy$ mit $y \in \langle t^2 \rangle \subseteq O_{2'}(H)$, so ist $\varphi(t) = \varphi(zy) = \varphi(y)$ für $\varphi \in \mathrm{Irr}(B_0(H))$ nach 39.3. Folglich ist $\chi(i \cdot gjg^{-1}) = \chi(t) = \chi(zy) = \chi(t)$. Andererseits ist $t = zt^{2n}$ für ein $n \in \mathbb{N}$, also $z = t \cdot t^{-2n} = i \cdot gjg^{-1} \cdot t^{-2n} = i \cdot t^{2n} \cdot gjg^{-1} = i \cdot t^n \cdot gjg^{-1} \cdot t^{-n}$. Da z eine Involution ist, folgt aus dem ersten Teil des Beweises der Behauptung $\chi(z) = \chi(i \cdot t^ngjg^{-1}t^{-n}) = \chi(ij)$. Damit ist die Behauptung vollständig bewiesen.
Seien I, J die Konjugationsklassen von i bzw. j in G. Dann ist

$$\frac{\chi(I^*)}{\chi(1)} \frac{\chi(J^*)}{\chi(1)} = \frac{\chi(I^+J^+)}{\chi(1)}.$$

Dabei ist I^+J^+ eine Summe von $|I|\cdot|J|$ Elementen der Form $(xix^{-1})(yjy^{-1}) = x(ix^{-1}yjy^{-1}x)x^{-1}$. Nach der obigen Behauptung ist also

$$\frac{|I|\,\chi(i)}{\chi(1)}\,\frac{|J|\,\chi(j)}{\chi(1)} = \frac{|I|\cdot|J|\,\chi(ij)}{\chi(1)},$$

d.h. $\chi(i)\chi(j) = \chi(1)\chi(ij)$.
Wegen $i \in Z(T)$ ist auch ij eine Involution in $T \setminus \{i\}$. Daher ist analog $\chi(i)\chi(ij) = \chi(1)\chi(j)$. Folglich ist $\chi(i)^2\chi(j) = \chi(i)\chi(1)\chi(ij) = \chi(1)^2\chi(j)$. Im Fall $\chi(j) \neq 0$ ist also $\chi(i) = \pm\chi(1)$ und damit $i \in Z(\chi)$. Wir haben also bewiesen: Ist $\chi\,\mathrm{Irr}(B_0(RG))$ und $\chi(j) \neq 0$ für eine Involution j in $T \setminus \{i\}$, so ist $i \in Z(\chi)$.
Sei N der Durchschnitt der Kerne aller $\chi \in \mathrm{Irr}(B_0(RG))$ mit $\chi(j) \neq 0$ für eine Involution $j \in T \setminus \{i\}$. Dann ist $iN \in Z(G/N)$. Wegen $O_{2'}(G) = 1$ ist $T \cap N \neq 1$. Wir nehmen zunächst an, daß $T \cap N$ eine Involution $j \neq i$ enthält. Für $\chi \in \mathrm{Irr}(B_0(RG))$ ist dann $\chi(j) = 0$ oder $\chi(j) = \chi(1)$. Daher ist

$$0 = \sum_{\chi \in \mathrm{Irr}(B_0(RG))} \chi(j)\,\chi(1) = \sum_{\substack{\chi \in \mathrm{Irr}(B_0(RG)) \\ \chi(j) \neq 0}} \chi(1)^2.$$

Dies ist ein Widerspruch, da 1_G zu $B_0(RG)$ gehört. Daher ist i die einzige Involution in $T \cap N$. Wegen $i \in N$ ist dann $N = G$, d.h. N enthält doch eine weitere Involution aus $T \setminus \{i\}$. Widerspruch. □

Bemerkung. Für ungerade Primzahlen gilt ein analoger Satz. Ein Beweis ohne Verwendung der Klassifikation der endlichen einfachen Gruppen ist jedoch unbekannt.

39.5. Satz. *Seien S, T p-Sylowgruppen von G und Q eine Untergruppe von $Z(S)$ mit $Q \trianglelefteq T$. Dann ist $Q \leq Z(T)$.*

Beweis. Offenbar sind S, T p-Sylowgruppen von $N_G(Q)$. Daher existiert ein Element $g \in N_G(Q)$ mit $T = gSg^{-1} \subseteq gC_G(Q)g^{-1} = C_G(gQg^{-1}) = C_G(Q)$. Folglich ist $Q \subseteq Z(T)$. □

39.6. Satz. *Zu jeder p-Untergruppe P von G, die in einer p-Sylowgruppe S von G normal, in einer anderen p-Sylowgruppe T von G nicht normal enthalten ist, existiert eine Zahl $r \in \mathbb{N}$ und paarweise verschiedene Untergruppen $P_1 = P, P_2, \ldots, P_r$ von G mit folgenden Eigenschaften:*

(a) *$r > 1$ und $p \nmid r$.*
(b) *Für $i = 1, \ldots, r$ ist $P_i \trianglelefteq P_0 := \langle P_1, \ldots, P_r\rangle \subseteq S$.*
(c) *Zu jeder p-Sylowgruppe U von G existiert ein $i \in \{1, \ldots, r\}$ mit $P_i \ntrianglelefteq U$.*
(d) *$P_1, \ldots, P_r$ sind genau die verschiedenen Konjugierten von P in $N_G(P_0)$.*
(e) *$N_S(P_0)$ und $C_S(P_0)$ sind p-Sylowgruppen von $N_G(P_0)$ bzw. $C_G(P_0)$.*
(f) *$P_1, \ldots, P_r$ sind genau die Konjugierten von P in $N_G(P_0) \cap N_G(C_S(P_0))$.*
(g) *Es existiert eine Primzahl $q \neq p$ und ein q-Element $g \in N_G(P_0) \cap N_G(C_S(P_0))$ mit $g \notin N_G(P)$.*

Beweis. Wir wählen T so, daß $D := N_T(P)$ möglichst groß ist. Wegen $P < T$ ist $P < D$, und wegen $D < T$ ist $D < N_T(D)$; isnbesondere ist $N_T(D) \nsubseteq N_G(P)$. Seien $Q_1 = P, Q_2, \ldots, Q_s$ die verschiedenen Konjugierten von P in $N_G(D)$. Wegen $N_G(D) \nsubseteq N_G(P)$ ist $s > 1$. Wegen $P \trianglelefteq D$ ist $Q_i \trianglelefteq D$, also $Q_i \trianglelefteq Q_0 := \langle Q_1, \ldots, Q_s\rangle \trianglelefteq D$ für $i = 1, \ldots, s$.
Sei R_1 eine p-Sylowgruppe von $N_G(P) \cap N_G(D)$ mit $D \subseteq R_1$, und sei S_1 eine p-Sylowgruppe von $N_G(P)$ mit $R_1 \subseteq S_1$. Nach Vorraussetzung ist S_1 auch eine p-Sylowgruppe von G. Wegen $D < S_1$ ist $D < N_{S_1}(D) = R_1 \subseteq N_G(D) \subseteq N_G(Q_0) =: H$. Sei S_2 eine p-Sylowgruppe von H mit $R_1 \subseteq S_2$, und sei T_2 eine p-Sylowgruppe von G mit $S_2 \subseteq T_2$. Wegen $N_{T_2}(P) \supseteq R_1 > D$ ist $P \trianglelefteq T_2$, d.h. $T_2 \subseteq N_G(P)$ und $N_H(P) \supseteq H \cap T_2 = S_2$.
Seien $Q_1 = P, Q_2, \ldots, Q_s, \ldots, Q_r$ die verschiedenen Konjugierten von P in H. Wegen $P = Q_1 \trianglelefteq Q_0$ ist $Q_i \trianglelefteq Q_0$ für $i = 1, \ldots, r$, also $Q_0 = \langle Q_1, \ldots, Q_r\rangle$. Offenbar ist $r = |H : N_H(P)|$. Da $N_H(P)$ die p-Sylowgruppe S_2 von H enthält, ist $p \nmid r$. Damit gilt (a).
Wir nehmen an, daß eine p-Sylowgruppe U von G mit $Q_i \trianglelefteq U$ für $i = 1, \ldots, r$ existiert. Dann ist $U \subseteq N_G(Q_0) = H$. Folglich ist $Q_0 \trianglelefteq U_1$ für $i = 1, \ldots, r$ und jede p-Sylowgruppe U_1 von H. Dies steht jedoch im Widerspruch zu $P \ntrianglelefteq N_T(D) \leq N_G(D) \subseteq H$. Da S und T_2 p-Sylowgruppen von $N_G(P)$ sind,

existiert ein Element $x \in N_G(P)$ mit $S = xT_2x^{-1}$. Wir setzen $P_i := xQ_ix^{-1}$ für $i = 0, \dots, r$. Dann ist $P_i \trianglelefteq P_0 = \langle P_1, \dots, P_r \rangle$ für $i = 1, \dots, r$. Wegen $Q_0 \subseteq D \subseteq R_1 \subseteq S_2 \subseteq T_2$ ist $P_0 \subseteq S$. Daher gilt (b).
(c) und (d) folgen aus der entsprechenden Eigenschaft von $Q_1, \dots Q_r$.
Da $N_{T_2}(Q_0) = T_2 \cap H = S_2$ eine p-Sylowgruppe von $H = N_G(Q_0)$ ist, ist $N_S(P_0)$ eine p-Sylowgruppe von $N_G(P_0)$. Daher ist $C_S(P_0)$ eine p-Sylowgruppe von $C_G(P_0)$. Folglich gilt (e).
Wir setzen $J := N_G(P_0) \cap N_G(C_S(P_0))$. Seien $i \in \{1, \dots, r\}$ und $h \in N_G(P_0)$ mit $P_i = hPh^{-1}$. Dann ist $hC_S(P_0)h^{-1}$ eine p-Sylowgruppe von $hC_G(P_0)h^{-1} = C_G(hP_0h^{-1}) = C_G(P_0)$. Daher existiert ein $k \in C_G(P_0)$ mit $C_S(P_0) = khC_S(P_0)h^{-1}k^{-1}$. Dann ist $g := kh \in J$ mit $gPg^{-1} = khPh^{-1}k^{-1} = kP_ik^{-1} = P_i$. Folglich gilt (f).
Sei jetzt q ein Primteiler von r, und sei Q eine q-Sylowgruppe von J. Dann ist $q \neq p$ nach (a) und $Q \not\subseteq N_J(P)$ nach (f). Also gilt (g). $\square$

39.7. Satz (Glauberman)**.** *Seien S eine 2-Sylowgruppe von G und $x \in S$. Für jedes Element $g \in G$ mit $g^{-1}xg \in S$ sei $g^{-1}xg = x$. Dann ist $xO_{2'}(G) \in Z(G/O_{2'}(G))$.*

Beweis. (Induktion nach $|G| + |\langle x \rangle|$) O.B.d.A. sei $x \neq 1$. Nach Voraussetzung ist $x \in Z(S)$, also auch $y := x^2 \in Z(S)$. Wir betrachten zunächst den Fall, daß ein Element $h \in G$ mit $h^{-1}yh \in S \setminus \{y\}$ existiert. Ist $h^{-1}yh \in Z(S)$, so existiert, wie in der Gruppentheorie gezeigt, ein Element $g \in N_G(S)$ mit $g^{-1}yg = h^{-1}yh \neq y$. Wegen $y = x^2$ ist dann auch $g^{-1}xg \neq x$ im Widerspruch zur Voraussetzung. Daher ist $h^{-1}yh \notin Z(S)$.
Wir setzen $P := \langle y \rangle$ und $T := hSh^{-1}$. Wegen $h^{-1}Ph \not\subseteq Z(S)$ ist $P \not\subseteq Z(T)$, also auch $P \ntrianglelefteq T$ nach 39.5. Damit ist 39.6 anwendbar. Wir wählen P_0 und g wie in 39.6. Wegen $g^{-1}Pg \neq P$ ist $g^{-1}yg \neq y$, also $g^{-1}xg \neq x$. Andererseits ist $x \in Z(S) \subseteq C_S(P_0)$, also $g^{-1}xg \in C_S(P_0) \subseteq S$ im Widerspruch zur Voraussetzung.
Dieser Widerspruch zeigt, daß $h^{-1}yh = y$ für alle $h \in G$ mit $h^{-1}yh \in S$ ist. Nach Induktion ist $yO_{2'}(G) \in Z(G/O_{2'}(G))$. Wir nehmen $M := O_{2'}(G) \neq 1$ an. Ist $gM \in G/M$ mit $SM/M \ni (gM)(xM)(gM)^{-1} = gxg^{-1}M$, so ist $gxg^{-1} \in SM$, also $hgxg^{-1}h^{-1} \in S$ für ein $h \in M$. Nach Voraussetzung ist $hgxg^{-1}h^{-1} = x$, also $gxg^{-1}M = hgxg^{-1}h^{-1}M = xM$. Dies zeigt, daß $\overline{G} := G/M$, $\overline{S} := SM/M$ und $\overline{x} := xM$ die Voraussetzungen des Satzes erfüllen. Nach Induktion ist also $\overline{x}O_{2'}(\overline{G}) \in Z(\overline{G}/O_{2'}(\overline{G}))$. Wegen $O_{2'}(\overline{G}) = 1$ ist also $\overline{x} \in Z(\overline{G})$. Daher können wir $O_{2'}(G) = 1$ annehmen. Dann ist $y \in Z(G)$. Wir setzen $\overline{G} := G/\langle y \rangle$, $\overline{S} := S/\langle y \rangle$, $\overline{x} := x\langle y \rangle$. Ist $\overline{g} = g\langle y \rangle \in \overline{G}$ mit $\overline{gxg}^{-1} \in \overline{S}$, so ist $gxg^{-1} \in S$, also $gxg^{-1} = x$ nach Voraussetzung und $\overline{gxg}^{-1} = \overline{x}$. Dies zeigt, daß $\overline{G}, \overline{S}, \overline{x}$ die Voraussetzungen von 39.4 erfüllen. Folglich ist $\overline{x}O_{2'}(\overline{G}) \in Z(\overline{G}/O_{2'}(\overline{G}))$. Wir schreiben $O_{2'}(\overline{G}) = M/\langle y \rangle$ mit einem Normalteiler M von G. Nach Schur-Zassenhaus besitzt die normale 2-Sylowgruppe $\langle y \rangle$ von M ein Komplement X in M. Wegen $y \in Z(G)$ ist $M = \langle y \rangle \times X$, also $X = O_{2'}(M) \subseteq O_{2'}(G) = 1$. Daher ist $M = \langle y \rangle$ und $O_{2'}(\overline{G}) = 1$. Folglich ist $\overline{x} \in Z(\overline{G})$ und $\langle x \rangle \trianglelefteq G$. Für $g \in G$ ist also $gxg^{-1} \in \langle x \rangle \subseteq S$, d.h. $gxg^{-1} = x$. Dies zeigt $x \in Z(G)$. $\square$

Bemerkung. Man kann die obigen Sätze dazu verwenden, um zu zeigen, daß viele 2-Gruppen nicht 2-Sylowgruppen von endlichen einfachen Gruppen sein können. Zur Illustration beweisen wir die folgende Verallgemeinerung des Satzes von Brauer-Suzuki.

39.8. Satz. *Besitzt G eine 2-Sylowgruppe S, die direktes Produkt (verallgemeinerter) Quaternionengruppen ist, so ist G nicht einfach.*

Beweis. Sei $S = Q_1 \times \ldots \times Q_n$ mit (verallgemeinerten) Quaternionengruppen $Q_1, \dots, Q_n$. Für $i = 1, \dots, n$ sei u_i die einzige Involution in Q_i. Dann ist $u_i \in Z(Q_i)$, und es existieren $x_i, y_i \in Q_i$ mit $u_i = x_iy_ix_i^{-1}y_i^{-1}$. Wir setzen $u := u_1 \dots u_n$ und werden $uO_{2'}(G) \in Z(G/O_{2'}(G))$ zeigen. Dazu sei $g \in G$ mit $gug^{-1} \in S$. Da alle Involutionen von S in $Z(S)$ liegen, folgt $gug^{-1} \in Z(S)$. Wegen $u \in Z(S)$ existiert also ein $h \in N_G(S)$ mit $gug^{-1} = huh^{-1}$. Offenbar ist $S = hSh^{-1} = hQ_1h^{-1} \times \ldots \times hQ_nh^{-1}$. Nach Krull-Schmidt existiert eine Permutation σ von $1, \dots, n$ und ein normaler Automorphismus α von S mit $hQ_ih^{-1} = \alpha(Q_{\sigma(i)})$. Da α normal ist, ist $\alpha(x_i) = x_iz_i$ und $\alpha(y_i) = y_ic_i$ mit $c_i, z_i \in Z(S)$. Folglich ist

$$\begin{aligned} hu_ih^{-1} &= \alpha(u_{\sigma(i)}) = \alpha(x_{\sigma(i)}y_{\sigma(i)}x_{\sigma(i)}^{-1}y_{\sigma(i)}^{-1}) \\ &= x_{\sigma(i)}z_{\sigma(i)}y_{\sigma(i)}c_{\sigma(i)}z_{\sigma(i)}^{-1}x_{\sigma(i)}^{-1}c_{\sigma(i)}^{-1}y_{\sigma(i)}^{-1} = u_{\sigma(i)}. \end{aligned}$$

für $i = 1, \ldots, n$. Folglich ist $gug^{-1} = huh^{-1} = u$. Aus 39.4 folgt $uO_{2'}(G) \in Z(G/O_{2'}(G))$. $\square$

KAPITEL 40

Brauer-Charaktere

Sei φ eine vollständige diskrete Bewertung eines Körpers K der Charakteristik 0 mit Bewertungsring R, Bewertungsideal $\mathrm{Rad}(R) = \pi R$ und algebraisch abgeschlossenem Restklassenkörper $F = R/\pi R$ der Charakteristik $p > 0$. Ferner sei G eine endliche Gruppe, und K enthalte die $|G|$-ten Einheitswurzeln; insbesondere ist K ein Zerfällungskörper für G.

40.1. Bemerkung. Sei $\Delta : G \to \mathrm{GL}(n, F)$ eine Matrixdarstellung von G über F. Dann bezeichnet man die Abbildung $\chi_\Delta : G \to F,\ g \mapsto \mathrm{spur}(\Delta(g))$ als *Charakter* von Δ. Für jede zu Δ äquivalente Matrixdarstellung Δ' von G ist wie üblich $\chi_\Delta = \chi_{\Delta'}$. Dies erlaubt es, zu jedem endlich-dimensionalen FG-Modul M einen *Charakter* $\chi_M : G \to F$ durch $\chi_M = \chi_\Delta$ zu definieren, wobei Δ eine Matrixdarstellung zu M ist. Für konjugierte Elemente $g, g' \in G$ ist natürlich $\chi_M(g) = \chi_M(g')$, d.h. χ_M ist eine Klassenfunktion. Zu jedem $g \in G$ existiert ein $T \in \mathrm{GL}(n, F)$ mit der Eigenschaft, daß

$$T\Delta(g)T^{-1} = \begin{pmatrix} \lambda_1 & & 0 \\ & \ddots & \\ * & & \lambda_n \end{pmatrix}$$

mit $\lambda_1, \ldots, \lambda_n \in F$ ist. Dabei sind $\lambda_1, \ldots \lambda_n$ $|\langle g \rangle|$-te Einheitswurzeln in F. Wir bezeichnen mit g_p den p-Faktor und mit $g_{p'}$ den p'-Faktor von g. Bekanntlich sind g_p und $g_{p'}$ Potenzen von g. Da 1 die einzige Einheitswurzel von p-Potenzordnung in F ist, hat $T\Delta(g_p)T^{-1}$ die Form

$$T\Delta(g_p)T^{-1} = \begin{pmatrix} 1 & & 0 \\ & \ddots & \\ * & & 1 \end{pmatrix}.$$

Folglich hat $T\Delta(g_{p'})T^{-1}$ die Form

$$T\Delta(g_{p'})T^{-1} = \begin{pmatrix} \lambda_1 & & 0 \\ & \ddots & \\ * & & \lambda_n \end{pmatrix};$$

insbesondere ist $\chi_M(g) = \chi_M(g_{p'})$.
Wir schreiben $FG/JFG \cong \mathrm{Mat}(d_1, F) \times \ldots \times \mathrm{Mat}(d_l, F)$ mit $d_1, \ldots, d_l \in \mathbb{N}$. Bekanntlich ist l die Anzahl der p-regulären Konjugationsklassen von G, und die entsprechenden Abbildungen $\Delta_i : FG \to FG/JFG \to \mathrm{Mat}(d_i, F)$ $(i = 1, \ldots, l)$ sind bis auf Äquivalenz genau die irreduziblen Darstellungen von FG. Offenbar sind $\chi_{\Delta_1}, \ldots, \chi_{\Delta_l}$ linear unabhängig über F. Dennoch sind diese Charaktere nicht sehr aussagekräftig, da z.B. $\chi_{M^p} = p\chi_M = 0$ für jeden FG-Modul M gilt.

40.2. Bemerkung. Sei $\Delta : G \to \mathrm{GL}(n, F)$ eine Matrixdarstellung von G über F, und sei $|G| = p^a r$ mit $p \nmid r$. Für $g \in G_{p'}$ ist dann $\Delta(g)^r = 1$, d.h. das Minimalpolynom von $\Delta(g)$ teilt $X^r - 1$. Die Nullstellen von $X^r - 1$ sind die r verschiedenen r-ten Einheitswurzeln in F. Daher ist $\Delta(g)$ diagonalisierbar, d.h. es existiert ein $T \in \mathrm{GL}(n, F)$ mit der Eigenschaft, daß

$$T\Delta(g)T^{-1} = \begin{pmatrix} \lambda_1 & & 0 \\ & \ddots & \\ 0 & & \lambda_n \end{pmatrix}$$

mit r-ten Einheitswurzeln $\lambda_1, \ldots, \lambda_n$ in F ist. Die r-ten Einheitswurzeln bilden eine zyklische Gruppe V der Ordnung r in $F^\times$. Analog bilden die r-ten Einheitswurzeln eine zyklische Gruppe U der Ordnung r in $K^\times$. Offensichtlich ist $U \subseteq R$, und die Einschränkung der kanonischen Abbildung $\overline{} : R \to R/\pi R = F$ liefert einen Homomorphismus $U \to V$. Dieser ist surjektiv; setzt man nämlich $\overline{}$ in kanonischer Weise zu einem Homomorphismus $\overline{} : R[X] \to F[X]$ fort, so ist

$$\prod_{v \in V} (X - v) = X^r - 1_F = \overline{X^r - 1_R} = \overline{\prod_{u \in U} (X - u)} = \prod_{u \in U} (X - \overline{u}).$$

Daher ist der kanonische Homomorphismus $U \to V$ sogar bijektiv. Zu jeder r-ten Einheitswurzel existiert also genau eine r-te Einheitswurzel $\hat{\lambda}$ in R mit $\lambda = \hat{\lambda} + \pi R$. Setzt man also $\varphi_\Delta(g) := \hat{\lambda_1} + \ldots + \hat{\lambda_n}$, so erhält man auf diese Weise eine Abbildung $\varphi_\Delta : G_{p'} \to R$. Wir nennen φ_Δ den *Brauer-Charakter* von Δ. Ist Δ' eine zu Δ äquivalente Matrixdarstellung, so sind für $g \in G_{p'}$ die Matrizen $\Delta(g)$ und $\Delta'(g)$ ähnlich, besitzen also die gleichen Eigenwerte (mit Vielfachheiten). Daher ist $\varphi_\Delta(g) = \varphi_{\Delta'}(g)$. Ist M ein endlich-dimensionaler FG-Modul und $\Delta : G \to \mathrm{GL}(n, F)$ eine entsprechende Matrixdarstellung, so setzen wir $\varphi_M := \varphi_\Delta$ und nennen φ_M den *Brauer-Charakter* von M; diese Definition hängt nicht von der Wahl von Δ ab. Eine ähnliche Überlegung zeigt, daß $\varphi_\Delta(g) = \varphi_\Delta(g')$ für konjugierte Elemente $g, g' \in G_{p'}$ gilt. Ferner ist $\varphi_\Delta(g) + \pi R = \chi_\Delta(g)$. Für jeden Untermodul N von M ist außerdem $\varphi_M = \varphi_N + \varphi_{M/N}$; denn zu M gehört eine Matrixdarstellung der Form $g \mapsto \begin{pmatrix} \Delta'(g) & * \\ 0 & \Delta''(g) \end{pmatrix}$, wobei Δ' und Δ'' Matrixdarstellungen zu N bzw. M/N sind.

Satz. *Seien $M_1, \ldots, M_l$ Repräsentanten für die Isomorphieklassen einfacher FG-Moduln. Dann sind die Brauercharaktere $\varphi_{M_1}, \ldots, \varphi_{M_l}$ linear unabhängig über K.*

Beweis. Wir nehmen an, daß es eine nichttriviale Relation $\alpha_1 \varphi_{M_1} + \ldots + \alpha_l \varphi_{M_l} = 0$ mit $\alpha_1, \ldots, \alpha_l \in K$ gibt. Wir können annehmen, daß $\alpha_1, \ldots, \alpha_l \in R$ sind. Außerdem können wir annehmen, daß nicht $\alpha_1, \ldots, \alpha_l \in \pi R$ sind. Nach 40.1 ist dann $\overline{\alpha_1} \chi_{M_1} + \ldots + \overline{\alpha_l} \chi_{M_l} = 0$ eine nichttriviale Realtion mit $\overline{\alpha_1}, \ldots, \overline{\alpha_l} \in F$. Dies widerspricht der linearen Unabhängigkeit von $\chi_{M_1}, \ldots, \chi_{M_l}$. □

Definition. Wir nennen $\varphi_{M_1}, \ldots, \varphi_{M_l}$ die *irreduziblen* Brauercharakter von G und setzen $\mathrm{IBr}(G) := \{\varphi_{M_1}, \ldots, \varphi_{M_l}\}$.

40.3. Bemerkung. Seien $M_1, \ldots, M_l$ Repräsentanten für die Isomorphieklassen einfacher FG-Moduln, und sei M ein beliebiger endlich-dimensionaler FG-Modul. Für $i = 1, \ldots, l$ sei n_i die Vielfachheit von M_i als Kompositionsfaktor von M. Dann ist $\varphi_M = n_1 \varphi_{M_1} + \ldots + n_l \varphi_{M_l}$. Zwei FG-Moduln M, N haben also genau dann den gleichen Brauercharakter, wenn sie die gleichen Kompositionsfaktoren (mit gleichen Vielfachheiten) haben. Da l auch die Anzahl der p-regulären Konjugationsklassen von G ist, bilden $\varphi_{M_1}, \ldots, \varphi_{M_l}$ eine Basis für den K-Vektorraum $\mathrm{Cf}_{p'}(G)$ aller Funktionen $\psi : G_{p'} \to K$ mit $\psi(yxy^{-1}) = \psi(x)$ für $x \in G_{p'}$, $y \in G$.

40.4. Bemerkung. Sei $\Delta : G \to \mathrm{GL}(n, R)$ eine Darstellung von G über R uns sei $g \in G_{p'}$. Schreibt man $|G| = p^a r$ mit $p \nmid r$, dann sind die Eigenwerte $\mu_1, \ldots, \mu_n$ von $\Delta(g)$ r-te Einheitswurzeln. Durch *Reduktion modulo* π wird aus Δ eine Matrixdarstellung $\overline{\Delta} : G \to \mathrm{GL}(n, F)$. Die Eigenwerte von $\overline{\Delta}(g)$ sind dabei $\overline{\mu_1}, \ldots, \overline{\mu_n}$; denn das charakteristische Polynom von $\overline{\Delta}(g)$ entsteht aus dem charakteristischen Polynom von $\Delta(g)$ durch Reduktion nach π. Daher ist $\varphi_{\overline{\Delta}}(g) = \chi_\Delta(g)$, d.h. $\varphi_{\overline{\Delta}} = \chi_\Delta | G_{p'}$. Für jeden Charakter $\chi : G \to K$ ist also $\chi | G_{p'}$ ein Brauercharakter von G. Ist $\Delta' : G \to \mathrm{GL}(n, R)$ eine Matrixdarstellung von G, die über K zu Δ zu Δ äquivalent ist, so ist $\chi_\Delta = \chi_{\Delta'}$, also auch $\varphi_{\overline{\Delta}} = \varphi_{\overline{\Delta'}}$. Gehört Δ zum RG-Gitter L, so gehört $\overline{\Delta}$ zum FG-Modul $L/\pi L$. Man erhält:

Satz. *Seien L_1, L_2 R-Formen eines KG-Moduls V. Dann haben die FG-Moduln $L_1/\pi L_1, L_2/\pi L_2$ die gleichen Kompositionsfaktoren (mit Vielfachheiten).*

Beweis. Wegen $\chi_{L_1} = \chi_V = \chi_{L_2}$ ist $\varphi_{L_1/\pi L_1} = \chi_{L_1} | G_{p'} = \chi_{L_2} | G_{p'} = \varphi_{L_2/\pi L_2}$. Aus 40.3 folgt also die Behauptung. □

40.5. Bemerkung. Nach 40.4 existieren zu jedem $\chi \in \mathrm{Irr}(G)$ Zahlen $d_{\chi\varphi} \in \mathbb{N}$ mit

$$\chi|G_{p'} = \sum_{\varphi \in \mathrm{IBr}(G)} d_{\chi\varphi}\varphi.$$

Für jeden irreduziblen KG-Modul V mit Charakter χ, jede R-Form L von V und jeden einfachen FG-Modul M mit Brauercharakter φ ist $d_{\chi\varphi}$ nämlich die Vielfachheit von M als Kompositionsfaktor von $L/\pi L$. Man nennt die Zahlen $d_{\chi\varphi}$ *Zerlegungszahlen* und die Matrix $D := (d_{\chi\varphi})_{\chi\in\mathrm{Irr}(G),\varphi\in\mathrm{IBr}(G)}$ die *Zerlegungsmatrix* von RG.
Wir bezeichnen die p-regulären Konjugationsklassen von G mit $C_1, \ldots, C_l$ und wählen für $i = 1, \ldots, l$ ein Element $x_i \in C_i$. Schreibt man $\mathrm{IBr}(G) = \{\varphi_1, \ldots, \varphi_l\}$, so nennt man die Matrix $\Phi := (\varphi_i(x_j))_{i,j=1}^l$ die *Brauercharaktertafel* von RG. Offenbar ist $\det(\Phi) \in R$. Da $\overline{\varphi_1}, \ldots, \overline{\varphi_l} : G_{p'} \to F$ linear unabhängig sind, ist $\det(\Phi) \notin \pi R$, also $\det(\Phi) \in R^\times$.
Schreibt man $\mathrm{Irr}(G) = \{\chi_1, \ldots, \chi_k\}$ und setzt man $X := (\chi_i(x_j))_{i=1,\ldots,k.\ j=1,\ldots,l}$, so ist $X = D\Phi$.

40.6. Bemerkung. Seien Λ eine R-Ordnung und $e_1, \ldots, e_n$ Repräsentanten für die Konjugationsklassen primitiver Idempotente in Λ. Bekanntlich sind Idempotente e, f genau dann konjugiert, wenn die von ihnen erzeugten Linksideale $\Lambda e, \Lambda f$ isomorphe Λ-Gitter sind. Daher sind $\Lambda e_1, \ldots \Lambda e_n$ Repräsentanten für die Isomorphieklasenn unzerlegbarer projektiver Λ-Gitter. Wir wissen auch, daß die Bilder $\overline{e_1}, \ldots, \overline{e_n}$ von $e_1, \ldots, e_n$ in $\overline{\Lambda} := \Lambda/\pi\Lambda$ auch Repräsentanten für die Konjugationsklassen primitiver Idempotente von $\overline{\Lambda}$ sind. Daher sind $\overline{\Lambda}\overline{e_1}, \ldots, \overline{\Lambda}\overline{e_n}$ Repräsentanten für die Isomorphieklassen unzerlegbarer projektiver $\overline{\Lambda}$-Moduln. Für $i = 1, \ldots, n$ ist dabei $\overline{\Lambda}\overline{e_i} \simeq \Lambda e_i/\pi\Lambda e_i$. Bekanntlich sind $\overline{\Lambda}\overline{e_1}/J(\overline{\Lambda})\overline{e_1}, \ldots \overline{\Lambda}\overline{e_n}/J(\overline{\Lambda})\overline{e_n}$ Repräsentanten für die Isomorphieklassen einfacher $\overline{\Lambda}$-Moduln. Für $i = 1, \ldots, n$ ist dabei $\overline{\Lambda}\overline{e_i}/J(\overline{\Lambda})\overline{e_i} \simeq \Lambda e_i/J(\Lambda)e_i$.

Satz (Brauer-Reziprozität). *Seien $e_1, \ldots, e_l$ Repräsentanten für die Konjugationsklassen primitiver Idempotente in RG. Für $i = 1, \ldots, l$ sei η_i der Charakter des unzerlegbaren projektiven RG-Gitters RGe_i und φ_i der Brauercharakter des entsprechenden einfachen FG-Moduls $M_i := RGe_i/\operatorname{Rad}(RG)e_i$. Dann ist $\eta_i = \sum_{\chi\in\mathrm{Irr}(G)} d_{\chi\varphi_i}\chi$ mit den früher definierten Zerlegungszahlen $d_{\chi\varphi_i}$.*

Beweis. Sei $\chi \in \mathrm{Irr}(G)$, V ein KG-Modul mit Charakter χ und L eine R-Form von V. Für $i = 1, \ldots, l$ ist $d_{\chi\varphi_i}$ die Vielfachheit von M_i als Kompositionsfaktor von $\overline{L} := L/\pi L$. Daher ist

$$\begin{aligned} d_{\chi\varphi_i} &= \dim_F \operatorname{Hom}_{FG}(FG\overline{e_i}, \overline{L}) = \dim_F \overline{e_i}\overline{L} = \dim_F e_iL/\pi e_iL \\ &= \operatorname{rk}_R e_iL = \dim_K e_iV; \end{aligned}$$

denn offenbar ist e_iL eine R-Form des K-Vektorraums e_iV. Daher ist

$$d_{\chi\varphi_i} = \dim_K \operatorname{Hom}_{KG}(KGe_i, V),$$

und dies ist die Vielfachheit von V als Kompositionsfaktor des halbeinfachen KG-Moduls KGe_i. □

Definition. Wir nennen die Charaktere $\eta_1, \ldots, \eta_l$ der unzerlegbaren projektiven RG-Gitter $RGe_1, \ldots, RGe_l$ die *unzerlegbaren projektiven Charaktere* von RG und schreiben $\mathrm{IPr}(G) := \{\eta_1, \ldots, \eta_l\}$.

40.7. Satz. *Seien $\chi_1, \ldots, \chi_k$ die irreduziblen Charaktere, $\varphi_1, \ldots, \varphi_l$ die irreduziblen Brauercharaktere und $\eta_1, \ldots, \eta_l$ die entsprechenden unzerlegbaren projektiven Charaktere von RG. Sind $D = (d_{ij}) \in \mathrm{Mat}(k, l, \mathbb{Z})$ die entsprechende Zerlegungsmatrix und $C = (c_{ij}) \in \mathrm{Mat}(l, \mathbb{Z})$ die entsprechende Cartanmatrix, so gilt $C = D^TD$; insbesondere ist $\det(C) \geq 0$.*

Beweis. Für $i = 1, \ldots, l$ ist $\eta_i = \sum_{r=1}^k d_{ri}\chi_r$ nach 40.6, also

$$\eta_i|G_{p'} = \sum_{r=1}^k d_{ri}\chi_r|G_{p'} = \sum_{r=1}^k\sum_{s=1}^l d_{ri}d_{rs}\varphi_s.$$

Daher ist $\sum_{r=1}^k d_{ri}d_{rj}$ für $j = 1, \ldots, l$ gleich der Vielfachheit des zu φ_j gehörigen einfachen FG-Moduls als Kompositionsfaktor des zu η_i gehörigen unzerlegbaren projektiven FG-Moduls, d.h. es ist $D^TD = C$. Für $x \in \mathbb{R}^l$ ist also $x^TCx = x^TD^TDx = (Dx)^T(Dx) \geq 0$. Daher ist die durch C definierte symmetrische Bilinearform positiv semidefinit. Folglich ist $\det(C) \geq 0$. □

Bemerkung. Nach 37.4 verschwinden $\eta_1, \dots, \eta_l$ auf $G \setminus G_{p'}$. Für $x, y \in G_{p'}$ folgt aus der zweiten Orthogonalitätsrelation:

$$\begin{aligned}\sum_{j=1}^{l} \eta_j(x)\varphi_j(y^{-1}) &= \sum_{j=1}^{l}\sum_{i=1}^{k} d_{ij}\chi_i(x)\varphi_j(y^{-1}) = \sum_{i=1}^{k} \chi_i(x)\chi_j(y^{-1}) \\ &= \begin{cases} |C_G(y)| & \text{falls } x, y \text{ konjugiert} \\ 0 & \text{sonst} \end{cases}.\end{aligned}$$

Daraus folgt, daß $\eta_1, \dots, \eta_l$ den K-Vektorraum der Klassenfunktionen $\psi : G \to K$ mit $\psi|G \setminus G_{p'} = 0$ aufspannen; insbesondere sind $\eta_1, \dots, \eta_l$ eine Basis dieses K-Vektorraums. Daher sind auch $\eta_1|G_{p'}, \dots, \eta_l|G_{p'}$ linear unabhängig über K. Wegen $\eta_i|G_{p'} = \sum_{j=1}^{l} c_{ij}\varphi_j$ für $i = 1, \dots, l$ ist also C regulär.

40.8. Satz. *Seien $\varphi_1, \dots, \varphi_l$ die irreduziblen Brauercharaktere und $\eta_1, \dots, \eta_l$ die entsprechenden unzerlegbaren projektiven Charaktere von G. Dann gilt:*

(i) *Für $i, j = 1, \dots, l$ ist*

$$\frac{1}{|G|} \sum_{x \in G_{p'}} \eta_i(x)\varphi_j(x^{-1}) = \delta_{ij}.$$

(ii) *Für $x \in G_{p'}$ ist $\varphi(|C_G(x)|) = \max\{\varphi(\eta_i(x)) : i = 1, \dots, l\}$.*

Beweis. Seien $x_1, \dots, x_l$ Repräsentanten für die Konjugationsklassen p-regulärer Elemente in G, $\Phi := (\varphi_i(x_j^{-1}))$, $H := (\eta_i(x_j))$ und $S := (\delta_{ij}|C_G(x_i)|)$. Aus Bemerkung 40.7 folgt dann $S = H^T\Phi$, d.h. $H^T\Phi S^{-1} = 1_l$. Folglich ist auch $\Phi S^{-1} H^T = 1_l$. Das bedeutet, daß für $i, j = 1, \dots, l$ gilt:

$$\delta_{ij} = \sum_{r=1}^{l} \varphi_i(x_r^{-1}) \frac{1}{|C_G(x_r))|} \eta_j(x_r) = \frac{1}{|G|} \sum_{x \in G_{p'}} \varphi_i(x^{-1})\eta_j(x).$$

Für $x \in G_{p'}$ ist

$$\begin{aligned}\varphi(|C_G(x)|) &= \varphi\Big(\sum_{i=1}^{l} \eta_i(x)\varphi_i(x^{-1})\Big) \\ &\leq \max\{\varphi(\eta_1(x)\varphi_1(x^{-1})), \dots, \varphi(\eta_l(x)\varphi_l(x^{-1}))\} \\ &\leq \max\{\varphi(\eta_1(x)), \dots, \varphi(\eta_l(x))\}.\end{aligned}$$

Außerdem ist $H^T = S\Phi^{-1}$ mit $\Phi^{-1} =: (\varphi'_{ij}) \in \mathrm{GL}(l, R)$ nach 40.5. Für $i, j = 1, \dots, l$ ist also

$$\varphi(\eta_j(x_i)) = \varphi(|C_G(x_i)|\varphi'_{ij}) \leq \varphi(|C_G(x_i)|).$$

$\square$

Definition. Für Funktionen $\alpha, \beta : G_{p'} \to K$ setzen wir

$$(\alpha|\beta)'_G := \frac{1}{|G|} \sum_{x \in G_{p'}} \alpha(x)\beta(x^{-1}).$$

Bemerkung. Im Fall $p \nmid |G|$ ist jede Konjugationsklasse von G p-regulär. Daher ist $k := |\mathrm{Irr}(G)| = |\mathrm{IBr}(G)|$. Ferner ist FG nach Maschke halbeinfach, d.h. jeder unzerlegbare projektive FG-Modul ist einfach. Daher ist die Cartanmatrix von FG die $k \times k$-Einheitsmatrix. Wegen $D^TD = C$ ist dann auch die Zerlegungsmatrix D von RG die $k \times k$-Einheitsmatrix (bei passender Numerierung von $\mathrm{Irr}(G)$). Daher ist $\mathrm{Irr}(G) = \mathrm{IBr}(G) = \mathrm{IPr}(G)$.

40.9. Satz. *Sei φ ein Brauercharakter von G, und sei $\tilde{\varphi} : G \to K$ durch $\tilde{\varphi} := \varphi(g_{p'})$ für $g \in G$ definiert. Dann ist $\tilde{\varphi}$ ein verallgemeinerter Charakter von G; insbesondere ist jeder Brauercharakter Einschränkung eines verallgemeinerten Charakters von G.*

Beweis. Sei E eine elementare Untergruppe von G. Wir schreiben $E = P \times Q$ mit einer p-Gruppe P und einer p'-Gruppe Q. Dann ist $\mathrm{Res}^G_E(\tilde{\varphi}) = 1_P \times \mathrm{Res}^G_Q(\varphi)$. Dabei ist $\mathrm{Res}^G_Q(\varphi)$ ein Brauercharakter von Q. Wegen $p \nmid |Q|$ ist $\mathrm{Res}^G_Q(\varphi)$ nach der obigen Bemerkung auch ein gewöhnlicher Charakter von Q. Nach Brauers Charakterisierung von Charakteren ist also $\tilde{\varphi}$ ein verallgemeinerter Charakter von G. □

Bemerkung. Für $\varphi \in \mathrm{IBr}(G)$ existieren also Zahlen $m_{\varphi\chi} \in \mathbb{Z}$ mit

$$\varphi = \sum_{\chi \in \mathrm{Irr}(G)} m_{\varphi\chi} \chi | G_{p'} = \sum_{\chi \in \mathrm{Irr}(G)} \sum_{\psi \in \mathrm{IBr}(G)} m_{\varphi\chi} d_{\chi\psi} \psi.$$

Setzt man also $M := (m_{\varphi\chi})$, $D := (d_{\chi\varphi})$, so ist $MD = 1_l$. Dies bedeutet, daß die Elementarteiler von D alle gleich 1 sind.

40.10. Satz.

(i) $\mathrm{IPr}(G)$ *ist eine* $\mathbb{Z}$*-Basis für den* Z*-Modul* $X(G|G_{p'})$ *aller verallgemeinerten Charaktere von* G*, die auf* $G \setminus G_{p'}$ *verschwinden.*

(ii) *Seien* $\varphi_1, \dots, \varphi_l$ *die irreduziblen Brauercharaktere von* G*. Dann bilden die in 40.9 definierten verallgemeinerten Charaktere* $\tilde{\varphi}_1, \dots, \tilde{\varphi}_l$ *von* G *eine* R*-Basis für den* R*-Modul aller Klassenfunktionen* $\psi : G \to R$*, die konstant auf jeder* p'*-Sektion von* G *sind.*

Beweis. Seien $\chi_1, \dots, \chi_k$ die irreduziblen Charaktere, $\varphi_1, \dots, \varphi_l$ die irreduziblen Brauercharaktere, $\eta_1, \dots, \eta_l$ die entsprechenden unzerlegbaren projektiven Charaktere und $x_1, \dots, x_l$ Repräsentanten für die p-regulären Konjugationsklassen von G. Wir schreiben $\tilde{\varphi}_i = \sum_{j=1}^k m_{ij}\chi_j$ mit $m_{ij} \in \mathbb{Z}$ für $i = 1, \dots, l$, $j = 1, \dots, k$. Wir haben gesehen, daß $\eta_1, \dots, \eta_l$ eine K-Basis des K-Vektorraums aller Klassenfunktionen von G bilde, die auf $G \setminus G_{p'}$ verschwinden. Ist also ϑ ein verallgemeinerter Charakter von G, der auf $G \setminus G_{p'}$ verschwindet, so ist $\vartheta = \alpha_1\eta_1 + \ldots + \alpha_l\eta_l$ mit $\alpha_1, \ldots \alpha_l \in K$. Nach 40.8 gilt dabei für $i = 1, \dots, l$:

$$\alpha_i = (\vartheta|\varphi_i)'_G = (\vartheta|\tilde{\varphi}_i)'_G = \sum_{j=1}^k m_{ij}(\vartheta|\chi_j)_G \in \mathbb{Z}.$$

Analog bilden $\tilde{\varphi}_1, \dots, \tilde{\varphi}_l$ eine K-Basis für den K-Vektorraum aller Klassenfunktionen auf G, die auf jeder p'-Sektion von G konstant sind. Ist also $\vartheta : G \to R$ eine solche Klassenfunktion, so ist $\vartheta = \alpha_1\tilde{\varphi}_1 + \ldots + \alpha_l\tilde{\varphi}_l$ mit $\alpha_1, \dots, \alpha_l \in K$. Wegen $(\tilde{\varphi}_i|\eta_j)_G = (\varphi_i|\eta_j)'_G = \delta_{ij}$ für $i, j = 1, \dots, l$ gilt nach 40.8:

$$\alpha_j = (\vartheta|\eta_j)_G = \sum_{r=1}^l \frac{1}{|C_G(x_r)|} \vartheta(x_r)\eta_j(x_r^{-1}) \in R.$$

□

Bemerkung. Für $S \in \mathrm{Sec}_{p'}(G)$ ist also die charakteristische Funktion auf S eine R-Linearkombination von $\tilde{\varphi}_1, \dots, \tilde{\varphi}_l$.

KAPITEL 41

Brauer-Charaktere in Blöcken

Sei φ eine vollständige diskrete Bewertung eines Körpers K der Charakteristik 0 mit Bewertungsring R, Bewertungsideal $\mathrm{Rad}(R) = \pi R$ und algebraisch abgeschlossenem Restklassenkörper $F = R/\pi R$ der Charakteristik $p > 0$. Ferner sei G eine endliche Gruppe, und K enthalte die $|G|$-ten Einheitswurzeln.

41.1. Bemerkung. Wie üblich verteilen wir die Elemente in $\mathrm{IBr}(G)$ und $\mathrm{IPr}(G)$ auf Blöcke:

$$\mathrm{IBr}(G) = \dot{\bigcup_{B \in \mathrm{Bl}(RG)}} \mathrm{IBr}(B), \qquad \mathrm{IPr}(G) = \dot{\bigcup_{B \in \mathrm{Bl}(RG)}} \mathrm{IPr}(B).$$

Seien V ein KG-Modul und L eine R-Form von V. Gehört V zum Block B von RG, so gehören auch L, $L/\pi L$ und die Kompositionsfaktoren von $L/\pi L$ zu B. Bei entsprechender Numerierung von $\mathrm{Irr}(G)$ und $\mathrm{IBr}(G)$ haben also die Zerlegungsmatrix D und die Cartanmatrix C von RG eine den Blöcken $B_1, \dots, B_r$ von RG entsprechende Form:

$$D = \begin{pmatrix} D_1 & & 0 \\ & \ddots & \\ 0 & & D_r \end{pmatrix}, \qquad C = \begin{pmatrix} C_1 & & 0 \\ & \ddots & \\ 0 & & C_r \end{pmatrix}.$$

Für $i = 1, \dots, r$ nennt man D_i die *Zerlegungsmatrix* und C_i die *Cartanmatrix* von B_i. Dabei ist D_i eine $|\mathrm{Irr}(B_i)| \times |\mathrm{IBr}(B_i)|$-Matrix und C_i eine $|\mathrm{IBr}(B_i)| \times |\mathrm{IBr}(B_i)|$-Matrix mit $D_i^T D_i = C_i$. Da C_i wie C regulär ist, folgt $|\mathrm{Irr}(B_i)| \geq |\mathrm{IBr}(B_i)|$.

Satz. *Sei $B \in \mathrm{Bl}(RG)$. Es ist nicht möglich, die irreduziblen Charaktere und die irreduziblen Brauercharaktere in B so zu numerieren, daß die Cartanmatrix C von B die Form $\left(\begin{smallmatrix} C_1 & 0 \\ 0 & C_2 \end{smallmatrix}\right)$ oder die Zerlegungsmatrix D von B die Form $\left(\begin{smallmatrix} D_1 & 0 \\ 0 & D_2 \end{smallmatrix}\right)$ hat.*

Beweis. Wegen $D^T D = C$ genügt es zu zeigen, daß C nicht diese Form haben kann. Dazu nehmen wir das Gegenteil an und schreiben $1_{\overline{B}} = e_1 + \ldots + e_n$ mit paarweise orthogonalen primitiven Idempotenten $e_1, \dots, e_n$ in $\overline{B} = B/\pi B$. Die Numerierung sei dabei so gewählt, daß $e_1, \dots, e_m$ zu C_1 und $e_{m+1}, \dots, e_n$ zu C_2 gehören. Dann ist $e_i \overline{B} e_j = 0 = e_j \overline{B} e_i$ für $i = 1, \dots, m$, $j = m+1, \dots, n$. Setzt man $f := e_1 + \ldots + e_m$, so ist also $\overline{B} = f\overline{B}f \oplus (1-f)\overline{B}(1-f)$. Für $x \in \overline{B}$ ist daher $fx = fxf = xf$, d.h. $f \in Z(\overline{B})$. Da $Z(\overline{B})$ lokal ist, ist dies ein Widerspruch. $\square$

41.2. Bemerkung. Wir definieren einen Graph mit den irreduziblen Charakteren von G als Vertizes. Dabei verbinden wir $\chi, \chi' \in \mathrm{Irr}(G)$ durch eine Kante, wenn $d_{\chi\varphi} \neq 0 \neq d_{\chi'\varphi}$ für ein $\varphi \in \mathrm{IBr}(G)$ ist. Die Zusammenhangskomponenten dieses Graphen entsprechen nach 41.1 genau den Blöcken von RG.
Wir definieren einen anderen Graph mit den irreduziblen Brauercharakteren von G als Vertizes. Dabei verbinden wir $\varphi, \varphi' \in \mathrm{IBr}(G)$ durch eine Kante, wenn $d_{\chi\varphi} \neq 0 \neq d_{\chi\varphi'}$ für ein $\chi \in \mathrm{Irr}(G)$ ist. Die Zusammenhangskomponenten dieses Graphen entsprechen nach 41.1 wieder genau den Blöcken von RG.

41.3. Bemerkung. Bekanntlich ist $KG \cong \mathrm{Mat}(d_1, K) \oplus \ldots \oplus \mathrm{Mat}(d_k, K)$ mit $k = |\mathrm{Irr}(G)|$ und $d_1, \dots, d_k \in \mathbb{N}$. Die entsprechenden Abbildungen $\Delta_i : KG \to \mathrm{Mat}(d_i, K)$ sind bis auf Äquivalenz alle irreduziblen Matrixdarstellungen von KG. Wir bezeichnen mit $\chi_1, \dots, \chi_k$ die entsprechenden Charaktere. Ferner ist $ZKG = Ke_1 \oplus \ldots \oplus Ke_k$ mit paarweise orthogonalen primitiven Idempotenten in ZKG. Sei $i \in \{1, \dots, k\}$

und $e_i = \sum_{g\in G} \alpha_g g$ mit $\alpha_g \in K$ für $g \in G$. Für $j = 1, \dots, k$ gilt dann

$$\chi_i(1)\delta_{ij} = \chi_j(e_i) = \sum_{g\in G} \alpha_g \chi_j(g).$$

Für $h \in G$ gilt also

$$\begin{aligned} \chi_i(1)\chi_i(h^{-1}) &= \sum_{j=1}^{k} \delta_{ij}\chi_i(1)\chi_j(h^{-1}) = \sum_{j=1}^{k}\sum_{g\in G} \alpha_g\chi_j(g)\chi_j(h^{-1}) \\ &= \sum_{g\in G} \alpha_g \sum_{j=1}^{k} \chi_j(g)\chi_j(h^{-1}) = |G : C_G(h)|\alpha_h|C_G(h)| \\ &= |G|\alpha_h. \end{aligned}$$

Daher ist

$$e_i = \frac{\chi_i(1)}{|G|} \sum_{g\in G} \chi_i(g^{-1})g.$$

Statt e_i schreiben wir auch e_{χ_i}.

Satz (Osima). *Für $B \in \mathrm{Bl}(RG)$ ist 1_B eine R-Linearkombination p-regulärer Elemente in G.*

Beweis. Offenbar ist

$$1_B = \sum_{\chi\in\mathrm{Irr}(B)} e_\chi = \sum_{g\in G}\sum_{\chi\in\mathrm{Irr}(B)} \frac{\chi(1)}{|G|}\chi(g^{-1})g.$$

Für $g \in G \setminus G_{p'}$ gilt aber nach der zweiten Orthogonalitätsrelation für Blöcke:

$$\sum_{\chi\in\mathrm{Irr}(B)} \chi(1)\chi(g^{-1}) = 0.$$

□

41.4. Satz. *Sei $|G| = p^a r$ mit $p \nmid r$. Für $B \in \mathrm{Bl}(RG)$ existiert dann ein $\eta \in \mathrm{IPr}(B)$ mit $p^{a+1} \nmid \eta(1)$.*

Bemerkung. Wir wissen bereits, daß $p^a \mid \eta(1)$ für alle $\eta \in \mathrm{IPr}(B)$ ist.

Beweis. Wir schreiben $1_B = \sum_{g\in G_{p'}} \alpha_g g$ mit $\alpha_g \in R$ für $g \in G_{p'}$. Wie im Beweis von 41.3 gilt dann für $g \in G_{p'}$:

$$\begin{aligned} \alpha_g &= \frac{1}{|G|}\sum_{\chi\in\mathrm{Irr}(B)} \chi(1)\chi(g^{-1}) = \frac{1}{|G|}\sum_{\chi\in\mathrm{Irr}(B)}\sum_{\varphi\in\mathrm{IBr}(B)} \chi(1)d_{\chi\varphi}\varphi(g^{-1}) \\ &= \frac{1}{|G|}\sum_{\varphi\in\mathrm{IBr}(G)} \eta_\varphi(1)\varphi(g^{-1}), \end{aligned}$$

wobei η_φ den φ entsprechenden unzerlegbaren projektiven Charakter von G bezeichnet. Wegen $\overline{1_B} \neq 0$ kann nicht $p^{a+1} \mid \eta_\varphi(1)$ für alle $\varphi \in \mathrm{IBr}(B)$ sein. □

41.5. Satz. *Seien $B \in \mathrm{Bl}(RG)$, $D \in \mathrm{Def}(B)$ und $P \in \mathrm{Syl}_p(G)$ mit $D \subseteq P$. Dann existiert ein $\varphi \in \mathrm{IBr}(B)$ mit $p \nmid \frac{\varphi(1)}{|P:D|}$.*

Bemerkung. Nach 37.5 ist $\frac{\varphi(1)}{|P:D|} \in \mathbb{Z}$ für alle $\varphi \in \mathrm{IBr}(B)$. Ist $p \nmid \frac{\varphi(1)}{|P:D|}$ und M ein einfacher FG-Modul mit Brauercharakter φ, so ist $D \in \mathrm{Vtx}(M)$.

Beweis. Wir schreiben wieder $1_B = \sum_{g\in G_{p'}} \alpha_g g$ mit $\alpha_g \in R$ für $g \in G_{p'}$. Die Definition einer Defektgruppe von B zeigt, daß ein Element $g \in G_{p'}$ mit der Eigenschaft existiert, daß D eine p-Sylowgruppe von $C_G(g)$ und $\overline{\alpha_g} \neq 0$ ist. Wie im Beweis von 41.1 ist

$$\begin{aligned} R^\times \ni \alpha_g &= \frac{1}{|G|} \sum_{\chi\in\mathrm{Irr}(B)} \chi(1)\chi(g^{-1}) \\ &= \frac{1}{|G|} \sum_{\chi\in\mathrm{Irr}(B)} \sum_{\varphi\in\mathrm{IBr}(B)} d_{\chi\varphi}\varphi(1)\chi(g^{-1}) \\ &= \frac{1}{|G|} \sum_{\varphi\in\mathrm{IBr}(B)} \varphi(1)\eta_\varphi(g^{-1}) \\ &= \sum_{\varphi\in\mathrm{IBr}(B)} \underbrace{\frac{\varphi(1)}{G : C_G(g)}}_{\in R} \underbrace{\frac{\eta_\varphi(g^{-1})}{|C_G(g)|}}_{\in R}. \end{aligned}$$

Daher existiert ein $\varphi \in \mathrm{IBr}(B)$ mit $\frac{\varphi(1)}{|G:C_G(g)|} \in R^\times$, d.h. $\frac{\varphi(1)}{|P:D|} \in R^\times$. Folglich ist $p \nmid \frac{\varphi(1)}{|P:D|}$. □

41.6. Bemerkung. Für $B \in \mathrm{Bl}(RG)$ ist jedes $\varphi \in \mathrm{IBr}(B)$ eine $\mathbb{Z}$-Linearkombination der Elemente $\chi|G_{p'}$ ($\chi \in \mathrm{Irr}(B)$). Andererseits ist $\chi|G_{p'}$ für $\chi \in \mathrm{Irr}(B)$ eine $\mathbb{Z}$-Linearkombination der Elemente $\varphi \in \mathrm{IBr}(B)$. Daher ist $\mathrm{ggT}\{\chi(1) : \chi \in \mathrm{Irr}(B)\} = \mathrm{ggT}\{\varphi(1) : \varphi \in \mathrm{IBr}(B)\}$. Damit folgt aus 41.5:

Satz. *Seien $B \in \mathrm{Bl}(RG)$, $D \in \mathrm{Def}(B)$ und $P \in \mathrm{Syl}_p(G)$ mit $D \subseteq P$. Dann ist $|P : D| \mid \chi(1)$ für alle $\chi \in \mathrm{Irr}(B)$, und es existiert ein $\chi \in \mathrm{Irr}(B)$ mit $p \nmid \frac{\chi(1)}{|P:D|}$.*

41.7. Bemerkung. Sei $B \in \mathrm{Bl}(RG)$, $D \in \mathrm{Def}(B)$ und $P \in \mathrm{Syl}_p(G)$ mit $D \subseteq P$. Brauers Höhe-Null-Vermutung besagt, daß D genau dann abelsch ist, wenn $p \nmid \frac{\chi(1)}{|P:D|}$ für alle $\chi \in \mathrm{Irr}(B)$ gilt.

Satz. *Seien $B \in \mathrm{Bl}(RG)$, $D \in \mathrm{Def}(B)$, $P \in \mathrm{Syl}_p(G)$ und $\chi \in \mathrm{Irr}(B)$. Dann sind äquivalent:*
(1) $|D| = 1$.
(2) $|P| \mid \chi(1)$.
(3) $|\mathrm{Irr}(B)| = 1$.
(4) *Die Zerlegungsmatrix D_B von B ist* (1).
(5) *Die Cartanmatrix C_B von B ist* (1).
(6) $\chi(x) = 0$ *für alle* $x \in G \setminus G_{p'}$.
(7) $\chi(x) = 0$ *für alle* $x \in G_p \setminus \{1\}$.

Beweis.
(1)⇒(2): 41.6.
(2)⇒(3): Im Fall $|P| \mid \chi(1)$ ist

$$e_\chi = \frac{\chi(1)}{|G|} \sum_{x\in G} \chi(x^{-1})\chi \in RG,$$

also $1_B = e_\chi$ und daher $|\mathrm{Irr}(B)| = 1$.
(3)⇒(4): Aus $|\mathrm{Irr}(B)| = 1$ folgt $|\mathrm{IBr}(B) = 1|$ wegen $|\mathrm{IBr}(B)| \leq |\mathrm{Irr}(B)|$. Daher ist D_B eine 1×1-Matrix. Da alle Elementarteiler von D_B gleich 1 sind, folgt $D_B = (1)$.
(4)⇒(5): $C_B = D_B^T D_B$.
(5)⇒(6): Aus $C_B = 1$ folgt $D_B = 1$. Daher ist $\mathrm{IPr}(B) = \{\chi\}$, woraus (6) folgt.
(6)⇒(7): Trivial.
(7)⇒(1): Aus (7) folgt

$$\mathbb{Z} \ni (\mathrm{Res}_P^G \chi | 1_P)_P = \frac{1}{|P|} \sum_{x\in P} \chi(x) = \frac{\chi(1)}{|P|}.$$

Daher ist $e_\chi = \frac{\chi(1)}{|G|}\sum_{x\in G}\chi(x^{-1})\chi \in RG$, also $1_B = e_\chi$ und $\mathrm{Irr}(B) = \{\chi\}$. Aus 41.6 folgt dann $D = 1$.

□

41.8. Bemerkung. Seien $S \in \mathrm{Syl}_p(G)$,

$$X := \sum_{\varphi\in\mathrm{IBr}(G)} \mathbb{Z}\varphi, \qquad Y := \sum_{\varphi\in\mathrm{IBr}(G)} \mathbb{Z}(\eta_\varphi|G_{p'})$$

und C die Cartanmatrix von FG. Für $\varphi \in \mathrm{IBr}(G)$ ist dann $\eta_\varphi|G_{p'} = \sum_{\psi\in\mathrm{IBr}(G)} c_{\varphi\psi}\psi$. Sind also $a_1, \dots, a_l$ die Elementarteiler von C, so ist $X/Y \cong \mathbb{Z}/a_1\mathbb{Z} \times \ldots \times \mathbb{Z}/a_l\mathbb{Z}$ und $|X/Y| = a_1 \ldots a_l = \det(C)$.
Ist ϑ eine Abbildung von G oder $G_{p'}$ nach K, so definieren wir

$$\hat\vartheta(x) := \begin{cases} |S|\vartheta(x) & \text{für } x \in G_{p'} \\ 0 & \text{sonst} \end{cases}.$$

Satz.
(i) *Für $\vartheta \in \mathrm{Irr}(G) \cup \mathrm{IBr}(G)$ ist $\hat\vartheta$ ein verallgemeinerter Charakter.*
(ii) *Für $\vartheta \in \mathrm{IBr}(G)$ ist $|S|\vartheta \in Y$.*
(iii) *Die Elementarteiler von C sind Potenzen von p.*

Beweis.
(i) Sei E eine elementare Untergruppe von G und $E = P \times Q$ mit einer p-Gruppe P und einer p'-Gruppe Q. Dann ist $\mathrm{Res}^G_E\,\hat\vartheta = |S : P|\rho_P \times \mathrm{Res}^G_Q\,\vartheta$, wobei ρ_P den regulären Charakter von P bezeichnet. Offenbar ist $\mathrm{Res}^G_Q\,\vartheta$ ein Charakter von Q. Nach Brauers Charakterisierung ist also $\hat\vartheta$ ein verallgemeinerter Charakter von G.
(ii) Für $\vartheta \in \mathrm{IBr}(G)$ ist

$$\hat\vartheta = \sum_{\varphi\in\mathrm{IBr}(G)} m_\varphi\eta_\varphi$$

mit $m_\varphi \in \mathbb{Z}$ nach (i) und 40.10. Daher ist

$$|S|\vartheta = \hat\vartheta|G_{p'} = \sum_{\varphi\in\mathrm{IBr}(G)} m_\varphi\eta_\varphi|G_{p'} \in Y.$$

(iii) Wegen (ii) ist X/Y eine endliche p-Gruppe.

□

41.9. Satz. *Es seien $C_1, \dots, C_l$ die p-regulären Konjugationsklassen von G, und für $i = 1, \dots, l$ sei D_i eine p-Defektgruppe von C_i. Dann sind $|D_1|, \dots, |D_l|$ die Elementarteiler der Cartanmatrix C von RG.*

Beweis. Da die Elementarteiler von C Potenzen von p sind, ändern sie sich nicht, wenn man C als Matrix mit Koeffizienten aus dem Hauptidealring R auffaßt. Seien $\varphi_1, \dots, \varphi_l$ die irreduziblen Brauercharaktere von G, $\eta_1, \dots, \eta_l$ die zugehörigen unzerlegbaren projektiven Charaktere von G und $x_i \in C_i$ für $i = 1, \dots, l$. Für $i = 1, \dots, l$ gilt dann:

$$\delta_{ij}|C_G(x_i)| = \sum_{r=1}^{l} \eta_r(x_j)\varphi_r(x_i^{-1}) = \sum_{r,s=1}^{l} c_{rs}\varphi_s(x_j)\varphi_r(x_i^{-1}).$$

Dies kann man auch als Matrixgleichung schreiben:

$$\begin{pmatrix} |C_G(x_1)| & & 0 \\ & \ddots & \\ 0 & & |C_G(x_l)| \end{pmatrix} = \Phi^T C \Psi$$

mit Matrizen $\Phi, \Psi \in \mathrm{GL}(l, R)$. Wegen $|C_G(x_i)|_p = |D_i|$ folgt die Behauptung. □

KAPITEL 42

Cartanmatrizen und Blöcke

Sei φ eine vollständige diskrete Bewertung eines Körpers K der Charakteristik 0 mit Bewertungsring R, Bewertungsideal $\mathrm{Rad}(R) = \pi R$ und algebraisch abgeschlossenem Restklassenkörper $F = R/\pi R$ der Charakteristik $p > 0$. Ferner sei G eine endliche Gruppe, und K enthalte die $|G|$-ten Einheitswurzeln.

42.1. Bemerkung. Sei B ein Block von RG mit Cartanmatrix C_B,

$$X(B) := \sum_{\chi \in \mathrm{Irr}(B)} \mathbb{Z}\chi, \qquad X'(B) := \sum_{\varphi \in \mathrm{IBr}(B)} \mathbb{Z}\varphi, \qquad Y(B) := \sum_{\varphi \in \mathrm{IBr}(B)} \mathbb{Z}(\eta_\varphi | G_{p'}).$$

Dann ist $X'(B)/Y(B) \cong \mathbb{Z}/a_1\mathbb{Z} \times \ldots \times \mathbb{Z}/a_l\mathbb{Z}$, wobei $a_1, \ldots, a_l$ die Elementarteiler von C_B sind, und $|X'(B)/Y(B)| = \det(C_B)$.

Satz. *Seien $B \in \mathrm{Bl}(RG)$, $D \in \mathrm{Def}(B)$, $P \in \mathrm{Syl}_p(G)$ mit $D \subseteq P$, $\vartheta \in X(B) \cup X'(B)$, $\hat{\vartheta}$ wie in 41.8 und $\hat{\vartheta} = \sum_{\chi \in \mathrm{Irr}(B)} n_{\vartheta,\chi}\chi$ mit $n_{\vartheta,\chi} \in \mathbb{Z}$ für $\chi \in \mathrm{Irr}(G)$. Dann gilt:*

(i) $\hat{\vartheta} \in X(B)$.
(ii) *Für $\chi \in \mathrm{Irr}(B)$ ist $\frac{n_{\vartheta,\chi}}{\chi(1)} \in R$. Insbesondere ist $|P : D| \bigm| n_{\vartheta,\chi}$.*
(iii) *Für $\chi, \chi' \in \mathrm{Irr}(B)$ ist $\frac{n_{\vartheta,\chi}}{\chi(1)} \equiv \frac{n_{\vartheta,\chi'}}{\chi'(1)} \pmod{\pi R}$.*
(iv) *Ist $\vartheta \in X'(B)$, so ist $|D|\vartheta \in Y(B)$.*
(v) *Ist $\vartheta \in X'(B)$ und $e \in \mathbb{N}_0$ mit $p^e\vartheta \in Y(B)$, so ist $\frac{p^e}{|P|}\hat{\vartheta} \in X(B)$.*

Beweis.

(i) Nach 41.8 ist $\hat{\vartheta}$ ein verallgemeinerter Charakter von G. Da $\hat{\vartheta}$ auf $G \setminus G_{p'}$ verschwindet, existieren Zahlen $m_\varphi \in \mathbb{Z}$ mit $\hat{\vartheta} = \sum_{\varphi \in \mathrm{IBr}(G)} m_\varphi \eta_\varphi$. Für $\varphi \in \mathrm{IBr}(G) \setminus \mathrm{IBr}(B)$ ist

$$m_\varphi = (\hat{\vartheta}|\varphi)'_G = (|P|\vartheta \,|\, \varphi)'_G = 0,$$

da $\vartheta|G_{p'}$ eine $\mathbb{Q}$-Linearkombination der Elemente $\psi|G_{p'}$ mit $\psi \in \mathrm{IBr}(B)$ ist.

(ii) Seien $x_1, \ldots, x_l$ Repräsentanten für die p-regulären Konjugationsklassen $C_1, \ldots, C_l$ von G. Für jedes $\chi \in \mathrm{Irr}(B)$ ist dann

$$\begin{aligned} n_{\vartheta,\chi} &= (\chi|\hat{\vartheta})_G = (\chi \,|\, |P|\vartheta)'_G = \frac{1}{|G:P|} \sum_{x \in G_{p'}} \chi(x)\vartheta(x^{-1}) \\ &= \frac{1}{|G:P|} \sum_{i=1}^{l} |C_i|\chi(x_i)\vartheta(x_i^{-1}) = \frac{\chi(1)}{|G:P|} \sum_{i=1}^{l} \omega_\chi(C_i^+)\vartheta(x_i^{-1}). \end{aligned}$$

Also ist $\frac{n_{\vartheta,\chi}}{\chi(1)} \in R$. Wegen $|P : D| \bigm| \chi(1)$ folgt $|P : D| \bigm| n_{\vartheta,\chi}$.

(iii) Für $\chi, \chi' \in \mathrm{Irr}(B)$ ist

$$\begin{aligned} \frac{n_{\vartheta,\chi}}{\chi(1)} &= \frac{1}{|G:P|} \sum_{i=1}^{l} \omega_\chi(C_i^+)\vartheta(x_i^{-1}) \equiv \frac{1}{|G:P|} \sum_{i=1}^{l} \omega_{\chi'}(C_i^+)\vartheta(x_i^{-1}) \\ &= \frac{n_{\vartheta,\chi'}}{\chi'(1)} \pmod{\pi R}. \end{aligned}$$

(iv) Nach (ii) ist $\frac{1}{|P:D|}\hat{\vartheta}$ ein verallgemeinerter Charakter von G, der auf $G \setminus G_{p'}$ verschwindet. Daher ist

$$\frac{1}{|P:D|}\,\hat{\vartheta} = \sum_{\varphi \in \mathrm{IBr}(B)} l_\varphi \eta_\varphi$$

mit $l_\varphi \in \mathbb{Z}$ für $\varphi \in \mathrm{IBr}(B)$. Folglich ist $|D|\vartheta = \frac{1}{|P:D|}\hat{\vartheta}|G_{p'} \in Y(B)$.

(v) Sei $\vartheta \in X'(B)$ und $e \in \mathbb{N}_0$ mit $p^e\vartheta \in Y(B)$. Dann ist

$$\frac{p^e}{|P|}\,\hat{\vartheta}|G_{p'} = p^e\vartheta = \sum_{\varphi \in \mathrm{IBr}(B)} a_\varphi(\eta_\varphi|G_{p'})$$

mit $a_\varphi \in \mathbb{Z}$ für $\varphi \in \mathrm{IBr}(B)$. Daher ist $\frac{p^e}{|P|}\hat{\vartheta} = \sum_{\varphi \in \mathrm{IBr}(B)} a_\varphi \eta_\varphi \in X(B)$.

$\square$

42.2. Bemerkung. Seien $B \in \mathrm{Bl}(RG)$, $D \in \mathrm{Def}(B)$ und $P \in \mathrm{Syl}_p(G)$ mit $D \subseteq P$. Für $\vartheta \in X(B) \cup X'(B)$ ist

$$\dot{\vartheta} := \frac{1}{|P:D|}\,\hat{\vartheta}.$$

Nach 42.1 ist $\dot{\vartheta} \in X(B)$. Daher ist $\dot{\vartheta} = \sum_{\chi \in \mathrm{Irr}(B)} a_{\vartheta,\chi}\chi$ mit $a_{\vartheta,\chi} \in \mathbb{Z}$ für $\chi \in \mathrm{Irr}(B)$ und

$$\dot{\vartheta}(x) = \begin{cases} |D|\vartheta(x) & \text{für } x \in G_{p'} \\ 0 & \text{sonst} \end{cases}.$$

In der Notation von 42.1 ist also $a_{\vartheta,\chi} = \frac{n_{\vartheta,\chi}}{|P:D|}$ für $\chi \in \mathrm{Irr}(G)$.

Satz. *Im Fall* $p \nmid \frac{\vartheta(1)}{|P:D|}$ *gilt:*

(i) *Ist* $\chi_0 \in \mathrm{Irr}(B)$ *mit* $p \nmid \frac{\chi_0(1)}{|P:D|}$, *so ist* $p \nmid a_{\vartheta,\chi_0}$.

(ii) *Für alle* $\chi \in \mathrm{Irr}(B)$ *ist* $a_{\vartheta,\chi} \neq 0$.

Beweis.

(i) Wir nehmen an, daß ein $\chi_0 \in \mathrm{Irr}(B)$ existiert mit $p \nmid \frac{\chi_0(1)}{|P:D|}$, aber $p \mid a_{\vartheta,\chi_0}$. Dann ist $\frac{n_{\vartheta,\chi_0}}{\chi_0(1)} \in \pi R$. Für jeden irreduziblen Charakter $\chi \in \mathrm{Irr}(B)$ ist also $\frac{n_{\vartheta,\chi}}{\chi(1)} \in \pi R$ nach 42.1(iii). Daher gilt $a_{\vartheta,\chi} \in \pi R$, also $p \mid a_{\vartheta,\chi}$ für $\chi \in \mathrm{Irr}(B)$. Folglich ist $\frac{1}{p}\dot{\vartheta} \in X(B)$ und damit $\frac{1}{p}\dot{\vartheta} = \sum_{\varphi \in \mathrm{IBr}(B)} m_\varphi \eta_\varphi$ mit $m_\varphi \in \mathbb{Z}$ für $\varphi \in \mathrm{IBr}(B)$. Wegen $|P| \mid \eta_\varphi(1)$ für $\varphi \in \mathrm{IBr}(B)$ gilt $p \cdot |P:D| \mid \vartheta(1)$. Widerspruch.

(ii) Wir nehmen an, daß für ein $\chi \in \mathrm{Irr}(B)$ $a_{\vartheta,\chi} = 0$ gilt. Dann ist $n_{\vartheta,\chi} = 0$. Aus 42.1(iii) folgt $\frac{n_{\vartheta,\chi_0}}{\chi_0(1)} \in \pi R$, also $a_{\vartheta,\chi_0} \in \pi R$ im Widerspruch zu (i).

$\square$

42.3. Satz. *Seien* $B \in \mathrm{Bl}(RG)$, $D \in \mathrm{Def}(B)$ *und* C *die Cartanmatrix von* B. *Dann ist* $|D|$ *der größte Elementarteiler von* C, *und er tritt mit Vielfachheit 1 auf.*

Beweis. Wir verwenden die Notation von 42.1 und 42.2. Nach 42.1(iv) sind die Elementarteiler von C Teiler von $|D|$. Sei $\varphi \in \mathrm{IBr}(B)$ mit $p \nmid \frac{\varphi(1)}{|P:D|}$, und sei $\chi_0 \in \mathrm{Irr}(B)$ mit $p \nmid \frac{\chi_0(1)}{|P:D|}$. Nach 42.2 ist dann $p \nmid a_{\vartheta,\chi_0}$. Daher ist $\frac{|D|}{p|P|}\hat{\varphi} = \frac{1}{p}\dot{\varphi} \notin X(B)$. Nach 42.1(v) ist also $\frac{|D|}{p}\varphi \notin Y(B)$. Folglich hat das Element $\varphi + Y(B)$ in $X'(B)/Y(B)$ die Ordnung $|D|$. Dies zeigt, daß $|D|$ Elementarteiler von C ist.
Seien $\chi_1, \ldots, \chi_k$ die irreduziblen Charaktere, $\varphi_1, \ldots, \varphi_l$ die irreduziblen Brauercharaktere und $\eta_1, \ldots, \eta_l$ die entsprechenden unzerlegbaren projektiven Charaktere in B. Dann existieren Zahlen $l_{ij} \in \mathbb{Z}$ mit

$$|D|\varphi_i = \sum_{j=1}^{l} l_{ij}(\eta_j|G_{p'}) = \sum_{j=1}^{l}\sum_{j=1}^{l} l_{ij}c_{jr}\varphi_r$$

für $i = 1, \dots, l$. Setzt man $L := (l_{ij})$, so gilt also $LC = |D|\, 1_l$. Wir setzen $a_{ij} := a_{\varphi_i, \chi_j}$ für $i = 1, \dots, l$, $j = 1, \dots, k$- Dann ist $\dot{\varphi_i} = \sum_{j=1}^{k} a_{ij}\chi_j$ und $\tilde{\varphi_i} = \sum_j m_{ij}\chi_j m_{ij}\chi_j$ mit $m_{ij} \in \mathbb{Z}$ für $i = 1, \dots, l$. Folglich ist

$$l_{ij} = (|D|\varphi_i \,|\, \varphi_j)'_G = (\dot{\varphi_i}|\tilde{\varphi_j})_G = \sum_{r=1}^{k} a_{ir} m_{jr}$$

für $i, j = 1, \dots, l$. Setzt man $A := (a_{ij})$ und $M := (m_{ij})$, so gilt also $|D|C^{-1} = L = AM^T$. Wir werden zeigen, daß 1 genau einmal als Elementarteiler von $|D|C^{-1}$ auftritt. Dazu genügt zu zeigen, daß $\overline{|D|C^{-1}}$ Rang 1 hat. Aus 42.1(iii) folgt, daß die Matrix $\overline{A}$ mit Koeffizienten in $Z/p\mathbb{Z}$ Rang 1 hat. Daher hat auch $\overline{|D|C^{-1}}$ höchstens Rang 1, und wir sind fertig. $\square$

42.4. Satz. *Seien $B \in \mathrm{Bl}(RG)$ und $1 \neq D \in \mathrm{Def}(B)$. Dann ist $|\,\mathrm{IBr}(B)| < |\,\mathrm{Irr}(B)|$.*

Beweis. Im Fall $|\,\mathrm{IBr}(B)| = |\,\mathrm{Irr}(B)|$ ist die Zerlegungsmatrix D_B von B quadratisch. Da alle Elementarteiler von D_B gleich 1 sind, ist $D_B \in \mathrm{GL}(l, \mathbb{Z})$, also auch $C_B = D_B^T D_B \in \mathrm{GL}(l, \mathbb{Z})$. Daher sind alle Elementarteiler von C_B gleich 1. Nach 42.3 ist also $|D| = 1$. $\square$

42.5. Satz (Brauer-Feit)**.** *Seien $B \in \mathrm{Bl}(RG)$, $D \in \mathrm{Def}(B)$. Dann ist $|\,\mathrm{Irr}(B)| \leq \frac{1}{4}|D|^2 + 1$.*

Beweis. Seien $P \in \mathrm{Syl}_p(G)$ mit $D \subseteq P$, $\chi_0 \in \mathrm{Irr}(B)$ mit $p \not| \frac{\chi_0(1)}{|P:D|}$ und $\dot{\chi_0} = \sum_{\chi \in \mathrm{Irr}(B)} a_\chi \chi$ mit $a_\chi \in \mathbb{Z}$ für $\chi \in \mathrm{Irr}(B)$. Nach 42.2 ist $a_\chi \neq 0$ für $\chi \in \mathrm{Irr}(B)$. Daher ist

$$\begin{aligned} |\,\mathrm{Irr}(B)| - 1 + a_{\chi_0}^2 \quad &\leq \sum_{\chi \in \mathrm{Irr}(B)} a_\chi^2 \;=\; (\dot{\chi_0}|\dot{\chi_0})_G \\ &= \;|D|(\dot{\chi_0}|\chi_0)_G \;=\; |D|a_{\chi_0}. \end{aligned}$$

Folglich ist $|\,\mathrm{Irr}(B)| \leq -a_{\chi_0}^2 + |D|a_{\chi_0} + 1$. Die Funktion $f : \mathbb{R} \to \mathbb{R}$, $t \mapsto -t^2 + |D|t + 1$ nimmt ihr Maximum bei $t = \frac{|D|}{2}$ an, und diese Maximum ist genau $\frac{1}{4}|D|^2 + 1$. $\square$

Bemerkung. R. Brauer vermutete, daß stets $|\,\mathrm{Irr}(B)| \leq |D|$ gilt. Dies wurde für Gruppen ungerader Ordnung durch Knörr und Gluck bewiesen.

Beispiel. Sei $|D| = 2$ (und $p = 2$). Der obige Satz liefert $|\,\mathrm{Irr}(B)| \leq 2$. Wegen $D \neq 1$ ist also $|\,\mathrm{Irr}(B)| = 2$, und nach 42.4 ist $|\,\mathrm{IBr}(B)| = 1$. Daher ist die Cartanmatrix C_B von B eine 1×1-Matrix, und nach 42.3 ist $C_B = (2)$. Folglich hat die Zerlegungsmatrix D_B von B die Form $D_B = \binom{1}{1}$. Insbesondere haben die beiden irreduziblen Charaktere in B den gleichen Grad.

42.6. Satz. *Seien $B \in \mathrm{Bl}(RG)$ mit $|\,\mathrm{IBr}(B)| = 1$ und $D \in \mathrm{Def}(B)$. Dann ist $|\,\mathrm{Irr}(B)| \leq |D|$.*

Beweis. Die Cartanmatrix C von B hat nach 42.3 die Form $C = \big(|D|\big)$. Für die Zerlegungszahlen $d_{\chi\psi}$ gilt also:

$$|D| = \sum_{\chi \in \mathrm{Irr}(B)} d_{\chi\varphi}^2 \geq |\,\mathrm{Irr}(B)|.$$

$\square$

42.7. Satz. *Seien $B \in \mathrm{Bl}(RG)$, $D \in \mathrm{Def}(B)$, $\mathrm{Irr}(B) = \{\chi_1, \dots, \chi_k\}$, $\dot{\chi_i} = \sum_{j=1}^{k} a_{ij}\chi_j$ mit $a_{ij} \in \mathbb{Z}$ für $i, j = 1, \dots, k$, $A =: (a_{ij})$, $D_B = (d_{ij})$ die Zerlegungsmatrix und $C_B = (c_{ij})$ die Cartanmatrix von B. Dann gilt:*

(i) $A = |D|D_B C_B^{-1} D_B^T$; *insbesondere ist A symmetrisch.*
(ii) $A^2 = |D|A$.
(iii) $\mathrm{spur}(A) = |D| \cdot |\,\mathrm{IBr}(B)|$.

Beweis.

(i) Wir schreiben $\mathrm{IBr}(B) = \{\varphi_1, \ldots, \varphi_l\}$ und $C_B^{-1} = (\gamma_{ij})$. Für $i, j = 1, \ldots, k$ gilt dann:

$$\begin{aligned} a_{ij} &= (\dot{\chi}_i|\chi_j)_G = |D|(\chi_i|\chi_j)'_G = |D| \sum_{r,s=1}^{l} d_{ir} d_{js} (\varphi_r|\varphi_s)'_G \\ &= |D| \sum_{r,s,t=1}^{l} d_{ir}\gamma_{rt} d_{js} (\eta_t|\varphi_s)'_G = |D| \sum_{r,s=1}^{l} d_{ir}\gamma_{rs} d_{js}. \end{aligned}$$

(ii) $A^2 = |D|^2 \cdot D_B C_B^{-1} \underbrace{D_B^T D_B}_{=C_B} C_B^{-1} D_B^T = |D|A.$

(iii) $\mathrm{spur}(A) = |D| \,\mathrm{spur}(D_B C_B^{-1} D_B^T) = |D| \,\mathrm{spur}(D_B^T D_B C_B^{-1}) = |D| \,\mathrm{spur}(1_l) = |D| \cdot |\mathrm{IBr}(B)|.$

□

42.8. Bemerkung. Seien $B \in \mathrm{Bl}(RG)$, $D \in \mathrm{Def}(B)$ und $P \in \mathrm{Syl}_p(G)$ mit $D \subseteq P$. Für $\chi \in \mathrm{Irr}(B)$ ist dann $|P : D| \mid \chi(1)$. Daher existiert eine Zahl $\mathrm{ht}(\chi) \in \mathbb{N}_0$ mit $|P : D|\, p^{\mathrm{ht}(\chi)} \mid \chi(1)$, aber $|P : D|\, p^{\mathrm{ht}(\chi)+1} \nmid \chi(1)$. Wir nennen $\mathrm{ht}(\chi)$ die *Höhe*. Es gilt also: $\mathrm{ht}(\chi) = 0 \iff p \nmid \frac{\chi(1)}{|P:D|}$. Daher enthält jeder Block irreduzible Charaktere der Höhe 0.

Satz. *Seien $B \in \mathrm{Bl}(RG)$, $1 \neq D \in \mathrm{Def}(B)$ und $\dot{\chi} = \sum_{\chi' \in \mathrm{Irr}(B)} a_{\chi\chi'} \chi'$ mit $a_{\chi\chi'} \in \mathbb{Z}$ für $\chi, \chi' \in \mathrm{Irr}(B)$. Dann gilt:*

(i) *Für $\chi, \chi' \in \mathrm{Irr}(B)$ ist $|a_{\chi\chi'}| < |D|$.*
(ii) *Für $\chi \in \mathrm{Irr}(B)$ ist $a_{\chi\chi} > 0$.*
(iii) *Im Fall $\mathrm{ht}(\chi) = 0$ ist $\frac{a_{\chi\chi'}}{p^{\mathrm{ht}(\chi')}} \in R^\times$.*
(iv) *Im Fall $\mathrm{ht}(\chi) > 0$ ist $\frac{a_{\chi\chi'}}{p^{\mathrm{ht}(\chi')}} \in \pi R$.*

Beweis.

(i) Für $\chi \in \mathrm{Irr}(B)$ gilt wegen $D \neq 1$ und 41.7:

$$a_{\chi\chi} = (\dot{\chi}|\chi)_G = |D|(\chi|\chi)'_G = \frac{|D|}{|G|} \sum_{x \in G_{p'}} |\chi(x)|^2 < \frac{|D|}{|G|} \sum_{x \in G} |\chi(x)|^2 = |D|.$$

Daher ist $|D|^2 > |D| a_{\chi\chi} = \sum_{\chi' \in \mathrm{Irr}(B)} a_{\chi\chi'}^2$, also $|a_{\chi\chi'}| < |D|$ für alle $\chi' \in \mathrm{Irr}(B)$.

(ii) Analog gilt für $\chi \in \mathrm{Irr}(B)$:

$$a_{\chi\chi} \geq \frac{|D|}{|G|} |\chi(1)|^2 > 0.$$

(iii) Nach 42.1 ist stets $\frac{a_{\chi\chi'}}{p^{\mathrm{ht}(\chi')}} \in R$. Im Fall $\frac{a_{\chi\chi'}}{p^{\mathrm{ht}(\chi')}} \in \pi R$ wäre auch $\frac{a_{\chi\chi}}{p^{\mathrm{ht}(\chi)}} \in \pi R$ nach 42.1(iii), was 42.2(i) widerspricht.

(iv) Sei $\mathrm{ht}(\chi) > 0$. Im Fall $\mathrm{ht}(\chi') = 0$ ist dann $a_{\chi\chi'} = a_{\chi'\chi} \in p^{\mathrm{ht}(\chi)} R \subseteq \pi R$ nach (iii). Daher folgt die Behauptung aus 42.1(iii).

□

42.9. Satz. *Seien $B \in \mathrm{Bl}(RG)$, $D \in \mathrm{Def}(B)$, $|D| = p^d$ und $\chi \in \mathrm{Irr}(B)$. Dann gilt:*

(i) *Im Fall $d \leq 2$ ist $\mathrm{ht}(\chi) = 0$.*
(ii) *Im Fall $d \geq 2$ ist $\mathrm{ht}(\chi) \leq d - 2$.*

Beweis. Sei $\mathrm{ht}(\chi) > 0$. Nach 42.8 ist dann $p^{\mathrm{ht}(\chi)+1} \mid a_{\chi\chi} < |D|$, also $\mathrm{ht}(\chi) + 1 < d$. □

Bemerkung. Für irreduzible Charaktere χ, χ' in verschiedenen Blöcken von RG ist offenbar $(\chi|\chi')'_G = 0$. Für irreduzible Charaktere χ, χ' im gleichen Block B von RG ist $|D|(\chi|\chi')'_G = a_{\chi\chi'} \neq 0$ nach 42.8(iii), falls χ oder χ' die Höhe 0 hat. Definiert man also einen Graphen mit den irreduziblen Charakteren von G als Ecken und verbindet man $\chi, \chi' \in \mathrm{Irr}(G)$ durch eine Kante, falls $(\chi|\chi')'_G \neq 0$ ist, so entsprechen die Zusammenhangskomponenten dieses Graphen genau den Blöcken von RG. Die Einteilung der irreduziblen

Charaktere von G in Blöcke hängt also nur von der Primzahl p, nicht aber von dem Bewertungsring R ab.

42.10. Bemerkung. Für $B \in \mathrm{Bl}(RG)$ und $i \in \mathbb{N}_0$ bezeichnen wir mit $k_i(B)$ die Anzahl der irreduziblen Charaktere der Höhe i in B.

Satz. *Seien $B \in \mathrm{Bl}(RG)$, $1 \neq D \in \mathrm{Def}(B)$ und $|D| = p^d$. Dann gilt:*

(i) $k_0(B) \geq 2$.
(ii) *Im Fall $p = 3$ ist $3 \mid k_0(B)$.*
(iii) *Im Fall $p = 2$ und $|D| \geq 4$ ist $4 \mid k_0(B)$.*
(iv) *Ist $p = 2$ und enthält $\mathrm{Irr}(B)$ einen irreduziblen Charakter der Höhe $d - 2 > 0$, so ist $k_0(B) = 4$ und $k_{d-2}(B) \leq 3$.*

Beweis. Sei $\mathrm{Irr}(B) = \{\chi_1, \ldots, \chi_k\}$ und $\dot{\chi}_i = \sum_{j=1}^k a_{ij}\chi_j$ mit $a_{ij} \in \mathbb{Z}$ für $i, j = 1, \ldots, k$. Für $i = 1, \ldots, k$ ist dann

$$\sum_{j=1}^{k} a_{ij}^2 = |D| a_{ii} \equiv 0 \pmod{|D|}.$$

Sei $\mathrm{ht}(\chi_i) = 0$. Im Fall $\mathrm{ht}(\chi_j) > 0$ ist dann $p \mid a_{ij}$, und im Fall $\mathrm{ht}(\chi_j) = 0$ ist $p \nmid a_{ij}$. Daher ist

$$\sum_{\substack{j=1 \\ \mathrm{ht}(\chi_j)=0}}^{k} a_{ij}^2 \equiv 0 \pmod{p}$$

und $k_0(B) \geq 2$.
Im Fall $p = 3$ ist 1 das einzige von 0 verschiedene Quadrat modulo p. Daher ist

$$k_0(B) \equiv \sum_{\substack{j=1 \\ \mathrm{ht}(\chi_j)=0}}^{k} a_{ij}^2 \equiv 0 \pmod{p}.$$

Im Fall $p = 2$ und $|D| \geq 4$ ist analog 1 das einzige von 0 verschiedene Quadrat modulo 4. Daher ist

$$k_0(B) \equiv \sum_{\substack{j=1 \\ \mathrm{ht}(\chi_j)=0}}^{k} a_{ij}^2 \equiv |D| a_{ii} \equiv 0 \pmod{4}.$$

Sei jetzt $p = 2$ und $\mathrm{ht}(\chi_k) = d - 2 > 0$. Nach (iii) enthält $\mathrm{Irr}(B)$ irreduzible Charaktere $\chi_1, \chi_2, \chi_3, \chi_4$ der Höhe 0. Für $i = 1, 2, 3, 4$ ist $2^{d-2} \mid a_{ki} \neq 0$, also

$$2^{2d-2} = 4(2^{d-2})^2 \sum_{i=1}^{k} a_{ki}^2 \leq \sum_{i=1}^{k-1} a_{ki}^2 = 2^d a_{kk} - a_{kk}^2 \leq 2^{2d-2};$$

denn die Funktion $f : \mathbb{R} \to \mathbb{R}$, $t \mapsto 2^d t - t^2$ nimmt ihr Maximum 2^{2d-2} bei $t = 2^{d-1}$ an. Für $i = 5, \ldots, k-1$ ist also $a_{ki} = 0$ und daher $\mathrm{ht}(a_{ki}) \neq 0$. Analog ist

$$2^{2d-2} \geq 2^d a_{11} - a_{11}^2 = \sum_{i=2}^{k} a_{1i}^2 \geq 3 + k_{d-2}(B) 2^{2d-4},$$

also $k_{d-2}(B) \leq 3$. $\square$

Beispiel.

(i) Sei $|D| = 3$ (und $p = 3$). Nach 42.9 haben alle irreduziblen Charaktere in B die Höhe 0. Nach 42.5 ist $|\mathrm{Irr}(B)| \leq \frac{1}{4}9 + 1$, also $|\mathrm{Irr}(B)| \leq 3$. Aus Teil (ii) des obigen Satzes folgt also $|\mathrm{Irr}(B)| = 3$.

(ii) Sei $|D| = 4$ (und $p = 2$). Nach 42.9 haben alle irreduziblen Charaktere in B die Höhe 0. Nach 42.8 gilt für alle $\chi, \chi' \in \mathrm{Irr}(B)$: $0 < |a_{\chi\chi'}| < 4$. Andererseits ist $a_{\chi\chi'}$ ungerade, also $|a_{\chi\chi'}| \in \{1, 3\}$. Im Fall $a_{\chi\chi} = 3$ ist

$$|\operatorname{Irr}(B)| - 1 \leq \sum_{\chi \in \operatorname{Irr}(B) \setminus \{\chi\}} a_{\chi\chi'}^2 = 4a_{\chi\chi} - a_{\chi\chi}^2 = 12 - 9 = 3,$$

und im Fall $a_{\chi\chi} = 1$ ist analog

$$|\operatorname{Irr}(B)| - 1 \leq \sum_{\chi \in \operatorname{Irr}(B) \setminus \{\chi\}} a_{\chi\chi'}^2 = 4a_{\chi\chi} - a_{\chi\chi}^2 = 4 - 1 = 3,$$

Daher ist in jedem Fall $|\operatorname{Irr}(B)| \leq 4$. Aus Teil (iii) des obigen Satzes folgt also $|\operatorname{Irr}(B)| = 4$.

42.11. Satz. *Seien $B \in \mathrm{Bl}(RG)$, $D \in \mathrm{Def}(B)$, $b \in \mathrm{Bl}(RDC_G(D))$ mit $\mathrm{Br}_D(\overline{1_B})\overline{1_b} \neq 0$ und $N_G(D, b) := \{g \in N_G(D) : gbg^{-1} = b\}$. Ist $|\mathrm{IBr}(B)| = 1$ und $|\mathrm{Irr}(B)| = |D|$, so gilt:*

(i) *D ist abelsch.*
(ii) *$N_G(D, b) = C_G(D)$.*
(iii) *$\overline{B} \cong \mathrm{Mat}(n, FD)$ für ein $n \in \mathbb{N}$.*

Bemerkung. Es ist auch $B \cong \mathrm{Mat}(n, RD)$, aber das ist schwieriger zu beweisen.

Beweis. Wegen $|\mathrm{IBr}(B)| = 1$ besitzt $\overline{B}$ bis auf Isomorphie genau einen einfachen Modul, also auch genau einen unzerlegbaren projektiven Modul P. Als $\overline{B}$-Modul ist $\overline{B} \simeq P^n$ für ein $n \in \mathbb{N}$. Als Algebra ist dann $\overline{B} \cong \mathrm{End}_{\overline{B}}(\overline{B})^o \cong \mathrm{End}_{\overline{B}}(p^n)^o \cong \mathrm{Mat}(n, \mathrm{End}_{\overline{B}}(P))^o$. Dabei ist $E := \mathrm{End}_{\overline{B}}(P)$ eine lokale F-Algebra, und die Dimension von E ist die einzige Cartaninvariante von $\overline{B}$. Also ist $\dim_F E = |D|$. Andererseits ist $K \otimes_R B \cong \mathrm{Mat}(d_1, K) \oplus \ldots \oplus \mathrm{Mat}(d_k, K)$ und

$$|D| = |\operatorname{Irr}(B)| = k = \dim_K Z(K \otimes_R B) = \dim_F Z\overline{B} = \dim_F ZE \leq \dim_F E = |D|.$$

Daher ist E kommutativ und $E \cong Z\overline{B}$. Wegen $E \cong e\overline{B}e$ für ein Idempotent e in $\overline{B}$ ist E symmetrisch, also auch $Z\overline{B}$. Als lokale F-Algebra besitzt daher $Z\overline{B}$ genau ein minimales Ideal, nämlich den Annullator des Radikals, und dieses minimale Ideal hat Dimension 1. Bekanntlich ist das Element $\overline{1_B}G_p^+$ von 0 verschieden und annulliert das Radikal. Daher wird das minimale Ideal in $Z\overline{B}$ von $\overline{1_B}G_p^+$ aufgespannt; insbesondere liegt $\overline{1_B}G_p^+$ in jedem von 0 verschiedenen Ideal von $Z\overline{B}$. Schreibt man $\overline{1_B}G_p^+ = \sum_{g \in G} \alpha_g g$ mit $\alpha_g \in F$ für $g \in G$, so ist bekanntlich $\overline{1_B} = \sum_{g \in G_{p'}} \alpha_g g$. Wegen $\overline{1_B} \notin I_{<D}(FG)$ ist also $\overline{1_B}G_p^+ \notin I< D(FG)\overline{1_B}$. Daher verschwindet $I_{<D}(FG)\overline{1_B}$ in $ZFG\overline{1_B} = Z\overline{B}$. Folglich ist

$$Z\overline{B} = I_D(FG)\overline{1_B} \cong I_D(FG)\overline{1_B}/I_{<D}(FG)\overline{1_B}.$$

Bekanntlich bilden die Restklassen der Klassensummen der Konjugationsklassen von G mit p-Defektgruppe D eine Basis von $I_D(FG)/I_{<D}(FG)$, und der Brauerhomomorphismus Br_D induziert einen Isomorphismus $I_D(FG)/I_{<D}(FG) \to I_D(FN_G(D))/I_{<D}(FN_G(D))$. Daher ist

$$Z\overline{B} \cong I_D(FN_G(D))\,\mathrm{Br}_D(\overline{1_B}) \;/\; I_{<D}(FN_G(D))\,\mathrm{Br}_D(\overline{1_B});$$

dabei ist $\mathrm{Br}_D(\overline{1_B})$ das Blockidempotent des Brauerkorrespondenten von $\overline{B}$ in $FN_G(D)$. Dies ist ein Block in $FN_G(D)$ mit Defektgruppe D.
Konjugationsklassen in $N_G(D)$ mit Defektgruppe D liegen bekanntlich in $C_G(D)$. Daher ist

$$I_D(FN_G(D)) = FC_G(D)^{N_G(D)} \oplus I_{<D}(FN_G(D));$$

insbesondere hat man einen Isomorphismus $Z\overline{B} \to FC_G(D)^{N_G(D)}\,\mathrm{Br}_D(\overline{1_B})$. Wir in der Darstellungstheorie II gezeigt, liefert die Multiplikation mit $\overline{1_b}$ einen Isomorphismus $ZFN_G(D)\,\mathrm{Br}_D(\overline{1_B}) \to ZFN_G(D, b)\overline{1_b}$. Auf diese Weise erhält man einen Monomorphismus $Z\overline{B} \to FC_G(D)^{N_G(D,b)}\overline{1_b}$. Wie in der Darstellungstheorie II gezeigt, ist D auch Defektgruppe von b, und wir haben $\overline{b} \cong \mathrm{Mat}(m, FD)$ für ein $m \in \mathbb{N}$. Daher ist $Z\overline{b} \cong ZFD$. Genauer ist die Abbildung $ZFD \to Z\overline{b}$, $z \mapsto z\overline{1_b}$ ein solcher Isomorphismus. Daher ist

$$FC_G(D)^{N_G(D,b)}\overline{1_b} = (Z\overline{b})^{N_G(D,b)} = (ZFG\overline{1_b})^{N_G(D,b)} \cong (ZFD)^{N_G(D,b)}.$$

Insbesondere ist

$$|D| = \dim E = \dim Z\overline{B} \leq \dim FC_G(D)^{N_G(D,b)}\overline{1_b} \leq \dim(ZFG)^{N_G(D,b)} \leq |D|.$$

Daraus folgt, daß D abelsch und $N_G(D,b) = C_G(D)$ ist. Ferner zeigt der Beweis, daß $Z\overline{B} \cong FD$ ist. Daher ist

$$\overline{B} \cong \mathrm{Mat}(n, E) = \mathrm{Mat}(n, Z\overline{B}) \cong \mathrm{Mat}(n, FD).$$

□

KAPITEL 43

Verallgemeinerte Zerlegungszahlen

Sei φ eine vollständige diskrete Bewertung eines Körpers K der Charakteristik 0 mit Bewertungsring R, Bewertungsideal $\mathrm{Rad}(R) = \pi R$ und algebraisch abgeschlossenem Restklassenkörper $F = R/\pi R$ der Charakteristik $p > 0$. Ferner sei G eine endliche Gruppe, und K enthalte die $|G|$-ten Einheitswurzeln.

43.1. Bemerkung. Zerlegungszahlen, wie wir sie bisher kennen, dienen zur Beschreibung der Werte eines Charakters $\chi \in \mathrm{Irr}(G)$ auf p-regulären Elementen. Wir werden jetzt höhere Zerlegungszahlen einführen, die die Werte von χ auf einer beliebigen p-Sektion beschreiben.
Sei also $u \in G_p$ fest. Dann ist jedes Element in der p-Sektion von u zu einem Element der Form us mit $s \in C_G(u)_{p'}$ in G konjugiert. Daher bestimmen die Werte von χ auf solchen Elementen us die Werte von χ auf der gesamten p-Sektion von u.
Sei jetzt $\chi \in \mathrm{Irr}(G)$, $H := C_G(u)$ und $\mathrm{Res}_H^G(\chi) = \sum_{\psi \in \mathrm{Irr}(H)} a_{\chi\psi}\psi$ mit $a_{\chi\psi} \in \mathbb{N}_0$ für $\psi \in \mathrm{Irr}(H)$. Wegen $u \in Z(H)$ wird u bei jeder irreduziblen Darstellung von H auf eine Skalarmatrix abgebildet. Für $\psi \in \mathrm{Irr}(H)$ existiert daher eine $|\langle u\rangle|$-te Einheitswurzel ζ_ψ mit $\psi(us) = \zeta_\psi\psi(s)$ für $s \in H_{p'}$. Ferner ist $\psi|H_{p'} = \sum_{\mu \in \mathrm{IBr}(H)} d_{\psi\mu}\mu$, wobei $d_{\psi\mu}$ die entsprechende Zerlegungszahl von RH bezeichnet. Für $s \in H_{p'}$ ist also

$$\chi(us) = \sum_{\mu \in \mathrm{IBr}(H)} \Bigg(\sum_{\psi \in \mathrm{Irr}(H)} a_{\chi\psi}\zeta_\psi d_{\psi\mu} \Bigg) \mu(s).$$

Wir nennen

$$d^u_{\chi\mu} := \sum_{\psi \in \mathrm{Irr}(H)} a_{\chi\psi}\zeta_\psi d_{\psi\mu}$$

die durch u, χ und μ bestimmte *höhere* oder *verallgemeinerte Zerlegungszahl.* Da die Elemente in $\mathrm{IBr}(H)$ linear unabhängig über K sind, sind diese höheren Zerlegungszahlen durch die Gleichungen

$$\chi(us) = \sum_{\mu \in \mathrm{IBr}(H)} d^u_{\chi\mu}\mu(s) \qquad (s \in H_{p'})$$

eindeutig bestimmt. Im Fall $u = 1$ sind dies die gewöhnlichen Zerlegungszahlen.
Bezeichnet ζ eine primitive $|\langle u\rangle|$-te Einheitswurzel in K, so ist $d^u_{\chi\mu} \in \mathbb{Z}[\zeta]$ für alle χ und μ.
Für $g \in G$ und $s \in H_{p'}$ ist

$$\chi(gug^{-1} \cdot gsg^{-1}) = \chi(us) = \sum_{\mu \in \mathrm{IBr}(H)} d^u_{\chi\mu}\mu(s) = \sum_{\mu \in \mathrm{IBr}(H)} d^u_{\chi\mu}({}^g\mu)(gsg^{-1}).$$

Daher ist $d^{{}^g u}_{\chi,{}^g\mu} = d^u_{\chi\mu}$.

43.2. Bemerkung. Seien $u_1, \dots, u_m$ Repräsentanten für die Konjugationsklassen von p-Elementen in G. Sind für $i = 1, \dots, m$ Repräsentanten $s_1, \dots, s_{l_i}$ für die Konjugationsklassen von p'-Elementen in $C_G(u_i)$ gegeben, so sind, wie in der Darstellungstheorie II gezeigt, die Elemente u_is_j mit $i \in \{1, \dots, m\}$, $j \in \{1, \dots, l_i\}$ Repräsentanten für die Konjugationsklassen von G; insbesondere ist $|\,\mathrm{Irr}(G)| = |\,\mathrm{Cl}(G)| = \sum_{i=1}^m |\,\mathrm{IBr}(C_G(u_i))|$. Daher bilden die höheren Zerlegungszahlen $d^{u_i}_{\chi\mu}$ mit $\chi \in \mathrm{Irr}(G)$ und $\mu \in \mathrm{IBr}(C_G(u_i))$ für $i = 1, \dots, m$ eine quadratische Matrix D der Größe $|\,\mathrm{Cl}(G)|$. Man nennt D die *vollständige Zerlegungsmatrix* von RG.

43.3. Bemerkung. Für jeden einfachen FG-Modul M ist $M^* := \mathrm{Hom}_F(M,F)$ bekanntlich auch ein einfacher FG-Modul. Ist $g \in G_{p'}$ und sind $\lambda_1,\ldots,\lambda_n$ die Eigenwerte der linearen Abbildung $M \to M$, $m \mapsto gm$, so sind $\lambda_1^{-1},\ldots,\lambda_n^{-1}$ die Eigenwerte der linearen Abbildung $M^* \to M^*$, $f \mapsto gf$. Daher ist $\varphi_{M^*}(g) = \varphi_M(g^{-1}) = \overline{\varphi_M(g)}$; dabei ist $\overline{} : \mathbb{Q}(\zeta) \to \mathbb{Q}(\zeta)$ die Einschränkung der komplexen Konjugation auf den $|G|$-ten Kreisteilungskörper $\mathbb{Q}(\zeta) \subseteq K$.

Satz. *Seien $u, v \in G_p$, $\varphi \in \mathrm{IBr}(C_G(u))$ und $\psi \in \mathrm{IBr}(C_G(v))$. Für die entsprechenden Zerlegungszahlen gilt dann:*

$$\begin{aligned} \sum_{\chi\in\mathrm{Irr}(G)} \overline{d^u_{\chi\varphi}} d^v_{\chi\psi} &= 0, \qquad \textit{falls } u \textit{ und } v \textit{ nicht konjugiert sind,} \\ \sum_{\chi\in\mathrm{Irr}(G)} \overline{d^u_{\chi\varphi}} d^u_{\chi\psi} &= c^u_{\varphi\psi}; \end{aligned}$$

dabei bezeichnet $c^u_{\varphi\psi}$ die entsprechende Cartaninvariante von $RC_G(u)$.

Beweis. Für $s \in C_G(u)_{p'}$ und $t \in C_G(v)_{p'}$ ist

$$\sum_{\varphi\in\mathrm{IBr}(C_G(u))} \sum_{\chi\in\mathrm{Irr}(G)} \sum_{\psi\in\mathrm{IBr}(C_G(v))} \overline{d^u_{\chi\varphi}}\, \overline{\varphi(s)}\, d^v_{\chi\psi}\psi(t) = \sum_{\chi\in\mathrm{Irr}(G)} \overline{\chi(us)}\,\chi(vt) = 0,$$

falls u und v nicht konjugiert sind. Dies kann man auch als Matrixgleichung

$$\overline{\Phi}^T \overline{d^u_{\chi\varphi}}^T d^v_{\chi\psi} \Psi = 0$$

mit invertierbaren Matrizen Φ, Ψ schreiben. Daraus ergibt sich die erste Behauptung.
Sei jetzt $u = v$ und $s = t$. Dann ist

$$\sum_{\chi\in\mathrm{Irr}(G)} \overline{\chi(us)}\,\chi(us) = |C_G(us)| = |C_{C_G(u)}(s)|.$$

Andererseits ist

$$\sum_{\varphi,\psi\in\mathrm{IBr}(C_G(u))} \overline{\varphi(s)}\, c^u_{\varphi\psi}\psi(s) = \sum_{\vartheta\in\mathrm{Irr}(C_G(u))} \overline{\vartheta(s)}\,\vartheta(s) = |C_{C_G(u)}(s)|.$$

Aus der Invertierbarkeit von Φ folgt wieder die Behauptung. □

43.4. Bemerkung. Seien D die vollständige Zerlegungsmatrix von RG, $u_1,\ldots,u_r$ Repräsentanten für die Konjugationsklassen von p-Elementen in G und C_i die Cartanmatrix von $RC_G(u_i)$ für $i = 1,\ldots,r$. Nach Satz 43.3 ist dann

$$\overline{D}^T D = \begin{pmatrix} C_1 & & 0 \\ & \ddots & \\ 0 & & C_r \end{pmatrix}.$$

Satz. $|\det D^2|$ *ist eine Potenz von p.*

Beweis. Aus $\chi(us) = \sum_{\varphi\in\mathrm{IBr}(C_G(u))} d^u_{\chi\varphi}\varphi(s)$ folgt $\overline{\chi}(us) = \sum_{\varphi\in\mathrm{IBr}(C_G(u))} \overline{d^u_{\chi\varphi}}\,\overline{\varphi}(s)$. Daher ist $\overline{d^u_{\chi\varphi}} = d^u_{\overline{\chi}\,\overline{\varphi}}$. Folglich unterscheidet sich $\overline{D}$ von D nur durch eine Permutation der Zeilen und Spalten. Es ist also $|\det D^2| = \det \overline{D}^T D = \prod_{i=1}^r \det C_i$ eine p-Potenz. □

43.5. Bemerkung. Seien $B \in \mathrm{Bl}(RG)$, $\chi \in \mathrm{Irr}(B)$ und $u \in G_{p'}$. Nach Brauers Zweitem Hauptsatz kann man die Funktion $C_G(u)_{p'} \to K$, $s \mapsto \chi(us)$ als Linearkombination von gewöhnlichen, also auch von irreduziblen Brauer-Charakteren in Blöcken b von $RC_G(u)$ mit $\mathrm{Br}_{\langle u\rangle}(\overline{1_B})\overline{1_b} \neq 0$ schreiben. Daher verschwindet die höhere Zerlegungszahl $d^u_{\chi\varphi}$, falls χ und φ in Blöcken B von RG und b von $RC_G(u)$ mit $\mathrm{Br}_{\langle u\rangle}(\overline{1_B})\overline{1_b} = 0$ liegen. Wir benutzen dies, um die Spalten der vollständigen Zerlegungsmatrix D folgendermaßen zu organisieren:

Wir bezeichnen die Blöcke von RG mit $B_1, \dots, B_n$. Die ersten Spalten von F enthalten die höheren Zerlegungszahlen $d^u_{\chi\varphi}$ zu irreduziblen Charakteren χ in B_1 und irreduziblen Brauercharakteren φ in Blöcken b_1 mit $\mathrm{Br}_{\langle u\rangle}(\overline{1_{B_1}})\overline{1_{b_1}} \neq 0$, usw. Die vollständige Zerlegungsmatrix von RG hat dann die Form

$$D = \begin{pmatrix} D_1 & & 0 \\ & \ddots & \\ 0 & & D_n \end{pmatrix}.$$

Denn ist $u \in G_p$, $b \in \mathrm{Bl}(RC_G(u))$ und sind $B, B' \in \mathrm{Bl}(RG)$ mit $\mathrm{Br}_{\langle u\rangle}(\overline{1_B})\overline{1_b} \neq 0 \neq \mathrm{Br}_{\langle u\rangle}(\overline{1_{B'}})\overline{1_b}$, so ist

$$\mathrm{Br}_{\langle u\rangle}(\overline{1_B}\,\overline{1_{B'}})\overline{1_b} = \mathrm{Br}_{\langle u\rangle}(\overline{1_B})\,\mathrm{Br}_{\langle u\rangle}(\overline{1_{B'}})\overline{1_b} = \mathrm{Br}_{\langle u\rangle}(\overline{1_B})\overline{1_b} = \overline{1_b} \neq 0,$$

also $\overline{1_B} = \overline{1_{B'}}$ und damit $B = B'$.
Da D regulär ist, müssen $D_1, \dots, D_r$ quadratisch und regulär sein; insbesondere gilt:

Satz. *Seien $B \in \mathrm{Bl}(RG)$ und $u_1, \dots, u_r$ Repräsentanten von p-Elementen in G. Dann ist*

$$|\,\mathrm{Irr}(B)| = \sum_{i=1}^{r} \sum_{\substack{b\in \mathrm{Bl}(RC_G(u_i)) \\ \mathrm{Br}_{\langle u\rangle}(\overline{1_B})\overline{1_b}\neq 0}} |\,\mathrm{IBr}(b)|.$$

43.6. Definition. Sei $B \in \mathrm{Bl}(RG)$. Ein *B-Element* ist ein Paar (u, b), wobei $u \in G_p$ und $b \in \mathrm{Bl}(RC_G(u))$ mit $\mathrm{Br}_{\langle u\rangle}(\overline{1_B})\overline{1_b} \neq 0$ ist.

Bemerkung. Offenbar operiert G auf der Menge der B-Elemente durch Konjugation: ${}^g(u,b) := ({}^gu, {}^gb)$ für $g \in G$. Ist also $\mathcal{R}$ ein Repräsentantensystem für die Konjugationsklassen von B-Elementen, so gilt nach 43.5:

$$|\,\mathrm{Irr}(B)| = \sum_{(u,b)\in\mathcal{R}} |\,\mathrm{IBr}(b)|.$$

Man beachte, daß in der Summation auch das B-Element $(1, B)$ vorkommt. Ist (u, b) ein B-Element, so nennt man jede Defektgruppe von b auch eine *Defektgruppe* von (u, b).

Satz. *Seien $B \in \mathrm{Bl}(RG)$, $D \in \mathrm{Def}(B)$, (u, b) ein B-Element und $Q \in \mathrm{Def}(b)$. Dann ist $u \in Z(Q) \leq Q \leq_G D$.*

Beweis. Wegen $\overline{1_B} \in I_D(FG)$ ist $\mathrm{Br}_{\langle u\rangle}(\overline{1_B}) \in \sum_{\substack{P\leq C_G(u)\\ P\leq_G D}} I_P(FC_G(u))$, also auch

$$\overline{1_b} = \mathrm{Br}_{\langle u\rangle}(\overline{1_B})\overline{1_b} \in \sum_{\substack{P\leq C_G(u)\\ P\leq_G D}} I_P(FC_G(u)).$$

Nach Rosenbergs Lemma ist daher $\overline{1_b} \in I_P(FC_G(u))$ für eine Untergruppe P von $C_G(u)$ mit $P \leq_G D$. Für jede Defektgruppe Q von b gilt also $Q \leq_G P \leq_G D$. Bekanntlich ist $u \in O_p(C_G(u)) \subseteq Q$. □

43.7. Satz. *Seien $B \in \mathrm{Bl}(RG)$, $D \in \mathrm{Def}(B)$ und $b \in \mathrm{Bl}(RDC_G(D))$ mit $\mathrm{Br}_D(\overline{1_B})\overline{1_b} \neq 0$. Dann ist jedes B-Element mit einer Defektgruppe der Ordnung $|D|$ zu einem B-Element der Form (u, b_u) mit Defektgruppe D und $\mathrm{Br}_D(\overline{1_{b_u}})\overline{1_b} \neq 0$ konjugiert.*

Beweis. Sei (u, b_u) ein B-Element. Nach 43.6 könenn wir $D \in \mathrm{Def}(b_u)$ annehmen. Dann ist $u \in Z(D)$ und $\mathrm{Br}_D(\overline{1_{b_u}}) \neq 0$, also $\mathrm{Br}_D(\overline{1_{b_u}})\overline{1_{b'}} \neq 0$ für einen Block b' von $RDC_{C_G(u)}(D) = RDC_G(D)$. Daher ist

$$\begin{aligned} \mathrm{Br}_D(\overline{1_B})\overline{1_{b'}} &= \mathrm{Br}_D(\mathrm{Br}_{\langle u\rangle}(\overline{1_B}))\,\mathrm{Br}_D(\overline{1_{b_u}})\overline{1_{b'}} \\ &= \mathrm{Br}_D(\mathrm{Br}_{\langle u\rangle}(\overline{1_B})\overline{1_{b_u}})\overline{1_{b'}} \\ &= \mathrm{Br}_D(\overline{1_{b_u}})\overline{1_{b'}} \;\neq\; 0. \end{aligned}$$

Nach Brauers I. Hauptsatz existiert also ein Element $g \in N_G(D)$ mit ${}^gb' = b$. Folglich hat das B-Element $({}^gu, {}^gb_u)$ die gewünschte Eigenschaft. □

43.8. Satz. *Seien $B \in \mathrm{Bl}(RG)$, $D \in \mathrm{Def}(B)$ und $b \in \mathrm{Bl}(RDC_G(D))$ mit $\mathrm{Br}_D(\overline{1_B})\overline{1_b} \neq 0$. Seien (u, b_u) und (v, b_v) zwei B-Elemente mit Defektgruppe D und $\mathrm{Br}_D(\overline{1_{b_u}})\overline{1_b} \neq 0 \neq \mathrm{Br}_D(\overline{1_{b_v}})\overline{1_b}$. Existiert ein Element $g \in G$ mit ${}^g(u, b_u) = (v, b_v)$, so auch ein Element $h \in N_G(D, b)$ mit ${}^h(u, b_u) = (v, b_v)$.*

Beweis. Sei $g \in G$ mit $(v, b_v) = {}^g(u, b_u) = ({}^g u, {}^g b_u)$. Dann ist ${}^g D$ eine Defektgruppe von ${}^g b_u = b_v$. Folglich existiert ein Element $x \in C_G(v)$ mit ${}^{xg}D = D$. Dann ist $(v, b_v) = {}^{xg}(u, b_u)$ und $\mathrm{Br}_D(\overline{1_{b_v}})\overline{1_{{}^{xg}b}} \neq 0$. Nach Brauers I. Hauptsatz existiert also ein Element $y \in N_{C_G(v)}(D)$ mit ${}^{yxg}b = b$. Man ersetze also g durch yxg. □

43.9. Satz. *Seien $B \in \mathrm{Bl}(RG)$, $D \in \mathrm{Def}(B)$, $b \in \mathrm{Bl}(RDC_G(D))$ mit $\mathrm{Br}_D(\overline{1_B})\overline{1_b} \neq 0$ und $u \in Z(D)$. Dann existiert genau ein Block b_u von $RC_G(u)$ mit Defektgruppe D und $\mathrm{Br}_D(\overline{1_{b_u}})\overline{1_b} \neq 0$.*

Beweis. Wegen $0 \neq \mathrm{Br}_D(\overline{1_B})\overline{1_b} = \mathrm{Br}_D(\mathrm{Br}_{\langle u\rangle}(\overline{1_B}))\overline{1_b}$ existiert ein Block b_u von $RC_G(u)$ mit $\mathrm{Br}_{\langle u\rangle}(\overline{1_B})\overline{1_{b_u}}$ $\neq 0 \neq \mathrm{Br}_D(\overline{1_{b_u}})\overline{1_b}$. Wegen $\mathrm{Br}_{\langle u\rangle}(\overline{1_B})\overline{1_{b_u}} = \overline{1_{b_u}}$ ist jede Defektgruppe von b_u zu einer Untergruppe von D kunjugiert, und wegen $\mathrm{Br}_D(\overline{1_{b_u}})\overline{1_b} = \overline{1_b}$ ist die Defektgruppe D von b zu einer Untergruppe einer Defektgruppe von b_u konjugiert. Daher ist $D \in \mathrm{Def}(b_u)$.
Ist b'_u ein weiterer Block von $RC_G(u)$ mit Defektgruppe D und $\mathrm{Br}_D(\overline{1_{b'_u}})\overline{1_b} \neq 0$, so ist $\mathrm{Br}_D(\overline{1_{b_u}}\,\overline{1_{b'_u}})\overline{1_b} = \mathrm{Br}_D(\overline{1_{b_u}})\,\mathrm{Br}_D(\overline{1_{b'_u}})\overline{1_b} = \mathrm{Br}_D(\overline{1_{b_u}})\overline{1_b} \neq 0$, also auch $\overline{1_{b_u}}\,\overline{1_{b'_u}} \neq 0$ und damit $b_u = b'_u$. □

Bemerkung. Wählt man also ein Repräsentantensystem $\mathcal{U}$ für die Bahnen von $N_G(D, b)$ auf $Z(D)$ und für jedes $u \in \mathcal{U}$ den Block b_u von $RC_G(u)$ mit Defektgruppe D und $\mathrm{Br}_D(\overline{1_{b_u}})\overline{1_b} \neq 0$, so bilden die B-Elemente (u, b_u) mit $u \in \mathcal{U}$ nach den obigen Sätzen ein Repräsentantensystem für die Konjugationsklassen von B-Elementen mit einer Defektgruppe der Ordnung $|D|$; insbesondere ist also

$$|\,\mathrm{Irr}(B)| \geq \sum_{u \in \mathcal{U}} |\,\mathrm{IBr}(b_u)| \geq |\mathcal{U}|.$$

43.10. Satz. *Seien $B \in \mathrm{Bl}(RG)$, Q eine p-Untergruppe von G und $b_Q \in \mathrm{Bl}(RQC_G(Q))$ mit Defektgruppe Q und $\mathrm{Br}_Q(\overline{1_B})\overline{1_{b_Q}} \neq 0$. Dann existiert eine Defektgruppe D von B mit $Z(D) \subseteq Q \subseteq D$.*

Beweis. (Induktion nach $|G : Q|$) Sei $b \in \mathrm{Bl}(RN_G(Q))$ mit $\overline{1_b}\,\overline{1_{b_Q}} \neq 0$, also $\overline{1_b}\,\overline{1_{b_Q}} = \overline{1_{b_Q}}$ wegen $\overline{1_b} \in FQC_G(Q)$. Sei $\beta \in \mathrm{Bl}(RN_G(Q, b_Q))$ mit $\overline{1_\beta} = \overline{1_b}\,\overline{1_{b_Q}} = \overline{1_{b_Q}}$, und sei $P \in \mathrm{Def}(\beta)$. Wie in der Darstellungstheorie II gezeigt, ist dann $P \in \mathrm{Def}(b)$ und $P \cap QC_G(Q) \in \mathrm{Def}(b_Q)$, also $P \cap QC_G(Q) = Q$. Offenbar ist $\overline{1_{b_Q}}$ ein Blockidempotent in $FPC_G(Q)$ mit Defektgruppe P. Daher existiert ein Block b_P von $RPC_G(P)$ mit Defektgruppe P und $\mathrm{Br}_P(\overline{1_{b_Q}})\overline{1_{b_P}} \neq 0$. Folglich ist

$$\begin{aligned}\mathrm{Br}_P(\overline{1_B})\overline{1_{b_P}} &= \mathrm{Br}_P(\mathrm{Br}_Q(\overline{1_B}))\,\mathrm{Br}_P(\overline{1_{b_Q}})\overline{1_{b_P}} = \mathrm{Br}_P(\mathrm{Br}_Q(\overline{1_B})\overline{1_{b_Q}})\overline{1_{b_P}}\\ &= \mathrm{Br}_P(\overline{1_{b_Q}})\overline{1_{b_P}} \neq 0.\end{aligned}$$

Im Fall $Q < P$ existiert also nach Induktion eine Defektgruppe D von B mit $Z(D) \subseteq P \subseteq D$. Dann ist $Q \subseteq P \subseteq D$ und $Z(D) \subseteq C_P(Q) \subseteq Q$.
Sei also $Q = P \in \mathrm{Def}(b)$. Nach Brauers I. Hauptsatz ist dann auch Q eine Defektgruppe von B, und die Aussage ist trivial. □

43.11. Satz. *Seien $B \in \mathrm{Bl}(RG)$, $D \in \mathrm{Def}(B)$ und (u, b_u) ein B-Element. Ist D abelsch, so hat b_u eine Defektgruppe der Ordnung $|D|$.*

Beweis. Sei $Q \in \mathrm{Def}(b_u)$, also $u \in Z(Q)$ und $C_G(Q) = C_{C_G(u)}(Q)$. Sei ferner $b_Q \in \mathrm{Bl}(RQC_G(Q))$ mit $\mathrm{Br}_Q(\overline{1_{b_u}})\overline{1_{b_Q}} \neq 0$. Dann ist

$$\begin{aligned}\mathrm{Br}_Q(\overline{1_B})\overline{1_{b_Q}} &= \mathrm{Br}_Q(\mathrm{Br}_{\langle u\rangle}(\overline{1_B}))\,\mathrm{Br}_Q(\overline{1_{b_u}})\overline{1_{b_Q}} = \mathrm{Br}_Q(\mathrm{Br}_{\langle u\rangle}(\overline{1_B})\overline{1_{b_u}})\overline{1_{b_Q}}\\ &= \mathrm{Br}_Q(\overline{1_{b_u}})\overline{1_{b_Q}} \neq 0.\end{aligned}$$

Nach 43.10 existiert also eine Defektgruppe $\tilde{D}$ von B mit $\tilde{D} = Z(\tilde{D}) \subseteq Q \subseteq \tilde{D}$. Folglich ist $|Q| = |\tilde{D}| = |D|$. □

Bemerkung. Ist also B ein Block von RG mit abelscher Defektgruppe D, ist b ein Block von $RC_G(D)$ mit $\mathrm{Br}_D(\overline{1_B})\overline{1_b} \neq 0$, ist $\mathcal{U}$ ein Repräsentantensystem für die Bahnen von $N_G(D, b)$ auf D und ist b_u für $u \in \mathcal{U}$ der Block von $RC_G(u)$ mit Defektgruppe D und $\mathrm{Br}_D(\overline{1_{b_u}})\overline{1_b} \neq 0$, so ist $|\,\mathrm{Irr}(B)| = \sum_{u \in \mathcal{U}} |\,\mathrm{IBr}(b_u)|$.

Beispiel.

(i) Sei D zyklisch der Ordnung 4, also $|\operatorname{Irr}(B)| = 4$ nach früheren Ergebnissen. Bekanntlich ist $\operatorname{Aut}(D) \cong \mathbb{Z}/2\mathbb{Z}$, also $|N_G(D,b) : C_G(D)| \mid 2$. Wie in der Darstellungtheorie II gezeigt, ist $p \nmid |N_G(D,b) : DC_G(D)|$. Daher ist $N_G(D,b) = C_G(D)$, also $\mathcal{U} = D$. Folglich ist $|\operatorname{IBr}(b_u)| = 1$ für $u \in D$; insbesondere ist $|\operatorname{IBr}(B)| = 1$. Die Cartanmatrix von B hat die Form $C_B = (4)$, die Zerlegungsmatrix von B hat die Form $D_B = \begin{pmatrix} 1 \\ 1 \\ 1 \\ 1 \end{pmatrix}$; insbesondere haben die 4 irreduziblen Charaktere in B den gleichen Grad.

(ii) Sei D elementarabelsch der Ordnung 4, also $|\operatorname{Irr}(B)| = 4$. Bekanntlich ist $\operatorname{Aut}(D) \cong \operatorname{Sym}(3)$, also $|N_G(D,b) : C_G(D)| \in \{1,3\}$. Im Fall $N_G(D,b) = C_G(D)$ erhält man wie in (i) $|\operatorname{IBr}(b_u)| = 1$ für $u \in D$ und damit $|\operatorname{IBr}(B)| = 1$.

Sei also $|N_G(D,b) : C_G(D)| = 3$. Dann ist $|\mathcal{U}| = 2$, etwa $\mathcal{U} = \{1, u\}$. Der Block b_u von $RC_G(u)$ hat ebenfalls eine elementarabelsche Defektgruppe der Ordnung 4. Wegen $u \in Z(C_G(u))$ sind nicht alle Elemente in $D \setminus \{1\}$ auch in $C_G(u)$ konjugiert. Nach dem ersten Teil von (ii) ist also $|\operatorname{IBr}(b_u)| = 1$. Wegen $4 = |\operatorname{Irr}(B)| = |\operatorname{IBr}(B)| + |\operatorname{IBr}(b_u)|$ ist also $|\operatorname{IBr}(B)| = 3$. Cartanmatrix und Zerlegungsmatrix lassen sich in diesem Fall nicht ohne weiteres berechnen.

KAPITEL 44

Blöcke mit abelscher Defektgruppe

Sei φ eine vollständige diskrete Bewertung eines Körpers K der Charakteristik 0 mit Bewertungsring R, Bewertungsideal $\mathrm{Rad}(R) = \pi R$ und algebraisch abgeschlossenem Restklassenkörper $F = R/\pi R$ der Charakteristik $p > 0$. Ferner sei G eine endliche Gruppe, und K enthalte die $|G|$-ten Einheitswurzeln.

44.1. Bemerkung. Sei $n = |G| = p^a m$ mit $p \nmid m$ und sei $\mathbb{Q}(\zeta_n) \subseteq K$ der n-te Kreisteilungskörper. Bezeichnet φ ausnahmsweise die Eulersche φ-Funktion, so ist

$$[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \varphi(n) = \varphi(p^a)\varphi(m),$$

$$[\mathbb{Q}(\zeta_m) : \mathbb{Q}] = \varphi(m),$$

und daher

$$[\mathbb{Q}(\zeta_n) : \mathbb{Q}(\zeta_m)] = \varphi(p^a) = [\mathbb{Q}(\zeta_{p^a}) : \mathbb{Q}].$$

Daher ist $\mathcal{G} := \mathrm{Gal}(\mathbb{Q}(\zeta_n)|\mathbb{Q}(\zeta_m)) \cong \mathrm{Gal}(\mathbb{Q}(\zeta_{p^a})|\mathbb{Q})$; einen entsprechenden Isomorphismus erhält man durch Einschränken.
Für $\chi \in \mathrm{Irr}(G)$ und $\sigma \in \mathcal{G}$ ist ${}^\sigma\chi \in \mathrm{Irr}(G)$; man nennt χ und ${}^\sigma\chi$ *p-konjugiert.* Ist $u \in G_p$ und

$$\chi(us) = \sum_{\varphi \in \mathrm{IBr}(C_G(u))} d^u_{\chi\varphi}\varphi(s)$$

für $s \in C_G(u)_{p'}$, so ist

$$(\sigma\chi)(us) = \sigma(\chi(us)) = \sum_{\varphi \in \mathrm{IBr}(C_G(u))} \sigma(d^u_{\chi\varphi})\varphi(s)$$

für $s \in C_G(u)_{p'}$, also $\sigma(d^u_{\chi\varphi}) = d^u_{{}^\sigma\chi,\varphi}$ für $\varphi \in \mathrm{IBr}(C_G(u))$. Insbesondere gilt für die gewöhnlichen Zerlegungszahlen $d_{\chi\varphi} = d_{{}^\sigma\chi,\varphi}$ für $\chi \in \mathrm{Irr}(G)$, $\varphi \in \mathrm{IBr}(G)$. Gehört also χ zum Block B von RG, so auch ${}^\sigma\chi$.

44.2. Satz. *Seien $B \in \mathrm{Bl}(RG)$, $D \in \mathrm{Def}(B)$, $u \in D$ und $\chi \in \mathrm{Irr}(B)$. Dann gilt:*

(i) *Im Fall $\mathrm{ht}(\chi) = 0$ existiert ein $s \in C_G(u)_{p'}$ mit $\chi(us) \in R^\times$.*
(ii) *Im Fall $u \in Z(D)$ existiert ein Element $s \in C_G(u)_{p'}$ mti $\frac{\chi(us)}{p^{\mathrm{ht}(\chi)}} \in R^\times$.*

Beweis. Sei $\mathrm{ht}(\chi) = 0$. Wegen $\overline{\omega_\chi}(\overline{1_B}) \neq 0$ und $\overline{1_B} \in I_D(FG)$ existiert nach Osima eine p-reguläre Konjugationsklasse C von G mit Defektgruppe $Q \subseteq D$ und $\overline{\omega_\chi}(C^+) \neq 0$. Wegen $\overline{\omega_\chi}(I_{<D}(FG)) = 0$ ist $Q = D$. Für $s \in C$ ist

$$0 \not\equiv \omega_\chi(C^+) = \frac{|G : C_G(s)|}{\chi(1)}\chi(s) \pmod{\pi R},$$

also auch $0 \not\equiv \chi(s) \equiv \chi(us) \pmod{\pi R}$. Daher ist $\chi(us) \in R^\times$.
Sei jetzt $u \in Z(D)$, also $D \subseteq C_G(u)$. Für $\chi' \in \mathrm{Irr}(B)$ ist also

$$0 \not\equiv \frac{|G : C_G(us)|}{\chi(1)}\chi(us) \equiv \frac{|G : C_G(us)|}{\chi'(1)}\chi'(us) \pmod{\pi R}.$$

Daher ist $\frac{\chi'(us)}{p^{\mathrm{ht}(\chi')}} \in R^\times$. □

Bemerkung. Im Fall (i) können also nicht alle höheren Zerlegungszahlen $d^u_{\chi\varphi}$ ($\varphi \in \mathrm{IBr}(C_G(u))$) in πR liegen, und im Fall (ii) können nicht alle höheren Zerlegungszahlen $d^u_{\chi\varphi}$ verschwinden.

44.3. Satz (R. Brauer). *Seien $B \in \mathrm{Bl}(RG)$, $D \in \mathrm{Def}(B)$ und $b \in Bl(RC_G(D))$ mit $\mathrm{Br}_D(\overline{1_B})\overline{1_b} \neq 0$. Ist D abelsch und $N_G(D,b) = C_G(D)$, so gilt:*

(i) $|\operatorname{Irr}(B)| = |D|$ *und* $|\operatorname{IBr}(B)| = 1$.
(ii) *Alle Zerlegungszahlen sind gleich 1.*
(iii) $\mathrm{ht}(\chi) = 0$ *für alle* $\chi \in \operatorname{Irr}(B)$.
(iv) $\overline{B} := B/\pi B \cong \mathrm{Mat}(t, FD)$ *für ein* $t \in \mathbb{N}$.

Beweis.

(i) (Induktion nach $|G|$) Im Fall $D \subseteq Z(G)$ ist $\overline{B} \cong \mathrm{Mat}(t, FD)$ für ein $t \in \mathbb{N}$, wie in Darstellungstheorie II gezeigt. Daher ist $|\operatorname{IBr}(B)| = 1$ und $|\operatorname{Irr}(B)| = \dim_K Z(K \otimes_R B) = \mathrm{rk}_R\, ZB = \dim_F Z\overline{B} = \dim_F FD = |D|$. Sei also $D \not\subseteq Z(G)$ und $u \in D \setminus Z(G)$, d.h. $H := C_G(u) < G$. Sei ferner b_u der Block von $RC_G(u)$ mit Defektgruppe D und $\mathrm{Br}_D(\overline{1_{b_u}})\overline{1_b} \neq 0$. Der Block b_u erfüllt dann die gleichen Voraussetzungen wie B. Nach Induktion können wir also $|\operatorname{IBr}(b_u)| = 1$ annehmen. Sei $\operatorname{IBr}(b_u) = \{\varphi\}$. Nach Bemerkung 44.2 ist $0 \neq d^u_{\chi\varphi} \in \mathbb{Q}(\zeta_{p^a})$ für $\chi \in \operatorname{Irr}(B)$. Daher ist

$$0 \neq \prod_{\chi \in \operatorname{Irr}(B)} d^u_{\chi\varphi} \in \mathbb{Q}(\zeta_{p^a}) \cap \mathbb{Q}(\zeta_m) = \mathbb{Q}.$$

Andererseits ist $\prod_{\chi \in \operatorname{Irr}(B)} d^u_{\chi\varphi}$ eine ganz-algebraische Zahl. Daher ist $0 \neq \prod_{\chi \in \operatorname{Irr}(B)} d^u_{\chi\varphi} \in \mathbb{Z}$, also $\prod_{\chi \in \operatorname{Irr}(B)} |d^u_{\chi\varphi}| \in \mathbb{N}$ und $\prod_{\chi \in \operatorname{Irr}(B)} |d^u_{\chi\varphi}|^2 \in \mathbb{N}$. Aus der Ungleichung zwischen dem arithmetischen und geometrischen Mittel folgt also mit $k := |\operatorname{Irr}(B)|$:

$$1 \leq \left(\prod_{\chi \in \operatorname{Irr}(B)} |d^u_{\chi\varphi}|^2 \right)^{\frac{1}{k}} \leq \frac{1}{k} \prod_{\chi \in \operatorname{Irr}(B)} |d^u_{\chi\varphi}|^2 = \frac{1}{k}|D|.$$

(ii) Die Cartanmatrix von B hat offenbar die Form $C_B = (|D|)$. Wegen $|\operatorname{Irr}(B)| = |D|$ sind also alle Zerlegungszahlen gleich 1.

(iii) Daher gilt für die Zerlegungsmatrix D_B von B:

$$D_B C_B^{-1} D_B^T = \begin{pmatrix} 1 \\ \vdots \\ 1 \end{pmatrix} \left(|D|^{-1}\right)(1, \ldots, 1) = \begin{pmatrix} 1 & \cdots & 1 \\ \vdots & & \vdots \\ 1 & \cdots & 1 \end{pmatrix}.$$

Folglich ist $\mathrm{ht}(\chi) = 0$ für alle $\chi \in \operatorname{Irr}(B)$.

(iv) 42.11.

□

44.4. Satz. *Sei B ein Block mit einer zyklischen Defektgruppe D. Besitzt G eine zentrale p-Untergruppe $Q \neq 1$, so ist $|\operatorname{Irr}(B)| = |D|$ und $|\operatorname{IBr}(B)| = 1$; insbesondere ist $\overline{B} := B/\pi B \cong \mathrm{Mat}(n, FD)$ für ein $n \in \mathbb{N}$.*

Beweis. Sei $b \in \mathrm{Bl}(RC_G(D))$ mit $\mathrm{Br}_D(\overline{1_B})\overline{1_b} \neq 0$ und $N := N_G(D,b)$. Nach 44.3 genügt zu zeigen: $N \subseteq C_G(D)$. Bekanntlich ist $N/C_G(D)$ in natürlicher Weise isomorph zu einer p'-Untergruppe von $\mathrm{Aut}(D) \cong (\mathbb{Z}/|D|\mathbb{Z})^\times$. Sei $D = \langle u \rangle$ und $|D| = p^d$. Sei $x \in N$ und $k + p^d\mathbb{Z}$ das Bild von $xC_G(D)$ in $(\mathbb{Z}/p^d\mathbb{Z})^\times$. Dann ist $xux^{-1} = u^k$. Bekanntlich ist $1 \neq Q \subseteq D$, also $u^{p^{d-1}} \in Q \subseteq Z(G)$. Folglich ist $u^{p^{d-1}} = xu^{p^{d-1}}x^{-1} = u^{p^{d-1}k}$, d.h. $p^{d-1}(k-1) \equiv 0 \pmod{p^d}$ und $k - 1 \equiv 0 \pmod{p}$. Daher liegt $k + p^d\mathbb{Z}$ im Kern der kanonischen Abbildung $(\mathbb{Z}/p^d\mathbb{Z})^\times \to (\mathbb{Z}/p\mathbb{Z})^\times$. Wegen $|(\mathbb{Z}/p\mathbb{Z})^\times| = p - 1$ und $|(\mathbb{Z}/p^d\mathbb{Z})^\times| = p^{d-1}(p-1)$ ist dieser Kern eine p-Gruppe. Folglich ist $k + p^d\mathbb{Z} = 1$ und $xC_G(D) = 1$, d.h. $x \in C_G(D)$. □

44.5. Satz. *Sei $B \in \mathrm{Bl}(RG)$ mit zyklischer Defektgruppe D, b ein Block von $RC_G(D)$ mit $\mathrm{Br}_D(\overline{1_B})\overline{1_b} \neq 0$, $E := N_G(D,b)/C_G(D)$ und L das semidirekte Produkt von D und E (bzgl. der kanonischen Operation* *von E auf D). Im Fall $O_p(G) \neq 1$ existiert dann ein $n \in \mathbb{N}$ mit der Eigenschaft, daß $\overline{B} := B/\pi B$ zu* $\mathrm{Mat}(n, FL)$ *isomorph ist.*

Beweis. Bekanntlich ist $Q := O_p(G) \subseteq D \subseteq C_G(Q) \trianglelefteq G$ und $\overline{1_B} \in FC_G(Q)$. Daher existiert ein Block A von $RC_G(Q)$ mit $\overline{1_B 1_A} = \overline{1_A}$ und $\mathrm{Br}_D(\overline{1_A})\overline{1_b} \neq 0$. Dieser besitzt eine zu D konjugierte Defektgruppe. Wegen $\mathrm{Br}_D(\overline{1_A})\overline{1_b} = \overline{1_b}$ ist ferner die Defektgruppe D von b zu einer Untergruppe einer Defektgruppe von A konjugiert. Daher ist $D \in \mathrm{Def}(A)$. Ferner existiert ein Block β von $RN_G(Q, A)$ mit Blockidempotent $\overline{1_\beta} = \overline{1_B 1_A} = \overline{1_A}$. Es ist leicht zu sehen, daß dieser auch Defektgruppe D hat. Es ist $N_G(D, b) \subseteq N_G(Q, A)$; denn für $x \in N_G(D, b)$ ist ${}^xA \in \mathrm{Bl}(RC_G(Q))$ mit $\mathrm{Br}_D(\overline{1_{{}^xA}})\overline{1_b} \neq 0$, also ${}^xA = A$. Daher bleiben die Voraussetzungen erhalten, wenn man B durch β ersetzt. Andererseits ist, wie in der Darstellungstheorie II gezeigt, $B \cong \mathrm{Mat}(m, \beta)$ für ein $m \in \mathbb{N}$. Daher können wir G durch $N_G(Q, A)$ und B durch β ersetzen und $\overline{1_B} = \overline{1_A}$ annehmen.
Wir zeigen jetzt $G = N_G(D, b)C_G(Q)$. Für $g \in G$ ist ${}^gD$ eine Defektgruppe von ${}^gA = A$. Daher existiert ein Element $x \in C_G(Q)$ mit ${}^{xg}D = D$. Folglich ist $\mathrm{Br}_D(\overline{1_A})\overline{1_{{}^{xg}b}} \neq 0$ und es existiert ein Element $y \in C_G(Q) \cap N_G(D)$ mit ${}^{yxg}b = b$. Also ist $yxg \in N_G(D, b)$ und $g \in C_G(Q)N_G(D, b) = N_G(D, b)C_G(Q)$. Das Argument aus dem Beweis von 44.4 zeigt: $N_G(D, b) \cap C_G(Q) = C_G(D)$. Daher hat man einen kanonischen Isomorphismus $E = N_G(D, b)/C_G(D) \to G/C_G(Q)$.
Wir fassen FG als E-graduierte F-Algebra auf. Wegen $\overline{1_B} = \overline{1_A}$ ist $\overline{B} = \overline{1_B}FG$ dann eine E-graduierte F-Algebra mit 1-Komponente $\overline{1_B}FC_G(Q) = \overline{1_A}FC_G(Q) = \overline{A}$. Diese ist ein verschränktes Produkt; denn wählt man zu jedem Element $x \in E$ ein Element $t_x \in N_G(D, b)$ mit $x = t_xC_G(D)$, so ist $t_x\overline{1_B}$ eine graduierte Einheit in der x-Komponente von $\overline{B}$. Nach 44.4 ist $\overline{A} \cong \mathrm{Mat}(n, FD)$ für ein $n \in \mathbb{N}$. Insbesondere ist $Z\overline{A} \cong FD$. Wir erinnern uns, daß ein expliziter Isomorphismus folgendermaßen zustande kommt:

$$f : Z\overline{A} \xrightarrow{\mathrm{Br}_D} ZFN_{C_G(Q)}(D)\,\mathrm{Br}_D(\overline{1_A}) \xrightarrow{\cdot\overline{1_b}} ZFC_G(Q)\overline{1_b} \xleftarrow{\cdot\overline{1_b}} FD.$$

Dies zeigt, daß f mit der Operation von $N_G(D, b)$ verträglich ist. Wir wählen eine Unteralgebra S von $\overline{A}$ mit $\overline{A} = S \oplus J\overline{A}$, also $S \cong \mathrm{Mat}(n, F)$. Wie in der Darstellungstheorie II gezeigt, ist dann $\overline{B} \cong S \otimes_F C_{\overline{B}}(S) \cong \mathrm{Mat}(n, C_{\overline{B}}(S))$. Daher genügt zu zeigen: $C_{\overline{B}}(S) \cong FL$.
Bekanntlich ist $C_{\overline{B}}(S)$ eine E-graduierte F-Algebra mit 1-Komponente $C_{\overline{A}}(S) = Z\overline{A} \cong FD$. Wir wissen auch, daß $C_{\overline{B}}(S)$ ein verschränktes Produkt ist. Für $x \in E$ sei u_x eine graduierte Einheit in der x-Komponente von $C_{\overline{B}}(S)$. Dann unterscheiden sich u_x und $t_x\overline{1_B}$ durch eine Einheit in $\overline{A}$, operieren also in der gleichen Weise auf $Z\overline{A}$. Unter dem Isomorphismus $f : Z\overline{A} \to FD$ geht also die Abbildung $Z\overline{A} \to Z\overline{A},\ z \mapsto u_xzu_x^{-1}$ in die Abbildung $FD \to FD,\ z \mapsto t_xzt_x^{-1}$ über. Ferner ist

$$C_{\overline{B}}(S) = \bigoplus_{x \in E} Z\overline{A}\,u_x = \bigoplus_{d \in D}\bigoplus_{x \in E} Ff(d)u_x.$$

Wie der Beweis von 44.4 zeigt, ist E zu einer Untergruppe von $(\mathbb{Z}/p\mathbb{Z})^\times$ isomorph; insbesondere ist E zyklisch, etwa $E = \langle y \rangle$. Wir können annehmen, daß $u_{y^k} = (u_y)^k$ für $k = 0, \dots, |E| - 1$ ist. Dann ist $(u_y)^{|E|} \in (Z\overline{A})^\times = F^\times \times (1 + JZ\overline{A})$. Wegen $p \nmid |E|$ ist die Abbildung $F^\times \to F^\times,\ z \mapsto z^{|E|}$ surjektiv. Daher existiert ein Element $z \in (Z\overline{A})^\times$ mit $z^{|E|} = (u_y)^{|E|}$. Dann ist $v_y := z^{-1}u_y$ eine graduierte Einheit in der y-Komponente von $C_{\overline{B}}(S)$, die den gleichen Automorphismus auf $Z\overline{A}$ induziert wie u_y. Wegen $(v_y)^{|E|} = 1$ ist

$$C_{\overline{B}}(S) = \bigoplus_{d \in D}\bigoplus_{i=0}^{|E|-1} f(d)(v_y)^i \cong FL,$$

und wir sind fertig. $\square$

44.6. Satz. *Für einen FG-Modul M sind äquivalent:*

(1) *M besitzt genau eine Kompositionsreihe.*
(2) *Für $i \in \mathbb{N}_0$ ist $(JFG)^{i-1}M/(JFG)^iM$ entweder einfach oder 0.*

Beweis.

(1)⇒(2): Ist $(JFG)^{i-1}M/(JFG)^iM$ für ein $i \in \mathbb{N}_0$ weder einfach noch 0, so kann man die Reihe

$$M \supseteq (JFG)M \supseteq (JFG)^2M \supseteq \ldots \supseteq (JFG)^{i-1}M \supseteq (JFG)^iM \supseteq \ldots \supseteq 0$$

auf mehr als eine Weise zu einer Kompositionsreihe von M verfeinern.

(2)⇒(1): Sei $M = M_0 \supseteq M_1 \supseteq \ldots \supseteq 0$ eine Kompositionsreihe von M. Dann ist $(JFG)M \subseteq M_1$. Ist $M/(JFG)M$ einfach, so ist $(JFG)M = M_1$. Analog zeigt man $M_2 = (JFG)M_1 = (JFG)^2M$, usw.

□

Definition. Sind (1) und (2) erfüllt, so nennt man M *einreihig.*

Bemerkung. Dann ist $M \supseteq (JFG)M \supseteq (JFG)^2M \supseteq \ldots \supseteq 0$ die einzige Kompositionsreihe von M.

Beispiel. Sei $P = \langle x \rangle$ eine zyklische Gruppe der Ordnung p^n. Dann ist $JFP = FP(x-1)$, also $(JFP)^i = FP(x-1)^i$ für $i \in \mathbb{N}$. Wegen $(x-1)^{p^n-1} \neq 0$ ist daher

$$FP > JFP > (JFP)^2 > \ldots > (JFP)^{p^n-1} > (JFP)^{p^n} = 0.$$

Folglich ist $\dim(JFP)^{i-1}/(JFP)^i = 1$ für $i = 1, \ldots, p^n$. Dies zeigt, daß FP als FP-Modul einreihig ist.

44.7. Satz. *Seien P eine zyklische p-Gruppe, E eine p'-Untergruppe von* $\mathrm{Aut}(P)$ *und L das semidirekte Produkt von P und E. Dann ist jeder unzerlegbare projektive FL-Modul einreihig.*

Beweis. Bekanntlich ist E zu einer Untergruppe von $(\mathbb{Z}/p^n\mathbb{Z})^\times$ isomorph; insbesondere ist E zyklisch. Daher ist $FE \cong F \times \ldots \times F$. Wir schreiben $FE = Fe_1 \oplus \ldots \oplus Fe_t$ mit paarweise verschiedenen Idempotenten $e_1, \ldots, e_t$ in FE. Wegen $L = PE$ ist also $FL = \bigoplus_{i=1}^t FLe_i = \bigoplus_{i=1}^t FPe_i$ mit $\dim FPe_i = |P|$ für $i = 1, \ldots, t$. Insbesondere sind $e_1, \ldots, e_t$ primitive Idempotente in FL. Wegen $JFL = (JFP)FL$ gilt für $i = 1, \ldots, t$ und $j \in \mathbb{N}_0$:

$$\dim(JFL)^{j-1}e_i/(JFL)^je_i = \dim(JFP)^{j-1}e_i/(JFP)^je_i \in \{0, 1\}.$$

Mit 44.6 folgt die Behauptung. □

44.8. Satz. *Seien P eine zyklische p-Gruppe, E eine p'-Untergruppe von* $\mathrm{Aut}(P)$ *und L das semidirekte Produkt von P und E. Dann ist jeder unzerlegbare FL-Modul M einreihig.*

Beweis. Wir wählen Untermoduln U, V von M mit $V \subseteq U$, so daß U/V einreihig und möglichst groß ist. Schreibt man $(JFG)(U/V) = W/V$, so ist $U/W \cong (U/V)/(W/V) = (U/V)/(JFG)(U/V)$ einfach. Sei Q ein unzerlegbarer projektiver FL-Modul mit $Q/(JFL)Q \cong U/W$. Dann existiert ein Homomorphismus $\varphi : Q \to U$ mit der Eigenschaft, daß folgendes Diagramm kommutiert:

$$\begin{tikzcd}
& Q \arrow[d] \arrow[dl, dotted, "\varphi"'] & \\
U \arrow[r] & U/W \arrow[r] & 0
\end{tikzcd}$$

Dann ist $\varphi(Q) \subseteq U$ und $U/W = \varphi(Q) + W/W$, also $U = \varphi(Q) + W$ und $U/V = (\varphi(Q) + V/V) + (W/V)$. Aus Nakayamas Lemma folgt daher $U/V = \varphi(Q) + V/V$, d.h. $U = \varphi(Q) + V$ und $U/V \cong \varphi(Q)/\varphi(Q) \cap V$. Nach 44.7 sind Q und $\varphi(Q)$ einreihig. Nach Wahl von U und V ist also $\varphi(Q) \cap V = 0$, d.h. $U = \varphi(Q) \oplus V$. Man kann also U durch $\varphi(Q)$ und V durch 0 ersetzen und daher $V = 0$ annehmen.

Wir gehen jetzt zum dualen Modul M^* über. Offenbar ist $M^*/U^\perp \cong U^*$ einreihig und maximal unter den einreihigen Faktormoduln von M^*. Das Argument aus dem ersten Teil des Beweises zeigt dann, daß ein einreihiger Untermodul N von M^* existiert mit $M^* = N \oplus U^\perp$. Da auch M^* unzerlegbar ist, folgt $U^\perp = 0$ und $M^* = N$. Daher ist $M \cong N^*$ einreihig. □

Bemerkung. Wegen $JFL = (JFP)FL$ ist $FL/JFL \cong FE$, d.h. FL besitzt bis auf Isomorphie genau $t := |E|$ einfache Moduln und genau t unzerlegbare projektive Moduln. Jeder von diesen hat Dimension $|P|$ und genau $|P|$ verschiedene Faktormoduln $\neq 0$. Wie der obige Beweis zeigt, ist jeder unzerlegbare FL-Modul zu einem Faktormodul eines unzerlegbaren projektiven FL-Moduls isomorph. Daher besitzt FL bsi auf Isomorphie genau $t \cdot |P|$ unzerlegbare Moduln.

44.9. Definition. Seien M und N FG-Moduln. Man nennt einen FG-Homomorphismus $f : M \to N$ *projektiv*, falls f durch einen projektiven FG-Modul P faktorisiert, d.h. falls ein kommutatives Diagramm der Form

$$\begin{tikzcd} M \arrow[rr, "f"] \arrow[dr] & & N \\ & P \arrow[ur] & \end{tikzcd}$$

existiert.

Bemerkung. Sind $f, f' : M \to N$ projektiv, so auch $f + f'$; denn faktorisieren f und f' durch projektive Moduln P bzw. P', so faktorisiert $f + f'$ durch $P \oplus P'$. Analog ist auch αf für $\alpha \in F$ projektiv. Daher bilden die projektiven FG-Homomorphismen $f : M \to N$ einen Untervektorraum von $\mathrm{Hom}_{FG}(M, N)$, und den entsprechenden Quotienten bezeichnen wir mit $\overline{\mathrm{Hom}}_{FG}(M, N)$. Für FG-Moduln L, Q und FG-Homomorphismen $g : L \to M$ und $h : N \to Q$ sind mit $f : M \to N$ auch $h \circ f$ und $f \circ g$ projektiv. Daraus folgt leicht, daß für FG-Moduln M, M', N, N' stets gilt:

$$\begin{aligned} \overline{\mathrm{Hom}}_{FG}(M \oplus M', N) &\cong \overline{\mathrm{Hom}}_{FG}(M, N) \oplus \overline{\mathrm{Hom}}_{FG}(M', N), \\ \overline{\mathrm{Hom}}_{FG}(M, N \oplus N') &\cong \overline{\mathrm{Hom}}_{FG}(M, N) \oplus \overline{\mathrm{Hom}}_{FG}(M, N'). \end{aligned}$$

Satz. *Seien H eine Untergruppe von G, M ein FG-Modul und N ein FH-Modul. Dann ist*

$$\overline{\mathrm{Hom}}_{FH}(N, \mathrm{Res}_H^G(M)) \cong \overline{\mathrm{Hom}}_{FG}(\mathrm{Ind}_H^G(M), N).$$

Beweis. Wir haben einen kanonischen Isomorphismus $\mathrm{Hom}_{FH}(N, \mathrm{Res}_H^G(M)) \to \mathrm{Hom}_{FG}(\mathrm{Ind}_H^G(N), M)$, der einem FH-Homomorphismus $f : N \to \mathrm{Res}_H^G(M)$ den FG-Homomorphismus

$$\begin{aligned} \hat{f} : FG \otimes_{FH} N \xrightarrow{\mathrm{id}_{FG} \otimes f} FG \otimes_{FH} M &\longrightarrow M \\ x \otimes m &\longmapsto xm \end{aligned}$$

zuordnet. Faktorisiert f durch einen projektiven FH-Modul Q,

$$\begin{tikzcd} N \arrow[rr, "f"] \arrow[dr] & & M \\ & Q \arrow[ur] & \end{tikzcd}$$

so faktorisiert $\hat{f}$ durch den projektiven FG-Modul $FG \otimes_{FH} Q$:

$$\begin{tikzcd} FG \otimes_{FH} N \arrow[rr] \arrow[dr] & & FG \otimes_{FH} M \arrow[r] & M \\ & FG \otimes_{FH} Q \arrow[ur] & & \end{tikzcd}$$

Ist umgekehrt $g : FG \otimes_{FH} N \to M$ ein FG-Homomorphismus, so gehört dazu der FH-Homomorphismus

$$\begin{aligned} \tilde{g} : N &\longrightarrow FG \otimes_{FH} N \xrightarrow{g} M \\ n &\longmapsto 1 \otimes n \end{aligned}$$

Faktorisiert g durch einen projektiven FG-Modul P,

$$\begin{tikzcd} FG \otimes_{FH} N \arrow[rr, "g"] \arrow[dr] & & M \\ & P \arrow[ur] & \end{tikzcd}$$

so faktorisiert $\tilde{g}$ durch den projektiven FH-Modul $\mathrm{Res}_H^G(P)$:

$$\begin{tikzcd} N \arrow[r] & FG \otimes_{FH} N \arrow[rr, "g"] \arrow[dr] & & M \\ & & P \arrow[ur] & \end{tikzcd}$$

□

44.10. Satz. *Seien M, N FG-Moduln mit $N \neq 0$ und $f : M \to N$ ein projektiver Epimorphismus. Dann besitzt M einen unzerlegbaren projektiven direkten Summanden.*

Beweis. Wir können annehmen, daß N einfach ist und wählen einen projektiven FG-Modul P und ein kommutatives Diagramm der Form

$$\begin{tikzcd} M \arrow[rr, "f"] \arrow[dr, "g"'] & & N \\ & P \arrow[ur, "h"'] & \end{tikzcd}$$

Dann ist $g(M) \not\subseteq \mathrm{Rad}(P)$; denn sonst wäre $f(M) = h(g(M)) \subseteq h(\mathrm{Rad}(P)) \subseteq \mathrm{Rad}(N) = 0$. Wir schreiben $P = P_1 \oplus \ldots \oplus P_n$ mit unzerlegbaren projektiven FG-Moduln $P_1, \ldots, P_n$ und bezeichnen mit $p_i : P \to P_i \to P_i / \mathrm{Rad}(P_i)$ für $i = 1, \ldots, n$ die jeweilige kanonische Abbildung. Dann ist $p_i(g(M)) \neq 0$ für ein $i \in \{1, \ldots, n\}$. Folglich existiert ein Homomorphismus $\alpha : M \to P_i$ mit $\alpha(M) \not\subseteq \mathrm{Rad}(P_i)$. Daher ist $\alpha(M) = P_i$. Da die exakte Folge $0 \longrightarrow \mathrm{Ker}(\alpha) \longrightarrow M \xrightarrow{\alpha} P_i \longrightarrow 0$ zerfällt, folgt die Behauptung. □

Bemerkung. Analog zeigt man die duale Aussage: Seien M, N FG-Moduln mit $M \neq 0$ und $f : M \to N$ ein projektiver Monomorphismus. Dann besitzt N einen unzerlegbaren projektiven direkten Summanden.

44.11. Satz. *Seien A ein Block von RG mit einer Defektgruppe D der Ordnung p und B der Brauerkorrespondent von A in $H := N_G(D)$. Dann ist $|\mathrm{IBr}(A)| = |\mathrm{IBr}(B)|$.*

Beweis. Sei S ein einfacher FG-Modul in A. Dann ist $D \in \mathrm{Vtx}(S)$; denn sonst wäre S projektiv, was in der Cartanmatrix zu einer Zeile der Form $(0, \ldots, 0, 1, 0, \ldots, 0)$ führen würde, was unmöglich ist. Die Greenkorrespondenz zeigt, daß $\mathrm{Res}_H^G(S) = T \oplus Y$ ist, wobei T ein unzerlegbarer FH-Modul mit Vertex D und Y ein $\mathcal{Y}$-projektiver FH-Modul mit $\mathcal{Y} := \{H \cap gDg^{-1} : g \in G \setminus H\}$ ist. Nach der modularen Version von 36.5 gehört T zu B. Nach 44.5 und 44.8 ist T einreihig. Wir bezeichnen mit $\overline{T}$ den einzigen einfachen Faktormodul von T und werden zeigen, daß man durch $S \mapsto \overline{T}$ eine Bijektion zwischen den Isomorphieklassen einfacher FG-Moduln in A und den Isomorphieklassen einfacher FH-Moduln in B erhält.
Sei also S' ein weiterer einfacher FG-Modul in A und analog $\mathrm{Res}_H^G(S') = T' \oplus Y'$. Wegen $D \notin \mathcal{Y}$ ist Y' eine direkte Summe von projektiven FH-Moduln und Moduln in Blöcken $B' \neq B$ von RH. Ist $\overline{T'} \neq \overline{T}$, so sind T und T' Quotienten des gleichen unzerlegbaren projektiven FH-Moduls in B. Daher ist T Quotient von T' oder umgekehrt. Wir können annehmen, daß ein FH-Epimorphismus $f : T \to T'$ existiert. Nach 44.10 ist f nicht projektiv. Nach der Greenkorrespondenz ist $\mathrm{Ind}_H^G(T) \simeq S \oplus X$, wobei X ein $\mathcal{X}$-projektiver FG-Modul mit $\mathcal{X} := \{D \cap gDg^{-1} : g \in G \setminus H\} = \{1\}$ ist. Folglich ist X ein projektiver Modul und

$$\begin{aligned} 0 &\neq \overline{\mathrm{Hom}}_{FH}(T, T') \cong \overline{\mathrm{Hom}}_{FH}(T, T' \oplus Y') \\ &= \overline{\mathrm{Hom}}_{FH}(T, \mathrm{Res}_H^G(S')) \cong \overline{\mathrm{Hom}}_{FG}(\mathrm{Ind}_H^G(T), S') \\ &\cong \overline{\mathrm{Hom}}_{FG}(S \oplus X, S') \cong \overline{\mathrm{Hom}}_{FG}(S, S'); \end{aligned}$$

insbesondere ist $\mathrm{Hom}_{FG}(S, S') \neq 0$, d.h. $S \simeq S'$ nach Schurs Lemma.
Jetzt sei W ein beliebiger einfacher FH-Modul in B. Nach der Greenkorrespondenz ist $\mathrm{Ind}_H^G(W) = V \oplus P$, wobei V ein unzerlegbarer FG-Modul mit Vertex D und P ein projektiver FG-Modul ist. Analog ist $\mathrm{Res}_H^G(V) \simeq W \oplus Q$, wobei Q eine direkte Summe von projektiven FH-Moduln und FH-Moduln in Blöcken $B' \neq B$ ist. Sei A' der Block von FG, zu dem V gehört. Nach Nagao ist $\mathrm{Res}_H^G(V) = \mathrm{Br}_D(\overline{1_{A'}})V \oplus U$, wobei U ein $\mathcal{H}$-projektiver FH-Modul und $\mathcal{H}$ die Menge aller p-Untergruppen von H ist, die D nicht enthalten. Daher ist $W \mid \mathrm{Br}_D(\overline{1_{A'}})V$; insbesondere ist $0 \neq \mathrm{Br}_D(\overline{1_A})\,\mathrm{Br}_D(\overline{1_{A'}}) = \mathrm{Br}_D(\overline{1_A}\,\overline{1_{A'}})$ und daher $A = A'$. Dies zeigt, daß V ein unzerlegbarer FG-Modul in A ist. Wir wählen einen einfachen Untermodul S von V und schreiben $\mathrm{Res}_H^G(S) = T \oplus Y$ und $\mathrm{Ind}_H^G(T) \simeq S \oplus X$ wie oben. Nach 44.10 ist

$$\begin{aligned} 0 &\neq \overline{\mathrm{Hom}}_{FG}(S, V) \;\cong\; \overline{\mathrm{Hom}}_{FG}(S \oplus X, V) \\ &= \overline{\mathrm{Hom}}_{FG}(\mathrm{Ind}_H^G(T), V) \;\cong\; \overline{\mathrm{Hom}}_{FH}(T, \mathrm{Res}_H^G(V)) \\ &= \overline{\mathrm{Hom}}_{FH}(T, W \oplus Q) \;\cong\; \overline{\mathrm{Hom}}_{FH}(T, W); \end{aligned}$$

insbesondere ist $\mathrm{Hom}_{FH}(T, W) \neq 0$, d.h. $W \simeq \overline{T}$, und wir sind fertig. □

44.12. Satz. *Seien B ein Block von RG mit Defektgruppe D der Ordnung p, b ein Block von $RC_G(D)$ mit $\mathrm{Br}_D(\overline{1_B})\overline{1_b} \neq 0$ und $t := |N_G(D,b) : C_G(D)|$. Dann ist $|\,\mathrm{IBr}(B)| = t \mid p-1$ und $|\,\mathrm{Irr}(B)| = t + \frac{p-1}{t}$.*

Beweis. Sei B' der Brauerkorrespondent von B in $N_G(D)$. Nach 44.11 ist dann $|\,\mathrm{IBr}(B)| = |\,\mathrm{IBr}(B')|$, und nach 44.5 und 44.8 ist $|\,\mathrm{IBr}(B')| = t$. Da $N_G(D,b)/C_G(D)$ zu einer Untergruppe von $(\mathbb{Z}/p\mathbb{Z})^\times$ isomorph ist, ist $t \mid p-1$. Das Argument aus dem Beweis von 44.4 zeigt, daß jede Bahn von $N_G(D,b)/C_G(D)$ auf $D \setminus \{1\}$ die Länge t hat. Für jedes B-Element (u, b_u) ist o.B.d.A. $D \in \mathrm{Def}(b_u)$. Wegen $u \in Z(C_G(u))$ ist aber die t entsprechende Zahl $t_u = 1$ im Fall $u \neq 1$. Daher gilt für jedes Repräsentantensystem $\mathcal{R}$ für die Konjugationsklassen von B-Elementen $(u, b_u) \neq (1, B)$:

$$|\,\mathrm{Irr}(B)| = |\,\mathrm{IBr}(B)| + \sum_{(u,b_u)\in\mathcal{R}} |\,\mathrm{IBr}(b_u)| = t + \frac{p-1}{t}.$$

□

Index