Darstellungstheorie

Bettina Eick

(Braunschweig, SS 03)

Vorwort

Darstellungstheorie ist eine wichtige Teildisziplin der Gruppentheorie. Dabei werden Homomorphismen $G \to GL(n, K)$ für ein $n \in \mathbb{N}$ und einen Körper K untersucht. Anstatt also mit Gruppen G abstrakt zu rechnen, werden ihre 'Darstellungen' als Matrixgruppen betrachtet. Das hört sich sehr wild an, aber es wird sich herausstellen, daß man damit sehr viel hübsche Sätze über Gruppen beweisen kann.
Ein Beispiel dafür ist der Satz von Burnside: *eine endliche Gruppe der Ordnung $p^a \cdot q^b$ für zwei Primzahlen p und q ist auflösbar.* Wenn man diesen Satz mit Gruppentheoretischen Methoden zeigen will, ist er schwer zu beweisen. Daher wird er meistens mit Hilfe der Darstellungstheorie gezeigt, wo der Beweis dann nicht mehr so schwer ist.

- Algebren und Moduln
  Eine Einführung in diese algebraischen Strukturen
- Darstellungen
  Eine Einführung in die Darstellungstheorie von Algebren und Gruppen
- Klassische Darstellungstheorie
  - Darstellungen über $\mathbb{C}$
  - Eine Einführung in die Charaktertheorie
  - Produkte von Charakteren
  - Induzierte Charaktere
  - Normalteiler
- Modulare Darstellungstheorie
  - Darstellungen über endlichen Körpern $\mathbb{F}_p$
  - Die "Meataxe"

Inhaltsverzeichnis

Kapitel 1

Algebren und Moduln

Zunächst sollen zwei algebraische Strukturen eingeführt werden, die für die Darstellungstheorie wesentlich sind.

1.1 Algebren

1.1. Definition: Sei K ein Körper und A ein Vektorraum über K, so daß A auch gleichzeitig ein Ring ist (im weiteren werden nur Ringe mit Einselement betrachtet). Wenn außerdem noch für $k \in K$ und $a, b \in A$ die Gleichung

$$k(ab) = (ka)b = a(kb)$$

gilt, dann heißt A eine K-Algebra.

1.2. Beispiel: Ein elementares Beispiel für eine Algebra ist die Menge $M_n(K)$ aller $n \times n$-Matrixen über K. Diese bilden einen Vektorraum der Dimension n^2 über K und sind auch ein Ring.

Wozu braucht man Algebren? Sie bieten eine Möglichkeit, aus der algebraischen Struktur der Gruppen (mit nur einer Operation) die algebraischen Strukturen der Ringe und Vektorräume (mit je zwei Operationen) zu machen. Das ist ein wesentlicher Trick in der Darstellungstheorie. Die folgende Konstruktion wird dazu benutzt.

1.3. Definition: Sei G eine endliche Gruppe und K ein Körper. Dann ist

$$K[G] = \left\{ \sum_{g \in G} k_g g \mid k_g \in K \text{ für jedes } g \in G \right\}$$

die Menge der formalen Summen von Elementen in G.

Wie rechnet man in $K[G]$? Es gilt

$$\begin{aligned}\left(\sum_{g\in G} k_g g\right) + \left(\sum_{g\in G} l_g g\right) &= \sum_{g\in G} (k_g + l_g)\, g \\ \left(\sum_{g\in G} k_g g\right) \cdot \left(\sum_{g\in G} l_g g\right) &= \sum_{g\in G, g_1 g_2 = g} (k_{g_1} \cdot l_{g_2}) g\end{aligned}$$

Das folgende Lemma zeigt, daß $K[G]$ mit diesen Rechenregeln eine Algebra ist.

1.4. Lemma: *Sei G eine endliche Gruppe und K ein Körper.*

- $K[G]$ *ist ein K-Vektorraum der Dimension $|G|$.*
- $K[G]$ *ist ein Ring.*
- $K[G]$ *ist eine K-Algebra.*

$K[G]$ *wird auch die Gruppenalgebra von G über K genannt.*

Beweis: a) Das ist ziemlich klar.
b) Muß man nachrechnen.
c) Ist nun trivial. •

Ein wesentlicher Trick in der Darstellungstheorie ist, daß man ringtheoretische Methoden oder Methoden aus der Linearen Algebra auf $K[G]$ anwendet, um etwas über G herauszubekommen. Zur Untersuchung von $K[G]$ und anderer Algebren führen wir zunächst noch etwas Notation ein.

1.5. Definition: Sei A eine K-Algebra mit Basis $\{a_1, \ldots, a_d\}$. Dann gilt

$$a_i a_j = \sum_{k=1}^{d} c_{ijk} a_k$$

für gewisse $c_{ijk} \in K$. Diese Elemente c_{ijk} werden die Strukturkonstanten von A genannt.

1.6. Bemerkung: Die Algebra A ist durch ihre Strukturkonstanten vollständig bestimmt. Daher kann jede d-dimensionale Algebra durch d^3 Körperelemente vollständig beschrieben werden.

Man kann den Körper K in eine K-Algebra einbetten und die Gruppe G in ihre Gruppenalgebra $K[G]$. Das zeigt die folgende Bemerkung.

1.7. Bemerkung:

- Sei A eine K-Algebra und sei 1 das Einselement des Ringes A. Dann ist $K \cong K \cdot 1 \subseteq A$. Der Körper K kann also in A eingebettet werden.
- Sei G eine endliche Gruppe. Dann kann jedes Element $h \in G$ mit der formalen Summe $1h + \sum_{g\in G, g\neq h} 0g$ identifiziert werden. Die Gruppe G kann also in $K[G]$ eingebettet werden.

Meistens werden K und G einfach mit ihren Einbettungen in A bzw. $K[G]$ identifiziert.

1.2 Ideale und Homomorphismen in Algebren

Jede K-Algebra A ist auch ein Ring. Also kann A auch Ideale haben. Aber A ist meistens kein kommutativer Ring, also müssen wir zwischen Rechts- und Linksidealen unterscheiden. Deren Definition wird hier wiederholt.

1.8. Definition: Sei A ein Ring und sei $I \subseteq A$, so daß gilt

(1) $0 \in I$,

(2) sind $a, b \in I$, so ist auch $a - b$ und $a + b$ in I.

Dann heißt I

- ein Rechtsideal von A, wenn $ar \in I$ für $a \in I$ und $r \in A$,
- ein Linksideal von A, wenn $ra \in I$ für $a \in I$ und $r \in A$,
- ein (zweiseitiges) Ideal von A, wenn I sowohl Rechts- als auch Linksideal ist.

Ideale von Algebren haben zusätzliche Eigenschaften, wie das folgende Lemma zeigt.

1.9. Lemma: *Sei A eine K-Algebra.*

- *Ist I ein Rechts- oder Linksideal von A, dann ist I ein Teilraum von A.*
- *Ist I ein Ideal von A, dann ist A/I eine K-algebra.*

Beweis: a) Sei $k \in K$ und $a \in I$. Dann gilt $ka = k(1a) = (k1)a \in I$ und $ak = (a1)k = a(1k) \in I$. Also ist I ein Teilraum von A.
b) Das kann man leicht nachrechnen. •

1.10. Definition: Seien A und B zwei K-Algebren. Sei $\psi : A \to B$ eine Abbildung mit

- ψ ist eine linear Abbildung der Vektorräume A und B,
- $\psi(ab) = \psi(a)\psi(b)$ für alle $a, b \in A$, und
- $\psi(1) = 1$.

Dann heißt ψ ein Algebrahomomorphismus von A nach B.

Damit ist ein Algebrahomomorphismus sowohl ein Ringhomomorphismus, wie auch eine lineare Abbildung. Man kann nun wieder die üblichen Zusammenhänge zwischen Homomorphismen und Idealen nachrechnen.

1.11. Lemma: *Sei $\psi : A \to B$ ein Algebrahomomorphismus. Dann ist $Ker(\psi)$ ein Ideal in A und $Bild(\psi)$ eine Teilalgebra von B.*

Man kann noch viele weitere Aussagen von linearen Abbildungen oder Ringhomomorphismen auf Algebrahomomorphismen übertragen. Dabei muß man nur jeweils nachschauen, ob die gegebene Aussage für beide Typen von Homomorphismen gilt, dann gilt sie auch für Algebrahomomorphismen.

1.12. Bemerkung: Im folgenden sollen alle Algebren endlich dimensional sein.

1.3 Moduln

Jetzt lassen wir Algebren auf Vektorräumen operieren. Wieder sollen alle betrachteten Vektorräume endlich dimensional sein.

1.13. Definition: Sei A eine K-Algebra und V ein K-Vektorraum. Es sei eine Abbildung $V \times A \to V : (v, a) \mapsto va$ gegeben, die die folgenden Gesetze erfüllt:

- $(v + w)a = va + wa$ für $v, w \in V$ und $a \in A$,
- $v(a + b) = va + vb$ für $v \in V$ und $a, b \in A$,
- $v(ab) = (va)b$ für $v \in V$ und $a, b \in A$,
- $(kv)a = k(va) = v(ka)$ für $v \in V$ und $a \in A$ und $k \in K$,
- $v1 = v$.

Dann heißt V ein A-(Rechts-)Modul und A operiert auf V per Multiplikation von rechts.

1.14. Beispiel: Sei $A = M_n(K)$ und $V = K^n$. Dann kann man va als Multiplikation von Vektor mit Matrix auffassen und damit ist V ein A-Modul.

1.15. Definition: Sei V ein A-Modul.

- Wenn $W \leq V$ ein Unterraum ist mit $wa \in W$ für alle $w \in W$ und $a \in A$, dann heißt W ein A-Untermodul von V. Wir schreiben auch $W \leq_A V$.
- Wenn $W \leq V$ ein A-Untermodul ist, dann ist V/W der zugehörige Faktormodul. (Es muß eigentlich gezeigt werden, daß V/W ein Modul ist, aber das ist Standard.)

Viele Aussagen über Vektorräume übertragen sich auf Moduln. Hier ist ein Beispiel.

1.16. Lemma: *Seien $U, W \leq_A V$. Dann sind auch $U \cap W$ und $U + W$ Untermoduln von V.*

Es gibt einige Moduln, die sich besonders auszeichnen in der Menge aller Moduln. Diese sollen im folgenden definiert werden.

1.17. Definition: Sei V ein A-Modul. Wir schreiben $V = U \oplus W$ für zwei Untermoduln U und W, wenn $V = U + W$ und $U \cap W = \{0\}$ ist. Der Modul V heißt dann die direkte Summe aus U und W, und U ist ein Komplement zu W. (Wenn $V = U + W$ gilt, dann ist V die Summe aus U und W.)

1.18. Definition: Sei V ein A-Modul.

- V heißt irreduzibel, wenn V nur die trivialen Untermoduln $\{0\}$ und V hat.
- V heißt vollständig reduzibel, wenn für jeden Untermodul W von V ein Komplement U zu W in V existiert (d.h. $V = W \oplus U$ gilt).

Damit ist jeder irreduzible Modul auch vollständig reduzibel. Die Umkehrung gilt aber nicht, wie das folgende Beispiel zeigt.

1.19. Beispiel: Sei E_{ij} die Standartbasis der Algebra $M_n(K)$.

- Sei $A \leq M_2(\mathbb{Q})$ die Algebra mit der Basis E_{11}, E_{22} und sei $V = \mathbb{Q}^2$. Dann sind $W = \langle(1,0)\rangle$ und $U = \langle(0,1)\rangle$ zwei A-Untermoduln von V und es gilt $V = W \oplus U$. Sicher sind W und U irreduzibel. Aber wie sieht man damit, daß V schon vollständig irreduzibel ist? Die Definition nachzurechnen ist schwierig, da V unendlich viele A-Untermoduln hat!
- Sei $A \leq M_2(\mathbb{F}_2)$ die Algebra mit der Basis E_{12}. Dann hat V genau einen irreduziblen Teilmodul $U = \langle(0,1)\rangle$. Da U kein Komplement in V hat, ist V sicher nicht vollständig reduzibel.

Als nächstes wird jetzt eine Charakterisierung der vollständig reduziblen Moduln vorgestellt, die es erlaubt, diese Eigenschaft leichter nachzurechnen.

1.20. Lemma: *Sei V ein A-Modul. Wenn V als Summe von irreduziblen Moduln geschrieben werden kann, dann ist V vollständig reduzibel.*

Beweis: Sei V eine Summe von irreduziblen Moduln, d.h $V = V_1 + \ldots + V_l$. Sei $W \leq V$. Wähle U maximal mit der Eigenschaft, daß $W \cap U = 0$ gilt. (U existiert, daß V endlich dimensional ist.) Wir zeigen, daß $W + U = V$ gilt. Annahme: $W + U < V$. Dann existiert ein V_i mit $V_i \not\leq W + U$. Dann gilt $V_i \not\leq U$ und so $U < U + V_i$. Andererseits gilt $(W + U) \cap V_i = 0$, da V_i irreduzibel ist. Damit gilt auch $W \cap (U + V_i) = 0$: denn sei $v \in W \cap (U + V_i)$. Dann gilt $v = u + l$ und somit $v - u \in V_i \cap (W + U)$. Daraus folgt $v - u = 0$ und $v = u \in W \cap U = 0$. Also erhalten wir $W \cap (U + V_i) = 0$ und das Widerspricht der Maximalität von U. •

1.21. Lemma: *Sei V ein A-Modul. Wenn V vollständig reduzibel ist, dann kann V als Summe von irreduziblen Moduln geschrieben werden kann.*

Beweis: Sei S die Summe aller irreduzibler Untermoduln von V. Falls $S < V$ ist, dann gibt es ein $T \neq 0$ mit $S \oplus T = V$. Aber auch T enthält einen irreduziblen Teilmodul U und $U \not\leq S$. Das ist ein Widerspruch zur Wahl von S. •

1.22. Lemma: *Sei V ein A-Modul. Wenn V als Summe von irreduziblen Untermoduln geschrieben werden kann, dann kann V auch als direkte Summe von einigen dieser irreduziblen Untermoduln geschrieben werden.*

Beweis: Sei $V = V_1 + \ldots + V_r$ und sei W maximal mit der Eigenschaft, daß W eine direkte Summe von einigen der V_i's ist. Annahme: $W < V$. Dann gibt es ein V_i mit $V_i \not\leq W$. Da V_i irreduzibel ist, gilt dann $V_i \cap W = 0$. Also ist $U = W \oplus V_i$ ein Untermodul von V mit $U > W$. Das ist ein Widerspruch zur Wahl von W. •

Insgesamt haben wir jetzt den folgenden Satz.

1.23. Satz: *Sei V ein A-Modul. Genau dann ist V vollständig reduzibel, wenn V als direkte Summe von irreduziblen Moduln geschrieben werden kann.*

Damit kann jetzt das Beispiel 1.19 a) ganz leicht gerechnet werden, und der dort vorgestellte Modul ist vollständig reduzibel.

1.4 Homomorphismen von Moduln

Genau wie es lineare Abbildungen zwischen Vektorräumen gibt, so gibt es auch Homomorphismen zwischen Moduln. Das sind diejenigen linearen Abbildungen, die die Modulstruktur respektieren.

1.24. Definition:

- Seien V und W zwei A-Moduln. Die Abbildung $\varphi : V \to W$ heißt ein A-Modulhomomorphismus, wenn φ linear ist und $\varphi(va) = \varphi(v)a$ für alle $v \in V$ und $a \in A$ gilt.
- Ein injektiver Homomorphismus wird auch Monomorphismus genannt.
- Ein surjektiver Homomorphismus wird auch Epimorphismus genannt.
- Ein bijektiver Homomorphismus wird auch Isomorphismus genannt.
- Zwei A-Moduln V und W heißen isomorph, wenn es einen Modulisomorphismus zwischen ihnen gibt.

1.25. Bemerkung: Wie in der linearen Algebra sind Kern und Bild eines Modulhomomorphismus Untermoduln.

Aus der linearen Algebra ist bekannt, daß jede lineare Abbildung zwischen zwei Vektorräumen durch eine Matrix dargestellt werden kann. Das gilt dann natürlich auch für die Modulhomomorphismen und so stellt man sich diese Abbildungen meistens vor.

1.26. Definition:

- Die Menge $Hom_A(V, W)$ ist die Menge aller A-Modulhomomorphismen von V nach W.
- Die Menge $Hom(V, V)$ ist die Menge aller linearen Abbildungen von V nach V.

Diese Mengen wollen wir etwas genauer untersuchen.

1.27. Lemma: *Sei A eine K-Algebra mit zwei Moduln V und W.*

- *Die Menge $Hom_A(V, W)$ ist ein K-Vektorraum.*
- *Die Menge $Hom_A(V, V)$ ist eine K-Algebra.*

Beweis: Beides ist elementar. •

1.28. Lemma: *Sei A eine K-Algebra und V ein K-Modul.*

- *Jedes $a \in A$ definiert eine lineare Abbildung $a_V : V \to V : v \mapsto va$.*
- *Die Abbildung $A \to Hom(V, V) : a \mapsto a_V$ ist ein Algebrenhomomorphismus.*

Beweis: a) Die Definition eines Moduls bedeutet, daß die Abbildung a_V linear ist.
b) Die Definition eines Moduls liefert, daß die Abbildung linear und multiplikativ ist. Sicherlich operiert die 1 wie die 1. •

Aus der linearen Algebra ist bekannt, daß $Hom(V, V) \cong M_n(K)$ gilt. Somit kann man mit Hilfe des obigen Lemmas Homomorphismen in die Menge aller Matrizen machen. (Insofern ist das obige Lemma eine Beschreibung von “Darstellungen” von Algebren.)

1.5 Endomorphismen von Moduln

Später werden wir noch etwas mehr Notation über Homomorphismen von Moduln brauchen.

1.29. Definition: Sei V ein A-Modul.

- Die K-Algebra $Hom(V, V)$ wird auch als $End(V)$ bezeichnet. Die Elemente in $End(V)$ heißen Endomorphismen.
- Das Bild von $A \to End(V) : a \mapsto a_V$ wird mit A_V bezeichnet.
- Die K-Algebra $Hom_A(V, V)$ wird auch als $End_A(V)$ bezeichnet.

Bild über A, A_V und $End_A(V)$. Was ist $Z(A)$?
Es gilt ein paar Bemerkungen über Endomorphismen, die hier interessant sind.

1.30. Lemma: *Sei V ein A-Modul.*

- *V ist auch ein A_V-Modul.*
- *V ist auch ein $End_A(V)$-Modul.*
- *$End_A(V)$ ist der Zentralisator in $End(V)$ unter A_V; das heißt $End_A(V) = \{\varphi \in End(V) \mid \varphi a_v = a_v \varphi$ für alle $a \in A\}$.*

Beweis: a) A_V ist nichts anderes als die Operation von A auf V.
b) Der Vektorraum V ist ein $End(V)$-Modul und damit auch ein Modul für jede Teilalgebra von $End(V)$.
c) Sei $\varphi \in End_A(V)$. Dann ist $\varphi \in End(V)$, da φ eine lineare Abbildung von V ist. Weiter gilt für $a \in A$ die Gleichung $(\varphi a_V)(v) = \varphi(v)a_V = \varphi(v)a = \varphi(va) = \varphi(va_V) = (a_V\varphi)(v)$. •

Schlußendlich folgen alle diese Aussagen aus den Definitionen, die eben gerade so gemacht sind, daß diese Dinge zusammenpassen. Das obige Lemma liefert eine angenehme Art und Weise Endomorphismen auszurechnen.

1.31. Beispiel: Sei $A \leq M_2(\mathbb{Q})$ die Algebra mit der Basis E_{11} und sei $V = \mathbb{Q}^2$ der natürliche Modul. Dann gilt

- $End(V) = Hom(V, V) \cong M_2(\mathbb{Q})$.
- $A_V = A$, da A selber schon in den Endomorphismen liegt.
- $End_A(V)$ kann als die Menge aller Matrizen berechnet werden, die mit A kommutieren. Dabei reicht es, eine Basis von A zu betrachten. Es folgt (Nachrechnen), daß $End_A(V)$ die K-Algebra mit der Basis E_{11} und E_{22} ist.

1.6 Der reguläre Modul

Hat eigentlich jede Algebra einen Modul? Ja, es gibt immer einen ausgezeichneten Modul, nämlich die Algebra selbst!

1.32. Definition: Sei A eine K-Algebra. Dann operiert A per Multiplikation von rechts auf sich selbst. Dieser Modul wird auch der reguläre Modul genannt und mit A^o bezeichnet.

Der reguläre Modul einer Algebra spielt eine wichtige Rolle. Wir wollen diesen Modul noch genauer untersuchen.

1.33. Lemma: *Sei A eine K-Algebra. Die A-Untermoduln von A^o entsprechen gerade den Rechtsidealen von A.*

Beweis: Das sieht man sofort. •

Der folgende Satz zeigt, daß die Faktormoduln von A^o eine sehr wichtige Rolle in der Untersuchung aller Moduln spielen werden.

1.34. Satz: *Sei A eine K-Algebra und sei V ein irreduzibler A-Modul. Dann ist V isomorph zu einem Faktormodul von A^o.*

Beweis: Sei $0 \neq v \in V$ und definiere $\varphi : A \to V : a \mapsto va$. Dann ist φ eine lineare Abbildung, die mit A verträglich ist. Also gilt $\varphi \in Hom_A(A^o, V)$. Weiter ist das Bild von φ ein Untermodul von V, der v enthält. Da V irreduzibel ist, gilt $Bild(\varphi) = V$ und φ ist ein Epimorphismus. Also ist V ein Faktor von A^o. •

Man kann also sagen, daß der reguläre Modul der "Urgroßvater" aller irreduziblen Moduln ist, denn er enthält alle irreduziblen Moduln als Faktoren.

1.35. Definition: Sei A eine K-Algebra. Dann heißt A halbeinfach, wenn A^o ein vollständig reduzibler Modul ist.

1.36. Lemma: *Sei A eine halbeinfache K-Algebra und sei V ein irreduzibler A-Modul. Dann ist V isomorph zu einem Untermodul von A^o.*

Beweis: Der Modul V ist isomorph zu einem Faktor A^o/W. Da A^o vollständig reduzibel ist, hat W ein Komplement U in A^o. Es gilt $V \cong_A U$. •

1.37. Beispiel: Sei $A = M_2(K)$. Dann ist A eine 4-dimensionale K-Algebra mit der Basis $E_{11}, E_{12}, E_{21}, E_{22}$. Wie operiert A auf sich selbst?

- $A \to End_A(A) : a \mapsto a_A$ ist der Operationshomomorphismus. Wie sieht dieser hier explizit aus? Es gilt $M_2(K) \mapsto M_4(K) : a \mapsto a_A$. Wir berechnen die Bilder der Basiselemente von A. (Nachrechnen)
- $End_A(A)$ ist die zugehörige Endorphismenalgebra. Wie sieht diese aus?

Kapitel 2

Einige elementare Sätze über Algebren

In diesem Kapitel werden einige elementare Aussagen über Algebren und ihre Moduln gezeigt. Diese Aussagen bilden die Grundlage für alle späteren Untersuchungen.

2.1 Der Satz von Schur

Dieser Satz spielt eine wesentliche Rolle in der gesamten Darstellungstheorie. Meistens wird er 'Lemma von Schur' genannt, weil der Beweis so einfach ist.

2.1. Lemma: (Schur)
Seien V und W zwei irreduzible A-Moduln. Dann hat jedes nicht-triviale Element aus der K-Algebra $Hom_A(V, W)$ ein inverses in $Hom_A(W, V)$.

Beweis: Sei $\varphi \in Hom_A(V, W)$ mit $\varphi \neq 0$. Dann ist $B = Bild(\varphi)$ ein nicht-trivaler Untermodul von W. Da W irreduzibel ist, gilt $B = W$. Weiter ist $K = Kern(\varphi)$ ein echter Untermodul von V. Da V irreduzibel ist, gilt $K = 0$. Also ist φ bijektiv. •

Das Lemma von Schur hat viele hübsche Anwendungen. Hier soll an dieser Stelle nur einige elementare Bemerkungen gemacht werden.

2.2. Lemma: *Sei V ein irreduzibler A-Modul. Dann hat jedes Element in $End_A(V)$ ein inverses; d.h. $End_A(V)$ ist ein Schiefkörper. (Auch Divisionsalgebra genannt).*

Beweis: Folgt sofort aus 2.1. •

Das folgende Lemma zeigt, daß das Lemma von Schur weitreichende Konsequenzen hat.

2.3. Lemma: *Sei V ein irreduzibler A-Modul und sei K algebraisch abgeschlossen. Dann gilt $End_A(V) = Kid_V$.*

Beweis: Sicherlich gilt $Kid \subseteq End_A(V)$. Sei andersherum $\varphi \in End_A(V)$. Da K algebraisch abgeschlossen ist, hat φ einen Eigenwert k in K. Es gilt $\varphi - kid \in End_A(V)$ und diese lineare Abbildung ist nicht invertierbar. Also folgt: $\varphi - kid$ ist die 0-Abbildung nach Lemma 2.1 und daher $\varphi = kid$. •

2.2 Der Satz von Maschke

2.4. Satz: (Maschke)
Sei G eine endliche Gruppe und K ein Körper, dessen Charakteristik kein Teiler von $|G|$ ist. Dann ist jeder $K[G]$-Modul vollständig reduzibel.

Bevor wir diesen Satz beweisen, noch ein paar wichtige Anmerkungen. Die Charakteristik eines Körpers ist entweder 0 (und dann ist $\mathbb{Q}$ in dem Körper enthalten) oder sie ist eine Primzahl p (und dann ist $\mathbb{Z}_p$ in dem Körper enthalten). Die Zahl 0 teilt niemals $|G|$. Daher ist der Satz von Maschke auf alle Körper der Charakteristik 0 anwendbar und damit also eine ziemlich weitreichende Aussage!
Die Voraussetzung in diesem Satz besagt im wesentlichen, daß $|G|$ in K invertierbar ist. So wird diese Voraussetzung auch verwendet werden.

Beweis: Sei V ein $K[G]$-Modul. Sei W ein Teilmodul von V. Wir müssen ein Komplement zu W in V konstruieren. Sicher gibt es einen Teilraum U von V mit $V = U \oplus W$, aber U muß ja kein Teilmodul sein. Wir wandeln U so ab, daß es ein Teilmodul wird. Jedes Element $v \in V$ hat eine eindeutige Darstellung $v = u + w \in U + W$. Sei $\psi : V \to W : v \mapsto w$ die Projektion von V auf W. Dazu definieren wir

$$\theta : V \to W : v \mapsto \frac{1}{|G|} \sum_{g \in G} \psi(vg)g^{-1}.$$

Das kann man so definieren, weil man in K durch $|G|$ teilen darf, denn die Charakteristik von K teilt $|G|$ nicht. Sicherlich ist θ eine lineare Abbildung. Es gilt für $v \in V$ und $h \in G$:

$$\begin{aligned}
\theta(vh) &= \frac{1}{|G|} \sum_{g \in G} \psi(vhg)g^{-1} \\
&= \frac{1}{|G|} \sum_{g \in G} \psi(vhg)g^{-1}h^{-1}h \\
&= \frac{1}{|G|} \sum_{g \in G} \psi(vhg)(hg)^{-1}h \\
&= \frac{1}{|G|} \sum_{k \in G} \psi(vk)(k)^{-1}h \\
&= \theta(v)h
\end{aligned}$$

Also ist θ ein Modulhomomorphismus. Sei $L = Kern(\theta)$. Dann ist L ein Teilmodul von V. Wir zeigen, daß L ein Komplement zu W in V ist. Zunächst kann man beobachten, daß $\theta(w) = w$ ist für alle $w \in W$. Sei $v \in V$ mit $\theta(v) = w$. Dann gilt für $l = v - w$ die Gleichung $\theta(l) = \theta(v-w) = \theta(v) - \theta(w) = w - w = 0$ und damit ist $l \in L$. Also folgt $v = l + w \in L + W$ und $V = L + W$. Sei $v \in L \cap W$. Dann gilt $0 = \theta(v) = v$ und damit ist $L \cap W = 0$. Insgesamt folgt $V = L \oplus W$. •

Aus Satz 2.4 folgt sofort das Folgende.

2.5. Lemma: *Sei G eine endliche Gruppe und K ein Körper, dessen Charakteristik kein Teiler von $|G|$ ist (z.B. Char 0). Dann ist $K[G]$ halbeinfach.*

2.3 Der Satz von Wedderburn

In diesem Abschnitt sollen die vollständig reduziblen Moduln genauer untersucht werden. Nach Satz 1.23 sind solche Moduln direkte Summen ihrer irreduziblen Untermoduln. Aber solche direkten Summen sind nicht eindeutig. Wie sieht so eine direkte Summe genau aus? Wenn man zwei Zerlegungen als direkte Summen hat, wie unterscheiden die sich dann? Das soll hier näher analysiert werden.

2.6. Definition: Sei V ein vollständig reduzibler A-Modul und sei M ein irreduzibler A-Modul. Sei $M(V)$ die Summe aller derjenigen irreduziblen Untermoduln von V, die zu M isomorph sind. Dann ist $M(V)$ ein Untermodul von V und dieser Untermodul wird auch die M-homogene Komponente in V genannt.

2.7. Bemerkung: Seien M, N irreduzible A-Moduln und sei V vollständig reduzibel.

- $M(V)$ eine direkte Summe von Untermoduln von V. (Lemma 1.22.)
- Falls $M \cong_A N$, dann folgt $M(V) = N(V)$.
- Falls $M \not\cong_A N$, dann folgt $M(V) \cap N(V) = \{0\}$.

Ein vollständig reduzibler Modul zerfällt also in eine direkte Summe von homogenen Komponenten. Wie kann man so eine homogene Komponente berechnen? Zu beachten ist, daß ein Modul V unendlich viele Untermodul besitzen kann, die zu einem gegebenen Untermodul isomorph sind. (Beispiel : der triviale Modul.) Also ist die Definition vielleicht nicht unbedingt geeignet zur Berechnung von homogenen Komponenten.

2.8. Lemma: *Sei V ein vollständig reduzibler A-Modul und sei $V = V_1 \oplus \ldots \oplus V_r$ eine Zerlegung von V in eine direkte Summe irreduzibler Untermoduln. Sei M ein irreduzibler A-Modul und seien (OBdA) $V_1, \ldots, V_s$ die zu M isomorphen Moduln in $V_1, \ldots, V_r$. Dann gilt*

- *$M(V)$ ist ein $End_A(V)$-Untermodul von V.*
- *$M(V) = V_1 \oplus \ldots \oplus V_s$.*
- *Die Anzahl s ist unabhängig von der gewählten Zerlegung von V in irreduzible. (Diese Anzahl s wird auch mit $n_M(V)$ bezeichnet.)*

Beweis: a) Sei $\varphi \in End_A(V)$ und sei W ein zu M isomorpher Untermodul von V. Dann ist $\varphi(W) \cong_A W \cong_A M$, da φ ein mit der Operation von A vertäglicher Homomorphismus ist. Also gilt $\varphi(W) \subseteq M(V)$ und so $\varphi(M(V)) \subseteq M(V)$.
a) Sei $U = V_1 \oplus \ldots \oplus V_s$. Per Definition gilt dann $U \subseteq M(V)$. Sei W ein zu M isomorpher Untermodul von V. Es ist zu zeigen, daß $W \subseteq U$ gilt. Sei π_i die Projektion von V auf V_i. Falls $\pi_i(W) \neq 0$ gilt, dann gilt $\pi_i(W) = V_i$ und daher $W \cong_A V_i$. Also folgt $\pi_i(W) \subseteq U$ für alle $i \in \{1, \ldots, r\}$. Damit gilt nun $W \subseteq \sum_{i=1}^{r} \pi_i(W) \subseteq U$.
b) Es gilt $Dim(V_i) = Dim(M)$ für $1 \leq i \leq s$ und damit nach b) $s = Dim(M(V))/Dim(M)$. •

Damit “kennt” man einen vollständig reduziblen Modul also dann, wenn man seine irreduziblen Teilmoduln bis auf Isomorphie kennt und ihre Vielfachheit $n_M(V)$, mit der sie in dem Modul V auftreten.
Der Satz von Wedderburn beschäftigt sich nun mit den irreduziblen Moduln im regulären Modul einer Algebra. Wir zeigen den Satz von Wedderburn in einer Sequenz von Sätzen.

2.9. Satz: (Wedderburn I)
Sei A eine halbeinfache Algebra und sei M ein irreduzibler A-Modul. Dann ist $M(A)$ ein Ideal von A.

Beweis: Sei $a \in A$ und sei $\theta_a : A \to A : b \mapsto ab$. Dann ist $\theta_a \in End_A(A)$, denn θ_a ist linear und für $c \in A$ gilt $\theta_a(bc) = abc = \theta_a(b)c$. Da $M(A)$ ein $End_A(A)$-Modul ist, ist $M(A)$ invariant unter der Operation von $End_A(A)$. Daher folgt $aM(A) = \theta_a(M(A)) \subseteq M(A)$ und $M(A)$ ist ein Linksideal von A. Da $M(A)$ ein Untermodul von A ist, ist es auch ein Rechtsideal und daher ein Ideal. •

Sei nun $\mathcal{M}(A)$ die Menge der irreduziblen A (bis auf Isomorphie). Wir wollen diese Menge genauer studieren. Der reguläre Modul ist dabei ein Schlüssel zu dieser Untersuchung. Wir wissen schon, daß

$$A = \bigoplus_{M \in \mathcal{M}(A)} M(A)$$

gilt, denn A ist die direkte Summe von irreduziblen Untermoduln und jeder direkte Summand gehört zu genau einem $M(A)$. Es ist nun also von Interesse, die Menge $\mathcal{M}(A)$ sowie jede homogene Komponente $M(A)$ genauer zu studieren.

2.10. Satz: (Wedderburn II)
Sei A eine halbeinfache Algebra und sei M ein irreduzibler A-Modul. Sei $A \to End(M) : a \mapsto a_M$ der zugehörige Homomorphimus mit Bild A_M.

- *Sei W ein irreduzibler A-Modul mit $W \not\cong_A M$. Dann gilt $Wa = 0$ für alle $a \in M(A)$. (Man sagt: W wird von $M(A)$ annihiliert.)*
- *$M(A) \cong A_M$.*

Beweis: a) Es gilt $W(A) \cap M(A) = 0$. Da $W(A)$ und $M(A)$ Ideale sind in A, folgt nun $W(A)M(A) \leq W(A) \cap M(A) = 0$. Nun hat A einen Untermodul U mit $U \cong_A W$. Es gilt

$U \subseteq W(A)$ und U wird von $M(A)$ annihiliert. Damit wird auch W von A annihiliert.
b) Es gilt $A = \oplus_{N \in \mathcal{M}(A)} N(A) = B \oplus M(A)$. Nach a) liegt B im Kern des Homomorphismus $A \to End(M)$. Also ist $M(A) \to A_M$ noch surjektiv. Es bleibt zu zeigen, daß dieser Homomorphismus auch injektiv ist. Sei a ein Element im Kern des Homomorphismus. Dann gilt $Ba = 0$ nach a) und es gilt $Ma = 0$. Also folgt $Aa = 0$. Daraus folgt nun für die 1 in A die Gleichung $a = 1a = 0$ und damit ist der Homomorphismus injektiv. •

2.11. Satz: (Wedderburn III)
Sei A eine halbeinfache Algebra und sei $\mathcal{M}(A)$ die Menge der irreduziblen A-Moduln (bis auf Isomorphie).

- *$A = \sum_{M \in \mathcal{M}(A)} M(A)$ ist eine direkte Zerlegung in minimale Ideale von A.*
- *Die Menge $\mathcal{M}(A)$ ist endlich und es gilt $Dim(A) = \sum_{M \in \mathcal{M}(A)} Dim(M(A))$.*

Beweis: a) Es ist nur zu zeigen, daß $M(A)$ ein minimales Ideal in A ist. Sei $0 < I < M(A)$ ein Ideal in A. Das Ideal $M(A)$ ist die Summe von irreduziblen Teilmoduln von A, die alle isomorph sind zu M. Also ist auch I von dieser Sorte. Da $I < M(A)$, gilt es einen irreduziblen Teilmodul W von A mit $W \cong_A M$ und $W \cap I = 0$. Daraus folgt $IW \subseteq I \cap W = 0$ und damit annihiliert I den Modul W. Nach dem Satz von Wedderburn II folgt dann $I = 0$.
b) Es gilt $M(A) \neq 0$ für jedes $M \in \mathcal{M}(A)$ und damit folgt b) sofort. •

Damit bekommt man nun also schon einen ganz guten Überblick über die irreduziblen Moduln, die eine Algebra überhaupt haben kann. Diese Menge $\mathcal{M}(A)$ wird später noch genauer analysiert werden und wir werden feststellen, daß man noch viel mehr sagen kann.

2.4 Der Doppelzentralisatorsatz

Der Doppelzentralisatorsatz sieht zunächst sehr technisch aus, hat aber viele Konsequenzen. Seinen Beweis wollen wir hier überspringen.

2.12. Satz: (Doppelzentralisatorsatz)
Sei A eine halbeinfache Algebra und sei M ein irreduzibler A-Modul. Dann gilt für die "doppelten Endomorphismen" $End_{End_A(M)}(M) = A_M$.

Dieser Satz schränkt die Möglichkeiten für Endomorphismen reichlich ein. Insbesondere für algebraisch abgeschlossene Körper kann man damit viel erreichen wie der folgende Satz zeigt.

2.13. Satz: *Sei A eine halbeinfache K-Algebra und sei K algebraisch abgeschlossen. Sei $\mathcal{M}(A)$ die Menge der irreduziblen A-Moduln und $M \in \mathcal{M}(A)$.*

- *$A_M = End(M)$.*
- *$Dim(A_M) = Dim(M(A)) = Dim(M)^2$.*
- *$n_M(A) = Dim(M)$.*
- *$Dim(A) = \sum_{M \in \mathcal{M}(A)} Dim(M)^2$.*

Beweis: a) Es gilt $End_A(M) = Kid$ und damit $A_M = End_{End_A(M)} = End(M)$.
b) $Dim(A_M) = Dim(M(A)) = Dim(End(M)) = Dim(M)^2$ nach a).
c) $n_M(A) = Dim(M(A))/Dim(M) = Dim(M)$ nach b).
d) $Dim(A) = \sum_{M \in \mathcal{M}(A)} Dim(M(A)) = \sum_{M \in \mathcal{M}(A)} Dim(M)^2$. •

Es fehlt nun noch eine Idee, wie man die Anzahl der irreduziblen A-Moduln bestimmt. Dazu diehnt der folgende Satz.

2.14. Satz: *Sei A eine halbeinfache K-Algebra und sei K algebraisch abgeschlossen. Dann gilt $Dim(Z(A)) = |\mathcal{M}(A)|$.*

Beweis: Es gilt $Z(M(A)) \cong Z(A_M) = A_M \cap End_A(M) = A_M \cap Kid = Kid$ für jedes $M \in \mathcal{M}(A)$. Daraus folgt $Dim(Z(M(A)) = 1$ und somit $\sum_{M \in \mathcal{M}(A)} Z(M(A)) = |\mathcal{M}(A)|$. Weiter gilt sicher $\sum_{M \in \mathcal{M}(A)} Z(M(A)) \subseteq Z(A)$. Sei $a \in Z(A)$ und schreibe $a = \sum_{M \in \mathcal{M}(A)} a_M$. Sei $u \in M(A)$. Dann gilt $ua_M = ua = au = a_M u$, da die verschiedenen Komponenten von A sich gegenseitig annihilieren. Also ist $a_M \in Z(M(A))$ und damit $a \in Z(A)$. Damit folgt die Behauptung. •

Kapitel 3

Darstellungen und Charaktere

In diesem Kapitel wird eine elementare Einführung über Darstellungen von Gruppen und Algebren gegeben.

3.1 Darstellungen von Algebren

3.1. Definition: Sei A eine K-Algebra und sei $\varphi : A \to M_n(K)$ ein Algebrenhomomorphismus. Dann heißt φ eine Darstellung von A. Die Zahl n heißt die Dimension von φ.

Schlußendlich sind Darstellungen nichts anderes als Moduln, wenn man so möchte. Denn wenn V ein A-Modul ist, dann ist V ein Vektorraum einer Dimension n und somit kann man V mit K^n identifizieren (wobei man eine explizite Basis von V wählen muß). Damit ist eine Darstellung nichts anderes als ein Algebrahomomorphismus $A \to Hom(V, V) = M_n(K)$.
Andererseits, wenn eine Darstellung φ von A gegeben ist, dann wird $V = K^n$ damit zum A-Modul. Also entsprechen sich Darstellungen und Moduln genau, man muß nur alle Aussagen für abstrakte Moduln in die konkrete Welt der Matrizen übersetzen. Zunächst wollen wir dabei untersuchen, was Isomorphie von Moduln für die Darstellungen bedeutet.

3.2. Definition: Zwei Darstellungen φ und σ einer Algebra A heißen ähnlich, wenn es eine invertierbare Matrix $P \in GL(n, K)$ gibt mit der Eigenschaft, daß $P^{-1}\sigma(a)P = \varphi(a)$ für alle $a \in A$ gilt.

3.3. Lemma: *Zwei Darstellungen φ und σ sind genau dann ähnlich, wenn die zugehörigen Moduln M und N isomorph sind.*

Beweis: Nachrechnen. •

3.4. Bemerkung: Sei V ein A-Modul und seien $\mathcal{B}_1$ und $\mathcal{B}_2$ zwei Basen für V. Dann sind die Darstellungen von A auf V bezüglich dieser beider Basen ähnlich.

Was bedeuten Untermoduln, Faktormoduln und vollständig reduzible Moduln für die Matrixdarstellung von A?

3.5. Bemerkung: Sei V ein A-Modul und sei W ein Teilmodul von V. Wähle eine Basis von V durch W. Dann hat die Darstellung von A bezüglich dieser Basis eine Gestalt

$$A \mapsto \begin{pmatrix} A_{V/W} & \nu(A) \\ 0 & A_W \end{pmatrix}.$$

Unter- und Faktormoduln werden also bei geschickter Basiswahl öffentlich gemacht.

3.6. Bemerkung: Sei $V = U \oplus W$ als A-Modul. Wähle eine Basis von V, die aus einer Basis für U und einer Basis aus W besteht. Dann hat die Darstellung von A bezüglich dieser Basis die Gestalt

$$A \mapsto \begin{pmatrix} A_U & 0 \\ 0 & A_W \end{pmatrix}.$$

Vollständig reduzible Moduln haben also Darstellungen, die in sogenannte Blöcke zerfallen.

3.2 Darstellungen von Gruppen

Sei G eine endliche Gruppe und K ein Körper. Sei $\varphi : K[G] \to M_n(K)$ eine Darstellung der Gruppenalgebra von G über K. Die Elemente von G können in $K[G]$ eingebettet werden und wir bekommen damit eine Abbildung $\varphi : G \to M_n(K)$. Eine einfache Rechnung zeigt, daß die Bilder dieser Abbildung invertierbar sind.

3.7. Bemerkung: Die Abbildung $\varphi : G \to M_n(K)$ ist ein Gruppenhomomorphismus und die Bilder von G sind invertierbar, denn $\varphi(1) = I_n$.

Damit können wir das folgende definieren.

3.8. Definition: Eine Darstellung von G ist ein Homomorphismus $\varphi : G \to GL(n, K)$.

Die Darstellungen einer Gruppe G entsprechen also genau den Darstellungen von $K[G]$. Wir werden diese beiden Darstellungen nicht genauer unterscheiden.

3.9. Lemma: *Sei G eine endliche Gruppe und N ein Normalteiler von G. Dann entsprechen die Darstellungen von G/N genau den Darstellungen φ von G mit $N \leq Kern(\varphi)$.*

Beweis: Elementar. •

3.3 Charaktere von Darstellungen

Ein Ziel der Darstellungstheorie ist es, „alle“ Darstellungen von einer gegebenen endlichen Gruppe G zu verstehen. Aber ähnliche Darstellungen sollen dabei eigentlich nicht unterschieden werden, denn die gehören ja zu isomorphen Moduln. Eine Abhilfe für dieses Problem schaffen die Charaktere.

3.10. Definition: Sei $\varphi : G \to GL(n, K)$ eine Darstellung von G. Dann ist $\chi : G \to K : g \mapsto Spur(\varphi(g))$ der zugehörige Charakter.

Man kann den Charakter auch als Funktion der Gruppenalgebra $K[G]$ auffassen. Aber meistens wird hier wirklich nur die Gruppe betrachtet.

3.11. Bemerkung: Vorsicht: Ein Charakter ist kein Homomorphismus, sondern nur eine Abbildung!

Zunächst ein Lemma mit einer wesentlichen Aussage über Charaktere.

3.12. Lemma: *Zwei ähnliche Darstellungen von G haben den gleichen Charakter.*

Beweis: Seien $\varphi, \sigma : G \to GL(n, K)$ und sei $P \in GL(n, K)$ mit $\varphi(g) = P^{-1}\sigma(g)P$ für alle $g \in G$. Dann gilt $Spur(\varphi(g)) = Spur(P^{-1}\sigma(g)P) = Spur(\sigma(g))$ und die Charaktere sind gleich. •

Charaktere haben also die gewünschte Eigenschaft: sie unterscheiden nicht zwischen ähnlichen Darstellungen. Man kann mit dem gleichen Beweis noch mehr einsehen.

3.13. Lemma: *Sei χ ein Charakter von G. Dann gilt $\chi(g) = \chi(h)$, wenn g und h in G konjugiert sind. (D.h. es gibt ein $k \in G$ mit $g^k = k^{-1}gk = h$.)*

Hier spielen nun die Konjugiertenklassen der Gruppe G eine große Rolle. Konjugiertheit definiert eine Äquivalenzrelation auf der Menge der Elemente von G und die Konjugiertenklassen sind die zugehörigen Äquivalenzklassen. Das obige Lemma sagt nun, daß jeder Charakter von G auf den Äquivalenzklassen konstant ist. Damit braucht man die Werte eines Charakters also nur auf den Klassen anzugeben, um den Charakter vollständig zu beschreiben.

3.14. Lemma: *Sei χ ein Charakter von G zur Darstellung $\varphi : G \to GL(n, K)$.*

- *$\chi(1) = n$. Man kann die Dimension der Darstellung also aus dem Charakter ablesen, zumindest wenn $Char(K) = 0$ gilt.*
- *Falls $n = 1$ ist, dann gilt $\varphi : G \to GL(1, K)$ und $\chi(g) = Spur(\varphi(g))$ kann mit φ identifiziert werden.*

Beweis: Beides ist elemenar. •

3.15. Definition: Ein Charakter zu einer 1-dimensionalen Darstellung heißt linearer Charakter.

Ein linearer Charakter ist tatsächlich ein Homomorphismus.

Kapitel 4

Klassische Darstellungstheorie

In diesem Kapitel untersuchen wir den Fall $K = \mathbb{C}$. Nach dem Satz von Maschke sind alle Darstellungen vollständig reduzibel in diesem Fall. Sei $\mathcal{M}(G) = \mathcal{M}(\mathbb{C}[G])$ die Menge der irreduziblen Moduln von G oder von $\mathbb{C}[G]$ in diesem Fall. Da $\mathbb{C}$ algebraisch abgeschlossen ist, gilt die Folgerung aus dem Doppelzentralisatorsatz:

$$|G| = Dim(\mathbb{C}[G]) = \sum_{M \in \mathcal{M}(G)} Dim(M)^2.$$

4.1 Eigenschaften von Charakteren

Zunächst legen wir einige Notation fest, die für den Rest des Kapitels gelten soll.

4.1. Definition:

- Sei $\mathcal{M}(G) = \{M_1, \ldots, M_k\}$.
- Sei $\varphi_i : G \to GL(n_i, \mathbb{C})$ eine Darstellung zu M_i.
- Sei χ_i der Charakter zu φ.

Dann hängt χ_i nur von M_i, aber nicht von φ_i ab. Also bekommen wir eine Menge $Irr(G) = \{\chi_1, \ldots, \chi_k\}$ irreduzibler Charaktere von G.

4.2. Lemma:

- *Jede nicht-triviale Linearkombination $\chi = \sum_{i=1}^k n_i \chi_i$ mit $n_i \in \mathbb{N}_0$, ist wieder ein Charakter von G.*
- *Jeder Charakter von G ist von der Form $\sum_{i=1}^k n_i \chi_i$, wobei $n_i \in \mathbb{N}_0$ gilt.*

Beweis: a) Sei $M = M_1^{n_1} \oplus \ldots \oplus M_r^{n_k}$. Dann hat die Darstellung von G auf M den Charakter χ.
b) Sei M ein beliebiger Modul. Dann ist M vollständig reduzibel und daher eine direkte Summe von irreduziblen. Also ist M von der Form $M = M_1^{n_1} \oplus \ldots \oplus M_r^{n_k}$. •

4.3. Lemma: *Es gilt* $|G| = \sum_{i=1}^{k} \chi_i(1)^2$.

Beweis: Das folgt nun sofort aus dem Doppelzentralisatorsatz. •

Wie kann man k bestimmen, ohne die Darstellungen zu kennen? Das ist erstaunlich einfach, wie der folgende Satz zeigt.

4.4. Satz: *Seien* $\mathcal{K}_1, \ldots, \mathcal{K}_l$ *die Konjugiertenklassen von* G *und sei* $K_i = \sum_{g \in \mathcal{K}_i} g \in \mathbb{C}[G]$ *die Klassensumme.*

- $K_1, \ldots, K_l$ *ist eine Basis von* $Z(\mathbb{C}[G])$.
- $k = l$, *d.h. die Anzahl der irreduziblen Charaktere und die Anzahl der Konjugiertenklassen stimmen überein.*

Beweis: a) Sicher gilt $K_i \in Z(\mathbb{C}[G])$ und außerdem sind die K_i linear unabhängig. Wir müssen also nur zeigen, daß sie das Zentrum der Gruppenalgebra erzeugen. Sei $a \in Z(\mathbb{C}[g])$ und schreibe $a = \sum a_g g$. Dann gilt für $h \in G$ die Gleichung $\sum a_g g = a = a^h = \sum a_g g^h$. Damit folgt $a_{g^h} = a_g$ für alle $g \in G$. Also sind die Koeffizienten von a konstant auf Konjugiertenklassen von G. Daher kann man a als Linearkombination der K_i schreiben.
b) Das folgt nun sofort, da $k = |\mathcal{M}(G)| = Dim(Z(\mathbb{C}[G])) = l$. •

Man kann also die Anzahl der irreduziblen Darstellungen von G aus der Anzahl der Konjugiertenklassen von G ablesen! Man kann sogar noch etwas mehr aus den Konjugiertenklassensummen ablesen.

4.5. Lemma: *Sei* $K_i K_j = \sum a_{ijv} K_v$. *Dann sind die Multiplikationskonstanten* $a_{ijv} \in \mathbb{N}_0$.

Beweis: Sei $g \in \mathcal{K}_v$. Dann ist a_{ijv} der Koeffizient von g in $K_i K_j$. Es gilt $a_{ijv} = |\{(x, y) \mid x \in \mathcal{K}_i, y \in \mathcal{K}_j, xy = g\}|$. Diese Anzahl liegt sicher in $\mathbb{N}_0$. •

4.6. Lemma: *Eine Gruppe ist abelsch genau dann, wenn jeder irreduzible Charakter linear ist.*

Beweis: Wenn G abelsch ist, dann ist $k = |G|$. Andererseits gilt $|G| = \sum_{i=1}^{k} \chi_i(1)^2$ und damit folgt $\chi_i(1) = 1$ für alle i. Damit sind alle Charaktere linear. Die Umkehrung gilt analog. •

4.7. Lemma: *Die Charaktere* $\chi_1, \ldots, \chi_k$ *sind alle verschieden.*

Beweis: Sei $\mathbb{C}[G] = \oplus M_i(\mathbb{C}[G])$ und sei $1 = \sum e_i$ eine Zerlegung der 1 in die direkten Summanden. Dann gilt $e_j M_i = 0$ falls $i \neq j$. Also ist $\varphi_i(e_j) = 0$ and $\chi_i(e_j) = 0$ falls $i \neq j$. Weiter gilt $\chi_i(e_i) = \chi_i(1) \neq 0$. Also sind alle χ_i verschieden als Abbildungen von $\mathbb{C}[G]$. Da G eine Basis von $\mathbb{C}[G]$ ist, sind sie damit auch verschieden als Abbildungen von G. •

Damit können wir jetzt schon die Grade der irreduziblen Darstellungen für kleine Gruppen bestimmen.

4.8. Beispiel: Sei $G = S_3$ die symmetrische Gruppe.

- Dann ist $|G| = 6$ und G hat 3 Konjugiertenklassen. Also gibt es drei irreduzible Charaktere χ_1, χ_2 und χ_3. Es folgt
$$6 = |G| = \chi_1(1)^2 + \chi_2(1)^2 + \chi_3(1)^2.$$
Damit müssen die Grade der Charaktere $1, 1$ und 2 sein.
- χ_1 ist der triviale Charakter $\chi_1(g) = 1$ für alle $g \in G$.
- χ_2 und χ_3 können wir im Moment noch nicht komplett berechnen.

4.2 Klassenfunktionen

Man kann von den Charakteren ausgehend noch ein wenig verallgemeinern.

4.9. Definition: Eine Abbildung $\nu : G \to \mathbb{C}$ heißt eine Klassenfunktion, wenn ν konstant ist auf den Konjugiertenklassen von G.

Damit ist jeder Charakter eine Klassenfunktion.

4.10. Satz:

- *Jede Klassenfunktion ν von G kann eindeutig in der Form $\nu = \sum_{i=1}^{k} n_i \chi_i$ darstellt werden, wobei $n_i \in \mathbb{Z}$ gilt.*
- *Eine Klassenfunktion ist genau dann ein Charakter, wenn $n_i \in \mathbb{N}_0$ gilt und nicht alle $n_i = 0$ sind.*

Beweis: a) Die Menge aller Klassenfunktionen ist ein Vektorraum über $\mathbb{C}$. Seine Dimension ist die Menge alle Konjugiertenklassen von G. Wir zeigen, daß $\chi_1, \dots, \chi_k$ eine Basis dafür ist. Da k die Dimension des Vektorraumes ist, reicht es dafür zu zeigen, daß diese Funktionen linear unabhängig sind. Das folgt aber analog zu der Aussage, daß die Konjugiertenklassensummen eine Basis von $Z(\mathbb{C}[G])$ sind, durch Evaluation der e_i. •

4.11. Definition: Wenn χ ein Charakter ist und $\chi = \sum_{i=1}^{k} n_i \chi_i$ gilt, dann heißen diejenigen χ_i mit $n_i \neq 0$ die Konstituenten von χ.

4.12. Satz: *Zwei Darstellungen φ und σ haben genau dann den gleichen Charakter, wenn die beiden Darstellungen ähnlich sind.*

Beweis: Wenn zwei Darstellungen ähnlich sind, dann haben sie den gleichen Charakter. Wir zeigen die umgekehrte Richtung. Seien V und W Moduln zu den zwei Darstellungen. Dann hat V den Charakter $\sum n_{M_i}(V)\chi_i$ und W hat den Charakter $\sum n_{M_i}(W)\chi_i$. Wenn diese beiden Charaktere gleich sind, dann gilt $n_{M_i}(W) = n_{M_i}(V)$. Damit sind aber schon V und W isomorph. •

4.3 Charaktertafeln

Die Menge aller irreduziblen Charaktere wird auch oft mit $Irr(G)$ bezeichnet. Eine Charaktertafel ist eine Tabelle, die die Abbildungen in $Irr(G)$ beschreibt.

4.13. Definition: Ist G eine endliche Gruppe und $Irr(G) = \{\chi_1, \ldots, \chi_k\}$ die Menge der irreduziblen Charaktere von G, so ist die Charaktertafel von G eine $k \times k$-Matrix mit den Einträgen $(\chi_i(g_j))_{i,j\in\{1,\ldots,k\}}$, wobei $g_i \in \mathcal{K}_i$ ist.

4.14. Beispiel: Die Charaktertafel der symmetrischen Gruppe S_3 lautet

$\lvert\mathcal{K}_i\rvert$	1	3	2
g_i	()	$(1,2)$	$(1,2,3)$
χ_1	1	1	1
χ_2	1	-1	1
χ_3	2	0	-1

Im weiteren wird den folgenden Fragen nachgegangen: Wie ermittelt man eine Charaktertafel? Kann man eine Charaktertafel vielleicht sogar algorithmisch bestimmen? Was kann man aus einer Charaktertafel an Eigenschaften der dargestellten Gruppe ablesen?
Mittlerweile gibt es einen Algorithmus von Dixon und Schneider, mit dem man Charaktertafeln berechnen kann. Dieses Verfahren wird hier jedoch nicht dargestellt, da für die Untersuchung und für das Verständnis kleiner Gruppen besser ist, die begriffliche Theorie zu kennen und aus diesem Hintergrundwissen zu jeder Gruppe einzeln und „ad hoc“ Argumente für die Korrektheit einer Charaktertafel zusammenzustellen.

4.15. Bemerkung: In vielen Fällen ist $\chi_i(g) \in \mathbb{Z}$, aber nicht in allen. Allgemein gilt, daß $\chi_i(g)$ eine ganzalgebraische Zahl ist.

4.4 Die Orthogonalitätsrelationen

Mit den Ortogonalitätsrelationen wird eine (wenn nicht die wichtigste) Möglichkeit dargestellt, mit der man in vielen Fällen eine Charaktertafel ohne Algorithmus aufstellen kann. Für das weitere sei $A = \mathbb{C}[G]$ der reguläre $\mathbb{C}[G]$-Modul und ϱ der zugehörige Charakter.

4.16. Lemma: *Es gilt*

1. $\varrho(1) = |G|$.
2. $\varrho(g) = 0$ *für* $g \neq 1$.

Beweis: Man wähle G als Basis von A, und es sei $\sigma : G \to GL(n, \mathbb{C})$ die zugehörige Darstellung, wobei $n = |G|$ sei. Dann ist $\sigma(g_i) = (a_{ij})$ die Matrix, auf die $g_i \in G$ mit $i \in \{1, \ldots, n\}$ abgebildet wird. Dabei ist a_{ii} der Koeffizient von g_i in $g_i g$. Dann gilt

$$g_i g = \begin{cases} g_i & \text{für } g = 1 \\ g_k & \text{mit } k \neq i \text{ für } g \neq 1 \end{cases}$$

Also ist

$$\varrho(g) = \sum_{i=1}^{n} a_{ii} = \begin{cases} |G| & \text{für } g = 1 \\ 0 & \text{für } g \neq 1 \end{cases}$$

•

4.17. Lemma: *Es ist*

$$\varrho = \sum_{i=1}^{k} \chi_i(1)\chi_i.$$

Beweis: Nach den Sätzen von Wedderburn ist $A = \bigoplus_{i=1}^{k} M_i(A)$ und $M_i(A)$ ist isomorph zur $dim(M_i)$-fachen, d. h. $\chi_i(1)$-fachen direkten Summe von M_i. •

Nach Wedderburn gibt es $e_1, \ldots, e_k$, die sogenannten zentral primitiven Idempotenten mit den Eigenschaften $1 = e_1 + \ldots + e_k$ und

$$e_i e_j = \begin{cases} 0 & \text{für } i \neq j \\ e_i & \text{für } i = j \end{cases},$$

da sich $M_i(A)$ und $M_j(A)$ für $i \neq j$ annihilieren. Nun kann Aussagen über die Werte von $e_1, \ldots, e_k$ machen.

4.18. Satz: *Für die zentral primitiven Idempotenten* $e_1, \ldots, e_k$ *gilt*

$$e_i = \frac{1}{|G|} \sum_{g \in G} \chi_i(1)\chi_i(g^{-1})g$$

Beweis: Wie für alle Elemente aus $\mathbb{C}[G]$ gibt $a_g \in \mathbb{C}$ mit $e_i = \sum_{g \in G} a_g g$. Dann ist

$$\varrho(e_i g^{-1}) = \varrho\left(a_h h g^{-1}\right) = a_g |G|.$$

Weiterhin ist

$$a_g |G| = \sum_{j=1}^{k} \chi_k(1)\chi_j(e_i g^{-1}).$$

Nun sei ϕ_j eine Darstellung zu χ_j. Dann ist

$$\phi_j(e_i g^{-1}) = \phi_j(e_i)\phi_j(g^{-1}) = \begin{cases} 0 & \text{für } i \neq j \\ \phi_j(g^{-1}) & \text{für } i = j \end{cases}.$$

Daher ist

$$\chi_j(e_i g^{-1}) = \begin{cases} 0 & \text{für } i \neq j \\ \chi_j(g^{-1}) & \text{für } i = j \end{cases}$$

Insgesamt erhält man $a_g = \frac{1}{|G|}\sum_{g\in G}\chi_i(1)\chi_i(g^{-1})$ und damit die Aussage. •

4.19. Satz: *(Verallgemeinerte Orthogonalitätsrelation) Es gilt*

$$\frac{1}{|G|}\sum_{g\in G}\chi_i(gh)\chi_j(g^{-1}) = \delta_{ij}\frac{\chi_i(h)}{\chi_i(1)},$$

wobei δ das Kroneckerdelta ist.

Beweis: Aus den Sätzen von Wedderburn ist bekannt, daß für die tentral primitiven Idempotenten $e_1, \ldots, e_k$ gerade $e_i e_j = \delta_{ij} e_i$ gilt. Nach 4.18 läßt sich diese Beziehung genauer aufschlüsseln:

$$\frac{1}{|G|^2}\sum_{g,k\in G}\chi_i(1)\chi_i(k^{-1})k\chi_j(1)\chi_j(g^{-1})g = \delta_{ij}\frac{1}{|G|}\sum_{g\in G}\chi_i(1)\chi_i(g^{-1})g$$

Durch Koeffizientenvergleich für $gk = h$ erhält man aus der rechten Seite $\delta_{ij}\chi_i(1)\chi(h^{-1})$ als Koeffizienten und damit die Gleichung

$$\frac{1}{|G|}\sum_{g\in G}\chi_i(1)\chi_j(1)\chi_i(hg^{-1})^{-1}\chi_j(g^{-1}) = \frac{\chi_i(1)\chi_j(1)}{|G|}\sum_{g\in G}\chi_i(gh^{-1})\chi_i(g^{-1}).$$

Ersetzt man nun h durch h^{-1}, so erhält man die Behauptung. •

4.20. Lemma: *Es sei φ eine Darstellung von G mit Charakter χ und $g \in G$ mit $o = |g|$. Dann gilt*

1. *$\varphi(g)$ ist ähnlich zu einer Diagonalmatrix D mit den Diagonaleinträgen $\varepsilon_1, \ldots, \varepsilon_n$, die den folgenden Eigenschaften genügen.*
2. *Für jedes i mit $1 \leq i \leq n$ gilt $\varepsilon_i^o = 1$.*
3. *Es ist $\chi(g) = \varepsilon_1 + \ldots + \varepsilon_n$ und $|\chi(g)| \leq \chi(1)$.*
4. *Es ist $\chi(g^{-1}) = \overline{\chi(g)}$.*

Damit sind Charakterwerte Summen von Einheitswurzel, deren Ordnung die Ordnung des abgebildeten Elementes teilt.

Beweis: Teil 1 ist aus der linearen Algebra bekannt. Der zweite Teil ergibt sich folgendermaßen: Es ist $\varphi(g)^o = \varphi(g^o) = \varphi(1) = E$, wobei E die Einheitsmatrix ist. Drittens ist $\chi(g) = Spur(D) = \varepsilon_1 + \dots \varepsilon_n$ und nach dem zweiten Teil $|\varepsilon_i| = 1$. Daher ist $|\chi(g)| = |\varepsilon_1 + \dots + \varepsilon_n| \leq |\varepsilon_1| + \dots + |\varepsilon_n| = n = \chi(1)$. Viertens ist $\overline{\varepsilon_i} = \varepsilon_i^{-1}$, da ε_i eine Einheitswurzel ist. Also ist $\chi(g^{-1}) = Spur(D^{-1}) = \varepsilon_1^{-1} + \dots + \varepsilon_n^{-1} = \overline{\varepsilon_1} + \dots + \overline{\varepsilon_n} = \overline{\varepsilon_1 + \dots + \varepsilon_n} = \overline{\chi(g)}$. •

4.21. Satz: *(1. Orthogonalitätsrelation) Es gilt*

$$\frac{1}{|G|} \sum_{g \in G} \chi_i(g) \overline{\chi_j(g)} = \delta_{ij}.$$

Beweis: Man wähle $h = 1$ im vorangegangenem Lemma und im Satz über die verallgemeinerte Orthogonalitätsrelation. •

4.22. Bemerkung: Es gilt

$$\frac{1}{|G|} \sum_{a=1}^{k} |\mathcal{K}_a| \chi_i(g_a) \overline{\chi_j(g_a)} = \sum_{a=1}^{k} \frac{1}{|C_G(g_a)|} \chi_i(g_a) \overline{\chi_j(g_a)} = \delta_{ij}.$$

4.23. Definition: Es seien φ und σ zwei Klassenfunktionen von G. Dann ist

$$[\varphi, \sigma] = \frac{1}{|G|} \sum_{g \in G} \varphi(g) \overline{\sigma(g)}$$

das Skalarprodukt von φ und σ.

4.24. Bemerkung: Es gilt

1. $[\varphi, \sigma] = \overline{[\sigma, \varphi]}$.
2. $[\varphi, \varphi] = \frac{1}{|G|} \sum_{g \in G} \varphi(g)^2 > 0$ für $\varphi \neq 0$.
3. $[a_1\varphi_1 + a_2\varphi_2, \sigma] = a_1[\varphi_1, \sigma] + a_2[\varphi_2, \sigma]$.

Damit ist $Irr(G)$ eine Orthonormalbasis des Raumes der klassenfunktionen.

4.25. Folgerung: *Sind χ und ψ Charaktere, dann ist $[\chi, \psi] \in \mathbb{N}_0$, und χ ist genau dann irreduzibel, wenn $[\chi, \chi] = 1$ ist.*

4.26. Satz: *(2. Orthogonalitätsrelation) Es seien $g, h \in G$. Dann ist*

$$\sum_{\chi \in Irr(G)} \chi(g)\overline{\chi(h)} = \begin{cases} 0 & \text{für } \mathcal{K}_g \neq \mathcal{K}_h \\ |C_G(g)| = |C_G(h)| & \text{für } \mathcal{K}_g = \mathcal{K}_h \end{cases}$$

Beweis: Es seien $g_1, \ldots, g_k$ Repräsentanten der konjugiertenklassen von G und $X = ((\chi_i(g_j))$ eine Matrixdarstellung von $Irr(G)$ sowie $D = (\delta_{ij}|\mathcal{K}_i|)$ die Diagonalmatrix mit der Mächtigkeit der Konjugiertenklasse auf der Diagonalen. Nach der 1. Orthogonalitätsrelation ist dann

$$|G|\delta_{ij} = \sum_{g \in G} \chi_i(g)\overline{\chi_j(g)} = \sum_{v=1}^{k} |\mathcal{K}_v|\chi_i(g_v)\overline{\chi_j(g_v)}.$$

Diesem Gleichungssystem entspricht die Gleichung

$$|G|E = XD\overline{X}^T.$$

Da Diagonalmatrizen im Zentrum der Matrixgruppe liegen, ist $|G|E = (|G|E)^X = (XD\overline{X}^T)^X = X^{-1}XD\overline{X}^T X = D\overline{X}^T X$. Also ist

$$|G|\delta_{ij} = \sum_{v=1}^{k} |\mathcal{K}_i|\overline{\chi_v(g_i)}\chi_v(g_j).$$

Über $|G|/|\mathcal{K}_i| = |C_G(g_i)|$ ergibt sich die Behauptung. •

4.5 Kerne und Normalteiler

Während im vorangegangenen Abschnitt Methoden von Interesse waren, mit denen man charaktertaafeln ermitteln kann, so wird jetzt der Frage nachgegangen, welche Eigenschaften einer Gruppe man aus ihrer Charaktertafel ablesen kann. Es wird sich zeigen, daß man vollständigen Aufschluß über die Normalteilerstruktur der Gruppe erhält und damit auch über aller Eigenschaften der Gruppe, die über Normalteiler definiert sind – wie z. B. Einfachheit und Auflösbarkeit.

4.27. Lemma: *Ist φ eine darstellung von G mit Charakter χ, so ist $g \in G$ genau dann im Kern von φ enthalten, wenn $\chi(g) = \chi(1)$ ist.*

Beweis: Es sei $g \in Kern(\varphi)$. Dann ist $\varphi(g) = E_n$ und $\chi(g) = n = \chi(1)$. Es sei umgekehrt $\chi(g) = \chi(1) = n$. Da $n = \varepsilon_1 + \ldots + \varepsilon_n$ mit $|\varepsilon_1| = \ldots = |\varepsilon_n| = 1$ ist, ist $\varepsilon_1 = \ldots = \varepsilon_n = 1$. •

4.28. Definition: Es ist $Kern(\chi) = \{g \in G \mid \chi(g) = \chi(1)\}$.

Nach dem vorangegangenen Lemma ist $Kern(\chi) = Kern(\varphi)$.

4.29. Lemma: *Es sei φ ein Charakter von G mit $\chi = \sum_{i=1}^{k} n_i\chi_i$ für irreduzible Charaktere $\chi_1, \ldots, \chi_k$. Dann ist*

$$Kern(\chi) = \bigcap_{n_i>0} Kern(\chi_i) \quad \textit{und} \quad \bigcap_{i=1}^{k} Kern(\chi_i) = \{1\}$$

Beweis: Es ist $g \in Kern(\varphi)$ genau dann, wenn $\chi(g) = \chi(1) = \sum_{n_i>0} n_i\chi_i(g)$. Dann ist $|\chi_i(g)| \leq |\chi_i(1)|$ für alle i mit $1 \leq i \leq k$. Also ist $\chi_i(g) = \chi_i(1)$. In umgekehrte Inklusion besteht offensichtlich.
Es sei ϱ der reguläre Charakter. Es ist $Kern(\varrho) = \{1\}$ und $Kern(\varrho) = \bigcap_{i=1}^{k} Kern(\chi_i)$ nach dem ersten Teil. •

4.30. Lemma: *Jeder Normalteiler von G ist der Schnitt gewisser Kerne von $\chi_1, \ldots, \chi_k$.*

Beweis: Es sei $N \trianglelefteq G$ und $M = K[G/N]$ ein Modul für G per Multiplikation. Es sei φ die zugehörige Darstellung mit Charakter χ. Dann ist $Ker(\varphi) = N = Kern(\chi)$, und damit ist N nach dem vorangegangenen Lemma ein Schnitt gewisser Kerne von $\chi_1, \ldots, \chi_k$. •

Damit kann man jeden Normalteiler aus der Charaktertafel ablesen, indem man Vereinigungen der Konjugiertenklassen bildet, die ein Charakter auf denselben Wert wie 1 abbildet, und dann Schnitte dieser Vereinigungen betrachtet (da Normalteiler invariant unter Konjugation sind, enthalten sie Konjugiertenklassen ganz oder gar nicht und sind daher Vereinigungen dieser Klassen).

4.31. Folgerung: *Eine Gruppe G ist genau dann einfach, wenn die Kerne aller irreduziblen Charaktere von G gleich $\{1\}$ (und im Fall des trivialen Charaters gleich G) sind.*

4.32. Bemerkung: Die Ordnung des Kerns eines irreduziblen Charakters χ_i kann aus der Charaktertafel berechnet werden, denn es ist

$$|Kern(\chi_i)| = \sum_{\chi_i(g_j)=\chi_i(1)} |\mathcal{K}_j|.$$

4.33. Bemerkung: Da eine Gruppe genau dann auflösbar ist, wenn es eine Reihe $G_0 \triangleright G_1 \triangleright \ldots \triangleright G_l \triangleright G_{l+1}\{1\}$ mit $G_i \trianglelefteq G$ und $[G_i : G_{i+1}] = p_i^{e_i}$ für Primzahlen p_i gibt, kann man über die Auflösbarkeit einer Gruppe durch Aufsuchen einer solchen Reihe aus der Charaktertafel entscheiden, da nur eine vollständige Liste der Normalteiler und ihrer Ordnung benötigt wird.

Kennt man einen Normalteiler N von G und die irreduziblen Charaktere von G, kann man dann auf einfacher Weise daraus Rückschlüsse auf $Irr(N)$ und $Irr(G/N)$ ziehen? Es wird sich zeigen: Für $Irr(G/N)$ ist das möglich, für $Irr(N)$ im allgemeinen nicht.

4.34. Lemma: *Es sei $N \trianglelefteq G$. Dann gilt:*

1. *Es sei χ ein Charakter von G mit $N \leq Kern(\chi)$. Dann ist $\hat{\chi} : G/N \to \mathbb{C} : gN \mapsto \chi(g)$ ein Charakter von G/N. Ist χ irreduzibel, so auch $\hat{\chi}$.*
2. *Ist $\hat{\chi}$ ein Charakter von G/N, so ist $\chi : G \to \mathbb{C} : g \mapsto \hat{\chi}(gN)$ ein Charakter von G. Ist $\hat{\chi}$ irreduzibel, so auch χ.*

Oft werden χ und $\hat{\chi}$ identifiziert.

4.35. Lemma: *Es sei G eine Gruppe und G' die Kommutatorgruppe von G. Dann ist*

$$G' = \bigcap_{\chi_i(1)=1} Kern(\chi_i)$$

und $[G : G']$ ist die Anzahl der linearen irreduziblen Charaktere.

Damit kann auch G' aus der Charaktertafel abgelesen werden.

4.6 Das Zentrum eines Charakters

Als nächstes wird uns die Frage beschäftigen, ob man die Nilpotenz einer Gruppe aus ihrer Charaktertafel ablesen kann.

4.36. Definition: Es sei G eine Gruppe.

1. Die Menge $Z(G) = \{g \in G \mid gh = hg$ für alle $h \in G\}$ ist das Zentrum von G.
2. Die Reihe von Untergruppen $\{1\} = Z_0 \leq Z_1 < \ldots Z_c \leq G$, die durch die Bedingung $Z_{i+1}/Z_i = Z(G/Z_i)$ für alle i mit $0 \leq i \leq c$ definiert ist, ist die aufsteigende Zentralreihe von G.
3. Die Gruppe G ist genau dann nilpotent, wenn es ein $c \in \mathbb{N}_0$, so daß $Z_c = G$ ist.

4.37. Bemerkung: Ist G nilpotent, so ist G auch auflösbar. Ist G eine p-Gruppe, so gilt auch die Umkehrung.

Die Nilpotenz einer Gruppe kann offenbar dann aus ihrer Charaktertafel abgelesen, wenn man aus ihr das Zentrum der Gruppe erkennen. Indem man einen Zentrumsbegriff auch für Charaktere definiert, soll das Ablesen des Zentrums der Gruppe ermöglicht werden.

4.38. Definition: Ist χ ein Charakter einer Gruppe G, so ist $Z(\chi) = \{|\chi(g)| = \chi(1)\}$ das Zentrum von χ.

4.39. Bemerkung: Der Kern $Kern(\chi) = \{g \in G \mid \chi(g) = \chi(1)\}$ eines Charakters χ ist eine Untergruppe von $Z(\chi)$.

4.40. Definition: Es sei H eine Untergruppe von G und χ ein Charakter von G. Dann ist χ_H die Einschränkung von χ auf H.

4.41. Bemerkung: Ist χ ein Charakter von G und $H \leq G$, so ist auch χ_H ein Charakter von H. Ist χ_H irreduzibel über H, so ist auch χ irreduzibel über G. Die Umkehrung gilt hingegen nicht im allgemeinen.

4.42. Lemma: *Es sei χ ein Charakter zur Darstellung φ einer Gruppe G, und es sei $Z = Z(\chi)$ und $K = Kern(\chi)$ sowie $n = \chi(1)$.*

1. *Es ist $Z = \{g \in G \mid \text{Es gibt ein } \varepsilon \in \mathbb{C}, \text{ so daß } \varphi(g) = \varepsilon E_n \text{ ist}\}$. Insbesondere ist $Z \leq G$ und $Z/K \leq Z(G/K)$.*

2. *Es gibt einen linearen Charakter λ von Z, so daß $\chi_Z = n\lambda$ ist.*

3. *Die Faktorgruppe Z/K ist zyklisch.*

Beweis: Zum ersten Teil: Es sei $g \in Z$. Dann ist $\varphi(g)$ zu einer Diadonalmatrix D mit Diagonaleinträgen $\varepsilon_1, \ldots, \varepsilon_n$ ähnlich, so daß $\chi(g) = \varepsilon_1 + \ldots + \varepsilon_n$ ist und für alle i mit $1 \leq i \leq n$ die Bedingung $|\varepsilon_i| = 1$ erfüllt ist. Da $|\chi(g)| = n$ ist, gibt es ein $\varepsilon \in \mathbb{C}$ mit $\varepsilon_1 = \ldots \varepsilon_n = \varepsilon$. Also ist $\varphi(g) = D = \varepsilon E_n$, da Diagonalmatrizen nur zu sich selbst ähnlich sind. Daher ist $g \in \{h \in G \mid \text{Es gibt ein } \varepsilon \in \mathbb{C}, \text{ so daß } \varphi(h) = \varepsilon E_n \text{ ist}\}$. Nun sei umgekehrt $g \in G$ und $\varphi(g) = \varepsilon E_n$. Dann ist $\chi(g) = n\varepsilon$. Also ist $|\chi(g)| = |n\varepsilon| = n|\varepsilon| = n = \chi(1)$. Es ist $Z/K = G/K \cap \{aE_n \mid a \in \mathbb{C}\}$ mit $\varphi(Z) \cong Z/K$ und $G/K \cong \varphi(G)$. Also ist $Z/K \leq G/K$ und $Z \leq G$. Da Diagonalmatrizen mit allen anderen Matrizen vertauschen, ist $Z/K \leq Z(G/K)$.
Zum zweiten Teil: Für $g \in G$ ist dem ersten Teil zufolge $\varphi(g) = \varepsilon E_n$. Man definiere $\lambda : Z \to \mathbb{C} : g \mapsto \varepsilon$. Dann ist λ ein linearer Homomorphismus von Z nach $\mathbb{C}$, d.h. λ ist ein linearer Charakter. Ferner ist $\chi(g) = Spur(\varepsilon E_n) = \varepsilon n = n\lambda(g)$ für alle $g \in Z$.
Es ist $K = Kern(\lambda)$. Also ist $Z/K \cong Bild(\lambda)$, und $Bild(\lambda)$ ist eine endliche Untergruppe der multiplikativen Gruppe von $\mathbb{C}$. Da jede endlich Gruppe der multiplikativen Gruppe eines Körpers zyklisch ist, ist auch $Bild(\lambda)$ zyklisch. •

4.43. Lemma: *Es sei $\chi \in Irr(G)$ und $Z = Z(\chi)$ sowie $K = Kern(\chi)$. Dann ist $Z/K = Z(G/K)$.*

Beweis: Die Inklusion „$\subseteq$“ ist bereits im Beweis zu 4.42 gezeigt. Die umgekehrte ergibt sich folgendermaßen: Es sei $gk \in Z(G/K)$, d.h. $\varphi(g) \in Z(\varphi(G))$, wobei φ eine Darstellung zu χ ist. Nach dem Doppelzentralisatorsatz ist $\varphi(g) \in End_{\mathbb{C}[G]}(M)$, wobei M der Modul zur Darstellung von φ ist, und daher ist $End_{\mathbb{C}[G]}(M) = \mathbb{C} \cdot id$. Also ist $\varphi(g) \in \varphi(Z)$ und $gK \in Z/K$. •

4.44. Lemma: *Es ist*

$$Z(G) = \bigcap_{\chi \in Irr(G)} Z(\chi).$$

Beweis: Da $Z(G)Kern(\chi)/Kern(\chi) \leq Z(G/Kern(\chi)) = Z(\chi)/Kern(\chi)$ für $\chi \in Irr(G)$. Also ist auch $Z(G) \leq Z(G)Kern(\chi) = Z(\chi)$ für jeden irreduziblen Charakter χ.
Nun sei umgekehrt $g \in Z(\chi)$ für alle $\chi \in Irr(G)$. Dann ist $gKern(\chi) \in Z(G/Kern(\chi))$ für alle $\chi \in Irr(G)$. Dann gilt für alle $x \in G$, daß $[g,x] = g^{-1}x^{-1}gx \in Kern(\chi)$ für alle $\chi \in Irr(G)$ ist. Also ist $[g,x] = 1$, da $\bigcap_{\chi \in Irr(G)} Kern(\chi) = \{1\}$ ist. •

Damit läßt sich $Z(G)$ aus der Charaktertafel ablesen und ebenso in der folgenden Weise die Nilpotenz einer Gruppe:

1. Man bestimme $Z(G)$ aus der Charaktertafel von G.
2. Man bestimme $Z(G/Z(G))$ aus der Charaktertafel von $G/Z(G)$ und iteriere diesen Schritt.

4.45. Lemma: *Es sei H eine Untergruppe einer Gruppe G und χ ein Charakter von G. Dann ist $[\chi_H, \chi_H] \leq [G:H][\chi,\chi]$ und $[\chi_H,\chi_H] = [G:H][\chi,\chi]$ genau dann, wenn $\chi(g) = 0$ für alle $g \in G \backslash H$ ist.*

Beweis: Es ist

$$|H|[\chi_H, \chi_H] = \sum_{h \in H} |\chi(h)|^2 \leq \sum_{g \in G} |\chi(g)|^2 = |G|[\chi,\chi].$$

•

4.46. Lemma: *Es sei $\chi \in Irr(G)$. Dann ist $\chi(1)^2 \leq [G:Z(\chi)]$ und $\chi(1)^2 = [G:Z(\chi)]$ genau dann, wenn $\chi(g) = 0$ für alle $g \in G \backslash Z(\chi)$ ist.*

Beweis: Man wähle $H = Z(\chi)$ in 4.45. Dann ist $\chi_{Z(H)} = \chi(1)\lambda$ für einen linearen Charakter λ. Also ist $[\chi_{Z(H)}, \chi_{Z(H)}] = \chi(1)^2[\lambda,\lambda] = \chi(1)^2$, da λ irreduzibel ist. Weiterhin ist $[G:Z(G)][\chi,\chi] = [G:Z(\chi)]$, da χ ebenfalls irreduzibel ist. •

4.47. Definition: Ein Charakter χ ist treu, wenn $Kern(\chi) = \{1\}$ ist.

4.48. Satz:

1. *Hat die Gruppe G einen treuen und irreduziblen Charakter, dann ist $Z(G)$ zyklisch.*
2. *Ist G ein p-Gruppe und ist $Z(G)$ zyklisch, so hat G einen treuen und irreduziblen Charakter.*

Beweis: Zum ersten Teil: Es sei $\chi \in Irr(G)$ treu. Dann ist $Z(G) = Z(\chi)$ zyklisch, da $Z(\chi) \leq Kern(\chi) = \{1\}$ ist.
Zum zweiten Teil: Es sei G eine p-Gruppe mit zyklischem Zentrum. Dann gibt es genau einen Normalteiler $N \trianglelefteq G$ mit $|N| = p$ und $N \leq Z(G)$. Ist M ein beliebiger nichttrivialer Normalteiler von G, so ist nach der p-Gruppentheorie $N \leq M$. Es ist $\bigcap_{\chi \in Irr(G)} Kern(\chi) = \{1\}$, d.h. es gibt ein $\chi \in Irr(G)$ mit $N \not\leq Kern(\chi)$. Also ist $Kern(\chi) = \{1\}$. •

4.7 Produkte von Charakteren

Bisher ist bekannt: Sind χ und ψ Charaktere, so ist auch $\chi + \psi$ ein Charakter, und ebenso ist $M \oplus N$ ein Modul, wenn M und N Moduln sind. Nun soll gezeigt werden, daß auch das Produkt zweier Charaktere ein Charakter ist.

4.49. Definition: Es seien V und W zwei $\mathbb{C}[G]$-Moduln und $\{v_1, \ldots, v_l\}$ eine Basis von V und $\{w_1, \ldots, w_m\}$ eine Basis von W. Dann ist

$$V \otimes W = \left\{ \sum_{i=1}^{m} \sum_{j=1}^{l} a_{ij}(v_i \otimes w_j) \mid a_{ij} \in \mathbb{C} \right\}$$

ein Vektorraum der Dimension ml, wobei $v_i \otimes w_j$ formale, abstrakte Elemente sind. Weiterhin sei für $v = \sum_{i=1}^{l} a_i v_i \in V$ und $w = \sum_{j=1}^{m} b_j w_j \in W$

$$v \otimes w = \sum_{i=1}^{l} \sum_{j=1}^{m} a_i b_j (v_i \otimes w_j)$$

das Tensorprodukt von v mit w.

4.50. Lemma: *Sind V und W zwei G-Moduln, so ist $V \otimes W$ vermittels $(v \otimes w)g = vg \otimes wg$ ein G-Modul und vermittels*

$$x \left(\sum_{g \in G} a_g g \right) = \sum_{g \in G} a_g (xg)$$

für alle $x \in V \otimes W$ ein $\mathbb{C}[G]$-Modul.

Nicht für jedes $x \in V \otimes W$ gibt es ein $v \in V$ und ein $w \in W$, so daß $x = v \otimes w$ ist, und nicht für jedes $\alpha \in \mathbb{C}[G]$ gilt $(v \otimes w)\alpha = v\alpha \otimes w\alpha$. Führt man das Tensorprodukt in der Weise ein, wie es eben geschehen ist, so muß man sich davon überzeugen, daß diese Definition unabhängig von der Wahl einer Basis ist. Man kann auch über abstrakte Eigenschaften einführen (vgl. homologische Algebra).

4.51. Satz: *Es seien V und W zwei $\mathbb{C}[G]$-Moduln mit Charakteren χ und φ. Dann ist $V \otimes W$ ein $\mathbb{C}[G]$-Modul mit Charakter $\chi\varphi$ (unabhängig von der Basiswahl für V und W).*

Beweis: Es sei $\{v_1, \ldots, v_n\}$ eine Basis von V und $\{w_1, \ldots, w_m\}$ eine Basis von W und $g \in G$ mit $v_i g = \sum a_{ij} v_j$ und $w_r g = \sum b_{rs} w_s$. Dann ist $\chi(g) = a_{11} + \ldots + a_{nn}$ und $\varphi(g) = b_{11} + \ldots + b_{mm}$. Es sei δ der Charakter zu $V \otimes W$. Dann ist $(v_i \otimes w_r)g = (\sum a_{ij} v_j) \otimes (\sum b_{rs} w_s) = \sum_{j,s} b_{rs}(v_j \otimes w_s)$ und damit $\delta(g) = \sum_i a_{ii} \sum_r b_{rr} = \chi(g)\varphi(g)$. •

4.52. Folgerung: *Produkte von Charakteren sind ihrerseits Charaktere.*

4.53. Bemerkung: Es gilt

$$[\chi_1\psi, \chi_2] = \frac{1}{|G|}\sum_{g\in G}\chi_1(g)\psi(g)\chi_2(g) = [\chi_1, \overline{\psi}\chi_2].$$

4.54. Bemerkung: In der Regel sind Produkte irreduzibler Charaktere nicht unbedingt irreduzibel. Beispielsweise ist $[\chi\overline{\chi}, 1_G] = [\chi, \chi 1_G] = [\chi, \chi] = 1$. Daher ist 1_g ein Konstituent des Produktes $\chi\overline{\chi}$.

4.8 Induzierte Charaktere

Schränkt man einen Charakter auf eine Untergruppe ein, so erhält man einen Charakter dieser Untergruppe. Nun wird ein Weg angeben, wie man umgekehrt aus Charakteren einer Untergruppe Charaktere der gesamten Gruppe gewinnen kann.

4.55. Definition: Es sei H eine Untergruppe der Gruppe G und φ eine Klassenfunktion von H. Dann ist

$$\varphi^G : G \to \mathbb{C} : g \mapsto \frac{1}{|H|}\sum_{x\in G}\varphi^o(xgx^{-1})$$

die von φ induzierte Klassenfunktion, wobei

$$\varphi^o(h) = \begin{cases} \varphi(h) & \text{für } h \in H \\ 0 & \text{für } h \in G\backslash H \end{cases}$$

ist.

4.56. Bemerkung:

1. Die Abbildung φ^G ist eine Klassenfunktion von G.
2. Es ist $\varphi^G(1) = \frac{1}{|H|}\sum_{x\in G}\varphi^o(x1x^{-1}) = [G:H]\cdot\varphi(1)$.
3. Ist T eine Transversale von H in G, so ist
$$\varphi^G(g) = \sum_{t\in T}\varphi^o(tgt^{-1}).$$

4.57. Satz: *(Frobenius-Reziprozität) Es sei H eine Untergruppe von G sowie φ eine Klassenfunktion von H und ϑ eine von G. Dann ist $[\varphi, \vartheta_H] = [\varphi^G, \vartheta]$.*

Beweis: Es ist

$$[\varphi^G, \vartheta] = \frac{1}{|G|}\varphi^G(g)\overline{\vartheta(g)}$$

$$\begin{aligned}
&= \frac{1}{|G|}\sum_{g\in G}\left(\frac{1}{|H|}\sum_{x\in G}\varphi^o\left(xgx^{-1}\right)\right)\overline{\vartheta(g)} \\
&= \frac{1}{|G|}\frac{1}{|H|}\sum_{y\in G}\sum_{x\in G}\varphi^o(y)\overline{\vartheta(y)} \\
&= \frac{1}{|H|}\sum_{y\in G}\varphi^o(y)\overline{\vartheta(y)} \\
&= \frac{1}{|H|}\sum_{y\in H}\varphi^o(y)\overline{\vartheta(y)} \\
&= [\varphi, \vartheta_H]
\end{aligned}$$

•

4.58. Folgerung: *Es sei $H \leq G$ und φ ein Charakter von H. Dann ist φ^G ein Charakter von G.*

Beweis: Es sei $\chi \in Irr(G)$. Dann ist $[\varphi^G, \chi] = [\varphi, \chi_H]$ eine nichtnegative ganze Zahl. •

4.59. Bemerkung: Es sei $H \leq G$ und $\varphi \in Irr(H)$. Dann ist φ^G in der Regel nicht irreduzibel, aber es gibt ein $\chi \in Irr(G)$, so daß χ ein Konstituent von φ^G ist. Damit besteht die Möglichkeit, aus irreduziblen Charakteren von H irreduzible Charaktere von G zu konstruieren. Weiterhin ist φ ein Konstituent von χ_H.

4.60. Bemerkung: Es sei $H \leq G$ und φ ein nicht irreduzibler Charakter von H. Dann ist auch φ^G nicht irreduzibel.

Beweis: Es ist $(\varphi_1 + \varphi_2)^G = \varphi_1^G + \varphi_2^G$. •

4.61. Bemerkung: Es sei $H \leq G$ und φ ein Charakter von H sowie $g \in G$. Dann ist

$$\varphi^G(g) = |C_G(g)| \sum_{i=1}^{m} \frac{\varphi(x_i)}{C_H(x_i)},$$

wobei $x_1, \ldots, x_m$ Repräsentanten der Konjugationsklassen von H, enthalten in der Klasse von g in G, sind.

4.9 Normalteiler und Cliffordtheorie

Es sei $\chi \in Irr(G)$ und $H \leq G$. Über χ_H ist im allgemeinen sehr wenig bekannt. Wenn N allerdings ein Normalteiler von G ist, dann kann man durchaus mehr über χ_N sagen.

4.62. Definition: Ist N ein Normalteiler von G und χ ein Charakter von N sowie $g \in G$, so ist

$$\chi^g : N \to \mathbb{C} : h \mapsto \chi\left(ghg^{-1}\right)$$

der zu χ unter g konjugierte Charakter.

4.63. Bemerkung: Es ist $[\varphi^g, \vartheta^g] = [\varphi, \vartheta]$, wenn φ und ϑ Charaktere von $N \trianglelefteq G$ sind, und es ist $[\chi_H, \varphi^g] = [\chi_H, \varphi]$, wenn χ ein Charakter von G und φ einer von $N \trianglelefteq G$ ist.

4.64. Satz: *(Satz von Clifford) Es sei $N \trianglelefteq G$ und $\chi \in Irr(G)$ sowie $\vartheta \in Irr(N)$ ein Konstituent von χ_N, d.h. es ist $[\chi_N, \vartheta] \neq 0$. Weiterhin seien $\vartheta_1, \ldots, \vartheta_t$ die verschiedenen zu ϑ konjugierten Charaktere. Dann ist*

$$\chi_H = e(\vartheta_1 + \ldots + \vartheta_t),$$

wobei $e = [\chi_N, \vartheta]$ ist.

Beweis: Man berechne $(\vartheta^G)_N$. Es sei $h \in N$. Dann ist

$$\vartheta^G(h) = \frac{1}{|N|} \sum_{x \in G} \vartheta^o(xhx^{-1}) = \frac{1}{|N|} \sum_{x \in G} \vartheta^x(h).$$

Also ist $|N|\vartheta^G(h) = \sum_{g \in G} \vartheta^x(h)$. Es sei $\varphi \in Irr(G) \backslash \{\vartheta_1 \ldots \vartheta_t\}$. Dann ist $0 = [\varphi, \sum \vartheta^x] = [\varphi, (\vartheta^G)_N]$. Nach 4.57 ist $[\chi, \vartheta^G] = [\chi_N, \vartheta] \neq 0$. Daher ist $[\chi_N, \varphi] = 0$ Also sind die irreduziblen Konstituenten von χ_N unter $\vartheta_1, \ldots, \vartheta_t$ zu finden. Daher ist

$$\chi_N = \sum_{i=1}^{t} \underbrace{[\chi_N, \vartheta_i]}_{[\chi_N, \vartheta]} \vartheta_i = [\chi_N, \vartheta] \sum_{i=1}^{t} \vartheta_i.$$

•

4.65. Bemerkung: In der Charaktertheorie auflösbarer Gruppen versucht man, so dicht wie möglich an eine Umkehrung des Satzes von Clifford heranzukommen, um z.B. Charaktere auflösbarer Gruppen zu finden.

4.10 Eine Anwendung der Charaktertheorie: Der Satz von Burnside

Eines der Hauptanliegen bei der Entwicklung der Charaktertheorie war das Ziel, die endlichen, einfachen Gruppen zu klassifizieren. Um das Jahr 1950 herum waren etwa die folgenden wesentlichen Ergebnisse bekannt:

- Die abelschen, einfachen, endlichen Gruppen sind leicht zu klassifizieren: Es sind genau die zyklischen von Primzahlordnung. Daher waren im wesentlichen die nichtabelschen, einfachen, endlichen Gruppen gesucht.

- Schon länger waren (vor allem aus der Geometrie) unendliche Serien einfacher, endlicher Gruppen bekannt, beispielsweise die alternierende Gruppe A_n für $n \geq 5$ oder die Gruppen $PSL_n(q), PSO_n(q), PSU_n(q)$ und PSp für fast alle n und q.
- Man kannte ebenfalls seit längerer Zeit fünf sporadische einfache, endliche Gruppen, d.h. solche, die in keiner der unendlichen Reihen vorkommen. Dies sind die sogenannten Matthieu-Gruppen $M_{11}, M_{12}, M_{22}, M_{23}$ und M_{24}.

Für die Forschung auf diesem Gebiet waren zu diesem Zeitpunkt die folgenden Fragen von Interesse:

- Wie findet man weitere einfache, endliche Gruppen (falls es überhaupt noch unentdeckte gibt)?
- Wie zeigt man, wenn man meint, alle gefunden zu haben, daß es in der Tat keine weiteren gibt?

Die erste Frage wurde ausgehend von Janko in der folgenden Weise angegangen: Man sucht eine mögliche Gruppenordnung, für die nichts dagegen spricht, daß es zu ihr eine einfache Gruppe gibt. Dann versucht man, für diese Ordnung eine Gruppe zu konstruieren. Wichtig ist bei diesem Vorgehen, möglichst umfassende Ausschlußkriterien für die möglichen Gruppenordnung zu haben. So wird beispielsweise im folgenden der Satz von Burnside vorgestellt, nach dem jede Gruppe der Ordnung $p^a q^b$ für Primzahlen p und q auflösbar und damit nicht einfach ist. Die zweite Frage gilt gegenwärtig als beantwortet (nachdem man nach 1950 noch weitere sporadische Gruppen gefunden hat). Der Beweis ist allerdings noch nicht vollständig notiert und soll in der endgültigen Fassung in dreizehn Bänden veröffentlicht werden, von denen derzeit fünf geschrieben sind. Nun wird der Satz von Burnside, vorbereitet durch einige Lemmata, bewiesen.

4.66. Definition: Es sei $\chi \in Irr(G)$ und φ die zu χ gehörende Darstellung. Weiterhin sei $z \in Z(\mathbb{C}[G])$ und $\varepsilon \in \mathbb{C}$ die nach 4.42 eindeutig bestimmte Zahl, so daß $\varphi(z) = \varepsilon E_n$ ist. Dann ist $w(z) = \varepsilon$ oder auch $w_\chi(z) = \varepsilon$.

4.67. Bemerkung: Die Abbildung $w : Z(\mathbb{C}[G]) \to \mathbb{C}$ ist ein Algebrenhomomorphismus. Die Klassensummen $K_1, \ldots, K_r$ bilden eine Basis von $Z(\mathbb{C}[G])$. Damit gilt

$$\chi(1)w(K_i) = Spur(\varphi(K_i)) = \chi(K_i) = \sum_{g \in \mathcal{K}_i} \chi(g) = |\mathcal{K}|\chi(g),$$

wobei g ein Element der Konjugiertenklasse $\mathcal{K}_i$ und $K_i = \sum_{g \in \mathcal{K}_i} g$ ist. Daher ist

$$w(K_i) = \frac{|\mathcal{K}_i|\chi(g)}{\chi(1)}$$

aus der Charaktertafel ablesbar.

4.68. Definition: Es sei $\theta \in \mathbb{C}$. Die Zahl θ ist ganzalgebraisch, wenn es ein $f \in \mathbb{Z}[x]$ gibt, so daß f normiert ist und $f(\theta) = 0$ erfüllt ist.

4.69. Lemma: *Es sei χ ein irreduzibler Charakter und K eine Klassensumme von G. Dann ist $w_\chi(K)$ ganzalgebraisch.*

Beweis: (Nur die Beweisidee wird vermittelt) Für zwei Klassensummen K_i und K_j ist

$$K_i \cdot K_j = \sum_{v=1}^{r} a_{ijv} K_v$$

für $a_{ijv} \in \mathbb{Z}$. Daher ist

$$w(K_i)w(K_j) = \sum_{v=1}^{r} a_{ijv} w(K_v).$$

Man betrachte

$$S = \left\{ \sum_{i=1}^{r} b_i w(K_i) \mid b_i \in \mathbb{Z} \right\}.$$

Die Menge S ist multiplikativ abgeschlossen, und es ist $1 \in S$, da $w(1) = 1$ ist. Also ist $\mathbb{Z} \subseteq S \subseteq \mathbb{C}$, und S ist eine $\mathbb{Z}$-Ordnung. Mit den Methoden der algebraischen Zahlentheorie kann man zeigen, daß die Elemente von S ganzalgebraisch sind. Der Beweisgang erfolgt analog zum Fall der Maximalordnungen in Zahlkörpern. •

Der folgende Satz ist noch nicht *der* bekannte Satz von Burnside über auflösbare Gruppen, aber ein Satz, auf den sich der Beweis des bekannten Satzes im wesentlichen stützt. Daher wird er ebenfalls häufig Satz von Burnside genannt.

4.70. Satz: *(Satz von Burnside) Es sei $\chi \in Irr(G)$ und $\mathcal{K}$ eine Konjugiertenklasse einer endlichen Gruppe G sowie $g \in \mathcal{K}$. Falls $ggT(\chi(1), |\mathcal{K}|) = 1$ ist, so ist entweder $g \in Z(\chi)$ oder $\chi(g) = 0$.*

Beweis: Die Zahl

$$\frac{|\mathcal{K}|\chi(g)}{\chi(1)}$$

ist ganzalgebraisch. Nach dem chinesischen Restsatz gibt es $u, v \in \mathbb{Z}$, so daß $u\chi(1) + v|\mathcal{K}| = 1$, d. h. daß $v|\mathcal{K}| = 1 - u\chi(1)$ ist. Dann ist

$$\underbrace{v\frac{|\mathcal{K}|\chi(g)}{\chi(1)}}_{\text{ganzalg.}} = \frac{(1 - u\chi(1))\chi(g)}{\chi(1)} = \underbrace{\frac{\chi(g)}{\chi(1)}}_{=\alpha} - \underbrace{u\chi(g)}_{\text{ganzalg.}}.$$

Da die Menge der ganzalgebraischen Zahlen additiv abgeschlossen ist, ist auch α eine ganzalgebraische Zahl. Es sei $g \notin Z(\chi)$, d. h. $|\chi(g)| < |\chi(1)|$. Also ist $|\alpha| < 1$. Es sei k der Zerfällungskörper von $x^n - 1$ über $\mathbb{Q}$ mit $n = |g|$. Dann ist $\alpha \in K$, denn $\chi(g)$ ist eine Summe n-ter Einheitswurzeln, und es ist $\chi(1) \in \mathbb{N}$. Es sei G die Galoisgruppe der Körpererweiterung

$K/\mathbb{Q}$ und σ ein Element aus G. Auch $\chi(g)^\sigma$ ist eine Summe n-ter Einheitswurzeln (und zwar von $\chi(1)$ Stück). Daher ist $|\chi(g)^\sigma| \leq \chi(1)$ und somit $|\alpha^\sigma| = |\chi(g)^\sigma/\chi(1)^\sigma| = |(\chi(g)/\chi(1))^\sigma| \leq 1$ Es sei $\beta = \prod_{\sigma\in G} \alpha^\sigma$. Dann ist $\beta \in \mathbb{Q}$, da $\mathbb{Q}$ der Fixkörper von G ist, und β ist außerdem ganzalgebraisch. Also ist $\beta \in \mathbb{Z}$ und $|\beta| = |\prod_{\sigma\in G} \alpha^\sigma| = \prod_{\sigma\in G} |\alpha^\sigma| < 1$, da $|\alpha^\sigma| \leq 1$ und $|\alpha| < 1$ ist. Also ist $\beta = 0$ und daher $\alpha = 0$ und somit $\chi(g) = 0$. •

4.71. Satz: *Es sei G eine nichtabelsche, einfache Gruppe. Dann ist $\{1\}$ die einzige Konjugiertenklasse von G mit Primzahlpotenzlänge.*

Beweis: Es sei $1 \neq g \in G$ mit $|\mathcal{K}_g| = p^a$ für eine Primzahl p. Es sei χ ein irreduzibler Charakter von G und $\chi \neq 1_G$. Daher ist $Kern(\chi) = \{1\}$, da G einfach ist. Da $Z(\chi)$ eine Untergruppe von $Kern(\chi)$ ist, ist auch $Z(\chi) = \{1\}$, da G einfach und $Z(\chi) = Z(G)$ und G nichtablesch sind. Falls p kein Teiler von $\chi(1)$ ist, so ist $\chi(g) = 0$. Es sei ϱ der reguläre Charakter von G. Dann ist

$$0 = \varrho(g) = \sum_{\chi\in Irr(G)} \chi(1)\chi(g) = 1 + \sum_{\chi\in Irr(G) \text{ und } p|\chi(1)} \chi(1)\chi(g).$$

Es sei

$$\alpha = \sum_{\chi\in Irr(G) \text{ und } p|\chi(1)} \frac{\chi(1)}{p}\chi(g).$$

Dann ist α ganzalgebraisch. Also ist $\alpha = -\frac{1}{p}$ im Widerspruch dazu, daß α ganzalgebraisch ist. •

4.72. Satz: *(Satz von Burnside) Es sei G ein Gruppe mit $|G| = p^a q^b$, so daß p und q Primzahlen und $a, b \in \mathbb{N}_0$ sind. Dann ist G auflösbar.*

Beweis: Es sei G ein minimales Gegenbeispiel. Falls es einen Normalteiler N von G mit $\{1\} \neq N \neq G$ gibt, dann sind N und G/N nach Voraussetzung der Minimalität auflösbar und damit auch G. Falls G einfach ist, dann betrachte man eine p-Sylowgruppe P von G und ein $g \in Z(P)$. In diesem Fall ist $|\mathcal{K}_g| = q^c$ für ein $c \leq b$. Also ist G abelsch. •

Mit dem Satz von Burnside kann man etliche Gruppenordnungen als Kandidaten für einfache Gruppen ausschließen, aber nicht besonders viele. Eine weitaus größere Zahl von Gruppenordnungen schließt der Satz von Thompson aus, dessen bislang kürzesten Beweise ungefähr 300 Seiten einnehmen und deshalb hier nur ohne Beweis zitiert werden kann.

4.73. Satz: *(Satz von Thompson oder Odd-order-theorem) Jede Gruppe von ungerader Ordnung ist auflösbar.*

Bisher wurden Sätze vorgestellt, mit denen man gewisse Gruppenordnungen für einfache Gruppen ausschließen kann. Was macht man aber, wenn man eine Gruppenordnung hat, von der man glaubt, daß es zu ihr eine einfache Gruppe gibt? Der übliche Weg ist der, daß man versucht, eine Charaktertafel zu dieser Ordnung zu konstruieren, die die Charaktertafel einer einfachen Gruppe ist, und wenn man damit erfolgreich ist (andernfalls gibt es keine einfache Gruppe dieser Ordnung), Rückschlüsse auf die Struktur der zugehörigen Gruppe zu ziehen. Dieses Verfahren wird nun an einem Beispiel veranschaulicht.

4.74. Beispiel: Es sei $n = 168 = 2^3 \cdot 3 \cdot 7$. Nach den bisherigen Sätzen ist es nicht ausgeschlossen, daß es eine einfache Gruppe der Ordnung n gibt. Es wird versucht, eine Charaktertafel zu einer einfachen Gruppe der Ordnung n zu konstruieren. Dazu betrachte man das folgende Resultat der Gruppentheorie: Ist G eine einfache Gruppe und P eine p-Sylowgruppe von G, dann gilt:

- Da P kein Normalteiler von G ist, ist die Anzahl der p-Sylowuntergruppe $n_G(p)$ zur Primzahl p größer als 1.
- Es ist $n_G(p) \equiv 1 \bmod p$ und $n_G(p) | [G : P]$.
- Es ist $P \not\leq Z(N_G(P))$.

Diese Ergebnisse werden nun benutzt, um zu den Primteilern von n Rückschlüsse auf die Anzahl der zugehörigen p-Sylowgruppen und die Struktur ihrer Normalisatoren zu ziehen.

- Es sei $p = 7$. Da $n_G(p)$ ein Teiler von $[G : P]$ ist, ist $n_G \in \{1, 2, 4, 8, 3, 6, 12, 24\}$, und da $n_G(p) \equiv 1 \bmod p$ ist, ist $n_G(p) = 8$. Außerdem ist P_7 isomorph zu C_7. Es sei $N_7 = N_G(P_7)$. Die Untergruppe N_7 hat die Ordnung $7 \cdot 3$ und ist daher ein semidirektes Produkt von C_7 und C_3. Also ist $N_7 = C_7 \rtimes C_3$, wobei C_3 nichttrivial auf C_7 operiert, da P_7 keine Untergruppe von $Z(N_7)$ ist. Insbesondere ist C_3 in $Aut(C_7) \cong C_6$ eingebettet. Da sich die acht 7-Sylowgruppen trivial schneiden, gibt es 48 Elemente der Ordnung 7. Diese zerfallen unter Konjugation in zwei Bahnen von 24 Elementen.
- Ebenso erhält man für $p = 3$, daß $n_G(3) \in \{4, 7, 28\}$ ist.
- Analog ergibt sich, daß $n_G(2) \in \{3, 7, 21\}$ ist.

Mit einigen weiteren Argumenten kann man die Anzahl der Sylowgruppen weiter einschränken und zusätzliche Angaben über die Strukturen dieser Gruppen bekommen:

- Es sei $U < G$ mit $[G : U] = l$. Dann operiert G auf den Nebenklassen G/U, d. h. es gibt einen nichttrivialen Homomorphismus von G in die symmetrische Gruppe S_l. Da G einfach ist, ist dieser Homomorphismus injektiv. Also ist $|G|$ ein Teiler von $|S_l| = l!$. Also ist $l \geq 7$ und daher $n_G(3) \in \{7, 28\}$ sowie $n_G(2) \in \{7, 21\}$.
- Man nehme an, daß $n_G(3) = 7$ sei. Es gilt $n_{N_7}(3) = 7 = n_G(3)$. Also liegen alle 3-Sylowgruppen in N_7, und damit ist $\langle P_3 \mid P_3 \in Syl_3(G) \rangle \leq N_7$ im Widerspruch dazu ein Normalteiler von G, daß G einfach ist. Daher ist $n_G(3) = 28$ und $P_3 \cong C_3$ sowie $N_3 = C_3 \rtimes U$ mit $|U| = 2$. Also gibt es 56 Elemente der Ordnung 3, die unter Konjugation in einer Bahn liegen.
- Mit demselben Argument zeigt man, daß $n_G(2) = 21$ ist. Damit ist $P_2 = N_2$, und da P_2 keine Untergruppe von $Z(N_2)$ ist, ist N_2 bzw. P_2 nicht abelsch. Also ist P_2 isomorph zu D_8 oder Q_8. Da N_3 ein Element der Ordnung 2 enthält, ist P_2 isomorph zu D_8. Es gibt also 42 Elemente der Ordnung 4, die in einer Konjugiertenklasse liegen, und 21 Elemente der Ordnung 2, die ebenfalls in einer Konjugiertenklasse liegen.

Mit diesen Ergebnissen sind zugleich die Konjugiertenklassen von G bestimmt worden. Den 6 Konjugiertenklassen entsprechend, gibt es 6 irreduzible Charaktere $\chi_1, \ldots, \chi_6$. Da $\sum_{i=1}^{6} \chi_i(1)^2 = 168$ ist, ergeben sich die Charaktergrade als $1, 3, 3, 6, 7$ und 8. Man kann nun das Verfahren der Induktion verwenden, um aus Charakteren der Untergruppen Charaktere der gesamten Gruppe zu berechnen. So erhält die folgende Charaktertafel. Dabei ist $\varepsilon = w^2 + w^5 + w^6$ und $\delta = w + w^2 + w^6$, wobei w eine siebte komplexe Einheitswurzel ist. Die Gruppe $PSL(2, 3)$ hat diese Tafel.

	1	2	4	3	7	7
	1	21	42	56	24	24
χ_1	1	1	1	1	1	1
χ_2	3	-1	1	0	ε	δ
χ_3	3	-1	1	0	δ	ε
χ_4	6	2	0	0	-1	-1
χ_5	7	-1	-1	1	0	0
χ_6	8	0	0	-1	1	1

Kapitel 5

Modulare Darstellungstheorie

In diesem Kapitel untersuchen wir den Fall, daß K ein beliebiger Körper der Charakteristik $p > 0$ ist. Für viele Anwendungen wird K ein endlicher Körper sein. In diesem Fall sind nicht alle Darstellungen vollständig reduzibel und die gesamte Theorie ist nicht annähernd so einfach zu überblicken wie über $\mathbb{C}$. Leider tritt genau dieser Fall in Anwendungen oft auf, und daher ist es doch von Interesse, hier einiges drüber zu lernen.
Im modularen Fall werden wir nicht so viele theoretische Aussagen finden. Insbesondere ist hier die Theorie der Charaktere nicht so hilfreich. Dafür kann man im Fall der endlichen Körper durchaus einige Algorithmen entwickeln, mit denen man zumindest in einem gegebenen Fall Moduln untersuchen kann. Der wichtigste Algorithmus ist die sogenannte "Meataxe" (die Fleischaxt).

5.1 Die Radikal- und die Sockelreihe

5.1. Bemerkung: Ist p eine Primzahl und gibt es ein $f \in \mathbb{N}$, so daß $q = p^f$ ist, so ist $\mathbb{F}_q$ der endliche Körper aus q Elementen und mit der Charakteristik p. Ist G eine endliche Gruppe und ist p kein Teiler von $|G|$, so ist nach dem Satz von Maschke 2.4 der Vektorraum $V = \mathbb{F}_q^n$ für jeden $n \in \mathbb{N}$ vollständig reduzibel.

Die Notation aus dieser Bemerkung wird im weiteren benutzt. Das folgende Beispiel zeigt, wie sich die Fälle $p \mid |G|$ und $p \nmid |G|$ unterscheiden können.

5.2. Beispiel: Es sei $G = C_2$ und x sei der Erzeuger von G, d. h. es ist $G = \{x, x^2\} = \{x, 1\}$. Es sei $V = \langle v_1, v_2\rangle_{\mathbb{F}_q}$, so daß G vermittels $v_1x = v_2$ und $v_2x = v_1$ auf V operiert. Wie findet man Untermuduln in V? Man nehme an, daß $\langle a_1v_1 + a_2v_2\rangle_{F_q}$ ein Untermudul von V sei. Dann ist $a_1 \neq 0$. Ohne Beschränkung der Allgemeingültigkeit kann man annehmen, daß $a_1 = 1$ ist. Man betrachte also $U = \langle v_1 + av_2\rangle$. Dann ist $av_1 + v_2 = (v_1 + av_2)x = b(v_1 + av_2) = bv_1 + abv_2$ für ein $b \neq 0$. Über Koeffizientenvergleich erhält man $a = b$ und $ab = 1$. Also ist $a = b^{-1}$ bzw. $b = b^{-1}$, also $b^2 = 1$. Aus der Theorie endlicher Körper folgt dann:

- Ist q ungerade, so ist $b \in \{1, -1\}$ bzw. $a \in \{1, -1\}$. Also sind sowohl $U_1 = \langle v_1 + v_2 \rangle$ als auch $U_2 = \langle v_1 - v_2 \rangle$ Untermoduln von V, und V ist die direkte Summe von U_1 und U_2.
- Ist q gerade, so ist $b = 1 = a$ die einzige Lösung. Daher ist $\langle v_1 + v_2 \rangle = \langle v_1 - v_2 \rangle$ der einzige Submodul von V. In diesem Fall ist V nicht vollständig reduzibel.

5.3. Definition: Eine endliche Folge von Untermoduln $V = V_1 > V_2 > \ldots > V_l > V_{l+1} = \{0\}$ ist eine Kompositionsreihe des Moduls V, wenn der Faktormodul V_i/V_{i+1} für jedes i mit $1 \leq i \leq l$ irreduzibel ist.

5.4. Beispiel:

- Ist der Modul V die direkte Summe der irreduziblen Untermoduln $U_1, \ldots, U_l$, so ist $V = V_1 > V_2 = U_2 \oplus \ldots \oplus U_l > V_3 = U_3 \oplus \ldots \oplus U_l > \ldots > V_{l-1} = U_{l-1} \oplus U_l > V_l = U_l > V_{l+1} = \{0\}$ eine Kompositionsreihe von V.
- Ist V vollständig irreduzibel und hat V die Kompositionsreihe $V = V_1 > V_2 > \ldots > V_l > V_{l+1} = \{0\}$, so ist V isomorph zu $V_1/V_2 \oplus \ldots \oplus V_l/V_{l+1}$.
- Ist V wie im vorangegangenen Beispiel definiert und ist q gerade, so ist zwar $V_1 = V > V_2 = \langle v_1 + v_2 \rangle > V_3 = \{0\}$ eine Kompositionsreihe von V und auch $V_2 \cong V_1/V_2 \cong F_q$, aber V ist nicht isomorph zu $V_2 \oplus V_1/V_2$.

5.5. Definition: Ist V ein Modul einer Gruppe G so ist

$$Rad_G(V) = \bigcap_{W<V \text{ und } W \text{ ist maximal}} W$$

das Radikal und

$$Soc_G(V) = \sum_{W<V \text{ und } W \text{ ist minimal}} W$$

der Sockel von V.

5.6. Lemma: *Ist V ein Modul zu einer Gruppe G, so sind die folgenden drei Aussagen äquivalent:*

- *V ist vollständig reduzibel.*
- *$Rad_G(V) = \{0\}$.*
- *$Soc_G(V) = V$.*

Beweis: Die Äquivalenz der ersten beiden Aussagen: Es sei V vollständig reduzibel. Man nehme an, daß $R = Rad_G(V) \neq \{0\}$ sei. Dann gibt es ein $U < V$ mit $V = R \otimes U$. Dann gibt es einen maximalen Teilmodul $W < V$, so daß $U \leq W$ ist. In diesem Fall ergibt sich der Widerspruch $V = R \otimes U \leq W < V$. Also ist $R = \{0\}$. Nun seien umgekehrt $W_1, \ldots, W_m$ sämtliche maximale Untermoduln von V (für den Fall, daß $|V| < \infty$ ist). Es sei $U_i = V/W_i$ und $U = U_1 \oplus \ldots \oplus U_m$. Man betrachte die Abbildung $\varphi : V \to U : \varphi(v) = (v + W_1, \ldots, v + W_m)$. Offensichtlich ist $\varphi \in Hom_G(V, U)$. Es ist $Kern(\varphi) = \{0\}$, da $W_1 \cap \ldots \cap W_m = \{0\}$ ist. Es ist $V \cong V/Kern(\varphi) \cong \varphi(V) = U \leq_G V$. Ist U vollständig reduzibel, so auch $\varphi(V)$ und damit V.

Die Äquivalenz der ersten und dritten Aussage: Es sei V vollständig reduzibel. Dann ist $V = V_1 \oplus \ldots \oplus V_m$, wobei $V_1, \ldots, V_m$ irreduzibel sind. Dann ist $V = V_1 \oplus \ldots \oplus V_m \leq Soc_G(V) \leq V$. Also ist $V = Soc_G(V)$. Nun sei umgekehrt $V = Soc_G(V)$. Es wird gezeigt, daß $Soc_G(V)$ vollständig reduzibel ist. Es seien $W_1, \ldots, W_m$ sämtliche irreduziblen Untermoduln von V, und es sei $U_i = W_1 + \ldots + W_i$ für alle i mit $1 \leq i \leq m$. Über Induktion wird gezeigt, daß U_i für alle i mit $1 \leq i \leq m$ reduzibel ist. Für den Induktionsanfang ist nichts zu zeigen. Es sei U_{i-1} vollständig reduzibel. Es ist $U_i = U_{i-1} + W_i$. Dann ist

$$U_{i-1} \cap W_i = \begin{cases} W_i & \text{falls } W_i \leq U_{i-1}, \\ \{0\} & \text{sonst,} \end{cases}$$

und daher

$$U_i = \begin{cases} U_{i-1} & \text{falls } W_i \leq U_{i-1}, \\ U_{i-1} \oplus W_i & \text{sonst.} \end{cases}$$

In beiden Fällen ist U_i vollständig reduzibel. •

5.7. Satz: *Ist V ein Modul zu einer Gruppe G, so gilt:*

- *$Rad_G(V)$ ist der kleinste Untermodul von V, so daß $V/Rad_G(V)$ vollständig reduzibel ist.*
- *$Soc_G(V)$ ist der größte vollständig reduzible Untermodul von V.*

Beweis: Es ist zu zeigen, daß $Rad_G(V/Rad_G(V)) = \{0\}$ ist. Es sei $R = Rad_G(V)$. Dann ist der Faktormodul W/R genau dann maximal in V/R, wenn W maximal in V ist, und es ist $W \geq R$ genau dann, wenn W maximal in V ist. Es ist daher

$$Rad_G(V/R) = \bigcap_{W <_{\max} V} W/R = \bigcap_{W \geq_{\max} V} W/R = R/R = \{0\}.$$

Also ist V/R vollständig reduzibel. Es sei $U \leq_G V$, so daß V/U vollständig reduzibel ist. Es reicht zu zeigen, daß $U \geq R$ ist. Es ist genau dann $W/U <_{\max} V/U$, wenn $W <_{\max} V$ und $W \geq U$. Daher ist

$$\{0\} = Rad_G(V/U) = \bigcap_{U \leq W <_{\max} V} W/U$$

und

$$R = \bigcap_{U \leq W <_{\max} V} W \leq U.$$

Nach dem Beweis zum vorangegangenen Satz ist $Soc_G(V)$ vollständig reduzibel. Es sei $U = U_1 \oplus \ldots \oplus U_m \leq_G V$, wobei U_i für alle i mit $a \leq i \leq m$ irreduzibel sind. Dann ist $U_i \leq Soc_G(V)$ und daher $U \leq Soc_G(V)$. •

5.2 Die Meataxe

5.8. Bemerkung: Im weiteren wird die folgende Notation benutzt: Es sei G eine Untergruppe von $GL(n,q)$ und $V = \mathbb{F}_q^n$ der natürliche G-Modul. Die Gruppe G operiert durch Matrixmultiplikation von rechts auf V und von links auf $\bar{V}$, wobei $\bar{V} = \bar{\mathbb{F}}_q$ der zu V duale Raum der Spaltenvektoren ist. Ist U ein Unterraum von V, so ist $\bar{U} = \{\bar{v} \in \bar{V} \mid u\bar{v} = 0 \text{ für alle } u \in U\} \leq \bar{V}$.

5.9. Lemma: *Der Unterraum $U \leq V$ ist genau dann ein G-Untermodul in V, wenn $\bar{U}$ ein G=Üntermodul in $\bar{V}$ ist.*

Beweis: Es sei $U \leq_G V$ und $\bar{u} \in \bar{U}$ sowie $g \in G$. Dann ist $u(g\bar{u}) = (ug)\bar{u} = 0$ für alle $u \in U$ und damit $g\bar{u} \in \bar{U}$. Also ist $\bar{U} \leq \bar{V}$. Die Umkehrung zeigt man ebenso. •

5.10. Folgerung: *V ist genau dann ein irreduzibeler G-Modul, wenn $\bar{V}$ ein irreduzibler G-Modul ist.*

5.11. Definition: Ist $U \leq V$, so ist $U^\perp = \{\bar{v} \in \bar{V} \mid u\bar{v} = 0 \text{ für alle } u \in U\}$, und ist $\bar{U} \leq \bar{V}$, so ist $\bar{U}^\perp = \{v \in V \mid \bar{u}v = 0 \text{ für alle } \bar{u} \in \bar{U}\}$. Es sei A_G die Teilalgebra von $M_n(\mathbb{F}_q)$, die von G erzeugt wird, und für $a \in M_n(\mathbb{F}_q)$ sei $Null(a) = \{v \in V \mid va = 0\}$ sowie $\overline{Null(a)} = \{\bar{v} \in \bar{V} \mid a\bar{v} = 0\}$.

5.12. Bemerkung: Für alle $U \leq V$ und $\bar{U} \leq \bar{V}$ gilt:

- Es ist $(U^\perp)^\perp = U$ und $(\bar{U}^\perp)^\perp = \bar{U}$.
- Es ist $dim(U^\perp) = dim(V) - dim(U)$.
- Es ist $dim(\bar{U}^\perp) = dim(\bar{V}) - dim(\bar{U})$.
- Es ist genau dann $U \leq_G V$, wenn $U^\perp \leq_G \bar{V}$.

5.13. Lemma: *Es sei $\{0\} \neq U \leq_G V$ und $0 \neq a \in A_G$, so daß $det(a) = 0$ ist. Dann ist $Null(a) \cap U \neq \{0\}$ oder $\overline{Null(a)} \cap U^\perp \neq \{0\}$.*

Beweis: Es sei $B = \{b_1, \ldots, b_{n-r}, b_{n-r+1}, \ldots, b_n\}$ eine Basis von V, so daß $\{b_1, \ldots, b_{n-r}\}$ eine Basis von U ist. Bezüglich der Basis B hat a die Gestalt

$$a = \begin{pmatrix} a_1 & 0 \\ * & a_2 \end{pmatrix},$$

wobei $a_1 \in M_{n-r}(q)$, $a_2 \in M_r(q)$ und $*$ eine $r \times (n-r)$-Matrix über $\mathbb{F}_q$ ist. Es ist $det(a) = det(a_1)det(a_2) = 0$. Falls $det(a_2) = 0$ ist, dann wähle man $0 \neq \hat{v} \in Null(a_2) \leq \mathbb{F}_q^r$. Es sei $v = (0, \ldots, 0, \hat{v}) \in V$. Dann ist $v \in U$, und nach der Wahl von $\hat{v}$ ist $va = 0$. Also ist $0 \neq v \in U \cap Null(a)$. Falls $det(a_1) = 0$ ist, dann wähle man $0 \neq \hat{v} \in \overline{Null(a_1)} \leq \overline{\mathbb{F}_q^{n-r}}$. Es sei $\bar{v} = (0, \ldots, 0, \hat{v})^T \in \bar{V}$, wobei T die Transpositionsabbildung ist. Dann ist $\bar{v} \in U^\perp$, und nach der Wahl von $\hat{v}$ ist $a\bar{v} = 0$. Also ist $0 \neq \bar{v} \in U^\perp \cap \overline{Null(a)}$. •

5.14. Folgerung: *(Das Irreduzibilitätskriterium von Norton) Es sei* $\{0\} \neq U \leq_G V$ *und* $0 \neq a \in A_G$*, so daß* $det(a) = 0$ *ist. Dann ist* G *genau dann irreduzibel über* V*, wenn* $Gx = V$ *für alle* $0 \neq x \in Null(a)$ *und* $yG = \bar{V}$ *für alle* $0 \neq y \in \overline{Null(a)}$ *ist.*

Beweis: Es sei G irreduzibel. Dann ist $xG \neq \{0\}$ und $Gy \neq \{0\}$, wenn $x \neq 0$ und $y \neq 0$ ist. Daher ist $Gx = V$ für alle $x \neq 0$ und $yG = \bar{V}$ für alle $y \neq 0$. Es sei $\{0\} \neq U <_G V$. Dann ist $Null(a) \cap U \neq \{0\}$ oder $\overline{Null(a)} \cap U^{\perp} \neq \{0\}$. Fall $0 \neq x \in Null(a) \cap U$ ist, dann ist $xG \leq U < V$, und wenn $0 \neq y \in \overline{Null(a)} \cap U^{\perp}$ ist, dann ist $Gy \leq U^{\perp}$. •

Auf dieses Kriterium baut die Meataxe auf, deren einfache Version nun dargestellt wird.

5.15. Bemerkung: (Die Meataxe) Als Eingabe verwendet der Algorithmus ein Erzeugendensystem $\{g_1, \ldots, g_m\}$ einer Untergruppe G von $GL(n, q)$. Das Ziel ist es, ein $a \in A_G$ zu finden, so daß $0 < dim(Null(a)) < n$ ist. Zum Beginn der Suche wähle man zufällig ein $a \in A_G$. Wenn a die gewünschte Eigenschaft besitzt, so hat die Suche ein Ende. Andernfalls liefert das Irreduzibilitätskriterium von Norton einen Untermodul U. Dann wende man dasselbe Verfahren auf U und V/U an. Man erhält einen minimalen Untermodul $U_0 <_G V$. Anschließend wende man das Verfahren auf V/U_0 an. Man erhält aus den Kompositionsreihen

$$V/U > V_1/U > \ldots > V_s/U > U/U$$

und

$$U > U_1 > \ldots > U_k > \{0\}$$

eine Kompositionsreihe

$$V > V_1 > \ldots V_s > U > U_1 > \ldots > U_k > \{0\}$$

von V.