Algebra

Vorlesung im Wintersemester 1991/92
und Sommersemester 1992

Prof. Dr. B. Külshammer

Ausarbeitung: Markus Deiml

Inhaltsverzeichnis

Kapitel 1

Gleichungen kleinen Grades

1.1 Gleichungen 2. Grades

Gegeben sei die Gleichung

$$X^2 + aX + b = 0 \qquad \text{mit } a, b \in \mathbb{C}\,.$$

„Quadratische Ergänzung“ führt auf

$$0 = \left(X + \frac{a}{2}\right)^2 + b - \frac{a^2}{4}.$$

Damit ist die Gleichung auf eine Gleichung der Form $Y^2 = c$ zurückgeführt. Diese hat in $\mathbb{C}$ i.a. zwei Lösungen, von denen keine schöner ist als die andere. Wir vermeiden daher das $\sqrt{\ }$-Zeichen.

Beispiel:

$$0 = X^2 + X + 1 = \left(X + \frac{1}{2}\right)^2 + \frac{3}{4}$$

$$\Rightarrow \; X + \frac{1}{2} = \pm\frac{\sqrt{3}i}{2} \;\Rightarrow\; X = -\frac{1}{2} \pm \frac{\sqrt{3}i}{2}$$

Wegen $(X^2 + X + 1)(X - 1) = X^3 - 1$ sind diese Zahlen Lösungen von $X^3 - 1 = 0$.

1.2 Gleichungen 3. Grades

Gegeben sei die Gleichung

$$X^3 + aX^2 + bX + c = 0 \qquad \text{mit } a, b, c \in \mathbb{C}\,.$$

„Kubische Ergänzung“ führt auf

$$\begin{aligned}
0 &= \left(X + \frac{a}{3} - \frac{a}{3}\right)^3 + a\left(X + \frac{a}{3} - \frac{a}{3}\right)^2 + b\left(X + \frac{a}{3} - \frac{a}{3}\right) + c \;= \\
&= \left(X + \frac{a}{3}\right)^3 - a\left(X + \frac{a}{3}\right)^2 + \frac{a^2}{3}\left(X + \frac{a}{3}\right) - \frac{a^3}{27} + \\
&\quad + a\left(X + \frac{a}{3}\right)^2 - \frac{2a^2}{3}\left(X + \frac{a}{3}\right) + \frac{a^3}{9} + b\left(X + \frac{a}{3}\right) - \frac{ab}{3} + c \;= \\
&= \left(X + \frac{a}{3}\right)^3 + \left(b - \frac{a^2}{3}\right)\left(X + \frac{a}{3}\right) + \left(\frac{2a^3}{27} - \frac{ab}{3} + c\right).
\end{aligned}$$

Damit ist die Gleichung auf eine Gleichung der Form

$$Y^3 + pY + q = 0$$

zurückgeführt.
Ansatz: $Y = U + V$.

$$\begin{aligned} 0 &= (U+V)^3 + p(U+V) + q = \\ &= U^3 + 3U^2V + 3UV^2 + V^3 + pU + pV + q = \\ &= U^3 + V^3 + q + (U+V)(3UV + p) \end{aligned}$$

Es genügt also, die Gleichungen $U^3 + V^3 + q = 0$ und $3UV = -p$ zu lösen. U^3 und V^3 sind die Lösungen der folgenden quadratischen Gleichung in T:

$$\begin{aligned} 0 &= (T - U^3)(T - V^3) = \\ &= T^2 - (U^3 + V^3)T + U^3V^3 = \\ &= T^2 + qT - \frac{p^3}{27} \end{aligned}$$

Dabei muß man U und V so wählen, daß $3UV = -p$ gilt.

Beispiel:

$$X^3 - 18X - 35 = 0$$

führt auf

$$T^2 - 35T + 216 = 0$$

Lösungen: $T_1 = 27,\ T_2 = 8$.
Die Lösungen von $U^3 = 27$ sind nach 1.1 die Zahlen 3 und $\frac{3}{2}(-1 \pm \sqrt{3}i)$.

$$\begin{array}{lll} U_1 = 3,\ 3U_1V_1 = 18, & V_1 = 2, & X_1 = 5 \\ U_2 = \frac{3}{2}(-1 + \sqrt{3}i), & V_2 = -1 - \sqrt{3}i, & X_2 = -\frac{5}{2} + \frac{\sqrt{3}i}{2} \\ U_3 = \frac{3}{2}(-1 - \sqrt{3}i), & V_3 = -1 + \sqrt{3}i, & X_3 = -\frac{5}{2} - \frac{\sqrt{3}i}{2} \end{array}$$

1.3 Gleichungen 4. Grades

Gegeben sei die Gleichung

$$X^4 + aX^3 + bX^2 + cX + d = 0.$$

Wie in 1.2 reduziert man zunächst auf eine Gleichung der Form

$$Y^4 + pY^2 + qY + r = 0.$$

Dann führt man eine neue Variable Z ein und erhält:

$$\begin{aligned} (Y^2 + Z)^2 &= Y^4 + 2Y^2Z + Z^2 = \\ &= -pY^2 - qY - r + 2Y^2Z + Z^2 = \\ &= (-p + 2Z)Y^2 - qY + Z^2 - r = \\ &= (-p + 2Z)\left(Y - \frac{q}{2(-p+2Z)}\right)^2 - \frac{q^2}{4(-p+2Z)} + Z^2 - r \end{aligned}$$

Wir wählen Z nun so, daß der absolute Koeffizient verschwindet.

$$\begin{aligned} 0 &= -q^2 + 4(Z^2 - r)(-p + 2Z) = \\ &= 8Z^3 - 4pZ^2 - 8rZ + 4rp - q^2 \end{aligned}$$

Diese Gleichung 3. Grades kann man wie in 1.2 auflösen. Bezeichnet z eine Lösung, so hat man noch die Gleichung

$$(Y^2 + z)^2 = (-p + 2z)\left(Y - \frac{q}{2(-p+2z)}\right)^2$$

zu lösen. Dies führt auf zwei quadratische Gleichungen.

Beispiel: Gegeben sei die Gleichung

$$X^4 - 10X^2 - 20X - 16 = 0.$$

Die zugehörige kubische Gleichung ist

$$0 = 8Z^3 + 40Z^2 + 128Z + 240$$

oder

$$0 = Z^3 + 5Z^2 + 16Z + 30.$$

Eine Lösung ist $Z = -3$. Man erhält

$$(Y^2 - 3)^2 = (10 - 6)\left(Y + \frac{20}{8}\right)^2 = (2Y + 5)^2.$$

Also ist $Y^2 - 3 = 2Y + 5$ oder $Y^2 - 3 = -2Y - 5$, d.h. $Y^2 - 2Y - 8 = 0$ oder $Y^2 + 2Y + 2 = 0$.
Folglich ist $Y \in \{-2, 4, -1 + i, -1 - i\}$.

1.4 Gleichungen 5. Grades

Abel (1802–1829): Es gibt keine allgemeine Lösungsformel.
Galois (1811–1832): Charakterisierung aller Gleichungen, die sich auflösen lassen.

Kapitel 2

Halbgruppen

Definition 2.1 *Eine (innere)* Verknüpfung *auf einer Menge M ist eine Abbildung $M \times M \to M$. Das Bild von $(a, b) \in M \times M$ schreibt man häufig in der Form $a * b,\ a \cdot b,\ a + b,\ ab$.*

Beispiel:

(a) Addition, Multiplikation, Subtraktion in $\mathbb{Z}$, $\mathbb{R}$, $\mathbb{C}$.

(b) Durchschnitt und Vereinigung auf der *Potenzmenge* $\mathcal{P}(X)$, der Menge aller Teilmengen der Menge X.

(c) ggT und kgV in $\mathbb{N}$.

(d) Komposition von Abbildungen auf der Menge $\mathrm{Abb}(X)$ aller Abbildungen $X \to X$.

(e) A sei eine Menge (*Alphabet*) und W die Menge aller endlichen Folgen (*Wörter*) $a_1, \ldots, a_n$ von Elementen in A (*Buchstaben*). Die Verknüpfung von zwei Wörtern $a_1 \ldots a_n$ und $b_1 \ldots b_n$ ist das Wort $a_1 \ldots a_n b_1 \ldots b_n$.

Bemerkung: Verknüpfungen auf kleinen Mengen kann man oft durch ihre Verknüpfungstafel angeben:

$$\begin{array}{c|ccc}
 & \cdots & b & \cdots \\
\hline
\vdots & & \vdots & \\
a & \cdots & ab & \cdots \\
\vdots & & \vdots &
\end{array}$$

$$\text{z.B.} \quad \begin{array}{c|cc}
\wedge & w & f \\
\hline
w & w & f \\
f & f & f
\end{array}$$

Definition 2.2 *Sei M eine Menge mit einer Verknüpfung $*$. Ein Element $e \in M$ heißt* rechtsneutral*, falls $a * e = a$ für alle $a \in M$ ist. Analog definiert man* linksneutral*. Ist e rechtsneutral und linksneutral, so nennt man e* neutral.

Satz: *Sei M eine Menge mit einer Verknüpfung $*$. Ist $e \in M$ rechtsneutral und $f \in M$ linksneutral, so ist $e = f$. Insbesondere gibt es in M höchstens ein neutrales Element.*

Beweis: $f = f * e = e$.

Definition 2.3 *Sei M eine Menge mit Verknüpfung $*$. Man nennt $*$ (und M)*

(i) assoziativ*, falls $a * (b * c) = (a * b) * c$ für alle $a, b, c \in M$.*

(ii) kommutativ *oder* abelsch*, falls $a * b = b * a$ für alle $a, b \in M$.*

Eine Halbgruppe *ist eine Menge mit einer assoziativen Verknüpfung. Ein* Monoid *ist eine Halbgruppe mit neutralem Element.*

Beispiel: $(\mathbb{N}, +)$ ist Halbgruppe, $(\mathbb{N}_0, +)$ ist Monoid.

Bemerkung: Im folgenden schreiben wir statt $a * b$ meist ab. Neutrale Elemente bezeichnen wir meist mit 1.

Definition 2.4 *Sei M Monoid und $a \in M$. Ein Element $b \in M$ heißt* rechtsinvers *zu $a \in M$, falls $ab = 1$. Analog definiert man* linksinvers*. Ist b rechtsinvers und linksinvers zu a, so nennt man b* invers *zu a.*

Beispiel: In $(\mathbf{Z}, +)$ ist -2 zu 2 invers.

Satz: *Sei M Monoid und $a \in M$. Ist $b \in M$ rechtsinvers und $c \in M$ linksinvers zu a, so ist $b = c$. Insbesondere besitzt a höchstens ein inverses Element. Dieses bezeichnet man i.a. mit a^{-1}. (Schreibt man die Verknüpfung mit dem $+$-Zeichen, so nimmt man 0 statt 1 und $-a$ statt a^{-1}.)*

Beweis: $b = 1b = (ca)b = c(ab) = c1 = c$.

Satz 2.5 *Seien M ein Monoid und $a, b \in M$ invertierbar. Dann sind auch a^{-1} und ab invertierbar mit $(a^{-1})^{-1} = a$ und $(ab)^{-1} = b^{-1}a^{-1}$.*

Beweis: $aa^{-1} = 1 = a^{-1}a$.
$(ab)(b^{-1}a^{-1}) = abb^{-1}a^{-1} = a1a^{-1} = aa^{-1} = 1$.
Analog $(b^{-1}a^{-1})(ab) = 1$.

Definition 2.6 *In einer Halbgruppe H definiert man für $a \in H$ und $n \in \mathbb{N}$ die n-te* Potenz *a^n durch $a^n := aa \ldots a$ (n Faktoren). Ist M Monoid, so definiert man zusätzlich $a^0 := 1$. Ist a invertierbar, so setzt man $a^{-n} := (a^{-1})^n$.*

Bemerkung: Dann gelten die üblichen Regeln: $a^m a^n = a^{m+n}$, $(a^m)^n = a^{mn}$. Jedoch ist i.a. $(ab)^n \neq a^n b^n$.

Kapitel 3

Gruppen

Definition 3.1 *Eine* Gruppe *ist eine Halbgruppe G, in der ein Element e mit folgender Eigenschaft existiert:*

(i) $eg = g$ *für* $g \in G$.

(ii) Für $g \in G$ *existiert* $h \in G$ *mit* $hg = e$.

Bemerkung: Man zeigt leicht, daß dann auch $ge = g$ für $g \in G$ gilt. Daher ist e neutrales Element in G. Ferner gilt in (ii) auch $gh = e$, d.h. g ist invertierbar mit $g^{-1} = h$.
Man nennt die Anzahl der Elemente in G die *Ordnung* von G. Schreibweise: $|G|$

Beispiel:

(i) $(\mathbf{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{C}, +)$ sind abelsche Gruppen, jedoch nicht $(\mathbb{N}, +)$.

(ii) $(\mathbb{Q} \setminus \{0\}, \cdot)$, $(\mathbb{R} \setminus \{0\}, \cdot)$, $(\mathbb{C} \setminus \{0\}, \cdot)$, $(]0, \infty[, \cdot)$ sind abelsche Gruppen, aber nicht $(\mathbf{Z} \setminus \{0\}, \cdot)$ und $(\mathbb{Q}, \cdot)$.

(iii) $\{1\}$ ist Gruppe bzgl. $\cdot$, $\{0\}$ Gruppe bzgl. $+$.

(iv) Für jede Menge X ist die Menge $\mathrm{Sym}(X)$ aller Bijektionen $X \to X$ eine Gruppe bzgl. der Komposition von Abbildungen. Man nennt $\mathrm{Sym}(X)$ die *symmetrische Gruppe* auf X und ihre Elemente *Permutationen.* Ist $|X| = n < \infty$, so ist $|\mathrm{Sym}(X)| = n!$. Wir schreiben $\mathrm{Sym}(n)$ statt $\mathrm{Sym}(\{1, \dots, n\})$ und nennen dies die symmetrische Gruppe des Grades n.
Schreibweise: $f = \begin{pmatrix} 1 & 2 & \cdots & n \\ f(1) & f(2) & \cdots & f(n) \end{pmatrix}$, z.B. $\left(\begin{smallmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{smallmatrix}\right)$.

(v) Sind $G_1, \dots, G_n$ Gruppen, so auch das kartesische (direkte) Produkt

$$G_1 \times \ldots \times G_n = \{(g_1, \dots, g_n) : g_i \in G_i \text{ für } i = 1, \dots, n\}$$

mit der Verknüpfung $(g_1, \dots, g_n)(h_1, \dots, h_n) := (g_1 h_1, \dots, g_n h_n)$.

(vi) Für jeden Körper K und $n \in \mathbb{N}$ bilden die invertierbaren $n \times n$-Matrizen mit Koeffizienten in K eine Gruppe bzgl. $\cdot$, die *allgemeine lineare Gruppe* $\mathrm{GL}(n, K)$ des Grades n über K.

Definition 3.2 *Seien G, H Gruppen und $f : G \to H$ eine Abbildung. Man nennt f einen*

(i) Homomorphismus*, falls $f(ab) = f(a)f(b)$ für $a, b \in G$ ist.*

(ii) Monomorphismus*, falls f ein injektiver Homomorphismus ist.*

(iii) Epimorphismus*, falls f ein surjektiver Homomorphismus ist.*

(iv) Isomorphismus*, falls f ein bijektiver Homomorphismus ist.*

(v) Endomorphismus*, falls f ein Homomorphismus und $G = H$ ist.*

(vi) Automorphismus*, falls f ein bijektiver Endomorphismus ist.*

Bemerkung: Ist f ein Homomorphismus, so ist $f(1_G) = 1_H$ und $f(g)^{-1} = f(g^{-1})$ für $g \in G$. Sind G, H, K Gruppen und $f : G \to H,\ g : H \to K$ Homomorphismen, so ist auch $g \circ f : G \to K$ ein Homomorphismus.
Ist f ein Isomorphismus, so auch f^{-1}. Daher bilden die Automorphismen von G eine Gruppe bzgl. der Komposition von Abbildungen, die *Automorphismengruppe* $\mathrm{Aut}(G)$ von G.

Beispiel:

(i) Für $n \in \mathbb{N}$ ist die Abbildung $(\mathbf{Z}, +) \to (\mathbf{Z}, +),\ k \mapsto kn$ ein Homomorphismus.

(ii) Die Abbildung $(\mathbb{R}, +) \to (]0, \infty[, \cdot),\ x \mapsto e^x$ ist ein Isomorphismus.

(iii) Für jede Gruppe G und jedes Element $a \in G$ ist die Abbildung $f_a : G \to G,\ g \mapsto aga^{-1}$ ein Automorphismus von G. Man nennt f_a den von a induzierten *inneren Automorphismus* von G. Für $a, b \in G$ ist $f_a \circ f_b = f_{ab}$. Daher ist die Abbildung $G \to \mathrm{Aut}(G),\ a \mapsto f_a$ ein Homomorphismus.

(iv) Für $n \in \mathbb{N}$ ist der *alternierende Charakter*

$$\mathrm{sgn} : \mathrm{Sym}(n) \to (\{1, -1\}, \cdot),\ g \mapsto \prod_{\substack{i,j \in \mathbb{N} \\ 1 \le i < j \le n}} \frac{g(i) - g(j)}{i - j}$$

ein Homomorphismus. Man nennt $\mathrm{sgn}(g)$ das *Vorzeichen* oder *Signum* von g. Ist $\mathrm{sgn}(g) = 1$, so nennt man g *gerade*, sonst *ungerade*.

(v) Für jeden Körper K und $n \in \mathbb{N}$ ist $\det : \mathrm{GL}(n, K) \to (K \setminus \{0\}, \cdot)$ ein Homomorphismus.

Definition 3.3 *Man nennt zwei Gruppen G, H* isomorph*, falls es einen Isomorphismus $G \to H$ gibt. Schreibweise: $G \cong H$.*

Bemerkung: Die Isomorphie von Gruppen ist eine Äquivalenzrelation, d.h. es gilt:

(i) $G \cong G$ (Reflexivität)

(ii) $G \cong H \Rightarrow H \cong G$ (Symmetrie)

(iii) $G \cong H \wedge H \cong K \Rightarrow G \cong K$ (Transitivität)

Definition 3.4 *Eine nichtleere Teilmenge H einer Gruppe G nennt man* Untergruppe*, falls für $a, b \in H$ stets $ab^{-1} \in H$ ist.*

Bemerkung:

(i) Wegen $H \neq \emptyset$ existiert ein Element $b \in H$. Dann ist auch $1 = bb^{-1} \in H$ und $b^{-1} = 1b^{-1} \in H$. Für $a \in H$ ist damit auch $ab = a(b^{-1})^{-1} \in H$. Damit bildet H eine Gruppe mit der entsprechend eingeschränkten Verknüpfung.

(ii) Ist H Untergruppe von G, so schreibt man: $H \le G$, ist H echte Untergruppe von G (d.h. $H \neq G$), so schreibt man: $H < G$.

Beispiel:

(i) Für jede Gruppe G sind $\{1_G\}$ und G selbst Untergruppen von G. Man nennt $\{1_G\}$ die *triviale* Unterguppe von G und schreibt: $\{1_G\} = 1$.

(ii) Ist $I \neq \emptyset$ eine Menge und $H_i \leq G$ für $i \in I$, so ist $\bigcap_{i\in I} H_i \leq G$.

(iii) $(\mathbf{Z}, +) \leq (\mathbb{Q}, +) \leq (\mathbb{R}, +) \leq (\mathbb{C}, +)$
$(\mathbb{Q} \setminus \{0\}, \cdot\,) \leq (\mathbb{R} \setminus \{0\}, \cdot\,) \leq (\mathbb{C} \setminus \{0\}, \cdot\,)$

(iv) Für jede Teilmenge X von G ist der *Normalisator* $N_G(X) := \{g \in G : gX = Xg\}$ (wobei $gX = \{gx : x \in X\}$) Untergruppe von G; wegen $1X = X = X1$ ist nämlich $1 \in N_G(X)$, und für $a, b \in N_G(X)$ ist

$$ab^{-1}X = ab^{-1}Xbb^{-1} = ab^{-1}bXb^{-1} = aXb^{-1} = Xab^{-1},$$

also $ab^{-1} \in N_G(X)$.
Analog ist der *Zentralisator* $C_G(X) = \{g \in G : gx = xg \text{ für } x \in X\} \leq G$ mit $C_G(X) \leq N_G(X)$. Ist $X = \{x\}$ einelementig, so schreibt man $C_G(x)$ statt $C_G(\{x\})$.
Man nennt $Z(G) := C_G(G) = \{g \in G : gx = xg \text{ für } x \in G\}$ das *Zentrum* von G. Es ist also $Z(G)$ eine abelsche Untergruppe von G.
Dagegen ist $N_G(G) = G$, denn für $g \in G$ ist $gG \subseteq G = gg^{-1}G \subseteq gG$, also $gG = G$ und analog $Gg = G$.

(v) Sind G, H Gruppen und ist $f : G \to H$ ein Homomorphismus, so ist $f(U) \leq H$ und $f^{-1}(V) \leq G$ für $U \leq G$, $V \leq H$. Insbesondere ist $f(G) \leq H$ und $\ker(f) := f^{-1}(\{1_H\}) = \{g \in G : f(g) = 1_H\} \leq G$. Man nennt $\ker(f)$ den *Kern* von f. Genau dann ist f injektiv, wenn $\ker(f) = \{1_G\}$ ist.
Im Spezialfall $G = \mathrm{Sym}(n)$ für ein $n \in \mathbb{N}$, $H = \{1, -1\}$ und $f = \mathrm{sgn}$ erhält man $\ker(f) = \{g \in \mathrm{Sym}(n) : \mathrm{sgn}(g) = 1\}$. Man nennt diese Untergruppe die *alternierende* Gruppe des Grades n. Schreibweise: $\mathrm{Alt}(n)$.
Im Spezialfall $G = \mathrm{GL}(n, K)$ für ein $n \in \mathbb{N}$ und einen Körper K, $H = K \setminus \{0\}$ und $f = \det$ erhält man $\ker(f) = \{g \in \mathrm{GL}(n, K) : \det(g) = 1\}$. Diese Untergruppe bezeichnet man als *spezielle lineare* Gruppe des Grades n über K. Schreibweise: $\mathrm{SL}(n, K)$.

Satz: *Alle Untergruppen von $(\mathbf{Z}, +)$ haben die Form $n\mathbf{Z}$ für ein $n \in \mathbb{N}_0$.*

Beweis: Für ein $n \in \mathbb{N}_0$ ist $n\mathbf{Z}$ das Bild des Homomorphismus $(\mathbf{Z}, +) \to (\mathbf{Z}, +)$, $k \mapsto nk$, also eine Untergruppe von $(\mathbf{Z}, +)$.
Sei umgekehrt $U \leq \mathbf{Z}$, o.B.d.A. $U \neq 0 = 0\mathbf{Z}$. Ist $u \in U \setminus \{0\}$, so ist auch $-u \in U$. Daher ist $U \cap \mathbb{N} \neq \emptyset$. Bekanntlich enthält jede nichtleere Teilmenge von $\mathbb{N}$ ein kleinstes Element. Sei $n := \min(U \cap \mathbb{N})$. Damit ist $n \in U$, $2n = n + n \in U$, $3n = 2n + n \in U$, $\ldots$, also $kn \in U$ für $k \in \mathbb{N}$. Daher ist auch $-kn \in U$ für $k \in \mathbb{N}$, also $n\mathbf{Z} \subseteq U$.
Ist $u \in U$ beliebig, so existieren nach Division mit Rest $q, r \in \mathbf{Z}$ mit $u = qn + r$ und $0 \leq r < n$. Wegen $n\mathbf{Z} \subseteq U$ ist $r = u - qn \in U$, also ist $r = 0$ nach Wahl von n. Folglich ist $u \in n\mathbf{Z}$. Dies zeigt: $U = n\mathbf{Z}$.

Satz 3.5 *Für jede Teilmenge X einer Gruppe G ist $\{x_1^{\varepsilon_1} x_2^{\varepsilon_2} \ldots x_k^{\varepsilon_k} : x_i \in X,\ \varepsilon_i = \pm 1,\ k \in \mathbb{N}_0\}$ der Durchschnitt aller Untergruppen von G, die X enthalten.*

Beweis: Ist $H \leq G$ mit $X \subseteq H$, so enthält H auch alle Elemente $x_1^{\varepsilon_1} x_2^{\varepsilon_2} \ldots x_k^{\varepsilon_k}$ mit $x_i \in X$, $\varepsilon_i = \pm 1$, $k \in \mathbb{N}_0$. Daher enthält der Durchschnitt D aller Untergruppen H von G mit $X \subseteq H$ auch alle Elemente dieser Form. Andrerseits ist die angegebene Menge offenbar eine Untergruppe U von G (1 = leeres Produkt, $k = 0$), die X enthält. Nach Definition von D ist also $D \subseteq U$.

Bemerkung: Man nennt die angegebene Menge die von X erzeugte Untergruppe von G und schreibt dafür $\langle X\rangle$; im Fall $X=\{x_1,\ldots,x_n\}$ schreibt man auch $\langle x_1,\ldots,x_n\rangle$.

Beispiel:

(i) Für Elemente $a,b\in G$ nennt man $[a,b]:=aba^{-1}b^{-1}$ den *Kommutator* von a und b. Beachte: $[a,b]ba=ab$.
Die von allen Kommutatoren $[a,b]$ $(a,b\in G)$ erzeugte Untergruppe von G nennt man die *Kommutatorgruppe* von G. Bezeichnung: G'.
Wegen $[a,b]^{-1}=[b,a]$ für $a,b\in G$ gilt:
$$G':=\{[a_1,b_1][a_2,b_2]\ldots[a_k,b_k]:a_1,b_1,\ldots,a_k,b_k\in G,\ k\in\mathbb{N}_0\}$$

(ii) Die von den Elementen $a=\left(\begin{smallmatrix}1&2&3&4\\2&1&4&3\end{smallmatrix}\right)$ und $b=\left(\begin{smallmatrix}1&2&3&4\\3&4&1&2\end{smallmatrix}\right)$ erzeugte Untergruppe V_4 von $\mathrm{Sym}(4)$ nennt man *Kleinsche Vierergruppe*.
$a^2=\mathrm{id}=b^2\Rightarrow a^{-1}=a,\ b^{-1}=b,\ ab=\left(\begin{smallmatrix}1&2&3&4\\4&3&2&1\end{smallmatrix}\right)=ba=:c$
Also $|V_4|=4$.

Verknüpfungstafel:

	1	a	b	c
1	1	a	b	c
a	a	1	c	b
b	b	c	1	a
c	c	b	a	1

Satz 3.6 *Seien G Gruppe, $H\leq G$, $a,b\in G$. Wir schreiben $a\sim_H b$, falls $a^{-1}b\in H$. Dann ist $\sim_H$ eine Äquivalenzrelation auf G, und für $g\in G$ ist $gH:=\{gh:h\in H\}$ die Äquivalenzklasse von g bzgl. $\sim_H$.*

Definition: *Die Äquivalenzklasse gH $(g\in G)$ nennt man* Linksnebenklasse *nach H in G. Die Menge der Linksnebenklassen bezeichnen wir mit G/H. Die Äquivalenzrelation nennt man* Linkskongruenz *modulo H.*

Bemerkung: Analog definiert man *Rechtskongruenz* modulo H: $a\ {}_H\!\sim b\Leftrightarrow ab^{-1}\in H$. Die Äquivalenzklassen haben in diesem Fall die Form $Hg=\{hg:h\in H\}$. Diese nennt man *Rechtsnebenklassen* nach H in G. Ihre Gesamtheit bezeichnet man mit $H\backslash G$.

Beweis: Reflexivität: Für $g\in G$ ist $g^{-1}g=1\in H$, also $g\sim_H g$.
Symmetrie: Seien $a,b\in G$ mit $a\sim_H b$. Dann ist $a^{-1}b\in H$, also auch $b^{-1}a=(a^{-1}b)^{-1}\in H$, d.h. $b\sim_H a$.
Transitivität: Seien $a,b,c\in G$ mit $a\sim_H b$ und $b\sim_H c$. Dann ist $a^{-1}b\in H$ und $b^{-1}c\in H$, also auch $a^{-1}c=(a^{-1}b)(b^{-1}c)\in H$, d.h. $a\sim_H c$.
Äquivalenzklasse: Für $g\in G$ und $h\in H$ ist $g^{-1}gh=h\in H$, also $g\sim_H gh$. Daher ist gH in der Äquivalenzklasse von g enthalten. Liegt umgekehrt $a\in G$ in der Äquivalenzklasse von g, so ist $g\sim_H a$, also $g^{-1}a\in H$. Folglich ist $a=gg^{-1}a\in gH$.

Beispiel: Für $k\in\mathbf{Z}$ und $n\in\mathbb{N}_0$ ist $k+n\mathbf{Z}$ die Links- und Rechtsnebenklasse von k nach $n\mathbf{Z}$, z.B.
$$2+5\mathbf{Z}=\{\ldots,-13,-8,-3,2,7,12,17,\ldots\}$$
In diesem Fall schreibt man $a\equiv b\pmod n$ statt $a\sim_{n\mathbf{Z}} b$.

Satz 3.7 *Sei G Gruppe und $H\leq G$.*

(i) Für $g\in G$ ist dann die Abbildung $H\to gH,\ h\mapsto gh$ eine Bijektion, insbesondere enthalten je zwei Linksnebenklassen nach H die gleiche Anzahl von Elementen, nämlich $|H|$.

(ii) Analog für Rechtsnebenklassen.

(iii) Die Abbildung $G/H\to H\backslash G,\ gH\mapsto Hg^{-1}$ ist bijektiv, insbesondere stimmt die Anzahl der Linksnebenklassen nach H mit der Anzahl der Rechtsnebenklassen nach H überein. Diese gemeinsame Anzahl nennt man den Index *von H in G. Schreibweise: $|G:H|$.*

Beweis:

(i) Die Abbildung $gH \to H,\ x \mapsto g^{-1}x$ ist offenbar Umkehrabbildung.

(ii) Klar.

(iii) Es genügt, die Wohldefiniertheit der Abbildung zu zeigen, denn die Umkehrabbildung wird gegeben durch $Hg \mapsto g^{-1}H$.
Sei also $aH = bH$, d.h. $a^{-1}b \in H$. Dann ist $Ha^{-1} = Ha^{-1}bb^{-1} \subseteq Hb^{-1}$ und analog $Hb^{-1} \subseteq Ha^{-1}$, also $Ha^{-1} = Hb^{-1}$.

Beispiel: Für $n \in \mathbb{N}$ ist $\mathbf{Z}/n\mathbf{Z} = \{0 + n\mathbf{Z}, 1 + n\mathbf{Z}, \ldots, (n-1) + n\mathbf{Z}\}$ und $|\mathbf{Z} : n\mathbf{Z}| = n$.

Satz 3.8 (Lagrange, 1736–1813) *Für jede Untergruppe H einer Gruppe G ist*

$$|G| = |H| \cdot |G : H|$$

(mit den üblichen Regeln für das Rechnen mit ∞). Im Fall $|G| < \infty$ sind also $|H|$ und $|G : H|$ Teiler von $|G|$.

Beweis: Jedes Element aus G liegt genau in einer Nebenklasse nach H. Jede Nebenklasse enthält genau $|H|$ Elemente. Insgesamt gibt es $|G : H|$ Nebenklassen.

Beispiel: $|V_4| = 4$, $|\operatorname{Sym}(4)| = 24$, also $|\operatorname{Sym}(4) : V_4| = 6$.

Definition 3.9 *Eine Gruppe G heißt* zyklisch*, falls $G = \langle g \rangle$ für $g \in G$.*

Beispiel:

(i) $\mathbf{Z} = \langle 1 \rangle = \langle -1 \rangle$.

(ii) Gruppen von Primzahlordnungen sind zyklisch; ist nämlich G eine Gruppe mit $|G| = p$ Primzahl, so wähle man $g \in G \setminus \{1\}$. Nach Lagrange ist $1 \neq \langle g \rangle \leq G$, also $1 \neq |\langle g \rangle| \mid |G| = p$, d.h. $|G| = |\langle g \rangle|$. Folglich ist $G = \langle g \rangle$ zyklisch.

(iii) 0 ist zyklisch.

Kapitel 4

Normalteiler und Faktorgruppen

Definition 4.1 *Für Teilmengen X, Y einer Gruppe G definiert man:*

$$XY := \{xy : x \in X, y \in Y\}, \quad X^{-1} := \{x^{-1} : x \in X\}.$$

Bemerkung: Für Teilmengen X, Y, Z von G ist dann:

$$(X^{-1})^{-1} = X, \quad (XY)^{-1} = Y^{-1}X^{-1}, \quad (XY)Z = X(YZ).$$

Satz 4.2 *Für eine Untergruppe N einer Gruppe G sind äquivalent:*

(1) $gNg^{-1} \subseteq N$ *für* $g \in G$.

(2) $gNg^{-1} = N$ *für* $g \in G$.

(3) $gN = Ng$ *für* $g \in G$.

(4) G/N *ist Gruppe bzgl. der Verknüpfung in 4.1.*

(5) Es gibt eine Gruppe H *und einen Homomorphismus* $f : G \to H$ *mit Kern* N.

Definition: *Sind diese Bedingungen erfüllt, so nennt man N eine* normale *Untergruppe oder einen* Normalteiler *von G.*
Schreibweise: $N \trianglelefteq G$ ($N \triangleleft G$ im Fall $N \neq G$).
Man bezeichnet G/N ($= N\backslash G$) als Faktorgruppe *von G nach N. Statt $gN = hN$ schreibt man auch $g \equiv h \pmod{N}$.*

Beweis:

(1)⇒(2): Sei (1) erfüllt. Für $g \in G$ ist dann $N = gg^{-1}N(g^{-1})^{-1}g^{-1} \subseteq gNg^{-1}$.

(2)⇒(3): Ist $g \in G$ und $gNg^{-1} = N$, so ist $gN = gNg^{-1}g = Ng$.

(3)⇒(4): Ist (3) erfüllt, so gilt für $g, h \in G$:

$$(gN)(hN) = gNhN = ghNN = ghN \in G/N.$$

Daher liegt eine Verknüpfung auf G/N vor. Die Assoziativität folgt aus 4.1. Für $g \in G$ ist $1N \cdot gN = 1gN = gN$ und $g^{-1}N \cdot gN = g^{-1}gN = 1N = N$. Daher ist G/N Gruppe mit neutralem Element $N = 1N$ und $(gN)^{-1} = g^{-1}N$ für $g \in G$.

(4)⇒(5): Sei (4) erfüllt. Wir setzen $H := G/N$ und definieren $f : G \to H$ durch $f(g) = gN$ für $g \in G$. Für $g, h \in G$ ist $(gN)(hN)$ eine Linksnebenklasse nach N, die gh enthält. Folglich ist $\underbrace{(gN)}_{=f(g)}\underbrace{(hN)}_{=f(h)} = \underbrace{ghN}_{=f(gh)}$. Dies zeigt, daß f ein Homomorphismus ist, insbesondere ist $f(1) = 1N = N$ das neutrale Element in G/N. Für $n \in N$ ist $f(n) = nN = N$, und für $g \in \ker(f)$ ist $gN = f(g) = N = 1N$, also $g \in N$. Also ist $N = \ker(f)$.

(5)⇒(1): Sei (5) erfüllt. Für $g \in G$ und $n \in N$ ist dann

$$f(gng^{-1}) = f(g)\underbrace{f(n)}_{=1}f(g)^{-1} = f(g)f(g)^{-1} = 1,$$

d.h. $gng^{-1} \in \ker(f) = N$.

Bemerkung: Den im Beweis vorkommenden Homomorphismus $f : G \to G/N,\ g \mapsto gN$ nennt man den *kanonischen* oder *natürlichen* Epimorphismus von G auf G/N. Für $g, h \in G$ ist $(gN)(hN) = ghN$ und $(gN)^{-1} = g^{-1}N$. Neutrales Element in G/N ist $1N = N$.

Beispiel:

(i) Für jede Gruppe G sind 1 und G Normalteiler in G. Ist $G \neq 1$ und sind 1 und G die einzigen Normalteiler von G, so nennt man G *einfach*. Nach dem Satz von Lagrange sind Gruppen von Primzahlordnungen stets einfach. Nicht einfache Gruppen kann man sich aus Normalteiler und Faktorgruppe zusammengesetzt denken: $G : \begin{array}{|c|}\hline G/N \\ \hline N \\ \hline\end{array}$. Aus dieser Sicht werden die einfachen Gruppen zu Elementarbausteinen für beliebige Gruppen. Die Bestimmung aller endlichen einfachen Gruppen war eines der größten Projekte in der Mathematik. Beteiligt waren ca. 50–100 Mathematiker. Die entsprechenden Arbeiten haben einen Umfang von ca. 10000 Seiten. Das Projekt wurde etwa 1980 erfolgreich abgeschlossen.

(ii) Ist G Gruppe und $H \leq Z(G)$, so ist $H \trianglelefteq G$ wegen (3), insbesondere $Z(G) \trianglelefteq G$, und in jeder abelschen Gruppe ist wegen $Z(G) = G$ jede Untergruppe normal.

(iii) Ist G Gruppe und $G' \leq H \leq G$, so ist $H \trianglelefteq G$ und G/H abelsch; für $g \in G$ und $h \in H$ ist nämlich

$$ghg^{-1} = ghg^{-1}h^{-1}h = [g, h]h \in H,$$

und für $a, b \in G$ gilt:

$$(aH)(bH) = abH = ab\underbrace{[b^{-1}, a^{-1}]}_{\in G' \leq H}H = abb^{-1}a^{-1}baH = baH = (bH)(aH).$$

Umgekehrt ist $G' \subseteq N$ für jeden Normalteiler N von G mit abelscher Faktorgruppe G/N. Für $a, b \in G$ ist nämlich

$$\begin{aligned}[a, b]N &= aba^{-1}b^{-1}N = (aN)(bN)(aN)^{-1}(bN)^{-1} = \\ &= (aN)(aN)^{-1}(bN)(bN)^{-1} = N,\end{aligned}$$

also $[a, b] \in N$. Nach Definition von G' ist also $G' \subseteq N$.
Insgesamt ist also G' der „kleinste“ Normalteiler von G mit abelscher Faktorgruppe.

(iv) Ist G Gruppe und $H \leq G$ mit $|G : H| = 2$, so ist $H \trianglelefteq G$; für $g \in H$ ist nämlich $gH = H = Hg$, und für $g \in G \setminus H$ ist $gH = G \setminus H = Hg$.

(v) Für jede Gruppe G und $H \leq G$ ist $H \trianglelefteq N_G(H)$; wegen $hHh^{-1} \subseteq H$ für $h \in H$ ist $H \leq N_G(H)$, und der Rest folgt aus der Definition von $N_G(H)$.

(vi) Für jede Gruppe G und jede Teilmenge X von G ist $C_G(X) \trianglelefteq N_G(X)$; für $x \in X$, $c \in C_G(X)$ und $n \in N_G(X)$ gilt nämlich:

$$ncn^{-1}x = nc\underbrace{n^{-1}xn}_{\in X}n^{-1} = nn^{-1}xncn^{-1} = xncn^{-1},$$

d.h. $ncn^{-1} \in C_G(X)$.

(vii) Für $n \in \mathbb{N}$ ist $\mathrm{Alt}(n) = \ker(\mathrm{sgn}) \trianglelefteq \mathrm{Sym}(n)$.

(viii) Für jeden Körper K und $n \in \mathbb{N}$ ist $\mathrm{SL}(n,K) = \ker(\det) \trianglelefteq \mathrm{GL}(n,K)$.

(ix) Ist $G = \mathrm{Sym}(3)$ und

$$H = \langle \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \rangle = \{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \},$$

so ist $H \ntrianglelefteq G$, denn

$$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}^{-1} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & \cdot & \cdot \end{pmatrix} \notin H.$$

Satz 4.3 (Homomorphiesatz) *Seien G, H Gruppen, $f : G \to H$ Homomorphismus und $N := \ker(f)$. Dann ist die Abbildung $F : G/N \to f(G)$, $gN \mapsto f(g)$ ein Isomorphismus; insbesondere ist $G/\ker(f) \cong f(G)$.*

Beweis: Sind $a, b \in G$ mit $aN = bN$, so ist $a^{-1}b \in N$, also $f(b) = f(aa^{-1}b) = f(a)\underbrace{f(a^{-1}b)}_{=1} = f(a)$. Daher ist F wohldefiniert und offenbar surjektiv. Für $x, y \in G$ ist

$$F(xN)F(yN) = f(x)f(y) = f(xy) = F(xyN) = F((xN)(yN)).$$

Daher ist F Epimorphismus. Ist $g \in G$ mit $gN \in \ker(F)$, so ist $1 = F(gN) = f(g)$, d.h. $g \in \ker(f) = N$, also $gN = N$. Folglich ist $\ker(F) = 1$, d.h. F ist injektiv.

Satz 4.4 (Klassifikationsatz für zyklische Gruppen) *Sei G eine zyklische Gruppe und $g \in G$ mit $G = \langle g \rangle$. Dann gilt:*

(i) Ist $|G| = \infty$, so ist $G \cong \mathbf{Z}$, $G = \{g^n : n \in \mathbf{Z}\}$ und $g^i \neq g^j$ für $i \neq j$.

(ii) Ist $|G| = n < \infty$, so ist $G \cong \mathbf{Z}/n\mathbf{Z}$, $G = \{1, g, g^2, \ldots, g^{n-1}\}$, und für $i, j \in \mathbf{Z}$ gilt: $g^i = g^j \;\Leftrightarrow\; i \equiv j \pmod{n}$.

Beweis: Nach 3.5 ist $G = \langle g \rangle = \{g^n : n \in \mathbf{Z}\}$. Wegen $g^m g^n = g^{m+n}$ für $m, n \in \mathbf{Z}$ ist die Abbildung $f : \mathbf{Z} \to G$, $n \mapsto g^n$ ein Epimorphismus. Ist f injektiv, so ist f ein Isomorphismus, insbesondere ist $|G| = \infty$ und $g^i \neq g^j$ für $i \neq j$. Sei also f nicht injektiv. Dann ist $\ker(f) = n\mathbf{Z}$ für ein $n \in \mathbb{N}$ nach 3.4. Nach 4.3 ist die Abbildung $F : \mathbf{Z}/n\mathbf{Z} \to G$, $k + n\mathbf{Z} \mapsto g^k$ ein Isomorphismus; insbesondere ist $G \cong \mathbf{Z}/n\mathbf{Z}$. Nach 3.7 ist $\mathbf{Z}/n\mathbf{Z} = \{0+n\mathbf{Z}, 1+n\mathbf{Z}, \ldots, (n-1)+n\mathbf{Z}\}$ und $|\mathbf{Z}/n\mathbf{Z}| = n$. Also ist $G = \{1, g, g^2, \ldots, g^{n-1}\}$ und $g^i = g^j \Leftrightarrow i - j \in n\mathbf{Z} \Leftrightarrow n \mid i - j$.

Satz 4.5 (Fermat, 1601–1665) *Seien G eine endliche Gruppe, $g \in G$ und $k \in \mathbf{Z}$. Dann gilt:*

$$g^k = 1 \Leftrightarrow |\langle g \rangle| \mid k.$$

Insbesondere ist $g^{|G|} = 1$.

Beweis: $|G| < \infty \Rightarrow |\langle g \rangle| < \infty$. Nach 4.4 gilt:

$$g^k = 1 = g^0 \;\Leftrightarrow\; k \equiv 0 \pmod{|\langle g \rangle|} \;\Leftrightarrow\; |\langle g \rangle| \;\big|\; k.$$

Definition: *Man nennt* $|\langle g \rangle|$ *die* Ordnung *von* g.

Bemerkung: Nach Lagrange ist $|\langle g \rangle| \;\big|\; |G|$, und nach 4.4 ist $|\langle g \rangle| = \inf\{n \in \mathbb{N} : g^n = 1\}$.

Satz 4.6 (Erster Isomorphiesatz) *Sei* G *Gruppe,* $H \leq G$, $N \trianglelefteq G$. *Dann ist* $HN \leq G$, $N \trianglelefteq HN$, $H \cap N \trianglelefteq H$ *und*

$$H/H \cap N \cong HN/N.$$

Beweis: Durch Einschränkung erhält man aus dem natürlichen Epimorphismus $f : G \to G/N$ einen Homomorphismus $g : H \to G/N$ mit Kern $H \cap N$ und Bild $\{hN : h \in H\}$. Insbesondere ist $H \cap N \trianglelefteq H$. Das Urbild von $\{hN : h \in H\}$ unter f ist $\{hn : h \in H, n \in N\} = HN$. Insbesondere ist $HN \leq G$. Wegen $N \trianglelefteq G$ ist $N \trianglelefteq HN$ und $HN/N = \{hnN : h \in H, n \in N\} = \{hN : h \in H\}$. 4.3 $\Rightarrow$ $H/H \cap N \cong HN/N$.

Bemerkung: Ist auch $H \trianglelefteq G$, so ist $HN \trianglelefteq G$; denn für $g \in G$ ist $gHN = HgN = HNg$.

Satz 4.7 (Zweiter Isomorphiesatz) *Für jede Gruppe* G *und jeden Normalteiler* N *von* G *ist die Abbildung* $H \mapsto H/N$ *eine Bijektion zwischen der Menge aller Untergruppen* H *von* G*, die* N *enthalten, und der Menge aller Untergruppen von* G/N. *Eine Untergruppe* H *von* G *mit* $N \subseteq H$ *ist genau dann normal in* G*, wenn* H/N *normal in* G/N *ist. In diesem Fall ist*

$$(G/N)/(H/N) \cong G/H.$$

Beweis: Sei $f : G \to G/N$, $g \mapsto gN$ der natürliche Epimorphismus. Für jede Untergruppe H von G mit $N \subseteq H$ ist $H/N = f(H) \leq G/N$ nach 3.4, und $H = f^{-1}(H/N)$. Für jede Untergruppe U von G/N ist umgekehrt $N = \ker(f) = f^{-1}(1) \leq f^{-1}(U) \leq G$ und $f(f^{-1}(U)) = U$. Daher ist die angegebene Abbildung bijektiv.
Ist $N \leq H \trianglelefteq G$ und $g \in G$, so gilt:

$$(gN)(H/N)(gN)^{-1} = f(g)f(H)f(g)^{-1} = f(gHg^{-1}) = f(H) = H/N.$$

Ist umgekehrt $H/N \trianglelefteq G/N$, so gilt für $g \in G$, $h \in H$:

$$ghg^{-1}N = (gN)(hN)(gN)^{-1} \in H/N,$$

also $ghg^{-1} \in H$. Daher ist $H \trianglelefteq G$.
Im Fall $H \trianglelefteq G$ hat der Epimorphismus $G \to G/N \to (G/N)/(H/N)$ den Kern H. Homomorphiesatz: $G/H \cong (G/N)/(H/N)$.

Satz 4.8 *Jede Untergruppe einer zyklischen Gruppe ist zyklisch.*

Beweis: Nach 4.4 ist jede zyklische Gruppe isomorph zu $\mathbf{Z}$ oder $\mathbf{Z}/n\mathbf{Z}$ für ein $n \in \mathbb{N}$. Daher genügt es zu zeigen, daß jede Untergruppe von $\mathbf{Z}$ und von $\mathbf{Z}/n\mathbf{Z}$ für $n \in \mathbb{N}$ zyklisch ist.
Nach 3.4 ist jede Untergruppe von $\mathbf{Z}$ von der Form $k\mathbf{Z} = \langle k \rangle$ für ein $k \in \mathbb{N}_0$, und nach 4.7 ist jede Untergruppe von $\mathbf{Z}/n\mathbf{Z}$ von der Form $k\mathbf{Z}/n\mathbf{Z} = \langle k + n\mathbf{Z} \rangle$ für ein $k \in \mathbb{N}_0$ mit $n\mathbf{Z} \subseteq k\mathbf{Z}$, d.h. $k \;\big|\; n$.

Satz 4.9 (Dedekind-Identität) *Für Untergruppen* U, V, W *einer Gruppe* G *gilt:*

$$U \subseteq W \;\Rightarrow\; W \cap UV = U(W \cap V).$$

Beweis: Sei $U \subseteq W$. Dann ist $U(W \cap V) \subseteq W$ und $U(W \cap V) \subseteq UV$, also $U(W \cap V) \subseteq W \cap UV$. Sei umgekehrt $w \in W \cap UV$, also $w = uv$ mit $u \in U,\ v \in V$. Dann ist $v = u^{-1}w \in W \cap V$, also $w = uv \in U(W \cap V)$.

Satz 4.10 (Dritter Isomorphiesatz, Zassenhaus) *Sei G Gruppe, $U, V \leq G$, $U_0 \trianglelefteq U$, $V_0 \trianglelefteq V$. Dann gilt*

$$U_0(U \cap V_0) \trianglelefteq U_0(U \cap V), \quad V_0(V \cap U_0) \trianglelefteq V_0(V \cap U),$$

$$(U_0 \cap V)(V_0 \cap U) \trianglelefteq U \cap V$$

und

$$\begin{aligned} U_0(U \cap V)/U_0(U \cap V_0) &\cong V_0(V \cap U)/V_0(V \cap U_0) \cong \\ &\cong (U \cap V)/(U_0 \cap V)(V_0 \cap U). \end{aligned}$$

Beweis: Wegen $U_0 \trianglelefteq U$ ist $U_0(U \cap V_0) \leq U$. Wegen $V_0 \trianglelefteq V$ ist $U \cap V_0 = (U \cap V) \cap V_0 \trianglelefteq U \cap V$ nach dem 1. Isomorphiesatz. Für $x \in U_0$ und $y \in U \cap V$ ist also

$$\begin{aligned} xyU_0(U \cap V_0)y^{-1}x^1 &= xU_0yy^{-1}(U \cap V_0)x^{-1} = U_0(U \cap V_0)x^{-1} = \\ &= (U \cap V_0)U_0x^{-1} = (U \cap V_0)U_0 = U_0(U \cap V_0). \end{aligned}$$

Daher ist $U_0(U \cap V_0) \trianglelefteq U_0(U \cap V)$. Wir schränken den natürlichen Epimorphismus $f : U_0(U \cap V) \to U_0(U \cap V)/U_0(U \cap V_0)$ ein zu einer Abbildung $g : U \cap V \to U_0(U \cap V)/U_0(U \cap V_0),\ x \mapsto xU_0(U \cap V_0)$. Dann ist g ein Homomorphismus mit Bild

$$\begin{aligned} (U \cap V)U_0(U \cap V_0)/U_0(U \cap V_0) &= (U \cap V)(U \cap V_0)U_0/U_0(U \cap V_0) = \\ &= (U \cap V)U_0/U_0(U \cap V_0) = \\ &= U_0(U \cap V)/U_0(U \cap V_0) \end{aligned}$$

und Kern

$$U_0(U \cap V_0) \cap (U \cap V) \overset{4.9}{=} (U_0 \cap U \cap V)(U \cap V_0) = (U_0 \cap V)(U \cap V_0).$$

Insbesondere ist $(U_0 \cap V)(U \cap V_0) \trianglelefteq U \cap V$. Aus dem Homomorphiesatz folgt:

$$(U \cap V)/(U_0 \cap V)(U \cap V_0) \cong U_0(U \cap V)/U_0(U \cap V_0).$$

Die übrigen Aussagen beweist man analog.

Kapitel 5

Normalreihen

Definition 5.1 *Unter einer* Subnormalreihe *einer Gruppe G versteht man eine endliche Folge $G = G_0 \trianglerighteq G_1 \trianglerighteq G_2 \trianglerighteq \ldots \trianglerighteq G_l = 1$ von Untergruppen von G mit $G_i \trianglelefteq G_{i-1}$ für $i = 1, \ldots, l$. Ist sogar $G_i \trianglelefteq G$ für $i = 0, \ldots, l$, so spricht man von einer* Normalreihe *von G. Die Gruppen G_{i-1}/G_i $(i = 1, \ldots, l)$ nennt man die* Faktoren *und die Zahl l der Faktoren die* Länge *der (Sub-)Normalreihe. Ist $G_{i-1} \neq G_i$ für $i = 1, \ldots, l$, so spricht man von einer (Sub-) Normalreihe* ohne Wiederholungen. *Eine (Sub-)Normalreihe $G = H_0 \trianglerighteq H_1 \trianglerighteq \ldots \trianglerighteq H_m = 1$ von G nennt man* Verfeinerung *der obigen (Sub-)Normalreihe, falls es eine injektive Abbildung $f : \{1, \ldots, l\} \to \{1, \ldots, m\}$ gibt mit $G_i = H_{f(i)}$ für $i = 1, \ldots, l$.*

Beispiel: $\mathrm{Sym}(4) \trianglerighteq \mathrm{Alt}(4) \trianglerighteq V_4 \trianglerighteq \langle \left(\begin{smallmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{smallmatrix}\right) \rangle \trianglerighteq 1$ ist eine Subnormalreihe, aber keine Normalreihe, denn $\langle \left(\begin{smallmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{smallmatrix}\right) \rangle \ntrianglelefteq \mathrm{Sym}(4)$.
$\mathrm{Sym}(4) \trianglerighteq \mathrm{Alt}(4) \trianglerighteq V_4 \trianglerighteq 1$ ist Normalreihe.

Definition 5.2 *Zwei Subnormalreihen $G = G_0 \trianglerighteq G_1 \trianglerighteq \ldots \trianglerighteq G_l = 1$ und $G = H_0 \trianglerighteq H_1 \trianglerighteq \ldots \trianglerighteq H_m = 1$ nennt man* isomorph, *wenn $l = m$ ist und ein $f \in \mathrm{Sym}(l)$ existiert mit $G_{i-1}/G_i \cong H_{f(i)-1}/H_{f(i)}$ für $i = 1, \ldots, l$.*

Beispiel: $\mathbf{Z}/6\mathbf{Z}$ hat isomorphe Subnormalreihen:

$$\mathbf{Z}/6\mathbf{Z} \trianglerighteq 2\mathbf{Z}/6\mathbf{Z} \trianglerighteq 1 \quad \text{und} \quad \mathbf{Z}/6\mathbf{Z} \trianglerighteq 3\mathbf{Z}/6\mathbf{Z} \trianglerighteq 1$$

Satz: (Verfeinerungssatz, Schreier) *Je zwei Subnormalreihen einer Gruppe G besitzen isomorphe Verfeinerungen.*

Beweis: Seien $G = G_0 \trianglerighteq G_1 \trianglerighteq \ldots \trianglerighteq G_l = 1$ und $G = H_0 \trianglerighteq H_1 \trianglerighteq \ldots \trianglerighteq H_m = 1$ Subnormalreihen der Gruppe G. Zwischen G_{i-1} und G_i fügt man jeweils die Gruppen $G_{ik} := G_i(G_{i-1} \cap H_k)$ $(k = 1, \ldots, m-1)$ ein, und zwischen H_{k-1} und H_k die Gruppen $H_{ik} = H_k(H_{k-1} \cap G_i)$ $(i = 1, \ldots, l-1)$ ein. Die Untergruppen $G_{i0} = G_{i-1}$, $G_{im} = G_i$, $H_{0k} = H_{k-1}$, $H_{lk} = H_k$ kommen bereits in den ursprünglichen Subnormalreihen vor. Es ist jeweils (4.10) $G_{ik} \trianglelefteq G_{i,k-1}$ und $H_{ik} \trianglelefteq H_{i-1,k}$, und es gilt: $G_{i,k-1}/G_{ik} \cong H_{i-1,k}/H_{ik}$.

Definition 5.3 *Eine* Kompositionsreihe *einer Gruppe G ist eine Subnormalreihe von G ohne Wiederholungen, die keine echte Verfeinerung ohne Wiederholungen besitzt.*

Beispiel:

(i) $\mathbf{Z}$ besitzt keine Kompositionsreihe; denn jede Subnormalreihe $\mathbf{Z} \trianglerighteq n_1\mathbf{Z} \trianglerighteq \ldots \trianglerighteq n_{i-1}\mathbf{Z} \trianglerighteq 0$ kann man zu $\mathbf{Z} \trianglerighteq n_1\mathbf{Z} \trianglerighteq \ldots \trianglerighteq n_{i-1}\mathbf{Z} \trianglerighteq n_{i-1}^2\mathbf{Z} \trianglerighteq 0$ verfeinern.

(ii) $\mathrm{Sym}(4) \trianglerighteq \mathrm{Alt}(4) \trianglerighteq V_4 \trianglerighteq \langle \left(\begin{smallmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{smallmatrix}\right) \rangle \trianglerighteq 1$ ist Kompositionsreihe.

(iii) Jede endliche Gruppe besitzt eine Kompositionsreihe.

Bemerkung: Nach dem 2. Isomorphiesatz ist eine Subnormalreihe genau dann eine Kompositionsreihe, wenn alle ihre Faktoren einfache Gruppen sind.

Satz: (Jordan-Hölder) *Besitzt die Gruppe G eine Kompositionsreihe, so sind je zwei Kompositionsreihen von G isomorph.*

Beweis: Nach Schreier besitzen je zwei Kompositionsreihen von G isomorphe Verfeinerungen. Indem man Wiederholungen streicht, kann man annehmen, daß die Verfeinerungen ohne Wiederholungen sind. Andrerseits besitzen Kompositionsreihen keine echte Verfeinerungen. Daher müssen die ursprünglichen Kompositionsreihen bereits isomorph sein.

Definition: *Die Faktoren einer Kompositionsreihe von G nennt man die* Kompositionsfaktoren *von G und die Länge einer Kompositionsreihe die* Kompositionslänge *von G. Nach Jordan-Hölder hängen diese Begriffe nicht von der Wahl der Kompositionsreihe ab.*

Definition 5.4 *Eine Gruppe heißt* auflösbar*, wenn sie eine Subnormalreihe mit abelschen Faktoren besitzt.*

Satz: *Eine endliche Gruppe G ist genau dann auflösbar, wenn alle Kompositionsfaktoren von G Primzahlordnung haben.*

Beweis:

„$\Leftarrow$“: Trivial, da Gruppen von Primzahlordnung zyklisch und damit isomorph zu $\mathbf{Z}/p\mathbf{Z}$ für eine Primzahl p sind.

„$\Rightarrow$“: Sei G auflösbar, d.h. G besitzt Subnormalreihe mit abelschen Faktoren, o.B.d.A. ohne Wiederholungen. Diese verfeinern wir zu einer Kompositionsreihe. Da Untergruppen und Faktorgruppen abelscher Gruppen wieder abelsch sind, besitzt die Verfeinerung auch abelsche Faktoren. Es genügt also zu zeigen, daß jede abelsche einfache Gruppe H Primzahlordnung hat.
Für $1 \neq h \in H$ ist $1 \neq \langle h \rangle \trianglelefteq H$, d.h. $H = \langle h \rangle$ zyklisch, etwa $H \cong \mathbf{Z}/n\mathbf{Z}$ für ein $n \in \mathbb{N}$, $n \neq 1$. Für jeden Primteiler p von n ist $p\mathbf{Z}/n\mathbf{Z} \underset{\neq}{\triangleleft} \mathbf{Z}/n\mathbf{Z}$ also $p\mathbf{Z}/n\mathbf{Z} = 0$, d.h. $p\mathbf{Z} = n\mathbf{Z}$, d.h. $p = n$ und $|H| = |\mathbf{Z}/n\mathbf{Z}| = n = p$.

Beispiel:

(i) Abelsche Gruppen sind auflösbar.

(ii) $\mathrm{Sym}(3)$ und $\mathrm{Sym}(4)$ sind auflösbar:
$\mathrm{Sym}(3) \trianglerighteq \mathrm{Alt}(3) \trianglerighteq 1$
$\mathrm{Sym}(4) \trianglerighteq \mathrm{Alt}(4) \trianglerighteq V_4 \trianglerighteq \langle \left(\begin{smallmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{smallmatrix}\right) \rangle \trianglerighteq 1$

Definition 5.5 *Die* höheren Kommutatorgruppen *einer Gruppe G werden definiert durch*

$$G^{(0)} := G, \quad G^{(1)} := G', \quad G^{(2)} := (G')' = G'',$$
$$G^{(i+1)} := \left(G^{(i)}\right)' \quad \text{für } i \geq 0.$$

Bemerkung: Durch Induktion erhält man leicht:

(i) $G^{(i)} \trianglelefteq G$ für $i \in \mathbb{N}_0$.

(ii) $H \leq G \;\Rightarrow\; H^{(i)} \leq G^{(i)}$ für $i \in \mathbb{N}_0$.

(iii) $N \trianglelefteq G \;\Rightarrow\; (G/N)^{(i)} = G^{(i)}N/N$ für $i \in \mathbb{N}_0$.

Satz: *Eine Gruppe G ist genau dann auflösbar, wenn $G^{(s)} = 1$ für ein $s \in \mathbb{N}_0$.*

Beweis:

„$\Rightarrow$“: Sei G auflösbar und $G = G_0 \trianglerighteq G_1 \trianglerighteq \ldots \trianglerighteq G_r = 1$ eine Subnormalreihe mit abelschen Faktoren. Es genügt zu zeigen: $G^{(i)} \subseteq G_i$, denn dann ist $G^{(r)} = 1$. Offenbar ist $G^{(0)} = G = G_0$. Sei also $i \in \mathbb{N}_0$ und $G^{(i)} \subseteq G_i$. Dann ist $G^{(i+1)} = \left(G^{(i)}\right)' \subseteq (G_i)' \subseteq G_{i+1}$, da G_i/G_{i+1} abelsch ist (siehe 4.2, Beispiel (iii)). Mit Induktion folgt die Behauptung.

„$\Leftarrow$“: Falls $G^{(s)} = 1$ ist, so ist $G = G^{(0)} \trianglerighteq G^{(1)} \trianglerighteq \ldots \trianglerighteq G^{(s)} = 1$ eine Normalreihe von G mit abelschen Faktoren.

Satz 5.6 *Untergruppen und Faktorgruppen auflösbarer Gruppen sind auflösbar.*

Beweis: Sei G auflösbare Gruppe und $s \in \mathbb{N}_0$ mit $G^{(s)} = 1$. Für $H \leq G$ ist dann $H^{(s)} \subseteq G^{(s)} = 1$, und für $N \trianglelefteq G$ ist $(G/N)^{(s)} = G^{(s)}N/N = 1N/N = N/N = \{1\}$.

Bemerkung:

(i) Wir werden später sehen, daß ein enger Zusammenhang zwischen der Auflösbarkeit von Gruppen und der Auflösbarkeit von Gleichungen besteht.

(ii) Burnside 1911: Gruppen der Ordnung $p^a q^b$ (p, q Primzahlen, $a, b \in \mathbb{N}$) sind auflösbar.

(iii) Feit-Thompson 1963: Gruppen ungerader Ordnung sind auflösbar. (Der Beweis hat 254 Seiten.)

Satz 5.7 *Sei G eine Gruppe und $N \trianglelefteq G$. Genau dann ist G auflösbar, wenn N und G/N auflösbar sind.*

Beweis:

„$\Rightarrow$“: Satz 5.6.

„$\Leftarrow$“: Seien N und G/N auflösbar und $r, s \in \mathbb{N}_0$ mit $N^{(r)} = 1$ und $\underbrace{(G/N)^{(s)}}_{=G^{(s)}N/N} = 1$. Dann ist

$G^{(s)} \subseteq N$ und $G^{(r+s)} = \left(G^{(s)}\right)^{(r)} \subseteq N^{(r)} = 1$.

Kapitel 6

Gruppenoperationen

Definition 6.1 *Eine* Operation *(action) der Gruppe G auf der nichtleeren Menge Ω ist eine Abbildung $G \times \Omega \to \Omega,\ (g,\omega) \mapsto {}^g\omega$ mit folgenden Eigenschaften:*

(i) ${}^1\omega = \omega$ *für* $\omega \in \Omega$.

(ii) ${}^a({}^b\omega) = {}^{ab}\omega$ *für* $a, b \in G,\ \omega \in \Omega$.

Man sagt auch: „G operiert *auf Ω“ und „Ω ist eine G-Menge“. Der* Kern *der Operation ist* $\{g \in G : {}^g\omega = \omega$ *für* $\omega \in \Omega\}$.
Die Operation heißt

(a) treu*, wenn sie den Kern 1 hat.*

(b) trivial*, wenn sie den Kern G hat.*

(c) transitiv*, wenn zu je zwei $\alpha, \beta \in \Omega$ ein $g \in G$ existiert mit ${}^g\alpha = \beta$.*

Für $\omega \in \Omega$ nennt man ${}^G\omega = \{{}^g\omega : g \in G\}$ die Bahn *(orbit) von ω unter G und $|{}^G\omega|$ ihre* Länge.

Bemerkung: Man beachte die Analogie zur Skalarmultiplikation bei Vektorräumen.

Beispiel:

(i) $\Omega = \{1, \ldots, n\},\ G = \mathrm{Sym}(n),\ {}^g\omega = g(\omega)$.

(ii) G Gruppe, $H \leq G,\ \Omega = G/H,\ {}^g(aH) = gaH$.

(iii) G Gruppe, $\Omega = G,\ {}^gx = gxg^{-1}$. Diese Operation nennt man *Konjugation* und die entsprechenden Bahnen *Konjugationsklassen*. Sind $a, x, y \in G$ mit $axa^{-1} = y$, so sagt man, x ist zu y *konjugiert*. Die Anzahl der Konjugationsklassen nennt man die *Klassenzahl* von G.

Satz: *Gegeben sei eine Operation der Gruppe G auf der Menge $\Omega \neq \emptyset$. Definiert man $\alpha \sim \beta$, falls ein $g \in G$ existiert mit ${}^g\alpha = \beta$, so ist $\sim$ eine Äquivalenzrelation auf Ω. Die Äquivalenzklassen bzgl. $\sim$ sind die Bahnen von Ω unter G. Die Operation ist genau dann transitiv, wenn es nur eine einzige Bahn gibt.*

Beweis: Reflexivität: Für $\alpha \in \Omega$ ist $\alpha \sim \alpha$ wegen ${}^1\alpha = \alpha$.
Symmetrie: Seien $\alpha, \beta \in \Omega$ mit $\alpha \sim \beta$, also ${}^g\alpha = \beta$ für ein $g \in G$. Dann ist ${}^{g^{-1}}\beta = {}^{g^{-1}}({}^g\alpha) = {}^{g^{-1}g}\alpha = {}^1\alpha = \alpha$, also $\beta \sim \alpha$.
Transitivität: Seien $\alpha, \beta, \gamma \in \Omega$ mit $\alpha \sim \beta$ und $\beta \sim \gamma$. Dann existieren $g, h \in G$ mit ${}^g\alpha = \beta$ und ${}^h\beta = \gamma$. Folglich ist ${}^{hg}\alpha = {}^h({}^g\alpha) = {}^h\beta = \gamma$.

Satz 6.2 *Operiert die Gruppe G auf der Menge $\Omega \neq \emptyset$, so gilt:*

(i) Für $g \in G$ ist die Abbildung $\tau_g : \Omega \to \Omega,\ \omega \mapsto {}^g\omega$ bijektiv, d.h. $\tau_g \in \mathrm{Sym}(\Omega)$.

(ii) Die Abbildung $\tau : G \to \mathrm{Sym}(\Omega),\ g \mapsto \tau_g$ ist ein Homomorphismus.

(iii) $\ker(\tau)$ ist der Kern der Operation.

Beweis: Für $g, h \in G$ und $\omega \in \Omega$ ist $(\tau_g \circ \tau_h)(\omega) = {}^g({}^h\omega) = {}^{gh}\omega = \tau_{gh}(\omega)$ und $\tau_1(\omega) = {}^1\omega = \omega$, also $\tau_g \circ \tau_h = \tau_{gh}$ und $\tau_1 = \mathrm{id}_\Omega$. Insbesondere ist $\tau_g \circ \tau_{g^{-1}} = \tau_{gg^{-1}} = \tau_1 = \mathrm{id}_\Omega$ und analog $\tau_{g^{-1}} \circ \tau_g = \mathrm{id}_\Omega$. Folglich ist τ_g bijektiv und $(\tau_g)^{-1} = \tau_{g^{-1}}$. Ferner ist $\tau : G \to \mathrm{Sym}(\Omega),\ g \mapsto \tau_g$ wegen $\tau_g \circ \tau_h = \tau_{gh}$ für $g, h \in G$ ein Homomorphismus. Ein Element $g \in G$ liegt genau dann im Kern von τ, wenn $\tau_g = \mathrm{id}_\Omega$, d.h. wenn ${}^g\omega = \omega$ für $\omega \in \Omega$ ist.

Satz 6.3 (Cayley) *Jede Gruppe ist zu einer Untergruppe einer symmetrischen Gruppe isomorph.*

Beweis: Jede Gruppe G operiert auf sich selbst durch ${}^g\alpha = g\alpha$ für $g, \alpha \in G$. Diese Operation ist treu, denn aus ${}^g\alpha = \alpha$ für $\alpha \in G$ folgt $g = 1$. Nach 6.2 gibt es einen Monomorphismus $\tau : G \to \mathrm{Sym}(\Omega)$, d.h. $G \cong \tau(G) \leq \mathrm{Sym}(\Omega)$.

Satz 6.4 *Operiert die Gruppe G auf der Menge $\Omega \neq \emptyset$, so gilt:*

(i) Für $\omega \in \Omega$ ist der Stabilisator $G_\omega := \{g \in G : {}^g\omega = \omega\} \leq G$.

(ii) Für $\omega \in \Omega$ ist die Abbildung $G/G_\omega \to {}^G\omega,\ gG_\omega \mapsto {}^g\omega$ bijektiv; insbesondere ist $|{}^G\omega| = |G : G_\omega|$.

(iii) Ist die Teilmenge R von Ω ein Repräsentantensystem für die Bahnen, d.h. enthält R aus jeder Bahn genau ein Element, so hat man die Bahnengleichung*:*

$$|\Omega| = \sum_{\omega \in R} |G : G_\omega|.$$

Beweis:

(i) Sei $\omega \in \Omega$. Wegen ${}^1\omega = \omega$ ist dann $1 \in G_\omega$, und für $a, b \in G_\omega$ ist

$${}^{ab^{-1}}\omega = {}^{ab^{-1}}({}^b\omega) = {}^{ab^{-1}b}\omega = {}^a\omega = \omega,$$

also $ab^{-1} \in G_\omega$.

(ii) Seien $\omega \in \Omega$ und $g, h \in G$ mit $gG_\omega = hG_\omega$, d.h. $g^{-1}h \in G_\omega$. Dann ist ${}^g\omega = {}^g({}^{g^{-1}h}\omega) = {}^{gg^{-1}h}\omega = {}^h\omega$, d.h. die Abbildung ist wohldefiniert und offenbar surjektiv. Sind $g, h \in G$ mit ${}^g\omega = {}^h\omega$, so ist

$${}^{g^{-1}h}\omega = {}^{g^{-1}}({}^h\omega) = {}^{g^{-1}}({}^g\omega) = {}^{g^{-1}g}\omega = {}^1\omega = \omega,$$

d.h. $g^{-1}h \in G_\omega$. Folglich ist $gG_\omega = hG_\omega$. Dies zeigt, daß die Abbildung auch injektiv ist.

(iii) Die Anzahl der Elemente in Ω ist die Summe der Bahnlängen, und für $\omega \in \Omega$ hat die Bahn von ω nach (ii) genau die Länge $|G : G_\omega|$.

Beispiel:

(i) Operiert die Gruppe G auf sich selbst durch ${}^g x = gxg^{-1}$ für $g, x \in G$, so ist der Stabilisator von x genau $\{g \in G : gxg^{-1} = x\} = \{g \in G : gx = xg\} = C_G(x)$. Die Bahngleichung hat hier die Form

$$|G| = \sum_{x \in R} |G : C_G(x)|,$$

dabei ist R ein Repräsentantensystem für die Konjugationsklassen von G. Diese Gleichung nennt man auch *Klassengleichung* von G. Für $x \in G$ gilt:

$$|G : C_G(x)| = 1 \;\Leftrightarrow\; G = C_G(x) \;\Leftrightarrow\; \forall g \in G : xg = gx \;\Leftrightarrow\; x \in Z(G).$$

(ii) Jede Gruppe G operiert auf $\mathcal{P}(G)$ durch ${}^g M = gMg^{-1}$ für $g \in G,\ M \subseteq G$. Auch hier spricht man von Konjugation und Konjugationsklassen. Für $M \subseteq G$ ist der Stabilisator von M die Menge $\{g \in G : gMg^{-1} = M\} = \{g \in G : gM = Mg\} = N_G(M)$.

Satz 6.5 *Sei p Primzahl und G eine Gruppe der Ordnung p^k für ein $k \in \mathbb{N}$. Dann gilt: $p \mid |Z(G)|$; insbesondere ist $Z(G) \neq 1$. Ferner ist G auflösbar.*

Beweis: Betrachte die Klassengleichung $|G| = \sum_{x \in R} |G : C_G(x)|$. Die Bahnen der Länge 1 bestehen gerade aus den Elementen in $Z(G)$. Für $x \in R \setminus Z(G)$ ist $|G : C_G(x)|$ nach Lagrange eine von 1 verschiedene Potenz von p. Es ergibt sich:

$$0 \equiv |G| \equiv \sum_{x \in R} |G : C_G(x)| \equiv |Z(G)| \pmod p.$$

Also ist $p \mid |Z(G)|$ und $Z(G) \neq 1$.
Die Auflösbarkeit zu G zeigen wir durch Induktion nach k. Offenbar ist jede Gruppe der Ordnung 1 oder p auflösbar. Sei also $k \in \mathbb{N}$ und schon gezeigt, daß Gruppen der Ordnung p^l mit $l < k$ auflösbar sind. Ist G eine Gruppe der Ordnung p^k, so ist $|Z(G)| \neq 1$, also $|G/Z(G)| = p^l$ für ein $l < k$. Nach Induktion ist $G/Z(G)$ auflösbar. Da $Z(G)$ abelsch ist, folgt die Auflösbarkeit von G aus 5.7.

Definition: *Gruppen der Ordnung p^k für eine Primzahl p und ein $k \in \mathbb{N}_0$ nennt man auch* p-Gruppen. *Elemente der Ordnung p^l für ein $l \in \mathbb{N}_0$ nennt man auch* p-Elemente.

Satz 6.6 (Sylow, 1832–1918) *Sei p Primzahl und G eine Gruppe der Ordnung $n = p^a m$ ($a \in \mathbb{N}_0,\ m \in \mathbb{N}, p \nmid m$). Dann gilt für $b \leq a$ ($b \in \mathbb{N}_0$):*

(i) Die Anzahl $z_G(p^b)$ der Untergruppen der Ordnung p^b von G ist kongruent zu 1 modulo p: $z_G(p^b) \equiv 1 \pmod p$; insbesondere enthält G eine Untergruppe der Ordnung p^b.

(ii) Jede Untergruppe der Ordnung p^b ist in einer Untergruppe der Ordnung p^a enthalten. (Die Untergruppen der Ordnung p^a bezeichnet man als p-Sylowgruppen *von G.)*

(iii) Je zwei p-Sylowgruppen von G sind in G konjugiert; insbesondere ist $|G : N_G(P)|$ für jede p-Sylowgruppe P von G die Anzahl der p-Sylowgruppen von G: $z_G(p^a) = |G : N_G(P)|$.

Beweis:

(i) Sei $\Omega := \{M \subseteq G : |M| = p^b\}$, also $|\Omega| = \binom{n}{p^b}$. Dann operiert G auf Ω durch ${}^gM = gM$ für $g \in G,\ M \in \Omega$. Wir bezeichnen mit $\mathcal{R}$ ein Repräsentantensystem für die Bahnen. Bahnengleichung: $\binom{n}{p^b} = |\Omega| = \sum_{M \in \mathcal{R}} |G : G_M|$.

Beh. 1: $M \in \mathcal{R} \ \Rightarrow\ |G_M| \mid p^b$.

Bew.: Wegen $G_M = \{g \in G : gM = M\}$ ist $G_M M = M$. Daher operiert G_M auf M durch ${}^gm = gm$ für $g \in G,\ m \in M$, und für $m \in M$ ist $G_M m$ die Bahn von m. Daher hat jede Bahn die Länge $|G_M|$. Daher ist auch $|M| = p^b$ durch $|G_M|$ teilbar.

Beh. 2: Im Fall $|G_M| = p^b$ enthält die Bahn von $M \in \Omega$ eine Untergruppe von G.

Bew.: Im Fall $|G_M| = p^b$ operiert G_M transitiv auf M, d.h. $M = G_M m$ für ein $m \in M$. Dann ist $m^{-1}M = m^{-1}G_M m$ eine Untergruppe von G in der Bahn von M.

Beh. 3: Enthält die Bahn von $M \in \Omega$ eine Untergruppe U von G, so ist G/U diese Bahn. Insbesondere ist $|G : G_M| = |G : U| = p^{a-b}m$, und U ist die einzige Untergruppe dieser Bahn.

Bew.: Unter den obigen Voraussetzungen stimmt die Bahn von M mit der Bahn von U, d.h. mit G/U überein. Daher ist

$$|G : G_M| = |\{gM : g \in G\}| = |\{gU : g \in G\}| = |G : U| = p^{a-b}m.$$

Ist $gU \leq G$, so ist $1 \in gU$, also $gU = 1U = U$.

Beh. 4: $\binom{n}{p^b} \equiv p^{a-b}mz_G(p^b) \pmod{p^{a-b+1}m}$.

Bew.: Enthält die Bahn von $M \in \Omega$ keine Untergruppe von G, so gilt nach Beh. 1 und Beh. 2: $|G_M| \mid p^{b-1}$, also $|G : G_M| \equiv 0 \pmod{p^{a-b+1}m}$ nach Lagrange. Enthält die Bahn von $M \in \Omega$ eine Untergruppe von G, so gilt nach Beh. 3: $|G : G_M| = p^{a-b}m$. Bahnengleichung:

$$\binom{n}{p^b} = \sum_{M \in \mathcal{R}} |G : G_M| \equiv z_G(p^b)p^{a-b}m \pmod{p^{a-b+1}m}.$$

Beh. 5: $z_G(p^b) \equiv 1 \pmod{p}$.

Bew.: Ist H eine beliebige Gruppe der Ordnung n, so gilt nach Beh. 4:

$$p^{a-b}mz_H(p^b) \equiv \binom{n}{p^b} \equiv p^{a-b}mz_G(p^b) \pmod{p^{a-b+1}m}.$$

Wir setzen $H := \mathbf{Z}/n\mathbf{Z}$. Nach Aufgabe 3 von Blatt 4 enthält H genau eine Untergruppe der Ordnung p^b, d.h. $z_H(p^b) = 1$. Folglich ist

$$p^{a-b}mz_G(p^b) \equiv p^{a-b}m \pmod{p^{a-b+1}m},$$

d.h.

$$p^{a-b+1}m \mid p^{a-b}mz_G(p^b) - p^{a-b}m.$$

Schließlich: $p \mid z_G(p^b) - 1$, d.h. $z_G(p^b) \equiv 1 \pmod{p}$.

(ii) Seien $U \leq G,\ |U| = p^b,\ P \leq G,\ |P| = p^a$. Dann operiert G transitiv auf $\Omega := \{gPg^{-1} : g \in G\}$ durch ${}^x(gPg^{-1}) = xgPg^{-1}x^{-1}$ für $x, g \in G$; dabei ist $P \in \Omega$ und $G_P = N_G(P)$, also $|\Omega| = |G : N_G(P)|$. Wegen $P \leq N_G(P)$ ist $|P| \mid |N_G(P)|$, also $p \nmid |G : N_G(P)|$ nach Lagrange. Analog operiert U auf Ω durch ${}^u(gPg^{-1}) = ugPg^{-1}u^{-1}$. Sei $\mathcal{R}$ ein Repräsentantensystem für die Bahnen. Bahnengleichung: $|\Omega| = \sum_{Q \in \mathcal{R}} |U : U_Q|$. Nach Lagrange ist $|U : U_Q| \mid |U| = p^b$ für $Q \in \mathcal{R}$, und wegen $p \nmid |\Omega|$ ist $|U : U_Q| = 1$ für mindestens ein $Q \in \mathcal{R}$. Dann ist $U = U_Q$, also $uQu^{-1} = Q$ für $u \in U$. Folglich ist $U \leq N_G(Q)$. Andrerseits ist $Q \trianglelefteq N_G(Q)$. Nach dem 1. Isomorphiesatz ist $UQ \leq N_G(Q)$ und $|UQ/Q| = |U/U \cap Q|$; insbesondere ist $|UQ| = |UQ : Q| \cdot |Q| = |U : U \cap Q| \cdot |Q|$ p-Potenz mit $|UQ| \mid |G|$ nach Lagrange, also $|UQ| \mid p^a$. Wegen $|Q| = |P| = p^a$ und $Q \leq UQ$ folgt $Q = UQ$, d.h. $U \leq Q$. Wegen $Q \in \Omega$ ist auch Q p-Sylowgruppe von G.

(iii) Ist $|U| = p^a$, so zeigt der Beweis von (ii): $U \leq Q = gPg^{-1}$ für ein $g \in G$. Wegen $|U| = |Q| = p^a$ folgt: $U = gPg^{-1} \in \Omega$, und $|\Omega| = |G : N_G(P)|$ ist die Anzahl der p-Sylowgruppen von G.

Satz 6.7 (Cauchy, 1789–1857) *Ist G eine endliche Gruppe der Ordnung n und p ein Primteiler von n, so enthält G ein Element der Ordnung p.*

Beweis: Nach Sylow enthält G unter diesen Voraussetzungen eine Untergruppe U der Ordnung p. Nach 3.9 ist $U = \langle g \rangle$ für ein $g \in U$.

Satz 6.8 *Für beliebige Primzahlen p, q sind Gruppen der Ordnung pq oder p^2q auflösbar.*

Beweis:

(i) Sei G Gruppe, $|G| = pq$, p, q Primzahlen, o.B.d.A. $p > q$ wegen 6.5. Sylow: $z_G(p) \mid |G| = pq$ und $z_G(p) \equiv 1 \pmod p$, also $z_G(p) \in \{1, q\}$. Wegen $q < p$ ist $p \nmid q - 1$, also $q \not\equiv 1 \pmod p$. Daher ist $z_G(p) = 1$, d.h. G besitzt genau eine p-Sylowgruppe P. Dann ist $G = N_G(P)$ und $P \trianglelefteq G$. Wegen $|P| = p$ und $|G/P| = q$ sind $P, G/P$ auflösbar, also auch G auflösbar nach 5.7.

(ii) Sei G Gruppe, $|G| = p^2q$, p, q Primzahlen, o.B.d.A. $p \neq q$ wegen 6.5. Sylow: $z_G(p^2) \in \{1, q\}$, $z_G(q) \in \{1, p, p^2\}$. Falls $z_G(p^2) = 1$, so erhält G genau eine p-Sylowgruppe P, und wegen $G = N_G(P)$ ist $P \trianglelefteq G$. Nach 6.5 sind dann P und G/P auflösbar, also auch G nach 5.7.
Sei also $z_G(p^2) = q$. Sylow: $q = z_G(p^2) \equiv 1 \pmod p$, also $p \mid q - 1$ und $p < q$. Dann $q \nmid p - 1$, also $z_G(q) \neq p$ nach Sylow. Annahme: $z_G(q) = p^2$. Sind Q_1, Q_2 verschiedene q-Sylowgruppen von G, so ist $|Q_1 \cap Q_2| < |Q_1| = q$, also $|Q_1 \cap Q_2| = 1$. Daher enthalten die q-Sylowgruppen von G insgesamt $1 + p^2(q-1) = |G| - p^2 + 1$ Elemente. Andrerseits enthält jede p-Sylowgruppe von G genau p^2 Elemente. Daher kann es nur noch eine p-Sylowgruppe geben im Widerspruch zu $z_G(p^2) = q$. Also ist $z_G(q) = 1$, und wie oben schließt man, daß G auflösbar ist.

Kapitel 7

Permutationsgruppen

Definition 7.1 *Seien $n \in \mathbb{N}$ und $g \in \mathrm{Sym}(n)$. Man nennt g einen* Zyklus *der* Länge *k oder einen k-*Zyklus*, falls paarweise verschiedene Elemente $x_1, \ldots, x_k \in \{1, \ldots, n\}$ existieren mit $g(x_1) = x_2,\ g(x_2) = x_3,\ \ldots,\ g(x_{k-1}) = x_k,\ g(x_k) = x_1$ und $g(x) = x$ sonst. Schreibweise: $g = (x_1, \ldots, x_k)$.*
Zyklen der Länge 2 nennt man Transpositionen*. Zwei Zyklen $(x_1, \ldots, x_k)$ und $(y_1, \ldots, y_l)$ mit $\{x_1, \ldots, x_k\} \cap \{y_1, \ldots, y_l\} = \emptyset$ nennt man* disjunkt.

Bemerkung:

(i) $(x_1, \ldots, x_k) = (x_2, \ldots, x_k, x_1) = \ldots = (x_k, x_1, \ldots, x_{k-1})$.

(ii) $(x_1, \ldots, x_k), (y_1, \ldots, y_l)$ disjunkt $\Rightarrow$ $(x_1, \ldots, x_k)(y_1, \ldots, y_l) = (y_1, \ldots, y_l)(x_1, \ldots, x_k)$.

(iii) Es ist klar, daß man jede Permutation $g \in \mathrm{Sym}(n)$ als Produkt disjunkter Zyklen schreiben kann, z.B.

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 \\ 8 & 4 & 9 & 5 & 2 & 6 & 3 & 1 & 10 & 7 & 12 & 11 \end{pmatrix} = $$
$$= (1,8)(2,4,5)(3,9,10,7)(6)(11,12).$$

Die dabei auftretenden Zyklen sind (bis auf die Reihenfolge und Zyklen der Länge 1) eindeutig. Wir ordnen die Längen der Größe nach: $k_1 \geq k_2 \geq \ldots \geq k_l,\ k_1 + k_2 + \ldots + k_l = n$. Dann nennt man $(k_1, \ldots, k_l)$ den *Typ* von g.

Satz: *Seien $n \in \mathbb{N}$ und $g, h \in \mathrm{Sym}(n)$. Genau dann sind g, h in $\mathrm{Sym}(n)$ konjugiert, wenn sie den gleichen Typ haben.*

Beweis:

„$\Rightarrow$" Sei $g = (x_1, \ldots, x_{k_1})(x_{k_1+1}, \ldots, x_{k_1+k_2}) \ldots$ die Zyklenzerlegung von g. Für $f \in \mathrm{Sym}(n)$ gilt dann:
$$fgf^{-1} = (f(x_1), \ldots, f(x_{k_1}))(f(x_{k_1+1}), \ldots, f(x_{k_1+k_2})) \ldots,$$
denn z.B. $fgf^{-1}(f(x_1)) = fg(x_1) = f(x_2)$.

„$\Leftarrow$" Die Zyklenzerlegungen von g, h seien $g = (x_1, \ldots, x_{k_1})(x_{k_1+1}, \ldots, x_{k_1+k_2}) \ldots$ und $h = (y_1, \ldots, y_{k_1})(y_{k_1+1}, \ldots, y_{k_1+k_2}) \ldots$. Setzt man $f := \left(\begin{smallmatrix} x_1 & \cdots & x_n \\ y_1 & \cdots & y_n \end{smallmatrix}\right)$, so ist $fgf^{-1} = h$ wie in „$\Rightarrow$".

Bemerkung: Es gibt also für $n \in \mathbb{N}$ eine Bijektion zwischen der Menge der Konjugationsklassen von $\mathrm{Sym}(n)$ und der Menge der Partitionen von n. (Eine *Partition* von n ist eine endliche Folge $(k_1, \ldots, k_l)$ natürlicher Zahlen mit $k_1 + \ldots + k_l = n$ und $k_1 \geq k_2 \geq \ldots \geq k_l$.)

Beispiel: $5 = 4+1 = 3+2 = 3+1+1 = 2+2+1 = 2+1+1+1 = 1+1+1+1+1$.
Daher hat $\mathrm{Sym}(5)$ Klassenzahl 7.

Satz 7.2 *Für $n \in \mathbb{N}$ ist jedes $g \in \mathrm{Sym}(n)$ ein Produkt von Transpositionen.*

Beweis: $(x_1, \ldots, x_k) = (x_1, x_k)(x_1, x_{k-1}) \ldots (x_1, x_2)$.

Bemerkung:

(i) Wegen $(k,l) = (1,l)(1,k)(1,l)$ genügen sogar die Transpositionen $(1,2), \ldots, (1,n)$.

(ii) Wegen $(1,i) = (i-1,i) \ldots (2,3)(1,2)(2,3) \ldots (i-1,i)$ genügen analog die Transpositionen $(1,2), (2,3), \ldots, (n-1,n)$.

(iii) Für $n \in \mathbb{N}$ ist $\mathrm{Sym}(n) = \langle (1,2), (1,2,\ldots,n) \rangle$ wegen

$$\begin{array}{rcc} (1,2,\ldots,n)(1,2)(1,2,\ldots,n)^{-1} & = & (2,3) \\ (1,2,\ldots,n)(2,3)(1,2,\ldots,n)^{-1} & = & (3,4) \\ \vdots & & \vdots \\ (1,2,\ldots,n)(n-2,n-1)(1,2,\ldots,n)^{-1} & = & (n-1,n). \end{array}$$

Satz 7.3 *Für $n \in \mathbb{N}$ gilt: $\mathrm{Sym}(n)$ auflösbar $\Longleftrightarrow n \leq 4$.*

Beweis: Wegen $|\mathrm{Sym}(1)| = 1$, $|\mathrm{Sym}(2)| = 2$ und Beispiel 5.4 ist $\mathrm{Sym}(n)$ für $n = 1,2,3,4$ auflösbar.
Sei also $n \geq 5$ und G die von allen 3-Zyklen erzeugte Untergruppe von $\mathrm{Sym}(n)$. Sind $i,j,k \in \{1,\ldots,n\}$ paarweise verschieden, so existieren wegen $n \geq 5$ $l,m \in \{1,\ldots,n\}$ mit $|\{i,j,k,l,m\}| = 5$. Offenbar ist

$$(i,j,k) = (i,j,l)(i,k,m)(i,j,l)^{-1}(i,k,m)^{-1} \in G',$$

also $G = G' = G'' = \ldots \neq 1$. Daher ist G nicht auflösbar, also auch nicht $\mathrm{Sym}(n)$.

Bemerkung: In der Gruppentheorie zeigt man, daß $\mathrm{Alt}(n)$ für $n \geq 5$ einfach ist.

Satz 7.4 *Für $n \in \mathbb{N}$ mit $n \geq 3$ erzeugen die Elemente $a = (1,2,\ldots,n)$ der Ordnung n und $b = (1,n)(2,n-1)(3,n-2)\ldots$ der Ordnung 2 eine Untergruppe D_{2n} von $\mathrm{Sym}(n)$ mit $|D_{2n}| = 2n$ und $bab^{-1} = a^{-1}$.*

Definition: *Man nennt D_{2n} die* Diedergruppe *der Ordnung $2n$.*

Bemerkung:

(i) Manche Autoren schreiben D_n statt D_{2n}.

(ii) Manchmal wird die Kleinsche Vierergruppe V_4 auch als Diedergruppe D_4 der Ordnung 4 bezeichnet.

Beweis: Man sieht sofort, daß a die Ordnung n und b die Ordnung 2 hat. Ferner ist

$$bab^{-1} = (b(1), b(2), \dots, b(n)) = (n, n-1, \dots, 1) = a^{-1}.$$

Daher ist $a^n = 1 = b^2,\ a^{-1} = a^{n-1},\ b^{-1} = b,\ ba = a^{-1}b = a^{n-1}b$ und

$$\begin{aligned} \langle a, b \rangle &= \{x_1^{\varepsilon_1} \dots x_k^{\varepsilon_k} : x_i \in \{a, b\},\ \varepsilon_i = \pm 1,\ k \in \mathbb{N}_0\} = \\ &= \{y_1 \dots y_l : y_i \in \{a, b\},\ l \in \mathbb{N}_0\} = \\ &= \{a^i b^j : i, j \in \mathbb{N}_0\} = \\ &= \{a^i b^j : i = 0, \dots, n-1,\ j = 0, 1\}. \end{aligned}$$

Folglich ist $|\langle a, b \rangle| \leq 2n$. Wäre $|\langle a, b \rangle| < 2n$, so wäre $|\langle a, b \rangle| = n$ wegen $n = |\langle a \rangle| \mid |\langle a, b \rangle|$. Dann wäre aber $\langle a, b \rangle = \langle a \rangle$ zyklisch, insbesondere abelsch. Daher wäre dann $ab = ba = a^{n-1}b$, also $a^{n-2} = 1$ im Widerspruch zur Tatsache, daß a die Ordnung $n \geq 3$ hat.

Satz 7.5 *Für jede ungerade Primzahl p existieren bis auf Isomorphie genau 2 Gruppen der Ordnung $2p$, nämlich $\mathbf{Z}/2p\mathbf{Z}$ und D_{2p}.*

Beweis: Wir haben gesehen, daß D_{2p} nicht abelsch und daher nicht zu $\mathbf{Z}/2p\mathbf{Z}$ isomorph ist. Daher existieren mindestens 2 nichtisomorphe Gruppen der Ordnung $2p$, und es genügt zu zeigen, daß es andrerseits höchstens eine nichtzyklische Gruppe der Ordnung $2p$ gibt.
Sei also G eine nichtzyklische Gruppe der Ordnung $2p$, P eine p-Sylowgruppe von G und Q eine 2-Sylowgruppe von G. Wegen $|P| = p$ und $|Q| = 2$ sind P und Q zyklisch, etwa $P = \langle a \rangle,\ Q = \langle b \rangle$. Wegen $|G : P| = 2$ ist $P \trianglelefteq G$, und nach Sylow ist P dann die einzige p-Sylowgruppe von G. Daher enthält P alle Elemente der Ordnung p. Nach Lagrange haben alle Elemente in $G \setminus P$ die Ordnung 2; insbesondere ist $(ab)(ab) = 1$, also $ba = a^{-1}b^{-1} = a^{-1}b$. Wie im Beweis von 7.4 erhält man $G = \langle a, b \rangle = \{a^i b^j : i = 0, \dots, p-1,\ j = 0, 1\}$. Die Regeln $a^p = 1 = b^2$ und $ba = a^{-1}b$ legen die Multiplikationstafel von G fest:

$$\begin{aligned} a^i \cdot a^j b^k &= a^{i+j} b^k = \begin{cases} a^{i+j} b^k & \text{falls } i + j < p \\ a^{i+j-p} b^k & \text{falls } i + j \geq p \end{cases} \\ a^i b \cdot a^j &= a^i b a^j b^{-1} b = a^i (\underbrace{bab^{-1}}_{=a^{-1}})^j b = a^{i-j} b = \begin{cases} a^{i-j} b & \text{falls } i \geq j \\ a^{i-j+p} b & \text{falls } i < j \end{cases} \\ a^i b \cdot a^j b &= \begin{cases} a^{i-j} & \text{falls } i \geq j \\ a^{i-j+p} & \text{falls } i < j \end{cases} \end{aligned}$$

Kapitel 8

Die Konstruktion der ganzen Zahlen

Bemerkung 8.1 Wir wollen aus einer abelschen Halbgruppe H eine Gruppe G konstruieren.

Beispiel:

(i) $H = (\mathbb{N}, +),\ G = (\mathbf{Z}, +)$.

(ii) $H = (\mathbb{N}, \cdot),\ G = (\{q \in \mathbb{Q} : q > 0\}, \cdot)$.

Satz: *Sei H eine nichtleere abelsche Halbgruppe. Wir definieren folgendermaßen eine Äquivalenzrelation auf $H \times H$:*

$$(a, b) \sim (a', b') \ :\Leftrightarrow\ \exists h \in H : ab'h = a'bh.$$

Dann bilden die Äquivalenzklassen $[a, b]$ $(a, b \in H)$ eine abelsche Gruppe G, wenn man definiert:

$$[a, b][c, d] := [ac, bd] \quad (a, b, c, d \in H).$$

Für $z \in H$ ist $[z, z]$ neutrales Element in G, und für $a, b \in H$ ist $[a, b]^{-1} = [b, a]$.
Die Abbildung $F : H \to G,\ h \mapsto [h^2, h]$ ist ein Homomorphismus von Halbgruppen, d.h. es ist $F(hk) = F(h)F(k)$ für $h, k \in H$. Genau dann ist F injektiv, wenn für alle $a, b, c \in H$ gilt: $ac = bc \ \Leftrightarrow\ a = b$.

Definition: *Man nennt G die* Grothendieckgruppe *zu H und die Abbildung $F : H \to G$ kanonisch.*

Beweis: Wir zeigen zunächst, daß $\sim$ eine Äquivalenzrelation ist.
Reflexivität: Wegen $aba = aba$ ist $(a, b) \sim (a, b)$ für $a, b \in H$.
Symmetrie: Seien $a, b, a', b' \in H$ mit $(a, b) \sim (a', b')$. Dann existiert $h \in H$ mit $ab'h = a'bh$. Folglich ist auch $(a', b') \sim (a, b)$.
Transitivität: Seien $a, b, a', b', a'', b'' \in H$ mit $(a, b) \sim (a', b'),\ (a', b') \sim (a'', b'')$. Dann existieren $h, h' \in H$ mit $ab'h = a'bh,\ a'b''h' = a''b'h'$. Folglich ist $ab''b'hh' = a'bhb''h' = a''b'h'bh = a''bb'hh'$, also $(a, b) \sim (a'', b'')$.
Als nächstes zeigen wir, daß die Multiplikation in G wohldefiniert ist. Sind $a, b, a', b', c, d \in H$ mit $[a, b] = [a', b']$, so existiert $h \in H$ mit $ab'h = a'bh$, also auch $acb'dh = a'cbdh$. Daher ist $[ac, bd] = [a'c, b'd]$. Analog ist $[ac, bd] = [ac', bd']$ für $c', d' \in H$ mit $[c, d] = [c', d']$.
Für $a, b, c, d, e, f \in H$ ist

$$\begin{aligned}\big([a, b][c, d]\big)[e, f] &= [ac, bd][e, f] = [(ac)e][(bd)f] = [a(ce)][b(df)] = \\ &= [a, b][ce, df] = [a, b]\big([c, d][e, f]\big).\end{aligned}$$

Daher ist G kommutative Halbgruppe.
Für $a, b, z \in H$ ist $[z, z][a, b] = [za, zb] = [a, b]$ wegen $za \cdot b \cdot z = a \cdot zb \cdot z$ und $[b, a][a, b] = [ba, ab] = [ab, ab]$. Daher ist G Gruppe.
Für $h, k \in H$ ist

$$F(h)F(k) = [h^2, h][k^2, k] = [h^2k^2, hk] = [(hk)^2, hk] = F(hk).$$

Ist F injektiv und sind $a, b, c \in H$ mit $ac = bc$, so ist

$$F(a) = [a^2, a] = [a^2c, ac] = [ac, c] = [bc, c] = [b^2c, bc] = [b^2, b] = F(b),$$

also $a = b$.
Sei umgekehrt für $a, b, c \in H$ die Bedingung „$ac = bc \;\Leftrightarrow\; a = b$" erfüllt. Sind $a, b \in H$ mit $F(a) = F(b)$, so ist $[a^2, a] = [b^2, b]$, also $a^2bh = b^2ah$ für ein $h \in H$. Setzt man $c := abh$, so folgt aus der Bedingung $a = b$. Folglich ist F injektiv.

Bemerkung 8.2 Sei H abelsche Halbgruppe, G die Grothendieckgruppe von H und $F : H \to G$ die kanonische Abbildung. Ist F injektiv, so können (und werden) wir H mit $F(H)$ identifizieren und so H als Teilmenge von G auffassen. Wegen

$$F(a)F(b)^{-1} = [a^2, a][b, b^2] = [a^2b, ab^2] = [a, b]$$

für $a, b \in H$ ist dann jedes Element in G von der Form ab^{-1} $(a, b \in H)$.

Beispiel:

(i) Im Fall $H = (\mathbb{N}, +)$ gilt: $(a, b) \sim (a', b') \;\Leftrightarrow\; a - b = a' - b'$. Daher ist dann die Abbildung $f : G \to (\mathbb{Z}, +),\; [a, b] \mapsto a - b$ ein Isomorphismus.

(ii) Im Fall $H = (\mathbb{N}, \cdot)$ gilt: $(a, b) \sim (a', b') \;\Leftrightarrow\; \frac{a}{b} = \frac{a'}{b'}$. Daher ist die Abbildung $f : G \to (\{q \in \mathbb{Q} : q > 0\}, \cdot),\; [a, b] \mapsto \frac{a}{b}$ ein Isomorphismus.

Kapitel 9

Ringe

Definition 9.1 *Ein* Ring *ist eine Menge R mit zwei Verknüpfungen $\overset{+}{\cdot} : R \times R \to R$, so daß gilt:*

(i) $(R, +)$ *ist abelsche Gruppe.*

(ii) $(R, \cdot\,)$ *ist Monoid.*

(iii) $a, b, c \in R \;\Rightarrow\; a(b+c) = ab + ac,\; (a+b)c = ac + bc$ *(Distributivgesetze)*

Ist außerdem $ab = ba$ für $a, b \in R$, so nennt man R kommutativ.

Bemerkung: Das neutrale Element bzgl. $+$ bezeichnet man mit 0 (*Nullelement*), das neutrale Element bzgl. $\cdot$ mit 1 (*Einselement*). Manche Bücher verlangen nicht die Existenz des Einselements. Statt $a + (-b)$ schreibt man meist $a - b$. Um Klammern zu sparen, rechnet man nach der Regel: Punktrechnung geht vor Strichrechnung.
Wie in der Linearen Algebra beweist man, daß für Elemente x, y eines Ringes R gilt:

(i) $0x = 0 = x0$.

(ii) $(-x)y = -(xy) = x(-y)$.

(iii) $(-x)(-y) = xy$.

Beispiel:

(i) $\{0\}$ ist ein Ring bzgl. $+, \cdot$; dabei ist $1 = 0$.

(ii) $\mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R} \subset \mathbb{C}$ sind Ringe.

(iii) Ist I eine nichtleere Menge und R_i ein Ring für $i \in I$, so ist auch das *direkte Produkt* $\times_{i \in I} R_i = \{(r_i)_{i \in I} : r_i \in R_i$ für $i \in I\}$ ein Ring, wobei $(r_i)_{i \in I} \overset{+}{\cdot} (s_i)_{i \in I} := (r_i \overset{+}{\cdot} s_i)_{i \in I}$. Im Fall $R_i = R$ für alle $i \in I$ erhält man also den Ring $\times_{i \in I} R = \mathrm{Abb}(I, R)$ aller Abbildungen $I \to R$, und im Fall $I = \{1, \ldots, n\}$ für $n \in \mathbb{N}$ erhält man den Ring $R_1 \times \ldots \times R_n$.

(iv) Ist R Ring mit den Verknüpfungen $+, \cdot$, so auch mit den Verknüpfungen $+, \circ$, wobei $a \circ b := ba$ für $a, b \in R$. Den so entstehenden Ring R^o nennt man den zu R *entgegengesetzten Ring*. R kommutativ $\Leftrightarrow\; R = R^o$.

(v) Ist R ein Ring und $n \in \mathbb{N}$, so ist auch die Menge $\mathrm{Mat}(n, R)$ aller $n \times n$-Matrizen mit Koeffizienten in R ein Ring bzgl. der üblichen Addition und Multiplikation von Matrizen. Man nennt $\mathrm{Mat}(n, R)$ den *vollen Matrixring* des *Grades* n über R.

(vi) Für jeden Ring R bildet die Menge aller Folgen $(a_0, a_1, a_2, \dots)$ von Elementen in R mit $|\{i \in \mathbb{N}_0 : a_i \neq 0\}| < \infty$ einen Ring S bzgl. der Verknüpfungen

$$\begin{aligned} (a_0, a_1, a_2, \dots) + (b_0, b_1, b_2, \dots) &:= (a_0 + b_0, a_1 + b_1, a_2 + b_2, \dots) \\ (a_0, a_1, a_2, \dots) \cdot (b_0, b_1, b_2, \dots) &:= (c_0, c_1, c_2, \dots), \end{aligned}$$

wobei $c_n := \sum_{k=0}^{n} a_k b_{n-k}$ für $n \in \mathbb{N}_0$. Nullelement ist $(0, 0, 0, \dots)$, Einselement $(1, 0, 0, \dots)$, und es ist $-(a_0, a_1, a_2, \dots) = (-a_0, -a_1, -a_2, \dots)$. Man definiert auch eine Multiplikation mit Elementen aus R durch $r(a_0, a_1, a_2, \dots) := (ra_0, ra_1, ra_2, \dots)$.
Setzt man $X := (0, 1, 0, 0, \dots)$, so ist $X^k = (\underbrace{0, \dots, 0}_{k}, 1, 0, 0, \dots)$ für $k \in \mathbb{N}_0$, also $\sum_{k=0}^{n} a_k X^k = (a_0, a_1, a_2, \dots, a_n, 0, 0, \dots)$ für $a_0, a_1, \dots, a_n \in R$. Daher läßt sich jedes Element in S in der Form $\sum_{k=0}^{n} a_k X^k$ mit eindeutig bestimmten $a_0, a_1, \dots, a_n \in R$ schreiben. Dies werden wir in Zukunft tun. Dabei gilt:

$$\begin{aligned} \sum_{k=0}^{n} a_k X^k + \sum_{k=0}^{n} b_k X^k &= \sum_{k=0}^{n} (a_k + b_k) X^k, \\ \left(\sum_{k=0}^{m} a_k X^k\right) \left(\sum_{k=0}^{n} b_k X^k\right) &= \sum_{i=0}^{m+n} \left(\sum_{j=0}^{i} a_j b_{i-j}\right) X^i. \end{aligned}$$

Man nennt $S := R[X]$ den *Polynomring* in der *Unbestimmten* X über R und seine Elemente *Polynome*. Ist $f = \sum_{k=0}^{m} a_k X^k$ mit $a_m \neq 0$, so nennt man $a_0, a_1, \dots, a_m$ die *Koeffizienten* von f. Der *höchste Koeffizient* (*Leitkoeffizient*) ist a_m, der *Grad* von f ist m $(=: \deg(f))$, das *höchste Glied* von f ist $a_m X^m$. (Das Nullpolynom $0 + 0 \cdot X + \dots$ erhält keinen Grad.) Ist $a_m = 1$, so nennt man f *normiert*. Die Elemente $a \cdot X^0 \in R[X]$ $(a \in R)$ addiert und multipliziert man wie zwei Elemente in R: $aX^0 \overset{+}{\cdot} bX^0 = (a \overset{+}{\cdot} b)X^0$. Wir werden daher die Elemente aX^0 $(a \in R)$ mit den Elementen in R identifizieren und so R als Teilmenge von $R[X]$ auffassen.

(vii) Für jede abelsche Gruppe $(A, +)$ bilden die Endomorphismen von A einen Ring $\mathrm{End}(A)$ mit den Verknüpfungen $+, \circ$, wobei $\alpha + \beta$, $\alpha \circ \beta$ für $\alpha, \beta \in \mathrm{End}(A)$ durch $(\alpha + \beta)(x) := \alpha(x) + \beta(x)$, $(\alpha \circ \beta)(x) := \alpha(\beta(x))$ für $x \in A$ definiert sind (Beweis siehe Lineare Algebra). Man nennt $\mathrm{End}(A)$ den *Endomorphismenring* von A.

Definition 9.2 *Ein Element a eines Ringes R heißt*

(a) invertierbar *oder* Einheit *(unit) in R, falls ein Element $b \in R$ existiert mit $ab = 1 = ba$.*

(b) Nullteiler *in R, falls ein Element $b \in R \setminus \{0\}$ existiert mit $ab = 0$ oder $ba = 0$.*

Bemerkung: Es ist leicht zu sehen, daß die Einheiten in R eine Gruppe bzgl. $\cdot$ bilden, die *Einheitengruppe* $R^\times$ oder $U(R)$ von R.

Beispiel:

(i) Ist $R \neq \{0\}$, so existiert $r \in R$ mit $r \neq 0$. Wegen $0 = r0$ ist 0 Nullteiler in R, und wegen $r \cdot 1 = r \neq 0$ ist $1 \neq 0$.

(ii) Ist a Einheit in R, so ist a kein Nullteiler in R; denn aus $ax = 0$ für ein $x \in R$ folgt $0 = a^{-1}0 = a^{-1}ax = x$.

(iii) Wegen $\left(\begin{smallmatrix} 1 & 0 \\ 0 & 0 \end{smallmatrix}\right) \left(\begin{smallmatrix} 0 & 0 \\ 0 & 1 \end{smallmatrix}\right) = 0$ sind $\left(\begin{smallmatrix} 1 & 0 \\ 0 & 0 \end{smallmatrix}\right)$, $\left(\begin{smallmatrix} 0 & 0 \\ 0 & 1 \end{smallmatrix}\right)$ Nullteiler in $\mathrm{Mat}(2, \mathbb{R})$.

(iv) $U(\mathrm{Mat}(n, R)) := \mathrm{GL}(n, R)$ nennt man *allgemeine lineare Gruppe* des *Grades* $n \in \mathbb{N}$ über R.

Definition 9.3 *Ein Ring R heißt*

(i) nullteilerfrei*, falls $R \neq 0$ und 0 der einzige Nullteiler in R ist.*

(ii) Integritätsbereich*, falls R nullteilerfrei und kommutativ ist.*

(iii) Schiefkörper*, falls $R \neq 0$ und $U(R) = R \setminus \{0\}$ ist.*

(iv) Körper*, falls R ein kommutativer Schiefkörper ist.*

Beispiel:

(i) Schiefkörper sind nullteilerfrei. Daher sind Körper Integritätsbereiche.

(ii) $\mathbf{Z}$ ist Integritätsbereich.

(iii) Ist R ein Integritätsbereich, so auch $R[X]$; denn offenbar ist mit R auch $R[X]$ kommutativ, und für $f, g \in R[X] \setminus \{0\}$ ist der höchste Koeffizient von fg das Produkt der Leitkoeffizienten von f und g. Das gleiche Argument zeigt, daß in diesem Fall $\deg(fg) = \deg(f) + \deg(g)$ gilt und daß $U(R[X]) = U(R)$ ist.

Definition 9.4 *Eine Teilmenge S eines Ringes R nennt man* Teilring *von R, falls S mit den entsprechend eingeschränkten Verknüpfungen ein Ring ist.*

Bemerkung: Wir verlangen nicht, daß die Einselemente von R und S übereinstimmen. Ist dies der Fall, so nennen wir S einen *unitären* Teilring von R. (Diese Konvention ist nicht einheitlich.) Eine Teilmenge S von R ist also genau dann ein unitärer Teilring von R, wenn gilt:

(i) $0, 1 \in S$,

(ii) $a, b \in S \ \Rightarrow \ a - b, ab \in S$.

Beispiel:

(a) $\mathbf{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$ ist eine Folge von unitären Teilringen.

(b) $\mathbb{Q} + \mathbb{Q}\, i := \{a + bi : a, b \in \mathbb{Q}\}$ ist ein unitärer Teilring von $\mathbb{C}$ wegen $(a + bi)(c + di) = (ac - bd) + (ad + bc)i$ für $a, b, c, d \in \mathbb{Q}$. Die Elemente von $\mathbb{Q} + \mathbb{Q}\, i$ nennt man *gaußsche Zahlen*. $\mathbb{Q} + \mathbb{Q}\, i$ ist Körper, denn für $a, b \in \mathbb{Q}$ mit $a + bi \neq 0$ ist

$$\frac{1}{a + bi} = \frac{a - bi}{(a + bi)(a - bi)} = \frac{a}{a^2 + b^2} + \frac{-b}{a^2 + b^2} i \in \mathbb{Q} + \mathbb{Q}\, i.$$

(c) $\mathbf{Z} + \mathbf{Z}i := \{a + bi : a, b \in \mathbf{Z}\}$ ist ein unitärer Teilring von $\mathbb{Q} + \mathbb{Q}\, i$ und damit ein Integritätsbereich. Die Elemente von $\mathbf{Z} + \mathbf{Z}i$ nennt man *gaußsche ganze Zahlen*.

(d) $\mathbf{Z} + \mathbf{Z}\sqrt{-5}$ ist ein Teilring von $\mathbb{C}$; denn für $a, b, c, d \in \mathbf{Z}$ gilt $(a + b\sqrt{-5})(c + d\sqrt{-5}) = (ac - 5bd) + (ad + bc)\sqrt{-5}$. Insbesondere ist $\mathbf{Z} + \mathbf{Z}\sqrt{-5}$ ein Integritätsbereich.

(e) Die Menge $\mathbb{H} := \{\left(\begin{smallmatrix} a & b \\ -\bar{b} & \bar{a} \end{smallmatrix}\right) : a, b \in \mathbb{C}\}$ der *Quaternionen* ist ein Teilring von $\mathrm{Mat}(2, \mathbb{C})$ wegen

$$\begin{pmatrix} a & b \\ -\bar{b} & \bar{a} \end{pmatrix} \begin{pmatrix} c & d \\ -\bar{d} & \bar{c} \end{pmatrix} = \begin{pmatrix} ac - b\bar{d} & ad + b\bar{c} \\ -\bar{b}c - \bar{a}\bar{d} & -\bar{b}d + \bar{a}\bar{c} \end{pmatrix} \in \mathbb{H}$$

für $a, b, c, d \in \mathbb{C}$. Wegen $\left(\begin{smallmatrix} a & b \\ -\bar{b} & \bar{a} \end{smallmatrix}\right)^{-1} = \frac{1}{a\bar{a} + b\bar{b}} \left(\begin{smallmatrix} \bar{a} & -b \\ \bar{b} & a \end{smallmatrix}\right) \in \mathbb{H}$ ist $\mathbb{H}$ Schiefkörper (Hamilton 1843).

(f) Für jeden Ring R ist das *Zentrum* $Z(R) := \{z \in R : zr = rz$ für $r \in R\}$ ein unitärer Teilring von R.

(g) Jeder Ring R ist unitärer Teilring des Polynomrings $R[X]$.

Kapitel 10

Homomorphismen, Ideale, Restklassenringe

Definition 10.1 *Seien R, S Ringe. Eine Abbildung $\varphi : R \to S$ nennt man* (Ring-)Homomorphismus, *falls $\varphi(a \overset{+}{\cdot} b) = \varphi(a) \overset{+}{\cdot} \varphi(b)$ für $a, b \in R$ gilt. Wie bei Gruppen definiert man Monomorphismen, Epimorphismen, ..., und den Isomorphiebegriff $\cong$ für Ringe. Ist φ ein Homomorphismus, so nennt man $\{r \in R : \varphi(r) = 0\} =: \ker(\varphi)$ den* Kern *von φ.*

Bemerkung:

(i) Im Gegensatz zu manchen Büchern verlangen wir nicht $\varphi(1_R) = 1_S$; ist dies jedoch der Fall, so nennen wir φ *unitär*. Für einen unitären Homomorphismus und ein $x \in U(R)$ ist $\varphi(x) \in U(S)$ und $\varphi(x)^{-1} = \varphi(x^{-1})$.

(ii) Wie bei Gruppen beweist man, daß die Komposition von Homomorphismen ein Homomorphismus ist. Analog ist die Umkehrabbildung φ^{-1} eines Isomorphismus φ ein Isomorphismus. Daher bilden die Automorphismen eines Ringes R eine Gruppe bzgl. der Komposition von Abbildungen, die *Automorphismengruppe* $\mathrm{Aut}(R)$ von R.

Beispiel:

(i) Die komplexe Konjugation $\mathbb{C} \to \mathbb{C},\ z \mapsto \bar{z}$ ist ein Automorphismus von $\mathbb{C}$.

(ii) Ist R ein Ring, $n \in \mathbf{Z}$ und $a \in R$, so ist (wie früher)

$$na := \begin{cases} a + \ldots + a \text{ (n Summanden)} & \text{falls } n \in \mathbb{N} \\ 0 & \text{falls } n = 0 \\ -(|n|a) & \text{falls } -n \in \mathbb{N}\,. \end{cases}$$

Die Abbildung $\mathbf{Z} \to R,\ n \mapsto n1$ ist dann ein Homomorphismus. Sein Kern ist Untergruppe von $(\mathbf{Z},+)$, also von der Form $k\mathbf{Z}$ für ein eindeutig bestimmtes $k \in \mathbb{N}_0$. Man nennt k die *Charakteristik* von R: $k = \mathrm{char}(R)$. Z.B. haben $\mathbf{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ die Charakteristik 0.

(iii) Sei S ein kommutativer Ring und R ein unitärer Teilring von S. Für $s \in S$ ist dann die Abbildung $R[X] \to S,\ f = \sum_{k=0}^{n} a_k X^k \mapsto f(s) := \sum_{k=0}^{n} a_k s^k$ ein Homomorphismus, der *Einsetzungshomomorphismus*. Man nennt $f(s)$ auch ein *Polynom* in s. Ist $f(s) = 0$, so nennt man s *Nullstelle* von f.

Satz 10.2 *Für einen Ring R und eine Untergruppe $(I, +)$ von $(R, +)$ sind äquivalent:*

(1) $r \in R,\ x \in I \;\Rightarrow\; rx, xr \in I$.

(2) *Die Gruppe* $(R/I,+)$ *wird durch folgende Multiplikation zu einem Ring:* $(r+I)(s+I) := rs+I$ *für* $r,s \in R$.

(3) *Es gibt einen Ring* S *und einen Homomorphismus* $\varphi : R \to S$ *mit Kern* I.

In diesem Fall ist die Abbildung $\nu : R \to R/I,\ r \mapsto r+I$ *ein Epimorphismus mit Kern* I.

Definition: *Sind (1), (2), (3) erfüllt, so nennt man* I *ein* Ideal *in* R, R/I *den* Restklassenring *von* R *nach* I, *seine Elemente* Restklassen *modulo* I *und* ν *den* kanonischen *Epimorphismus . Statt* $r+I = s+I$ *schreibt man (wie früher) auch* $r \equiv s \pmod{I}$.

Beweis:

(1)⇒(2): Sei (1) erfüllt. Wir wissen schon, daß $(R/I,+)$ abelsche Gruppe ist. Sind r,r', $s,s' \in R$ mit $r+I = r'+I,\ s+I = s'+I$, so existieren $x,y \in I$ mit $r' = r+x,\ s' = s+y$. Daher ist

$$r's'+I = (r+x)(s+y)+I = rs+\underbrace{ry+xs+xy}_{\in I}+I = rs+I.$$

Daher ist die Multiplikation in R/I wohldefiniert. Man rechnet leicht nach, daß R/I so zu einem Ring wird.

(2)⇒(3): Man nehme $S := R/I$ und $\varphi := \nu$.

(3)⇒(1): Sei S Ring und $\varphi : R \to S$ Homomorphismus mit Kern I. Für $r \in R$ und $x \in I$ ist dann $\varphi(rx) = \varphi(r)\underbrace{\varphi(x)}_{=0} = 0$, also $rx \in \ker(\varphi) = I$. Analog ist $xr \in I$.

Beispiel:

(a) Für jeden Ring R sind 0 und R Ideale in R. Ist $R \neq 0$ und gibt es keine weiteren Ideale, so nennt man R *einfach*. Die endlichen einfachen Ringe wurden ca. 1900 von Wedderburn klassifiziert. Es sind dies genau die vollen Matrixringe über endlichen Körpern.

(b) Enthält ein Ideal I eines Ringes R eine Einheit u von R, so ist $r = ru^{-1} \cdot u \in I$ für $r \in R$, d.h. $R = I$. Insbesondere ist jeder Schiefkörper ein einfacher Ring.

(c) Für jede nichtleere Menge $\mathcal{I}$ von Idealen I eines Ringes R ist $\bigcap_{I \in \mathcal{I}} I$ ein Ideal in R. Für jede Teilmenge A von R ist also insbesondere

$$(A) := \bigcap_{\substack{I \text{ Ideal in } R \\ A \subseteq I}} I$$

ein Ideal in R, das von A *erzeugte* Ideal in R. Wie bei Gruppen zeigt man:

$$(A) = \{\sum_{i=1}^{k} r_i a_i s_i : r_i, s_i \in R,\ a_i \in A,\ k \in \mathbb{N}_0\}.$$

Ist R kommutativ, so ist also

$$(A) = \{\sum_{i=1}^{k} r_i a_i : r_i \in R,\ a_i \in A,\ k \in \mathbb{N}_0\},$$

und ist $A = \{a\}$ außerdem einelementig, so ist $(a) := (\{a\}) = \{ra : r \in R\} =: Ra$, und man nennt (a) das von a erzeugte *Hauptideal*.

(d) Die Ideale in $\mathbf{Z}$ sind genau die Mengen $n\mathbf{Z} = (n)$ $(n \in \mathbb{N}_0)$. Man erhält so die bekannten Restklassenringe $\mathbf{Z}/n\mathbf{Z}$.

(e) Für Ideale I und J eines Ringes R sind auch die *Summe* $I+J := \{i+j : i \in I,\ j \in J\}$ und das *Produkt* $IJ := \{\sum_{i=1}^{k} x_i y_i : x_i \in I,\ y_i \in J,\ k \in \mathbb{N}_0\}$ Ideale in R. Dabei gilt:

  (i) $I+J = (I \cup J),\ IJ = (xy : x \in I,\ y \in J) \subseteq I \cap J$,

  (ii) $(IJ)K = I(JK),\ I(J+K) = IJ + IK,\ (I+J)K = IK + JK$.

(f) In $\mathbf{Z}$ gilt: $(m)(n) = (mn),\ (m)+(n) = (\mathrm{ggT}(m,n))$; offenbar ist nämlich $m,n \in (\mathrm{ggT}(m,n))$, und umgekehrt ist $\mathrm{ggT}(m,n) = am+bn \in (m)+(n)$ für geeignete $a,b \in \mathbf{Z}$.

Satz 10.3 (Homomorphiesatz) *Seien R,S Ringe, $\varphi : R \to S$ Homomorphismus und $I := \ker(\varphi)$. Dann ist die Abbildung $\varphi' : R/I \to \varphi(R),\ r+I \mapsto \varphi(r)$ ein Isomorphismus; insbesondere ist $R/I \cong \varphi(R)$.*

Beweis: Man rechnet leicht nach, daß $\varphi(R)$ ein Teilring von S ist. Wie früher gezeigt, ist φ' wohldefiniert und ein Isomorphismus zwischen den Gruppen $(R/I,+)$ und $(\varphi(R),+)$. Die Behauptung folgt, da für $a,b \in R$ gilt:

$$\varphi'((a+I)(b+I)) = \varphi'(ab+I) = \varphi(ab) = \varphi(a)\varphi(b) = \varphi'(a+I)\varphi'(b+I).$$

Satz 10.4 (Erster Isomorphiesatz) *Seien R Ring, S ein unitärer Teilring von R und I ein Ideal in R. Dann ist $S+I := \{s+x : s \in S,\ x \in I\}$ ein unitärer Teilring von R, I ein Ideal in $S+I$, $S \cap I$ Ideal in S und*

$$S+I/I \cong S/S\cap I.$$

Beweis: Offenbar ist $1 = 1+0 \in S+I$, und für $s,t \in S,\ x,y \in I$ ist

$$(s+x)(y+t) = \underbrace{st}_{\in S} + \underbrace{sy+xt+xy}_{\in I} \in S+I.$$

Daher ist $S+I$ ein unitärer Teilring von R. Da I ein Ideal in R ist, ist I auch ein Ideal in $S+I$. Die Einschränkung des natürlichen Epimorphismus $\nu : R \to R/I$ ist ein Homomorphismus $\varphi : S \to R/I$ mit Kern $S \cap I$ ($\Rightarrow$ $S \cap I$ Ideal in S) und Bild $\{s+I : s \in S\} = \{s+x+I : s \in S,\ x \in I\} = S+I/I$. Homomorphiesatz: $S/S\cap I \cong S+I/I$.

Satz 10.5 (Zweiter Isomorphiesatz) *Für jedes Ideal I eines Ringes R ist die Abbildung $J \mapsto J/I$ eine Bijektion zwischen der Menge der Ideale in R, die I enthalten, und der Menge der Ideale in R/I. Dabei gilt:*

$$(R/I)/(J/I) \cong R/J.$$

Beweis: Bezeichnet $\nu : R \to R/I$ den kanonischen Epimorphismus und ist J ein Ideal in R mit $I \subseteq J$, so ist $\nu(J) = J/I$ ein Ideal in R/I; denn für $r \in R$ und $y \in J$ ist

$$(r+I)(y+I) = \underbrace{ry}_{\in J} \in J/I$$

und analog $(y+I)(r+I) \in J/I$.
Ist umgekehrt K ein Ideal in R/I, so ist $K = J/I$ für eine Untergruppe $(J,+)$ von $(R,+)$ mit $I \subseteq J$. Für $r \in R$ und $y \in J$ ist

$$ry + I = (r+I)\underbrace{(y+I)}_{\in J/I=K} \in K = J/I,$$

also $ry \in J$. Analog ist $yr \in J$. Daher ist J Ideal in R.
Der Kern des Epimorphismus $R \to R/I \to (R/I)/(J/I),\ r \mapsto r+I \mapsto (r+I)+(J/I)$ ist offenbar J. Homomorphiesatz: $R/J \cong (R/I)/(J/I)$.

Satz 10.6 (Chinesischer Restsatz) *Seien $I_1, \ldots, I_n$ Ideale in einem Ring R. Dann ist die Abbildung $f : R \to R/I_1 \times \ldots \times R/I_n$, $r \mapsto (r+I_1, \ldots, r+I_n)$ ein Homomorphismus mit Kern $I_1 \cap \ldots \cap I_n$; insbesondere ist $R/I_1 \cap \ldots \cap I_n$ isomorph zu einem Teilring von $R/I_1 \times \ldots \times R/I_n$. Ist $I_i + I_j = R$ für $i \neq j$, so ist f surjektiv. In diesem Fall ist also $R/I_1 \cap \ldots \cap I_n \cong R/I_1 \times \ldots \times R/I_n$. Ist außerdem R kommutativ, so ist $I_1 \cap \ldots \cap I_n = I_1 I_2 \ldots I_n$.*

Beweis: Offenbar ist f ein Homomorphismus und $\ker(f) = I_1 \cap \ldots \cap I_n$. Homomorphiesatz: $R/I_1 \cap \ldots \cap I_n \cong f(R) \subseteq R/I_1 \times \ldots \times R/I_n$.
Sei also $I_i + I_j = R$ für $i \neq j$. Wähle $a_{ij} \in I_i$, $b_{ij} \in I_j$ mit $1 = a_{ij} + b_{ij}$ $(i \neq j)$. Dann ist $s_j := \prod_{k \neq j} a_{kj} \in I_i$ für $i \neq j$ und $s_j + I_j = \prod_{k \neq j}(1 - b_{kj}) + I_j = 1 + I_j$. Sind $r_1, \ldots, r_n \in R$ und ist $r := \sum_{j=1}^n r_j s_j$, so ist

$$r + I_i = \sum_{j=1}^{n} r_j s_j + I_i = r_i s_i + I_i = r_i + I_i \quad \text{für } i = 1, \ldots, r,$$

d.h. $f(r) = (r_1 + I_1, \ldots, r_n + I_n)$. Daher ist f surjektiv, und $R/I_1 \cap \ldots \cap I_n \cong f(R) = R/I_1 \times \ldots \times R/I_n$.
Sei zusätzlich R kommutativ. Offenbar ist $I_1 \ldots I_n \subseteq I_1 \cap \ldots \cap I_n$. Ist $n = 2$, so gilt für $r \in I_1 \cap I_2$:

$$r = r1 = r(a_{12} + b_{12}) = \underbrace{r}_{\in I_2} \underbrace{a_{12}}_{\in I_1} + \underbrace{r}_{\in I_1} \underbrace{b_{12}}_{\in I_2} \in I_1 I_2.$$

Ist $n \geq 2$ und $I_1 \ldots I_{n-1} = I_1 \cap \ldots \cap I_{n-1}$, so ist

$$1 = \prod_{i=1}^{n-1} (a_{in} + b_{in}) \in I_1 \ldots I_{n-1} + I_n,$$

also $R = I_1 \ldots I_{n-1} + I_n = (I_1 \cap \ldots \cap I_{n-1}) + I_n$. Der Fall $n = 2$ liefert also

$$(I_1 \ldots I_{n-1}) I_n = (I_1 \ldots I_{n-1}) \cap I_n = (I_1 \cap \ldots \cap I_{n-1}) \cap I_n.$$

Satz 10.7 *Sind $m_1, \ldots, m_r \in \mathbb{N}$ paarweise teilerfremd und $a_1, \ldots, a_r \in \mathbf{Z}$ beliebig, so bilden die Elemente $x \in \mathbf{Z}$ mit $x \equiv a_i \pmod{m_i}$ für $i = 1, \ldots, r$ eine Restklasse nach $m_1 \ldots m_r \mathbf{Z}$; insbesondere existiert ein Element $x \in \mathbf{Z}$ mit $x \equiv a_i \pmod{m_i}$ für $i = 1, \ldots, r$.*

Beweis: Unter den obigen Voraussetzungen ist $(m_i) + (m_j) = (\mathrm{ggT}(m_i, m_j)) = (1) = \mathbf{Z}$. Nach 10.6 ist also die Abbildung $f : \mathbf{Z} \to \mathbf{Z}/m_1\mathbf{Z} \times \ldots \times \mathbf{Z}/m_r\mathbf{Z}$, $z \mapsto (z + m_1\mathbf{Z}, \ldots, z + m_r\mathbf{Z})$ surjektiv. Die Elemente $x \in \mathbf{Z}$ mit $x \equiv a_i \pmod{m_i}$ für $i = 1, \ldots, r$ sind genau die Urbilder von $(a_1 + m_1\mathbf{Z}, \ldots, a_r + m_r\mathbf{Z})$ unter f. Für $x, y \in \mathbf{Z}$ gilt aber:

$$f(x) = f(y) \;\Leftrightarrow\; f(x-y) = 0 \;\Leftrightarrow\; x - y \in \ker(f) \;\Leftrightarrow\; x + \ker(f) = y + \ker(f).$$

Wegen $\ker(f) = (m_1) \ldots (m_r) = (m_1 \ldots m_r)$ folgt die Behauptung.

Definition 10.8 *Die* Eulersche φ-Funktion *wird definiert durch $\varphi(n) := |(\mathbf{Z}/n\mathbf{Z})^\times|$ für $n \in \mathbb{N}$. Man nennt $(\mathbf{Z}/n\mathbf{Z})^\times$ die* prime Restklassengruppe *und ihre Elemente* prime Restklassen *modulo n.*

Bemerkung:

(i) Für $a \in \mathbf{Z}$ gilt:

$$\begin{aligned} a + n\mathbf{Z} \in (\mathbf{Z}/n\mathbf{Z})^\times \quad &\Leftrightarrow \quad \exists b \in \mathbf{Z} : \underbrace{(a+n\mathbf{Z})(b+n\mathbf{Z})}_{ab+n\mathbf{Z}} = 1 + n\mathbf{Z} \;\Leftrightarrow \\ &\Leftrightarrow \quad \exists b, c \in \mathbf{Z} : ab + nc = 1 \;\Leftrightarrow\; \mathrm{ggT}(a,n) = 1. \end{aligned}$$

Daher ist $\varphi(n)$ die Anzahl der natürlichen Zahlen a mit $1 \le a \le n$ und $\mathrm{ggT}(a,n) = 1$.

(ii) Nach dem Chinesischen Restsatz gilt für paarweise teilerfremde $m_1, \dots, m_r \in \mathbb{N}$:

$$\mathbf{Z}/m_1 \dots m_r\mathbf{Z} \;\cong\; \mathbf{Z}/m_1\mathbf{Z} \times \dots \times \mathbf{Z}/m_r\mathbf{Z},$$

also

$$\begin{aligned} (\mathbf{Z}/m_1 \dots m_r\mathbf{Z})^\times \quad &\cong \quad (\mathbf{Z}/m_1\mathbf{Z} \times \dots \times \mathbf{Z}/m_r\mathbf{Z})^\times \;= \\ &= \quad (\mathbf{Z}/m_1\mathbf{Z})^\times \times \dots \times (\mathbf{Z}/m_r\mathbf{Z})^\times; \end{aligned}$$

insbesondere gilt $\varphi(m_1 \dots m_r) = \varphi(m_1) \dots \varphi(m_r)$.

(iii) Für jede Primzahl p und $k \in \mathbb{N}$ gibt es genau $p^k - p^{k-1}$ prime Restklassen modulo p^k, nämlich alle außer denen der Form $pa + p^k\mathbf{Z}$. Daher ist $\varphi(p^k) = p^k - p^{k-1} = p^k(1 - \frac{1}{p})$.

(iv) Für ein $n \in \mathbb{N}$ mit Primfaktorzerlegung $n = p_1^{k_1} \dots p_r^{k_r}$ gilt also:

$$\varphi(n) = (p_1^{k_1} - p_1^{k_1-1}) \dots (p_r^{k_r} - p_r^{k_r-1}) = n\left(1 - \frac{1}{p_1}\right) \dots \left(1 - \frac{1}{p_r}\right).$$

(v) Für jede Primzahl p ist $\varphi(p) = p - 1$, d.h. $\mathbf{Z}/p\mathbf{Z}$ ist Körper.

(vi) Ist $n \in \mathbb{N}$ keine Primzahl, so ist $\varphi(n) < n - 1$, also $\mathbf{Z}/n\mathbf{Z}$ kein Körper.

Satz 10.9 (Fermat) *Für $n \in \mathbb{N}$ und $a \in \mathbf{Z}$ gilt:*

$$a^{\varphi(n)} \equiv 1 \pmod{n} \;\Leftrightarrow\; \mathrm{ggT}(a,n) = 1.$$

Insbesondere gilt für jede Primzahl p und $a \in \mathbf{Z}$:

$$a^{p-1} \equiv 1 \pmod{p} \;\Leftrightarrow\; p \not| \, a.$$

Beweis: Ist $a^{\varphi(n)} \equiv 1 \pmod{n}$, so ist $a^{\varphi(n)} = 1 + nx$ für ein $x \in \mathbf{Z}$, also $\mathrm{ggT}(a,n) = 1$. Ist umgekehrt $\mathrm{ggT}(a,n) = 1$, so ist $a + n\mathbf{Z} \in (\mathbf{Z}/n\mathbf{Z})^\times$, also $1 + n\mathbf{Z} = (a+n\mathbf{Z})^{\varphi(n)} = a^{\varphi(n)} + n\mathbf{Z}$, d.h. $a^{\varphi(n)} \equiv 1 \pmod{n}$.

Satz 10.10 (Wilson) *Für jede Primzahl p gilt:* $(p-1)! \equiv -1 \pmod{p}$.

Beweis: Wegen $1! = 1 \equiv -1 \pmod{2}$ können wir annehmen, daß p ungerade ist. In $(p-1)! + p\mathbf{Z} = \prod_{i=1}^{p-1}(i + p\mathbf{Z})$ faßt man jeweils den Faktor $i + p\mathbf{Z}$ mit dem Faktor $(i + p\mathbf{Z})^{-1}$ zusammen. Dadurch fallen alle Faktoren weg außer denen mit $(i + p\mathbf{Z})^{-1} = i + p\mathbf{Z}$. Es gilt aber

$$\begin{aligned} i + p\mathbf{Z} = (i + p\mathbf{Z})^{-1} \quad &\Leftrightarrow \quad (i + p\mathbf{Z})^2 = 1 + p\mathbf{Z} \;\Leftrightarrow\; i^2 - 1 \equiv 0 \pmod{p} \;\Leftrightarrow \\ &\Leftrightarrow \quad p \mid (i-1)(i+1) \;\Leftrightarrow\; p \mid i - 1 \,\vee\, p \mid i + 1 \;\Leftrightarrow \\ &\Leftrightarrow \quad i \equiv 1 \pmod{p} \,\vee\, i \equiv -1 \pmod{p}. \end{aligned}$$

Satz 10.11 *Für ein echtes Ideal M in einem Ring R sind äquivalent:*

(1) Es existiert kein Ideal I in R mit $M \subsetneq I \subsetneq R$.

(2) R/M ist einfach.

Beweis: 2. Isomorphiesatz.

Definition: *Man nennt dann M ein* maximales Ideal *in R.*

Satz 10.12 *Jeder einfache kommutative Ring ist ein Körper. Daher ist ein Ideal M in einem kommutativen Ring R genau dann maximal, wenn R/M Körper ist.*

Beweis: Ist R ein einfacher kommutativer Ring, so ist $(a) = R$ für $a \in R \setminus \{0\}$. Daher existiert zu jedem $a \in R \setminus \{0\}$ ein $b \in R$ mit $ab = 1$. Folglich ist R Körper. Die weitere Aussage folgt aus 10.11.

Beispiel: Für jede Primzahl p ist also $p\mathbf{Z} = (p)$ ein maximales Ideal in $\mathbf{Z}$.

Satz 10.13 *Für ein echtes Ideal P in einem kommutativen Ring R sind äquivalent:*

(1) $a, b \in R$ mit $ab \in P \;\Leftrightarrow\; a \in P$ oder $b \in P$.

(2) R/P ist Integritätsbereich.

Definition: *In diesem Fall nennt man P ein* Primideal *in R.*

Bemerkung: In manchen Büchern ist auch R ein Primideal in R.

Beispiel:

(a) Da jeder Körper Integritätsbereich ist, ist jedes maximale Ideal in einem kommutativen Ring auch ein Primideal.

(b) 0 ist Primideal in $\mathbf{Z}$, aber kein maximales Ideal.

Beweis:

(1)⇒(2): Sei (1) erfüllt. Wegen $P \neq R$ ist $R/P \neq 0$, und mit R ist auch R/P kommutativ. Sind $a, b \in R$ mit $0 = (a + P)(b + P) = ab + P$, so ist $ab \in P$, also $a \in P$ oder $b \in P$. Folglich ist $a + P = 0$ oder $b + P = 0$.

(2)⇒(1): Sei (2) erfüllt. Sind $a, b \in R$ mit $ab \in P$, so ist $0 = ab + P = (a + P)(b + P)$, also $a + P = 0$ oder $b + P = 0$, d.h. $a \in P$ oder $b \in P$.

Kapitel 11

Quotientenkörper

Bemerkung 11.1 Es ist klar, daß jeder unitäre Teilring eines Körpers ein Integritätsbereich ist. Wir zeigen jetzt umgekehrt, daß jeder Integritätsbereich unitärer Teilring eines Körpers ist. Man kann dies benutzen, um etwa den Körper $\mathbb{Q}$ aus dem Integritätsbereich $\mathbf{Z}$ zu konstruieren.

Satz: *Sei R Integritätsbereich. Dann definiert man eine Äquivalenzrelation $\sim$ auf $R \times (R \setminus \{0\})$ durch*

$$(a, b) \sim (a', b') :\Leftrightarrow\ ab' = a'b.$$

Bezeichnet man für $a, b \in R$ mit $b \neq 0$ die Äquivalenzklasse von (a, b) mit $[a, b]$, so ist $Q(R) := \{[a, b] : a, b \in R,\ b \neq 0\}$ ein Körper mit

$$[a, b] + [c, d] := [ad + bc, bd], \qquad [a, b][c, d] := [ac, bd].$$

Nullelement in $Q(R)$ ist $[0, 1]$, Einselement $[1, 1]$, und es gilt: $-[a, b] = [-a, b]$, $[a, b]^{-1} = [b, a]$. Die Abbildung $\iota : R \to Q(R),\ a \mapsto [a, 1]$ ist ein unitärer Monomorphismus, und für $a, b \in R$ mit $b \neq 0$ ist $[a, b] = \iota(a)\iota(b)^{-1}$.

Definition: *Man nennt $Q(R)$ den* Quotientenkörper *von R und ι die* kanonische Einbettung.

Beweis: Wir zeigen zunächst, daß $\sim$ eine Äquivalenzrelation ist.
Reflexivität: Wegen $ab = ab$ ist $(a, b) \sim (a, b)$ für $a, b \in R$ mit $b \neq 0$.
Symmetrie: Seien $a, b, a', b' \in R$ mit $(a, b) \sim (a', b')$ und $b \neq 0 \neq b'$. Dann ist $ab' = a'b$, also auch $(a', b') \sim (a, b)$.
Transitivität: Seien $a, b, a', b', a'', b'' \in R$ mit $b \neq 0,\ b' \neq 0,\ b'' \neq 0$ und $(a, b) \sim (a', b')$, $(a', b') \sim (a'', b'')$. Dann ist $ab' = a'b,\ a'b'' = a''b'$, also $ab'b'' = a'bb'' = a''b'b$. Folglich ist $b'(ab'' - a''b) = 0$, also $ab'' - a''b = 0$. Daher ist $(a, b) \sim (a'', b'')$.
Für $a, b, c \in R$ mit $b \neq 0 \neq c$ ist $(ac, bc) \sim (a, b)$ wegen $acb = abc$. Daher ist $[ac, bc] = [a, b]$.
Als nächstes zeigen wir die Wohldefiniertheit der Verknüpfungen. Seien also $a, b, a', b', c, d, c', d' \in R$ mit $b \neq 0 \neq b',\ d \neq 0 \neq d',\ [a, b] = [a', b'],\ [c, d] = [c', d']$. Dann ist $ab' = a'b,\ cd' = c'd$, also

$$(ad + bc)b'd' = ab'dd' + bcb'd' = a'bdd' + bc'db' = (a'd' + b'c')bd.$$

Folglich ist $[ad + bc, bd] = [a'd' + b'c', b'd']$. Analog ist $[ac, bd] = [a'c', b'd']$. Daher sind die Verknüpfungen wohldefiniert.
Für $a, b, c, d, e, f \in R$ mit $b \neq 0,\ d \neq 0,\ f \neq 0$ gilt:

$$\begin{aligned}
\big([a, b] + [c, d]\big) + [e, f] &= [ad + bc, bd] + [e, f] \;=\; [adf + bcf + bde, bdf] \;= \\
&= [a, b] + [cf + de, df] \;=\; [a, b] + \big([c, d] + [e, f]\big), \\
[a, b] + [c, d] &= [ad + bc, bd] \;=\; [cb + da, db] \;=\; [c, d] + [a, b], \\
[a, b] + [0, 1] &= [a1 + b0, b1] \;=\; [a, b], \\
[a, b] + [-a, b] &= [ab + b(-a), b^2] \;=\; [0, b^2] \;=\; [0, 1], \\
[a, b][c, d] &= [ac, bd] \;=\; [ca, db] \;=\; [c, d][a, b],
\end{aligned}$$

$$\begin{aligned}
[a,b][1,1] &= [a1,b1] \;=\; [a,b],\\
\big([a,b][c,d]\big)[e,f] &= [ac,bd][e,f] \;=\; [ace,bdf] \;=\; [a,b][ce,df] \;=\\
&= [a,b]\big([c,d][e,f]\big),\\
[a,b]\big([c,d]+[e,f]\big) &= [a,b][cf+de,df] \;=\; [acf+ade,bdf] \;=\\
&= [abcf+abde,b^2df] \;=\; [ac,bd]+[ae,bf] \;=\\
&= [a,b][c,d]+[a,b][e,f].
\end{aligned}$$

Dies zeigt, daß $Q(R)$ ein kommutativer Ring ist.
Seien $a,b \in R$ mit $b \neq 0$ und $[a,b] \neq [0,1]$, also $a1 \neq 0b$, d.h. $a \neq 0$. Dann ist $[a,b][b,a] = [ab,ba] = [1,1]$. Folglich ist $Q(R)$ Körper.
Ferner ist $\iota : R \to Q(R),\ a \mapsto [a,1]$ ein unitärer Homomorphismus, da gilt:

$$\begin{aligned}
\iota(a)+\iota(b) &= [a,1]+[b,1] \;=\; [a1+1b,1\cdot 1] \;=\; [a+b,1] \;=\; \iota(a+b),\\
\iota(a)\iota(b) &= [a,1][b,1] \;=\; [ab,1\cdot 1] \;=\; \iota(ab).
\end{aligned}$$

ι ist injektiv, denn ist $a \in R$ mit $0 = \iota(a) = [a,1]$, so ist $a1 = 1\cdot 0$, also $a = 0$.
Schließlich gilt für $a,b \in R$ mit $b \neq 0$:

$$\iota(a)\iota(b)^{-1} \;=\; [a,1][1,b] \;=\; [a1,1b] \;=\; [a,b].$$

Bemerkung 11.2 Sei R Integritätsbereich mit Quotientenkörper $Q(R)$ und kanonischer Einbettung $\iota : R \to Q(R)$. Jedes $r \in R$ identifiziert man dann mit $\iota(r) \in Q(R)$ und kann so R als unitären Teilring von $Q(R)$ auffassen. Hat man dies getan, so ist jedes Element in $Q(R)$ von der Form ab^{-1} $(a,b \in R,\ b \neq 0)$.

Satz: *Sei R Integritätsbereich mit Quotientenkörper $Q(R) \supseteq R$, K ein Körper und $\varphi : R \to K$ Monomorphismus. Dann kann man φ auf eindeutig bestimmte Weise zu einem Monomorphismus $\psi : Q(R) \to K$ fortsetzen.*

Beweis: Ist $\psi : Q(R) \to K$ eine Fortsetzung von φ, so gilt für $a,b \in R$ mit $b \neq 0$:

$$\psi(ab^{-1}) = \psi(a)\psi(b)^{-1} = \varphi(a)\varphi(b)^{-1}.$$

Daher ist ψ durch φ eindeutig bestimmt.
Umgekehrt definieren wir bei vorgegebenem φ die Abbildung ψ durch

$$\psi(ab^{-1}) := \varphi(a)\varphi(b)^{-1} \qquad \text{für } a,b \in R \text{ mit } b \neq 0.$$

Dies ist wohldefiniert; sind nämlich $a',b' \in R$ mit $b' \neq 0$ und $ab^{-1} = a'(b')^{-1}$, so ist $ab' = a'b$, also

$$\varphi(a)\varphi(b') = \varphi(ab') = \varphi(a'b) = \varphi(a')\varphi(b).$$

Folglich ist $\varphi(a)\varphi(b)^{-1} = \varphi(a')\varphi(b')^{-1}$. Offenbar ist ψ eine Fortsetzung von φ. Ferner ist ψ Homomorphismus; denn für $a,b,c,d \in R$ mit $b \neq 0 \neq d$ gilt:

$$\begin{aligned}
\psi(ab^{-1})+\psi(cd^{-1}) &= \varphi(a)\varphi(b)^{-1}+\varphi(c)\varphi(d)^{-1} \;=\\
&= \big(\varphi(a)\varphi(d)+\varphi(b)\varphi(c)\big)\varphi(b)^{-1}\varphi(d)^{-1} \;=\\
&= \varphi(ad+bc)\varphi(bd)^{-1} \;=\; \psi((ad+bd)(bd)^{-1}) \;=\\
&= \psi(ab^{-1}+cd^{-1}),\\
\psi(ab^{-1})\psi(cd^{-1}) &= \varphi(a)\varphi(b^{-1})\varphi(c)\varphi(d^{-1}) \;=\; \varphi(ac)\varphi(bd)^{-1} \;=\\
&= \psi((ac)(bd)^{-1}) \;=\; \psi(ab^{-1}\cdot cd^{-1}).
\end{aligned}$$

ψ ist injektiv; denn $\ker(\psi)$ ist ein Ideal im Körper $Q(R)$, $1 \notin \ker(\psi)$. Also $\ker(\psi) = 0$.

Beispiel:

(i) $Q(\mathbf{Z}) \cong \mathbb{Q}$.

(ii) $Q(\mathbf{Z} + \mathbf{Z}i) \cong \mathbb{Q} + \mathbb{Q}\, i$.

(iii) Für jeden Körper K ist der Polynomring $K[X]$ ein Integritätsbereich. Man nennt $Q(K[X])$ den Körper der *rationalen Funktionen* in der Unbestimmten X über K.
Schreibweise: $K(X)$. Die Elemente in $K(X)$ haben also die Form $\frac{f}{g}$ $(f, g \in K[X],\ g \neq 0)$.
Dabei gilt: $\frac{f_1}{g_1} = \frac{f_2}{g_2} \;\Leftrightarrow\; f_1 g_2 = f_2 g_1$.

Kapitel 12

Teilbarkeit

Satz 12.1 *Für Elemente a, b eines Integritätsbereiches R sind äquivalent:*

(1) $\exists x \in R : b = ax$.

(2) $(b) \subseteq (a)$.

Definition: *Man sagt in diesem Fall: a* teilt *b, a ist* Teiler *von b, b ist* Vielfaches *von a etc.*
Schreibweise: $a \mid b$.

Beweis:

(1)⇒(2): Ist $x \in R$ mit $b = ax$, so ist $(b) = bR = axR \subseteq aR = (a)$.

(2)⇒(1): Ist $(b) \subseteq (a)$, so ist insbesondere $b \in (a) = aR$, also $b = ax$ für ein $x \in R$.

Satz 12.2 *Für jeden Integritätsbereich R gilt:*

(i) $a \in R \;\Rightarrow\; a \mid a \;\wedge\; a \mid 0$.

(ii) $a \in R \;\wedge\; 0 \mid a \;\Rightarrow\; a = 0$.

(iii) $u \in U(R) \;\wedge\; a \in R \;\Rightarrow\; u \mid a$.

(iv) $a \in R \;\wedge\; a \mid 1 \;\Rightarrow\; a \in U(R)$.

(v) $a, b, c \in R,\; a \mid b,\; b \mid c \;\Rightarrow\; a \mid c$.

(vi) $a, b_1, \ldots, b_n, x_1, \ldots, x_n \in R \;\wedge\; a \mid b_1 \;\wedge\; \ldots \;\wedge\; a \mid b_n \;\Rightarrow\; a \mid x_1 b_1 + \ldots + x_n b_n$.

Beweis:

(i) $a = a1,\; 0 = a0$.

(ii) Ist $a \in R$ mit $0 \mid a$, so existiert $x \in R$ mit $a = 0x$, d.h. $a = 0$.

(iii) $a = u \cdot u^{-1} a$.

(iv) $a \mid 1 \;\Rightarrow\; \exists b \in R : ab = 1 \;\Rightarrow\; a \in U(R)$.

(v) Sind $a, b, c \in R$ mit $a \mid b$ und $b \mid c$, so existieren $x, y \in R$ mit $b = ax,\; c = by$. Folglich ist $c = by = a \cdot xy$, also $a \mid c$.

(vi) Seien $a, b_1, \ldots, b_n, x_1, \ldots, x_n \in R$ mit $a \mid b_1, \ldots, a \mid b_n$. Dann existieren $y_1, \ldots, y_n \in R$ mit $b_1 = ay_1, \ldots, b_n = ay_n$. Folglich ist

$$x_1 b_1 + \ldots + x_n b_n = a x_1 y_1 + \ldots + a x_n y_n = a(x_1 y_1 + \ldots + x_n y_n),$$

d.h. $a \mid x_1 b_1 + \ldots + x_n b_n$.

Satz 12.3 *Für Elemente a, b eines Integritätsbereiches R sind äquivalent:*

(1) $a \mid b$ *und* $b \mid a$.

(2) $\exists u \in U(R) : b = ua$.

(3) $(a) = (b)$.

Definition: *In diesem Fall nennt man a und b* assoziiert.

Beweis:

(1)⇔(3): 12.1.

(1)⇒(2): Seien $a, b \in R$ mit $a \mid b$ und $b \mid a$. Dann existieren $x, y \in R$ mit $b = ax,\ a = by$. Folglich ist $a = axy$, d.h. $a(1 - xy) = 0$. Im Fall $a = 0$ ist $b = ax = 0x = 0$, also $b = a1$, und im Fall $a \neq 0$ ist $xy = 1$, also $x \in U(R)$.

(2)⇒(3): Ist $u \in U(R)$ mit $b = au$, so ist $(b) = bR = auR \subseteq aR = (a)$. Wegen $a = bu^{-1}$ ist analog $(a) \subseteq (b)$.

Beispiel:

(a) In $\mathbf{Z}$ ist jeweils a zu $-a$ assoziiert.

(b) Die zu 1 assoziierten Elemente in R sind genau die Einheiten in R.

Bemerkung:

(i) Seien $a, a', b, b' \in R$, a assoziiert zu a' und b zu b'. Dann gilt: $a \mid b \ \Leftrightarrow\ a' \mid b'$.

(ii) $U(R)$ operiert auf R durch ${}^u a := ua$ für $u \in U(R),\ a \in R$. Zwei Elemente a, a' liegen genau in der gleichen Bahn, wenn sie in R assoziiert sind. Daher ist Assoziiertheit eine Äquivalenzrelation auf R.

Satz 12.4 *Für Elemente $a_1, \ldots, a_n, t$ eines Integritätsbereiches R sind äquivalent:*

(1) $t \mid a_i$ *für* $i = 1, \ldots, n$.

(2) $(a_1, \ldots, a_n) := (\{a_1, \ldots, a_n\}) \subseteq (t)$.

Definition: *In diesem Fall nennt man t einen* gemeinsamen Teiler *von $a_1, \ldots, a_n$.*

Bemerkung: Offenbar ist $(a_1, \ldots, a_n) = \{\sum_{i=1}^n r_i a_i : r_1, \ldots, r_n \in R\} = (a_1) + \ldots + (a_n)$.

Beweis:

(1)⇒(2): Ist $t \mid a_i$ für $i = 1, \ldots, n$, so ist $(a_i) \subseteq (t)$ für $i = 1, \ldots, n$, also $(a_1, \ldots, a_n) = (a_1) + \ldots + (a_n) \subseteq (t)$.

(2)⇒(1): Ist $(a_1, \ldots, a_n) \subseteq (t)$, so ist insbesondere $(a_i) \subseteq (t)$, also $t \mid a_i$ für $i = 1, \ldots, n$.

Beispiel: Jede Einheit ist gemeinsamer Teiler von $a_1, \ldots, a_n$. Sind diese die einzigen gemeinsamen Teiler, so nennt man $a_1, \ldots, a_n$ *teilerfremd* .

Satz 12.5 *Für Elemente $a_1, \ldots, a_n, v$ eines Integritätsbereiches R sind äquivalent:*

(1) $a_1 \mid v, \ldots, a_n \mid v$.

(2) $(v) \subseteq (a_1) \cap \ldots \cap (a_n)$.

Beweis: $a_1 \mid v, \ldots, a_n \mid v \;\Leftrightarrow\; (v) \subseteq (a_i)$ für $i = 1, \ldots, n \;\Leftrightarrow\; (v) \subseteq (a_1) \cap \ldots \cap (a_n)$.

Definition: *In diesem Fall nennt man v* gemeinsames Vielfaches *von $a_1, \ldots, a_n$.*

Beispiel: 0 und $a_1 \ldots a_n$ sind stets gemeinsame Vielfache von $a_1, \ldots, a_n$.

Definition 12.6 *Seien $a_1, \ldots, a_n$ Elemente eines Integritätsbereiches R.*

(i) Ein gemeinsamer Teiler d von $a_1, \ldots, a_n$ heißt größter gemeinsamer Teiler (ggT) *von $a_1, \ldots, a_n$, falls d durch jeden gemeinsamen Teiler von $a_1, \ldots, a_n$ teilbar ist.*

(ii) Ein gemeinsames Vielfaches w von $a_1, \ldots, a_n$ heißt kleinstes gemeinsames Vielfaches (kgV) *von $a_1, \ldots, a_n$, falls jedes gemeinsame Vielfache von $a_1, \ldots, a_n$ durch w teilbar ist.*

Bemerkung: Mit d ist auch jedes zu d assoziierte Element in R ein ggT von $a_1, \ldots, a_n$. Umgekehrt sind je zwei ggT von $a_1, \ldots, a_n$ assoziiert in R. Analog für kgV. Jedoch brauchen ggT und kgV nicht zu existieren.

Beispiel: Wir betrachten den Integritätsbereich $R = \mathbf{Z} + \mathbf{Z}\sqrt{-5}$ und benutzen die Abbildung $N : R \to \mathbb{N}_0,\ r = a + b\sqrt{-5} \mapsto |r|^2 = r\bar{r} = a^2 + 5b^2,\ a, b \in \mathbf{Z}$. Dann ist $N(rs) = N(r)N(s)$; insbesondere gilt: $x \mid y$ in $R \Rightarrow N(x) \mid N(y)$ in $\mathbf{Z}$. Ist $u \in R^\times$, so ist $1 = N(1) = N(u)N(u^{-1})$ in $\mathbb{N}$, also $N(u) = 1$. Schreibt man $u = a + b\sqrt{-5},\ a, b \in \mathbf{Z}$, so ist also $a^2 + 5b^2 = 1$, d.h. $b = 0$ und $a^2 = 1$. Folglich sind $-1, 1$ die einzigen Einheiten in R. Sind $r, s \in R$ mit $9 = rs$, so ist $81 = N(9) = N(r)N(s)$, also $N(r) \in \{1, 3, 9, 27, 81\}$. Die Gleichungen $x^2 + 5y^2 = 3$ und $x^2 + 5y^2 = 27$ sind in $\mathbf{Z}$ unlösbar. Im Fall $N(r) = 1$ ist $r \in \{-1, 1\}$, und im Fall $N(r) = 81$ ist $N(s) = 1$, also $s \in \{-1, 1\}$ und $r \in \{-9, 9\}$. Ist $N(r) = 9$ und schreibt man $r = a + b\sqrt{-5}$ mit $a, b \in \mathbf{Z}$, so ist $9 = a^2 + 5b^2$, also entweder $b^2 = 1,\ a^2 = 4$ oder $b = 0,\ a^2 = 9$, also $r \in \{\pm(2 + \sqrt{-5}), \pm(2 - \sqrt{-5}), \pm 3\}$. Wegen $(2 + \sqrt{-5})(2 - \sqrt{-5}) = 9$ sind also $\pm 1, \pm 3, \pm(2 + \sqrt{-5}), \pm(2 - \sqrt{-5}), \pm 9$ die einzigen Teiler von 9 in R. Wegen $\frac{3(2+\sqrt{-5})}{2-\sqrt{-5}} = \frac{-1+4\sqrt{-5}}{3} \notin R$ sind also $\pm 1, \pm 3, \pm(2 + \sqrt{-5})$ die gemeinsamen Teiler von 9 und $3(2 + \sqrt{-5})$. Wegen $\frac{2+\sqrt{-5}}{3} \notin R$ und $\frac{3}{2+\sqrt{-5}} = \frac{2-\sqrt{-5}}{3} \notin R$ gibt es unter diesen keinen größten.

Definition 12.7 *Seien R Integritätsbereich, $p \in R \setminus R^\times$, $p \neq 0$. Man nennt p*

(i) unzerlegbar *oder* irreduzibel*, falls für $a, b \in R$ gilt: $p = ab \;\Rightarrow\; a \in R^\times$ oder $b \in R^\times$.*

(ii) Primelement*, falls für $a, b \in R$ gilt: $p \mid ab \;\Rightarrow\; p \mid a$ oder $p \mid b$.*

Bemerkung:

(i) Mit p ist auch jedes zu p assoziierte Element unzerlegbar bzw. ein Primelement.

(ii) Jedes Primelement p ist irreduzibel; sind nämlich $a, b \in R$ mit $p = ab$, so ist $p \mid a$ oder $p \mid b$, o.B.d.A. $p \mid a$. Wegen $a \mid p$ sind a und p dann assoziiert, also $p = au$ für ein $u \in R^\times$. Daher ist $a(u - b) = 0$, und $a \neq 0$ wegen $p \neq 0$. Folglich ist $b = u \in R^\times$.

Beispiel:

(a) In $\mathbf{Z}$ gilt: p Primelement $\Leftrightarrow$ p irreduzibel $\Leftrightarrow$ $|p|$ Primzahl.

(b) In $R := \mathbf{Z} + \mathbf{Z}\sqrt{-5}$ ist $2 + \sqrt{-5}$ irreduzibel; ist nämlich $2 + \sqrt{-5} = rs$ mit $r, s \in R$, so ist $9 = N(2 + \sqrt{-5}) = N(r)N(s)$ in $\mathbf{Z}$. Ist $N(r) = 1$, so ist $r \in \{\pm 1\}$. Ist $N(r) = 9$, so ist $N(s) = 1$, also $s \in \{\pm 1\}$. Der Fall $N(r) = 3$ tritt nicht auf, da die Gleichung $x^2 + 5y^2 = 3$ in $\mathbf{Z}$ unlösbar ist. $2 + \sqrt{-5}$ ist kein Primelement; denn wegen $(2 + \sqrt{-5})(2 - \sqrt{-5}) = 9 = 3 \cdot 3$ ist einerseits $2 + \sqrt{-5} \mid 9$, aber $2 + \sqrt{-5} \nmid 3$.

Satz 12.8 *Ein Element $p \neq 0$ in einem Integritätsbereich R ist genau dann ein Primelement, wenn (p) ein Primideal ist.*

Beweis:

⇒: Sei p ein Primelement. Wegen $p \notin R^\times$ ist $(p) \neq R$. Sind $a, b \in R$ mit $ab \in (p)$, so ist $p \mid ab$, also $p \mid a$ oder $p \mid b$. Daher ist $a \in (p)$ oder $b \in (p)$.

⇐: Sei (p) Primideal. Wegen $(p) \neq R$ ist $p \notin R^\times$. Sind $a, b \in R$ mit $p \mid ab$, so ist $ab \in (p)$, also $a \in (p)$ oder $b \in (p)$, d.h. $p \mid a$ oder $p \mid b$.

Satz 12.9 *Sind $p_1, \ldots, p_r, q_1, \ldots, q_s$ Primelemente in einem Integritätsbereich R mit $p_1 \ldots p_r = q_1 \ldots q_s$, so ist $r = s$, und bei geeigneter Numerierung ist p_i zu q_i assoziiert für $i = 1, \ldots, r$.*

Beweis: (Induktion nach r) Im Fall $r = 0$ ist $q_1 \ldots q_s = 1$, also $q_i \in R^\times$ für $i = 1, \ldots, s$, also $s = 0$ nach Definition der Primelemente. Sei also $r \geq 1$ und die Behauptung für $r - 1$ bewiesen. Aus $p_1 \ldots p_r = q_1 \ldots q_s$ folgt $p_r \mid q_1 \ldots q_s$, also $p_r \mid q_i$ für ein $i \in \{1, \ldots, s\}$, o.B.d.A. $p_r \mid q_s$. Dann ist also $q_s = p_r u$ für ein $u \in R^\times$, da q_s irreduzibel ist. Folglich ist $0 = (p_1 \ldots p_{r-1} - q_1 \ldots q_{s-1} u) p_r$, also $p_1 \ldots p_{r-1} = q_1 \ldots q_{s-1} u$. Nach Induktionsvoraussetzung ist $r - 1 = s - 1$ (also auch $r = s$), und bei geeigneter Numerierung ist p_i zu q_i bzw. $q_i u$ assoziiert für $i = 1, \ldots, r - 1$. Die Behauptung folgt.

Kapitel 13

Faktorielle Ringe, Hauptidealringe, euklidische Ringe

Satz 13.1 *Für einen Integritätsbereich R sind äquivalent:*

(1) Jedes Element $a \in R \backslash R^\times$ mit $a \neq 0$ läßt sich als Produkt von Primelementen schreiben.

(2) Jedes Element $a \in R \backslash R^\times$ mit $a \neq 0$ läßt sich als Produkt irreduzibler Elemente schreiben, und ist $p_1 \dots p_r = q_1 \dots q_s$ mit irreduziblen Elementen $p_1, \dots, p_r, q_1, \dots, q_s$, so ist $r = s$, und bei geeigneter Numerierung ist p_i zu q_i assoziiert für $i = 1, \dots, r$.

(3) Jedes Element $a \in R \backslash R^\times$ mit $a \neq 0$ läßt sich als Produkt irreduzibler Elemente schreiben, und jedes irreduzible Element in R ist ein Primelement.

Definition: *In diesem Fall nennt man R* gaußsch *oder* faktoriell *oder* ZPE-Ring.

Beweis:

(3)⇒(2): 12.9.

(2)⇒(3): Sei (2) erfüllt, also auch der erste Teil von (3). Sei $p \in R$ irreduzibel. Sind $a, b \in R$ mit $p \mid ab$, so existiert $c \in R$ mit $ab = pc$. O.B.d.A. $a \neq 0$ (sonst $p \mid a$) und $b \neq 0$. O.B.d.A. $a \notin R^\times$ (sonst $p \mid b$ wegen $b = pca^{-1}$) und $b \notin R^\times$. Dann ist $0 \neq c \notin R^\times$ (sonst $p = abc^{-1}$ nicht irreduzibel). Folglich existieren irreduzible Elemente $p_1, \dots, p_k, q_1, \dots, q_l, r_1 \dots, r_m$ mit $a = p_1 \dots p_k,\ b = q_1 \dots q_l,\ c = r_1 \dots r_m$. Daher ist $pr_1 \dots r_m = p_1 \dots p_k q_1 \dots q_l$, also p zu einem p_i oder q_i assoziiert, d.h. $p \mid a$ oder $p \mid b$.

(1)⇒(3): Ist (1) erfüllt, so auch der erste Teil von (3). Ist $p \in R$ irreduzibel, so existieren nach (1) Primelemente $p_1, \dots, p_r$ mit $p = p_1 \dots p_r$. Da p irreduzibel ist, folgt $r = 1$, und $p = p_1$ ist Primelement.

(3)⇒(1): Trivial.

Bemerkung: Ist R ein faktorieller Ring und P ein Repräsentantensystem für die Klassen assoziierter Primelemente in R, so hat jedes Element $a \in R \setminus \{0\}$ eine eindeutige *Primfaktorzerlegung* $a = u \prod_{p \in P} p^{\alpha_p}$ mit $u \in R^\times,\ \alpha_p \in \mathbb{N}_0$ für $p \in P$ und $|\{p \in P : \alpha_p \neq 0\}| < \infty$. Analog hat jedes Element $x \in Q(R) \setminus \{0\}$ eine eindeutige Primfaktorzerlegung $x = v \prod_{p \in P} p^{\xi_p}$ mit $v \in R^\times,\ \xi_p \in \mathbf{Z}$ für $p \in P$ und $|\{p \in P : \xi_p \neq 0\}| < \infty$.

Beispiel:

(a) $\mathbf{Z}+\mathbf{Z}\sqrt{-5}$ ist nicht faktoriell, da $2+\sqrt{-5}$ irreduzibel, aber kein Primelement ist.

(b) $\mathbf{Z}$ ist faktoriell; P ist meist die Menge der (positiven) Primzahlen, die Primfaktorzerlegungen haben die Form $\pm\prod_{p\in P} p^{\alpha_p}$.

Satz 13.2 *Sei R faktorieller Ring und $a, b \in R\backslash\{0\}$ mit Primfaktorzerlegung $a = u\prod_{p\in P} p^{\alpha_p}$, $b = v\prod_{p\in P} p^{\beta_p}$. Dann gilt:*

(i) $a \mid b \;\Leftrightarrow\; \alpha_p \leq \beta_p$ *für* $p \in P$.

(ii) $\prod_{p\in P} p^{\min\{\alpha_p,\beta_p\}}$ *ist ein* ggT *von a und b.*

(iii) $\prod_{p\in P} p^{\max\{\alpha_p,\beta_p\}}$ *ist ein* kgV *von a und b.*

(iv) Sind a und b teilerfremd und ist $c \in R$ mit $a \mid c$ und $b \mid c$, so ist $ab \mid c$.

Beweis: Betrachte Primfaktorzerlegungen.

Definition 13.3 *Ein Integritätsbereich R heißt* Hauptidealring*, falls jedes Ideal I in R ein Hauptideal, d.h. von der Form $I = (a)$ für ein $a \in R$ ist.*

Beispiel: $\mathbf{Z}$ ist Hauptidealring, da jedes Ideal in $\mathbf{Z}$ die Form $n\mathbf{Z} = (n)$ für $n \in \mathbb{N}$ hat.

Satz: *Für jedes Element $p \neq 0$ in einem Hauptidealring R gilt: (p) maximales Ideal $\Leftrightarrow$ (p) Primideal $\Leftrightarrow$ p Primelement $\Leftrightarrow$ p irreduzibel.*

Beweis: Bekannt: (p) maximal $\Rightarrow$ (p) Primideal $\Rightarrow$ p Primelement $\Rightarrow$ p irreduzibel. Sei p irreduzibel. Dann ist $(p) \neq R$ wegen $p \notin R^\times$. Sei also $I = (a)$ ein Ideal in R mit $(p) \subseteq I \neq R$. Dann ist $p = ab$ für ein $b \in R$. Wegen $I \neq R$ ist $a \notin R^\times$, also $b \in R^\times$. Daher sind p und a assoziiert. d.h. $(p) = (a) = I$.

Satz 13.4 *Hauptidealringe sind faktoriell.*

Beweis: Sei R Hauptidealring. Ist R nicht faktoriell, so existiert $a_1 \in R \setminus R^\times$, $a_1 \neq 0$, so daß a_1 kein Produkt irreduzibler Elemente ist. Insbesondere ist a_1 nicht irreduzibel, also $a_1 = a_2 b_2$ mit Elementen $a_2, b_2 \in R\backslash R^\times$. Mindestens eines der Elemente a_2, b_2 ist kein Produkt irreduzibler Elemente, etwa a_2. Da a_1 und a_2 nicht assoziiert sind, ist $(a_1) \subsetneq (a_2)$. Auf a_2 kann man das gleiche Argument anwenden. Auf diese Weise erhält man Elemente $a_1, a_2, a_3, \ldots$ in R mit $(a_1) \subsetneq (a_2) \subsetneq (a_3) \subsetneq \ldots$. Dann ist $I := \bigcup_{i=1}^{\infty} (a_i)$ ein Ideal in R; sind nämlich $a, b \in I$, so existieren $m, n \in \mathbb{N}$ mit $a \in (a_m)$, $b \in (a_n)$, o.B.d.A. $m \leq n$, also $(a_m) \subseteq (a_n)$. Dann ist $a - b \in (a_n) \subseteq I$ und $ra \in (a_n) \subseteq I$ für $r \in R$. Da R Hauptidealring ist, existiert ein $x \in R$ mit $I = (x)$. Daher ist $x \in (a_k)$ für ein $k \in \mathbb{N}$, also $(a_k) \subsetneq (a_{k+1}) \subseteq I = (x) \subseteq (a_k)$. Widerspruch.

Satz 13.5 (Bézout) *Ein Element d in einem Hauptidealring R ist genau dann ein* ggT *der Elemente $a_1, \ldots, a_n \in R$, wenn $(d) = (a_1, \ldots, a_n)$ gilt. Insbesondere existieren in diesem Fall Elemente $r_1, \ldots, r_n \in R$ mit $d = r_1 a_1 + \ldots + r_n a_n$.*

Beweis:

$\Rightarrow$: Sei d ein ggT von $a_1, \ldots, a_n$. Da R Hauptidealring ist, existiert $a \in R$ mit $(a_1 \ldots, a_n) = (a)$. Nach 12.4 ist a ein ggT von $a_1, \ldots, a_n$, also zu d assoziiert. Folglich ist $(a_1, \ldots, a_n) = (a) = (d)$.

$\Leftarrow$: 12.4.

Satz 13.6 *Elemente $a_1, \ldots, a_n$ in einem Hauptidealring R sind genau dann teilerfremd, wenn Elemente $r_1, \ldots, r_n \in R$ existieren mit $r_1 a_1 + \ldots + r_n a_n = 1$.*

Beweis:

$\Rightarrow$**:** Sind $a_1, \ldots, a_n \in R$ teilerfremd, so sind die Einheiten die einzigen gemeinsamen Teiler von $a_1 \ldots, a_n$, d.h. 1 ist ggT von $a_1 \ldots, a_n$. Die Behauptung folgt aus 13.5.

$\Leftarrow$**:** Sind $r_1, \ldots, r_n \in R$ mit $r_1 a_1 + \ldots + r_n a_n = 1$, so ist jeder gemeinsame Teiler von $a_1, \ldots, a_n$ auch Teiler von 1, also eine Einheit in R.

Definition 13.7 *Ein Integritätsbereich R heißt* euklidischer Ring*, wenn eine Abbildung $H : R \setminus \{0\} \to \mathbb{N}_0$ mit folgenden Eigenschaften existiert:*

(i) Für $a, b \in R$ mit $b \neq 0$ existieren $q, r \in R$ mit $a = bq + r$, wobei $r = 0$ oder $H(r) < H(b)$.

(ii) Für $a, b \in R$ mit $ab \neq 0$ ist $H(a) \leq H(ab)$.

Bemerkung: In manchen Büchern wird (ii) nicht verlangt. Man nennt $H(a)$ die *Höhe* von $a \in R \setminus \{0\}$.

Beispiel:

(i) $\mathbf{Z}$ ist euklidisch mit $H(a) = |a|$ für $a \in \mathbf{Z} \setminus \{0\}$.

(ii) $R := \mathbf{Z} + \mathbf{Z}i$ ist euklidisch mit $H(r) = r\bar{r} = |r|^2$ für $r \in R \setminus \{0\}$. Sind nämlich $a, b \in R$ mit $b \neq 0$, so ist $\frac{a}{b} \in \mathbb{C}$, etwa $\frac{a}{b} = x + iy$ mit $x, y \in \mathbb{R}$. Wählt man $m, n \in \mathbf{Z}$ mit $|x - m| \leq \frac{1}{2}$, $|y - n| \leq \frac{1}{2}$ und setzt man $q := m + in$, $r := a - bq$, so ist

$$\begin{aligned} H(r) &= |a - bq|^2 = |b|^2 |\frac{a}{b} - q|^2 = |b|^2 \left((x-m)^2 + (y-n)^2\right) \leq \\ &\leq |b|^2 \left(\frac{1}{4} + \frac{1}{4}\right) < |b|^2 = H(b). \end{aligned}$$

(iii) Für jeden Körper K ist $K[X]$ euklidisch mit $H(f) = \deg(f)$ für $f \in K[X] \setminus \{0\}$; dies folgt aus der Division mit Rest für Polynome.

Satz 13.8 *Euklidische Ringe sind Hauptidealringe und damit faktoriell.*

Beweis: Sei R euklidischer Ring und I Ideal in R, o.B.d.A. $I \neq 0 = (0)$. Dann ist $M := \{H(x) : x \in I, x \neq 0\}$ eine nichtleere Teilmenge von $\mathbb{N}$, enthält also ein kleinstes Element $H(a)$, $a \in I \setminus \{0\}$. Dann ist $(a) \subseteq I$. Ist $b \in I$, so existieren $q, r \in R$ mit $b = aq + r$, wobei $r = 0$ oder $H(r) < H(a)$. Im Fall $r \neq 0$ wäre $H(r) < H(a)$, was wegen $r = b - aq \in I$ ein Widerspruch zur Wahl von a wäre. Also ist $r = 0$ und $b = aq \in (a)$. Insgesamt ist also $I \subseteq (a)$.

Bemerkung: In einem euklidischen Ring kann man einen ggT von Elementen $a \neq 0, b \neq 0$ durch den folgenden *euklidischen Algorithmus* berechnen:

(1) Setze $(u_1, v_1, w_1) := (1, 0, a)$, $(u_2, v_2, w_2) := (0, 1, b)$.

(2) Solange $w_i \neq 0$ setze

$$(u_{i+1}, v_{i+1}, w_{i+1}) := (u_{i-1} - q_i u_i, v_{i-1} - q_i v_i, w_{i-1} - q_i w_i),$$

wobei $w_{i-1} = q_i w_i + r_i$, $r_i = 0$ oder $H(r_i) < H(w_i)$.

(3) Schließlich ist $w_{i-1} = u_{i-1} a + v_{i-1} b$ ein ggT von a und b.

Satz 13.9 *In einem euklidischen Ring R mit Höhe H sind zwei Elemente a, b mit $a, b \neq 0$ genau dann assoziiert, wenn $a \mid b$ und $H(a) = H(b)$ ist.*

Beweis:

⇒: Sind $a, b \in R \setminus \{0\}$ assoziiert, so ist $a = bu$ für ein $u \in R^\times$, also $H(b) \leq H(bu) = H(a)$ und analog $H(a) \leq H(b)$.

⇐: Seien $a, b \in R \setminus \{0\}$, $a \mid b$ und $H(a) = H(b)$. Es existieren $x, q, r \in R$ mit $b = ax$ und $a = bq + r$, wobei $r = 0$ oder $H(r) < H(b)$. Im Fall $r \neq 0$ wäre $H(r) = H(a - bq) = H(a(1 - xq)) \geq H(a) = H(b) > H(r)$. Widerspruch. Daher ist $r = 0$ und $b \mid a$.

Bemerkung: Es folgt, daß in einem euklidischen Ring R mit Höhe H ein Element $u \neq 0$ genau dann eine Einheit ist, wenn $H(u) = H(1)$ gilt.

Beispiel: Wir wissen bereits, daß $R := \mathbf{Z} + \mathbf{Z}i$ ein euklidischer Ring mit $H(\alpha) = |\alpha|^2 = \alpha\bar{\alpha}$ für $\alpha \in R$ ist. In diesem Fall ist sogar $H(\alpha\beta) = H(\alpha)H(\beta)$ für $\alpha, \beta \in R$. Ist $\varepsilon = a + ib \in R^\times$ mit $a, b \in \mathbf{Z}$, so ist $1 = H(1) = H(\varepsilon) = a^2 + b^2$, also $\varepsilon \in \{\pm 1, \pm i\}$. Daher ist $R^\times = \{\pm 1, \pm i\}$.
Jedes Primelement π in R teilt genau eine Primzahl $p \in \mathbb{N}$; wegen $\bar{\pi} \in R$ ist nämlich $\pi \mid \pi\bar{\pi} = H(\pi) \neq 1$. Daher teilt π einen der Primfaktoren p von $H(\pi)$ in $\mathbf{Z}$. Ist q eine von p verschiedene Primzahl, so existieren $x, y \in \mathbf{Z}$ mit $1 = px + qy$. Wegen $\pi \nmid 1$ ist also $\pi \nmid q$.
Um also alle Primelemente in R zu bestimmen, muß man die Primzahlen $p \in \mathbb{N}$ in Primelemente in R zerlegen. Ist $\pi \in R$ und $H(\pi)$ Primzahl, so ist π Primelement in R; ist nämlich $\alpha \in R$ mit $\alpha \mid \pi$, so ist $H(\alpha) \mid H(\pi)$ in $\mathbf{Z}$, also $H(\alpha) = 1$ oder $H(\alpha) = H(\pi)$. Folglich ist $\alpha \in R^\times$ oder α zu π assoziiert.
Die Primfaktorzerlegung von 2 in R ist $(-i)(1+i)^2$; denn wegen $H(1+i) = 2$ ist $1+i$ Primelement in R.
Jede Primzahl p mit $p \equiv 3 \pmod 4$ ist ein Primelement in R; ist nämlich π ein Primelement in R mit $\pi \mid p$ und schreibt man $\pi = a + bi$ mit $a, b \in \mathbf{Z}$, so ist $H(\pi) \mid H(p) = p^2$, also $H(\pi) \in \{p, p^2\}$. Im Fall $p = H(\pi) = a^2 + b^2$ wäre $(a + 4\mathbf{Z})^2 + (b + 4\mathbf{Z})^2 = p + 4\mathbf{Z} = 3 + 4\mathbf{Z}$, was wegen $(0 + 4\mathbf{Z})^2 = 0 = (2 + 4\mathbf{Z})^2$ und $(1 + 4\mathbf{Z})^2 = 1 = (3 + 4\mathbf{Z})^2$ unmöglich ist. Daher ist $H(\pi) = p^2 = H(p)$, d.h. π und p sind assoziiert in R. Mit π ist also auch p ein Primelement in R.
Sei p eine Primzahl mit $p \equiv 1 \pmod 4$ und π ein Primelement in R mit $\pi \mid p$. Dann ist $\bar{\pi}$ ein nicht zu π assoziiertes Primelement in R mit $p = \pi\bar{\pi}$; denn es ist $\frac{p-1}{2}$ gerade, also $-1 \equiv (p-1)! \equiv \prod_{k=1}^{\frac{p-1}{2}} k \prod_{k=1}^{\frac{p-1}{2}} (p-k) \equiv (-1)^{\frac{p-1}{2}} z^2 \equiv z^2 \pmod p$ mit $z := (\frac{p-1}{2})!$. Folglich ist $\pi \mid p \mid z^2 + 1 = (z+i)(z-i)$, also $\pi \mid z+i$ oder $\pi \mid z-i$. Wegen $p \nmid z+i$ und $p \nmid z-i$ sind π und p nicht assoziiert. Daher ist also $H(\pi) \neq H(p) = p^2$. Wegen $1 \neq H(\pi) \mid H(p) = p^2$ folgt $p = H(\pi) = \pi\bar{\pi}$. Wegen $H(\bar{\pi}) = H(\pi) = p$ ist auch $\bar{\pi}$ ein Primelement in R. Wir schreiben $\pi = x + iy$ mit $x, y \in \mathbf{Z}$. Im Fall $\bar{\pi} = \pi$ wäre $\pi = x$, also $p = x^2$. Im Fall $\bar{\pi} = -\pi$ wäre $\pi = iy$, also $p = y^2$. Im Fall $\bar{\pi} = i\pi$ wäre $x = y$, also $p = 2x^2$. Im Fall $\bar{\pi} = (-i)\pi$ wäre $x = -y$, also $p = 2x^2$. Dies zeigt, daß π und $\bar{\pi}$ in R nicht assoziiert sind.
Damit haben wir die Primfaktorzerlegungen aller Primzahlen in R bestimmt. Wir halten fest, daß zu jeder Primzahl p mit $p \equiv 1 \pmod 4$ Elemente $x, y \in \mathbf{Z}$ existieren mit $p = x^2 + y^2$.

Satz 13.10 *Ist $n \in \mathbb{N}$ mit Primfaktorzerlegung*

$$n = 2^\alpha \prod_{\substack{p \text{ Primzahl} \\ p \equiv 1 \pmod 4}} p^{\beta_p} \prod_{\substack{q \text{ Primzahl} \\ q \equiv 3 \pmod 4}} q^{\gamma_q},$$

so gilt: $\exists x, y \in \mathbf{Z}$ mit $n = x^2 + y^2 \Leftrightarrow \gamma_q$ gerade für alle Primzahlen q mit $q \equiv 3 \pmod 4$.

Beweis:

⇒: Seien $x, y \in \mathbf{Z}$ mit $n = x^2 + y^2 = (x + iy)(x - iy)$. Wie in 13.9 gezeigt, kann man die Primfaktorzerlegung von $x + iy$ in $\mathbf{Z} + \mathbf{Z}i$ in der folgenden Form schreiben:

$$x + iy = u(1+i)^\delta \prod_{\substack{p \text{ Primzahl} \\ p \equiv 1 \pmod 4}} \pi_p^{\varepsilon_p} \bar{\pi}_p^{\zeta_p} \prod_{\substack{q \text{ Primzahl} \\ q \equiv 3 \pmod 4}} q^{\eta_q}.$$

Folglich ist

$$n = (x+iy)(x-iy) = 2^\delta \prod_{\substack{p \text{ Primzahl} \\ p \equiv 1 \pmod 4}} p^{\varepsilon_p + \zeta_p} \prod_{\substack{q \text{ Primzahl} \\ q \equiv 3 \pmod 4}} q^{2\eta_q}$$

die Primfaktorzerlegung von n.

$\Leftarrow$: Sei γ_q gerade für alle Primzahlen q mit $q \equiv 3 \pmod 4$. Wir schreiben $p = x_p^2 + y_p^2$ mit $x_p, y_p \in \mathbf{Z}$ für alle Primzahlen p mit $p \equiv 1 \pmod 4$. Dann ist $n = H(\xi) = \xi\bar{\xi}$ mit

$$\xi = (1+i)^\delta \prod_{\substack{p \text{ Primzahl} \\ p \equiv 1 \pmod 4}} (x_p + iy_p)^{\beta_p} \prod_{\substack{q \text{ Primzahl} \\ q \equiv 3 \pmod 4}} q^{\gamma_q/2}.$$

Schreibt man $\xi = x + iy$ mit $x, y \in \mathbf{Z}$, so ist $n = x^2 + y^2$.

Kapitel 14

Polynomringe

Definition 14.1 *Sei R Integritätsbereich und $f \in R[X] \setminus \{0\}$. Man nennt f* primitiv*, falls die Koeffizienten von f teilerfremd sind.*

Satz: *Sei R ein faktorieller Ring mit Quotientenkörper K. Dann existieren zu jedem $f \in K[X] \setminus \{0\}$ ein Element $a \in K$ und ein primitives Polynom g in $R[X]$ mit $f = ag$. Ist $b \in K$ und h ein primitives Polynom in $R[X]$ mit $f = bh$, so existiert ein $u \in R^\times$ mit $h = ug,\ b = au^{-1}$.*

Beweis: Schreibt man $f = \sum_{i=0}^n \frac{r_i}{s_i} X^i$ mit $r_0, s_0, \dots, r_n, s_n \in R$ und setzt man $s := s_0 \dots s_n$, so ist $sf \in R[X]$, etwa $sf = \sum_{i=0}^n t_i X^i$ mit $t_0, \dots, t_n \in R$. Wählt man einen ggT d von $t_0, \dots, t_n$, so sind $\frac{t_0}{d}, \dots, \frac{t_n}{d}$ teilerfremd in R. Folglich ist $g := \frac{s}{d} f$ primitiv in $R[X]$ und $f = \frac{d}{s} g$ mit $a := \frac{d}{s} \in K$.
Sei auch $f = bh$ mit $b \in K,\ h \in R[X]$ primitiv. Schreibt man $b = \frac{e}{t}$ mit $e, t \in R$, so ist also $tdg = seh$. Daher ist td gemeinsamer Teiler der Koeffizienten von seh. Da h primitiv ist, folgt $td \mid se$. Analog ist $se \mid td$. Folglich existiert ein $u \in R^\times$ mit $td = use$. Daher ist $a = \frac{d}{s} = u\frac{e}{t} = ub$ und $h = b^{-1} f = ua^{-1} f = ug$.

Satz 14.2 (Gauß, 1777–1855) *Ist R ein faktorieller Ring, so gilt für $f, g \in R[X]$: f und g primitiv $\Leftrightarrow$ fg primitiv.*

Beweis:

$\Rightarrow$: Ist fg nicht primitiv, so existiert ein Primelement $p \in R$, das alle Koeffizienten von fg teilt. Diese liegen also im Kern des natürlichen Epimorphismus $\nu : R \to R/(p)$. Die Abbildung $\varphi : R[X] \to (R/(p))[X],\ \sum_{i=0}^n a_i X^i \mapsto \sum_{i=0}^n \nu(a_i) X^i$ ist offenbar ein Epimorphismus mit $0 = \varphi(fg) = \varphi(f)\varphi(g)$. Mit $R/(p)$ ist auch $(R/(p))[X]$ Integritätsbereich. Daher ist $\varphi(f) = 0$ oder $\varphi(g) = 0$, o.B.d.A. $\varphi(f) = 0$. Dann liegen alle Koeffizienten von f in $\ker(\nu) = (p)$, sind also durch p teilbar. Folglich ist f nicht primitiv.

$\Leftarrow$: Ist f nicht primitiv, so existiert ein Primelement p in R, das alle Koeffizienten von f teilt. Daher ist $f = ph$ für ein $h \in R[X]$. Folglich ist $fg = pgh$ nicht primitiv.

Satz: *Für einen faktoriellen Ring R mit Quotientenkörper K und ein Polynom $f \in R[X]$ sind äquivalent:*

(1) f irreduzibel in $R[X]$.

(2) Entweder ist f irreduzibel in R, oder f ist primitiv in $R[X]$ und irreduzibel in $K[X]$.

Beweis:

(1)⇒(2): Ist f irreduzibel in $R[X]$, so ist $f \neq 0$ und $f \notin R[X]^\times = R^\times$. Im Fall $\deg(f) = 0$ ist $f \in R \setminus R^\times$. Ist $f = ab$ mit $a, b \in R \subseteq R[X]$, so ist $a \in R[X]^\times = R^\times$ oder $b \in R[X]^\times = R^\times$. Also ist f irreduzibel in R.
Im Fall $\deg(f) > 0$ ist $f \notin K^\times = K[X]^\times$, und f ist primitiv in $R[X]$; denn sonst existieren ein Primelement p in R und ein $g \in R[X]$ mit $f = pg$, und $p \notin R^\times = R[X]^\times$ und $g \notin R^\times = R[X]^\times$ im Widerspruch zur Irreduzibilität von f. Ist $f = gh$ mit $g, h \in K[X]$, so existieren nach 14.1 $a, b \in K$ und primitive $g_1, h_1 \in R[X]$ mit $g = ag_1,\ h = bh_1$. Dann ist $1 \cdot f = (ab)g_1h_1$ mit $ab \in K$ und dem primitiven Polynom $g_1h_1 \in R[X]$. Nach 14.1 existiert ein $u \in R^\times$ mit $ug_1h_1 = f$ und $abu^{-1} = 1$. Wegen der Irreduzibilität von f in $R[X]$ ist $ug_1 \in R[X]^\times = R^\times$ oder $h_1 \in R[X]^\times = R^\times$, also $g \in K^\times = K[X]^\times$ oder $h \in K^\times = K[X]^\times$. Daher ist f irreduzibel in $K[X]$.

(2)⇒(1): Ist f irreduzibel in R, so ist $f \neq 0$ und $f \notin R^\times = R[X]^\times$. Ist $f = gh$ mit $g, h \in R[X]$, so ist $0 = \deg(f) = \deg(g) + \deg(h)$, also $\deg(g) = 0 = \deg(h)$, d.h. $g, h \in R$. Da f irreduzibel in R ist, folgt $g \in R^\times = R[X]^\times$ oder $h \in R^\times = R[X]^\times$. Also ist f irreduzibel in $R[X]$.
Ist f primitiv in $R[X]$ und irreduzibel in $K[X]$, so ist $0 \neq f \notin K[X]^\times = K^\times$, also $\deg(f) > 0$ und $f \notin R[X]^\times = R^\times$. Ist $f = gh$ mit $g, h \in R[X]$, so ist $g \in K[X]^\times = K^\times$ oder $h \in K[X]^\times = K^\times$, o.B.d.A. $g \in K^\times$, also $g \in K^\times \cap R[X] = R \setminus \{0\}$. Dann teilt g alle Koeffizienten von f, d.h. $g \in R^\times$ wegen der Primitivität von f.

Satz 14.3 *Mit R ist auch $R[X]$ ein faktorieller Ring.*

Beweis: Wir zeigen zunächst, daß jedes Element $f \in R[X] \setminus R[X]^\times$ mit $f \neq 0$ eine Zerlegung in irreduzible Elemente besitzt. Im Fall $f \in R$ ist das klar. Sei also $\deg(f) \geq 1$ und d ein ggT der Koeffizienten von f, also $f = dg$ mit einem primitiven Polynom $g \in R[X]$. Andrerseits ist $f = f_1 \dots f_r$ mit irreduziblen Polynomen $f_1, \dots, f_r$ in $K[X]$, wobei $K := Q(R)$. Für $i = 1, \dots, r$ existiert dann ein $x_i \in K$ und ein primitives Polynom $g_i \in R[X]$ mit $f_i = x_ig_i$. Offenbar ist g_i irreduzibel in $R[X]$ für $i = 1, \dots, r$, und $f = x_1 \dots x_r g_1 \dots g_r$. Da $g_1 \dots g_r$ nach Gauß primitiv ist, existiert ein $u \in R^\times$ mit $x_1 \dots x_r = du$ und $g = ug_1 \dots g_r$. Somit ist $f = dug_1 \dots g_r$. Ist $d \in R^\times$, so sind wir fertig. Andernfalls zerlegen wir d in irreduzible Faktoren in R und sind dann fertig.
Sei nun $r_1 \dots r_m p_1 \dots p_n = s_1 \dots s_k q_1 \dots q_l$ mit irreduziblen Elementen $r_1, \dots, r_m, s_1 \dots, s_k$ in R und primitiven Polynomen $p_1, \dots, p_n, q_1, \dots, q_l$ in $R[X]$, die irreduzibel in $K[X]$ sind. Da $p_1 \dots p_n$ und $q_1 \dots q_l$ primitiv sind, existiert nach 14.1 ein $u \in R^\times$ mit $r_1 \dots r_m = s_1 \dots s_k u^{-1}$, $p_1 \dots p_n = q_1 \dots q_l u$. Da R faktoriell ist, muß $k = m$ und r_i zu s_i assoziiert für $i = 1, \dots, k$ bei geeigneter Numerierung sein. Da $K[X]$ faktoriell ist, muß $l = n$ und p_i zu q_i für $i = 1, \dots, l$ bei geeigneter Numerierung in $K[X]$ assoziiert sein. Daher ist $1 \cdot p_i = x_i q_i$ mit $x_i \in K^\times$ für $i = 1, \dots, l$. Nach 14.1 existiert für $i = 1, \dots, l$ ein $u_i \in R^\times$ mit $x_i = u_i^{-1} \cdot 1$ und $q_i = u_i p_i$. Daher ist p_i zu q_i auch in $R[X]$ assoziiert.

Satz 14.4 (Irreduzibilitätskriterium von Eisenstein, 1823–1852)
Sei R ein Integritätsbereich und $f = \sum_{i=0}^n a_i X^i$ ein primitives Polynom in $R[X]$ vom Grad $n > 0$. Gibt es ein Primelement p in R mit $p \mid a_i$ für $i = 0, \dots, n-1$, $p \nmid a_n$ und $p^2 \nmid a_0$, so ist f irreduzibel in $R[X]$.

Beweis: Nach Voraussetzung ist $f \neq 0$ und $f \notin R^\times = R[X]^\times$. Sei $f = gh$ mit $g = \sum_{i=0}^k b_i X^i$, $h = \sum_{j=0}^l c_j X^j \in R[X]$, $b_k \neq 0 \neq c_l$. Wegen $p \mid a_0 = b_0c_0$ und $p^2 \nmid a_0 = b_0c_0$ ist entweder $p \nmid b_0$ oder $p \nmid c_0$, o.B.d.A. $p \mid b_0$, $p \nmid c_0$. Wegen $p \nmid a_n = b_kc_l$ existiert ein $j \in \{1, \dots, k\}$ mit $p \mid b_i$ für $i = 0, \dots, j-1$ und $p \nmid b_j$. Setzt man $c_i := 0$ für $i > l$, so ist also $a_j = b_jc_0 + b_{j-1}c_1 + \ldots + b_0c_j$ und $p \nmid b_jc_0$. Also ist $p \nmid a_j$, also $j = n$ und $k = n$. Wegen $f = gh$ ist $\deg(h) = 0$, also $h \in R$. Da f und h primitiv sind, folgt $h \in R^\times$.

Bemerkung 14.5 Für jede Primzahl p und $i = 1, \dots, p-1$ ist

$$\binom{p}{i} = \frac{p!}{i!(p-i)!} \in \mathbf{Z}$$

mit $p \mid p!$, $p \nmid i!$, $p \nmid (p-i)!$, also $p \mid \binom{p}{i}$.

Satz: *Für jede Primzahl p ist $f := 1 + X + X^2 + \dots + X^{p-1}$ irreduzibel in $\mathbb{Q}[X]$.*

Beweis: Sei $\varphi : \mathbf{Z}[X] \to \mathbf{Z}[X]$, $\sum_{i=0}^n a_i X^i \mapsto \sum_{i=0}^n a_i (X+1)^i$ der Einsetzungshomomorphismus. Wegen $(X-1)f = X^p - 1$ ist

$$X\varphi(f) = \varphi((X-1)f) = \varphi(X^p - 1) = (X+1)^p - 1 = \sum_{i=1}^{p} \binom{p}{i} X^i,$$

also

$$\varphi(f) = X^{p-1} + \binom{p}{p-1} X^{p-2} + \dots + \binom{p}{1}.$$

Wegen $p^2 \nmid p = \binom{p}{1}$, $p \mid \binom{p}{i}$ für $i = 1, \dots, p-1$ und $p \nmid 1$ ist $\varphi(f)$ nach Eisenstein irreduzibel in $\mathbf{Z}[X]$. Ist $f = gh$ mit $g, h \in \mathbf{Z}[X]$, so ist $\varphi(f) = \varphi(g)\varphi(h)$, d.h. $\varphi(g) \in R^\times$ oder $\varphi(h) \in R^\times$. Da φ bijektiv ist, folgt $g \in R^\times$ oder $h \in R^\times$. Daher ist f irreduzibel in $\mathbf{Z}[X]$ und damit auch in $\mathbb{Q}[X]$.

Lemma 14.6 *Seien R ein kommutativer Ring, $f \in R[X]$ und $a \in R$ mit $f(a) = 0$. Dann existiert ein $g \in R[X]$ mit $f = (X-a)g$.*

Beweis: Ist $f = \sum_{i=0}^n a_i X^i$ mit $a_0, a_1, \dots, a_n \in R$, so ist auch $f = \sum_{i=0}^n a_i (X - a + a)^i = \sum_{i=0}^n b_i (X-a)^i$ mit gewissen $b_0, b_1, \dots, b_n \in R$. Wegen $0 = f(a) = b_0$ ist $f = (X - a) \sum_{i=1}^n b_i (X-a)^{i-1}$.

Satz 14.7 *In einem Integritätsbereich R besitzt jedes Polynom $f \in R[X] \setminus \{0\}$ höchstens $\deg(f)$ verschiedene Nullstellen.*

Beweis: Wir argumentieren durch Induktion nach $\deg(f)$, wobei $\deg(f) = 0$ ein trivialer Fall ist. Sei also $n := \deg(f) \geq 1$ und die Aussage für Polynome kleineren Grades bereits bewiesen. Hat f keine Nullstelle, so sind wir fertig. Sei also $a \in R$ mit $f(a) = 0$. Nach 14.6 existiert ein $g \in R[X]$ mit $f = (X-a)g$, also $\deg(g) = n - 1$. Ist $b \in R \setminus \{a\}$ mit $0 = f(b) = (b-a)g(b)$, so ist $g(b) = 0$. Nach Induktion hat g höchstens $n-1$ verschiedene Nullstellen, also f höchstens n.

Satz 14.8 (Interpolationssatz) *Seien K Körper, $a_0, a_1, \dots, a_n \in K$ paarweise verschieden und $b_0, b_1, \dots, b_n \in K$ beliebig. Dann existiert genau ein $f \in K[X]$ mit $\deg(f) \leq n$ (oder $f = 0$) und $f(a_i) = b_i$ für $i = 0, \dots, n$.*

Beweis: Sind $f, g \in K[X]$ mit $\deg(f) \leq n$, $\deg(g) \leq n$ (bzw. $f = 0$, $g = 0$) und $f(a_i) = b_i = g(a_i)$ für $i = 0, \dots, n$, so ist $f - g = 0$ nach 14.7, d.h. $f = g$. Die Existenz zeigt das Polynom

$$\sum_{i=0}^{n} b_i \prod_{\substack{j=0 \\ j \neq i}}^{n} \frac{X - a_j}{a_i - a_j}.$$

Beispiel 14.9 Wir erläutern das sogenannte Kronecker-Verfahren zur Konstruktion der Primfaktorzerlegung von Elementen in $\mathbf{Z}[X]$ am Beispiel

$$f = X^6 - 5X^5 + 6X^4 - 3X^3 + 15X^2 - 17X - 3.$$

Ist $f = (X-a)g$ mit $g \in \mathbf{Z}[X]$, so ist $-3 = f(0) = -ag(0)$, also $a \mid -3$, d.h. $a \in \{\pm 1, \pm 3\}$. Einsetzen ergibt $f(\pm 1) \neq 0,\ f(3) = 0$. Division liefert $f = (X-3)g$ mit

$$g = X^5 - 2X^4 - 3X^2 + 6X + 1.$$

Ist $g = (X-a)h$ mit $h \in \mathbf{Z}[X]$, so ist $1 = g(0) = -ah(0)$, also $a \mid 1$, d.h. $a \in \{\pm 1\}$. Einsetzen liefert $g(\pm 1) \neq 0$. Folglich besitzt g keine Linearfaktoren. Ist $g = (X^2 + aX + b)h$ mit $h \in \mathbf{Z}[X]$, so gilt:

$$\begin{aligned} 1 = g(0) = bh(0) \ &\Rightarrow\ b \mid 1 \ \Rightarrow\ b \in \{\pm 1\}, \\ 1 = g(2) = (4 + 2a + b)h(2) \ &\Rightarrow\ 4 + 2a + b \mid 1 \ \Rightarrow\ 4 + 2a + b \in \{\pm 1\}. \end{aligned}$$

Ist $b = 1$ und $4 + 2a + b = 1$, so ist $a = -2$ im Widerspruch zu $3 = g(1) = 0h(1)$. Ist $b = 1$ und $4 + 2a + b = -1$, so ist $a = -3$ im Widerspruch zu $-87 = g(-2) = 11h(2)$. Ist $b = -1$ und $4 + 2a + b = 1$, so ist $a = -1$ im Widerspruch zu $-87 = g(-2) = 5h(-2)$. Ist $b = -1$ und $4 + 2a + b = -1$, so ist $a = -2$ im Widerspruch zu $3 = g(1) = -2h(1)$. Dies zeigt, daß g irreduzibel ist. Folglich hat f die Primfaktorzerlegung $f = (X-3)g$.

Satz 14.10 *Jede endliche Untergruppe G der multiplikativen Gruppe eines Körpers K ist zyklisch; insbesondere ist die multiplikative Gruppe eines endlichen Körpers zyklisch.*

Beweis: Sei $|G| = p_1^{a_1} \dots p_r^{a_r}$ die Primfaktorzerlegung von $|G|$ und P_i eine p_i-Sylowgruppe von G für $i = 1, \dots, r$. Wäre P_i nicht zyklisch, so wäre $g^{p_i^{a_i - 1}} = 1$ für alle $g \in P_i$, d.h. das Polynom $X^{p_i^{a_i - 1}} - 1$ hätte zu viele Nullstellen. Daher ist P_i zyklisch, etwa $P_i = \langle x_i \rangle$ für $i = 1, \dots, r$, und die Abbildung $\mathbf{Z}/p_i^{a_i}\mathbf{Z} \to P_i,\ n + p_i^{a_i}\mathbf{Z} \mapsto x_i^n$ ist ein Isomorphismus für $i = 1, \dots, r$. Daher ist die Abbildung $\varphi : \mathbf{Z}/p_1^{a_1}\mathbf{Z} \times \dots \times \mathbf{Z}/p_r^{a_r}\mathbf{Z} \to G,\ (n_1 + p_1^{a_1}\mathbf{Z}, \dots, n_r + p_r^{a_r}\mathbf{Z}) \mapsto x_1^{n_1} \dots x_r^{n_r}$ ein Homomorphismus, dessen Bild für $i = 1, \dots, r$ das Element x_i der Ordnung $p_i^{a_i}$ enthält. Sein Bild hat also mindestens die Ordnung $p_1^{a_1} \dots p_r^{a_r} = |G|$, d.h. φ ist surjektiv. Wegen $|\mathbf{Z}/p_1^{a_1}\mathbf{Z} \times \dots \times \mathbf{Z}/p_r^{a_r}\mathbf{Z}| = p_1^{a_1} \dots p_r^{a_r}$ ist also φ bijektiv, d.h. Isomorphismus. Aus dem Chinesischen Restsatz folgt:

$$\mathbf{Z}/|G|\mathbf{Z} \ \cong\ \mathbf{Z}/p_1^{a_1}\mathbf{Z} \times \dots \times \mathbf{Z}/p_r^{a_r}\mathbf{Z} \ \cong\ G.$$

Beispiel: $\mathbf{Z}/17\mathbf{Z}$:

n	1	2	3	4	5	6	7	8
2^n	2	4	8	16				1
3^n	3	9	10	13				$\neq 1$

Also $(\mathbf{Z}/17\mathbf{Z})^\times = \langle 3 + 17\mathbf{Z} \rangle$.

Satz 14.11 (Partialbruchzerlegung rationaler Funktionen) *Für jeden Körper K und $f, g \in K[X] \setminus \{0\}$ gilt:*

(i) Es existieren $q, r \in K[X]$ mit

$$\frac{f}{g} = q + \frac{r}{g},$$

wobei $r = 0$ oder $\deg(r) < \deg(g)$.

(ii) Ist $\deg(f) < \deg(g)$ und $g = g_1 g_2$ mit teilerfremden $g_1, g_2 \in K[X]$, so existieren $u_1, u_2 \in K[X]$ mit

$$\frac{f}{g} = \frac{u_1}{g_1} + \frac{u_2}{g_2},$$

wobei $u_i = 0$ oder $\deg(u_i) < \deg(g_i)$ für $i = 1, 2$.

(iii) Ist $e \in \mathbb{N}$ und $\deg(f) < \deg(g^e)$, so existieren $f_0, \dots, f_{e-1} \in K[X]$ mit

$$\frac{f}{g^e} = \frac{f_0}{g^e} + \frac{f_1}{g^{e-1}} + \dots + \frac{f_{e-1}}{g},$$

wobei $f_i = 0$ oder $\deg(f_i) < \deg(g)$ für $i = 0, \dots, e-1$.

Beweis:

(i) Division mit Rest liefert $f = gq + r$, wobei $r = 0$ oder $\deg(r) < \deg(g)$. Division durch g liefert die Behauptung.

(ii) Nach Bézout existieren $w_1, w_2 \in K[X]$ mit $1 = w_2 g_1 + w_1 g_2$, also $f = v_2 g_1 + v_1 g_2$ mit $v_i = f w_i$ für $i = 1, 2$. Division mit Rest liefert $v_i = g_i q_i + u_i$, wobei $u_i = 0$ oder $\deg(u_i) < \deg(g_i)$. Dann ist $f = g(q_1 + q_2) + u_2 g_1 + u_1 g_2$. Dabei ist $q_1 + q_2 = 0$, da sonst $\deg(g) > \deg(f - u_2 g_1 - u_1 g_2) = \deg(g(q_1 + q_2)) \geq \deg(g)$. Division durch g liefert $\frac{f}{g} = \frac{u_1}{g_1} + \frac{u_2}{g_2}$.

(iii) Wir argumentieren durch Induktion nach e. Ist $e = 1$, setze man $f_0 := f$. Im Fall $e > 1$ liefert Division mit Rest: $f = gq + f_0$, wobei $f_0 = 0$ oder $\deg(f_0) < \deg(g)$. Dann ist $q = 0$ oder $\deg(q) < \deg(g^{e-1})$. Nach Induktion ist $\frac{q}{g^{e-1}} = \frac{q_0}{g^{e-1}} + \frac{q_1}{g^{e-2}} + \dots + \frac{q_{e-2}}{g}$, wobei $q_i = 0$ oder $\deg(q_i) < \deg(g)$ für alle i. Dann ist $\frac{f}{g^e} = \frac{q_0}{g^{e-1}} + \dots + \frac{q_{e-2}}{g} + \frac{f_0}{g^e}$.

Bemerkung 14.12 Die Konstruktion des Polynomrings in einer Unbestimmten über einem kommutativen Ring R kann man iterieren. Man erhält so z.B.

$$R[X,Y] := \big(R[X]\big)[Y] = \{\sum_{i,j} a_{ij} X^i Y^j : a_{ij} \in R,\ a_{ij} \neq 0 \text{ nur für endlich viele } i,j\}.$$

Wir unterscheiden im folgenden nicht zwischen $R[X,Y]$ und $R[Y,X]$.
Induktiv erhält man:

$$R[X_1, \dots, X_n] := \{\sum_{i_1,\dots,i_n} a_{i_1\dots i_n} X_1^{i_1} \dots X_n^{i_n} : a_{i_1\dots i_n} \in R,\ a_{i_1\dots i_n} \neq 0 \text{ nur für endlich viele } i_1, \dots, i_n\}.$$

Polynomringe in einer unendlichen Menge $\mathcal{X} = \{X_i : i \in I\}$ von Unbestimmten kann man dann folgendermaßen definieren:

$$R[\mathcal{X}] := R[X_i : i \in I] := \bigcup_{\substack{J \subseteq I \\ J \text{ endlich}}} R[X_j : j \in J].$$

Die entsprechenden Quotientenkörper bezeichnet man mit $R(X,Y), R(X_1, \dots, X_n), R(\mathcal{X}), \dots$.
Auch für solche Polynomringe hat man *Einsetzungshomomorphismen* :

$$\varphi : R[X_1, \dots, X_n] \to S,$$
$$f = \sum a_{i_1\dots i_n} X_1^{i_1} \dots X_n^{i_n} \mapsto f(s_1, \dots, s_n) := \sum a_{i_1\dots i_n} s_1^{i_1} \dots s_n^{i_n}.$$

Dabei ist S ein kommutativer Ring mit $1_S \in R$, und $s_1, \dots, s_n \in S$ fest.

Kapitel 15

Körpererweiterungen

Definition 15.1 *Ein Teilring K eines Körpers L heißt* Teilkörper *von L, falls $xy^{-1} \in K$ für alle $x, y \in K$ mit $y \neq 0$. In diesem Fall nennt man L einen* Erweiterungskörper *oder eine* Körpererweiterung *von K und schreibt: $L|K$.*

Beispiel: $\mathbb{C} \,|\, \mathbb{R}$, $\mathbb{C} \,|\, \mathbb{Q}$, $\mathbb{Q}(X) | \mathbb{Q}$.

Bemerkung:

(i) Ist $L|K$ Körpererweiterung, so wird K mit den entsprechend eingeschränkten Verknüpfungen Körper.

(ii) Der Durchschnitt von Teilkörpern von L ist wieder ein Teilkörper von L, insbesondere ist der Durchschnitt aller Teilkörper von L ein Teilkörper von L. Diesen nennt man den *Primkörper* von L.

Satz: *Ist K ein Körper und P der Primkörper von K, so gilt:*

(i) Ist $\mathrm{char}(K) = 0$*, so ist* $P \cong \mathbb{Q}$.

(ii) Ist $\mathrm{char}(K) = p \neq 0$*, so ist* $P \cong \mathbf{Z}/p\mathbf{Z}$.

Beweis:

(i) Im Fall $\mathrm{char}(K) = 0$ ist die Abbildung $\varphi : \mathbf{Z} \to K,\ n \mapsto n \cdot 1$ ein Monomorphismus von Ringen. Nach 11.2 kann man φ zu einen Monomorphismus $\psi : \mathbb{Q} \to K$ fortsetzen. Dann ist $\psi(\mathbb{Q})$ Teilkörper von K, also $P \subseteq \psi(\mathbb{Q})$.
Andrerseits ist

$$\psi(\mathbb{Q}) = \{\psi(q) : q \in \mathbb{Q}\} = \{\frac{\psi(m)}{\psi(n)} : m, n \in \mathbf{Z},\ n \neq 0\}.$$

Wegen $\psi(1) = 1 \in P$ ist auch $\psi(n) = \psi(1 + \ldots + 1) = \psi(1) + \ldots + \psi(1) = 1 + \ldots + 1 \in P$ für $n \in \mathbb{N}$, $\psi(n) \in P$ für $n \in \mathbf{Z}$, also auch $\frac{\psi(m)}{\psi(n)} \in P$ für $m, n \in \mathbf{Z},\ n \neq 0$. Daher ist $\psi(\mathbb{Q}) \subseteq P$.
Insgesamt ist $P = \psi(\mathbb{Q}) \cong \mathbb{Q}$.

(ii) In diesem Fall ist p eine Primzahl und $\mathbf{Z}/p\mathbf{Z}$ Körper. Nach der Definition der Charakteristik ist die Abbildung $\varphi : \mathbf{Z} \to K,\ n \mapsto n \cdot 1$ ein Homomorphismus mit Kern $p\mathbf{Z}$. Also ist $\varphi(\mathbf{Z}) \cong \mathbf{Z}/p\mathbf{Z}$ Teilkörper von K; insbesondere ist $P \subseteq \varphi(\mathbf{Z})$.
Andrerseits ist $1 \in P,\ 1 + 1 \in P,\ \ldots$, d.h. $n1 \in P$ für $n \in \mathbb{N}$, also $\varphi(\mathbf{Z}) \subseteq P$.
Insgesamt ist $P = \varphi(\mathbf{Z}) \cong \mathbf{Z}/p\mathbf{Z}$.

Bemerkung 15.2 Ist $L|K$ Körpererweiterung, so ist L ein K-Vektorraum vermöge der Addition $L \times L \to L$ und der Einschränkung $K \times L \to L$ der Multiplikation $L \times L \to L$. Man bezeichnet die Dimension von L über K als *Grad* von L über K und schreibt $[L : K]$. Im Fall $[L : K] < \infty$ nennt man L eine *endliche* Körpererweiterung von K.

Beispiel:

(a) $[\mathbb{C} : \mathbb{R}] = 2$, $\{1, i\}$ ist Basis.

(b) $[\mathbb{R} : \mathbb{Q}] = \infty$; denn im Fall $[\mathbb{R} : \mathbb{Q}] = n < \infty$ wäre $\mathbb{R} \cong \mathbb{Q}^n$ abzählbar.

(c) $[K(X) : K] = \infty$ für jeden Körper K; linear unabhängig sind $1, X, X^2, \ldots$.

(d) Jeder endliche Körper K ist offensichtlich eine endliche Erweiterung seines Primkörpers P. Wegen $|\mathbb{Q}| = \infty$ ist also $P \cong \mathbf{Z}/p\mathbf{Z}$ für eine Primzahl p, $p = \mathrm{char}(K)$. Als P-Vektorraum ist $K \cong P^{[K:P]}$; insbesondere ist $|K| = p^{[K:P]}$ eine p-Potenz.

Satz: (Gradsatz) *Für Körpererweiterungen $L|K$, $M|L$ gilt:*

$$[M : K] = [M : L][L : K].$$

$$\begin{array}{cc} & M \\ [M:L] & | \\ & L \\ [L:K] & | \\ & K \end{array} \left.\vphantom{\begin{array}{c} M \\ | \\ L \\ | \\ K \end{array}}\right) [M : K]$$

Beweis: Seien $l_1, \ldots, l_r \in L$ linear unabhängig über K, und $m_1, \ldots, m_s \in M$ linear unabhängig über L. Wir zeigen, daß die Elemente $l_i m_j$ $(i = 1, \ldots, r;\ j = 1, \ldots, s)$ linear unabhängig über K sind. Hat man nämlich Elemente $\alpha_{ij} \in K$ mit

$$0 = \sum_{i,j} \alpha_{ij} l_i m_j = \sum_j \underbrace{\left(\sum_i \alpha_{ij} l_i \right)}_{\in L} m_j,$$

so folgt aus der linearen Unabhängigkeit von $m_1, \ldots, m_s$ zunächst $\sum_i \alpha_{ij} l_i = 0$ für alle j und dann aus der linearen Unabhängigkeit von $l_1, \ldots, l_r$ auch $\alpha_{ij} = 0$ für alle i, j.
Im Fall $[M : L] = \infty$ oder $[L : K] = \infty$ ist $[M : K] = \infty = [M : L][L : K]$. Sei also $[M : L] < \infty$, $[L : K] < \infty$, $l_1, \ldots, l_r$ Basis von L über K und $m_1, \ldots, m_s$ Basis von M über L. Ist $x \in M$, so existieren $\lambda_1, \ldots, \lambda_s \in L$ mit $x = \sum_{j=1}^s \lambda_j m_j$, und für $j = 1, \ldots, s$ existieren $\kappa_{1j}, \ldots, \kappa_{rj} \in K$ mit $\lambda_j = \sum_{i=1}^r \kappa_{ij} l_i$. Daher ist $x = \sum_{i,j} \kappa_{ij} l_i m_j$, d.h. die Elemente $l_i m_j$ $(i = 1, \ldots, r;\ j = 1, \ldots, s)$ bilden eine Basis von M über K.

Bemerkung 15.3 Ist $L|K$ eine Körpererweiterung und $A \subseteq L$, so ist

$$\begin{aligned} K(A) \quad := \quad & \{\frac{f(a_1, \ldots, a_n)}{g(a_1, \ldots, a_n)} : a_1, \ldots, a_n \in A,\ f, g \in K[X_1, \ldots, X_n], \\ & g(a_1, \ldots, a_n) \neq 0,\ n \in \mathbb{N}_0\} \end{aligned}$$

der Durchschnitt aller Teilkörper von L, die K und A enthalten. Man sagt, $K(A)$ entsteht durch *Adjunktion* von A zu K. Im Fall $A = \{a_1, \ldots, a_n\}$ schreibt man $K(a_1, \ldots, a_n)$ statt $K(A)$. Ist $L = K(a)$ für ein $a \in L$, so nennt man die Körpererweiterung $L|K$ *einfach* und a ein *primitives* Element von $L|K$.
Analog ist

$$K[A] := \{f(a_1, \ldots, a_n) : a_1, \ldots, a_n \in A,\ f \in K[X_1, \ldots, X_n],\ n \in \mathbb{N}_0\}$$

der Durchschnitt aller Teilringe von L, die K und A enthalten.

Beispiel:

(a) $\mathbb{C} \mid \mathbb{R}$ ist einfach: $\mathbb{C} = \mathbb{R}(i)$.

(b) Für jeden Körper K ist $K(X)|K$ einfach mit primitivem Element X.

(c) Jede endliche Erweiterung L eines endlichen Körpers K ist einfach; denn wegen $|L| = |K^{[L:K]}| < \infty$ ist $L^\times$ nach 14.10 zyklisch, etwa $L^\times = \langle a \rangle$. Wegen $L = \{0, a, a^2, \ldots, a^{|L|-1} = 1\}$ ist $L = K(a)$.

Definition 15.4 *Seien $L|K$ und $M|K$ Körpererweiterungen und $\varphi : L \to M$ ein Ringhomomorphismus mit $\varphi(x) = x$ für $x \in K$. Dann nennt man φ einen Homomorphismus* über K *oder einen* K-Homomorphismus.

Bemerkung: In diesem Fall ist φ injektiv; denn wegen $\varphi(1) = 1 \neq 0$ ist $\varphi \neq 0$, also $\ker(\varphi) \neq L$. Da L Körper ist folgt: $\ker(\varphi) = 0$. Ferner ist φ K-linear; denn für $a \in K$ und $b \in L$ gilt: $\varphi(ab) = \varphi(a)\varphi(b) = a\varphi(b)$.

Beispiel: Die komplexe Konjugation $\mathbb{C} \to \mathbb{C},\ z \mapsto \bar{z}$ ist ein $\mathbb{R}$-Automorphismus von $\mathbb{C}$.

Definition 15.5 *Sei $L|K$ Körpererweiterung. Ein $a \in L$ heißt* algebraisch *über K, falls ein $f \in K[X] \setminus \{0\}$ existiert mit $f(a) = 0$. Andernfalls heißt a* transzendent *über K. Sind alle Elemente in L algebraisch über K, so nennt man L* algebraisch *über K, andernfalls* transzendent *über K.*

Beispiel:

(a) Jedes $k \in K$ ist algebraisch über K als Nullstelle von $X - k$.

(b) Die Unbestimmte X in $K(X)$ ist transzendent über K.

(c) i ist algebraisch über $\mathbb{R}$ als Nullstelle von $X^2 + 1$.

(d) Die über $\mathbb{Q}$ algebraischen Elemente in $\mathbb{C}$ nennt man *algebraische Zahlen*. Davon gibt es nur abzählbar viele; denn aus den abzählbar vielen Elementen in $\mathbb{Q}$ kann man nur abzählbar viele Polynome mit Koeffizienten in $\mathbb{Q}$ machen, und jedes von diesen (außer 0) hat nur endlich viele Nullstellen. Insbesondere kann nicht jede komplexe Zahl algebraisch über $\mathbb{Q}$ sein.
Hermite 1873: e ist transzendent.
Lindemann 1882: π ist transzendent.

(e) Jede endliche Erweiterung $L|K$ ist algebraisch; denn für $a \in L$ können die Elemente $1, a, a^2, \ldots, a^{[L:K]}$ nicht linear unabhängig sein. Also ist $\sum_{i=0}^{[L:K]} \alpha_i a^i = 0$ für geeignete $\alpha_0, \ldots, \alpha_{[L:K]} \in K$ mit $(\alpha_0, \ldots, \alpha_{[L:K]}) \neq 0$.

Satz: *Ist $L|K$ Körpererweiterung und $a \in L$ transzendent über K, so gibt es genau einen K-Homomorphismus $\varphi : K(X) \to L$ mit $\varphi(X) = a$. Dabei ist $\varphi(K(X)) = K(a) \cong K(X)$.*

Beweis: Ist $a \in L$ transzendent über K, so ist der Einsetzungshomomorphismus $\psi : K[X] \to L,\ f \mapsto f(a)$ injektiv, läßt sich also zu einem eindeutig bestimmten Monomorphismus $\varphi : K(X) \to L$ fortsetzen nach 11.2. Für $k \in K$ ist $\varphi(k) = \psi(k) = k$ und $\varphi(X) = \psi(X) = a$. Wegen

$$K(a) = \{\frac{f(a)}{g(a)},\ f, g \in K[X],\ \underbrace{g(a) \neq 0}_{g \neq 0}\} = \varphi(K(X))$$

bleibt nur die Eindeutigkeit zu zeigen. Ist $\varphi' : K(X) \to L$ ein K-Homomorphismus mit $\varphi'(X) = a$, so gilt für $\alpha_0, \dots, \alpha_n \in K$:

$$\begin{aligned} \varphi'\left(\sum_{i=0}^{n} \alpha_i X^i\right) &= \sum_{i=0}^{n} \underbrace{\varphi'(\alpha_i)}_{\alpha_i} \underbrace{\varphi'(X)}_{a}{}^i = \sum_{i=0}^{n} \alpha_i a^i = \\ &= \psi\left(\sum_{i=0}^{n} \alpha_i X^i\right). \end{aligned}$$

Daher ist $\varphi'(f) = \psi(f)$ für $f \in K[X]$. Aus der Eindeutigkeit der Fortsetzung φ nach 11.2 folgt $\varphi = \varphi'$.

Satz 15.6 *Sei $L|K$ Körpererweiterung und $a \in L$ algebraisch. Dann existiert genau ein normiertes irreduzibles Polynom $m_{K,a} \in K[X]$ mit*

$$m_{K,a}(a) = 0.$$

Der Einsetzungshomomorphismus $\varphi : K[X] \to L,\ f \mapsto f(a)$ hat Bild $K(a)$ und Kern $(m_{K,a})$; insbesondere ist $K(a) \cong K[X]/(m_{K,a})$. Jedes Polynom $f \in K[X]$ mit $f(a) = 0$ ist durch $m_{K,a}$ teilbar. Die Elemente $1, a, a^2, \dots, a^{n-1}$, wobei $n = \deg(m_{K,a})$, bilden eine K-Basis von $K(a)$; insbesondere ist $[K(a) : K] = \deg(m_{K,a}) < \infty$.

Definition: *Man nennt $m_{K,a}$ das* Minimalpolynom *von a über K.*

Beweis: Da a algebraisch über K ist, existiert ein $g \in K[X] \setminus \{0\}$ mit $g(a) = 0$, d.h. $g \in \ker(\varphi)$. Da $K[X]$ Hauptidealring ist, existiert ein $h \in K[X] \setminus \{0\}$ mit $\ker(\varphi) = (h)$. Wegen $K[X]^\times = K^\times$ existiert genau ein normiertes Polynom $m_{K,a} \in K[X]$ mit $\ker(\varphi) = (m_{K,a})$.
Nach dem Homomorphiesatz ist $K[X]/(m_{K,a}) \cong \mathrm{Bild}(\varphi) \subseteq L$ Integritätsbereich. Folglich ist $(m_{K,a})$ Primideal, und $m_{K,a}$ ist irreduzibel. Daher ist $(m_{K,a})$ maximales Ideal in $K[X]$, d.h. $\mathrm{Bild}(\varphi) \cong K[X]/(m_{K,a})$ sind Körper. Insbesondere ist $K(a) \subseteq \mathrm{Bild}(\varphi)$.
Andrerseits ist $\mathrm{Bild}(\varphi) = \{\sum_{i=0}^{n} \alpha_i a^i : \alpha_0, \dots, \alpha_n \in K,\ n \in \mathbb{N}\} \subseteq K(a)$. Insgesamt ist also $K(a) = \varphi(K[X]) \cong K[X]/(m_{K,a})$.
Jedes Polynom $f \in K[X]$ mit $f(a) = 0$ liegt in $\ker(\varphi) = (m_{K,a})$, ist also durch $m_{K,a}$ teilbar. Ist f zusätzlich irreduzibel, so sind also f und $m_{K,a}$ assoziiert in $K[X]$. Ist f außerdem normiert, so folgt $f = m_{K,a}$.
Jedes Element in $K(a)$ hat die Form $f(a)$ für ein $f \in K[X]$. Division mit Rest liefert $f = q m_{K,a} + r$, wobei $r = 0$ oder $\deg(r) < \deg(m_{K,a})$. Dann ist

$$f(a) = q(a) \underbrace{m_{K,a}(a)}_{=0} + r(a) = r(a) = \sum_{i=0}^{n-1} \alpha_i a^i$$

für geeignete $\alpha_0, \dots, \alpha_{n-1} \in K$. Daher spannen $1, a, \dots, a^{n-1}$ den K-Vektorraum $K(a)$ auf.
Sind $\beta_0, \dots, \beta_{n-1} \in K$ mit $0 = \sum_{i=0}^{n-1} \beta_i a^i$, so ist $g := \sum_{i=0}^{n-1} \beta_i X^i \in \ker(\varphi) = (m_{K,a})$, d.h. $m_{K,a} \mid g$. Im Fall $g \neq 0$ wäre $\deg(m_{K,a}) \leq \deg(g) < n = \deg(m_{K,a})$. Also ist $g = 0$ und $\beta_0 = \dots = \beta_{n-1} = 0$. Daher sind $1, a, \dots, a^{n-1}$ linear unabhängig über K.

Beispiel: $m_{\mathbb{R},i} = X^2 + 1$, $\mathbb{C} = \mathbb{R}(i) \cong \mathbb{R}[X]/(X^2+1)$.

Satz 15.7 *Für jede Körpererweiterung $L|K$ gilt:*

(i) Sind $a_1, \dots, a_n \in L$ algebraisch über K, so ist $K(a_1, \dots, a_n)|K$ endlich und daher algebraisch.

(ii) Ist A eine Menge von Elementen in L, die alle algebraisch über K sind, so ist $K(A)|K$ algebraisch.

(iii) $F := \{a \in L : a$ algebraisch über $K\}$ ist ein Teilkörper von L mit $K \subseteq F$.

(iv) Ist M Teilkörper von L mit $K \subseteq M$, so gilt:
$L|K$ algebraisch $\Leftrightarrow$ $L|M$, $M|K$ algebraisch.

Beweis:

(i) Ist a_i algebraisch über K für $i = 1, \dots, n$, so auch über $K(a_1, \dots, a_{i-1})$. Nach 15.6 ist $[K(a_1, \dots, a_i) : K(a_1, \dots, a_{i-1})] < \infty$. Nach dem Gradsatz ist

$$[K(a_1, \dots, a_n) : K] = \prod_{i=1}^{n} [K(a_1, \dots, a_i) : K(a_1, \dots, a_{i-1})] < \infty.$$

Nach 15.5 ist $K(a_1, \dots, a_n)|K$ algebraisch.

(ii) Ist $x \in K(A)$, so existieren $a_1, \dots, a_n \in A$ und $f, g \in K[X_1, \dots, X_n]$ mit $x = \frac{f(a_1,\dots,a_n)}{g(a_1,\dots,a_n)}$ und $g(a_1, \dots, a_n) \neq 0$. Daher ist $x \in K(a_1, \dots, a_n)$. Nach (i) ist $K(a_1, \dots, a_n)|K$ algebraisch; insbesondere ist x algebraisch über K.

(iii) Nach 15.5 ist $K \subseteq F$. Für $a, b \in F$ ist $K(a,b)|K$ algebraisch nach (i). Daher sind auch $a \pm b, ab^{\pm 1} \in K(a,b) \subseteq F$. Somit ist F Teilkörper von L.

(iv) $\Rightarrow$**:** Trivial.

$\Leftarrow$**:** Seien $L|M$, $M|K$ algebraisch, $a \in L$ und $m_{M,a} = \sum_{i=0}^{n} m_i X^i$ mit $m_0, \dots, m_n \in M$. Da $m_0, \dots, m_n$ algebraisch über K sind, ist $[K(m_0, \dots, m_n) : K] < \infty$ nach (i). Da a algebraisch über $K(m_0, \dots, m_n)$ ist, ist $[K(m_0, \dots, m_n, a) : K(m_0, \dots, m_n)] < \infty$. Nach dem Gradsatz ist $[K(m_0, \dots, m_n, a) : K] < \infty$, also $K(m_0, \dots, m_n, a)|K$ algebraisch. Insbesondere ist a algebraisch über K.

Beispiel: Die algebraischen Zahlen bilden einen abzählbaren Teilkörper A von $\mathbb{C}$, der $\mathbb{Q}$ enthält.

Satz 15.8 *Sei $L|K$ Körpererweiterung, $a \in L$ algebraisch über K und M Teilkörper von $K(a)$ mit $K \subseteq M$. Ist $m_{M,a} = \sum_{i=0}^{r} m_i X^i$ mit $m_0, \dots, m_r \in M$, so ist $M = K(m_0, \dots, m_r)$.*

Beweis: Offenbar ist $M' := K(m_0, \dots, m_r) \subseteq M$. Außerdem ist $m_{M,a} \in M'[X]$ irreduzibel in $M'[X]$, d.h. $m_{M,a} = m_{M',a}$. Wegen $K(a) = M'(a) = M(a)$ ist also

$$[K(a) : M] = \deg(m_{M,a}) = \deg(m_{M',a}) = [K(a) : M'] = [K(a) : M][M : M'].$$

Folglich ist $[M : M'] = 1$, d.h. $M = M'$.

Satz 15.9 *Für eine Körpererweiterung $L|K$ sind äquivalent:*

(1) Es existiert ein über K algebraisches Element $a \in L$ mit $L = K(a)$.

(2) L besitzt nur endlich viele Teilkörper, die K enthalten.

Beweis:

(1) $\Rightarrow$ (2)**:** Sei $L = K(a)$ für ein über K algebraisches Element $a \in L$. Ist M Teilkörper von L mit $K \subseteq M$, und schreibt man $m_{M,a} = \sum_{i=0}^{r} m_i X^i$ mit $m_0, \ldots, m_r \in M$, so ist $M = K(m_0, \ldots, m_r)$ nach 15.8. Wegen $m_{K,a} \in K[X] \subseteq M[X]$ und $m_{K,a}(a) = 0$ ist $m_{M,a} \mid m_{K,a}$ in $M[X] \subseteq L[X]$ nach 15.6. Das Polynom $m_{K,a}$ hat aber in $L[X]$ nur endlich viele Teiler. Also gibt es für $m_{M,a}$ und damit für M nur endlich viele Möglichkeiten.

(2) $\Rightarrow$ (1)**:** Sei (2) erfüllt. Für $a \in L \setminus \{0\}$ existiert wegen

$$L \supseteq K(a) \supseteq K(a^2) \supseteq K(a^4) \supseteq \ldots \supseteq K$$

ein $n \in \mathbb{N}$ mit $K(a^{2^n}) = K(a^{2^{n+1}})$, d.h. $a^{2^n} = \frac{f(a^{2^{n+1}})}{g(a^{2^{n+1}})}$ für geeignete $f, g \in K[X]$ mit $g(a^{2^{n+1}}) \neq 0$. Dann ist $a^{2^n} g(a^{2^{n+1}}) = f(a^{2^{n+1}})$. Wäre $X^{2^n} g(X^{2^{n+1}}) = f(X^{2^{n+1}})$, so wäre $2^n + 2^{n+1}\deg(g) = 2^{n+1}\deg(f)$, also $2^{n+1} \mid 2^n$. Widerspruch. Daher ist $X^{2^n} g(X^{2^{n+1}}) - f(X^{2^{n+1}}) \in K[X] \setminus \{0\}$ mit Nullstelle a. Folglich ist a algebraisch über K. Somit ist $L|K$ algebraisch.
Im Fall $L = K$ ist $L = K(1)$. Im Fall $L \neq K$ wähle man $a_1 \in L \setminus K$. Im Fall $K(a_1) = L$ ist man fertig. Im Fall $K(a_1) \neq L$ wähle man $a_2 \in L \setminus K(a_1)$. Da a_2 algebraisch über K ist, ist $[K(a_1, a_2) : K] < \infty$. Ist K endlich, so ist $K(a_1, a_2)|K$ einfach nach Beispiel 15.3.
Wir zeigen, daß dies auch im Fall $|K| = \infty$ gilt. Für $z \in K$ ist $K \subseteq K(a_1 + a_2 z) \subseteq K(a_1, a_2)$. Unter den Körpern $K(a_1 + a_2 z)$, $z \in K$ gibt es nach (2) nur endlich viele verschiedene. Ist $|K| = \infty$, so existieren verschiedene $z_1, z_2 \in K$ mit $K(a_1 + a_2 z_1) = K(a_1 + a_2 z_2)$. Dann ist $a_1 + a_2 z_1 \in K(a_1 + a_2 z_2)$, $a_2 \underbrace{(z_1 - z_2)}_{\neq 0} = a_1 + a_2 z_1 - (a_1 + a_2 z_2) \in K(a_1 + a_2 z_2)$, $a_2 \in K(a_1 + a_2 z_2)$, $a_1 \in K(a_1 + a_2 z_2)$, also $K(a_1, a_2) \subseteq K(a_1 + a_2 z_2) \subseteq K(a_1, a_2)$, d.h. $K(a_1, a_2) = K(a_1 + a_2 z_2)$. Daher existiert in jedem Fall $b_1 \in L$ mit $K(a_1, a_2) = K(b_1)$. Im Fall $K(b_1) = L$ ist man fertig. Im Fall $K(b_1) \neq L$ wählt man $b_2 \in L \setminus K(b_1)$ und wiederholt das obige Verfahren. Auf diese Weise erhält man eine Folge von einfachen Körpererweiterungen $K \underset{\neq}{\subset} K(c_1) \underset{\neq}{\subset} K(c_2) \underset{\neq}{\subset} \ldots \underset{\neq}{\subset} L$. Nach (2) bricht das Verfahren ab, d.h. es existiert ein $n \in \mathbb{N}$ mit $L = K(c_n)$.

Satz 15.10 *Ist $L|K$ eine Körpererweiterung, $a \in L$ algebraisch über K und M ein Teilkörper von $K(a)$ mit $K \subseteq M$, so existiert ein über K algebraisches Element $b \in M$ mit $M = K(b)$.*

Beweis: Nach 15.9 existieren unter diesen Voraussetzungen nur endlich viele Körper zwischen K und $K(a)$. Daher existieren auch nur endlich viele Körper zwischen K und M. Aus 15.9 folgt die Behauptung.

Bemerkung: Eine entsprechende Aussage gilt auch, falls a transzendent über K ist. (Satz von Lüroth)

Kapitel 16

Zerfällungskörper

Satz 16.1 *Sei K Körper und $f \in K[X]$ irreduzibel. Dann existiert eine Körpererweiterung $L|K$, in der f eine Nullstelle a hat.*

Bemerkung: Nach 15.6 ist in diesem Fall $K(a) \cong K[X]/(f)$. Wir werden daher umgekehrt versuchen, L auf diese Weise zu konstruieren.

Beweis: Da f irreduzibel ist, ist (f) maximales Ideal in $K[X]$, d.h. $\tilde{L} := K[X]/(f)$ ist Körper. Die Einschränkung das natürlichen Epimorphismus $\nu : K[X] \to \tilde{L}$ ist ein Homomorphismus $\varphi : K \to \tilde{L}$ mit $\varphi(1) = 1 \neq 0$. Da $\ker(\varphi)$ Ideal im Körper K ist, folgt $\ker(\varphi) = 0$, d.h. φ ist injektiv. Insbesondere ist $\tilde{K} := \varphi(K) \cong K$ und $\tilde{L}|\tilde{K}$ Körpererweiterung. Der Isomorphismus $K \to \tilde{K},\ \alpha \mapsto \varphi(\alpha) = \alpha + (f)$ induziert einen Isomorphismus

$$\Phi : K[X] \to \tilde{K}[\tilde{X}],\ \sum \alpha_i X^i \mapsto \sum \varphi(\alpha_i)\tilde{X}^i;$$

dabei ist $\tilde{X}$ eine Unbestimmte über $\tilde{K}$. Mit f ist auch $\tilde{f} := \Phi(f)$ irreduzibel. Schreibt man $f = \sum_{i=0}^n \alpha_i X^i$ mit $\alpha_0, \ldots, \alpha_n \in K$, so ist $\tilde{f} = \sum_{i=0}^n (\alpha_i + (f))\tilde{X}^i$, und für $\tilde{\alpha} := X + (f) \in \tilde{L}$ gilt:

$$\tilde{f}(\tilde{\alpha}) = \sum_{i=0}^n (\alpha_i + (f))(X + (f))^i = \sum_{i=0}^n \alpha_i X^i + (f) = f + (f) = (f) = 0 \in \tilde{L}.$$

Daher erfüllen der zu K isomorphe Körper $\tilde{K}$ und das f entsprechende Polynom $\tilde{f}$ die Behauptung das Satzes. Analoges gilt daher für K und f.

Satz 16.2 (Fortsetzungssatz) *Seien $K, \tilde{K}$ Körper, $\varphi : K \to \tilde{K}$ ein Isomorphismus, $f = \sum_{i=0}^n \alpha_i X^i \in K[X]$ irreduzibel mit $\alpha_0, \ldots, \alpha_n \in K$, a eine Nullstelle von f in einer Körpererweiterung $L|K$ und $\tilde{a}$ eine Nullstelle von $\tilde{f} := \sum_{i=0}^n \varphi(\alpha_i)X^i$ in einer Körpererweiterung $\tilde{L}|\tilde{K}$. Dann existiert genau ein Isomorphismus $\psi : K(a) \to \tilde{K}(\tilde{a})$ mit $\psi(a) = \tilde{a}$ und $\psi(x) = \varphi(x)$ für $x \in K$.*

Beweis: Man setzt zunächst φ zu einem Isomorphismus

$$\Phi : K[X] \to \tilde{K}[X],\ \sum_{i=0}^m \beta_i X^i \mapsto \sum_{i=0}^m \varphi(\beta_i)X^i$$

fort; dabei ist $\Phi(f) = \tilde{f}$. Daher induziert Φ einen Isomorphismus

$$\Psi : K[X]/(f) \to \tilde{K}[X]/(\tilde{f}),\ y + (f) \mapsto \Phi(y) + (\tilde{f}).$$

Da f irreduzibel ist, ist $(f) = (m_{K,a})$. Nach 15.6 ist also die Abbildung $K[X]/(f) \to K(a),\ g + (f) \mapsto g(a)$ ein Isomorphismus. Da mit f auch $\Phi(f) = \tilde{f}$ irreduzibel ist, ist analog die

Abbildung $\tilde{K}[X]/(\tilde{f}) \to \tilde{K}(\tilde{a}),\ g + (\tilde{f}) \mapsto g(\tilde{a})$ ein Isomorphismus. Der zusammengesetzte Isomorphismus

$$\psi : K(a) \to K[X]/(f) \to \tilde{K}[X]/(\tilde{f}) \to \tilde{K}(\tilde{a})$$

erfüllt dann:

$$\begin{aligned} &x \in K \;\Rightarrow\; x \mapsto x + (f) \mapsto \varphi(x) + (\tilde{f}) \mapsto \varphi(x), \\ &a \mapsto X + (f) \mapsto X + (\tilde{f}) \mapsto \tilde{a} \end{aligned}$$

wie gewünscht. Offenbar ist $K(a) = \{\sum_{i=0}^{n-1} \beta_i a^i : \beta_0, \dots, \beta_{n-1} \in K\}$ und $\tilde{K}(\tilde{a}) = \{\sum_{i=0}^{n-1} \tilde{\beta}_i \tilde{a}^i : \tilde{\beta}_0, \dots, \tilde{\beta}_{n-1} \in \tilde{K}\}$. Ist also $\psi' : K(a) \to \tilde{K}(\tilde{a})$ ein Isomorphismus mit $\psi'(x) = \varphi(x)$ für $x \in K$ und $\psi'(a) = \tilde{a}$, so gilt für $\beta_0, \dots, \beta_{n-1} \in K$:

$$\psi'(\sum_{i=0}^{n-1} \beta_i a^i) \;=\; \sum_{i=0}^{n-1} \underbrace{\psi'(\beta_i)}_{\varphi(\beta_i)} \underbrace{\psi'(a)}_{\tilde{a}}{}^i \;=\; \sum_{i=0}^{n-1} \underbrace{\varphi(\beta_i)}_{\psi(\beta_i)} \underbrace{\tilde{a}}_{\psi(a)}{}^i \;=\; \psi(\sum_{i=0}^{n-1} \beta_i a^i).$$

Daher ist $\psi' = \psi$.

Satz 16.3 *Sei K Körper, $f \in K[X]$ irreduzibel und a, b Nullstellen von f in einer Körpererweiterung $L|K$. Dann gibt es genau einen K-Isomorphismus $\sigma : K(a) \to K(b)$ mit $\sigma(a) = b$.*

Beweis: 16.2 mit $\varphi = \mathrm{id}_K$.

Beispiel: Da i und $-i$ zwei Nullstellen des irreduziblen Polynoms $X^2 + 1$ in $\mathbb{R}[X]$ sind, gibt es einen $\mathbb{R}$-Isomorphismus $\mathbb{C} = \mathbb{R}(i) \to \mathbb{C} = \mathbb{R}(-i)$, der i auf $-i$ abbildet (komplexe Konjugation).

Definition 16.4 *Sei K Körper und $f \in K[X] \setminus K$. Eine Körpererweiterung $L|K$ heißt* Zerfällungskörper *von f über K, wenn Elemente $a_1, \dots, a_r, c \in L$ existieren mit $L = K(a_1, \dots, a_r)$ und $f = c(X - a_1) \dots (X - a_r)$.*

Satz: *Sei K Körper und $f = \sum_{i=0}^{n} \alpha_i X^i \in K[X] \setminus K$ mit $\alpha_0, \dots, \alpha_n \in K$.*

(i) Es existiert ein Zerfällungskörper L von f über K mit $[L : K] \leq n!$.

(ii) Ist L Zerfällungskörper von f über K, $\varphi : K \to \tilde{K}$ ein Körperisomorphismus und $\tilde{L}$ ein Zerfällungskörper von $\tilde{f} = \sum_{i=0}^{n} \varphi(\alpha_i) \tilde{X}^i \in \tilde{K}[\tilde{X}]$ über $\tilde{K}$, so gibt es einen Isomorphismus $\psi : L \to \tilde{L}$, der φ fortsetzt. Insbesondere sind je zwei Zerfällungskörper von f über K K-isomorph.

Bemerkung: Man spricht daher auch von *dem* Zerfällungskörper von f über K.

Beweis:

(i) (Induktion nach $m := \deg(f)$) Im Fall $m = 1$ ist $f = \alpha_1 X + \alpha_0 = \alpha_1(X - \frac{\alpha_0}{\alpha_1})$ mit $\alpha_1 \neq 0$. In diesem Fall ist $K(\frac{\alpha_0}{\alpha_1}) = K$ Zerfällungskörper von f über K, und $[K : K] = 1 \leq 1!$. Sei also $m > 1$ und p ein irreduzibler Faktor von f in $K[X]$. Nach 16.1 existiert eine Körpererweiterung $L_1|K$, in der p eine Nullstelle a_1 hat, o.B.d.A. $L_1 = K(a_1)$, d.h. $[L_1 : K] = \deg(p) \leq \deg(f) = m$. Es existiert $g \in L_1[X]$ mit $f = (X - a_1)g$ und $\deg(g) = m - 1$. Nach Induktion existieren eine Körpererweiterung $L|L_1$ und Elemente $a_2, \dots, a_m, c \in L$ mit $g = c(X - a_2) \dots (X - a_m),\ L = L_1(a_2, \dots, a_m)$ und $[L : L_1] \leq (m-1)!$. Dann ist $f = c(X - a_1) \dots (X - a_m),\ L = K(a_1, a_2, \dots, a_m)$ und $[L : K] = [L : L_1][L_1 : K] \leq m!$.

(ii) (Induktion nach $m := [L : K]$) Im Fall $m = 1$ ist $L = K$, d.h. es existieren $a_1, \ldots, a_r, c \in K$ mit $f = c(X - a_1) \ldots (X - a_r)$. Da die Abbildung $\Phi : K[X] \to \tilde{K}[\tilde{X}]$, $\sum \beta_i X^i \mapsto \sum \varphi(\beta_i) \tilde{X}^i$ ein Isomorphismus ist, ist

$$\tilde{f} = \Phi(f) = \varphi(c)\big(X - \varphi(a_1)\big) \ldots \big(X - \varphi(a_r)\big)$$

in $\tilde{K}[\tilde{X}]$, d.h. $\tilde{L} = \tilde{K}(\varphi(a_1), \ldots, \varphi(a_r)) = \tilde{K}$. In diesem Fall hat $\psi := \varphi$ die gewünschten Eigenschaften.

Im Fall $m > 1$ existiert ein irreduzibler Faktor p von f in $K[X]$ mit $\deg(p) > 1$. Dann ist $\tilde{p} := \Phi(p)$ ein irreduzibler Faktor von $\Phi(f) = \tilde{f}$. Mit f zerfällt auch p in $L[X]$ in Linearfaktoren, hat also mindestens eine Nullstelle $a \in L$. Analog enthält $\tilde{L}$ eine Nullstelle $\tilde{a}$ von $\tilde{p}$. Nach 16.2 existiert eine Fortsetzung von φ zu einem Isomorphismus $\varphi' : K(a) \to \tilde{K}(\tilde{a})$ mit $\varphi'(a) = \tilde{a}$. Offenbar ist L auch Zerfällungskörper von f über $K(a)$, und $\tilde{L}$ ist Zerfällungskörper von $\tilde{f}$ über $\tilde{K}(\tilde{a})$. Nach dem Gradsatz ist

$$[L : K(a)] \;=\; [L : K] \big/ [K(a) : K] \;=\; m \big/ \deg(p) \;<\; m.$$

Nach Induktion kann man also φ' zu einem Isomorphismus $\psi : L \to \tilde{L}$ fortsetzen.

Beispiel: Das Polynom $f := X^3 - 2$ besitzt in $\mathbb{R}$ genau eine Nullstelle, nämlich $\sqrt[3]{2}$. Daher ist

$$f = \left(X - \sqrt[3]{2}\right)\left(X^2 + \sqrt[3]{2}X + \sqrt[3]{2}^{\,2}\right)$$

in $\big(\mathbb{Q}(\sqrt[3]{2})\big)[X]$. Die weiteren Nullstellen von f sind $\sqrt[3]{2}\rho$ und $\sqrt[3]{2}\rho^2$ mit $\rho = \frac{1}{2}(-1 + \sqrt{-3}) \in \mathbb{C} \setminus \mathbb{R}$. Daher ist $L := \mathbb{Q}(\sqrt[3]{2}, \sqrt[3]{2}\rho, \sqrt[3]{2}\rho^2) = \mathbb{Q}(\sqrt[3]{2}, \rho)$ Zerfällungskörper von f über $\mathbb{Q}$, und $[L : \mathbb{Q}] = 6$.

Definition 16.5 *Eine algebraische Körpererweiterung $L|K$ heißt* normal*, falls jedes irreduzible Polynom in $K[X]$, das in L eine Nullstelle hat, in $L[X]$ in Linearfaktoren zerfällt.*

Satz: *Für eine endliche Körpererweiterung $L|K$ sind äquivalent:*

(1) $L|K$ ist normal.

(2) L ist Zerfällungskörper eines Polynoms $f \in K[X]$ über K.

(3) Ist $M|L$ eine Körpererweiterung und $\varphi : L \to M$ ein K-Homomorphismus, so ist $\varphi(L) \subseteq L$.

Beweis:

(1)⇒(2): Wir wählen eine K-Basis $a_1, \ldots, a_n$ von L und setzen $f := \prod_{i=1}^n m_{K,a_i}$. Ist (1) erfüllt, so zerfällt f wegen $m_{K,a_i}(a_i) = 0$ für $i = 1, \ldots, n$ in $L[X]$ in Linearfaktoren. Wegen $L = K(a_1, \ldots, a_n)$ ist L Zerfällungskörper von f über K.

(2)⇒(3): Sei (2) erfüllt. Dann existieren $a_1, \ldots, a_n, c \in L$ mit $f = c(X - a_1) \ldots (X - a_n)$ und $L = K(a_1, \ldots, a_n)$. Wir schreiben $f = \sum_{i=0}^n \alpha_i X^i$ mit $\alpha_0, \ldots, \alpha_n \in K$. Sei $M|L$ Körpererweiterung und $\varphi : L \to M$ ein K-Homomorphismus. Für $j = 1, \ldots, n$ gilt dann:

$$\begin{aligned} 0 \;&=\; \varphi(0) \;=\; \varphi(f(a_j)) \;=\; \varphi\left(\sum_{i=0}^n \alpha_i a_j^i\right) \;=\; \sum_{i=0}^n \alpha_i \varphi(a_j)^i \;= \\ &=\; f(\varphi(a_j)) \;=\; c(\varphi(a_j) - a_1) \ldots (\varphi(a_j) - a_n). \end{aligned}$$

Daher existiert ein $i \in \{1, \ldots, n\}$ mit $\varphi(a_j) = a_i \in L$. Folglich ist $\varphi(L) = \varphi(K(a_1, \ldots, a_n)) \subseteq L$.

(3)⇒(1): Sei (3) erfüllt und $f \in K[X]$ irreduzibel mit Nullstelle $a \in L$. Wir wählen eine K-Basis $a_1, \ldots, a_n$ von L und einen Zerfällungskörper M von $f m_{K,a_1} \ldots m_{K,a_n}$ über L. Ist $b \in M$ mit $f(b) = 0$, so existiert nach 16.3 ein K-Isomorphismus $\sigma : K(a) \to K(b)$ mit $\sigma(a) = b$. Wegen $L = K(a_1, \ldots, a_n)$ ist M auch Zerfällungskörper von $f m_{K,a_1} \ldots m_{K,a_n}$ über $K, K(a), K(b)$. Nach 16.4 kann man σ zu einem K-Automorphismus φ von M fortsetzen. Wegen (3) ist $b = \varphi(a) \in \varphi(L) \subseteq L$. Daher zerfällt f in $L[X]$ in Linearfaktoren.

Beispiel: Jede Körpererweiterung $L|K$ mit $[L:K]=2$ ist normal; ist nämlich $y \in L \setminus K$, so ist $L = K(y)$, also $\deg(m_{K,y}) = [L:K] = 2$. Daher ist $m_{K,y} = (X-y)g$ für ein $g \in L[X]$ mit $\deg(g) = 1$. Folglich ist L Zerfällungskörper von $m_{K,y}$ über K.

Satz 16.6 *Zu jeder endlichen Körpererweiterung $L|K$ existiert eine endliche normale Körpererweiterung $M|K$ mit $K \subseteq L \subseteq M$.*

Beweis: Wir wählen eine K-Basis $a_1, \ldots, a_n$ von L und einen Zerfällungskörper M von $f := m_{K,a_1} \ldots m_{K,a_n}$ über L. Dann ist M auch Zerfällungskörper von f über K, d.h. $M|K$ ist nach 16.5 normal.

Kapitel 17

Separabilität

Definition 17.1 *Seien K Körper, $a \in K$ und $f \in K[X] \setminus K$ mit $f(a) = 0$. Dann nennt man $m := \max\{n \in \mathbb{N} : (X-a)^n \mid f \text{ in } K[X]\}$ die* Vielfachheit *der Nullstelle a von f. Im Fall $m = 1$ nennt man a eine* einfache*, sonst eine* mehrfache *Nullstelle von f.*

Definition 17.2 *Seien R ein kommutativer Ring und $f = \sum_{i=0}^{n} a_i X^i \in R[X]$ mit $a_0, \ldots, a_n \in R$. Dann nennt man $f' := \sum_{i=1}^{n} i a_i X^{i-1}$ die* (formale) Ableitung *von f.*

Bemerkung: Man rechnet nach, daß für $f, g \in R[X]$, $a \in R$ gilt:

(i) $(f+g)' = f' + g'$, $(af)' = af'$.

(ii) $(fg)' = f'g + fg'$.

(iii) $(f \circ g)' = (f' \circ g)g'$; dabei ist $f \circ g := f(g)$.

Satz: *Sei K Körper, $a \in K$ und $f \in K[X] \setminus K$ mit $f(a) = 0$. Genau dann ist a eine einfache Nullstelle von f, wenn $f'(a) \neq 0$ ist.*

Beweis: Sei m die Vielfachheit der Nullstelle a von f. Dann ist $f = (X-a)^m g$ für ein $g \in K[X]$ mit $g(a) \neq 0$. Folglich ist $f' = m(X-a)^{m-1}g + (X-a)^m g'$. Im Fall $m \geq 2$ ist also $f'(a) = 0$, und im Fall $m = 1$ ist $f'(a) = g(a) \neq 0$.

Satz 17.3 *Für einen Körper K und ein Polynom $f \in K[X] \setminus K$ sind äquivalent:*

(1) f hat in jedem Zerfällungskörper L von f über K eine mehrfache Nullstelle.

(2) Es gibt eine Körpererweiterung $L|K$, in der f eine mehrfache Nullstelle hat.

(3) f und f' sind in $K[X]$ nicht teilerfremd.

Bemerkung: Ist f irreduzibel, so ist dazu auch äquivalent:

(4) $f' = 0$.

Beweis:

(1)⇒(2): Trivial wegen der Existenz von Zerfällungskörpern.

(2)⇒(3): Sei (2) erfüllt und $a \in L$ mehrfache Nullstelle von f. Nach 17.2 ist $f(a) = 0 = f'(a)$, also $m_{K,a} \mid f$ und $m_{K,a} \mid f'$.

(3)⇒(1): Sei (3) erfüllt und $g \in K[X] \setminus K$ mit $g \mid f$ und $g \mid f'$. Ist L Zerfällungskörper von f über K, so zerfällt auch g in $L[X]$ in Linearfaktoren. Ist $a \in L$ mit $g(a) = 0$, so ist also $f(a) = 0 = f'(a)$. Nach 17.2 ist daher a mehrfache Nullstelle von f.

(3)⇒(4): Sei f irreduzibel und $f' \neq 0$. Dann ist $\deg(f') < \deg(f)$, also $f \nmid f'$. Daher sind f und f' teilerfremd.

(4)⇒(3): Sei f irreduzibel und $f' = 0$. Dann ist f gemeinsamer Teiler von f und f'.

Satz 17.4 *Für einen Körper K und $f \in K[X]$ gilt:*

$$f' = 0 \iff \begin{cases} f \in K & , \mathrm{char}(K) = 0 \\ \exists g \in K[X],\ f = g(X^p) & , \mathrm{char}(K) = p \neq 0 \end{cases}$$

Beweis: Sei $f = \sum_{i=0}^{n} a_i X^i$ mit $a_0, \ldots, a_n \in K$, also $f' = \sum_{i=1}^{n} i a_i X^{i-1}$. Ist $\mathrm{char}(K) = 0$, so gilt:

$$\begin{aligned} f' = 0 &\Leftrightarrow i a_i = 0 \text{ für } i = 1, \ldots, n \\ &\Leftrightarrow a_i = 0 \text{ für } i = 1, \ldots, n \\ &\Leftrightarrow f \in K \end{aligned}$$

Ist $\mathrm{char}(K) = p \neq 0$, so gilt:

$$\begin{aligned} f' = 0 &\Leftrightarrow i a_i = 0 \text{ für } i = 1, \ldots, n \\ &\Leftrightarrow i1 = 0 \ \vee\ a_i = 0 \text{ für } i = 1, \ldots, n \\ &\Leftrightarrow p \mid i \ \vee\ a_i = 0 \text{ für } i = 1, \ldots, n \\ &\Leftrightarrow f = a_0 + a_p X^p + a_{2p} X^{2p} + \ldots \end{aligned}$$

Satz 17.5 *Für einen Körper K und ein $f \in K[X] \setminus K$ sind äquivalent:*

(1) Ist p ein irreduzibler Faktor von f in $K[X]$, so hat p in keinem Erweiterungskörper $L|K$ eine mehrfache Nullstelle.

(2) Ist p ein irreduzibler Faktor von f in $K[X]$ und L Zerfällungskörper von f über K, so hat p in L keine mehrfachen Nullstellen.

(3) Ist p ein irreduzibler Faktor von f, so ist $p' \neq 0$.

Beweis: 17.3.

Definition: *In diesem Fall nennt man f* separabel*, andernfalls* inseparabel *über K.*

Beispiel:

(a) Im Fall $\mathrm{char}(K) = 0$ ist jedes $f \in K[X]$ separabel über K.

(b) Sei $K := (\mathbf{Z}/2\mathbf{Z})(Y)$ mit einer Unbestimmten Y und $f := X^2 - Y \in K[X]$. Dann ist f irreduzibel in $K[X]$; denn sonst hätte f eine Nullstelle in K, etwa $\frac{p^2}{q^2} = Y$ mit $p, q \in (\mathbf{Z}/2\mathbf{Z})[Y]$, $q \neq 0$. Dann wäre $p^2 = q^2 Y$, was unmöglich ist ($\deg(p^2)$ ist gerade, $\deg(q^2 Y)$ ungerade). Also ist f irreduzibel in $K[X]$ und $f' = 0$. Daher ist f inseparabel über K.

Satz 17.6 *Für eine Körpererweiterung $L|K$ und $a \in L$ sind äquivalent:*

(1) a ist Nullstelle eines über K separablen Polynoms $f \in K[X]$.

(2) a ist algebraisch über K, und $m_{K,a}$ ist separabel über K.

Beweis: Trivial wegen $m_{K,a} \mid f$ für jedes $f \in K[X]$ mit $f(a) = 0$.

Definition: *In diesem Fall nennt man a* separabel, *andernfalls* inseparabel *über K. Ist jedes Element in L separabel über K, so nennt man $L|K$* separabel, *andernfalls* inseparabel.

Satz 17.7 *Für jeden Körper K der Charakteristik $p \neq 0$ ist die Abbildung $\varphi : K \to K$, $x \mapsto x^p$ ein Homomorphismus.*

Definition: *Man nennt φ den* Frobenius-Homomorphismus *von K.*

Beweis: Da p Primzahl ist, folgt aus 14.5 $p \mid \binom{p}{i}$ für $i = 1, \ldots, p-1$. Wegen $pa = 0$ für $a \in K$ ist $(x+y)^p = \sum_{i=0}^{p} \binom{p}{i} x^i y^{p-i} = x^p + y^p$. Trivialerweise ist $(xy)^p = x^p y^p$ für $x, y \in K$.

Satz 17.8 *Für einen Körper K sind äquivalent:*

(1) Jede algebraische Erweiterung $L|K$ ist separabel.

(2) Jedes $f \in K[X] \setminus K$ ist separabel über K.

(3) Jedes irreduzible $f \in K[X]$ ist separabel über K.

(4) Entweder ist $\mathrm{char}(K) = 0$ *oder* $\mathrm{char}(K) \neq 0$ *und der Frobenius-Homomorphismus von K ist bijektiv.*

Definition: *In diesem Fall nennt man K* vollkommen *oder* perfekt.

Beweis:

(1)⇒(2): Sei (1) erfüllt, $f \in K[X] \setminus K$, p ein irreduzibler Faktor von f, L ein Zerfällungskörper von f über K und $a \in L$ Nullstelle von p. Dann ist $p = c m_{K,a}$ für ein $c \in K$. Da a separabel über K ist, hat $m_{K,a}$ keine mehrfachen Nullstellen in L, also auch p. Daher ist f separabel über K.

(2)⇒(3): Trivial.

(3)⇒(4): Sei (3) erfüllt und o.B.d.A. $\mathrm{char}(K) = p \neq 0$. Es genügt zu zeigen, daß der Frobenius-Homomorphismus $\varphi : K \to K$, $x \mapsto x^p$ surjektiv ist. Dazu sei $a \in K$ und b eine Nullstelle von $X^p - a \in K[X]$ in einem Zerfällungskörper L von $X^p - a$ über K. Dann ist $m_{K,b} \mid X^p - a$ in $K[X]$, d.h. es existiert ein $g \in K[X]$ mit $m_{K,b} g = X^p - a = X^p - b^p = (X-b)^p$ in $L[X]$. Da $L[X]$ faktoriell ist, existiert ein $r \in \mathbb{N}$ mit $m_{K,b} = (X-b)^r$. Wegen (3) ist $r = 1$, d.h. $X - b = m_{K,b} \in K[X]$, insbesondere $b \in K$ und $b^p = a$.

(4)⇒(1): Sei (4) erfüllt, $L|K$ algebraische Körpererweiterung und $a \in L$. Ist a nicht separabel über K, so ist $m_{K,a}$ nicht separabel über K, also $m'_{K,a} = 0$ nach 17.5. Im Fall $\mathrm{char}(K) = 0$ widerspricht dies 17.4 wegen $m_{K,a} \notin K$. Im Fall $\mathrm{char}(K) = p \neq 0$ existieren nach 17.4 $\alpha_0, \ldots, \alpha_n \in K$ mit $m_{K,a} = \sum_{i=0}^n \alpha_i X^{pi}$. Wegen (4) existiert für $i = 0, \ldots, n$ ein $\beta_i \in K$ mit $\alpha_i = \beta_i^p$. Folglich ist

$$m_{K,a} = \sum_{i=0}^n \beta_i^p X^{ip} = \left(\sum_{i=0}^n \beta_i X^i\right)^p,$$

im Widerspruch zur Irreduzibilität von $m_{K,a}$.

Bemerkung: Jeder endliche Körper K ist vollkommen, denn in diesem Fall folgt aus der Injektivität des Frobenius-Homomorphismus die Surjektivität.

Satz 17.9 *Für eine Körpererweiterung $L|K$ mit $\mathrm{char}(K) = p \neq 0$ und für $a \in L$ gilt: a separabel über $K \iff K(a) = K(a^p)$.*

Beweis:

⇒: Sei a separabel über K. Da a Nullstelle ist von $X^p - a^p \in \big(K(a^p)\big)[X]$, ist $m_{K(a^p),a} \mid X^p - a^p = (X-a)^p \in L[X]$. Daher ist a die einzige Nullstelle von $m_{K(a^p),a}$. Andrerseits ist $m_{K,a}$ separabel und $m_{K(a^p),a} \mid m_{K,a}$ in $\big(K(a^p)\big)[X]$. Daher ist a einfache Nullstelle von $m_{K(a^p),a}$, d.h. $X - a = m_{K(a^p),a} \in \big(K(a^p)\big)[X]$. Folglich ist $a \in K(a^p)$ und $K(a) \subseteq K(a^p)$.

⇐: Ist $K(a) = K(a^p)$, so existieren $f, g \in K[X]$ mit $g(a^p) \neq 0$ und $a = \frac{f(a^p)}{g(a^p)}$, d.h. $ag(a^p) = f(a^p)$. Im Fall $Xg(X^p) = f(X^p)$ hätte man den Widerspruch $p \mid \deg(f(X^p)) = \deg(Xg(X^p)) = 1 + p\deg(g)$. Daher ist $Xg(X^p) - f(X^p) \in K[X] \setminus \{0\}$ mit Nullstelle a, d.h. a ist algebraisch über K. Wäre a nicht separabel über K, so wäre $m_{K,a}$ nicht separabel über K, also $m'_{K,a} = 0$, d.h. $m_{K,a} = h(X^p)$ für ein $h \in K[X]$; dabei ist h normiert und irreduzibel in $K[X]$ mit Nullstelle a^p, also $h = m_{K,a^p}$. Wegen

$$[K(a^p) : K] = \deg(m_{K,a^p}) = \deg(h) < \deg(m_{K,a}) = [K(a) : K]$$

wäre dann $K(a) \neq K(a^p)$.

Satz 17.10 *Sei $L|K$ Körpererweiterung, $a_1, \ldots, a_n \in L$ und a_i separabel über $K_{i-1} := K(a_1, \ldots, a_{i-1})$ für $i = 1, \ldots, n$. Dann ist $K(a_1, \ldots, a_n)|K$ separabel.*

Beweis: O.B.d.A. ist $\mathrm{char}(K) = p \neq 0$. Für $i = 1, \ldots, n$ ist $K_i = K_{i-1}(a_i) = K_{i-1}(a_i^p)$ nach 17.9, d.h. jedes Element in K_i ist Linearkombination p-ter Potenzen mit Koeffizienten aus K_{i-1}. Daher ist jedes Element in $K_n = K(a_1, \ldots, a_n)$ Linearkombination p-ter Potenzen mit Koeffizienten aus K. Sei $b \in K_n$ und $k := \deg(m_{K,b}) = [K(b) : K]$. Dann bilden $b_1 := 1, b_2 := b, \ldots, b_k := b^{k-1}$ eine K-Basis von $K(b)$. Diese ergänzen wir zu einer K-Basis $b_1, \ldots, b_l$ von K_n. Ist $x \in K_n$, so existieren $\xi_1, \ldots, \xi_l \in K$ mit $x = \sum_{i=1}^l \xi_i b_i$. Dann ist $x^p = \sum_{i=1}^l \xi_i^p b_i^p$ Linearkombination von $b_1^p, \ldots, b_l^p$ mit Koeffizienten aus K. Da sich jedes Element in K_n als Linearkombination p-ter Potenzen mit Koeffizienten in K schreiben läßt, spannen $b_1^p, \ldots, b_l^p$ den K-Vektorraum K_n auf. Wegen $[K_n : K] = l$ sind sie auch linear unabhängig über K. Insbesondere sind also $1, b^p, \ldots, b^{(k-1)p}$ linear unabhängig über K. Daher ist $k = [K(b) : K] \geq [K(b^p) : K] \geq k$, also $K(b) = K(b^p)$. Nach 17.9 ist b separabel über K.

Satz 17.11 *Für Körpererweiterungen $M|L$ und $L|K$ gilt: $M|K$ separabel $\iff$ $M|L$ und $L|K$ separabel.*

Beweis:

$\Rightarrow$**:** Trivial wegen $m_{L,a} \mid m_{K,a}$ in $L[X]$ für $a \in M$.

$\Leftarrow$**:** Seien $M|L$, $L|K$ separabel und $a \in M$. Wir schreiben $m_{L,a} = \sum_{i=0}^{n} \alpha_i X^i$ mit $\alpha_0, \ldots, \alpha_n \in L$. Wegen $m_{L,a} = m_{K(\alpha_0,\ldots,\alpha_n),a}$ ist a auch separabel über $K(\alpha_0, \ldots, \alpha_n)$. Die Elemente $\alpha_0, \ldots, \alpha_n \in L$ sind separabel über K. Wegen $m_{K(\alpha_0,\ldots,\alpha_{i-1}),\alpha_i} \mid m_{K,\alpha_i}$ ist also α_i auch separabel über $K(\alpha_0, \ldots, \alpha_{i-1})$ für $i = 1, \ldots, n$. Nach 17.10 ist $K(\alpha_0, \ldots, \alpha_n, a)|K$ separabel; insbesondere ist a separabel über K.

Satz 17.12 *Für jede Körpererweiterung $L|K$ ist $F := \{a \in L : a$ separabel über $K\}$ ein Teilkörper von L mit $K \subseteq F$.*

Beweis: Für $a \in K$ ist $m_{K,a} = X - a$ separabel über K, also $K \subseteq F$. Für $a, b \in F$ ist $K(a)|K$ separabel nach 17.10, und b ist separabel über $K(a)$ wegen $m_{K(a),b} \mid m_{K,b}$. Nach 17.10 ist also $K(a,b)|K$ separabel, und $a \overset{\pm}{\underset{/}{\cdot}} b \in K(a,b)$.

Satz 17.13 (Satz vom primitiven Element) *Sei $L = K(a_1, \ldots, a_n)|K$ eine algebraische Körpererweiterung, wobei $a_2, \ldots, a_n$ separabel über K sind. Dann ist $L|K$ einfach; insbesondere ist jede endliche separable Körpererweiterung einfach.*

Beweis: Nach 15.3 ist jede endliche Erweiterung eines endlichen Körpers einfach. Daher sei o.B.d.A. $|K| = \infty$ und $n \geq 2$. Sei M Zerfällungskörper von $m_{K,a_1} m_{K,a_2}$ über $K(a_1, a_2)$ und

$$m_{K,a_1} = \prod_{i=1}^{r} (X - \alpha_i), \qquad m_{K,a_2} = \prod_{j=1}^{s} (X - \beta_j)$$

mit $\alpha_1 = a_1, \alpha_2, \ldots, \alpha_r, \beta_1 = a_2, \beta_2, \ldots, \beta_s \in M$. Wegen der Separabilität von a_2 sind $\beta_1, \ldots, \beta_s$ paarweise verschieden. Wegen $|K| = \infty$ existiert ein $c \in K$ mit $c \neq \frac{\alpha_i - \alpha_1}{\beta_1 - \beta_k}$ für $i = 1, \ldots, r$, $k = 2, \ldots, s$. Setzt man $\vartheta := a_1 + c a_2 = \alpha_1 + c\beta_1$, so ist $K(\vartheta) \subseteq K(a_1, a_2)$. Wegen $m_{K,a_2}(a_2) = 0 = m_{K,a_1}(\vartheta - c a_2)$ ist $X - a_2$ gemeinsamer Teiler von m_{K,a_2} und $m_{K,a_1}(\vartheta - cX)$ in $K(a_1, a_2)[X]$. Nach Wahl von c ist $\vartheta - c\beta_k = \alpha_1 + c\beta_1 - c\beta_k \neq \alpha_i$, also $m_{K,a_1}(\vartheta - c\beta_k) \neq 0$ für $k = 2, \ldots, s$. Daher ist $X - a_2$ ggT von m_{K,a_2} und $m_{K,a_1}(\vartheta - cX)$ in $K(a_1, a_2)[X]$. Andrerseits liegen m_{K,a_2} und $m_{K,a_1}(\vartheta - cX)$ in $K(\vartheta)[X]$, also nach dem euklidischen Algorithmus auch ihr ggT $X - a_2$. Daher ist $a_2 \in K(\vartheta)$, $a_1 = \vartheta - c a_2 \in K(\vartheta)$, d.h. $K(a_1, a_2) \subseteq K(\vartheta)$ und $L = K(\vartheta, a_3, \ldots, a_n)$. Durch Induktion erhält man die Behauptung.

Kapitel 18

Galoistheorie

Satz 18.1 (Dedekind) *Seien G Gruppe, K Körper und $\sigma_1, \ldots, \sigma_n : G \to K^\times$ paarweise verschiedene Homomorphismen. Dann sind $\sigma_1, \ldots, \sigma_n$ linear unabhängig im Vektorraum* $\mathrm{Abb}(G, K)$.

Beweis: (Induktion nach n) Im Fall $n = 1$ ist $\sigma_1(1) = 1$, also $\sigma_1 \neq 0$. Sei also $n > 1$ und die Aussage für $n - 1$ bewiesen. Wegen $\sigma_1 \neq \sigma_n$ existiert ein $g \in G$ mit $\sigma_1(g) \neq \sigma_n(g)$. Sind $\alpha_1, \ldots, \alpha_n \in K$ mit $\alpha_1\sigma_1 + \ldots + \alpha_n\sigma_n = 0$, so ist

$$0 = \alpha_1\sigma_1(gh) + \ldots + \alpha_n\sigma_n(gh) = \alpha_1\sigma_1(g)\sigma_1(h) + \ldots + \alpha_n\sigma_n(g)\sigma_n(h)$$

und

$$0 = \sigma_n(g)\big(\alpha_1\sigma_1(h) + \ldots + \alpha_n\sigma_n(h)\big) = \alpha_1\sigma_n(g)\sigma_1(h) + \ldots + \alpha_n\sigma_n(g)\sigma_n(h)$$

für $h \in G$. Subtraktion ergibt:

$$\alpha_1\big(\sigma_1(g) - \sigma_n(g)\big)\sigma_1 + \ldots + \alpha_{n-1}\big(\sigma_{n-1}(g) - \sigma_n(g)\big)\sigma_{n-1} = 0.$$

Nach Induktion ist $\alpha_i\big(\sigma_i(g) - \sigma_n(g)\big) = 0$ für $i = 1, \ldots, n-1$; insbesondere ist $\alpha_1 = 0$. Dann ist $\alpha_2\sigma_2 + \ldots + \alpha_n\sigma_n = 0$ und nach Induktion $\alpha_2 = \ldots = \alpha_n = 0$.

Satz 18.2 *Sind L, M Körper und $\varphi_1, \ldots, \varphi_n : L \to M$ paarweise verschiedene Homomorphismen, so gilt:*

(i) $\varphi_1, \ldots, \varphi_n$ *sind linear unabhängig im M-Vektorraum* $\mathrm{Abb}(L, M)$.

(ii) $K := \{x \in L : \varphi_1(x) = \ldots = \varphi_n(x)\}$ *ist ein Teilkörper von L mit $[L : K] \geq n$.*

Beweis:

(i) Wende 18.1 an auf die Einschränkungen $L^\times \to M^\times$ von $\varphi_1, \ldots, \varphi_n$.

(ii) Man rechnet leicht nach, daß K Teilkörper von L ist. Wäre $r := [L : K] < n$, so wähle man eine K-Basis $a_1, \ldots, a_r$ von L. Dann hat das lineare Gleichungssystem

$$\sum_{i=1}^{n} \varphi_i(a_j)X_i = 0 \qquad (j = 1, \ldots, r)$$

eine Lösung $(x_1, \ldots, x_n) \in M^n \setminus \{0\}$. Für $\lambda_1, \ldots, \lambda_r \in K$ gilt dann:

$$\begin{aligned}\sum_{i=1}^{n} x_i\varphi_i\left(\sum_{j=1}^{r}\lambda_j a_j\right) &= \sum_{i,j} x_i\varphi_i(\lambda_j)\varphi_i(a_j) = \sum_{i,j} x_i\varphi_1(\lambda_j)\varphi_i(a_j) = \\ &= \sum_{j}\varphi_1(\lambda_j)\sum_{i} x_i\varphi_i(a_j) = 0.\end{aligned}$$

Daher ist $\sum_{i=1}^{n} x_i\varphi_i = 0$ im Widerspruch zu (i).

Bemerkung 18.3 Seien $L|K,\ M|K$ Körpererweiterungen, $\varphi : L \to M$ ein K-Homomorphismus, $a \in L$ und $f \in K[X]$. Dann ist $\varphi(f(a)) = f(\varphi(a))$.

Satz: *Ist $L|K$ eine endliche Körpererweiterung und $M|K$ eine normale Körpererweiterung mit $L \subseteq M$, so sind äquivalent:*

(1) $L|K$ separabel.

(2) Es gibt genau $[L : K]$ verschiedene K-Homomorphismen $L \xrightarrow{\varphi} M$.

Beweis:

(1)⇒(2): Sei $L|K$ separabel. Nach 17.13 existiert ein $a \in L$ mit $L = K(a)$. Nach Voraussetzung zerfällt $m_{K,a}$ in $M[X]$ in Linearfaktoren. Da a separabel über K ist, hat $m_{K,a}$ genau $\deg(m_{K,a}) = [L : K]$ verschiedene Nullstellen $a_1 = a, a_2, \ldots, a_n$ in M. Nach 16.3 existiert für $i = 1, \ldots, n$ genau ein K-Isomorphismus $\sigma_i : K(a) \to K(a_i) \subseteq M$ mit $\sigma_i(a) = a_i$. Ist $\varphi : L \to M$ ein beliebiger K-Homomorphismus, so ist $m_{K,a}(\varphi(a)) = \varphi(m_{K,a}(a)) = \varphi(0) = 0$, also $\varphi(a) = a_i$ für ein $i \in \{1, \ldots, n\}$. Wegen $L = K(a)$ ist also $\varphi = \sigma_i$. Daher sind $\sigma_1, \ldots, \sigma_n$ die einzigen K-Homomorphismen $L \to M$.

(2)⇒(1): Sei (2) erfüllt und $a \in L$. Für jeden K-Homomorphismus $\varphi : L \to M$ sei $\varphi' : K(a) \to M$ die Einschränkung von φ und $\Phi(\varphi) := \{\psi : L \to M : \psi\ K\text{-Homomorphismus und } \psi' = \varphi'\}$. Dann ist $K(a) \subseteq K_\varphi := \{x \in L : \psi(x) = \varphi(x) \text{ für } \psi \in \Phi(\varphi)\}$, also $|\Phi(\varphi)| \overset{18.2}{\leq} [L : K_\varphi] \leq [L : K(a)]$. Daher liefern die Einschränkungen der $[L : K]$ verschiedenen K-Homomorphismen $\varphi : L \to M$ mindestens $[K(a) : K]$ verschiedene K-Homomorphismen $K(a) \to M$. Ist $\sigma : K(a) \to M$ ein K-Homomorphismus, so ist $m_{K,a}(\sigma(a)) = \sigma(m_{K,a}(a)) = \sigma(0) = 0$, und σ ist durch $\sigma(a)$ eindeutig bestimmt. Daher hat $m_{K,a}$ mindestens $[K(a) : K] = \deg(m_{K,a})$ verschiedene Nullstellen. Folglich sind $m_{K,a}$ und a separabel über K.

Bemerkung 18.4 Für jeden Körper K bilden die Automorphismen von K bzgl. der Komposition eine Gruppe $\operatorname{Aut}(K)$. Für jeden Teilkörper K von L ist die Menge $\operatorname{Gal}(L|K)$ aller K-Automorphismen von L eine Untergruppe von $\operatorname{Aut}(L)$; diese nennt man die *Galoisgruppe* von L über K. Ist $L|K$ endlich, so ist $|\operatorname{Gal}(L|K)| \leq [L : K]$, denn sind $\sigma_1, \ldots, \sigma_n \in \operatorname{Gal}(L|K)$ paarweise verschieden, so ist $\sigma_i(x) = x$ für $x \in K$ und $i = 1, \ldots, n$, also $K \subseteq K' := \{x \in L : \sigma_1(x) = \ldots = \sigma_n(x)\}$ und daher $n \overset{18.2}{\leq} [L : K'] \leq [L : K]$.

Beispiel: $\operatorname{Gal}(\mathbb{C}\,|\,\mathbb{R}) = \{\mathrm{id}, \overline{}\}$; denn für jeden $\mathbb{R}$-Automorphismus φ von $\mathbb{C}$ ist $\varphi(i)^2 = \varphi(i^2) = \varphi(-1) = -1$, also $\varphi(i) \in \{i, -i\}$. Wegen $\mathbb{C} = \mathbb{R} + \mathbb{R}\,i$ folgt die Behauptung.

Bemerkung 18.5 Für jeden Körper K und jede Untergruppe G von $\operatorname{Aut}(K)$ ist $\operatorname{Fix}(G) := \{x \in K : \varphi(x) = x \text{ für } \varphi \in G\}$ ein Teilkörper von K, der *Fixkörper* von G. Offenbar ist $G \subseteq \operatorname{Gal}(K|\operatorname{Fix}(G))$.

Beispiel: Der Fixkörper der Untergruppe $\{\mathrm{id}, \overline{}\}$ von $\operatorname{Aut}(\mathbb{C})$ ist $\mathbb{R}$.

Satz: *Für jeden Körper K und jede endliche Untergruppe G von* $\operatorname{Aut}(K)$ *ist* $[K : \operatorname{Fix}(G)] = |G|$ *und* $G = \operatorname{Gal}(K|\operatorname{Fix}(G))$.

Beweis: Wir schreiben $G = \{\varphi_1 = \mathrm{id}_K, \varphi_2, \ldots, \varphi_n\}$, $n = |G|$. Dann ist $\mathrm{Fix}(G) = \{x \in K : x = \varphi_1(x) = \ldots = \varphi_n(x)\}$, also $[K : \mathrm{Fix}(G)] \geq n$ nach 18.2. Im Fall $[K : \mathrm{Fix}(G)] > n$ wähle man $a_1, \ldots, a_{n+1} \in K$, die linear unabhängig über $\mathrm{Fix}(G)$ sind. Das lineare Gleichungssystem

$$\sum_{j=1}^{n+1} \varphi_i^{-1}(a_j) X_j = 0 \qquad (i = 1, \ldots, n)$$

besitzt dann eine Lösung $(y_1, \ldots, y_{n+1}) \in K^{n+1} \setminus \{0\}$. Sei $l \in \{1, \ldots, n+1\}$ mit $y_l \neq 0$. Da $\varphi_1, \ldots, \varphi_n$ linear unabhängig über K sind, existiert ein $z \in K$ mit $\varphi_1(z) + \ldots + \varphi_n(z) \neq 0$. Dann ist auch $zy_l^{-1}(y_1, \ldots, y_{n+1}) =: (x_1, \ldots, x_{n+1})$ nichttriviale Lösung des Gleichungssystems, und $x_l = z$. Für $i = 1, \ldots, n$ ist

$$0 = \varphi_i(0) = \sum_{j=1}^{n+1} a_j \varphi_i(x_j),$$

also auch

$$0 = \sum_{i=1}^{n} \sum_{j=1}^{n+1} a_j \varphi_i(x_j) = \sum_{j=1}^{n+1} \left(\sum_{i=1}^{n} \varphi_i(x_j) \right) a_j.$$

Dabei ist

$$\psi \left(\sum_{i=1}^{n} \varphi_i(x_j) \right) = \sum_{i=1}^{n} \psi(\varphi_i(x_j)) = \sum_{i=1}^{n} \varphi_i(x_j) \qquad \text{für } \psi \in G$$

wegen $G = \{\psi\varphi_1, \ldots, \psi\varphi_n\}$. Daher ist $\sum_{i=1}^{n} \varphi_i(x_j) \in \mathrm{Fix}(G)$ für $j = 1, \ldots, n+1$, also $\sum_{i=1}^{n} \varphi_i(x_j) = 0$ für $j = 1, \ldots, n+1$ wegen der linearen Unabhängigkeit von $a_1, \ldots, a_{n+1}$. Dies ergibt einen Widerspruch zu $\sum_{i=1}^{n} \varphi_i(x_l) \neq 0$.
Also ist $[K : \mathrm{Fix}(G)] = |G|$. Ist $G \neq \mathrm{Gal}(K | \mathrm{Fix}(G))$, so existiert ein $\varphi \in \mathrm{Gal}(K | \mathrm{Fix}(G)) \setminus G$. Dann ist aber $\mathrm{Fix}(G) = \{x \in K : x = \varphi_1(x) = \ldots = \varphi_n(x) = \varphi(x)\}$, also $[K : \mathrm{Fix}(G)] \geq n+1$ nach 18.2. Widerspruch.

Satz 18.6 *Für eine Körpererweiterung $L|K$ sind äquivalent:*

(1) Es existiert eine Untergruppe G von $\mathrm{Aut}(L)$ *mit* $K = \mathrm{Fix}(G)$.

(2) $K = \mathrm{Fix}(\mathrm{Gal}(L|K))$.

Definition: *Gegebenenfalls nennt man $L|K$* Galoiserweiterung.

Beweis:

(1)⇒(2): Sei $G \leq \mathrm{Aut}(L)$ mit $K = \mathrm{Fix}(G)$, also $G \subseteq \mathrm{Gal}(L|K)$. Daher ist $\mathrm{Fix}(\mathrm{Gal}(L|K)) \subseteq \mathrm{Fix}(G) = K$. Offenbar ist $K \subseteq \mathrm{Fix}(\mathrm{Gal}(L|K))$.

(2)⇒(1): Trivial.

Beispiel: $\mathbb{C} \,|\, \mathbb{R}$ ist Galoiserweiterung.

Satz 18.7 *Für eine endliche Körpererweiterung $L|K$ sind äquivalent:*

(1) $L|K$ ist Galoiserweiterung.

(2) $L|K$ ist Zerfällungskörper eines über K separablen Polynoms $f \in K[X]$.

(3) $L|K$ ist normal und separabel.

(4) $[L : K] = |\,\mathrm{Gal}(L|K)|$.

Beweis:

(1)⇒(2): Sei $L|K$ Galoiserweiterung, $a \in L$ und $\{\sigma(a) : \sigma \in \mathrm{Gal}(L|K)\} = \{a_1, \ldots, a_n\}$ mit paarweise verschiedenen $a_1, \ldots, a_n \in L$. (Nach 18.4 ist $|\,\mathrm{Gal}(L|K)| < \infty$.) Wir setzen $f_a := \prod_{i=1}^n (X - a_i)$ und schreiben $f_a = \sum_{j=0}^n b_j X^j$ mit $b_0, \ldots, b_n \in L$. Für $\sigma \in \mathrm{Gal}(L|K)$ ist $\tilde{\sigma} : L[X] \to L[X]$, $\sum c_i X^i \mapsto \sum \sigma(c_i) X^i$ ein Automorphismus von $L[X]$. Da $a_1, \ldots, a_n$ durch σ nur permutiert werden, ist

$$\begin{aligned}\sum_{j=0}^n \sigma(b_j) X^j \;&=\; \tilde{\sigma}(f_a) \;=\; \prod_{i=1}^n (X - \sigma(a_i)) \;=\; \prod_{i=1}^n (X - a_i) \;=\\ &=\; f_a \;=\; \sum_{j=0}^n b_j X^j,\end{aligned}$$

also $\sigma(b_j) = b_j$ für $j = 0, \ldots, n$. Daher ist $b_0, \ldots, b_n \in \mathrm{Fix}(\mathrm{Gal}(L|K)) = K$, d.h. $f_a \in K[X]$ mit $f_a(a) = 0$. Da $a_1, \ldots, a_n$ paarweise verschieden sind, sind f_a und a separabel über K. Folglich ist $L|K$ separabel. Nach 17.13 existiert ein $a \in L$ mit $L = K(a)$. Für dieses a ist L Zerfällungskörper des über K separablen Polynoms $f_a \in K[X]$.

(2)⇒(3): Ist $L|K$ Zerfällungskörper eines über K separablen Polynoms $f \in K[X]$, so ist $L|K$ normal, und die Nullstellen von f sind separabel über K. Da L durch Adjunktion dieser Nullstellen zu K entsteht, ist $L|K$ separabel nach 17.10.

(3)⇒(4): Sei $L|K$ normal und separabel. Nach 18.3 existieren dann genau $[L:K]$ K-Homomorphismen $L \to L$. Wegen $[L:K] < \infty$ sind diese bijektiv, d.h. in $\mathrm{Gal}(L|K)$. Folglich ist $|\,\mathrm{Gal}(L|K)| = [L:K]$.

(4)⇒(1): Sei $|\,\mathrm{Gal}(L|K)| = [L:K]$. Nach 18.5 ist $|\,\mathrm{Gal}(L|K)| = [L : \mathrm{Fix}(\mathrm{Gal}(L|K))]$. Offenbar ist $K \subseteq \mathrm{Fix}(\mathrm{Gal}(L|K)) \subseteq L$. Aus dem Gradsatz folgt $K = \mathrm{Fix}(\mathrm{Gal}(L|K))$.

Satz 18.8 *Sei $L|K$ endliche Galoiserweiterung und M ein Teilkörper von L mit $K \subseteq M$. Dann ist $L|M$ auch Galoiserweiterung.*

Beweis: Nach 18.7 ist L Zerfällungskörper eines $f \in K[X]$ über K. Daher ist L auch Zerfällungskörper von f über M. Also ist $L|M$ normal nach 16.5. Andrerseits ist $L|M$ nach 17.11 auch separabel. Nach 18.7 ist also $L|M$ Galoiserweiterung.

Satz 18.9 (Hauptsatz der Galoistheorie) *Für jede endliche Galoiserweiterung $L|K$ sind die Abbildungen $F \mapsto \mathrm{Gal}(L|F)$ und $H \mapsto \mathrm{Fix}(H)$ zueinander inverse Bijektionen zwischen der Menge der Teilkörper F von L mit $K \subseteq F \subseteq L$ und der Menge der Untergruppen H von $\mathrm{Gal}(L|K)$. Dabei ist $[L:F] = |\,\mathrm{Gal}(L|F)|$ und $[F:K] = |\,\mathrm{Gal}(L|K) : \mathrm{Gal}(L|F)|$.*

$$\begin{array}{rcccl}
 & L & \longleftrightarrow & \mathrm{Gal}(L|L) = 1 & \\
{[L:F]} & \Big| & & & \Big\}\; |H| \\
 & F & \longleftrightarrow & \mathrm{Gal}(L|F) = H & \\
{[F:K]} & \Big| & & & \Big\}\; |G:H| \\
 & K & \longleftrightarrow & \mathrm{Gal}(L|K) = G &
\end{array}$$

Beweis: Für jeden Teilkörper F von L mit $K \subseteq F$ ist offenbar $\mathrm{Gal}(L|F) \leq \mathrm{Gal}(L|K)$. Da $L|F$ nach 18.8 eine Galoiserweiterung ist, hat man $F = \mathrm{Fix}(\mathrm{Gal}(L|F))$ und $|\,\mathrm{Gal}(L|F)| = [L:F]$ nach 18.7, und aus dem Gradsatz bzw. dem Satz von Lagrange erhält man

$$\begin{aligned}[F:K] \;&=\; [L:K] \,\big/\, [L:F] \;=\; |\,\mathrm{Gal}(L|K)| \,\big/\, |\,\mathrm{Gal}(L|F)| \;=\\ &=\; |\,\mathrm{Gal}(L|K) : \mathrm{Gal}(L|F)|.\end{aligned}$$

Für jede Untergruppe H von $\mathrm{Gal}(L|K)$ ist $\mathrm{Fix}(H)$ Teilkörper von L mit $K = \mathrm{Fix}(\mathrm{Gal}(L|K)) \subseteq \mathrm{Fix}(H) \subseteq L$. Wegen $|H| \leq |\,\mathrm{Gal}(L|K)| = [L:K] < \infty$ ist $H = \mathrm{Gal}(L|\,\mathrm{Fix}(H))$ nach 18.5, und die Behauptung ist bewiesen.

Bemerkung: In der obigen Situation ist $\sigma(F)$ für $\sigma \in \mathrm{Gal}(L|K)$ ein Teilkörper von L mit $K \subseteq \sigma(F)$ und $\mathrm{Gal}(L|\sigma(F)) = \sigma\,\mathrm{Gal}(L|F)\sigma^{-1}$; denn für $\tau \in \mathrm{Gal}(L|K)$ gilt:

$$\begin{aligned}\tau \in \mathrm{Gal}(L|\sigma(F)) \quad &\Leftrightarrow \quad \tau(\sigma(x)) = \sigma(x) \qquad \forall x \in F\\ &\Leftrightarrow \quad \sigma^{-1}\tau\sigma(x) = x \qquad \forall x \in F\\ &\Leftrightarrow \quad \sigma^{-1}\tau\sigma \in \mathrm{Gal}(L|F)\\ &\Leftrightarrow \quad \tau \in \sigma\,\mathrm{Gal}(L|F)\sigma^{-1}.\end{aligned}$$

Satz 18.10 *Für jede endliche Galoiserweiterung $L|K$ und jeden Teilkörper F von L mit $K \subseteq F$ sind äquivalent:*

(1) $F|K$ *Galoiserweiterung.*

(2) $F|K$ *normal.*

(3) $\sigma(F) \subseteq F \quad \forall \sigma \in \mathrm{Gal}(L|K)$.

(4) $\mathrm{Gal}(L|F) \trianglelefteq \mathrm{Gal}(L|K)$.

In diesem Fall liefert die Einschränkung einen Epimorphismus $\mathrm{Gal}(L|K) \to \mathrm{Gal}(F|K)$ *mit Kern* $\mathrm{Gal}(L|F)$*; insbesondere ist*

$$\mathrm{Gal}(F|K) \cong \mathrm{Gal}(L|K)/\,\mathrm{Gal}(L|F).$$

Beweis:

(1)⇒(2): 18.7.

(2)⇒(3): 16.5.

(3)⇒(4): Sei (3) erfüllt und $\sigma \in \mathrm{Gal}(L|K)$. Dann ist $\sigma^{-1} \in \mathrm{Gal}(L|K)$, also $\sigma^{-1}(F) \subseteq F$. Daher ist $F = \sigma(\sigma^{-1}(F)) \subseteq \sigma(F) \subseteq F$, d.h. $F = \sigma(F)$. Daher liegt die Einschränkung $\sigma' : F \to F$ von σ in $\mathrm{Gal}(F|K)$. Die Abbildung $\mathrm{Gal}(L|K) \to \mathrm{Gal}(F|K),\ \sigma \mapsto \sigma'$ ist also ein Homomorphismus mit Kern $\mathrm{Gal}(L|F)$. Daher ist $\mathrm{Gal}(L|F) \trianglelefteq \mathrm{Gal}(L|K)$ mit $|\,\mathrm{Gal}(F|K)| \geq |\,\mathrm{Gal}(L|K)/\,\mathrm{Gal}(L|F)| = [F:K] \geq |\,\mathrm{Gal}(F|K)|$ nach 18.4. Daher ist die Abbildung $\sigma \mapsto \sigma'$ surjektiv, und $\mathrm{Gal}(F|K) \cong \mathrm{Gal}(L|K)/\,\mathrm{Gal}(L|F)$ nach dem Homomorphiesatz.

(4)⇒(1): Ist (4) erfüllt und $\sigma \in \mathrm{Gal}(L|K)$, so ist $\sigma(F)$ nach Bemerkung 18.9 ein Teilkörper von L mit $K \subseteq \sigma(F)$ und $\mathrm{Gal}(L|\sigma(F)) = \sigma\,\mathrm{Gal}(L|F)\sigma^{-1} = \mathrm{Gal}(L|F)$. Nach 18.9 ist also $F = \sigma(F)$. Der Beweis von (3)⇒(4) zeigt: $|\,\mathrm{Gal}(F|K)| = [F:K]$. Nach 18.7 ist also $F|K$ Galoiserweiterung.

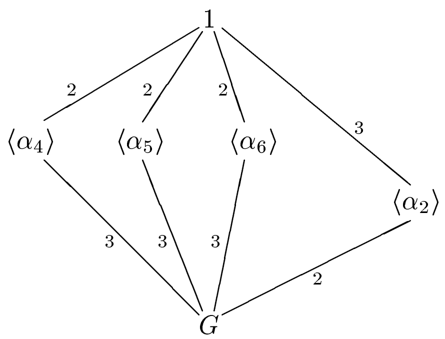
Bemerkung: Es gibt auch eine Galoistheorie für unendliche Erweiterungen.

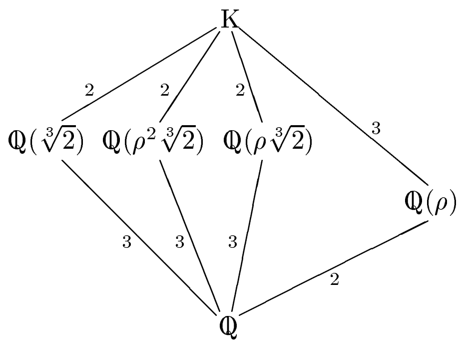
Beispiel: Das Polynom $X^3 - 2 \in \mathbb{Q}[X]$ ist wegen $\mathrm{char}(\mathbb{Q}) = 0$ separabel über $\mathbb{Q}$. Seine Nullstellen in $\mathbb{C}$ sind $\sqrt[3]{2} \in \mathbb{R},\ \rho\sqrt[3]{2}, \rho^2\sqrt[3]{2} \in \mathbb{C}\setminus\mathbb{R},\ \rho = \frac{1}{2}(-1+\sqrt{-3})$, also $\rho^3 = 1 \neq \rho$, d.h. $\rho^2+\rho+1 = 0$. Der Zerfällungskörper $K = \mathbb{Q}(\sqrt[3]{2}, \rho\sqrt[3]{2}, \rho^2\sqrt[3]{2}) = \mathbb{Q}(\sqrt[3]{2}, \rho)$ von X^3-2 über $\mathbb{Q}$ ist also nach 18.7 eine Galoiserweiterung von $\mathbb{Q}$. Da X^3-2 in $\mathbb{Q}[X]$ irreduzibel ist, hat man $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$. Wegen $\rho \notin \mathbb{Q}(\sqrt[3]{2})$ ist $[K : \mathbb{Q}(\sqrt[3]{2})] = 2$, also $[K:\mathbb{Q}] = 6$. Nach 18.7 ist $|\,\mathrm{Gal}(K|\,\mathbb{Q})| = 6$.
Jedes Element $\alpha \in G := \mathrm{Gal}(K|\,\mathbb{Q})$ ist durch $\alpha(\sqrt[3]{2})$ und $\alpha(\rho)$ eindeutig bestimmt, und $\alpha(\sqrt[3]{2}), \alpha(\rho)$ sind Nullstellen von X^3-2 bzw. X^2+X+1. Die Elemente von G sind also:

$$\begin{array}{lcll}\alpha_1 = \mathrm{id} & : & \sqrt[3]{2} \mapsto \sqrt[3]{2}, & \rho \mapsto \rho\\ \alpha_2 & : & \sqrt[3]{2} \mapsto \rho\sqrt[3]{2}, & \rho \mapsto \rho\\ \alpha_3 = \alpha_2^2 & : & \sqrt[3]{2} \mapsto \rho^2\sqrt[3]{2}, & \rho \mapsto \rho\\ \alpha_4 & : & \sqrt[3]{2} \mapsto \sqrt[3]{2}, & \rho \mapsto \rho^2\\ \alpha_5 & : & \sqrt[3]{2} \mapsto \rho\sqrt[3]{2}, & \rho \mapsto \rho^2\\ \alpha_6 & : & \sqrt[3]{2} \mapsto \rho^2\sqrt[3]{2}, & \rho \mapsto \rho^2\end{array}$$

Wegen $|G| = 6$ ist jede echte Untergruppe von G zyklisch; daher sind 1, $\langle\alpha_2\rangle = \{1, \alpha_2, \alpha_2^2 = \alpha_3\} = \langle\alpha_3\rangle$, $\langle\alpha_4\rangle = \{1, \alpha_4\}$, $\langle\alpha_5\rangle = \{1, \alpha_5\}$, $\langle\alpha_6\rangle = \{1, \alpha_6\}$, G die einzigen Untergrupppen von G. Da G genau 3 Untergruppen der Ordnung 2 enthält, ist G nicht zyklisch. Da es bis auf Isomorphie genau 2 Gruppen der Ordnung 6 gibt, ist $G \cong \mathrm{Sym}(3)$. Offenbar gilt:

$$\begin{aligned}
&\mathrm{Fix}(1) = K\\
&\mathrm{Fix}(\langle\alpha_2\rangle) \supseteq \mathbb{Q}(\rho)\\
&\mathrm{Fix}(\langle\alpha_4\rangle) \supseteq \mathbb{Q}(\sqrt[3]{2})\\
&\mathrm{Fix}(\langle\alpha_5\rangle) \supseteq \mathbb{Q}(\rho^2\sqrt[3]{2})\\
&\mathrm{Fix}(\langle\alpha_6\rangle) \supseteq \mathbb{Q}(\rho\sqrt[3]{2})
\end{aligned}$$





Durch Vergleich der Grade erhält man überall „=“. Nach Sylow sind die Untergruppen der Ordnung 2 konjugiert in G. Daher ist keine von ihnen normal in G. Nach 18.10 sind $\mathbb{Q}(\sqrt[3]{2})$, $\mathbb{Q}(\rho\sqrt[3]{2})$, $\mathbb{Q}(\rho^2\sqrt[3]{2})$ keine Galoiserweiterungen von $\mathbb{Q}$. Wegen $|G : \langle\alpha_2\rangle| = 2$ ist $\langle\alpha_2\rangle \trianglelefteq G$, also $\mathbb{Q}(\rho)|\mathbb{Q}$ Galoiserweiterung. Ferner ist $\mathrm{Gal}(\mathbb{Q}(\rho)|\mathbb{Q}) \cong G/\langle\alpha_2\rangle$ eine Gruppe der Ordnung 2.

Kapitel 19

Anwendungen der Galoistheorie

Satz 19.1 *Für einen Körper K sind äquivalent:*

(1) Jedes Polynom in $K[X] \setminus K$ hat eine Nullstelle in K.

(2) Jedes Polynom in $K[X] \setminus K$ zerfällt in $K[X]$ in Linearfaktoren.

(3) Jedes irreduzible Polynom in $K[X]$ hat Grad 1.

(4) Ist $L|K$ eine algebraische Körpererweiterung, so ist $L = K$.

Beweis:

(1)⇒(2): Sei (1) erfüllt und $f \in K[X] \setminus K$. Dann existiert ein $a \in K$ mit $f(a) = 0$. Folglich ist $f = (X - a)g$ für ein $g \in K[X]$. Ist g konstant, so sind wir fertig. Ist $g \notin K$, so wenden wir (1) auf g an und fahren so fort, bis wir f in Linearfaktoren zerlegt haben.

(2)⇒(3): Trivial.

(3)⇒(4): Sei (3) erfüllt, $L|K$ algebraische Körpererweiterung und $a \in L$. Dann ist $X - a = m_{K,a} \in K[X]$, also $a \in K$.

(4)⇒(1): Sei (4) erfüllt, $f \in K[X] \setminus K$ und L Zerfällungskörper von f über K. Dann ist $L|K$ algebraisch, also $L = K$, d.h. f zerfällt in $K[X]$ in Linearfaktoren.

Definition: *Sind (1)–(4) erfüllt, so nennt man K* algebraisch abgeschlossen.

Satz 19.2 (Fundamentalsatz der Algebra, Gauß, 1777–1855)
$\mathbb{C}$ ist algebraisch abgeschlossen.

Beweis: Sei $f \in \mathbb{C}[X] \setminus \mathbb{C}$ und Z Zerfällungskörper von f über $\mathbb{C}$. Wegen $[Z : \mathbb{R}] < \infty$ existiert nach 16.6 eine endliche normale Körpererweiterung $K|\,\mathbb{R}$ mit $Z \subseteq K$. Wegen $\operatorname{char}(\mathbb{R}) = 0$ ist $K|\,\mathbb{R}$ separabel, also eine Galoiserweiterung. Wir wählen eine 2-Sylowgruppe P von $G := \operatorname{Gal}(K|\,\mathbb{R})$ und setzen $L := \operatorname{Fix}(P)$.

$$\begin{array}{ccccl} K & \qquad\qquad & 1 & & \\ \Big| & & \Big| & \Big\} & \text{2er-Potenz} \\ L & & P & & \\ \Big| & & \Big| & \Big\} & \text{ungerade} \\ \mathbb{R} & & G & & \end{array}$$

Da $L|\,\mathbb{R}$ separabel ist, existiert ein $a \in L$ mit $L = \mathbb{R}(a)$. Dann ist $\deg(m_{\mathbb{R},a}) = [L : \mathbb{R}] = |G : P|$ ungerade. Nach dem Zwischensatz der Analysis besitzt $m_{\mathbb{R},a}$ eine reelle Nullstelle, d.h. $m_{\mathbb{R},a}$ ist linear. Daher ist $G = P$ eine Gruppe von 2-Potenzordnung. Die Untergruppe $U := \mathrm{Gal}(K|\mathbb{C})$ hat also die Ordnung 2^r für ein $r \in \mathbb{N}_0$. Wäre $r > 0$, so könnte man nach Sylow eine Untergruppe V von U mit $|V| = 2^{r-1}$ wählen. Für den Fixkörper F von V würde dann gelten: $[F : \mathbb{C}] = |U : V| = 2$ im Widerspruch zu Aufgabe 6 von Blatt 12.

$$\begin{array}{ccc}
K & \qquad\qquad & 1 \\
| & & | \\
F & & V \\
| & & |\,{\scriptstyle 2} \\
\mathbb{C} & & U \\
| & & | \\
\mathbb{R} & & G
\end{array}$$

Daher ist $r = 0$, d.h. $\mathrm{Gal}(K|\mathbb{C}) = 1$. Folglich ist $K = \mathbb{C}$. Also zerfällt f auch in $\mathbb{C}[X]$ in Linearfaktoren.

Bemerkung 19.3 (Zusammenfassung der Theorie endlicher Körper)
Für jeden endlichen Körper K ist $\mathrm{char}(K)$ eine Primzahl p. Der Primkörper P von K ist zu $\mathbf{Z}/p\mathbf{Z}$ isomorph, $|K| = p^{[K:P]}$, und $K^\times$ ist zyklisch. Umgekehrt existiert zu jeder Primzahl p und jeder natürlichen Zahl n bis auf Isomorphie genau ein Körper K mit $|K| = p^n$. Man nennt K das *Galoisfeld* mit p^n Elementen und schreibt $K = \mathbb{F}_{p^n} = \mathrm{GF}(p^n)$. Ist L ein Teilkörper von K, so ist $|L| = p^d$ für einen Teiler d von n. Umgekehrt existiert zu jedem Teiler d von n genau ein Teilkörper L von K mit $|L| = p^d$, nämlich $L = \{x \in K : x^{p^d} = x\}$. Für $m \in \mathbb{N}$ existiert bis auf K-Isomorphie genau ein Erweiterungskörper M von K mit $[M : K] = m$. M ist Zerfällungskörper von $X^{p^{nm}} - X$ über K. $M|K$ ist Galoiserweiterung mit zyklischer Galoisgruppe. $\mathrm{Gal}(M|K)$ wird erzeugt durch den *Frobenius-Automorphismus* von $M|K$: $\varphi : M \to M,\ x \mapsto x^{p^n}$.

Beweis: Übungen.

Definition 19.4 *Sei K ein Körper und $n \in \mathbb{N}$.*

(i) *Ein Element $\zeta \in K$ mit $\zeta^n = 1$ nennt man n-te* Einheitswurzel. *Hat ζ die Ordnung n, so nennt man ζ eine* primitive *n-te Einheitswurzel.*

(ii) *Den Zerfällungskörper K_n von $X^n - 1$ über K nennt man den n-ten* Kreisteilungskörper *über K. Sind $\zeta_1, \ldots, \zeta_k$ die primitiven n-ten Einheitswurzeln in K_n, so nennt man $\Phi_n := \prod_{i=1}^k (X - \zeta_i)$ das n-te* Kreisteilungspolynom *über K.*

Bemerkung:

(i) Da $X^n - 1$ höchstens n Nullstellen in K hat, gibt es in K höchstens n verschiedene n-te Einheitswurzeln. Diese bilden bzgl. der Multiplikation eine Untergruppe von $K^\times$; diese ist nach 14.10 zyklisch.

(ii) Enthält K eine primitive n-te Einheitswurzel ζ, so ist $|\langle\zeta\rangle| = n$, d.h. $\langle\zeta\rangle$ ist die Gruppe *aller* n-ten Einheitswurzeln in K. Für $m, k \in \mathbb{N}$ gilt:

$$(\zeta^m)^k = 1 \ \Leftrightarrow\ n \,\big|\, mk \ \Leftrightarrow\ \frac{n}{\mathrm{ggT}(m,n)} \,\Big|\, k.$$

Daher hat ζ^m die Ordnung $\frac{n}{\mathrm{ggT}(m,n)}$. Insbesondere ist ζ^m genau dann eine primitive n-te Einheitswurzel, wenn $\mathrm{ggT}(m,n) = 1$ ist. Also ist die Anzahl der primitiven n-ten Einheitswurzeln gleich der Anzahl der zu n teilerfremden ganzen Zahlen $m \in \{1, \ldots, n\}$, d.h. gleich $\varphi(n)$, wobei φ die Eulersche φ-Funktion bezeichnet. Insbesondere ist $\deg(\Phi_n) = \varphi(n)$.

(iii) Ist $\mathrm{char}(K) = p \neq 0$, so ist jede pn-te Einheitswurzel in K auch eine n-te Einheitswurzel; denn aus $0 = \zeta^{pn} - 1 = (\zeta^n - 1)^p$ folgt $\zeta^n = 1$. Daher gibt es keine primitiven pn-ten Einheitswurzeln in K.

(iv) Ist $\mathrm{char}(K) \nmid n$ (z.B. $\mathrm{char}(K) = 0$), so ist $(X^n - 1)' = nX^{n-1}$ zu $X^n - 1$ teilerfremd. Daher sind alle Nullstellen von $X^n - 1$ in K_n einfach, d.h. in K_n existieren genau n verschiedene n-te Einheitswurzeln. Nach (i) bilden diese eine zyklische Gruppe $\langle\zeta\rangle$ der Ordnung n. Dabei ist ζ eine primitive n-te Einheitswurzel. Ferner ist $K_n = K(\zeta)$ wegen $X^n - 1 = \prod_{i=1}^n (X - \zeta^i)$.

(v) Für jeden Teiler d von n ist jede primitive d-te Einheitswurzel auch eine n-te Einheitswurzel. Umgekehrt ist für jede n-te Einheitswurzel ζ die Ordnung d von ζ ein Teiler von n, und ζ ist eine primitive d-te Einheitswurzel. Ist ζ eine primitive n-te Einheitswurzel, so ist $\zeta^{n/d}$ eine primitive d-te Einheitswurzel. Ist $\mathrm{char}(K) \nmid n$, so kann man in

$$X^n - 1 = \prod_{\zeta \ n\text{-te Einheitswurzel in } K_n} (X - \zeta)$$

die Faktoren nach der Ordnung von ζ sortieren. Man erhält so:

$$X^n - 1 = \prod_{d|n} \Phi_d;$$

insbesondere ist $n = \deg(X^n - 1) = \sum_{d|n} \varphi(d)$. Ferner ist

$$\Phi_n = \frac{X^n - 1}{\prod_{\substack{d|n \\ d\neq n}} \Phi_d};$$

dies liefert wegen $\Phi_1 = X - 1$ die Möglichkeit zur induktiven Berechnung von Φ_n. Da Φ_n normiert ist, treten bei der Division keine Nenner auf. Die Koeffizienten von Φ_n sind also von der Form $m1_K$ mit $m \in \mathbf{Z}$; insbesondere ist $\Phi_n \in K[X]$, sogar $\Phi_n \in \mathbf{Z}[X]$ im Fall $K = \mathbb{Q}$.

Beispiel:

(a) In $\mathbb{R}$ sind ± 1 die einzigen Einheitswurzeln.

(b) In $\mathbb{C}$ ist $\zeta = e^{\frac{2\pi i}{n}} = \cos \frac{2\pi}{n} + i \sin \frac{2\pi}{n}$ eine primitive n-te Einheitswurzel.

(c) In jedem endlichen Körper K ist jedes Element $a \neq 0$ nach Lagrange eine $(|K| - 1)$-te Einheitswurzel.

(d) Für jede Primzahl p ist $\Phi_p = \frac{X^p - 1}{X - 1} = X^{p-1} + X^{p-2} + \ldots + X + 1$.

(e) Nach Aufgabe 3 von Blatt 9 ist $\Phi_4 = X^2 + 1$, $\Phi_6 = X^2 - X + 1$.

Satz: *Für $n \in \mathbb{N}$ und jeden Körper K mit $\mathrm{char}(K) \nmid n$ ist der n-te Kreisteilungskörper K_n eine Galoiserweiterung von K, und $G := \mathrm{Gal}(K_n|K)$ ist isomorph zu einer Untergruppe von $(\mathbf{Z}/n\mathbf{Z})^\times$; insbesondere ist G abelsch und $|G| \mid \varphi(n)$.*

Beweis: Nach der Bemerkung existiert in K_n eine primitive n-te Einheitswurzel ζ, und es ist $K_n = K(\zeta)$. Ferner ist $X^n - 1$ separabel über K; nach 18.7 ist also $K_n|K$ Galoiserweiterung. Für $\sigma \in G$ ist auch $\sigma(\zeta)$ eine primitive n-te Einheitswurzel, also von der Form ζ^m für ein $m \in \mathbf{Z}$ mit $\mathrm{ggT}(m,n) = 1$. Für $m' \in \mathbf{Z}$ gilt:

$$\zeta^m = \zeta^{m'} \;\Leftrightarrow\; \zeta^{m-m'} = 1 \;\Leftrightarrow\; n \;\big|\; m - m' \;\Leftrightarrow\; m + n\mathbf{Z} = m' + n\mathbf{Z}.$$

Daher existiert zu $\sigma \in G$ genau ein Element $\Phi(\sigma) \in (\mathbf{Z}/n\mathbf{Z})^\times$ mit $\sigma(\zeta) = \zeta^m$ für $m \in \Phi(\sigma)$. Ist auch $\rho \in G$ und $\rho(\zeta) = \zeta^l$ mit $l \in \mathbf{Z}$, so ist $(\rho \circ \sigma)(\zeta) = \rho(\zeta^m) = \rho(\zeta)^m = \zeta^{lm}$. Daher ist die Abbildung $\Phi : G \to (\mathbf{Z}/n\mathbf{Z})^\times$ ein Homomorphismus. Wegen $K_n = K(\zeta)$ ist jedes $\sigma \in G$ durch $\sigma(\zeta)$ und damit durch $m + n\mathbf{Z} = \Phi(\sigma)$ eindeutig bestimmt. Folglich ist Φ injektiv.

Satz 19.5 *Für $n \in \mathbb{N}$ ist das n-te Kreisteilungspolynom Φ_n irreduzibel in $\mathbb{Q}[X]$, der n-te Kreisteilungskörper $\mathbb{Q}_n = \mathbb{Q}\left(e^{\frac{2\pi i}{n}}\right)$ ist eine Galoiserweiterung des Grades $\varphi(n)$ von $\mathbb{Q}$, und* $\mathrm{Gal}(\mathbb{Q}_n\,|\,\mathbb{Q}) \cong (\mathbf{Z}/n\mathbf{Z})^\times$.

Beweis: Sei f ein irreduzibler Faktor von Φ_n in $\mathbf{Z}[X]$, o.B.d.A. sei f normiert. Wegen $f \;\big|\; \Phi_n \;\big|\; X^n - 1$ existiert $g \in \mathbf{Z}[X]$ mit $X^n - 1 = fg$. Mit $X^n - 1$ zerfällt auch f in $\mathbb{Q}_n[X]$ in Linearfaktoren. Ist ζ eine Nullstelle von f in $\mathbb{Q}_n$, so ist $f = m_{\mathbb{Q},\zeta}$, und wegen $\Phi_n(\zeta) = 0$ ist ζ eine primitive n-te Einheitswurzel.
Annahme: Es existiert eine Primzahl p mit $p \nmid n$ und $f(\zeta^p) \neq 0$. Wegen $f(\zeta^p)g(\zeta^p) = \zeta^{pn} - 1 = 1 - 1 = 0$ ist also $g(\zeta^p) = 0$. Wegen $f = m_{\mathbb{Q},\zeta}$ existiert also ein $h \in \mathbb{Q}[X]$ mit $g(X^p) = fh$. Da f normiert ist, treten bei der Division von $g(X^p)$ durch f keine Nenner auf. Folglich ist $h \in \mathbf{Z}[X]$. Wir setzen den natürlichen Epimorphismus $\nu : \mathbf{Z} \to \mathbf{Z}/p\mathbf{Z}$ fort zu dem Epimorphismus $\varphi : \mathbf{Z}[X] \to (\mathbf{Z}/p\mathbf{Z})[X], \sum \alpha_i X^i \mapsto \sum \nu(\alpha_i)X^i$. Da f normiert ist, ist $\varphi(f) \notin \mathbf{Z}/p\mathbf{Z}$, d.h. $\varphi(f)$ hat mindestens einen irreduziblen Faktor q in $(\mathbf{Z}/p\mathbf{Z})[X]$. Für $\alpha \in \mathbf{Z}/p\mathbf{Z}$ ist $\alpha^p = \alpha$. Schreibt man $g = \sum_{i=0}^k \alpha_i X^i$ mit $\alpha_0, \ldots, \alpha_k \in \mathbf{Z}$, so ist also

$$\begin{aligned} \varphi(f)\varphi(h) \;&=\; \varphi(g(X^p)) \;=\; \sum_{i=0}^k \nu(\alpha_i)X^{pi} \;=\; \sum_{i=0}^k \nu(\alpha_i)^p X^{ip} = \\ &=\; \left(\sum_{i=0}^k \nu(\alpha_i)X^i\right)^p \;=\; \varphi(g)^p. \end{aligned}$$

Daher ist $q \;\big|\; \varphi(g)$ und $q^2 \;\big|\; \varphi(f)\varphi(g) = \varphi(fg) = \varphi(X^n - 1) = X^n - 1$. Daher hat $X^n - 1$ mehrfache Nullstellen in seinem Zerfällungskörper über $\mathbf{Z}/p\mathbf{Z}$ im Widerspruch zu Bemerkung 19.4.
Daher ist ζ^p Nullstelle von f für jede Primzahl p mit $p \nmid n$. Durch Induktion erhält man: $f(\zeta^{p_1 \cdots p_r}) = 0$ für beliebige Primzahlen $p_1, \ldots, p_r$ mit $p_1, \ldots, p_r \nmid n$. Daher ist $f(\zeta^m) = 0$ für alle $m \in \mathbb{N}$ mit $\mathrm{ggT}(m,n) = 1$. Folglich ist jede primitive m-te Einheitswurzel Nullstelle von f, d.h. $\Phi_n = f$ ist irreduzibel in $\mathbf{Z}[X]$ und $\mathbb{Q}[X]$. Wegen $\mathbb{Q}_n = \mathbb{Q}(\zeta)$ ist also $[\mathbb{Q}_n : \mathbb{Q}] = \deg(\Phi_n) = \varphi(n)$. Nach 19.4 ist $\mathbb{Q}_n\,|\,\mathbb{Q}$ Galoiserweiterung, also $|\,\mathrm{Gal}(\mathbb{Q}_n\,|\,\mathbb{Q})| = [\mathbb{Q}_n : \mathbb{Q}] = \varphi(n) = |(\mathbf{Z}/n\mathbf{Z})^\times|$. Aus 19.4 folgt die Behauptung.

Bemerkung 19.6 Sei p ungerade Primzahl. Für $x \in (\mathbf{Z}/p\mathbf{Z})^\times$ ist dann $0 = x^{p-1} - 1 = (x^{\frac{p-1}{2}} - 1)(x^{\frac{p-1}{2}} + 1)$, also entweder $x^{\frac{p-1}{2}} = 1$ oder $x^{\frac{p-1}{2}} = -1$ (nicht beides). Ferner ist

$$|\{x \in \mathbf{Z}/p\mathbf{Z} : x^{\frac{p-1}{2}} = 1\}| = \frac{p-1}{2} = |\{x \in \mathbf{Z}/p\mathbf{Z} : x^{\frac{p-1}{2}} = -1\}|.$$

Für $a \in \mathbf{Z} \setminus p\mathbf{Z}$ definiert man das *Legendre-Symbol* $(\frac{a}{p}) \in \mathbf{Z}$ durch

$$\left(\frac{a}{p}\right) := \begin{cases} \;\;\,1 & \text{falls } a^{\frac{p-1}{2}} \equiv 1 \pmod{p} \\ -1 & \text{falls } a^{\frac{p-1}{2}} \equiv -1 \pmod{p} \end{cases}$$

Für $a, b \in \mathbf{Z} \setminus p\mathbf{Z}$ gilt dann:

(i) $a \equiv b \pmod p \Rightarrow (\frac{a}{p}) = (\frac{b}{p})$.

(ii) $(\frac{ab}{p}) = (\frac{a}{p})(\frac{b}{p})$.

(iii) $(\frac{a}{p}) = a^{\frac{p-1}{2}} \pmod p$.

Satz: *Ist p ungerade Primzahl, $p^* := (-1)^{\frac{p-1}{2}}p$, und ζ eine primitive p-te Einheitswurzel in $\mathbb{C}$, so ist $\mathbb{Q}(\sqrt{p^*})$ der einzige Teilkörper K von $\mathbb{Q}(\zeta)$ mit $[K:\mathbb{Q}] = 2$.*

Beweis: Da $\mathrm{Gal}(\mathbb{Q}(\zeta)|\mathbb{Q}) \cong (\mathbf{Z}/p\mathbf{Z})^\times$ zyklisch ist, enthält $\mathrm{Gal}(\mathbb{Q}(\zeta)|\mathbb{Q})$ genau eine Untergruppe U mit $|\mathrm{Gal}(\mathbb{Q}(\zeta)|\mathbb{Q}) : U| = 2$. Nach 18.9 enthält $\mathbb{Q}(\zeta)$ genau einen Teilkörper K mit $[K:\mathbb{Q}] = 2$. Daher genügt es zu zeigen: $\sqrt{p^*} \in \mathbb{Q}(\zeta)$. Für $\alpha := \sum_{i=1}^{p-1} (\frac{i}{p})\zeta^i \in \mathbb{Q}(\zeta)$ gilt aber:

$$\alpha^2 = \sum_{i,j=1}^{p-1} \left(\frac{i}{p}\right)\left(\frac{j}{p}\right)\zeta^i\zeta^j = \sum_{i,k=1}^{p-1} \left(\frac{i}{p}\right)\left(\frac{ik}{p}\right)\zeta^i\zeta^{ik},$$

denn mit k durchläuft auch ik die von 0 verschiedenen Restklassen in $\mathbf{Z}/p\mathbf{Z}$. Folglich ist

$$\alpha^2 = \sum_{i,k=1}^{p-1} \left(\frac{k}{p}\right)\left(\zeta^{k+1}\right)^i = \left(\frac{p-1}{p}\right)(p-1) - \sum_{k=1}^{p-2} \left(\frac{k}{p}\right),$$

denn für $k \neq p-1$ ist $\zeta^{k+1} =: \eta$ eine primitive p-te Einheitswurzel, also $\sum_{i=1}^{p-1} \eta^i = -1$ wie man durch Vergleich der Koeffizienten von X^{p-2} in $\prod_{i=1}^{p-1}(X-\eta^i) = \Phi_p = X^{p-1}+X^{p-2}+\ldots+X+1$ erkennt. Folglich ist

$$\alpha^2 = \left(\frac{-1}{p}\right)p - \underbrace{\sum_{k=1}^{p-1}\left(\frac{k}{p}\right)}_{=0} = (-1)^{\frac{p-1}{2}}p = p^*.$$

Satz 19.7 (Quadratisches Reziprozitätsgesetz, Gauß, 1777–1855)
Für verschiedene ungerade Primzahlen p, q ist

$$\begin{aligned}\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) &= (-1)^{\frac{p-1}{2}\frac{q-1}{2}} = \\ &= \begin{cases} 1 & \text{falls } p \equiv 1 \pmod 4 \quad \text{oder} \quad q \equiv 1 \pmod 4 \\ -1 & \text{falls } p \equiv 3 \pmod 4 \quad \text{und} \quad q \equiv 3 \pmod 4 \end{cases}\end{aligned}$$

Beweis: Sei $p^* := (-1)^{\frac{p-1}{2}}p$, ζ eine primitive p-te Einheitswurzel in $\mathbb{C}$, $R := \mathbf{Z}[\zeta] = \mathbf{Z} + \mathbf{Z}\zeta + \ldots + \mathbf{Z}\zeta^{p-2}$ und $\alpha := \sum_{i=1}^{p-1}(\frac{i}{p})\zeta^i \in R$, also $\alpha^2 = p^*$ nach dem Beweis von 19.6. Es gilt also:

$$\begin{aligned}\alpha^q &= \left(\sum_{i=1}^{p-1}\left(\frac{i}{p}\right)\zeta^i\right)^q \equiv \sum_{i=1}^{p-1}\left(\frac{i}{p}\right)^q \zeta^{iq} = \sum_{i=1}^{p-1}\left(\frac{i}{p}\right)\zeta^{iq} = \\ &= \left(\frac{q}{p}\right)\sum_{i=1}^{p-1}\left(\frac{iq}{p}\right)\zeta^{iq} = \left(\frac{q}{p}\right)\alpha \pmod{qR};\end{aligned}$$

denn mit i durchläuft auch iq die von 0 verschiedenen Restklassen in $\mathbf{Z}/p\mathbf{Z}$. Wegen $\alpha^2 = p^*$ ist also $(\frac{q}{p})p^* \equiv \alpha^{q+1} = (p^*)^{\frac{q+1}{2}} \pmod{qR}$. Daher ist $(\frac{q}{p})p^* - (p^*)^{\frac{q+1}{2}} \in qR \cap \mathbf{Z} = q\mathbf{Z}$, d.h. $(\frac{q}{p})p^* \equiv (p^*)^{\frac{q+1}{2}} \pmod q$. Wegen $q \not| \, p^*$ folgt

$$\begin{aligned}\left(\frac{q}{p}\right) &\equiv (p^*)^{\frac{q-1}{2}} \equiv \left(\frac{p^*}{q}\right) \equiv \left(\frac{-1}{q}\right)^{\frac{p-1}{2}}\left(\frac{p}{q}\right) = \\ &= (-1)^{\frac{p-1}{2}\frac{q-1}{2}}\left(\frac{p}{q}\right) \pmod q.\end{aligned}$$

Daher ist $(\frac{q}{p}) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}(\frac{p}{q})$. Multiplikation mit $(\frac{p}{q})$ liefert die Behauptung.

Satz 19.8 (Ergänzungssätze) *Für jede ungerade Primzahl p ist*

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = \begin{cases} 1 & \textit{falls } p \equiv 1 \pmod 4 \\ -1 & \textit{falls } p \equiv -1 \pmod 4 \end{cases}$$

und

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = \begin{cases} 1 & \textit{falls } p \equiv \pm 1 \pmod 8 \\ -1 & \textit{falls } p \equiv \pm 3 \pmod 8 \end{cases}$$

Beweis: Die erste Formel folgt aus der Definition von $(\frac{-1}{p})$.
Sei ζ eine primitive achte Einheitswurzel in $\mathbb{C}$. Dann ist $\zeta^4 = -1$, also $(\zeta+\zeta^{-1})^2 = \zeta^2+\zeta^{-2}+2 = 2$ wegen $\zeta^2 \in \{i, -i\}$. Folglich ist

$$\begin{aligned}
&(\zeta+\zeta^{-1})^p \equiv \zeta^p + \zeta^{-p} = \\
&\quad = \left.\begin{cases} \zeta+\zeta^{-1} & \text{falls } p \equiv \pm 1 \pmod 8 \\ \zeta^3+\zeta^{-3} = \zeta^4(\zeta+\zeta^{-1}) = -(\zeta+\zeta^{-1}) & \text{falls } p \equiv \pm 3 \pmod 8 \end{cases}\right\} \equiv \\
&\quad \equiv (-1)^{\frac{p^2-1}{8}}(\zeta+\zeta^{-1}) \pmod{p\mathbf{Z}[\zeta]}.
\end{aligned}$$

Daher ist

$$(\zeta+\zeta^{-1})^{p+1} \equiv (-1)^{\frac{p^2-1}{8}} 2 \pmod{p\mathbf{Z}[\zeta]}$$

und

$$(-1)^{\frac{p^2-1}{8}} \equiv (\zeta+\zeta^{-1})^{p-1} \equiv 2^{\frac{p-1}{2}} \equiv \left(\frac{2}{p}\right) \pmod{p\mathbf{Z}[\zeta]}.$$

Wegen $p\mathbf{Z}[\zeta] \cap \mathbf{Z} = p\mathbf{Z}$ folgt

$$(-1)^{\frac{p^2-1}{8}} \equiv \left(\frac{2}{p}\right) \pmod p,$$

also die Behauptung.

Beispiel:

$$\begin{aligned}
\left(\frac{221}{383}\right) &= \left(\frac{13}{383}\right)\left(\frac{17}{383}\right) = \left(\frac{383}{13}\right)\left(\frac{383}{17}\right) = \left(\frac{6}{13}\right)\left(\frac{9}{17}\right) = \\
&= \left(\frac{2}{13}\right)\left(\frac{3}{13}\right) = -\left(\frac{13}{3}\right) = -\left(\frac{1}{3}\right) = -1.
\end{aligned}$$

Bemerkung 19.9 Man setzt das Legendre-Symbol $(\frac{a}{p})$ fort zum *Jacobi-Symbol* $(\frac{a}{b})$, indem man für $b \in \mathbb{N}$, b ungerade mit Primfaktorzerlegung $b = p_1 \dots p_r$, und $a \in \mathbf{Z}$ mit $\mathrm{ggT}(a,b) = 1$ definiert:

$$\left(\frac{a}{b}\right) := \left(\frac{a}{p_1}\right) \cdots \left(\frac{a}{p_r}\right).$$

Dann gilt:

(i) $a \equiv a' \pmod b \Rightarrow (\frac{a}{b}) = (\frac{a'}{b})$.

(ii) $(\frac{aa'}{b}) = (\frac{a}{b})(\frac{a'}{b})$, $(\frac{a}{bb'}) = (\frac{a}{b})(\frac{a}{b'})$.

(iii) a, b ungerade mit $\mathrm{ggT}(a,b) = 1 \Rightarrow (\frac{a}{b})(\frac{b}{a}) = (-1)^{\frac{a-1}{2}\frac{b-1}{2}}$.

(iv) $(\frac{-1}{b}) = (-1)^{\frac{b-1}{2}}$, $(\frac{2}{b}) = (-1)^{\frac{b^2-1}{8}}$.

Beweis:

(i)-(ii) Klar.

(iii) Sei $a = p_1 \dots p_r,\ b = q_1 \dots q_s$ mit Primzahlen $p_1, \dots, p_r, q_1, \dots, q_s$. Dann ist

$$\begin{aligned}\left(\frac{a}{b}\right)\left(\frac{b}{a}\right) &= \prod_{i=1}^{r}\prod_{j=1}^{s}\left(\frac{p_i}{q_j}\right)\left(\frac{q_j}{p_i}\right) = \prod_{i,j}(-1)^{\frac{p_i-1}{2}\frac{q_j-1}{2}} = \\ &= (-1)^{\sum_{i,j}\frac{p_i-1}{2}\frac{q_j-1}{2}}.\end{aligned}$$

Es genügt also zu zeigen:

$$\sum_{i=1}^{r}\frac{p_i-1}{2} \equiv \frac{p_1\dots p_r - 1}{2} \pmod 2$$

bzw.

$$\sum_{i=1}^{r}(p_i - 1) \equiv p_1 \dots p_r - 1 \pmod 4.$$

Für $r = 1$ ist nichts zu beweisen. Sei also $r > 1$ und $\sum_{i=1}^{r-1}(p_i - 1) \equiv p_1 \dots p_{r-1} - 1 \pmod 4$ bewiesen. Dann ist

$$\begin{aligned}\sum_{i=1}^{r}(p_i - 1) &\equiv p_1 \dots p_{r-1} - 1 + p_r - 1 \equiv \\ &\equiv p_1 \dots p_r - 1 - (p_1 \dots p_{r-1} - 1)(p_r - 1) \equiv \\ &\equiv p_1 \dots p_r - 1 \pmod 4,\end{aligned}$$

da $p_1, \dots, p_r$ ungerade sind.

(iv) Sei $b = p_1 \dots p_r$ mit Primzahlen $p_1, \dots, p_r$. Wie in (iii) ist dann:

$$\begin{aligned}\left(\frac{-1}{b}\right) &= \left(\frac{-1}{p_1}\right)\dots\left(\frac{-1}{p_r}\right) = (-1)^{\frac{p_1-1}{2}}\dots(-1)^{\frac{p_r-1}{2}} = \\ &= (-1)^{\sum_{i=1}^{r}\frac{p_i-1}{2}} = (-1)^{\frac{p_1\dots p_r-1}{2}} = (-1)^{\frac{b-1}{2}},\end{aligned}$$

$$\begin{aligned}\left(\frac{2}{b}\right) &= \left(\frac{2}{p_1}\right)\dots\left(\frac{2}{p_r}\right) = (-1)^{\frac{p_1^2-1}{8}}\dots(-1)^{\frac{p_r^2-1}{8}} = \\ &= (-1)^{\sum_{i=1}^{r}\frac{p_i^2-1}{8}}.\end{aligned}$$

Es genügt also zu zeigen:

$$\sum_{i=1}^{r}(p_i^2 - 1) \equiv p_1^2 \dots p_r^2 - 1 \pmod{16}.$$

Für $r = 1$ ist das klar. Sei also $r > 1$ und $\sum_{i=1}^{r-1}(p_i^2 - 1) \equiv p_1^2 \dots p_{r-1}^2 - 1 \pmod{16}$. Dann ist

$$\begin{aligned}\sum_{i=1}^{r}(p_i^2 - 1) &\equiv p_1^2 \dots p_{r-1}^2 - 1 + p_r^2 - 1 \equiv \\ &\equiv p_1^2 \dots p_r^2 - 1 - (p_1^2 \dots p_{r-1}^2 - 1)(p_r^2 - 1) \equiv \\ &\equiv p_1^2 \dots p_r^2 - 1 \pmod{16},\end{aligned}$$

da $p_1, \dots, p_r$ ungerade sind.

Beispiel:

$$\left(\frac{221}{383}\right) = \left(\frac{383}{221}\right) = \left(\frac{162}{221}\right) = \left(\frac{2}{221}\right)\left(\frac{81}{221}\right) = \left(\frac{2}{221}\right) = -1.$$

Man kann also das Jacobi-Symbol sehr einfach berechnen.

Kapitel 20

Reine Gleichungen

Bemerkung 20.1 Für einen kommutativen Ring R und Elemente $r \in R,\ u \in R^\times$ definiert man eine Abbildung $f_{u,r} : R \to R$ durch $f_{u,r}(x) := ux + r$ für $x \in R$. Dann ist $f_{1,0} = \mathrm{id}_R$ und $f_{u,r} \circ f_{v,s} = f_{uv,us+r}$; denn für $x \in R$ ist $f_{u,r}(f_{v,s}(x)) = u(vx + s) + r = uvx + (us + r) = f_{uv,us+r}(x)$. Insbesondere ist $f_{u,r} \circ f_{u^{-1},-u^{-1}r} = f_{1,0} = f_{u^{-1},-u^{-1}r} \circ f_{u,r}$. Daher ist $f_{u,r}$ bijektiv mit $f_{u,r}^{-1} = f_{u^{-1},-u^{-1}r}$. Folglich ist $\mathrm{Aff}(R) := \{f_{u,r} : u \in R^\times, r \in R\}$ eine Untergruppe von $\mathrm{Sym}(R)$. Man nennt $\mathrm{Aff}(R)$ die *affine Gruppe* von R.
Wegen $f_{u,0} \circ f_{v,0} = f_{uv,0}$ für $u, v \in R^\times$ ist die Abbildung $\varphi_1 : R^\times \to \mathrm{Aff}(R),\ u \mapsto f_{u,0}$ ein Monomorphismus. Wegen $f_{1,r} \circ f_{1,s} = f_{1,r+s}$ für $r, s \in R$ ist die Abbildung $\varphi_2 : (R, +) \to \mathrm{Aff}(R),\ r \mapsto f_{1,r}$ ein Monomorphismus. Ferner ist die Abbildung $\psi : \mathrm{Aff}(R) \to R^\times,\ f_{u,r} \mapsto u$ ein Epimorphismus mit $\psi \circ \varphi_1 = \mathrm{id}_{R^\times}$.

Satz: *Für $n \in \mathbb{N}$, jeden Körper K mit $\mathrm{char}(K) \nmid n$ und $a \in K^\times$ gilt:*

(i) Der Zerfällungskörper L von $X^n - a$ über K enthält eine primitive n-te Einheitswurzel ζ.

(ii) Ist $b \in L$ mit $b^n = a$, so sind $b, \zeta b, \ldots, \zeta^{n-1}b$ die Nullstellen von $X^n - a$ in L; insbesondere ist $L = K(b, \zeta)$.

(iii) $L|K$, $L|K(\zeta)$ und $K(\zeta)|K$ sind Galoiserweiterungen.

(iv) $\mathrm{Gal}(L|K)$ *ist zu einer Untergruppe von* $\mathrm{Aff}(\mathbf{Z}/n\mathbf{Z})$ *isomorph.*

(v) $\mathrm{Gal}(L|K(\zeta))$ *ist zu einer Untergruppe von* $\mathbf{Z}/n\mathbf{Z}$ *isomorph.*

Definition: *Man nennt ein Polynom der Form $X^n - a$ und die entsprechende Gleichung* $X^n - a = 0$ rein. *Ein Element b mit $b^n = a$ nennt man eine n-te* Wurzel *aus a.*

Beweis:

(i) $X^n - a$ und $(X^n - a)' = nX^{n-1} \neq 0$ sind teilerfremd. Daher besitzt $X^n - a$ in L genau n verschiedene Nullstellen $b_1, \ldots, b_n$. Für $i = 1, \ldots, n$ ist dann $(\frac{b_i}{b_1})^n = \frac{b_i^n}{b_1^n} = \frac{a}{a} = 1$, d.h. $1 = \frac{b_1}{b_1}, \frac{b_2}{b_1}, \ldots, \frac{b_n}{b_1}$ sind n verschiedene n-te Einheitswurzeln in L. Diese bilden nach 19.4 eine zyklische Gruppe $\langle\zeta\rangle$ der Ordnung n, d.h. ζ ist eine primitive n-te Einheitswurzel in L.

(ii) Wegen $a \neq 0$ ist $b \neq 0$. Daher sind $b, \zeta b, \ldots, \zeta^{n-1}b$ paarweise verschieden mit $(\zeta^i b)^n = \zeta^{in}b^n = b^n = a$ für $i = 0, \ldots, n-1$.

(iii) L ist als Zerfällungskörper des separablen Polynoms $X^n - a$ eine Galoiserweiterung von K und $K(\zeta)$. $K(\zeta)|K$ ist als n-ter Kreisteilungskörper über K eine Galoiserweiterung von K.

(iv) Für $\sigma \in \mathrm{Gal}(L|K)$ ist $\sigma(\zeta)$ wieder eine primitive n-te Einheitswurzel in L, und $\sigma(b)^n = \sigma(b^n) = \sigma(a) = a$. Daher existieren $l, m \in \mathbf{Z}$ mit $\mathrm{ggT}(l,n) = 1$ und $\sigma(\zeta) = \zeta^l$, $\sigma(b) = \zeta^m b$. Bekanntlich gilt: $\zeta^l = \zeta^{l'} \Leftrightarrow l + n\mathbf{Z} = l' + n\mathbf{Z}$. Daher sind $l + n\mathbf{Z}$ und $m + n\mathbf{Z}$ durch σ eindeutig bestimmt, und die Abbildung $\Phi : \mathrm{Gal}(L|K) \to \mathrm{Aff}(\mathbf{Z}/n\mathbf{Z})$, die σ auf $f_{l+n\mathbf{Z},m+n\mathbf{Z}}$ abbildet, ist wohldefiniert. Ist auch $\sigma' \in \mathrm{Gal}(L|K)$ und $\sigma'(\zeta) = \zeta^{l'}$, $\sigma'(b) = \zeta^{m'} b$ mit $l', m' \in \mathbf{Z}$, $\mathrm{ggT}(l', n) = 1$, so ist $(\sigma' \circ \sigma)(\zeta) = \sigma'(\zeta^l) = \sigma'(\zeta)^l = \zeta^{l'l}$ und $(\sigma' \circ \sigma)(b) = \sigma'(\zeta^m b) = \sigma'(\zeta)^m \sigma'(b) = \zeta^{l'm}\zeta^{m'} b = \zeta^{l'm+m'} b$. Daher ist

$$\begin{aligned} \Phi(\sigma' \circ \sigma) &= f_{l'l+n\mathbf{Z},l'm+m'+n\mathbf{Z}} = f_{l'+n\mathbf{Z},m'+n\mathbf{Z}} \circ f_{l+n\mathbf{Z},m+n\mathbf{Z}} = \\ &= \Phi(\sigma') \circ \Phi(\sigma), \end{aligned}$$

d.h. Φ ist Homomorphismus. Für $\sigma \in \ker(\Phi)$ ist $f_{l+n\mathbf{Z},m+n\mathbf{Z}} = \Phi(\sigma) = \mathrm{id}_{\mathbf{Z}/n\mathbf{Z}} = f_{1,0}$, also $l + n\mathbf{Z} = 1$ und $m + n\mathbf{Z} = 0$. d.h. $\sigma(\zeta) = \zeta^l = \zeta$ und $\sigma(b) = \zeta^m b = b$. Wegen $L = K(b, \zeta)$ ist also $\sigma = \mathrm{id}_L$, d.h. Φ ist injektiv.

(v) Für $\sigma \in \mathrm{Gal}(L|K(\zeta))$ ist $\sigma(\zeta) = \zeta$, also $l + n\mathbf{Z} = 1 + n\mathbf{Z}$ in der Notation von (iv). Daher ist $\Phi(\mathrm{Gal}(L|K(\zeta))) \subseteq \{f_{1,r} : r \in \mathbf{Z}/n\mathbf{Z}\} = \mathrm{Bild}(\varphi_2) \cong \mathbf{Z}/n\mathbf{Z}$.

Satz 20.2 *Für $n \in \mathbb{N}$, jeden Körper K, der eine primitive n-te Einheitswurzel ζ enthält, und jedes $a \in K^\times$ ist der Zerfällungskörper L von $X^n - a$ über K eine Galoiserweiterung von K mit zyklischer Galoisgruppe G, deren Ordnung d ein Teiler von n ist. Ist $b \in L$ mit $b^n = a$, so ist $m_{K,b} = X^d - b^d$; insbesondere ist d die kleinste natürliche Zahl e mit $b^e \in K$.*

Beweis: Da K eine primitive n-te Einheitswurzel enthält, ist $\mathrm{char}(K) \nmid n$ nach 19.4. Nach 20.1 ist also $L|K$ Galoiserweiterung, deren Galoisgruppe G zu einer Untergruppe der zyklischen Gruppe $\mathbf{Z}/n\mathbf{Z}$ isomorph ist. Mit $\mathbf{Z}/n\mathbf{Z}$ ist G zyklisch mit $d := |G| \mid n$. Sei $\sigma \in G$ mit $G = \langle\sigma\rangle$ und $b \in L$ mit $b^n = a$. Nach 20.1 ist $L = K(b)$, also $\deg(m_{K,b}) = [L : K] = |G| = d$. Nach dem Beweis von 20.1 ist die Abbildung $\Psi : G \to \langle\zeta\rangle$, $\rho \mapsto \rho(b)/b$ ein Homomorphismus. Es ist also $(\sigma(b)/b)^d = \Psi(\sigma)^d = \Psi(\sigma^d) = \Psi(1) = 1$, also $\sigma(b^d) = b^d$, d.h. $b^d \in \mathrm{Fix}(G) = K$. Folglich ist $X^d - b^d \in K[X]$ mit Nullstelle b, also $m_{K,b} \mid X^d - b^d$. Wegen $\deg(m_{K,b}) = d$ folgt die Behauptung.

Satz 20.3 *Für $n \in \mathbb{N}$, jeden Körper K, der eine primitive n-te Einheitswurzel ζ enthält, und jede Galoiserweiterung $L|K$ des Grades n mit zyklischer Galoisgruppe $G = \langle\sigma\rangle$ existiert ein $a \in K^\times$, so daß L Zerfällungskörper von $X^n - a$ über K ist.*

Beweis: Nach Dedekind sind $\mathrm{id}, \sigma, \sigma^2, \ldots, \sigma^{n-1}$ linear unabhängig über K. Daher existiert ein $b \in L$ mit $0 \neq b + \zeta\sigma(b) + \ldots + \zeta^{n-1}\sigma^{n-1}(b) =: c$. Dann ist $\sigma(c) = \sigma(b) + \zeta\sigma^2(b) + \ldots + \zeta^{n-1}\sigma^n(b) = \zeta^{-1}c$. Für $m \in \mathbb{N}$ ist also $\sigma^m(c) = \zeta^{-m}c$, d.h. die Einschränkungen von $\mathrm{id}, \sigma, \sigma^2, \ldots, \sigma^{n-1}$ auf $K(c)$ sind paarweise verschieden. Daher ist $n \leq |\,\mathrm{Gal}(K(c)|K)| = [K(c) : K] \leq [L : K] = n$, also $L = K(c)$. Wegen $\sigma(c^n) = \sigma(c)^n = (\zeta^{-1}c)^n = c^n$ ist $c^n \in \mathrm{Fix}(\langle\sigma\rangle) = K$, also $X^n - c^n \in K[X]$. Die Nullstellen von $X^n - c^n$ in L sind $c, \zeta c, \ldots, \zeta^{n-1}c$. Wegen $L = K(c) = K(c, \zeta c, \ldots, \zeta^{n-1}c)$ ist also L Zerfällungskörper von $X^n - c^n$ über K.

Bemerkung 20.4 Für $n \in \mathbb{N}$ und jeden Körper K ist

$$\left(K^\times\right)^n := \{x^n : x \in K^\times\} \leq K^\times.$$

Satz: (Kummer) *Sei $n \in \mathbb{N}$ und K ein Körper, der eine primitive n-te Einheitswurzel enthält. Für $a \in K^\times$ sei K_a Zerfällungskörper von $X^n - a$ über K. Dann liefert die Abbildung $a \mapsto K_a$ eine Bijektion zwischen der Menge aller zyklischen Untergruppen der Ordnung n von $(K^\times)/(K^\times)^n$ und der Menge aller K-Isomorphie-Klassen von Galoiserweiterungen des Grades n von K mit zyklischer Galoisgruppe.*

Beweis: Sei $a \in K^\times$ mit $|\langle a(K^\times)^n\rangle| = n$. Nach 20.2 ist $K_a|K$ eine Galoiserweiterung mit zyklischer Galoisgruppe und $d := [K_a : K] \bigm| n$. Ist $b \in K_a$ mit $b^n = a$, so ist ferner $K_a = K(b)$ und $b^d \in K$. Folglich ist $a^d = b^{nd} \in (K^\times)^n$, also $n = |\langle a(K^\times)^n\rangle| \leq d$, d.h. insgesamt $d = n$. Für $c \in K^\times$ ist $bc \in K_a^\times$ mit $(bc)^n = b^n c^n = ac^n$ und $K_a = K(b) = K(bc)$. Daher ist K_a auch Zerfällungskörper von $X^n - ac^n$ über K und damit zu K_{ac^n} K-isomorph. Für $k \in \mathbb{N}$ ist $b^k \in K_a$ mit $(b^k)^n = a^k$. Daher enthält K_a einen Zerfällungskörper von $X^n - a^k$, o.B.d.A. $K_{a^k} \subseteq K_a$. Im Fall $\langle a(K^\times)^n\rangle = \langle a^k(K^\times)^n\rangle$ ist analog o.B.d.A. $K_a \subseteq K_{a^k}$, also $K_a = K_{a^k}$.
Sei umgekehrt $a' \in K$ mit $K_{a'} = K_a$, und sei $b' \in K_{a'}$ mit $(b')^n = a'$. Schreibt man $\mathrm{Gal}(K_a|K) = \langle\sigma\rangle$, so sind $\zeta := \sigma(b)/b$ und $\zeta' := \sigma(b')/b'$ primitive n-te Einheitswurzeln in K, also $\zeta' = \zeta^k$ für ein $k \in \{1, \ldots, n-1\}$. Schreibt man $b' = a_0 + a_1 b + \ldots + a_{n-1}b^{n-1}$ mit $a_0, \ldots, a_{n-1} \in K$, so ist also

$$\begin{aligned} a_0\zeta^k + a_1\zeta^k b + \ldots + a_{n-1}\zeta^k b^{n-1} \quad &= \quad \zeta^k b' \ = \ \zeta' b' \ = \ \sigma(b') \ = \\ &= \quad a_0 + a_1\zeta b + \ldots + a_{n-1}\zeta^{n-1}b^{n-1}. \end{aligned}$$

Koeffizientenvergleich liefert $a_j = 0$ für $j \neq k$, $b' = a_k b^k$ und daher $a' = (b')^n = a_k^n a^k \in \langle a, (K^\times)^n\rangle$. Analog ist $a \in \langle a', (K^\times)^n\rangle$, also $\langle a(K^\times)^n\rangle = \langle a'(K^\times)^n\rangle$.
Sei schließlich $L|K$ Galoiserweiterung des Grades n mit zyklischer Galoisgruppe. Nach 20.3 existiert ein $a \in K^\times$, so daß L Zerfällungskörper von $X^n - a$ über K ist. Wegen $a^n \in (K^\times)^n$ ist $m := |\langle a(K^\times)^n\rangle| \bigm| n$. Zu zeigen bleibt $m \geq n$. Sei $b \in L$ mit $b^n = a$. Nach 20.2 ist dann n die kleinste Zahl, so daß $b^n \in K$. Sei nun $a^m = (a')^n$ mit $a' \in K^\times$. Dann ist $b^{nm} = (a')^n$, also b^m Nullstelle von $X^n - (a')^n$, d.h. $b^m \in \{a'\zeta^i : 1 \leq i \leq n,\ \zeta \text{ primitive } n\text{-te Einheitswurzel in } K\} \subseteq K$. Daraus folgt $m \geq n$.

Kapitel 21

Die Auflösbarkeit algebraischer Gleichungen

Definition 21.1 *Eine Körpererweiterung $L|K$ heißt* Radikalerweiterung, *wenn es eine Folge von Teilkörpern $K = K_0 \subseteq K_1 \subseteq \ldots \subseteq K_r = L$ und Elemente $b_i \in K_i$, $n_i \in \mathbb{N}$ gibt mit $K_i = K_{i-1}(b_i)$ und $b_i^{n_i} \in K_{i-1}$ für $i = 1, \ldots, r$. Ein Polynom $f \in K[X]$ heißt über K* durch Radikale auflösbar, *wenn es eine Radikalerweiterung $L|K$ gibt, in der f in Linearfaktoren zerfällt.*

Bemerkung: Dies präzisiert den Begriff der Auflösbarkeit der Gleichung $f(X) = 0$ durch Addition, Subtraktion, Multiplikation, Division und Wurzelziehen.

Satz: *Zu jedem Körper K der Charakteristik 0 und jeder Radikalerweiterung $L|K$ existiert eine Radikal- und Galoiserweiterung $M|K$ mit $L \subseteq M$.*

Beweis: Sei $K = K_0 \subseteq K_1 \subseteq \ldots \subseteq K_r = L$ mit $K_i = K_{i-1}(b_i)$ und $b_i^{n_i} \in K_{i-1}$ wie oben. Nach 16.6 existiert eine endliche normale Körpererweiterung $N|K$ mit $L \subseteq N$. Wegen $\mathrm{char}(K) = 0$ ist $N|K$ Galoiserweiterung. Wir schreiben $\mathrm{Gal}(N|K) = \{\sigma_1 = \mathrm{id}, \sigma_2, \ldots, \sigma_s\}$ und setzen

$$K_{ij} := K\big(\sigma_1(b_1), \ldots, \sigma_s(b_1), \ldots, \sigma_1(b_{i-1}), \ldots, \sigma_s(b_{i-1}), \sigma_1(b_i), \ldots, \sigma_j(b_i)\big)$$

für $i = 1, \ldots, r,\ j = 1, \ldots, s$. Dann ist

$$K \subseteq K_{11} \subseteq K_{12} \subseteq \ldots \subseteq K_{1s} \subseteq K_{21} \subseteq K_{22} \subseteq \ldots \subseteq K_{2s} \subseteq \ldots \subseteq K_{r1} \subseteq \ldots \subseteq K_{rs}.$$

Für $i = 1 \ldots, r$ ist $K_{is} = K\big(\sigma(b_k) : k = 1, \ldots, i,\ \sigma \in \mathrm{Gal}(N|K)\big)$. Jedes $\tau \in \mathrm{Gal}(N|K)$ permutiert die Elemente $\sigma(b_k)$ $(k = 1, \ldots, i,\ \sigma \in \mathrm{Gal}(N|K))$, d.h. $\tau(K_{is}) \subseteq K_{is}$. Nach 18.10 ist $K_{is}|K$ Galoiserweiterung; insbesondere ist $K_{rs}|K$ Galoiserweiterung.
Offenbar ist $K_1 = K(b_1) = K(\sigma_1(b_1)) = K_{11}$. Sei nun $i > 1$ und bereits $K_{i-1} \subseteq K_{i-1,1}$ bewiesen. Dann ist $K_i = K_{i-1}(b_i) \subseteq K_{i-1,1}(b_i) \subseteq K_{i-1,s}(b_i) = K_{i1}$ und $\sigma_1(b_i)^{n_i} = b_i^{n_i} \in K_{i-1} \subseteq K_{i-1,1} \subseteq K_{i-1,s}$. Daher ist $K_i \subseteq K_{i1}$ und $K_{i1} = K_{i-1,s}(b_i)$ mit $b_i^{n_i} \in K_{i-1,s}$; insbesondere ist $L = K_r \subseteq K_{r1} \subseteq K_{rs}$. Für $j > 1$ ist $K_{ij} = K_{i,j-1}(\sigma_j(b_i))$ mit $\sigma_j(b_i)^{n_i} = \sigma_j(b_i^{n_i}) \in \sigma_j(K_{i-1}) \subseteq \sigma_j(K_{i-1,1}) \subseteq \sigma_j(K_{i-1,s}) \subseteq K_{i-1,s} \subseteq K_{i1} \subseteq K_{i,j-1}$. Daher ist $K_{rs}|K$ auch Radikalerweiterung.

Satz 21.2 *Ist K ein Körper der Charakteristik 0 und $L|K$ Radikal- und Galoiserweiterung, so ist* $\mathrm{Gal}(L|K)$ *auflösbar.*

Beweis: Sei $K = K_0 \subseteq K_1 \subseteq \ldots \subseteq K_r = L$ mit Körpern $K_i = K_{i-1}(b_i)$, $b_i^{n_i} \in K_{i-1}$ wie oben. Sei $n := n_1 \ldots n_r$ und M der n-te Kreisteilungskörper über L, also $M = L(\zeta)$ mit einer primitiven n-ten Einheitswurzel ζ. Dann ist $K \subseteq K(\zeta) \subseteq K_1(\zeta) \subseteq \ldots \subseteq K_r(\zeta) = M$ mit $\zeta^n = 1$, $K_i(\zeta) = K_{i-1}(b_i, \zeta)$ mit $b_i^{n_i} \in K_{i-1} \subseteq K_{i-1}(\zeta)$ für alle i. Nach 19.4 ist $K(\zeta)|K$ Galoiserweiterung mit abelscher Galoisgruppe. Da $K_{i-1}(\zeta)$ eine primitive n_i-te Einheitswurzel enthält, nämlich ζ^{n/n_i}, ist $K_i(\zeta)|K_{i-1}(\zeta)$ nach 20.1 eine Galoiserweiterung mit zyklischer Galoisgruppe für alle i. Mit $L|K$ und $K(\zeta)|K$ ist auch $M = L(\zeta)|K$ Galoiserweiterung nach Aufgabe 3 von Blatt 14. Nach 18.10 ist also

$$\begin{aligned} 1 = \operatorname{Gal}(M|M) = \operatorname{Gal}(M|K_r(\zeta)) \trianglelefteq \\ \trianglelefteq \operatorname{Gal}(M|K_{r-1}(\zeta)) \trianglelefteq \ldots \trianglelefteq \operatorname{Gal}(M|K(\zeta)) \trianglelefteq \operatorname{Gal}(M|K) \end{aligned}$$

mit

$$\operatorname{Gal}(M|K)/\operatorname{Gal}(M|K(\zeta)) \cong \operatorname{Gal}(K(\zeta)|K)$$

und

$$\operatorname{Gal}(M|K_{i-1}(\zeta))/\operatorname{Gal}(M|K_i(\zeta)) \cong \operatorname{Gal}(K_i(\zeta)|K_{i-1}(\zeta)) \quad \text{für alle } i.$$

Daher ist $\operatorname{Gal}(M|K)$ auflösbar. Da $L|K$ Galoiserweiterung ist, ist $\operatorname{Gal}(M|L) \trianglelefteq \operatorname{Gal}(M|K)$ mit $\operatorname{Gal}(M|K)/\operatorname{Gal}(M|L) \cong \operatorname{Gal}(L|K)$ nach 18.10. Daher ist auch $\operatorname{Gal}(L|K)$ auflösbar.

Satz 21.3 *Sei $L|K$ Galoiserweiterung, $n := [L : K] < \infty$, $\operatorname{char}(K) = 0$ und $\operatorname{Gal}(L|K)$ auflösbar. Dann ist der n-te Kreisteilungskörper M über L eine Radikalerweiterung von K.*

Beweis: Es ist $M = L(\zeta)$ mit einer primitiven n-ten Einheitswurzel ζ. Nach Aufgabe 2 von Blatt 14 ist $M|K(\zeta)$ Galoiserweiterung mit $G := \operatorname{Gal}(M|K(\zeta)) \cong \operatorname{Gal}(L|L \cap K(\zeta)) \leq \operatorname{Gal}(L|K)$; insbesondere ist G auflösbar. Daher existiert eine Subnormalreihe $G = G_0 \trianglerighteq G_1 \trianglerighteq \ldots \trianglerighteq G_{r-1} \trianglerighteq G_r = 1$ von G, so daß G_{i-1}/G_i für $i = 1, \ldots, r$ zyklisch ist. Für $i = 0, \ldots, r$ ist M Galoiserweiterung von $F_i := \operatorname{Fix}(G_i)$ und $G_i = \operatorname{Gal}(M|F_i)$, und es ist $K(\zeta) = F_0 \subseteq F_1 \subseteq \ldots \subseteq F_r = M$.

$$\begin{array}{ccc} M = F_r & \qquad\qquad & G_r = 1 \\ | & & | \\ F_{r-1} & & G_{r-1} \\ | & & | \\ \vdots & & \vdots \\ | & & | \\ F_1 & & G_1 \\ | & & | \\ F_0 = K(\zeta) & & G_0 = G \end{array}$$

Nach 18.10 ist $F_i|F_{i-1}$ jeweils Galoiserweiterung mit

$$\operatorname{Gal}(F_i|F_{i-1}) \cong \operatorname{Gal}(M|F_{i-1})/\operatorname{Gal}(M|F_i) = G_{i-1}/G_i.$$

Nach Lagrange ist $n_i = |G_{i-1}/G_i| \bigm| |G| \bigm| |\operatorname{Gal}(L|K)| = [L : K] = n$. Da F_{i-1} eine primitive n_i-te Einheitswurzel enthält, nämlich ζ^{n/n_i}, ist F_i nach 20.3 Zerfällungskörper eines reinen Polynoms $X^{n_i} - a_i$ über F_{i-1}. Daher ist $F_i = F_{i-1}(b_i)$, wobei $b_i^{n_i} = a_i$ nach 20.1. Dies zeigt, daß $M|K$ Radikalerweiterung ist.

Satz 21.4 *Für jeden Körper K der Charakteristik 0, jedes Polynom $f \in K[X]$ und jeden Zerfällungskörper L von f über K sind äquivalent:*

(1) f ist über K durch Radikale auflösbar.

(2) $\operatorname{Gal}(L|K)$ ist auflösbar.

Bemerkung: Man nennt $\mathrm{Gal}(L|K)$ auch die *Galoisgruppe* von f über K und schreibt $\mathrm{Gal}(f|K)$.

Beweis:

(1)⇒(2): Sei $M|K$ Radikalerweiterung, in der f in Linearfaktoren zerfällt, o.B.d.A. $M|K$ auch Galoiserweiterung nach 21.1. Sind $a_1, \ldots, a_n$ die Nullstellen von f in M, so ist $L' := K(a_1, \ldots, a_n)$ Zerfällungskörper von f über K, also wegen $\mathrm{char}(K) = 0$ Galoiserweiterung von K. Nach 18.10 ist $\mathrm{Gal}(M|L') \trianglelefteq \mathrm{Gal}(M|K)$ mit $\mathrm{Gal}(L'|K) \cong \mathrm{Gal}(M|K)/\mathrm{Gal}(M|L')$. Nach 21.2 ist $\mathrm{Gal}(M|K)$ auflösbar, also auch $\mathrm{Gal}(L'|K)$. Da L und L' K-isomorph sind, ist $\mathrm{Gal}(L|K) \cong \mathrm{Gal}(L'|K)$ auflösbar.

(2)⇒(1): Sei $\mathrm{Gal}(L|K)$ auflösbar. Nach 21.3 existiert eine endliche Erweiterung $M|L$, so daß $M|K$ Radikalerweiterung ist. Da f über L in Linearfaktoren zerfällt, zerfällt f auch über M in Linearfaktoren.

Lemma 21.5

(i) Für jede Primzahl p, jeden p-Zyklus $\sigma \in \mathrm{Sym}(p)$ und jede Transposition $\tau \in \mathrm{Sym}(p)$ ist $\mathrm{Sym}(p) = \langle \sigma, \tau \rangle$.

(ii) Für jede Primzahl p ist jedes Element der Ordnung p in $\mathrm{Sym}(p)$ ein p-Zyklus.

Beweis:

(i) Wir schreiben $\sigma = (a_1, \ldots, a_p)$ und $\tau = (a_i, a_j)$. Wegen $\sigma = (a_i, \ldots, a_p, a_1, \ldots, a_{i-1})$ sind also σ und τ von der Form $\sigma = (b_1, \ldots, b_p)$, $\tau = (b_1, b_k)$. Dann ist $\sigma' := \sigma^k$ ein p-Zyklus von der Form $\sigma' = (b_1, b_k, \ldots)$. Folglich sind σ', τ von der Form $\sigma' = (c_1, c_2, \ldots, c_p)$, $\tau = (c_1, c_2)$. Setzt man $\rho := \begin{pmatrix} 1 & 2 & \cdots & p \\ c_1 & c_2 & \cdots & c_p \end{pmatrix}$, so ist $\rho^{-1}\sigma'\rho = (1, 2, \ldots, p)$ und $\rho^{-1}\tau\rho = (1, 2)$. Wegen 7.2 ist $\mathrm{Sym}(p) = \langle (1, 2, \ldots, p), (1, 2) \rangle = \langle \rho^{-1}\sigma'\rho, \rho^{-1}\tau\rho \rangle = \rho^{-1}\langle \sigma', \tau \rangle \rho \subseteq \rho^{-1}\langle \sigma, \tau \rangle \rho \subseteq \mathrm{Sym}(p)$, also $\mathrm{Sym}(p) = \rho\,\mathrm{Sym}(p)\rho^{-1} = \langle \sigma, \tau \rangle$.

(ii) $\mathrm{Sym}(p)$ operiert auf $\{1, \ldots, p\}$ durch ${}^{\tau}j := \tau(j)$, also auch $\langle \sigma \rangle$. Wegen $\sigma \neq \mathrm{id}$ gibt es eine Bahn B der Länge $\neq 1$. Wegen $|B| \mid |\langle \sigma \rangle| = p$ ist $B = \{1, 2, \ldots, p\}$. Für $i = 1, \ldots, p$ existieren also $\tau_i \in \langle \sigma \rangle$ mit $\tau_i(1) = i$. Wegen $|\langle \sigma \rangle| = p$ ist $\langle \sigma \rangle = \{\tau_1, \ldots, \tau_p\}$, also $\sigma^i(1) \neq 1$ für $i = 1, \ldots, p-1$. Folglich ist $\sigma = (1, \sigma(1), \sigma^2(1), \ldots, \sigma^{p-1}(1))$.

Satz 21.6 *Für jede Primzahl p und jedes irreduzible Polynom f vom Grad p in $\mathbb{Q}[X]$, das genau $p-2$ reelle Nullstellen hat, ist $\mathrm{Gal}(f|\mathbb{Q}) \cong \mathrm{Sym}(p)$; insbesondere ist f im Fall $p \geq 5$ nicht durch Radikale auflösbar.*

Beweis: In $\mathbb{C}[X]$ zerfällt f in Linearfaktoren, etwa $f = c(X - \alpha_1) \ldots (X - \alpha_p)$. Dann ist $L := \mathbb{Q}(\alpha_1, \ldots, \alpha_p)$ Zerfällungskörper von f über $\mathbb{Q}$ und daher eine Galoiserweiterung von $\mathbb{Q}$. Mit α_i ist auch $\bar{\alpha}_i$ Nullstelle von f. Daher liefert die komplexe Konjugation ein Element $\tau \in \mathrm{Gal}(L|\mathbb{Q})$, das die $p-2$ reellen Nullstellen von f festläßt und die beiden anderen vertauscht. Wegen $f(\alpha_1) = 0$ ist $m_{\mathbb{Q},\alpha_1} \mid f$, wegen der Irreduzibilität von f also $p = \deg(f) = \deg(m_{\mathbb{Q},\alpha_1}) = [\mathbb{Q}(\alpha_1)|\mathbb{Q}] \mid [L : \mathbb{Q}] = |\mathrm{Gal}(L|\mathbb{Q})|$. Die Abbildung $\Phi : \mathrm{Gal}(L|\mathbb{Q}) \to \mathrm{Sym}(\{\alpha_1, \ldots, \alpha_p\})$, $\sigma \mapsto \begin{pmatrix} \alpha_1 & \cdots & \alpha_p \\ \sigma(\alpha_1) & \cdots & \sigma(\alpha_p) \end{pmatrix}$ ist ein Homomorphismus. Wegen $L = \mathbb{Q}(\alpha_1, \ldots, \alpha_p)$ ist jedes $\sigma \in \mathrm{Gal}(L|\mathbb{Q})$ eindeutig bestimmt durch $\sigma(\alpha_1), \ldots, \sigma(\alpha_p)$. Daher ist Φ injektiv. $\Phi(\tau)$ ist eine Transposition, und wegen $p \mid |\Phi(\mathrm{Gal}(L|\mathbb{Q}))|$ enthält $\Phi(\mathrm{Gal}(L|\mathbb{Q}))$ ein Element der Ordnung p. Nach 21.5 ist $\Phi(\mathrm{Gal}(L|\mathbb{Q})) = \mathrm{Sym}(\{\alpha_1, \ldots, \alpha_p\}) \cong \mathrm{Sym}(p)$. Nach 7.3 ist $\mathrm{Sym}(p)$ für $p \geq 5$ nicht auflösbar.

Beispiel: $f := X^5 - 4X + 2$ ist nach Eisenstein irreduzibel in $\mathbf{Z}[X]$ und $\mathbb{Q}[X]$. Kurvendiskussion zeigt, daß f genau 3 reelle Nullstellen hat. Nach 21.6 ist $\mathrm{Gal}(f|\mathbb{Q}) \cong \mathrm{Sym}(5)$; insbesondere ist f nicht durch Radikale auflösbar.

Kapitel 22

Norm und Spur

Bemerkung 22.1 Sei $L|K$ eine endliche Körpererweiterung und $a \in L$. Dann ist die Abbildung $\mu_a : L \to L,\ x \mapsto ax$ K-linear. Wir setzen $N_K^L(a) := \det(\mu_a) \in K$ und $T_K^L(a) := \mathrm{spur}(\mu_a) \in K$ und nennen $N_K^L(a)$ und $T_K^L(a)$ die *Norm* bzw. die *Spur* (trace) von a in $L|K$. Wählt man eine K-Basis $b_1, \ldots, b_n$ von L und schreibt man $ab_j = \sum_{i=1}^n a_{ij} b_i$ mit $a_{ij} \in K$ für $i, j = 1, \ldots, n$, so ist also $N_K^L(a) = \det(a_{ij})$ und $T_K^L(a) = \sum_{i=1}^n a_{ii}$.

Satz:

(i) Für $a, b \in L$ ist $T_K^L(a+b) = T_K^L(a) + T_K^L(b),\ N_K^L(ab) = N_K^L(a) N_K^L(b)$.

(ii) Für $a \in K,\ b \in L$ ist $T_K^L(ab) = a T_K^L(b),\ N_K^L(ab) = a^{[L:K]} N_K^L(b)$.

(iii) $T_K^L(0) = 0,\ T_K^L(1) = [L:K]1,\ N_K^L(0) = 0,\ N_K^L(1) = 1$.

Beweis: Übung.

Beispiel: Für $z = u + iv \in \mathbb{C}$ mit $u, v \in \mathbb{R}$ ist $z1 = u + iv,\ zi = -v + iu$, also $T_{\mathbb{R}}^{\mathbb{C}}(z) = \mathrm{spur}\left(\begin{smallmatrix} u & -v \\ v & u \end{smallmatrix}\right) = 2u = 2\mathrm{Re}(z)$ und $N_{\mathbb{R}}^{\mathbb{C}}(z) = \det\left(\begin{smallmatrix} u & -v \\ v & u \end{smallmatrix}\right) = u^2 + v^2 = z\bar{z} = |z|^2$.

Satz 22.2 *Sei $L|K$ endliche Körpererweiterung, V endlichdimensionaler L-Vektorraum, und $f : V \to V$ L-linear. Dann ist V auch ein K-Vektorraum der Dimension $[L:K]\dim_L V$, die Abbildung f ist auch K-linear, und mit offensichtlicher Notation gilt:*

$$\mathrm{spur}_K(f) = T_K^L(\mathrm{spur}_L(f)) \quad \textit{und} \quad \det{}_K(f) = N_K^L(\det{}_L(f)).$$

Beweis: Offenbar ist V auch K-Vektorraum. Sei $v_1, \ldots, v_n$ eine L-Basis von V und $b_1, \ldots, b_m$ eine K-Basis von L. Wie beim Gradsatz beweist man, daß die Elemente $b_i v_j$ $(i = 1, \ldots, m,\ j = 1, \ldots, n)$ eine K-Basis von V bilden. Wir schreiben $f(v_s) = \sum_{r=1}^n \beta_{rs} v_r$ mit $\beta_{rs} \in L$ für $r, s = 1, \ldots, n$ und $\beta_{rs} b_j = \sum_{i=1}^m \alpha_{rsij} b_i$ mit $\alpha_{rsij} \in K$ für $r, s = 1, \ldots, n,\ i, j = 1, \ldots, m$. Dann ist

$$f(b_j v_s) = b_j f(v_s) = \sum_{r=1}^n \beta_{rs} b_j v_r = \sum_{r=1}^n \sum_{i=1}^m \alpha_{rsij} b_i v_r$$

für $s = 1, \ldots, n,\ j = 1, \ldots, m$. Folglich ist

$$\mathrm{spur}_K(f) = \sum_{r=1}^m \sum_{i=1}^m \alpha_{rrii} = \sum_{r=1}^n T_K^L(\beta_{rr}) = T_K^L\left(\sum_{r=1}^m \beta_{rr}\right) = T_K^L(\mathrm{spur}_L(f)).$$

Beim Beweis von $\det_K(f) = N_K^L(\det_L(f))$ können wir annehmen, daß f bijektiv ist; denn sonst verschwinden beide Determinanten. Aus der Linearen Algebra ist bekannt, daß sich jede invertierbare Matrix als Produkt von Matrizen der folgenden Form schreiben läßt:

$$\begin{pmatrix} 1 & & & & \\ & \ddots & & & \\ & & \ddots & & \\ & & & \ddots & \\ & & & & \ddots \\ & & & & & 1 \end{pmatrix} + \begin{array}{c} \begin{pmatrix} & & & 0 & & & \\ & & & \vdots & & & \\ & & & 0 & & & \\ 0 & \cdots & 0 & \alpha & 0 & \cdots & 0 \\ & & & 0 & & & \\ & & & \vdots & & & \\ & & & 0 & & & \end{pmatrix} \\ \uparrow \\ i \end{array} \begin{array}{l} \\ \\ \\ \leftarrow j \\ \\ \\ \\ \\ \end{array}$$

Daher ist f Produkt von linearen Abbildungen $g_{ij\alpha}$, die v_i auf $v_i+\alpha v_j$ und v_k für $k \neq i$ auf v_k abbilden. Wegen der Multiplikativität von Determinante und Norm kann man also annehmen, daß f selbst von dieser Form ist. Im Fall $i \neq j$ ist $f - \mathrm{id}_V$ nilpotent, also triangularisierbar mit Nullen auf der Hauptdiagonale (über K und L). Daher ist f triangularisierbar mit Einsen auf der Hauptdiagonale (über K und L). Folglich ist $\det_K(f) = 1 = N_K^L(1) = N_K^L(\det_L(f))$. Es bleibt also nur noch der Fall $i = j$ zu betrachten. Nach Umnumerierung der Basiselemente können wir annehmen: $f(v_1) = \beta v_1, f(v_2) = v_2, \ldots, f(v_n) = v_n$, wobei $\beta \in L$ fest. Schreibt man $b_j\beta = \sum_{i=1}^m \alpha_{ij} b_i$ mit $\alpha_{ij} \in K$ für $i, j = 1, \ldots, m$, so ist also

$$\begin{aligned} f(b_j v_1) &= b_j f(v_1) = b_j \beta v_1 = \sum_{i=1}^m \alpha_{ij} b_i v_1 \qquad \text{und} \\ f(b_j v_i) &= b_j f(v_i) = b_j v_i \end{aligned}$$

für $i = 2, \ldots, n,\ j = 1, \ldots, m$. Daher hat die Matrix von f bzgl. $b_j v_i$ $(i = 1, \ldots, n,\ j = 1, \ldots, m)$ die Form

$$\begin{pmatrix} A & & & \\ & E & & \\ & & \ddots & \\ & & & E \end{pmatrix};$$

dabei ist $A = (\alpha_{ij})$ die Matrix von μ_β bzgl. $b_1, \ldots, b_m$. Also ist $\det_K(f) = \det(A) = \det(\mu_\beta) = N_K^L(\beta) = N_K^L(\det_L(f))$.

Satz 22.3 *Für endliche Körpererweiterungen $M|L|K$ ist $T_K^M = T_K^L \circ T_L^M$ und $N_K^M = N_K^L \circ N_L^M$.*

Beweis: 22.2 mit $V = M$ und $f = \mu_a$ für $a \in M$.

Satz 22.4 *Sei $L|K$ endliche Körpererweiterung und $a \in L$ mit $m_{K,a} = X^n + a_{n-1}X^{n-1} + \ldots + a_1X + a_0$, wobei $a_0, \ldots, a_{n-1} \in K$. Dann ist*

$$T_K^L(a) = -[L : K(a)]a_{n-1} \quad \textit{und} \quad N_K^L(a) = (-1)^{[L:K]} a_0^{[L:K(a)]}.$$

Beweis: Die Elemente $1, a, \ldots, a^{n-1}$ bilden eine K-Basis des Teilkörpers $K(a)$ von L. Die Matrix von $\mu_a : K(a) \to K(a),\ x \mapsto ax$ bzgl. dieser Basis hat die Form

$$\begin{pmatrix} 0 & & & & -a_0 \\ 1 & \ddots & & & -a_1 \\ & \ddots & \ddots & & \vdots \\ & & \ddots & 0 & \vdots \\ & & & 1 & -a_{n-1} \end{pmatrix}.$$

Daher ist $T_K^{K(a)}(a) = \mathrm{spur}(\mu_a) = -a_{n-1}$ und $N_K^{K(a)} = \det(\mu_a) = (-1)^n a_0$. Nach 22.1 und 22.3 ist also

$$\begin{aligned} T_K^L(a) &= T_K^{K(a)}(T_{K(a)}^L(a)) = T_K^{K(a)}([L:K(a)]a) = \\ &= [L:K(a)]T_K^{K(a)}(a) = -[L:K(a)]a_{n-1}, \\ N_K^L(a) &= N_K^{K(a)}(N_{K(a)}^L(a)) = N_K^{K(a)}(a^{[L:K(a)]}) = \\ &= N_K^{K(a)}(a)^{[L:K(a)]} = (-1)^{[L:K]}a_0^{[L:K(a)]}. \end{aligned}$$

Bemerkung: Ist M Zerfällungskörper von $m_{K,a}$ über L und $m_{K,a} = (X-b_1)\dots(X-b_n)$ mit $b_1,\dots,b_n \in M$, so ist $a_0 = (-1)^n b_1 \dots b_n$ und $a_{n-1} = -b_1 - \dots - b_n$. Daher ist $T_K^L(a) = [L:K(a)](b_1 + \dots + b_n)$ und $N_K^L(a) = (b_1 \dots b_n)^{[L:K(a)]}$.

Satz 22.5 *Seien $L|K$ eine endliche separable Körpererweiterung, $M|K$ eine endliche normale Körpererweiterung mit $L \subseteq M$, $\sigma_1,\dots,\sigma_n$ die K-Homomorphismen $L \to M$ und $a \in L$. Dann ist*

$$T_K^L(a) = \sigma_1(a) + \dots + \sigma_n(a) \quad \textit{und} \quad N_K^L(a) = \sigma_1(a)\dots\sigma_n(a).$$

Beweis: Da $m_{K,a}(a) = 0$ und $M|K$ normal ist, existieren $b_1 = a, b_2, \dots, b_m \in M$ mit $m_{K,a} = (X-b_1)\dots(X-b_m)$. Für $i = 1,\dots,m$ existiert also genau ein K-Homomorphismus $\tau_i : K(a) \to M$ mit $\tau_i(a) = b_i$, und $\tau_1,\dots,\tau_m$ sind die einzigen K-Homomorphismen $K(a) \to M$. Da $L|K(a)$ auch separabel ist, existiert ein $b \in L$ mit $L = K(a,b)$. Da $m_{K(a),b}(b) = 0$ und $M|K(a)$ normal ist, zerfällt $m_{K(a),b}$ in $M[X]$ in Linearfaktoren. Da b separabel über $K(a)$ ist, hat $m_{K(a),b}$ genau $l := [L:K(a)]$ verschiedene Nullstellen in M. Nach 16.2 besitzt τ_i für $i = 1,\dots,m$ genau l Fortsetzungen zu K-Homomorphismen $\tau_{ij} : L \to M$ $(j = 1,\dots,l)$. Nach 18.3 ist $\{\sigma_1,\dots,\sigma_n\} = \{\tau_{ij} : i = 1,\dots,m,\ j = 1,\dots,l\}$. Nach 22.4 ist also

$$\sigma_1(a) + \dots + \sigma_n(a) = \sum_{i=1}^m \sum_{j=1}^l \tau_{ij}(a) = l\sum_{i=1}^m \tau_i(a) = [L:K(a)](b_1 + \dots + b_m) = T_K^L(a).$$

Analog für $N_K^L(a)$.

Bemerkung: Für eine endliche Galoiserweiterung $L|K$ mit Galoisgruppe G und für $a \in L$ ist also

$$T_K^L(a) = \sum_{\sigma \in G} \sigma(a) \quad \text{und} \quad N_K^L(a) = \prod_{\sigma \in G} \sigma(a).$$

Satz 22.6 *Für eine endliche Körpererweiterung $L|K$ gilt: $L|K$ separabel $\Leftrightarrow$ $T_K^L \neq 0$ $\Leftrightarrow$ T_K^L surjektiv.*

Beweis: Ist $L|K$ separabel, so existiert eine endliche normale Körpererweiterung $M|K$ mit $L \subseteq M$. Da die verschiedenen K-Homomorphismen $\sigma_1,\dots,\sigma_n : L \to M$ linear unabhängig sind, existiert ein $a \in L$ mit $0 \neq \sigma_1(a) + \dots + \sigma_n(a) = T_K^L(a)$.
Ist $T_K^L \neq 0$, so ist T_K^L surjektiv, da $T_K^L : L \to K$ K-linear ist. Ist umgekehrt T_K^L surjektiv, so ist natürlich $T_K^L \neq 0$.
Sei nun $T_K^L \neq 0$. Wir wollen zeigen, daß $L|K$ separabel ist. Wegen der Transitivität von Separabilität und Spur können wir annehmen, daß zwischen K und L keine weiteren Teilkörper liegen. Ferner sei $p := \mathrm{char}(K) \neq 0$; denn sonst ist nichts zu zeigen. Für $a \in L \setminus K$ ist dann $L = K(a)$. Ist a inseparabel über K, so ist $K(a^p)$ nach 17.9 ein echter Teilkörper von $K(a) = L$, also $K(a^p) = K$ und damit $a^p \in K$. Folglich ist $X^p - a^p \in K[X]$ mit Nullstelle a, d.h. $m_{K,a} \mid X^p - a^p$. Andrerseits ist $m_{K,a}$ inseparabel über K, also $m'_{K,a} = 0$ und damit $m_{K,a} = g(X^p)$ für ein $g \in K[X]$; insbesondere ist $\deg(m_{K,a}) \geq p$, also $m_{K,a} = X^p - a^p$. Nach 22.4 ist also $T_K^L(a) = 0$. Für $b \in K$ ist außerdem $T_K^L(b) = [L:K]b = pb = 0$. Es gibt also ein Element $c \in L \setminus K$, das separabel über K ist. Wegen $L = K(c)$ ist also $L|K$ separabel.

Satz 22.7 (Hilberts Satz 90) *Für eine endliche Galoiserweiterung $L|K$ mit zyklischer Galoisgruppe $G = \langle\sigma\rangle$ und für $x \in L$ gilt:*

(i) $T_K^L(x) = 0 \;\Leftrightarrow\; \exists y \in L : x = \sigma(y) - y$.

(ii) $N_K^L(x) = 1 \;\Leftrightarrow\; \exists y \in L : x = \sigma(y)/y$.

Beweis:

$\Leftarrow$: Für $y \in L$ ist $T_K^L(\sigma(y)) = \sum_{\sigma\in G} \tau(\sigma(y)) = \sum_{\rho\in G} \rho(y) = T_K^L(y)$ und $N_K^L(\sigma(y)) = \prod_{\sigma\in G} \tau(\sigma(y)) = \prod_{\rho\in G} \rho(y) = N_K^L(y)$.

$\Rightarrow$: (i) Da $L|K$ separabel ist, existiert nach 22.6 ein $z \in L$ mit $T_K^L(z) = -1$. Sei $x \in L$ mit $T_K^L(x) = 0$. Für $n := [L:K]$ und $y := x\sigma(z) + (x+\sigma(x))\sigma^2(z) + \ldots + (x + \sigma(x) + \ldots + \sigma^{n-2}(x))\sigma^{n-1}(z)$ gilt also:

$$\begin{aligned} y - \sigma(y) &= \\ &= x\sigma(z) + x\sigma^2(z) + \ldots + x\sigma^{n-1}(z) - \underbrace{(\sigma(x) + \sigma^2(x) + \ldots + \sigma^{n-1}(x))}_{\underbrace{T_K^L(x)}_{=0} - x}\underbrace{\sigma^n(z)}_{z} = \\ &= x(z + \sigma(z) + \ldots + \sigma^{n-1}(z)) \;=\; xT_K^L(z) \;=\; -x. \end{aligned}$$

(ii) Setzt man $n := [L:K] = |G|$, so sind $\mathrm{id}_L, \sigma, \ldots, \sigma^{n-1}$ linear unabhängig über L; insbesondere ist $\varphi := \mathrm{id}_L + x\sigma + x\sigma(x)\sigma^2 + \ldots + x\sigma(x)\ldots\sigma^{n-2}(x)\sigma^{n-1} \neq 0$. Wählt man $z \in L$ mit $\varphi(z) \neq 0$, so ist

$$\begin{aligned} x\sigma(\varphi(z)) &= x\sigma(z) + x\sigma(x)\sigma^2(z) + \ldots + \underbrace{x\sigma(x)\ldots\sigma^{n-1}(x)}_{N_K^L(x)=1}\underbrace{\sigma^n(z)}_{z} = \\ &= \varphi(z). \end{aligned}$$

Setze $y := \varphi(z)^{-1}$.

Satz 22.8 *Für jede Erweiterung $L|K$ endlicher Körper ist N_K^L surjektiv.*

Beweis: Sei $q := |K|$, $n := [L:K]$ und $x \in L$ mit $L^\times = \langle x\rangle$. Dann haben x die Ordnung $q^n - 1$ und

$$N_K^L(x) = xx^q x^{q^2}\ldots x^{q^{n-1}} = x^{1+q+q^2+\ldots+q^{n-1}} = x^{(q^n-1)/(q-1)}$$

die Ordnung $q-1$. Daher ist $K^\times = \langle N_K^L(x)\rangle \subseteq N_K^L(L^\times)$.

Kapitel 23

Zorns Lemma und Anwendungen

Definition 23.1 *Eine Relation $\leq$ auf einer Menge M, die* reflexiv *(d.h. $a \leq a$ für alle $a \in M$),* antisymmetrisch *(d.h. $a \leq b \ \wedge \ b \leq a \ \Rightarrow \ a = b$) und* transitiv *(d.h. $a \leq b \ \wedge \ b \leq c \ \Rightarrow \ a \leq c$) ist, nennt man* Ordnungsrelation. *Das Paar $(M, \leq)$ oder auch M selbst nennt man dann eine* (partiell) geordnete Menge.

Beispiel:

(i) $\leq$ auf $\mathbb{R}$.

(ii) $\subseteq$ auf $\mathcal{P}(X)$ für jede Menge X.

(iii) Teilbarkeit auf $\mathbb{N}$.

Definition 23.2 *Sei $(M, \leq)$ eine geordnete Menge und $N \subseteq M$.*

(i) Eine obere Schranke *von N in M ist ein Element $s \in M$ mit $n \leq s$ für alle $n \in N$.*

(ii) Ein maximales Element *in N ist ein Element $x \in N$, für das gilt: $y \in N \ \wedge \ x \leq y \ \Rightarrow x = y$.*

(iii) Ein größtes Element *in N ist ein Element $x \in N$ mit $y \leq x$ für alle $y \in N$.*

(iv) Analog definiert man untere Schranken, minimale *und* kleinste Elemente.

(v) Man nennt N total geordnet *oder* Kette *in M, falls je zwei Elemente $x, y \in N$* vergleichbar *(d.h. $x \leq y \ \vee \ y \leq x$) sind.*

Bemerkung: Weder obere Schranken noch maximale Elemente noch größte Elemente brauchen zu existieren. Größte Elemente sind eindeutig, maximale Elemente i.a. jedoch nicht.

Satz 23.3 (Zorns Lemma) *Sei $(M, \leq)$ eine nichtleere geordnete Menge. Besitzt jede (nichtleere) total geordnete Teilmenge von M eine obere Schranke in M, so besitzt M ein maximales Element.*

Bemerkung: Zorns Lemma ist ein Axiom der Mengenlehre. Wir werden es daher nicht beweisen. Man kann zeigen, daß es zu jedem der beiden folgenden Axiome äquivalent ist.

Auswahlaxiom: Ist $\mathcal{M}$ eine Menge von nichtleeren Mengen, so existiert eine Abbildung

$$f : \mathcal{M} \to \bigcup_{M \in \mathcal{M}} M$$

mit $f(M) \in M$ für alle $M \in \mathcal{M}$.

Wohlordnungsaxiom: Auf jeder Menge M existiert eine Ordnungsrelation $\leq$ mit der Eigenschaft, daß jede nichtleere Teilmenge von M ein kleinstes Element besitzt.

Satz 23.4 *Gegeben seien ein Körper K, ein K-Vektorraum V, eine Teilmenge E von V, die V aufspannt, und eine linear unabhängige Teilmenge U von E. Dann existiert eine Basis B von V mit $U \subseteq B \subseteq E$.*

Beweis: $\mathcal{M} := \{M \subseteq E : U \subseteq M,\ M \text{ linear unabhängig}\}$ ist wegen $U \in \mathcal{M}$ nichtleer und durch $\subseteq$ geordnet. Ist $\mathcal{N}$ eine nichtleere total geordnete Teilmenge von $\mathcal{M}$, so ist $U \subseteq S := \bigcup_{N \in \mathcal{N}} N \subseteq E$. Sind $s_1, \ldots, s_n \in S$, und $\alpha_1, \ldots, \alpha_n \in K$ mit $\alpha_1 s_1 + \ldots + \alpha_n s_n = 0$, so wähle man für $i = 1, \ldots, n$ ein $N_i \in \mathcal{N}$ mit $s_i \in N_i$. Da $\mathcal{N}$ total geordnet ist, existiert ein $j \in \{1, \ldots, n\}$ mit $N_i \subseteq N_j$ für $i = 1, \ldots, n$; insbesondere sind $s_1, \ldots, s_n \in N_j$. Da N_j linear unabhängig ist, folgt $\alpha_1 = \ldots = \alpha_n = 0$. Dies zeigt, daß S linear unabhängig ist. Daher ist $S \in \mathcal{M}$, und S ist obere Schranke von $\mathcal{N}$. Nach Zorn enthält also $\mathcal{M}$ ein maximales Element B. Wegen $B \in \mathcal{M}$ ist B linear unabhängig mit $U \subseteq B \subseteq E$. Wäre B keine Basis von V, so könnte man ein Element $v \in V \setminus \mathrm{Span}(B)$ finden; o.B.d.A. $v \in E$. Dann wäre aber $B \cup \{v\} \in \mathcal{M}$ im Widerspruch zur Maximalität von B.

Bemerkung: Nach 23.4 besitzt also insbesondere jeder Vektorraum eine Basis (setze $U := \emptyset,\ E := V$). Man kann auch zeigen, daß je zwei Basen eines Vektorraums die gleiche Anzahl von Elementen enthalten, braucht dazu jedoch wieder mehr Kenntnisse aus der Mengenlehre.

Satz 23.5 *Zu jedem Ring R und jedem echten Ideal I von R existiert ein maximales Ideal M in R mit $I \subseteq M$.*

Beweis: Die Menge $\mathcal{M}$ aller Ideale J von R mit $I \subseteq J \subsetneqq R$ ist wegen $I \in \mathcal{M}$ nichtleer und durch $\subseteq$ geordnet. Sei $\mathcal{N}$ eine nichtleere total geordnete Teilmenge von $\mathcal{M}$ und $K := \bigcup_{N \in \mathcal{N}} N$. Dann ist $I \subseteq K$; insbesondere ist $0 \in K$. Sind $k, k' \in K$, so wähle man $N, N' \in \mathcal{N}$ mit $k \in N,\ k' \in N'$. Da $\mathcal{N}$ total geordnet ist, ist $N \subseteq N'$ oder $N' \subseteq N$, o.B.d.A. $N \subseteq N'$. Dann ist $k, k' \in N$, also auch $k \pm k' \in N \subseteq K$. Analog ist $rk, kr \in K$ für $r \in R$. Folglich ist K Ideal in R. Für $J \in \mathcal{M}$ ist $1 \notin J$. Daher ist $1 \notin K$, also $K \neq R$. Folglich ist $K \in \mathcal{M}$, und K ist obere Schranke von $\mathcal{N}$. Nach Zorn enthält $\mathcal{M}$ ein maximales Element M. Offenbar ist $I \subseteq M \subsetneqq R$. Ist L ein Ideal in R mit $M \subsetneqq L$, so ist $L \notin \mathcal{M}$ wegen der Maximalität von M, also $L = R$ wegen $I \subseteq M \subseteq L$. Dies zeigt, daß M ein maximales Ideal in R ist.

Bemerkung: In jedem Ring $R \neq 0$ existiert also ein maximales Ideal (setze $I := 0$).

Satz 23.6 *Zu jedem Körper K existiert eine algebraische Körpererweiterung $L|K$, in der jedes Polynom $f \in K[X] \setminus K$ eine Nullstelle hat.*

Beweis: Für jedes $f \in K[X] \setminus K$ sei X_f eine Unbestimmte über K. Ferner sei I das von allen Polynomen $f(X_f)$ erzeugte Ideal im Polynomring $R := K[X_f : f \in K[X] \setminus K]$.
Annahme: $I = R$. Dann existieren $f_1, \ldots, f_n \in K[X] \setminus K,\ g_1, \ldots, g_n \in R$ mit $1 = g_1 f_1(X_{f_1}) + \ldots + g_n f_n(X_{f_n})$. Sei Z Zerfällungskörper von $f_1 \ldots f_n$ über K und $z_i \in Z$ mit $f_i(z_i) = 0$ für $i = 1, \ldots, n$. Einsetzen von z_i für X_{f_i} in obige Gleichung liefert den Widerspruch $1 = 0$.
Also ist $I \neq R$. Nach 23.5 existiert ein maximales Ideal M in R mit $I \subseteq M$. Folglich ist $L := R/M$ Körper, und die Abbildung $\varphi : K \to L,\ a \mapsto a + M$ ist ein Homomorphismus mit $\varphi(1) = 1$; insbesondere ist φ injektiv. Wir können also K mit $\varphi(K)$ identifizieren und so als Teilkörper von L auffassen. Für $f \in K[X] \setminus K$ und $x_f := X_f + M$ gilt dann:

$$f(x_f) = f(X_f + M) = \underbrace{f(X_f)}_{\in I \subseteq M} + M = 0.$$

Daher ist x_f algebraisch über K. Wegen

$$L = K[X_f : f \in K[X] \setminus K] \,/\, M = K[x_f : f \in K[X] \setminus K] = K(x_f : f \in K[X] \setminus K)$$

ist also $L|K$ algebraisch.

Satz 23.7 *Zu jedem Körper K existiert eine algebraische Körpererweiterung $M|K$, so daß M algebraisch abgeschlossen ist.*

Definition: *Man nennt jedes solche M einen* algebraischen Abschluß *von K.*

Beispiel: $\mathbb{C}$ ist algebraischer Abschluß von $\mathbb{R}$.

Beweis: Nach 23.6 existiert eine algebraische Körperweiterung $L_1|K$, in der jedes Polynom $f \in K[X]\setminus K$ eine Nullstelle hat. Analog existiert eine algebraische Körperweiterung $L_2|L_1$, in der jedes Polynom $f \in L_1[X]\setminus L_1$ eine Nullstelle hat. Fahrt man so fort, so erhält man Körper $K = L_0 \subseteq L_1 \subseteq L_2 \subseteq \ldots$ mit der Eigenschaft, daß L_i/L_{i-1} für $i \in \mathbb{N}$ algebraisch ist. Es ist leicht zu sehen, daß $M := \bigcup_{i\in\mathbb{N}} L_i$ ein Körper ist, dessen Elemente alle algebraisch über K sind. Sei nun $f \in M[X]\setminus M$ und $f = a_nX^n + a_{n-1}X^{n-1} + \ldots + a_1X + a_0$ mit $a_0, \ldots, a_n \in M$. Für $i = 0, \ldots, n$ existieren $j_i \in \mathbb{N}_0$ mit $a_i \in L_{j_i}$. Setzt man $j := \max\{j_0, \ldots, j_n\}$, so sind $a_0, \ldots, a_n \in L_j,\ f \in L_j[X]\setminus L_j$. Daher besitzt f eine Nullstelle in $L_{j+1} \subseteq M$. Dies zeigt, daß M algebraisch abgeschlossen ist.

Satz 23.8 *Sei $L|K$ eine algebraische Körpererweiterung und M ein algebraisch abgeschlossener Körper. Dann läßt sich jeder Monomorphismus $\sigma : K \to M$ zu einem Monomorphismus $\tau : L \to M$ fortsetzen.*

Beweis: Sei σ gegeben und $\mathcal{M} := \{(F,\rho) : F \text{ Körper},\ K \subseteq F \subseteq L,\ \rho : F \to M$ Monomorphismus, $\rho|K = \sigma\}$. Wegen $(K,\sigma) \in \mathcal{M}$ ist $\mathcal{M} \neq \emptyset$. Wir definieren eine Ordnungsrelation $\leq$ auf $\mathcal{M}$ durch:

$$(F,\rho) \leq (F',\rho') \;:\Leftrightarrow\; F \subseteq F' \;\wedge\; \rho'|F = \rho.$$

Ist $\mathcal{N}$ eine nichtleere total geordnete Teilmenge von $\mathcal{M}$, so ist $S := \bigcup_{(N,\rho)\in\mathcal{N}} N$ ein Teilkörper von L mit $K \subseteq S$, und es existiert genau eine Abbildung $\omega : S \to M$ mit $\omega|N = \rho$ für alle $(N,\rho) \in \mathcal{N}$. Ferner ist $(S,\omega) \in \mathcal{M}$, und (S,ω) ist obere Schranke von $\mathcal{N}$. Nach Zorn enthält also $\mathcal{M}$ ein maximales Element (E,ε).
Annahme: $E \neq L$. Sei $a \in L\setminus E$ und $m_{E,a} = \sum_{i=0}^n \alpha_i X^i$ mit $\alpha_0, \ldots, \alpha_n \in E$ ($L|E$ ist algebraisch!). Da M algebraisch abgeschlossen ist, existiert eine Nullstelle $\tilde{a} \in M$ von $\sum_{i=0}^n \varepsilon(\alpha_i)X^i$. Nach 16.2 kann man ε zu einem Monomorphismus $\zeta : E(a) \to M$ fortsetzen. Dann ist aber $(E(a),\zeta) \in \mathcal{M}$ im Widerspruch zur Maximalität von (E,ε).

Satz 23.9 *Je zwei algebraische Abschlüsse M, M' eines Körpers K sind K-isomorph.*

Bemerkung: Daher spricht man auch von *dem* algebraischen Abschluß eines Körpers.

Beweis: Sind K, M, M' gegeben, so läßt sich id_K nach 23.8 zu einem Monomorphismus $\varphi : M \to M'$ fortsetzen. Offenbar ist $L := \varphi(M)$ ein algebraisch abgeschlossener Teilkörper von M', der K enthält. Für $a \in M'$ zerfällt also $m_{K,a}$ in $L[X]$ in Linearfaktoren, etwa $m_{K,a} = (X - b_1)\ldots(X - b_n)$ mit $b_1, \ldots, b_n \in L$. Folglich ist $a \in \{b_1, \ldots, b_n\} \subseteq L$. Dies zeigt $L = M'$, d.h. φ ist K-Isomorphismus.

Kapitel 24

Transzendenzbasen

Definition 24.1 *Sei $L|K$ Körperweiterung und $U \subseteq L$. Man nennt U* algebraisch unabhängig *über K, falls jedes $a \in U$ transzendent über $K(U \setminus \{a\})$ ist. Andernfalls nennt man U* algebraisch abhängig *über K.*

Bemerkung: Eine Teilmenge A von L ist also genau dann algebraisch abhängig über K, wenn ein $a \in A$ und ein $f \in K(A \setminus \{a\})[X] \setminus \{0\}$ existieren mit $f(a) = 0$. In diesem Fall schreiben wir $f = \sum_{i=0}^{n} f_i X^i$ mit $f_0, \dots, f_n \in K(A \setminus \{a\})$. Für $i = 0, \dots, n$ ist f_i von der Form

$$f_i = \frac{g_i(a_{i1}, \dots, a_{ik_i})}{h_i(a_{i1}, \dots, a_{ik_i})}$$

mit Polynomen $g_i, h_i \in K[X_1, \dots, X_{k_i}]$ und Elementen $a_{i1}, \dots, a_{ik_i} \in A \setminus \{a\}$. Setzt man $A' := \bigcup_{i=0}^{n} \{a_{i1}, \dots, a_{ik_i}\}$, so ist also auch $A' \cup \{a\}$ algebraisch abhängig über K. Eine Teilmenge A von L ist also genau dann algebraisch abhängig über K, wenn A eine endliche über K algebraisch abhängige Teilmenge enthält. Daher ist eine Teilmenge U von L genau dann algebraisch unabhängig über K, wenn jede endliche Teilmenge von U über K algebraisch unabhängig ist.

Beispiel:

(i) $\emptyset$ ist algebraisch unabhängig über K.

(ii) $\{a\}$ algebraisch unabhängig über $K \Leftrightarrow a$ transzendent über K.

(iii) U algebraisch unabhängig über K und $V \subseteq U \Rightarrow V$ algebraisch unabhängig über K.

(iv) A algebraisch abhängig über K und $A \subseteq B \subseteq L \Rightarrow B$ algebraisch abhängig über K.

Satz 24.2 *Sei $L|K$ Körpererweiterung, und seien $a_1, \dots, a_n \in L$ paarweise verschieden. Genau dann ist $\{a_1, \dots, a_n\}$ algebraisch unabhängig über K, wenn gilt: Ist $f \in K[X_1, \dots, X_n]$ mit $f(a_1, \dots, a_n) = 0$, so ist $f = 0$.*

Beweis:

$\Rightarrow$: Sei $\{a_1, \dots, a_n\}$ algebraisch unabhängig über K und $f \in K[X_1, \dots, X_n]$ mit $f(a_1, \dots, a_n) = 0$. Wir schreiben $f = \sum_{i=0}^{m} g_i X_n^i$ mit $g_0, \dots, g_m \in K[X_1, \dots, X_{n-1}]$. Dann ist $0 = f(a_1, \dots, a_n) = \sum_{i=0}^{m} g_i(a_1, \dots, a_{n-1}) a_n^i$. Da a_n transzendent über $K(a_1, \dots, a_{n-1})$ ist, folgt $g_i(a_1, \dots, a_{n-1}) = 0$ für $i = 0, \dots, m$. Argumentiert man durch Induktion nach n, so kann man $g_i = 0$ für $i = 0, \dots, m$ voraussetzen. Man erhält also $f = 0$.

$\Leftarrow$: Sei $\{a_1, \dots, a_n\}$ algebraisch abhängig über K und $i \in \{1, \dots, n\}$, so daß a_i algebraisch über $K(a_1, \dots, a_{i-1}, a_{i+1}, \dots, a_n)$ ist, o.B.d.A. $i = n$. Es existiert also ein $f \in K(a_1, \dots, a_{n-1})[X] \setminus \{0\}$ mit $f(a_n) = 0$. Wir schreiben $f = \sum_{i=0}^{m} g_i X^i$ mit $g_0, \dots, g_m \in$

$K(a_1,\dots,a_{n-1})$, o.B.d.A. $g_0,\dots,g_m \in K[a_1,\dots,a_{n-1}]$. Für $i=0,\dots,m$ sei $h_i \in K[X_1,\dots,X_{n-1}]$ mit $g_i = h_i(a_1,\dots,a_{n-1})$. Dann ist $F := \sum_{i=0}^m h_i X_n^i \in K[X_1,\dots,X_n] \setminus \{0\}$ mit

$$F(a_1,\dots,a_n) = \sum_{i=0}^m \underbrace{h_i(a_1,\dots,a_{n-1})}_{=g_i} a_n^i = f(a_n) = 0.$$

Bemerkung: Ist $\{a_1,\dots,a_n\}$ algebraisch unabhängig über K, so liefert Einsetzen einen Isomorphismus $K[X_1,\dots,X_n] \to K[a_1,\dots,a_n]$. Dieser läßt sich zu einem Isomorphismus der Quotientenkörper fortsetzen: $K(X_1,\dots,X_n) \to K(a_1,\dots,a_n)$.

Definition 24.3 *Eine* Transzendenzbasis *der Körpererweiterung $L|K$ ist eine über K algebraisch unabhängige Teilmenge T von L mit der Eigenschaft, daß $L|K(T)$ algebraisch ist.*

Satz: *Sei $L|K$ Körperweiterung, E eine Teilmenge von L mit der Eigenschaft, daß $L|K(E)$ algebraisch ist, und U eine über K algebraisch unabhängige Teilmenge von E. Dann existiert eine Transzendenzbasis B von $L|K$ mit $U \subseteq B \subseteq E$.*

Beweis: $\mathcal{M} := \{M \subseteq E : U \subseteq M,\ M$ algebraisch unabhängig über $K\}$ ist nichtleer wegen $U \in \mathcal{M}$. Ferner ist $\mathcal{M}$ durch $\subseteq$ geordnet. Sei $\mathcal{N}$ eine nichtleere total geordnete Teilmenge von $\mathcal{M}$ und $S := \bigcup_{N\in\mathcal{N}} N$, also $U \subseteq S \subseteq E$.
Annahme: S algebraisch abhängig über K. Dann existiert eine endliche Teilmenge S' von S, die algebraisch abhängig über K ist. Da $\mathcal{N}$ total geordnet ist, existiert ein $N \in \mathcal{N}$ mit $S' \subseteq N$. Mit N ist aber auch S' algebraisch unabhängig über K. Widerspruch.
Folglich ist $S \in \mathcal{M}$, und S ist obere Schranke von $\mathcal{N}$. Nach Zorn enthält $\mathcal{M}$ ein maximales Element B; insbesondere ist B algebraisch unabhängig über K und $U \subseteq B \subseteq E$.
Annahme: $L|K(B)$ transzendent. Da $L|K(E)$ algebraisch ist, ist also $K(E)|K(B)$ transzendent. Folglich existiert ein über $K(B)$ transzendentes Element $e \in E$; insbesondere ist $e \notin B$. Wegen der Maximalität von B ist $B \cup \{e\} \notin \mathcal{M}$, d.h. $B \cup \{e\}$ ist algebraisch abhängig über K. Folglich existieren paarweise verschiedene $b_1,\dots,b_r \in B$, so daß $\{b_1,\dots,b_r,e\}$ algebraisch abhängig über K ist. Es existiert also ein $f \in K[X_1,\dots,X_r,Y] \setminus \{0\}$ mit $f(b_1,\dots,b_r,e) = 0$. Wir schreiben $f = \sum_{i=0}^m f_i Y^i$ mit $f_0,\dots,f_m \in K[X_1,\dots,X_r]$. Dann ist $0 = f(b_1,\dots,b_r,e) = \sum_{i=0}^m f_i(b_1,\dots,b_r)e^i$. Da e transzendent über $K(B)$ ist, folgt $f_i(b_1,\dots,b_r) = 0$ für $i = 0,\dots,m$. Da $\{b_1,\dots,b_r\}$ algebraisch unabhängig über K ist, ist also $f_i = 0$ für $i = 0,\dots,m$. Damit hat man den Widerspruch $f = 0$.

Bemerkung: Nach 24.3 besitzt jede Körpererweiterung $L|K$ eine Transzendenzbasis (setze $U := \emptyset,\ E := L$).

Satz 24.4 *Gegeben sei eine Körpererweiterung $L|K$ mit einer endlichen Transzendenzbasis B und eine über K algebraisch unabhängige Teilmenge C von L. Dann ist $|C| \le |B|$. Insbesondere hat also jede Transzendenzbasis von $L|K$ die gleiche Anzahl von Elementen wie B.*

Bemerkung: Dies gilt auch ohne Endlichkeitsvoraussetzung, erfordert zum Beweis jedoch mehr Mengenlehre.

Beweis: Sei $|B| = m,\ |C| = n,\ C = \{c_1,\dots,c_n\}$. Es genügt zu zeigen, daß für $k = 0,\dots,n$ Teilmengen $B_0,\dots,B_k$ von B mit folgenden Eigenschaften existieren:

(i) $B = B_0 \underset{\neq}{\supset} B_1 \underset{\neq}{\supset} \dots \underset{\neq}{\supset} B_k$.

(ii) $\{c_1,\dots,c_k\} \cup B_k$ ist Transzendenzbasis von $L|K$.

(iii) $\{c_1,\dots,c_k\} \cap B_k = \emptyset$.

Dies beweisen wir durch Induktion nach k. Der Fall $k = 0$ ist trivial. Seien also für ein $k \in \{0, \dots, n-1\}$ schon Teilmengen $B_0, \dots, B_k$ von B mit den gewünschten Eigenschaften gefunden. Wir wenden 24.3 an mit $U := \{c_1, \dots, c_{k+1}\}$ und $E := \{c_1, \dots, c_{k+1}\} \cup B_k$. Es existiert also eine Transzendenzbasis T von $L|K$ mit $U \subseteq T \subseteq E$. Für $B_{k+1} := T \setminus U$ ist dann $\{c_1, \dots, c_{k+1}\} \cap B_{k+1} = U \cap (T \setminus U) = \emptyset$ und $\{c_1, \dots, c_{k+1}\} \cup B_{k+1} = U \cup (T \setminus U) = T$ Transzendenzbasis von $L|K$. Ferner ist $B_{k+1} \subseteq E \setminus U \subseteq B_k$. Im Fall $B_{k+1} = B_k$ wäre auch $\{c_1, \dots, c_k\} \cup B_{k+1}$ Transzendenzbasis von $L|K$, also c_{k+1} algebraisch über $K(\{c_1, \dots, c_k\} \cup B_{k+1})$ im Widerspruch zur algebraischen Unabhängigkeit von $\{c_1, \dots, c_{k+1}\} \cup B_{k+1}$.

Definition: *In der obigen Situation nennt man* $|B|$ *den* Transzendenzgrad *von* $L|K$ *und schreibt* $\operatorname{trg}(L|K) = |B|$. *Hat* $L|K$ *keine endliche Transzendenzbasis, so schreiben wir* $\operatorname{trg}(L|K) = \infty$.

Satz 24.5 *Für Körpererweiterungen* $M|L|K$ *gilt:* $\operatorname{trg}(M|K) = \operatorname{trg}(M|L) + \operatorname{trg}(L|K)$.

Beweis: Seien B, C Transzendenzbasen von $L|K$ bzw. $M|L$. Es genügt zu zeigen, daß $B \cup C$ Transzendenzbasis von $M|K$ mit $B \cap C = \emptyset$ ist. Jedes $x \in C$ ist transzendent über L. Daher ist $x \notin L$, insbesondere $x \notin B$. Dies zeigt $B \cap C = \emptyset$. Nach Voraussetzung sind $M|L(C)$ und $L|K(B)$ algebraisch. Daher sind auch $L(C)|K(B \cup C)$ und $M|K(B \cup C)$ algebraisch. Nach 24.3 existiert also eine Transzendenzbasis T von $M|K$ mit $B \subseteq T \subseteq B \cup C$. Jedes Element in C ist dann algebraisch über $K(T)$ und über $L(T) = L(T \cap C)$. Da C algebraisch unabhängig über L ist, folgt $T \cap C = C$, also $T = B \cup C$.

Kapitel 25

Bewertungen

Definition 25.1 *Eine (multiplikative)* Bewertung *eines Körpers K ist eine Abbildung $\varphi : K \to \mathbb{R}$, so daß für $a, b \in K$ gilt:*

(i) $\varphi(a) \geq 0$.

(ii) $\varphi(a) = 0 \;\Leftrightarrow\; a = 0$.

(iii) $\varphi(ab) = \varphi(a)\varphi(b)$.

(iv) $\varphi(a+b) \leq \varphi(a) + \varphi(b)$. *(Dreiecksungleichung)*

Man nennt das Paar (K, φ) dann auch einen bewerteten Körper.

Beispiel:

(i) Der Absolutbetrag auf jedem Teilkörper von $\mathbb{C}$.

(ii) Für jeden Körper K die *triviale Bewertung*, definiert durch $\varphi(0) = 0$ und $\varphi(a) = 1$ für $a \neq 0$.

(iii) Sei R ein faktorieller Ring mit Quotientenkörper K und p ein Primelement in R. Dann kann man jedes $a \in K^\times$ in der Form $a = p^r \frac{b}{c}$ mit $r \in \mathbf{Z}$, $b, c \in R \setminus (p)$ schreiben, dabei ist r durch a eindeutig bestimmt. Wir schreiben $r = v_p(a)$ und setzen $v_p(0) := \infty$. Für $a, a' \in K$ ist dann $v_p(aa') = v_p(a) + v_p(a')$ und $v_p(a + a') \geq \min\{v_p(a), v_p(a')\}$. Wählt man also ein festes $\gamma \in \mathbb{R}$ mit $0 < \gamma < 1$ und definiert man $\varphi_p : K \to \mathbb{R}$ durch $\varphi(0) := 0$ und $\varphi_p(a) := \gamma^{v_p(a)}$ für $a \neq 0$, so ist φ_p eine Bewertung von K. Insbesondere erhält man auf diese Weise für jede Primzahl p eine Bewertung φ_p von $\mathbb{Q}$. In diesem Fall wählt man i.a. $\gamma = \frac{1}{p}$. Der Absolutbetrag ist eine weitere Bewertung φ_∞ von $\mathbb{Q}$.

Bemerkung:

(i) Ist $\varphi : K \to \mathbb{R}$ eine Bewertung, so ist $\varphi(1) = \varphi(1 \cdot 1) = \varphi(1)\varphi(1)$, also $\varphi(1) = 1$ wegen $\varphi(1) \neq 0$. Ist ζ eine n-te Einheitswurzel in K für ein $n \in \mathbb{N}$, so ist also $1 = \varphi(1) = \varphi(\zeta^n) = \varphi(\zeta)^n$, also $\varphi(\zeta) = 1$ wegen $\varphi(\zeta) > 0$. Daher besitzen endliche Körper nur die triviale Bewertung. Ferner ist stets $\varphi(-1) = 1$. Für $a \in K$ ist also $\varphi(-a) = \varphi(-1)\varphi(a) = \varphi(a)$.
Für $a, b \in K$ ist außerdem $\varphi(a) = \varphi(a-b+b) \leq \varphi(a-b) + \varphi(b)$, also $\varphi(a) - \varphi(b) \leq \varphi(a-b)$. Analog ist $\varphi(b) - \varphi(a) \leq \varphi(b-a) = \varphi(a-b)$. Insgesamt ist also $\varphi(a-b) \geq |\varphi(a) - \varphi(b)|$.

(ii) Jede Bewertung φ eines Körpers K definiert einen Homomorphismus $K^\times \to \mathbb{R}^\times$, $a \mapsto \varphi(a)$. Man nennt $\varphi(K^\times)$ die *Wertegruppe* von φ. Genau im Fall $\varphi(K^\times) = 1$ ist φ trivial. Ist $\varphi(K^\times)$ eine unendliche zyklische Gruppe (etwa im Fall $\varphi = \varphi_p$), so nennt man die Bewertung φ *diskret*.

(iii) Für jede Bewertung φ eines Körpers K ist die Abbildung $d : K \times K \to \mathbb{R},\ (a,b) \mapsto \varphi(a-b)$ eine Metrik auf K, d.h. für $a, b, c \in K$ gilt:

(α) $d(a,b) \geq 0$.

(β) $d(a,b) = 0 \Leftrightarrow a = b$.

(γ) $d(a,b) = d(b,a)$.

(δ) $d(a,c) \leq d(a,b) + d(b,c)$.

Damit stehen Grundbegriffe der Analysis zur Verfügung wie z.B. offene, abgeschlossene, kompakte Mengen, konvergente Folgen, Cauchy-Folgen, stetige Abbildungen, usw. Eine Folge $(x_n)_{n\in\mathbb{N}}$ in K, die bzgl. φ (d.h. bzgl. d) gegen 0 konvergiert, nennt man eine *Nullfolge*. Ein metrischer Raum heißt bekanntlich vollständig, falls in ihm jede Cauchy-Folge konvergiert. In unserem Fall spricht man dann von *vollständigen Bewertungen* bzw. von *vollständig bewerteten Körpern*.

Definition 25.2 *Zwei Bewertungen φ, φ' eines Körpers K nennt man äquivalent, wenn jede Nullfolge bzgl. φ auch eine bzgl. φ' ist und umgekehrt.*

Bemerkung: Dies liefert eine Äquivalenzrelation auf der Menge aller Bewertungen von K.

Beispiel:

(i) Verschiedene Wahlen der Konstanten γ in Beispiel 25.1 (ii) führen zu äquivalenten Bewertungen. Für nichtassoziierte Primelemente p, p' in einem faktoriellen Ring R sind φ_p und $\varphi_{p'}$ nicht äquivalent, denn $(p^n)_{n\in\mathbb{N}}$ ist eine Nullfolge bzgl. φ_p, aber nicht bzgl. $\varphi_{p'}$.

(ii) Auf $\mathbb{Q}$ sind φ_p und φ_∞ für jede Primzahl p nicht äquivalent, denn $(p^n)_{n\in\mathbb{N}}$ ist keine Nullfolge bzgl. φ_∞.

Satz: *Für nichttriviale Bewertungen φ, φ' eines Körpers K sind äquivalent:*

(1) φ äquivalent zu φ'.

(2) $a \in K \ \wedge\ \varphi(a) < 1 \ \Rightarrow\ \varphi'(a) < 1$.

(3) Es existiert ein $\rho \in \mathbb{R}$ mit $\rho > 0$ und $\varphi'(a) = \varphi(a)^\rho$ für $a \in K$.

Beweis:

(1)⇒(2): Sei (1) erfüllt und $a \in K$ mit $\varphi(a) < 1$. Dann ist $(a^n)_{n\in\mathbb{N}}$ eine Nullfolge bzgl. φ, also auch bzgl. φ'. Daher ist $\varphi'(a) < 1$.

(2)⇒(3): Sei (2) erfüllt. Ist $b \in K$ mit $\varphi(b) > 1$, so ist $\varphi(b^{-1}) = \varphi(b)^{-1} < 1$, also auch $\varphi'(b^{-1}) < 1$ und damit $\varphi'(b) > 1$. Da φ nichttrivial ist, existiert ein $c \in K$ mit $\varphi(c) > 1$. Wir schreiben $\varphi'(c) = \varphi(c)^\rho$ mit $\rho \in \mathbb{R},\ \rho > 0$. Ist $a \in K^\times$ beliebig, so existiert ein $\alpha \in \mathbb{R}$ mit $\varphi(a) = \varphi(c)^\alpha$. Für $m \in \mathbf{Z},\ n \in \mathbb{N}$ mit $\frac{m}{n} < \alpha$ ist dann $\varphi(a^n) = \varphi(a)^n = \varphi(c)^{\alpha n} > \varphi(c)^m = \varphi(c^m)$, also $\varphi(\frac{a^n}{c^m}) = \frac{\varphi(a^n)}{\varphi(c^m)} > 1$. Daher ist auch $\varphi'(\frac{a^n}{c^m}) > 1$, d.h. $\varphi'(a) > \varphi'(c)^{\frac{m}{n}}$. Da dies für beliebige m, n gilt, folgt $\varphi'(a) \geq \varphi'(c)^\alpha$. Analog zeigt man $\varphi'(a) \leq \varphi'(c)^\alpha$. Man erhält insgesamt $\varphi'(a) = \varphi'(c)^\alpha = \varphi(c)^{\rho\alpha} = \varphi(a)^\rho$.

(3)⇒(1): Trivial.

Satz 25.3 *Für eine nichttriviale Bewertung φ eines Körpers K sind äquivalent:*

(1) $\varphi(n1_K) \leq 1$ für $n \in \mathbb{N}$.

(2) $\exists c \in \mathbb{R}\ \forall n \in \mathbb{N} : \varphi(n1_K) \leq c$.

(3) Für $a, b \in K$ ist $\varphi(a+b) \leq \max\{\varphi(a), \varphi(b)\}$. (starke Dreiecksungleichung)

(4) Für jedes $\rho \in \mathbb{R}$ mit $\rho > 0$ ist φ^ρ Bewertung von K.

Definition: *Gegebenenfalls nennt man φ* nichtarchimedisch*, sonst* archimedisch.

Beispiel: Auf $\mathbb{Q}$ ist φ_∞ archimedisch, φ_p nichtarchimedisch für jede Primzahl p.

Beweis:

(1)⇒(2): Trivial.

(2)⇒(3): Sei (2) erfüllt, und seien $a, b \in K$. O.B.d.A. sei $\varphi(a) \geq \varphi(b)$. Für $m \in \mathbb{N}$ ist dann

$$\begin{aligned} \varphi(a+b)^m &= \varphi\left((a+b)^m\right) = \varphi\left(\sum_{i=0}^{m}\binom{m}{i}a^i b^{m-i}\right) \leq \\ &\leq \sum_{i=0}^{m}\varphi\left(\binom{m}{i}1_K\right)\varphi(a)^i\varphi(b)^{m-i} \leq \\ &\leq (m+1)c\,\varphi(a)^m, \end{aligned}$$

also

$$\varphi(a+b) \leq \sqrt[m]{m+1}\,\sqrt[m]{c}\,\varphi(a).$$

Da m beliebig ist, erhält man $\varphi(a+b) \leq \varphi(a) = \max\{\varphi(a), \varphi(b)\}$.

(3)⇒(4): Sei (3) erfüllt und $\rho \in \mathbb{R}$ mit $\rho > 0$. Für $a, b \in K$ ist dann $\varphi(a+b)^\rho \leq \max\{\varphi(a), \varphi(b)\}^\rho = \max\{\varphi(a)^\rho, \varphi(b)^\rho\} \leq \varphi(a)^\rho + \varphi(b)^\rho$. Die restlichen Eigenschaften sind klar.

(4)⇒(1): Sei (4) erfüllt. Für $m, n \in \mathbb{N}$ ist dann $\varphi^m(n1_K) \leq n\varphi^m(1_K) = n$, also $\varphi(n1_K) \leq \sqrt[m]{n}$. Da m beliebig ist, folgt $\varphi(n1_K) \leq 1$.

Satz 25.4 *Jede nichttriviale Bewertung φ von $\mathbb{Q}$ ist zu φ_∞ oder zu φ_p für eine Primzahl p äquivalent.*

Beweis:

(i) Sei φ nichtarchimedisch, also $\varphi(n) \leq 1$ für $n \in \mathbb{N}$. Da φ nichttrivial ist, existiert ein $n \in \mathbb{N}$ mit $\varphi(n) < 1$. Folglich ist $\{n \in \mathbb{N} : \varphi(n) < 1\}$ nichtleer, enthält also ein kleinstes Element p. Offenbar ist p Primzahl. Wir zeigen, daß φ zu φ_p äquivalent ist. Wir schreiben $\varphi(p) = (\frac{1}{p})^\rho$ mit $\rho \in \mathbb{R}$, $\rho > 0$. Ist $a \in \mathbf{Z}$ mit $\varphi(a) < 1$, so liefert die Division mit Rest $q, r \in \mathbf{Z}$ mit $a = qp + r$ und $0 \leq r < p$. Dann ist $\varphi(r) = \varphi(a - qp) \leq \max\{\varphi(a), \varphi(q)\varphi(p)\} < 1$, also $r = 0$ wegen der Minimalität von p. Folglich ist $p \mid a$. Ist $b \in \mathbf{Z}$ und $b = p^r b'$ mit $r \in \mathbb{N}_0$, $b' \in \mathbf{Z}$, $p \nmid b'$, so ist $\varphi(b') = 1$ und $\varphi(b) = \varphi(p)^r = (\frac{1}{p})^{\rho r} = \varphi_p(b)^\rho$.

(ii) Sei φ archimedisch, und seien $n, n' \in \mathbb{N}\setminus\{1\}$, $k \in \mathbb{N}_0$ mit $n^k \leq n' < n^{k+1}$. Dann ist $k\log n \leq \log n'$ und $k \leq \frac{\log n'}{\log n}$. Schreibt man $n' = \sum_{i=0}^{k} a_i n^i$ mit $a_0, \ldots, a_k \in \{0, 1, \ldots, n-1\}$, so ist

$$\begin{aligned} \varphi(n') &\leq \sum_{i=0}^{k}\varphi(a_i)\varphi(n)^i < (k+1)n\,\max\{1, \varphi(n)^k\} \leq \\ &\leq n\left(\frac{\log n'}{\log n} + 1\right)\max\{1, \varphi(n)^{\frac{\log n'}{\log n}}\}. \end{aligned}$$

Wendet man dies an mit $n' = (n'')^r$ für feste $n'', r \in \mathbb{N}_0$, $n'' \neq 1$, so erhält man:

$$\varphi(n'')^r \leq n\left(\frac{r\log n''}{\log n} + 1\right)\max\{1, \varphi(n)^{\frac{r\log n''}{\log n}}\},$$

also

$$\varphi(n'') \leq \sqrt[r]{n}\sqrt[r]{\frac{r\log n''}{\log n} + 1}\,\max\{1, \varphi(n)^{\frac{\log n''}{\log n}}\}.$$

Da dies für beliebige r gilt, folgt:

$$\varphi(n'') \ \leq \ \max\{1, \varphi(n)^{\frac{\log n''}{\log n}}\} \quad \text{für beliebige } n, n'' \in \mathbb{N} \setminus \{1\}.$$

Da φ archimedisch ist, existiert ein $n'' \in \mathbb{N}$ mit $\varphi(n'') > 1$, also $1 < \varphi(n'') \leq \varphi(n)^{\frac{\log n''}{\log n}}$ für $n \in \mathbb{N} \setminus \{1\}$. Insbesondere ist $\varphi(n) > 1$ für $n \in \mathbb{N} \setminus \{1\}$. Daher können wir die Rollen von n und n'' vertauschen und erhalten: $\varphi(n) \leq \varphi(n'')^{\frac{\log n}{\log n''}} \leq \varphi(n)$, also

$$\varphi(n)^{\frac{1}{\log n}} \ = \ \varphi(n'')^{\frac{1}{\log n''}}$$

und

$$\frac{\log \varphi(n)}{\log n} \ = \ \frac{\log \varphi(n'')}{\log n''} \quad \text{für } n, n'' \in \mathbb{N} \setminus \{1\}.$$

Mit $s := \frac{\log \varphi(2)}{\log 2}$ ist also $\frac{\log \varphi(n)}{\log n} = s$ für $n \in \mathbb{N} \setminus \{1\}$, also $\log \varphi(n) = s \log n = \log n^s$ und damit $\varphi(n) = n^s$ für $n \in \mathbb{N} \setminus \{1\}$. Daraus ergibt sich $\varphi(q) = |q|^s$ für $q \in \mathbb{Q}$.

Satz 25.5 *Für jede nichtarchimedische Bewertung φ eines Körpers K gilt:*

(i) $a, b \in K \ \wedge \ \varphi(a) \neq \varphi(b) \ \Rightarrow \ \varphi(a+b) = \max\{\varphi(a), \varphi(b)\}$.

(ii) $R := \{a \in K : \varphi(a) \leq 1\}$ *ist Teilring von K.*

(iii) Für $a \in K \setminus R$ ist $\frac{1}{a} \in R$; insbesondere ist K (isomorph zum) Quotientenkörper von R.

(iv) $R^\times = \{a \in K : \varphi(a) = 1\}$.

(v) $M := \{a \in K : \varphi(a) < 1\}$ *ist das einzige maximale Ideal in R.*

(vi) Für $a, b \in R$ gilt: $a \mid b \ \Leftrightarrow \ \varphi(b) \leq \varphi(a)$.

(vii) Ist φ diskret, so ist R Hauptidealring.

Definition: *Man nennt R den* Bewertungsring, *M das* Bewertungsideal *und R/M den* Restklassenkörper *bzgl. φ.*

Beweis:

(i) Seien $a, b \in K$ mit $\varphi(a) \neq \varphi(b)$, o.B.d.A. $\varphi(b) < \varphi(a)$, also $\varphi(a+b) \leq \varphi(a)$. Im Fall $\varphi(a+b) < \varphi(a)$ wäre $\varphi(a) = \varphi(a+b-b) \leq \max\{\varphi(a+b), \varphi(b)\} < \varphi(a)$. Widerspruch.

(ii) Für $a, b \in R$ ist $\varphi(ab) = \underbrace{\varphi(a)}_{\leq 1}\underbrace{\varphi(b)}_{\leq 1} \leq 1$ und $\varphi(a \pm b) \leq \max\{\varphi(a), \varphi(b)\} \leq 1$. Außerdem ist $\varphi(0) = 0 \leq 1$ und $\varphi(1) = 1 \leq 1$.

(iii) $a \in K \setminus R \ \Rightarrow \ \varphi(a) > 1 \ \Rightarrow \ \varphi(a^{-1}) = \varphi(a)^{-1} < 1 \ \Rightarrow \ a^{-1} \in R$.

(iv) Für $a \in R \setminus \{0\}$ ist $\varphi(a) \leq 1$, also $\varphi(a^{-1}) \geq 1$. Daher gilt: $a \in R^\times \ \Leftrightarrow \ a^{-1} \in R \ \Leftrightarrow \ \varphi(a^{-1}) \leq 1 \ \Leftrightarrow \ \varphi(a^{-1}) = 1 \ \Leftrightarrow \ \varphi(a) = 1$.

(v) Analog zu (ii) zeigt man, daß M ein Ideal in R ist. Für jedes echte Ideal I von R ist aber $I \cap R^\times = \emptyset$, also $I \subseteq R \setminus R^\times = M$.

(vi) **$\Rightarrow$:** $a \mid b \ \Rightarrow \ \exists x \in R : b = ax \ \Rightarrow \ \varphi(b) = \varphi(a)\varphi(x) \leq \varphi(a)$.

$\Leftarrow$: Sei $\varphi(b) \leq \varphi(a)$, o.B.d.A. $b \neq 0$, also $a \neq 0$ und $\varphi(\frac{b}{a}) \leq 1$, also $\frac{b}{a} \in R$. Daher ist $a \mid b$.

(vii) Sei φ diskret, also $\varphi(K^\times) = \langle \varphi(a) \rangle$ für ein $a \in K^\times$, o.B.d.A. $\varphi(a) < 1$, also $a \in M$. Für $x \in M$ existiert ein $k \in \mathbb{N}$ mit $\varphi(x) = \varphi(a)^k \leq \varphi(a)$. Nach (vi) ist $a \mid x$ und $x \in Ra$. Folglich ist $M = Ra$. Offenbar ist $\bigcap_{k \in \mathbb{N}} Ra^k = 0$. Ist I ein Ideal in R mit $I \neq 0$, so existiert ein $n \in \mathbb{N}_0$ mit $I \subseteq Ra^n$, aber $I \not\subseteq Ra^{n+1}$. Sei $x \in I \setminus Ra^{n+1}$. Wegen $I \subseteq Ra^n$ können wir $x = ra^n$ mit $r \in R$ schreiben. Daher ist $r \notin Ra = M$, also $r \in R^\times$ und $I \supseteq Rx = Rra^n = Ra^n \supseteq I$, d.h. $I = Ra^n$.

Beispiel: Ist $K = \mathbb{Q}$ und $\varphi = \varphi_p$ für eine Primzahl p, so ist

$$\begin{aligned} R &= \{p^r \frac{a}{b} : a, b \in \mathbf{Z} \setminus p\mathbf{Z},\ r \in \mathbb{N}_0\} \cup \{0\}, \\ M &= \{p^r \frac{a}{b} : a, b \in \mathbf{Z} \setminus p\mathbf{Z},\ r \in \mathbb{N}\} \cup \{0\} \ = \ pR, \end{aligned}$$

und die Abbildung $\mathbf{Z} \to R/M,\ z \mapsto z + M$ ist ein Homomorphismus mit Kern $\mathbf{Z} \cap M = p\mathbf{Z}$. Sind $r \in \mathbb{N}_0$ und $a, b \in \mathbf{Z} \setminus p\mathbf{Z}$, so wähle man $c \in \mathbf{Z}$ mit $bc \equiv 1 \pmod{p}$. Dann ist $p^r \frac{a}{b} - p^r ac = p^r \frac{a}{b}(1 - bc) \in M$. Daher ist die Abbildung $\mathbf{Z}/p\mathbf{Z} \to R/M,\ z + p\mathbf{Z} \mapsto z + M$ ein Isomorphismus. (Analog für einen beliebigen faktoriellen Ring F und ein Primelement $p \in F$)

Satz 25.6 *Für jede Bewertung φ eines Körpers K bilden die Cauchy-Folgen in K bzgl. komponentenweise definierten Verknüpfungen einen Ring $\mathcal{C}$, und die Nullfolgen in K bilden ein maximales Ideal $\mathcal{N}$ in $\mathcal{C}$.*

Beweis: Es ist leicht zu sehen, daß $\mathcal{C}$ ein Ring und $\mathcal{N}$ ein echtes Ideal in $\mathcal{C}$ ist. Sei $a = (a_n)_{n\in\mathbb{N}} \in \mathcal{C}\setminus\mathcal{N}$. Dann besitzt a auch keine Teilfolge, die gegen 0 konvergiert. Daher existieren $N \in \mathbb{N}$ und $\varepsilon > 0$ mit $\varphi(a_n) \geq \varepsilon$ für $n \geq N$. Insbesondere ist $a_n \neq 0$ für $n \geq N$. Wir wählen ein Folge $(b_n)_{n\in\mathbb{N}}$ mit $b_n = \frac{1}{a_n}$ für $n \geq N$. Für $m, n \in \mathbb{N}$ mit $m, n \geq N$ gilt dann:

$$\begin{aligned} \varphi(b_m - b_n) &= \varphi\left(\frac{1}{a_m} - \frac{1}{a_n}\right) = \varphi\left(\frac{a_n - a_m}{a_n a_m}\right) = \frac{\varphi(a_n - a_m)}{\varphi(a_n)\varphi(a_m)} \leq \\ &\leq \frac{1}{\varepsilon^2}\,\varphi(a_n - a_m). \end{aligned}$$

Daher ist $b = (b_n)_{n\in\mathbb{N}} \in \mathcal{C}$ und $ab - 1 \in \mathcal{N}$. Dies zeigt: $\mathcal{C}/\mathcal{N}$ ist Körper.

Bemerkung: Man nennt $\hat{K} := \mathcal{C}/\mathcal{N}$ die *Vervollständigung* oder *Komplettierung* von K. Die Abbildung $K \to \hat{K},\ a \mapsto (a, a, a, \ldots) + \mathcal{N}$ ist offenbar ein Monomorphismus. Wir können und werden also K mit seinem Bild in $\hat{K}$ identifizieren und so K als Teilkörper von $\hat{K}$ auffassen. Für jede Cauchy-Folge $a = (a_n)_{n\in\mathbb{N}}$ in K ist $(\varphi(a_n))_{n\in\mathbb{N}}$ wegen $|\varphi(a_n) - \varphi(a_m)| \leq \varphi(a_n - a_m)$ für $m, n \in \mathbb{N}$ eine Cauchy-Folge in $\mathbb{R}$, konvergiert also dort wegen der Vollständigkeit von $\mathbb{R}$. Ist $b = (b_n)_{n\in\mathbb{N}}$ eine Nullfolge in K, so ist $(\varphi(b_n))_{n\in\mathbb{N}}$ eine Nullfolge in $\mathbb{R}$. Folglich ist $\lim_{n\to\infty} \varphi(a_n + b_n) = \lim_{n\to\infty} \varphi(a_n)$. Man kann also eine Abbildung $\hat{\varphi} : \hat{K} \to \mathbb{R}$ definieren durch $\hat{\varphi}((a_n) + \mathcal{N}) = \lim_{n\to\infty} \varphi(a_n)$. Man rechnet leicht nach, daß $\hat{\varphi}$ eine Bewertung von $\hat{K}$ ist, die φ fortsetzt. Man nennt $\hat{\varphi}$ die *kanonische Fortsetzung* von φ auf $\hat{K}$.
Ist $\alpha \in \hat{K}$ und schreibt man $\alpha = (a_n)_{n\in\mathbb{N}} + \mathcal{N}$, so ist $\hat{\varphi}(\alpha - a_m) = \lim_{n\to\infty} \varphi(a_n - a_m)$ für $m \in \mathbb{N}$. Daher konvergiert $(a_m)_{m\in\mathbb{N}}$ in $\hat{K}$ gegen α, d.h. K ist dicht in $\hat{K}$.
Ferner ist $\hat{K}$ vollständig bzgl. $\hat{\varphi}$. Ist nämlich $(\alpha_n)_{n\in\mathbb{N}}$ eine Cauchy-Folge in $\hat{K}$, so wähle man für $n \in \mathbb{N}$ ein $a_n \in K$ mit $\hat{\varphi}(\alpha_n - a_n) < \frac{1}{n}$. Dann ist $(\alpha_n - a_n)_{n\in\mathbb{N}}$ Nullfolge in $\hat{K}$. Wegen $a_n = \alpha_n - (\alpha_n - a_n)$ ist also $a := (a_n)_{n\in\mathbb{N}}$ Cauchy-Folge in $\hat{K}$ und in K. Setzt man $\alpha := a + \mathcal{N}$, so konvergiert $(\alpha_n)_{n\in\mathbb{N}}$ gegen α wegen $\alpha - \alpha_n = (\alpha - a_n) + (a_n - \alpha_n)$. Daher ist $\hat{K}$ vollständig bzgl. $\hat{\varphi}$.

Satz 25.7 *Sei (K, φ) ein bewerteter Körper mit Vervollständigung $(\hat{K}, \hat{\varphi})$, (L, ψ) ein vollständig bewerteter Körper und $\sigma : K \to L$ ein Monomorphismus mit $\psi \circ \sigma = \varphi$. Dann läßt sich σ eindeutig zu einem Monomorphismus $\tau : \hat{K} \to L$ mit $\psi \circ \tau = \hat{\varphi}$ fortsetzen.*

Beweis: Ist $\alpha \in \hat{K}$, so existiert eine Folge $(a_n)_{n\in\mathbb{N}}$ in K mit $\alpha = \lim_{n\to\infty} a_n$. Wegen $\psi(\sigma(a_n)) = \varphi(a_n)$ für $n \in \mathbb{N}$ ist $(\sigma(a_n))_{n\in\mathbb{N}}$ Cauchy-Folge in L, konvergiert also dort. Man setzt $\tau(\alpha) := \lim_{n\to\infty} \sigma(a_n)$ und rechnet leicht nach, daß die so entstehende Abbildung $\tau : \hat{K} \to L$ wohldefiniert und ein Monomorphismus mit $\psi \circ \tau = \hat{\varphi}$ ist.
Ist $\tau' : \hat{K} \to L$ ein beliebiger Monomorphismus, der σ fortsetzt und $\psi \circ \tau' = \hat{\varphi}$ erfüllt, so gilt für $n \in \mathbb{N}$: $\psi(\tau'(\alpha) - \sigma(a_n)) = \psi(\tau'(\alpha - a_n)) = \hat{\varphi}(\alpha - a_n)$. Daher ist $\tau'(\alpha) = \lim_{n\to\infty} \sigma(a_n) = \tau(\alpha)$.

Bemerkung: Ist K Teilkörper eines Körpers $\tilde{K}$ und $\tilde{\varphi}$ eine Bewertung von $\tilde{K}$, die φ fortsetzt, ist K dicht in $\tilde{K}$ und $\tilde{K}$ vollständig bzgl. $\tilde{\varphi}$, so existiert also genau ein Isomorphismus $\tau : \hat{K} \to \tilde{K}$ mit $\tau|K = \mathrm{id}_K$ und $\tilde{\varphi} \circ \tau = \hat{\varphi}$.

Beispiel: Im Fall $K = \mathbb{Q}$ und $\varphi = \varphi_\infty$ ist also $\hat{K}$ zu $\mathbb{R}$ isomorph. Im Fall $K = \mathbb{Q}$ und $\varphi = \varphi_p$ für eine Primzahl p erhält man einen Körper $\mathbb{Q}_p = \hat{K}$, den man den Körper der *p-adischen Zahlen* nennt. (Hensel, 1861–1941)

Satz 25.8 *Sei (K, φ) ein nichtarchimedisch bewerteter Körper mit Vervollständigung $(\hat{K}, \hat{\varphi})$. Dann haben φ und $\hat{\varphi}$ die gleichen Wertegruppen. Sind $R, \hat{R}, M, \hat{M}$ die entsprechenden Bewertungsringe und -ideale, so ist die Abbildung $R/M \to \hat{R}/\hat{M},\ a+M \mapsto a+\hat{M}$ ein Isomorphismus.*

Beweis: Ist $\alpha \in \hat{K} \setminus \{0\}$, so existiert eine Folge $a = (a_n)_{n\in\mathbb{N}}$ in K mit $\alpha = \lim_{n\to\infty} a_n$. Daher existiert ein $N \in \mathbb{N}$ mit $\hat{\varphi}(\alpha - a_n) < \hat{\varphi}(\alpha)$ für $n \geq N$. Dann ist

$$\varphi(a_N) = \hat{\varphi}(a_N) = \hat{\varphi}(\alpha - (\alpha - a_N)) = \max\{\hat{\varphi}(\alpha), \hat{\varphi}(\alpha - a_N)\} = \hat{\varphi}(\alpha).$$

Dies ergibt die erste Behauptung.
Ist $\alpha \in \hat{R}$, so ist $\varphi(a_N) = \hat{\varphi}(\alpha) \leq 1$, also $a_N \in R$ und $\alpha - a_N \in \hat{M}$ wegen $\hat{\varphi}(\alpha - a_N) < \hat{\varphi}(\alpha) \leq 1$. Daher ist die Abbildung $R/M \to \hat{R}/\hat{M},\ r + M \mapsto r + \hat{M}$ surjektiv, und der Rest folgt unmittelbar.

Beispiel: Im Fall $\hat{K} = \mathbb{Q}_p$ setzt man $\hat{R} = \mathbf{Z}_p$ und nennt die Elemente in $\mathbf{Z}_p$ *ganze p-adische Zahlen*. In diesem Fall ist $\hat{M} = p\mathbf{Z}_p$ nach 25.5.

Satz 25.9 *Für jeden vollständig nichtarchimedisch bewerteten Körper (K, φ) gilt:*

(i) Eine Reihe $\sum_{n=1}^\infty a_n$ in K konvergiert genau dann in K, wenn $(a_n)_{n\in\mathbb{N}}$ eine Nullfolge ist.

(ii) Eine Folge $(b_n)_{n\in\mathbb{N}}$ konvergiert genau dann in K, wenn $(b_{n+1} - b_n)_{n\in\mathbb{N}}$ eine Nullfolge ist.

(iii) Ist $(a_n)_{n\in\mathbb{N}}$ eine Folge im Bewertungsring R und x ein Element im Bewertungsideal M von φ, so konvergiert die Potenzreihe $\sum_{n=0}^\infty a_n x^n$, und zwar gegen ein Element in R.

Beweis:

(i) Für $n \in \mathbb{N}$ sei $b_n := \sum_{k=1}^n a_k$. Für $m, n \in \mathbb{N}$ mit $n > m$ gilt dann: $b_n - b_m = a_{m+1} + \ldots + a_n$. Ist also $(a_n)_{n\in\mathbb{N}}$ eine Nullfolge, so ist $(b_n)_{n\in\mathbb{N}}$ wegen der starken Dreiecksungleichung eine Cauchy-Folge, konvergiert also in K. Die Umkehrung ist trivial.

(ii) $b_{n+1} - b_1 = \sum_{m=1}^n (b_{m+1} - b_m)$ und Teil (i).

(iii) Wegen $\varphi(a_n x^n) = \varphi(a_n)\varphi(x)^n \leq \underbrace{\varphi(x)}_{<1}{}^n$ konvergiert die Potenzreihe unter den gegebenen Voraussetzungen. Ist α ihr Grenzwert, so gilt nach dem Beweis von 25.8 $\varphi(\alpha) = \varphi(\sum_{n=0}^N a_n x^n)$ für ein $N \in \mathbb{N}$, also $\varphi(\alpha) \leq \max\{\varphi(a_n x^n) : n = 0, \ldots, N\} \leq 1$.

Satz 25.10 *Sei p Primzahl.*

(i) Jedes Element $a \in \mathbf{Z}_p$ läßt sich in der Form $a = \sum_{i=0}^\infty a_i p^i$ mit eindeutig bestimmten Elementen $a_0, a_1, a_2, \ldots \in \{0, 1, \ldots, p-1\}$ schreiben.

(ii) Jedes Element $a \in \mathbb{Q}_p$ läßt sich in der Form $a = \sum_{i=-\infty}^\infty a_i p^i$ mit eindeutig bestimmten Elementen $\ldots, a_{-2}, a_{-1}, a_0, a_1, a_2, \ldots \in \{0, 1, \ldots, p-1\}$ schreiben, wobei $|\{i \in \mathbb{N} : a_{-i} \neq 0\}| < \infty$ ist.

Beweis:

(i) Wegen $\mathbf{Z}/p\mathbf{Z} = \{0+p\mathbf{Z}, 1+p\mathbf{Z}, \ldots, (p-1)+p\mathbf{Z}\}$ gilt nach 25.8: $\mathbf{Z}_p/p\mathbf{Z}_p = \{0+p\mathbf{Z}_p, 1+p\mathbf{Z}_p, \ldots, (p-1)+p\mathbf{Z}_p\}$. Ist also $a \in \mathbf{Z}_p$, so existiert genau ein $a_0 \in \{0, 1, \ldots, p-1\}$ mit $a \equiv a_0 \pmod{p\mathbf{Z}_p}$. Wir schreiben $a - a_0 = pa'$ mit $a' \in \mathbf{Z}_p$. Dann existiert genau ein $a_1 \in \{0, 1, \ldots, p-1\}$ mit $a' \equiv a_1 \pmod{p\mathbf{Z}_p}$. Wir schreiben $a' - a_1 = pa''$ mit $a'' \in \mathbf{Z}_p$. Es ist also $a = a_0 + a_1 p + a'' p^2$. Fährt man so fort, so erhält man Elemente $a_0, a_1, a_2, \ldots \in \{0, 1, \ldots, p-1\}$ mit $a \equiv a_0 + a_1 p + \ldots + a_n p^n \pmod{p^{n+1}\mathbf{Z}_p}$ für $n \in \mathbb{N}$. Es ist also $a = \sum_{i=0}^{\infty} a_i p^i$.
Ist auch $a = \sum_{i=0}^{\infty} b_i p^i$ mit Elementen $b_0, b_1, b_2, \ldots \in \{0, 1, \ldots, p-1\}$, so ist $a_0 + p\mathbf{Z}_p = a + p\mathbf{Z}_p = b_0 + p\mathbf{Z}_p$, also $a_0 = b_0$ und $\sum_{i=1}^{\infty} a_i p^i = \sum_{i=1}^{\infty} b_i p^i$ bzw. $\sum_{i=1}^{\infty} a_i p^{i-1} = \sum_{i=1}^{\infty} b_i p^{i-1}$. Induktiv erhält man $a_i = b_i$ für $i \in \mathbb{N}_0$.

(ii) Ist $a \in \mathbb{Q}_p \setminus \{0\}$ und $\hat{\varphi}_p(a) = (\frac{1}{p})^r$, so ist $\hat{\varphi}_p(p^{-r}a) = 1$, also $p^{-r}a \in \mathbf{Z}_p^{\times}$. Nach (i) existieren Elemente $b_0, b_1, b_2, \ldots \in \{0, 1, \ldots, p-1\}$ mit $p^{-r}a = \sum_{i=0}^{\infty} b_i p^i$, also $a = \sum_{i=0}^{\infty} b_i p^{r+i}$. Daher besitzt jedes Element in $\mathbb{Q}_p$ eine Darstellung der gewünschten Art. Hat man zwei solche Darstellungen $a = \sum_{i=-\infty}^{\infty} c_i p^i = \sum_{i=-\infty}^{\infty} d_i p^i$, so wähle man $r \in \mathbf{Z}$ mit $p^r a \in \mathbf{Z}_p$. Dann sind $\sum_{i=-r}^{\infty} c_i p^{r+i} = \sum_{i=-r}^{\infty} d_i p^{r+i}$ zwei Darstellungen von $p^r a$ in $\mathbf{Z}_p$, und aus (i) folgt $c_i = d_i$ für $i \in \mathbf{Z}$.

Beispiel:

(i) In $\mathbb{Q}_p$ ist $-1 = \sum_{i=0}^{\infty}(p-1)p^i$; denn

$$\sum_{i=0}^{\infty}(p-1)p^i = (p-1)\sum_{i=0}^{\infty} p^i = (p-1)\frac{1}{1-p} = -1.$$

(ii) In $\mathbb{Q}_7$ ist

$$\begin{aligned}
\frac{3}{5} &= 1 - \frac{2}{5} = 1 - \frac{2 \cdot 480}{5 \cdot 480} = 1 - \frac{960}{7^4 - 1} = 1 + 960\frac{1}{1 - 7^4} = \\
&= 1 + 960\sum_{i=0}^{\infty}(7^4)^i = 1 + (2 \cdot 7^3 + 5 \cdot 7^2 + 4 \cdot 7 + 1)\sum_{i=0}^{\infty}(7^4)^i = \\
&= 2 + 4 \cdot 7 + 5 \cdot 7^2 + 2 \cdot 7^3 + 1 \cdot 7^4 + 4 \cdot 7^5 + 5 \cdot 7^6 + 2 \cdot 7^7 + \ldots
\end{aligned}$$

Bemerkung: Die Bedeutung der Körper $\mathbb{Q}_p$ geht u.a. aus dem Satz von *Hasse-Minkowski* aus der Zahlentheorie hervor:
Eine Gleichung der Form $a_1 x_1^2 + \ldots + a_n x_n^2 = 0$ mit $a_1, \ldots, a_n \in \mathbb{Q}$ hat genau dann eine von 0 verschiedene Lösung in $\mathbb{Q}^n$, wenn sie in $\mathbb{R}^n$ und in $\mathbb{Q}_p^n$ für jede Primzahl p eine von 0 verschiedene Lösung hat.

Kapitel 26

Moduln

Sei R ein Ring.

Definition 26.1 *Ein R-*Linksmodul *ist ein Tripel $(M, +, \cdot)$, das aus einer Menge M und zwei Abbildungen $+ : M \times M \to M,\ (a,b) \mapsto a+b,\ \cdot : R \times M \to M,\ (r,a) \mapsto ra$ besteht und folgende Eigenschaften hat:*

(i) $(M, +)$ *ist abelsche Gruppe.*

(ii) $(rs)m = r(sm) \qquad \forall r,s \in R,\ \forall m \in M.$

(iii) $(r+s)m = rm + sm \qquad \forall r,s \in R,\ \forall m \in M.$

(iv) $r(m+n) = rm + rn \qquad \forall r \in R,\ \forall m,n \in M.$

(v) $1m = m \qquad \forall m \in M.$

*Analog definiert man R-*Rechtsmoduln.

Beispiel:

(i) Für jeden Körper K sind die K-Linksmoduln genau die K-Vektorräume.

(ii) Für jeden Körper K wird jeder K-Vektorraum V zu einem Linksmodul über dem Endomorphismenring $\mathrm{End}(V)$, wenn man definiert: $\varphi v := \varphi(v)$ für $\varphi \in \mathrm{End}(V),\ v \in V$.

(iii) Für jeden Körper K und $m, n \in \mathbb{N}$ wird $\mathrm{Mat}(m,n,K)$ durch die gewöhnliche Matrizenmultiplikation zu einem Linksmodul über $\mathrm{Mat}(m,K)$ und einem Rechtsmodul über $\mathrm{Mat}(n,K)$.

(iv) Für jeden Körper K, jeden K-Vektorraum V und jede lineare Abbildung $\varphi : V \to V$ wird V zu einem Linksmodul über dem Polynomring $K[X]$, wenn man definiert: $fv := (f(\varphi))(v)$ für $f \in K[X],\ v \in V$.

(v) Jede abelsche Gruppe $(A, +)$ wird zu einem $\mathbf{Z}$-Linksmodul, wenn man na für $n \in \mathbf{Z},\ a \in A$ wie früher definiert: $na = \underbrace{a + \ldots + a}_{n \text{ Summanden}}$ für $n \in \mathbb{N}$.

Umgekehrt ist in jedem $\mathbf{Z}$-Linksmodul m die Multiplikation mit Skalaren durch die Addition bestimmt: $na = (1 + \ldots + 1)a = 1a + \ldots + 1a = a + \ldots + a$ für $n \in \mathbb{N},\ a \in A$. Daher sind $\mathbf{Z}$-Linksmoduln nichts anderes als abelsche Gruppen.

(vi) Jeder Ring R wird durch Ringaddition und Ringmultiplikation zu einem R-Linksmodul und einem R-Rechtsmodul.

(vii) Jeder R-Linksmodul wird zu einem R-Rechtsmodul über dem entgegengesetzten Ring R^o, wenn man definiert: $mr := rm$ für $r \in R^o = R,\ m \in M$. Ist R kommutativ, so ist also jeder R-Linksmodul auch ein R-Rechtsmodul (und umgekehrt).

(viii) Seien R, S Ringe, $\varphi : R \to S$ ein unitärer Ringhomomorphismus und M ein S-Linksmodul. Dann wird M zu einem R-Linksmodul, wenn man für $r \in R$ und $m \in M$ definiert: $rm := \varphi(r)m$. Ein wichtiger Spezialfall ist der, daß R ein unitärer Teilring von S und φ die Inklusionsabbildung ist. In diesem Fall nennt man den R-Linksmodul M die *Restriktion* des S-Linksmoduls M und schreibt dafür $\mathrm{Res}_R^S(M)$.

(ix) Ist I eine nichtleere Menge und M_i ein R-Linksmodul für $i \in I$, so ist $\times_{i\in I} M_i = \prod_{i\in I} M_i := \{(m_i)_{i\in I} : m_i \in M_i \text{ für } i \in I\}$ ein R-Linksmodul mit den üblichen Verknüpfungen. Man nennt $\prod_{i\in I} M_i$ das *direkte* oder *kartesische* Produkt der Moduln M_i $(i \in I)$. Im Fall $I = \{1, \ldots, n\}$ für ein $n \in \mathbb{N}$ schreibt man wie üblich: $M_1 \times \ldots \times M_n = \times_{i=1}^n M_i = \prod_{i=1}^n M_i = \{(m_1, \ldots, m_n) : m_i \in M_i \text{ für } i = 1, \ldots, n\}$.

(x) Für jede nichtleere Menge I und jeden R-Linksmodul M ist nach (ix) auch $\mathrm{Abb}(I, M) := \prod_{i\in I} M$ ein R-Linksmodul. Für $r \in R$ und $f \in \mathrm{Abb}(I, M)$ ist dabei $rf : I \to M$ definiert durch $(rf)(i) := rf(i)$ für $i \in I$. Im Fall $I = \{1, \ldots, n\}$ für ein $n \in \mathbb{N}$ schreibt man wie üblich einfacher M^n statt $\mathrm{Abb}(\{1, \ldots, n\}, M)$.

Bemerkung:

(i) Wie bei Vektorräumen beweist man, daß in jedem R-Linksmodul M gilt: $r0 = 0$ für $r \in R$, $0m = 0$ für $m \in M$, $(-1)m = -m$ für $m \in M$, etc.

(ii) Wir werden im folgenden Aussagen meist für R-Linksmoduln formulieren und beweisen. Sie gelten aber analog auch für R-Rechtsmoduln. Zur Vereinfachung sagen wir auch kurz „R-Modul“ statt „R-Linksmodul“.

Definition 26.2 *Ein* Untermodul *eines R-Moduls ist eine Teilmenge von M, die mit den entsprechend eingeschränkten Verknüpfungen ein R-Modul ist.*

Bemerkung: Eine Teilmenge N von M ist also genau dann ein Untermodul von M, wenn N nichtleer ist und mit n, n' auch die Elemente $rn + r'n'$ für $r, r' \in R$ enthält.

Beispiel:

(a) Für einen Vektorraum V über dem Körper K sind die Untermoduln von V genau die Untervektorräume von V.

(b) In Beispiel 26.1 (iv) sind die $K[X]$-Untermoduln von V genau die Untervektorräume U von V mit $\varphi(U) \subseteq U$ (d.h. die φ-invarianten Untervektorräume von V).

(c) Für einen $\mathbf{Z}$-Modul A (d.h. eine abelsche Gruppe) sind die $\mathbf{Z}$-Untermoduln von A genau die Untergruppen von A.

(d) Ist M ein R-Modul, I eine nichtleere Menge und N_i ein R-Untermodul von M für $i \in I$, so ist auch $\bigcap_{i\in I} N_i$ ein Untermodul von M. Insbesondere ist für jede Teilmenge X von M der Durchschnitt D aller Untermoduln von M, die X enthalten, ein Untermodul von M. Man zeigt leicht, daß D aus allen *Linearkombinationen* $r_1x_1 + \ldots + r_nx_n$ mit $r_1, \ldots, r_n \in R$, $x_1, \ldots, x_n \in X$, $n \in \mathbb{N}$ besteht. Man schreibt $D = RX$, im Fall $X = \{x\}$ für ein $x \in M$ auch $D = Rx$. Ein *Erzeugendensystem* von M ist eine Teilmenge Y von M mit $M = RY$. Besitzt M ein endliches Erzeugendensystem, so nennt man M *endlich erzeugt*. Ist $M = Ry$ für ein $y \in M$, so nennt man M *zyklisch*.

(e) Ist M ein R-Modul, I eine (nichtleere) Menge und N_i ein R-Untermodul von M für $i \in I$, so bilden die Elemente $\sum_{i\in I} x_i$, wobei $x_i \in N_i$ für $i \in I$ und $|\{i \in I : x_i \neq 0\}| < \infty$ ist, einen Untermodul von M, den man die *Summe* der Untermoduln N_i nennt und mit $\sum_{i\in I} N_i$ bezeichnet. Offenbar ist $\sum_{i\in I} N_i$ der von $\bigcup_{i\in I} N_i$ erzeugte Untermodul von M. Im Fall $I = \{1, \ldots, n\}$ für ein $n \in \mathbb{N}$ schreibt man auch $\sum_{i=1}^n N_i$ oder $N_1 + \ldots + N_n$ statt $\sum_{i\in I} N_i$.

(f) Ist I eine nichtleere Menge und M_i ein R-Modul für $i \in I$, so bilden die Elemente $(m_i)_{i\in I} \in \prod_{i\in I} M_i$ mit $|\{i \in I : m_i \neq 0\}| < \infty$ einen Untermodul von $\prod_{i\in I} M_i$, den man als *Koprodukt* der Moduln M_i bezeichnet. Schreibweise: $\coprod_{i\in I} M_i$.

(g) Die R-Untermoduln des R-Linksmoduls R nennt man die *Linksideale* von R. Ein Linksideal von R ist also eine nichtleere Teilmenge L von R, die mit x, y auch $rx + sy$ für $r, s \in R$ enthält. Analog definiert man *Rechtsideale*. Eine Teilmenge I von R ist also genau dann Ideal in R, wenn I gleichzeitig ein Linksideal und ein Rechtsideal in R ist.

(h) Für jeden R-Modul M sind 0 und M Untermoduln von M. Ist $M \neq 0$ und sind dies die einzigen Untermoduln von M, so nennt man M *einfach* oder *irreduzibel*.

Satz 26.3 *Für jeden R-Modul M und jeden R-Untermodul N von M wird M/N ein R-Modul, wenn man definiert: $r(m + N) := rm + N$ für $r \in R,\ m \in M$.*

Beweis: Man rechnet leicht nach, daß dies wohldefiniert ist und die gewünschten Eigenschaften hat.

Definition: *Man bezeichnet M/N als* Faktormodul *von M nach N.*

Definition 26.4 *Seien M, N R-Moduln und $f : M \to N$ eine Abbildung mit $f(rx + sy) = rf(x) + sf(y)$ für $r, s \in R,\ x, y \in M$. Dann nennt man f einen R-*Homomorphismus*, und wie üblich definiert man R-*Momomorphismus*, R-*Epimorphismus*, etc.*

Bemerkung:

(i) Für R-Homomorphismen $f, g : M \to N$ ist auch $f \pm g : M \to N$ ein R-Homomorphismus; $f \pm g$ ist dabei definiert durch $(f \pm g)(x) := f(x) \pm g(x)$ für $x \in M$. Ferner ist die Nullabbildung ein R-Homomorphismus. Daher bilden die R-Homomorphismen $f : M \to N$ eine abelsche Gruppe $\mathrm{Hom}_R(M, N)$.

(ii) Für einen R-Homomorphismus $f : M \to N$ und ein Element $r \in R$ definiert man eine Abbildung $rf : M \to N$ durch $(rf)(x) := rf(x)$ für $x \in M$. Im allgemeinen ist aber rf *kein* R-Homomorphismus. Ist jedoch R kommutativ, so ist rf stets ein R-Homomorphismus. In diesem Fall wird $\mathrm{Hom}_R(M, N)$ so selbst zu einem R-Modul.

(iii) Sind L, M, N R-Moduln, so ist für R-Homomorphismen $f : L \to M,\ g : M \to N$ auch $g \circ f : L \to N$ ein R-Homomorphismus. Ferner ist id_M ein R-Homomorphismus. Daher wird $\mathrm{Hom}_R(M, M)$ mit $+$ und $\circ$ zu einem Ring, dem *Endomorphismenring* $\mathrm{End}_R(M)$ von M. Außerdem wird M zu einem $\mathrm{End}_R(M)$-Modul, wenn man $fm := f(m)$ für $f \in \mathrm{End}_R(M),\ m \in M$ definiert.
Sind f, g R-Isomorphismen, so auch $g \circ f$ und f^{-1}. Insbesondere bilden die R-Automorphismen von M bzgl. $\circ$ eine Gruppe, die *Automorphismengruppe* $\mathrm{Aut}_R(M)$ von M.

(iv) Man nennt zwei R-Moduln M, N *isomorph* und schreibt $M \simeq N$ oder $M \simeq_R N$, wenn es einen R-Isomorphismus $f : M \to N$ gibt. Dieser Begriff hat die üblichen Eigenschaften (Reflexivität, Transitivität, ...).

(v) Seien M, N R-Moduln und $f : M \to N$ ein R-Homomorphismus. Wie bei Gruppen ist $f(U)$ für jeden Untermodul U von M ein Untermodul von N; insbesondere ist $\mathrm{Bild}(f) = f(M)$ ein Untermodul von N. Analog ist für jeden Untermodul V von N das Urbild $f^{-1}(V)$ ein Untermodul von M; insbesondere ist $\ker(f) = f^{-1}(0)$ ein Untermodul von M, und die Abbildung $M/\ker(f) \to f(M),\ m+\ker(f) \mapsto f(m)$ ist ein R-Isomorphismus (Homomorphiesatz).
Für jeden Untermodul U von M ist $f^{-1}(f(U)) = U + \ker(f)$; daher erhält man durch $U \mapsto f(U)$ und $V \mapsto f^{-1}(V)$ zueinander inverse Bijektionen zwischen der Menge der Untermoduln U von M mit $\ker(f) \subseteq U$ und der Menge der Untermoduln von $f(M)$.

Für Untermoduln K, L von M ist die Abbildung $K/K \cap L \to K + L/L,\ x + (K \cap L) \mapsto x + L$ ein R-Isomorphismus (1. Isomorphiesatz). Im Fall $K \subseteq L$ ist ferner $M/L \simeq (M/K)/(L/K)$ (2. Isomorphiesatz). Der 3. Isomorphiesatz überträgt sich ebenfalls auf R-Moduln.

Beispiel:

(i) Für jeden Untermodul N eines R-Moduls M sind die Inklusionsabbildung $N \to M$ und die kanonische Abbildung $M \to M/N$ R-Homomorphismen.

(ii) Ist I eine nichtleere Menge und M_i ein R-Modul für $i \in I$, so ist für $j \in I$ die j-te *Projektion*

$$p_j : \prod_{i \in I} M_i \to M_j,\ (m_i)_{i \in I} \mapsto m_j$$

ein R-Homomorphismus. Analog ist für $j \in I$ die j-te *Injektion*

$$q_j : M_j \to \coprod_{i \in I} M_i,\ m \mapsto (m_i)_{i \in I},$$

wobei $m_j := m$ und $m_i := 0$ für $i \in I \setminus \{j\}$, ein R-Homomorphismus. Ist I endlich, so ist $\prod_{i \in I} M_i = \coprod_{i \in I} M_i,\ p_i \circ q_i = \mathrm{id}_{M_i}$ für $i \in I$ und $p_j \circ q_i = 0$ für $i, j \in I$ mit $i \neq j$. Ferner ist $e_i := q_i \circ p_i \in \mathrm{End}_R(\prod_{i \in I} M_i)$ mit $e_i \circ e_i = e_i$ für $i \in I$, $e_i \circ e_j = 0$ für $i, j \in I$ mit $i \neq j$ und $\sum_{i \in I} e_i = \mathrm{id}$.

Bemerkung 26.5 Wie für Gruppen definiert man *Reihen* von Untermoduln eines R-Moduls:

$$M = M_0 \supseteq M_1 \supseteq \ldots \supseteq M_l = 0.$$

Die *Faktoren* dieser Reihe sind die R-Moduln M_{i-1}/M_i $(i = 1, \ldots, l)$, die *Länge* der Reihe ist l. Wie üblich definiert man *Verfeinerung* und *Isomorphie* solcher Reihen. Es gilt dann der Verfeinerungssatz von Schreier, daß je zwei Reihen eines R-Moduls isomorphe Verfeinerungen besitzen. Sind alle Faktoren der Reihe $M = M_0 \supseteq M_1 \supseteq \ldots \supseteq M_l = 0$ einfach, so spricht man von einer *Kompositionsreihe*. Dies ist äquivalent dazu, daß die Reihe selbst keine Wiederholung enthält, aber jede ihrer echten Verfeinungen. Es folgt wieder der Satz von Jordan-Hölder, daß je zwei Kompositionsreihen eines R-Moduls M (falls überhaupt vorhanden) isomorph sind. Dies erlaubt es von den *Kompositionsfaktoren* und der *Kompositionslänge* (kurz: Länge) von M zu reden.

Satz 26.6 *Für einen R-Modul M sind äquivalent:*

(1) (Aufsteigende Kettenbedingung)
Sind $N_1, N_2, N_3, \ldots$ Untermoduln von M mit $N_1 \subseteq N_2 \subseteq N_3 \subseteq \ldots$, so existiert ein $k \in \mathbb{N}$ mit $N_k = N_{k+1} = N_{k+2} = \ldots$.

(2) (Maximalbedingung für Untermoduln)
Jede nichtleere Menge von Untermoduln von M besitzt ein maximales Element (bzgl. $\subseteq$).

(3) Jeder Untermodul von M ist endlich erzeugt.

Definition: *Gegebenenfalls nennt man M* noethersch. *(Emmy Noether, 1882–1935)*

Beweis:

(1)⇒(2): Sei $\mathcal{M}$ eine nichtleere Menge von Untermoduln von M. Wir wählen $N_1 \in \mathcal{M}$. Ist N_1 maximal, so sind wir fertig. Andernfalls existiert ein $N_2 \in \mathcal{M}$ mit $N_1 \subsetneqq N_2$. Ist N_2 maximal, so sind wir fertig. Andernfalls existert ein $N_3 \in \mathcal{M}$ mit $N_1 \subsetneqq N_2 \subsetneqq N_3$. Auf diese Weise fahren wir fort. Ist (1) erfüllt, so muß dieses Verfahren bei einem N_k enden. Dann ist also N_k maximal in $\mathcal{M}$.

(2)⇒(3): Sei (2) erfüllt, N ein Untermodul von M und $\mathcal{N}$ die Menge aller endlich erzeugten Untermoduln von N. Wegen $0 \in \mathcal{N}$ ist $\mathcal{N} \neq \emptyset$, also enthält $\mathcal{N}$ ein maximales Element L. Ferner existieren $x_1, \ldots, x_n \in L$ mit $L = Rx_1 + \ldots + Rx_n$. Wäre $L \neq N$ und $y \in N \setminus L$, so wäre $L \subsetneqq Rx_1 + \ldots + Rx_n + Ry \subseteq N$, also $Rx_1 + \ldots + Rx_n + Ry \in \mathcal{N}$ im Widerspruch zur Maximalität von L. Daher ist $N = L = Rx_1 + \ldots + Rx_n$.

(3)⇒(1): Sei (3) erfüllt, und seien $N_1, N_2, N_3, \ldots$ Untermoduln von M mit $N_1 \subseteq N_2 \subseteq N_3 \subseteq \ldots$. Man rechnet leicht nach, daß $N := \bigcup_{i=1}^{\infty} N_i$ ein Untermodul von M ist. Wegen (3) existieren $x_1, \ldots, x_n \in N$ mit $N = Rx_1 + \ldots + Rx_n$. Für $i = 1, \ldots, n$ existieren $k_i \in \mathbb{N}$ mit $x_i \in N_{k_i}$. Mit $k := \max\{k_1, \ldots, k_n\}$ ist also $x_1, \ldots, x_n \in N_k$ und damit $N \subseteq N_k \subseteq N_{k+1} \subseteq \ldots \subseteq N$. Folglich gilt (1).

Satz 26.7 *Für jeden Untermodul N eines R-Moduls M gilt: M noethersch $\Leftrightarrow$ N und M/N noethersch.*

Beweis:

⇒: Mit M erfüllt auch N die Bedingung (2) aus 26.6. Analog erfüllt auch M/N diese Bedingung, da jeder Untermodul von M/N die Form U/N hat, wobei U ein Untermodul von M mit $N \subseteq U$ ist.

⇐: Seien N und M/N noethersch, und seien $M_1, M_2, M_3, \ldots$ Untermoduln von M mit $M_1 \subseteq M_2 \subseteq M_3 \subseteq \ldots$. Dann ist $M_1 \cap N \subseteq M_2 \cap N \subseteq M_3 \cap N \subseteq \ldots$ mit Untermoduln $M_i \cap N$ von N. Da N noethersch ist, existiert ein $k \in \mathbb{N}$ mit $M_k \cap N = M_{k+1} \cap N = M_{k+2} \cap N = \ldots$.
Analog ist $M_1 + N/N \subseteq M_2 + N/N \subseteq M_3 + N/N \subseteq \ldots$ mit Untermoduln $M_i + N/N$ von M/N. Da M/N noethersch ist, existiert also ein $l \in \mathbb{N}$ mit $M_l + N/N = M_{l+1} + N/N = M_{l+2} + N/N = \ldots$.
Für $n \geq \max\{k, l\}$ gilt nach der Dedekind-Identität:

$$\begin{aligned} M_n &= M_n + (M_n \cap N) = M_n + (M_{n+1} \cap N) = (M_n + N) \cap M_{n+1} = \\ &= (M_{n+1} + N) \cap M_{n+1} = M_{n+1}. \end{aligned}$$

Satz 26.8 *Für einen R-Modul M sind äquivalent:*

(1) (Absteigende Kettenbedingung)
Sind $N_1, N_2, N_3, \ldots$ Untermoduln von M mit $N_1 \supseteq N_2 \supseteq N_3 \supseteq \ldots$, so existiert ein $k \in \mathbb{N}$ mit $N_k = N_{k+1} = N_{k+2} = \ldots$.

(2) (Minimalbedingung für Untermoduln)
Jede nichtleere Menge von Untermoduln von M besitzt ein minimales Element (bzgl. $\subseteq$).

Definition: *Gegebenenfalls nennt man M* artinsch. *(Emil Artin, 1898–1962)*

Beweis:

(1)⇒(2): Analog zu 26.6

(2)⇒(1): Seien $N_1, N_2, N_3, \ldots$ Untermoduln von M mit $N_1 \supseteq N_2 \supseteq N_3 \supseteq \ldots$. Ist (2) erfüllt, so existiert in $\{N_i : i \in \mathbb{N}\}$ ein minimales Element N_k. Es ist also $N_k = N_{k+1} = N_{k+2} = \ldots$.

Bemerkung:

(i) Analog zu 26.7 beweist man, daß für einen R-Modul M und einen Untermodul N von M stets gilt: M artinsch $\Leftrightarrow$ N und M/N artinsch.

(ii) Sind N, N' artinsche (noethersche) Untermoduln eines R-Moduls M, so auch $N + N'$; denn $N + N'/N' \simeq N/N \cap N'$.

Satz 26.9 *Ein R-Modul M besitzt genau dann eine Kompositionsreihe, wenn er artinsch und noethersch ist.*

Beweis:

$\Rightarrow$: Sei $M = M_0 \supseteq M_1 \supseteq \ldots \supseteq M_l = 0$ eine Kompositionsreihe. Sind $N_1, N_2, N_3, \ldots$ Untermoduln mit $N_1 \supseteq N_2 \supseteq N_3 \supseteq \ldots$, so besitzen für $n \in \mathbb{N}$ die Reihen $M = M_0 \supseteq M_1 \supseteq \ldots \supseteq M_l = 0$ und $M = N_0 \supseteq N_1 \supseteq \ldots \supseteq N_n \supseteq 0$ isomorphe Verfeinerungen. Insbesondere sind höchstens l der Moduln N_i/N_{i+1} von 0 verschieden. Daher ist M artinsch und analog noethersch.

$\Leftarrow$: Sei M artinsch und noethersch und $\mathcal{N}$ die Menge aller Untermoduln von M, die eine Kompositionsreihe haben. Wegen $0 \in \mathcal{N}$ ist $\mathcal{N} \neq \emptyset$. Da M noethersch ist, enthält $\mathcal{N}$ ein maximales Element N. Es sei $N = N_0 \supseteq N_1 \supseteq \ldots \supseteq N_l = 0$ eine Kompositionsreihe von N.
Annahme: $M \neq N$. Die Menge $\mathcal{M}$ aller von 0 verschiedenen Untermoduln von M/N ist dann wegen $M/N \in \mathcal{M}$ nichtleer. Da mit M auch M/N artinsch ist, enthält $\mathcal{M}$ ein minimales Element L/N. Offenbar ist L/N einfach, also ist $L \supseteq N = N_0 \supseteq N_1 \supseteq \ldots \supseteq N_l = 0$ Kompositionsreihe von L im Widerspruch zur Maximalität von N.

Definition 26.10 *Man nennt R* linksnoethersch (linksartinsch), *wenn R als R-Linksmodul noethersch (artinsch) ist. Analog definiert man* rechtsnoethersche *und* rechtsartinsche *Ringe. Ist R linksnoethersch und rechtsnoethersch (linksartinsch und rechtsartinsch), so nennt man R* noethersch (artinsch).

Beispiel:

(i) Jeder Hauptidealring ist noethersch.

(ii) Für $n \in \mathbb{N}$ und jeden Körper K ist $R := \mathrm{Mat}(n, K)$ artinsch; denn jedes Links- oder Rechtsideal ist gleichzeitig ein Untervektorraum von R.

Satz: *Jeder endliche erzeugte Linksmodul M über einem linksnoetherschen (linksartinschen) Ring R ist noethersch (artinsch).*

Beweis: Sei $M = Rm_1 + \ldots + Rm_n$ mit $m_1, \ldots, m_n \in M$. Für $i = 1, \ldots, n$ ist dann $f : R \to Rm_i$, $r \mapsto rm_i$ ein R-Epimorphismus. Daher ist $Rm_i \simeq R/\ker(f_i)$; insbesondere ist Rm_i noethersch nach 26.7 (artinsch nach 26.8). Folglich ist M noethersch (artinsch) nach Bemerkung 26.8.

Satz 26.11 (Hilberts Basissatz, 1862–1943) *Für jeden kommutativen noetherschen Ring R ist auch der Polynomring $R[X]$ noethersch.*

Beweis: Wir nehmen an, daß $R[X]$ nicht noethersch ist. Dann existiert in $R[X]$ ein Ideal I, das nicht endlich erzeugt ist; insbesondere ist $I \neq 0$. Wir wählen ein Polynom f_1 kleinsten Grades in $I \setminus \{0\}$. Dann ist $I \neq (f_1)$. Wir wählen ein Polynom f_2 kleinsten Grades in $I \setminus (f_1)$. Dann ist $I \neq (f_1, f_2)$. Wir wählen ein Polynom f_3 kleinsten Grades in $I \setminus (f_1, f_2)$ und fahren so fort. Wir erhalten so Polynome $f_1, f_2, f_3, \ldots \in I$. Für $k \in \mathbb{N}$ sei $n_k := \deg(f_k)$ und a_k der höchste Koeffizient von f_k. Dann ist $n_1 \leq n_2 \leq n_3 \leq \ldots$ und $(a_1) \subseteq (a_1, a_2) \subseteq (a_1, a_2, a_3) \subseteq \ldots$. Da R noethersch ist, existiert ein $k \in \mathbb{N}$ mit $(a_1, \ldots, a_k) = (a_1, \ldots, a_k, a_{k+1})$. Es existieren also $b_1, \ldots, b_k \in R$ mit $a_{k+1} = \sum_{i=1}^{k} b_i a_i$. Folglich ist

$$g := f_{k+1} - \sum_{i=1}^{k} b_i X^{n_{k+1} - n_i} f_i \in I \setminus (f_1, \ldots, f_k)$$

mit $\deg(g) < \deg(f_{k+1})$ im Widerspruch zur Wahl von f_{k+1}.

Kapitel 27

Direkte Summen und unzerlegbare Moduln

Sei R ein Ring.

Definition 27.1 *Sei M ein R-Modul, I eine Menge und N_i ein Untermodul von M für $i \in I$. Man sagt, die Summe $\sum_{i\in I} N_i$ sei* direkt *und schreibt $\sum_{i\in I} N_i = \bigoplus_{i\in I} N_i$ falls gilt: Ist $x_i \in N_i$ für $i \in I$, $|\{i \in I : x_i \neq 0\}| < \infty$ und $\sum_{i\in I} x_i = 0$, so ist $x_i = 0$ für alle $i \in I$.*

Bemerkung:

(i) Wie in der Linearen Algebra zeigt man, daß diese Bedingung äquivalent ist zu: $N_i \cap \sum_{j\in I\setminus\{i\}} N_j = 0$ für $i \in I$.

(ii) Im Fall $I = \{1,\dots,n\}$ für ein $n \in \mathbb{N}$ ist $\sum_{i=1}^n N_i$ genau dann direkt, wenn gilt $N_i \cap \sum_{j=1}^{i-1} N_j = 0$ für $i = 1,\dots,n$. In diesem Fall schreibt man auch $\bigoplus_{i=1}^n N_i$ oder $N_1 \oplus \ldots \oplus N_n$ statt $\bigoplus_{i\in I} N_i$.

(iii) Jedes Element in $\sum_{i\in I} N_i$ hat die Form $n = \sum_{i\in I} n_i$, wobei $n_i \in N_i$ für $i \in I$ und $|\{i \in I : n_i \neq 0\}| < \infty$ ist. Ist $\sum_{i\in I} N_i = \bigoplus_{i\in I} N_i$, so sind dabei die Elemente $n_i \in N_i$ durch n eindeutig bestimmt. Daher ist die Abbildung $\coprod_{i\in I} N_i \to \bigoplus_{i\in I} N_i$, $(n_i)_{i\in I} \mapsto \sum_{i\in I} n_i$ ein R-Isomorphismus. (In manchen Büchern schreibt man daher auch $\bigoplus_{i\in I} N_i$ statt $\coprod_{i\in I} N_i$.)
Für $j \in I$ sind also die j-te *Projektion* $p_j : \bigoplus_{i\in I} N_i \to N_j$, $\sum_{i\in I} n_i \mapsto n_j$ und die j-te *Injektion* $q_j : N_j \to \bigoplus_{i\in I} N_i$, $n \mapsto n$ R-Homomorphismen. Dabei ist $p_i \circ q_i = \mathrm{id}_{N_i}$ für $i \in I$ und $p_i \circ q_j = 0$ für $i,j \in I$ mit $i \neq j$. Ferner ist $e_i := q_i \circ p_i \in \mathrm{End}_R(\bigoplus_{i\in I} N_i)$ mit $e_i \circ e_i = e_i$ für $i \in I$ und $e_i \circ e_j = 0$ für $i,j \in I$ mit $i \neq j$. Ist I endlich und $N := \bigoplus_{i\in I} N_i$, so ist außerdem $\sum_{i\in I} e_i = \mathrm{id}_N$.

Satz 27.2 *Seien M ein R-Modul, $n \in \mathbb{N}$ und $e_1,\dots,e_n \in \mathrm{End}_R(M)$ mit $e_1 + \ldots + e_n = \mathrm{id}_M$ und $e_i \circ e_j = \delta_{ij} e_i$ für $i,j = 1,\dots,n$. Dann ist $M = e_1(M) \oplus \ldots \oplus e_n(M)$.*

Beweis: Für $m \in M$ ist $m = \mathrm{id}_M(m) = (e_1 + \ldots + e_n)(m) = e_1(m) + \ldots + e_n(m)$. Daher ist $M = e_1(M) + \ldots + e_n(M)$. Sind $m_1,\dots,m_n \in M$ mit $0 = e_1(m_1) + \ldots + e_n(m_n)$, so ist

$$0 = e_j(0) = e_j(e_1(m_1) + \ldots + e_n(m_n)) = e_j(e_1(m_1)) + \ldots + e_j(e_n(m_n)) = e_j(m_j)$$

für $j = 1,\dots,n$, und die Behauptung folgt.

Bemerkung: Ist $e \in \mathrm{End}_R(M)$ mit $e \circ e = e$, so ist $\mathrm{id}_M - e \in \mathrm{End}_R(M)$ mit

$$\begin{aligned}
&e \circ (\mathrm{id}_M - e) = e - e \circ e = 0,\\
&(\mathrm{id}_M - e) \circ e = e - e \circ e = 0,\\
&(\mathrm{id}_M - e) \circ (\mathrm{id}_M - e) = \mathrm{id}_M - 2e + e \circ e = \mathrm{id}_M - e,\\
&e + (\mathrm{id}_M - e) = \mathrm{id}_M .
\end{aligned}$$

Daher gilt: $M = e(M) \oplus (\mathrm{id}_M - e)(M)$. Für $x \in \ker(e)$ ist

$$x = \mathrm{id}_M(x) = \underbrace{e(x)}_{=0} + (\mathrm{id}_M - e)(x) = (\mathrm{id}_M - e)(x).$$

Daher ist $\ker(e) \subseteq \mathrm{Bild}(\mathrm{id}_M - e)$. Wegen $e \circ (\mathrm{id}_M - e) = 0$ ist umgekehrt $\mathrm{Bild}(\mathrm{id}_M - e) \subseteq \ker(e)$. Insgesamt ist also $\ker(e) = \mathrm{Bild}(\mathrm{id}_M - e)$, d.h. $M = \mathrm{Bild}(e) \oplus \ker(e)$.

Satz 27.3 *Für einen R-Modul M sind äquivalent:*

(1) Sind M_1, M_2 Untermoduln von M mit $M = M_1 \oplus M_2$, so ist $M_1 = 0$ oder $M_2 = 0$.

(2) Ist $e \in \mathrm{End}_R(M)$ mit $e \circ e = e$, so ist $e \in \{0, \mathrm{id}_M\}$.

Beweis:

(1)⇒(2): Sei (1) erfüllt und $e \in \mathrm{End}_R(M)$ mit $e \circ e = e$. Nach Bemerkung 27.2 ist dann $M = \mathrm{Bild}(e) \oplus \ker(e)$, also $\mathrm{Bild}(e) = 0$ oder $\ker(e) = 0$ wegen (1). Im Fall $\mathrm{Bild}(e) = 0$ ist $e = 0$, und im Fall $\ker(e) = 0$ ist $M = \mathrm{Bild}(e)$, also e bijektiv. Wegen $e \circ e = e$ ist also $e = \mathrm{id}_M$.

(2)⇒(1): Sei (2) erfüllt und $M = M_1 \oplus M_2$ mit Untermoduln M_1, M_2 von M. Seien p_1, p_2 und q_1, q_2 die entsprechenden Projektionen und Injektionen. Für $i = 1, 2$ ist dann $e_i := q_i \circ p_i \in \mathrm{End}_R(M)$ mit $e_i \circ e_i = e_i$, also $e_i \in \{0, \mathrm{id}_M\}$ wegen (2). Im Fall $e_1 = 0$ ist $M_1 = e_1(M) = 0$, und im Fall $e_1 = \mathrm{id}_M$ ist $e_2 = 0$ wegen $e_1 + e_2 = \mathrm{id}_M$, also analog $M_2 = 0$.

Definition: *Sind (1) und (2) erfüllt und ist $M \neq 0$, so nennt man M* unzerlegbar*, sonst* zerlegbar.

Beispiel: Jeder einfache R-Modul ist unzerlegbar, aber die Umkehrung gilt i.a. nicht.

Satz 27.4 *Seien M, N R-Moduln, wobei $M \neq 0$ und N unzerlegbar ist, seien $f : M \to N$, $g : N \to M$ R-Homomorphismen, und sei $g \circ f$ ein R-Automorphismus. Dann sind f, g R-Isomorphismen.*

Beweis: Mit $h := (g \circ f)^{-1}$ ist $h \circ g \circ f = \mathrm{id}_M$. Daher ist $f \circ h \circ g \in \mathrm{End}_R(N)$ mit $(f \circ \underbrace{h \circ g) \circ (f}_{=\mathrm{id}} \circ h \circ g) = f \circ h \circ g$. Da N unzerlegbar ist, folgt $f \circ h \circ g \in \{0, \mathrm{id}_N\}$. Im Fall $f \circ h \circ g = 0$ wäre $\mathrm{id}_M = \mathrm{id}_M \circ \mathrm{id}_M = (h \circ g \circ \underbrace{f) \circ (h \circ g}_{=0} \circ f) = 0$, also $M = 0$. Daher ist $f \circ h \circ g = \mathrm{id}_N$; insbesondere ist f surjektiv. Wegen $h \circ g \circ f = \mathrm{id}_M$ ist f auch injektiv, also bijektiv. Folglich ist auch g bijektiv.

Satz 27.5 *Im Fall $R \neq 0$ sind äquivalent:*

(1) Sind $r, s \in R$ nichtinvertierbar, so ist $r + s$ nichtinvertierbar.

(2) Die Nichteinheiten in R bilden ein Ideal in R.

Beweis:

(2)⇒(1): Trivial.

(1)⇒(2): Ist $x \in R$ nichtinvertierbar, so auch rx und xr für $r \in R$; denn wäre etwa $rx \in R^\times$ und $y = (rx)^{-1}$, so wäre $yrx = 1$ und $(xyr)^2 = x\underbrace{yrx}_{=1}yr = xyr$. Im Fall $xyr \in R^\times$ ist man fertig. Sei also $xyr \notin R^\times$. Wegen $xyr + (1 - xyr) = 1 \in R^\times$ ist $1 - xyr \in R^\times$ wegen (1). Wegen $(1 - xyr)^2 = 1 - 2xyr + (xyr)^2 = 1 - xyr$ ist also $1 - xyr = 1$, d.h. $xyr = 0$ im Widerspruch zu $1 = 1 \cdot 1 = (y\underbrace{rx)(yr}_{=0}x)$.

Definition: *Ist $R \neq 0$ und gelten (1),(2), so nennt man R* lokal.

Beispiel:

(i) Jeder Schiefkörper ist lokal.

(ii) $\mathbf{Z}$ ist nicht lokal.

(iii) Jeder Bewertungsring einer nichtarchimedischen Bewertung ist lokal.

Bemerkung:

(i) Sei R lokal und I das Ideal der Nichteinheiten in R. Dann ist jedes Element in $R \setminus I$ invertierbar. Insbesondere ist jedes von 0 verschiedene Element in R/I invertierbar. Daher ist R/I ein Schiefkörper, und I ist ein maximales Ideal in R.

(ii) Sei R lokal und $e \in R$ mit $e^2 = e$, also $e(1 - e) = e - e^2 = 0$. Da $e + (1 - e) = 1 \in R^\times$ ist $e \in R^\times$ oder $1 - e \in R^\times$. Ist $e \in R^\times$, so ist $1 - e = 0$, also $e = 1$. Ist $1 - e \in R^\times$, so ist $e = 0$.

(iii) Ist also M ein R-Modul und $\mathrm{End}_R(M)$ lokal, so ist M unzerlegbar. Die Umkehrung gilt nicht.

Satz 27.6 (Azumaya-Krull-Remak-Schmidt) *Seien M, N isomorphe R-Moduln. Ferner sei $M = M_1 \oplus \ldots \oplus M_m$ mit Untermoduln $M_1, \ldots, M_m$ von M, deren Endomorphismenring lokal ist, und $N = N_1 \oplus \ldots \oplus N_n$ mit unzerlegbaren Untermoduln $N_1, \ldots, N_n$ von N. Dann ist $m = n$ und $M_i \simeq N_i$ für $i = 1, \ldots, n$ bei geeigneter Umnumerierung.*

Beweis: (Induktion nach m) Im Fall $m = 1$ ist M unzerlegbar nach Bemerkung 27.5 (iii), also auch N, d.h. $n = 1$. Sei also $m > 1$. Zu der Zerlegung $M = M_1 \oplus \ldots \oplus M_m$ gehören Projektionen $p_1, \ldots, p_m$ und Injektionen $q_1, \ldots, q_m$, zu der Zerlegung $N = N_1 \oplus \ldots \oplus N_n$ Projektionen $r_1, \ldots, r_n$ und Injektionen $s_1, \ldots, s_n$. Wir setzen $e_i := q_i \circ p_i$ für $i = 1, \ldots, m$, $f_j = s_j \circ r_j$ für $j = 1, \ldots, n$ und wählen einen R-Isomorphismus $g : M \to N$. Dann ist

$$\sum_{j=1}^{n} p_1 g^{-1} s_j r_j g q_1 = p_1 g^{-1} \underbrace{\left(\sum_{j=1}^{n} f_j \right)}_{=\mathrm{id}_N} g q_1 = p_1 q_1 = \mathrm{id}_{M_1} .$$

Da $\mathrm{End}_R(M_1)$ lokal ist, existiert ein $j \in \{1, \ldots, n\}$ mit $p_1 g^{-1} s_j r_j g q_1 \in \mathrm{Aut}_R(M_1)$, o.B.d.A. $j = 1$. Nach 27.4 sind dann $p_1 g^{-1} s_1 : N_1 \to M_1$ und $r_1 g q_1 : M_1 \to N_1$ R-Isomorphismen.
Beh.: $M = g^{-1}(N_1) \oplus (M_2 \oplus \ldots \oplus M_m)$.
Bew.: Ist $x \in g^{-1}(N_1) \cap (M_2 \oplus \ldots \oplus M_m)$, so ist $0 = p_1(x) = p_1(g^{-1}(\underbrace{g(x)}_{\in N_1})) = (p_1 g^{-1} s_1 g)(x)$,

also $g(x) = 0$ und damit $x = 0$. Für $y \in g^{-1}(N_1)$ sind $y, p_2(y), \ldots, p_m(y) \in g^{-1}(N_1) + (M_2 \oplus \ldots \oplus M_m)$, also auch $p_1(y) = y - p_2(y) - \ldots - p_m(y) \in g^{-1}(N_1) + (M_2 \oplus \ldots \oplus M_m)$. Folglich gilt:

$$g^{-1}(N_1) + (M_2 \oplus \ldots \oplus M_m) \supseteq p_1(g^{-1}(N_1)) = p_1(g^{-1}(s_1(N_1))) = M_1,$$

also $M = g^{-1}(N_1) + (M_2 \oplus \ldots \oplus M_m)$.
Nach der Behauptung ist die Abbildung $M/g^{-1}(N_1) \to N/N_1,\ m + g^{-1}(N_1) \mapsto g(m) + N_1$ ein R-Isomorphismus. Daher gilt:

$$M_2 \oplus \ldots \oplus M_m \;\simeq\; M/g^{-1}(N_1) \;\simeq\; N/N_1 \;\simeq\; N_2 \oplus \ldots \oplus N_n.$$

Nach Induktion ist $m - 1 = n - 1$ und $M_i \simeq N_i$ für $i = 2, \ldots, n$ nach geeigneter Umnumerierung.

Lemma 27.7 (Fittings Lemma) *Sei M ein artinscher und noetherscher R-Modul und $f \in \mathrm{End}_R(M)$. Dann existiert ein $k \in \mathbb{N}$, so daß gilt:*

(i) $M \supseteq f(M) \supseteq f^2(M) \supseteq \ldots \supseteq f^k(M) = f^{k+1}(M) = \ldots$

(ii) $0 \subseteq \ker(f) \subseteq \ker(f^2) \subseteq \ldots \subseteq \ker(f^k) = \ker(f^{k+1}) = \ldots$

(iii) $M = \ker(f^k) \oplus f^k(M)$.

Beweis: Da M artinsch ist, bricht die Folge der Untermoduln $M \supseteq f(M) \supseteq f^2(M) \supseteq \ldots$ ab. Da M noethersch ist, bricht analog die Folge $0 \subseteq \ker(f) \subseteq \ker(f^2) \subseteq \ldots$ ab. Daher existiert ein $k \in \mathbb{N}$ mit (i) und (ii). Ist $x \in \ker(f^k) \cap f^k(M)$, so ist $x = f^k(y)$ für ein $y \in M$ und $0 = f^k(x) = f^{2k}(y)$, also $y \in \ker(f^{2k}) = \ker(f^k)$, d.h. $0 = f^k(y) = x$. Für $m \in M$ existiert andrerseits wegen $f^k(M) = f^{2k}(M)$ ein $n \in M$ mit $f^k(m) = f^{2k}(n)$, also $0 = f^k(m - f^k(n))$. Daher ist $m = \underbrace{(m - f^k(n))}_{\in\ker(f^k)} + \underbrace{f^k(n)}_{\in f^k(M)}$.

Satz 27.8 *Sei M ein R-Modul, der artinsch, noethersch und unzerlegbar ist. Dann ist jeder R-Endomorphismus f von M invertierbar oder nilpotent (d.h. $f^n = 0$ für ein $n \in \mathbb{N}$), und $\mathrm{End}_R(M)$ ist lokal.*

Beweis: Sei $f \in \mathrm{End}_R(M)$, also $M = \ker(f^k) \oplus \mathrm{Bild}(f^k)$ für ein $k \in \mathbb{N}$. Da M unzerlegbar ist, folgt: $\ker(f^k) = 0$ oder $\mathrm{Bild}(f^k) = 0$. Im Fall $\ker(f^k) = 0$ ist $M = \mathrm{Bild}(f^k)$, also f^k bijektiv, d.h f bijektiv. Im Fall $f^k(M) = 0$ ist f nilpotent.
Seien $f, g \in \mathrm{End}_R(M)$ nilpotent; zu zeigen ist: $f + g$ nilpotent.
Annahme: $f + g$ invertierbar. Für $f' := (f+g)^{-1}f,\ g' := (f+g)^{-1}g$ gilt also: $f' + g' = \mathrm{id}_M$. Andrerseits sind f', g' nicht invertierbar, also nilpotent. Ist $n \in \mathbb{N}$ mit $(g')^n = 0$, so ist

$$\begin{aligned}(\mathrm{id}_M - g')(\mathrm{id}_M + g' + (g')^2 + \ldots + (g')^n) \;&= \\ =\; \mathrm{id}_M - (g')^{n+1} \;=\; \mathrm{id}_M \;&=\; (\mathrm{id}_M + g' + (g')^2 + \ldots + (g')^n)(\mathrm{id}_M - g').\end{aligned}$$

Also ist $f' = \mathrm{id}_M - g'$ invertierbar. Widerspruch.

Satz 27.9 *Jeder R-Modul M, der artinsch oder noethersch ist, hat eine Zerlegung $M = M_1 \oplus \ldots \oplus M_n$ in endlich viele unzerlegbare Untermoduln $M_1, \ldots, M_n$.*

Beweis: Sei M artinsch und $\mathcal{M}$ die Menge aller Untermoduln von M, die sich nicht als direkte Summe von endlich vielen unzerlegbaren Untermoduln schreiben lassen. Ist $\mathcal{M} \neq \emptyset$, so enthält $\mathcal{M}$ ein minimales Element N. Dann ist $N \neq 0$, und N ist zerlegbar, etwa $N = N_1 \oplus N_2$ mit echten Untermoduln N_1, N_2 von N. Für $i = 1, 2$ ist dann $N_i \notin \mathcal{M}$, d.h. N_i ist direkte Summe endlich vieler unzerlegbarer Untermoduln, also auch N. Widerspruch.
Sei M noethersch und $\mathcal{M}$ die Menge aller Untermoduln N von M mit der Eigenschaft, daß sich M/N nicht als direkte Summe endlich vieler unzerlegbarer Untermoduln schreiben läßt. Ist $\mathcal{M} \neq \emptyset$, so enthält $\mathcal{M}$ ein maximales Element N. Dann ist $M/N \neq 0$, und M/N ist zerlegbar, etwa $M/N = M_1/N \oplus M_2/N$ mit Untermoduln M_1, M_2 von M, die N echt enthalten. Für $i = 1, 2$ ist $M_i \notin \mathcal{M}$, d.h. M/M_i ist direkte Summe endlich vieler unzerlegbarer Untermoduln. Wegen $M/M_1 \simeq (M/N)/(M_1/N) \simeq M_2/N$ und $M/M_2 \simeq M_1/N$ sind $M_1/N, M_2/N$ direkte Summen endlich vieler unzerlegbarer Untermoduln, also auch M/N. Widerspruch.

Bemerkung: Ist M sowohl artinsch als auch noethersch, so folgt aus 27.6 und 27.8, daß die Zerlegung $M = M_1 \oplus \ldots \oplus M_n$ in unzerlegbare Untermoduln $M_1, \ldots, M_n$ im wesentlichen eindeutig ist.

Kapitel 28

Freie Moduln

Sei R ein Ring.

Definition 28.1 *Sei M ein R-Modul und $X \subseteq M$. Man nennt X* linear unabhängig *(über R), falls gilt: Ist $r_x \in R$ für $x \in X$, $|\{x \in X : r_x \neq 0\}| < \infty$ und $\sum_{x \in X} r_x x = 0$, so ist $r_x = 0$ für alle $x \in X$. Andernfalls nennt man X* linear abhängig *(über R).*

Bemerkung:

(i) Ist X linear unabhängig, so auch jede Teilmenge von X.

(ii) Ist jede endliche Teilmenge von X linear unabhängig, so auch X.

(iii) $\emptyset$ ist stets linear unabhängig.

(iv) $\{0\}$ ist für $R \neq 0$ linear abhängig.

(v) Für jede endliche abelsche Gruppe $(G, +)$ und $g \in G$ ist $|G|\, g = 0$ nach Lagrange. Daher ist $\emptyset$ die einzige linear unabhängige Teilmenge des $\mathbf{Z}$-Moduls G.

Definition 28.2 *Sei M ein R-Modul. Ein linear unabhängiges Erzeugendensystem von M nennt man auch* Basis *von M (über R). Besitzt M eine Basis, so nennt man M* frei *(über R).*

Beispiel:

(i) $\emptyset$ ist Basis von 0.

(ii) $\{1\}$ ist Basis von R über R. Allgemeiner bilden $(1, 0, \ldots, 0)$, $(0, 1, 0, \ldots, 0)$, $\ldots$, $(0, \ldots, 0, 1)$ eine Basis von R^n für $n \in \mathbb{N}$. Noch allgemeiner ist für jede nichtleere Menge I der R-Modul $\coprod_{i \in I} R_i$ mit $R_i = R$ für $i \in I$ frei mit Basis $\{e_i : i \in I\}$, wobei $e_i(j) = \delta_{ij} 1_R$ für $i, j \in I$.

(iii) Ist $(G, +)$ eine von 0 verschiedene endliche abelsche Gruppe, so besitzt G als $\mathbf{Z}$-Modul keine Basis. Statt „freier $\mathbf{Z}$-Modul“ sagt man auch *freie abelsche Gruppe.*

(iv) Ist R ein Schiefkörper, so besitzt jeder R-Modul eine Basis. Dies beweist man wie 23.4.

Bemerkung: Sei M ein freier R-Modul mit Basis B. Dann existieren zu jedem $m \in M$ eindeutig bestimmte Elemente $r_b \in R$ $(b \in B)$ mit $|\{b \in B : r_b \neq 0\}| < \infty$ und $\sum_{b \in B} r_b b = m$. Setzt man $R_b := R$ für $b \in B$, so ist also die Abbildung $\coprod_{b \in B} R_b \to M,\ (r_b)_{b \in B} \mapsto \sum_{b \in B} r_b b$ ein R-Isomorphismus.

Satz: *Jeder endlich erzeugte freie R-Modul M besitzt eine endliche Basis.*

Beweis: Sei $M = Rm_1 + \ldots + Rm_n$ und B eine Basis von M. Dann existiert eine endliche Teilmenge C von B, so daß $m_1, \ldots, m_n$ Linearkombinationen von Elementen in C sind. Daher wird M auch von C erzeugt, d.h. C ist Basis von M.

Bemerkung 28.3 Ein freier Modul kann Basen verschiedener Größe enthalten.

Beispiel: Sei V Vektorraum über dem Körper K mit abzählbar unendlicher Basis (z.B. $V = K[X]$). Dann hat auch $V \times V$ eine abzählbar unendliche Basis. Es existiert also eine lineare Bijektion $f : V \to V \times V$. Wir schreiben $f(v) = (f_1(v), f_2(v))$ für $v \in V$. Dann sind $f_1, f_2 : V \to V$ linear. Wir setzen $R := \mathrm{End}_K(V)$ und definieren eine Abbildung $F : R \times R \to R$ folgendermaßen: Für $\varphi, \psi \in R = \mathrm{End}_K(V)$ sei $F(\varphi, \psi) \in R = \mathrm{End}_K(V)$ definiert durch

$$\big(F(\varphi,\psi)\big)(v) := \varphi(f_1(v)) + \psi(f_2(v)) \qquad \text{für } v \in V.$$

Es ist leicht zu sehen, daß F wohldefiniert und additiv ist. Für $v \in V$ und $r, \varphi, \psi \in R$ ist

$$\begin{aligned} \big(F(r(\varphi,\psi))\big)(v) &= \big(F(r\varphi, r\psi)\big)(v) = (r\varphi)(f_1(v)) + (r\psi)(f_2(v)) = \\ &= r(\varphi(f_1(v)) + \psi(f_2(v))) = r\big(F(\varphi,\psi)\big)(v). \end{aligned}$$

Daher ist F ein R-Homomorphismus.
Ist $(\varphi, \psi) \in \ker(F)$, so ist $\varphi(f_1(v)) + \psi(f_2(v)) = 0$ für $v \in V$, also $\varphi(x) + \psi(y) = 0$ für alle $x, y \in V$ wegen der Surjektivität von f. Folglich ist $\varphi = 0 = \psi$. Dies zeigt, daß F injektiv ist.
Sei $g \in R$, und seien $q_1, q_2 : V \to V \times V$ die beiden Injektionen. Dann ist $(g \circ f^{-1} \circ q_1, g \circ f^{-1} \circ q_2) \in R \times R$ mit

$$\begin{aligned} \big(F(gf^{-1}q_1, gf^{-1}q_2)\big)(v) &= (gf^{-1}q_1)(f_1(v)) + (gf^{-1}q_2)(f_2(v)) = \\ &= gf^{-1}(f_1(v), f_2(v)) = g(v) \qquad \text{für } v \in V. \end{aligned}$$

Dies zeigt, daß F auch surjektiv ist. Also ist $R \simeq R \times R$, d.h. R hat R-Basen der Länge 1 und 2.

Satz: *Ist R kommutativ und F ein endlich erzeugter freier R-Modul, so besitzen je zwei Basen von F die gleiche Anzahl von Elementen.*

Beweis: Wir wissen, daß R ein maximales Ideal M enthält. Es ist leicht zu sehen, daß $MF := \{\sum_{i=1}^n m_i f_i : m_1, \ldots, m_n \in M,\ f_1, \ldots, f_n \in F,\ n \in \mathbb{N}_0\}$ ein R-Untermodul von F ist. Daher ist F/MF auch ein R-Modul. Man rechnet leicht nach, daß F/MF zu einem Vektorraum über dem Körper R/M wird, wenn man definiert: $(r + M)(f + MF) := rf + MF$ für $r \in R,\ f \in F$. Ist B eine Basis von F über R, so ist $F = \bigoplus_{b \in B} Rb,\ MF = \bigoplus_{b \in B} Mb,\ F/MF = \bigoplus_{b \in B} (R/M)(b + MF)$ und $b \notin MF$ für $b \in B$. Daher ist $\{b + MF : b \in B\}$ Basis von F/MF. Es ist also $|B| = \dim(F/MF)$.

Definition: *Ist R kommutativ und F ein endlich erzeugter freier R-Modul mit Basis B, so bezeichnet man $|B|$ als* Rang *von F und schreibt $|B| = \mathrm{rg}(F)$.*

Satz 28.4 *Ist R Schiefkörper und M ein endlich erzeugter R-Modul, so besitzen je zwei Basen von M die gleiche Anzahl von Elementen.*

Beweis: Für jede Basis $b_1, \ldots, b_n$ von M ist $0 \subsetneq Rb_1 \subsetneq Rb_1 + Rb_2 \subsetneq \ldots \subsetneq Rb_1 + \ldots + Rb_n = M$ eine Kompositionsreihe von M, d.h. n ist die Kompositionslänge von M.

Bemerkung: Man spricht hier auch von *Vektorräumen* über R und ihrer *Dimension* bzw. ihrem *Rang*.

Satz 28.5 *Jeder R-Modul M ist zu einem Faktormodul eines freien R-Moduls isomorph.*

Beweis: Sei E ein Erzeugendensystem von M (notfalls $E = M$). Dann ist $F := \coprod_{e \in E} R_e$, wobei $R_e := R$ für $e \in E$, ein freier R-Modul, und die Abbildung $f : F \to M,\ (r_e)_{e \in E} \mapsto \sum_{e \in E} r_e e$ ist ein R-Epimorphismus. Daher ist $M \simeq F/\ker(f)$.

Bemerkung: Der Beweis zeigt, daß man im Fall, daß M endlich erzeugt ist, F als endlich erzeugten freien R-Modul wählen kann.

Kapitel 29

Einfache und halbeinfache Moduln

Sei R ein Ring.

Satz 29.1 (Schurs Lemma, 1875–1941) *Für R-Moduln M, N gilt:*

(i) Ist M einfach, so ist jedes $f \in \mathrm{Hom}_R(M, N) \setminus \{0\}$ injektiv.

(ii) Ist N einfach, so ist jedes $f \in \mathrm{Hom}_R(M, N) \setminus \{0\}$ surjektiv.

(iii) Sind M und N einfach und nichtisomorph, so ist $\mathrm{Hom}_R(M, N) = 0$.

(iv) Ist M einfach, so ist $\mathrm{End}_R(M)$ Schiefkörper.

Beweis: Aufgabe 1 von Blatt 4.

Definition 29.2 *Ein echtes Linksideal M von R nennt man* maximal*, falls kein Linksideal L in R existiert mit $M \underset{\neq}{\subset} L \underset{\neq}{\subset} R$.*

Bemerkung:

(i) Ein Linksideal M in R ist also genau dann maximal, wenn R/M ein einfacher R-Modul ist.

(ii) Die Existenz maximaler Linksideale beweist man wie in 23.5 mit Zorns Lemma; insbesondere besitzt R im Fall $R \neq 0$ einfache Moduln.

Satz: *Zu jedem einfachen R-Modul S existiert ein maximales Linksideal M von R mit $S \simeq R/M$.*

Beweis: Sei $s \in S \setminus \{0\}$. Dann ist die Abbildung $f : R \to S,\ r \mapsto rs$ ein von 0 verschiedener R-Homomorphismus. Nach 29.1 ist f surjektiv, also $S \simeq R/M$ mit $M := \ker(f)$. Mit S ist auch R/M einfach, d.h. M ist maximales Linksideal in R.

Satz 29.3 *Für einen R-Modul M sind äquivalent:*

(1) M ist Summe einfacher Untermoduln.

(2) M ist direkte Summe einfacher Untermoduln.

(3) Jeder Untermodul von M ist direkter Summand von M, d.h. zu jedem Untermodul N von M existiert ein Untermodul N' von M mit $M = N \oplus N'$.

Definition: *Gegebenenfalls nennt man M* halbeinfach *oder* vollständig reduzibel.

Beweis:

(1)⇒(2): Sei $M = \sum_{i\in I} M_i$ mit einfachen Untermoduln M_i von M ($i \in I$). Dann ist $\mathcal{I} := \{J \subseteq I : \sum_{j\in J} M_j \text{ direkt}\}$ nichtleer wegen $\emptyset \in \mathcal{I}$ und geordnet durch $\subseteq$. Ist $\mathcal{K}$ eine nichtleere total geordnete Teilmenge von $\mathcal{I}$ und $S := \sum_{K\in\mathcal{K}} K$, so ist $\sum_{s\in S} M_s$ direkt, denn sonst existiert eine endliche Teilmenge T von S, so daß $\sum_{t\in T} M_t$ nicht direkt ist. Ferner ist dann $T \subseteq K$ für ein $K \in \mathcal{K}$, also auch $\sum_{k\in K} M_k$ nicht direkt im Widerspruch zu $K \in \mathcal{K} \subseteq \mathcal{I}$. Dies zeigt, daß S obere Schranke von $\mathcal{K}$ in $\mathcal{I}$ ist. Nach Zorn enthält also $\mathcal{I}$ ein maximales Element Z. Wäre $\sum_{z\in Z} M_z \neq M$, so wäre $M_i \not\subseteq \sum_{z\in Z} M_z$ für ein $i \in I$. Dann wäre aber $M_i \cap \sum_{z\in Z} M_z = 0$, da M_i einfach ist, also $M_i + \sum_{z\in Z} M_z$ direkt, d.h. $Z \cup \{i\} \in \mathcal{I}$ im Widerspruch zur Wahl von Z. Daher ist $M = \sum_{z\in Z} M_z = \bigoplus_{z\in Z} M_z$.

(2)⇒(3): Sei $M = \bigoplus_{i\in I} M_i$ mit einfachen Untermoduln M_i von M ($i \in I$), und sei N Untermodul von M. Dann ist $\mathcal{I} := \{J \subseteq I : N + \sum_{j\in J} M_j \text{ direkt}\}$ wegen $\emptyset \in \mathcal{I}$ nichtleer und geordnet durch $\subseteq$. Wie oben zeigt man, daß jede nichtleere total geordnete Teilmenge von $\mathcal{I}$ eine obere Schranke in $\mathcal{I}$ hat. Nach Zorn enthält $\mathcal{I}$ also ein maximales Element Z. Wäre $N + \sum_{z\in Z} M_z \neq M$, so wäre $M_i \not\subseteq N + \sum_{z\in Z} M_z$ für ein $i \in I$. Dann wäre aber $M_i \cap (N + \sum_{z\in Z} M_z) = 0$ wegen der Einfachheit von M_i, also $N + M_i + \sum_{z\in Z} M_z$ direkt und $Z \cup \{i\} \in \mathcal{I}$ im Widerspruch zur Wahl von Z.

(3)⇒(1): Sei (3) erfüllt und S die Summe aller einfachen Untermoduln von M. Dann existiert ein Untermodul N von M mit $M = S \oplus N$. Ist $N \neq 0$ und $x \in N \setminus \{0\}$, so ist die Abbildung $f : R \to N$, $r \mapsto rx$ ein von 0 verschiedener R-Homomorphismus mit Bild Rx. Nach Bemerkung 29.2 existiert dann ein maximales Linksideal L von R mit $\ker(f) \subseteq L \subseteq R$. Dann ist $f(L)$ ein Untermodul von $f(R) = Rx$ mit $R/L \simeq f(R)/f(L)$; insbesondere ist $Rx/f(L)$ einfach. Wegen (3) existiert ein Untermodul K von M mit $M = f(L) \oplus K$, also $Rx = Rx \cap M = Rx \cap (f(L) \oplus K) = f(L) \oplus (Rx \cap K)$ nach Dedekind. Wegen $K \cap Rx \simeq Rx/f(L)$ ist $K \cap Rx$ einfach, also $K \cap Rx \subseteq S \cap N = 0$. Widerspruch.

Satz 29.4 *Sei N Untermodul eines halbeinfachen R-Moduls M. Dann sind auch N und M/N halbeinfach.*

Beweis: Zu jedem Untermodul U von N existiert nach Voraussetzung ein Untermodul V von M mit $M = U \oplus V$. Nach Dedekind ist also $N = N \cap M = N \cap (U + V) = U + (N \cap V) = U \oplus (N \cap V)$. Daher ist N halbeinfach. Ferner existiert ein Untermodul N' von M mit $M = N \oplus N'$. Dann ist analog N' halbeinfach, also auch M/N wegen $M/N \simeq N'$.

Definition 29.5 *Man nennt R* halbeinfach, *wenn R als R-Modul halbeinfach ist.*

Bemerkung:

(i) Genauer müßte man „linkshalbeinfach“ sagen. Es wird sich aber bald herausstellen, daß jeder „linkshalbeinfache“ Ring auch „rechtshalbeinfach“ ist und umgekehrt.

(ii) Sei R halbeinfach und $R = \bigoplus_{i\in I} M_i$ mit einfachen Untermodulen (Linksidealen) M_i von R. Wir schreiben $1 = \sum_{i\in I} m_i$ mit $m_i \in M_i$ für $i \in I$; dabei ist $J := \{i \in I : m_i \neq 0\}$ endlich. Dann ist $1 = \sum_{i\in J} m_i$, also $r = r1 = \sum_{i\in J} rm_i \in \sum_{i\in J} M_i$ für $r \in R$. Folglich ist $R = \bigoplus_{i\in J} M_i$. Dies zeigt, daß R direkte Summe *endlich* vieler einfacher Untermoduln ist. Insbesondere ist R linksartinsch und linksnoethersch. Nach Jordan-Hölder und 29.2 existieren dann nur endlich viele Isomorphie-Klassen einfacher R-Moduln.

Satz: *Ist R halbeinfach, so auch jeder R-Modul M.*

Beweis: Für $m \in M$ ist die Abbildung $f_m : R \to M,\ r \mapsto rm$ ein R-Homomorphismus. Nach 29.4 ist also $Rm = f_m(R) \simeq R/\ker(f_m)$ halbeinfach, d.h. Summe von einfachen Untermoduln. Wegen $m \in Rm$ für $m \in M$ ist also auch M Summe einfacher Untermoduln.

Satz 29.6

(i) *Für* $n \in \mathbb{N}$ *und jeden* R*-Modul* M *ist* $\mathrm{End}_R(M^n) \cong \mathrm{Mat}(n, \mathrm{End}_R(M))$.

(ii) *Für* $n \in \mathbb{N}$ *und* R*-Moduln* $M_1, \ldots, M_n$ *mit* $\mathrm{Hom}_R(M_i, M_j) = 0$ *für alle* $i, j = 1, \ldots, n$ *mit* $i \neq j$ *ist* $\mathrm{End}_R(M_1 \times \ldots \times M_n) \cong \mathrm{End}_R(M_1) \times \ldots \times \mathrm{End}_R(M_n)$.

(iii) *Für jedes* $e \in R$ *mit* $e^2 = e$ *ist* $\mathrm{End}_R(Re) \cong (eRe)^o$*; insbesondere ist* $\mathrm{End}_R(R) \cong R^o$.

Beweis: Aufgabe 2 von Blatt 4.

Satz 29.7 (Wedderburn, 1882–1948) *Äquivalent sind:*

(1) R *ist halbeinfach.*

(2) *Es existieren* $l \in \mathbb{N}_0,\ d_1, \ldots, d_l \in \mathbb{N}$ *und Schiefkörper* $D_1, \ldots, D_l$ *mit*

$$R \ \cong\ \mathrm{Mat}(d_1, D_1) \times \ldots \times \mathrm{Mat}(d_l, D_l).$$

Gegebenenfalls sind $l, d_1, \ldots, d_l$ *eindeutig und* $D_1, \ldots, D_l$ *eindeutig bis auf Isomorphie.*

Beweis:

(1)⇒(2): Ist R halbeinfach, so existieren $l \in \mathbb{N}_0,\ d_1, \ldots, d_l \in \mathbb{N}$ und paarweise nichtisomorphe einfache R-Moduln $M_1, \ldots, M_l$ mit $R \cong M_1^{d_1} \times \ldots \times M_l^{d_l}$. Für $i, j = 1, \ldots, l$ mit $i \neq j$ ist $\mathrm{Hom}_R(M_i, M_j) = 0$ nach Schur (da M_i, M_j nichtisomorph), also $\mathrm{Hom}_R(M_i^{d_i}, M_j^{d_j}) = 0$. Daher gilt nach 29.6:

$$\begin{aligned} R^o &\cong \mathrm{End}_R(R) \ \cong \\ &\cong \mathrm{End}_R(M_1^{d_1} \times \ldots \times M_l^{d_l}) \ \cong \\ &\cong \mathrm{End}_R(M_1^{d_1}) \times \ldots \times \mathrm{End}_R(M_l^{d_l}) \ \cong \\ &\cong \mathrm{Mat}(d_1, \mathrm{End}_R(M_1)) \times \ldots \times \mathrm{Mat}(d_l, \mathrm{End}_R(M_l)). \end{aligned}$$

Nach Schur ist dabei $D_i := \mathrm{End}_R(M_i)$ Schiefkörper für $i = 1, \ldots, l$. Folglich gilt:

$$\begin{aligned} R &\cong (\mathrm{Mat}(d_1, D_1) \times \ldots \times \mathrm{Mat}(d_l, D_l))^o \ = \\ &= \mathrm{Mat}(d_1, D_1)^o \times \ldots \times \mathrm{Mat}(d_l, D_l)^o \ \cong \\ &\cong \mathrm{Mat}(d_1, D_1^o) \times \ldots \times \mathrm{Mat}(d_l, D_l^o) \end{aligned}$$

mit Schiefkörpern $D_1^o, \ldots, D_l^o$, wie man leicht nachrechnet.

(2)⇒(1): Sei $R := \mathrm{Mat}(d_1, D_1) \times \ldots \times \mathrm{Mat}(d_l, D_l)$ mit $l \in \mathbb{N}_0,\ d_1, \ldots, d_l \in \mathbb{N}$ und Schiefkörpern $D_1, \ldots, D_l$. Man rechnet leicht nach, daß

$$L_{ij} := 0 \times \ldots \times 0 \times \begin{array}{c} j\text{-te Spalte} \\ \downarrow \\ \underbrace{\begin{pmatrix} 0 & \cdots & 0 & * & 0 & \cdots & 0 \\ \vdots & & \vdots & \vdots & \vdots & & \vdots \\ 0 & \cdots & 0 & * & 0 & \cdots & 0 \end{pmatrix}}_{i} \end{array} \times 0 \times \ldots \times 0$$

für $i = 1, \ldots, l$, $j = 1, \ldots, d_i$ ein einfacher Untermodul von R ist. Wegen $R = \bigoplus_{i=1}^{l} \bigoplus_{j=1}^{d_i} L_{ij}$ ist also R halbeinfach.
Für verschiedene $i, i' \in \{1, \ldots, l\}$ und beliebige $j \in \{1, \ldots, d_i\}$, $j' \in \{1, \ldots, d_{i'}\}$ sind L_{ij} und $L_{i'j'}$ nichtisomorph, denn sie haben verschiedene Annullatoren. Für $i = 1, \ldots, l$ und $j, j' = 1, \ldots, d_i$ sind dagegen L_{ij} und $L_{ij'}$ isomorph, denn $L_{ij'}$ entsteht aus L_{ij} durch Multiplikation von rechts mit einer Permutationsmatrix. Daher ist l die Anzahl der Isomorphie-Klassen einfacher R-Linksmoduln, und $d_1, \ldots, d_l$ sind nach Jordan-Hölder eindeutig bestimmt.
Für $i = 1, \ldots, l$ ist

$$e_i := (0, \ldots, 0, \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & & & \\ \vdots & & 0 & \\ 0 & & & \end{pmatrix}, 0, \ldots, 0) \in R$$

mit $e_i^2 = e_i$ und $L_{i1} = Re_i$. Daher gilt nach 29.6

$$\begin{aligned} \mathrm{End}_R(L_{i1}) &= \mathrm{End}_R(Re_i) \cong (e_i R e_i)^o = \\ &= (0 \times \ldots \times 0 \times \begin{pmatrix} D_i & 0 & \cdots & 0 \\ 0 & & & \\ \vdots & & 0 & \\ 0 & & & \end{pmatrix} \times 0 \times \ldots \times 0)^o \cong D_i^o. \end{aligned}$$

Daher sind $D_1, \ldots, D_l$ eindeutig bestimmt.

Kapitel 30

Projektive und injektive Moduln

Sei R ein Ring.

Definition 30.1 *Eine Folge $L \xrightarrow{f} M \xrightarrow{g} N$ von R-Homomorphismen f, g zwischen R-Moduln L, M, N nennt man* exakt, *falls* $\mathrm{Bild}(f) = \ker(g)$.
Eine (endliche oder unendliche) Folge von R-Homomorphismen

$$\ldots \longrightarrow M_{n+1} \xrightarrow{f_{n+1}} M_n \xrightarrow{f_n} M_{n-1} \longrightarrow \ldots$$

nennt man exakt, *wenn jede Teilfolge der Form $M_{n+1} \xrightarrow{f_{n+1}} M_n \xrightarrow{f_n} M_{n-1}$ exakt ist.*
Eine kurze exakte Folge *von R-Homomorphismen ist eine exakte Folge von R-Homomorphismen der Form $0 \longrightarrow L \xrightarrow{f} M \xrightarrow{g} N \longrightarrow 0$; die Abbildungen von $0 \to L$ und $N \to 0$ sind dabei (natürlich) Nullabbildungen.*

Bemerkung:

(i) Eine Folge von R-Homomorphismen der Form $0 \longrightarrow L \xrightarrow{f} M$ ist genau dann exakt, wenn $\ker(f) = 0$, d.h. f injektiv ist.

(ii) Eine Folge von R-Homomorphismen der Form $M \xrightarrow{g} N \longrightarrow 0$ ist genau dann exakt, wenn $\mathrm{Bild}(g) = N$, d.h. g surjektiv ist.

(iii) Eine Folge von R-Homomorphismen der Form $0 \longrightarrow M \xrightarrow{g} N \longrightarrow 0$ ist genau dann exakt, wenn g bijektiv ist.

(iv) Eine Folge von R-Homomorphismen der Form $0 \longrightarrow L \xrightarrow{f} M \xrightarrow{g} N \longrightarrow 0$ ist genau dann exakt, wenn f injektiv, g surjektiv und $\mathrm{Bild}(f) = \ker(g)$ ist. In diesem Fall gilt nach dem Homomorphie-Satz: $N \simeq M/\ker(g) = M/\mathrm{Bild}(f)$ und $\mathrm{Bild}(f) \simeq L$.

Beispiel:

(i) Jeder R-Homomorphismus $f : M \to N$ induziert eine kurze exakte Folge

$$0 \longrightarrow \ker(f) \longrightarrow M \xrightarrow{f} \mathrm{Bild}(f) \longrightarrow 0,$$

dabei ist $\ker(f) \to M$ die Inklusionsabbildung und $M \to \mathrm{Bild}(f)$ die Einschränkung von f.

(ii) Für jeden Untermodul U eines R-Moduls M erhält man insbesondere eine kurze exakte Folge der Form

$$0 \longrightarrow U \longrightarrow M \longrightarrow M/U \longrightarrow 0,$$

dabei ist $U \to M$ die Inklusionsabbildung und $M \to M/U$ der kanonische Epimorphismus.

Satz 30.2 *Für eine kurze exakte Folge von R-Homomorphismen der Form* $0 \longrightarrow L \xrightarrow{f} M \xrightarrow{g} N \longrightarrow 0$ *sind äquivalent:*

(1) Es existiert ein R-Homomorphismus $g' : N \to M$ *mit* $g \circ g' = \mathrm{id}_N$.

(2) Es existiert ein R-Homomorphismus $f' : M \to L$ *mit* $f' \circ f = \mathrm{id}_L$.

(3) Es existiert ein Untermodul U *von* M *mit* $M = f(L) \oplus U$.

Bemerkung: Gegebenenfalls sagt man, die kurze exakte Folge $0 \longrightarrow L \longrightarrow M \longrightarrow N \longrightarrow 0$ *zerfällt*. Der Beweis wird zeigen, daß dann gilt: $M = \mathrm{Bild}(f) \oplus \ker(f') = \ker(g) \oplus \mathrm{Bild}(g')$.

Beweis:

(1)⇒(3): Sei (1) erfüllt. Für $m \in M$ ist dann $g(m - g'(g(m))) = g(m) - g(m) = 0$, also $m - g'(g(m)) \in \ker(g)$ und $m = (m - g'(g(m))) + g'(g(m))$ mit $g'(g(m)) \in \mathrm{Bild}(g')$.
Ist $x \in \ker(g) \cap \mathrm{Bild}(g')$ und $x = g'(y)$ mit $y \in N$, so ist $0 = g(x) = g(g'(y)) = y$, also $0 = g'(y) = x$.
Daher ist $M = \ker(g) \oplus \mathrm{Bild}(g') = \mathrm{Bild}(f) \oplus \mathrm{Bild}(g')$.

(3)⇒(1): Sei (3) erfüllt und $h : U \to N$ die Einschränkung von g. Wegen $f(L) = \ker(g)$ und der Surjektivität von g ist h bijektiv. Die Abbildung $g' : N \to M$, $n \mapsto h^{-1}(n)$ ist ein R-Homomorphismus mit $g(g'(n)) = h(h^{-1}(n)) = n$ für $n \in N$.

(2)⇔(3): Analog.

Beispiel: Für beliebige R-Moduln L, N zerfällt die exakte Folge $0 \longrightarrow L \underset{p_1}{\overset{q_1}{\rightleftarrows}} L \times N \underset{q_2}{\overset{p_2}{\rightleftarrows}} N \longrightarrow 0$, dabei sind p_1, p_2, q_1, q_2 die entsprechenden Projektionen bzw. Injektionen.

Satz 30.3 *Für einen R-Modul P sind äquivalent:*

(1) P ist zu einem direkten Summanden eines freien R-Moduls isomorph.

(2) Zu jedem R-Epimorphismus $M \xrightarrow{f} N$ *und jedem R-Homomorphismus* $g : P \to N$ *existiert ein R-Homomorphismus* $h : P \to M$ *mit* $g = f \circ h$.

$$\begin{tikzcd}
 & P \arrow[dl, "h"'] \arrow[d, "g"] & \\
M \arrow[r, "f"] & N \arrow[r] & 0
\end{tikzcd}$$

(3) Jede kurze exakte Folge von R-Homomorphismen der Form $0 \longrightarrow L \xrightarrow{f} M \xrightarrow{g} P \longrightarrow 0$ *zerfällt.*

Definition: *Gegebenenfalls nennt man P* projektiv.

Beweis:

(1)⇒(2): Sei (1) erfüllt und o.B.d.A. P selbst direkter Summand eines freien R-Moduls F, etwa $F = P \oplus Q$ mit einem Untermodul Q von F. Die zugehörigen Injektionen und Projektionen seien q_1, q_2 bzw. p_1, p_2. Ferner sei B R-Basis von F. Für $b \in B$ existiert wegen der Surjektivität von f ein $m_b \in M$ mit $g(p_1(b)) = f(m_b)$.

$$\begin{tikzcd}
 & F \arrow[d, "p_1"] \arrow[ddl, "k"'] & \\
 & P \arrow[d, "g"] \arrow[dl, "h"'] & \\
M \arrow[r, "g"] & N \arrow[r] & 0
\end{tikzcd}$$

Wir definieren eine Abbildung $k : F \to M$ durch $k(\sum_{b\in B} r_b b) := \sum_{b\in B} r_b m_b$ für Elemente $r_b \in R$ $(b \in B)$ mit $|\{b \in B : r_b \neq 0\}| < \infty$. Offenbar ist k ein R-Homomorphismus mit $f \circ k = g \circ p_1$. Für die Einschränkung $h : P \to M$ von k und $x \in P$ gilt dann: $f(h(x)) = f(k(x)) = g(p_1(x)) = g(x)$.

(2)⇒(3): Sei (2) erfüllt und $0 \longrightarrow L \xrightarrow{f} M \xrightarrow{g} P \longrightarrow 0$ eine exakte Folge von R-Homomorphismen. Dann existiert ein R-Homomorphismus $h : P \to M$ mit $g \circ h = \mathrm{id}_P$. Also zerfällt die Folge.

$$\begin{tikzcd}
 & P \arrow[d, "\mathrm{id}_P"] \arrow[dl, "h"'] & \\
M \arrow[r, "g"] & P \arrow[r] & 0
\end{tikzcd}$$

(3)⇒(1): Nach 28.5 existieren ein freier R-Modul F und ein R-Epimorphismus $g : F \to P$. Ist (3) erfüllt, so zerfällt die exakte Folge $0 \longrightarrow \ker(g) \longrightarrow F \underset{g'}{\overset{g}{\rightleftarrows}} P \longrightarrow 0$. Es existiert also ein R-Homomorphismus $g' : P \to F$ mit $g \circ g' = \mathrm{id}_P$. Nach 30.2 ist also $F = \ker(g) \oplus \mathrm{Bild}(g')$. Wegen $g \circ g' = \mathrm{id}_P$ ist g' injektiv, also $\mathrm{Bild}(g') \simeq P$.

Bemerkung:

(i) Der obige Beweis und 28.5 zeigen, daß jeder endlich erzeugte projektive R-Modul zu einem direkten Summanden eines endlich erzeugten freien R-Moduls isomorph ist.

(ii) Freie Moduln sind projektiv; insbesondere ist R selbst projektiv.

(iii) Direkte Summanden von projektiven R-Moduln sind projektiv; insbesondere sind direkte Summanden von R projektiv.

(iv) Da Koprodukte von freien R-Moduln frei sind, sind Koprodukte von projektiven R-Moduln projektiv.

Satz 30.4 *Für einen R-Modul Q sind äquivalent:*

(1) Zu jeder exakten Folge von R-Homomorphismen $0 \longrightarrow M \xrightarrow{f} N$ und jedem R-Homomorphismus $g : M \to Q$ existiert ein R-Homomorphismus $h : N \to Q$ mit $g = h \circ f$.

$$\begin{tikzcd}
0 \arrow[r] & M \arrow[r, "f"] \arrow[d, "g"'] & N \arrow[dl, "h"] \\
 & Q &
\end{tikzcd}$$

(2) Zu jedem Linksmodul L von R und jedem R-Homomorphismus $g : L \to Q$ existiert ein R-Homomorphismus $h : R \to Q$, der g fortsetzt.

(3) Zu jedem Linksideal L von R und jedem R-Homomorphismus $g : L \to Q$ existiert ein $x \in Q$ mit $g(a) = ax$ für $a \in L$.

Definition: *Gegebenenfalls nennt man Q* injektiv.

Beweis:

(1)⇒(2): (2) ist folgender Spezialfall von (1):

$$\begin{tikzcd}
0 \arrow[r] & L \arrow[r] \arrow[d, "g"'] & R \arrow[dl, "h"] \\
 & Q &
\end{tikzcd}$$

(2)⇒(3): Sei L Linksideal in R, $h : R \to Q$ ein R-Homomorphismus und $g : L \to Q$ die Einschränkung von h. Für $a \in L$ ist dann $g(a) = h(a) = h(a1) = a\underbrace{h(1)}_{x}$.

(3)⇒(1): Sei $0 \longrightarrow M \xrightarrow{f} N$ eine exakte Folge von R-Homomorphismen, $g : M \to Q$ ein R-Homomorphismus und $\mathcal{M}$ die Menge aller Paare (L, l), wobei L ein Untermodul von N mit $f(M) \subseteq L$ und $l : L \to Q$ ein R-Homomorphismus mit $l \circ f = g$ ist. Offenbar ist $\mathcal{M}$ nichtleer und durch $\leq$ geordnet, wenn man definiert:

$$(L, l) \leq (L', l') \;:\Leftrightarrow\; L \subseteq L' \;\wedge\; l = l'|L.$$

Man rechnet schnell nach, daß jede nichtleere total geordnete Teilmenge von $\mathcal{M}$ eine obere Schranke in $\mathcal{M}$ besitzt. Nach Zorn enthält $\mathcal{M}$ ein maximales Element (Z, z). Im Fall $Z = N$ sind wir fertig. Wir nehmen $Z \neq N$ an und wählen ein Element $y \in N \setminus Z$. Dann ist $I := \{a \in R : ay \in Z\}$ ein Linksideal in R, und die Abbildung $\gamma : I \to Q,\ a \mapsto z(ay)$ ist ein R-Homomorphismus. Ist (3) erfüllt, so existiert ein Element $x \in Q$ mit $\gamma(a) = ax$ für $a \in I$. Wir setzen $Z' := Z + Ry$ und definieren eine Abbildung $z' : Z' \to Q$ durch $z'(a + ry) := z(a) + rx$ für $a \in Z,\ r \in R$. Dies ist wohldefiniert; sind nämlich $a_1, a_2 \in Z,\ r_1, r_2 \in R$ mit $a_1 + r_1 y = a_2 + r_2 y$, so ist $(r_1 - r_2)y = a_2 - a_1 \in Z$, also $r_1 - r_2 \in I$ und $z(a_2 - a_1) = z((r_1 - r_2)y) = \gamma(r_1 - r_2) = (r_1 - r_2)x$, d.h. $z(a_1) + r_1 x = z(a_2) + r_2 x$. Man rechnet sofort nach, daß z' ein R-Homomorphismus mit $z'|Z = z$ ist. Daher ist $(Z, z) \lneq (Z', z')$ im Widerspruch zur Maximalität von (Z, z).

Satz 30.5 *Ist I eine nichtleere Menge und Q_i ein R-Modul für $i \in I$, so gilt: $\prod_{i \in I} Q_i$ injektiv $\Leftrightarrow$ Q_i injektiv für $i \in I$.*

Beweis: Sei $Q := \prod_{i \in I} Q_i$ und $p_j : Q \to Q_j,\ q_j : Q_j \to Q$ die j-te Projektion bzw. Injektion für $j \in I$. Ferner sei $0 \longrightarrow M \xrightarrow{f} N$ eine exakte Folge von R-Homomorphismen.

⇒: Sei Q injektiv, $j \in I$ und $g : M \to Q_j$ ein R-Homomorphismus. Dann existiert zu dem R-Homomorphismus $q_j \circ g : M \to Q$ ein R-Homomorphismus $k : N \to Q$ mit $q_j \circ g = k \circ f$.

$$\begin{tikzcd}
0 \arrow[r] & M \arrow[r, "f"] \arrow[d, "g"'] & N \arrow[dl, "h"] \arrow[ddl, "k"] \\
& Q_j \arrow[d, "q_j"'] & \\
& Q &
\end{tikzcd}$$

Daher ist $h := p_j \circ k : N \to Q_j$ ein R-Homomorphismus mit $h \circ f = p_j \circ k \circ f = p_j \circ q_j \circ g = \mathrm{id}_{Q_j} \circ g = g$.

$\Leftarrow$: Sei Q_i injektiv für alle $i \in I$ und $g : M \to Q$ ein R-Homomorphismus. Dann existiert für $i \in I$ zu dem R-Homomorphismus $p_i \circ g : M \to Q_i$ ein R-Homomorphismus $h_i : N \to Q_i$ mit $h_i \circ f = p_i \circ g$.

$$\begin{tikzcd}
0 \arrow[r] & M \arrow[r, "f"] \arrow[d, "g"'] & N \arrow[dl, "h"] \arrow[ddl, "h_i"] \\
& Q \arrow[d, "p_i"'] & \\
& Q_i &
\end{tikzcd}$$

Daher ist $h : N \to Q,\ x \mapsto \big(h_i(x)\big)_{i \in I}$ ein R-Homomorphismus mit $h(f(x)) = \big(h_i(f(x))\big)_{i \in I} = \big(p_i(g(x))\big)_{i \in I} = g(x)$ für $x \in N$.

Satz 30.6 *Ein $\mathbf{Z}$-Modul A ist genau dann injektiv, wenn für $n \in \mathbb{N}$ und $a \in A$ ein $b \in A$ mit $a = nb$ existiert.*

Bemerkung: Injektive $\mathbf{Z}$-Moduln nennt man daher auch *dividierbare* abelsche Gruppen.

Beweis:

$\Rightarrow$: Sei A injektiv, $a \in A$, $n \in \mathbb{N}$. Dann ist die Abbildung $g : \mathbf{Z}n \to A,\ zn \mapsto za$ ein Homomorphismus. Daher existiert ein Element $b \in A$ mit $g(x) = xb$ für $x \in \mathbf{Z}n$; insbesondere ist $a = g(n) = nb$.

$\Leftarrow$: Sei I Ideal in $\mathbf{Z}$ und $g : I \to A$ ein Homomorphismus, o.B.d.A. $I \neq 0$, also $I = \mathbf{Z}n$ für ein $n \in \mathbb{N}$. Wir setzen $a := g(n)$. Existiert ein $b \in A$ mit $a = nb$, so ist $g(zn) = zg(n) = znb$ für $z \in \mathbf{Z}$.

Beispiel:

(i) $\mathbb{Q}$ ist injektiver $\mathbf{Z}$-Modul, $\mathbf{Z}$ selbst nicht.

(ii) Jeder Faktormodul eines injektiven $\mathbf{Z}$-Moduls ist injektiv.

(iii) Koprodukte von injektiven $\mathbf{Z}$-Moduln sind injektiv.

Satz 30.7 *Jeder $\mathbf{Z}$-Modul M ist zu einem Untermodul eines injektiven $\mathbf{Z}$-Moduls isomorph.*

Beweis: Nach 28.5 existieren eine Menge I und ein Untermodul U von $\coprod_{i\in I}\mathbf{Z}$ mit

$$M \simeq \left(\coprod_{i\in I}\mathbf{Z}\right)\Big/U \subseteq \underbrace{\left(\coprod_{i\in I}\mathbb{Q}\right)\Big/U}_{\text{injektiver }\mathbf{Z}\text{-Modul nach 30.6}}$$

Bemerkung 30.8 Nach Aufgabe 1 von Blatt 5 ist $\mathrm{Hom}_{\mathbf{Z}}(R,A)$ für jeden R-Modul A ein R-Modul, wenn man $rf \in \mathrm{Hom}_{\mathbf{Z}}(R,A)$ für $r\in R$ und $f\in \mathrm{Hom}_{\mathbf{Z}}(R,A)$ durch $(rf)(s) := f(sr)$ für $s\in R$ definiert.

Satz: *Für jeden injektiven $\mathbf{Z}$-Modul A ist $\mathrm{Hom}_{\mathbf{Z}}(R,A)$ ein injektiver R-Modul.*

Beweis: Sei $0 \longrightarrow M \xrightarrow{f} N$ eine exakte Folge von R-Homomorphismen und $g: M\to \mathrm{Hom}_{\mathbf{Z}}(R,A)$ ein R-Homomorphismus. Dann ist $\gamma: M\to A,\ m\mapsto (g(m))(1)$ ein $\mathbf{Z}$-Homomorphismus. Ist A injektiv, so existiert ein $\mathbf{Z}$-Homomorphismus $\delta: N\to A$ mit $\delta\circ f=\gamma$. Man rechnet leicht nach, daß die Abbildung $h: N\to \mathrm{Hom}_{\mathbf{Z}}(R,A)$, die jedem $x\in N$ die Abbildung $R\to A,\ r\mapsto \delta(rx)$ zuordnet, wohldefiniert und ein R-Homomorphismus mit $h\circ f = g$ ist.

Bemerkung 30.9 Für jeden R-Modul M ist $\mathrm{Hom}_R(R,M)$ nach Aufgabe 1 von Blatt 5 ein zu M isomorpher R-Untermodul von $\mathrm{Hom}_{\mathbf{Z}}(R,M)$.

Satz: *Jeder R-Modul M ist zu einem Untermodul eines injektiven R-Moduls isomorph.*

Beweis: Nach 30.7 ist der $\mathbf{Z}$-Modul M Untermodul eines injektiven $\mathbf{Z}$-Moduls Q. Daher gilt:

$$M \simeq_R \mathrm{Hom}_R(R,M) \subseteq \mathrm{Hom}_{\mathbf{Z}}(R,M) \subseteq \mathrm{Hom}_{\mathbf{Z}}(R,Q),$$

und $\mathrm{Hom}_{\mathbf{Z}}(R,Q)$ ist nach 30.8 ein injektiver R-Modul.

Satz 30.10 *Ein R-Modul Q ist genau dann injektiv, wenn jede exakte Folge von R-Homomorphismen der Form $0\longrightarrow Q \xrightarrow{f} M \xrightarrow{g} N \longrightarrow 0$ zerfällt.*

Beweis:

$\Rightarrow$: Analog zu 30.3.

$\Leftarrow$: Nach 30.9 existiert ein injektiver R-Modul D mit $Q\subseteq D$. Zerfällt die exakte Folge $0\longrightarrow Q\longrightarrow D\longrightarrow D/Q\longrightarrow 0$, so ist $D\simeq Q\times D/Q$; insbesondere ist mit D auch Q injektiv nach 30.5.

Kapitel 31

Moduln über Hauptidealringen

Sei R ein Hauptidealring.

Definition 31.1 *Für $m, n \in \mathbb{N}$ heißen zwei Matrizen $A, B \in \mathrm{Mat}(m,n,R)$* äquivalent, *wenn Matrizen $U \in \mathrm{GL}(m,R)$, $V \in \mathrm{GL}(n,R)$ existieren mit $UAV = B$. Schreibweise $A \sim B$.*

Bemerkung:

(i) Für $m, n \in \mathbb{N}$ ist $\sim$ eine Äquivalenzrelation auf $\mathrm{Mat}(m,n,R)$.

(ii) Die Formel zur Berechnung der inversen Matrix durch Determinanten zeigt: $\mathrm{GL}(n,R) = \{X \in \mathrm{Mat}(n,R) : \det(X) \in R^\times\}$.

Satz: *Für $m, n \in \mathbb{N}$ ist jede Matrix $A \in \mathrm{Mat}(m,n,R)$ äquivalent zu einer Matrix der Form*

$$\begin{pmatrix} d_1 & & & 0 \\ & d_2 & & \\ & & d_3 & \\ 0 & & & \ddots \end{pmatrix}$$

mit $d_1 \mid d_2 \mid d_3 \mid \ldots$. Dabei sind die Ideale $(d_1), (d_2), (d_3), \ldots$ eindeutig bestimmt (d.h. $d_1, d_2, d_3, \ldots$ sind bis auf Multiplikation mit Einheiten eindeutig bestimmt).

Beweis: (und Algorithmus) Für $i, j = 1, \ldots, m$ mit $i \neq j$ und $a \in R$ sei $T_{ij}^m(a) \in \mathrm{GL}(m,R)$ die Matrix mit Einsen in der Hauptdiagonale, a an der Position (i,j) und 0 sonst. Dann entsteht $T_{ij}^m(a)A$ aus A durch Addition des a-fachen der j-ten Zeile von A zur i-ten. Analog entsteht $AT_{ij}^n(a)$ aus A durch Addition des a-fachen der i-ten Spalte zur j-ten. Ferner gilt für $i \neq j$:

$$\begin{pmatrix} \vdots \\ a_i \\ \vdots \\ a_j \\ \vdots \end{pmatrix} \sim \begin{pmatrix} \vdots \\ a_i + a_j \\ \vdots \\ a_j \\ \vdots \end{pmatrix} \sim \begin{pmatrix} \vdots \\ a_i + a_j \\ \vdots \\ -a_i \\ \vdots \end{pmatrix} \sim \begin{pmatrix} \vdots \\ a_j \\ \vdots \\ -a_i \\ \vdots \end{pmatrix}$$

Daher kann man zwei Zeilen (oder auch Spalten) von A bis auf ein Vorzeichen vertauschen, ohne die Äquivalenzklasse von A zu verlassen.
Im folgenden bezeichnen wir für $r \in R$ mit $L(r)$ die Anzahl der Primfaktoren (mit Vielfachheiten) in der Primfaktorzerlegung von r ($L(r) = 0 \Leftrightarrow r \in R^\times$, $L(r) = \infty \Leftrightarrow r = 0$). Für $A = (a_{ij}) \in \mathrm{Mat}(m,n,R)$ sei $M(A) := \min\{L(a_{ij}) : i = 1, \ldots, m,\ j = 1, \ldots, n\}$.
Sei jetzt A gegeben. Nach Vertauschen von Zeilen und Spalten können wir annehmen: $L(a_{11}) =$

$M(A)$. Ist $a_{11} \nmid a_{12}$, so wählen wir einen ggT d von a_{11} und a_{12} und schreiben $d = xa_{11} + ya_{12}$ mit $x, y \in R$. Wegen $1 = x\frac{a_{11}}{d} + y\frac{a_{12}}{d}$ ist dann

$$X := \begin{pmatrix} x & -a_{12}/d & & & \\ y & a_{11}/d & & 0 & \\ & & 1 & & \\ & 0 & & \ddots & \\ & & & & 1 \end{pmatrix} \in \mathrm{GL}(n, R)$$

mit

$$AX = \begin{pmatrix} d & * & \cdots & * \\ * & & & \\ \vdots & & * & \\ * & & & \end{pmatrix}$$

und $M(AX) < M(A)$. Man ersetzt also A durch AX und fängt wieder von vorne an. Wegen $M(AX) < M(A)$ kann man diesen Schritt nur endlich oft durchführen. Man gelangt so schließlich zu einer Matrix $B = (b_{ij}) \sim A$ mit $b_{11} \mid b_{12}$. Analog geht man für die anderen Koeffizienten in der ersten Zeile (und der ersten Spalte) vor. Man gelangt schließlich zu einer Matrix $C = (c_{ij}) \sim A$ mit $c_{11} \mid c_{1i}$ für $i = 1, \ldots, n$ und $c_{11} \mid c_{j1}$ für $j = 1, \ldots, m$. Dann ist aber C äquivalent zu einer Matrix $D = (d_{ij})$ der Form

$$D = \begin{pmatrix} d_{11} & 0 & \cdots & 0 \\ 0 & & & \\ \vdots & & * & \\ 0 & & & \end{pmatrix}.$$

Ist $d_{11} \nmid d_{ij}$ für gewisse $i \in \{2, \ldots, m\}$, $j \in \{2, \ldots, n\}$, so addiere man die i-te Zeile zur ersten und fange wieder von vorne an. Auf diese Weise nimmt $M(D)$ weiter ab. Wir kommen so schließlich zu einer Matrix $E = (e_{ij})$ der Form

$$E = \begin{pmatrix} e_{11} & 0 & \cdots & 0 \\ 0 & & & \\ \vdots & & E' & \\ 0 & & & \end{pmatrix}$$

mit $e_{11} \mid e_{ij}$ für alle i, j. Das gleiche Verfahren wenden wir dann auf die Matrix E' an und gelangen so am Ende zu einer Matrix der gewünschten Form.
Es bleibt die Eindeutigkeit von $(d_1), (d_2), (d_3), \ldots$ zu bewiesen. Dazu bezeichnen wir für $i = 1, \ldots, \min\{m, n\}$ mit $\delta_i(A)$ das von allen i-reihigen Unterdeterminanten von A erzeugte Ideal in R. Für $Q \in \mathrm{Mat}(m, R)$ sind die Zeilen von QA Linearkombinationen der Zeilen von A. Daher sind die i-reihigen Unterdeterminanten von QA Linearkombinationen der i-reihigen Unterdeterminanten von A. Folglich gilt $\delta_i(QA) \subseteq \delta_i(A)$. Ist $Q \in \mathrm{GL}(m, R)$, so kann man dieses Argument umdrehen und erhält $\delta_i(QA) = \delta_i(A)$. Analog ist $\delta_i(AP) = \delta_i(A)$ für $P \in \mathrm{GL}(n, R)$. Insbesondere ist

$$\delta_i(A) \;=\; \delta_i \begin{pmatrix} d_1 & & & 0 \\ & d_2 & & \\ & & d_3 & \\ 0 & & & \ddots \end{pmatrix} \;=\; (d_1 \ldots d_i).$$

Daher sind $d_1, d_1d_2, d_1d_2d_3, \ldots$ bis auf Multiplikation mit Einheiten durch A eindeutig bestimmt. Daher sind auch $d_1, d_2, d_3, \ldots$ bis auf Einheiten durch A eindeutig bestimmt.

Definition: *Für $i = 1, \ldots, \min\{m, n\}$ nennt man (d_i) den i-ten* Invariantenteiler *von A.*

Beispiel:

$$\begin{pmatrix} 2 & 3 & 2 \\ 3 & 2 & 3 \end{pmatrix} \sim \begin{pmatrix} 2 & 1 & 2 \\ 3 & -1 & 3 \end{pmatrix} \sim \begin{pmatrix} 1 & -2 & 2 \\ -1 & -3 & 3 \end{pmatrix} \sim \begin{pmatrix} 1 & -2 & 2 \\ 0 & -5 & 5 \end{pmatrix} \sim$$
$$\sim \begin{pmatrix} 1 & 0 & 0 \\ 0 & -5 & 5 \end{pmatrix} \sim \begin{pmatrix} 1 & 0 & 0 \\ 0 & 5 & -5 \end{pmatrix} \sim \begin{pmatrix} 1 & 0 & 0 \\ 0 & 5 & 0 \end{pmatrix}$$

Satz 31.2 *Für $m, n \in \mathbb{N}$ sind zwei Matrizen in $\mathrm{Mat}(m,n,R)$ genau dann äquivalent, wenn sie die gleichen Invariantenteiler haben.*

Beweis: 31.1.

Satz 31.3 *Sei F ein endlich erzeugter freier R-Modul und E ein Untermodul von F. Dann ist E frei mit $\mathrm{rg}(E) \le \mathrm{rg}(F)$, und es existieren Basen $b_1, \ldots, b_n$ von F und $c_1, \ldots, c_m$ von E sowie Elemente $d_1, \ldots, d_m \in R$ mit $d_1 \mid d_2 \mid d_3 \mid \ldots$ und $c_i = d_i b_i$ für $i = 1, \ldots, m$; dabei sind die Ideale $(d_1), \ldots, (d_m)$ eindeutig bestimmt.*

Beweis: Nach 28.2 besitzt F eine endliche Basis $a_1, \ldots, a_n$. Ferner ist F nach 26.10 noethersch, also E endlich erzeugt, etwa $E = Re_1 + \ldots + Re_l$. Wir schreiben $e_i = \sum_{j=1}^n r_{ij} a_j$ mit $r_{ij} \in R$ für $i = 1, \ldots, l$, $j = 1, \ldots, n$ und setzen $A := (r_{ij})$. Nach 31.1 existieren $U = (u_{ij}) \in \mathrm{GL}(l,R)$, $V = (v_{ij}) \in \mathrm{GL}(n,R)$, so daß UAV die folgende Form hat:

$$UAV = \begin{pmatrix} d_1 & & & 0 \\ & d_2 & & \\ & & d_3 & \\ 0 & & & \ddots \end{pmatrix}$$

mit $d_1 \mid d_2 \mid d_3 \mid \ldots$. Wir schreiben $V^{-1} = (v'_{ij})$ und setzen $c_i := \sum_{j=1}^l u_{ij} e_j$ für $i = 1, \ldots, l$, $b_i := \sum_{j=1}^n v'_{ij} a_j$ für $i = 1, \ldots, n$. Dann ist

$$\sum_{j=1}^n v_{ij} b_j = \sum_{j,k=1}^n v_{ij} v'_{jk} a_k = a_i \quad \text{für } i = 1, \ldots, n,$$

also

$$c_i = \sum_{j=1}^l \sum_{k=1}^n u_{ij} r_{jk} a_k = \sum_{j=1}^l \sum_{k,h=1}^n u_{ij} r_{jk} v_{kh} b_h = d_i b_i \quad \text{für } i = 1, \ldots, l.$$

Offenbar bilden $b_1, \ldots, b_n$ eine Basis von F und $c_1, \ldots, c_l$ ein Erzeugendensystem von E. Streicht man noch die Nullen unter den Elementen $c_1, \ldots, c_l$, so erhält man eine Basis $c_1, \ldots, c_m$ von E.
Seien $b'_1, \ldots, b'_n$ eine weitere Basis von F, $c'_1, \ldots, c'_m$ eine weitere Basis von E (vgl. 28.3) und $d'_1, \ldots, d'_m \in R$ mit $d'_1 \mid d'_2 \mid d'_3 \mid \ldots$ und $c'_i = d'_i b'_i$ für $i = 1, \ldots, m$. Wir schreiben $b_i = \sum_{j=1}^n p_{ij} b'_j$ mit $p_{ij} \in R$ für $i, j = 1, \ldots, n$ und $c'_i = \sum_{j=1}^m q_{ij} c_j$ mit $q_{ij} \in R$ für $i, j = 1, \ldots, m$. Dann ist

$$d'_i b'_i = c'_i = \sum_{j=1}^m q_{ij} \underbrace{c_j}_{= d_j b_j} = \sum_{j=1}^m \sum_{k=1}^n q_{ij} d_j p_{jk} b'_k \quad \text{für } i = 1, \ldots, m,$$

also

$$\begin{pmatrix} d'_1 & & & 0 \\ & d'_2 & & \\ & & d'_3 & \\ 0 & & & \ddots \end{pmatrix} = Q \begin{pmatrix} d_1 & & & 0 \\ & d_2 & & \\ & & d_3 & \\ 0 & & & \ddots \end{pmatrix} P$$

mit $Q = (q_{ij}) \in \mathrm{GL}(m,R)$, $P = (p_{ij}) \in \mathrm{GL}(n,R)$. Nach 31.1 ist also $(d_i) = (d'_i)$ für $i = 1, \ldots, m$.

Beispiel: Sei F ein freier $\mathbf{Z}$-Modul mit Basis a_1, a_2, a_3 und E der von den Elementen $e_1 := 2a_1 + 3a_2 + 2a_3,\ e_2 := 3a_1 + 2a_2 + 3a_3$ erzeugte Untermodul von F. Nach Beispiel 31.1 und dem Beweis von 31.3 besitzt F eine Basis b_1, b_2, b_3, so daß $b_1, 5b_2$ eine Basis von E bilden. Die Beweise zeigen auch ein Verfahren zur effektiven Berechnung von b_1, b_2, b_3 aus a_1, a_2, a_3.

Satz 31.4 *Zu jedem endlich erzeugten R-Modul M existieren echte Ideale $I_1, \ldots, I_n$ von R mit $M \simeq R/I_1 \times \ldots \times R/I_n$ und $I_1 \supseteq I_2 \supseteq I_3 \supseteq \ldots$.*

Bemerkung: Wir werden später sehen, daß dabei $I_1, \ldots, I_n$ eindeutig bestimmt sind.

Beweis: Nach 28.5 existiert ein endlich erzeugter freier R-Modul F und ein Untermodul E von F mit $M \simeq F/E$. Wählt man Basen wie in 31.3, so gilt

$$M \;\simeq\; R/Rd_1 \times \ldots \times R/Rd_m \times \underbrace{R \times \ldots \times R}_{n-m \text{ Faktoren}}$$

mit $Rd_1 \supseteq Rd_2 \supseteq Rd_3 \supseteq \ldots$. Dabei kann man Faktoren mit $Rd_i = R$ weglassen, und statt R kann man $R/0$ schreiben.

Bemerkung 31.5 Für jeden R-Modul M ist der *Torsionsmodul* $T(M) := \{m \in M : rm = 0 \text{ für ein } r \in R,\ r \neq 0\}$ von M nach Aufgabe 3 von Blatt 5 ein Untermodul von M.

Beispiel: Im Fall $M = R^k \times (R/d_1R) \times \ldots \times (R/d_lR)$ mit Elementen $d_1, \ldots, d_l \in R \setminus \{0\}$ ist $T(M) = 0^k \times (R/d_1R) \times \ldots \times (R/d_lR)$ und $M = T(M) \oplus F$ mit einem freien R-Modul $F = R^k \times 0 \times \ldots \times 0$ vom Rang k. Es ist also $M/T(M) \simeq F$ und $k = \mathrm{rg}(M/T(M))$.

Satz: *Jeder endlich erzeugte R-Modul M besitzt eine Zerlegung $M = T(M) \oplus F$, wobei F ein freier R-Modul ist, dessen Rang eindeutig bestimmt ist.*

Beweis: Klar nach obigem Beispiel.

Bemerkung 31.6 Für $a \in R \setminus R^\times$ mit $a \neq 0$ und Primfaktorzerlegung $a = p_1^{\alpha_1} \ldots p_r^{\alpha_r}$ ist $R/(a) \simeq R/(p_1^{\alpha_1}) \times \ldots \times R/(p_r^{\alpha_r})$ nach dem Chinesischen Restsatz; dabei sind die Faktoren $R/(p_i^{\alpha_i})$ nach Aufgabe 4 von Blatt 5 artinsch, noethersch und unzerlegbar. Für Primelemente p, q in R und $\alpha, \beta \in \mathbb{N}$ gilt ferner: $R/(p^\alpha) \simeq R/(q^\beta) \;\Leftrightarrow\; (p^\alpha) = (q^\beta)$.

Satz: *Für jeden endlich erzeugten R-Modul M hat man eine Zerlegung*

$$T(M) \;\simeq\; R/(p_1^{\alpha_1}) \times \ldots \times R/(p_s^{\alpha_s})$$

mit Primelementen $p_1, \ldots, p_s$ und $\alpha_1, \ldots, \alpha_s \in \mathbb{N}$. Dabei sind die Ideale $(p_1^{\alpha_1}), \ldots, (p_s^{\alpha_s})$ eindeutig bestimmt (bis auf ihre Reihenfolge).

Beweis: Beispiel 31.5, Bemerkung 31.6 und Krull-Schmidt.

Satz 31.7 *Seien $I_1, \ldots, I_m, J_1, \ldots, J_n$ echte Ideale in R mit $I_1 \supseteq \ldots \supseteq I_m,\ J_1 \supseteq \ldots \supseteq J_n$ und $R/I_1 \times \ldots \times R/I_m \simeq R/J_1 \times \ldots \times R/J_n$. Dann ist $m = n$ und $I_i = J_i$ für $i = 1, \ldots, m$.*

Beweis: Sei $I_i \neq 0$ für $i = 1, \ldots, k$, $J_l \neq 0$ für $j = 1, \ldots, l$, $I_{k+1} = \ldots = I_m = 0 = J_{l+1} = \ldots = J_n$. Nach 31.5 gilt also für $M := \prod_{i=1}^m R/I_i$, $N := \prod_{j=1}^n R/J_j$:

$$R/I_1 \times \ldots \times R/I_k \;\simeq\; T(M) \;\simeq\; T(N) \;\simeq\; R/J_1 \times \ldots \times R/J_l$$

und

$$R^{m-k} \;\simeq\; M/T(M) \;\simeq\; N/T(N) \;\simeq\; R^{n-l},$$

also $m - k = n - l$. Daher genügt es zu zeigen: $k = l$ und $I_i = J_i$ für $i = 1, \ldots, k$. Für $i = 1, \ldots, k$ sei $I_i = (d_i)$ und $d_i = \prod_j p_j^{\alpha_{ij}}$ die Primfaktorzerlegung von d_i. Für $i = 1, \ldots, l$ sei $J_i = (e_i)$ und $e_i = \prod_i p_j^{\beta_{ij}}$ die Primfaktorzerlegung von e_i. Dann ist

$$\prod_{i,j} R/(p_j^{\alpha_{ij}}) \;\simeq\; T(M) \;\simeq\; T(N) \;\simeq\; \prod_{i,j} R/(p_j^{\beta_{ij}}).$$

Nach 31.6 stimmen die Ideale $(p_j^{\alpha_{ij}})$ mit den Idealen $(p_j^{\beta_{ij}})$ bis evtl. auf die Reihenfolge überein. Wegen $d_1 \mid d_2 \mid d_3 \mid \ldots$ kann man $(d_1), (d_2), (d_3), \ldots$ aus den Idealen $(p_j^{\alpha_{ij}})$ rekonstruieren, und analog die Ideale $(e_1), (e_2), (e_3), \ldots$ aus den Idealen $(p_j^{\beta_{ij}})$. Daraus folgt die Behauptung.

Beispiel: $\mathbf{Z}/8\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/3\mathbf{Z} \times \mathbf{Z}/3\mathbf{Z} \;\simeq\; \mathbf{Z}/6\mathbf{Z} \times \mathbf{Z}/24\mathbf{Z}$.

Satz 31.8

(i) *Jede endlich erzeugte abelsche Gruppe ist isomorph zu* $\mathbf{Z}/d_1\mathbf{Z} \times \ldots \times \mathbf{Z}/d_n\mathbf{Z}$ *mit eindeutig bestimmten* $d_1, \ldots, d_n \in \mathbb{N}_0 \setminus \{1\}$, *die* $d_1 \mid d_2 \mid d_3 \mid \ldots$ *erfüllen.*

(ii) *Jede endlich erzeugte abelsche Gruppe ist isomorph zu* $\mathbf{Z}^k \times \mathbf{Z}/p_1^{\alpha_1}\mathbf{Z} \times \ldots \times \mathbf{Z}/p_s^{\alpha_s}\mathbf{Z}$ *mit eindeutig bestimmten* $k, s \in \mathbb{N}_0$, $\alpha_1, \ldots, \alpha_s \in \mathbb{N}$ *und eindeutig bestimmten Primzahlen* $p_1, \ldots, p_s$.

Beweis: Obige Sätze mit $R = \mathbf{Z}$.

Bemerkung: Anwendung der obigen Sätze auf den Polynomring $R = K[X]$ über einem Körper K liefert die bekannten Sätze über Normalformen von Matrizen.

Kapitel 32

Ganze Ringerweiterungen

Satz 32.1 *Für einen unitären Teilring R eines kommutativen Rings S und ein Element $s \in S$ sind äquivalent:*

(1) Es existiert ein normiertes Polynom $f \in R[X]$ mit $f(s) = 0$.

(2) $R[s]$ ist ein endlich erzeugter R-Modul.

(3) Es existiert ein endlich erzeugter R-Untermodul M von S mit $1 \in M$ und $sM \subseteq M$.

Definition: *Gegebenenfalls nennt man s* ganz *über R. Ist jedes Element in S ganz über R, so nennt man S eine* ganze Ringerweiterung *von R.*

Beispiel:

(i) Jedes $r \in R$ ist als Nullstelle von $X - r$ ganz über R.

(ii) Sind R, S Körper, so sind die über R ganzen Elemente in S genau die über R algebraischen Elemente in S.

(iii) Die über $\mathbf{Z}$ ganzen Zahlen in $\mathbb{C}$ nennt man *ganze (ganze algebraische)* Zahlen. Beispiele dafür sind $\sqrt{2}$, $1 + i$ und jede komplexe Einheitswurzel.

Beweis:

(1)⇒(2): Sei (1) erfüllt und $f = X^n + r_{n-1}X^{n-1} + \ldots + r_1X + r_0$ mit $r_0, \ldots, r_{n-1} \in R$. Dann ist $s^n = -r_{n-1}s^{n-1} - \ldots - r_1s - r_0$, also $R[s] = R1 + Rs + \ldots + Rs^{n-1}$.

(2)⇒(3): Setze $M := R[s]$.

(3)⇒(1): Sei (3) erfüllt und $M = Rm_1 + \ldots + Rm_n$ mit $m_1, \ldots, m_n \in M$. Wir schreiben $sm_i = \sum_{j=1}^n a_{ij}m_j$ mit $a_{ij} \in R$ für $i, j = 1, \ldots, n$ und setzen $A := (a_{ij}) \in \mathrm{Mat}(n, R)$, $B := A - sE$ (E Einheitsmatrix). In der Linearen Algebra zeigt man die Existenz einer Matrix $C \in \mathrm{Mat}(n, R)$ mit $CB = \det(B)E$. Wegen $0 = \sum_{j=1}^n (a_{ij} - \delta_{ij}s)m_j$ ist also $0 = \det(B)m_i = f_A(s)m_i$ für $i = 1, \ldots, n$, wobei f_A das charakteristische Polynom von A ist. Folglich ist $f_A(s)M = 0$; insbesondere ist $f_A(s) = f_A(s)1 = 0$.

Satz 32.2 *Für jeden unitären Teilring R eines kommutativen Rings S bilden die über R ganzen Elemente in S einen Teilring T von S mit $R \subseteq T$. Ferner enthält T jedes über T ganze Element in S.*

Beweis: Seien $a, b \in S$ ganz über R und M, N endlich erzeugte R-Untermoduln von S mit $1 \in M \cap N$, $aM \subseteq M$, $bN \subseteq N$. Wir schreiben $M = Rm_1 + \ldots + Rm_k$, $N = Rn_1 + \ldots + Rn_l$ mit $m_1, \ldots, m_k \in M$, $n_1, \ldots, n_l \in N$. Dann ist $L := \sum_{i=1}^k \sum_{j=1}^l Rm_in_j$ ein endlich erzeugter R-Untermodul von S mit $1 \in L$, $aL \subseteq L$, $bL \subseteq L$, also auch $(a \pm b)L \subseteq L$. Wegen Beispiel 32.1 (i) gilt also die erste Behauptung.
Sei $s \in S$ ganz über T und $f \in T[X]$ normiert mit $f(s) = 0$. Wir schreiben $f = X^n + a_{n-1}X^{n-1} + \ldots + a_1X + a_0$ mit $a_0, \ldots, a_{n-1} \in T$. Dann ist s auch ganz über $R[a_0, \ldots, a_{n-1}]$, d.h. $R[a_0, \ldots, a_{n-1}, s] = \sum_{j=0}^l R[a_0, \ldots, a_{n-1}]s^j$ für ein $l \in \mathbb{N}$. Andrerseits folgt aus 32.1 leicht, daß natürliche Zahlen $k_0, \ldots, k_{n-1}$ existieren mit

$$R[a_0, \ldots, a_{n-1}] = \sum_{i_0=0}^{k_0} \ldots \sum_{i_{n-1}=0}^{k_{n-1}} Ra_0^{i_0} \ldots a_{n-1}^{i_{n-1}}.$$

Dies zeigt, daß $R[a_0, \ldots, a_{n-1}, s]$ ein endlich erzeugter R-Modul ist. Nach 32.1 ist s daher ganz über R.

Definition: *Sei R ein unitärer Teilring eines kommutativen Rings S. Dann nennt man $T := \{s \in S : s$ ganz über $R\}$ den* ganzen Abschluß *von R in S. Im Fall $T = R$ nennt man R* ganz abgeschlossen *in S. Einen Integritätsbereich nennt man* ganz abgeschlossen *oder* normal, *wenn er in seinem Quotientenkörper ganz abgeschlossen ist.*

Beispiel: Den ganzen Abschluß von $\mathbf{Z}$ in einem algebraischen Zahlkörper K bezeichnet man als *Ganzheitsring* oder *Maximalordnung* von K. Schreibweise: $\mathcal{O}_K$ oder o_K.

Satz 32.3 *Jeder faktorielle Ring ist ganz abgeschlossen.*

Beweis: Sei K der Quotientenkörper von R, $\alpha \in K$ ganz über R und $f \in R[X]$ normiert mit $f(\alpha) = 0$. Wir schreiben $\alpha = \frac{a}{b}$ mit teilerfremden $a, b \in R$ und $f = X^n + a_{n-1}X^{n-1} + \ldots + a_1X + a_0$ mit $a_0, \ldots, a_{n-1} \in R$. Dann ist $0 = 0 \cdot b^n = f(\alpha)b^n = a^n + a_{n-1}a^{n-1}b + \ldots + a_1ab^{n-1} + a_0b^n$, also $b \mid a^n$. Daher ist $b \in R^\times$ und $\alpha = \frac{a}{b} \in R$.

Satz 32.4 *Sei R ein ganz abgeschlossener Integritätsbereich mit Quotientenkörper K, und seien $g, h \in K[X]$ normiert mit $f := gh \in R[X]$. Dann gilt: $g, h \in R[X]$.*

Beweis: Sei L Zerfällungskörper von f über K und $f = \prod_{k=1}^n (X - \alpha_k)$ mit $\alpha_1, \ldots, \alpha_n \in L$. Da f normiert ist, sind $\alpha_1, \ldots, \alpha_n$ ganz über R, und es existiert eine Teilmenge I von $\{1, \ldots, n\}$ mit $g = \prod_{i \in I}(X - \alpha_i)$. Die Koeffizienten von g sind nach 32.2 ganz über R und liegen in K. Da R ganz abgeschlossen ist, folgt: $g \in R[X]$. Analog ist $h \in R[X]$.

Satz 32.5 *Sei R ein ganz abgeschlossener Integritätsbereich mit Quotientenkörper K, L ein Erweiterungskörper von K und $a \in L$ ganz über R (also auch algebraisch über K). Dann ist $m_{K,a} \in R[X]$.*

Beweis: Sei $f \in R[X]$ normiert mit $f(a) = 0$. Dann gilt $m_{K,a} \mid f$ in $K[X]$, also $f = gm_{K,a}$ für ein $g \in K[X]$. Da g und $m_{K,a}$ normiert sind, folgt aus 32.4: $g, m_{K,a} \in R[X]$.

Bemerkung: Ist zusätzlich $L|K$ endlich, so sind nach 22.4 insbesondere $N_K^L(a), T_K^L(a) \in R$.

Beispiel: Sei K quadratischer Zahlkörper, d.h. $[K:\mathbb{Q}]=2$. Nach Aufgabe 3 von Blatt 1 existiert eine quadratfreie Zahl $d \in \mathbf{Z}$ mit $K=\mathbb{Q}(\sqrt{d})$. Für $a,b \in \mathbb{Q}$ und $x := a+b\sqrt{d}$ gilt: $T^K_{\mathbb{Q}}(x)=2a,\ N^K_{\mathbb{Q}}(x)=a^2-b^2d$.
Ist also x ganz über $\mathbf{Z}$, so ist $2a \in \mathbf{Z}$ und $a^2-b^2d \in \mathbf{Z}$. Im Fall $a \in \mathbf{Z}$ ist auch $b^2d \in \mathbf{Z}$, also $b \in \mathbf{Z}$, da d quadratfrei. Im Fall $a \notin \mathbf{Z}$ ist auch $b \notin \mathbf{Z}$, aber $(2b)^2d = 4(b^2d-a^2)+(2a)^2 \in \mathbf{Z}$, also $2b \in \mathbf{Z}$, da d quadratfrei. Wir schreiben $a=\frac{\alpha}{2},\ b=\frac{\beta}{2}$, wobei $\alpha,\beta \in \mathbf{Z}$ ungerade. Dann ist $0 \equiv \alpha^2-\beta^2d \equiv 1-d \pmod 4$, d.h. $d \equiv 1 \pmod 4$.
Ist umgekehrt $d \equiv 1 \pmod 4$ und sind $\alpha,\beta \in \mathbf{Z}$ ungerade, so gilt:

$$\left(X-\frac{\alpha}{2}-\frac{\beta}{2}\sqrt{d}\right)\left(X-\frac{\alpha}{2}+\frac{\beta}{2}\sqrt{d}\right) = X^2-\underbrace{\alpha}_{\in\mathbf{Z}}X+\underbrace{\left(\frac{\alpha}{2}\right)^2-\left(\frac{\beta}{2}\right)^2d}_{\in\mathbf{Z}}$$

wegen $\alpha^2-\beta^2d \equiv 1-d \equiv 0 \pmod 4$.
Folglich gilt:

$$\begin{aligned} \mathcal{O}_K &= \{a+b\sqrt{d} : a,b \in \mathbf{Z}\} && ,\text{falls } d \equiv 2,3 \pmod 4,\\ \mathcal{O}_K &= \{a+b\sqrt{d} : 2a,2b \in \mathbf{Z},\ 2a \equiv 2b \pmod 2\} && ,\text{falls } d \equiv 1 \pmod 4. \end{aligned}$$

Satz 32.6 *Sei R Integritätsbereich mit Quotientenkörper K, $L|K$ eine endliche Körpererweiterung, und S der ganze Abschluß von R in L. Zu jedem Element $b \in L$ existiert dann ein Element $r \in R\setminus\{0\}$ mit $rb \in S$; insbesondere ist L der Quotientenkörper von S.*

$$\begin{tikzcd} S \arrow[r, dash] \arrow[d, dash] & L \arrow[d, dash] \\ R \arrow[r, dash] & K \end{tikzcd}$$

Beweis: Sei $b \in L$ und $m_{K,b} = X^n + a_{n-1}X^{n-1}+\ldots+a_1X+a_0$ mit $a_0,\ldots,a_{n-1} \in K$. Wir wählen ein $r \in R\setminus\{0\}$ mit $ra_i \in R$ für $i=0,\ldots,n-1$. Dann ist $f := X^n+a_{n-1}rX^{n-1}+\ldots+a_1r^{n-1}X+a_0r^n \in R[X]$ normiert mit $f(rb)=r^nb^n+a_{n-1}r^nb^{n-1}+\ldots+a_1r^nb+a_0r^n = r^nm_{K,b}(b)=0$, also $rb \in S$.

Satz 32.7 *Sei R ein ganz abgeschlossener noetherscher Integritätsbereich mit Quotientenkörper K, $L|K$ eine endliche separable Körpererweiterung und S der ganze Abschluß von R in L. Dann ist S als R-Modul endlich erzeugt.*

Beweis: Da $L|K$ separabel ist, existieren nach 18.3 genau $n := [L:K]$ verschiedene K-Homomorphismen $\sigma_1,\ldots,\sigma_n : L \to M$; dabei ist M ein algebraischer Abschluß von L. Wir wählen eine K-Basis $b_1,\ldots,b_n$ von L, o.B.d.A. $b_1,\ldots,b_n \in S$ nach 32.6. Da $\sigma_1,\ldots,\sigma_n$ linear unabhängig sind, ist die Matrix $A := (\sigma_i(b_j)) \in \mathrm{Mat}(n,M)$ invertierbar; insbesondere ist $d := \det(A^TA) \neq 0$. Ferner ist $\sum_{i=1}^n \sigma_i(b_j)\sigma_i(b_k) = \sum_{i=1}^n \sigma_i(b_jb_k) = T^L_K(b_jb_k)$ für $j,k=1,\ldots,n$ nach 22.5, d.h. $A^TA = (T^L_K(b_jb_k))$. Sei $s \in S$ und $s = a_1b_1+\ldots+a_nb_n$ mit $a_1,\ldots,a_n \in K$. Für $k=1,\ldots,n$ ist $a_1b_1b_k+\ldots+a_nb_nb_k = sb_k \in S$, also $a_1T^L_K(b_1b_k)+\ldots+a_nT^L_K(b_nb_k) = T^L_K(sb_k) \in R$ nach 32.5. Aus Cramers Regel folgt: $da_1,\ldots,da_n \in R$, also $s \in R\frac{b_1}{d}+\ldots+R\frac{b_n}{d} =: N$. Daher ist S ein R-Untermodul des endlich erzeugten R-Moduls N. Mit R ist auch N noethersch nach 26.10. Folglich ist S als R-Modul endlich erzeugt.

Beispiel: $R = \mathbf{Z}$, $K = \mathbb{Q}$, L quadratischer Zahlkörper, also $L = \mathbb{Q}(\sqrt{d})$, $d \in \mathbf{Z}$ quadratfrei. Aus Beispiel 32.5 folgt leicht:

$$\begin{aligned} \mathcal{O}_L &= S = \mathbf{Z} + \mathbf{Z}\sqrt{d} &&, \text{falls } d \equiv 2,3 \pmod 4, \\ \mathcal{O}_L &= S = \mathbf{Z} + \mathbf{Z}\tfrac{1+\sqrt{d}}{2} &&, \text{falls } d \equiv 1 \pmod 4. \end{aligned}$$

Kapitel 33

Geometrische Konstruktionen

Satz 33.1 (Lindemann, 1852–1939) *π ist transzendent.*

Beweis: Ist π algebraisch, so auch $i\pi$. Wir schreiben $m_{\mathbb{Q},i\pi} = (X-\beta_1)\dots(X-\beta_m)$ mit $\beta_1 = i\pi, \beta_2, \dots, \beta_m \in \mathbb{C}$. Wegen $e^{i\pi} = -1$ ist dann

$$0 \;=\; (1+e^{\beta_1})(1+e^{\beta_2})\dots(1+e^{\beta_m}) \;=\; 1+\sum_{j=1}^{m} e^{\beta_j} + \sum_{j<k} e^{\beta_j+\beta_k} + \dots + e^{\beta_1+\dots+\beta_m}.$$

Wir bezeichnen mit $\alpha_1, \dots, \alpha_n$ die von 0 verschiedenen Zahlen unter den Exponenten $\beta_j, \beta_j + \beta_k, \dots, \beta_1 + \dots + \beta_m$ und erhalten so eine Gleichung der Form $0 = N + e^{\alpha_1} + \dots + e^{\alpha_n}$ mit $N \in \mathbb{N}$, wobei $\alpha_1, \dots, \alpha_n$ durch Automorphismen von $K := \mathbb{Q}(\beta_1, \dots, \beta_m)$ nur untereinander permutiert werden. Daher ist $(X-\alpha_1)\dots(X-\alpha_n) \in \mathbb{Q}[X]$, da $K|\mathbb{Q}$ Galoiserweiterung ist. Es existiert also ein $g \in \mathbf{Z}[X]$ mit Grad n und Nullstellen $\alpha_1, \dots, \alpha_n$. Wir schreiben $g = \sum_{i=0}^{n} b_i X^i$ mit $b_0, \dots, b_n \in \mathbf{Z}$ und wählen $b \in \mathbb{N}$, so daß $b\alpha_i^k$ für $i, k = 1, \dots, n$ ganz algebraisch ist. Dann setzen wir $C := \max\{\sum_{j=0}^{n} |b_j||\alpha_i|^{j+1} : i = 1, \dots, n\}$ und wählen eine Primzahl p mit $p > |Nb_0 b|$ und $\frac{b^p C^p}{(p-1)!} \sum_{i=1}^{n} e^{|\alpha_i|} < 1$. Wir schreiben $X^{p-1} g^p = \sum_{j=0}^{M} c_j X^j = \sum_{j=p-1}^{M} c_j X^j$ mit $c_0, \dots, c_M \in \mathbf{Z}$, $M := np + p - 1$. Für $x \in \mathbb{C}$ und $j \in \mathbb{N}_0$ ist

$$j!\,e^x \;=\; j! + j!\,x + \frac{j!}{2}x^2 + \dots + x^j + x^{j+1} q_j(x) e^{|x|}$$

mit

$$\begin{aligned} |q_j(x)| \;&=\; \frac{1}{e^{|x|}}\left|\frac{1}{j+1} + \frac{x}{(j+1)(j+2)} + \frac{x^2}{(j+1)(j+2)(j+3)} + \dots\right| \;\le \\ &\le\; \frac{1}{e^{|x|}}\left(1 + \frac{|x|}{1\cdot 2} + \frac{|x|^2}{1\cdot 2\cdot 3} + \dots\right) \;<\; 1. \end{aligned}$$

Daher ist

$$\begin{aligned} \sum_{j=0}^{M} c_j j!\,e^x \;&=\; c_0\left(0! + x q_0(x) e^{|x|}\right) \;+ \\ &\quad + c_1\left(1! + x + x^2 q_1(x) e^{|x|}\right) \;+ \\ &\quad + c_2\left(2! + 2!\,x + x^2 + x^3 q_2(x) e^{|x|}\right) \;+ \\ &\quad + \;\dots\; + \\ &\quad + c_M\left(M! + M!\,x + \frac{M!}{2}x^2 + \dots + x^M + x^{M+1} q_M(x) e^{|x|}\right) \;= \\ &=\; \sum_{j=0}^{M} c_j x^j + \left(\sum_{j=0}^{M} c_j x^j\right)' + \dots + \left(\sum_{j=0}^{M} c_j x^j\right)^{(M)} + \sum_{j=0}^{M} c_j x^{j+1} q_j(x) e^{|x|}. \end{aligned}$$

Wir setzen $f := \frac{1}{(p-1)!}X^{p-1}g^p$ und $F := f + f' + f'' + \ldots + f^{(M)}$. Dann ist $F(0)e^x = F(x)+Q(x)e^{|x|}$ mit $Q(x) := \sum_{j=0}^M \frac{c_j}{(p-1)!}x^{j+1}q_j(x)$. Für $i = 1, \ldots, n$ ist also $F(0)e^{\alpha_i} = F(\alpha_i)+Q(\alpha_i)e^{|\alpha_i|}$, und man erhält $-NF(0) = F(0)\sum_{i=1}^n e^{\alpha_i} = \sum_{i=1}^n F(\alpha_i) + \sum_{i=1}^n Q(\alpha_i)e^{|\alpha_i|}$, d.h.

$$NF(0) + \sum_{i=1}^n F(\alpha_i) \;=\; -\sum_{i=1}^n Q(\alpha_i)e^{|\alpha_i|}.$$

Für $i = 1, \ldots, n$ und $j = 0, \ldots, p-1$ ist $f^{(j)}(\alpha_i) = 0$. Daher existiert ein Polynom $h \in \mathbf{Z}[X]$ mit $\deg(h) < np$ und $F(\alpha_i) = \sum_{j=p}^M f^{(j)}(\alpha_i) = ph(\alpha_i)$ für $i = 1, \ldots, n$. Für $i = 1, \ldots, n$ ist $b^p h(\alpha_i)$ ganz algebraisch und $F(0) = \sum_{j=p-1}^M \frac{c_j}{(p-1)!}j! \in \mathbf{Z}$. Daher ist $b^p(NF(0)+\sum_{i=1}^n F(\alpha_i))$ ganz algebraisch. Andrerseits ist $b^p(NF(0) + \sum_{i=1}^n F(\alpha_i))$ fest unter allen Automorphismen von K, liegt also in $\mathbb{Q}$. Da $\mathbf{Z}$ ganz abgeschlossen ist, folgt: $b^p(NF(0) + \sum_{i=1}^n F(\alpha_i)) \in \mathbf{Z}$. Ferner ist $F(0) \equiv c_{p-1} = b_0^p \equiv b_0 \not\equiv 0 \pmod p$, also $0 \neq b^p(NF(0) + \sum_{i=1}^n ph(\alpha_i)) = b^p(NF(0) + \sum_{i=1}^n F(\alpha_i))$. Folglich ist

$$\left| b^p \sum_{i=1}^n Q(\alpha_i)e^{|\alpha_i|} \right| \;=\; \left| b^p \left(NF(0) + \sum_{i=1}^n F(\alpha_i) \right) \right| \;\in\; \mathbb{N}\,.$$

Andrerseits ist

$$\begin{aligned} (p-1)!\,|Q(x)| \;&\leq\; \sum_{j=0}^M |c_j||x|^{j+1} \;=\; |x| \sum_{j=0}^M |c_j||x|^j \;\leq \\ &\leq\; |x||x|^{p-1} \left(\sum_{j=0}^M |b_j||x|^j \right)^p \;=\; \left(\sum_{j=0}^M |b_j||x|^{j+1} \right)^p \end{aligned}$$

für $x \in \mathbb{C}$. Daher erhält man den Widerspruch

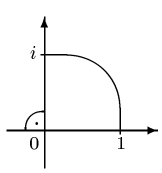
$$\begin{aligned} \left| b^p \sum_{i=1}^n Q(\alpha_i)e^{|\alpha_i|} \right| \;&\leq\; \frac{b^p}{(p-1)!} \sum_{i=1}^n \left(\sum_{j=0}^M |b_j||\alpha_i|^{j+1} \right)^p e^{|\alpha_i|} \;\leq \\ &\leq\; \frac{b^p C^p}{(p-1)!} \sum_{i=1}^n e^{|\alpha_i|} \;<\; 1. \end{aligned}$$

Definition 33.2 *Gegeben sei eine Teilmenge $M = M_0$ von $\mathbb{C} = \mathbb{R}^2$ mit $0, 1 \in M$. Mit $G(M)$ bezeichnen wir die Menge aller Geraden, die durch mindestens zwei Punkte in M gehen, und mit $K(M)$ die Menge aller Kreise, deren Mittelpunkt in M liegt und deren Radius der Abstand von zwei Punkten in M ist. Für $i \in \mathbb{N}$ sei M_i die Menge, die aus den Elementen in M_{i-1}, den Schnittpunkten von zwei verschiedenen Geraden in $G(M_{i-1})$, den Schnittpunkten von zwei verschiedenen Kreisen in $K(M_{i-1})$, und den Schnittpunkten einer Gerade in $G(M_{i-1})$ mit einem Kreis in $K(M_{i-1})$ besteht. Ferner setzen wir $M_\infty := \bigcup_{i\in\mathbb{N}_0} M_i$ und nennen die Punkte in M_∞ (mit Zirkel und Lineal)* konstruierbar *aus M.*

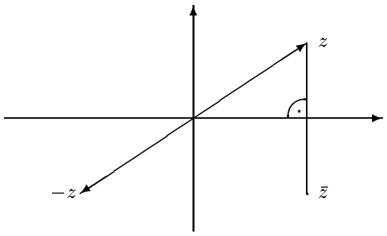
Satz: *Für jede Teilmenge M in $\mathbb{C}$ mit $0, 1 \in M$ ist M_∞ ein Teilkörper von $\mathbb{C}$, der mit z auch $\bar{z}$ und jede Quadratwurzel aus z enthält.*

Beweis:

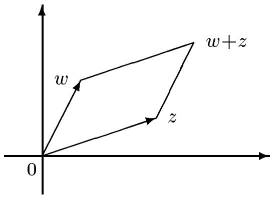
(i) $i \in M_\infty$:



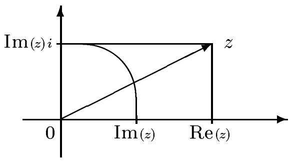
(ii) $z \in M_\infty \;\Rightarrow\; \bar{z}, -z \in M_\infty$:



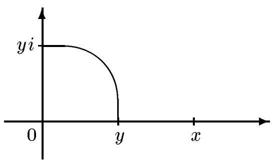
(iii) $w, z \in M_\infty \;\Rightarrow\; w + z \in M_\infty$:



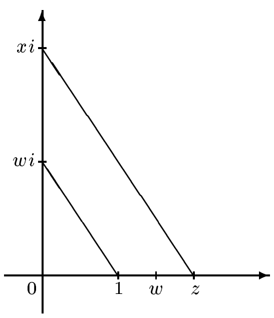
(iv) $z \in M_\infty \;\Rightarrow\; \mathrm{Re}(z), \mathrm{Im}(z) \in M_\infty$:



(v) $x, y \in M_\infty \cap \mathbb{R} \;\Rightarrow\; x + iy \in M_\infty$:

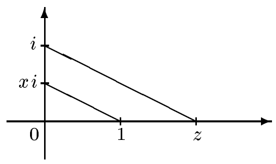


(vi) $w, z \in M_\infty \;\Rightarrow\; wz \in M_\infty$: o.B.d.A. $w, z \in \mathbb{R},\; w, z > 0$.



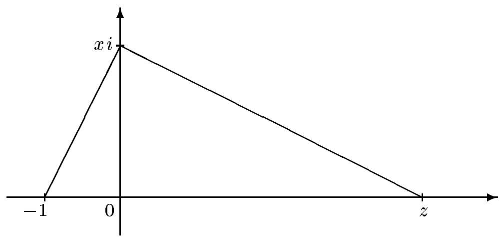
Strahlensatz: $\frac{z}{1} = \frac{x}{w}$, d.h. $x = zw$.

(vii) $z \in M_\infty \setminus \{0\} \;\Rightarrow\; \frac{1}{z} \in M_\infty$: $\frac{1}{z} = \frac{\bar z}{z\bar z}$, also o.B.d.A. $z \in \mathbb{R},\; z > 0$.



Strahlensatz: $\frac{1}{z} = \frac{x}{1} = x$.

(viii) $z \in M_\infty \;\Rightarrow\; w := \sqrt{z} \in M_\infty$: Schreibe $z = |z|(\cos\varphi + i\sin\varphi)$. Dann ist $\sqrt{z} = \sqrt{|z|}(\cos\frac{\varphi}{2} + i\sin\frac{\varphi}{2})$. Winkelhalbierung mit Zirkel und Lineal ist möglich, also o.B.d.A. $z \in \mathbb{R},\; z > 0$.



xi ist der Schnittpunkt des Thaleskreises über -1 und z mit der senkrechten Achse.
Höhensatz: $x^2 = 1 \cdot z$, d.h. $x = \sqrt{z}$.

Satz 33.3 *Für jeden Teilkörper L von $\mathbb{C}$ mit $L = \bar L$ und $i \in L$ gilt:*

(i) Ist $z \in \mathbb{C}$ Schnittpunkt von zwei verschiedenen Geraden in $G(L)$, so ist $z \in L$.

(ii) Ist $z \in \mathbb{C}$ Schnittpunkt einer Geraden in $G(L)$ und eines Kreises in $K(L)$, so ist $z \in L(w)$ für ein $w \in \mathbb{C}$ mit $w^2 \in L$.

(iii) Ist $z \in \mathbb{C}$ Schnittpunkt von zwei verschiedenen Kreisen in $K(L)$, so ist $z \in L(w)$ für ein $w \in \mathbb{C}$ mit $w^2 \in L$.

Beweis:

(i) Seien $a, b, c, d \in L$ mit $(a + \mathbb{R}\,b) \cap (c + \mathbb{R}\,d) = \{z\}$, also $a + \lambda b = z = c + \mu d$ für geeignete $\lambda, \mu \in \mathbb{R}$. Dann ist (λ, μ) die einzige Lösung des linearen Gleichungssystems

$$\begin{aligned} \lambda\,\mathrm{Re}(b) - \mu\,\mathrm{Re}(d) &= \mathrm{Re}(c-a) \\ \lambda\,\mathrm{Im}(b) - \mu\,\mathrm{Im}(d) &= \mathrm{Im}(c-a), \end{aligned}$$

liegt also in $L \times L$ wegen $\mathrm{Re}(b) = \frac{b+\bar b}{2}, \mathrm{Im}(b) = \frac{b-\bar b}{2i}, \ldots \in L$. Daher gilt: $z = a + \lambda b \in L$.

(ii) Sei z Schnittpunkt der Geraden $a + \mathbb{R}\,b$ $(a, b \in L)$ mit dem Kreis $\{x + iy : x, y \in \mathbb{R},\; (x-c)^2 + (y-d)^2 = \rho^2\}$ $(c, d, \rho \in L \cap \mathbb{R})$. Schreibt man $z = a + \lambda b$ mit $\lambda \in \mathbb{R}$, so ist also

$$(\mathrm{Re}(a) + \lambda\,\mathrm{Re}(b) - c)^2 + (\mathrm{Im}(a) + \lambda\,\mathrm{Im}(b) - d)^2 = \rho^2.$$

Dies ist eine quadratische Gleichung für λ mit Koeffizienten in $L \cap \mathbb{R}$. Ist D die entsprechende Diskriminante, so ist also $D \in L$ und $\lambda \in L(\sqrt{D})$, also auch $z = a + \lambda b \in L(\sqrt{D})$.

(iii) Sei z Schnittpunkt der Kreise mit folgenden Gleichungen: $(x - a_j)^2 + (y - b_j)^2 = \rho_j^2$ $(a_j, b_j, \rho_j \in L \cap \mathbb{R},\; j = 1, 2)$. Durch Subtraktion erhält man eine Gleichung der Form

$$(a_1 - a_2)x + (b_1 - b_2)y = c$$

mit $c \in L \cap \mathbb{R}$. Da die Mittelpunkte $a_1 + ib_1, a_2 + ib_2$ der gegebenen Kreise verschieden sind, beschreibt diese Gleichung eine Gerade, auf der mindestens zwei Punkte von L liegen. Also folgt die Behauptung aus (ii).

Satz 33.4 *Für eine Teilmenge M von $\mathbb{C}$ mit $0,1 \in M$ und ein Element $z \in \mathbb{C}$ sind äquivalent:*

(1) z ist aus M konstruierbar.

(2) Es gibt eine Kette $\mathbb{Q}(M \cup \bar{M}) = L_0 \subseteq L_1 \subseteq \ldots \subseteq L_m$ von Teilkörpern L_n von $\mathbb{C}$ mit $z \in L_m$ und $[L_n : L_{n-1}] = 2$ für $n = 1, \ldots, m$.

Beweis:

(2)⇒(1): Sei (2) erfüllt. Nach 33.2 ist $L_0 = \mathbb{Q}(M \cup \bar{M}) \subseteq M_\infty$. Sei also $n \in \{1, 2, \ldots, m\}$ mit $L_{n-1} \subseteq M_\infty$. Sei ferner $x \in L_n \backslash L_{n-1}$ und $m_{L_{n-1},x} = X^2 + aX + b$ mit $a, b \in L_{n-1}$. Dann ist $L_n = L_{n-1}(x) = L_{n-1}(x + \frac{a}{2})$ und $(x + \frac{a}{2})^2 = x^2 + ax + \frac{a^2}{4} = \frac{a^2}{4} - b \in L_{n-1} \subseteq M_\infty$, also auch $x + \frac{a}{2} \in M_\infty$ nach 33.2 und damit $L_n = L_{n-1}(x + \frac{a}{2}) \subseteq M_\infty$.

(1)⇒(2): Sei $z \in M_\infty$, also $z \in M_k$ für ein $k \in \mathbb{N}_0$, o.B.d.A. $k \in \mathbb{N}$. Dann ist z in einem Schritt aus endlich vielen Punkten $y_1, \ldots, y_n \in M_{k-1}$ konstruierbar. Wir können annehmen, daß $y_1, \ldots, y_n$ bereits (2) erfüllen. Für $j = 1, \ldots, n$ existiert also eine Kette $\mathbb{Q}(M \cup \bar{M}) = L_{j0} \subseteq L_{j1} \subseteq \ldots \subseteq L_{jl_j}$ von Teilkörpern von $\mathbb{C}$ mit $y_j \in L_{jl_j}$ und $[L_{jh} : L_{jh-1}] = 2$ für $h = 1, \ldots, l_j$. Jedes L_{jh} entsteht aus L_{jh-1} durch Adjunktion einer Quadratwurzel. Adjungiert man zu $\mathbb{Q}(M \cup \bar{M})$ nacheinander all diese Quadratwurzeln sowie ihre komplex Konjugierten und i, so erhält man eine Kette von Teilkörpern $\mathbb{Q}(M \cup \bar{M}) = K_0 \subseteq K_1 \subseteq \ldots \subseteq K_r$ mit $K_r = \bar{K_r}$ und $i, y_1, \ldots, y_n \in K_r$. Aus 33.3 folgt also die Behauptung für z.

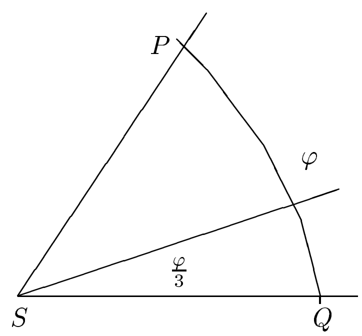
Bemerkung: Für jedes Element $z \in M_\infty$ ist also insbesondere $[\mathbb{Q}(M \cup \bar{M}, z) : \mathbb{Q}(M \cup \bar{M})]$ eine Potenz von 2.

Delisches Problem: Zu einem gegebenen Würfel der Kantenlänge a konstruiere man einen Würfel doppelten Volumens. Für die Kantenlänge x des gesuchten Würfels gilt also: $x^3 = 2a^3$. Im Fall $a = 1$ lautet die Frage: Ist $\sqrt[3]{2}$ aus $\{0, 1\}$ konstrierbar? Wegen $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$ ist dies nach 33.4 nicht möglich.

Quadratur des Kreises: Zu einem gegebenen Kreis vom Radius r konstruiere man ein Quadrat gleichen Flächeninhalts. Für die Seitenlänge x des gesuchten Quadrats muß also gelten: $x^2 = \pi r^2$. Im Fall $r = 1$ lautet also die Frage: Ist $\sqrt{\pi}$ aus $\{0, 1\}$ konstruierbar? Da mit π auch $\sqrt{\pi}$ transzendent über $\mathbb{Q}$ ist, ist dies nach 33.4 unmöglich.

Rektifikation des Kreises: Zu einem gegebenen Kreis vom Radius r konstruiere man eine Strecke, deren Länge x gleich dem Umfang des Kreises ist. Es muß also gelten: $x = 2\pi r$. Im Fall $r = 1$ lautet also die Frage: Ist 2π aus $\{0, 1\}$ konstruierbar? Da 2π transzendent über $\mathbb{Q}$ ist, ist dies unmöglich.

Dreiteilung von Winkeln: Zu einem gegebenen Winkel der Größe φ soll ein Winkel der Größe $\frac{\varphi}{3}$ konstruiert werden:



Sei o.B.d.A. $S = 0,\ Q = 1,\ P = e^{i\varphi}$. Dann lautet die Frage: Ist $e^{i\varphi/3}$ aus $\{0, 1, e^{i\varphi}\}$ konstruierbar? Äquivalent dazu ist die Konstruierbarkeit von $x := \cos\frac{\varphi}{3}$ aus $\{0, 1, c := \mathrm{Re}(e^{i\varphi}) = \cos\varphi\}$. Wegen $\cos(3\beta) = 4\cos^3\beta - 3\cos\beta$ ist x Nullstelle des Polynoms $4X^3 - 3X - c$. Im Fall $\varphi = \frac{\pi}{3}$ ist $\cos\varphi = \frac{1}{2}$, also x Nullstelle von $8X^3 - 6X - 1$ und $2x$ Nullstelle von $X^3 - 3X - 1$. Dieses Polynom ist irreduzibel in $\mathbf{Z}[X]$ und $\mathbb{Q}[X]$, d.h. $[\mathbb{Q}(x) : \mathbb{Q}] = 3$. Nach 33.4 ist also die Dreiteilung von Winkeln i.a. unmöglich.

Konstruktion regelmäßiger n-Ecke: Für welche $n \in \mathbb{N}$ kann man ein regelmäßiges n-Eck mit Zirkel und Lineal konstruieren? Die Frage ist also: Für welche $n \in \mathbb{N}$ ist die Zahl $e^{2\pi i/n}$ aus $\{0, 1\}$ konstruierbar? Nach 33.4 ist dies äquivalent zu der Frage, für welche $n \in \mathbb{N}$ $[\mathbb{Q}(e^{2\pi i/n}) : \mathbb{Q}]$ eine Potenz von 2 ist. Bekanntlich ist $[\mathbb{Q}(e^{2\pi i/n}) : \mathbb{Q}] = \varphi(n)$. Hat n die Primfaktorzerlegung $n = 2^a p_1^{b_1} \ldots p_t^{b_t}$, so ist $\varphi(n) = 2^{a-1} p_1^{b_1 - 1}(p_1 - 1) \ldots p_t^{b_t - 1}(p_t - 1)$. Dies ist genau dann eine 2-Potenz, wenn $b_i = 1$ und $p_i - 1$ Potenz von 2 für $i = 1, \ldots, t$ ist. Eine Primzahl p mit der Eigenschaft, daß $p - 1$ eine 2-Potenz ist, nennt man eine *Fermatsche Primzahl*. Ein regelmäßiges n-Eck ist also genau dann mit Zirkel und Lineal konstruierbar, wenn n Produkt einer 2-Potenz mit paarweise verschiedenen Fermatschen Primzahlen ist. Für $r, s \in \mathbb{N}$ mit $s \equiv 1 \pmod 2$ ist $2^{rs} + 1 = (2^r + 1)(2^{r(s-1)} - 2^{r(s-2)} + - \ldots - 2^r + 1)$. Daher ist eine Fermatsche Primzahl stets von der Form $2^{2^n} + 1$ für ein $n \in \mathbb{N}_0$. Für $n = 0, 1, 2, 3, 4$ erhält man die Primzahlen $3, 5, 17, 257, 65537$. Fermat vermutete, daß alle Zahlen der Form $2^{2^n} + 1$ Primzahlen sind. Euler bewies jedoch $641 \mid 2^{2^5} + 1$. Bis heute hat man außer den obigen keine weitere Fermatsche Primzahl gefunden. Es ist unbekannt, ob es unendlich viele Fermatsche Primzahlen gibt. Allerdings ist auch unbekannt, ob $2^{2^n} + 1$ für unendlich viele $n \in \mathbb{N}$ keine Primzahl ist. Die kleinste natürliche Zahl n, für die unbekannt ist, ob $2^{2^n} + 1$ Primzahl ist oder nicht, ist $n = 22$ (Stand $\sim$ 1987).

Kapitel 34

Dedekindringe

Definition 34.1 *Sei R Integritätsbereich mit Quotientenkörper K. Ein* gebrochenes Ideal *von R (oder auch ungenauer von K) ist ein R-Untermodul $I \neq 0$ von K mit $rI \subseteq R$ für ein $r \in R \setminus \{0\}$.*

Bemerkung:

(i) Die in R enthaltenen gebrochenen Ideale von R sind genau die von 0 verschiedenen Ideale in R.

(ii) Für gebrochene Ideale I, J von R sind auch $I \cap J,\ I + J,\ IJ := \{\sum_{i=1}^n a_i b_i : a_1, \dots, a_n \in I,\ b_1, \dots, b_n \in J,\ n \in \mathbb{N}_0\}$ gebrochene Ideale von R; für $r, s \in R \setminus \{0\}$ mit $rI \subseteq R,\ sJ \subseteq R$ ist nämlich $rs \in R \setminus \{0\}$ mit

$$(rs)(I + J) = rsI + rsJ \subseteq sR + rR \subseteq R + R = R,$$
$$(rs)(IJ) = (rI)(sJ) \subseteq RR \subseteq R$$

und

$$I \cap J \supseteq rI \cap sJ \supseteq (rI)(sJ) \neq 0.$$

(iii) Die gebrochenen Ideale von R bilden bzgl. der in (ii) definierten Multiplikation ein kommutatives Monoid mit Einselement R.

(iv) Jeder endlich erzeugte R-Untermodul $I \neq 0$ von K ist ein gebrochenes Ideal von R; ist nämlich $I = R\frac{x_1}{y_1} + \dots + R\frac{x_n}{y_n}$ mit $x_1, \dots, x_n \in R,\ y_1, \dots, y_n \in R \setminus \{0\}$, so ist $(y_1 \dots y_n)I \subseteq R$.

(v) Für jedes gebrochene Ideal I von R ist auch $I^{-1} := \{x \in K : xI \subseteq R\}$ ein gebrochenes Ideal von R, denn offenbar ist I^{-1} ein R-Untermodul von K mit $I^{-1} \neq 0$, und für $r \in R \setminus \{0\}$ mit $rI \subseteq R$ und $a \in I \setminus \{0\}$ ist $ra \in R \setminus \{0\}$ mit $raI^{-1} \subseteq rR \subseteq R$.

Definition 34.2 *Sei R Integritätsbereich mit Quotientenkörper K und I ein gebrochenes Ideal von R mit $II^{-1} = R$. Dann nennt man I* invertierbar.

Bemerkung:

(i) Ein gebrochenes Ideal I von R ist genau dann invertierbar, wenn ein gebrochenes Ideal J von R mit $IJ = R$ existiert; denn dann ist offenbar $J \subseteq I^{-1}$, also $R = IJ \subseteq II^{-1} \subseteq R$.

(ii) Ist I invertierbar, so ist I^{-1} das Inverse zu I im Monoid der gebrochenen Ideale von R.

(iii) Jedes invertierbare gebrochene Ideal I von R ist endlich erzeugt; wegen $II^{-1} = R$ existieren nämlich $a_1, \dots, a_n \in I,\ b_1, \dots, b_n \in I^{-1}$ mit $a_1b_1 + \dots + a_nb_n = 1$. Für $x \in I$ ist also $x = x1 = a_1(xb_1) + \dots + a_n(xb_n)$ mit $xb_1, \dots, xb_n \in R$. Folglich ist $I = Ra_1 + \dots + Ra_n$.

(iv) Für $a \in K \setminus \{0\}$ ist Ra ein invertierbares gebrochenes Ideal von R mit $(Ra)^{-1} = Ra^{-1}$. Gebrochene Ideale dieser Form nennt man *gebrochene Hauptideale.*

Definition 34.3 *Ein* Dedekindring *ist ein noetherscher ganz abgeschlossener Integritätsbereich, in dem jedes von 0 verschiedene Primideal maximal ist.*

Beispiel: Jeder Hauptidealring ist ein Dedekindring.

Lemma: *Sei I ein Ideal in dem Dedekindring R mit $0 \neq I \neq R$. Dann existieren Primideale $P_1, \ldots, P_r$ von R mit $P_1 \ldots P_r \subseteq I \subseteq P_1 \cap \ldots \cap P_r$.*

Beweis: Ist die Menge aller Ideale von R, die diese Eigenschaft nicht erfüllen, nichtleer, so enthält sie ein maximales Element J. Dann ist J kein Primideal, es existieren also $a, b \in R \setminus J$ mit $ab \in J$. Für die Ideale $A := J + Ra,\ B := J + Rb$ von R gilt also: $AB \subseteq J + Rab \subseteq J \subseteq A \cap B$; insbesondere ist $A \neq R \neq B$. Daher erfüllen A, B die geforderten Eigenschaften, also auch J.

Satz 34.4 *In einem Dedekindring R ist jedes Primideal $P \neq 0$ invertierbar.*

Beweis: Sei $a \in P \setminus \{0\}$, und seien $P_1 \neq 0, \ldots, P_k \neq 0$ Primideale in R mit $P_1 \ldots P_k \subseteq Ra$; dabei sei k so klein wie möglich. Wegen $P_1 \ldots P_k \subseteq Ra \subseteq P$ ist $P_i \subseteq P$ für ein $i \in \{1, \ldots, k\}$, o.B.d.A. $i = 1$. Da P_1 maximales Ideal in R ist, folgt $P_1 = P$. Wegen $P_2 \ldots P_k \not\subseteq Ra$ existiert ein $b \in P_2 \ldots P_k \setminus Ra$. Dann ist $Pb \subseteq P_1 P_2 \ldots P_k \subseteq Ra$ und $a^{-1}bP \subseteq R$, d.h. $y := a^{-1}b \in P^{-1} \setminus R$.
Offenbar ist $P^{-1}P$ ein Ideal in R mit $P = RP \subseteq P^{-1}P \subseteq R$. Im Fall $P^{-1}P = R$ sind wir fertig. Sei d.h. $P^{-1}P \neq R$, also $P^{-1}P = P$ wegen der Maximalität von P. Folglich wäre dann $(P^{-1})^n P = P$ für $n \in \mathbb{N}_0$, also $xy^n \in P \subseteq R$ für $x \in P$ und $n \in \mathbb{N}_0$. Daher wäre $xR[y]$ ein Ideal in R, also endlich erzeugt nach Voraussetzung, etwa $xR[y] = Ra_1 + \ldots + Ra_n$. Dann wäre aber $R[y] = R\frac{a_1}{x} + \ldots + R\frac{a_n}{x}$ endlich erzeugt, also y ganz über R und damit $y \in R$. Widerspruch.

Satz 34.5 *In einem Dedekindring R ist jedes Ideal I Produkt von Primidealen. Sind $P_1, \ldots, P_r, Q_1, \ldots, Q_s$ von 0 verschiedene Primideale in R mit $P_1 \ldots P_r = Q_1 \ldots Q_s$, so ist $r = s$ und $Q_i = P_i$ für $i = 1, \ldots, r$ bei geeigneter Numerierung.*

Beweis: O.B.d.A. sei $R \neq I \neq 0$. Wir wählen Primideale $P_1 \neq 0, \ldots, P_r \neq 0$ von R mit $P_1 \ldots P_r \subseteq I$, r möglichst klein. Im Fall $r = 1$ ist $P_1 = I$ wegen der Maximalität von P_1. Sei also $r \geq 2$ und M ein maximales Ideal von R mit $I \subseteq M$. Wegen $P_1 \ldots P_r \subseteq I \subseteq M$ ist $P_i \subseteq M$ für ein $i \in \{1, \ldots, r\}$, o.B.d.A. $i = 1$. Wegen der Maximalität von P_1 ist $P_1 = M$ und $P_2 \ldots P_r = M^{-1}P_1P_2 \ldots P_r \subseteq M^{-1}I \subseteq M^{-1}M \subseteq R$. Argumentiert man durch Induktion nach r, so kann man annehmen, daß das Ideal $M^{-1}I$ von R Produkt von Primidealen in R ist. Folglich gilt dies auch für $M(M^{-1}I) = I$.
Sei nun $P_1 \ldots P_r = Q_1 \ldots Q_s$. Dann ist $Q_1 \ldots Q_s \subseteq P_1$, also $Q_i \subseteq P_1$ für ein $i \in \{1, \ldots, s\}$, o.B.d.A. $i = 1$. Aus der Maximalität von Q_1 folgt $Q_1 = P_1$. Damit ist $P_2 \ldots P_r = P_1^{-1}P_1P_2 \ldots P_r = Q_1^{-1}Q_1Q_2 \ldots Q_s = Q_2 \ldots Q_s$, und mit Induktion folgt die Behauptung.

Bemerkung:

(i) Dies verallgemeinert die eindeutige Primfaktorzerlegung von Hauptidealringen auf Dedekind-Ringe. Jedes Ideal $I \neq 0$ von R hat also eine eindeutige Primfaktorzerlegung $I = \prod_P P^{\alpha_P}$; dabei durchläuft P die von 0 verschiedenen Primideale von R, es ist $\alpha_P \in \mathbb{N}_0$ für alle P und $|\{P : \alpha_P \neq 0\}| < \infty$.

(ii) Es folgt leicht, daß jedes gebrochene Ideal von R eine eindeutige Primfaktorzerlegung $\prod_P P^{\alpha_P}$ mit $\alpha_P \in \mathbf{Z}$ für alle P und $|\{P : \alpha_P \neq 0\}| < \infty$ hat (I gebrochenes Ideal $\Rightarrow \exists r \in R \setminus \{0\} : rI \subseteq R$. Schreibe $rI = P_1 \ldots P_r$, $rR = Q_1 \ldots Q_s$. Dann ist $I = r^{-1}R \cdot rI = P_1 \ldots P_r Q_1^{-1} \ldots Q_s^{-1}$). Die gebrochenen Ideale von R bilden also bzgl. $\cdot$ eine freie abelsche Gruppe mit den von 0 verschiedenen Primidealen von R als Basis. Diese Gruppe nennt man die *Idealgruppe* von R.

(iii) Für gebrochene Ideale I, J von R mit Primfaktorzerlegungen $I = \prod_P P^{\alpha_P}$, $J = \prod_P P^{\beta_P}$ *gilt* : $I \subseteq J \Leftrightarrow \beta_P \leq \alpha_P$ für alle P. Daraus folgt leicht:

$$I + J = \prod_P P^{\min\{\alpha_P, \beta_P\}}, \quad I \cap J = \prod_P P^{\max\{\alpha_P, \beta_P\}}.$$

Satz 34.6 *Ein Integritätsbereich R ist genau dann Dedekindring, wenn jedes gebrochene Ideal von R invertierbar ist.*

Beweis:

⇒: Sei I gebrochenes Ideal mit Primfaktorzerlegung $I = P_1^{\alpha_1} \ldots P_r^{\alpha_r}$. Nach 34.4 ist P_i invertierbar für $i = 1, \ldots, r$, also auch I.

⇐: (i) R noethersch: Bemerkung 34.2(iii).

(ii) Jedes Primideal $P \neq 0$ in R ist maximal: Sei M maximales Ideal in R mit $P \subseteq M$. Dann ist $PM^{-1} \subseteq MM^{-1} = R$, also PM^{-1} Ideal in R. Wegen $PM^{-1}M = PR = P$ folgt: $PM^{-1} \subseteq P$ oder $M \subseteq P$. Im Fall $M = P$ sind wir fertig. Wäre $PM^{-1} \subseteq P$, so wäre $M^{-1} = P^{-1}(PM^{-1}) \subseteq P^{-1}P = R$, also $M^{-1} = R$ und damit $M = R$. Widerspruch.

(iii) R ganz abgeschlossen: Sei K der Quotientenkörper von R und $x \in K$ ganz über R, o.B.d.A. $x \neq 0$. Dann ist $R[x]$ ein endlich erzeugter R-Untermodul von K mit $R[x] \neq 0$, also ein gebrochenes Ideal von R und damit nach Voraussetzung invertierbar. Wegen $R[x]R[x] = R[x]$ ist also $R[x] = R$, insbesondere ist $x \in R$.

Satz 34.7 *Sei R ein Dedekindring mit Quotientenkörper K, $L|K$ eine endliche separable Körpererweiterung und S der ganze Abschluß von R in L. Dann ist auch S ein Dedekindring.*

Beweis:

(i) Nach 32.7 ist S als R-Modul endlich erzeugt, also noethersch. Daher ist jedes Ideal in S als R-Modul endlich erzeugt, also auch als S-Modul. Folglich ist S ein noetherscher Ring.

(ii) Sind Q, Q' Primideale in S mit $Q \subsetneq Q'$, so sind $P := Q \cap R$, $P' := Q' \cap R$ Primideale in R mit $P \subseteq P'$.
Annahme: $P = P'$. Für $x \in Q' \setminus Q$ ist $m_{K,x} \in R[X]$ nach 32.5, etwa $m_{K,x} = X^n + a_{n-1}X^{n-1} + \ldots + a_1X + a_0$ mit $a_0, \ldots, a_{n-1} \in R$. Wäre $a_i \in P$ für $i = 0, \ldots, n-1$, so wäre $x^n \in Q$, also auch $x \in Q$. Daher existiert ein $j \in \{0, \ldots, n-1\}$ mit $a_j \notin P$, $a_0, \ldots, a_{j-1} \in P$. Dann ist $x^j(x^{n-j} + \ldots + a_j) = -a_{j-1}x^{j-1} - \ldots - a_1x - a_0 \in Q$, also $x^{n-j} + \ldots + a_j \in Q \subseteq Q'$. Wegen $x^{n-j} + \ldots + a_{j+1}x \in Q'$ folgt der Widerspruch $a_j \in Q' \cap R = P' = P$.
Daher ist $P \subsetneq P'$, also $P = 0 = 0 \cap R$. Also ist $Q \cap R = 0 \cap R$ und $Q \supseteq 0$. Wie oben folgt $Q = 0$. Dies zeigt, daß jedes von 0 verschiedene Primideal in S maximal ist.

(iii) Ist $x \in L$ ganz über S, so auch ganz über R. Daher ist $x \in S$. Also ist S ganz abgeschlossen in L.

Bemerkung: Die Aussage stimmt auch noch, wenn $L|K$ inseparabel ist, siehe etwa Jacobson, Basic Algebra II.

Beispiel: $R = \mathbf{Z}$, $K = \mathbb{Q}$. In diesem Fall ist S der Ganzheitsring $\mathcal{O}_L$ eines algebraischen Zahlkörpers L. Dieser ist also stets ein Dedekindring, was für die Algebraische Zahlentheorie von fundamentaler Bedeutung ist. So ist z.B. $\mathbf{Z}[\sqrt{-5}]$ ein Dedekindring.

Lemma 34.8 *Zu Idealen $A \neq 0, B \neq 0$ eines Dedekindrings R existiert stets ein Ideal $C \neq 0$ von R, so daß $B + C = R$ und AC ein Hauptideal ist.*

Beweis: Sei $A = P_1^{a_1} \dots P_n^{a_n}$, $B = P_1^{b_1} \dots P_n^{b_n}$ mit paarweise verschiedenen Primidealen $P_1, \dots, P_n$ von R und $a_1, b_1, \dots, a_n, b_n \in \mathbb{N}_0$. Für $i = 1, \dots, n$ wählen wir ein $x_i \in P_i^{a_i} \setminus P_i^{a_i+1}$. Wegen $P_i^{a_i+1} + P_j^{a_j+1} = R$ für $i \neq j$ existiert nach dem Chinesischen Restsatz ein $x \in R$ mit $x \equiv x_i \pmod{P_i^{a_i+1}}$ für $i = 1, \dots, n$; insbesondere ist $x \in P_i^{a_i} \setminus P_i^{a_i+1}$ für $i = 1, \dots, n$, also $x \in P_1^{a_1} \dots P_n^{a_n} = A$. Wegen $Rx \subseteq A$ folgt aus der Eindeutigkeit der Primfaktorzerlegung $Rx + AB = A$. Ferner existiert ein Ideal $C \neq 0$ von R mit $AC = Rx$, also $AC + AB = A$. Dann ist $C + B = A^{-1}(AC + AB) = A^{-1}A = R$.

Bemerkung: Hat R nur endlich viele Primideale $P_1, \dots, P_r$, so betrachte man den Spezialfall $B := P_1 \dots P_r$. Wegen $B + C = R$ ist dann $C = R$, also A Hauptideal. Daher ist jeder Dedekindring mit nur endlich vielen Primidealen ein Hauptidealring.

Lemma 34.9 *Zu gebrochenen Idealen I, J eines Dedekindrings R mit Quotientenkörper K existieren stets $\alpha, \beta \in K \setminus \{0\}$ mit $\alpha I + \beta J = R$.*

Beweis: Wir wählen $\beta, \gamma \in K \setminus \{0\}$ mit $\beta J \subseteq R$ und $\gamma I^{-1} \subseteq R$. Nach 34.8 existiert ein Ideal $F \neq 0$ von R, so daß $\gamma I^{-1} F$ Hauptideal und $F + \beta J = R$ ist. Schreibt man $\gamma I^{-1} F = Rr$ mit $r \in R \setminus \{0\}$, so ist $F = r\gamma^{-1} I$ mit $r\gamma^{-1} \in K \setminus \{0\}$.

Kapitel 35

Quotientenmoduln und Quotientenringe

Sei R ein kommutativer Ring und W eine nichtleere multiplikativ abgeschlossene Teilmenge von R (d.h. $v, w \in W \;\Rightarrow\; vw \in W$).

Bemerkung 35.1 Nach Aufgabe 1 von Blatt 6 erhält man eine Äquivalenzrelation $\sim$ auf $M \times W$ (M ein R-Modul), wenn man definiert:

$$(m, w) \sim (m', w') \;\Leftrightarrow\; vw'm = vwm' \text{ für ein } v \in W.$$

Für $m \in M,\ w \in W$ bezeichnet man mit $\frac{m}{w}$ die Äquivalenzklasse von (m, w). Für $v \in W$ gilt dann: $\frac{m}{w} = \frac{vm}{vw}$, d.h. man kann mit Elementen aus W „erweitern“ bzw. „kürzen“.
$W^{-1}M := \{\frac{m}{w} : m \in M,\ w \in W\}$ wird zu einem R-Modul, wenn man definiert: $\frac{m}{v} + \frac{n}{w} := \frac{wm+vn}{vw}$, $r\frac{m}{w} := \frac{rm}{w}$ $(m, n \in M,\ v, w \in W,\ r \in R)$. Man nennt $W^{-1}M$ den *Quotientenmodul* von M bzgl. W.
Für $w \in W$ ist die Abbildung $\mu : M \to W^{-1}M,\ m \mapsto \frac{wm}{w}$ ein R-Homomorphismus. Dieser hängt nicht von w ab und wird als *kanonische Abbildung* von M in $W^{-1}M$ bezeichnet. Der Kern von μ ist der W-*Torsionsmodul* $T_W(M) := \{m \in M : wm = 0 \text{ für ein } w \in W\}$.
Für $w \in W$ ist die Abbildung $W^{-1}M \to W^{-1}M,\ x \mapsto wx$ bijektiv. Ist N ein beliebiger R-Modul mit der Eigenschaft, daß für $w \in W$ die Abbildung $N \to N,\ n \mapsto wn$ bijektiv ist, so existiert zu jedem R-Homomorphismus $f : M \to N$ genau ein R-Homomorphismus $F : W^{-1}M \to N$ mit $F \circ \mu = f$.

$$\begin{tikzcd} M \arrow[rr, "\mu"] \arrow[dr, "f"'] & & W^{-1}M \arrow[dl, "F"] \\ & N & \end{tikzcd}$$

Bemerkung 35.2 Nach Aufgabe 2 von Blatt 6 wird $W^{-1}R$ zu einem kommutativen Ring, wenn man definiert: $(\frac{r}{v})(\frac{s}{w}) := \frac{rs}{vw}$ für $r, s \in R,\ v, w \in W$. Man nennt $W^{-1}R$ den *Quotientenring* von R bzgl. W.
Die kanonische Abbildung $\rho : R \to W^{-1}R$ ist ein Ringhomomorphismus mit $\rho(W) \subseteq (W^{-1}R)^{\times}$. Ist S ein beliebiger kommutativer Ring und $g : R \to S$ ein Ringhomomorphismus mit $g(W) \subseteq S^{\times}$, so existiert genau ein Ringhomomorphismus $G : W^{-1}R \to S$ mit $G \circ \rho = g$.

$$\begin{tikzcd} R \arrow[rr, "\rho"] \arrow[dr, "g"'] & & W^{-1}R \arrow[dl, "G"] \\ & S & \end{tikzcd}$$

Satz: *Jeder R-Modul N mit der Eigenschaft, daß für $w \in W$ die Abbildung $\lambda_w : N \to N,\ n \mapsto wn$ bijektiv ist, wird zu einem $W^{-1}R$-Modul, wenn man definiert: $\frac{r}{w}n := \lambda_w^{-1}(rn)$ für $r \in R,\ w \in W,\ n \in N$.*

Beweis: Aufgabe 3 von Blatt 9.

Beispiel: Nach 35.1 hat $N := W^{-1}M$ für jeden R-Modul M die geforderten Eigenschaften, wird also auf diese Weise zu einem $W^{-1}R$-Modul. Wegen $\lambda_w(\frac{m}{vw}) = \frac{wm}{vw} = \frac{m}{v}$ ist $\lambda_w^{-1}(\frac{m}{v}) = \frac{m}{vw}$ für $m \in M,\ v, w \in W$, also $\frac{r}{w}\frac{m}{v} = \lambda_w^{-1}(\frac{rm}{v}) = \frac{rm}{vw}$ für $r \in R,\ v, w \in W,\ m \in M$.

Satz 35.3 *Für jeden R-Modul M mit der Eigenschaft, daß für $w \in W$ die Abbildung $\lambda_w : M \to M,\ m \mapsto wm$ bijektiv ist, ist die kanonische Abbildung $\mu : M \to W^{-1}M$ ein $W^{-1}R$-Isomorphismus.*

Beweis: Aufgabe 3 von Blatt 9.

Bemerkung 35.4 Sind M, N R-Moduln und ist $f : M \to N$ ein R-Homomorphismus, so ist nach Aufgabe 1 von Blatt 7 die Abbildung $W^{-1}f : W^{-1}M \to W^{-1}N,\ \frac{m}{w} \mapsto \frac{f(m)}{w}$ ein $W^{-1}R$-Homomorphismus. Man rechnet leicht nach, daß für R-Homomorphismen $f, f' : M \to N$ und $r \in R$ gilt: $W^{-1}(f + f') = W^{-1}f + W^{-1}f',\ W^{-1}(rf) = rW^{-1}f$. Daher ist die Abbildung

$$\mathrm{Hom}_R(M, N) \to \mathrm{Hom}_{W^{-1}R}(W^{-1}M, W^{-1}N),\ f \mapsto W^{-1}f$$

ein R-Homomorphismus. Außerdem rechnet man leicht nach, daß für R-Moduln L, M, N und R-Homomorphismen $f : L \to M,\ g : M \to N$ gilt:

$$\begin{aligned} &W^{-1}(g \circ f) = (W^{-1}g) \circ (W^{-1}f), \\ &W^{-1}(\mathrm{id}_M) = \mathrm{id}_{W^{-1}M}\,. \end{aligned}$$

Satz: *Für jede exakte Folge $L \xrightarrow{f} M \xrightarrow{g} N$ von R-Homomorphismen ist auch $W^{-1}L \xrightarrow{W^{-1}f} W^{-1}M \xrightarrow{W^{-1}g} W^{-1}N$ exakt.*

Beweis: Wegen $\mathrm{Bild}(f) \subseteq \ker(g)$ ist $g \circ f = 0$, also auch $0 = W^{-1}0 = W^{-1}(g \circ f) = (W^{-1}g) \circ (W^{-1}f)$ und damit $\mathrm{Bild}(W^{-1}f) \subseteq \ker(W^{-1}g)$.
Sind umgekehrt $m \in M,\ w \in W$ mit $0 = (W^{-1}g)(\frac{m}{w}) = \frac{g(m)}{w}$, so ist $0 = vg(m) = g(vm)$ für ein $v \in W$. Daher ist $vm \in \ker(g) = \mathrm{Bild}(f)$, d.h. $vm = f(l)$ für ein $l \in L$. Folglich ist $\frac{m}{w} = \frac{vm}{vw} = \frac{f(l)}{vw} = (W^{-1}f)(\frac{l}{vw}) \in \mathrm{Bild}(W^{-1}f)$.

Beispiel: Für jeden R-Monomorphismus $g : M \to N$ ist die Folge $0 \longrightarrow M \xrightarrow{g} N$ exakt, also auch $0 = W^{-1}0 \longrightarrow W^{-1}M \xrightarrow{W^{-1}g} W^{-1}N$. Folglich ist $W^{-1}g$ ein $W^{-1}R$-Monomorphismus. Analog ist für jeden R-Epimorphismus $f : L \to M$ auch $W^{-1}f : W^{-1}L \to W^{-1}M$ ein $W^{-1}R$-Epimorphismus.

Bemerkung 35.5 Sei M ein R-Modul, U ein Untermodul von M und $i : U \to M$ die Inklusionsabbildung. Nach 35.4 ist dann $W^{-1}i : W^{-1}U \to W^{-1}M,\ \frac{u}{w} \mapsto \frac{i(u)}{w} = \frac{u}{w}$ injektiv. Daher können und werden wir $W^{-1}U$ mit seinem Bild in $W^{-1}M$ identifizieren und so als $W^{-1}R$-Untermodul von $W^{-1}M$ auffassen.

Satz: *Für Untermoduln U, U' eines R-Moduls M gilt:*

(i) $U \subseteq U' \;\Rightarrow\; W^{-1}U \subseteq W^{-1}U'$.

(ii) $W^{-1}(U + U') = (W^{-1}U) + (W^{-1}U')$.

(iii) $W^{-1}(U \cap U') = (W^{-1}U) \cap (W^{-1}U')$.

(iv) $W^{-1}(M/U) \simeq_{W^{-1}R} (W^{-1}M)/(W^{-1}U)$.

Beweis:

(i)-(iii) Aufgabe 3 von Blatt 10.

(iv) Aufgabe 1 von Blatt 7.

Bemerkung 35.6 Sei M ein R-Modul und $\mu : M \to W^{-1}M$ die kanonische Abbildung. Für jeden $W^{-1}R$-Untermodul X von $W^{-1}M$ ist dann $W^{-1}(\mu^{-1}(X)) = X$ nach Aufgabe 1 von Blatt 7. Ferner ist $\mu^{-1}(W^{-1}U) = \{m \in M : wm \in U \text{ für ein } w \in W\}$ für jeden R-Untermodul U von M. Daher sind die Abbildungen $U \mapsto W^{-1}U$ und $X \mapsto \mu^{-1}(X)$ zueinander inverse Bijektionen zwischen der Menge aller R-Untermoduln U von M mit $T_W(M/U) = 0$ und der Menge aller $W^{-1}R$-Untermoduln von $W^{-1}M$.

Satz: *Sei M ein R-Modul und $\mu : M \to W^{-1}M$ die kanonische Abbildung. Dann gilt:*

(i) Für $m \in M$ ist $W^{-1}(Rm) = (W^{-1}R)\mu(m)$.

(ii) Ist M endlich erzeugt über R, so auch $W^{-1}M$ über $W^{-1}R$.

(iii) Ist M noethersch über R, so auch $W^{-1}M$ über $W^{-1}R$.

(iv) Für jeden R-Modul N ist $W^{-1}(M \times N) \simeq_{W^{-1}R} (W^{-1}M) \times (W^{-1}N)$.

Beweis:

(i) Für $m \in M$, $w \in W$ ist $\mu(m) = \frac{wm}{w} \in W^{-1}(Rm)$, also auch $(W^{-1}R)\mu(m) \subseteq W^{-1}(Rm)$. Für $r \in R$, $m \in M$, $w \in W$ ist umgekehrt $\frac{rm}{w} = \frac{r}{w}\frac{wm}{w} \in (W^{-1}R)\mu(m)$.

(ii) Sind $m_1, \ldots, m_n \in M$ mit $M = Rm_1 + \ldots + Rm_n$, so ist $W^{-1}M = W^{-1}(Rm_1) + \ldots + W^{-1}(Rm_n) = (W^{-1}R)\mu(m_1) + \ldots + (W^{-1}R)\mu(m_n)$.

(iii) Jeder $W^{-1}R$-Untermodul von $W^{-1}M$ hat die Form $W^{-1}U$ mit einem R-Untermodul U von M. Ist M noethersch, so ist U endlich erzeugt, also auch $W^{-1}U$ nach (ii).

(iv) Aufgabe 1 von Blatt 7.

Satz 35.7 *Für Ideale I, J von R gilt:*

(i) $(W^{-1}I)(W^{-1}J) = W^{-1}(IJ)$.

(ii) $W^{-1}I = W^{-1}R \;\Leftrightarrow\; I \cap W \neq \emptyset$.

(iii) Die Abbildung $P \mapsto W^{-1}P$ ist eine Bijektion zwischen der Menge aller Primideale P von R mit $P \cap W = \emptyset$ und der Menge aller Primideale von $W^{-1}R$.

Beweis:

(i) Aufgabe 3 von Blatt 10.

(ii)-(iii) Aufgabe 2 von Blatt 7.

Satz 35.8 *Ist* $0 \notin W$*, so gilt:*

(i) $W^{-1}R \neq 0$.

(ii) Ist R *Integritätsbereich, so auch* $W^{-1}R$.

(iii) Ist R *Hauptidealring, so auch* $W^{-1}R$.

(iv) Ist R *Dedekindring, so auch* $W^{-1}R$.

Beweis:

(i) Ist $W^{-1}R = 0$, so liegt 1_R im Kern der kanonischen Abbildung $\rho : R \to W^{-1}R$. Daher ist $0 = w1 = w$ für ein $w \in W$ nach 35.1.

(ii) Sind $r, s \in R,\ v, w \in W$ mit $0 = \frac{r}{v} \cdot \frac{s}{w} = \frac{rs}{vw}$, so existiert ein $x \in W$ mit $xrs = 0$. Wegen $x \neq 0$ ist $rs = 0$, also $r = 0$ oder $s = 0$. Damit ist $\frac{r}{v} = 0$ oder $\frac{s}{w} = 0$.

(iii) Für jedes Ideal J in $W^{-1}R$ ist $I := \rho^{-1}(J)$ ein Ideal in R mit $W^{-1}I = J$. Ist R Hauptidealring, so existiert ein $a \in R$ mit $I = Ra$, und nach 35.6 ist $J = W^{-1}I = W^{-1}(Ra) = (W^{-1}R)\rho(a)$.

(iv) Ist $J \neq 0$ ein Ideal in $W^{-1}R$, so ist $I = \rho^{-1}(J) \neq 0$ ein Ideal in R mit $W^{-1}I = J$. Ist R Dedekindring, so ist I^{-1} ein gebrochenes Ideal von R mit $II^{-1} = R$. Für $x \in I \setminus \{0\}$ ist also $I' := I^{-1}x$ ein Ideal in R mit $II' = Rx$. Daher ist $J' := W^{-1}I'$ ein Ideal in $W^{-1}R$ mit $JJ' = (W^{-1}I)(W^{-1}I') = W^{-1}(II') = W^{-1}(Rx) = (W^{-1}R)\rho(x)$. Folglich ist $J'\rho(x)^{-1}$ ein gebrochenes Ideal von $W^{-1}R$ mit $JJ'\rho(x)^{-1} = W^{-1}R$. Nach 34.6 und 34.2 ist $W^{-1}R$ Dedekindring.

Satz 35.9 *Sind* $P_1, \ldots, P_n$ *Primideale in* R *und ist* I *ein Ideal in* R *mit* $I \subseteq P_1 \cup \ldots \cup P_n$*, so ist* $I \subseteq P_k$ *für ein* $k \in \{1, \ldots, n\}$.

Beweis: Aufgabe 4 von Blatt 9.

Kapitel 36

Moduln über Dedekindringen

Bemerkung 36.1 Nach Aufgabe 2 von Blatt 8 ist ein Modul M über einem beliebigen Ring R genau dann projektiv, wenn Familien $(m_t)_{t\in T}$, $(f_t)_{t\in T}$ von Elementen $m_t \in M$, $f_t \in \mathrm{Hom}_R(M,R)$ existieren, so daß $|\{t \in T : f_t(m) \neq 0\}| < \infty$ und $m = \sum_{t\in T} f_t(m)m_t$ für $m \in M$ ist.

Satz: *Ein gebrochenes Ideal I eines Integritätsbereiches R ist genau dann invertierbar, wenn es als R-Modul projektiv ist. Daher ist ein Integritätsbereich genau dann ein Dedekindring, wenn jedes gebrochene Ideal von R projektiv ist.*

Beweis:

$\Rightarrow$: Ist I invertierbar, so existieren $a_1,\ldots,a_n \in I,\ b_1,\ldots,b_n \in I^{-1}$ mit $a_1b_1+\ldots+a_nb_n = 1$. Für $i = 1,\ldots,n$ ist $f_i : I \to R,\ x \mapsto xb_i$ ein R-Homomorphismus, und für $x \in I$ ist

$$\sum_{i=1}^{n} f_i(x)a_i = \sum_{i=1}^{n} xb_ia_i = x1 = x.$$

Nach obiger Bemerkung ist I projektiv.

$\Leftarrow$: Sei I projektiv, und seien $(m_t)_{t\in T}$, $(f_t)_{t\in T}$ wie oben. Für $t \in T,\ x,y \in I \setminus \{0\}$ ist $yf_t(x) = f_t(yx) = xf_t(y)$, also $f_t(x)/x = f_t(y)/y$. Daher ist $z_t := f_t(x)/x$ unabhängig von der Wahl von x. Wegen $z_tx = f_t(x) \in R$ für $x \in I$ ist $z_t \in I^{-1}$. Offenbar ist $|\{t \in T : z_t \neq 0\}| < \infty$ und $x = \sum_{t\in T} z_txm_t$, d.h. $1 = \sum_{t\in T} z_tm_t$. Folglich ist $1 \in I^{-1}I$, d.h. $I^{-1}I = R$.

Bemerkung 36.2 Sei M ein endlich erzeugter torsionsfreier Modul über dem Integritätsbereich R. Dann ist $W := R \setminus \{0\}$ eine multiplikativ abgeschlossene Teilmenge von R, und $K := W^{-1}R$ ist der Quotientenkörper von R. Daher ist $W^{-1}M$ ein K-Vektorraum, und die kanonische Abbildung $\mu : M \to W^{-1}M$ ist ein R-Homomorphismus mit Kern $\{m \in M : wm = 0 \text{ für ein } w \in W\} = 0$. Daher ist μ injektiv, und man kann M mit seinem Bild in $W^{-1}M$ identifizieren, also M als R-Untermodul von $W^{-1}M$ auffassen. Nach 35.6 ist $\dim_K(W^{-1}M) < \infty$, und man nennt diese Dimension den *Rang* von M über R. Schreibweise $\mathrm{rg}(M)$ oder $\mathrm{rg}_R(M)$. Ist M selbst frei, etwa $M \simeq R^n$ für ein $n \in \mathbb{N}$, so ist $W^{-1}M \simeq W^{-1}(R^n) \simeq (W^{-1}R)^n = K^n$. Daher stimmt der soeben definierte Rang mit dem früher definierten Rang überein, falls beide definiert sind.

Satz: *Zu jedem endlich erzeugen torsionsfreien R-Modul M über einem Integritätsbereich R existiert ein endlich erzeugter freier R-Modul N mit $M \subseteq N$.*

Beweis: Wie oben gezeigt, existiert ein endlich-dimensionaler Vektorraum V über dem Quotientenkörper K von R mit $M \subseteq V$. Sei $m_1, \dots, m_r$ ein Erzeugendensystem von M und $v_1, \dots, v_s$ eine Basis von V. Offenbar existiert ein $a \in R \setminus \{0\}$ mit $am_i \in Rv_1 + \dots + Rv_s$ für $i = 1, \dots, r$. Dann erfüllt $N := R\frac{v_1}{a} + \dots + R\frac{v_s}{a}$ die Behauptung.

Satz 36.3 *Zu jedem endlich erzeugten torsionsfreien R-Modul M über dem Dedekindring R existieren Ideale $I_1, \dots, I_n$ von R mit $M \simeq I_1 \times \dots \times I_n$; insbesondere ist M projektiv.*

Beweis: Nach 36.2 existiert ein endlich erzeugter freier R-Modul N mit $M \subseteq N$. Sei $x_1, \dots, x_n$ Basis von N. Im Fall $n = 0$ ist nichts zu beweisen. Sei also $n \geq 1$ und die Aussage für $n-1$ bewiesen. Jedes Element $x \in M$ hat die Form $x = r_1x_1 + \dots + r_nx_n$ mit eindeutig bestimmten $r_1, \dots, r_n \in R$. Daher ist die Abbildung $f : M \to R$, die ein Element der Form $r_1x_1 + \dots r_nx_n$ auf r_1 abbildet, ein R-Homomorphismus, und man erhält eine exakte Folge $0 \longrightarrow \ker(f) \longrightarrow M \longrightarrow f(M) \longrightarrow 0$, wobei $f(M)$ ein Ideal in R ist. Nach 36.1 ist $f(M)$ projektiv, d.h. diese exakte Folge zerfällt. Folglich ist $M \simeq \ker(f) \times f(M)$, und $\ker(f)$ ist ein endlich erzeugter torsionsfreier R-Modul mit $\ker(f) \subseteq Rx_2 + \dots + Rx_n$. Mit Induktion folgt die Behauptung.

Bemerkung: Ist L ein beliebiger endlich erzeugter Modul über dem Dedekindring R, so ist $L/T(L)$ endlich erzeugt, torsionsfrei und damit projektiv. Daher zerfällt die exakte Folge $0 \longrightarrow T(L) \longrightarrow L \longrightarrow L/T(L) \longrightarrow 0$, und man erhält: $L \simeq T(L) \times (L/T(L))$.

Satz 36.4 *Zwei gebrochene Ideale I, J eines Integritätsbereiches R mit Quotientenkörper K sind genau dann R-isomorph, wenn ein $a \in K$ mit $aI = J$ existiert.*

Beweis:

$\Leftarrow$: Ist $aI = J$ für ein $a \in K$, so ist die Abbildung $I \to J,\ x \mapsto ax$ ein R-Isomorphismus.

$\Rightarrow$: Wir können I, J durch xI, yJ für geeignete $x, y \in K \setminus \{0\}$ ersetzen und so $R \subseteq I \cap J$ annehmen. Für $z \in I$ und einen R-Isomorphismus $f : I \to J$ ist dann $f(z) = zf(1)$, also $J = If(1)$.

Satz 36.5 *Für gebrochene Ideale I, J eines Dedekindrings R gilt stets: $I \times J \simeq R \times IJ$.*

Beweis: O.B.d.A. sei $I + J = R$ nach 34.9. Wir wählen $a \in I,\ b \in J$ mit $a + b = 1$. Dann ist die Abbildung $f : I \times J \to R,\ (x, y) \mapsto x - y$ ein R-Homomorphismus mit $f(a, -b) = a + b = 1$, also surjektiv. Ferner ist $\ker(f) = \{(x, x) : x \in I \cap J\} \simeq I \cap J = IJ$. Man erhält so eine zerfallende exakte Folge $0 \longrightarrow IJ \longrightarrow I \times J \longrightarrow R \longrightarrow 0$, und die Behauptung folgt.

Bemerkung: Für gebrochene Ideale $I_1, \dots, I_n$ von R gilt also stets: $I_1 \times \dots \times I_n \simeq R^{n-1} \times (I_1 \dots I_n)$.

Satz 36.6 *Seien $I_1, \dots, I_m, J_1, \dots, J_n$ gebrochene Ideale eines Dedekindrings R mit Quotientenkörper K. Genau dann ist $I_1 \times \dots \times I_m \simeq J_1 \times \dots \times J_n$, wenn $m = n$ ist und ein $a \in K$ existiert mit $aI_1 \dots I_m = J_1 \dots J_n$.*

Beweis:

$\Leftarrow$: Sei $m = n$ und $a \in K$ mit $aI_1 \dots I_m = J_1 \dots J_n$. Dann ist

$$\begin{aligned} I_1 \times \dots \times I_m &\simeq R^{m-1} \times (I_1 \dots I_m) \simeq R^{m-1} \times (aI_1 \dots I_m) \simeq \\ &\simeq R^{n-1} \times (J_1 \dots J_n) \simeq J_1 \times \dots \times J_n. \end{aligned}$$

⇒: Sei $M := I_1 \times \ldots \times I_m \simeq J_1 \times \ldots \times J_n =: N$. Für die Quotientenmoduln bzgl. $W := R \backslash \{0\}$ gilt dann:

$$W^{-1}M \;\simeq\; W^{-1}I_1 \times \ldots \times W^{-1}I_m \;=\; W^{-1}R \times \ldots \times W^{-1}R \;=\; K^m$$

und analog $W^{-1}N \simeq K^n$. Wegen $W^{-1}M \simeq W^{-1}N$ ist also $m = \dim_K(W^{-1}M) = \dim_K(W^{-1}N) = n$. Es genügt also zu zeigen, daß ein $a \in K$ existiert mit $aI_1 \ldots I_n = J_1 \ldots J_n$. Nach 36.4 können wir $R \subseteq I_1 \cap \ldots \cap I_n \cap J_1 \cap \ldots \cap J_n$ annehmen und einen R-Isomorphismus $f : M \to N$ wählen. Dann induziert f einen K-Isomorphismus $W^{-1}f : W^{-1}M \to W^{-1}N$. Zusammen mit dem Isomorphismen $W^{-1}M \simeq K^n$ und $W^{-1}N \simeq K^n$ erhält man also eine K-lineare Abbildung $F : K^n \to K^n$, deren Einschränkung auf $I_1 \times \ldots \times I_n$ mit f übereinstimmt. Für $k = 1, \ldots, n$ sei $q_k : I_k \to M$ die k-te Injektion und $f(q_k(1)) = (\alpha_{k1}, \ldots, \alpha_{kn})$ mit $\alpha_{kl} \in J_l$ für $l = 1, \ldots, n$. Für $x_1 \in I_1, \ldots, x_n \in I_n$ gilt also:

$$\begin{aligned} f(x_1, \ldots, x_n) \;&=\; \sum_{k=1}^{n} F(q_k(x_k)) \;=\; \sum_{k=1}^{n} x_k f(q_k(1)) \;= \\ &=\; \sum_{k=1}^{n} x_k(\alpha_{k1}, \ldots, \alpha_{kn}) \;=\; \left(\sum_{k=1}^{n} \alpha_{k1} x_k, \ldots, \sum_{k=1}^{n} \alpha_{kn} x_k \right). \end{aligned}$$

Daher ist $J_l = \sum_{k=1}^{n} \alpha_{kl} I_k$ für $l = 1, \ldots, n$. Für $g \in \mathrm{Sym}(n)$ ist also $\alpha_{1g(1)} \ldots \alpha_{ng(n)}$ $I_1 \ldots I_n \subseteq J_{g(1)} \ldots J_{g(n)} = J_1 \ldots J_n$. Für $\delta := \det(\alpha_{ij} : i, j = 1, \ldots, n)$ gilt daher:

$$\delta\, I_1 \ldots I_n \subseteq J_1 \ldots J_n.$$

Umgekehrt sei $s_l : J_l \to N$ für $l = 1, \ldots, n$ die l-te Injektion und $s_l(1) = f(\beta_{l1}, \ldots, \beta_{ln})$ mit $\beta_{lk} \in I_k$ für $k = 1, \ldots, n$. Dann ist $s_l(1) = (\sum_{k=1}^{n} \alpha_{k1}\beta_{lk}, \ldots, \sum_{k=1}^{n} \alpha_{kn}\beta_{lk})$ für $l = 1, \ldots, n$, d.h. $(\beta_{ij}\alpha_{ij})$ ist die Einheitsmatrix; insbesondere ist $\det(\beta_{ij} : i, j = 1 \ldots, n) = \delta^{-1}$. Für $y_1 \in J_1, \ldots, y_n \in J_n$ gilt:

$$\begin{aligned} (y_1, \ldots, y_n) \;&=\; \sum_{l=1}^{n} y_l s_l(1) \;=\; \sum_{l=1}^{n} y_l F(\beta_{l1}, \ldots, \beta_{ln}) \;= \\ &=\; F\left(\sum_{l=1}^{n} y_l \beta_{l1}, \ldots, \sum_{l=1}^{n} y_l \beta_{ln} \right), \end{aligned}$$

also $I_k = \sum_{l=1}^{n} J_k \beta_{lk}$ für $k = 1, \ldots, n$. Wie oben ergibt sich also:

$$\delta^{-1} J_1 \ldots J_n \subseteq I_1 \ldots I_n,$$

und die Behauptung folgt.

Satz 36.7 *Zu jedem endlich erzeugten Torsionsmodul M über einem Dedekindring R existieren eindeutig bestimmte echte Ideale $I_1, \ldots, I_s$ von R mit $I_1 \supseteq I_2 \supseteq \ldots \supseteq I_s$ und $M \simeq R/I_1 \times \ldots \times R/I_s$.*

Beweis: Seien $m_1, \ldots, m_n \in M$ mit $M = Rm_1 + \ldots + Rm_n$. Für $j = 1, \ldots, n$ ist $\mathrm{Ann}_R(Rm_j) = \{r \in R : rm_j = 0\}$ ein von 0 verschiedenes Ideal in R. Daher ist

$$I := \mathrm{Ann}_R(M) = \bigcap_{j=1}^{n} \mathrm{Ann}_R(Rm_j) \supseteq \prod_{j=1}^{n} \mathrm{Ann}_R(Rm_j) \neq 0.$$

Wir schreiben $I = P_1^{a_1} \ldots P_r^{a_r}$ mit paarweise verschiedenen Primidealen $P_1, \ldots, P_r$ von R und $a_1, \ldots, a_r \in \mathbb{N}$. Dann ist

$$W := R \setminus \bigcup_{i=1}^{r} P_i = \bigcap_{i=1}^{r} (R \setminus P_i)$$

eine nichtleere multiplikativ abgeschlossene Teilmenge von R. Für $w \in W$ ist $Rw + I = R$, also $1 = r_w w + i_w$ mit $r_w \in R$, $i_w \in I$. Für $m \in M$ ist also $m = 1m = r_w wm + i_w m = wr_w m$. Daher ist für $w \in W$ die Abbildung $\lambda_w : M \to M$, $m \mapsto wm$ bijektiv. Nach 35.2 wird M zu einem $W^{-1}R$-Modul mit $\frac{r}{w}m := \lambda_w^{-1}(rm)$ für $r \in R$, $w \in W$, $m \in M$. Ferner ist $W^{-1}R$ Dedekindring, und die Primideale in $W^{-1}R$ entsprechen eindeutig den Primidealen P in R mit $P \cap W = \emptyset$, d.h. $P \subseteq \bigcup_{i=1}^r P_i$. Da P maximal in R ist, sind dies nach 35.9 genau die Primideale $P_1, \ldots, P_r$. Daher besitzt $W^{-1}R$ nur endlich viele Primideale, ist also ein Hauptidealring nach 34.8. Da M auch endlich erzeugt über $W^{-1}R$ ist, existieren nach 31.4 echte Ideale $J_1, \ldots, J_s$ von $W^{-1}R$ mit $J_1 \supseteq J_2 \supseteq \ldots \supseteq J_s$ und

$$M \ \simeq_{W^{-1}R} \ (W^{-1}R/J_1) \times \ldots \times (W^{-1}R/J_s).$$

Ist $\rho : R \to W^{-1}R$ die kanonische Abbildung, so sind $I_1 := \rho^{-1}(J_1), \ldots, I_s := \rho^{-1}(J_s)$ echte von 0 verschiedene Ideale in R mit $I_1 \supseteq I_2 \supseteq \ldots \supseteq I_s$ und $W^{-1}I_1 = J_1, \ldots, W^{-1}I_s = J_s$. Für $j = 1, \ldots, s$ ist also $W^{-1}R/J_j = W^{-1}R/W^{-1}I_j \simeq W^{-1}(R/I_j)$. Wegen $IM = 0$ ist auch $(W^{-1}I)M = 0$. Daher ist $(W^{-1}I)(W^{-1}R/J_j) = 0$, d.h. $W^{-1}I \subseteq J_j$ und $I \subseteq \rho^{-1}(W^{-1}I) \subseteq \rho^{-1}(J_j) = I_j$ für $j = 1, \ldots, s$. Wie oben ist also für $w \in W$ und $j = 1, \ldots, s$ die Abbildung $R/I_j \to R/I_j$, $x \mapsto wx$ bijektiv. Daher ist R/I_j ein $W^{-1}R$-Modul mit $W^{-1}(R/I_j) \simeq_{W^{-1}R} R/I_j$ nach 35.3. Folglich ist $M \simeq_{W^{-1}R} R/I_1 \times \ldots \times R/I_s$, also

$$M \ \simeq_R \ R/I_1 \times \ldots \times R/I_s.$$

Sind auch $I'_1, \ldots, I'_{s'}$ echte Ideale in R mit $M \simeq R/I'_1 \times \ldots \times R/I'_{s'}$ und $I'_1 \supseteq \ldots \supseteq I'_{s'}$, so ist $I(R/I'_j) = 0$ und damit $I \subseteq I'_j$ für $j = 1, \ldots, s'$ wegen $IM = 0$. Wie oben ist also für $j = 1, \ldots, s'$ und $w \in W$ die Abbildung $R/I'_j \to R/I'_j$, $x \mapsto wx$ bijektiv. Daher ist R/I'_j ein $W^{-1}R$-Modul mit

$$R/I'_j \ \simeq_{W^{-1}R} \ W^{-1}(R/I'_j) \ \simeq_{W^{-1}R} \ W^{-1}R/W^{-1}I'_j.$$

Daher sind $W^{-1}I'_1, \ldots, W^{-1}I'_{s'}$ echte Ideale in $W^{-1}R$ mit $W^{-1}I'_1 \supseteq \ldots \supseteq W^{-1}I'_{s'}$ und

$$M \ \simeq_{W^{-1}R} \ (W^{-1}R/W^{-1}I'_1) \times \ldots \times (W^{-1}R/W^{-1}I'_{s'}).$$

Nach 31.7 ist also $s = s'$ und $W^{-1}I'_1 = J_1, \ldots, W^{-1}I'_s = J_s$. Für $j = 1, \ldots, s$ gilt also nach 35.6: $I'_j \subseteq I_j \subseteq \{r \in R : wr \in I'_j \text{ für ein } w \in W\}$. Da aber für $w \in W$ die Abbildung $R/I'_j \to R/I'_j$, $x \mapsto wx$ bijektiv ist, folgt: $I'_j = \{r \in R : wr \in I'_j \text{ für ein } w \in W\}$, also auch $I_j = I'_j$.

Satz 36.8 *Zu jedem endlich erzeugten Torsionsmodul M über einem Dedekindring R existieren eindeutig bestimmte Primideale $P_1, \ldots, P_s$ und eindeutig bestimmte $a_1, \ldots, a_s \in \mathbb{N}$ mit $M \simeq R/P_1^{a_1} \times \ldots \times R/P_s^{a_s}$.*

Beweis: Analog.

Kapitel 37

Das Radikal

Sei R ein Ring.

Definition 37.1 *Für einen R-Modul M nennt man den Durchschnitt D aller maximalen Untermoduln von M das* Radikal *von M, und man schreibt: $D = \operatorname{Rad}(M) = \operatorname{Rad}_R(M)$. (Besitzt M keine maximale Untermoduln, so setzt man $\operatorname{Rad}(M) := M$.)*

Satz:

(i) Für R-Moduln M, N und jeden R-Homomorphismus $f : M \to N$ ist $f(\operatorname{Rad}(M)) \subseteq \operatorname{Rad}(N)$.

(ii) Für jeden Untermodul N eines R-Moduls M ist $\operatorname{Rad}(N) \subseteq \operatorname{Rad}(M)$ und $\operatorname{Rad}(M) + N/N \subseteq \operatorname{Rad}(M/N)$.

(iii) Für jeden Untermodul N eines R-Moduls M mit $N \subseteq \operatorname{Rad}(M)$ ist $\operatorname{Rad}(M/N) = \operatorname{Rad}(M)/N$; insbesondere ist $\operatorname{Rad}(M/\operatorname{Rad}(M)) = 0$.

(iv) Für jede Familie $(M_i)_{i\in I}$ von R-Moduln ist $\operatorname{Rad}(\prod_{i\in I} M_i) \subseteq \prod_{i\in I} \operatorname{Rad}(M_i)$ und $\operatorname{Rad}(\coprod_{i\in I} M_i) = \coprod_{i\in I} \operatorname{Rad}(M_i)$.

Beweis:

(i) Sei L ein maximaler Untermodul von N und $g : N \to N/L$ die kanonische Abbildung. Dann ist N/L einfach, und $g \circ f : M \to N/L$ ist ein R-Homomorphismus. Daher ist $\ker(g \circ f)$ ein maximaler Untermodul von M, oder $\ker(g \circ f) = M$. In jedem Fall ist $\operatorname{Rad}(M) \subseteq \ker(g \circ f)$, also $f(\operatorname{Rad}(M)) \subseteq \ker(g) = L$.

(ii) Wende (i) an auf die Inklusionsabbildung $N \to M$ bzw. den kanonischen Epimorphismus $M \to M/N$.

(iii) Im Fall $N \subseteq \operatorname{Rad}(M)$ entsprechen sich nach den Isomorphiesätzen die maximalen Untermoduln von M und M/N.

(iv) Ist $j \in I$ und $p_j : \prod_{i\in I} M_i \to M_j$ die j-te Projektion, so gilt nach (i): $p_j(\operatorname{Rad}(\prod_{i\in I} M_i)) \subseteq \operatorname{Rad}(M_j)$. Daher ist $\operatorname{Rad}(\prod_{i\in I} M_i) \subseteq \prod_{j\in I} \operatorname{Rad}(M_j)$.
Nach (ii) ist dann $\operatorname{Rad}(\coprod_{i\in I} M_i) \subseteq \operatorname{Rad}(\prod_{i\in I} M_i) \subseteq \prod_{i\in I} \operatorname{Rad}(M_i)$, also auch $\operatorname{Rad}(\coprod_{i\in I} M_i) \subseteq \coprod_{i\in I} \operatorname{Rad}(M_i)$. Ist $j \in I$ und $q_j : M_j \to \coprod_{i\in I} M_i$ die j-te Injektion, so ist $q_j(\operatorname{Rad}(M_j)) \subseteq \operatorname{Rad}(\coprod_{i\in I} M_i)$ nach (i). Daher ist $\coprod_{j\in I} \operatorname{Rad}(M_j) = \sum_{j\in I} q_j(\operatorname{Rad}(M_j)) \subseteq \operatorname{Rad}(\coprod_{i\in I} M_i)$.

Satz 37.2 *Für jeden R-Modul M gilt:*

(i) $\operatorname{Rad}(M) = 0 \Leftrightarrow M$ ist isomorph zu einem Untermodul eines direkten Produkts einfacher R-Moduln.

(ii) M *halbeinfach* $\Rightarrow \mathrm{Rad}(M) = 0$.

(iii) M *endlich erzeugt und halbeinfach* $\Leftrightarrow$ M *artinsch und* $\mathrm{Rad}(M) = 0$.

(iv) M *endlich erzeugt und* $M \neq 0 \Rightarrow \mathrm{Rad}(M) \neq M$.

Beweis:

(i) **$\Rightarrow$:** Sei $\mathrm{Rad}(M) = 0$ und $\mathcal{M}$ die Menge aller maximalen Untermoduln von M. Dann ist die Abbildung $f : M \to \prod_{N \in \mathcal{M}} M/N,\ m \mapsto (m+N)_{N \in \mathcal{M}}$ ein R-Homomorphismus mit Kern $\bigcap_{N \in \mathcal{M}} N = \mathrm{Rad}(M) = 0$. Daher ist $M \simeq f(M) \subseteq \prod_{N \in \mathcal{M}} M/N$.

$\Leftarrow$: Sei $(S_i)_{i \in I}$ eine Familie einfacher R-Moduln und $f : M \to \prod_{i \in I} S_i$ ein R-Monomorphismus. Dann ist nach 37.1

$$f(\mathrm{Rad}(M)) = \mathrm{Rad}(f(M)) \subseteq \mathrm{Rad}(\prod_{i \in I} S_i) \subseteq \prod_{i \in I} \underbrace{\mathrm{Rad}(S_i)}_{=0} = 0,$$

also auch $\mathrm{Rad}(M) = 0$.

(ii) Sei M halbeinfach und $(M_i)_{i \in I}$ eine Familie einfacher Untermoduln von M mit $M = \bigoplus_{i \in I} M_i$. Dann ist nach 37.1

$$\mathrm{Rad}(M) = \mathrm{Rad}(\bigoplus_{i \in I} M_i) \simeq \mathrm{Rad}(\prod_{i \in I} M_i) = \prod_{i \in I} \underbrace{\mathrm{Rad}(M_i)}_{=0} = 0.$$

(iii) **$\Rightarrow$:** Sei M endlich erzeugt und halbeinfach, also $M = \bigoplus_{i \in I} M_i$ mit einer Familie $(M_i)_{i \in I}$ einfacher Untermoduln von M. Wir schreiben $M = Rm_1 + \ldots + Rm_n$ mit $m_1, \ldots, m_n \in M$. Dann existiert eine endliche Teilmenge J von I mit $m_i \in \sum_{j \in J} M_j$ für $i = 1, \ldots, n$. Dann ist aber auch $M \subseteq \sum_{j \in J} M_j$, d.h. $M = \bigoplus_{j \in J} M_j$. Da M_j für $j \in J$ einfach ist, ist M artinsch. Der Rest folgt aus (ii).

$\Leftarrow$: Sei M artinsch und $\mathrm{Rad}(M) = 0$, o.B.d.A. $M \neq 0$. Dann ist $\mathcal{M} := \{N : N \text{ Durchschnitt endlich vieler maximaler Untermoduln von } M\} \neq \emptyset$. Folglich enthält $\mathcal{M}$ ein minimales Element D. Für jeden maximalen Untermodul L von M ist auch $D \cap L \in \mathcal{M}$, also $D \subseteq D \cap L \subseteq L$ nach Wahl von D. Dies zeigt: $D \subseteq \mathrm{Rad}(M) = 0$. Es existieren also endlich viele maximale Untermoduln $M_1, \ldots, M_n$ von M mit $M_1 \cap \ldots \cap M_n = 0$. Daher ist die Abbildung $f : M \to M/M_1 \times \ldots \times M/M_n,\ m \mapsto (m + M_1, \ldots, m + M_n)$ ein R-Monomorphismus. Da $M/M_1, \ldots, M/M_n$ einfach sind, ist $M/M_1 \times \ldots \times M/M_n$ halbeinfach und noethersch, also auch M.

(iv) Sei $M \neq 0$ endlich erzeugt, etwa $M = Rm_1 + \ldots + Rm_n$ mit $m_1, \ldots, m_n \in M$, n möglichst klein. Dann ist $N := Rm_2 + \ldots + Rm_n \neq M$, also $0 \neq M/N = R(m_1 + N)$. Die Abbildung $f : R \to M/N, r \mapsto r(m_1 + N)$ ist ein R-Epimorphismus. Daher ist $R/\ker(f) \simeq M/N \neq 0$. Folglich existiert ein maximales Linkesideal L von R mit $\ker(f) \subseteq L$. Dann ist $L/\ker(f)$ ein maximaler Untermodul von $R/\ker(f)$, also $\mathrm{Rad}(R/\ker(f)) \neq R/\ker(f)$. Daher ist $M/N \underset{\neq}{\supseteq} \mathrm{Rad}(M/N) \supseteq \mathrm{Rad}(M) + N/N$; insbesondere ist $M \neq \mathrm{Rad}(M)$.

Satz 37.3 (Nakayamas Lemma) *Sei* N *ein Untermodul eines endlich erzeugten* R*-Moduls* M *mit* $M = N + \mathrm{Rad}(M)$. *Dann ist* $M = N$.

Beweis: Aus $M = N + \mathrm{Rad}(M)$ folgt: $\mathrm{Rad}(M/N) \supseteq \mathrm{Rad}(M) + N/N = M/N$. Da M/N endlich erzeugt ist, folgt aus 37.2: $M/N = 0$, d.h. $M = N$.

Satz 37.4 *Ein Element* m *eines endlich erzeugten* R*-Moduls* M *liegt genau dann in* $\mathrm{Rad}(M)$, *wenn gilt: Für jeden Untermodul* N *von* M *mit* $M = N + Rm$ *ist* $M = N$.

Beweis:

⇒: Sei $m \in \mathrm{Rad}(M)$ und N ein Untermodul von M mit $M = N + Rm$. Dann ist auch $M = N + \mathrm{Rad}(M)$, also $M = N$ nach 37.3.

⇐: Sei $m \in M \setminus \mathrm{Rad}(M)$, also $m \notin N$ für einen maximalen Untermodul N von M. Dann ist $M = N + Rm$, aber $M \neq N$.

Definition 37.5 *Man nennt das Radikal des R-Moduls R auch das* (Jacobson-)Radikal *von R.*

Bemerkung:

(i) Dann ist $\mathrm{Rad}(R)$ der Durchschnitt aller maximalen Linksideale von R. Wir werden sehen, daß $\mathrm{Rad}(R)$ auch der Durchschnitt aller maximalen Rechtsideale von R ist.

(ii) Nach 37.2 ist $\mathrm{Rad}(R) \neq R$ im Fall $R \neq 0$.

(iii) Für jedes Element M eines R-Moduls M ist die Abbildung $f : R \to M, r \mapsto rm$ ein R-Homomorphismus. Daher ist $\mathrm{Rad}(R)m = f(\mathrm{Rad}(R)) \subseteq \mathrm{Rad}(M)$. Dies zeigt: $\mathrm{Rad}(R)M \subseteq \mathrm{Rad}(M)$. Insbesondere ist $\mathrm{Rad}(R)R \subseteq \mathrm{Rad}(R)$, d.h. $\mathrm{Rad}(R)$ ist ein (zweiseitiges) Ideal von R.

(iv) Für jedes Ideal I von R ist $\mathrm{Rad}(R){+}I/I \subseteq \mathrm{Rad}(R/I)$ nach 37.1, und im Fall $I \subseteq \mathrm{Rad}(R)$ gilt sogar $\mathrm{Rad}(R/I) = \mathrm{Rad}(R)/I$; insbesondere ist $\mathrm{Rad}(R/\mathrm{Rad}(R)) = 0$.

(v) Nach 37.2 ist R genau dann halbeinfach, wenn R linksartinsch und $\mathrm{Rad}(R) = 0$ ist.

(vi) Ist R linksartinsch, so ist $R/\mathrm{Rad}(R)$ halbeinfach; denn mit R ist auch $R/\mathrm{Rad}(R)$ linksartinsch mit $\mathrm{Rad}(R/\mathrm{Rad}(R)) = 0$ wegen (iv). Also folgt die Behauptung aus (v).

(vii) Ist R linksartinsch, so ist jeder R-Modul M mit $\mathrm{Rad}(R)M = 0$ halbeinfach; man kann M dann nämlich als Modul über dem nach (vi) halbeinfachen Ring $R/\mathrm{Rad}(R)$ auffassen. Als solcher ist M halbeinfach, also auch als R-Modul.

(viii) Ist R linksartinsch und M ein R-Modul, so ist $\mathrm{Rad}(R)M = \mathrm{Rad}(M)$; denn wegen $\mathrm{Rad}(R)(M/\mathrm{Rad}(R)M) = \mathrm{Rad}(R)M/\mathrm{Rad}(R)M = 0$ ist $M/\mathrm{Rad}(R)M$ halbeinfach nach (vii), also $0 = \mathrm{Rad}(M/\mathrm{Rad}(R)M) = \mathrm{Rad}(M)/\mathrm{Rad}(R)M$ nach (iii), 37.2 und 37.1.

Satz:
$$\begin{aligned} \mathit{Rad}(R) &= \{x \in R : 1 + axb \in R^\times \textit{ für alle } a, b \in R\} \\ &= \{x \in R : 1 + ax \in R^\times \textit{ für alle } a \in R\} \\ &= \{x \in R : xS = 0 \textit{ für jeden einfachen } R\textit{-Modul } S\} \end{aligned}$$

Beweis:

(i) Seien $x \in \mathrm{Rad}(R)$ und $a, b \in R$, also $y := -axb \in \mathrm{Rad}(R)$. Wir zeigen: $1 - y \in R^\times$.
Annahme: $R(1{-}y) \neq R$. Dann existiert ein maximales Linksideal L von R mit $R(1{-}y) \subseteq L$; insbesondere ist $1 - y \in L$, und wegen $y \in \mathrm{Rad}(R) \subseteq L$ erhält man den Widerspruch $1 \in L$.
Also ist $R(1 - y) = R$; insbesondere ist $1 = z(1 - y)$ für ein $z \in R$, d.h. $1 - z = -zy \in \mathrm{Rad}(R)$. Mit den gleichen Argumenten wie für y existiert ein $u \in R$ mit $1 = u(1 - (1 - z)) = uz$. Daher ist $u = u1 = uz(1 - y) = 1 - y$, also $1 - y \in R^\times$.

(ii) Sei $x \in R$ mit $1 + ax \in R^\times$ für $a \in R$.
Annahme: $xS \neq 0$ für einen einfachen R-Modul S. Dann ist $xs \neq 0$ für ein $s \in S$. Da S einfach ist, folgt $Rxs = S$, also $rxs = s$ für ein $r \in R$. Dann ist $0 = (1 - rx)s$, und wegen $1 - rx \in R^\times$ ergibt sich der Widerspruch $s = 0$.

(iii) Sei $x \in R$ mit $xS = 0$ für jeden einfachen R-Modul S. Dann ist $x(R/M) = 0$ für jedes maximale Linksideal M von R. Für jedes solche M ist also $xR \subseteq M$, d.h. $x \in M$. Folglich ist $x \in \mathrm{Rad}(R)$.

Bemerkung 37.6 Die erste Beschreibung von $\mathrm{Rad}(R)$ in Satz 37.5 ist unabhängig davon, ob man Linksmoduln oder Rechtsmoduln betrachtet. Daher ist $\mathrm{Rad}(R)$ auch der Durchschnitt aller maximalen Rechtsideale von R und der Annullator aller einfachen R-Rechtsmoduln.

Satz: $\mathrm{Rad}(R)$ *enthält jedes Linksideal N von R, das nur aus nilpotenten Elementen besteht. (Analog für Rechtsideale)*

Beweis: Sei $x \in N$ und $a \in R$. Dann ist $y := -ax \in N$, also $y^n = 0$ für ein $n \in \mathbb{N}$. Folglich ist

$$(1-y)(1+y+y^2+\ldots+y^{n-1}) = 1-y^n = 1 = (1+y+y^2+\ldots+y^{n-1})(1-y),$$

d.h. $1 + ax \in R^\times$, und die Behauptung folgt aus 37.5.

Definition 37.7 *Ein Ideal I von R heißt* nilpotent, *falls $I^n = 0$ für ein $n \in \mathbb{N}$.*

Bemerkung: $I^n = 0$ bedeutet $x_1 \ldots x_n = 0$ für alle $x_1, \ldots, x_n \in I$, nicht nur $x^n = 0$ für alle $x \in I$.

Satz: *Ist R linksartinsch (oder rechtsartinsch), so ist* $\mathrm{Rad}(R)$ *nilpotent.*

Beweis: Ist R linksartinsch, so existiert ein $m \in \mathbb{N}$ mit $\mathrm{Rad}(R) =: J \supseteq J^2 \supseteq \ldots \supseteq J^m = J^{m+1} = \ldots$. Wir nehmen $J^m \neq 0$ an. Da R linksartinsch ist, existiert in der Menge aller Linksideale I von R mit $J^m I \neq 0$ ein minimales Element L. Wegen $J^m L \neq 0$ ist $J^m a \neq 0$ für ein $a \in L$. Daher ist $J^m a$ ein Linksideal in R mit $J^m a \subseteq L$ und $J^m J^m a = J^{2m} a = J^m a \neq 0$. Nach Wahl von L ist also $J^m a = L$, d.h $xa = a$ für ein $x \in J^m \subseteq J$. Dann ist $(1-x)a = 0$, also $a = 0$ wegen $1 - x \in R^\times$. Widerspruch.

Satz 37.8 (Hopkins) *Ist R linksartinsch, so auch linksnoethersch.*

Beweis: Sei $J := \mathrm{Rad}(R)$ und $n \in \mathbb{N}$ mit $J^n = 0$. Für $k = 1, \ldots, n-1$ ist dann J^{k-1}/J^k ein artinscher R-Modul mit $J(J^{k-1}/J^k) = J^k/J^k = 0$. Nach 37.5 (vii) ist J^{k-1}/J^k halbeinfach. Nach Aufgabe 3 von Blatt 7 ist J^{k-1}/J^k noethersch. Daher ist R auch noethersch als R-Modul.

Bemerkung: Ist R linksartinsch, so ist jeder endlich erzeugte R-Modul artinsch und noethersch.

Index