Einführung in die Algebra[1]

Martin Ziegler

Freiburg, Wintersemester 1999/2000

[1]Version 3j (26.7.2014)

Inhaltsverzeichnis

Literaturverzeichnis

[1] Serge Lang. *Algebra*. Addison–Wesley Publishing Company, second edition, 1984.

[2] Derek J. S. Robinson. *A Course in the Theory of Groups*. Graduate Texts in Mathematics. Springer Verlag; Berlin, Göttingen, Heidelberg, 1982.

Kapitel 1

Gruppen

1.1 Der Satz von Cayley

Definition *Eine Halbgruppe ist eine Menge S, auf der eine zweistellige assoziative Operation $\cdot$ erklärt ist. Eine Halbgruppe ist also ein Paar*

$$(S, \cdot),$$

wobei die Operation $\cdot : S \times S \to S$ dem Assoziativgesetz

$$(x \cdot y) \cdot z = x \cdot (y \cdot z)$$

genügt.

Beispiele:

- Die Menge ${}^X X$ aller Abbildungen einer Menge X in sich ist, mit der Komposition als Operation, eine Halbgruppe.
- Die Menge A^* aller Wörter über einem Alphabet A ist mit der Verkettung als Operation eine Halbgruppe.

Definition *Eine Halbgruppe S heißt abelsch*[1]*, oder kommutativ, wenn*

$$s \cdot t = t \cdot s$$

für alle $s, t \in S$.

Beispiel:
Die natürlichen Zahlen $\mathbb{N}$ mit der Addition sind eine abelsche Halbgruppe.

Die Operation einer Halbgruppe nennt man im allgemeinen Multiplikation. Im abelschen Fall häufig auch Addition, wo man dann $s + t$ statt $s \cdot t$ schreibt.

[1] Niels Hendrik Abel (1802-1829)

Definition *Ein Element e einer Halbgruppe S heißt linksneutral, wenn*

$$e \cdot s = s$$

für alle $s \in S$. Wenn

$$s \cdot f = s$$

für alle s, heißt f rechtsneutral.

Lemma 1.1.1 *Wenn eine Halbgruppe S ein linksneutrales Element e und ein rechtsneutrales f hat, stimmen e und f überein. Man nennt $e = f$ (das)* neutrale Element *von S.*

Beweis :

$$e = e \cdot f = f$$

□

In multiplikativ geschrieben Halbgruppen nennt man das neutrale Element 1 (falls vorhanden) *Einselement*. In additiv geschriebenen (abelschen) Halbgruppen heißt das neutrale Element 0 die Null.

In ${}^X X$ ist die Identität id_X das neutrale Element, in A^* das leere Wort und in $(\mathbb{N}, +)$ die Null.

Sei nun S eine Halbgruppe mit Einselement 1. (Man nennt solche Halbgruppen auch *Monoide*.) Wenn

$$s \cdot t = 1,$$

nennen wir s *Linksinverses* von t und t *Rechtsinverses* von s.

Lemma 1.1.2 *Sei S eine Halbgruppe mit Einselement* 1*. Wenn s ein Linksinverses s' und ein Rechtsinverses s''hat, stimmen s' und s'' überein. Man nennt $s' = s''$ das* Inverse *von s.*

Beweis :

$$s' = s' \cdot 1 = s' \cdot s \cdot s'' = 1 \cdot s'' = s''$$

□

In multiplikativen Halbgruppen schreibt man s^{-1} für das Inverse von s, in additiv geschriebenen (abelschen) Halbgruppen schreibt man $-s$.

Definition *Eine Gruppe G ist eine Halbgruppe mit neutralem Element, in der jedes Element ein Inverses hat.*

Beispiel:
Die Menge $\mathrm{Sym}(X)$ aller Permutationen von X ist eine Gruppe, die *symmetrische* Gruppe von X. Allgemein gilt: Die Menge der invertierbaren Elemente eines Monoids ist eine Gruppe.

Beispiel:
Die ganzen Zahlen $\mathbb{Z}$ mit der Addition bilden ein Gruppe.

Satz 1.1.3 *Eine Halbgruppe G ist genau dann eine Gruppe, wenn es ein linksneutrales Element e gibt, für das jedes Element $g \in G$ ein Linksinverses hat, das heißt, eine Lösung der Gleichung $x \cdot g = e$.*

Beweis :
Sei g ein beliebiges Element, g' ein Linksinverses von g und g'' ein Linksinverses von g'. Aus

$$g \cdot g' = e \cdot g \cdot g' = (g'' \cdot g') \cdot g \cdot g' = g'' \cdot (g' \cdot g) \cdot g' = g'' \cdot e \cdot g' = g'' \cdot g' = e$$

liest man ab, daß g' auch Rechtsinverses von g ist. Die Gleichung

$$g \cdot e = g \cdot (g' \cdot g) = (g \cdot g') \cdot g = e \cdot g = g$$

zeigt, daß e auch rechtsneutral ist. □

Definition *Sei G eine Gruppe. Eine Untergruppe U von G ist eine unter der Gruppenoperation abgeschlossene Teilmenge von G, die (mit der eingeschränkten Operation) eine Gruppe ist.*

Notation $U \leq G$

Weil $ff = f \Rightarrow f = 1$, muß das Einselement einer Untergruppe das Einselement von G sein. Eine Teilmenge U von G ist also genau dann Untergruppe, wenn U das Einselement enthält und abgeschlossen ist unter Multiplikation und Inversenbildung.

Definition *Zwei Gruppen G und H sind isomorph*

$$G \cong H,$$

wenn es einen Isomorphismus $f : G \to H$ zwischen G und H gibt. Dabei heißt eine Bijektion f Isomorphismus, wenn

$$f(x \cdot y) = f(x) \cdot f(y) \tag{1.1}$$

für alle $x, y \in G$.

Eine Bijektion f ist Isomorphismus, wenn sie die Gruppenoperation von G in die Gruppenoperation von H überführt, wenn also

$$x \cdot y = z \Longleftrightarrow f(x) \cdot f(y) = f(z)$$

für alle $x, y, z \in G$. Man rechnet leicht nach, daß $\cong$ eine Äquivalenzrelation ist.

Satz 1.1.4 (Cayley[2]) *Jede Gruppe ist isomorph zu einer Untergruppe einer symmetrischen Gruppe.*

[2] Arthur Cayley (1821-1895)

BEWEIS :
Sei g ein Element von G und

$$\lambda_g : G \to G$$

definiert durch $\lambda_g(x) = g \cdot x$, die Linksmultiplikation mit g. Die durch $\Lambda(g) = \lambda_g$ definierte Abbildung

$$\Lambda : G \to {}^G G$$

ist injektiv, weil $\lambda_g(1) = g$. Außerdem gilt

$$\Lambda(gh) = \Lambda(g) \circ \Lambda(h).$$

Denn

$$\lambda_{g \cdot h}(x) = (g \cdot h) \cdot x = g \cdot \lambda_h(x) = \lambda_g(\lambda_h(x)) = (\lambda_g \circ \lambda_h)(x).$$

Die Menge $U = \Lambda(G)$ der Linksmultiplikationen enthält das Einselement λ_1 von ${}^G G$ und ist abgeschlossen unter $\circ$. Weil $\lambda_{g^{-1}}$ invers zu λ_g ist, sind die Linksmultiplikationen Permutationen von G; U ist also Untergruppe von $\mathrm{Sym}(G)$. Jetzt ist klar, daß Λ ein Isomorphismus zwischen G und U ist. □

1.2 Untergruppen

Sei U eine Untergruppe von G. Die *Rechtsnebenklasse* eines Gruppenelements g ist

$$Ug = \{ug \mid u \in U\}.$$

Lemma 1.2.1 *Die Rechtsnebenklassen von U bilden eine Partition von G. Die zugehörige Äquivalenzrelation ist*

$$Ug = Uh \Longleftrightarrow gh^{-1} \in U$$

Beweis :
Wenn Ug und Uh nicht leeren Schnitt haben, ist $ug = vh$ für zwei Elemente u, v von U. Es folgt dann $gh^{-1} = u^{-1}v \in U$. Aus $gh^{-1} \in U$ folgt umgekehrt $Ug = (Ugh^{-1})h = Uh$. □

Wir bezeichnen mit G/U die Menge der Rechtsnebenklassen von U und definieren den *Index* $(G : U)$ von U in G als die Zahl der Rechtsnebenklassen von U in G:

$$(G : U) = |G/U|\,.$$

Die *Linksnebenklassen* gU liefern eine Partition von G, die im allgemeinen von der Rechtszerlegung nach U verschieden ist. Es gibt aber ebensoviele Linksnebenklassen wie Rechtsnebenklassen. Die Inversenbildung $g \mapsto g^{-1}$ ist nämlich eine Permutation von G, die die Linksnebenklassen von U gerade auf die Rechtsnebenklassen von U abbildet. Wir haben nämlich $(gU)^{-1} = U^{-1}g^{-1} = Ug^{-1}$.

$u \mapsto ug$ ist eine Bijektion zwischen U und Ug. Die Rechtsnebenklassen von U haben also ebensoviele Elemente wie U. Es folgt

Lemma 1.2.2 $|G| = (G : U) \cdot |U|$

Als ein Beispiel bestimmen wir die Untergruppen von $\mathbb{Z}$.

Lemma 1.2.3 *Die Untergruppen von $\mathbb{Z}$ sind von der Form $m\mathbb{Z}$ für ein (eindeutig bestimmtes) $m \geq 0$.*

Beweis :
Sei U eine Untergruppe von $\mathbb{Z}$. Wenn $U = 0$, ist $U = 0\mathbb{Z}$. Sonst wählen wir für m die kleinste positive Zahl in U. Natürlich ist $m\mathbb{Z} \leq U$. Für die umgekehrte Inklusion fixieren wir ein beliebiges Element u von U. Wir dividieren u durch m mit Rest r:

$$u = sm + r, \qquad 0 \leq r < m.$$

Weil $r \in U$ und m minimal gewählt war, ist $r = 0$. Also haben wir $u = sm$. □

Weil jede ganze Zahl zu genau einer Zahl zwischen 0 und $m - 1$ modulo m kongruent ist, folgt

$$(\mathbb{Z} : m\mathbb{Z}) = m.$$

Sei a ein Element einer Halbgruppe G. Wir definieren $a^1 = a$, $a^2 = aa$, $a^3 = aaa$ und allgemein für alle positiven natürlichen Zahlen n:

$$a^n = \underbrace{a \dots a}_{n-mal}.$$

Wenn G ein Monoid ist, setzt man

$$a^0 = 1.$$

Schließlich nehmen wir an, daß G eine Gruppe ist und setzen für negative Exponenten:

$$a^{-n} = \left(a^{-1}\right)^n.$$

Man verifiziert leicht die folgenden Rechenregeln.

a) $a^m a^n = a^{m+n}$

b) $(a^m)^n = a^{mn}$

c) $a^1 = a$

d) $(ab)^n = a^n b^n$, wenn a und b kommutieren.

a und b *kommutieren*, wenn $ab = ba$. In additiven (abelschen) Gruppen schreibt man na statt a^n.

Weil der Durchschnitt einer Familie von Untergruppen von G wieder eine Untergruppe ist, gibt es zu jeder Teilmenge A von G eine kleinste Untergruppe $\langle A\rangle$, die A enthält, die von A *erzeugte* Untergruppe. Die von a erzeugte Untergruppe ist $< a >= \{a^n \mid n \in \mathbb{Z}\}$.

Die Menge $\{e \in \mathbb{Z} \mid a^e = 1\}$ der *Exponenten* von a ist eine Untergruppe von $\mathbb{Z}$, also von der Form $m\mathbb{Z}$ für ein $m \geq 0$. Wir nennen m die *Ordnung* von a. Man kann die Ordnung auch einfach so definieren:

Definition *Die Ordnung* $\mathrm{ord}(a)$ *von* a *ist die kleinste positive Zahl* m *mit* $a^m = 1$, *falls ein solches* m *existiert. Sonst ist* $\mathrm{ord}(a) = 0$.

Wenn a die Ordnung 0 hat, ist die Abbildung $n \mapsto a^n$ ein Isomorphismus zwischen $\mathbb{Z}$ und $\langle a\rangle$. Man sagt deshalb üblicherweise, daß a *unendliche* Ordnung hat.
Wenn $\mathrm{ord}(a) = m > 0$, ist $\langle a\rangle = \left\{1, a^1, a^2, \dots, a^{m-1}\right\}$. Weil aus $a^i = a^{i+k}$ folgt, daß $a^k = 1$, sind die Elemente $1, a^1, a^2, \dots, a^{m-1}$ paarweise verschieden. Das bedeutet, daß

$$|\langle a\rangle| = \mathrm{ord}(a).$$

Man spricht daher häufig statt von der Mächtigkeit einer Gruppe auch von ihrer *Ordnung*.

Folgerung 1.2.4 *Die Ordnungen der Elemente* a *einer endlichen Gruppe* G *teilen die Ordnung von* G. *Anders ausgedrückt:*

$$a^{|G|} = 1$$

1.3 Homomorphismen

Definition *Eine Abbildung $f : S \to T$ zwischen zwei Halbgruppen heißt Homomorphismus, wenn*

$$f(x \cdot y) = f(x) \cdot f(y)$$

für alle $x, y \in S$.

Beispiele:

- Wenn G eine Gruppe ist, und $a \in G$, ist die Abbildung $n \mapsto a^n$ ein Homomorphismus von $\mathbb{Z}$ nach G.
- Die Signaturabbildung $\operatorname{sign} : \mathrm{S}_n \to \{1, -1\}$ auf den endlichen Permutationsgruppen
$$\mathrm{S}_n = \mathrm{Sym}\{1, \ldots, n\}$$

Die Elemente t des Bildes $f(S)$ entsprechen den Äquivalenzklassen $f^{-1}(t)$ der von f bestimmten *Faserung*

$$x \sim y \Longleftrightarrow f(x) = f(y).$$

Die Halbgruppenstruktur von $f(S)$ überträgt sich auf die Menge $S/\!\sim$ der Äquivalenzklassen durch

$$(x/\!\sim) \cdot (y/\!\sim) = (x \cdot y)/\!\sim. \tag{1.2}$$

Eine Äquivalenzrelation $\sim$ auf S, für die (1.2) eine Operation auf $S/\!\sim$ erklärt, heißt *Kongruenzrelation*. Die Bedingung bedeutet, daß die Äquivalenzklasse eines Produktes nur von den Äquivalenzklassen der Faktoren abhängt:

$$x \sim x',\ y \sim y' \Rightarrow x \cdot y \sim x' \cdot y'. \tag{1.3}$$

Wenn $\sim$ eine Kongruenzrelation ist, ist $S/\!\sim$ mit der induzierten Operation wieder eine Halbgruppe. Die Projektion $\pi\colon S \to S/\!\sim$ erfüllt nämlich die Homomorphismusbedingung und wir haben:

$$\begin{aligned}(\pi(a)\pi(b))\pi(c) = \pi(ab)\pi(c) &= \pi((ab)c) = \\ &= \pi(a(bc)) = \pi(a)\pi(bc) = \pi(a)(\pi(b)\pi(c)).\end{aligned}$$

Der folgende Satz sollte jetzt klar sein. Er gilt natürlich nicht nur für Halbgruppen, sondern für beliebige Strukturen mit einer zweistelligen Operation.

Satz 1.3.1 (Abstrakter Homomorphiesatz) *Sei $f : S \to T$ ein Homomorphismus zwischen Halbgruppen. Dann ist die Faserung $\sim$ von f eine Kongruenzrelation auf S und f induziert durch*

$$x/\!\sim \mapsto f(x)$$

einen Isomorphismus zwischen den Halbgruppen $S/\!\sim$ und $f(S)$.

Bevor wir die Kongruenzrelationen in Gruppen bestimmen, zeigen wir daß homomorphe Bilder von Gruppen wieder Gruppen sind.[3]

Lemma 1.3.2 *Sei $f : G \to T$ ein Homomorphismus einer Gruppe G in eine Halbgruppe T. Dann ist das Bild $f(G)$ eine Gruppe.*

Beweis :
$f(1)$ ist Einselement von $f(G)$, weil $f(1)f(g) = f(1g) = f(g)$. $f(g^{-1})$ ist invers zu $f(g)$, weil $f(g^{-1})f(g) = f(g^{-1}g) = f(1)$. □

Sei nun $\sim$ eine Kongruenzrelation der Gruppe G. Weil

$$x \sim y \Longleftrightarrow xy^{-1} \sim 1,$$

ist $\sim$ durch die Äquivalenzklasse $N = 1/\sim$ schon bestimmt. Weil

$$x \sim 1,\ y \sim 1 \Longrightarrow xy^{-1} \sim 1,$$

ist N eine Untergruppe und die $\sim$–Äquivalenzklassen sind gerade die Rechtsnebenklassen von N. Wenn man umgekehrt eine Untergruppe N vorgibt, dann ist die durch

$$x \sim y \Longleftrightarrow xy^{-1} \in N$$

definierte Äquivalenzrelation im allgemeinen keine Kongruenzrelation. Es gilt zwar

$$x \sim y \Longrightarrow Nx = Ny \Longrightarrow Nxz = Nyz \Longrightarrow xz \sim yz, \tag{1.4}$$

aber im allgemeinen nicht

$$x \sim y \Longrightarrow zx \sim zy. \tag{1.5}$$

Wenn $\sim$ eine Kongruenzrelation ist, sind aber die Äquivalenzklassen auch ebensogut *Linksnebenklassen* von N. Diese Bedingung an N, nämlich, daß

$$Ng = gN$$

für alle g, impliziert die Gleichung (1.5). Untergruppen, deren Rechtsnebenklassen auch Linksnebenklassen sind, heißen *Normalteiler*:

Definition *Eine Untergruppe N von G heißt Normalteiler, wenn*

$$g^{-1}Ng = N$$

für alle $g \in G$.

Notation $N \lhd G$

In abelschen Gruppen sind alle Untergruppen Normalteiler. Unsere bisherigen Überlegungen zeigen:

Satz 1.3.3 (Homomorphiesatz) *Sei G eine Gruppe.*

[3] Das Lemma erscheint implizit schon am Endes des Beweises von 1.1.4.

1. *Wenn N ein Normalteiler von G ist, wird durch*

$$(Ng) \cdot (Nh) = N(gh)$$

eine Gruppenoperation auf G/N definiert. Die Projektion

$$\pi : G \to G/N$$

ist ein Homomorphismus.

2. *Sei $f : G \to H$ ein Homomorphismus und*

$$N = \ker(f) = \{g \in G \mid f(g) = 1\}$$

der Kern *von f. Dann ist N ein Normalteiler und*

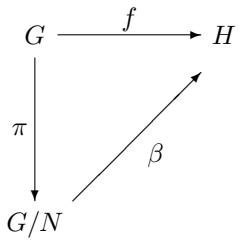
$$Ng \mapsto f(g)$$

definiert einen Isomorphismus zwischen G/N und $f(G)$.

□

Eine diagrammatische Variante:

Satz 1.3.4 *Sei $f : G \to H$ ein Homomorphismus. N sei ein Normalteiler von G, der von f auf das Einselement von H abgebildet wird. Dann gibt es einen (eindeutig bestimmten) Homomorphismus $\beta : G/N \to H$, der das Diagramm*



kommutativ macht.

Beweis :
Weil

$$\pi(g) = \pi(h) \Rightarrow gh^{-1} \in N \Rightarrow gh^{-1} \in \ker(f) \Rightarrow f(g) = f(h),$$

gibt es ein eindeutig bestimmtes β, das das Diagramm kommutativ macht. Daß β ein Homomorphismus ist, ist trivial:

$$\beta(\pi(g)\pi(h)) = \beta(\pi(gh)) = f(gh) = f(g)f(h) = \beta(\pi(g))\beta(\pi(h)).$$

□

Wenn m die Ordnung von a ist, ist $m\mathbb{Z}$ der Kern des Homomorphismus $\mathbb{Z} \to G$, der 1 auf a abbildet. Es folgt, daß $\langle a \rangle \cong \mathbb{Z}/m\mathbb{Z}$. Wir nennen

$$\mathrm{Z}_m = \mathbb{Z}/m\mathbb{Z}$$

die *zyklische* Gruppe der Ordnung m. In den Fällen $m = 0, 1$ pflegt man sich anders auszudrücken: $\mathbb{Z} = \mathrm{Z}_0$ heißt die *unendliche* zyklische Gruppe. Die Gruppe Z_1 besteht nur aus dem neutralen Element und heißt die *triviale* Gruppe. Für die triviale Gruppe schreibt man multiplikativ 1 und additiv 0.

Ein surjektiver Homomorphismus $f : G \to H$ vermittelt vermöge $U = f^{-1}(V)$ eine Bijektion zwischen den Untergruppen V von H und den Untergruppen U von G, die den Kern von f enthalten. V ist genau dann ein Normalteiler von H, wenn U Normalteiler von G ist. In diesem Fall ist U der Kern des zusammengesetzten Homomorphismus $G \xrightarrow{f} H \to H/V$ und wir erhalten einen Isomorphismus zwischen G/U und H/V. Im Fall $H = G/N$ erhalten wir für Normalteiler U, die N enthalten:

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

Die Untergruppen von Z_m entsprechen demgemäß, vermöge der Projektion $\mathbb{Z} \to \mathrm{Z}_m$, gerade denjenigen Untergruppen $d\mathbb{Z}$ von $\mathbb{Z}$, die $m\mathbb{Z}$ enthalten, das heißt, für die d ein Teiler von m ist. Es folgt, daß eine zyklische Gruppe der Ordnung m für jeden Teiler d von m genau eine Untergruppe vom Index d hat. Wenn $m = p^e$ Potenz einer Primzahl ist, bilden die Untergruppen von Z_m eine Kette mit den Ordnungen $1, p, \ldots, p^e$.

1.4 Der Satz von Jordan–Hölder

Das *Komplexprodukt* zweier Teilmengen A und B einer Gruppe ist die Menge

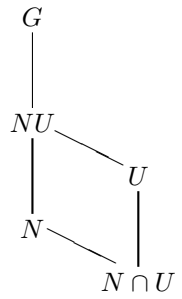
$$AB = \{ab \mid a \in A\,, b \in B\}.$$

Wenn A ein Normalteiler ist und B eine Untergruppe, ist AB eine Untergruppe. Das folgt aus dem Beweis des nächsten Satzes.

Satz 1.4.1 (Noetherscher[4]Isomorphiesatz) *Sei N ein Normalteiler und U eine Untergruppe von G. Dann ist $N \cap U$ ein Normalteiler von U, NU eine Untergruppe von G und es gibt einen natürlichen Isomorphismus*

$$U/(N \cap U) \cong NU/N.$$

Beweis :
Sei $\pi : G \to G/N$ die natürliche Projektion. Dann ist $NU = \pi^{-1}(\pi(U))$ Untergruppe von G.



Die beiden Einschränkungen $f : U \to G/N$ und $g : NU \to G/N$ haben das gleiche Bild H. Der Kern von f ist $N \cap U$, der Kern von g ist N. Also ist

$$U/(N \cap U) \cong H \cong NU/N.$$

□

Man überlegt sich leicht, daß N kein Normalteiler in G sein muß, es genügt vielmehr, zu fordern, daß N von U *normalisiert* wird. Das heißt, daß $u^{-1}Nu = N$ für alle $u \in U$. Dann ist nämlich NU eine Untergruppe von G und N Normalteiler von NU.

Eine *Normalreihe* $\mathcal{N}$ von G ist eine Kette

$$1 = N_0 \lhd N_1 \lhd \ldots \lhd N_{n-1} \lhd N_n = G.$$

Eine Normalreihe $\mathcal{N}'$ *verfeinert* $\mathcal{N}$, wenn $\mathcal{N} \subset \mathcal{N}'$. Eine *Kompositionsreihe* von G ist eine echt aufsteigende Normalreihe, die keine echten Verfeinerungen hat.

Eine nicht–triviale Gruppe G, die nur die trivialen Normalteiler 1 und G hat, heißt *einfach*.

[4]Amalie Emmy Noether (1882-1935)

Beispiel:
Die einfachen abelschen Gruppen sind die zyklischen Gruppen Z_p von Primzahlordnung.

Lemma 1.4.2 *Eine Normalreihe* $1 = N_0 \lhd N_1 \lhd \ldots \lhd N_{n-1} \lhd N_n = G$ *ist genau dann ein Kompositionsreihe, wenn die* Kompositionsfaktoren N_{i+1}/N_i *einfach sind.*

Beweis :
Die Normalteiler von N_{i+1}/N_i entsprechen den Normalteilern von N_{i+1}, die N_i enthalten. □

Endliche Gruppen haben immer Kompositionsreihen. Im allgemeinen brauchen sie aber nicht zu existieren. Unendliche abelsche Gruppen zum Beispiel haben keine Kompositionsreihen.

Zwei Normalreihen $M_0 \lhd M_1 \lhd \ldots \lhd M_{n-1} \lhd M_n$ und $N_0 \lhd N_1 \lhd \ldots \lhd N_{n-1} \lhd N_n$ heißen *isomorph*, wenn sie die gleiche Länge haben und wenn bis auf eine Permutation π der Indizes $\{0, \ldots, n-1\}$ die Quotienten isomorph sind, wenn also $M_{i+1}/M_i \cong N_{\pi(i)+1}/N_{\pi(i)}$.

Satz 1.4.3 (Jordan–Hölder[5]) *Alle Kompositionsreihen einer Gruppe G sind isomorph.*

Beweis :
Wir zeigen etwas mehr: Wenn $\mathcal{M}$ eine Kompositionsreihe von G ist und $\mathcal{N}$ eine echt aufsteigende Normalreihe, dann hat $\mathcal{N}$ eine zu $\mathcal{M}$ isomorphe Verfeinerung.

Wir verwenden Induktion über die Länge von $\mathcal{M}$. Wir können annehmen, daß weder $\mathcal{M}$ noch $\mathcal{N}$ die Länge 0 haben. $\mathcal{N}'$ und $\mathcal{M}'$ seien die beiden Reihen ohne G, M und N die letzten Glieder von $\mathcal{N}'$ und $\mathcal{M}'$.

Wir unterscheiden drei Fälle. Wenn $N = M$, hat nach Induktionsvoraussetzung $\mathcal{N}'$ eine zu $\mathcal{M}'$ isomorphe Verfeinerung $\mathcal{N}''$. $\mathcal{N}'' \cup \{G\}$ ist isomorph zu $\mathcal{M}$.

Wenn N eine echte Untergruppe von M ist, hat nach Induktionsvoraussetzung $\mathcal{N}' \cup \{M\}$ eine zu $\mathcal{M}'$ isomorphe Verfeinerung $\mathcal{N}''$. $\mathcal{N}'' \cup \{G\}$ ist isomorph zu $\mathcal{M}$ und eine Verfeinerung von $\mathcal{N}$.

Wenn N nicht in M enthalten ist, ist $G = MN$. Aus Satz 1.4.1 folgt, daß $G/M \cong N/(M \cap N)$ und $G/N \cong M/(M \cap N)$. Nach Induktionsvoraussetzung hat die Reihe[6] $\{1, M \cap N, M\}$ eine zu $\mathcal{M}'$ isomorphe Verfeinerung $\mathcal{K} \cup \mathcal{K}'$. Wir notieren hier die Reihe zwischen 1 und $M \cap N$ als $\mathcal{K}$ und die Reihe zwischen $M \cap N$ und M als $\mathcal{K}'$. Weil $G/N \cong M/(M \cap N)$, finden wir zwischen N und G eine Normalreihe $\mathcal{K}''$, die zu $\mathcal{K}'$ isomorph ist.

Weil $N/(M \cap N)$ einfach ist, ist $\mathcal{K}' \cup \{N\}$ eine Kompositionsreihe von N, die kürzer als $\mathcal{M}$ ist. $\mathcal{N}'$ hat also eine zu $\mathcal{K}' \cup \{N\}$ isomorphe Verfeinerung $\mathcal{N}''$.

[5] Marie Ennemond Camille Jordan (1838-1922), Ludwig Otto Hölder (1859-1937)
[6] Hier ist $1 = M \cap N$ möglich.

$\mathcal{N}'' \cup \mathcal{K}''$ ist eine zu $\mathcal{M}$ isomorphe Verfeinerung von $\mathcal{N}$. □

Der folgende Satz ist eine Verallgemeinerung von 1.4.3, der auch etwas für den Fall aussagt, daß G keine Kompositionsreihe hat.

Satz 1.4.4 (Verfeinerungssatz von Schreier) [7,8] *Zwei Normalreihen einer Gruppe besitzen isomorphe Verfeinerungen.*

Beweis :
Seien

$$\mathcal{M} = (1 = M_0 \lhd \ldots \lhd M_m = G)$$

und

$$\mathcal{N} = (1 = N_0 \lhd \ldots \lhd N_n = G)$$

zwei Normalreihen. Wir verfeinern $\mathcal{M}$ zu $\mathcal{M}'$, indem wir zwischen M_i und M_{i+1} jeweils die Reihe

$$M_i = M_i(M_{i+1} \cap N_0) \subset M_i(M_{i+1} \cap N_1) \subset \ldots \subset M_i(M_{i+1} \cap N_n) = M_{i+1}$$

einfügen. Zwischen N_j und N_{j+1} fügen wir

$$N_j = (M_0 \cap N_{j+1})N_j \subset (M_1 \cap N_{j+1})N_j \subset \ldots \subset (M_m \cap N_{j+1})N_j = N_{j+1}$$

ein und erhalten die Verfeinerung $\mathcal{N}'$. Daß $\mathcal{M}'$ und $\mathcal{N}'$ isomorphe Normalreihen sind, folgt aus dem nächsten Lemma, das wir auf $A_1 = M_i$, $A_2 = M_{i+1}$, $B_1 = N_j$ und $B_2 = N_{j+1}$ anwenden.

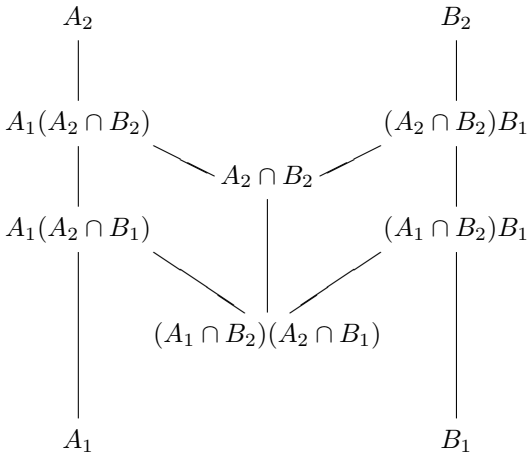
Lemma 1.4.5 (Lemma von Zassenhaus)[8] *Wenn $A_1 \lhd A_2$ und $B_1 \lhd B_2$ Untergruppen von G sind, ist $A_1(A_2 \cap B_1)$ Normalteiler in $A_1(A_2 \cap B_2)$, $(A_1 \cap B_2)B_1$ Normalteiler in $(A_2 \cap B_2)B_1$ und es ist*

$$A_1(A_2 \cap B_2)/A_1(A_2 \cap B_1) \cong (A_2 \cap B_2)B_1/(A_1 \cap B_2)B_1.$$

Beweis :
Weil $A_1 \lhd A_2$ ist $A_1(A_2 \cap B_2)$ eine Untergruppe. $A_2 \cap B_2$ normalisiert A_1, A_2 und B_1 und also auch $A_1(A_2 \cap B_1)$. Daraus folgt, daß $A_1(A_2 \cap B_1)$ ein Normalteiler von $A_1(A_2 \cap B_2)$ ist. Mit Hilfe des Modulargesetzes, das wir gleich erläutern, sehen wir, daß

$$A_1(A_2 \cap B_1) \cap (A_2 \cap B_2) = (A_1 \cap B_2)(A_2 \cap B_1).$$

[7] Otto Schreier (1901-1929)
[8] Nur SS 1995



Aus 1.4.1 folgt

$$A_1(A_2 \cap B_2)/A_1(A_2 \cap B_1) \cong (A_2 \cap B_2)/(A_1 \cap B_2)(A_2 \cap B_1).$$

Rechts steht aber ein in A, B symmetrischer Ausdruck, und wir erhalten

$$(A_2 \cap B_2)/(A_1 \cap B_2)(A_2 \cap B_1) \cong (A_2 \cap B_2)B_1/(A_1 \cap B_2)B_1.$$

□

Wenn A und $B \leq C$ Untergruppen von G sind, ist, wie man leicht nachrechnet

$$(AB) \cap C = (A \cap C)B.$$

Das ist das *Modulargesetz*. Die Normalteiler einer Gruppe bilden (ebenso wie die Untergruppen) einen Verband. Für Normalteiler ist AB das Supremum von A und B, $A \cap B$ das Infimum. Das Modulargesetz drückt gerade aus, daß der Verband der Normalteiler *modular* ist.

1.5 Innere Automorphismen

Definition *Sei G eine Gruppe und $a \in G$. Man konjugiert x mit a, indem man von x zu*

$$x^a = a^{-1}xa$$

übergeht. Die Abbildung

$$\tau_a(x) = x^a$$

heißt der durch a bestimmte innere Automorphismus von G.

Eine Untergruppe ist also genau dann Normalteiler, wenn sie unter allen inneren Automorphismen invariant bleibt.

Man verifiziert leicht, daß τ_a tatsächlich ein *Automorphismus* von G ist, das heißt ein Isomorphismus von G mit sich selbst. Außerdem gelten die Rechenregeln

$$\begin{aligned} x^1 &= x \\ x^{ab} &= (x^a)^b \end{aligned}$$

Die Gültigkeit dieser beiden Regeln bedeutet, daß G per Konjugation auf sich selbst *operiert*. Dabei operiert G (von rechts) auf einer Menge X, wenn eine Abbildung

$$\cdot : X \times G \to X$$

gegeben ist, die den Regeln

$$\begin{aligned} x \cdot 1 &= x \\ x \cdot (ab) &= (x \cdot a) \cdot b \end{aligned}$$

genügt. X wird durch die Operation in *Bahnen* (orbits)

$$x \cdot G = \{x \cdot a \mid a \in G\}$$

partitioniert. Die Abbildung $g \mapsto xg$ bildet G auf die Bahn von x ab. g und h werden auf dasselbe Element abgebildet, wenn $x \cdot (gh^{-1}) = x$, wenn also g und h in derselben Rechtsnebenklasse der *Stabilisatorgruppe*

$$\mathrm{Stab}(x) = \{a \in G \mid x \cdot a = x\}$$

liegen. Es folgt

$$|x \cdot G| = (G : \mathrm{Stab}(x)). \tag{1.6}$$

Die Bahnen der Konjugationsoperation von G heißen *Konjugationsklassen*. Der Stabilisator

$$\mathrm{C}_G(x) = \{a \in G \mid x^a = x\}$$

heißt *Zentralisator* von x. Die Konjugationsklasse von g besteht genau dann aus einem Element, wenn g von allen inneren Automorphismen fixiert wird, oder anders gesagt, wenn g zum *Zentrum* von G gehört.

Definition *Das Zentrum* $\mathrm{Z}(G)$ *einer Gruppe* G *ist die Untergruppe aller* g*, die mit allen* $a \in G$ *vertauschen.*

$\mathrm{Z}(G)$ ist eine abelsche Untergruppe von G, die unter allen Automorphismen von G invariant bleibt. Insbesondere ist $\mathrm{Z}(G)$ ein Normalteiler in G.

Satz 1.5.1 (Klassengleichung) *Sei* G *eine Gruppe und* $(a_i)_{i \in I}$ *ein Repräsentantensystem der Konjugationsklassen von nicht–zentralen Elementen. Dann ist*

$$|G| = |\mathrm{Z}(G)| + \sum_{i \in I} (G : C_G(a_i)).$$

Beweis :
Folgt sofort aus (1.6). □

1.6 Direkte Produkte

Definition *Das direkte Produkt der beiden Gruppen G und H ist das kartesische Produkt*

$$G \times H$$

mit komponentenweiser Multiplikation

$$(g, h) \cdot (g', h') = (g \cdot g', h \cdot h').$$

Man rechnet sofort nach, daß $G \times H$ eine Gruppe ist. $(1, 1)$ ist das Einselement und (g^{-1}, h^{-1}) das Inverse von (g, h). Die beiden Faktoren G und H sind in der Form $G \times 1$ und $1 \times H$ Untergruppen von $G \times H$, und $G \times H$ ist *inneres* direktes Produkt dieser Untergruppen im folgenden Sinn:

Definition *K ist inneres direktes Produkt der Untergruppen G und H, wenn*

a) sich jedes Element von K eindeutig als ein Produkt gh mit $g \in G,\ h \in H$ schreiben läßt,

b) und wenn die Elemente von G und H kommutieren:

$$gh = hg, \quad (g \in G,\ h \in H).$$

Wenn K inneres direktes Produkt von G und H ist, liefert $(g, h) \mapsto gh$ einen Isomorphismus zwischen $G \times H$ und K.

Lemma 1.6.1 *K ist genau dann inneres direktes Produkt der Untergruppen G und H, wenn*

a) $GH = K$,

b) $G \cap H = 1$,

c) $gh = hg, \quad (g \in G,\ h \in H)$.

Die letzte Bedingung kann man ersetzen durch die Forderung, daß G und H Normalteiler in K sind.

Beweis :
Wenn K inneres direktes Produkt von G und H ist, ist K isomorph zum direkten Produkt von G und H und man verifiziert leicht die drei Bedingungen. G und H sind als Kerne der Projektionshomomorphismen von $G \times H$ auf H und G Normalteiler.
Wenn umgekehrt die drei Bedingungen erfüllt sind, ist nur noch zu zeigen, daß die Darstellung $k = gh$ eindeutig ist. Das folgt aber aus (b).

Wenn G und H Normalteiler von K sind, betrachtet man den *Kommutator*

$$[g, h] = g^{-1}h^{-1}gh$$

zweier Elemente $g \in G$ und $h \in H$. Weil G Normalteiler ist, gehört $[g,h]$ zu G, und weil H Normalteiler ist, zu H. Also folgt aus (b), daß $[g,h] = 1$, was äquivalent ist zu $gh = hg$. □

Im Fall additiv geschriebener abelscher Gruppen schreibt man häufig

$$G \oplus H$$

statt $G \times H$.

Als ein Beispiel zeigen wir:

Lemma 1.6.2 *Wenn m und n teilerfremd sind, ist*

$$\mathrm{Z}_{mn} \cong \mathrm{Z}_m \oplus \mathrm{Z}_n.$$

Beweis :
Die zwei Projektionen von $\mathbb{Z}$ nach Z_m und Z_n setzen sich zu einem Homomorphismus

$$f : \mathbb{Z} \to \mathrm{Z}_m \oplus \mathrm{Z}_n$$

zusammen. Der Kern dieser Abbildung ist

$$m\mathbb{Z} \cap n\mathbb{Z} = mn\mathbb{Z}.$$

Das Bild ist also isomorph zu Z_{mn} und muß (aus Anzahlgründen) gleich $\mathrm{Z}_m \oplus \mathrm{Z}_n$ sein. □

Folgerung 1.6.3 *Wenn $m = p_1^{e_1} \cdots p_n^{e_n}$ die Primfaktorzerlegung von m ist, ist*

$$\mathrm{Z}_m \cong \mathrm{Z}_{p_1^{e_1}} \oplus \cdots \oplus \mathrm{Z}_{p_n^{e_n}}.$$

Das kartesische Produkt $\prod_{i\in I} G_i$ einer Familie von Gruppen ist mit komponentenweiser Multiplikation

$$(f \cdot g)_i = f_i \cdot g_i$$

wieder eine Gruppe. Für additiv geschriebene abelsche Gruppen betrachtet man noch die direkte Summe

$$\bigoplus_{i\in I} G_i = \Big\{ f \in \prod_{i\in I} G_i \;\Big|\; f_i = 0 \text{ für fast alle } i \Big\}.$$

$\bigoplus_{i\in I} G_i$ ist *innere direkte Summe* der isomorphen Kopien $G'_j = \big\{ f \in \bigoplus_{i\in I} G_i \;\big|\; f_i = 0 \text{ für alle } i \neq j \big\}$. Das heißt (für abelsche Gruppen), daß sich jedes Element von $\bigoplus_{i\in I} G_i$ eindeutig als eine Summe von Elementen der G'_i schreiben läßt.

1.7 Abelsche Gruppen

Definition *Ein Gruppe heißt Torsionsgruppe, wenn jedes Element endliche Ordnung hat. Eine Gruppe heißt p–Gruppe (für eine Primzahl p), wenn die Ordnung jedes Elements eine Potenz von p ist.*

In einer abelschen Gruppe G teilt die Ordnung von $a-b$ das kleinste gemeinschaftliche Vielfache der Ordnungen von a und b. Es folgt, daß $\mathrm{T}(M)$, die Menge aller Elemente endlicher Ordnung, und $\mathrm{T}_p(M)$, die Menge aller Elemente, deren Ordnung eine p–Potenz ist, Untergruppen sind: die *Torsionsuntergruppe* und die *p–Torsionsuntergruppe* von G.

Lemma 1.7.1 *Jede abelsche Torsionsgruppe ist direkte Summe von p–Gruppen.*

Beweis :
Sei G eine abelsche Torsionsgruppe. Wir zeigen, daß G die innere direkte Summe der p–Torsionsuntergruppen $\mathrm{T}_p(G)$ ist. Sei m die Ordnung von $a \in G$. Weil $\langle a\rangle \cong \mathrm{Z}_m$, ist nach (1.6.3) a Summe von Elementen, deren Ordnung eine Primzahlpotenz ist. Wir haben nur noch zu zeigen, daß eine solche Zerlegung eindeutig ist. Sei dazu $b_1 + \cdots + b_n = 0$, $b_i \in \mathrm{T}_{p_i}$ und die Primzahlen $p_1, \ldots, p_n$ paarweise verschieden. Dann ist aber $b_1 = -(b_2 + \cdots + b_n)$ und die Ordnung von b_1 daher ein Teiler des Produktes der Ordnungen der $b_2, \ldots, b_n$. Das ist nur möglich, wenn $b_1 = 0$. Es folgt, daß alle b_i gleich Null sein müssen. □

Lemma 1.7.2 *Jede abelsche p–Gruppe von endlichem Exponenten*[9] *ist direkte Summe von zyklischen Gruppen.*

Beweis :
Sei G vom Exponenten p^e, also $p^eG = 0$. Wir zeigen das Lemma zuerst für den Fall $e = 1$: Dann hängt na nur von $n \pmod p$ ab. Durch die skalare Multiplikation $(n + p\mathbb{Z})a = na$ wird G daher zu einem $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$–Vektorraum. Wenn $(a_i)_{i\in I}$ eine $\mathbb{F}_p$–Basis von G ist, ist

$$G = \bigoplus_{i\in I} \mathbb{F}_p a_i.$$

Nun zum allgemeinen Fall. Wir nennen den $\mathbb{F}_p$–Vektorraum

$$S = \{a \in G \mid pa = 0\}$$

der Elemente vom Exponenten p den *Sockel* von G. Die Unterräume $S^i = S \cap (p^iG)$ der Elemente des Sockels, die (in G) durch p^i teilbar sind, bilden eine Kette von Unterräumen:

$$0 = S^e \subset S^{e-1} \subset \ldots \subset S^1 \subset S^0 = S.$$

Wir wählen für jedes $i < e$ ein Basis $(s^i_j)_{j\in J_i}$ von S^i modulo S^{i+1}. Insgesamt bilden die s^i_j eine Basis des Sockels. Jetzt wählen wir für jedes s^i_j ein g^i_j mit

[9] n ist Exponent von G, wenn $g^n = 1$ für alle $g \in G$.

$p^i g_j^i = s_j^i$. Sei $G_j^i = \langle g_j^i \rangle$ die von g_j^i erzeugte zyklische Untergruppe (der Ordnung p^{i+1}). Wir werden zeigen, daß G die direkte Summe der G_j^i ist.

Sei H die Summe der G_j^i. Weil die s_j^i zu H gehören, enthält H den Sockel. Wir zeigen, daß alle a in H liegen, durch Induktion über die Ordnung von a. Nehmen wir an, daß $\mathrm{ord}(a) = p^{m+1}$ und daß die Behauptung schon für alle Elemente kleinerer Ordnung gezeigt ist. $p^m a$ liegt in S^m und ist daher eine Linearkombination von s_j^i mit $i \geq m$. Weil diese s_j^i in H durch p^m teilbar sind, ist auch $p^m a$ in H durch p^m teilbar. Es gibt also ein $h \in H$ mit $p^m h = p^m a$. $h - a$ hat höchstens die Ordnung p^m und liegt in H, also liegt auch a in H.

Schließlich müssen wir noch die Direktheit der Summe zeigen. Sei dazu (c_j^i) eine Familie von Elementen der G_j^i, die nicht alle Null sind. Sei p^{m+1} die größte Ordnung der c_j^i. Die $p^m c_j^i$ liegen dann in S und sind nicht alle Null. Nun ist aber die Summe der $S \cap G_j^i = \mathbb{F}_p s_j^i$ direkt und daher $\sum p^m c_j^i \neq 0$, woraus $\sum c_j^i \neq 0$ folgt. □

Aus den beiden Lemmas folgt:

Satz 1.7.3 (Hauptsatz über endliche abelsche Gruppen) *Jede endliche abelsche Gruppe (oder allgemeiner: jede abelsche Gruppe von endlichem Exponenten) ist direkte Summe von zyklischen Gruppen von Primpotenzordnung. Die Summanden sind bis auf Isomorphie und Reihenfolge eindeutig bestimmt.*

Beweis :
Nur die Eindeutigkeit ist noch zu zeigen: Sei

$$G = \bigoplus_{p,e} (\mathrm{Z}_{p^e})^{n_{p,e}} .$$

Für eine Primzahl p sei $G[p] = \{a \in G \mid pa = 0\}$ der p-Sockel von G. Man überlegt, daß

$$G[p] = \bigoplus_{e} \left(p^{e-1}\mathrm{Z}_{p^e}\right)^{n_{p,e}}$$

und für alle e

$$(p^e G)[p] = \bigoplus_{i>e} \left(p^{i-1}\mathrm{Z}_{p^i}\right)^{n_{p,i}} .$$

Es ist also

$$n_{p,e} = \dim_{\mathbb{F}_p} (p^{e-1}G)[p]/(p^e G)[p].$$

□

Definition *Eine Gruppe ohne Elemente endlicher Ordnung heißt torsionsfrei.*

Wir werden zeigen:

Satz 1.7.4 *Endlich erzeugte torsionsfreie abelsche Gruppen sind direkte Summen von Kopien von $\mathbb{Z}$. Die Zahl der Summanden ist eindeutig bestimmt.*

Sei $F = \bigoplus_{i \in I} \mathbb{Z}$ direkte Summe von Kopien von $\mathbb{Z}$. Sei e_i das Einselement der i-ten Kopie von $\mathbb{Z}$. Dann wird F (als abelsche Gruppe) von den e_i in folgendem Sinn *frei* erzeugt:

Für alle abelschen Gruppen A und für jede Familie $(a_i)_{i \in I}$ von Elementen von A gibt es genau einen Homomorphismus $f : F \to A$, der für alle $i \in I$ e_i auf a_i abbildet.

Man zeigt leicht, daß diese Eigenschaft F bis auf Isomorphie eindeutig bestimmt. Freie Gruppen sind *projektiv*:

Wenn A/B frei ist, ist B direkter Summand von A.

Beweis :
Wenn A/B von den $a_i + B$ $(i \in I)$ frei erzeugt wird, gibt es einen Homomorphismus $f : A/B \to A$ mit $f(a_i + B) = a_i$, also $\pi(f(a_i + B)) = a_i + B$ für die Projektion $\pi : A \to A/B$. Es gilt dann $\pi(f(x)) = x$ für alle $x \in A/B$. Sei C das Bild von f. Dann ist $A = B \oplus C$. (Existenz: $a = (a - f(\pi(a))) + f(\pi(a))$, Eindeutigkeit: $\pi(f(x) + b) = x$) □

Nicht alle torsionsfreien abelschen Gruppen sind frei, $\mathbb{Q}$, die additive Gruppe der rationalen Zahlen, ist das einfachste Gegenbeispiel. Wir beginnen den Beweis von (1.7.4) mit dem Nachweis, daß endlich erzeugte Untergruppen G von $\mathbb{Q}$ zyklisch sind: Wenn $g_1, \ldots, g_n$ die Erzeugenden von G sind, wählen wir eine ganze Zahl $N \neq 0$, sodaß alle Ng_i zu $\mathbb{Z}$ gehören. Die Gruppe NG ist zu G isomorph und als Untergruppe von $\mathbb{Z}$ zyklisch.

Sei G torsionsfrei und von $g_0, \ldots, g_n$ erzeugt. Sei $r = \frac{a}{b} \in \mathbb{Q}$. Für Elemente x, y von G schreiben wir

$$rx = y,$$

wenn $ax = by$. Weil G torsionsfrei ist, ist y durch x und r eindeutig bestimmt. Betrachte die Untergruppe

$$H = \{g \mid g = rg_0 \text{ für ein } r \in \mathbb{Q}\}.$$

Weil $ax \in H \Rightarrow x \in H$ für alle $a \neq 0$, ist G/H torsionsfrei. G/H wird von den Nebenklassen von $g_1, \ldots, g_n$ erzeugt, also können wir (Induktion!) annehmen, daß G/H frei ist, und $G = C \oplus H$ für eine isomorphe Kopie C von G/H. Wir sind fertig, wenn wir zeigen können, daß H zyklisch ist. Weil H als direkter Summand homomorphes Bild von G ist, ist H endlich erzeugt. H ist aber per $rg_0 \mapsto r$ isomorph zu einer Untergruppe von $\mathbb{Q}$, ist also zyklisch.

Wir zeigen noch, daß die Zahl der zyklischen Summanden eindeutig bestimmt ist: Wenn $G = \bigoplus_{i=1}^{n} \mathbb{Z}$, ist n die Dimension des $\mathbb{F}_p$–Vektorraums $G/(pG)$. □

Folgerung 1.7.5 *Endlich erzeugte abelsche Gruppen sind direkte Summen von zyklischen Gruppen.*

Beweis :
Sei G endlich erzeugt. Weil $G/\mathrm{T}(G)$ torsionsfrei, endlich erzeugt und daher projektiv ist, ist $G = C \oplus \mathrm{T}(G)$. Jetzt wendet man (1.7.4) und (1.7.3) auf C und $\mathrm{T}(G)$ an. □

1.8 Sylowgruppen

Wir halten in diesem Abschnitt eine Primzahl p fest.

Lemma 1.8.1 (Cauchy[10]) *Sei G eine endliche Gruppe und p ein Teiler der Ordnung von G. Dann hat G ein Element der Ordnung p.*

Beweis :
Aus der Klassengleichung (1.5.1) folgt, daß die Ordnung des Zentrums Z durch p teilbar ist, oder daß es ein nicht–zentrales Element a geben muß, für das $(G : \mathrm{C}_G(a))$ nicht durch p teilbar ist. Im ersten Fall folgt aus (1.7.3)[11], daß Z ein Element der Ordnung p hat. Im zweiten Fall ist $C_G(a)$ eine echte Untergruppe von G, deren Ordnung immer noch durch p teilbar ist und die daher (per Induktion!) ein Element der Ordnung p hat. □

Als Folgerung erhält man, daß die Ordnung endlicher p–Gruppen eine p–Potenz ist.

Definition *Sei G endlich und p^e die größte Potenz von p, die die Ordnung von G teilt. Eine p–Sylowgruppe von G ist eine Untergruppe der Ordnung p^e.*

Endliche abelsche Gruppen besitzen (jeweils eindeutig bestimmte) p–Sylowgruppen nach (1.7.1).

Satz 1.8.2 *In endlichen Gruppen gibt es immer p–Sylowgruppen.*

Beweis :
Sei G eine endliche Gruppe. Wir beweisen den Satz durch Induktion nach der Ordnung von G. Wenn p die Ordnung von G nicht teilt, ist 1 p–Sylowgruppe. Nehmen wir also an, daß p die Ordnung von G teilt. Wenn p auch die Ordnung des Zentrums teilt, gibt es eine zentrale Untergruppe A der Ordnung p. Nach Induktionsvoraussetzung hat G/A eine p–Sylowgruppe S/A. S ist dann p–Sylowgruppe von G. Wenn p die Ordnung des Zentrums nicht teilt, gibt es nach der Klassengleichung eine echte Untergruppe C, deren Index nicht durch p teilbar ist. C hat nach Induktionsvoraussetzung eine p–Sylowgruppe S. S ist auch p–Sylowgruppe von G. □

Satz 1.8.3 *Sei G endlich. Dann ist jede p–Untergruppe in einer p–Sylowgruppe enthalten und alle p–Sylowgruppen von G sind konjugiert.*

Beweis :
Sei U eine p–Untergruppe und S eine zunächst beliebige Untergruppe. Wir lassen U auf der Menge (G/S) der Rechtsnebenklassen von S vermöge

$$(Sg) \cdot u = Sgu$$

[10] Augustin Louis Cauchy (1789-1857)
[11] Man braucht eigentlich nur (1.7.1)

operieren. Eine Bahn SgU besteht genau dann aus genau einem Element Sg, wenn

$$S(gUg^{-1}) = S \Longleftrightarrow gUg^{-1} \leq S \Longleftrightarrow U \leq g^{-1}Sg.$$

Weil jede Bahn p–Potenz–viele Elemente hat, ist die Zahl dieser Nebenklassen Sg zum Index $(G : S)$ modulo p kongruent. Wenn S eine p–Sylowgruppe ist, ist $(G : S)$ nicht durch p teilbar. Es muß also ein g mit $U \leq g^{-1}Sg$ geben. □

Wenn wir die letzte Überlegung auf $S = U$ anwenden, erhalten wir

$$(\mathrm{N}_G(U) : U) \equiv (G : U) \pmod{p}. \tag{1.7}$$

Dabei ist $\mathrm{N}_G(U) = \{g \in G \mid U = g^{-1}Ug\}$ der *Normalisator* von U in G.

Wenn U keine Sylowgruppe ist, schließt man daraus, daß $(\mathrm{N}_G(U) : U)$ durch p teilbar ist. Nach (1.8.1) muß es ein Element $a \in \mathrm{N}_G(U)$ geben, das modulo U die Ordnung p hat. $\langle U, a\rangle$ ist dann eine p–Gruppe, die U echt erweitert. Wir haben also einen alternativen Beweis für die Existenz von Sylowgruppen.

Wenn U eine Sylowgruppe ist, schließt man aus (1.7)

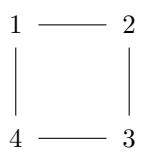
$$\text{Zahl der } p\text{–Sylowgruppen} = (G : \mathrm{N}_G(U)) \equiv 1 \pmod{p}.$$

Folgerung 1.8.4 *Der Normalisator einer p–Sylowgruppe S einer endlichen Gruppe G ist* selbstnormalisierend. *Das heißt*

$$\mathrm{N}_G(\mathrm{N}_G(S)) = \mathrm{N}_G(S)$$

Beweis :
S ist die einzige p–Sylowgruppe in $\mathrm{N}_G(S)$. Daher muß S unter allen Automorphismen von $\mathrm{N}_G(S)$ invariant bleiben. Wenn $a \in \mathrm{N}_G(\mathrm{N}_G(S))$, läßt der innere Automorphismus τ_a also S invariant und es folgt $a \in \mathrm{N}_G(S)$. □

Beispiel:
Wir wollen die 2–Sylowgruppen der S_4 bestimmen. S_4 hat triviales Zentrum. Also muß es eine Konjugationsklasse geben, die mehr als eins, aber ungerade viele Elemente enthält. Das ist die Konjugationsklasse der Produkte von disjunkten Transpositionen $\{(12)(34), (13)(24), (14)(23)\}$. Der Index des Zentralisators $\mathrm{C}((13)(24))$ ist die Zahl der Elemente, also drei. Es folgt, daß $S = \mathrm{C}((13)(24))$ die Ordnung acht hat. S ist die *Diedergruppe*[12] D_8, die Gruppe der Automorphismen des Quadrats



Die anderen 2–Sylowgruppen sind die Konjugierten $\mathrm{C}((12)(34))$ und $\mathrm{C}((14)(23))$.

[12]Die Diedergruppe D_{2n} ist die Automorphismengruppe des n–Ecks

1.9 Nilpotente Gruppen

Definition *Eine Gruppe G heißt nilpotent, wenn es eine* Zentralreihe *gibt. Das ist eine Folge von Normalteilern*

$$1 = N_0 \leq \ldots \leq N_n = G,$$

für die jeweils N_{i+1}/N_i im Zentrum von G/N_i liegt.

Abelsche Gruppen sind trivialerweise nilpotent.

Lemma 1.9.1 *Sei Z eine zentrale Untergruppe von G. Dann ist G genau dann nilpotent, wenn G/Z nilpotent ist.*

Beweis :
Homomorphe Bilder von nilpotenten Gruppen sind wieder nilpotent, weil homomorphe Bilder von Zentralreihen wieder Zentralreihen sind. Also ist G/Z nilpotent, wenn G nilpotent ist. Wenn umgekehrt N_i/Z eine Zentralreihe von G/Z ist, ist $1 \lhd N_0 \lhd \ldots N_n = G$ eine Zentralreihe von G. □

Beispiel:
Das Zentrum der Quaternionengruppe

$$\mathrm{Q}_8 = \{1, -1, \mathbf{i}, -\mathbf{i}, \mathbf{j}, -\mathbf{j}, \mathbf{k}, -\mathbf{k}\}$$

ist $Z = \{1, -1\}$, der Quotient $\mathrm{Q}_8/Z \cong \mathrm{Z}_2 \times \mathrm{Z}_2$ ist abelsch. $1 \leq Z \leq \mathrm{Q}_8$ ist also eine Zentralreihe.

Satz 1.9.2 *Endliche p–Gruppen sind nilpotent.*

Beweis :
Sei G eine endliche p–Gruppe. Nach (1.6) ist die Mächtigkeit aller Konjugationsklassen eine Potenz von p. Also ist die Zahl der ein–elementigen Konjugationsklassen, d.h. die Mächtigkeit von $\mathrm{Z}(G)$, durch p teilbar, wenn G nicht–trivial ist. $\mathrm{Z}(G)$ ist dann nicht–trivial und $G/\mathrm{Z}(G)$ eine p–Gruppe kleinerer Mächtigkeit als G, von der wir (per Induktion) annehmen können, daß sie nilpotent ist. Dann ist G nilpotent nach dem letzten Lemma. □

Satz 1.9.3 *Der Normalisator jeder echten Untergruppe U einer nilpotenten Gruppe G ist echt größer als U.*

Beweis :
Sei $1 = N_0 \lhd \ldots \lhd N_n = G$ eine Zentralreihe von G. Es gibt einen Index i, sodaß $N_i \leq U$ und $N_{i+1} \not\leq U$. Weil N_{i+1} zentral ist, modulo N_i, ist $[n, u] \in N_i \leq U$ für alle $n \in N_{i+1}$ und $u \in U$. Daraus folgt, daß $N_{i+1} \leq \mathrm{N}_G(U)$. □

Folgerung 1.9.4 *Endliche nilpotente Gruppen sind direkte Produkte von p–Gruppen.*

Beweis :
Nach (1.8.4) sind die p–Sylowgruppen S_p der nilpotenten Gruppe G normal. Daraus folgt leicht, daß das Produkt der S_p direkt ist. Das Produkt der S_p hat aber ebensoviel Elemente wie G. □

Beispiel:
Für jeden Körper K ist die Gruppe $\delta_n(K) \leq \mathrm{GL}_n(K)$ der oberen Dreiecksmatrizen, in deren Diagonale nur Einsen stehen, nilpotent. Die Untergruppen N_i derjenigen Matrizen aus $\delta_n(K)$, deren erste $n-i$ Nebendiagonalen verschwinden, bilden eine Zentralreihe der Länge $n-1$.

1.10 Auflösbare Gruppen

Definition *Ein Gruppe, die eine Normalreihe mit abelschen Faktoren (eine* abelsche *Normalreihe) besitzt, heißt auflösbar.*

Zentralreihen sind abelsch, nilpotente Gruppen also auflösbar.

Sei (N_i) eine abelsche Normalreihe von G. Wenn U eine Untergruppe ist, ist $(U \cap N_i)$ eine abelsche Normalreihe von U. Und wenn $f : G \to H$ ein Homomorphismus ist, ist $f(N_i)$ eine abelsche Normalreihe von $f(G)$. Das ist leicht zu zeigen und beweist die eine Hälfte von

Satz 1.10.1 *Sei N ein Normalteiler von G. Dann ist G genau dann auflösbar, wenn N und G/N auflösbar sind.*

Beweis :
Wenn $N_0 \lhd \ldots \lhd N_n$ eine abelsche Normalreihe von N ist und $G_0/N \lhd \ldots \lhd G_m/N$ eine abelsche Normalreihe von G/N, ist

$$N_0 \lhd \ldots \lhd N_n = G_0 \lhd \ldots \lhd G_m$$

eine abelsche Normalreihe von G. □

Definition *Die Kommutatorgruppe G' ist die von allen Kommutatoren $[a, b]$, $a, b \in G$ erzeugte Untergruppe.*

Wenn N ein Normalteiler von G ist, ist offenbar G/N genau dann abelsch, wenn $G' \leq N$. Weil die Menge aller Kommutatoren unter allen (inneren) Automorphismen abgeschlossen ist, ist G' ein Normalteiler von G. G' ist also der kleinste Normalteiler, für den G/N abelsch ist.

Wir definieren induktiv die Folge der *Derivierten* $G^{(i)}$ von G durch $G^{(0)} = G$ und $G^{(i+1)} = (G^{(i)})'$. Die $G^{(i)}$ sind unter allen Automorphismen von G invariant und daher Normalteiler.

Satz 1.10.2 *G ist genau dann auflösbar, wenn $G^{(n)} = 1$ für genügend großes n.*

Beweis :
Wenn $G^{(n)} = 1$, ist $G^{(n)} \lhd G^{(n-1)} \lhd \ldots G^{(0)} = G$ eine abelsche Normalreihe. Wenn umgekehrt $N_0 \lhd \ldots \lhd N_n$ eine abelsche Normalreihe von G ist, zeigt man induktiv, daß $G^{(i)} \leq N_{n-i}$:

$$G^{(i+1)} = (G^{(i)})' \leq (N_{n-i})' \leq (N_{n-i-1}).$$

□

Weil nach dem Satz von Cayley jede endlich Gruppe isomorph zu einer Untergruppe einer endlichen symmetrischen Gruppe ist, ist nicht zu erwarten, daß alle endlichen symmetrischen Gruppen auflösbar sind:

Beispiel:
Die endlichen symmetrischen Gruppen

$$\mathrm{S}_n = \mathrm{Sym}\{1, \ldots, n\}$$

sind genau dann auflösbar, wenn $n \leq 4$:

$\mathrm{S}_1 = 1$, $\mathrm{S}_2 = \mathrm{Z}_2$ sind abelsch.
S_3 hat die abelsche Normalreihe $1 \lhd \mathrm{A}_3 \lhd S_3$, wobei A_n der Normalteiler der geraden Permutationen (die *alternierende Gruppe*) ist.
S_4 hat die abelsche Normalreihe $1 \lhd \mathrm{V}_4 \lhd \mathrm{A}_4 \lhd \mathrm{S}_4$, mit der Kleinschen Vierergruppe

$$\mathrm{V}_4 = \{\, 1,\ (12)(34),\ (13)(24),\ (14)(23) \,\} \cong \mathrm{Z}_2 \times \mathrm{Z}_2.$$

Es ist tatsächlich $\mathrm{S}_4^{(1)} = \mathrm{A}_4$, $\mathrm{S}_4^{(2)} = \mathrm{V}_4$ und $\mathrm{S}_4^{(3)} = 1$.
Für $n \geq 5$ sind die S_n nicht auflösbar, weil die Reihe der derivierten Gruppen bei $\mathrm{S}_n^{(1)} = \mathrm{S}_n^{(2)} = \mathrm{A}_n$ stationär wird. Weil $\mathrm{S}_n^{(1)} \lhd \mathrm{A}_n$, ist zu zeigen, daß $\mathrm{A}_n' = \mathrm{A}_n$. Wegen

$$[(123), (12345)] = (253)$$

gehören (253) und damit auch alle Konjugierten, also alle Dreierzyklen, zu A_n'. Jede gerade Permutation laßt sich aber als Produkt von Dreierzyklen schreiben. Es genügt, das für Produkte von zwei Transpositionen einzusehen. Es ist $(ab)(bc) = (abc)$ und $(ab)(cd) = (abc)(bcd)$.

Mit ähnlichen Methoden zeigt man

Lemma 1.10.3 *Die alternierenden Gruppen* A_n *sind für* $n \geq 5$ *einfach.*

□

Beispiel:
Die Kommutatorgruppe der Gruppe $\Delta_n(K) \leq \mathrm{GL}_n(K)$ der invertierbaren oberen Dreiecksmatrizen ist $\delta_n(K)$ (S.29). $\Delta_n(K)$ ist also auflösbar.

Kapitel 2

Kommutative Ringe

2.1 Der Homomorphiesatz

Definition *Ein Ring $R = (R, +, \cdot)$ ist eine abelsche Gruppe $(R, +)$ mit einer bilinearen Halbgruppenoperation $\cdot$.*

Die Multiplikation erfüllt also die Rechenregeln

$$\begin{aligned} a(b+c) &= (ab) + (ac) \\ (a+b)c &= (ab) + (ac) \\ (ab)c &= a(bc). \end{aligned}$$

Weil $a0 = a(0+0) = a0 + a0$ und $0a = (0+0)a = 0a + 0a$, ist in allen Ringen

$$a0 = 0a = 0.$$

Wir werden im Folgenden nur *unitäre* Ringe mit einem Einselement 1 betrachten, für das also

$$1a = a1 = a.$$

Wenn in einem Ring $R \quad 1 = 0$, ist für alle $a \in R$

$$a = 1 \cdot a = 0 \cdot a = 0.$$

R ist also der *triviale* Ring 0, der nur aus dem Nullelement besteht.

Beispiel:
Ein *Endomorphismus* einer abelschen Gruppe A ist ein Homomorphismus $f : A \to A$. Elementweise Addition macht die Menge $\mathrm{End}(A)$ aller Endomorphismen von A zu einer abelschen Gruppe, Komposition zu einem Ring, dem *Endomorphismenring* von A.

Die (bzgl. $\cdot$) invertierbaren Elemente bilden die Gruppe R^* der *Einheiten* von R. Wenn R nichttrivial ist und alle von Null verschiedenen Elemente Einheiten sind, heißt R *Schiefkörper* oder *Divisionsring*.

Beispiel:
Die Quaternionenalgebra $\mathbb{H}$ ist ein Schiefkörper.

Ein Ring, dessen Multiplikationshalbgruppe kommutativ ist, heißt *kommutativer Ring*.

Beispiel:
Die ganzen Zahlen $\mathbb{Z}$ sind ein kommutativer Ring.

Ein *Homomorphismus*

$$f : R \to S$$

zwischen Ringen ist ein Homomorphismus zwischen den additiven Gruppen und den multiplikativen Halbgruppen von R und S. Es gilt also

$$\begin{aligned} f(x+y) &= f(x)+f(y) \\ f(xy) &= f(x)f(y) \end{aligned}$$

Wir betrachten im folgenden nur *unitäre* Homomorphismen, für die

$$f(1) = 1.$$

Entsprechend sei ein *Unterring* S von R immer unitär. Das heißt, daß das Einselement von S auch Einselement von R ist.

Beispiel:
Für jeden Ring R gibt es einen (und nur einen) Homomorphismus $\mathbb{Z} \to R$, definiert durch $z \mapsto z \cdot 1$.

Beispiel:
Das direkte Produkt $R_1 \times R_2$ von zwei Ringen ist, mit komponentenweisen Operationen wieder ein Ring, mit Einselement $(1,1)$. Die Projektionen $R_1 \times R_2 \to R_i$ sind unitäre Homomorphismen. Die durch $x \mapsto (x,0)$ definierte isomorphe Einbettung $R_1 \to R_1 \times R_2$ ist nicht *unitär*.[1]

Der *Kern* eines Ringhomomorphismus $f : R \to S$ ist der Kern

$$\ker(f) = \{g \in R \mid f(g) = 0\}$$

von f als Homomorphismus der additiven Gruppen. Weil $r0 = 0r = 0$ für alle $r \in R$, ist der Kern eines Homomorphismus ein *Ideal*.

Definition *Ein Ideal eines Ringes ist eine additive Untergruppe I mit*

$$rI \subset I, \quad Ir \subset I$$

für alle $r \in R$. Wir verwenden die gleiche Notation wie bei Normalteilern:

$$I \lhd R$$

Satz 2.1.1 (Homomorphiesatz) *Sei R ein Ring.*

[1] Einfachstes Beispiel eines Unterrings, der nicht (notwendig) unitärer Unterring ist, ist natürlich der triviale Ring 0.

1. *Wenn I ein Ideal von R ist, wird durch*
$$(I+g)\cdot(I+h) = I+(g\cdot h)$$
eine Ringoperation auf R/I definiert. Die Projektion
$$\pi : R \to R/I$$
ist ein Homomorphismus.

2. *Sei $f : R \to S$ ein Homomorphismus und $I = \ker(f)$ der Kern von f. Dann ist I ein Ideal und*
$$I+g \mapsto f(g)$$
definiert einen Isomorphismus zwischen R/I und $f(R)$.

□

Beweis :
Im wesentlichen ist nur zu zeigen, daß die Nebenklassenzerlegung nach einem Ideal eine Kongruenzrelation ist, daß also für jedes Ideal I

$$I+a = I+b \Longrightarrow I+ac = I+bc,\ I+ca = I+cb.$$

Es ist aber

$$a-b \in I \Longrightarrow ac-bc = (a-b)c \in I,\ ca-cb = c(a-b) \in I.$$

□

Jeder Ring R hat die beiden Ideale 0 und R. Ein von R verschiedenes Ideal heißt *echt*.

Beispiel:
Alle additiven Untergruppen von $\mathbb{Z}$ sind Ideale. Die abelschen Gruppen

$$\mathrm{Z}_m = \mathbb{Z}/m\mathbb{Z}$$

haben also eine natürliche Ringstruktur.

Eine additive Untergruppe I von R heißt *Linksideal*, wenn $RI = I$, und *Rechtsideal*, wenn $IR = I$.[2]

Beispiel:
Sei V ein endlich–dimensionaler Vektorraum und R der Endomorphismenring von V. Für jeden Unterraum W ist

$$\{f \in R \mid W \subset \ker(f)\}$$

ein Linksideal und

$$\{f \in R \mid \mathrm{Im}(f) \subset W\}$$

ein Rechtsideal. Alle Links– und Rechtsideale haben diese Form. Man sieht so, daß R außer 0 und R keine Ideale enthält. Ein Ring $R \neq 0$ mit dieser Eigenschaft heißt *einfach*.

Im Endomorphismenring eines unendlich–dimensionalen Vektorraums ist die Menge der Endomorphismen von endlichem Rang ein echtes Ideal.

[2] Es ist immer $I \subset RI$ und $I \subset IR$.

2.2 Moduln

In diesen Abschnitt sei R ein Ring.

Definition *Ein R–Linksmodul ist eine abelsche Gruppe M mit einer Multiplikation $R \times M \to M$, die den folgenden Regeln genügt:*

a) $r(x+y)=rx+ry$

b) $(r+s)x=rx+sx$

c) $(rs)x=r(sx)$

d) $1x=x$

R–Rechtsmoduln sind entsprechend definiert, R operiert von rechts. Die Unterscheidung ist nicht nur notationell. Wenn man R durch

$$a \cdot^{\text{opp}} b = b \cdot a$$

eine neue Multiplikation gibt, erhält man den *entgegengesetzen* Ring R^{opp}. Aus einem R–Linksmodul M wird durch die Setzung $xr = rx$ ein R^{opp}–Rechtsmodul.

Beispiel:
Jeder Ring R ist auf natürliche Weise ein R–Linksmodul, den man mit ${}_RR$ bezeichnet, und ein R–Rechtsmodul R_R.

Ab jetzt sind alle Moduln Linksmoduln.

Ein Ringhomomorphismus $\rho : S \to R$ macht aus einem R–Modul M einen S–Modul ${}_SM$ vermöge

$$sx = \rho(s)x.$$

Jede abelsche Gruppe A ist auf natürliche Weise ein $\mathbb{Z}$–Modul (vgl. Seite 9) und ein $\text{End}(A)$–Modul.

Eine R–Modulstruktur auf A liefert einen Homomorphismus $R \to \text{End}(A)$, man ordnet jedem r den Endomorphismus $x \mapsto rx$ zu. Umgekehrt definiert jeder Homomorphismus $R \to \text{End}(A)$ eine R–Modulstruktur auf der abelschen Gruppe A.

Definition *Sei M ein R–Modul.*

1. *Ein Untermodul N von M ist eine Untergruppe von $(M,+)$, die unter Multiplikation mit Elementen von R abgeschlossen ist.*
2. *Ein Homomorphismus f von M in den R–Modul L, ist ein Homomorphismus $f : (M,+) \to (L,+)$, der R–linear ist. Für den also*

   $$f(rx) = rf(x)$$

   für alle $x \in M$ und $r \in R$.

Den Ring der Endomorphismen[3] eines R–Moduls M bezeichnet man wieder mit $\mathrm{End}(M)$. Wenn $(M,+)$ mehrere Modulstrukturen hat, ist die Schreibweise $\mathrm{End}_R(M)$ genauer.

Beispiel:
$\mathrm{End}_R(M)$ ist ein Unterring von $\mathrm{End}_{\mathbb{Z}}(M)$.

Ebenso schreiben wir $\mathrm{Hom}_R(M,N)$ für die abelsche Gruppe der Homomorphismen von M nach N.

Die Untermoduln von ${}_RR$ sind die Linksideale von R. Linksmultiplikation mit einem Ringelement definiert einen Endomorphismus von R_R. Man erhält so einen Ringhomomorphismus $R \to \mathrm{End}(R_R)$.

Bemerkung *Die natürliche Abbildung $R \to \mathrm{End}(R_R)$ ist ein Ringisomorphismus.*

Beweis :
Weil $r1 = r$, ist die Abbildung injektiv (vgl. den Beweis von 1.1.4). Sei ϕ ein Endomorphismus von R_R. Dann ist ϕ Linksmultiplikation mit $r = \phi(1)$, weil $rs = \phi(1)s = \phi(1s) = \phi(s)$.

Satz 2.2.1 (Homomorphiesatz) *Sei M ein R–Modul.*

1. *Wenn N ein Untermodul von M ist, wird durch*

$$r(N+x) = N + rx$$

eine R–Modulstruktur auf M/N definiert. Die Projektion

$$\pi : M \to M/N$$

ist ein Homomorphismus.

2. *Sei $f : M \to L$ ein Homomorphismus und $N = \ker(f)$ der Kern von f. Dann ist N ein Untermodul und*

$$N + x \mapsto f(x)$$

definiert einen Isomorphismus zwischen M/N und $f(M)$.

□

Beweis :
Wir zeigen, daß $N + rx$ nur von $N + x$ abhängt: Wenn $N + x = N + x'$, ist

$$x - x' \in N \;\Rightarrow\; rx - rx' = r(x - x') \in N$$

und daher $N + rx = N + rx'$. Daraus folgt 1).

[3] Endomorphismen sind Homomorphismen in sich.

Für 2) überlegen wir, daß N ein Untermodul ist: Wenn $x \in N$, ist[4]

$$f(rx) = rf(x) = r \cdot 0 = 0.$$

□

Die direkte Summe $\bigoplus_{i \in I} M_i$ einer Familie von R–Moduln ist auf natürliche Weise wieder ein R–Modul. Man definiert (für $x_i \in M_i$)

$$r\big(\sum_{i \in I} x_i\big) = \big(\sum_{i \in I} rx_i\big).$$

Definition *Ein freier R–Modul F ist eine direkte Summe von Kopien von R. Die Einselemente der Summanden bilden die Basis von F.*

Lemma 2.2.2 *Ein freier Modul F wird von seiner Basis (f_i) frei erzeugt: Zu jedem R–Modul M und Elementen $m_i \in M$ gibt es genau einen Homomorphismus $F \to M$, der f_i auf m_i abbildet.*

Beweis :
Die Elemente f von F schreiben sich eindeutig als

$$f = \sum_{i \in I} r_i f_i.$$

Man bildet f ab auf $\sum_{i \in I} r_i m_i$. □

[4]Man sieht leicht, daß $r0 = 0y = 0$ für alle $r \in R$ und alle $y \in M$.

2.3 Polynomringe

In diesem Abschnitt und im Rest des Kapitels sind alle Ringe, insbesondere der Ring R, **kommutativ**.

Definition *Eine R–Algebra ist ein R–Modul A mit einer bilinearen Operation $A \times A \to A$. Wenn wir die Operation als Multiplikation schreiben, gelten also die Regeln*

a) $x(y+z) = xy + xz$

b) $(x+y)z = xz + yz$

c) $(rx)y = x(ry) = r(xy)$

Wenn die R–Algebra A ein (nicht notwendig kommutativer) Ring ist, ist die Abbildung $\mu : r \mapsto r1$ ein Ringhomomorphismus von R in das Zentrum

$$\mathrm{Z}(A) = \{a \in A \mid ab = ba \text{ für alle } b \in A\}$$

von A. Ein solcher Homomorphismus macht umgekehrt, vermöge $ra = \mu(r)a$, einen Ring A zu einer R–Algebra. Insbesondere ist jeder (kommutative) Ring, der R als Unterring enthält eine R–Algebra.

Wir betrachten im folgenden **nur** Algebren, die (nicht notwendig kommutative) Ringe sind. Unsere Algebren sind also assoziativ und haben ein Einselement.

Definition *Der Polynomring*

$$R[X]$$

ist eine kommutative R–Algebra mit einem ausgezeichneten Element X, in der sich jedes Element eindeutig als eine Summe

$$\sum_{i \in \mathbb{N}} r_i X^i$$

mit Koeffizienten $r_i \in R$ schreiben läßt. Die Elemente von $R[X]$ heißen Polynome mit Koeffizienten aus R.

Es ist klar, daß $R[X]$ bis auf Isomorphie eindeutig bestimmt ist. Wir müssen zeigen, daß $R[X]$ wirklich existiert. Dazu wählen wir einen freien R–Modul A mit Basis $m_0, m_1, \ldots$. Eine bilineare Abbildung $\mu : A \times A \to A$ wird durch die Werte $\mu(m_i, m_j)$ bestimmt, die man beliebig vorgeben kann. Wir definieren die Multiplikation von A durch $m_i \cdot m_j = m_{i+j}$. Es ist klar, daß $m_0 = 1$ Einselement von A ist. Für $X = m_1$ gilt dann $X^i = m_i$ $(i = 0, 1, \ldots)$. Zu zeigen ist noch, daß A assoziativ und kommutativ ist. Weil die Multiplikation auf der Basis assoziativ ist, stimmen die beiden multilinearen Abbildungen $(xy)z$ und $x(yz)$ auf der Basis überein und müssen daher gleich sein. Ebenso zeigt man die Kommutativität von $A = R[X]$.

Der Homomorphismus $R \to R[X]$ ist injektiv. Wir können deshalb R als Unterring von $R[X]$ auffassen.

Lemma 2.3.1 *Sei S eine R–Algebra und s ein Element von S. Dann gibt es einen eindeutig bestimmten Homomorphismus*[5] *$R[X] \to S$, der X auf s abbildet, den* Einsetzungshomomorphismus. *Man bezeichnet mit $f(s)$ das Bild von f.*

Beweis :
Wenn $f = \sum_{i\in\mathbb{N}} r_i X^i$, setze $f(s) = \sum_{i\in\mathbb{N}} r_i s^i$. (Per definitionem ist $s^0 = 1$.) □

Man beachte, daß im Fall $S = R[X]$ und $s = X$

$$f = f(X).$$

$R[X]$ wird (als Ring) von den Elementen von R und X erzeugt. Wenn S ein Oberring von R und s ein Element von S ist, bezeichnen wir mit $R[s]$ den von den Elementen von R und s erzeugten Teilring von S. Man sieht leicht, daß

$$R[s] = \{f(s) \mid f \in R[X]\}.$$

Definition *Der Grad eines Polynoms $f = \sum_{i\in\mathbb{N}} a_i X^i$ ist*

$$\deg(f) = \max\{\, i \mid a_i \neq 0\},$$

der größte Index eines nicht–verschwindenden Koeffizienten. Der Grad des Nullpolynoms ist $-\infty$. Wenn $\deg(f) = n$, nennt man a_n den Leitkoeffizienten von f.

Der Leitkoeffizient des Nullpolynoms ist definiert als 0. Polynome mit Leitkoeffizient 1 heißen *normiert*. Polynome vom Grad 0 und das Nullpolynom heißen *konstante* Polynome.

Satz 2.3.2 (Division mit Rest) *f und g seien Polynome aus $R[X]$. Wenn $g \neq 0$ und der Leitkoeffizient von g eine Einheit ist, gibt es Polynome h und r mit*

$$f = gh + r$$

und

$$\deg(r) < \deg(g).$$

Beweis :
Wenn $\deg(f) = m < n = \deg(g)$, setzen wir $h = 0$ und $r = f$ und sind fertig. Sonst wählen wir $c \in R$, sodaß f und cg den gleichen Leitkoeffizienten haben. Dann ist der Grad von $f - g \cdot cX^{m-n}$ kleiner als m und, mit Induktion, finden wir h und r mit

$$f - g \cdot cX^{m-n} = gh + r$$

und $\deg(r) < \deg(g)$. Es ist dann

$$f = g(cX^{m-n} + h) + r.$$

□

a heißt *Nullstelle* des Polynoms f, wenn $f(a) = 0$. In einem Ring S heißt b *Teiler* von a, wenn a ein Vielfaches von$b$ ist, wenn also $a = bc$ für ein $c \in S$.

[5]Ein Homomorphismus zwischen R–Algebren ist ein R–linearer unitärer Ringhomomorphismus.

Folgerung 2.3.3 *Sei $f \in R[X]$ und $a \in R$. Dann ist a genau dann eine Nullstelle von f, wenn $X - a$ ein Teiler von f ist.*

Beweis :
Sei $f = (X - a)h + r$ für ein $r \in R$. Dann ist a genau dann Nullstelle von f, und $X - a$ genau dann ein Teiler von f, wenn $r = 0$. □

Wenn man die Bildung des Polynomrings iteriert, erhält man Polynomringe in mehreren Variablen:

$$R[X_1, \dots X_n] = R[X_1] \dots [X_n].$$

Man sieht leicht, daß sich jedes Polynom aus $R[X_1, \dots X_n]$ eindeutig in der Form

$$\sum_{\nu \in \mathbb{N}^n} a_\nu X^\nu$$

schreiben läßt, wobei für einen *Multiindex* $\nu = (e_1, \dots, e_n)$

$$X^\nu = X_1^{e_1} \dots X_n^{e_n}.$$

Ein solches Produkt der Variablen heißt *Monom*.

Ganz allgemein läßt sich aus jeder Familie $(X_i)_{i \in I}$ von Unbestimmten ein Polynomring

$$R[X_i]_{i \in I}$$

bilden. Die Elemente von $R[X_i]_{i \in I}$ sind R–Linearkombinationen von Monomen $X_{i_1}^{e_1} \dots X_{i_n}^{e_n}$.

2.4 Körper und Integritätsbereiche

Wir betrachten in diesem Kapitel nur kommutative Ringe.

Definition *Ein Körper ist ein kommutativer Schiefkörper.*

Beispiele:
$\mathbb{Q}$, $\mathbb{R}$ und $\mathbb{C}$ und die endlichen Körper $\mathbb{F}_p$.

Lemma 2.4.1 *Ein Ring ist genau dann ein Körper, wenn* 0 *das einzige echte Ideal ist.*

Beweis :
Sei a ein Element von R. Dann ist a genau dann eine Einheit, wenn das von a erzeugte Ideal Ra die Eins enthält, das heißt wenn $Ra = R$. Daß 0 das einzige echte Ideal ist, bedeutet also, daß $K \setminus 0$ die Einheitengruppe von K ist, was bedeutet, daß K ein Körper ist. □

Es folgt, daß jeder Homomorphismus $f : K \mapsto R$ eines Körpers in einen Ring R entweder eine Einbettung ist, oder der Nullhomomorphismus.

Ein Körper kann keine *Nullteiler* haben. Ein Nullteiler ist ein Element $a \neq 0$, für das es ein $b \neq 0$ mit

$$ab = 0$$

gibt. (Es würde nämlich $1 = a^{-1}ab^{-1}b = a^{-1}b^{-1}ab = 0$ folgen.)

Definition *Ein nichttrivialer Ring ohne Nullteiler heißt Integritätsbereich.*

Ein Ring ist also genau dann ein Integritätsbereich, wenn

$$ab = 0 \;\Rightarrow\; a = 0 \text{ oder } b = 0.$$

Wir werden jeden Integritätsbereich in einen Körper, seinen Quotientenkörper, einbetten. Um die wohlbekannte Konstruktion nicht zu wiederholen, diskutieren wir das allgemeinere Konzept der *Quotientenringe*[6].

Satz 2.4.2 *Sei R ein Ring und S eine multiplikativ abgeschlossene Teilmenge von R. Dann gibt es einen Homomorphismus*

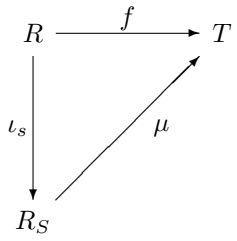
$$\iota_S : R \to R_S$$

in einen Ring R_S, der durch folgende universelle Eigenschaft eindeutig bestimmt ist:

a) ι_S bildet alle Elemente von S in Einheiten von R_S ab.

[6]Man verwechsle diese Quotientenringe nicht mit den Ringen R/I für ein Ideal I.

b) Jeder Homomorphismus $f : R \to T$, der die Elemente von S in Einheiten abbildet, faktorisiert in eindeutiger Weise durch ι_S. Das heißt, es gibt einen eindeutig bestimmten Homomorphismus $\mu : R_S \to T$, der das Diagramm



kommutativ macht.

Beweis :
Die Eindeutigkeit von $\iota_s : R \to R_S$ sieht man leicht mit folgenden Standardargument: Nehmen wir an, daß $\iota' : R \to R'$ ebenfalls die universelle Eigenschaft hat. Dann gibt es Homomorphismen $\mu : R_S \to R'$ und $\mu' : R' \to R_S$ mit $\iota' = \mu \circ \iota$ und $\iota = \mu' \circ \iota'$. Weil $\iota = (\mu'\mu) \circ \iota$, folgt aus der Eindeutigkeit des Homomorphismus, daß $\mu'\mu = 1$. Ebenso folgt $\mu\mu' = 1$.

Die Existenz folgt zwar mit *general nonsense*:

Drei-Sterne-General
Wir ordnen jedem $s \in S$ eine Variable X_s (für das Inverse von s) zu und betrachten den Polynomring $R[X_s]_{s\in S}$. Das Ideal I sei erzeugt von den Polynomen $sX_s - 1$. Dann ist $R_S = R[X_s]_{s\in S}/I$ und ι_S ist die Komposition $R \to R[X_s] \to R[X_s]_{s\in S}/I$.

Vier-Sterne-General
Wir betrachten alle[7]möglichen Homomorphismen $f_i : R \to T_i$, die die Elemente von S auf Einheiten abbilden. Sei R' das direkte Produkt aller dieser T_i und $\iota_S : R \to R'$ das Produkt der f_i. ι_S bildet wieder alle s auf Einheiten ab. R_S ist der Unterring von R', der vom Bild von R und den Inversen aller $\iota_S(s)$ erzeugt wird.

Wir ziehen aber eine spezifische Konstruktion vor, die mehr Information liefert. Wir können dabei ohne weiteres annehmen, daß S die 1 enthält. Wenn R_S konstruiert ist, wird R_S die Menge aller Quotienten

$$\frac{\iota_S(r)}{\iota_S(s)} \quad (r \in R,\, s \in S)$$

sein. Wir definieren nun R_S als die Menge aller Äquivalenzklassen von Paaren (r, s) $(r \in R,\, s \in S)$ unter der Äquivalenzrelation

$$(r_1, s_1) \sim (r_2, s_2) \iff \exists t \in S\; r_1 s_2 t = r_2 s_1 t.$$

Addition und Multiplikation definiert man durch

$$(r_1, s_1) + (r_2, s_2) = (s_2 r_1 + s_1 r_2, s_1 s_2)$$

[7]Das ist mengentheoretisch unsauber. Diese Homomorphismen bilden keine Menge.

und

$$(r_1, s_1) \cdot (r_2, s_2) = (r_1 r_2, s_1 s_2).$$

Daß $\sim$ tatsächlich eine Äquivalenzrelation ist, daß Addition und Multiplikation repräsentantenunabhängig definiert sind und daß R_S ein Ring ist, ist leicht nachzurechnen. Wir zeigen als ein Beispiel die Transitivität von $\sim$:
Sei

$$(r_1, s_1) \sim (r_2, s_2) \sim (r_3, s_3),$$

weil $r_1 s_2 t_1 = r_2 s_1 t_1$ und $r_2 s_3 t_2 = r_3 s_2 t_2$ für $t_1, t_2 \in S$. Wir multiplizieren die erste Gleichung mit $s_3 t_2$, die zweite mit $s_1 t_1$ und erhalten

$$r_1 s_3 s_2 t_1 t_2 = r_2 s_1 s_3 t_1 t_2 = r_3 s_1 s_2 t_1 t_2,$$

woraus $(r_1, s_1) \sim (r_3, s_3)$ folgt.

$\iota_S(r) = (r, 1)/\sim$ ist der gesuchte Homomorphismus von R nach R_S. Ein Homomorphismus $f : R \to T$, der die Elemente von R in Einheiten abbildet, faktorisiert als $f = \mu \circ \iota_S$, wobei $\mu\big((r, s)/\sim\big) = f(r) f(s)^{-1}$. □

Folgerung *Jeder Integritätsbereich R ist Unterring eines Körpers K. Man kann annehmen, daß*

$$K = \Big\{ \frac{r}{s} \in K \mid r \in R,\, s \in R \setminus 0 \Big\}.$$

Dadurch wird K bis auf Isomorphie über R eindeutig bestimmt und heißt der Quotientenkörper $\mathrm{Quot}(R)$ *von R.*

Beweis :
Setze $K = R_{R\setminus 0}$. Die Abbildung $\iota_S : R \to K$ ist injektiv, weil $(r, s)/\sim = 0 \Leftrightarrow \exists t \neq 0\ rt = 0 \Leftrightarrow r = 0$. K ist ein Körper, weil jedes $\frac{r}{s}$, das nicht Null ist, $\frac{s}{r}$ als Inverses hat. □

Wenn R ein Integritätsbereich ist, ist $R[X]$ ebenfalls ein Integritätsbereich. Die Gradfunktion deg( ) erfüllt hier die Rechenregeln

$$\begin{aligned} \deg(fg) &= \deg(f) + \deg(g) \\ \deg(f+g) &\leq \max\{\deg(f), \deg(g)\}. \end{aligned}$$

Für einen Körper K nennt man den Quotientenkörper

$$K(X) = \mathrm{Quot}(K[X])$$

den *rationalen Funktionenkörper* über K. Die Gradfunktion setzt sich per

$$\deg\left(\frac{f}{g}\right) = \deg(f) - \deg(g)$$

auf $K(X)$ fort.

Lemma 2.4.3 *Ein Polynom n–ten Grades ($n \geq 0$) über einem Integritätsbereich R hat höchstens n Nullstellen in R.*

BEWEIS :
Sei f ein Polynom von Grad n. Wir dividieren f solange wie möglich durch lineare normierte Polynome,

$$f = (X - a_1) \cdots (X - a_m)g.$$

Nach 2.3.2 hat g keine Nullstelle mehr. Weil R ein Integritätsbereich ist, sind die a_i genau die Nullstellen von f und natürlich ist $m \leq n$. □

Folgerung 2.4.4 *Ein Polynom von Grad n über einem Integritätsbereich R ist durch seine Werte $f(a_0), \ldots, f(a_n)$ an $n+1$ verschiedenen Stellen $a_i \in R$ eindeutig bestimmt.* □

2.5 Primideale

Definition *Sei R ein (kommutativer) Ring. Ein maximales Ideal M von R ist ein echtes Ideal, das in keinem anderen echten Ideal enthalten ist.*

Aus 2.4.1 folgt sofort

Lemma 2.5.1 *Ein Ideal M von R ist genau dann maximal, wenn R/M ein Körper ist.*

Beweis :
Die Projektion $R \to R/M$ vermittelt eine Bijektion zwischen den Idealen von R/M und den Idealen von R, die M enthalten. □

Weil ein Ideal genau dann echt ist, wenn es die 1 nicht enthält, folgt aus dem Zornschen Lemma leicht:

Lemma 2.5.2 *Jedes echte Ideal von R ist in einem maximalen Ideal enthalten.* □

Definition *Ein echtes Ideal P heißt prim (oder Primideal), wenn*

$$ab \in P \Longrightarrow a \in P \text{ oder } b \in P.$$

Lemma 2.5.3 *Ein Ideal P von R ist genau dann prim, wenn R/P ein Integritätsbereich ist.*

Beweis :
Klar. □

Lemma 2.5.4 *Sei S eine nicht–leere multiplikativ abgeschlossene Teilmenge von R. Sei P ein Ideal von R, das disjunkt ist zu S und maximal ist mit dieser Eigenschaft. Dann ist P ein Primideal.*

Beweis :
Wenn a und b nicht zu P gehören, sind $Ra + P$ und $Rb + P$ zwei echte Erweiterungsideale, die daher nicht disjunkt zu S sein können. Es gibt also $s, t \in R$ und $p, q \in P$, sodaß $sa+p$ und $tb+q$ zu S gehören. Das Produkt $(st)ab+saq+tbp+pq$ gehört wieder zu S. ab kann dann aber nicht zu P gehören. □

Maximale Ideale sind *teilerfremd* im Sinne der folgenden Definition.

Definition *Zwei Ideale I und J von R heißen relativ prim (oder teilerfremd), wenn*

$$I + J = R.$$

Satz 2.5.5 (Chinesischer Restsatz) *$I_1 \ldots, I_n$ seien paarweise teilerfremde Ideale von R. Dann induziert die natürliche Abbildung*

$$R \to R/I_1 \times \cdots \times R/I_n$$

einen Isomorphismus zwischen $R/(I_1 \cap \cdots \cap I_n)$ und $R/I_1 \times \cdots \times R/I_n$

BEISPIEL:

$$\mathbb{Z}_{12} \cong \mathbb{Z}_3 \times \mathbb{Z}_4$$

BEWEIS :
Der Kern der Abbildung ist offensichtlich $I_1 \cap \cdots \cap I_n$. Es ist also nur die Surjektivität zu zeigen. Wir wählen für jedes Paar $i \neq j$ ein Element $e_i^j \in I_i$, für das es ein $r \in I_j$ mit $e_i^j + r = 1$ gibt. Es ist also $e_i^j \equiv 1 \pmod{I_j}$ und $e_i^j \equiv 0 \pmod{I_i}$. Für $e^j = \prod_{i \neq j} e_i^j$ gilt dann $e^j \equiv 1 \pmod{I_j}$ und $e^j \equiv 0 \pmod{I_i}$ für alle $i \neq j$. Wenn $r_1, \ldots, r_n$ gegeben sind, setzen wir $x = \sum_j r_j e^j$ und haben dann $x \equiv r_j \pmod{I_j}$ für alle j. □

2.6 Teilbarkeit

Definition *Ein Integritätsbereich R mit einer* Betragsfunktion

$$|\quad| : R \to \mathbb{N} \cup \{-\infty\}$$

heißt euklidischer Ring, wenn $r = 0 \Leftrightarrow |r| = -\infty$ und wenn der Satz von der Division mit Rest gilt:
Für alle f und g aus R, $g \neq 0$ gibt es $h, r \in R$ mit

$$f = gh + r$$

und $|r| < |g|$.

Beispiel:
$\mathbb{Z}$ ist ein euklidischer Ring.

Beispiel:
Polynomringe $K[X]$ über einem Körper K sind nach 2.3.2 euklidisch.

Beispiel:
$\mathbb{Z}$[i] ist euklidisch mit der Betragsfunktion

$$|a + b\mathrm{i}| = a^2 + b^2.$$

Definition *Ein Integritätsbereich R heißt Hauptidealring, wenn jedes Ideal I* Hauptideal *ist, das heißt von der Form*

$$I = Ra.$$

Wir schreiben gelegentlich (a) für Ra.

Satz 2.6.1 *Euklidische Ringe sind Hauptidealringe.*

Beweis :
Wenn $I = 0$, ist $I = (0)$. Wenn $I \neq 0$, wählen wir ein $g \in I \setminus 0$ mit minimalem Betrag. Dann ist $I = (g)$. Denn wenn wir ein $f \in I$ mit Rest r durch g dividieren, muß auch r zu I gehören. Der Betrag von r kann aber nur dann kleiner sein als $|g|$, wenn $r = 0$. □

a und b seien Elemente eines kommutativen Ringes R. Wir sagen b *teilt* a

$$b|a$$

wenn $a = bc$ für ein $c \in R$. b heißt auch *Teiler* von a.

Wenn a und b sich gegenseitig teilen, heißen a und b *äquivalent*, in Zeichen

$$a \sim b.$$

Die Menge der Äquivalenzklassen wird durch die Teilbarkeitsrelation zu einer partiellen Ordnung mit kleinstem Element $1/\sim\ = R^*$ und größtem Element

$0/\sim = \{0\}$.
Ein Element $p \neq 0$ heißt *irreduzibel*, wenn p keine Einheit ist und jeder Teiler von p entweder eine Einheit oder zu p äquivalent ist. Ein Körper hat keine irreduziblen Elemente. Die irreduziblen Elemente von $\mathbb{Z}$ sind gerade die Primzahlen und ihre Negativen.

Für die von a und b erzeugten Hauptideale (a) und (b) bedeutet $b|a$, daß $(a) \subset (b)$, und $a \sim b$, daß $(a) = (b)$. p ist genau dann irreduzibel, wenn (p) ein maximales Hauptideal ist. In Hauptidealringen also, wenn (p) maximal ist.

Wenn R ein Integritätsbereich ist (und $a \neq 0$), folgt aus $a = bc$ und $b = ad$, daß $dc = 1$. Zwei Elemente sind also genau dann äquivalent, wenn sie durch Multiplikation mit einer Einheit auseinander hervorgehen.

Definition *Ein faktorieller Ring ist ein Integritätsbereich, in dem sich jede von Null verschiedene Nichteinheit (bis auf Reihenfolge und Äquivalenz) eindeutig als Produkt von irreduziblen Elementen schreiben läßt.*

Wenn (p_i) ein Vertretersystem der Äquivalenzklassen der irreduziblen Elemente ist, bedeutet das, daß sich jedes von Null verschiedene Element eindeutig in der Form

$$\epsilon \prod_{i \in I} p_i^{e_i} \ ,$$

mit einer Einheit ϵ und natürlichen Zahlen e_i, schreiben läßt.

Satz 2.6.2 *Hauptidealringe sind faktoriell.*

Beweis :
Sei $a \in R$ ungleich Null und eine Nichteinheit.

Existenz der Zerlegung:

Wenn a_0 keine Zerlegung in Irreduzible hat, hat a_0 einen Teiler a_1, der keine Einheit, nicht äquivalent zu a_0 ist und ebenfalls keine Zerlegung in Irreduzible hat. Man erhält also eine unendliche echte Teilerkette $\ldots a_2|a_1|a_0$, die es in Hauptidealringen nicht geben kann. Die Vereinigung der Hauptideale

$$(a)_0 \subset (a_1) \subset (a_2) \subset \ldots$$

kann nämlich kein endlich erzeugtes Ideal sein, also erst recht kein Hauptideal.

Eindeutigkeit

Für irreduzible p_i, q_j sei

$$a = p_1 \ldots p_m = q_1 \ldots q_n.$$

(p_1) ist als maximales Ideal auch prim. Also muß eins der Elemente $q_1, \ldots q_n$ zu (p_1) gehören. Wenn zum Beispiel q_1 zu (p_1) gehört, ist p_1 ein Teiler von q_1. p_1 und q_1 sind dann äquivalent und es folgt, daß auch $p_2 \ldots p_m$ und $q_2 \ldots q_n$

äquivalent sind. Wenn wir so fort fahren, erhalten wir das gewünschte Ergebnis: $m = n$ und (nach einer Permutation der Indizes) $p_i \sim q_i$. □

Ringe, in denen jedes Ideal endlich erzeugt ist, heißen *noethersch*. Man sieht leicht, daß ein Ring genau dann noethersch ist, wenn es keine unendliche, echt aufsteigende Kette von Idealen gibt.

In faktoriellen Ringen ist Rp genau dann prim, wenn $p = 0$ oder wenn p irreduzibel ist. Die Umkehrung gilt in allen Integritätsbereichen. Sei nämlich (p) prim und ungleich Null. Um zu zeigen, daß p irreduzibel ist, betrachten wir einen Teiler a von p. Es gibt ein b mit $p = ab$. Weil (p) prim ist muß p a oder b teilen. Wenn p a teilt, sind a und p äquivalent. Sonst sind b und p äquivalent, woraus in Integritätsbereichen folgt, daß a eine Einheit ist.

Für von Null verschiedene p gelten die folgenden Implikationen.

$$(p) \text{ maximal} \underset{\text{Hauptidealringe}}{\overset{\longrightarrow}{\longleftarrow}} (p) \text{ prim} \underset{\text{faktorielle Ringe}}{\overset{\text{Integritätsbereiche}}{\longleftarrow}} p \text{ irreduzibel}$$

In faktoriellen Ringen bildet $R/\!\sim$ mit der Teilbarkeitsrelation einen Verband. Das Infimum von

$$a = \epsilon \prod_{i \in I} p_i^{m_i} \quad \text{und} \quad b = \delta \prod_{i \in I} p_i^{n_i}$$

ist der (bis auf Äquivalenz eindeutig bestimmte) größte gemeinsame Teiler

$$\operatorname{ggT}(a, b) = (a, b) = \prod_{i \in I} p_i^{\min(m_i, n_i)}.$$

Das Supremum ist das kleinste gemeinschaftliche Vielfache

$$\operatorname{kgV}(a, b) = \prod_{i \in I} p_i^{\max(m_i, n_i)}.$$

Es ist $\operatorname{ggT}(a, 0) = a$, $\operatorname{ggT}(a, 1) = 1$, $\operatorname{kgV}(a, 0) = 0$ und $\operatorname{kgV}(a, 1) = a$.
Man definiert den ggT und kgV von mehr als zwei Ringelementen sinngemäß.

Weil $Ra + Rb$ das kleinste Ideal ist, das (a) und (b) enthält, und $Ra \cap Rb$ das größte Ideal, das in (a) und (b) enthalten ist, ist in Hauptidealringen

$$R \operatorname{ggT}(a, b) = Ra + Rb \quad \text{und} \quad R \operatorname{kgV}(a, b) = Ra \cap Rb.$$

In Hauptidealringen sind also von teilerfremden Elementen erzeugte Ideale teilerfremd. Das ist für faktorielle Ringe nicht mehr richtig. Wir werden gleich sehen, daß für jeden Körper K der Polynomring $K[X_1, X_2]$ faktoriell ist. X_1 und X_2 sind teilerfremd, die beiden Ideale (X_1) und (X_2) aber nicht. Denn ihre Summe kann keine Polynome enthalten, die einen nicht–verschwindenden konstanten Koeffizienten haben.

Wenn R faktoriell ist und die p_i ein Vertretersystem der irreduziblen Elemente von R, läßt sich jedes von Null verschiedene Element des Quotientenkörper K eindeutig in der Form

$$\epsilon \prod_{i \in I} p_i^{e_i} \ ,$$

mit einer Einheit ϵ und *ganzen* Zahlen e_i schreiben. Der Begriff der Teilbarkeit läßt sich sinnvoll auf K fortsetzen. Man definiert für $b, a \in K$

$$a|b$$

wenn $b \in Ra$. Es ist also

$$R = \{x \in K \mid 1|x\}.$$

Die Begriffe ggT und kgV übertragen sich unmittelbar auf Elemente[8] von K. Wir merken uns die Regel

$$\text{ggT}(xa, xb) = x\,\text{ggT}(a, b) \tag{2.1}$$

Satz 2.6.3 *Wenn R faktoriell ist, ist auch $R[X]$ faktoriell.*

Folgerung 2.6.4 *Für jeden Körper K ist $K[X_1, \ldots, X_n]$ faktoriell.*

Beweis (von 2.6.3):
K sei der Quotientenkörper von R. Wir definieren den *Inhalt eines Polynoms f* aus $K[X]$ als den größten gemeinsamen Teiler der Koeffizienten:

$$\text{Inhalt}(a_n X^n + \ldots + a_0) = \text{ggT}(a_n, \ldots, a_0).$$

f gehört genau dann zu $R[X]$, wenn sein Inhalt zu R gehört. Ein Polynom heißt *primitiv*, wenn $\text{Inhalt}(f) = 1$. Aus 2.1 folgt, daß (in $K[X]$) jedes Polynom zu einem primitiven Polynom äquivalent ist.

Sei $(f_i)_{i\in I}$ ein Repräsentantensystem für die Äquivalenzklassen irreduzibler Polynome aus $K[X]$. Wir haben gerade gesehen, daß wir annehmen können, daß die f_i primitiv sind. Die f_i sind dann irreduzibel in $R[X]$, weil jeder Teiler $r \in R$ von f_i den Inhalt von f_i teilen muß und also eine Einheit sein muß.

Sei $g \in R[X] \setminus \{0\}$. Weil $K[X]$ faktoriell ist, läßt sich g eindeutig als

$$g = r \prod_{i\in I} f_i^{e_i} \tag{2.2}$$

für ein $r \in K$ schreiben. Aus dem nächsten Lemma folgt, daß r gleich dem Inhalt von g ist und also zu R gehören muß. Daraus folgt, daß sich g eindeutig in Potenzen der f_i und in irreduzible Elemente von R zerlegt.

Lemma 2.6.5 (Gauß[9]) *Das Produkt von primitiven Polynomen ist primitiv.*

Beweis :
f und g seien primitiv und p ein irreduzibles Element von R. Wir bezeichnen mit $\overline{f}, \overline{g}$ und $\overline{fg}$ die homomorphen Bilder von f, g und fg in $R/(Rp)[X]$. Weil f und g primitiv sind, sind $\overline{f}$ und $\overline{g}$ ungleich Null. $R/(Rp)$ ist aber ein Integritätsbereich, woraus folgt, daß $\overline{f}\,\overline{g} = \overline{fg}$ ungleich Null ist. Das bedeutet, daß p den Inhalt von fg nicht teilt.

Damit haben wir gesehen, daß der Inhalt von fg keinen irreduziblen Faktor hat. fg ist also primitiv. □

[8] Man sollte aber nicht vergessen, daß ggT und kgV nicht nur von K, sondern von R abhängen!

[9] Karl Friedrich Gauß (1777-1855)

Kapitel 3

Körper

3.1 Grundlagen

Sei K ein Körper. Der Durchschnitt aller Unterkörper von K ist der kleinste Unterkörper von K, der *Primkörper* von K.

Satz 3.1.1 *Der Primkörper von K ist entweder isomorph zu $\mathbb{Q}$ oder isomorph zu $\mathbb{F}_p$ für eine Primzahl p.*

Beweis :
Betrachte den kanonischen Ringhomomorphismus

$$\pi : \mathbb{Z} \to K,$$

der z auf $z \cdot 1$ abbildet. Das Bild ist der kleinste Unterring $\mathbb{Z} \cdot 1$ von K, ein Integritätsbereich. Der Kern von π ist also ein Primideal von $\mathbb{Z}$. Es gibt zwei Fälle

1. $\ker(\pi) = 0$. Dann ist $\mathbb{Z} \cdot 1$ isomorph zu $\mathbb{Z}$. Der Primkörper ist dann der Quotientenkörper von $\mathbb{Z} \cdot 1$ und isomorph zu $\mathbb{Q}$.
2. $\ker(\pi) = \mathbb{Z}p$ für eine Primzahl p. Dann ist $\mathbb{Z} \cdot 1 \cong \mathbb{F}_p$ der Primkörper.

□

Wenn der Primkörper $\mathbb{Q}$ ist, sagen wir, daß K die *Charakteristik* 0 oder unendliche Charakteristik hat. Wenn der Primkörper $\mathbb{F}_p$ ist, ist p die Charakteristik. Die Charakteristik von K ist also die Ordnung von 1 in der additiven Gruppe von K.

Eine *Körpererweiterung*

$$K/k$$

besteht aus einem Körper K und einem Unterkörper k. Zwei Körpererweiterungen K/k und K'/k heißen isomorph (über k), wenn es einen Isomorphismus $\phi : K \to K'$ gibt, der auf k identisch operiert.

Sei $a_1, \ldots, a_n$ eine Folge von Elementen von K. Wir bezeichnen mit

$$k[a_1, \ldots, a_n] = \{f(a_1, \ldots, a_n) \mid f \in k[X_1, \ldots, X_n]\}$$

den von k und $a_1, \ldots, a_n$ erzeugten Teilring von K und mit

$$\begin{aligned} k(a_1, \ldots, a_n) &= \mathrm{Quot}(k[a_1, \ldots, a_n]) \\ &= \left\{ \frac{f(a_1, \ldots, a_n)}{g(a_1, \ldots, a_n)} \middle| f, g \in k[X_1, \ldots, X_n], g(a) \neq 0 \right\} \end{aligned}$$

den von k und $a_1, \ldots, a_n$ erzeugten Unterkörper.

K heißt *einfach*, wenn $K = k(a)$ für ein $a \in K$. a heißt dann *primitives* Element von (K/k).

Definition *Ein Element $a \in K$ heißt algebraisch über k, wenn a Nullstelle eines von Null verschiedenen Polynoms $f \in k[X]$. Wenn a nicht algebraisch ist, heißt a transzendent über k.*

Sei f ein irreduzibles Polynom aus $k[X]$. Weil (f) maximal ist und k nur in 0 schneidet, ist $K = k[X]/(f)$ ein Oberkörper von k. Sei a die Nebenklasse $X+(f)$ von X. Dann ist $K = k[a] = k(a)$ und a ist eine Nullstelle von f, denn

$$f(a) = f(X + (f)) = f(X) + (f) = (f).$$

Satz 3.1.2 *Sei K/k eine einfache Körpererweiterung mit primitivem Element a.*

1. *Wenn a algebraisch ist, ist $K \cong k[X]/(f)$ für ein eindeutig bestimmtes normiertes Polynom f in $k[X]$. f ist irreduzibel und heißt das* Minimalpolynom *von a über k.*
2. *Wenn a transzendent über k ist, ist K über k isomorph zum rationalen Funktionenkörper $k(X)$.*

Beweis :
Betrachte den Einsetzungshomomorphismus $\pi : f(X) \mapsto f(a)$. $k[a]$ ist das Bild von π und der Kern I besteht aus allen Polynomen $f \in k[X]$, die a als Nullstelle haben. Nach dem Homomorphiesatz ist $k[a] \cong k[X]/I$.

Wenn $I = 0$, ist a transzendent über k und $k[a] \cong k[X]/0 = k[X]$. $k(a)$ ist als Quotientenkörper von $k[a]$ isomorph zu $k(X)$.

Wenn $I \neq 0$, wird I von einem (eindeutig bestimmten) normierten Polynom f erzeugt. Weil $k[a]$ ein Integritätsbereich ist, ist (f) prim und daher f irreduzibel. Es folgt, daß (f) maximal ist. Das heißt, daß $k[a]$ schon ein Körper ist: $K = k[a]$. □

Sei $f \in k[X] \setminus 0$ und I ein Primideal von $k[X]$. Dann ist $I = (f)$ genau dann, wenn eine der folgenden äquivalenten Bedingungen erfüllt sind:

- f ist Polynom von minimalen Grad in $I \setminus 0$.
- f ist irreduzibel und gehört zu I.

Wenn a Element eines Oberkörpers ist, und f normiert, ist f genau dann Minimalpolynom von a über k, wenn

- a Nullstelle von f ist und f unter diesen Polynomen minimalen Grad hat.

  Oder äquivalent:

- wenn a Nullstelle von f und f irreduzibel ist.

Sei

$$K \subset L$$

eine Körpererweiterung. Dann ist L auf natürliche Weise ein K–Vektorraum L_K. Die Dimension dieses Vektorraums ist der *Grad* der Körpererweiterung:

$$[L : K] = \dim_K L$$

Beispiel:
Die Monome $1, X, X^2, \ldots$ bilden eine Basis von $k[X]$ über k. $k(X)$ hat also unendlichen Grad über k.

Beispiel:
Sei $f \in k[X]$ ein normiertes irreduzibles Polynom von Grad n. Wegen 2.3.2 läßt sich jedes Element von $k[X]/(f)$ durch ein eindeutig bestimmtes Polynom von kleinerem Grad repräsentieren. Die Nebenklassen von $1, X, \ldots, X^{n-1}$ bilden also eine Basis von $k[X]/(f)$ über k. Es folgt, daß

$$[k(a) : k] = n,$$

wenn a algebraisch über k ist und n der Grad des Minimalpolynoms.

Satz 3.1.3 *Sei*

$$F \subset K \subset L$$

ein Turm von Körpererweiterungen. Dann ist

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

Beweis :
Aus einer Basis $(a_i)_{i \in I}$ von K_F und einer Basis $(b_j)_{j \in J}$ von L_K gewinnt man eine Basis $(a_i b_j)_{(i,j) \in I \times J}$ von L_F. Denn jedes Element l von L läßt sich eindeutig schreiben als

$$l = \sum_{j \in J} k_j b_j$$

und die k_j lassen sich eindeutig schreiben als

$$k_j = \sum_{i \in I} f_{i,j} a_i.$$

Wir erhalten eine eindeutige Darstellung

$$l = \sum_{(i,j)\in I\times J} f_{i,j} a_i b_j.$$

□

Definition *Eine Körpererweiterung K/k heißt algebraisch, wenn jedes Element von K algebraisch über k ist und endlich, wenn $[K : k]$ endlich ist.*

Satz 3.1.4 *Sei K/k eine Körpererweiterung. Dann sind äquivalent:*

a) K/k ist endlich.

b) K/k ist endlich erzeugt und algebraisch.

c) K/k wird von endlich vielen über k algebraischen Elementen erzeugt.

Beweis :

a→b Wenn K/k endlich ist, ist K als k–Vektorraum, erst recht also als Körpererweiterung von k endlich erzeugt. Für jedes $a \in K$ ist $[k(a) : k]$ endlich, a also algebraisch über k.

b→c klar

c→a Sei $K = k(a_1, \ldots, a_n)$ für a_i, die algebraisch über k sind. Dann sind alle Erweiterungen

$$k(a_1, \ldots, a_{i+1})/k(a_1, \ldots, a_i)$$

endlich. Mit 3.1.3 folgt, daß K/k endlich ist.

Folgerung 3.1.5 *Sei $F \subset K \subset L$ ein Körperturm. Wenn die Erweiterungen L/K und K/F algebraisch sind, ist auch L/F algebraisch.*

Beweis :
Sei a ein Element von L und f das Minimalpolynom von a über K. Sei K' die von den Koeffizienten von f erzeugte Erweiterung von F. Dann ist mit $K'(a)/K'$ und K'/F auch $K'(a)/F$ endlich. Es folgt, daß a algebraisch über F ist. □

3.2 Der algebraische Abschluß

Ein Körper K heißt *algebraisch abgeschlossen* , wenn jedes nicht–konstante Polynom aus $K[X]$ eine Nullstelle hat. Aus 2.3.3 folgt, daß K genau dann algebraisch abgeschlossen ist, wenn jedes normierte Polynom $f \in K[X]$ in Linearfaktoren zerfällt:

$$f(X) = (X - \alpha_1) \dots (X - \alpha_n).$$

$\alpha_1, \dots, \alpha_n$ sind (mit ihrer Vielfachheit gezählt) die Nullstellen von f.

Definition *Eine algebraisch abgeschlossener, algebraischer Erweiterungskörper K von k heißt algebraischer Abschluß von k.*

Satz 3.2.1 *Jeder Körper k hat einen algebraischen Abschluß K. K ist bis auf Isomorphie über k eindeutig bestimmt.*

Beweis :

Existenz

Wir bemerken zunächst, daß es zu je endlich vielen nicht–konstanten Polynomen $f_1, \dots, f_n \in k[X]$ einen Oberkörper F von k gibt, in dem $f_1, \dots, f_n$ Nullstellen haben: Wir wählen einen irreduziblen Faktor $g_1 \in k[x]$ von f_1 und setzen $k_1 = k[X]/(g_1)$. Dann hat g_1 und damit f_1 eine Nullstelle in k_1. Dann erweitern wir k_1 zu einem Körper k_2, der eine Nullstelle von f_2 enthält und so weiter.

Sei $\{f_i \mid i \in I\}$ die Menge aller nicht–konstanten Polynome aus $k[X]$. Sei I das im Polynomring

$$R = k[X_i]_{i \in I}$$

von den Polynomen $f_i(X_i)$ erzeugte Ideal. Wir zeigen, daß I ein echtes Ideal ist: Sonst gibt es Polynome $f_{i_1}(X_{i_1}), \dots, f_{i_n}(X_{i_n})$ aus denen sich 1 kombinieren läßt:

$$1 = g_1 f_{i_1}(X_{i_1}) + \dots + g_n f_{i_n}(X_{i_n}) \tag{3.1}$$

$(g_1, \dots, g_n \in R)$. Sei F ein Oberkörper von k, in dem $f_{i_1}(X), \dots, f_{i_n}(X)$ Nullstellen $\alpha_1, \dots, \alpha_n$ haben. Wenn wir die $X_{i_1}, \dots, X_{i_n}$ durch $\alpha_1, \dots, \alpha_n$ und die übrigen Variablen (zum Beispiel) durch 0 ersetzen, wird die rechte Seite von in 3.1 Null, was nicht möglich ist.

Wir können also I zu einem maximalen Ideal M erweitern. $K_1 = R/M$ ist ein Oberkörper von k und wird über k von den Nebenklassen $X_i + M$ erzeugt, die jeweils Nullstelle von f_i sind. Man konstruiert ebenso einen algebraischen Oberkörper K_2 von K_1, in dem alle nicht–konstanten Polynome aus $K_1[X]$ eine Nullstelle haben, und so weiter. Die Vereinigung der Kette

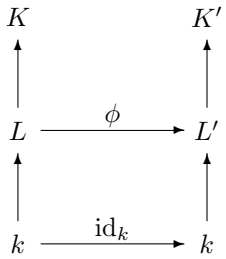
$$K_1 \subset K_2 \subset K_3 \dots$$

ist algebraisch über k und algebraisch abgeschlossen.

Eindeutigkeit

Sei K' ein zweiter algebraischer Abschluß von k. Sei $\phi : L \to L'$ ein maximaler

Isomorphismus zwischen zwei Zwischenkörpern L und L'. (Man findet ϕ mit Zorns Lemma.)



Um zu zeigen, daß $L = K$ betrachten wir ein Element $a \in K$. Sei

$$f = a_0 + a_1 X + \ldots + X^n$$

das Minimalpolynom von a über L und

$$\phi(f) = \phi(a_0) + \phi(a_1)X + X^n$$

das Bild von f in $L'[X]$. Sei a' eine Nullstelle von $\phi(f)$ in K'. Weil $\phi(f)$ das Minimalpolynom von a' über L' ist, kann man ϕ zu einem Isomorphismus $L(a) \to L'(a')$ fortsetzen. Wegen der Maximalität von ϕ ist $L(a) = L$. Ebenso (durch Vertauschen der Seiten) zeigt man, daß $L' = K'$. □

Wir bezeichnen den *algebraischen* Abschluß von k mit $\widetilde{k}$.

Folgerung 3.2.2 *Jede algebraische Erweiterung K von k läßt sich über k isomorph in den algebraischen Abschluß $\widetilde{k}$ einbetten.*

Beweis :
$\widetilde{K}$ ist auch algebraischer Abschluß von k. □

Sei $\phi : K \to L$ ein Isomorphismus über k von zwei Zwischenkörpern $k \subset K, L \subset \widetilde{k}$. Weil $\widetilde{k}$ algebraischer Abschluß von K und L ist, läßt sich ϕ zu einem Automorphismus $\widetilde{\phi}$ von $\widetilde{k}$ über k fortsetzen. Wir bezeichnen die Gruppe dieser Automorphismen mit $\mathrm{Aut}(\widetilde{k}/k)$. Allgemein bezeichnen wir die Gruppe aller Automorphismen von F, die alle Elemente des Unterkörpers k fixieren, mit

$$\mathrm{Aut}(F/k).$$

Sei f ein normiertes Polynom in $k[X]$. In $\widetilde{k}[X]$ zerfällt f in Linearfaktoren

$$f(X) = (X - \alpha_1) \ldots (X - \alpha_n).$$

Wir nennen $k(\alpha_1, \ldots, \alpha_n)$ den *Zerfällungskörper* von f über k.

Satz 3.2.3 *Eine endliche Körpererweiterung K/k (in $\widetilde{k}$) ist genau dann ein Zerfällungskörper, wenn sie* normal *ist: Jedes $\phi \in \mathrm{Aut}(\widetilde{k}/k)$ bildet K auf sich ab.*

Beweis :
Zerfällungskörper sind normal, weil jedes $\phi \in \mathrm{Aut}(\widetilde{k}/k)$ die Menge der Nullstellen von f auf sich abbildet.
Sei K/k normal. Wir wählen ein Erzeugendensystem

$$K = k(b_1, \ldots, b_k).$$

Für jedes b_i sei f_i das Minimalpolynom von b_i über k. Für jede Nullstelle α von f_i ist

$$k(b_i) \cong k(\alpha).$$

Es gibt also ein $\phi \in \mathrm{Aut}(\widetilde{k}/k)$, das b_i auf α abbildet und es folgt $\alpha \in K$. K enthält also alle Nullstellen der f_i und ist daher der Zerfällungskörper von

$$f = f_1 \ldots f_k.$$

□

3.3 Separable Erweiterungen

Satz 3.3.1 *Sei K/k eine endliche Körpererweiterung. Dann gibt es höchstens $[K : k]$ viele isomorphe Einbettungen von K in $\widetilde{k}$ über k.*

Wenn wir den *Separabilitätsgrad* $[K : k]_s$ als die Zahl aller isomorphen Einbettungen von K in $\widetilde{k}$ über k definieren, schreibt sich der Satz als

$$[K : k]_s \leq [K : k].$$

Zum Beweis zeigen wir zuerst

Lemma 3.3.2 *Für jeden Körperturm*

$$F \subset K \subset L$$

ist

$$[L : K]_s[K : F]_s = [L : F]_s.$$

Beweis :
Wir können annehmen, daß K ein Unterkörper von $\widetilde{F}$ ist. $\phi_1, \ldots, \phi_m$ seien die Einbettungen von K in $\widetilde{F}$ über F. Wir setzen jedes ϕ_i zu einem $\widetilde{\phi}_i \in \mathrm{Aut}(\widetilde{F}/F)$ fort. Weiterhin seien $\psi_1, \ldots, \psi_n$ alle Einbettungen von L in $\widetilde{F}$ über K. Dann ist

$$\widetilde{\phi}_i\psi_j \quad (i = 1, \ldots, m; j = 1, \ldots, n)$$

eine wiederholungsfreie Aufzählung aller Einbettungen von L in $\widetilde{F}$ über F. □

Beweis von 3.3.1:
Wenn $K = k(a)$ eine einfache algebraische Erweiterung ist, liefert jede Nullstelle $b \in \widetilde{k}$ des Minimalpolynoms f von a über k eine isomorphe Einbettung $K \to k(b) \subset \widetilde{k}$, die a auf b abbildet. Es ist also

$$[k(a) : k]_s = \text{Zahl der Nullstellen von } f \leq \deg(f) = [k(a) : k].$$

Für eine beliebige endliche Erweiterung

$$K = k(a_1, \ldots, a_n)$$

folgt die Behauptung aus

$$[K(a_1, \ldots, a_{i+1}) : K(a_1, \ldots, a_i)]_s \leq [K(a_1, \ldots, a_{i+1}) : K(a_1, \ldots, a_i)]$$

mit 3.1.3 und 3.3.2. □

Definition *Eine endliche Körpererweiterung K/k heißt separabel, wenn*

$$[K : k]_s = [K : k].$$

Aus 3.1.3 und 3.3.2 folgt sofort

Folgerung 3.3.3 *Für jeden Körperturm*

$$F \subset K \subset L$$

gilt: L/F ist genau separabel, wenn L/K und K/F separabel sind. □

Definition *a heißt separabel über k, wenn $k(a)/k$ separabel ist.*

Eine einfache algebraische Körpererweiterung $k(a)/k$ ist separabel, wenn das Minimalpolynom f von a über k keine doppelten Nullstellen hat (in $\widetilde{k}$), das heißt, daß in der Zerlegung (in $\widetilde{k}[X]$)

$$f(X) = (X - \alpha_1) \dots (X - \alpha_n)$$

alle α_i verschieden sind. Wir nennen nicht–konstante Polynome ohne doppelte Nullstellen *separabel*.

Folgerung 3.3.4 *Sei K/k eine endliche Körpererweiterung. Dann sind äquivalent*

a) K/k ist separabel

b) Alle Elemente von K sind separabel über k

c) $K = k(a_1, \dots, a_n)$ für Elemente a_i, die separabel über k sind.

Beweis :
a→b und b→c folgen aus 3.3.3 und 3.1.4.

Wenn $a_1, \dots, a_n$ separabel über k sind, ist jedes a_i auch separabel über $k(a_1, \dots, a_{i-1})$. Das Minimalpolynom von a_i über $k(a_1, \dots, a_{i-1})$ kann nämlich als Teiler des Minimalpolynoms von a_i über k keine doppelten Nullstellen haben. Jetzt folgt aus 3.3.3, daß K/k separabel ist. Damit ist c→a bewiesen. □

Definition *Für Polynome*

$$f(X) = a_0 + a_1 X + \ldots + a_n X^n$$

definieren wir die Ableitung durch

$$f'(X) = a_1 + \ldots + n a_n X^{n-1}.$$

Man verifiziert leicht die Rechenregeln

1. $f' = 0$, wenn f konstant ist.
2. $(f + g)' = f' + g'$
3. $(fg)' = f'g + fg'$

Lemma 3.3.5 *Ein nicht–konstantes Polynom f ist genau dann separabel, wenn f und f' teilerfremd sind.*

In Körpern der Charakteristik p kann auch für nicht konstante f die Ableitung f' Null sein. Zum Beispiel ist

$$(X^p - b)' = 0.$$

f und f' haben dann den gemeinsamen Teiler f.

Beweis :
Wenn

$$f(X) = (X - \alpha_1) \dots (X - \alpha_n),$$

ist

$$f'(X) = \sum_{i=1}^{n} \prod_{j \neq i} (X - \alpha_j).$$

f und f' sind genau dann nicht teilerfremd in $\widetilde{k}[X]$, wenn einer der Faktoren $(X - \alpha_i)$ die Ableitung f' teilt. $(X - \alpha_1)$ zum Beispiel teilt f' genau dann, wenn es $(X - \alpha_2) \dots (X - \alpha_n)$ teilt, das heißt, wenn $\alpha_1 = \alpha_j$ für ein $j \neq 1$.
Die Behauptung folgt nun aus der folgenden allgemeinen Bemerkung:

Bemerkung *Sei $f, g \in k[X]$ und K ein Oberkörper von k. Dann ist der größte gemeinsame Teiler $h = \mathrm{ggT}(f, g)$ von f und g in $k[X]$ auch größter gemeinsamer Teiler in $K[X]$.*

Das folgt leicht daraus, daß in Hauptidealringen a genau dann der ggT von b und c ist, wenn a ein gemeinsamer Teiler von b und c ist und a sich als $a = xb + yc$ darstellen läßt. □

Folgerung 3.3.6 *Ein irreduzibles Polynom hat genau dann mehrfache Nullstellen, wenn seine Ableitung das Nullpolynom ist.* □

Wenn $f' = 0$ für ein nicht–konstantes Polynom, muß die Charakteristik p von K endlich sein und f hat die Form $g(X^p)$.

Folgerung 3.3.7 *In der Charakteristik Null sind alle endlichen Körpererweiterungen separabel.*

Satz 3.3.8 (Satz vom primitiven Element) *Endliche separable Erweiterungen sind einfach erzeugt.*

Beweis :
Sei K eine (in $\widetilde{k}$ enthaltene) separable Erweiterung von k. Wir betrachten für jeden Zwischenkörper L die Menge

$$\Phi_L = \left\{ \phi : K \to \widetilde{k} \;\middle|\; \phi \text{ fixiert die Elemente von } L \right\}$$

aller Einbettungen von K in $\widetilde{k}$ über L. Weil K separable Erweiterung von L ist, gilt

$$|\Phi_L| = [K : L].$$

Wir können L durch

$$L = \{x \in K \mid \phi(x) = x \text{ für alle } \phi \in \Phi_L\}$$

aus Φ_L zurückgewinnen, denn $L' = \{x \in K \mid \phi(x) = x \text{ für alle } \phi \in \Phi_L\}$ ist ein Oberkörper von L mit $\Phi_{L'} = \Phi_L$. Es folgt $[K : L'] = [K : L]$ und daraus $L' = L$.

Wir haben damit gezeigt, daß es nur endlich viele ($\leq 2^{[K:k]}$) Zwischenkörper gibt. Den Fall, daß k endlich ist, behandeln wir im nächsten Abschnitt (3.4.5). Wenn k unendlich ist, folgt aus dem nächsten Lemma, daß K ein Element a hat, das in keinem echten Zwischenkörper liegt. Das heißt aber, daß $K = k(a)$. □

Lemma 3.3.9 *Sei V ein Vektorraum über einem unendlichen Körper k. Dann ist V nicht Vereinigung von endlich vielen echten Unterräumen.*

Beweis :
Lineare Algebra. □

3.4 Endliche Körper

Endliche Körper haben endliche Charakteristik. Wir betrachten in diesem Abschnitt ab jetzt nur Körper der Charakteristik $p \neq 0$.

Lemma 3.4.1 *Sei K ein Körper der Charakteristik p. Dann ist die* Frobeniusabbildung

$$x \mapsto x^p$$

eine isomorphe Abbildung von K auf einen Unterkörper von K.

Beweis :
Es gilt natürlich $(xy)^p = x^p y^p$ und

$$(x+y)^p = x^p + \binom{p}{1} x^{p-1}y + \ldots + \binom{p}{p-1} xy^{p-1} + y^p = x^p + y^p,$$

weil die Binomialkoeffizienten $\binom{p}{1}, \ldots, \binom{p}{p-1}$ durch p teilbar sind. Die Frobeniusabbildung ist injektiv. Denn wenn $a^p = b$, hat das Polynom

$$X^p - b = (X-a)^p$$

nur die (p–fache) Nullstelle a. □

Für jedes $q = p^n$ ist $x \mapsto x^q$ ebenfalls ein Isomorphismus, die n–te Potenz des Frobeniusisomorphismus.

Ein Körper K heißt *perfekt*, wenn jedes Element eine p–te Potenz ist[1]. Algebraisch abgeschlossene Körper und endliche Körper sind perfekt. In perfekten Körpern ist die Frobeniusabbildung ein Automorphismus. Endliche Erweiterungen perfekter Körper sind immer separabel. Denn inseparable irreduzible Polynome haben die Form $g(X^p)$. In perfekten Körpern sind solche Polynome p–te Potenzen und können nicht irreduzibel sein.

Sei K ein endlicher Körper der Charakteristik p und n der Grad von K über dem Primkörper $\mathbb{F}_p$. K hat dann p^n Elemente.

Satz 3.4.2 *Für jedes $q = p^n$ ($n \geq 1$) gibt es genau einen endlichen Körper $\mathbb{F}_q$ mit q Elementen. $\mathbb{F}_q$ ist der Zerfällungskörper von $X^q - X$ über $\mathbb{F}_p$*

Beweis :
Die multiplikative Gruppe eines Körpers mit q Elementen hat die Ordnung $q-1$. Also ist $a^{q-1} = 1$ für alle $a \in K^*$ und $a^q - a = 0$ für alle $a \in K$. K besteht also gerade aus allen Nullstellen von $X^q - X$ und ist also auch der Zerfällungskörper. Sei umgekehrt q gegeben und

$$N = \{x \in \widetilde{\mathbb{F}_p} \mid x^q = x\}.$$

[1] Körper der Charakteristik 0 werden ebenfalls perfekt genannt

Weil $(X^q - X)' = -1$ hat $X^q - X$ keine doppelten Nullstellen. Also hat N genau q Elemente. Auf der anderen Seite besteht N aus den Fixpunkten des Automorphismus $x \mapsto x^q$ und ist daher ein Körper. □

Sei Φ der Frobeniusautomorphismus von $\mathbb{F}_{p^n}$ und m ein Teiler von n. Dann besteht $\mathbb{F}_{p^m}$ aus den Elementen von $\mathbb{F}_{p^n}$, die von Φ^m fixiert werden. Weil n der kleinste Index i ist, für den Φ^i alle Elemente von $\mathbb{F}_{p^n}$ fixiert, sind alle Automorphismen $\Phi^0, \Phi^m, \ldots, \Phi^{(\frac{n}{m}-1)m}$ verschieden. Weil andererseits $\mathrm{Aut}(\mathbb{F}_{p^n}/\mathbb{F}_{p^m})$ höchstens $\frac{n}{m}$ Elemente hat, folgt

Folgerung 3.4.3 *$\mathbb{F}_{p^n}$ ist eine separable Erweiterung von $\mathbb{F}_{p^m}$. $\mathrm{Aut}(\mathbb{F}_{p^n}/\mathbb{F}_{p^m})$ ist isomorph zu $\mathrm{Z}_{\frac{n}{m}}$ und wird erzeugt von Φ^m.*

Lemma 3.4.4 *Sei K ein Körper und G eine endliche Untergruppe von K^*. Dann ist G zyklisch.*

Beweis :
Wenn G nicht zyklisch ist, enthält G eine nicht–zyklische q–Gruppe S für eine Primzahl q.[2] Der Sockel $\{s \in S \mid s^q = 1\}$ hat mindestens q^2 viele Elemente. In einem Körper kann aber die Gleichung $X^q - 1 = 0$ höchstens q Lösungen haben. □

Folgerung 3.4.5 *Die multiplikative Gruppe endlicher Körper ist zyklisch.*

Insbesondere sind endliche Körper einfach erzeugt über ihrem Primkörper.

[2]Sonst ist zum Beispiel $G = \mathrm{Z}_2^3 \oplus \mathrm{Z}_3^2 \oplus \mathrm{Z}_5 \cong \mathrm{Z}_{360}$.

3.5 Galoistheorie

Definition *Eine endliche Körpererweiterung K/k heißt galoissch*[3] *, wenn sie normal und separabel ist. Die Gruppe* $\mathrm{Aut}(K/k)$ *aller Automorphismen von K über k heißt Galoisgruppe von K über k.*

Über Körpern der Charakteristik 0 (oder allgemeiner über perfekten Körpern) sind also alle Zerfällungskörper galoissch. Wenn F ein Zwischenkörper ist, ist auch die Erweiterung K/F galoissch.

Satz 3.5.1 (Hauptsatz der Galoistheorie) *Sei K eine galoissche Erweiterung von k. Die Abbildung*

$$F \longmapsto \mathrm{Aut}(K/F)$$

liefert eine Bijektion zwischen der Menge der Zwischenkörper von K/k und der Menge der Untergruppen der Galoisgruppe $\mathrm{Aut}(K/k)$*. Die Umkehrabbildung wird gegeben durch*

$$G \longmapsto \mathrm{Fix}(G),$$

wobei

$$\mathrm{Fix}(G) = \{x \in K \mid \phi(x) = x \textit{ für alle } \phi \in G\}$$

der Fixkörper *von G ist.*

Beweis :
Daß $F = \mathrm{Fix}(\mathrm{Aut}(K/F))$, wurde schon im Beweis von 3.3.8 gezeigt. (Der Grund war, daß

$$|\mathrm{Aut}(K/F')| = [K : F'] \tag{3.2}$$

für alle Zwischenkörper F'.)
Es bleibt noch zu zeigen, daß jede Untergruppe G von $\mathrm{Aut}(K/k)$ von der Form $\mathrm{Aut}(K/F)$ für einen Zwischenkörper F ist. Wir machen dafür natürlich den Ansatz $F = \mathrm{Fix}(G)$. Klar ist zunächst, daß $G \leq \mathrm{Aut}(K/F)$. Wenn wir zeigen können, daß $|G| \geq [K : F]$, folgt aus 3.2 die Gleichheit.

Sei a ein primitives Element der Körpererweiterung K/k :

$$K = k(a)$$

Die Menge

$$\{\phi(a) \mid \phi \in G\}$$

der G–Konjugierten von a ist invariant unter den Automorphismen von G. Also werden auch die Koeffizienten von

$$f(X) = \prod_{\phi \in G} (X - \phi(a))$$

von allen $\phi \in G$ festgehalten. Das heißt $f \in F[X]$. Weil a Nullstelle von f ist, hat das Minimalpolynom von a über F höchstens den Grad

$$\deg(f) = |G| .$$

[3] Evariste Galois (1811-1832)

Also ist $[K : F] \leq |G|$. Damit ist alles bewiesen. □

Der Beweis zeigt auch, daß F über k von den Koeffizienten von f erzeugt wird, und daß f das Minimalpolynom von a über F ist.

Mit dem eben beschriebenen Galoiszusammenhang zwischen Zwischenkörpern F und Untergruppen $\mathrm{Aut}(K/F)$ lassen sich viele Körpereigenschaften in Gruppeneigenschaften übersetzen:
Seien F und F' zwei Zwischenkörper und $G = \mathrm{Aut}(K/F)$ und $G' = \mathrm{Aut}(K/F')$ die zugeordneten Gruppen.

1. Es ist klar, daß $F \subset F'$ genau dann, wenn $G' \leq G$. Der Galoiszusammenhang ist also ein Antiisomorphismus zwischen dem *Verband* der Zwischenkörper und dem Untergruppenverband. Daraus folgt, daß

   $$\mathrm{Aut}(K/(F \cap F')) = \langle G, G' \rangle$$

   und

   $$\mathrm{Aut}(K/(FF')) = G \cap G'.$$

   Dabei bezeichnet FF' den von F und F' erzeugten Unterkörper von K und $\langle G, G' \rangle$ die von $G \cup G'$ erzeugte Untergruppe von $\mathrm{Aut}(K/k)$.

2. Wenn $F \subset F'$, ist

   $$[F' : F] = (G : G')$$

Folgerung 3.5.2 *F sei ein Zwischenkörper der Galoiserweiterung K/k. Dann ist F/k genau dann normal, wenn $\mathrm{Aut}(K/F)$ Normalteiler in $\mathrm{Aut}(K/k)$ ist. Die Einschränkung*

$$\phi \mapsto \phi \restriction F$$

induziert dann einen Isomorphismus zwischen $\mathrm{Aut}(K/k)/\mathrm{Aut}(K/F)$ und $\mathrm{Aut}(F/k)$.

Beweis :
Sei $G = \mathrm{Aut}(K/F)$ und $\phi_0 \in \mathrm{Aut}(K/k)$. Dann gilt

$$\mathrm{Aut}(K/\phi_0(F)) = G^{\phi_0^{-1}}.$$

Denn ein $\phi \in \mathrm{Aut}(K/k)$ fixiert alle $y \in \phi_0(F)$ genau dann, wenn $\phi(\phi_0(x)) = \phi_0(x)$, oder äquivalent: $(\phi_0^{-1} \circ \phi \circ \phi_0)(x) = x$, für alle $x \in F$. Was aber bedeutet, daß $\phi_0^{-1} \circ \phi \circ \phi_0 \in G$, oder äquivalent: $\phi \in \phi_0 G \phi_0^{-1} = G^{\phi_0^{-1}}$.

Wenn F/k normal ist und $\phi \in \mathrm{Aut}(K/k)$, bildet $\phi \restriction F$ den Körper F auf sich ab. Die Einschränkung liefert also einen Homomorphismus

$$\rho : \mathrm{Aut}(K/k) \to \mathrm{Aut}(F/k).$$

ρ ist surjektiv, weil sich jeder Automorphismus von F/k zu einem Automorphismus von K fortsetzen läßt. Der Kern von ρ ist gerade G. □

3.6 Abelsche Körpererweiterungen

Definition *Eine galoissche Körpererweiterung mit abelscher (zyklischer) Galoisgruppe heißt abelsch (zyklisch).*

Die Nullstellen von $X^n - 1$ in K sind die n–ten *Einheitswurzeln* von K. Wenn n nicht durch die Charakteristik p teilbar ist, ist $X^n - 1$ separabel und hat (im algebraischen Abschluß $\widetilde{K}$) n verschieden Nullstellen[4].

Die n–ten Einheitswurzeln bilden eine (nach 3.4.4) zyklische Untergruppe der multiplikativen Gruppe von K. Ein erzeugendes Element ζ der Gruppe der n–ten Einheitswurzeln in $\widetilde{K}$ heißt *primitive* Einheitswurzel. Es ist also

$$X^n - 1 = (X-1)(X-\zeta)(X-\zeta^2)\dots(X-\zeta^{n-1})$$

$K(\zeta)$ ist der Zerfällungskörper von $X^n - 1$ über K.

Lemma 3.6.1 *Sei ζ primitive n–te Einheitswurzel. Dann ist $K(\zeta)/K$ abelsch. Die Galoisgruppe ist kanonisch isomorph zu einer Untergruppe der Einheitengruppe Z_n^* des Rings Z_n.*

Beweis :
Wir nehmen zunächst an, daß n nicht durch die Charakteristik von K teilbar ist. $K(\zeta)/K$ ist dann separabel.
Sei

$$E = \left\{1, \zeta \dots, \zeta^{n-1}\right\}$$

die Gruppe der n–ten Einheitswurzeln. Die Einschränkungsabbildung

$$\mathrm{Aut}(K(\zeta)/K) \to \mathrm{Aut}(E) \tag{3.3}$$

ist ein Homomorphismus, der injektiv ist, weil $K(\zeta)$ über K von E erzeugt wird. Die Behauptung folgt aus der folgenden Bemerkung:

Bemerkung *Sei A eine (additive) zyklische Gruppe der Ordnung n. Dann liefert die Abbildung*

$$\overline{m} \mapsto \textit{Multiplikation mit } m$$

einen Isomorphismus des Rings Z_n mit $\mathrm{End}(A)$. Die Einheitengruppe von Z_n entspricht dabei der Automorphismengruppe von A.

Beweis :
Sei $A = \mathbb{Z}a$ und $\phi \in \mathrm{End}(A)$. Wenn $\phi(a) = ma$, ist

$$\phi(xa) = x(ma) = m(xa)$$

für alle $x \in \mathbb{Z}$. m und m' liefern genau dann den gleichen Endomorphismus, wenn

$$ma = m'a \iff m \equiv m' \pmod{n}.$$

[4] $X^{p^k n} - 1$ hat n verschiedene Nullstellen.

Wenn n nicht teilerfremd zur Charakteristik p ist, zerlegen wir n in ein Produkt aus einer p–Potenz p^k und einer Zahl n', die nicht durch p teilbar ist. Weil ζ auch n'–te Einheitswurzel ist, ist die Galoisgruppe isomorph zu einer Untergruppe von $\mathrm{Z}_{n'}^*$. $\mathrm{Z}_{n'}^*$ wiederum ist isomorph zu einer Untergruppe von $\mathrm{Z}_n^* \cong \mathrm{Z}_{p^k}^* \times \mathrm{Z}_{n'}^*$. □

Wenn n sich in die Primfaktoren $p_1^{e_1} \dots p_k^{e_k}$ zerlegt, ist nach dem Chinesischen Restsatz der Ring Z_n das direkte Produkt der Ringe $\mathrm{Z}_{p^{e_i}}$.
Z_p ist ein Körper. Z_p^* ist daher zyklisch von der Ordnung $p-1$. $\mathrm{Z}_{p^e}^*$ hat die Ordnung $(p-1)p^{e-1}$. Weil Z_p^* homomorphes Bild von $\mathrm{Z}_{p^e}^*$ ist, ist $\mathrm{Z}_{p^e}^*$ isomorph zu einem direkten Produkt von Z_p^* und einer Gruppe der Ordnung[5] p^{e-1}. In der elementaren Zahlentheorie wird diese Gruppe genauer bestimmt: Für alle Primzahlen $p \neq 2$ ist

$$Z_{p^e}^* \cong \mathrm{Z}_{p-1} \oplus \mathrm{Z}_{p^{e-1}}$$

und für $p = 2$

$$Z_{2^e}^* \cong \mathrm{Z}_2 \oplus \mathrm{Z}_{2^{e-2}}.$$

Der folgende Satz zeigt, daß für $K = \mathbb{Q}$ und $n = p^k$ die Abbildung (3.3) ein Isomorphismus ist.

Satz 3.6.2 *Wenn ζ eine primitive p^k–te Einheitswurzel ist, ist*

$$[\mathbb{Q}(\zeta) : \mathbb{Q}] = (p-1)p^{k-1}.$$

Die Körper der Form $\mathbb{Q}(\zeta)$ für Einheitswurzeln ζ heißen *Kreisteilungskörper*.

Beweis :
Weil ζ Nullstelle von

$$f(X) = \frac{X^{p^k} - 1}{X^{p^{k-1}} - 1} = X^{(p-1)(p^{k-1})} + X^{(p-2)(p^{k-1})} + \ldots + 1$$

ist, müssen wir zeigen, daß f irreduzibel ist. Wir zeigen stattdessen, daß $g(X) = f(X+1)$ irreduzibel ist. Nehmen wir an, daß $g(X) = r(X)s(X)$ für zwei normierte Polynome $r, s \in \mathbb{Q}[X]$. Weil $\mathbb{Z}$ faktoriell ist, gehören r und s schon zu $\mathbb{Z}[X]$ (Übung). Wenn wir zu dem homomorphen Bildern $\overline{g}, \overline{r}, \overline{s}$ in $\mathrm{Z}_p[X]$ übergehen, haben wir:

$$\overline{g}(X) = \frac{(X+1)^{p^k} - 1}{(X+1)^{p^{k-1}} - 1} = \frac{X^{p^k}}{X^{p^{k-1}}} = X^{(p-1)(p^{k-1})}.$$

$\overline{r}$ und $\overline{s}$ müssen also beide eine Potenz von X sein. Es folgt insbesondere, daß der konstante Koeffizient von r und s jeweils durch p teilbar ist. Also muß der konstante Koeffizient von g durch p^2 teilbar sein. Der konstante Koeffizient von g ist aber p. [6] □

[5] Nach 1.7.1 ist $\mathrm{Z}_{p^e}^*$ direktes Produkt einer Gruppe der Ordnung $p-1$ und einer Gruppe der Ordnung p^{e-1}.

[6] Das Kriterium von Eisenstein faßt diese Schlußweise zusammen: *Sei $a_0 + a_1X + \ldots + a_nX^n$ ein Polynom mit ganzzahligen Koeffizienten und p sei eine Primzahl. Wenn a_n nicht durch p teilbar ist, alle $a_0, \ldots, a_{n-1}$ durch p teilbar sind, a_0 aber nicht durch p^2, dann ist f irreduzibel in $\mathbb{Q}[X]$.*

Satz 3.6.3 *Sei K ein Körper, der alle n–ten Einheitswurzeln enthält, $a \in K$ und α eine Nullstelle von $X^n - a$. Dann ist $K(\alpha)$ der Zerfällungskörper von $X^n - a$ über K. Wenn n teilerfremd zur Charakteristik ist, ist $K(\alpha)/K$ eine zyklische Erweiterung, deren Ordnung n teilt.*

Beweis :
Sei E die Gruppe der n–ten Einheitswurzeln. Dann ist

$$\{\zeta\alpha \mid \zeta \in E\}$$

die Menge aller Nullstellen von $X^n - a$. $K(\alpha)$ ist also der Zerfällungskörper von $X^n - a$ über K. Wenn n teilerfremd zur Charakteristik ist, gibt es n n–te Einheitswurzeln und $X^n - a$ ist separabel.
Ein Automorphismus $\phi \in \mathrm{Aut}(K(\alpha)/K)$ ist bestimmt durch sein Bild

$$\phi(\alpha) = e\alpha,$$

wobei $e \in E$. Wenn $\phi'(\alpha) = e'\alpha$, ist

$$\phi'(\phi(\alpha)) = \phi'(e\alpha) = e\phi'(\alpha) = ee'\alpha.$$

Die Zuordnung

$$\phi \mapsto e$$

definiert also einen Isomorphismus von $\mathrm{Aut}(K(\alpha)/K)$ mit einer Untergruppe U von E. □

Wir sagen, daß $K(\alpha)$ durch *Adjunktion einer n–ten Wurzel* entsteht.

Satz 3.6.4 *Sei p eine Primzahl, verschieden von der Charakteristik, und K ein Körper, der alle p–ten Einheitswurzeln enthält. Dann entsteht jede zyklische Erweiterung von K vom Grad p durch Adjunktion einer p–ten Wurzel.*

Die Bedingung, daß die Erweiterung zyklisch sei, ist natürlich redundant, weil Gruppen von Primzahlordnung immer zyklisch sind.

Beweis :
Sei L zyklische Erweiterung vom Grad p. ϕ_0 sei erzeugendes Element der Galoisgruppe $\mathrm{Aut}(L/K)$. Wähle ein $\beta \in L \setminus K$ und betrachte die Konjugierten

$$\beta_0 = \beta,\ \beta_1 = \phi_0(\beta), \ldots, \beta_{p-1} = \phi_0^{p-1}(\beta).$$

und das Polynom $f(X) = \beta_0 + \beta_1 X + \ldots + \beta_{p-1}X^{p-1}$. Wenn für alle p–ten Einheitswurzeln ζ die Werte $f(\zeta)$ in K liegen würden, müßte auch f in $K[X]$ liegen[7]. Es gibt also ein $\alpha = f(\zeta)$, das nicht in K liegt. Man hat also $L = K(\alpha)$. Man berechnet nun

$$\phi_0(\alpha) = \beta_1 + \beta_2\zeta + \ldots + \beta_0\zeta^{p-1} = \zeta^{-1}\alpha.$$

[7]Ein Polynom n–ten Grades läßt sich aus seinen Werten $f(a_i) = b_i$ an $n+1$ verschiedenen Stellen $a_0, \ldots, a_n$ berechnen durch die *Interpolationsformel* $f = \sum_{i<n} b_i \prod_{j\neq i} \frac{X-a_j}{a_i-a_j}$. Vergleiche dazu die Folgerung 2.4.4.

Daraus folgt $\phi_0(\alpha^p) = \alpha^p$, woraus wir schließen, daß $\alpha^p \in K$. □

Anhang
Wir beweisen noch eine allgemeinere Form von 3.6.4.

Satz 3.6.5 *K sei ein Körper, der alle n–ten Einheitswurzeln enthält, und n teilerfremd zur Charakteristik. Dann entsteht jede zyklische Erweiterung von K vom Grad n durch Adjunktion einer n–ten Wurzel.*

Beweis :
Sei L zyklische Erweiterung vom Grad n, ϕ ein erzeugendes Element von $\mathrm{Aut}(L/K)$ und ζ eine primitive Einheitswurzel $\zeta \in K$. Die Charaktere

$$\mathrm{id}, \phi, \ldots, \phi^{n-1} : L^* \to L^*$$

sind nach dem nächsten Lemma linear unabhängig. Insbesondere ist

$$\mathrm{id} + \zeta\phi + \cdots + \zeta^{n-1}\phi^{n-1} \neq 0.$$

Es gibt also ein $\beta \in L^*$ für das

$$\alpha = \beta + \zeta\phi(\beta) + \cdots + \zeta^{n-1}\phi^{n-1}(\beta) \neq 0.$$

Man berechnet leicht, daß $\phi(\alpha) = \zeta^{-1}\alpha$ und daher

$$\phi^i(\alpha) = \zeta^{-i}\alpha.$$

Daraus folgt einerseits, daß α von keinem der Automorphismen $\phi, \ldots, \phi^{n-1}$ fixiert wird. Also ist $L = K(\alpha)$. Andererseits folgt wieder $\alpha^n \in L$. □

Sei G eine Gruppe und K ein Körper. Wir nennen Homomorphismen $G \to K^*$ *Charaktere.*

Lemma 3.6.6 (Artins[8]Lemma) *Jede Menge von Charakteren $G \to K$ ist K–linear unabhängig.*

Beweis :
Nehmen wir an die Charaktere $\sigma_1, \ldots, \sigma_n$ wären linear abhängig und sei n minimal gewählt. Sei

$$\alpha_1\sigma_1(g) + \cdots + \alpha_n\sigma_n(g) = 0$$

eine nicht–triviale Relation. Fixiere ein $h \in G$. Wenn man $\beta_i = \sigma_i(h)$ setzt, erhalten wir durch Einsetzen von hg die neue Relation

$$\alpha_1\beta_1\sigma_1(g) + \cdots + \alpha_n\beta_n\sigma_n(g) = 0.$$

Wir subtrahieren das β_n–fache der ersten Gleichung und erhalten

$$\alpha_1(\beta_1 - \beta_n)\sigma_1(g) + \cdots + \alpha_{n-1}(\beta_{n-1} - \beta_n)\sigma_{n-1}(g) = 0.$$

Wenn man h so gewählt hat, daß nicht alle β_i gleich sind, ist die Gleichung nicht–trivial und wir haben einen Widerspruch zu Minimalität von n. □

[8]Emil Artin (1898-1962)

3.7 Anwendungen

3.7.1 Konstruktionen mit Zirkel und Lineal

Wir fassen $\mathbb{C}$ als Zeichenebene auf. Ein Punkt z ist aus einer Menge $E \subset \mathbb{C}$ *konstruierbar*, wenn man von den Punkten aus E ausgehend z mit Zirkel und Lineal konstruieren kann. Wir bezeichnen mit E^{qua} die Menge aller aus E konstruierbaren Punkte.

Lemma 3.7.1 *Sei $E \subset \mathbb{C}$ eine Menge, die 0 und 1 enthält. Dann ist E^{qua} der kleinste Unterkörper K von $\mathbb{C}$, der E enthält und* quadratisch *abgeschlossen ist. Dabei heißt K quadratisch abgeschlossen, wenn jedes Element eine Quadratwurzel in K hat.*

Beweis :
Man kann komplexe Zahlen (mit den Hilfspunkten 0 und 1) leicht geometrisch addieren, multiplizieren und aus ihnen Quadratwurzeln ziehen. Umgekehrt, wenn man den Schnittpunkt von Geraden und Kreisen algebraisch berechnet, genügt es, quadratische Gleichungen zu lösen. □

Folgerung 3.7.2 *Wenn $K \subset \mathbb{C}$ ein Körper ist, dann ist für alle $\alpha \in K^{\mathrm{qua}}$, der Grad $[K(\alpha) : K]$ eine Potenz von 2.*

Beweis :
α liegt in einem Körper, der aus K durch eine Folge von Adjunktionen von Quadratwurzeln entsteht. □

Folgerung 3.7.3

1. **Delisches Problem**
   Aus 2 läßt sich nicht mit Zirkel und Lineal die dritte Wurzel ziehen.
2. **Winkeldreiteilung**
   Es lassen sich nicht alle Winkel mit Zirkel und Lineal dreiteilen.

Beweis :
$X^3 - 2$ ist irreduzibel im $\mathbb{Q}[X]$, weil 2 keine dritte Potenz in $\mathbb{Q}$ ist. Also ist $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$. Eine komplexe Zahl $a \in \mathbb{C}$ der Länge 1, die transzendent ist, liefert einen Winkel, der nicht dreiteilbar ist, weil a keine dritte Potenz in $\mathbb{Q}(a)$ ist. □

Satz 3.7.4 (Gauss) *Das reguläre n–Eck ist genau dann mit Zirkel und Lineal konstruierbar, wenn*

$$n = 2^k p_1 \dots p_l,$$

wobei die p_i paarweise verschiedene Primzahlen der Form $2^i + 1$ (Fermatsche[9] Primzahlen) sind.

[9] Pierre de Fermat (1601-1665)

Beweis :
Das reguläre n–Eck ist genau dann mit Zirkel und Lineal konstruierbar, wenn die primitive n–te Einheitswurzel ζ in $\mathbb{Q}^{\mathrm{qua}}$ liegt. Sei

$$n = p_1^{e_1} \dots p_k^{e_k}$$

die Primfaktorzerlegung von n. Weil die Gruppe der n–ten Einheitswurzeln das direkte Produkt der Gruppen der $p_i^{e_i}$–ten Einheitswurzeln (für $i = 1, \dots, k$) ist, gehört ζ genau dann zu $\mathbb{Q}^{\mathrm{qua}}$, wenn alle $p_i^{e_i}$–ten Einheitswurzeln zu $\mathbb{Q}^{\mathrm{qua}}$ gehören. Wir können also annehmen, daß $n = p^e$ eine Primzahlpotenz ist.

Nach 3.6.2 ist $[\mathbb{Q}(\zeta) : \mathbb{Q}] = (p-1)p^{e-1}$, also genau dann eine Zweierpotenz, wenn $p = 2$ ist oder wenn $n = p$ eine Fermatsche Primzahl ist. Es bleibt zu zeigen, daß $\zeta \in \mathbb{Q}^{\mathrm{qua}}$, wenn $[\mathbb{Q}(\zeta) : \mathbb{Q}]$ eine Zweierpotenz ist. Das folgt aus der folgenden Überlegung:

Sei L/K eine galoissche Erweiterung, deren Grad eine Zweierpotenz ist. Dann ist $\mathrm{Aut}(L/K))$ eine 2–Gruppe. 2–Gruppen sind auflösbar (sogar nilpotent (1.9.2)). Also hat $\mathrm{Aut}(L/K)$ eine Normalreihe, deren Faktoren isomorph zu $\mathbb{Z}_2$ sind. Die zugehörigen Fixkörper bilden eine Folge

$$K = K_0 \subset K_1 \subset \ldots \subset K_n = L$$

von normalen Erweiterungen vom Grad 2. K_{i+1} entsteht also durch Adjunktion einer Quadratwurzel. Also ist $L \subset K^{\mathrm{qua}}$.

In unseren Fall $[\mathbb{Q}(\zeta) : \mathbb{Q}]$ müssen wir von 1.9.2 keinen Gebrauch machen, weil die Galoisgruppe abelsch ist. □

Weil für ungerade m das Polynom $X^n + 1$ ein Teiler von $X^{mn} + 1$ ist, kann $2^i + 1$ nur dann eine Primzahl sein, wenn i eine Zweierpotenz ist. Für $i = 1, 2, 4, 8, 16$ erhält man tatsächlich die Fermatschen Primzahlen

$$3, 5, 17, 257, 65537.$$

Die Konstruktion des regulären 5–Ecks findet sich bei Euklid[10]. Das reguläre 17–Eck wurde von Gauss konstruiert.
Ob es andere Fermatsche Primzahlen gibt, ist unbekannt. Die Faktorisierung

$$2^{32} + 1 = 641 \cdot 6700417$$

stammt von Euler.

Beispiel:
Als ein Beispiel berechnen wir, wie man die primitive 5–te Einheitswurzel

$$\zeta = e^{\frac{2\pi \mathrm{i}}{5}}$$

durch Quadratwurzelziehen aus rationalen Zahlen errechnet.

$\mathbb{Z}_5^* = \{1, 2, 3, 4\}$ operiert als Galoisgruppe von $\mathbb{Q}(\zeta)/\mathbb{Q}$ vermöge

$$m \longmapsto \phi_m,$$

[10]Euklid (365 v.Chr. – 300 v.Chr.)

wobei $\phi_m(\zeta) = \zeta^m$. $\mathbb{Z}_5^*$ ist als Einheitengruppe eines Körpers zyklisch und wird – weil $2^2 = 4 \not\equiv 1 \pmod 5$, von 2 erzeugt. $\mathbb{Z}_5^*$ hat eine Untergruppe G der Ordnung 2, die von $2^2 = 4$ erzeugt wird. Weil ζ^4 das komplex konjugierte von ζ ist, ist der zugehörige Automorphismus ϕ_4 die komplexe Konjugation.

Sei $K = \mathbb{Q}(\zeta) \cap \mathbb{R}$ der Fixkörper von G. Der Beweis von 3.5.1 zeigt, daß die Koeffizienten des Minimalpolynoms

$$(X - \zeta)(X - \zeta^4) = X^2 - (\zeta + \zeta^4)X + 1 \tag{3.4}$$

von ζ über K den Körper K über $\mathbb{Q}$ erzeugen. Es ist also

$$K = \mathbb{Q}(\delta)$$

für $\delta = \zeta + \zeta^4$.

Die Galoisgruppe $\mathbb{Z}_5^*/G$ von $K/\mathbb{Q}$ wird von ϕ_2 erzeugt. Betrachte

$$\alpha_0 = \delta + \phi_2(\delta)$$

und

$$\alpha_1 = \delta - \phi_2(\delta).$$

Man sieht wie Beweis von 3.6.4, daß α_0 und α_1^2 rational sind. Mit Hilfe von

$$1 + \zeta + \zeta^2 + \zeta^3 + \zeta^4 = 0$$

berechnet man, daß

$$\alpha_0 = (\zeta + \zeta^4) + (\zeta^2 + \zeta^3) = -1$$

und

$$\alpha_1^2 = \alpha_0^2 - 4(\zeta + \zeta^4)(\zeta^2 + \zeta^3) = 1 - 4(\zeta^3 + \zeta^4 + \zeta + \zeta^2) = 5.$$

Also ist

$$\delta = \frac{\alpha_1 + \alpha_0}{2} = \frac{\sqrt{5} - 1}{2}.$$

(Weil δ eine positive reelle Zahl ist, wählen wir die positive Wurzel aus.)

ζ erhalten wir als Nullstelle von (3.4) mit der Lösungsformel für quadratische Gleichungen oder mit der Methode von 3.6.4. Wir wählen die zweite Methode:
G ist die Galoisgruppe von $\mathbb{Q}(\zeta)/K$. Wir betrachten

$$\alpha_0' = \zeta + \phi_4(\zeta) = \delta$$

und

$$\alpha_1' = \zeta - \phi_4(\zeta) = \zeta - \zeta^4.$$

$\alpha_1'^2$ muß in K liegen, und in der Tat ist

$$\alpha_1'^2 = \zeta^2 - 2 + \zeta^3 = -3 - \delta.$$

Es ergibt sich

$$\zeta = \frac{\alpha_0' + \alpha_1'}{2} = \frac{\delta + \mathrm{i}\sqrt{\delta + 3}}{2} = \frac{\sqrt{5} - 1 + \mathrm{i}\sqrt{2\sqrt{5} + 10}}{4}$$

3.7.2 Auflösung von Gleichungen durch Radikale

Definition *Eine endliche Körpererweiterung L/K heißt* Radikalerweiterung, *wenn L aus K durch sukzessives Wurzelziehen entsteht.*

L ist also genau dann Radikalerweiterung von K, wenn es eine Folge

$$a_1, \dots a_l$$

von Elementen von L und natürlichen Zahlen $n_i > 0$ gibt, sodaß

$$L = K(a_1, \dots a_l) \tag{3.5}$$

und

$$a_i^{n_i} \in K(a_1, \dots a_{i-1})$$

für $i = 1, \dots, l$.
Insbesondere erhält man durch Adjunktion einer Einheitswurzel eine Radikalerweiterung.

Eine Gleichung

$$f(X) = 0$$

für ein Polynom $f \in K[X]$, heißt *auflösbar*, wenn alle Nullstellen von f in einer Radikalerweiterung von K liegen.

Man sieht leicht, daß der von einer endlichen Familie von Radikalerweiterungen von K in $\widetilde{K}$ erzeugte Körper wieder eine Radikalerweiterung von K ist. Wenn jede Nullstelle von f in einer Radikalerweiterung liegt, gibt es also eine Radikalerweiterung, die alle Nullstellen von f enthält.

Gleichungen zweiten Grades

$$X^2 + aX + b = 0$$

über einem Körper der Charakteristik 0 sind immer auflösbar, wie die Lösungsformel

$$\alpha_{1,2} = -\frac{a}{2} \pm \sqrt{\left(\frac{a}{2}\right)^2 - b}$$

zeigt.

Satz 3.7.5 *Sei K ein Körper der Charakteristik 0 und $f \in K[X]$. Dann ist die Gleichung*

$$f(x) = 0$$

genau dann auflösbar, wenn die Galoisgruppe des Zerfällungskörpers von f über K auflösbar ist.

Beweis :
Sei H der Zerfällungskörper von f über K.

Wir nehmen zunächst an, daß H in einer Radikalerweiterung (3.5) enthalten ist. Das Erzeugnis aller isomorphen Bilder von L in $\widetilde{K}$ (über K) ist wieder eine

Radikalerweiterung von K. Wir können also gleich annehmen, daß L normal über K ist. Sei n ein gemeinsames Vielfaches der Exponenten $n_1, \ldots, n_l$ und ζ eine primitive n–te Einheitswurzel. Dann sind nach 3.6.1 und 3.6.3 alle Stufen des Körperturms

$$K \subset K(\zeta) \subset K(\zeta, a_1) \subset K(\zeta, a_1, a_2) \subset \ldots \subset K(\zeta, a_1, \ldots, a_n) = L(\zeta)$$

galoissch mit auflösbarer Galoisgruppe. Also ist $\mathrm{Aut}(L(\zeta)/K)$ auflösbar und die Faktorgruppe $\mathrm{Aut}(L/K)$ ebenfalls.

Wenn umgekehrt $\mathrm{Aut}(H/K)$ auflösbar ist, gibt es eine Normalreihe mit zyklischen Faktoren von Primzahlordnung. Die zugehörigen Fixkörper

$$K = H_1 \subset H_2 \subset \ldots \subset H_h = H$$

bilden einen Körperturm von zyklischen Erweiterungen mit Ordnungen $p_1, \ldots, p_{h-1}$. Sei n ein gemeinsames Vielfaches der p_i und ζ eine primitive n–te Einheitswurzel. $H(\zeta)$ ist dann eine Radikalerweiterung von K. Denn einerseits entsteht $K(\zeta)$ aus K durch Adjunktion einer n-ten Wurzel von 1. Andererseits ist für jedes i

$$H_{i+1}(\zeta)/H_i(\zeta)$$

eine Galoiserweiterung. Eine Element ϕ der Galoisgruppe wird bestimmt durch seine Wirkung auf H_{i+1}. $\mathrm{Aut}(H_{i+1}(\zeta)/H_i(\zeta))$ ist also isomorph zu einer Untergruppe von $\mathrm{Aut}(H_{i+1}/H_i)$. Der Grad unserer Erweiterung ist daher p_i oder 1. Mit 3.6.4 ergibt sich, daß $H_{i+1}(\zeta)/H_i(\zeta)$ durch Adjunktion einer Wurzel entsteht. □

Folgerung 3.7.6 *Gleichungen der Grade* 1 *bis* 4 *sind auflösbar.*

Beweis :
Die Automorphismen des Zerfällungskörper von f werden dadurch bestimmt, wie sie die Nullstellen von f permutieren. Die Galoisgruppe einer Gleichung n–ten Grades ist also isomorph zu einer Untergruppe von S_n. Weil S_1, S_2, S_3 und S_4 auflösbar sind, sind auch ihre Untergruppen auflösbar. □

Wir werden im nächsten Abschnitt Gleichungen vom Grad 5 angeben, die nicht auflösbar sind.

Beispiel:
Die Lösung der Gleichung

$$X^3 + aX^2 + bX + c = 0 \tag{3.6}$$

durch Radikale kann man durch zwei Substitutionen finden:
Setzt man $X = Y - \frac{a}{3}$, ergibt sich die Gleichung

$$Y^3 + pY + q = 0 \tag{3.7}$$

für $p = -\frac{a^2}{3} + b$ und $q = \frac{2}{27}a^3 - \frac{ba}{3}$.

Durch die Substitution $Y = Z - \frac{p}{3Z}$ erhält man

$$Z^3 - \frac{p^3}{27Z^3} + q = 0$$

oder, für $Z^3 = W$, die quadratische Gleichung

$$W^2 + qW - \frac{p^3}{27} = 0. \tag{3.8}$$

Aus jeder Nullstelle

$$w = -\frac{q}{2} \pm \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}$$

von 3.8 und jeder dritten Wurzel $\sqrt[3]{w}$ von w erhalten wir eine Nullstelle

$$y = \sqrt[3]{w} - \frac{p}{3\sqrt[3]{w}}$$

von 3.7. (Natürlich sind nur 3 dieser 6 Nullstellen verschieden.)

3.7.3 Elementar–symmetrische Funktionen

Sei k ein Körper und $K = k(t_1, \ldots, t_n)$ der rationale Funktionenkörper über k in den Unbestimmten $t_1, \ldots, t_n$. Wir betrachten das Polynom

$$p(X) = (X - t_1) \cdots (X - t_n)$$

Die mit geeigneten Vorzeichen versehenen Koeffizienten von

$$p(X) = (-1)^n s_n + (-1)^{n-1} s_{n-1} X + \ldots - s_1 X^{n-1} + X^n,$$

die *elementar–symmetrischen* Funktionen in n Variablen, sind Polynome in $t_1, \ldots, t_n$ mit ganzzahligen Koeffizienten. Es ist[11]

$$\begin{aligned} s_1 &= t_1 + \cdots + t_n \\ s_i &= \sum_{\substack{x \subset \{1,\ldots,n\} \\ |x| = i}} \prod_{j \in x} t_j \\ s_n &= t_1 \cdots t_n. \end{aligned}$$

Setze

$$F = k(s_1, \ldots, s_n).$$

$p(X)$ gehört zu $F[X]$ und K ist der Zerfällungskörper von p über F. Weil p separabel ist, ist die Erweiterung K/F galoissch.

Lemma 3.7.7

$$\mathrm{Aut}(K/F) = \mathrm{Sym}(t_1, \ldots, t_n) \cong \mathrm{S}_n$$

Beweis :
Ein Automorphismus eines Zerfällungskörpers ist durch seine Wirkung auf den Nullstellen eindeutig bestimmt. Also können wir die Galoisgruppe von K/F als Untergruppe von $\mathrm{Sym}(t_1, \ldots, t_n)$ auffassen. Sei umgekehrt π eine Permutation der t_i. π setzt sich fort zu einem Automorphismus von K über k. Weil π die Faktoren von p nur permutiert, wird p und damit auch F von π fixiert. π gehört also zur Galoisgruppe von K über F.

[11] Man könnte sinnvoll auch $s_0 = 1$ setzen.

Folgerung 3.7.8 *Wenn k die Charakteristik Null hat und wenn $n \geq 5$, ist die Gleichung $p(X) = 0$ nicht auflösbar über F.*

Beweis :
S_n ist nicht auflösbar, wenn $n \geq 5$ (vergleiche Seite 31). □

Eine rationale Funktion $f \in k(t_1, \ldots, t_n)$ ist *symmetrisch*, wenn für alle $\sigma \in S_n$

$$f(t_{\sigma(1)}, \ldots, t_{\sigma(n)}) = f(t_1, \ldots, t_n).$$

Folgerung 3.7.9 *Jede symmetrische rationale Funktion läßt sich rational in den elementar–symmetrische Funktion ausdrücken.*

Beweis :
F ist der Fixkörper von $\mathrm{Aut}(K/F)$. □

Weil die über k algebraisch unabhängigen[12] $t_1, \ldots, t_n$ algebraisch über $k(s_1, \ldots, s_n)$ sind, kann man schließen, daß auch die s_i algebraisch unabhängig über k sind. Daraus folgt, daß eine Darstellung durch elementar–symmetrische Funktionen eindeutig ist.

Beispiel:

$$\frac{t_1^3 - t_2^3}{t_1^2 - t_2^2} = \frac{s_1^2 - s_2}{s_1}$$

Der **Hauptsatz über symmetrische Funktionen** besagt, daß jedes symmetrische Polynom ein Polynom in den elementar–symmetrischen Funktionen ist.
mode: latex

[12] Das heißt, daß die Folge der t_i keinen nichttrivialen algebraischen Gleichungen über k genügt.

Kapitel 4

Darstellungstheorie

4.1 Der Satz von Wedderburn

Wir fixieren einen, nicht notwendig kommutativen, unitären Ring R.

Lemma 4.1.1 *Sei $M = M_1 \oplus \cdots \oplus M_n$ eine direkte Zerlegung des R-Rechtsmoduls M. Dann läßt sich jeder Endomorphismus α von M beschreiben durch eine Matrix (α_{ij}) aus Homomorphismen $\alpha_{ij} : M_j \to M_i$. Wenn alle M_i isomorph sind, ist* $\mathrm{End}(M)$ *isomorph zum Matrixring* $\mathrm{M}_n(\mathrm{End}(M_1))$.

Beweis :
Sei die direkte Zerlegung gegeben durch die Einbettungen $\epsilon_j : M_j \to M$ und die Projektionen $\pi_i : M \to M_i$. Dann ist für jeden Endomorphismus α

$$\alpha = \sum_{ij} \epsilon_i \alpha_{ij} \pi_j,$$

wobei $\alpha_{ij} = \pi_i \alpha \epsilon_j$. Man sieht leicht, daß die Verknüpfung von Endomorphismen der Multiplikation von Matrizen entspricht:

$$(\alpha\beta)_{ik} = \sum_j \alpha_{ij}\beta_{jk}$$

Wir fixieren Isomorphismen $\phi_i : M_1 \to M_i$. Wenn wir jedem Homomorphismus $\alpha_{ij} : M_j \to M_i$ den Endomorphismus

$$\overline{\alpha_{ij}} = \phi_i^{-1} \alpha_{ij} \phi_j \in \mathrm{End}(M_1)$$

zuordnen, gilt

$$\overline{\alpha_{ij}\beta_{jk}} = \overline{\alpha_{ij}}\,\overline{\beta_{ik}}.$$

Daraus folgt die Behauptung. □

Definition *Sei M ein R-Rechtsmodul.*

1. *M heißt einfach, wenn M nicht Null ist und außer sich selbst und 0 keine Untermoduln hat.*

2. *M heißt halbeinfach, wenn M von einfachen Untermoduln erzeugt wird.*

Satz 4.1.2 *Ein R–Rechtsmodul M ist genau dann halbeinfach, wenn jeder Untermodul ein direkter Summand ist.*

Beweis :
Nehmen wir an, daß jeder Untermodul von M direkter Summand von M ist. Es ist klar, daß auch jeder Untermodul diese Eigenschaft hat[1]. Zyklische Untermoduln $\neq 0$ haben maximale Untermoduln, deren Komplement einfach sein muß. Also enthält jeder nicht–triviale Untermodul einen einfachen Untermodul. Sei U das Komplement des Erzeugnisses aller einfachen Untermoduln. Weil U keinen einfachen Untermodul enthält, muß $U = 0$ sein.

Für die Umkehrung betrachten wir ein halbeinfaches M und einen Untermodul U. Wir wählen einen maximalen Untermodul V, für den $U \cap V = 0$. Wenn wir zeigen können, daß $U + V$ alle einfachen Untermoduln L enthält, wissen wir, daß $M = U + V$ und V ein Komplement von U ist.

Wir können annehmen, daß $L \not\subset V$. Dann ist $V + L$ größer als V und wegen der Maximalität von V ist $U \cap (V + L) \neq 0$. Es folgt $(U + V) \cap L \neq 0$. Weil L einfach ist, muß $(U + V) \cap L = L$ sein. □

Folgerung 4.1.3 *Ein halbeinfacher Modul M ist direkte Summe von einfachen Untermoduln.*

$$M \cong \bigoplus_{i \in I} L_i$$

Die Zerlegung ist bis auf Permutation und Isomorphie eindeutig bestimmt[2]. Das Erzeugnis aller L_i, die zu einem festen L isomorph sind, hängt nicht von der Zerlegung ab.

Beweis :
Sei $(L_i)_{i \in I}$ eine maximale unabhängige Familie von einfachen Untermoduln von M. Sei U die (direkte) Summe der L_i und V ein Komplement von U in M. Nehmen wir an, daß $U \neq M$. Dann ist $V \neq 0$. Weil mit M auch V halbeinfach ist, enthält V einen einfachen Untermodul L. Wir könnten jetzt die unabhängige Familie der L_i durch L vergrößern, was der Wahl der L_i widerspricht. Also ist $U = M$.

Die Eindeutigkeit folgt für endliche Zerlegungen aus dem Satz von Jordan–Hölder. Für unendliche Zerlegungen geht man vor wie beim Beweis des Spezialfalls der Vektorräume. □

Halbeinfache Moduln mit endlicher Zerlegung in einfache Moduln nennen wir halbeinfach von *endlicher Länge*.

[1] Sei W ein Untermodul von $U \leq M$. Wenn $M = W \oplus V$, ist $U = W \oplus (V \cap U)$.
[2] Für jedes L ist die Zahl der i mit $L_i \cong L$ unabhängig von der Zerlegung.

Satz 4.1.4 *Der Endomorphismenring eines halbeinfachen Moduls endlicher Länge ist direktes Produkt von endlich vielen Matrixringen über Divisionsringen.*

Beweis :
Wenn wir M direkt in Untermoduln zerlegen, deren einfache Untermoduln jeweils untereinander isomorph sind, zerlegt sich der Endomorphismenring von M entsprechend in ein direktes Produkt, weil es zwischen den verschiedenen Summanden keine Homomorphismen geben kann. Das führt dazu, daß wir annehmen können, daß

$$M = L^1 \oplus \cdots \oplus L^n$$

für Moduln L^i, die alle isomorph sind. Aus 4.1.1 folgt $\mathrm{End}(M) \cong \mathrm{M}_n(\mathrm{End}(L^1))$. Nach dem folgenden Lemma ist $\mathrm{End}(L^1)$ ein Divisionsring. □

Lemma 4.1.5 (Schurs[3]Lemma) *Der Endomorphismenring eines einfachen Moduls ist ein Divisionsring.* □

Beweis :
Sei M einfach und $\alpha \in \mathrm{End}(M)$ nicht Null. Dann ist

- $\alpha(M)$ nicht Null. Also ist $\alpha(M) = M$ und α ist surjektiv.
- $\ker(\alpha) \neq M$. Also ist $\ker(\alpha) = 0$ und α ist injektiv.

□

Definition *Ein Ring R ist halbeinfach, wenn R_R halbeinfach ist.*

Satz 4.1.6 *R ist genau dann halbeinfach, wenn alle R–Rechtsmoduln halbeinfach sind. Wenn R halbeinfach ist, ist R direkte Summe von endlich vielen minimalen Rechtsidealen. Jeder einfache R–Modul ist isomorph zu einem minimalen Rechtsideal von R.*

Beweis :
Sei R halbeinfach und M ein Modul. M wird von seinen zyklischen Untermoduln erzeugt. Zyklische Moduln sind aber Quotienten von R und daher halbeinfach.

R ist nach 4.1.3 direkte Summe von minimalen Rechtsidealen L_i. 1 ist schon in einer endlichen Teilsumme enthalten, die dann schon ganz R sein muß.

Einfache Moduln sind zyklisch, also von der Form R/U. Wenn R halbeinfach ist, hat U ein Komplement L und es ist $R/U \cong L$. □

Ein Modul M heißt *irreduzibel*, wenn M nicht Null ist und außer sich selbst und 0 keine direkten Summanden hat. Wenn R halbeinfach ist, sind alle irreduziblen Moduln einfach.

Satz 4.1.7 (Satz von Wedderburn[4]) *Jeder halbeinfache Ring ist direktes Produkt von endlich vielen Matrixringen über Divisionsringen.*

[3] Issai Schur (1875-1941)
[4] Joseph Henry Maclagan Wedderburn (1882-1948)

BEWEIS :
Jeder Ring R ist isomorph zum Endomorphismenring von R_R (Bemerkung S.36). □

Wir wollen uns überlegen, daß jedes endliche direkte Produkt von Matrixringen über Schiefkörpern halbeinfach ist. Es genügt dafür natürlich, ein einzelnes $\mathrm{M}_n(D)$ zu betrachten. Sei N_i die Menge aller Matrizen, die höchstens in der i–ten Zeile von Null verschiedene Einträge haben. Die N_i sind minimale Rechtsideale, es ist $\mathrm{M}_n(D) = N_1 \oplus \cdots \oplus N_n$ und R ist tatsächlich halbeinfach.

Man sieht leicht, daß alle minimalen Rechtsideale die Gestalt

$$L_{s_0} = \{s_0 z \mid z \text{ Zeilenvektor}\}$$

für einen Spaltenvektor $s_0 \neq 0$ haben[5]. Für je zwei nicht–triviale Spalten s_0 und s_1 ist die Abbildung $s_0 z \mapsto s_1 z$ ein Isomorphismus zwischen L_{s_0} und L_{s_1}. Daraus folgt

Folgerung 4.1.8

$$R = \mathrm{M}_{n_1}(D_1) \times \cdots \times \mathrm{M}_{n_k}(D_k)$$

hat bis auf Isomorphie genau k viele einfache Rechtsmoduln. □

Sei $R = \mathrm{M}_n(D)$ ein Matrixring über einem Schiefkörper und N_1 das oben definierte minimale Rechtsideal. Weil sich alle Endomorphismen von N_1 zu Endomorphismen von R_R fortsetzen lassen, werden alle Endomorphismen von N_1 durch Linksmultiplikation mit geeigneten Elementen $r = (\delta_{ij})$ von R dargestellt. Damit $rN_1 \subset N_1$, muß $re_1 = \delta_{11}e_1$ sein und r operiert dann auf N_1 einfach als Linksmultiplikation mit δ_{11}. Es folgt, wie wegen des Beweises von 4.1.7 nicht anders zu erwarten, daß $\mathrm{End}(N_1) = D$. Der D–Linksmodul N_1 ist nicht anderes als der Vektorraum aller n–dimensionalen Zeilenvektoren und die Endomorphismen von ${}_D N_1$ sind Rechtsmultiplikationen mit Matrizen aus R. Also ist $R = \mathrm{End}_D^{\mathrm{opp}}(N_1)$. Das überträgt sich sofort auf Produkte von Matrixringen über Schiefkörpern:

Folgerung 4.1.9 *Sei L ein einfacher Rechtsmodul über einem halbeinfachen Ring R und D der Endomorphismenring von L. Dann ist der natürliche Ringhomomorphismus $R \to \mathrm{End}_D^{\mathrm{opp}}(L)$ ein Epimorphismus.* □

Natürlich sind Matrixringe über Schiefkörpern auch als Linksmoduln über sich selbst halbeinfach[6]. Also:

Folgerung 4.1.10 *Wenn R halbeinfach ist, ist ${}_R R$ ein halbeinfacher R–Linksmodul.* □

Folgerung 4.1.11 *Eine halbeinfache endlich–dimensionale Algebra über einem algebraisch abgeschlossenen Körper K ist direktes Produkt von Matrixringen über K.*

[5] Für die i–te Einheitsspalte e_i ist $N_i = L_{e_i}$.
[6] Transponieren liefert $\mathrm{M}_n^{\mathrm{opp}}(D) \cong \mathrm{M}_n(D^{\mathrm{opp}})$.

Beweis :
Sei R eine halbeinfache endlich–dimensionale K–Algebra. Dann ist R direktes Produkt von Matrixringen $\mathrm{M}_n(D)$, für Divisionsringe D, die Endomorphismenringe von minimalen Rechtsidealen sind. Die D sind also selbst endlich–dimensionale K–Algebren. Wir können annehmen, daß K Unterkörper des Zentrums von D ist (vgl. Seite 38). Wir werden zeigen, daß $K = D$. Sei a ein beliebiges Element von D. Weil K im Zentrum von D liegt, ist der Unterring $K[a]$ kommutativ und, als Unterring eines Divisionsrings, ein Integritätsbereich. Weil $K[a]$ endliche Dimension über K hat, ist a algebraisch über K. Wenn K algebraisch abgeschlossen ist, muß a in K liegen. □

4.2 Die Gruppenalgebra

Sei G eine Gruppe und V ein K–Vektorraum. Eine Darstellung von G in V ist ein Homomorphismus $\rho : G \to \mathrm{Aut}(V)$. Eine Darstellung macht V zu einem G–Modul mit der Operation

$$G \times V \to V,$$

definiert durch $gv = \rho(g)(v)$. Ein G–Modul ist das gleiche wie ein Linksmodul über der Gruppenalgebra $K[G]$. Alle Begriffe, die für Moduln geprägt worden sind, übertragen sich auf Darstellungen. Einfache Darstellungen zum Beispiel sind Darstellungen, die als $K[G]$–Modul einfach sind.

Definition *Die Gruppenalgebra $K[G]$ ist eine K-Algebra, die G als Basis und multiplikative Untergruppe enthält. $K[G]$ ist also der Ring aller formalen Summen*

$$\sum_{g \in G} a_g g \quad (a_g \in K, \ \textit{fast alle } = 0).$$

Sei X eine Menge, auf der G von links operiert. Wir machen aus X einen Vektorraum $K[X]$, mit X als Basis. Die Elemente von G, die X permutieren, definieren jetzt Automorphismen von $K[X]$. Man nennt diese Darstellung von G die zu X gehörende Permutationsdarstellung. $K[G]$, als G–Modul aufgefaßt, gehört zur Operation von G auf sich selbst durch Linksmultiplikation. Man nennt dieses Darstellung die *reguläre* Darstellung V_{reg}.

G operiert *trivial* auf U, wenn $gu = u$ für alle $g \in G$ und $u \in U$.

$$V^G = \{v \in V \mid \forall g \, gv = v\}$$

ist der größte Untermodul von V, auf dem G trivial operiert.

Aus G–Moduln V und W lassen sich auf vielfältige Weise neue G–Moduln bilden. Natürlich ist $V \oplus W$ wieder ein G–Modul. Die folgenden Konstruktionen aber lassen sich nur für Gruppenalgebren durchführen. Der Dualraum

$$V^*$$

wird durch die Definition $(g\lambda)v = \lambda(g^{-1}v)$ zu einem G–Modul[7]. Dazu muß man nachrechnen, daß $(gh)\lambda = \lambda(gh)^{-1} = \lambda h^{-1}g^{-1} = (h\lambda)g^{-1} = g(h\lambda)$.

Auf dem Vektorraum

$$\mathrm{Hom}_K(V, W)$$

kann man G operieren lassen durch

$${}^g\phi(v) = g\phi(g^{-1}v).$$

Wir schreiben $\mathrm{Hom}_G(V, W)$ für $\mathrm{Hom}_{K[G]}(V, W)$. Man rechnet leicht nach, daß

Lemma 4.2.1

$$\mathrm{Hom}_G(V, W) = \mathrm{Hom}_K(V, W)^G$$

[7] g operiert also auf V^* als das Duale des Inversen der Operation von g auf V.

G operiert auf dem Tensorprodukt

$$V \otimes_K W$$

durch $g(v \otimes w) = (gv) \otimes (gw)$. Man sieht leicht, daß für endlich–dimensionale V und W der natürliche Isomorphismus zwischen $\mathrm{Hom}_K(V, W)$ und $V^* \otimes_K W$ ein Isomorphismus von G–Moduln ist.

Satz 4.2.2 (Satz von Maschke) *Sei G endlich und K ein Körper. Dann ist $K[G]$ genau dann halbeinfach, wenn die Ordnung von G prim zur Charakteristik von K ist.*

Beweis :
Nehmen wir zuerst an, daß die Charakteristik p die Ordnung n von G teilt. Sei $V_{\mathrm{reg}} = K[G]$ die reguläre Darstellung. Der Untermodul V_{reg}^G wird als K–Vektorraum von $\nu = \sum_{g \in G} g$ erzeugt. Sei $\pi : V_{\mathrm{reg}} \to V_{\mathrm{reg}}^G$ ein Homomorphismus[8]. Wenn $\pi(1) = \alpha\nu$, ist aber

$$\pi(\nu) = \sum_{g \in G} g\pi(1) = n\pi(1) = 0.$$

π ist also die Nullabbildung auf V_{reg}^G. Es folgt, daß V_{reg}^G kein direkter Summand von V_{reg} sein kann. Also ist $K[G]$ nicht halbeinfach.

Wenn p kein Teiler von n ist, betrachten wir das Element

$$\mu_G = \frac{1}{n} \sum_{g \in G} g.$$

Man rechnet leicht nach, daß für alle g $g\mu_G = \mu_G g = \mu_G$. Wenn G trivial auf V operiert, ist $\mu_G v = v$ für alle $v \in V$. Daraus folgt sofort

Lemma 4.2.3 *Die Multiplikation mit μ_G projiziert V auf V^G.*

Wir wollen zeigen, daß jeder Untermodul W eines G–Moduls V direkter Summand ist. Sei $\epsilon : W \to V$ die Inklusionsabbildung. Wir wählen ein Linksinverses $\pi_0 \in \mathrm{Hom}_K(V, W)$ mit $\pi_0\epsilon = 1$. Setze $\pi = {}^{\mu_G}\pi_0$. Dann ist $\pi \in \mathrm{Hom}_G(V, W)$ und π ist ebenfalls ein Linksinverses von ϵ, weil

$$\pi\epsilon = {}^{\mu_G}\pi_0{}^{\mu_G}\epsilon = {}^{\mu_G}(\pi_0\epsilon) = {}^{\mu_G}1 = 1$$

Daraus folgt die Behauptung.[9] □

Angewendet auf den Körper der komplexen Zahlen ergibt sich

Satz 4.2.4 *Die Gruppenalgebra einer endlichen Gruppe G über $\mathbb{C}$ ist direktes Produkt von Matrixringen über $\mathbb{C}$.*

$$\mathbb{C}[G] = \mathrm{M}_{n_1}(\mathbb{C}) \times \cdots \mathrm{M}_{n_k}(\mathbb{C})$$

[8] Gemeint ist natürlich ein G–Modul–Homomorphismus.
[9] Für $K = \mathbb{C}$ ergibt sich ein anderer Beweis aus 4.3.8.

Die Faktoren entsprechen den Isomorphietypen $V_1,\ldots,V_k$ der irreduziblen[10] *Darstellungen. Ihre Anzahl k ist gleich der Zahl der Konjugationsklassen von G.*

Beweis :
Der erste Teil des Satzes folgt aus dem Satz von Wedderburn, weil $\mathbb{C}$ algebraisch abgeschlossen ist. Für den zweiten Teil beachtet man, daß das Zentrum eines Matrixrings der Grundkörper selbst ist. Also ist die $\mathbb{C}$–Dimension des Zentrums von $\mathbb{C}[G]$ gleich der Zahl der Faktoren. Andererseits gehört $\sum a_g g$ genau dann zum Zentrum, wenn für alle h

$$\sum_{g\in G} a_g g^h = \sum_{g\in G} a_g g,$$

wenn also die Koeffizienten a_g nur von der Konjugationsklasse von g abhängen. Es folgt, daß die Elemente $\sum_{g\in C} g$ für Konjugationsklassen C eine Basis des Zentrums bilden. Daraus folgt die Behauptung. □

Folgerung 4.2.5 *Die Dimension der i–ten irreduziblen Darstellung V_i ist n_i. Es gilt*

$$n = n_1^2 + \cdots + n_k^2.$$

□

Folgerung 4.2.6

$$V_{\text{reg}} = V_1^{n_1} \oplus \cdots \oplus V_k^{n_k}$$

□

[10] Man spricht von einfachen Darstellungen (im halbeinfachen Fall) gern als von *irreduziblen* Darstellungen

4.3 Charaktere

Wir betrachten in diesem Abschnitt endlich–dimensionale Darstellungen V einer endlichen Gruppe G über $\mathbb{C}$.

Definition *Die Funktion $\chi_V : G \to \mathbb{C}$, die jedem $g \in G$ die Spur $\mathrm{Tr}_V(g)$ der Operation von g auf V zuordnet, heißt der Charakter von V.*

Es ist klar, daß $\chi_V(g)$ nur von der Konjugationsklasse von g abhängt. Funktionen $G \to \mathbb{C}$, die auf Konjugationsklassen konstant sind, heißen *formale* Charaktere. Der Vektorraum Γ_G aller formalen Charaktere hat die Dimension k.

Beispiel:
In V_{reg} operieren (bezüglich der kanonischen Basis) die $g \in G$ durch Permutationsmatrizen, welche (außer für $g = 1$) nur Nullen in der Diagonale haben. Also ist

$$\chi_{\mathrm{reg}}(g) = \begin{cases} n & \text{wenn } g = 1 \\ 0 & \text{sonst.} \end{cases}$$

Lemma 4.3.1 *$\chi_V(1)$ ist die Dimension von V. Eine Abbildung $\chi : G \to \mathbb{C}$ ist genau dann ein eindimensionaler Charakter, wenn χ ein Homomorphismus von G nach $\mathbb{C}^\bullet$ ist.* □

Abelsche Gruppen der Ordnung n haben $k = n$ Konjugationsklassen und also n irreduzible Darstellungen. Aus der Formel 4.2.5 folgt:

Folgerung 4.3.2 *Alle irreduziblen Darstellungen einer endlichen abelschen Gruppe sind eindimensional.*

	1	a	a^2
χ_1	1	1	1
χ_2	1	$\mathrm{e}^{\frac{2\pi\mathrm{i}}{3}}$	$\mathrm{e}^{\frac{4\pi\mathrm{i}}{3}}$
χ_3	1	$\mathrm{e}^{\frac{4\pi\mathrm{i}}{3}}$	$\mathrm{e}^{\frac{2\pi\mathrm{i}}{3}}$

Charaktertafel $\mathrm{Z}_3 = \{1, a, a^2\}$

Die Gruppe G^* der eindimensionalen Charaktere einer endlichen abelschen Gruppe G (die Charaktergruppe[11] von G) ist (unkanonisch) isomorph zu G. Das sieht man leicht für zyklischen Gruppen ein, woraus dann mit 1.7.3 die Behauptung folgt.

Lemma 4.3.3 *Für alle Charaktere ρ gilt*

$$\rho(g^{-1}) = \overline{\rho(g)}.$$

[11] Wir werden in 4.3.4 sehen, daß G^* die Gruppe aller 1–dimensionalen Darstellungen mit dem Tensorprodukt als Multiplikation (und der dualen Darstellung als Inversen) ist.

BEWEIS :
Sei V eine Darstellung. $g \in G$ operiere auf V als ϕ. Wir müssen zeigen, daß

$$\mathrm{Tr}(\phi^{-1}) = \overline{\mathrm{Tr}(\phi)}.$$

Aus $\phi^n = 1$ folgt, daß die Jordanform von ϕ Diagonalgestalt haben muß, und die Eigenwerte n–te Einheitswurzeln sind. Das Inverse einer Einheitswurzel ist aber ihr konjugiert–komplexes. Für einen zweiten Beweis fixieren wir eine unitäre Struktur auf V, für die ϕ unitär ist (4.3.8). Für eine Orthonormalbasis ist dann die Matrix von ϕ^{-1} die Adjungierte der Matrix von ϕ, hat also wieder die konjugiert–komplexe Spur. □

Lemma 4.3.4 *V und W seien Darstellungen von G. Dann ist*

$$\begin{aligned} \chi_{V\oplus W} &= \chi_V + \chi_W \\ \chi_{V^*} &= \overline{\chi_V} \\ \chi_{V\otimes_{\mathbb{C}} W} &= \chi_V \cdot \chi_W \\ \chi_{\mathrm{Hom}_{\mathbb{C}}(V,W)} &= \overline{\chi}_V \cdot \chi_W \end{aligned}$$

BEWEIS :
Sei g ein Gruppenelement und ϕ und ψ die Endomorphismen die g in V und W darstellen. Die erste Behauptung des Lemmas folgt aus

$$\mathrm{Tr}(\phi \oplus \psi) = \mathrm{Tr}(\phi) + \mathrm{Tr}(\psi).$$

Die zweite Behauptung folgt aus dem letzten Lemma:

$$\mathrm{Tr}((\phi^{-1})^*) = \mathrm{Tr}(\phi^{-1}) = \overline{\mathrm{Tr}(\phi)}.$$

Die dritte Behauptung folgt aus

$$\mathrm{Tr}(\phi \otimes \psi) = \mathrm{Tr}(\phi) \cdot \mathrm{Tr}(\psi).$$

Das kann man entweder direkt den zuständigen Matrizen ansehen, oder man stellt (vermöge $\mathrm{End}_{\mathbb{C}}(U) = U^* \otimes_{\mathbb{C}} U$) ϕ und ψ dar als Summen von Tensoren $\lambda \otimes v$ und $\mu \otimes w$; und rechnet

$$\mathrm{Tr}((\lambda\otimes v)\otimes(\mu\otimes w)) = \mathrm{Tr}((\lambda\otimes\mu)\otimes(v\otimes w)) = \lambda(v)\cdot\mu(w) = \mathrm{Tr}(\lambda\otimes v)\cdot\mathrm{Tr}(\mu\otimes w).$$

Die letzte Behauptung folgt aus der zweiten und dritten. □

Definition $(\ ,\ )$ *sei die folgende unitäre Form auf Γ_G, dem Raum der formalen Charaktere,*

$$(\rho, \sigma) = \frac{1}{n} \sum_{g\in G} \overline{\rho(g)}\sigma(g)$$

Satz 4.3.5 (Orthogonalitätsrelationen I) *Die Charaktere der irreduziblen Darstellungen bilden eine Orthonormalbasis von Γ_G.*

BEWEIS :
Weil

$$\#\text{ irreduziblen Darstellungen} = \#\text{ Konjugationsklassen} = \text{Dimension von } \Gamma_G,$$

genügt es zu zeigen, daß irreduzible Charaktere die Länge 1 haben und aufeinander senkrecht stehen. Seien also V und W zwei irreduzible Darstellungen. Dann ist

$$(\chi_V, \chi_W) = \frac{1}{n} \sum_{g \in G} \mathrm{Tr}_{\mathrm{Hom}_{\mathbb{C}}(V,W)}(g) = \mathrm{Tr}_{\mathrm{Hom}_{\mathbb{C}}(V,W)}(\mu_G).$$

Die Spur einer Projektion ist die Dimension ihres Bildraums. Weil μ_G auf $\mathrm{Hom}_G(V,W)$ projiziert, ist

$$(\chi_V, \chi_W) = \dim \mathrm{Hom}_G(V,W).$$

□

Folgerung 4.3.6 *Darstellungen sind durch ihren Charakter bis auf Isomorphie bestimmt.*

Beweis :
Sei V eine beliebige Darstellung und W irreduzibel. Dann ist (χ_V, χ_W) die Vielfachheit mit der W in der direkten Zerlegung von V in Irreduzible vorkommt.□

Beispiel:
Wir wollen alle irreduziblen Charaktere von S_3 bestimmen. S_3 hat die drei Konjugationsklassen $\{1\}$, $\{(12),(23),(31)\}$ und $\{(123),(132)\}$ und damit drei irreduzible Charaktere. Es gibt zwei Homomorphismen $S_3 \to \mathbb{C}$:

$$\begin{aligned} \chi_1(g) &= 1 \\ \chi_2(g) &= \mathrm{sign}(g) \end{aligned}$$

Die Summe der Quadrate der Dimensionen der irreduziblen Darstellungen ist 6. Also muß die Dimension der dritten Darstellung 2 sein. Wir haben also für den dritten irreduziblen Charakter $\chi_3(1) = 2$. Daß χ_3 auf χ_1 und χ_2 senkrecht steht, bedeutet:

$$\begin{aligned} (\chi_1, \chi_3) &= \tfrac{1}{6}\big(2 + 3\chi_3(12) + 2\chi_3(123)\big) = 0 \\ (\chi_2, \chi_3) &= \tfrac{1}{6}\big(2 - 3\chi_3(12) + 2\chi_3(123)\big) = 0 \end{aligned}$$

Es folgt $\chi_3(12) = 0$ und $\chi_3(123) = -1$. Also haben wir die Charaktertafel

	1	(12)	(123)
χ_1	1	1	1
χ_2	1	−1	1
χ_3	2	0	−1

Charaktertafel S_3

Der dritte irreduzible Charakter von S_3 läßt sich auch auf folgende Weise bestimmen: Eine verdächtige (reelle) 2–dimensionale Darstellung V besteht aus den orthogonalen Abbildungen des $\mathbb{R}^2$, die die Ecken des Dreiecks

$$(1,0), \quad \big(\cos(2\pi/3), \sin(2\pi/3)\big), \quad \big(\cos(4\pi/3), \sin(4\pi/3)\big)$$

permutieren. In dieser Darstellung wird (12) durch die Spiegelung $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ und (123) durch die Drehung $\begin{pmatrix} \cos(2\pi/3) & -\sin(2\pi/3) \\ \sin(2\pi/3) & \cos(2\pi/3) \end{pmatrix}$ interpretiert. Die Spuren der beiden Matrizen sind $\chi_V(12) = 0$ und $\chi_V(123) = -1$. Man muß jetzt nur noch zeigen, daß V irreduzibel ist. Dafür gibt es wieder zwei Argumente. Erstens ist χ_V nicht Summe von zweien der Charaktere χ_1, χ_2. Oder, zweitens, berechnet man $(\chi_V, \chi_V) = 1$ und verwendet

Bemerkung *Eine Darstellung V ist genau dann irreduzibel, wenn*

$$(\chi_V, \chi_V) = 1.$$

Beweis :
Wenn man V in Irreduzible zerlegt,

$$V = m_1 V_1 \oplus \cdots \oplus m_k V_k,$$

ist $(\chi_V, \chi_V) = m_1^2 + \cdots + m_k^2$. □

Folgerung 4.3.7 *Sei $\chi_1, \ldots, \chi_k$ eine Liste der irreduziblen Charaktere. Dann gilt für zwei Gruppenelemente g, h*

$$\sum_{i=1}^{k} \overline{\chi_i}(g)\chi_i(h) = \begin{cases} \frac{n}{\#g^G} & \text{wenn } g^G = h^G \\ 0 & \text{sonst} \end{cases}$$

Dabei bezeichnet g^G die Konjugationsklasse von g.

Beweis :
Seien $g_1, \ldots, g_k$ Vertreter der Konjugationsklassen und k_j die Größe der Konjugationsklasse von g_j. Orthogonalität der χ_i bedeutet, daß die Matrix

$$\sqrt{\frac{k_j}{n}}\chi_i(g_j)$$

unitär ist. Also ist auch die Transponierte unitär, und das ist die Behauptung. □

Beispiel:
Für $g = 1$ folgt, daß $\sum_{i=1}^{k} n_i\chi_i(h)$ gleich n ist, wenn $h = 1$, und gleich Null sonst. Also ergibt sich noch einmal die Behauptung von 4.2.6:

$$\chi_{\text{reg}} = n_1\chi_1 + \cdots + n_k\chi_k$$

Beispiel:
Wir berechnen die Charaktertafel von S_4. Es gibt 5 Konjugationsklassen: die Klasse des Einselements, die 6 Transpositionen (ab), die 8 Dreierzyklen (abc), die 6 Viererzyklen $(abcd)$ und die 3 Produkte von disjunkten Transpositionen $(ab)(cd)$. Es gibt also 5 irreduzible Charaktere. Weil $S_3 \cong S_4/V_4$ ein Quotient

von S_4 ist, ist jede Darstellung von S_3 auch ein Darstellung von S_4. Das liefert uns die ersten drei irreduziblen Charaktere mit den Dimensionen $1, 1, 2$. Die Quadratsumme der Dimensionen ist 24, also kommt für χ_4 und χ_5 nur die Dimension 3 in Frage. Aus 4.3.7 folgt $\sum_i \overline{\chi_i(1)}\chi_i(ab) = 0$ und daraus $\chi_4(ab) + \chi_5(ab) = 0$. Andererseits folgt aus $\sum_i |\chi_i(ab)|^2 = \frac{24}{6} = 4$, daß $\chi_4(ab)$ und $\chi_5(ab)$ nur 1 und -1 sein können[12]. Wir nehmen $\chi_4(ab) = 1$ und $\chi_5(ab) = -1$. Die übrigen Werte von χ_4 und χ_5 ergeben sich sofort daraus, daß die ersten beiden Spalten der Charaktertafel auf den übrigen Spalten senkrecht stehen.

	1	(ab)	(abc)	$(abcd)$	$(ab)(cd)$
χ_1	1	1	1	1	1
χ_2	1	-1	1	-1	1
χ_3	2	0	-1	0	2
χ_4	3	1	0	-1	-1
χ_5	3	-1	0	1	-1

Charaktertafel S_4

Lemma 4.3.8 *Sei V eine Darstellung. Dann hat V eine unitäre Struktur, die von allen $g \in G$ invariant gelassen wird.*

Beweis :
Wir wählen uns irgend eine unitäre Form $(\ ,\ )_0$ und machen sie G–invariant:

$$(v_1, v_2) = \sum_{g \in G} (gv_1, gv_2)_0.$$

$(\ ,\ )$ ist positiv definit, weil für $v \neq 0$

$$(v, v) = \sum_{g \in G} (gv, gv)_0 > 0.$$

□

Man nennt eine Darstellung mit einer unitären G–invarianten Form eine *unitäre Darstellung*.

Das letzte Lemma ermöglicht einen alternativen Beweis für die Halbeinfachheit komplexer Darstellungen: Sei V eine unitäre Darstellung und W eine Unterdarstellung. Das orthogonale Komplement $W^\perp$ ist ein G–Untermodul und es ist $V = W \oplus W^\perp$.

Sei Γ'_G der Raum *aller* Funktionen $G \to \mathbb{C}$ mit der unitären Form

$$(\alpha, \beta) = \frac{1}{n} \sum_{g \in G} \overline{\alpha(g)}\beta(g)$$

Wir fixieren eine Aufzählung $V_1, \ldots, V_k$ der irreduziblen Darstellungen und für jedes V_l eine unitäre G–invariante Struktur und eine Orthonormalbasis $v_1^l, \ldots, v_{n_l}^l$. Die Wirkung von g sei für diese Basis von der unitären Matrix

$$A^l(g) = \left(\alpha_{ij}^l(g)\right)$$

[12] Weil in S_n alle Permutationen konjugiert zu ihrem Inversen sind, sind die Werte aller Charaktere *reell* (vgl. 4.3.3).

dargestellt.

Satz 4.3.9 (Orthogonalitätsrelationen II) *Die Funktionen $\sqrt{n_l}\alpha^l_{ij}$ bilden eine Orthonormalbasis von Γ'_G.*

Beweis :
Weil wir es mit genau $n = n_1^2 + \cdots + n_k^2$ Funktionen zu tun haben, müssen wir nur zeigen, daß sie zueinander orthogonal sind und daß $(\alpha^l_{ij}, \alpha^l_{ij}) = \frac{1}{n_l}$. Der Beweis ist eine „unitäre“ Version des Beweises von 4.3.5.

Eine unitäre Form auf V vermittelt einen Isomorphismus zwischen dem konjugierten[13] Raum $V^{(c)}$ und V^*, der v auf die Linearform $x \mapsto (v, x)$ abbildet. Die konjugierte Form $\overline{(x, y)}$ ist unitär auf $V^{(c)}$. Wenn G unitär auf V und damit auch auf $V^{(c)}$ operiert, sind $V^{(c)}$ und V^* auch als G–Moduln isomorph, weil $(gv, x) = (v, g^{-1}x)$.

Wir fixieren eine zweite unitäre Darstellung W und definieren auf

$$\mathrm{Hom}_{\mathbb{C}}(V, W) \cong V^{(c)} \otimes_{\mathbb{C}} W$$

eine unitäre Form durch

$$(v_1 \otimes w_1, v_2 \otimes w_2) = \overline{(v_1, v_2)}(w_1, w_2).$$

G operiert wieder unitär auf $\mathrm{Hom}_{\mathbb{C}}(V, W)$.

Bezogen auf diese unitäre Struktur wirkt μ_G als *die* orthogonale Projektion $\mathrm{Hom}_{\mathbb{C}}(V, W) \to \mathrm{Hom}_G(V, W)$. Alle $g \in G$ lassen nämlich den Unterraum $\mathrm{Hom}_G(V, W)$ und damit auch sein orthogonales Komplement X invariant. X wird also auch von μ_G invariant gelassen, woraus die Behauptung folgt.

Sei nun (v_i) eine Orthonormalbasis von V und $(w_{i'})$ eine Orthonormalbasis von W. Dann bilden die $v_i \otimes w_{i'}$ eine Orthonormalbasis von $V^{(c)} \otimes_{\mathbb{C}} W$. Bezüglich dieser Basen wird g auf V und W durch die Matrizen

$$\alpha_{ij}(g) = (u_i, gu_j) \text{ und } \beta_{i'j'}(g) = (w_{i'}, gw_{j'})$$

dargestellt. Also ist

$$\begin{aligned}(\alpha_{ij}, \beta_{i'j'}) &= \frac{1}{n}\sum_{g\in G} \overline{(v_i, gv_j)}(w_{i'}, gw_{j'}) \\ &= \frac{1}{n}\sum_{g\in G}(v_i \otimes w_{i'}, g(v_j \otimes w_{j'})) \\ &= (v_i \otimes w_{i'}, \mu_G(v_j \otimes w_{j'}))\end{aligned}$$

Wir nehmen jetzt an, daß V und W irreduzibel sind. Wenn $V \ncong W$ ist $\mathrm{Hom}_G(V, W) = 0$. Also ist μ_G gleich Null auf $\mathrm{Hom}_{\mathbb{C}}(V, W)$ und es folgt $(\alpha_{ij}, \beta_{i'j'}) = 0$.

[13] $V^{(c)}$ ist V mit der Skalarmultiplikation $\lambda \cdot^{(c)} v = \overline{\lambda}v$. Für $V^{(c)}$ gibt es auch die Schreibweise $\overline{V}$

Wenn $V = W$, besteht $\mathrm{Hom}_G(V, V)$ aus den Vielfachen der Identität

$$1_V = v_1 \otimes v_1 + \cdots + v_m \otimes v_m,$$

wobei $m = \dim V$. Wenn $j \neq j'$, bildet μ_G, die orthogonale Projektion auf $\mathbb{C} \cdot 1_V$, $(v_j \otimes v_{j'})$ auf Null ab, also ist $(\alpha_{ij}, \alpha_{i'j'}) = 0$. Wenn $i \neq i'$, ist $(v_i \otimes v_{i'})$ orthogonal zum Bild von μ_G, woraus ebenfalls $(\alpha_{ij}, \alpha_{i'j'}) = 0$ folgt. Schließlich bemerken wir,[14] daß

$$\mu_G(v_j \otimes v_j) = \frac{1}{m} 1_V.$$

Daraus folgt

$$(\alpha_{ij}, \alpha_{ij}) = (v_i \otimes v_i, \frac{1}{m} 1_V) = \frac{1}{m}.$$

□

[14] Das folgt daraus, daß die Spur eines durch $v \otimes v'$ gegebenen Endomorphismus das Skalarprodukt (v, v') ist. Also hat $\mu_G(v_j \otimes v_j)$ die Spur 1. Andererseits ist $\frac{1}{m} 1_V$ das einzige Vielfache von 1_V, das die Spur 1 hat.

4.4 Ganzheitseigenschaften

Definition *Eine komplexe Zahl heißt ganz–algebraisch, wenn sie Nullstelle eines normierten Polynoms mit ganzzahligen Koeffizienten ist.*

Die ganzen Zahlen, alle Einheitswurzeln, alle n–ten Wurzeln aus ganzen Zahlen sind ganz–algebraisch.

Lemma 4.4.1 *Rationale ganz–algebraische Zahlen sind ganzzahlig.*

Beweis :
Sei $f(X) \in \mathbb{Z}[X]$ ein normiertes Polynom und $f = gh$ für zwei normierte Polynome aus $\mathbb{Q}[X]$. Aus 2.6.5 folgt, daß Inhalt$(f) = 1$ das Produkt der Inhalte von g und h ist. Weil die Inhalte von g und h Teiler von 1 sind, ist das nur möglich, wenn beide Inhalte 1 sind, das heißt, wenn g und h ganzzahlig sind. Insbesondere ist jeder Teiler $X - r$ ($r \in \mathbb{Q}$) ganzzahlig. □

Lemma 4.4.2 *z ist genau dann ganz–algebraisch, wenn es eine nicht–triviale, endlich–erzeugte additive Untergruppe von $\mathbb{C}$ gibt, die unter Multiplikation mit z abgeschlossen ist.*

Beweis :
Wenn z Nullstelle eines normierten ganzzahligen Polynoms von Grad n ist, gehört z^n zu der von $1, z, \ldots, z^{n-1}$ erzeugten additiven Gruppe A. A ist unter Multiplikation mit z abgeschlossen.

Sei $\mathbb{Z}a_1 + \cdots + \mathbb{Z}a_k \neq 0$ abgeschlossen unter Multiplikation mit z. Dann gibt es eine ganzzahlige Matrix $M = (m_{ij})$ mit $za_i = \sum_j m_{ij}a_j$ für $i = 1, \ldots, k$ oder

$$z \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} = M \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix}.$$

Also ist z Eigenwert von M und Nullstelle des charakteristischen Polynoms von M, das normiert und ganzzahlig ist. □

Satz 4.4.3 *Die ganz–algebraischen Zahlen bilden einen Ring.*

Beweis :
α und β seien ganz–algebraisch. A und B seien endlich erzeugte Untergruppen von $\mathbb{C}$, A sei unter Multiplikation mit α und B unter Multiplikation mit β abgeschlossen. Die von den Produkten AB erzeugte additive Untergruppe C ist wieder endlich erzeugt und abgeschlossen unter Multiplikation mit α und β. C ist also auch abgeschlossen unter Multiplikation mit $\alpha - \beta$ und $\alpha\beta$. □

Folgerung 4.4.4 *Charaktere nehmen nur ganz–algebraische Werte an.*

Beweis :
Die Werte von Charakteren sind Summen von Eigenwerten. Die Eigenwerte von Endomorphismen endlicher Ordnung sind Einheitswurzeln. □

Satz 4.4.5 *Sei χ_i ein irreduzibler Charakter der Dimension n_i, g_j ein Gruppenelement mit k_j Konjugierten. Dann ist $\frac{k_j}{n_i}\chi_i(g_j)$ ganz–algebraisch.*

Beweis :
χ_i sei der Charakter von V_i. Das Zentrum von $\mathbb{Z}[G]$ ist multiplikativ abgeschlossen und wird als additive Gruppe erzeugt von allen Summen $\sum_{g\in C} g$ von Konjugationsklassen C. Weil die $\sum_{g\in C} g$ mit allen Elementen von $\mathbb{C}[G]$ kommutieren, operieren sie auf V_i als komplexe Zahlen γ_C, die nach 4.4.2 ganz–algebraisch sind. Wenn C die Konjugationsklasse von g_j ist, ist

$$n_i\gamma_C = \mathrm{Tr}_{V_i}(\sum_{g\in C} g) = k_j\chi_i(g_j)$$

□

Folgerung 4.4.6 *Die Dimensionen n_i der irreduziblen Darstellungen teilen die Ordnung n von G.*

Beweis :
Sei $g_1, \ldots, g_k$ ein Vertretersystem der Konjugationsklassen und k_j die Größe der Konjugationsklasse von g_j. Dann ist nach 4.3.5

$$\frac{n}{n_i} = \frac{1}{n_i}\sum_{g\in G}\chi_i(g)\overline{\chi_i(g)} = \sum_{j=1}^{k}\frac{k_j}{n_i}\chi_i(g_j)\overline{\chi_i(g_j)}.$$

Aus 4.4.4 und 4.4.5 folgt, daß $\frac{n}{n_i}$ ganz–algebraisch ist. Und daher, wegen 4.4.1, ganzzahlig. □

Satz 4.4.7 (Solomon) *Sei $g_1, \ldots, g_k$ ein Vertretersystem der Konjugationsklassen, $\chi_1, \ldots, \chi_k$ die irreduziblen Charaktere von G. Dann gilt:*

1) Für jedes i ist $\sum_{j=1}^{k}\chi_i(g_j)$ eine natürliche Zahl.

2) Für jedes j ist $\sum_{i=1}^{k}\chi_i(g_j)$ eine ganze Zahl.

Beweis :
1) G operiert durch Konjugation auf sich selbst. In der zugehörigen Permutationsdarstellung V operiert G durch Permutationsmatrizen, deren Spur die Zahl der Fixpunkte der dargestellten Permutation ist. Der Charakter dieser Darstellung ist daher

$$\chi_V(g_j) = \#\mathrm{C}_G(g_j) = \frac{n}{k_j}.$$

Also ist $\sum_j \chi_i(g_j) = (\chi_V, \chi_i)$ die Vielfachheit von V_i in V, und damit eine natürliche Zahl.

2) Sei ϕ ein Automorphismus von $\mathbb{C}$ und V eine Darstellung von G mit Charakter χ. Wenn wir die Skalarmultiplikation umdefinieren durch $\lambda \cdot^{\phi} v = \phi(\lambda)v$, erhält man ein Darstellung V^{ϕ} mit dem Charakter $\phi(\chi)$. Wenn V irreduzibel ist, ist auch V^{ϕ} irreduzibel. ϕ permutiert also die irreduziblen Charaktere. Daher ist

$$\phi(\sum_i \chi_i) = \sum_i \phi(\chi_i) = \sum_i \chi_i.$$

Weil nur rationale Zahlen von allen Automorphismen von $\mathbb{C}$ festgehalten werden[15], müssen die Werte von $\sum_i \chi_i$ rationale Zahlen und, wegen 4.4.1 und 4.4.4, ganze Zahlen sein. □

[15]Das ist nicht so einfach einzusehen. Man kann aber $\mathbb{C}$ durch den algebraischen Abschluß $\widetilde{\mathbb{Q}}$ von $\mathbb{Q}$ ersetzen. Es ist klar, daß nur die Elemente von $\mathbb{Q}$ von allen Automorphismen von $\widetilde{\mathbb{Q}}$ fixiert werden.

Index

Entstehung

Die ersten drei Kapitel sind aus dem Skript einer Algebravorlesung im Sommersemester 1995 entstanden. Die im April 1996 publizierte Version war von Gunter Geisler durchgesehen worden.

Im Wintersemester 1999/2000 kam das vierte Kapitel hinzu. Zwei Hörer der Vorlesung habe ich für Fehlerlisten zu danken: S. Holzmann (Version 2d) und O. Schnürer (Version 3c). In Version 3c wurde auch Folgerung 4.1.9 richtiggestellt[1].

In Version 3d wurde nur das Inhaltsverzeichnis geändert und kleine Druckfehler, die zum Teil von L. Stieber gefunden wurden, beseitigt.

Viele Fehler in Version 3e wurden von Nina Frohn gefunden. Rechts- und Linksnebenklassen richtig definiert.

Version 3f enthält einen Beweis des Jordan-Höldersatzes, der den Verfeinerungssatz von Schreier nicht benutzt. Der Beweis von 1.10.1 wurde gekürzt. Die Formel für $\deg(fg)$ auf Seite 43 wurde korrigiert. Der Beweis von 2.5.5 wurde geändert.

In Version 3g gibt es jetzt das Eisensteinkriterium. In Version 3h wurde ein Druckfehler in Beweis von Folgerung 4.3.6 verbessert, den M. Biehl gefunden hat. In Version 3i wurde die Notation im Beweis von Lemma 4.1.1 verbessert. In Version wurde dem Beweis von 4.3.9 eine erklärende Fußnote angefügt.

[1] Orthographien, die hier „richtig gestellt“ vorschlagen, sollte man lieber nicht verwenden.