OSNABRÜCKER SCHRIFTEN ZUR MATHEMATIK

Reihe V Vorlesungsskripten

EHeft 8 Sommersemester 2001

Einführung in die Algebra

W. Bruns

Fachbereich Mathematik/Informatik
Universität Osnabrück

OSM Osnabrücker Schriften zur Mathematik

März 2002

Herausgeber	Selbstverlag der Universität Osnabrück Fachbereich Mathematik/Informatik 49069 Osnabrück
Geschäftsführer	Prof. Dr. W. Bruns
Berater:	Prof. Dr. P. Brucker (Angew. Mathematik) Prof. Dr. E. Cohors-Fresenborg (Didaktik der Mathematik) Prof. Dr. V. Sperschneider (Informatik) Prof. Dr. R. Vogt (Reine Mathematik)
Druck	Hausdruckerei der Universität Osnabrück

Weitere Reihen der OSM:

Reihe D	Mathematisch-didaktische Manuskripte
Reihe I	Manuskripte der Informatik
Reihe M	Mathematische Manuskripte
Reihe P	Preprints
Reihe U	Materialien zum Mathematikunterricht

Einführung in die Algebra

Winfried Bruns

Skript zur Vorlesung SS 2001

Inhaltsverzeichnis

ABSCHNITT 1

Ringe

Wir ergänzen in diesem Abschnitt die in der Linearen Algebra (im folgenden als [LA] zitiert) eingeführten Begriffe. Zunächst eine Abschwächungen des Begriffs „Gruppe“: Eine Menge H mit einer assoziativen Verknüpfung nennt man auch eine *Halbgruppe*, und wenn H ein neutrales Element hat, spricht man von einem *Monoid*. Diese Begriffe sind so allgemein, daß es kaum möglich ist, eine Theorie ohne zusätzliche Einschränkungen an die betrachteten Halbgruppen oder Monoide aufzubauen. Immerhin können wir für Monoide M folgendes feststellen:

(a) Das neutrale Element ist eindeutig bestimmt.
(b) Wenn $a \in M$ ein inverses Element besitzt, so ist dieses eindeutig bestimmt.
(c) Wir können (bei multiplikativer Schreibweise der Verknüpfung) *Potenzen* der Elemente $a \in M$ definieren: Wir setzen $a^0 = 1$ und definieren rekursiv $a^{n+1} = a^n a$ für $n \in \mathbb{N}$, $n \geq 1$. Besitzt a ein Inverses a^{-1}, so kann man $a^n = (a^{-1})^n$ für $n \in \mathbb{Z}$, $n < 0$, setzen.
(d) Es gelten die Potenzrechenregeln

$$a^{m+n} = a^m a^n, \qquad (a^m)^n = a^{mn},$$

und, falls $ab = ba$, $(ab)^n = a^n b^n$. Dabei sind $a, b \in M$ und $m, n \in \mathbb{N}$ (oder gegebenenfalls $\in \mathbb{Z}$).

Bei additiver Schreibweise (dies impliziert in der Regel die Kommutativität) spricht man wie gewohnt von *Vielfachen* und schreibt analog na. (Vergleiche auch dazu [LA].)

Vektorräume sind abelsche Gruppen bezüglich ihrer Addition. Zusätzlich hat man eine – mit dieser Addition verträgliche – Multiplikation mit Skalaren. Etwas anders ist die Situation bei einem Körper K: Hier hat man auf K selbst zwei Verknüpfungen, eine Addition und eine Multiplikation; bezüglich der Addition ist K eine abelsche Gruppe, bezüglich der Multiplikation ist $K \setminus \{0\}$ eine abelsche Gruppe, und es gelten die Distributivgesetze (vgl. [LA]). Ähnlich hat man z.B. auf $\mathbb{Z}$ eine Addition und eine Multiplikation derart, daß $(\mathbb{Z}, +)$ eine abelsche Gruppe ist und $(\mathbb{Z}, \cdot)$ immerhin ein kommutatives Monoid; außerdem gelten die gleichen Distributivgesetze wie bei einem Körper. Allerdings gibt es nicht zu jedem von 0 verschiedenen Element aus $\mathbb{Z}$ ein Inverses bezüglich der Multiplikation. Wir verallgemeinern den Begriff „Körper“ daher wie folgt:

Definition. Es sei R eine Menge, auf der zwei Verknüpfungen erklärt sind, eine Addition $+$ und eine Multiplikation $\cdot$. Dann heißt $(R,+,\cdot)$ ein *Ring*, wenn gilt:

(a) $(R,+)$ ist eine abelsche Gruppe.
(b) $(R,\cdot)$ ist ein Halbgruppe mit neutralem Element.
(c) Es gelten die *Distributivgesetze*:

$$a(b_1+b_2)=ab_1+ab_2, \quad (a_1+a_2)b=a_1b+a_2b$$

für alle $a,b_1,b_2,a_1,a_2,b\in R$.

Ist $(R,\cdot)$ kommutativ, dann heißt $(R,+,\cdot)$ ein *kommutativer* Ring.

Bemerkung 1.1. Zur Vermeidung von Klammern vereinbart man, daß die Multiplikation in einem Ring stärker bindet als die Addition ($ab+cd$ bedeutet demnach $(ab)+(cd)$). Ferner schreiben wir R statt $(R,+,\cdot)$, wenn klar ist, um welche Ringstruktur auf R es sich handelt. Wie allgemein üblich bei additiv notierter Gruppenverknüpfung, bezeichnen wir das neutrale Element von $(R,+)$ mit 0 und sprechen vom *Nullelement* oder der *Null* von R; das neutrale Element von $(R,\cdot)$ heißt *Eins* oder *Einselement* und wird in der Regel mit 1 bezeichnet, zur besseren Unterscheidung manchmal auch mit 1_R.

Beispiele. Wie oben schon gesagt, ist $\mathbb{Z}$, versehen mit der üblichen Addition und Multiplikation, ein Ring. Jeder Körper ist ein Ring. Ein anderer aus [LA] bekannter Ring ist der Polynomring $K[X]$ über einem Körper K. (Polynomringe werden wir später noch gründlich diskutieren.)

Jede einelementige Menge $\{a\}$ läßt sich zu einem Ring machen: Man setzt $a+a=aa=a$; da a notwendig das Nullelement dieses Ringes (natürlich auch sein Einselement) ist, heißt dieser Ring *Nullring* (und wird einfach mit 0 bezeichnet). Der Nullring ist der einzige Ring, in dem Null und Eins übereinstimmen.

Interessanter ist der Ring $M(n\times n;K)$ aller $(n\times n)$-Matrizen über einem Körper K; Addition und Multiplikation sind hier die Matrizenaddition und Matrizenmultiplikation. Für $n\geq 2$ ist dieser Ring nicht kommutativ – ein Paradebeispiel ebenso wie der aus [LA] bekannte Schiefkörper $\mathbb{H}$ der Quaternionen.

Der Beweis der folgenden Regeln verläuft wörtlich so wie der in [LA] geführte Beweis bei einem Körper.

Satz 1.2 (Vorzeichenregeln)**.** *Es seien R ein Ring und a, b Elemente von R. Dann gilt:*

(a) $a0=0a=0$;
(b) $a(-b)=(-a)b=-ab$;
(c) $(-a)(-b)=ab$.

Für einen Ring R sind die ganzahligen Vielfachen der Elemente von R wohldefiniert, und zwar weil R bezüglich der Addition eine Gruppe ist. Dies haben wir

auch schon in [LA] diskutiert und oben noch einmal wiederholt. Eine zusätzliche Regel für Vielfache, bei der nun die Ringstruktur eingeht, ist

$$(mn)a = m(na).$$

Wir überlassen den Beweis dem Leser.

Zwischen den Körpern als den „stärksten“ Ringen und Ringen ganz allgemein kann man viele Zwischenstufen betrachten. Eine besonders wichtige führen wir nun ein:

Definition. Das Element a des Ringes R heißt ein *Nullteiler*, wenn es ein Element $b \in R$, $b \neq 0$, gibt mit $ab = 0$ oder $ba = 0$. Besitzt R keine von 0 verschiedenen Nullteiler, so heißt R *nullteilerfrei*. Ist $R \neq 0$ ein nullteilerfreier, kommutativer Ring, dann heißt R ein *Integritätsbereich* (oder *Integritätsring*).

In Integritätsberecihen kann man kürzen:

Satz 1.3. *Ein kommutativer Ring R ist genau dann ein Integritätsbereich, wenn in ihm die Kürzungsregel*

$$ab = ac,\ a \neq 0 \implies b = c$$

gilt.

Beweis. Ist a ein Nullteiler, $ab = 0$ für $b \neq 0$, so ist die Kürzungsregel wegen $ab = a0$ sicherlich verletzt. Für die Umkehrung hat man nur zu beachten, daß $a(b-c) = 0$, wenn $ab = ac$. □

Der Ring $\mathbb{Z}$ ist ein Integritätsbereich. Jeder Körper K ist ein Integritätsbereich und ebenso der Polynomring $K[X]$. Hingegen ist der Matrizenring $M(n \times n; K)$ für $n \geq 2$ nicht nullteilerfrei. (Jede Matrix vom Rang $< n$ ist ein Nullteiler. Beweis?)

$R \neq 0$ sei ein Ring. Die invertierbaren Elemente in dem Monoid $(R, \cdot)$ heißen *Einheiten* von R. Natürlich sind Einheiten niemals Nullteiler. Die Menge aller Einheiten von R ist offensichtlich eine Gruppe bezüglich der Multiplikation von R, die *Einheitengruppe* R^* von R. Beispielsweise ist $\mathbb{Z}^* = \{-1, 1\}$ und $M(n \times n; K)^* = \mathrm{GL}(n; K)$. Bei kommutativem R gilt genau dann $R^* = R \setminus \{0\}$, wenn R ein Körper ist.

Eine unscheinbare, aber nicht unwichtige Aussage:

Satz 1.4. *Jeder endliche Integritätsbereich R ist ein Körper.*

Beweis. Für $a \in R$, $a \neq 0$, betrachten wir die Abbildung $\mu_a : R \to R$, $\mu_a(b) = ab$. Die Kürzungsregel besagt gerade, daß μ_a injektiv ist. Da R endlich ist, ist μ_a dann auch surjektiv. Es gibt also ein b mit $1 = \mu_a(b) = ab$. □

Wir verallgemeinern nun den in [LA] eingeführten Begriff der Charakteristik.

Definition. Es sei R ein Ring. $\operatorname{ord}_+ a$ bezeichne die Ordnung des Elementes $a \in R$ in der Gruppe $(R,+)$. Unter der *Charakteristik* von R versteht man die natürliche Zahl

$$\operatorname{char} R = \begin{cases} 0, & \text{falls } \operatorname{ord}_+ a = \infty \text{ für alle } a \in R, a \neq 0, \\ \min\{\operatorname{ord}_+ a \mid a \in R, a \neq 0\} & \text{andernfalls .} \end{cases}$$

Es ist klar, daß die Charakteristik eines Ringes R immer von 1 verschieden ist. Es sei $p = \operatorname{char} R > 0$. Dann gibt es ein $b \in R,\ b \neq 0$, mit $pb = 0$. Wenn $p = mn$ gilt mit positiven ganzen Zahlen m, n, so hat man $0 = pb = (mn)b = m(nb)$. Nach Definition der Charakteristik folgt hieraus $n = p$ oder $n = 1$, d.h. p ist Primzahl.

Satz 1.5. *Die Charakteristik eines Ringes R ist entweder 0 oder eine Primzahl. Ist R ein Integritätsbereich und* $\operatorname{char} R > 0$*, so gilt* $\operatorname{char} R = \operatorname{ord} 1_R$ *und* $(\operatorname{char} R)a = 0$ *für alle $a \in R$.*

Beweis. Es sei R ein Integritätsbereich, $p = \operatorname{char} R > 0$ und $b \in R$, $b \neq 0$, mit $pb = 0$. Es ist $pb = p(1_R b) = (p1_R)b$. Da R ein Integritätsbereich und $b \neq 0$ ist, gilt $p1_R = 0$ und damit auch $pa = p(1_R a) = (p1_R)a = 0$ für alle $a \in R$. □

Die Ringe $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ sind Beispiele für Integritätsbereiche der Charakteristik 0. Ein einfaches Beispiel für einen Körper der Charakteristik 2 ist der wohlbekannte Körper mit 2 Elementen.

Ähnlich wie der Begriff Untergruppe wird der Begriff des Unterringes eingeführt.

Definition. Eine Teilmenge S des Ringes R heißt ein *Unterring* von R, wenn gilt:

(a) $1_R \in S$;
(b) Addition und Multiplikation von R lassen sich auf S beschränken, und S ist bezüglich dieser induzierten Verknüpfungen ein Ring.

Offenbar ist S genau dann ein Unterring des Ringes R, wenn gilt: Es ist $1_R \in S$, und für alle a, $b \in S$ liegen sowohl $a - b$ als auch ab wieder in S. Der Begriff *Teilkörper* wird entsprechend eingeführt.

Der einzige Unterring von $\mathbb{Z}$ ist $\mathbb{Z}$ selbst. $M(n \times n; \mathbb{R})$ ist ein Unterring von $M(n \times n; \mathbb{C})$. $\mathbb{Q}$ ist Teilkörper von $\mathbb{R}$. Jeder Körper ist Unterring von $K[X]$ (wobei wir Elemente von K mit den konstanten Polynomen identifizieren.)

In Analogie zur direkten Summe von Vektorräumen definiert man das *direkte Produkt* $R_1 \times R_2$ von Ringen R_1, R_2, indem man für Elemente $(a_1, a_2), (b_1, b_2)$ des kartesischen Produkts $R_1 \times R_2$ definiert:

$$(a_1, a_2) + (b_1, b_2) = (a_1 + b_1, a_2 + b_2), \qquad (a_1, a_2)(b_1, b_2) = (a_1 b_1, a_2 b_2).$$

Mit R_1 und R_2 ist auch $R_1 \times R_2$ kommutativ. Es ist aber fast nie ein Integritätsbereich (ausgenommen welche Situation?). Man beachte, daß die Einbettung $R_1 \to R_1 \times R_2$, $r \mapsto (r, 0)$, den Ring R_1 *nicht* zu einem

Unterring von $R_1 \times R_2$ macht, ausgenommen R_2 ist der Nullring: $1_{R_1 \times R_2} = (1,1)$ liegt nicht in der betrachteten Teilmenge.

ABSCHNITT 2

Homomorphismen, Ideale und Restklassenringe

Definition. Eine Abbildung $\varphi\colon R \to R'$ von Ringen heißt ein (*Ring-*) *Homomorphismus,* wenn für alle $a, b \in R$ gilt:

$$\varphi(a+b) = \varphi(a) + \varphi(b), \quad \varphi(ab) = \varphi(a)\varphi(b) \quad \text{und} \quad \varphi(1_R) = 1_{R'}.$$

Ein bijektiver Homomorphismus φ ist ein *(*Ring-*)Isomorphismus*. Der Ring R heißt *isomorph* zum Ring R', wenn es einen Isomorphismus von R auf R' gibt.

Bemerkung 2.1. Sei $\varphi\colon R \to R'$ ein Homomorphismus von Ringen. Dann ist φ insbesondere ein Homomorphismus der Gruppe $(R,+)$ in die Gruppe $(R',+)$. Hieraus folgt z.B. $\varphi(0) = 0$, und φ ist genau dann injektiv, wenn $\operatorname{Kern}\varphi = \{0\}$ gilt.

In Analogie zu Gruppenhomomorphismen (vgl. dazu [LA]) gilt: die Komposition von Homomorphismen ergibt wieder einen Homomorphismus. Die Umkehrabbildung eines Isomorphismus ist ein Homomorphismus und daher ein Isomorphismus. Die Isomorphie von Ringen ist folglich eine Äquivalenzrelation.

Die Begriffe (*Ring-*)*Endomorphismus* und (*Ring-*)*Automorphismus* werden analog den entsprechenden Begriffen in der Linearen Algebra eingeführt.

Beispiele. (a) Es seien R und R' Ringe. Das Bild eines Homomorphismus von R in R' ist ein Unterring von R'. Eine Teilmenge $R \subset R'$ ist genau dann ein Unterring von R', wenn die natürliche Injektion $R \to R'$ ein Homomorphismus ist.

(b) Sei K ein Körper und V ein K-Vektorraum. Wir haben in [LA] gesehen, daß die Summe und die Komposition zweier Endomorphismen von V (also linearen Abbildungen $V \to V$) wieder Endomorphismen sind. Ferner ist $\operatorname{End}(V)$ sogar ein K-Vektorraum, also $(\operatorname{End}(V),+)$ bestimmt eine abelsche Gruppe. Da id_V neutral ist bezüglich der Komposition und die Distributivgesetze gelten, ist $(\operatorname{End}(V),+,\circ)$ ein Ring.

Wir nehmen nun an, daß $\dim V = n < \infty$ und $v_1,\ldots,v_n$ eine Basis von V ist. Jedem Endomorphismus sei seine Matrix bezüglich $v_1,\ldots,v_n$ zugeordnet. Diese Zuordnung ist mit Addition und Multiplikation verträglich, und stellt sich als ein Isomorphismus $\operatorname{End}(V) \to M(n\times n, K)$ heraus.

(c) Die Zuordnung $n \mapsto n1_R$ ist für jeden Ring R ein Homomorphismus $\mathbb{Z} \to R$. Dies folgt aus den Rechenregeln für Vielfache.

(d) Wir können das Beispiel (c) noch etwas ausbauen, indem wir die Regeln für das Rechnen mit Vielfachen in einer *abelschen* Gruppe $(G,+)$ als Homomorphie-Eigenschaft einer Abbildung interpretieren. Sei $R = \mathrm{End}(G)$. Wie bei Vektorräumen folgt, daß $(\mathrm{End}(G),+,\circ)$ ein Ring ist. (Die Vektorraum-Struktur fehlt natürlich.)

Wir definieren

$$\Phi : \mathbb{Z} \to R \quad \text{durch} \quad \Phi(n)(a) = na$$

für alle $n \in \mathbb{Z}$ und alle $a \in G$. In der Tat ist $\Phi(n)$ für jedes $n \in \mathbb{Z}$ ein Element von R, weil $n(a+b) = na+nb$ für $n \in \mathbb{Z}$ und $a,b \in G$ gilt. Die Regel $(mn)a = m(na)$ bedeutet einfach, daß Φ die Bedingung $\Phi(mn) = \Phi(m)\Phi(n)$ erfüllt, und schließlich besagt $(m+n)a = ma+na$, daß auch $\Phi(m+n) = \Phi(m)+\Phi(n)$ ist. Also ist Φ ein Homomorphismus von Ringen. Genau dann ist Φ injektiv, wenn jedes Element von G endliche Ordnung hat.

Es sei $\varphi : R \to R'$ ein Homomorphismus von Ringen. Dann ist natürlich $\mathrm{Kern}\,\varphi$ eine Untergruppe von $(R,+)$. Es gilt aber noch mehr: Für beliebige Elemente $r \in R$ und $a \in \mathrm{Kern}\,\varphi$ ist sowohl ra als auch ar wieder ein Element von $\mathrm{Kern}\,\varphi$, denn $\varphi(a) = 0$ impliziert $\varphi(ra) = \varphi(r)\varphi(a) = \varphi(r)0 = 0$, und ebenso ist $\varphi(ar) = 0$.

Definition. Es sei R ein Ring. Eine nichtleere Teilmenge I von R heißt ein (zweiseitiges) *Ideal*, wenn gilt:

(a) Mit $a,b \in I$ ist auch $a-b \in I$;

(b) Mit $a \in I$ und $r \in R$ hat man auch $ra \in I$ und $ar \in I$.

Ein Ideal im Ring R ist also eine Untergruppe von $(R,+)$, für die zusätzlich die Bedingung (b) der Definition erfüllt ist. Als erstes Beispiel haben wir: Kerne von Ringhomomorphismen sind Ideale. Weitere einfache Beispiele sind das *Nullideal* 0 von R, das nur aus der Null besteht, und R selbst, das sogenannte *Einsideal*. Eine Teilmenge des Ringes $\mathbb{Z}$ ist genau dann ein Ideal, wenn sie eine Untergruppe von $(\mathbb{Z},+)$ ist, d.h. von der Form $\mathbb{Z}m$ mit einem $m \in \mathbb{Z}$. (Im allgemeinen ist das natürlich nicht richtig; Beispiel?)

Bedingung (a) kann man durch die folgende Bedingung ersetzen (weshalb?):

(a′) Mit a, $b \in I$ gilt auch $a+b \in I$.

Ist R kommutativ, dann genügt es statt (b) zu fordern:

(b′) Mit $a \in I$ und $r \in R$ gilt auch $ra \in I$.

Im allgemeinen ist (b′) jedoch schwächer als (b): Die Teilmenge $J = \{(a_{ij}) \in M(2\times 2;\mathbb{R}) \mid a_{12} = a_{22} = 0\}$ von $M(2\times 2;\mathbb{R})$ genügt den Bedingungen (a) und (b′), ist aber kein Ideal in diesem Ring.

Es sei R ein Ring und $(I_j)_{j\in J}$ eine Familie von Idealen in R. Dann ist sofort zu sehen, daß auch $\bigcap_{j\in J} I_j$ wieder ein Ideal in R ist. Ist insbesondere M eine beliebige Teilmenge von R, dann ist der Durchschnitt $I(M)$ aller M umfassenden Ideale von

R ebenfalls ein Ideal in R, *das von M erzeugte Ideal* von R. Es ist dies das kleinste M umfassende Ideal von R. Offenbar gilt $I(\emptyset) = 0$. Gilt $M \neq \emptyset$, dann besteht $I(M)$ aus allen Summen

$$a_1 f_1 b_1 + \cdots + a_n f_n b_n$$

mit a_j, $b_j \in R$, $f_j \in M$. Die Teilmenge M von R heißt ein *Erzeugendensystem* des Ideals I, wenn $I(M) = I$ gilt.

Für Ideale I_1, I_2 können wir wie für Untervektorräume die *Summe*

$$I_1 + I_2 = \{r_1 + r_2 : r_1 \in I_1, r_2 \in I_2\}$$

betrachten. Sie ist wieder ein Ideal, und zwar gilt $I_1 + I_2 = I(I_1 \cup I_2)$. Wie Durchschnitte kann man auch Summen $\sum_{j\in J} I_j$ einer Familie von Idealen bilden.

Eine weitere nützliche Operation für Ideale ist das Produkt

$$I_1 I_2 = I(\{r_1 r_2 : r_1 \in I_1, r_2 \in I_2\}).$$

Die Produktbildung können wir auf endlich viele Ideale erweitern.

Ein Beispiel: Sei $R = \mathbb{Z}$, $I_1 = I(4)$, $I_2 = I(6)$. Dann ist

$$I_1 + I_2 = I(2), \quad I_1 \cap I_2 = I(12), \quad I_1 I_2 = I(24).$$

Wir werden die idealtheoretischen Operationen später mit den zahlentheoretischen Begriffen „größter gemeinsamer Teiler“ und „kleinstes gemeinsames Vielfaches“ in Beziehung setzen (jedenfalls in $\mathbb{Z}$ und geeigneten anderen Ringen).

Im kommutativen Fall, an dem wir hauptsächlich interessiert sind, verwenden wir stets die Schreibweise

$$I(f_1, \ldots, f_n) = Rf_1 + \cdots + Rf_n.$$

Dies macht offensichtlich Sinn.

Zur Motivation der nun folgenden Konstruktion wollen wir den Anfang eines zahlentheoretischen Problems betrachten, nämlich der Frage nachgehen, welche $n \in \mathbb{N}$ sich in der Form $x^2 + y^2$ mit $x, y \in \mathbb{Z}$ darstellen lassen. Wir behaupten: Dies ist sicher nicht möglich, wenn n bei Division durch 4 den Rest 3 läßt. Wir schreiben dazu $x = 4m + r$, $y = 4n + s$, $0 \leq r, s < 4$. Dann ist

$$x^2 + y^2 = 16m^2 + 8mr + r^2 + 16n^2 + 8ns + s^2.$$

Wenn wir den Divionsrest von $x^2 + y^2$ ermitteln wollen, können wir alle Vielfachen von 4 in der Summe vergessen. Wir brauchen also nur die 16 Summen $r^2 + s^2$ auf ihre Divisonsreste hin durchprüfen. Und selbst das läßt sich noch vereinfachen. Wir schreiben

$$r = 2a + b, \qquad s = 2c + d, \qquad a, b, c, d \in \{0, 1\},$$

und haben nun nur noch vier Summen $b^2 + d^2$ zu prüfen. Diese haben aber nur die Werte $0, 1, 2$. Das angewandte Prinzip: Vielfache von 4 werden systematisch vernachlässigt.

Eleganter könnte man so vorgehen. Angenommen, es gibt einen Ringhomomorphismus $\pi : \mathbb{Z} \to S$ mit folgender Eigenschaft: $\pi(u) = \pi(v)$ genau dann, wenn $u - v$ ein Vielfaches von 4 ist, mit anderen Worten: wenn $u - v$ im Ideal $\mathbb{Z}4$ liegt. Dann können wir unser Problem in S lösen, denn

$$\pi(x^2 + y^2) = \pi(x)^2 + \pi(y)^2,$$

und wenn wir zeigen können, daß die rechte Seite stets ungleich $\pi(3)$ ist, haben wir das gewünschte Ergebnis. Der gesuchte Homomorphismus muß einfach die Bedingung $\operatorname{Kern}\pi = \mathbb{Z}4$ erfüllen.

Wie wir jetzt sehen werden, ist es für jeden Ring R und jedes Ideal I möglich, einen Ring S und einen Homomorphismus $\pi : R \to S$ mit $\operatorname{Kern}\pi = I$ zu konstruieren. Wir wissen aus [LA], daß im Fall $I = \operatorname{Kern}\pi$ das Urbild von $\pi(x)$ unter π durch

$$\pi^{-1}(\pi(x)) = x + \operatorname{Kern}\pi = x + I$$

gegeben ist, wenn $I = \operatorname{Kern}\pi$ ist. Mit anderen Worten, es gilt:

$$\pi(x) = \pi(y) \iff y \in x + I. \qquad (*)$$

Um dies zu erreichen, definieren wir eine neue Menge:

$$R/I = \{x + I : x \in R\}.$$

Die Elemente von R/I sind also Teilmengen von R. Diese zunächst „schwierig“ anmutende Tatsache kann man nach Abschluß der Konstruktion wieder vergessen – es kommt nur auf die Eigenschaften des neu konstruierten Obkjekts an.

Wir betrachten nun die Abbildung $\pi : R \to R/I$, $\pi(x) = x + I$, und weisen zunächst nach, daß sie die gewünschte Eigenschaft hat. Sei $\pi(x) = \pi(y)$. Dies bedeutet nach Definition von π, daß $x + I = y + I$ ist. Wegen $0 \in I$ gilt dann speziell $y \in x + I$, womit eine Richtung von $(*)$ nachgewiesen ist.

Sei umgekehrt $y \in x + I$, $y = x + a$ mit $a \in I$. Für jedes $b \in I$ ist dann $y + b = x + a + b \in x + I$, denn $a + b \in I$. Folglich gilt $y + I \subset x + I$. Für die umgekehrte Inklusion beachten wir, daß $x = y - a \in y + I$, denn $-a \in I$. Dies impliziert, wie schon gesehen, daß $x + I \subset y + I$, und insgesamt gilt $x + I = y + I$, also $\pi(x) = \pi(y)$, so daß die Eigenschaft $(*)$ für unsere Abbildung π tatsächlich erfüllt ist.

Um π zu einem Ringhomomorphismus zu machen, brauchen wir noch eine Ringstruktur auf R/I. Wir setzen dazu

$$(x + I) + (y + I) = (x + y) + I, \qquad (x + I) \cdot (y + I) = xy + I.$$

So glatt sich diese Definition liest: Sie hat einen Haken, denn wir definieren diese Verknüpfungen mittels ausgewählter Elemente in $x + I$ und $y + I$.

Eine ähnliche Situation ist uns schon aus der Schule bekannt: Um Summe und Produkt zweier Brüche zu definieren, müssen wir eine Darstellung des Bruches mit Zähler und Nenner heranziehen. Summe und Produkt machen nur dann Sinn,

wenn das Ergebnis nur von den beteiligten Brüchen, nicht aber von der Auswahl der Zähler und Nenner abhängt.

Ähnliches gilt aber auch hier. Wenn $x+I = x'+I$, $y+I = y'+I$, $x' = x+a$, $y' = y+b$, mit $a,b \in I$, so folgt

$$x'+y' = (x+a)+(y+b) = x+y+(a+b) \in (x+y)+I,$$

und wie bereits gezeigt, ergibt sich daraus $(x'+y')+I = (x+y)+I$. Ferner ist

$$x'y' = (x+a)(y+b) = xy+(xb+ay+ab),$$

und weil I nicht nur eine Untergrupppe von $(R,+)$, sondern sogar ein Ideal ist, gilt $xb+ay+ab \in I$, also $x'y' \in xy+I$, was wiederum $x'y'+I = xy+I$ nach sich zieht.

Die Ringstruktur auf R/I ist definiert und π ist sogar ein surjektiver Homomorphismus! Die Surjektivität ist klar, denn $x+I = \pi(x)$ und die Homomorphie folgt aus

$$\begin{aligned} \pi(x+y) &= (x+y)+I = (x+I)+(y+I) = \pi(x)+\pi(y), \\ \pi(xy) &= xy+I = (x+I)(y+I) = \pi(x)\pi(y). \end{aligned}$$

Dabei ergeben sich das erste und das dritte Gleichheitszeichen aus der Definition von π, das mittlere aus der Definition von Addition und Multiplikation in R/I. Offensichtlich ist $1+I$ das Einselement von R/I, also $\pi(1) = 1$. Ferner ist $\operatorname{Kern}\pi = I$, wie wir schon gesehen haben. Aber noch einmal: $\pi(x) = 0 = \pi(0)$ genau dann, wenn $x \in 0+I$, also $x \in I$.

An dieser Stelle kann man die konkrete Konstruktion von R/I (fast) vergessen. Man muß nur wissen: R/I ist ein Ring und es gibt einen surjektiven Homomorphismus $\pi : R \to R/I$ mit $\operatorname{Kern}\pi = I$.

Satz 2.2. *Es sei R ein Ring, I ein Ideal in R. Dann ist R/I mit den oben definierten Verknüpfungen ein Ring, und die Abbildung $\pi : R \to R/I$, $\pi(x) = x+I$, ist ein surjektiver Ringhomomorphismus mit* $\operatorname{Kern}\pi = I$. *Ist R kommutativ, dann ist auch R/I kommutativ.*

Die Aussage über die Kommutativität ist trivial.

Definition. R sei ein Ring und I ein Ideal in R. Der Ring R/I heißt *Faktor-* oder *Restklassenring* von R *nach* oder *modulo* I. Das Element $x+I$ heißt *Restklasse* von x *nach* oder *modulo* I.

Wir haben oben gezeigt, ohne dies hervorzuheben, daß R disjunkte Vereinigung der Restklassen ist. Bei jeder Abbildung $\varphi : R \to S$ zerfällt der Definitionsbereich ja in die Urbildmengen $\varphi^{-1}(\varphi(x))$, $x \in R$. Man nennt $\varphi^{-1}(\varphi(x))$ anschaulich die *Faser* von x bezüglich φ. Man kann dies auch noch so beschreiben: Die Relation $x \sim y \iff x-y \in I$ ist eine Äquivalenzrelation auf R, und die Restklassen sind gerade die Klassen von $\sim$.

Um die Definition von R/I in den Hintergrund treten zu lassen, sollte man die Schreibweise $x+I$ vermeiden, sondern einfach $\bar{x}$ verwenden. Der Nachteil ist allerdings, daß man das Ideal I dann nicht mit aufführen kann, so daß klar sein muß, wie I gewählt ist.

Wir kommen zurück zu unserem Beispiel $R=\mathbb{Z}$, $I=\mathbb{Z}4$. Es gibt dann offensichtlich 4 Restklassen, nämlich die von $0,1,2,3$:

$$\begin{aligned}\bar{0} &= 0+\mathbb{Z}4 = \{\dots,-8,-4,0,4,8,\dots\}\\ \bar{1} &= 1+\mathbb{Z}4 = \{\dots,-7,-3,1,5,9,\dots\}\\ \bar{2} &= 2+\mathbb{Z}4 = \{\dots,-6,-2,2,6,10,\dots\}\\ \bar{3} &= 3+\mathbb{Z}4 = \{\dots,-5,-1,3,7,11,\dots\}.\end{aligned}$$

Ist allgemeiner $m\in\mathbb{Z}$, $m>0$, so besitzt $\mathbb{Z}_m=\mathbb{Z}/\mathbb{Z}m$ genau m Elemente, nämlich die Restklassen von $0,\dots,m-1$. Es ist aber häufig sinnvoll, nicht nur mit diesen Repräsentanten zu arbeiten, sondern z.B. die Restklasse von -1 nicht durch $m-1$ zu repräsentieren, sondern durch -1. An diesem Beispiel sehen wir, woher die Bezeichnung „Restklasse“ kommt: x und y haben genau dann die gleiche Restklasse, wenn sie bei Division durch m den gleichen Rest lassen. In der Zahlentheorie (und nicht nur dort) schreibt man nach Gauß

$$x\equiv y \mod m \quad \text{oder} \quad x\equiv y \ (m),$$

wenn x und y die gleiche Restklasse modulo m besitzen.

Mittels der Ringe $\mathbb{Z}/\mathbb{Z}m$ können wir interessante neue Beispiele konstruieren, für die es keine „natürlichere“ Beschreibung gibt.

Satz 2.3. *Es sei $m\geq 2$. Dann sind die folgenden Eigenschaften äquivalent:*

(a) *$\mathbb{Z}_m$ ist ein Integritätsbereich.*
(b) *$\mathbb{Z}_m$ ist ein Körper.*
(c) *m ist Primzahl.*

Beweis. Da $\mathbb{Z}_m$ endlich ist, sind (a) und (b) wegen Satz 1.4 äquivalent.

Ist m keine Primzahl, dann gibt es $a,b\in\mathbb{Z}$ mit $1<a,\ b<m$ und $m=ab$. Bezeichnet $\pi:\mathbb{Z}\to\mathbb{Z}_m$ die natürliche Projektion, so hat man $\pi(a)\neq 0\neq\pi(b)$, aber $\pi(a)\pi(b)=\pi(m)=0$; $\mathbb{Z}_m$ ist also kein Integritätsbereich. Umgekehrt sei m Primzahl. Es gelte $\pi(a)\pi(b)=0$ für $a,b\in\mathbb{Z}$, also $\pi(ab)=0$. Dann heißt das $ab\in\mathbb{Z}m$. Da m Primzahl ist, folgt: m teilt a oder m teilt b. Das bedeutet aber $\pi(a)=0$ oder $\pi(b)=0$. $\mathbb{Z}_m$ ist also Integritätsbereich.

Die soeben benutzte Eigenschaft von Primzahlen werden wir in Abschnitt 4 noch aus der Division mit Rest herleiten. □

Es sei $\varphi:R\to R'$ ein Homomorphismus von Ringen und I ein Ideal von R. Dann ist $\varphi(I)$ natürlich eine Untergruppe von $(R',+)$ (sogar ein Unterring von R'), i.a. aber kein Ideal in R' (Beispiel?). Immerhin ist $\varphi(I)$ ein Ideal in R', wenn φ

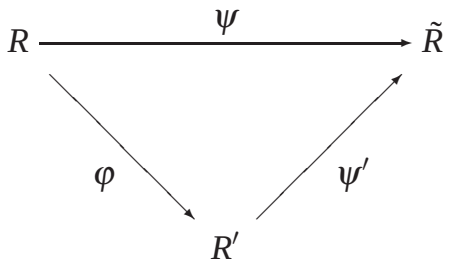
surjektiv ist. Hingegen gilt: Ist I' ein Ideal in R', dann ist $\varphi^{-1}(I')$ ein Ideal in R; insbesondere ist $\operatorname{Kern}\varphi = \varphi^{-1}(0)$ ein Ideal in R.

Die folgenden Sätze vergleichen die Restklassenringe mit den homomorphen Bildern von R. Zunächst der *Satz vom induzierten Homomorphismus:*

Satz 2.4. *Es seien $\varphi : R \to R'$, $\psi : R \to \tilde{R}$ Homomorphismen von Ringen. φ sei surjektiv, und es gelte* $\operatorname{Kern}\psi \supset \operatorname{Kern}\varphi$. *Dann gibt es genau eine Abbildung ψ': $R' \to \tilde{R}$ mit $\psi' \circ \varphi = \psi$. Es ist* $\operatorname{Bild}\psi = \operatorname{Bild}\psi'$. *$\psi'$ ist ein Homomorphismus, und es gilt $\varphi(\operatorname{Kern}\psi) = \operatorname{Kern}\psi'$.*

Ist ψ surjektiv, dann ist auch ψ' surjektiv. Bei $\operatorname{Kern}\psi = \operatorname{Kern}\varphi$ *ist ψ' injektiv.*

Die Beziehung der Homomorphismen in Satz 2.4 bringt man auch so zum Ausdruck: Das Diagramm



ist *kommutativ*. Damit meint man: Die Verkettung von Abbildungen längs Wegen mit gleichem Start und Ziel ergibt das gleiche, nur von Start und Ziel abhängende Resultat.

Beweis von Satz 2.4. Da das obige Diagramm kommutativ werden soll, gibt es nur eine Möglichkeit, ψ' zu definieren. Sei dazu $y \in R'$. Da φ surjektiv ist, gibt es ein $x \in R$ mit $y = \varphi(x)$. Wir möchten erreichen, daß $\psi'(y) = \psi'(\varphi(x)) = \psi(x)$ gilt. Also *müssen* wir

$$\psi'(y) = \psi(x)$$

setzen. Da die Auswahl eines Urbilds x von y im allgemeinen keineswegs eindeutig ist, müssen wir uns überzeugen, daß jede Wahl von $x \in \varphi^{-1}(y)$ das gleiche Resultat liefert. Das folgt aus der Voraussetzung über die Kerne:

$$\varphi(x) = \varphi(x') \iff x - x' \in \operatorname{Kern}\varphi \implies x - x' \in \operatorname{Kern}\psi \iff \psi(x) = \psi(x').$$

Damit ist die Abbildung ψ' wohldefiniert (und eindeutig).

Zum Testen der Homomorphie wählen wir zu $y, z \in R'$ Urbilder $w, x \in R$. Dann ist $w + x$ ein Urbild von $y + z$ und es folgt

$$\psi'(y+z) = \psi(w+x) = \psi(w) + \psi(x) = \psi'(y) + \psi'(z).$$

Analog zeigt man $\psi'(yz) = \psi'(y)\psi'(z)$. Offensichtlich ist auch $\psi'(1) = \psi(1) = 1$.

Wenn ψ surjektiv ist, ist $\psi' \circ \varphi$ surjektiv und damit auch ψ'.

Wenn $\operatorname{Kern}\varphi = \operatorname{Kern}\psi$ gilt, haben wir in der obigen Implikationskette überall Äquivalenz. Mit den bekannten Bedeutungen von w,x,y,z ergibt sich:

$$\psi'(y) = \psi'(z) \iff \psi(w) = \psi(x) \iff \varphi(w) = \varphi(x) \iff y = z.$$

Dies aber ist gerade die Injektivität von ψ'. □

Man nennt ψ' den *induzierten Homomorphismus*. Restklassenringe haben im vorangegangenen Satz gar keine Rolle gespielt, aber er fordert seine Anwendung auf die Situation $I = \operatorname{Kern}\psi$, $R' = R/I$ geradezu heraus. Wir erhalten den *Homomorphiesatz* oder *ersten Isomorphiesatz für Ringe*.

Satz 2.5. *Sei $\psi : R \to \tilde{R}$ ein surjektiver Homomorphismus von Ringen mit $I = \operatorname{Kern}\psi$. Dann ist der induzierte Homomorphsimus $\psi' : R/I \to \tilde{R}$ (für die Restklassenabbildung $\pi : R \to R/I = R'$) ein Isomorphismus.*

Dieser Satz ist ein Paradigma der modernen Algebra. Er betont das Isomorphieprinzip: Es kommt nicht darauf an, welcher Natur die Elemente eines algebraischen Objektes sind. Entscheidend ist die Struktur, und isomorphe Objekte haben die gleiche Struktur.

Der Homomorphiesatz, der für andere Klassen von Objekten analog gilt, sagt, daß wir mit den Restklassenringen alle Bilder von R bis auf Isomorphie kennen.

Eine Anwendung des Satzes vom induzierten Homomorphismus ist der *chinesische Restsatz*. In seiner elementaren Fassung beschreibt er die Lösung etwa der folgenden Frage: Welche Zahlen $n \in \mathbb{Z}$ lassen bei Division durch 7 den Rest 3 und bei Divison durch 8 den Rest 5? Besitzt ein solches System *simultaner Kongruenzen*, nämlich

$$x \equiv 3 \ (7)$$
$$x \equiv 5 \ (8)$$

überhaupt stets eine Lösung, wie findet man sie und wie kann man gegebenenfalls die Lösungsmenge beschreiben? Es ist sofort klar, daß die Lösung bestenfalls modulo 56 eindeutig bestimmt sein kann, denn wenn $x \equiv y \ (56)$, dann $x \equiv y \ (7)$ und $x \equiv y \ (8)$.

Allgemeiner können wir fragen: Kann man zu Idealen $I_1,\dots,I_n$ eines Ringes R stets ein Element $x \in R$ finden, das modulo $I_1,\dots,I_n$ vorgegebene Restklassen hat? Der folgende Satz gibt eine Antwort. Wir nennen Ideale I_1, I_2 *komaximal*, wenn $I_1 + I_2 = R$ ist.

Satz 2.6. *Sei R ein kommutativer Ring und seien $I_1,\dots,I_n$ Ideale von R, für die I_i und I_j komaximal sind, wenn $i \neq j$ ist. Dann gilt:*

(a) $I_1 \cap \dots \cap I_n = I_1 \cdots I_n$.

(b) *Der Homomorphismus*

$$R \to (R/I_1) \times \dots \times (R/I_n), \quad x \mapsto (x + I_1, \dots, x + I_n),$$

ist surjektiv. Sein Kern ist $I_1 \cap \cdots \cap I_n$, und er induziert einen Isomorphismus

$$R/(I_1 \cap \cdots \cap I_n) \cong (R/I_1) \times \cdots \times (R/I_n).$$

Beweis. (a) Wir beweisen dies durch Induktion über n. Sei zunächst $n = 2$. Für beliebige Ideale I_1, I_2 ist natürlich $I_1 I_2 \subset I_1 \cap I_2$. Ferner gilt

$$(I_1 + I_2)(I_1 \cap I_2) \subset I_1 I_2.$$

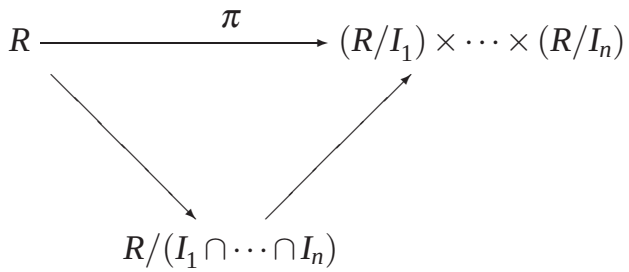
Für $a \in I_1$, $b \in I_2$, $c \in I_1 \cap I_2$ ist nämlich $(a+b)c \in I_1 I_2$, weil $ac \in I_1 I_2$ und $bc \in I_1 I_2$. Da nun $I_1 + I_2 = R$ in unserem Fall, erhalten wir unmittelbar $I_1 \cap I_2 \subset I_1 I_2$, womit Teil (a) für $n = 2$ bewiesen ist.

Es ist klar, daß daraus der allgemeine Fall folgt, wenn wir zeigen können, daß I_1 und $I_2 \cdots I_n$ komaximal sind. Da $I_1 + I_j = R$ für $j > 1$, existieren $u_j \in I_1$, $v_j \in I_j$ mit $1 = u_j + v_j$. Dann ist aber

$$1 = (u_2 + v_2) \cdots (u_n + v_n) \in I_1 + I_2 \cdots I_n$$

denn alle beim Ausmultiplizieren entstehenden Terme gehören zu I_1, mit Ausnahme von $v_2 \ldots v_n$, das aber in $I_2 \cdots I_n$ liegt.

(b) Die Aussage über den Kern des betrachteten Homomorphismus ist für beliebige Ideale richtig, denn die Bilder $x + I_j$ sind genau alle das jeweilige Nullelement, wenn $x \in I_j$ für alle j. Damit hat man unabhängig von der Voraussetzung stets einen induzierten *injektiven* Homomorphismus



Der entscheidende Punkt ist die Surjektivität von π. Dann ist auch der induzierte Homomorphismus surjektiv.

Wir haben bereits in Teil (a) gesehen, daß für jedes k die Ideale I_k und $J_k = I_1 \cdots I_{k-1} I_{k+1} \cdots I_n$ komaximal sind. Wir wählen nun $u_k \in I_k$, $v_k \in J_k$ mit $u_k + v_k = 1$, $k = 1, \ldots, n$.

Sei ein Element $(y_1 + I_1, \ldots, y_n + I_n) \in (R/I_1) \times \cdots \times (R/I_n)$ gegeben. Wir setzen nun

$$x = y_1 v_1 + \cdots + y_n v_n.$$

Für $k = 1, \ldots, n$ ist $v_j \in I_k$ sobald $j \neq k$. Also

$$x + I_k = y_k v_k + I_k = y_k(1 - u_k) + I_k = y_k + I_k,$$

denn $u_k \in I_k$. □

Im Fall $R = \mathbb{Z}$ sind $\mathbb{Z}m_1$ und $\mathbb{Z}m_2$ gerade dann komaxinal, wenn m_1 und m_2 teilerfremd sind. (Wir werden dies noch näher betrachten.) Zur Lösung eines Systems simultaner Kongruenzen $x \equiv y_1 \ (m_1)$, $x \equiv y_2 \ (m_2)$, also der Bestimmung des Elementes x im obigen Beweis, muß man die Gleichung $a_1m_1 + a_2m_2 = 1$ lösen. Dann ist $v_1 = a_2m_2$, $v_2 = a_1m_1$. Die Lösung $x = y_1v_1 + y_2v_2$ ist nach dem Satz modulo m_1m_2 eindeutig bestimmt.

Im konkreten Beispiel ist $(-1)\cdot 7 + 1\cdot 8 = 1$. Wir erhalten $x = 3\cdot 8 + 5\cdot(-7) = -11 \equiv 45 \ (56)$.

Für $R = \mathbb{Z}$ ziehen wir noch eine Folgerung von prinzipieller Bedeutung.

Satz 2.7. (a) *Wenn u und v teilerfremd sind, so sind $\mathbb{Z}_{uv}$ und $\mathbb{Z}_u \times \mathbb{Z}_v$ als Ringe isomorph. Wenn u und v nicht teillerfremd sind, sind $\mathbb{Z}_{uv}$ und $\mathbb{Z}_u \times \mathbb{Z}_v$ nicht (einmal als additive Gruppen) isomorph.*

(b) *Sei $m = p_1^{e_1} \cdots p_r^{e_r}$ die Zerlegung von m in paarweise teilerfremde Primzahlpotenzen. Dann ist*

$$\mathbb{Z}_m \cong \mathbb{Z}_{{p_1}^{e_1}} \times \cdots \times \mathbb{Z}_{{p_r}^{e_r}}.$$

Beweis. Einzig zu zeigen ist nur noch, daß $\mathbb{Z}_{uv}$ und $\mathbb{Z}_u \times \mathbb{Z}_v$ als additive Gruppen nicht isomorph sind, wenn u und v nicht teilerfremd sind. Aber dann ist $s := \mathrm{kgV}(u,v) < uv$. In $\mathbb{Z}_{uv}$ hat $\overline{1}$ die Ordnung uv bezüglich $+$, aber sowohl in $\mathbb{Z}_u$ als auch in $\mathbb{Z}_v$, und damit in $\mathbb{Z}_u \times \mathbb{Z}_v$, wird jedes Element von s annuliert, so daß es dort kein Element der Ordnung uv gibt. □

Teil (b) zeigt, daß es für das Verständnis aller Restklassenringe von $\mathbb{Z}$ genügt, die Restklassenringe nach Primzahlpotenzen zu untersuchen. Dies kann man oft zur Vereinfachung von zahlentheoretischen Problemen heranziehen.

Anhang: Restklassenbildung bei Vektorräumen.

Sei K ein Körper, V ein K-Vektorraum und U ein Untervektoraum. Dann können wir in völliger Analogie den *Restklassenvektorraum* V/U erklären. Wir setzen

$$V/U = \{v + U; v \in V\}$$

und definieren die Restklassenabbildung $\pi : V \to V/U$ wieder durch $\pi(v) = v + U$. Die Vektorraumstruktur auf V/U wird erkärt durch

$$(v+U)+(w+U) = (v+w)+U, \qquad r(v+U) = rv+U, \qquad v,w \in V,\ r \in K.$$

Wieder hat man zu zeigen, daß diese Verknüpfungen wohldefiniert sind, was genauso geht wie bei Restklassenringen. Die Sätze 2.2, 2.4 und 2.5 gelten analog, und wir verzichten darauf, diese für Vektorräume zu formulieren.

Die Dimensionsformel liest sich nun so:

$$\dim V = \dim U + \dim V/U.$$

Es lohnt sich, die Restklassen eines Untervektorraums U zu veranschaulichen. Sie sind genau die „Parallelen“ zu U, vgl. Abbildung 1.

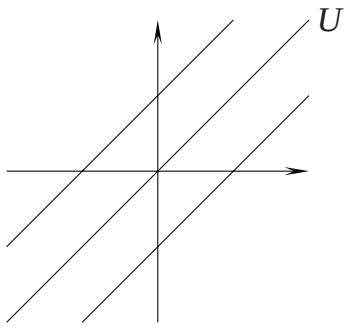


ABBILDUNG 1

Die Restklassenbildung kann man in der Linearen Algebra umgehen, weil jeder endlichdimensionale K-Vektorraum isomorph zu K^n, $n = \dim V$, ist. Insofern führt die Restklassenbildung dort nicht zu strukturell neuen Objekten.

ABSCHNITT 3

Körper und Integritätsbereiche

Wie man sich leicht überlegt, ist der Durchschnitt von Teilkörpern eines Integritätsringes R wieder ein Teilkörper von R.

Definition. Es sei R ein Integritätsbereich, der wenigstens einen Teilkörper enthält. Dann heißt der Durchschnitt aller Teilkörper von R der *Primkörper* von R.

Unter der Voraussetzung in der Definition ist der Primkörper von R der kleinste Teilkörper von R, d.h. er ist in jedem Teilkörper von R enthalten. Jeder Körper hat einen Primkörper; z.B. ist $\mathbb{Q}$ Primkörper von $\mathbb{R}$ und von $\mathbb{C}$ (warum?). Der Ring $\mathbb{Z}$ enthält keinen Teilkörper, hat also auch keinen Primkörper.

Satz 3.1. *Es sei R ein Integritätsbereich der Charakteristik $p > 0$. Dann hat R einen Primkörper. Dieser ist isomorph zu $\mathbb{Z}_p$.*

Beweis. Es sei $\psi : \mathbb{Z} \to R$ der Ring-Homomorphismus $n \mapsto n \cdot 1_R$. Wegen Satz 1.5 gilt $\mathbb{Z}p \subset \operatorname{Kern} \psi$. Also induziert ψ einen Ring-Homomorphismus $\psi' : \mathbb{Z}_p \to R$ (Satz 2.4). Da $\mathbb{Z}_p$ ein Körper ist, muß ψ' injektiv sein (vgl. Übungsaufgabe 8). □

Als Folgerung aus 3.1 erhalten wir:

Satz 3.2. *Es sei K ein endlicher Körper der Charakteristik $p > 0$. Dann ist die Anzahl der Elemente von K eine Potenz von p.*

Beweis. Der Primkörper k von K hat nach Satz 3.1 genau p Elemente. Offenbar ist K auf natürliche Weise ein (endlich-dimensionaler) k-Vektorraum. Folglich ist K (als k-Vektorraum) isomorph zu einem k-Vektorraum k^n. Das beweist die Behauptung. □

Hat der Integritätsbereich R die Charakteristik 0, dann hat R im allgemeinen keinen Primkörper, wie wir am Beispiel $\mathbb{Z}$ gesehen haben. Enthält R hingegen mindestens einen Teilkörper, dann ist der Primkörper von R im betrachteten Fall isomorph zu $\mathbb{Q}$, wie wir unten sehen werden.

Der Integritätsbereich R sei Unterring des Körpers K. Der Durchschnitt aller Teilkörper von K, die R umfassen, ist natürlich wieder ein R umfassender Teilkörper von K.

Definition. Ist der Integritätsbereich R Unterring des Körpers K, dann heißt der Durchschnitt aller R umfassenden Teilkörper von K der *Körper der Brüche* oder *Quotientenkörper* von R in K.

Bemerkung 3.3. (a) Es seien R, K wie in der Definition und Q der Quotientenkörper von R in K. Dann ist

$$Q = \{ab^{-1} \mid a,b \in R,\ b \neq 0\}.$$

Zum *Beweis* zeigt man, daß die rechts stehende Teilmenge von K ein R umfassender Teilkörper von K ist. Außerdem ist sie offenbar in jedem Teilkörper von K enthalten, der R umfaßt.

(b) Die Integritätsbereiche R, R' seien Unterringe von Körpern K bzw. K', und Q, Q' seien die Quotientenkörper von R, R' in K bzw. K'. Dann läßt sich jeder injektive Ring-Homomorphismus $\varphi : R \to R'$ auf genau eine Weise zu einem Ring-Homomorphismus $\Phi : Q \to Q'$ fortsetzen (der natürlich auch injektiv ist). Ist φ ein Isomorphismus, dann ist auch Φ ein Isomorphismus.

Zum *Beweis* zeigt man zunächst, daß aus $a, b, \tilde{a}, \tilde{b} \in R$, $b \neq 0$, $\tilde{b} \neq 0$ mit $ab^{-1} = \tilde{a}\tilde{b}^{-1}$ folgt: $\varphi(a)\varphi(b)^{-1} = \varphi(\tilde{a})\varphi(\tilde{b})^{-1}$, d.h. das Produkt $\varphi(a)\varphi(b)^{-1}$ ist unabhängig von der Darstellung des Elementes ab^{-1}. Durch die Zuordnung $ab^{-1} \mapsto \varphi(a)\varphi(b)^{-1}$ wird also eine Abbildung Φ: $Q \to Q'$ definiert, die auf R offenbar mit φ übereinstimmt. Φ ist surjektiv, wenn dies für φ gilt. Es ist unmittelbar zu sehen, daß Φ ein Homomorphismus ist. Im übrigen folgt aus $\Phi(ab^{-1}) = \varphi(a)\varphi(b)^{-1}$, daß Φ eindeutig bestimmt ist.

Aus Bemerkung 3.3(a) ergibt sich beispielsweise, daß $\mathbb{Q}$ der Quotientenkörper von $\mathbb{Z}$ in $\mathbb{Q}$ (oder $\mathbb{R}$ oder $\mathbb{C}$) ist. Ist der Integritätsbereich R Unterring eines Körpers, so können wir wegen Anmerkung 3.3(b) von *dem* Quotientenkörper von R sprechen. Es folgt

Satz 3.4. *Es sei R ein Integritätsbereich der Charakteristik 0, der wenigstens einen Teilkörper enthält. Dann ist der Primkörper von R isomorph zum Körper $\mathbb{Q}$ der rationalen Zahlen.*

Beweis. Wir betrachten den Homomorphismus $\psi : \mathbb{Z} \to R$ aus dem Beweis zu Satz 3.1. ψ ist hier wegen $\operatorname{char} R = 0$ injektiv. $\operatorname{Bild}\psi$ ist in jedem Teilkörper von R enthalten. Das gilt dann auch für den Quotientenkörper Q von $\operatorname{Bild}\psi$. Also ist Q der Primkörper von R. Nach Anmerkung 3.3(b) läßt sich ψ auf genau eine Weise zu einem Isomorphismus $\Psi : \mathbb{Q} \to Q$ fortsetzen. □

Nun beweisen wir, daß jeder Integritätsbereich als Unterring eines Körpers aufgefaßt werden kann, also einen Quotientenkörper besitzt.

Satz 3.5. *Es sei R ein Integritätsbereich. Dann gibt es einen injektiven Homomorphismus von R in einen Körper K.*

Beweis. Die Konstruktion von K geschieht wie die Konstruktion der rationalen Zahlen $\mathbb{Q}$ aus den ganzen Zahlen $\mathbb{Z}$. Es sei

$$X = \{(a,b) \in R \times R \mid b \neq 0\}.$$

Auf X definieren wir eine Äquivalenzrelation $\sim$ durch

$$(a,b) \sim (c,d) \quad \Longleftrightarrow \quad ad = cb.$$

Es läßt sich ohne Mühe nachrechnen, daß $\sim$ tatsächlich eine Äquivalenzrelation ist. Mit K bezeichnen wir die Menge der Äquivalenzklassen von X bezüglich $\sim$, und mit a/b die Äquivalenzklasse von (a,b). Die Abbildung $a \mapsto a/1$ nennen wir φ; sie ist offenbar injektiv.

Addition $+$ und Multiplikation $\cdot$ auf K erklären wir durch

$$\frac{a}{b} + \frac{c}{d} = \frac{ad+cb}{bd}, \qquad \frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd};$$

dabei sind a, b, c, $d \in R$ und $b \neq 0$, $d \neq 0$, also auch $bd \neq 0$. (Hier wird benutzt, daß R nullteilerfrei ist.) Natürlich hat man nachzuweisen, daß diese Definitionen repräsentantenunabhängig sind. Das ist aber problemlos möglich.

$(K,+)$ ist eine abelsche Gruppe: Aus der Definition der Addition ersieht man, daß sie assoziativ und kommutativ ist. Neutrales Element bezüglich $+$ ist $0/1$, und das Inverse von a/b bezüglich der Addition ist $(-a)/b$.

$(K,\cdot)$ ist ein abelsches Monoid: Man sieht wieder sofort, daß die Multiplikation assoziativ und kommutativ ist und daß $1/1$ bezüglich $\cdot$ neutral ist.

Der Nachweis der Distributivgesetze ist eine einfache Rechnung. $(K,+,\cdot)$ ist also ein kommutativer Ring mit Einselement. Zum Beweis dafür, daß K sogar ein Körper ist, sei $a/b \in K$, $a/b \neq 0/1$. Das bedeutet $a \neq 0$, und das Element $b/a \in K$ ist offenbar invers zu a/b bezüglich der Multiplikation.

Daß φ ein Ring-Homomorphismus ist, rechnet man leicht nach. □

Es ist in der Situation des letzten Satzes üblich (wie im Falle $\mathbb{Z}$ und $\mathbb{Q}$), die Elemente $a \in R$ mit ihren φ-Bildern $a/1 \in K$ zu identifizieren, R also als Unterring von K zu betrachten. Nach Bemerkung 3.3 ist dann K der Quotientenkörper von R.

In einer Übungsaufgabe wird die Konstruktion aus dem letzten Satz verallgemeinert.

Nachdem wir nun Teilkörper von Integritätsbereichen und umgekehrt Integritätsbereiche als Unterringe von Körpern diskutiert haben, wollen wir untersuchen, welche Ideale als Kerne von (surjektiven) Homomorphismen $\varphi : R \to S$ auftreten, wenn R kommutativ und S ein Integritätsbereich oder gar ein Körper ist.

Sei S ein Integritätsbereich. Für Elemente $a,b \in R$ mit $\varphi(ab) = \varphi(a)\varphi(b) = 0$ folgt dann $\varphi(a) = 0$ oder $\varphi(b) = 0$. Mit anderen Worten gilt für $I = \operatorname{Kern}\varphi$: $ab \in I \implies a \in I$ oder $b \in I$.

Definition. Ein Ideal $\mathfrak{p} \neq R$ eines kommutativen Ringes R heißt *Primideal*, wenn für alle $a,b \in R$ aus $ab \in \mathfrak{p}$ folgt: $a \in \mathfrak{p}$ oder $b \in \mathfrak{p}$.

Ist $\mathfrak{p}$ ein Primideal, so sieht man sofort, daß $R/\mathfrak{p}$ ein Integritätsbereich ist. Daher sind die Primideale genau die Kerne von Ringhomomorphismen von R in Integritätsbreiche S.

Sei nun K ein Körper und $\varphi : R \to K$ ein surjektiver Ringhomomorphismus mit Kern I. Da K nicht der Nullring ist, muß $I \neq R$ gelten. Andererseits „paßt“ aber auch kein Ideal zwischen I und R. Es genügt dazu, daß $I + Ra = R$ für jedes Element $a \in R \setminus I$. Für solches a gilt $\varphi(a) \neq 0$. Da φ surjektiv ist, existiert ein $b \in R$ mit $\varphi(b) = \varphi(a)^{-1}$. Es folgt $\varphi(ab) = 1$, also $1 - ab \in I$ und $1 \in I + Ra$.

Definition. Ein Ideal $\mathfrak{M} \neq R$ eines kommutativen Ringes R heißt *maximal*, wenn kein Ideal I mit $\mathfrak{M} \subsetneq I \subsetneq R$ existiert.

Die der Definition vorangegangene Überlegung läßt sich auch umkehren, wie leicht zu überprüfen ist. Also gilt: $R/\mathfrak{M}$ ist genau dann ein Körper, wenn $\mathfrak{M}$ ein maximales Ideal ist.

ABSCHNITT 4

Teilbarkeitstheorie

Jede von 0 verschiedene ganze Zahl läßt sich als Produkt von Primzahlen (und eventuell der Einheit -1) schreiben, und diese Darstellung ist im wesentlichen eindeutig. Wir wollen dies im Rahmen einer allgemeinen Teilbarkeitstheorie in Ringen beweisen und analoge Aussagen für eine größere Klasse von Ringen bereitstellen.

In diesem Abschnitt sei R stets ein *Integritätsbereich*. Wie in $\mathbb{Z}$ sagt man, $a \in R$ sei ein *Teiler* von $b \in R$, in Zeichen $a \mid b$, wenn es ein $c \in R$ mit $b = ac$ gibt. Wir sagen dann auch, b sei *Vielfaches* von a.

Jedes Element $a \in R$ besitzt triviale Teiler, z.B. $1 \in R$ und a selbst, und wenn $a \mid b$ sogilt auch $ea \mid b$ für alle Einheiten e. Wir berücksichtigen dies in der folgenden Terminologie: a ist *assoziiert* zu b, wenn es eine Einheit $e \in R$ mit $b = ea$ gibt, und a ist ein *echter Teiler* von b, wenn $a \mid b$, aber a weder eine Einheit, noch assoziiert zu b ist.

Es lohnt sich, die genannten Beziehungen zwischen a und b idealtheoretisch zu beschreiben:

$$\begin{aligned} a \text{ ist Teiler von } b &\iff Rb \subset Ra, \\ a \text{ assoziiert zu } b &\iff Rb = Ra, \\ a \text{ echter Teiler von } b &\iff Rb \subsetneq Ra \subsetneq R \end{aligned}$$

In Körpern gibt es keine unzerlegbaren Elemente, und die von 0 verschiedenen Elemente sind sämtlich assoziiert. Im Ring $\mathbb{Z}$ sind genau diejenigen Elemente unzerlegbar, deren Betrag eine Primzahl ist. Die ganzen Zahlen m und n sind genau dann assoziiert, wenn $m = \pm n$ ist. Vom Nullpolynom verschiedene Polynome $f, g \in K[X]$ sind assoziiert genau dann, wenn es eine Konstante $c \in K^*$ mit $g = cf$ gibt.

Die Primzahlen p und die Zahlen $-p$ in $\mathbb{Z}$ sind diejenigen Elemente $\neq 0$, die selbst keine Einheiten sind, aber keine echten Teiler besitzen. Wir verallgemeinern dies wie folgt:

Definition. Eine Nichteinheit $u \neq 0$ in R heißt *irreduzibel* oder *unzerlegbar*, wenn u keine echten Teiler besitzt.

Neben den Primzahlen in $\mathbb{Z}$ sind irreduzible Polynome wie $X^2 + 1 \in \mathbb{R}[X]$ weitere Beispiele unzerlegbarer Elemente.

Es ist uns geläufig, daß jedes $n \in \mathbb{Z}$, $n \neq 0, \pm 1$ sich als Produkt irreduzibler Elemente darstellen läßt, und dies ist ja auch sehr einfach einzusehen: Wenn n keine echtenTeiler besitzt, ist es per Definition irreduzibel, also von der Form $\pm p$, p Primzahl, und andernfalls gibt es eine Zerlegung $n = rs$ mit echten Teilern r und s. Da dann $|r|, |s| < |n|$, können wir per Induktion weiterschließen.

Völlig analog sieht man, daß sich jedes Element f im Polynomring $K[X]$ über einem Körper K als Produkt irreduzible Polynme schreiben läßT: in diesem Fall benutzt man den Grad für die Induktion.

Es ist uns aber auch geläufig, daß diese Darstellungen im wesentlichen eindeutig sind, und dies ist eine nichttriviale Feststellung, die „aus dem Stand“ nicht so einfach zu beweisen ist. Wir werden sie im folgenden für eine größere Klasse von Ringen beweisen. Daß man sich bei der Forderung nach Eindeutigkeit natürlichen Einschränkungen unterwerfen muß, ist klar: Aus algebraischer Sicht kann man keiner der Darstellungen

$$6 = 2 \cdot 3 = (-3) \cdot (-2)$$

einen Vorzug geben. Der folgende Satz beschreibt dies präzise und gibt ein Kriterium für die Eindeutigkeit der Darstellung:

Satz 4.1. *Im Integritätsbereich R sei jede von 0 verschiedene Nichteinheit Produkt von unzerlegbaren Elementen. Dann sind folgende Eigenschaften äquivalent:*

(a) *Gilt $u_1 \dots u_r = v_1 \dots v_s$ mit unzerlegbaren Elementen u_i, $v_j \in R$, dann gilt $r = s$, und es gibt eine Permutation $\pi \in S_r$, so daß v_i und $u_{\pi(i)}$ assoziiert sind für $i = 1, \dots, r$.*

(b) *Für jedes unzerlegbare Element u in R gilt:*

$$u \mid ab \implies u \mid a \text{ oder } u \mid b.$$

Beweis. (a) $\implies$ (b): Wenn $u \mid ab$, so existiert ein $c \in R$ mit $uc = ab$. Wir zerlegen a, b, c in Produkte unzerlegbarer Elemente und erhalten eine Gleichung

$$ut_1 \cdots t_k = v_1 \cdots v_m w_1 \cdots w_n$$

Nach (a) muß u zu einem der Elemente v_i oder w_j assoziiert sein, also a oder b teilen.

(b) $\implies$ (a): Wir stellen sofort per Induktion fest, daß sich die in (b) genannte Eigenschaft auf Produkte aus mehr als zwei Elementen ausdehnt: Wenn $u \mid a_1 \cdots a_n$, so $u \mid a_i$ für ein i.

Es sei $u_1 \dots u_r = v_1 \dots v_s$ mit unzerlegbaren Elementen u_i, $v_j \in R$. Wir beweisen (b) durch Induktion über r. Da v_s das Produkt $u_1 \dots u_r$ teilt, gibt es ein u_i, das von v_s geteilt wird. Weil u_i unzerlegbar ist, sind u_i und v_s assoziiert. Insbesondere ist $s = 1$ bei $r = 1$. Bei $r > 1$ gestattet die Behauptung immerhin, die Reihenfolge der Faktoren zu verändern, d.h. wir dürfen $i = r$ annehmen. Es gilt dann $u_1 \dots u_{r-1} = v_1 \dots (v_{s-1} e)$ mit einer Einheit $e \in R$. Mit der Induktionsvoraussetzung folgt $r - 1 =$

$s-1$, also $r=s$, und nach eventueller Vertauschung der Faktoren ist u_j assoziiert zu v_j für $j=1,\ldots,r-1$. □

Ringe, in denen der Satz von der Eindeutigkeit der Primfaktorzerlegung analog gilt, erhalten einen speziellen Namen:

Definition. Ein Integritätsbereich, in dem sich jede von 0 verschiedene Nichteinheit im wesentlichen eindeutig als Produkt von unzerlegbaren Elementen darstellen läßt, heißt *faktoriell*.

Satz 4.1 macht klar, was wir für die Eindeutigkeit der Primfaktorzerlegung in $\mathbb{Z}$ oder der Zerlegung in irreduzible Polynome zu zeigen haben, nämlich die Eigenschaft (a) unzerlegbarer Elemente. Auch ihr geben wir einen Namen:

Definition. Eine von 0 verschiedene Nichteinheit $u \in R$ heißt *Primelement*, wenn folgende Bedingung erfüllt ist: Sind $a,b \in R$ und teilt u das Produkt ab, dann teilt u mindestens einen der Faktoren a oder b.

Wir können nun die Definition von „faktoriell“ kompakter auch so formulieren: R ist faktoriell, wenn sich jede von 0 verschiedene Nichteinheit als Produkt von Primelementen schreiben läßt. Offensichtlich ist jedes Primelement unzerlegbar.

Daß die Unterscheidung von unzerlegbaren Elementen und Primelementen notwendig ist, zeigt folgendes

Beispiel. Die Teilmenge

$$D = \left\{ a+bi\sqrt{5} \;\middle|\; a,b \in \mathbb{Z} \right\}$$

ist ein Unterring von $\mathbb{C}$ (insbesondere ein Integritätsbereich), wie man leicht nachprüft. Wir setzen

$$N\left(a+bi\sqrt{5}\right) := \left|a+bi\sqrt{5}\right|^2 = a^2+5b^2$$

$(a,b \in \mathbb{Z})$. Es gilt offenbar

$$N(xy) = N(x)N(y)$$

für alle $x, y \in D$, und ein Element $x \in D$ ist genau dann eine Einheit, wenn $N(x)=1$ gilt, d.h. wenn $x = \pm 1$. Daraus folgt, daß $N(a) < N(b)$, falls a ein echter Teiler von b ist, und man sieht sofort, daß jedes Element von D Produkt unzerlegbarer Elemente ist.

Aber nicht jedes unzerlegbare Element ist ein Primelement, wie sich aus folgender Gleichung ergibt:

$$\left(1+i\sqrt{5}\right)\left(1-i\sqrt{5}\right) = 2\cdot 3.$$

Das Element 2 ist unzerlegbar: Aus $2=xy$ mit Elementen $x, y \in D$ folgt $4 = N(x)N(y)$. Da $N(x)=2$ offenbar nicht möglich ist, muß $N(x)=1$ oder $N(x)=4$ gelten. Entsprechend ist x oder y eine Einheit. 2 teilt jedoch keines der Elemente

$1 \pm i\sqrt{5}$: Aus $1 \pm i\sqrt{5} = 2 \cdot x$ mit $x \in D$ folgt $6 = 4N(x)$, was nicht sein kann. 2 ist also kein Primelement. Speziell ist D nicht faktoriell.

Der Leser stellt leicht fest, daß wir auch das „kleinere Beispiel" $E = \mathbb{Z} + \mathbb{Z}i\sqrt{3}$ hätten betrachten können. Dies hat einen guten Grund, der an dieser Stelle aber schwer zu erklären ist.

Wie wir gleich sehen werden, lohnt es sich, Unzerlegbarkeit und Primeigenschaft idealtheoretisch zu beschreiben, wobei sich auch eine Rechtfertigung dieser Terminologie ergibt:

Satz 4.2. *Sei R ein Integritätsbereich und $u \neq 0$ eine Nichteinheit.*

(a) *u ist irreduzibel genau dann, wenn es kein Ideal Rv mit $Ru \subsetneq Rv \subsetneq R$ gibt.*
(b) *u ist Primelement ganau dann, wenn Ru ein Primideal ist.*

Beweis. (a) Die echten Teiler von u sind genau diejenigen Elemente v, die Hauptideale Rv mit $Ru \subsetneq Rv \subsetneq R$ erzeugen. Das Fehlen solcher Hauptideale ist also äquivalent zum Fehlen echter Teiler.

(b) Ist u ein Primelement, dann gilt nach Definition $Ru \neq 0$ und $Ru \neq R$. Es seien $a, b \in R$ mit $ab \in Ru$. Dann ist u Teiler von ab. Also teilt u einen der Faktoren a oder b, und dementsprechend gilt $a \in Ru$ oder $b \in Ru$.

Ist umgekehrt Ru ein von 0 verschiedenes Primideal, dann ist u natürlich eine von 0 verschiedene Nichteinheit. Sind $a, b \in R$ und teilt u das Produkt ab, also $ab \in Ru$, dann gilt nach Voraussetzung $a \in Ru$ oder $b \in Ru$, und das wiederum heißt: u teilt a oder b. □

Als nun leichte Folgerung erhalten wir:

Satz 4.3. *Der Ring $\mathbb{Z}$ der ganzen Zahlen ist faktoriell.*

Beweis. Einzig zu zeigen ist noch, daß Primzahlen p in $\mathbb{Z}$ wirklich Primelemente sind. Da p keine echten Teiler besitzt, gibt es kein Ideal $\mathbb{Z}n$ mit $\mathbb{Z}p \subsetneq \mathbb{Z}n \subsetneq \mathbb{Z}$. Da nun aber in $\mathbb{Z}$ *jedes* Ideal von der Form $\mathbb{Z}n$ ist, folgt: $\mathbb{Z}p$ ist ein maximales Ideal, und damit ein Primideal. Also ist p ein Primelement. □

In beliebigen kommutativen Ringen S nennt man die von *einem* Element erzeugten Ideale Sf *Hauptideale*. Der Beweis von Satz 4.3 zeigt an, daß die Teilbarkeitstheorie dann besonders einfach ist, wenn jedes Ideal in R ein Hauptideal ist, und dies trifft in der Tat zu.

Definition. Ein Integritätsbereich, dessen Ideale alle Hauptideale sind, heißt ein *Hauptidealbereich* (auch *Hauptidealring*).

Beispiele für Hauptidealbereiche sind alle Euklidischen Ringe:

Definition. Der Integritätsbereich R heißt *Euklidisch*, wenn es eine Abbildung

$$\text{grad} : R \setminus \{0\} \longrightarrow \mathbb{N}$$

gibt (die sogenannte *Gradfunktion*) mit folgender Eigenschaft: Sind $a, b \in R$, $b \neq 0$, dann gibt es Elemente $q, r \in R$, so daß gilt:

$$a = qb + r, \quad \text{wobei entweder} \quad r = 0 \quad \text{oder} \quad \operatorname{grad} r < \operatorname{grad} b.$$

Beispiele. (a) Bekanntestes Beispiel für einen Euklidischen Ring ist $\mathbb{Z}$ versehen mit der Betragsfunktion als Gradfunktion.

(b) Ein weiteres uns bekanntes Beispiel ist der Polynomring $R = K[X]$ über einem Körper. Wir werden dieses Beispiel in den nächsten Abschnitten noch ausführlich diskutieren.

(c) Auch der Unterring

$$G = \mathbb{Z} + \mathbb{Z}i = \{a + bi \mid a, b \in \mathbb{Z}\}$$

der komplexen Zahlen ist ein Euklidischer Ring, wie wir gleich sehen werden. Man nennt ihn den *Ring der ganzen Gaußschen Zahlen*. Er wird von den ganzzahligen Punkten der komplexen Ebene gebildet, siehe Abbildung 1.

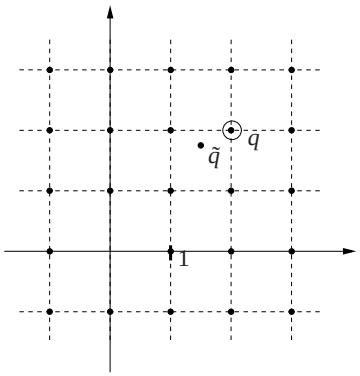


ABBILDUNG 1. Die ganzen Gaußschen Zahlen

Seien $a, b \in G$, $b \neq 0$. Um q und r zu bestimmen, setzen wir $\tilde{q} := a/b \in \mathbb{C}$ und wählen $q \in G$, so daß

$$|q - \tilde{q}| = \min\{|\tilde{q} - c| : c \in G\}.$$

Dann ist $|\tilde{q} - q| \leq (1/2)\sqrt{2}$ (siehe Abbildung 1). Für $r := a - bq$ gilt

$$|r| = |a - bq| = |b|\,|\tilde{q} - q| \leq |b| \cdot \frac{1}{2}\sqrt{2} < |b|.$$

Satz 4.4. *Jeder Euklidische Ring ist ein Hauptidealbereich.*

Beweis. Es sei R ein Euklidischer Ring, grad seine Gradfunktion und I ein von 0 verschiedenes Ideal in R. Es sei $a \in I$, $a \neq 0$, derart, daß $\operatorname{grad}(a)$ in $\operatorname{grad}(I \setminus \{0\})$ minimal ist. Wir behaupten, daß $I = Ra$ gilt.

Zum Beweis sei $b \in I$. Nach Voraussetzung gibt es dann $q, r \in R$ mit

$$b = qa + r, \quad \text{wobei entweder} \quad r = 0 \quad \text{oder} \quad \operatorname{grad} r < \operatorname{grad} a.$$

Mit b gehört auch $r = b - qa$ zu I. Nach Wahl von a muß dann $r = 0$ gelten. Es folgt $b \in Ra$. □

Es gibt aber Hauptidealbereiche, die nicht Euklidisch sind. Dies nachzuweisen, ist nichttrivial, und wir verzichten auf die Diskussion eines Beispiels.

Satz 4.5. *In einem Hauptidealbereich R gilt:*

(a) *Jede von 0 verschiedene Nichteinheit ist Produkt unzerlegbarer Elemente.*
(b) *Für eine von 0 verschiedene Nichteinheit u sind äquivalent:*
  (i) *u ist irreduzibel.*
  (ii) *Ru ist ein maximales Ideal.*
  (iii) *Ru ist ein Primideal.*
  (iv) *u ist ein Primelement.*
(c) *Insbesondere ist R faktoriell.*

Beweis. Wir haben zu zeigen, daß die Menge

$$S = \{a \in R \mid a \notin R^*,\, a \neq 0\,,\, a \text{ ist nicht Produkt unzerlegbarer Elemente}\}$$

leer ist. Angenommen $S \neq \emptyset,\ a \in S$. Wir behaupten: Dann gibt es Elemente a_0, $a_1, \cdots \in S$ mit

$$Ra_0 \subsetneqq Ra_1 \subsetneqq Ra_2 \subsetneqq \ldots \qquad (*)$$

Zum Beweis dieser Behauptung setzen wir $a_0 = a$. Sind $a_0, a_1, \ldots, a_i$ bereits gefunden, dann hat a_i eine Zerlegung $a_i = a_{i+1}b_{i+1}$ mit echten Teilern a_{i+1}, b_{i+1}, von denen zumindest einer in S sein muß, etwa $a_{i+1} \in S$. Insbesondere gilt $Ra_i \subsetneqq Ra_{i+1}$, und die Behauptung ist bewiesen.

Die Teilmenge $\cup_{i=0}^{\infty} Ra_i$ ist ein Ideal in R, wie man sofort sieht, also $\cup_{i=0}^{\infty} Ra_i = Rb$ mit einem $b \in R$. Es gibt dann ein n mit $b \in Ra_n$. Folglich ist $Rb = Ra_n$ und weiter $Ra_i = Ra_n$ für $i \geq n$, was $(*)$ widerspricht.

Es sei noch einmal betont, daß man in Ringen wie $\mathbb{Z}$, $K[X]$, D und G die Eigenschaft (a) einfacher nachweisen kann, wie wir schon gesehen haben.

(b) Die Implikationen (ii) $\Longrightarrow$ (iii) $\Longrightarrow$ (iv) $\Longrightarrow$ (i) gelten in allen Integritätsbereichen. Für die Implikation (i) $\Longrightarrow$ (ii) argumentiert man genau so, wie wir es oben für $\mathbb{Z}$ getan haben. □

Im nächsten Abschnitt werden wir faktorielle Ringe kennenlernen, die keine Hauptidealbereiche sind.

Im zweiten Teil dieses Abschnitts verallgemeinern wir nun die aus der Schule bekannten Begriffe „größter gemeinsamer Teiler“ und „kleinstes gemeinsames Vielfaches“ auf beliebige Integritätsbereiche und untersuchen sie insbesondere in faktoriellen Ringen und Hauptidealbereichen.

Definition. (a) Das Element $d \in R$ heißt ein *gemeinsamer Teiler* (gT) der Elemente $a_1, \ldots, a_n \in R$, wenn d jedes a_i teilt, d.h. wenn es zu jedem $i = 1, \ldots, n$ ein $b_i \in R$ gibt mit $a_i = b_i d$.

(b) Das Element $v \in R$ heißt ein *gemeinsames Vielfaches* (gV) der Elemente $a_1, \ldots, a_n \in R$, wenn v Vielfaches eines jeden a_i ist, d.h. wenn es zu jedem $i = 1, \ldots, n$ ein $c_i \in R$ gibt mit $v = c_i a_i$.

Bemerkung 4.6. Mit den Bezeichnungen der Definition hat man offenbar:

(a) d ist genau dann gT von $a_1, \ldots, a_n \in R$, wenn $Rd \supset Ra_1 + \cdots + Ra_n$ gilt.
(b) v ist genau dann gV von $a_1, \ldots, a_n \in R$, wenn $Rv \subset Ra_1 \cap \cdots \cap Ra_n$ gilt.

Definition. (a) Die Elemente $a_1, \ldots, a_n \in R$ heißen *teilerfremd*, wenn jeder gemeinsame Teiler von $a_1, \ldots, a_n$ eine Einheit ist.

(b) $d \in R$ heißt ein *größter gemeinsamer Teiler* (ggT) von $a_1, \ldots, a_n \in R$, wenn d ein gT von $a_1, \ldots, a_n$ ist und von jedem gT dieser Elemente geteilt wird.

(c) $v \in R$ heißt ein *kleinstes gemeinsames Vielfaches* (kgV) von $a_1, \ldots, a_n \in R$, wenn v ein gV von $a_1, \ldots, a_n$ ist und jedes gV von $a_1, \ldots, a_n$ teilt.

Die Beweise der folgenden Bemerkungen ergeben sich alle unmittelbar aus den Definitionen.

Bemerkung 4.7. Es seien $a_1, \ldots, a_n \in R$. Dann gilt für d, d', v, $v' \in R$:

(a) Ist d ein ggT von $a_1, \ldots, a_n$ und sind d, d' assoziiert, dann ist auch d' ein ggT von $a_1, \ldots, a_n$. Umgekehrt: Sind d, d' ggT von $a_1, \ldots, a_n$, dann sind d, d' assoziiert.

(b) Ist v ein kgV von $a_1, \ldots, a_n$ und sind v, v' assoziiert, dann ist auch v' ein kgV von $a_1, \ldots, a_n$. Umgekehrt: Sind v, v' kgV von $a_1, \ldots, a_n$, dann sind v, v' assoziiert.

(c) Sind $a_1, \ldots, a_n$ nicht alle 0, ist d ein ggT von $a_1, \ldots, a_n$ und gilt $a_i = da_i'$ für $i = 1, \ldots, n$ mit Elementen $a_i' \in R$, dann sind $a_1', \ldots, a_n'$ teilerfremd.

Satz 4.8. *R sei ein faktorieller Ring, $a_1, \ldots, a_n$ seien Elemente von R. Dann besitzen $a_1, \ldots, a_n$ einen ggT und ein kgV.*

Beweis. Wir dürfen annehmen, daß $a_1, \ldots, a_n$ von 0 verschiedene Nichteinheiten sind. Nach Satz 4.1 gibt es unzerlegbare, paarweise nicht zueinander assoziierte Elemente $u_1, \ldots, u_r \in R$ und zu jedem $i = 1, \ldots, n$ natürliche Zahlen $k_1(a_i), \ldots, k_r(a_i)$ und Einheiten $e_i \in R$, derart daß

$$a_i = e_i u_1^{k_1(a_i)} \cdots u_r^{k_r(a_i)}.$$

Setzt man für $\rho = 1, \ldots, r$

$$s_\rho = \min\{k_\rho(a_i) \mid i = 1, \ldots, n\}, \quad t_\rho = \max\{k_\rho(a_i) \mid i = 1, \ldots, n\},$$

dann ist $u_1^{s_1} \cdots u_r^{s_r}$ ein ggT und $u_1^{t_1} \cdots u_r^{t_r}$ ein kgV von $a_1, \ldots, a_n$. □

Bemerkung 4.9. Ist Q Quotientenkörper des faktoriellen Ringes R, dann hat wegen Satz 4.8 jedes von 0 verschiedene Element aus Q eine Darstellung ab^{-1} mit teilerfremden Elementen $a, b \in R$. Man nennt dies dann eine *gekürzte* Darstellung.

Satz 4.10. *Es sei R ein Hauptidealbereich, $a_1, \ldots, a_n$ seien Elemente von R. Ist d ein ggT von $a_1, \ldots, a_n$, so gilt $Rd = Ra_1 + \cdots + Ra_n$. Insbesondere sind $a_1, \ldots, a_n$ genau dann teilerfremd, wenn $R = Ra_1 + \cdots + Ra_n$ ist.*

Beweis. Es ist wegen 4.6 lediglich $Rd \subset Ra_1 + \cdots + Ra_n$ zu zeigen. Nach Voraussetzung ist $Ra_1 + \cdots + Ra_n$ ein Hauptideal, also $Ra_1 + \cdots + Ra_n = Rc$ mit einem $c \in R$. Dann ist insbesondere c ein gT von $a_1, \ldots, a_n$, also auch ein Teiler von d. Das bedeutet aber $Rd \subset Rc$. □

Aus Satz 4.10 ergibt sich beispielsweise, daß es zu zwei teilerfremden ganzen Zahlen m, n stets ganze Zahlen x, y gibt mit $xm + yn = 1$.

In Euklidischen Ringen berechnet man $d = \mathrm{ggT}(a, b)$ mit dem *Euklidischen Algorithmus*, der überdies auch Koeffizienten x und y für die Darstellung $d = xa + yb$ mitliefert.

Sei $r_0 := a,\ r_1 := b \neq 0$. Nach Voraussetzung gibt es $q_1, r_2 \in R$ mit

$$r_0 = q_1 r_1 + r_2, \qquad \text{und} \quad r_2 = 0 \quad \text{oder} \quad \varphi(r_2) < \varphi(r_1).$$

Falls $r_2 = 0$, ist offensichtlich $r_1 = \mathrm{ggT}(r_0, r_1)$. Andernfalls ist immerhin noch $\mathrm{ggT}(r_0, r_1) = \mathrm{ggT}(r_1, r_2)$, denn jeder Teiler von r_0 und r_1 ist ein Teiler von r_1 und r_2, und umgekehrt. Also fährt man fort:

$$r_1 = q_2 r_2 + r_3, \quad \ldots, \quad r_{n-1} = q_n r_n + r_{n+1}, \quad r_n = q_{n+1} r_{n+1}.$$

Dabei seien $r_1, \ldots, r_{n+1} \neq 0$, und es gelte $\varphi(r_k) < \varphi(r_{k-1})$ für $k \geq 2$. Daher bricht dieses Verfahren stets nach endlich vielen Schritten ab, und liefert, wie oben bereits begründet, in r_{n+1} den ggT von a und b. Um eine Darstellung $r_{n+1} = xa + yb$ zu erhalten, beachtet man:

$$\begin{array}{llll}
r_0 = a = x_0 a + y_0 b & \text{mit} \quad x_0 := 1 & \text{und} & y_0 := 0, \\
r_1 = b = x_1 a + y_1 b & \text{mit} \quad x_1 := 0 & \text{und} & y_1 := 1, \\
r_2 = r_0 - q_1 r_1 = x_2 a + y_2 b & \text{mit} \quad x_2 := x_0 - q_1 x_1 & \text{und} & y_2 := y_0 - q_1 y_1, \\
\vdots & \vdots & & \vdots
\end{array}$$

Beispiel. Zu bestimmen ist $\mathrm{ggT}(705,423)$ in $\mathbb{Z}$.

$$\begin{array}{lll} & x_0 = 1 & y_0 = 0 \\ & x_1 = 0 & y_1 = 1 \\ r_0 = 705 = 1\cdot 423 + 282 & x_2 = 1 & y_2 = -1 \\ r_1 = 423 = 1\cdot 282 + 141 & x_3 = -1 & y_3 = 2 \\ r_2 = 282 = 2\cdot 141 & & \end{array}$$

Also ist $\mathrm{ggT}(705,423) = 141 = -705 + 2\cdot 423$.

Das soeben beschriebene Verfahren zur Bestimmung von $d = \mathrm{ggT}(a,b)$ und einer Darstellung $d = xa + yb$ ist für das Rechnen in Restklassenringen wichtig, weil es uns erlaubt, multiplikativ inverse Elemente zu bestimmen. Zunächst einmal können wir leicht beschreiben, welche Elemente Inverse besitzen:

Satz 4.11. *Sei R ein Hauptidealbereich und $a,u \in R$. Genau dann ist $\bar{a}$ eine Einheit in R/Ra, wenn a und u teilerfremd sind.*

Beweis. Seien zunächst a und u teilerfremd. Dann existieren $b,v \in R$ mit $ba+vu = 1$. Mithin ist $\bar{b}\bar{a} = \bar{1}$.

Umgekehrt: Es gelte $\bar{b}\bar{a} = \bar{1}$. Das heißt: $1 - ba \in Ru$. Also existiert ein $v \in R$ mit $1 - ba = vu$, äquivalent $ba + vu = 1$. □

Der Beweis zeigt uns, wie wir in Euklidischen Ringen mittels des Euklidischen Algorithmus die Invertierbarkeit von a testen und zugleich das Inverse bestimmen können: diese Daten sind in der Gleichung $\mathrm{ggT}(a,u) = by + vu$ enthalten.

Damit haben wir auch den Schlußstein zur Lösung simultaner Kongruenzen gemäß dem chinesichen Restsatz gefunden, denn dabei benötigt man ja eine Darstellung $1 = xm + yn$ für teilerfremde $m,n \in \mathbb{Z}$.

ABSCHNITT 5

Polynomringe

Der Polynomring $K[X]$ über einem Körper K wurde schon in [LA] eingeführt. Seine Elemente haben die Form

$$a_0 + a_1X + \cdots + a_nX^n$$

und wir rechnen mit Ihnen nach den üblichen Regeln. Insbesondere sollen zwei Polynome genau dann gleich sein, wenn sie die gleichen Koeffizienten besitzen. Ein Problem, vor dem wir uns in [LA] gedrückt haben, ist eine formal korrekte Konstruktion von $K[X]$. Es ist ja nicht offensichtlich, ob es überhaupt einen Ring $S \supset K$ und ein Element $X \in S$ gibt, so daß zwei „Ausdrücke“ $a_0 + a_1X + \cdots + a_nX^n$ und $b_0 + b_1X + \cdots + b_nX^n$ nur dann übereinstimmen, wenn $a_i = b_i$ für $i = 0, \ldots, n$. Wir wollen die Konstruktion des Polynomrings nun durchführen und ersetzen den Koeffizientenkörper K dabei gleich durch einen *kommutativen* Ring R. Die Konstruktion ist sehr einfach: Wir betrachten das Polynom einfach als die Folge seiner Koeffizienten!

Es lohnt sich, gleich einen Ring zu konstruieren, der noch größer als der Polynomring ist. Sei dazu

$$R^{\mathbb{N}} \quad \text{die Menge aller Folgen} \quad (a_n) = (a_0, a_1, \ldots) \quad \text{mit} \quad a_n \in R.$$

Wir versehen $R^{\mathbb{N}}$ mit einer Addition:

$$(a_n) + (b_n) = (a_n + b_n), \tag{$*$}$$

d.h. zwei Folgen werden addiert, indem man entsprechende Folgenglieder addiert. Es ist sofort klar, daß $(R^{\mathbb{N}}, +)$ eine abelsche Gruppe ist. Wir definieren ferner eine Multiplikation auf $R^{\mathbb{N}}$:

$$(a_n)(b_n) = \left(\sum_{i=0}^{n} a_i b_{n-i} \right), \tag{$**$}$$

d.h. das n-te Glied des Produktes ist $\sum_{i=0}^{n} a_i b_{n-i}$. Die Multiplikation ist kommutativ, da

$$\sum_{i=0}^{n} a_i b_{n-i} = \sum_{i=0}^{n} b_{n-i} a_i = \sum_{i=0}^{n} b_i a_{n-i}.$$

Sie ist assoziativ; denn

$$\big((a_n)(b_n)\big)(c_n) = \left(\sum_{j=0}^{n} a_j b_{n-j}\right)(c_n) = \left(\sum_{i=0}^{n}\left(\sum_{j=0}^{i} a_j b_{i-j}\right) c_{n-i}\right),$$

$$\begin{aligned}
&\sum_{i=0}^{n}\left(\sum_{j=0}^{i} a_j b_{i-j}\right) c_{n-i} \\
&\quad = (a_0b_0)c_n + (a_0b_1 + a_1b_0)c_{n-1} + \cdots + (a_0b_n + \cdots + a_nb_0)c_0 \\
&\quad = a_0(b_0c_n + \cdots + b_nc_0) + a_1(b_0c_{n-1} + \cdots + b_{n-1}c_0) + \cdots + a_n(b_0c_0) \\
&\quad = \sum_{i=0}^{n} a_i \left(\sum_{j=0}^{n-i} b_j c_{(n-i)-j}\right)
\end{aligned}$$

und

$$\left(\sum_{i=0}^{n} a_i \left(\sum_{j=0}^{n-i} b_j c_{(n-i)-j}\right)\right) = (a_n)\big((b_n)(c_n)\big).$$

Offenbar ist $(1,0,0,\dots)$ neutrales Element bezüglich der Multiplikation. Es ist ferner unschwer einzusehen, daß die Distributivgesetze gelten. Man hat also:

Satz 5.1. *$R^{\mathbb{N}}$ ist, versehen mit der durch $(*)$ definierten Addition und der durch $(**)$ definierten Multiplikation, ein kommutativer Ring. Die Abbildung $a \mapsto (a,0,0,\dots)$ von R in $R^{\mathbb{N}}$ ist ein injektiver Ringhomomorphismus.*

Beweis. Der erste Teil der Aussage ist bereits klar, der zweite sehr leicht zu zeigen. □

Auf Grund der letzten Aussage können wir R als Unterring von $R^{\mathbb{N}}$ auffassen. Dementsprechend schreiben wir für die Elemente $(a,0,0,\dots)$ von $R^{\mathbb{N}}$ einfach a.

Der Ring $R^{\mathbb{N}}$ enthält zum Beispiel das Element

$$(1,1,1,\dots),$$

in dem alle Folgenglieder 1 sind. Diese Folge ist offenbar nicht die Koeffizientenfolge (a_n) eines Polynoms p, denn es sollte ja $a_k = 0$ für $k > \operatorname{grad} p$ gelten.

Wir sondern jetzt die „Polynome“ in $R^{\mathbb{N}}$ aus: Sei

$$R^{(\mathbb{N})} = \big\{(a_n) \in R^{\mathbb{N}} \mid a_n = 0 \ \text{ für fast alle } \ n\big\}.$$

Dabei heißt „fast alle“: mit nur endlich vielen Ausnahmen. Man sieht sofort:

Satz 5.2. *$R^{(\mathbb{N})}$ ist ein Unterring von $R^{\mathbb{N}}$ und R ein Unterring von $R^{(\mathbb{N})}$.*

Für $X := (0,1,0,0,\dots) \in R^{(\mathbb{N})}$ gilt

$$X^2 = (0,0,1,0,\dots), \quad X^3 = (0,0,0,1,0,\dots)$$

usw. Also hat jedes $(a_n) \in R^{(\mathbb{N})}$ eine (eindeutige) Darstellung als Linearkombination von Potenzen von X mit Koeffizienten aus R,

$$(a_n) = \sum_n a_n X^n, \qquad (***)$$

wobei die „unendliche“ Summe Sinn macht, denn nur endlich viele Summanden sind $\neq 0$.

Definition. Der Ring $R^{(\mathbb{N})}$ heißt der *Ring der Polynome* über R in der *Unbestimmten* X und seine Elemente entsprechend *Polynome* über R in X. Übliche Bezeichnung für $R^{(\mathbb{N})}$ ist $R[X]$. In der Darstellung $(***)$ heißen die a_n die *Koeffizienten* dieses Polynoms. Die Elemente aus R nennt man *konstante* Polynome.

Die Addition zweier Polynome geschieht nach $(*)$ koeffizientenweise. Für das Produkt von $f = \sum a_n X^n$ und $g = \sum b_n X^n$ gilt gemäß $(**)$:

$$fg = \sum_n \left(\sum_{i=0}^{n} a_i b_{n-i} \right) X^n.$$

Es ist übrigens üblich, die Schreibweise $(***)$ für alle Elemente von $R^{\mathbb{N}}$ zu übernehmen: Für $f = (a_n) \in R^{\mathbb{N}}$ ist a_m der Koeffizient bei X^m. Die Elemente von $R^{\mathbb{N}}$ nennt man deshalb auch *formale Potenzreihen* über R in der *Unbestimmten* X und schreibt statt $R^{\mathbb{N}}$ meist $R[\![X]\!]$.

Definition. Es sei R ein Ring und $f \in R[X]$, $f = \sum a_n X^n$. Ist $f \neq 0$, dann heißt die größte Zahl n mit $a_n \neq 0$ der *Grad* von f, Bezeichnung: $\operatorname{grad}(f)$. Der Koeffizient $a_{\operatorname{grad}(f)}$ heißt *Leitkoeffizient* von f. Ist der Leitkoeffizient von f gleich 1, dann heißt f *normiert*. Für das *Nullpolynom* 0 setzt man $\operatorname{grad}(0) = -\infty$.

Bemerkung 5.3. Seien R ein kommutativer Ring und $f, g \in R[X]$. Dann gilt:

(a) $\operatorname{grad}(f+g) \leq \max\{\operatorname{grad}(f), \operatorname{grad}(g)\}$.
(b) $\operatorname{grad}(fg) \leq \operatorname{grad}(f) + \operatorname{grad}(g)$.
(c) Sind $f, g \neq 0$, sind a, b die Leitkoeffizienten von f bzw. g und gilt $ab \neq 0$, dann ist $\operatorname{grad}(fg) = \operatorname{grad}(f) + \operatorname{grad}(g)$ *(Gradformel)*.
(d) Ist R ein Integritätsbereich, dann ist auch $R[X]$ ein Integritätsbereich, und es gilt $(R[X])^* = R^*$.

Beweis. Die ersten drei Aussagen sind sehr einfach zu beweisen. Den ersten Teil von (d) bekommt man mit (c). (Im übrigen gilt sogar: Ist R ein Integritätsbereich, dann ist auch $R[\![X]\!]$ ein Integritätsbereich.) Natürlich ist jede Einheit in R auch Einheit in $R[X]$, d.h. es gilt (immer) $R^* \subset (R[X])^*$. Ist umgekehrt (R ein Integritätsbereich und) $f \in (R[X])^*$, dann gibt es ein $g \in R[X]$ mit $fg = 1$. Mit der Gradformel erhält man $\operatorname{grad}(f) + \operatorname{grad}(g) = 0$, also $\operatorname{grad}(f) = \operatorname{grad}(g) = 0$. Das bedeutet $f, g \in R$. □

Der zweite Teil von Aussage (d) gilt nicht für beliebige Ringe. Für das Polynom $f = 1+2X \in \mathbb{Z}_4[X]$ gilt z.B. $f^2 = 1$.

Die folgende Aussage ist die uns geläufige Division mit Rest:

Satz 5.4. *R sei ein kommutativer Ring, $g \in R[X]$, $g \neq 0$, und der Leitkoeffizient b von g sei eine Einheit in R. Dann gibt es zu jedem $f \in R[X]$ eindeutig bestimmte Polynome $q, r \in R[X]$ mit*

$$f = qg + r \quad \textit{und} \quad \operatorname{grad}(r) < \operatorname{grad}(g).$$

Beweis. Der Fall $f = 0$ ist trivial. Es sei also $f \neq 0$. Den Existenzbeweis für q, r führen wir durch Induktion über $n = \operatorname{grad}(f)$. Es sei $n = 0$, also $f \in R$. Bei $\operatorname{grad}(g) > 0$ setzen wir $q = 0$ und $r = f$. Bei $\operatorname{grad}(g) = 0$, also $g = b$, sei $q = fb^{-1}$ und $r = 0$. Es sei jetzt $n > 0$. Bei $n < \operatorname{grad}(g)$ setzen wir wieder $q = 0$ und $r = f$. Bei $n \geq \operatorname{grad}(g) = m$, $f = a_nX^n + \cdots + a_1X + a_0$, ist

$$\operatorname{grad}(f - a_nb^{-1}X^{n-m}g) < n.$$

Nach Induktionsvoraussetzung existieren also Polynome $q_1, r \in R[X]$ mit

$$f - a_nb^{-1}X^{n-m}g = q_1g + r \quad \text{und} \quad \operatorname{grad}(r) < \operatorname{grad}(g).$$

Wir setzen dann $q = a_nb^{-1}X^{n-m} + q_1$.

Für den Eindeutigkeitsbeweis nehmen wir an, daß es $q_i, r_i \in R[X]$ gibt mit

$$\begin{aligned} f &= q_1g + r_1 \quad \text{und} \quad \operatorname{grad}(r_1) < \operatorname{grad}(g), \\ f &= q_2g + r_2 \quad \text{und} \quad \operatorname{grad}(r_2) < \operatorname{grad}(g). \end{aligned}$$

Dann ist $(q_1 - q_2)g = r_2 - r_1$. Insbesondere ist

$$\operatorname{grad}(q_1 - q_2) + \operatorname{grad}(g) = \operatorname{grad}(r_2 - r_1) < \operatorname{grad}(g).$$

Das kann nur bei $q_1 = q_2$ und $r_1 = r_2$ gelten. □

Die algorithmische Bestimmung von *Quotient* q und *Rest* r läßt sich wie bei den ganzen Zahlen durchführen. Z.B. ist

$$\begin{array}{rrrrrl} (X^4 & +3X^3 & +2X^2 & -X & +4) & : (X^2-1) = X^2+3X+3 \ (=q) \\ -(X^4 & & -\ X^2) & & & \\ & 3X^3 & +3X^2 & -X & +4 & \\ & -(3X^3 & & -3X) & & \\ & & 3X^2 & +2X & +4 & \\ & & -(3X^2 & & -3) & \\ & & & 2X & +7 & \qquad (=r). \end{array}$$

Satz 5.5. *Ist K ein Körper, dann ist $K[X]$ ein Euklidischer Ring, insbesondere also ein Hauptidealbereich.*

Wir definieren im folgenden einen (aus der Analysis oder der Linearen Algebra) in Spezialfällen wohlbekannten Begriff, den *Wert* eines Polynoms an einer Stelle des Koeffizientenringes. Die Möglichkeit, für X „einzusetzen“, ist die strukturell entscheidende Eigenschaft des Polynomrings. Die Bedeutung des nächsten Satzes ist mit der des Homomorphiesatzes vergleichbar. Die Konstruktion des Polynomrings wird dann zur Nebensache.

Satz 5.6. *Es sei $\tau : R \to S$ ein Homomorphismus von Ringen und $b \in S$. Dann gibt es genau einen Ringhomomorphismus $\tau^* : R[X] \to S$ mit $\tau^*(X) = b$ und $\tau^*|R = \tau$.*

Beweis. Es sei $f = \sum a_n X^n \in R[X]$. Wir setzen

$$\tau^*(f) = \sum \tau(a_n) b^n.$$

Es bereitet keine Mühe zu zeigen, daß τ^* die im Satz genannten Eigenschaften hat. Überdies folgt aus der Homomorphie-Eigenschaft, daß unsere Definition von τ^* die einzig mögliche ist. □

Wir halten einige Anwendungen von 5.6 fest.

Bemerkung 5.7. (a) Es sei R ein Unterring des Ringes S, $\iota : R \to S$ die natürliche Injektion, $b \in S$. Das Bild von $R[X]$ unter ι^* bezeichnet man mit $R[b]$. Für $f \in R[X]$ heißt $f(b) = \iota^*(f)$ der *Wert* von f an der Stelle b. Man sagt auch: $R[b]$ entsteht aus R durch *Adjunktion* von b und $f(b)$ aus f durch *Substitution* von b.

Insbesondere ist damit erklärt, was der Wert $f(b)$ eines Polynoms $f \in R[X]$ an der Stelle $b \in R$ ist. Gilt $f(b) = 0$, dann heißt b eine *Nullstelle* von f (in R). Wir betrachten die Abbildung

$$\alpha : R[X] \longrightarrow \mathrm{Abb}(R, R),$$

die jedem $f \in R[X]$ die Abbildung $x \mapsto f(x)$ von R in R zuordnet. α ist offenbar ein Homomorphismus von Ringen, der – wie das Beispiel zu Beginn des Abschnitts zeigt – i.a. nicht injektiv ist.

(b) Es sei $\tau : R \to S$ ein Homomorphismus von Ringen. Nach 5.6 gibt es genau einen Ringhomomorphismus φ: $R[X] \to S[X]$ mit $\varphi(X) = X$ und $\varphi(a) = \tau(a)$ für alle $a \in R$. Es ist

$$\varphi(\sum a_n X^n) = \sum \tau(a_n) X^n,$$

die Koeffizienten der Polynome über R werden also durch ihre τ-Bilder ersetzt.

Ist insbesondere R Unterring von S, dann können wir nach der vorangegangenen Überlegung $R[X]$ als Unterring von $S[X]$ auffassen. In der Tat ist φ injektiv, wenn dies für τ gilt.

Eine weitere Anwendung erfährt Satz 5.6 im Beweis der folgenden Aussage, die wir sehr häufig benutzen werden.

Satz 5.8. *R sei ein Ring, I ein Ideal in R und $\tilde{I}$ das von I in $R[X]$ erzeugte Ideal. Dann gilt:*

(a) $\tilde{I} \cap R = I$;
(b) $R[X]/\tilde{I} \cong (R/I)[X]$;
(c) *$\tilde{I}$ ist genau dann ein Primideal in $R[X]$, wenn I ein Primideal in R ist.*

Beweis. Man überlegt sich leicht, daß $\tilde{I}$ gerade die Menge derjenigen Elemente von $R[X]$ ist, deren Koeffizienten zu I gehören. Damit ist (a) klar. Es sei $\pi\colon R \to R/I$ die natürliche Projektion. Nach 5.6 gibt es einen (surjektiven) Homomorphismus $\pi^*\colon R[X] \to (R/I)[X]$ mit $\pi^*(X) = X$ und $\pi^*|R = \pi$. Genau dann ist $\pi^*(f) = 0$, wenn die Koeffizienten von f zu I gehören. D.h. $\mathrm{Kern}(\pi^*) = \tilde{I}$. Es folgen (b) und (c). □

Mittels der Division mit Rest (Satz 5.4) können wir zeigen, daß Linearfaktoren zu Nullstellen abspalten:

Satz 5.9. *R sei ein Ring, $f \in R[X]$, $a \in R$. Genau dann ist a Nullstelle von f (d.h. $f(a) = 0$), wenn $f = g \cdot (X - a)$ für ein $g \in R[X]$ gilt.*

Beweis. Es sei a Nullstelle von f. Nach 5.4 ist $f = g \cdot (X - a) + r$ mit $r \in R[X]$, $\mathrm{grad}(r) \leq 0$. Wegen $f(a) = 0$ ist $r(a) = 0$, also $r = 0$. □

Satz 5.10. *R sei ein Ring und $f \in R[X]$ nicht konstant. Hat f wenigstens eine Nullstelle in R, so gibt es eine Darstellung*

$$f = (X - x_1)^{m_1} \cdots (X - x_r)^{m_r} g \qquad (*)$$

mit paarweise verschiedenen $x_i \in R$ und positiven ganzen Zahlen m_i und einem $g \in R[X]$, das keine Nullstelle in R hat. Insbesondere gilt $\sum_{i=1}^{r} m_i \leq \mathrm{grad}(f)$.

Ist R ein Integritätsbereich, dann hat f folglich höchstens $\mathrm{grad}(f)$ verschiedene Nullstellen. In diesem Fall ist $\{x_1, \ldots, x_r\}$ die Gesamtheit der Nullstellen von f in R, und die Faktoren in der Darstellung $(*)$ sind eindeutig bestimmt.

Beweis. Die Darstellung $(*)$ erhält man sofort mittels Satz 5.9 durch Induktion über den Grad von f unter Verwendung der Gradformel, aus der dann auch $\sum_{i=1}^{r} m_i \leq \mathrm{grad}(f)$ folgt.

R sei jetzt ein Integritätsbereich. Ist $a \in R$ eine Nullstelle von f, dann muß wegen $g(a) \neq 0$ einer der übrigen Faktoren auf der rechten Seite von $(*)$ in a verschwinden. Das bedeutet aber $a \in \{x_1, \ldots, x_r\}$. Ebenso erhält man, daß der Faktor $X - x_i$ in jeder Darstellung von f der Form $(*)$ vorkommen muß. Die behauptete Eindeutigkeit ergibt sich hieraus mittels der Kürzungsregel. □

Satz 5.11. *R sei ein Integritätsbereich. Dann ist ein von 0 verschiedenes Polynom über R eines Grades $\leq m$ schon durch seine Werte auf $m+1$ verschiedenen*

Elementen von R eindeutig bestimmt. Insbesondere ist der in 5.7 (a) *definierte Homomorphismus* $\alpha : R[X] \to \mathrm{Abb}(R,R)$ *injektiv, wenn R unendlich viele Elemente enthält.*

Beweis. Die zweite Aussage ergibt sich sofort aus der ersten. Zum Beweis der ersten betrachte man von 0 verschiedene Polynome f und g über R eines Grades $\leq m$, deren Werte auf $m+1$ verschiedenen Elementen von R übereinstimmen. Dann hat auch $f-g$ einen Grad $\leq m$ und überdies $m+1$ verschiedene Nullstellen. Wegen Satz 5.10 folgt $f-g=0$. □

Nachdem wir Polynomringe über einem Ring konstruiert haben, kann man die Konstruktion iterieren, speziell also den Polynomring

$$(R[X])[Y]$$

betrachten usw. Wir kommen so zu den Polynomringen in mehreren Unbestimmten, die in dieser Vorlesung aber keine Rolle spielen. Eine andere (und bessere) Möglichkeit, Polynomringe in mehreren Unbestimmten zu definieren, bekommt man, wenn man in der Konstruktion $\mathbb{N}$ durch $\mathbb{N}^n$ in geeigneter Weise ersetzt.

ABSCHNITT 6

Irreduzibilitätskriterien für Polynome

Wie wir in den folgenden Abschnitten noch sehen werden, ist es oft wichtig zu entscheiden, ob ein Polynom irreduzibel ist. Diese Aufgabe ist wesentlich schwieriger zu lösen als die, eine gegebene natürliche Zahl als Primzahl nachzuweisen, wo wenigstens ein elementarer Algorithmus auf der Hand liegt.

Von besonderem Interesse ist die Irreduzibilität von Polynomen mit ganzzahligen Koeffizienten im Ring $\mathbb{Q}[X]$. Wie wir sehen werden, kann man dies im wesentlichen schon in $\mathbb{Z}[X]$ entscheiden, was eine wesentliche Vereinfachung bedeutet. Hier kann man $\mathbb{Z}$ durch einen beliebigen faktoriellen Ring ersetzen und $\mathbb{Q}$ durch den Körper $Q(R)$ der Brüche von R.

Sehr einfach zu sehen ist, was mit den Primelementen und irreduziblen Elementen von R in $R[X]$ geschieht:

Satz 6.1. *R sei Integritätsbereich, $u \in R$.*

(a) *Genau dann ist u Primelement in R, wenn u Primelement in $R[X]$ ist.*
(b) *Genau dann ist u irreduzibel in R, wenn u irreduzibel in $R[X]$ ist.*
(c) *Ist der Ring $R[X]$ faktoriell, dann ist auch R faktoriell.*

Beweis. Aussage (a) ist äquivalent zu: Genau dann ist Ru ein Primideal in R, wenn $R[X]u$ ein Primideal in $R[X]$ ist. Sie ergibt sich also direkt aus Satz 5.8 (c).

(b) folgt sofort aus der Gradformel: Jeder Teiler von u in $R[X]$ muß Grad 0 haben.

(c) folgt aus (a) und der Gradformel. □

Auch die Umkehrung von (c) ist richtig und ein wichtiger Satz. Wir werden ihn unten beweisen. Eine erste Aussage in dieser Richtung ist

Satz 6.2. *Sei $f = X^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0 \in R[X]$ ein normiertes Polynom über dem faktoriellen Ring R mit Quotientenkörper Q. Dann liegt jede Nullstelle $x_0 \in Q$ von f schon in R und teilt dort a_0.*

Beweis. Wir wählen eine Darstellung $x_0 = r/s$ mit teilerfremden $r, s \in R$. Nach Multiplikation der Gleichung $f(x_0) = 0$ mit s^n ergibt sich

$$r^n + a_{n-1}r^{n-1}s + \cdots + a_1rs^{n-1} + a_0s^n = 0.$$

Also ist r^n durch s teilbar, was der Teilerfremdheit widerspricht, es sei denn, s ist eine Einheit. Mithin gilt $x_0 \in R$ und $x_0 \mid a_0$. □

Als kleine Anwendung beweisen wir, daß das Polynom $f = X^3 + X^2 + 2X + 1$ irreduzibel über $\mathbb{Q}$ ist. Andernfalls hat es eine Nullstelle $x_0 \in \mathbb{Q}$. Diese muß nach dem Satz in $\mathbb{Z}$ liegen und ein Teiler von 1 sein; also $x_0 = \pm 1$. Keine der Zahlen ± 1 ist aber Nullstelle von f.

Auch wenn man häufig an normierten Polynomen interessiert ist, lohnt es sich, diesen Begriff etwas zu verallgemeinern.

Definition. R sei ein Integritätsbereich. Dann heißt $f \in R[X]$ *primitiv*, wenn die Koeffizienten von f teilerfremd sind. Mit anderen Worten: f hat keinen echten Teiler aus R.

Insbesondere sind normierte Polynome primitiv. Wir beweisen nun das *Lemma von Gauß*.

Satz 6.3. *R sei ein faktorieller Ring, Q der Quotientenkörper von R und $f \in R[X]$ ein irreduzibles Polynom. Dann gilt:*

(a) *f ist auch in $Q[X]$ irreduzibel (und damit ein Primelement).*
(b) *Wenn f primitiv ist, ist es ein Primelement in $R[X]$.*

Beweis. (a) Angenommen, es gilt $f = gh$ mit $g, h \in Q[X]$, $\operatorname{grad}(g) \geq 1$, $\operatorname{grad}(h) \geq 1$. Es gibt dann $a, b \in R \setminus \{0\}$ mit ag, $bh \in R[X]$. Betrachte $abf = (ag)(bh)$. ab ist keine Einheit in R, da andernfalls f in $R[X]$ zerlegbar wäre, ab kann aber auch keine Nichteinheit in R sein: Andernfalls wäre ab Produkt von Primelementen aus R. Jeder Primfaktor u von ab in R (ist auch Primelement in $R[X]$ und) teilt ag oder bh. Durch sukzessives Kürzen erhält man also eine Gleichung $f = g_0 h_0$ mit g_0, $h_0 \in R[X]$, wobei g und g_0 bzw. h und h_0 sich nur um Faktoren ($\neq 0$) aus R unterscheiden. Insbesondere ist $\operatorname{grad}(g_0) \geq 1$, $\operatorname{grad}(h_0) \geq 1$. Widerspruch!

(b) Zunächst ist klar, daß f ein Primelement in $Q[X]$ ist, denn irreduzible Elemente eines Hauptidealbereiches sind prim.

Seien $g, h \in R[X]$, und f teile gh in $R[X]$. In $Q[X]$ gilt: f teilt g oder f teilt h, etwa f teilt g, also $g = fg_1$ mit $g_1 \in Q[X]$. Es sei $a \in R$ mit $a \neq 0$ und $ag_1 \in R[X]$. Wir setzen $g_2 = ag_1$. Dann ist $fg_2 = ag$. Bei $a \in R^*$ sind wir fertig. Ist a keine Einheit in R und u Primfaktor von a in R, dann gilt: u teilt g_2 in $R[X]$, da f primitiv ist. Folglich läßt sich a gegen einen Faktor von g_2 kürzen, also: f teilt g in $R[X]$. □

Bevor wir Satz 6.3 zur Untersuchung der Irreduzibilität konkreter Polynome anwenden, ziehen wir eine Konsequenz von prinzipieller Bedeutung.

Satz 6.4. *Ist der Ring R faktoriell, so ist auch $R[X]$ faktoriell.*

Beweis. Es sei $f \in R[X]$, $f \neq 0$, f keine Einheit. d sei ein ggT der Koeffizienten von f in R. Dann ist $f = dg$ mit einem primitiven Polynom $g \in R[X]$. Da d in R (und damit in $R[X]$) Produkt von Primelementen ist, müssen wir wegen 6.3 lediglich noch zeigen, daß jedes primitive Polynom aus $R[X]$ Produkt unzerlegbarer

Elemente von $R[X]$ ist. Es sei $f \in R[X]$ ein primitives Polynom und $f = gh$ mit Nichteinheiten $g, h \in R[X]$. Dann sind offenbar auch g und h wieder primitiv, und es gilt $\operatorname{grad}(g), \operatorname{grad}(h) < \operatorname{grad}(f)$. Die behauptete Faktorisierung läßt sich somit durch Induktion über den Grad von f beweisen. □

Mit Hilfe des letzten Satzes können wir jetzt leicht einen faktoriellen Ring angeben, der kein Hauptidealbereich ist: $\mathbb{Z}$ ist faktoriell, nach 6.4 ist dann auch $\mathbb{Z}[X]$ faktoriell. $\mathbb{Z}[X]$ ist aber kein Hauptidealbereich.

Mit Satz 6.3 kann man zum Beispiel die Irreduzibilität von Polynomen in $\mathbb{Q}[X]$ über $\mathbb{Z}$ testen. Ein klassisches Kriterium, das dann manchmal anwendbar ist, ist das *Kriterium von Eisenstein*:

Satz 6.5. *R sei ein Integritätsbereich und $f \in R[X]$ ein primitives Polynom, $f = \sum_{i=0}^{n} a_i X^i$, $n = \operatorname{grad}(f) \geq 1$. Es gebe ein Primelement u in R mit den folgenden Eigenschaften:*

(a) *u teilt a_i für $i = 0, \ldots, n-1$;*
(b) *u^2 ist kein Teiler von a_0.*

Dann ist f irreduzibel.

Beweis. Angenommen $f = gh$ mit $g, h \in R[X]$, $r = \operatorname{grad}(g) \geq 1$, $s = \operatorname{grad}(h) \geq 1$, $g = b_0 + \cdots + b_r X^r$, $h = c_0 + \cdots + c_s X^s$. Wegen $a_0 = b_0 c_0$ ist u Teiler von b_0 oder von c_0. Im ersten Fall sei b_k der erste Koeffizient von g, der nicht von u geteilt wird. Da g wie f primitiv ist, ist b_k wohlbestimmt. Es ist $a_k = b_0 c_k + \cdots + b_k c_0$. Da $b_0, \ldots, b_{k-1}$ und auch a_k (wegen $k \leq r < n$) von u geteilt werden, ist u Teiler von $b_k c_0$, also von c_0. Folglich ist u^2 Teiler von a_0 im Widerspruch zu (b). □

Ist der Ring R im Eisenstein-Kriterium faktoriell, dann ist – unter den dort angegebenen Voraussetzungen – das Polynom f nach Satz 6.3 sogar irreduzibel über dem Quotientenkörper von R. Man erhält so zum Beispiel sofort, daß das Polynom $X^4 + 6X^3 + 2X^2 + 2$ irreduzibel über $\mathbb{Q}$ ist.

Ein Kunstgriff ist das Anwenden einer geeigneten Substitution $X \mapsto X + a$ mit einem geeigneten $a \in R$. Sei $g = f(X + a)$. Dann gilt $f = g(X - a)$, und f ist genau dann irreduzibel, wenn g es ist. Wir zeigen damit:

Satz 6.6. *Es sei p eine Primzahl und $f = 1 + X + \cdots + X^{p-1}$. Dann ist f irreduzibel in $\mathbb{Q}[X]$.*

Beweis. Es ist $(X-1)f = X^p - 1$. Mittels der Substitution $X \mapsto X + 1$ erhält man aus dieser Gleichung $Xg = (X+1)^p - 1$, $g = 1 + (X+1) + \cdots + (X+1)^{p-1}$, also

$$Xg = X^p + \binom{p}{1} X^{p-1} + \cdots + \binom{p}{p-1} X = X\left(X^{p-1} + pX^{p-2} + \cdots + \binom{p}{p-1}\right).$$

Auf g läßt sich das Eisenstein-Kriterium mit $u = p$ anwenden: g ist irreduzibel über $\mathbb{Z}$ und damit auch über $\mathbb{Q}$. □

Häufig kann man das folgende *Reduktionsverfahren* benutzen, insbesondere dann, wenn der Ring R/P endlich ist, wie etwa im Fall $R = \mathbb{Z}$, $P = \mathbb{Z}p$.

Satz 6.7. *Es sei R ein Integritätsbereich, $f \in R[X]$ ein primitives Polynom und P ein Primideal in R derart, daß der Leitkoeffizient von f nicht in P liegt. $\pi : R \to R/P$ sei die kanonische Projektion und $\pi^* : R[X] \to (R/P)[X]$ die Fortsetzung von π gemäß* 5.7 (b). *Dann gilt: Ist $\pi^*(f)$ irreduzibel, so ist auch f irreduzibel.*

Dies ist offensichtlich: Wenn $f = gh$ mit Polynomen g, h, deren Grad kleiner ist als der von f, so ist $\pi^*(f) = \pi^*(g)\pi^*(h)$, und $\pi^*(f)$ hat nach Voraussetzung den gleichen Grad wie f. Dies ergibt einen Widerspruch zur Irreduzibilität von $\pi^*(f)$.

Als Beispiel betrachten wir $f = X^5 + X^2 + 1 \in \mathbb{Q}[X]$. Zunächst ist klar, daß wir die Irreduzibilität nur über $\mathbb{Z}$ testen müssen. Wir betrachten nun $\pi : \mathbb{Z} \to \mathbb{Z}_2$. Dann ist $\pi^*(f) = X^5 + X^2 + 1$. Dieses Polynom hat keine Nullstelle in $\mathbb{Z}_2$. Wenn es überhaupt zerfällt, dann in der Form gh, wobei $\operatorname{grad} g = 2$, $\operatorname{grad} h = 3$ und g und h irreduzibel. Nun gibt es aber nur ein einziges irreduzibles Polynom des Grades 2 über $\mathbb{Z}_2$, nämlich $X^2 + X + 1$. Man stellt sofort fest, daß es $X^5 + X^2 + 1$ nicht teilt, und hat insgesamt die Irreduzibilität von f (über $\mathbb{Q}$) bewiesen.

Das Kriterium von Eisenstein kann man als Verfeinerung von Satz 6.7 ansehen. Die Voraussetzung dort, angewandt auf das Ideal $P = Rp$, ergibt, daß $\pi^*(f) = aX^n$ ist mit $a \in R/P$, $a \neq 0$. Das Polynom aX^n hat aber nur Zerlegungen in der Form $(bX^r)(cX^s)$, und bei einer eventuellen Zerlegung $f = gh$ in $R[X]$ muß $\pi^*(g) = bX^r$, $\pi^*(h) = cX^s$ sein. Dann aber sind sämtliche Koeffizienten von g und h außer den Leitkoeffizienten durch p teilbar, und der konstante Term von f durch p^2, was einen Widerspruch ergibt.

Schließlich sollte man noch die *Methode der unbestimmten Koeffizienten* erwähnen. Bei ihr macht man einen Ansatz $f = gh$, wobei die Koeffizienten von g und h als Unbestimmte gewählt werden. Man zeigt dann, daß das durch Koeffizientenvergleich entstehende Gleichungssystem nicht lösbar ist.

Hierzu ein einfaches Beispiel (bei dem man allerdings besser mit der Methode der Nullstellen argumentieren sollte): $f = 1 + 5X + 4X^2 + X^3 \in \mathbb{Z}[X]$. Angenommen, f ist reduzibel, also $f = gh$ mit $g, h \in \mathbb{Z}[X]$, $\operatorname{grad}(g) = 2$, $\operatorname{grad}(h) = 1$. Man darf g und h als normiert annehmen. Mit $g = X^2 + aX + b$, $h = X + c$, erhält man das Gleichungssystem

$$\begin{aligned} bc &= 1 \\ ac + b &= 5 \\ a + c &= 4. \end{aligned}$$

Ganze Zahlen a, b, c, die diesen Gleichungen genügen, gibt es aber nicht. Also ist f irreduzibel.

ABSCHNITT 7

Algebraische Körpererweiterungen

Nach dem Fundamentalsatz der Algebra besitzt jedes nichtkonstante Polynom $f \in \mathbb{C}[X]$ eine Nullstelle in $\mathbb{C}$. Speziell gilt dies für Polynome $f \in \mathbb{Q}[X]$ und allgemeiner für Polynome $f \in K[X]$, wenn K ein Teilkörper von $\mathbb{C}$ ist. Wann immer polynomiale Gleichungen zu lösen sind, muß man wissen, daß man zu einem gegebenen Polynom $f \in K[X]$ eine Nullstelle wenigstens in einem Erweiterungskörper L von K finden kann, wenn schon in K selbst keine exisiert. Wie wir gerade gesehen haben, ist die Existenz einer solchen Nullstelle für $K \subset \mathbb{C}$ gesichert.

Ganz anders ist die Situation etwa, wenn K ein endlicher Körper ist. Uns ist keine solche K umfassende „Universalerweiterung“ wie $\mathbb{C}$ für $\mathbb{Q}$ bekannt. Eine geeignete Erweiterung muß vielmehr erst konstruiert werden. Dies ist – mit den Mitteln der modernen Algebra – sehr einfach.

Satz 7.1. *K sei ein Körper und f ein nicht konstantes Polynom über K. Dann gibt es einen K enthaltenden Körper, in dem f eine Nullstelle hat.*

Beweis. Wir zerlegen f in irreduzible Faktoren. Da jede Nullstelle eines irreduziblen Faktors von f auch Nullstelle von f ist, dürfen wir annehmen, daß f selbst irreduzibel ist.

Dann ist $K[X]f$ ein maximales Ideal in $K[X]$, $L = K[X]/K[X]f$ also ein Körper. Es bezeichne $\pi : K[X] \to L$ die kanonische Projektion. Da $(K[X]f) \cap K$ das Nullideal ist, ist $\pi|K$ injektiv. Wir können also K vermöge π als Unterkörper von L und f als Polynom über L auffassen (vgl. 5.7 (a)). Dann ist $0 = \pi(f) = f(\pi(X))$. Das Element $\pi(X)$ ist also Nullstelle von f in L. □

Die Struktur des Körpers L wird von dem irreduziblen Polynom f bestimmt. Daher ist es wichtig, Polynome auf Irreduzibilität untersuchen zu können. Dafür haben wir im vorangegangenen Abschnitt einige Hilfsmittel bereitgestellt.

Man kann die Struktur des im Beweis von Satz 7.1 konstruierten Körpers sehr leicht konkret so beschreiben, daß man in ihm gut rechnen kann. Wir dürfen annehmen, daß f normiert ist, $f = X^n + a_{n-1}X^{n-1} + \cdots + a_0$. Für $x = \pi(X)$ gilt dann $x^n = -(a_{n-1}x^{n-1} + \cdots + a_1x + a_0)$.

Sei $g \in K[X]$. Mittels Division mit Rest hat man

$$g = qf + r, \qquad \operatorname{grad} r < n,$$

so daß die Restklasse von g vom Divisionsrest r repräsentiert wird. Andererseits liegen verschiedene Polynome r,s mit $\operatorname{grad} r, \operatorname{grad} s < n$ niemals in der gleichen Restklasse. Die Abbildung

$$K^n \to L, \qquad (b_{n-1},\dots,b_0) \mapsto b_{n-1}x^{n-1}+\cdots+b_1x+b_0,$$

bildet K^n bijektiv auf L ab, und sie ist sogar K-linear. Damit ist L als K-Vektorraum beschrieben.

Die Multiplikation führen wir aus, indem wir $b_{n-1}x^{n-1}+\cdots+b_1x+b_0$ und $c_{n-1}x^{n-1}+\cdots+c_1x+c_0$ nach den gewohnten Regeln multiplizieren, und dann die Potenzen x^m mit $m \geq n$ mittels der Gleichungen

$$x^m = -(a_{n-1}x^{m-1}+\cdots+a_0x^{m-n})$$

sukzessiv ersetzen. (Dies läuft natürlich auf die Division durch f mit Rest hinaus.) Das Endergebnis hat dann die Form $d_{n-1}x^{n-1}+\cdots+d_1x+d_0$, wie gewünscht.

Die Irreduzibilität von f hat bisher keine Rolle gespielt, aber für die Division in L ist sie natürlich wichtig. Zu $b_{n-1}x^{n-1}+\cdots+b_0 \neq 0$ betrachten wir das Polynom $g = b_{n-1}X^{n-1}+\cdots+b_0 \in K[X]$. Da f irreduzibel ist, sind g und f teilerfremd. Es gibt also Polynome u und v mit

$$1 = uf+vg.$$

Die Restklasse von v ist dann das Inverse von $\bar{g}$ in L.

Nachdem wir uns der Existenz von Nullstellen von Polynomen durch die Konstruktion von Erweiterungskörpern versichert haben, kehren wir die Situation in gewisser Weise um: Wir starten mit einem Erweiterungskörper L von K und interessieren uns vor allem dafür, ob und welche Elemente von L Nullstelle eines Polynoms $f \in K[X]$ sind. Man nennt dann $L:K$ (oder L/K) eine *Körpererweiterung*.

Beispiele. Bei der Körpererweiterung $\mathbb{C}:\mathbb{R}$ ist jede komplexe Zahl $a+bi$, $a,b \in \mathbb{R}$, Nullstelle eines nicht konstanten Polynoms aus $\mathbb{R}[X]$, nämlich von $X^2-2aX+a^2+b^2$. Anders ist die Situation bei $\mathbb{R}/\mathbb{Q}$: Es gibt reelle Zahlen, die nicht Nullstelle eines Polynoms $\neq 0$ über $\mathbb{Q}$ sind. Zum *Beweis* dieser Aussage zeigen wir, daß die Menge

$$\mathbb{A} = \{x \in \mathbb{C} : f(x) = 0 \text{ für ein } f \in \mathbb{Q}[X],\ f \neq 0\}.$$

der *algebraischen Zahlen* abzählbar ist – im Gegensatz zu $\mathbb{R}$. Für jedes $n \in \mathbb{N}$ ist nämlich $\mathbb{Q}^{n+1}$ bijektiv abbildbar auf die Menge der Polynome vom Grad $\leq n$; man ordne jedem $(a_0,a_1,\dots,a_n) \in \mathbb{Q}^{n+1}$ das Polynom $a_0+a_1X+\cdots+a_nX^n$ zu. Also ist die Menge der Polynome vom Grad $\leq n$ abzählbar. Als Vereinigung abzählbar vieler abzählbarer Mengen ist dann auch $\mathbb{Q}[X]$ abzählbar. Da jedes Polynom $\neq 0$ aus $\mathbb{Q}[X]$ nur endlich viele Nullstellen hat, ist $\mathbb{A}$ eine Vereinigung abzählbar vieler endlicher Mengen, also wieder abzählbar. (Es ist schwierig, für eine gegebene reelle Zahl nachzuweisen, daß sie nicht Nullstelle eines Polynoms $\neq 0$ über $\mathbb{Q}$ ist; bekannte Beispiele dafür sind die Kreiszahl π und die Eulersche Zahl e.)

Definition. Es sei L Erweiterungskörper des Körpers K. Dann heißt $\alpha \in L$ *algebraisch* über K, wenn es ein Polynom $f \in K[X]$, $f \neq 0$, gibt mit $f(\alpha) = 0$. Andernfalls heißt α *transzendent* über K. Ist jedes Element von L algebraisch über K, dann heißt $L : K$ eine *algebraische Körpererweiterung*.

Natürlich ist jedes $\alpha \in K$ algebraisch über K. Zum Beispiel ist $\mathbb{C} : \mathbb{R}$ eine algebraische Körpererweiterung, $\mathbb{R} : \mathbb{Q}$ hingegen nicht.

$L : K$ sei eine Körpererweiterung und $\alpha \in L$. Mit $K(\alpha)$ bezeichnen wir den Quotientenkörper von $K[\alpha]$ in L. (Wir erinnern daran, daß $K[\alpha]$ aus allen Summen der Form $a_0 + a_1\alpha + \cdots + a_n\alpha^n$ mit $n \in \mathbb{N}$ und $a_0, \ldots, a_n \in K$ besteht.)

Satz 7.2. *Es sei $L : K$ eine Körpererweiterung und $\alpha \in L$. Dann sind die folgenden Aussagen äquivalent:*

(a) *α ist algebraisch über K.*
(b) *Der Substitutionshomomorphismus $K[X] \to L$, $X \mapsto \alpha$, ist nicht injektiv.*
(c) *$K[\alpha]$ ist ein Körper.*
(d) *Es ist $K[\alpha] = K(\alpha)$.*
(e) *Der Kern des Substitutionshomomorphismus $K[X] \to L$, $X \mapsto \alpha$, wird von einem irreduziblen normierten Polynom $f_\alpha \in K[X]$ erzeugt.*

Ist α algebraisch über K, dann ist das Polynom f_α unter (e) *eindeutig bestimmt.*

Beweis. Die Äquivalenz von (a) und (b) folgt unmittelbar aus der Definition oben.

Das Bild $K[\alpha]$ des Substitutionshomomorphismus $\varphi : K[X] \to L$, $X \mapsto \alpha$, ist ein Integritätsbereich, so daß sein Kern P in jedem Falle ein Primideal ist.

Der Homomorphismus φ ist genau dann nicht injektiv, wenn P nicht das Nullideal, im Hauptidealring $K[X]$ also maximal ist. Dies wiederum ist äquivalent dazu, daß $K[\alpha] \cong K[X]/P$ ein Körper ist. Dies ist gerade die Äquivalenz von (b) und (c). Jene von (c) und (d) ist trivial.

Die Äquivalenz von (c) und (e) folgt schließlich aus der Tatsache, daß ein Ideal $\neq 0$ in einem Hauptidealring genau dann maximal ist, wenn es von einem irreduziblen Element erzeugt wird. Überdies ist jedes irreduzible Polynom in $K[X]$ zu einem normierten Polynom assoziiert.

Da zwei normierte assoziierte Polynome über K schon übereinstimmen, sind wir mit dem Beweis fertig. □

Definition. $L : K$ sei eine Körpererweiterung und $\alpha \in L$ algebraisch über K. Dann heißt das eindeutig bestimmte Polynom f_α aus 7.2 das *Minimalpolynom* von α über K.

In der Situation der Definition ist $g \in K[X]$ genau dann das Minimalpolynom von α über K, wenn g eine der beiden folgenden Eigenschaften erfüllt:

(a) g ist ein irreduzibles, normiertes Polynom mit $g(\alpha) = 0$.
(b) g ist ein normiertes Polynom minimalen Grades mit $g(\alpha) = 0$.

Beispielsweise ist X^2+1 das Minimalpolynom von i über $\mathbb{R}$ und X^2-2 das Minimalpolynom von $\sqrt{2}$ über $\mathbb{Q}$. In der eingangs betrachteten Situation $L = K[X]/I(f)$ mit einem irreduziblen normierten Polynom $f \in K[X]$ ist f das Minimalpolynom der Restklasse x von X.

Ist $L : K$ eine Körpererweiterung, dann ist insbesondere L ein K-Vektorraum, dessen Dimension wir mit $[L : K]$ bezeichnen und den *Grad* von L über K nennen. Die Körpererweiterung $L : K$ heißt *endlich*, wenn $[L : K] < \infty$ gilt. Direkt aus der Definition ergibt sich:

$$[L : K] = 1 \quad \Longleftrightarrow \quad L = K.$$

Ein einfaches nichttriviales Beispiel ist $[\mathbb{C} : \mathbb{R}] = 2$, da 1, i bekanntlich eine Basis von $\mathbb{C}$ über $\mathbb{R}$ bilden. Es ist $\mathbb{C} = \mathbb{R}(i)$ und 2 auch der Grad des Minimalpolynoms von i über $\mathbb{R}$. Allgemein hat man (und das erklärt die Wahl des Begriffes „Grad“ einer Körpererweiterung):

Satz 7.3. *Es sei $L : K$ eine Körpererweiterung und $\alpha \in L$ algebraisch über K. Das Minimalpolynom f_α von α über K besitze den Grad n. Die Substitution $X \mapsto \alpha$ induziert einen Isomorphismus $K[X]/K[X]f_\alpha \cong K(\alpha)$. Insbesondere ist $K(\alpha) : K$ eine endliche Körpererweiterung des Grades n, und die Potenzen $1, \alpha, \ldots, \alpha^{n-1}$ bilden eine K-Basis von $K(\alpha)$.*

Beweis. Dies haben wir im wesentlichen ja schon in Satz 7.2 festgestellt. Mittels des Isomorphismus übertragen sich die eingangs ermittelten Eigenschaften von $K[X]/K[X]f_\alpha$ auf $K(\alpha)$. □

Der Grad von Körpererweiterungen verhält sich multiplikativ in folgendem Sinne:

Satz 7.4. [Gradsatz] *Es seien $L : L'$ und $L' : K$ endliche Körpererweiterungen. Dann ist auch $L : K$ endlich, und es gilt: $[L : K] = [L : L'] \cdot [L' : K]$.*

Beweis. Es sei $x_1, \ldots, x_n$ eine Basis von L über L' und $y_1, \ldots, y_m$ eine Basis von L' über K. Es genügt zu zeigen, daß die Elemente $x_i y_j$, $i = 1, \ldots, n$, $j = 1, \ldots, m$, eine Basis von L über K bilden.

Zum Beweis der linearen Unabhängigkeit über K betrachten wir eine Gleichung $\sum_{i,j} a_{ij} x_i y_j = 0$ mit $a_{ij} \in K$. Wegen $\sum_{i,j} a_{ij} x_i y_j = \sum_i (\sum_j a_{ij} y_j) x_i$ und der linearen Unabhängigkeit von $x_1, \ldots, x_n$ über L' folgt hieraus $\sum_j a_{ij} y_j = 0$ für $i = 1, \ldots, n$. Wegen der linearen Unabhängigkeit von $y_1, \ldots, y_m$ über K folgt weiter $a_{ij} = 0$ für $i = 1, \ldots, n$ und $j = 1, \ldots, m$.

Es sei $x \in L$. Dann ist x Linearkombination der Produkte $x_i y_j$ über K: Zunächst hat man eine Darstellung $x = \sum_i a_i x_i$ mit Elementen $a_i \in L'$ und weiter Darstellungen $a_i = \sum_j b_{ij} y_j$ mit Elementen $b_{ij} \in K$. Insgesamt erhält man $x = \sum_i a_i x_i = \sum_i (\sum_j b_{ij} y_j) x_i = \sum_{i,j} b_{ij} x_i y_j$. □

Wir merken an, daß umgekehrt die Körpererweiterungen $L : L'$ und $L' : K$ natürlich endlich sind, wenn dies für $L : K$ gilt. Bevor wir den zentralen Satz in der Theorie der endlichen Körpererweiterungen formulieren, führen wir noch eine Schreibweise ein: Es sei $L : K$ eine beliebige Körpererweiterung. Dann ist für Elemente $\alpha_1, \ldots, \alpha_n \in L$ der Unterring $K[\alpha_1, \ldots, \alpha_n]$ von L wohldefiniert: Er besteht aus allen Elementen $f(\alpha_1, \ldots, \alpha_n) \in L$ mit $f \in K[X_1, \ldots, X_n]$. Wir bezeichnen mit $K(\alpha_1, \ldots, \alpha_n)$ den Quotientenkörper von $K[\alpha_1, \ldots, \alpha_n]$ in L. Man beachte, daß $K[\alpha_1, \ldots, \alpha_n] = K[\alpha_1, \ldots, \alpha_{n-1}][\alpha_n]$ und $K(\alpha_1, \ldots, \alpha_n) = K(\alpha_1, \ldots, \alpha_{n-1})(\alpha_n)$ bei $n \geq 1$.

Satz 7.5. *Jede endliche Körpererweiterung ist algebraisch. Eine Körpererweiterung $L : K$ ist genau dann endlich, wenn es endlich viele über K algebraische Elemente $\alpha_1, \ldots, \alpha_n \in L$ gibt, so daß $L = K(\alpha_1, \ldots, \alpha_n)$ gilt.*

Beweis. Die Körpererweiterung $L : K$ besitze den Grad $n < \infty$. Es sei $\alpha \in L$. Da $n+1$ Elemente aus L über K linear abhängig sind, gilt eine Gleichung $a_0 + a_1\alpha + \cdots + a_n\alpha^n$ mit Elementen $a_0, \ldots, a_n \in K$, die nicht alle verschwinden. Das von Null verschiedene Polynom $a_0 + a_1X + \cdots + a_nX^n \in K[X]$ hat also α als Nullstelle. Folglich ist α algebraisch über K.

Ist die Körpererweiterung $L : K$ endlich vom Grad n, dann gibt es eine Basis $\alpha_1, \ldots, \alpha_n$ von L über K. Insbesondere ist $L \subset K[\alpha_1, \ldots, \alpha_n] \subset K(\alpha_1, \ldots, \alpha_n)$. Da L ein K und die Elemente $\alpha_1, \ldots, \alpha_n$ enthaltender Körper ist, gilt trivialerweise $K(\alpha_1, \ldots, \alpha_n) \subset L$. Aus dem ersten Teil des Satzes und dem Gradsatz folgt ferner, daß $\alpha_1, \ldots, \alpha_n$ über K algebraisch sind.

Umgekehrt gebe es endlich viele über K algebraische Elemente $\alpha_1, \ldots, \alpha_n \in L$, so daß $L = K(\alpha_1, \ldots, \alpha_n)$ gilt. Für $n = 1$ folgt die zu beweisende Aussage dann aus 7.3. Es sei $n > 1$. Nach Induktionsvoraussetzung ist $K(\alpha_1, \ldots, \alpha_{n-1}) : K$ eine endliche Körpererweiterung. Da das Element α_n algebraisch ist über K, ist es erst recht algebraisch über $K(\alpha_1, \ldots, \alpha_{n-1})$. Folglich ist die Körpererweiterung $K(\alpha_1, \ldots, \alpha_{n-1})(\alpha_n) : K(\alpha_1, \ldots, \alpha_{n-1})$ endlich. Nach dem Gradsatz ist dann auch $K(\alpha_1, \ldots, \alpha_{n-1})(\alpha_n) : K$, d.h. $L : K$ eine endliche Körpererweiterung. □

Aus Satz 7.5 ergibt sich die Transitivität der Eigenschaft von Körpererweiterungen, algebraisch zu sein:

Satz 7.6. *Es seien $L : L'$ und $L' : K$ Körpererweiterungen. Genau dann ist die Körpererweiterung $L : K$ algebraisch, wenn $L : L'$ und $L' : K$ algebraisch sind.*

Beweis. Ist $L : K$ algebraisch, dann sind natürlich $L : L'$ und $L' : K$ algebraisch. Es sei dies umgekehrt der Fall und $\alpha \in L$. Da $L : L'$ algebraisch ist, gilt eine Gleichung $b_0 + b_1\alpha + \cdots + b_n\alpha^n = 0$ mit Elementen $b_0, \ldots, b_n \in L'$, die nicht alle verschwinden. Insbesondere ist α algebraisch über dem Körper $K(b_0, \ldots, b_n)$ und $K(b_0, \ldots, b_n)(\alpha) : K(b_0, \ldots, b_n)$ endlich (nach Satz 7.3). Da die Elemente $b_0, \ldots, b_n$

nach Voraussetzung algebraisch sind über K, ist $K(b_0,\dots,b_n):K$ nach Satz 7.5 eine endliche Körpererweiterung. Mit dem Gradsatz erhalten wir schließlich, daß $K(b_0,\dots,b_n)(\alpha):K$ eine endliche Körpererweiterung ist. Dann ist aber – nach der ersten Aussage von Satz 7.5 – α algebraisch über K. □

Eine weitere wichtige Folgerung aus Satz 7.5 ist

Satz 7.7. *Es sei $L:K$ eine Körpererweiterung und $H_a(L:K)$ die Gesamtheit aller über K algebraischen Elemente von L. Dann ist $H_a(L:K)$ ein K enthaltender Unterkörper von L.*

Beweis. Sind $\alpha,\beta\in L$ algebraisch über K, dann ist $K(\alpha,\beta):K$ nach Satz 7.5 eine algebraische Körpererweiterung. Insbesondere sind die Elemente $\alpha\pm\beta$ und $\alpha\cdot\beta$ sowie, falls $\beta\neq 0$, $\alpha\cdot\beta^{-1}$ wieder algebraisch über K. Das beweist bereits die Behauptung. □

Hieraus ergibt sich zum Beispiel, daß die zu Beginn dieses Abschnitts betrachtete Menge $\mathbb{A}$ der algebraischen Zahlen ein $\mathbb{Q}$ enthaltender Unterkörper von $\mathbb{C}$ ist. $\mathbb{A}:\mathbb{Q}$ ist nicht endlich: Für jedes $n\in\mathbb{N}$, $n\geq 1$, ist $f=X^n-2$ ein irreduzibles Polynom in $\mathbb{Q}[X]$ (warum?). Folglich ist f das Minimalpolynom von $\sqrt[n]{2}$ über $\mathbb{Q}$ und $[\mathbb{Q}(\sqrt[n]{2}):\mathbb{Q}]=n$ (nach Satz 7.3). Nach dem Gradsatz kann $\mathbb{A}:\mathbb{Q}$ nicht endlich sein.

ABSCHNITT 8

Zerfällungskörper von Polynomen

Es sei K ein Körper und f ein nicht konstantes Polynom in $K[X]$. Wegen Satz 7.1 gibt es einen Erweiterungskörper L von K, über dem f in Linearfaktoren zerfällt; denn wenn dies über K noch nicht der Fall sein sollte, erweitern wir K einfach durch Adjunktion einer Nullstelle. Spätestens nach grad f solchen Erweiterungen haben wir unser Ziel erreicht. Sind $\alpha_1, \ldots, \alpha_n$ die verschiedenen Nullstellen von f in L, dann zerfällt f natürlich schon über dem Teilkörper $K(\alpha_1, \ldots, \alpha_n)$ von L in Linearfaktoren. Da jeder K umfassende Teilkörper von L, über dem f in Linearfaktoren zerfällt, die Elemente $\alpha_1, \ldots, \alpha_n$ enthalten muß, ist $K(\alpha_1, \ldots, \alpha_n)$ der kleinste K umfassende Teilkörper von L, über dem f in Linearfaktoren zerfällt.

Definition. K sei ein Körper und f ein nicht konstantes Polynom über K. Ein Erweiterungskörper L von K heißt *Zerfällungskörper* von f (über K), wenn f über L in Linearfaktoren zerfällt und $L = K(\alpha_1, \ldots, \alpha_n)$ gilt, wobei $\alpha_1, \ldots, \alpha_n$ die Nullstellen von f in L sind.

Wir betrachten dazu folgende

Beispiele. (a) Sei $f = X^3 - 1 = (X-1)(X^2+X+1) \in \mathbb{Q}[X]$. Dieses Polynom hat die Nullstellen 1, $\zeta_1 = (1+i\sqrt{3})/2$ und $\zeta_2 = \zeta_1^2$. Folglich liegt $\zeta_2 \in L = \mathbb{Q}[\zeta_1]$, und f zerfällt über L in Linearfaktoren.

Das können wir leicht verallgemeinern: Wenn g ein irreduzibles Polynom des Grades 2 über K ist und $L = K[\alpha]$ für eine Nullstelle α von g, dann zerfällt g über $K[\alpha]$ natürlich in Linearfaktoren, und der Zerfällungskörper ist gefunden.

(b) Sei nun $f = X^3 - 2$. Dieses Polynom hat keine Nullstelle in $\mathbb{Q}$ und ist daher irreduzibel. Sei $K = \mathbb{Q}[\sqrt[3]{2}]$. Dann gilt $[K : \mathbb{Q}] = 3$. Keineswegs aber ist K der Zerfällungskörper, denn $K \subset \mathbb{R}$, und f hat ja zwei nichtreelle Nullstellen, nämlich $\rho_1 = \sqrt[3]{2}\zeta_1$ und $\rho_2 = \sqrt[3]{2}\zeta_2$ (mit den Bezeichnungen aus (a)). Sei $f = (X - \sqrt[3]{2})g$. Dann hat $g \in K[X]$ den Grad 2, und wenn wir $L = K[\zeta_1]$ setzen, haben wir den Zerfällungskörper von f gefunden. Da $[L : K] = 2$, folgt nach dem Gradsatz insgesamt $[L : \mathbb{Q}] = 6$. (Man sieht übrigens leicht, daß $\mathbb{Q}[\zeta_1] \subset L$, nämlich wie?)

Natürlich sind Zerfällungskörper immer endlich über dem Grundkörper. Die Existenz von Zerfällungskörpern ist, wie wir gesehen haben, gesichert. Wir widmen uns jetzt dem Eindeutigkeitsproblem, d.h. wir wollen zeigen, daß die Zerfäl-

lungskörper, die man in verschiedenen Körpern über dem Grundkörper konstruieren kann, auf natürliche Weise zueinander isomorph sind.

Sind L und $\tilde{L}$ Erweiterungskörper des Körpers K, dann nennt man einen Homomorphismus von L in $\tilde{L}$, der die Elemente von K fest läßt, einen *K-Homomorphismus*. Offenbar ist ein Ring-Homomorphismus $\psi\colon L \to \tilde{L}$ genau dann ein K-Homomorphismus, wenn ψ gleichzeitig eine K-lineare Abbildung im Sinne der linearen Algebra ist. Die Begriffe *K-Isomorphismus* und *K-Automorphismus* werden entsprechend eingeführt.

Satz 8.1. *Seien K ein Körper, f ein irreduzibles Polynom über K und α, β Nullstellen von f in Erweiterungskörpern von K. Dann gibt es genau einen K-Isomorphismus $\psi : K[\alpha] \to K[\beta]$ mit $\psi(\alpha) = \beta$.*

Beweis. Sei grad $f = n$. Nehmen wir an, ein K-Homomorphismus ψ mit $\psi(\alpha) = \beta$ sei gefunden. Dann gilt für alle $c_0, \ldots, c_{n-1} \in K$:

$$\psi(c_{n-1}\alpha^{n-1} + \cdots + c_0) = c_{n-1}\beta^{n-1} + \cdots + c_0.$$

Dies zeigt unmittelbar, daß ψ ein Isomorphismus sein muß und eindeutig bestimmt ist, denn $\alpha^{n-1}, \ldots, 1$ und $\beta^{n-1}, \ldots, 1$ sind Basen der K-Vektorräume $K[\alpha]$ und $K[\beta]$. Wir könnten ψ direkt durch die obige Gleichung definieren, müssten dann aber zeigen, daß es wirklich ein Ringhomomorphismus ist. Das ist nicht schwer, aber wir wollen stattdessen den Satz vom induzierten Homomorphismus heranziehen, und zwar schon deshalb, um seine Anwendung zu üben.

Wir betrachten die Substitutionshomomorphismen $\pi : K[X] \to K[\alpha]$, $\pi(X) = \alpha$, und $\varphi : K[X] \to K[\beta]$, $\varphi(X) = \beta$. Beide sind surjektiv und haben den gleichen Kern $P = K[X]f$ (siehe Satz 7.2). Nach dem Satz vom induzierten Homomorphismus können wir dann einen Homomorphismus $\psi : K[\alpha] \to K[\beta]$ mit $\psi \circ \pi = \varphi$ finden.

Da $\pi(x) = x = \varphi(x)$ für alle $x \in K$ gilt, trifft dies auch auf ψ zu, denn $\psi(x) = \psi(\pi(x) = \varphi(x) = x$. Ferner ist $\psi(\alpha) = \psi(\pi(X)) = \varphi(X) = \beta$. □

Der letzte Satz ist der wesentliche Schritt beim Beweis von

Satz 8.2. *Seien L und $\tilde{L}$ Erweiterungen von K, die beide Zerfällungskörper des Polynoms f über K sind. Dann gibt es einen K-Isomorphismus $\varphi : L \to \tilde{L}$ mit $\varphi|K = \mathrm{id}_K$.*

Beweis. Wir beweisen die Behauptung durch Induktion über den (endlichen) Grad von $L : K$. Bei $[L : K] = 1$ ist $L = \tilde{L} = K$, und man setze $\varphi = \mathrm{id}_K$.

Es sei $[L : K] > 1$. Es gibt einen irreduziblen Faktor g von f mit $\operatorname{grad} g \geq 2$. Dieser hat in L eine Nullstelle α, in $\tilde{L}$ eine Nullstelle β. Nach Satz 8.1 gibt es einen K-Isomorphismus $\psi : K[\alpha] \to K[\beta]$ mit $\psi(\alpha) = \beta$. Wir dürfen $K[\alpha]$ und $K[\beta]$ mittels ψ identifizieren, also annehmen, daß $\tilde{K} = K[\alpha]$ in $\tilde{L}$ enthalten ist und $\alpha = \beta$ gilt.

Nun sind L und $\tilde{L}$ Zerfällungskörper von f auch als Polynom aus $\tilde{K}[X]$. Da $[L:\tilde{K}] < [L:K]$, können wir die Induktionsvoraussetzung anwenden und erhalten einen $\tilde{K}$-Isomorphismus $L \cong \tilde{L}$. Dieser ist auch ein K-Isomorphismus. □

Satz 8.2 erlaubt es uns, von *dem* Zerfällungskörper des Polynoms f über dem Körper K zu sprechen. Man sollte aber beachten, daß der Isomorphismus in Satz 8.2 keineswegs eindeutig bestimmt ist. Dies würde ja im Fall $L = \tilde{L}$ insbesondere bedeuten, daß der einzige K-Automorphismus von L die Identität ist, was nun keineswegs zutrifft. Wir diskutieren dazu zwei Beispiele.

Beispiele. (a) Sei $[L:K] = 2$, etwa $L = K[\alpha]$ mit Minimalpolynom f vom Grad 2. Wir setzen voraus, daß $\operatorname{char} K \neq 2$. Dann gilt $\beta \neq \alpha$ für die zweite Nullstelle β von f. Nach Satz 8.1 gibt es also einen K-Automorphismus φ von L mit $\varphi(\alpha) = \beta$,

$$\varphi(x + y\alpha) = x + y\beta,$$

für alle $x, y \in K$. Wegen $\varphi(\alpha) = \beta \neq \alpha$ ist $\varphi \neq \mathrm{id}_L$. Mann nennt φ üblicherweise die *Konjugation* auf L (bezüglich K), denn im Spezialfall $K = \mathbb{R}$, $L = \mathbb{C}$ ist φ die komplexe Konjugation.

Andererseits ist jeder K-Automorphismus ψ von L durch seinen Wert auf α bestimmt, denn jedes Element von L hat die Form $x + y\alpha$ mit $x, y \in K$. Da nun aber auch $\psi(\alpha)$ Nullstelle von f sein muß, gilt $\psi(\alpha) = \alpha$ oder $\psi(\alpha) = \beta$. Es folgt $\psi = \mathrm{id}_L$ oder $\psi = \varphi$.

(b) Wir betrachten noch einmal den Zerfällungskörper L des Polynoms $f = X^3 - 2$ über $\mathbb{Q}$. Wir wissen, daß $L = K[\alpha]$ mit $K = \mathbb{Q}[\sqrt[3]{2}]$, $\alpha = \sqrt[3]{2}\zeta_1$, $\zeta_1^3 = 1$, ist. Da $[L:K] = 2$, gibt es nach (a) einen K-Automorphismus φ von L mit $\varphi(\alpha) = \beta = \sqrt[3]{2}\zeta_1^2$. Wegen $\mathbb{Q} \subset K$ ist φ ein $\mathbb{Q}$-Automorphismus mit $\varphi(\sqrt[3]{2}) = \sqrt[3]{2}$. φ ist die Einschränkung der komplexen Konjugation von $\mathbb{C}$ auf L.

Wir können analog Automorphismen konstruieren, die eine der anderen beiden Nullstellen α und β von f festhalten und die dritte mit $\sqrt[3]{2}$ vertauschen. Wenn wir dann noch Kompositionen dieser drei Automorphismen betrachten, sehen wir, daß sich jede Permutation der 3 Nullstellen durch $\mathbb{Q}$-Automorphismen von L realisieren läßt. Damit besitzt L mindestens 6 $\mathbb{Q}$-Automorphismen. Mehr können es andererseits nicht sein, denn jeder solche Automorphismus ist durch seine Werte auf den 3 Nullstellen eindeutig bestimmt: Jedes Element von L ist $\mathbb{Q}$-Linearkombination von Produkten ihrer Potenzen.

Mit der genaueren Untersuchung der Automorphismen von Körpern beschäftigt sich die *Galois-Theorie*.

Am Schluß dieses Abschnitts wollen wir auf das Existenz- und Eindeutigkeitsproblem endlicher Körper eingehen. Dafür stellen wir noch einen Hilfssatz bereit.

Satz 8.3. *Sei G eine (multiplikativ geschriebene) abelsche Gruppe der Ordnung n. Dann ist $a^n = e$ für alle $a \in G$.*

Beweis. Die Multiplikation mit a ist eine bijektive Abbildung von G auf sich selbst. Daher, und weil G abelsch ist, ist

$$\prod_{b\in G} b = \prod_{b\in G} ab = a^n \prod_{b\in G} b.$$

Kürzen von $\prod_{b\in G} b$ liefert $a^n = e$. □

Wie wir bereits wissen, ist die Mächtigkeit eines endlichen Körpers immer eine Primzahlpotenz. Wir können als erstes zeigen, daß es bis auf Isomorphie höchstens einen endlichen Körper mit p Elementen gibt.

Satz 8.4. *Es sei p eine Primzahl, n eine positive ganze Zahl und L ein Körper mit p^n Elementen. Dann ist L Zerfällungskörper des Polynoms $X^{p^n} - X$ über dem Primkörper $\mathbb{Z}_p$ von L.*

Beweis. Die Einheitengruppe L^* von L hat $p^n - 1$ Elemente. Nach Satz 8.3 gilt folglich $a^{p^n-1} = 1$ für alle $a \in L^*$, also $a^{p^n} - a = 0$ für alle $a \in L$. Damit sind alle Elemente von L Nullstellen des Polynoms $X^{p^n} - X \in K[X]$, wobei $K \cong \mathbb{Z}_p$ den Primkörper von L bezeichne, vgl. Satz 3.1. Da der Grad dieses Polynoms p^n ist, zerfällt es über L in Linearfaktoren; L ist folglich Zerfällungskörper von $X^{p^n} - X$ über K. □

Wir wollen jetzt umgekehrt zeigen, daß der Zerfällungskörper von $X^{p^n} - X$ über $\mathbb{Z}_p$ genau p^n Elemente enthält. Hierzu benötigen wir als Beweis-Instrument den Begriff der (formalen) Ableitung eines Polynoms. Im folgenden sei R stets ein *kommutativer Ring mit Einselement*.

Definition. Es sei $f = \sum_{i=0}^{n} a_i X^i \in R[X]$. Dann heißt das Polynom

$$f' = \begin{cases} 0, & \text{falls } f \text{ konstant ist,} \\ \sum_{i=1}^{n} i a_i X^{i-1} & \text{andernfalls,} \end{cases}$$

die *Ableitung* von f.

Mit diesem Ableitungsbegriff können wir so umgehen, wie wir das aus der Analysis gewohnt sind:

Satz 8.5. *Für alle $f, g \in R[X]$, $a \in R$ und $n \in \mathbb{N}$, $n > 0$, gilt:*

(a) $(f+g)' = f' + g'$;
(b) $(af)' = af'$;
(c) $(fg)' = f'g + fg'$;
(d) $(f^n)' = nf^{n-1}f'$.

Der *Beweis* erfolgt durch Nachrechnen. Mit Hilfe der Ableitung können wir kontrollieren, ob ein gegebenes Polynom $f \in R[X]$, $f \neq 0$, mehrfache Nullstellen in R hat.

Satz 8.6. *Es sei $f \in R[X]$, $f \neq 0$. Genau dann hat f in $a \in R$ eine einfache Nullstelle, wenn $f(a) = 0$ und $f'(a) \neq 0$ gilt.*

Beweis. $f(a) = 0$ ist gleichbedeutend mit $f = (X-a)g$, $g \in R[X]$ (Satz 5.9). Hat f in $a \in R$ eine einfache Nullstelle, dann ist $g(a) \neq 0$. Wegen $f' = g + (X-a)g'$ gilt dann $f'(a) \neq 0$. Hat f in a eine mehrfache Nullstelle, so gilt $f = (X-a)^2 h$ mit einem $h \in R[X]$ und $f' = 2(X-a)h + (X-a)^2 h'$, also $f'(a) = 0$. □

Satz 8.7. *Es sei p eine Primzahl und n eine positive ganze Zahl. Dann ist der Zerfällungskörper des Polynoms $X^{p^n} - X$ über $\mathbb{Z}_p$ bis auf Isomorphie der einzige Körper mit p^n Elementen.*

Beweis. Das Polynom $f = X^{p^n} - X$ hat wegen $f' = -1$ (beachte in $\mathbb{Z}_p[X]$: $(X^{p^n})' = p^n X^{p^n-1} = 0$) im Zerfällungskörper L über $\mathbb{Z}_p$ nur einfache Nullstellen.

Es genügt zu zeigen, daß diese Nullstellen einen Teilkörper K von L bilden. Wir wissen, daß die Abbildung $F : L \to L$, $F(x) = x^p$ ein Endomorphismus von L in sich ist (damit sogar ein Automorphismus, denn L hat nur endlich viele Elemente). Sei G die n-fache Komposition von F mit sich selbst. Dann ist auch G ein Endomorphismus von L und die Teilmenge $\{x \in L : G(x) = x\}$ ist ein Teilkörper. Nach Definition besteht er gerade aus den Nullstellen von f.

Nach Definition des Zerfällungskörpers gilt $K = L$. Die Eindeutigkeitsaussage hatten wir bereits bewiesen. □

ABSCHNITT 9

Konstruktionen mit Zirkel und Lineal

Konstruktionen mit Zirkel und Lineal sind nach Platon solche, bei denen nur die folgenden Konstruktionsschritte zulässig sind:

(a) Zeichnen einer Geraden durch zwei bereits vorhandene Punkte.
(b) Zeichnen eines Kreises um einen bereits vorhandenen Punkt als Mittelpunkt mit dem Abstand zweier vorhandener Punkte als Radius.
(c) Hinzufügen der Schnittpunkte der so konstruierten Geraden und Kreise zu den vorhandenen Punkten.

Wir wollen dies zunächst präzisieren. Dazu bezeichne E die euklidische Ebene, und für $M \subset E$, $|M| \geq 2$, sei $G(M)$ die Menge der aus M mittels der Schritte (a) und (b) konstruierbaren Figuren. Also besteht besteht $G(M)$ aus allen Geraden durch zwei Punkte in M und allen Kreisen, deren Mittelpunkt in M liegt und deren Radius der Abstand zweier Punkte aus M ist.

Definition. Der Punkt $a \in E$ *entsteht aus M durch Elementarkonstruktion*, wenn a Schnittpunkt zweier Figuren aus $G(M)$ ist.

Der Punkt $a \in E$ *ist aus M konstruierbar*, wenn es Punkte $a_1, \ldots, a_n \in E$ gibt mit $a_n = a$, so daß a_1 aus M und a_{i+1} für $i = 1, \ldots, n-1$ aus $M \cup \{a_1, \ldots, a_i\}$ durch Elementarkonstruktion entsteht.

Insbesondere sind die Punkte von M aus M (elementar) konstruierbar (weshalb?). Wir vereinbaren noch folgende vereinfachende Sprechweise: Die Gerade g heißt aus M konstruierbar, wenn es auf g mindestens zwei verschiedene Punkte gibt, die aus M konstruierbar sind. Leicht einzusehen sind die im folgenden häufig verwendeten Aussagen:

(a) Sind zwei Punkte aus M konstruierbar, dann ist auch der Mittelpunkt der Verbindungsstrecke aus M konstruierbar.
(b) Sind der Punkt P und die Gerade g aus M konstruierbar, dann ist auch die Senkrechte zu g durch P aus M konstruierbar.

Zum *Beweis* von (a) seien P, Q aus M konstruierbar. Wir dürfen $P \neq Q$ annehmen. Die Kreise um P und Q mit dem Abstand von P und Q als Radius schneiden sich in zwei verschiedenen Punkten; die Verbindungsgerade (ist die Mittelsenkrechte und) schneidet die Gerade durch P und Q im gesuchten Mittelpunkt. Bei (b) sei $Q \neq P$ ein aus M konstruierbarer Punkt von g und r der Abstand von P und Q. Der Kreis

um P mit dem Radius r schneidet die Gerade g in Q und einem weiteren Punkt Q'. Bei $Q' \neq Q$ bestimmen die Kreise um Q, Q' mit dem Abstand von Q und Q' als Radius die Senkrechte auf g durch P. Ist $Q' = Q$, dann ist die Verbindungsgerade von P und Q bereits die gesuchte Senkrechte.

Wir identifizieren jetzt E mit $\mathbb{R}^2$, um algebraische Methoden verwenden zu können. Dabei wählen wir die Koordinaten in $\mathbb{R}^2$ so, daß die Punkte $(0,0)$ und $(1,0)$ in M liegen. Die Punkte $(r,0)$ identifizieren wir wie üblich mit den Körperelementen $r \in \mathbb{R}$. Es gilt:

(c) Der Punkt $(x,y) \in \mathbb{R}^2$ ist genau dann aus M konstruierbar, wenn x und y aus M konstruierbar sind.

Beim *Beweis* von (c) beachte man, daß die y-Achse nach (b) aus M konstruierbar ist. Ist (x,y) aus M konstruierbar, dann sind es nach (b) auch die Senkrechten durch (x,y) auf die x-Achse und die y-Achse. Also sind x, y aus M konstruierbar. Ist dies umgekehrt der Fall, dann ist offenbar auch $(0,y)$ aus M konstruierbar. Da (x,y) Schnittpunkt der Lote durch x und $(0,y)$ auf die x- bzw. y-Achse ist, sind wir fertig.

Satz 9.1. *Es sei $M \subset \mathbb{R}^2$ mit $0,1 \in M$. Dann gilt:*

(a) *Die Menge K_M der aus M konstruierbaren Punkte von $\mathbb{R}$ ist ein ($\mathbb{Q}$ enthaltender) Teilkörper von $\mathbb{R}$.*
(b) *Ist $r \in K_M$, $r \geq 0$, dann ist auch $\sqrt{r} \in K_M$.*

Beweis. (a) Wir wissen, daß 0 und 1 in K_M liegen. Es seien $x, y \in K_M$. Der Kreis um x mit dem Radius $|y|$ schneidet $\mathbb{R}$ in den Punkten $x \pm y$. Also gilt $x - y \in K_M$. Es sei $y \neq 0$. Zum Beweis von $xy^{-1} \in K_M$ dürfen wir $x, y > 0$ annehmen. Nach Aussage (c) oben sind auch $(0,x), (1, x-y)$ aus M konstruierbar. Die Gerade durch $(0,x)$ und $(1, x-y)$ schneidet $\mathbb{R}$ nach dem Strahlensatz im Punkt xy^{-1}.

(b) Der Punkt $\frac{r-1}{2}$ liegt wegen (a) in K_M. Der Kreis um $\frac{r-1}{2}$ mit dem Radius $\frac{r+1}{2}$ schneidet die (positive) y-Achse in einem Punkt $(0,s)$. Das von den Punkten -1, r, $(0,s)$ gebildete Dreieck ist nach dem Satz des Thales in $(0,s)$ rechtwinklig. Nach dem Höhensatz des Euklid gilt $s^2 = r$. Also gilt $\sqrt{r} \in K_M$. □

Bevor wir das eigentliche Konstruierbarkeitskriterium formulieren, zwei Hilfsaussagen:

Satz 9.2. *Es sei $M \subset \mathbb{R}^2$ mit $0,1 \in M$. K sei ein Teilkörper von $\mathbb{R}$, der die Koordinaten aller Punkte von M enthält. Dann gibt es zu jedem durch Elementarkonstruktion aus M entstehenden Punkt (x,y) einen Teilkörper L von $\mathbb{R}$ mit $L \supset K$, $x, y \in L$ und $[L : K] \leq 2$.*

Beweis. Wir haben drei Fälle zu betrachten:

1. (x,y) ist Schnittpunkt zweier Geraden $g, g' \in G(M)$.

2. (x,y) ist Schnittpunkt einer Geraden g und eines Kreises k aus $G(M)$.
3. (x,y) ist Schnittpunkt zweier Kreise $k,k' \in G(M)$.

Wir untersuchen die drei Fälle. 1. Fall: g und g' seien gegeben durch Punkte (x_1,y_1), (x_2,y_2) und (x'_1,y'_1), (x'_2,y'_2) von M. Der Schnittpunkt (x,y) ist die eindeutige Lösung des linearen Gleichungssystems

$$\begin{aligned}(X-x_1)(y_2-y_1)-(Y-y_1)(x_2-x_1)&=0\\(X-x'_1)(y'_2-y'_1)-(Y-y'_1)(x'_2-x'_1)&=0.\end{aligned}$$

Die Koeffizienten dieses Gleichungssystems gehören zu K, also auch die Koordinaten x,y der Lösung. Setze in diesem Falle $L=K$.

2. Fall: Es sei g wie im 1. Fall. Der Kreis k ist gegeben durch den Mittelpunkt $(x_3,y_3) \in M$ und den Radius r, wobei $r^2=(x_4-x_5)^2+(y_4-y_5)^2$ mit Punkten (x_4,y_4), $(x_5,y_5) \in M$. (x,y) ist Lösung des Gleichungssystems

$$\begin{aligned}(X-x_1)(y_2-y_1)-(Y-y_1)(x_2-x_1)&=0\\(X-x_3)^2+(Y-y_3)^2-r^2&=0,\end{aligned}$$

dessen Koeffizienten wieder zu K gehören. Setze $L=K(x,y)$. Da sich eine der Koordinaten x,y mittels der Gleichung für g durch die andere K-linear ausdrücken läßt, wählen wir $L=K(x)$. Setzt man entsprechend in die Gleichung für k ein, so erhält man eine quadratische Gleichung (über K) in x. D.h. $[L:K] \leq 2$.

3. Fall: Der Kreis k sei gegeben wie im 2. Fall, der Kreis k' entsprechend. (x,y) ist Lösung des Systems der zugehörigen Kreisgleichungen. Durch Subtraktion dieser Gleichungen erhält man ein Gleichungssystem wie im 2. Fall. □

Der folgende Satz benutzt das Prinzip der quadratischen Ergänzung, mittels dessen wir die Lösung von quadratischen Gleichungen auf das Wurzelziehen reduzieren.

Satz 9.3. *Sei K ein Körper mit von 2 verschiedener Charakteristik und $L:K$ eine Erweiterung des Grades 2. Dann gibt es ein $r \in K$ mit $L=K(\sqrt{r})$.*

Beweis. Es sei $\alpha \in L \setminus K$. Dann ist $K \subsetneq K(\alpha)$. Wegen $[L:K]=2$ gilt $K(\alpha)=L$. Insbesondere gilt eine Gleichung $\alpha^2+a\alpha+b=0$ mit $a,b \in K$. Es ist dann $\alpha+a/2=\pm\sqrt{r}$ mit $r=a^2/4-b \in K$ und folglich $K(\alpha)=K(\alpha+a/2)=K(\sqrt{r})$. □

Wir können nun ein algebraisches Konstruierbarkeitskriterium formulieren.

Satz 9.4. *Es sei M eine Teilmenge von $\mathbb{R}^2$ mit $0,1 \in M$. $Q(M)$ bezeichne den kleinsten Teilkörper von $\mathbb{R}$, der die Koordinaten aller Punkte von M enthält. Genau dann ist der Punkt $(x,y) \in \mathbb{R}^2$ aus M konstruierbar, wenn es eine Kette $K_0 \subset K_1 \subset \cdots \subset K_n$ von Teilkörpern von $\mathbb{R}$ gibt mit $K_0=Q(M)$, $[K_{i+1}:K_i] \leq 2$ für $i=0,\ldots,n-1$ und $x,y \in K_n$.*

Beweis. Der Punkt $a = (x,y) \in \mathbb{R}^2$ sei aus M konstruierbar. Dann gibt es Punkte $a_1,\dots,a_n \in \mathbb{R}^2$ mit $a_n = a$, so daß a_1 aus M und a_{i+1} aus $M \cup \{a_1,\dots,a_i\}$, $i = 1,\dots,n-1$, elementar konstruierbar ist. Wir setzen $K_0 = Q(M)$ und nehmen an, wir haben bereits eine Kette $K_0 \subset \cdots \subset K_j$, $0 \le j < n$, von Teilkörpern von $\mathbb{R}$ gefunden mit $[K_{i+1} : K_i] \le 2$ für $0 \le i \le j-1$ und derart, daß die Koordinaten von $a_1,\dots,a_j$ in K_j liegen. Nach Satz 9.2 existiert dann ein Teilkörper K_{j+1} von $\mathbb{R}$ mit $K_{j+1} \supset K_j$, $[K_{j+1} : K_j] \le 2$ und derart, daß die Koordinaten von a_{j+1} in K_{j+1} liegen.

Umgekehrt existiere eine Kette von Teilkörpern von $\mathbb{R}$ wie in der Behauptung des Satzes beschrieben. Es sei dann

$$K_M = \{x \in \mathbb{R} : x \text{ ist aus } M \text{ konstruierbar}\}.$$

Dann ist K_M nach Satz 9.1 ein Teilkörper von $\mathbb{R}$. Da K_M die Koordinaten sämtlicher Punkte von M enthält, gilt $K_0 = Q(M) \subset K_M$. Wegen $[K_1 : K_0] \le 2$ ist ($K_0 = K_1$ oder) $K_1 = K_0(\sqrt{r_0})$ mit einem $r_0 \in K_0$, $r_0 \ge 0$ (Satz 9.3). Wieder nach Satz 9.1 gilt $\sqrt{r_0} \in K_M$, also $K_1 \subset K_M$. Indem man diesen Schluß iteriert, erhält man nach n Schritten $K_n \subset K_M$, insbesondere $x,y \in K_M$. □

Eine unmittelbare Folgerung aus Satz 9.4 ist

Satz 9.5. *M und $Q(M)$ seien wie in der Voraussetzung von Satz 9.4. Ist der Punkt $(x,y) \in \mathbb{R}^2$ aus M konstruierbar, dann sind x,y algebraisch über $Q(M)$ und die Grade der zugehörigen Minimalpolynome sind Potenzen von 2.*

Beweis. Der Körper K_n in Satz 9.4 ist endlich über $K_0 = Q(M)$ und sein Grad über $Q(M)$ eine Potenz von 2. Also sind $x,y \in K_n$ algebraisch über $Q(M)$ und $[K_0(x) : Q(M)]$, $[K_0(y) : Q(M)]$ als Teiler von $[K_n : Q(M)]$ ebenfalls Potenzen von 2. □

Aus dem ersten Teil von 9.5 erhält man bereits die Unlösbarkeit einiger klassischer Konstruierbarkeitsprobleme:

(a) Die *Quadratur des Kreises* mit Zirkel und Lineal ist nicht möglich (d.h. es ist nicht möglich, zu einem gegebenen Kreis mit Zirkel und Lineal ein flächengleiches Quadrat zu konstruieren).

Beweis. In einem geeigneten Koordinatensystem ist $(0,0)$ der Mittelpunkt des gegebenen Kreises und sein Radius der Abstand der Punkte $(0,0)$ und $(1,0)$. Insbesondere liegt der Kreis in $G(M)$ mit $M = \{(0,0),(1,0)\}$. Ein Quadrat ist gegeben durch seine Kantenlänge. Ein Quadrat mit dem gleichen Flächeninhalt wie der vorgegebene Kreis hat die Kantenlänge $\sqrt{\pi}$. Die Quadratur des vorgegebenen Kreises würde also bedeuten, daß sich zwei Punkte in $\mathbb{R}^2$ aus M konstruieren ließen, deren Abstand $\sqrt{\pi}$ ist. Dann ließe sich auch $\sqrt{\pi}$ aus M konstruieren und weiter π. Nach Satz 9.5 wäre dann π algebraisch über $Q(M) = \mathbb{Q}$. Widerspruch! □

Einen Beweis dafür, daß π transzendent ist über $\mathbb{Q}$, findet man zum Beispiel in der Literatur.

(b) Das *Delische Problem* der Würfelverdopplung ist nicht lösbar. (D.h. es ist nicht möglich, aus einem gegebenen Würfel mit Zirkel und Lineal einen Würfel des doppelten Volumens zu konstruieren. Das Orakel hatte die Einwohner von Delos aufgefordert, einen würfelförmigen Altar des Apollon zu verdoppeln.)

Beweis. Bei geeigneten Koordinaten ist die Kantenlänge l des gegebenen Würfels der Abstand der Punkte $(0,0)$ und $(1,0)$, also $l = 1$. Ein Würfel mit doppeltem Volumen hätte dann die Kantenlänge $\sqrt[3]{2}$. Einen solchen Würfel aus dem gebenen Würfel mit Zirkel und Lineal zu konstruieren hieße, zwei Punkte in $\mathbb{R}^2$ aus $M = \{(0,0),(1,0)\}$ zu konstruieren, deren Abstand $\sqrt[3]{2}$ ist. Dann wäre auch $\sqrt[3]{2}$ aus M konstruierbar. Der Grad des Minimalpolynoms von $\sqrt[3]{2}$ über $\mathbb{Q}$ ist aber, im Widerspruch zu Satz 9.5, keine Potenz von 2. □

(c) Es ist im allgemeinen nicht möglich, einen vorgegebenen Winkel mit Zirkel und Lineal in drei gleiche Teile zu zerlegen.

Beweis. Ein Winkel ist gegeben durch die Punkte $(0,0),(1,0)$ und einen weiteren Punkt auf dem Einheitskreis. Es sei wieder $M = \{(0,0),(1,0)\}$. Dann ist der Punkt a auf dem Einheitskreis, der den 60°-Winkel bestimmt, offenbar aus M elementar konstruierbar (als Schnittpunkt des Einheitskreises und des Kreises um $(1,0)$ mit dem Radius 1). Den Winkel $\alpha = 60^\circ$ dreiteilen hieße, den Punkt $(\cos\beta, \sin\beta)$ mit $\beta = 20^\circ$ aus M zu konstruieren. Dann wäre auch $c = 2\cos\beta$ aus M konstruierbar. Das ist aber wegen Satz 9.5 nicht möglich, da der Grad des Minimalpolynoms von c über $\mathbb{Q}$ gleich 3 ist, wie wir jetzt zeigen werden. Es ist

$$c^3 - 3c - 1 = 2(4\cos^3\beta - 3\cos\beta) - 1 = 2\cos\alpha - 1 = 0,$$

da $\cos 3x = 4\cos^3 x - 3\cos x$. Also ist c Nullstelle des Polynoms $X^3 - 3X - 1 \in \mathbb{Q}[X]$. Dieses ist irreduzibel über $\mathbb{Z}$, da es keine ganzzahlige Nullstelle hat. Also ist es nach Satz 6.3 auch irreduzibel über $\mathbb{Q}$. □

Verwandt mit dem zuletzt diskutierten Problem ist das Problem, zu vorgegebenem positiven ganzen $n \geq 3$ mit Zirkel und Lineal ein reguläres n-Eck zu konstruieren: Es handelt sich um die n-Teilung des speziellen Winkels von 360°. Offenbar ist eine solche möglich für $n = 2^m$, da jeder vorgegebene Winkel mit Zirkel und Lineal halbiert werden kann. Auch das reguläre 3-Eck ist konstruierbar, da dies – wie wir wissen – für das reguläre 6-Eck gilt. Etwas komplizierter ist der Fall $n = 5$: Hier hat man den Einheitskreis-Punkt $(\cos 72^\circ, \sin 72^\circ)$ aus $M = \{(0,0),(1,0)\}$ zu konstruieren. Mit Hilfe der Additionstheoreme zeigt man

$$0 = \sin 5\alpha = 16\sin^5\alpha - 20\sin^3\alpha + 5\sin\alpha$$

für $\alpha = 72^\circ$. $\sin 72^\circ$ ist also Nullstelle des Polynoms $16X^4 - 20X^2 + 5$. Die Nullstellen

$$\pm\frac{1}{2}\sqrt{\frac{5\pm\sqrt{5}}{2}}$$

dieses Polynoms sind nach Satz 9.1 aus M konstruierbar. Insbesondere ist $x = \sin 72^\circ$ aus M konstruierbar und damit auch $\cos 72^\circ = \sqrt{1-x^2}$.

Für $n = 7$ ist eine entsprechende Konstruktion jedoch nicht möglich, wie die folgende allgemeine Aussage zeigt. Wir benutzen darin einen neuen Begriff:

Definition. Eine Primzahl der Form $2^k + 1$ heißt *Fermatsche Primzahl*.

Es ist leicht zu sehen, daß $2^k + 1$ nur dann eine Primzahl sein kann, wenn $k = 0$ oder eine Potenz von 2 ist. Man setzt $F_m = 2^{2^m} + 1$. Dann sind $F_0, \ldots, F_4$ Primzahlen, eine weitere Fermatsche Primzahl ist aber noch nicht gefunden worden. Insbesondere ist nicht bekannt, ob es unendlich viele Fermatsche Primzahlen gibt.

Satz 9.6. *Die Primfaktorzerlegung der positiven ganzen Zahl n enthalte eine Primzahl $p \geq 3$, die keine Fermatsche Primzahl ist. Dann ist das reguläre n-Eck nicht mit Zirkel und Lineal konstruierbar.*

Beweis. Nehmen wir an, das reguläre n-Eck sei konstruierbar. Dann ist der Punkt $(\cos\alpha, \sin\alpha)$ mit $\alpha := 360^\circ/n$ aus $M = \{(0,0),(1,0)\}$ konstruierbar. Natürlich ist nun auch der Punkt $(\cos\beta, \sin\beta)$ mit $\beta := 360^\circ/p$ aus M konstruierbar. L sei der Zerfällungskörper (in $\mathbb{C}$) des Polynoms $X^p - 1$ über $\mathbb{Q}$. Die Potenzen von

$$\zeta_p = \cos\beta + i\sin\beta,$$

sind offenbar Nullstellen dieses Polynoms, und das sind die p verschiedenen komplexen Zahlen $\cos k\beta + i\sin k\beta$, $k = 1, \ldots, p$, die p-ten Einheitswurzeln. Es folgt $L = \mathbb{Q}(\zeta_p)$. Mit ζ_p ist auch die konjugiert-komplexe Zahl $\bar{\zeta}_p$ Nullstelle von $X^p - 1$. Folglich ist $2\cos\beta = \zeta_p + \bar{\zeta}_p \in L$ und $\tilde{L} = \mathbb{Q}(\cos\beta) \subset L$. Wegen $\tilde{L} \subset \mathbb{R}$ gilt $\zeta_p \notin \tilde{L}$. Andererseits ist ζ_p Nullstelle von

$$g = (X - \zeta_p)(X - \bar{\zeta}_p) = X^2 - 2\cos\beta \cdot X + 1 \in \tilde{L}[X].$$

Also ist g das Minimalpolynom von ζ_p über $\tilde{L}$ und $[L : \tilde{L}] = 2$. Da $X^p - 1 = (X-1)f$ mit $f = X^{p-1} + X^{p-2} + \cdots + 1$ und $\zeta_p \neq 1$, gilt $f(\zeta_p) = 0$. Nach Satz 6.6 ist f irreduzibel über $\mathbb{Q}$, also das Minimalpolynom von ζ_p über $\mathbb{Q}$. Folglich gilt $[L : \mathbb{Q}] = p - 1$ und $[\mathbb{Q}(\cos\beta) : \mathbb{Q}] = [\tilde{L} : \mathbb{Q}] = (p-1)/2$. Nach Voraussetzung ist $(p-1)/2$ aber keine Potenz von 2, im Widerspruch zu Satz 9.5. □

Wir haben die Konstruierbarkeit nur für Teilkörper von $\mathbb{R}$ formuliert. Wenn man sie stattdessen in $\mathbb{C}$ entwickelt, kann man natürlich direkt mit ζ_p argumentieren.

Für $n = 7, 11, 13$ ist beispielsweise das reguläre n-Eck nicht konstruierbar. Wie der Fall $n = 9$ zeigt, ist die Bedingung in Satz 9.6 zwar hinreichend, aber nicht

notwendig: In der Primfaktorzerlegung von 9 kommt nur die Fermatsche Primzahl 3 vor; dennoch ist das reguläre 9-Eck nicht konstruierbar. Andernfalls könnte man den Punkt $(\cos 40^\circ, \sin 40^\circ)$ aus $M = \{(0,0),(1,0)\}$ konstruieren und hieraus den Punkt $(\cos 20^\circ, \sin 20^\circ)$. Das ist aber – wie im Beweis von (c) gezeigt – nicht möglich.

Wir geben noch ohne Beweis den folgenden Satz von Gauß an, der ein notwendiges und hinreichendes Kriterium für die Konstruierbarkeit des regulären *n*-Ecks enthält.

Satz 9.7. *Genau dann ist das reguläre n-Eck mit Zirkel und Lineal konstruierbar, wenn* $n = 2^m p_1 \cdots p_r$ *gilt mit paarweise verschiedenen ungeraden Fermatschen Primzahlen* $p_1, \ldots, p_r$.

Einen Beweis dieses Satzes findet man in der Literatur. Die Konstruktion des regulären 17-Ecks war der erste mathematische Triumph von Gauß.

ABSCHNITT 10

Ordnung und Index

Sei G eine Gruppe mit multiplikativ geschriebener Verknüpfung. Wir erinnern daran, daß $|G|$ die Anzahl der Elemente von G bezeichnet und *Ordnung* von G genannt wird.

Nachdem wir in der Ringtheorie (und zuvor in [LA]) ausgiebig von Homomorphismen Gebrauch gemacht haben, setzen wir sie auch in der Gruppentheorie ein, um Informationen zwischen Gruppen zu transportieren. Zur Wiederholung fassen wir einige wichtige Aussagen über Gruppenhomomorphismen zusammen.

Satz 10.1. *Seien G und H Gruppen mit den neutralen Elementen e und e' und $f : G \to H$ ein Gruppenhomomorphismus. Dann gilt:*

(a) *Für jede Untergruppe U von G ist $f(U)$ eine Untergruppe von H.*
(b) *Für jede Untergruppe V von H ist $f^{-1}(V)$ eine Untergruppe von G.*
(c) *Speziell ist der Kern $K = f^{-1}(e')$ von f eine Untergruppe von G.*
(d) *Für $x, y \in G$ gilt*

$$f(x) = f(y) \iff xy^{-1} \in K \iff y^{-1}x \in K.$$

Ebenfalls ist die Ordnung eines Elementes schon betrachtet worden:

Definition. Falls $a^n \neq e$ für alle $n \in \mathbb{Z}$, $n > 0$, hat *a unendliche Ordnung*. Andernfalls ist

$$\min\{n > 0 : a^n = e\}$$

die *Ordnung* von a. Wir schreiben dafür $\operatorname{ord} a$.

Diese Definition der Ordnung eines Elementes hat nicht nur dem Namen nach mit der Ordnung einer Gruppe zu tun. In der Tat ist $\operatorname{ord} a$ die Ordnung der Untergruppe

$$\langle a \rangle = \{a^n : n \in \mathbb{Z}\}$$

von G, wie wir gleich sehen werden. Offensichtlich ist $\langle a \rangle$ die kleinste a enthaltende Untergruppe von G.

Satz 10.2. *Sei G eine Gruppe und $a \in G$ ein Element.*

(a) *Ist $\operatorname{ord} a = \infty$, so sind die Potenzen a^k, $k \in \mathbb{Z}$, paarweise verschieden.*
(b) *Ist $\operatorname{ord} a = m < \infty$, so ist $\operatorname{ord} a = |\langle a \rangle|$. Für $r, s \in \mathbb{Z}$ gilt $a^r = a^s$ genau dann, wenn $r \equiv s \mod m$.*

Beweis. Wegen der Potenzrechenregel $a^{u+v} = a^u a^v$ ist $f : (\mathbb{Z}, +) \to G$, $f(k) = a^k$, ein Homomorphismus. Nach Definition ist $\langle a \rangle = \text{Bild}\, f$. Sei $U = \text{Kern}\, f$. Wir wissen aus [LA], daß U eine Untergruppe von $\mathbb{Z}$ ist und daher ein $n \in \mathbb{Z}$, $n \geq 0$, existiert mit $U = \mathbb{Z}n$.

Im Fall (a) muß $n = 0$ gelten, denn $a^k \neq e$ für alle $k \geq 1$. Folglich ist f injektiv, und die Potenzen a^k sind paarweise verschieden.

Im Fall (b) ist n die Ordnung von a gemäß deren Definition. Der Homomorphismus f ist surjektiv, und für $r, s \in \mathbb{Z}$ gilt $f(r) = f(s)$ genau dann, wenn $r - s \in U$. Dies ist genau dann der Fall, wenn $r \equiv s \mod n$. Insbesondere hat $\langle a \rangle$ genau so viele Elemente, wie es Restklassen modulo n gibt, nämlich n. □

Die Anwendung des Homomorphismus f „verbirgt“ in diesem Beweis die direkte Anwendung der Potenzrechenregeln und die Division mit Rest. Wir wollen zum Vergleich (b) direkt damit beweisen. Sei zunächst $r \equiv s \mod m$. Dann gilt $r = s + mk$ mit einem $k \in \mathbb{Z}$. Es folgt

$$a^r = a^{s+mk} = a^s a^{mk} = a^s (a^m)^k = a^s e^k = a^s.$$

Sei umgekehrt $a^r = a^s$. Dann ist $a^{r-s} = e$, und wir haben zu zeigen, daß $a^t = e$ nur dann gilt, wenn $t = mk$ mit einem $k \in \mathbb{Z}$ ist. Wir schreiben $t = mk + w$, wobei $0 \leq w < m$. Dann folgt $a^w = e$, und nach Definition der Ordnung von a muß $w = 0$ sein.

Es lohnt sich für das Folgende, daß wir die Erkenntnis aus dem Beweis von Satz 10.2 noch einmal abstrakt formulieren:

Satz 10.3. *Sei G eine Gruppe, $a \in G$ ein Element und $f : \mathbb{Z} \to G$, $f(k) = a^k$, die „Exponentialabbildung“.*

(a) *Ist* $\text{ord}\, a = \infty$, *so ist $f : \mathbb{Z} \to \langle a \rangle$ ein Isomorphismus.*

(b) *Ist* $\text{ord}\, a = m < \infty$, *so induziert f einen Isomorphismus $\overline{f} : (\mathbb{Z}_m, +) \to \langle a \rangle$.*

Wir wollen nun eine Beziehung herstellen zwischen der Ordnung einer endlichen Gruppe G und den Ordnungen der Elemente $a \in G$, allgemeiner: den Ordnungen der Untergruppen von G.

Sei G eine Gruppe und H eine Untergruppe. Für $a \in G$ setzen wir

$$Ha = \{ba : b \in H\}$$

und nennen Ha eine *Rechtsklasse* von H mit *Repräsentanten* a. Analog kann man die *Linksklasse* aH von H definieren.

Dieser Begriff verallgemeinert den Begriff der Restklasse von Idealen: Für ein Ideal I eines Ringes R ist die Linksklasse $a + I$ (in der Gruppe $(R, +)$) gerade die Restklasse von a bezüglich I. In diesem Fall, und allgemeiner in abelschen Gruppen, stimmen Links- und Rechtsklassen überein, denn es ist dann $aH = Ha$. In beliebigen Gruppen gilt diese Gleichung aber nicht, wie wir an einem sehr einfachen Beispiel noch sehen werden.

Satz 10.4. *Sei G eine Gruppe, H eine Untergruppe von G.*

(a) *Für $a,b \in G$ gilt: $Ha \neq Hb \Rightarrow Ha \cap Hb = \emptyset$.*

(b) *Für jedes $a \in G$ ist die Abbildung $\mu_a : H \to Ha$, $\mu_a(h) = ha$, bijektiv.*

Beweis. (a) Seien $a,b \in G$ mit $Ha \cap Hb \neq \emptyset$. Wir müssen zeigen: $Ha = Hb$. Dazu wählen wir $c \in Ha \cap Hb$.

Es existiert ein $h \in H$ mit $c = ha$. Für alle $h' \in H$ gilt also $h'c = h'ha = (h'h)a \in Ha$, folglich $Hc \subset Ha$. Und für $d \in Ha$, $d = h''a$, hat man

$$d = h''a = h''h^{-1}ha = (h''h^{-1})(ha) = h'''c \in Hc,$$

weil $h''' = h''h^{-1} \in H$. Insgesamt zeigt dies: $Ha = Hc$. Genauso folgt $Hb = Hc$.

(b) Nach Definition von Ha ist μ_a surjektiv. Die Injektivität folgt aus der Kürzungsregel. □

Als Folgerung aus 10.4 erhalten wir den *Satz von Lagrange*, der die gesuchte Beziehung zwischen der Ordnung einer Gruppe und den Ordnungen ihrer Untergruppen herstellt. In ihm verwenden wir die Bezeichnung

$$[G : H]$$

für die Anzahl der Rechtsklassen von G bezüglich der Untergruppe H. Man nennt $[G : H]$ den *Index* von H in G.

Satz 10.5. *Sei G eine endliche Gruppe und H eine Untergruppe. Dann ist*

$$|G| = |H| \cdot [G : H].$$

Beweis. Seien $R_1, \ldots, R_m$, $m = [G : H]$, die verschiedenen Rechtsklassen von G bezüglich H. Jedes $g \in G$ gehört zu einer Rechtsklasse, nämlich zu Hg. Also ist

$$G = \bigcup_{i=1}^{m} R_i.$$

Nach 10.4 (a) sind $R_1, \ldots, R_m$ paarweise disjunkt, und nach 10.4 (b) gilt $|R_i| = |H|$ für alle i. Also ist

$$|G| = m \cdot |H|.$$ □

Die Gleichung im Satz von Lagrange zeigt, daß wir den Index auch mittels der Linksnebenklassen hätten definieren können.

Als Folgerung aus Satz 10.5 erhalten wir den sogenannten *Kleinen Fermatschen Satz:*

Satz 10.6. *Sei G eine endliche Gruppe und $a \in G$. Dann gilt:* ord a *teilt* $|G|$, *und*

$$a^{|G|} = e.$$

Beweis. Anwendung von 10.5 auf die Untergruppe $\langle a \rangle$ ergibt die erste Behauptung. Daß dann $a^{|G|} = e$ ist, haben wir beim Beweis von 10.2 schon gesehen. □

Für abelsche Gruppen haben wir diesen Satz schon auf anderem Wege bewiesen (siehe Satz 8.3).

Ein einfaches Beispiel für die Anwendung der vorangegangenen Sätze ist die Bestimmung der Untergruppen der Gruppe S_3. Diese hat 6 Elemente, nämlich

$$\mathrm{id} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \quad \zeta_1 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \quad \zeta_2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix},$$
$$\sigma_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \quad \sigma_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \quad \sigma_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}.$$

Man sieht sofort:

$$\langle \zeta_i \rangle = \{\mathrm{id}, \zeta_1, \zeta_2\}, \qquad i = 1,2,$$
$$\langle \sigma_i \rangle = \{\mathrm{id}, \sigma_i\}, \qquad i = 1,2,3.$$

Sei nun U eine Untergruppe, $U \neq G, \{\mathrm{id}\}$. Dann gilt $|U| = 2$ oder $|U| = 3$ nach Satz 10.5. Im Fall $|U| = 2$ enthält U ein Element der Ordnung 2 und damit ist $U = \langle \sigma_i \rangle$ für ein i. Im Fall $|U| = 3$ enthält U ein Element der Ordnung 3, also ist $U = \{\mathrm{id}, \zeta_1, \zeta_2\}$.

Es gilt $\zeta_i U \neq U \zeta_i$ für jede Untergruppe U der Ordnung 2 von S_3. Dies zeigt, daß im allgemeinen Links- und Rechtsklassen einer Untergruppe nicht übereinstimmen.

Ein wesentliches Ziel der Gruppentheorie ist es, aus der Ordnung einer endlichen Gruppe möglichst viel über ihre Struktur zu schließen. Sehr einfach ist dies für Gruppen von Primzahlordnung.

Satz 10.7. *Die Ordnung der Gruppe G sei eine Primzahl p. Dann gilt $G = \langle a \rangle$ für jedes $a \in G$, $a \neq e$. Speziell ist G zu $(\mathbb{Z}_p, +)$ isomorph.*

Beweis. Da $|\langle a \rangle| > 1$ und p der einzige Teiler > 1 von p ist, gilt $|\langle a \rangle| = p$. Daß G zu $(\mathbb{Z}_p, +)$ isomorph ist, haben wir schon in Satz 10.3 festgestellt. □

Die Gruppen von Primzahlordnung gehören damit zu den zyklischen Gruppen:

Definition. Eine Gruppe G heißt *zyklisch*, wenn es ein $a \in G$ mit $\langle a \rangle = G$ gibt.

Satz 10.3 beschreibt die zyklischen Gruppen bis auf Isomorphie. Man sollte aber für die endlichen zyklischen Gruppen noch mindestens drei weitere „Modelle“ vor Augen haben:

Beispiele. (a) Die zyklischen Permutationen

$$\zeta_k = \begin{pmatrix} 1 & 2 & \dots & k & k+1 & k+2 & \dots & n \\ n-k+1 & n-k+2 & \dots & n & 1 & 2 & \dots & n-k \end{pmatrix} \in S_n$$

bilden eine zyklische Gruppe der Ordnung n, die von ζ_1 erzeugt wird und die Ordnung n hat. Es gilt $\zeta_k = \zeta_1^k$.

(b) Die Drehungen ρ_k des $\mathbb{R}^2$ mit Drehzentrum 0 und Drehwinkel $\alpha_k = 2\pi k/n$ bilden eine Untergruppe der Isometrien der Ebene, die von ρ_1 erzeugt wird. Einen

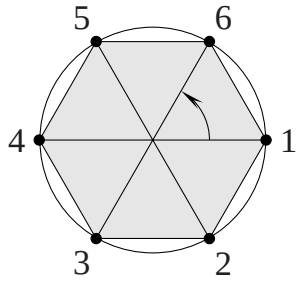


ABBILDUNG 1

Isomorphismus dieser Gruppe zu der in (a) genannten Gruppe von Permutationen erhalten wir, wenn wir die von den Drehungen bewirkten Permutationen der im Uhrzeigersinn numerierten Ecken eines regelmäßigen n-Ecks mit Zentrum 0 betrachten. Abbildung 1 veranschaulicht die Situation für $n = 6$.

(c) Die Menge $\{z \in \mathbb{C} : z^n = 1\}$ der n-ten Einheitswurzeln ist eine Untergruppe von $\mathbb{C}^*$, die von $\zeta = \cos(2\pi/n) + i\sin(2\pi/n)$ erzeugt wird. Wir erhalten einen Isomorphismus zu der in (b) betrachteten Gruppe von Drehungen, wenn wir jeder Einheitswurzel ζ^k die durch Multiplikation mit ζ^k bewirkte Drehung der Ebene zuordnen.

Satz 10.8. *Sei $G = \langle a \rangle$ eine zyklische Gruppe. Dann gilt:*

(a) *Im Fall $|G| = \infty$ ist jede Untergruppe von der Form $\langle a^m \rangle$, $m \geq 0$, und diese Untergruppen sind paarweise verschieden.*

(b) *Im Fall $|G| = n < \infty$ gibt es zu jedem Teiler d von n genau eine Untergruppe U der Ordnung d. Sie wird von $a^{n/d}$ erzeugt.*

Beweis. (a) Die Abbildung $f : \mathbb{Z} \to G$, $f(k) = a^k$, ist ein Isomorphismus von Gruppen (Satz 10.3). Daher ist $U \subset \mathbb{Z}$ genau dann eine Untergruppe von $\mathbb{Z}$, wenn $f(U)$ eine Untergruppe von G ist. Die Untergruppen von $\mathbb{Z}$ sind aber genau die Teilmengen $\mathbb{Z}m$, $m \in \mathbb{Z}$, $m \geq 0$. Es ist $f(\mathbb{Z}m) = \langle a^m \rangle$.

(b) Das Element $a^{n/d}$ hat Ordnung d, denn $(a^{n/d})^k \neq e$ für $0 < k < d$ und $(a^{n/d})^d = e$. Also erzeugt $a^{n/d}$ eine Untergruppe der Ordnung d.

Umgekehrt sei U eine Untergruppe der Ordnung d. Wir betrachten den Homomorphismus f wie in (a). Dieser hat aber den Kern $\mathbb{Z}n$, und $f^{-1}(U)$ ist eine Untergruppe von $\mathbb{Z}$, die $\mathbb{Z}n$ umfaßt. Es gilt $U = \mathbb{Z}m$ für genau ein $m \geq 0$, und m ist ein Teiler von n, weil $n \in \mathbb{Z}m$. Mithin gibt es höchstens so viele Untergruppen von G, wie n Teiler hat.

Da es zu jedem Teiler d von n aber auch mindestens eine Untergruppe der Ordnung d gibt, existiert zu jedem Teiler d genau eine Untergruppe mit d Elementen. □

Es gilt auch die Umkehrung von Satz 10.8 (b), die wir aber nur für abelsche Gruppen beweisen.

Satz 10.9. *Sei G eine endliche abelsche Gruppe.*

(a) *Für Elemente $x,y \in G$ teilerfremder Ordnungen m und n ist* $\operatorname{ord}(xy) = mn$.
(b) *Sei $E = \max\{\operatorname{ord}(x) : x \in G\}$. Dann gilt* $\operatorname{ord}(x) \mid E$ *für alle $x \in G$.*
(c) *Wenn es zu jedem Teiler d von $|G|$ höchstens eine Untergruppe U der Ordnung d in G gibt, ist G zyklisch.*

Beweis. (a) Sei $(xy)^k = e$ mit $k > 0$. Dann gilt $x^k = y^{-k}$, weil die Elemente x und y vertauschbar sind. Also ist $z = x^k \in \langle x\rangle \cap \langle y\rangle$. Speziell gilt $\operatorname{ord}(z) \mid m$ und $\operatorname{ord}(z) \mid n$. Da m und n aber teilerfremd sind, muß $\operatorname{ord}(z) = 1$ sein; mithin ist $z = e$. Dies impliziert $m \mid k$ und $n \mid k$. Wir nutzen die Teilerfremdheit noch einmal aus und erhalten $mn \mid k$.

Andererseits ist $(xy)^{mn} = (x^m)^n (y^n)^m = e$, so daß insgesamt $\operatorname{ord}(xy) = mn$ ist.

(b) Wir wählen ein Element $y \in G$ mit $\operatorname{ord} y = E$. Für $x \in G$ sei dann $k = \operatorname{ggT}(E, \operatorname{ord} x)$, $q = \operatorname{ord}(x)/k$ und $z = x^k$. Dann gilt, wie wir oben gesehen haben, $\operatorname{ord}(z) = q$. Da q und E teilerfremd sind, hat yz nach Teil (a) die Ordnung qE. Nach Voraussetzung ist $qE \leq E$, was aber nur bei $q = 1$ möglich ist. Es folgt $k = \operatorname{ord}(x) \mid E$.

(c) Wir wählen wieder $y \in G$ mit $\operatorname{ord} y = E$. Sei $x \in G$. Dann erzeugt x eine Untergruppe der Ordnung $m = \operatorname{ord} x$. Nach (b) ist m ein Teiler von E, und $\langle y\rangle$ enthält nach Satz 10.8 eine Untergruppe U der Ordnung m. Nach Voraussetzung ist $U = \langle x\rangle$. Dies zeigt $x \in \langle y\rangle$. Mithin ist G zyklisch und erzeugt von y. □

Man nennt die Zahl E den *Exponenten* von G (daher die Wahl des Buchstabens). Bereits die Gruppe S_3 zeigt, daß die Teile (a) und (b) für nicht abelsche Gruppen nicht ohne weiteres gelten; bei (a) genügt es aber vorauszusetzen, daß x und y vertauschbar sind. Teil (c) gilt allgemein, muß dann aber anders (und etwas unangenehmer) bewiesen werden.

Die wichtigste Folgerung aus Satz 10.9 ist

Satz 10.10. *Sei K ein Körper. Dann ist jede endliche Untergruppe G von K^* zyklisch. Insbesondere sind die Einheitengruppen endlicher Körper zyklisch.*

Beweis. Sei U eine Untergruppe von K^*, $|U| = m$. Dann ist $x^m = 1$ für alle $x \in U$. Also besteht U genau aus den Nullstellen des Polynoms $X^m - 1$, denn einerseits ist jedes der m Elemente von U eine solche Nullstelle, und andererseits gibt es höchstens m Nullstellen. Dies zeigt, daß G zu jedem Teiler m von $|G|$ höchstens eine Untergruppe der Ordnung m besitzt. Nach Satz 10.9 ist G zyklisch. □

Man nennt jedes erzeugende Element der Einheitengruppe eines endlichen Körpers K eine *Primitivwurzel* von K.

Für einen endlichen Körper K der Charakteristik p und eine Primitivwurzel x von K ist offensichtlich $K = \mathbb{Z}_p(x)$. Daraus folgt, daß es zu jedem $n \in \mathbb{N}$, $n \geq 1$, ein irreduzibles Polynom des Grades n über $\mathbb{Z}_p$ gibt.

ABSCHNITT 11

Operation von Gruppen

Sei G eine Gruppe und X eine Menge.

Definition. Eine *Operation* von G auf X ist eine Abbildung $G \times X \to X$, $(g,x) \mapsto gx$, die folgende Regeln erfüllt:

$$ex = x \quad \text{und} \quad g(hx) = (gh)x$$

für alle $g,h \in G$, $x \in X$.

Das Standardbeispiel dafür ist die Operation der symmetrischen Gruppe $S(X)$ auf X. (Zur Erinnerung: $S(X)$ ist die Gruppe aller Permutationen von X, also aller bijektiven Abbildungen $X \to X$.) Dieses Beispiel enthält in gewisser Weise auch alle anderen. Sei dazu eine Operation einer Gruppe G auf einer Menge X gegeben. Die Abbildung

$$\mu_g : X \to X, \quad \mu_g(x) = gx,$$

ist ja bijektiv, denn sie hat $\mu_{g^{-1}}$ als Umkehrabbildung:

$$\mu_{g^{-1}}(\mu_g(x)) = g^{-1}(gx) = (g^{-1}g)x = ex = x$$

für alle $x \in X$. Ebenso ist $\mu_g(\mu_{g^{-1}}(x)) = x$. Also gilt $\mu_g \in S(X)$ für alle $g \in G$, und die zweite Regel in der Definition können wir nun so interpretieren:

$$\mu_g \mu_h = \mu_{gh}.$$

Dies ist gerade die Homomorphiebedingung für die Abbildung $\varphi : G \to S(X)$, $\varphi(g) = \mu_g$. Die Operation von G ist also im wesentlichen eine Operation der Untergruppe $\varphi(G) \subset S(X)$ auf X.

Wir können uns vorstellen, daß die Gruppe G die Elemente von X bewegt. Dementsprechend sind die folgenden Begriffe gewählt:

Definition. Die Gruppe G operiere auf der Menge X. Dann heißt

$$Gx = \{gx : g \in G\} \subset X$$

die *Bahn* von x unter G. Die Untergruppe

$$G_x = \{g \in G : gx = x\} \subset G$$

heißt die *Standgruppe* von x.

Wie schon bei Links- bzw. Rechtsklassen, oder durch Einführung einer geeigneten Äquivalenzrelation auf X, zeigt man: Zwei Bahnen Gx und Gy sind entweder gleich oder disjunkt. D.h. die Menge X wird durch die Operation von G in Teilmengen (nämlich die Bahnen) zerlegt.

Bahn und Standgruppe eines Elementes $x \in X$ stehen in einer engen Beziehung:

Satz 11.1. *Sei $x \in X$. Die Abbildung $G \to Gx$, $g \mapsto gx$, induziert eine Bijektion zwischen der Menge der Linksklassen von G_x und der Bahn Gx:*

$$gx = hx \iff g \in hG_x.$$

Dies ist trivial, und wir können es auch so ausdrücken: g und h haben genau dann die gleiche Wirkung auf x, wenn die Linksklassen gG_x und hG_x übereinstimmen. Eine unmittelbare Folgerung:

Satz 11.2. *Die Gruppe G operiere auf der Menge X.*

(a) *Für alle $x \in X$ ist $|Gx| = [G : G_x]$.*

(b) *X sei endlich und zerfalle in die disjunkten Bahnen $Gx_1, \ldots, Gx_m$. Dann gilt:*

$$|X| = \sum_{i=1}^{m} [G : G_{x_i}].$$

Dieser Satz enthält ein sehr wirksames kombinatorisches Prinzip, also eine Methode zum Zählen der Elemente von X. Das erste Beispiel, das wir schon kennengelernt haben, ist der Satz von Lagrange: Die Rolle von X wird jetzt von der Gruppe G selbst gespielt, und eine Untergruppe H übernimmt die von G. Die Operation $H \times G \to G$ ist einfach die Multiplikation $(h,g) \mapsto hg$. In diesem Fall sind die Bahnen die Rechtsklassen Hg, und alle Standgruppen sind trivial, denn $hg = g \iff h = e$. Aus Teil (b) von Satz 11.2 ergibt sich unmittelbar $|G| = m|H|$, wobei m die Anzahl der Bahnen, also der Rechtsklassen von H ist.

Die zweite wichtige Operation innerhalb der Gruppentheorie ist die Konjugation:

Satz 11.3. *Sei G eine Gruppe.*

(a) *Für jedes $g \in G$ ist die Abbildung*

$$\kappa_g : G \to G, \quad \kappa_g(h) = ghg^{-1},$$

ein Automorphismus von G.

(b) *Die Zuordnung $g \mapsto \kappa_g$ ist ein Homomorphismus von G in $\mathrm{Aut}(G)$, insbesondere definiert $(g,h) \mapsto ghg^{-1}$ eine Operation von G auf G.*

Beweis. (a) Es gilt

$$\kappa_{g^{-1}}(\kappa_g(x)) = g^{-1}gxg^{-1}g = x$$

für alle $x \in G$, und genauso gilt $\kappa_g(\kappa_{g^{-1}}(x)) = x$. Also ist κ_g bijektiv. Wegen

$$\kappa_g(xy) = g(xy)g^{-1} = gxg^{-1}gyg^{-1} = \kappa_g(x)\kappa_g(y)$$

für $x,y \in G$ ist κ_g ein Automorphismus.

(b) Nachzuweisen ist die Gleichung

$$\kappa_{gh} = \kappa_g \kappa_h.$$

Für alle $x \in G$ ist aber

$$\kappa_{gh}(x) = (gh)x(gh)^{-1} = g(hxh^{-1})g^{-1} = \kappa_g(\kappa_h(x)). \qquad \square$$

Definition. Die Abbildung κ_g heißt *Konjugation* mit g. Zwei Elemente $x,y \in G$ heißen *konjugiert*, falls es eine Konjugationsabbildung κ_g gibt mit $\kappa_g(x) = y$, d.h. falls es ein $g \in G$ gibt mit $gxg^{-1} = y$. Dementsprechend heißen zwei Untergruppen $U,V \subset G$ *konjugiert*, falls es ein $g \in G$ gibt mit $gUg^{-1} = V$, d.h. mit $gU = Vg$.

Die Bahn eines Elementes $x \in G$ unter der Konjugationsoperation heißt die *Konjugationsklasse* von x und wird mit $C(x)$ bezeichnet:

$$C(x) = \{gxg^{-1} : g \in G\}.$$

Sie besteht genau aus den zu x konjugierten Elementen von G. Das *Zentrum* einer Gruppe G schließlich ist

$$Z(G) = \{g \in G : gh = hg \text{ für alle } h \in G\}.$$

Für abelsche Gruppen hat die Konjugation natürlich keine Bedeutung, denn dann ist $ghg^{-1} = h$ für alle $g,h \in G$. Für die Untersuchung von Gruppen im allgemeinen ist sie aber ein wichtiges Hilfsmittel.

Wir können das Zentrum auf folgende Weisen beschreiben: (i) Es besteht aus allen Elementen, deren Standgruppe unter der Konjugation ganz G ist. (ii) Es ist der Kern des Homomorphismus $G \to \operatorname{Aut} G : g \mapsto \kappa_g$. Die Beschreibung (ii) zeigt, daß das Zentrum eine Untergruppe ist, was man natürlich auch sehr leicht direkt begründet. Die Beschreibung (i) ergibt durch Kombination von Satz 11.2 und Satz 11.3 die *Klassengleichung:*

Satz 11.4. *Sei G eine endliche Gruppe und seien $C_1,\dots,C_m$ die verschiedenen Konjugationsklassen von G, die mindestens 2 Elemente enthalten. Dann gilt*

$$|G| = |Z(G)| + |C_1| + \cdots + |C_m|,$$

wobei $|C_i|$ für $i = 1,\dots,m$ der Index einer Untergruppe von G und insbesondere jeder der Summanden ein Teiler von $|G|$ ist.

Beweis. Offensichtlich ist $Z(G)$ die Vereinigung der einelementigen Bahnen unter der Konjugation. $\square$

Besonders wirkungsvoll ist die Klassengleichung dann, wenn $|G|$ nur wenige Teiler hat, zum Beispiel eine Primzahlpotenz ist.

Satz 11.5. *Sei p eine Primzahl und G eine Gruppe der Ordnung p^n, $n \geq 1$. Dann ist $|Z(G)| > 1$. Speziell ist eine Gruppe der Ordnung p^2 stets abelsch.*

Beweis. In der Klassengleichung

$$|G| = |Z(G)| + |C_1| + \cdots + |C_m|$$

sind die linke Seite und die Summanden $|C_i|$ durch p teilbar. Also gilt dies auch für $|Z(G)|$, was $|Z(G)| = 1$ ausschließt.

Sei nun $|G| = p^2$. Wir haben die Annahme $|Z(G)| = p$ zum Widerspruch zu führen. (Denn dann folgt $|Z(G)| = p^2$, also $Z(G) = G$.) Sei $a \in G$, $a \notin Z(G)$. Die von $Z(G)$ und a erzeugte Untergruppe U muß dann ganz G sein, denn ihr Index ist einerseits ein Teiler von p^2, andererseits kleiner als der Index p von $Z(G)$. Also besitzt jedes Element von G eine Darstellung za^j mit $z \in Z(G)$ und $j \in \mathbb{Z}$. Zwei Elemente za^j, $z'a^k$ kommutieren aber miteinander. Es folgt, daß G abelsch ist, im Widerspruch zur Annahme $|Z(G)| = p$. □

Wir wollen uns nun noch einmal mit den Permutationen von $\{1,\ldots,n\}$ befassen und eine neue, wichtige Darstellung für sie gewinnen. Wir erinnern an einige aus [LA] bekannte Aussagen:

(a) Die Gruppe $S_n = S(\{1,\ldots,n\})$ hat die Ordnung $n!$.
(b) Jede Permutation ist Produkt von Transpositionen τ_{ij}, $i < j$, (mit $\tau_{ij}(i) = j$, $\tau_{ij}(j) = i$, $\tau_{ij}(k) = k$ für $k \neq i, j$).
(c) Es gibt einen Homomorphismus $\operatorname{sign} : S_n \to \{\pm 1\}$ mit $\operatorname{sign}(\tau_{ij}) = -1$ für alle Transpositionen τ_{ij}. Man nennt $\operatorname{sign}(\pi)$ das *Signum* von π.
(d) Die Untergruppe $A_n = \operatorname{Kern} \operatorname{sign}$ der *geraden* Permutationen hat $n!/2$ Elemente und heißt die *alternierende Gruppe*.

Wir lassen im folgenden das Zeichen $\circ$ bei der Komposition von Permutationen aus.

Jeder Permutation π ordnen wir ihren *Wirkungsbereich*

$$W(\pi) = \{x : \pi(x) \neq x\}$$

zu. Der Wirkungsbereich besteht also aus allen Nichtfixpunkten von π. Offensichtlich gilt:

$$W(\pi) \cap W(\rho) = \emptyset \implies \pi\rho = \rho\pi.$$

Man sagt, daß π und ρ *disjunkt* sind, wenn $W(\pi) \cap W(\rho) = \emptyset$. Unter der *Bahn* von x unter π verstehen wir die Bahn von x unter der von π erzeugten Untergruppe von S_n, also die Menge

$$B(\pi, x) = \{\pi^j(x) : j \in \mathbb{Z}\}.$$

Wir verfolgen einmal eine Bahn

$$x, \pi(x), \ldots, \pi^{m-1}(x), \pi^m(x)$$

so weit, bis sich beim Exponenten m zum ersten Mal ein Element wiederholt. Dann ist $\pi^m(x) = x$, denn aus $\pi^m(x) = \pi^k(x)$ folgt $\pi^{m-k}(x) = x$. Ferner folgt

$$\pi^j(x) = \pi^r(x) \quad \text{für } r \equiv j \mod m,$$

so daß $B(\pi, x) = \{x, \pi(x), \ldots, \pi^{m-1}(x)\}$. Anschaulich können wir die Wirkung von π auf x so darstellen:

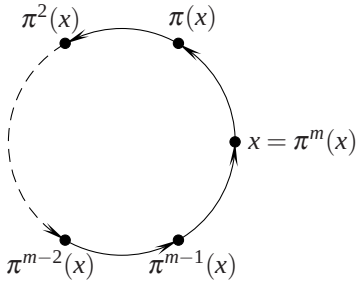


ABBILDUNG 1

Man nennt $\zeta \in S_n$ einen *Zykel* der *Länge m*, wenn $W(\zeta)$ aus genau einer Bahn mit m Elementen besteht oder $\zeta = \mathrm{id}$ ist. (Der Identität ordnen wir die Länge 1 zu.) Man schreibt in diesem Fall

$$\zeta = (x_1 \ \ldots \ x_m),$$

wobei $x_1 \in W(\zeta)$, $x_2 = \zeta(x_1)$, …, $x_m = \zeta(x_{m-1})$, $\zeta(x_m) = x_1$. Zum Beispiel ist

$$\zeta = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 2 & 1 & 3 \end{pmatrix} \in S_4$$

der Zykel $\zeta = (1\ 4\ 3)$ der Länge 3.

Für das Rechnen mit Permutationen ist der folgende Satz von grundlegender Bedeutung:

Satz 11.6. *Jede Permutation $\pi \in S_n$ ist Produkt paarweise disjunkter Zykel. Bis auf die Reihenfolge und Zykel der Länge* 1 *sind diese eindeutig bestimmt.*

Beweis. Wir zerlegen die Menge $\{1, \ldots, n\}$ in ihre Bahnen $B(\pi, x)$. Diese seien $B_1, \ldots, B_q$. Für $j = 1, \ldots, q$ definieren wir eine Permutation $\zeta_j \in S_n$: Wir setzen $\zeta_j(x) = \pi(x)$ für $x \in B_j$ und $\zeta_j(x) = x$ für $x \notin B_j$. Hierdurch wird wirklich eine Permutation ζ_j definiert, weil $\pi(B_j) = B_j$. Ferner ist ζ_j ein Zykel, weil $B_j = B(\zeta_j, x) = W(\zeta_j)$ für jedes $x \in B_j$ ist. Es gilt $\pi = \zeta_1 \cdots \zeta_q$.

Die Eindeutigkeit der Zerlegung folgt einfach daraus, daß jede Bahn von π mit einer Bahn $B(\zeta_j, x)$ übereinstimmt, wenn die Wirkungsbereiche der Zykel ζ_j in einer Produktdarstellung $\pi = \zeta_1 \cdots \zeta_q$ von π disjunkt sind. □

Wir sehen uns ein kleines Beispiel an: Die Permutation

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 4 & 7 & 5 & 2 & 3 & 6 & 1 \end{pmatrix} \in S_7$$

hat die disjunkte Zykelzerlegung $\pi = (1\,4\,2\,7)(3\,5)(6)$. Hat man einmal die Zerlegung einer Permutation in disjunkte Zykel bestimmt, so kann man leicht ihre Ordnung, ihr Inverses und viele andere Daten bestimmen: In unserem Beispiel ist $\pi = \zeta_1\zeta_2$ mit $\zeta_1 = (1\,4\,2\,7)$ und $\zeta_2 = (3\,5)$, also ist $\operatorname{ord}\pi = \operatorname{ord}\zeta_1 = 4$ und $\pi^{-1} = \zeta_1^{-1}\zeta_2^{-1} = (1\,7\,2\,4)(3\,5)$.

Auch die Konjugationsklasse läßt sich aus der disjunkten Zykelzerlegung leicht ablesen. Sei

$$\zeta = (x_1\ \dots\ x_m)$$

ein Zykel der Länge m. Für jedes $\rho \in S_n$ ist dann

$$\rho\zeta\rho^{-1} = (\rho(x_1)\ \dots\ \rho(x_m))$$

wieder ein Zykel gleicher Länge: Es gilt ja

$$\rho\zeta\rho^{-1}(\rho(x_i)) = \rho(\zeta(x_i)) = \rho(x_{i+1}),$$

wobei der Index i modulo m zu lesen ist, und für $x \notin \rho(\{x_1,\dots,x_m\})$ ist $\rho\zeta\rho^{-1}(x) = x$. Ist also $\pi = \zeta_1\cdots\zeta_q$, so ist $\rho\pi\rho^{-1} = \zeta_1'\cdots\zeta_q'$ Produkt disjunkter Zykel $\zeta_j' = \rho\zeta_j\rho^{-1}$, wobei ζ_j und ζ_j', $j = 1,\dots,q$, die gleiche Länge haben.

Sei $\pi \in S_n$. Wir schreiben $\{1,\dots,n\}$ als disjunkte Vereinigung von π-Bahnen $B_1,\dots,B_q$, wobei wir $|B_1| \geq |B_2| \geq \cdots \geq |B_q|$ annehmen. Dann heißt das q-Tupel $(|B_1|,\dots,|B_q|) \in \mathbb{N}^q$ der *Zerlegungstyp* von π. Das oben angegebene Beispiel aus S_7 hat dann den Zerlegungstyp $(4,2,1)$, und $\mathrm{id} \in S_n$ hat den Zerlegungstyp $(1,\dots,1) \in \mathbb{N}^n$. Wie wir oben gesehen haben, besitzt eine Permutation π des Zerlegungstyps $(b_1,\dots,b_q)$ eine disjunkte Zykeldarstellung $\pi = \zeta_1\cdots\zeta_q$, wobei ζ_i die Länge b_i hat, $i = 1,\dots,q$.

Satz 11.7. *Zwei Permutationen $\pi,\pi' \in S_n$ sind genau dann konjugiert, wenn sie den gleichen Zerlegungstyp besitzen.*

Beweis. Die Implikation „$\Longrightarrow$“ haben wir schon bewiesen. Für die Implikation „$\Longleftarrow$“ betrachten wir Permutationen π und π' mit gleichem Zerlegungstyp $(b_1,\dots,b_q)$, $\pi = \zeta_1\cdots\zeta_q$ und $\pi' = \zeta_1'\cdots\zeta_q'$, wobei die Zykel ζ_i und ζ_i' beide die Länge b_i haben (für $i = 1,\dots,q$). Sei $\zeta_i = (x_{i1}\ \dots\ x_{ib_i})$, $\zeta_i' = (x_{i1}'\ \dots\ x_{ib_i}')$.

Nun definiert man $\rho \in S_n$ mittels $\rho(x_{ij}) = x_{ij}'$, $i = 1,\dots,q$, $j = 1,\dots,b_i$. Diese Definition erfaßt alle Elemente von $\{1,\dots,n\}$, weil dies die Vereinigung der Bahnen von π ist; sie ist widerspruchsfrei, weil die Zykel ζ_i paarweise disjunkt sind; und sie ist bijektiv, weil $\{1,\dots,n\}$ disjunkte Vereinigung der Bahnen von π' ist. Wie wir oben bereits gesehen haben, ist $\rho\pi\rho^{-1} = \pi'$. □

Hieran kann man zahlreiche kombinatorische Überlegungen anschließen, die wir in den Übungsaufgaben weiter verfolgen.

ABSCHNITT 12

Normalteiler und Faktorgruppen

Wir haben für einen Ring R und ein Ideal I den Restklassenring R/I konstruiert. Seine Elemente sind die Restklassen $x+I$, $x \in R$. Für die Struktur der Gruppe $(R/I,+)$ spielt die Multiplikation auf R gar keine Rolle. Wir können also versuchen, die gleiche Konstruktion für eine Gruppe G und eine Untergruppe H auszuführen. Ohne weiteres geht das aber nicht, und bei genauem Nachprüfen stellt man fest, daß beim Beweis der Wohldefiniertheit der Addition auf R/I die Gleichung

$$x+I = I+x$$

für alle $x \in R$ benötigt wird. Da $(R,+)$ kommutativ ist, ist sie trivialerweise erfüllt. Für eine beliebige Untergruppe H einer Gruppe G und $x \in G$ ist im allgemeinen aber $xH \neq Hx$, wie wir an einem Beispiel gesehen haben, so daß die Konstruktion von G/H nur für spezielle Untergruppen H möglich sein kann. Die natürliche Abbildung $\pi : G \to G/H$ soll ja auch ein Gruppenhomomorphismus mit Kern H werden, und dies erzwingt ebenfalls die Gleichung $xH = Hx$ für alle $x \in G$:

Satz 12.1. *Seien G, G' Gruppen, $\varphi : G \to G'$ sei ein Homomorphismus und $H =$ Kern φ. Dann gilt für alle $a \in G$:*

$$aH = \varphi^{-1}(\varphi(a)) = Ha.$$

Beweis. Für $h \in H$ ist $\varphi(ah) = \varphi(a)\varphi(h) = \varphi(a)$, also $ah \in \varphi^{-1}(\varphi(a))$.

Ist umgekehrt $b \in \varphi^{-1}(\varphi(a))$, so gilt $\varphi(b) = \varphi(a)$, mithin $\varphi(a^{-1}b) = e'$ und $a^{-1}b \in H$. Somit ist

$$b = a(a^{-1}b) \in aH.$$

Genauso zeigt man $\varphi^{-1}(\varphi(a)) = Ha$. □

Definition. Sei G eine Gruppe, H eine Untergruppe von G. Man nennt H einen *Normalteiler*, wenn für alle $a \in G$ gilt: $aH = Ha$. Häufig schreibt man die Bedingung $aH = Ha$ zweckmäßig in der Form

$$aHa^{-1} = H.$$

Spätestens an dieser Stelle wollen wir für Teilmengen $K, L \subset G$ die sogenannte *Komplexmultiplikation*

$$KL = \{kl : k \in K,\ l \in L\}$$

einführen. Besteht K nur aus einem Element k, so schreibt man auch kL für KL. Die Komplexmultiplikation ist in offensichtlicher Weise assoziativ, und es gilt $k^{-1}kL = L = Lkk^{-1}$ für alle $k \in G$, $L \subset G$.

Ist die Gruppe G abelsch, so ist jede Untergruppe ein Normalteiler. Die Umkehrung ist falsch: Es gibt eine Gruppe mit 8 Elementen, die zwar diese Eigenschaft besitzt, aber nicht abelsch ist. Wichtige Beispiele von Normalteilern sind:

Beispiele. (a) Die alternierende Gruppe A_n ist ein Normalteiler in der symmetrischen Gruppe S_n, denn A_n ist ja der Kern des Signums $\operatorname{sign} : S_n \to \{\pm 1\}$.

(b) Die Gruppe $\mathrm{SL}(n,K)$, die aus allen $(n \times n)$-Matrizen der Determinante 1 über einem Körper K besteht, ist ein Normalteiler von $\mathrm{GL}(n,K)$, denn sie ist der Kern der Determinantenfunktion.

(c) Das Zentrum einer Gruppe G ist stets ein Normalteiler, denn für alle $g \in G$ gilt offensichtlich $gZ(G) = Z(G)g$. Ebenso ist jede Untergruppe des Zentrums ein Normalteiler von G (und nicht nur von $Z(G)$!).

(d) Jede Untergruppe U vom Index 2 in der Gruppe G ist ein Normalteiler. Denn für jedes $g \in G \setminus U$ ist $G = U \cup gU = U \cup Ug$, wobei beide Vereinigungen disjunkt sind. Z.B. ist A_n auch aus diesem Grund normal in S_n.

(e) Ist U die einzige Untergruppe der Ordnung $n = |U|$ in der Gruppe G, so ist U normal in G. Denn für alle $g \in G$ muß die Untergruppe gUg^{-1} der Ordnung n dann mit U übereinstimmen.

Satz 12.1 können wir jetzt auch so formulieren: Der Kern eines Homomorphismus ist ein Normalteiler. Das wesentliche Ziel dieses Abschnitts ist die Umkehrung dieser Aussage, mit der wir aber wegen unserer Vorübung mit den Ringen wenig Mühe haben.

Sei N Normalteiler der Gruppe G. Wir dürfen statt Links- oder Rechtsklassen einheitlich von *Nebenklassen* sprechen und bezeichnen mit G/N die Menge der Nebenklassen nach N. Seien $a, b \in G$. Dann gilt

$$(aN)(bN) = (aN)(Nb) = a(NN)b = aNb = abN.$$

Das in naheliegender Weise gebildete (Komplex-)Produkt zweier Nebenklassen ist also wieder eine Nebenklasse.

Satz 12.2. *Sei G eine Gruppe und N ein Normalteiler in G.*

(a) *Mit dem soeben eingeführten Produkt ist G/N eine Gruppe.*
(b) *Die Abbildung $\pi : G \to G/N$, $\pi(a) = aN$, ist ein surjektiver Gruppenhomomorphismus. Es gilt* $\operatorname{Kern} \pi = N$.

Beweis. (a) Die Assoziativität der Multiplikation auf G/N ist einfach die Assoziativität der Komplexmultiplikation. Offensichtlich ist $N = eN$ das neutrale Element in G/N und $a^{-1}N$ die zu aN inverse Nebenklasse.

(b) Die Homomorphie ist noch einmal die Gleichung $(aN)(bN) = (ab)N$:

$$\pi(a)\pi(b) = (aN)(bN) = (ab)N = \pi(ab).$$

Die Surjektivität von π ist offensichtlich, und ebenso, daß $\operatorname{Kern}\pi = N$ ist. □

Definition. Man nennt G/N die *Faktorgruppe* von G nach N und $\pi : G \to G/N$ den *natürlichen Homomorphismus*.

Die Anwendung des natürlichen Homomorphismus $\pi : G \to G/N$ bezeichnet man wie bei Ringen oft mit einem Querstrich, schreibt also $\overline{a}$ statt $\pi(a)$.

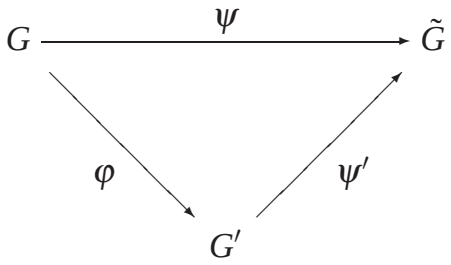
Wie schon bei den Restklassenringen gilt: Man sollte sich die Elemente von G/N nicht als Mengen vorstellen, sondern einfach als Elemente einer neuen Gruppe, in der man nach den Regeln der Gruppentheorie genauso rechnet wie in G.

In Analogie zur Situation bei den Ringen gilt auch bei Gruppen der *Satz vom induzierten Homomorphismus*.

Satz 12.3. *Es seien $\varphi : G \to G'$, $\psi : G \to \tilde{G}$ Homomorphismen von Gruppen. φ sei surjektiv, und es gelte* $\operatorname{Kern}\psi \supset \operatorname{Kern}\varphi$. *Dann gibt es genau eine Abbildung $\psi' : G' \to \tilde{G}$ mit $\psi' \circ \varphi = \psi$. Es ist* $\operatorname{Bild}\psi = \operatorname{Bild}\psi'$. *$\psi'$ ist ein Homomorphismus, und es gilt $\varphi(\operatorname{Kern}\psi) = \operatorname{Kern}\psi'$.*

Ist ψ surjektiv, dann ist auch ψ' surjektiv. Bei $\operatorname{Kern}\psi = \operatorname{Kern}\varphi$ *ist ψ' injektiv.*

Die Beziehung der Homomorphismen in Satz 12.3 bringt man wieder so zum Ausdruck: Das Diagramm



ist kommutativ. Der Beweis des Satzes ist völlig analog zum Satz vom induzierten Homomorphismus für Ringe, so daß wir uns ersparen, ihn auszuführen.

Ebenso gilt in der Gruppentheorie der *Homomorphiesatz:*

Satz 12.4. *Sei $\psi : G \to \tilde{G}$ ein surjektiver Homomorphismus von Gruppen mit* $I = \operatorname{Kern}\psi$. *Dann ist der induzierte Homomorphismus $\psi' : G/I \to \tilde{G}$ (für die Nebenklassenabbildung $\pi : G \to G/I = G'$) ein Isomorphismus.*

Sei G eine endliche Gruppe und N ein Normalteiler. Nach dem Satz von Lagrange ist $|G/N| = |G|/|N|$. Wir ergänzen diese Aussage noch etwas, zu einem oft sehr wirkungsvollen Zählprinzip:

Satz 12.5. *Seien G,H endliche Gruppen und $\varphi : G \to H$ ein Homomorphismus.*

(a) *Für jede Untergruppe U von G ist*

$$|U| = |\varphi(U)| \cdot |U \cap \operatorname{Kern}\varphi|.$$

(b) *Wenn φ surjektiv ist, dann gilt für jede Untergruppe V von H:*

$$|\varphi^{-1}(V)| = |V| \cdot |\operatorname{Kern}\varphi|.$$

Beweis. (a) Wir setzen $\varphi_0 = \varphi|U$. Dann ist $\varphi_0 : U \to \varphi(U)$ ein surjektiver Homomorphismus mit $\operatorname{Kern}\varphi_0 = U \cap \operatorname{Kern}\varphi$. Nach dem Homomorphiesatz ist

$$\varphi(U) \cong U/\operatorname{Kern}\varphi_0.$$

Also gilt nach dem Satz von Lagrange:

$$|\varphi(U)| = [U : (U \cap \operatorname{Kern}\varphi)] = |U|/|U \cap \operatorname{Kern}\varphi|.$$

(b) Wir setzen $U = \varphi^{-1}(V)$. Da φ surjektiv ist, folgt $V = \varphi(U)$. Ferner ist $\operatorname{Kern}\varphi \subset U$, so daß (b) aus (a) folgt. □

Als erste Anwendung der Konstruktion von Faktorgruppen beweisen wir den *Satz von Cauchy* – eine Aussage über die Existenz von Elementen vorgegebener Ordnung, die wir dann noch erheblich verschärfen werden.

Satz 12.6. *Sei G eine endliche abelsche Gruppe und p ein Primteiler von $|G|$. Dann existiert in G ein Element der Ordnung p.*

Beweis. Wir führen eine Induktion über $|G|$ mit dem trivialen Induktionsbeginn $|G| = p$.

Sei nun $|G| > p$. Wir wählen $a \in G$, $a \neq e$. Falls p die Ordnung von a teilt, enthält die zyklische Gruppe $\langle a\rangle$ gemäß Satz 10.8 ein Element der Ordnung p.

Wir dürfen also annehmen: $p \nmid \operatorname{ord} a$. Wegen

$$|G| = (\operatorname{ord} a) \cdot [G : \langle a\rangle]$$

teilt p dann $[G : \langle a\rangle]$. Da G abelsch ist, ist $\langle a\rangle$ ein Normalteiler, mithin ist

$$[G : \langle a\rangle] = |G/\langle a\rangle|.$$

Auf die Gruppe $G/\langle a\rangle$ können wir die Induktionsvoraussetzung anwenden. Es existiert also ein $b \in G$ mit $\operatorname{ord}\overline{b} = p$. Sei $m = \operatorname{ord} b$. Dann ist

$$\overline{b}^m = \overline{b^m} = \overline{e}.$$

Also teilt $\operatorname{ord}\overline{b} = p$ die Ordnung m von b in G, und wir haben wie oben eine zyklische Untergruppe gefunden, deren Ordnung von p geteilt wird. □

Die Sätze von Sylow sind die ersten substantiellen Resultate in jeder Vorlesung über Gruppentheorie. Wir werden einen dieser Sätze beweisen, auch um die Wirksamkeit der Konstruktion von Faktorgruppen zu demonstrieren.

Am Beispiel der Gruppe A_4 sieht man, daß es zu einem Teiler d der Gruppenordnung im allgemeinen keine Untergruppe der Ordnung d gibt: A_4 enthält keine Untergruppe der Ordnung 6. Wenn d aber von spezieller Gestalt ist, kann man eine solche Existenzaussage doch machen. Dies besagt der *erste Satz von Sylow:*

Satz 12.7. *Sei G eine endliche Gruppe, p eine Primzahl und p^m ein Teiler der Ordnung von G. Dann gibt es eine Untergruppe der Ordnung p^m in G.*

Beweis. Wir führen einen Induktionsbeweis über die Ordnung von G. Da der Fall $m = 0$ trivial ist, dürfen wir $m \geq 1$ annehmen.

Die kleinste dann für G in Frage kommende Ordnung ist p. In diesem Fall ist G selbst die gesuchte Untergruppe. Für den Induktionsschritt betrachten wir zwei Fälle:

(a) $p \mid |Z(G)|$,
(b) $p \nmid |Z(G)|$.

(a) In diesem Fall gibt es nach Satz 12.6 ein Element $z \in Z(G)$ der Ordnung p. Die Untergruppe $\langle z \rangle$ ist wie jede Untergruppe des Zentrums ein Normalteiler von G. Ferner gilt

$$p^{m-1} \mid |G/\langle z \rangle|.$$

Nach Induktionsvoraussetzung existiert eine Untergruppe V von $G/\langle z \rangle$ der Ordnung p^{m-1}. Sei $\pi : G \to G/\langle z \rangle$ der natürliche Homomorphismus und $U = \pi^{-1}(V)$. Nach Satz 12.5 ist $|U| = |V| \cdot |\operatorname{Kern} \pi| = p^m$.

(b) Im Fall $p \nmid |Z(G)|$ betrachten wir die Klassengleichung

$$|G| = |Z(G)| + \sum_{i=1}^{r} C_i.$$

Die Zahl $|G|$ ist durch p teilbar, $|Z(G)|$ nicht. Also muß es unter den Zahlen $C_1, \ldots, C_r$ eine nicht durch p teilbare geben. Sei dies etwa C_1. Nach Satz 11.4 gibt es eine Untergruppe H mit

$$C_1 = [G : H].$$

Zunächst notieren wir, daß H wegen $C_1 \geq 2$ eine echte Untergruppe von G ist. Sodann schließen wir aus der Gleichung

$$|G| = |H| \cdot C_1,$$

daß $|H|$ durch p^m teilbar ist. Wir können also die Induktionsvoraussetzung auf H anwenden. □

Definition. Sei p eine Primzahl. Wenn p^m die Ordnung von G teilt, p^{m+1} aber nicht, so heißt eine Untergruppe der Ordnung p^m eine *p-Sylow-Untergruppe* von G.

Der erste Satz von Sylow, den wir gerade bewiesen haben, besagt also insbesondere, daß eine endliche Gruppe stets eine p-Sylow-Untergruppe besitzt. Dieser Existenzsatz wird wirkungsvoll ergänzt durch den *zweiten und dritten Satz von Sylow:*

Satz 12.8. *Sei p eine Primzahl, G eine endliche Gruppe, U eine Untergruppe, deren Ordnung eine Potenz von p ist, und H eine p-Sylow-Untergruppe. Dann existiert ein $g \in G$ mit $gUg^{-1} \subset H$. Speziell sind alle p-Sylow-Untergruppen konjugiert zueinander.*

Satz 12.9. *Sei p eine Primzahl, G eine endliche Gruppe und s die Anzahl ihrer p-Sylow-Untergruppen. Dann ist $s \equiv 1 \mod p$.*

Ein wesentliches Ziel der Gruppentheorie ist es, die Struktur der endlichen Gruppen auf die Kenntnis möglichst weniger Gruppen zurückzuführen. Ist N ein Normalteiler der Gruppe G, so können wir uns G in gewisser Weise aus N und G/N zusammengesetzt denken (wobei freilich die Isomorphieklasse von G im allgemeinen nicht nur von den Isomorphieklassen von N und G/N abhängt). Eine Gruppe G ist in diesem Sinn nicht aus kleineren Gruppen zusammensetzbar, wenn es außer G und $\{e\}$ keine Normalteiler in G gibt.

Definition. Eine Gruppe G heißt *einfach*, wenn sie keine nichttrivialen Normalteiler besitzt.

Es ist der größte Triumph der Gruppentheorie, daß es vor etwa 20 Jahren gelungen ist, *alle* endlichen einfachen Gruppen zu beschreiben. Diese treten in 4 Serien mit je unendlich vielen Elementen auf, und als sogenannte *sporadische Gruppen*, deren größte das *Monster* ist. Es gibt auch noch ein *Babymonster*. Zwei der Serien kann man sehr einfach beschreiben, nämlich die zyklischen Gruppen von Primzahlordnung (sie enthalten als einzige Gruppen überhaupt keine nichttrivialen Untergruppen) und die alternierenden Gruppen A_n, $n \geq 5$.

Wir wollen zum Abschluß der Vorlesung folgenden Satz beweisen:

Satz 12.10. *Die alternierende Gruppe A_5 ist einfach.*

Beweis. Die Idee des Beweises (die man allerdings kaum auf alle $n \geq 6$ übertragen kann) ist sehr einfach. Sei N ein Normalteiler einer Gruppe G und $x \in N$. Dann gilt $gxg^{-1} \in N$ für alle $g \in G$. Daher enthält N mit jedem Element gleich die ganze Konjugationsklasse und ist damit (disjunkte) Vereinigung von Konjugationsklassen.

Wir behaupten: Die Klassengleichung von A_5 hat die Form

$$60 = 1 + 15 + 20 + 12 + 12.$$

Wenn N ein Normalteiler von A_5 ist, muß $|N|$ sich aus Summanden der rechten Seite zusammensetzen, wobei jeder Summand höchstens einmal vorkommt, und

die 1 ganz bestimmt. (In diesem Sinn betrachten wir die beiden Summanden 12 als verschieden.) Wie man aber auch immer die Summe bildet: Die einzigen Teiler von 60, die so entstehen, sind 1 und 60.

Zum Beweis der Klassengleichung müssen wir die Konjugationsklassen in A_5 bestimmen. Natürlich setzt sich A_5 als Normalteiler von S_5 selbst aus Konjugationsklassen von S_5 zusammen, und letztere entsprechen genau den Zerlegungstypen

$$(5), \quad (4,1), \quad (3,2), \quad (3,1,1), \quad (2,2,1), \quad (2,1,1,1), \quad (1,1,1,1,1).$$

Da ein Zyklus genau dann eine gerade Permutation ist, wenn er ungerade Länge hat, folgt, daß sich A_5 aus den S_5-Konjugationsklassen zu den Zerlegungstypen (5), $(3,1,1)$, $(2,2,1)$ und $(1,1,1,1,1)$ zusammensetzt. Wir müssen nun untersuchen, wie sich diese S_5-Konjugationsklassen weiter aufspalten, wenn wir die Gruppe zu A_5 einschränken.

Nichts zu zeigen ist für $(1,1,1,1,1)$. Diese Klasse besteht nur aus id. Ebenso sehen wir leicht, daß auch zwei Permutationen

$$\pi = (ab)(cd)(e) \quad \text{und} \quad \pi' = (pq)(rs)(t)$$

des Zerlegungstyps $(2,2,1)$ bereits in A_5 konjugiert sind. Ist nämlich $\rho\pi\rho^{-1} = \pi'$, so gilt auch $(\rho\tau)\pi(\rho\tau)^{-1} = \pi'$ mit $\tau = (ab)$, weil diese Transposition mit π kommutiert. Eine der Permutationen ρ oder $\rho\tau$ ist aber gerade. Es gibt 15 Permutationen π des Typs $(2,2,1)$, denn man kann als Wirkungsbereich 5 verschiedene 4-elementige Teilmengen von $\{1,\ldots,5\}$ auswählen und jeden dieser möglichen Wirkungsbereiche auf 3 Arten in 2-elementige Teilmengen zerlegen.

Wenn die Konjugation mit ρ die Permutation $\pi = (abc)(d)(e)$ des Zerlegungstyps $(3,1,1)$ in $\pi' = (pqr)(s)(t)$ überführt, so tut dies auch die Konjugation mit $\rho\tau$, $\tau = (de)$, und wir können analog argumentieren. Es gibt 20 Permutationen vom Typ $(3,1,1)$, denn man kann als Wirkungsbereich eine der 10 3-elementigen Teilmengen von $\{1,\ldots,5\}$ wählen, und zu jedem dieser Wirkungsbereiche gibt es genau zwei 3-Zykel.

Den einzig schwierigeren Fall bilden die 5-Zykel vom Typ (5). Wir stellen erst einmal fest, daß es davon $60-1-15-20 = 24$ gibt. Da die S_5-Konjugationsklasse 24 Elemente hat, muß die Standgruppe jedes einzelnen 5-Zykels ζ genau $|S_5|/24 = 5!/4! = 5$ Elemente haben. Dies sind dann natürlich die Potenzen $\mathrm{id}, \zeta, \zeta^2, \zeta^3, \zeta^4$. Mithin hat ζ in A_5 die gleiche Standgruppe wie in S_5. Da diese in A_5 den Index $60/5 = 12$ hat, besteht die A_5-Konjugationsklasse nur noch aus 12 Elementen. Das bedeutet: Die S_5-Konjugationsklasse spaltet in zwei A_5-Konjugationsklassen zu je 12 Elementen. □

Literaturverzeichnis

[Art] Artin, M.: Algebra. Birkhäuser, Basel 1993.

[FSa] Fischer, G., Sacher, R.: Einführung in die Algebra. Teubner, Stuttgart 1978.

[Kun] Kunz, E.: Algebra. Vieweg, Braunschweig 1994.

[Lor] Lorenz, F.: Einführung in die Algebra I, II. BI, Mannheim 1996.

[Lün] Lüneburg, H.: Einführung in die Algebra. Springer, Berlin 1973.

[Mey] Meyberg, K.: Algebra I, II. Hanser, München 1976.

[MVa] Meyberg, K., Vachenauer, P.: Aufgaben und Lösungen zur Algebra. Hanser, München 1978.

[RSV] Reiffen, H.-J., Scheja, G., Vetter, U.: Algebra. BI, Mannheim 1969.

[SSt] Scheja, G., Storch, U.: Lehrbuch der Algebra, Teil 1, 2. Teubner, Stuttgart 1980.

[Tra] Trapp, H.W.: Einführung in die Algebra. Rasch, Osnabrück 1995.