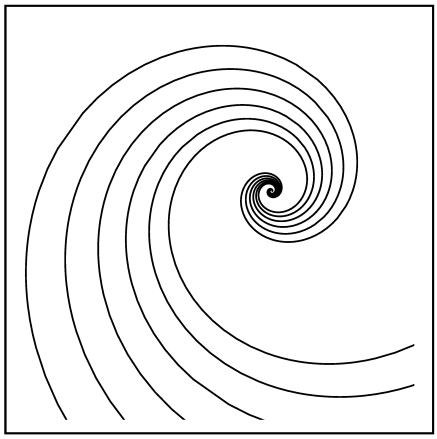
Urs Stammbach Prof. em. ETH



Algebra

Gruppen
Ringe
Körper

Modultheorie
Elemente der Darstellungstheorie
Abriss der Galoistheorie

Wissen entsteht nicht durch Anhäufung von Einzelinformationen, sondern durch theoretisch angeleitete Integration in grössere Zusammenhänge.

T.A. Becker

Vorwort

Der vorliegende Text entspricht dem Skript der Vorlesung *Algebra*, die ich an der ETH für Mathematiker und Physiker mehrmals gehalten habe. Der Text wurde zwischen 1993 (Kapitel I, II, III, VI) und 1995 (Kapitel IV, V) fertiggestellt und in vervielfältigter Form abgegeben; im Jahre 1999 wurde er im Internet verfügbar gemacht. Er erscheint hier erstmals, nur an einigen wenigen Stellen korrigiert und ergänzt, als kleines Buch.

Begriffe und Resultate der abstrakten Algebra spielen in fast allen Gebieten der Mathematik eine grundlegende Rolle. Die Vorlesung, aus der dieser Text entstanden ist, hat zum Ziel, die Studierenden der Mathematik und Physik an der ETH Zürich mit dem zentralen Inhalt der Algebra bekannt zu machen.

Im ersten Teil des Textes werden die grundlegenden Begriffe *Gruppe*, *Ring* und *Körper* eingeführt. Inhalt und Aufbau dieser Kapitel entsprechen im wesentlichen dem Kanon, dem Algebra-Lehrbücher üblicherweise verpflichtet sind. Allerdings sind hier zusätzlich einige Abschnitte aufgenommen, die in anderen Algebra-Texten nicht zu finden sind. Es sind dies das Resultat über die Darstellung von Primzahlen als Summe von zwei Quadraten (II.5), ein Abschnitt über den Satz von Fermat für komplexe Polynomringe (II.6), eine elementare Behandlung des Problems der Konstruktion mit Zirkel und Lineal (III.3) und ein Abschnitt über Codierungstheorie (III.5), in dem u.a. auch die klassischen Newtonschen Identitäten behandelt werden.

Jedes der drei Kapitel zu Gruppen, Ringen und Körpern beginnt mit einer Einleitung, welche ganz kurz die Bedeutung und die historische Entwicklung der Gebiete beschreiben.

Im zweiten Teil des Textes werden drei algebraische Gebiete näher behandelt, nämlich die *Modultheorie*, die *Darstellungstheorie* und die *Galoistheorie*. Es werden damit drei algebraische Themenkreise berührt, die bei jeder weiteren Beschäftigung mit Algebra fundamental sind und die ferner historisch zu Resultaten geführt haben, die für benachbarte Fachgebiete wichtig sind: Die Modultheorie bildet die Grundlage der homologischen Algebra und stellt damit für das Gebiet der algebraischen Topologie den abstrakten, al-

gebraischen Apparat bereit. Die Darstellungstheorie der Gruppen führt nicht nur zu tiefliegenden mathematischen Resultaten innerhalb der Gruppentheorie, sondern sie spielt beispielsweise auch in der mathematischen Behandlung der Quantentheorie eine grosse Rolle. Die Galoistheorie, ursprünglich entstanden, um die Auflösung von polynomialen Gleichungen durch Radikale zu behandeln, wurde in der historischen Entwicklung bald auch grundlegend für viele Resultate der algebraischen Zahlentheorie. Der Text folgt dem Grundsatz, die einzelnen Gebiete nicht völlig voneinander getrennt darzustellen, sondern immer auch Querbezüge zuzulassen. So enthält der Abschnitt IV.5 als Anwendung der Modultheorie nicht nur den Hauptsatz für endlich erzeugte abelsche Gruppen sondern auch einige Resultate zu Normalformen von Matrizen, im Abschnitt V.8 wird in einem Beispiel gezeigt, wie die Darstellungstheorie in der Quantenmechanik verwendet wird und im Abschnitt VI.11 wird mit Hilfe der Galoistheorie ein wichtiger Satz der Darstellungstheorie endlicher Gruppen bewiesen.

Zürich, im September 2009 Urs Stammbach

Inhaltsverzeichnis

Kapitel I. Gruppen

Einleitung

In fast allen Gebieten der Mathematik spielen Gruppen implizit oder explizit eine grosse Rolle: Es besteht kein Zweifel, dass es sich beim Begriff der Gruppe um eine der wichtigsten mathematischen Ideen überhaupt handelt. Auch ausserhalb der Mathematik wird davon häufig Gebrauch gemacht; die Quantentheorie bildet nur eines von vielen Beispielen, wo die Gruppentheorie als wesentliches Hilfsmittel auftritt.

Die Theorie der Gruppen ist der älteste Zweig der modernen Algebra. Ihr Ursprung kann zurückverfolgt werden bis zu J.-L. Lagrange (1736-1813), P. Ruffini (1765-1822) und E. Galois (1811-1832). In deren Werk treten Gruppen in natürlicher Weise als Permutationsgruppen der Nullstellen eines Polynoms auf, und in der Tat verstand man im 19. Jahrhundert unter einer Gruppe gewöhnlich eine endliche *Permutations*gruppe.

Der Begriff einer *abstrakten* Gruppe kann bereits in den Arbeiten von A. Cayley (1821-1895) erkannt werden; aber erst als W. van Dyck (1856-1934) (freie) Präsentierungen von Gruppen einführte, setzte sich diese Sichtweise langsam durch. Die Notwendigkeit, auch *unendliche* Gruppen zu betrachten, zeigte sich dann vor allem in der Geometrie und der Topologie (F. Klein (1849-1925), S. Lie (1842-1899), H. Poincaré (1854-1912), M. Dehn (1878-1952)).

Die erste Hälfte des 20. Jahrhunderts sah die Entwicklung der *Darstellungstheorie* der diskreten Gruppen durch G.F. Frobenius (1849-1917), W. Burnside (1852-1927), I. Schur (1875-1936) und R. Brauer (1901-1977). Ab 1950 beschäftigte sich eine grössere Anzahl von Gruppentheoretikern mit dem Problem, die endlichen *einfachen* Gruppen zu klassifizieren. Das Vorhaben konnte um 1980 herum nach Arbeiten im Umfang von rund 10'000 Seiten abgeschlossen werden (J.G. Thompson (1932-), W. Feit (1930-2004), D. Gorenstein (1923-1992), M. Aschbacher (1944-). Aber auch die Theorie unendlicher diskreter Gruppen schritt in dieser Zeit rasch voran (B. Neumann (1909-2002), W. Magnus (1907-1990), G. Baumslag (1933-), M. Gromov (1943-).

Der vorliegende Text beschränkt sich auf die Behandlung von grundlegenden Resultaten für diskrete, endliche Gruppen; auf die wichtigen Weiterentwicklungen in Richtung unendlicher Gruppen, wie insbesondere auf die umfangreiche Theorie der Liegruppen und der algebraischen Gruppen kann hier nicht eingegangen werden.

I.1 Axiome, Beispiele

Definition Eine *Gruppe* G ist eine Menge zusammen mit einer Abbildung $* : G \times G \to G$, welche jedem Paar (a, b), $a, b \in G$ ein Elemente $a * b$ zuordnet, so dass gilt:

(a) $a * (b * c) = (a * b) * c$, für alle $a, b, c, \in G$ (*assoziativ*).

(b) Es gibt ein Element $e \in G$ mit den folgenden Eigenschaften:

(1) $e * a = a = a * e$, für alle $a \in G$ (*Neutralelement*).

(2) Zu jedem $a \in G$ existiert $b \in G$ mit $a * b = e = b * a$ (*Inverses*).

Folgerungen

(1) Das Neutralelement ist eindeutig bestimmt: Es sei $e' \in G$ mit $a = e' * a$ für alle $a \in G$. Dann gilt $e' = e$. [Ebenso für $a = a * e'$.]

Beweis Es gilt $e' * e = e'$, da e Neutralelement ist, ferner $e' * e = e$ laut Voraussetzung.

(2) Das Inverse ist eindeutig bestimmt: Es sei $a \in G$. Gilt $b' * a = e$, so folgt $b' = b$. [Ebenso für $e = a * b'$.] Notation: $b = a^{-1}$.

Beweis Aus $b' * a = e$ folgt $(b' * a) * b = e * b = b$ und andererseits $(b' * a) * b = b' * (a * b) = b' * e = b'$.

(3) Zu $a, b \in G$ existiert eindeutig $x \in G$ mit $a * x = b$ [und eindeutig ein $y \in G$ mit $y * a = b$].

Beweis Existenz: Man setze $x = a^{-1} * b$. Dann gilt $a * x = a * (a^{-1} * b) = (a * a^{-1}) * b = e * b = b$. Eindeutigkeit: Sei $\overline{x} \in G$ mit $a * \overline{x} = b$. Dann folgt $a^{-1} * b = a^{-1} * (a * \overline{x}) = e * \overline{x} = \overline{x}$. [Ebenso für y, $y = b * a^{-1}$.]

(4) $e^{-1} = e$

Beweis Es gilt $e = e * e$. Daraus folgt mit (2) $e^{-1} = e$.

(5) $(a^{-1})^{-1} = a$

Beweis Es gilt $a * a^{-1} = e$. Nach (2) folgt $(a^{-1})^{-1} = a$.

(6) $(a * b)^{-1} = b^{-1} * a^{-1}$

Beweis $(a*b)*(b^{-1}*a^{-1}) = a*(b*(b^{-1}*a^{-1})) = a*(b*b^{-1})*a^{-1} = a*(e*a^{-1}) = a*a^{-1} = e$. Nach (2) folgt $(a * b)^{-1} = b^{-1} * a^{-1}$.

(7) Jedes beliebig geklammerte Produkt $a_1 * a_2 * \cdots * a_n$ lässt sich in linksnormierter Weise schreiben, nämlich als $(\cdots((a_1 * a_2) * a_3) * \cdots * a_n)$. Mit anderen Worten: Klammern dürfen weggelassen werden.

Beweis Induktion nach n. Für $n = 3$ stimmt die Behauptung mit Axiom (a) überein. Sei $n \geq 4$. Dann gilt mit Induktion

$$(\cdots(a_1 * \cdots * a_j) * (a_{j+1} * \cdots * a_n)\cdots) = (\cdots(a_1 * \cdots * a_j) * ((a_{j+1} * \cdots * a_{n-1}) * a_n) =$$

$$= ((\cdots(a_1 * \cdots * a_j) * (a_{j+1} * \cdots * a_{n-1})) * a_n) = (\cdots((a_1 * a_2) * a_3) * \cdots * a_n) \ .$$

Die Gruppenoperation wird in vielen Beispielen mit "$\cdot$" bezeichnet (und dann wird dieses Zeichen oft auch einfach weggelassen). Man spricht dann von einer *multiplikativen* Gruppe. In anderen Beispielen wird die Gruppenoperation mit "+" bezeichnet, konsequenterweise heisst dann das Neutralelement 0 und das Inverse von a heisst $-a$. In diesem Fall spricht man von einer *additiven* Gruppe.

(8) Notation: Es sei G eine multiplikative Gruppe. Für ein Element $a \in G$ und eine ganze Zahl $n \in \mathbb{Z}$ setzen wir:

$$a^n = \begin{cases} a \cdot a \cdots a & n\text{-fach, } n \geq 2 \\ a & n = 1 \\ e & n = 0 \\ (a^{-n})^{-1} & n \leq -1 \end{cases}$$

Beachte

$$a^{-m} = (a^m)^{-1} = (a \cdots a)^{-1} = (a^{-1})^m \ , \ m \geq 1 \ ,$$

$$a^k \cdot a^l = a^{k+l} \ , \ k, l \in \mathbb{Z} \ ,$$

$$(a^k)^l = a^{kl} \ , \ k, l \in \mathbb{Z} \ ,$$

In ähnlicher Weise benutzen wir für additive Gruppen die Notation: $na = a + a + \cdots + a$, n-fach.

Definition Die Gruppe G heisst *abelsch* oder *kommutativ*, wenn $a * b = b * a$ gilt für alle $a, b \in G$.

Beispiele

(a) Die ganzen Zahlen $\mathbb{Z}$ bilden eine (abelsche) Gruppe unter der Addition "+", aber keine Gruppe unter der Multiplikation "$\cdot$".

Es sei K ein (kommutativer) Körper. Unter + bildet K eine (abelsche) Gruppe und unter $\cdot$ bilden die Nichtnullelemente von K eine (abelsche) Gruppe. Letztere bezeichnet man

oft mit $K^\bullet$.
Die Menge $\{z \in \mathbb{C} \mid |z| = 1\} \subset \mathbb{C}$ ist unter $\cdot$ eine Gruppe. Die Menge $\{z \in \mathbb{R} \mid |z| = 1\} = \{+1, -1\} \subset \mathbb{R}$ ist unter $\cdot$ eine Gruppe mit der *Multiplikationstafel*

	1	−1
1	1	−1
−1	−1	1

Man beachte, das sich jede Gruppe – im Prinzip – durch ihre Multiplikationstafel beschreiben lässt.

(b) Ein Vektorraum V über dem Körper K bildet definitionsgemäss unter der Addition eine abelsche Gruppe.

In den Beispielen (c) bis (g) sind die Gruppen im allgemeinen nicht abelsch.

(c) $\mathrm{GL}(n, K)$: Die Elemente sind die $n \times n$-Matrizen A über dem Körper K mit $\det A \neq 0$. Diese Gruppe heisst die *allgemeine lineare Gruppe* der Dimension n über K.
$\mathrm{SL}(n, K)$: Die Elemente sind die $n \times n$-Matrizen A über K mit $\det A = +1$. Diese Gruppe heisst die *spezielle lineare Gruppe* der Dimension n über K.

(d) $\mathrm{O}(n)$: *orthogonale Gruppe* über $\mathbb{R}$; $\mathrm{SO}(n)$: *spezielle orthogonale Gruppe* über $\mathbb{R}$.

(e) $\mathrm{U}(n)$: *unitäre Gruppe* über $\mathbb{C}$; $\mathrm{SU}(n)$: *spezielle unitäre Gruppe* über $\mathbb{C}$.

(f) Es sei V ein n-dimensionaler Vektorraum über K. Die Menge der regulären linearen Selbstabbildungen f von V bilden unter der Zusammensetzung $\circ$ eine Gruppe. Diese ist "isomorph" zu $\mathrm{GL}(n, K)$. Der "Isomorphismus" kommt zustande, indem man in V eine Basis wählt und jeder Abbildung f die (reguläre) $n \times n$-Matrix zuordnet, die f in dieser Basis beschreibt.

(g) Es sei Ω eine beliebige Menge. Die Menge der bijektiven Selbstabbildungen von Ω bilden unter der Zusammensetzung eine Gruppe $\mathrm{S}(\Omega)$, die sogenannte *symmetrische Gruppe* von Ω.

(h) Es sei m eine beliebige ganze Zahl. Genau dann liegen zwei Zahlen $a,\ b$ in derselben *Restklasse* modulo m, wenn die Division durch m den gleichen Rest ergibt: $m \mid (a-b)$. Die Einteilung der ganzen Zahlen in Restklassen modulo m ist eine Einteilung in disjunkte Teilmengen. Jede Restklasse R modulo m lässt sich beschreiben durch $r + m\mathbb{Z}$, wobei r

irgend eine Zahl der Restklasse ist. Eine derartige Zahl r heisst ein Repräsentant von R. Für r kann der Rest der Division durch m genommen werden, d.h. $0 \leq r < n$.

Die Addition in $\mathbb{Z}$ induziert in der Menge der Restklassen modulo m, $\mathbb{Z}_m$ eine Verknüpfungsvorschrift, die $\mathbb{Z}_m$ zu einer (abelschen) Gruppe macht, die *Gruppe der Restklassen modulo m* genannt wird:

Es sei $R = r+m\mathbb{Z}$, $S = s+m\mathbb{Z}$. Dann ist $R+S$ definiert durch $R+S = (r+s)+m\mathbb{Z}$.

Man beachte, dass $R + S$ von der Auswahl der Repräsentanten r aus R und s aus S unabhängig ist. Die Axiome sind in offensichtlicher Weise erfüllt.

Beispiel Es sei $m = 6$. Wir wählen als Repräsentanten der Elemente von $\mathbb{Z}_6$ die Zahlen 1,2,. . .,5.

$$\begin{aligned}(2+6\mathbb{Z})+(3+6\mathbb{Z}) &= 5+6\mathbb{Z},\\ (3+6\mathbb{Z})+(4+6\mathbb{Z}) &= 7+6\mathbb{Z} = 1+6\mathbb{Z},\\ (2+6\mathbb{Z})+(4+6\mathbb{Z}) &= 6+6\mathbb{Z} = 0+6\mathbb{Z}\ .\end{aligned}$$

(i) Es sei $m \geq 2$ eine beliebige ganze Zahl, und es sei G die Menge der zu m teilerfremden Restklassen modulo m, d.h. $R = r + m\mathbb{Z}$ und $(r, m) = 1$. Beachte, dass mit $(r, m) = 1$ jedes Element der Restklase von r modulo m zu m teilerfremd ist. Wir definieren in G eine Verknüpfungsvorschrift durch

$$R \cdot S = rs + m\mathbb{Z}\ .$$

Behauptung Unter dieser Operation ist G eine (abelsche) Gruppe. Wir nennen G die multiplikative *Gruppe der zu m teilerfremden Restklassen.*

Beweis Es sei $(r, m) = 1 = (s, m)$. Dann gilt auch $(rs, m) = 1$. Es ist zuerst zu zeigen, dass die Operation wohldefiniert ist. Aus $r' = r+mk$, $s' = s+mk'$ folgt $r's' = rs+msk+mrk'+m^2kk'$ und damit $(r' + m\mathbb{Z}) \cdot (s' + m\mathbb{Z}) = (r + m\mathbb{Z}) \cdot (s + m\mathbb{Z})$.

Das Neutralelement ist offensichtlich durch $E = 1 + m\mathbb{Z}$ gegeben. Um die Existenz eines Inversen zu zeigen, muss zu $R = r + m\mathbb{Z}$ mit $(r, m) = 1$ ein $t + m\mathbb{Z}$ gefunden werden mit

(a) $(t, m) = 1$, und

(b) $rt + m\mathbb{Z} = 1 + m\mathbb{Z}$, d.h. $rt \equiv 1$ modulo m.

Falls t existiert mit (b), so gilt automatisch $(t, m) = 1$. Denn aus $p \mid t$ folgt $p \mid rt$ und damit $p \mid (1 + km)$. Gilt auch $p \mid m$, so folgt $p \mid 1$.

Es bleibt, (b) zu beweisen. Wir gehen indirekt vor und nehmen an, dass kein solches t existiert. Wir betrachten dann die Funktion $\Psi : G \to G$ definiert durch $\Psi(S) = R \cdot S$, $S \in G$. Nach Annahme tritt $E = 1 + m\mathbb{Z}$ nicht als Bild unter Ψ auf. Da G endlich ist, müssten dann mindestens zwei *verschiedene* Restklassen S_1 und S_2 unter Ψ auf die gleiche Restklasse abgebildet werden. Dies bedeutet aber

$$\Psi(S_1) = rs_1 + m\mathbb{Z} = rs_2 + m\mathbb{Z} = \Psi(S_2) \ , \text{ mit } s_1 \not\equiv s_2 \text{ modulo } m \ .$$

Daraus folgt $rs_1 \equiv rs_2 \bmod m$, also $m \mid r(s_1 - s_2)$. Wegen $(m, r) = 1$ folgt weiter $m \mid (s_1 - s_2)$ und damit

$$S_1 = s_1 + m\mathbb{Z} = s_2 + m\mathbb{Z} = S_2 \ .$$

Dies ist ein Widerspruch zur Voraussetzung $S_1 \neq S_2$.

Beispiel Es sei $m = 8$. Dann gilt $G = \{1 + 8\mathbb{Z},\ 3 + 8\mathbb{Z},\ 5 + 8\mathbb{Z},\ 7 + 8\mathbb{Z}\}$. Die Gruppenoperation ist definiert durch

$$(x + 8\mathbb{Z}) \cdot (y + 8\mathbb{Z}) = (xy + 8\mathbb{Z}) \ .$$

Die Multiplikationstafel von G lautet also

$\cdot$	1	3	5	7
1	1	3	5	7
3	3	1	7	5
5	5	7	1	3
7	7	5	3	1

Das Neutralelenment ist $1+8\mathbb{Z}$, und das Inverse ist gegeben durch $(x+8\mathbb{Z})^{-1} = (x+8\mathbb{Z})$.

Definition Die Anzahl der zu m teilerfremden Restklasen modulo m wird mit $\phi(m)$ bezeichnet; ϕ heisst die *Eulersche Funktion*.

Für $m = p$ eine Primzahl gilt natürlich $\phi(p) = p - 1$.

(k) Symmetriegruppe eines regulären n-Ecks (*Diedergruppe* D_{2n}).

Die Kongruenzabbildungen der Ebene, welche ein gegebenes reguläres n-Eck in sich abbilden, sind offenbar die folgenden: Drehungen um den Mittelpunkt um den Winkel $2r\pi/n$, $0 \leq r < n$; und Spiegelungen an den n Symmetrieachsen. Die Symmetriegruppe eines regulären n-Ecks enthält also $2n$ Elemente.

Man beachte ausserdem: Die Zusammensetzung "Drehung um $2r\pi/n \circ$ Spiegelung an der 0-ten Symmetrieachse" ist die "Spiegelung an der r-ten Symmetrieachse".

Die Drehungen sind orientierungserhaltend, sie bilden für sich ebenfalls eine Gruppe, diese ist in offensichtlicher Weise"isomorph" zu $\mathbb{Z}_m$.

(l) Symmetriegruppe eines Würfels W

Die Bewegungen des dreidimensionalen Raumes, welche einen festen Würfel in sich überführen, bilden offensichtlich eine Gruppe, die Symmetriegruppe W des Würfels. Die Elemente dieser Gruppe sind Drehungen um den Mittelpunkt des Würfels. Da jede Drehung eine Achse besitzt, lassen sich die Elemente von W ohne grosse Schwierigkeiten aufzählen.

Achse durch zwei gegenüberliegende Ecken:
es gibt 4 verschiedene solche Achsen, die Ordnung der Drehung ist 3.

Achse durch die Mitten von zwei gegenüberliegenden Kanten:
es gibt 6 verschiedene solche Achsen, die Ordnung der Drehung ist 2.

Achse durch die Mitten von zwei gegenüberliegenden Seitenflächen:
es gibt 3 verschiedene solche Achsen, die Ordnung der Drehung ist 4.

In der Gruppe W gibt es neben der Identität also $4 \cdot 2 + 6 \cdot 1 + 3 \cdot 3 = 23$ Elemente. Die Gesamtzahl der Elemente in W ist also 24.

I.2 Untergruppen

Es sei G eine multiplikative Gruppe

Definition Eine nichtleere Untermenge U von G heisst eine *Untergruppe* von G, wenn mit $a,\ b \in U$ stets gilt $a^{-1} \in U$ und $ab \in U$. Die Menge U ist dann unter der Verknüpfungsvorschrift, die in G gegeben ist, selbst eine Gruppe.

Beispiele

(a) $\{z \in \mathbb{C} \mid |z| = 1\}$ ist eine Untergruppe von $\mathbb{C}^\bullet$.

(b) Jede Gruppe G besitzt als "triviale" Untergruppen $\{e\}$ und G.

(c) Es sei $G = \mathrm{GL}(n, \mathbb{R})$, und H sei die Menge der Elemente in G, welche das Standardskalarprodukt in $\mathbb{R}^n$ invariant lassen. Dann ist H eine Untergruppe, nämlich $\mathrm{O}(n) \subseteq \mathrm{GL}(n, \mathbb{R})$. Nimmt man ein anderes Skalarprodukt, so erhält man im allgemeinen eine andere (allerdings zu $\mathrm{O}(n)$ "isomorphe") Untergruppe. Weitere Gruppen, die wir zum Teil bereits in Abschnitt 1 definiert haben, sind in offensichtlicher Weise Untergruppen von $\mathrm{GL}(n, \mathbb{R})$:

$$\begin{array}{ccccc} \mathrm{O}(n) & \subseteq & \mathrm{GL}(n,\mathbb{R}) & \supseteq & \mathrm{SL}(n,\mathbb{R}) \\ & & \cup| & & \cup| \\ & & \mathrm{GL}(n,\mathbb{Z}) & \supseteq & \mathrm{SL}(n,\mathbb{Z})\ . \end{array}$$

(d) Es sei $G = \mathbb{Z}$. Zu gegebenem $m \in \mathbb{Z}$ betrachten wir die Untermenge $U = m\mathbb{Z}$. Dann ist U eine Untergruppe.

Beweis Wegen $m \in U$ ist U nicht leer. Mit $a = mk$ und $b = ml$ ist auch $-a = m(-k)$ und $a + b = m(k + l)$ in U. Damit ist U eine Untergruppe.

Wir behaupten ferner: *Jede Untergruppe U von $\mathbb{Z}$ ist von der Form $m\mathbb{Z}$ für ein gewisses $m \geq 0$.*

Beweis Es ist $\{0\} = 0\mathbb{Z}$. Falls $U \neq \{0\}$, so existiert $0 \neq a \in U$ und damit enthält U auch positive Zahlen. Wir wählen nun $0 \neq a \in U$ mit $|a|$ minimal, setzen $m = |a|$ und betrachten $V = m\mathbb{Z}$. Dann gilt sicher $V \subseteq U$. Um das Umgekehrte zu zeigen, nehmen wir $c \in U$ mit $c \notin V$. Dann ist nach Voraussetzung $m = |a| < |c|$. Wir schreiben dann c in der Form $mk + r$ mit $0 \leq r \leq m - 1$. Aus $c \notin V$ folgt $r \neq 0$. Da U eine Untergruppe ist, folgt weiter $r = |c| - mk \in U$, aber $0 \neq |r| < m$. Dies ist ein Widerspruch.

Man beachte $(-m)\mathbb{Z} = m\mathbb{Z}$. Ausserdem ist $m\mathbb{Z}$ für $m \neq \pm 1$ eine *echte* Untergruppe von $\mathbb{Z}$.

(e) Es sei G eine multiplikative Gruppe und $a \in G$. Wir betrachten die Untermenge $H = \langle a \rangle = \{a^n \mid n \in \mathbb{Z}\} \subseteq G$.

Wir behaupten: *$\langle a \rangle$ ist eine Untergruppe von G.*

Beweis Wegen $a \in \langle a \rangle$ ist $\langle a \rangle$ nicht leer. Mit a^n und a^m ist auch $(a^n)^{-1} = a^{-n}$ und $a^n a^m = a^{n+m}$ in $\langle a \rangle$.

Definition Für $a \in G$ heisst $\langle a \rangle$ die von a erzeugte *zyklische Untergruppe* von G. Eine Gruppe H heisst *zyklisch*, wenn $a \in H$ existiert mit $\langle a \rangle = H$. Man sagt dann, a sei ein *erzeugendes Element* von H.

(f) Jede Untergruppe von $\mathbb{Z}$ ist zyklisch: $m\mathbb{Z} = \langle m \rangle$.

(g) Die Gruppe $\mathbb{Z}_m$ ist zyklisch, $\mathbb{Z}_m = \langle 1 + m\mathbb{Z} \rangle$. Man beachte, dass in $\mathbb{Z}_m$ auch andere Elemente erzeugend sein können; z.B. ist in $\mathbb{Z}_7$ *jedes* nicht triviale Element erzeugend.

Für die zyklische Gruppe $H = \langle a \rangle$ gilt $a^n a^m = a^{n+m} = a^m a^n$, d.h. H ist abelsch.

Ist $a^n \neq e$ für alle $0 \neq n \in \mathbb{Z}$ so heisst $\langle a \rangle$ *unendlich zyklisch*. Für die (multiplikativ geschriebene) unendlich zyklische Gruppe verwenden wir die Notation C. Die Elemente von C lassen sich aufzählen. Es gilt: $C = \{\ldots, a^{-n}, \ldots, a^{-1}, e, a, a^2, \ldots\}$. Es ist klar, dass

die multiplikative Gruppe C "isomorph" ist zur additiven Gruppe $\mathbb{Z}$.
Es sei $a^n = e$ für gewisses $n \neq 0$. Wir können offenbar $n > 0$ annehmen, denn mit $a^n = e$ ist auch $a^{-n} = e$. Es sei m die kleinste positive Zahl mit $a^m = e$. Dann besteht $\langle a \rangle$ aus den Elementen $\{e, a, a^2, \cdots, a^{m-1}\}$, und es gilt $a^k \cdot a^l = a^{k+l} = a^r$ mit $0 \leq r \leq m-1$ und $k + l = r$ modulo m. Diese *zyklische Gruppe der Ordnung* m bezeichnen wir mit C_m. Es ist klar, dass die multiplikative Gruppe C_m "isomorph" ist zur additiven Grupe $\mathbb{Z}_m$.

Definition Die kleinste positive Zahl m mit $a^m = e$ heisst *Ordnung* $|a|$ des Elementes a. Die *Ordnung* $|G|$ einer Gruppe G ist die Anzahl Elemente in der Menge G.
Beispiel $|\langle a \rangle| = |a|$, $|\{e\}| = 1$, $|S_m| = m!$.

I.3 Endliche Permutationsgruppen

Definition Die *symmetrische Gruppe* S_m ist definiert als die Gruppe der bijektiven Abbildungen $\{1, 2, \ldots, m\}$ unter der Verknüpfungsvorschrift, die durch durch die Zusammensetzung der Abbildungen gegeben ist.

Für die Ordnung gilt $|S_m| = m!$

Ein Element $\sigma \in S_m$ ist gegeben durch die Angabe der m Bilder $\sigma(\nu) = i_\nu$, $\nu = 1, 2, \ldots, m$, $1 \leq i_\nu \leq m$, wobei die i_ν paarweise verschieden sind. Jedes Element σ kann deshalb durch eine zweireihige Matrix dargestellt werden, wobei die Reihenfolge der Spalten keine Rolle spielt:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & \cdots & m \\ i_1 & i_2 & i_3 & \cdots & i_m \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & \cdots & m \\ \sigma(1) & \sigma(2) & \sigma(3) & \cdots & \sigma(m) \end{pmatrix} .$$

Das Inverse ist gegeben durch

$$\sigma^{-1} = \begin{pmatrix} i_1 & i_2 & i_3 & \cdots & i_m \\ 1 & 2 & 3 & \cdots & m \end{pmatrix} .$$

Die Zusammensetzung ist gegeben durch

$$\sigma = \begin{pmatrix} \nu \\ i_\nu \end{pmatrix} , \ \tau = \begin{pmatrix} \mu \\ j_\mu \end{pmatrix} , \ \tau \circ \sigma = \begin{pmatrix} \nu \\ j_{i_\nu} \end{pmatrix} .$$

Beispiel

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 4 & 1 & 2 \end{pmatrix} \quad , \quad \tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 5 & 3 & 1 & 4 \end{pmatrix} \tag{1}$$

$$\sigma^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 5 & 1 & 3 & 2 \end{pmatrix} \ , \ \tau \circ \sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 1 & 2 & 5 \end{pmatrix} \ , \ \sigma \circ \tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 2 & 4 & 3 & 1 \end{pmatrix}$$

Wegen $\sigma \circ \tau \neq \tau \circ \sigma$ ist S_5 nicht abelsch!

Neben der Darstellung von Permutationen durch zweireihige Matrizen gibt es die Darstellung durch Zyklen:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 4 & 1 & 2 \end{pmatrix} = (1,3,4)(2,5)$$

Definition. Der *Zyklus* $(i_1, i_2, i_3, \ldots, i_l)$ der Länge l, beschreibt in S_m die Permutation:

$$\sigma = \begin{pmatrix} i_1 & i_2 & i_3 & \ldots & i_{l-1} & i_l & i_{l+1} & \cdots & i_m \\ i_2 & i_3 & i_4 & \ldots & i_l & i_1 & i_{l+1} & \cdots & i_m \end{pmatrix} .$$

Es ist klar, dass eine zyklische Vertauschung der Zahlen $i_1, i_2, \ldots, i_l$ die durch den Zyklus $(i_1, i_2, i_3, \ldots, i_l)$ beschriebene Permutation nicht verändert. Einerzyklen werden in der Zyklenschreibweise gewöhnlich einfach weggelassen. Zweierzyklen (i, j) heissen auch *Transpositionen*.

Man zeigt sehr leicht, dass für die Zyklen die folgenden Aussagen erfüllt sind:

- Elementfremde Zyklen vertauschen.
- Jede Permutation ist Produkt von elementfremden Zyklen.
- Die Zerlegung in elementfremde Zyklen ist (bis auf Reihenfolge) eindeutig.
- Jeder Zyklus und damit jede Permutation ist Produkt von Transpositionen.

Nur die letzte Behauptung verlangt einen *Beweis:* Es gilt offensichtlich

$$(i_1, i_2, \ldots, i_l) = (i_1 i_2) \circ \cdots \circ (i_{l-2}, i_{l-1}) \circ (i_{l-1} i_l) \ .$$

Beispiel Die Gruppe S_3 besitzt $3! = 6$ Elemente, nämlich

$$\{e, (1,2), (2,3), (1,3), (1,2,3), (1,3,2)\} \ .$$

Es gilt $(1,2)(2,3) = (1,2,3)$ und $(1,3)(3,2) = (1,3,2)$.

Definition Es sei G eine multiplikative Gruppe, und $x,\ y \in G$. Das *unter y zu x konjugierte Element* ist definiert durch $y \cdot x \cdot y^{-1}$.

Es sei

$$\sigma = \begin{pmatrix} \nu \\ i_\nu \end{pmatrix} \ , \ \tau = \begin{pmatrix} \mu \\ j_\mu \end{pmatrix} \ .$$

Dann gilt

$$\tau \circ \sigma \circ \tau^{-1}(j_\mu) = j_{i_\mu} \ .$$

Beispiel Für die in (1) explizit gegebenen Elemente σ und τ gilt

$$\tau \circ \sigma \circ \tau^{-1} = \begin{pmatrix} 2 & 5 & 3 & 1 & 4 \\ 3 & 4 & 1 & 2 & 5 \end{pmatrix} \ .$$

Ist $\bar{\sigma}$ ein Zyklus, so lässt sich die Konjugation sehr einfach beschreiben. Für

$$\bar{\sigma} = (i_1, i_2, i_3, \ldots, i_l) \ , \quad \tau = \begin{pmatrix} \mu \\ j_\mu \end{pmatrix}$$

gilt

$$\tau \circ \bar{\sigma} \circ \tau^{-1} = \begin{pmatrix} j_{i_k} \\ j_{i_{k+1}} \end{pmatrix}_{1 \le k \le l} = (j_{i_1}, j_{i_2}, j_{i_3}, \ldots, j_{i_l})$$

Wir haben damit festgestellt: *Das Konjugieren eines Zyklus mit τ entspricht einfach der Ausübung der Permutation τ auf die im Zyklus vorkommenden Elemente.*

Da jede Permutation Produkt elementfremder Zyklen ist, kann in der Zyklendarstellung leicht konjugiert werden. Es gilt nämlich:

$$\tau \circ (z_1 \circ \cdots \circ z_k) \circ \tau^{-1} = (\tau \circ z_1 \circ \tau^{-1}) \circ (\tau \circ z_2 \circ \tau^{-1}) \circ \cdots \circ (\tau \circ z_k \circ \tau^{-1}) \ .$$

Beispiel Es sei $\sigma = (1,3,4)(2,5)$, τ wie in (1). Dann gilt $\tau \circ \sigma \circ \tau^{-1} = (2,3,1)(5,4)$.

Definition Es sei σ eine Permutation in S_m. In der Darstellung von σ als Produkt von elementfremden Zyklen sei q_i die Anzahl der Zyklen der Länge i. Dann heisst $(q_1, q_2, \ldots, q_m)$ der *(Zyklen-)Typus* von σ. Es gilt $\sum_{i=1}^{m} i \cdot q_i = m$.

Satz 3.1 *Zwei Permutationen von m Elementen sind genau dann konjugiert in S_m, wenn sie denselben Typus haben.*

Beispiel Es sei $\sigma_1 = (2,3,4)(1,5)$ und $\sigma_2 = (1,3,5)(2,4)$. Da σ_1 und σ_2 vom selben Zyklentypus sind, müssen sie nach obigem Satz in S_5 konjugiert sein. Offensichtlich gilt

$$\tau \circ \sigma_1 \circ \tau^{-1} = \sigma_2$$

für

$$\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 3 & 5 & 4 \end{pmatrix} .$$

Definition Das Signum einer Permutation σ ist definiert durch

$$\operatorname{sign}(\sigma) = (-1)^{\text{Anzahl Fehlstände in } \sigma} ,$$

wobei ein *Fehlstand* definiert ist als ein Paar (i,j) mit $i < j$ aber $\sigma(i) > \sigma(j)$.

– Ist τ eine Transposition, so ist $\operatorname{sign}(\tau \circ \sigma) = -\operatorname{sign}(\sigma)$.

Beweis Die Permutation $\tau \circ \sigma$ entsteht aus σ durch Vertauschen zweier Zahlen. Vertauscht man benachbarte Zahlen in σ, so ändert sich die Anzahl der Fehlstände um eins. Vertauscht man zwei Zahlen, zwischen denen k weitere vorkommen, so hat man $2k+1$ Vertauschungen von benachbarten Zahlen vorzunehmen. In beiden Fällen ändert sich das Vorzeichen von sign.

– Es sei $\sigma = \tau_1 \circ \tau_2 \circ \cdots \circ \tau_r$, wo τ_i für $i = 1, 2, \ldots, r$ eine Transposition ist. Dann gilt $\operatorname{sign}(\sigma) = (-1)^r$.

– Es gilt $\operatorname{sign}(\sigma \circ \sigma') = \operatorname{sign}(\sigma) \cdot \operatorname{sign}(\sigma')$.

Beweis Schreibe σ und σ' als Produkt von Transpositionen.

Definition In S_m ist $\{\sigma \mid \operatorname{sign}(\sigma) = +1\}$ eine Untergruppe; sie heisst die *alternierende Gruppe* A_m vom Grade m.

Offenbar gilt $|A_m| = |S_m|/2 = m!/2$.

I.4 Homomorphismen

Unter den Abbildungen zwischen Gruppen spielen naturgemäss diejenigen eine besondere Rolle, die mit der Gruppenstruktur verträglich sind. Dies sind die Homomorphismen. Es seien G, H zwei multiplikativ geschriebene Gruppen.

Definition Eine Abbildung $\phi : G \to H$ heisst *homomorph* (ein *Homomorphismus*), wenn für alle $a, b \in G$ gilt $\phi(ab) = \phi(a)\phi(b)$.

Satz 4.1 *Es sei $\phi : G \to H$ ein Homomorphismus. Dann gilt $\phi(e_G) = e_H$ und für jedes $a \in G$ gilt $\phi(a^{-1}) = (\phi a)^{-1}$.*
Beweis Es gilt $\phi(e_G) = \phi(e_G e_G) = \phi(e_G)\phi(e_G)$. Daraus folgt durch Multiplikation mit $(\phi(e_G))^{-1}$ sofort $e_H = \phi(e_G)$. Aus $e_H = \phi(e_G) = \phi(a \cdot a^{-1}) = \phi(a) \cdot \phi(a^{-1})$ folgt wegen der Eindeutigkeit des Inversen $\phi(a^{-1}) = (\phi a)^{-1}$.

Beispiele
(a) Die Identität $1_G : G \to G$ ist ein Homomorphismus.

(b) Es sei G die multiplikative Gruppe der positiven reellen Zahlen und H die additive Gruppe der reellen Zahlen. Die Abbildung $\phi : G \to H$ definiert durch $\phi(a) = \log a$, $a \in G$ ist homomorph: $\phi(ab) = \log(ab) = \log a + \log b = \phi(a) + \phi(b)$.

(c) Es sei $G = \mathbb{Z}$ die additive Gruppe der ganzen Zahlen, und $H = \mathbb{Z}_m$ die Gruppe der Restklassen ganzer Zahlen modulo m. Die Abbildung $\phi : G \to H$, definiert durch $\phi(a) = a + m\mathbb{Z}$, $a \in G$ ist homomorph, denn es gilt $\phi(a+b) = (a+b) + m\mathbb{Z} = (a + m\mathbb{Z}) + (b + m\mathbb{Z}) = \phi(a) + \phi(b)$.

(d) Es sei V ein Vektorraum über $\mathbb{R}$, $G = \mathrm{GL}(n, \mathbb{R})$, und H sei die multiplikative Gruppe der reellen Zahlen $\mathbb{R}$. Die Abbildung $\phi : G \to H$ sei definiert durch $\phi(a) = \det a$, $a \in G$. Dann ist ϕ ein Homomorphismus, denn es gilt $\phi(ab) = \det(ab) = \det a \cdot \det b = \phi(a) \cdot \phi(b)$.

(e) Das Signum einer Permutation $\sigma \in S_m$ kann als Homomorphismus $\mathrm{sign} : S_m \to C_2$ interpretiert werden.

Satz 4.2 *Es seien $\phi : G \to H$ und $\psi : H \to K$ Homomorphismen. Dann ist auch $\psi \circ \phi : G \to K$ ein Homomorphismus.*
Beweis $\psi \circ \phi(a \cdot b) = \psi(\phi(a \cdot b)) = \psi(\phi a \cdot \phi b) = \psi(\phi a) \cdot \psi(\phi b) = (\psi \circ \phi)(a) \cdot (\psi \circ \phi)(b)$.

Definition Ein Homomorphismus $\phi : G \to H$ heisst *Isomorphismus* $\phi : G \xrightarrow{\sim} H$, wenn ein Homomorphismus $\psi : H \to G$ existiert mit $\psi \circ \phi = 1_G$ und $\phi \circ \psi = 1_H$.

– Ist ϕ ein Isomophismus, so ist auch ψ ein Isomorphismus.
– Falls ψ existiert, so ist ψ eindeutig bestimmt. In der Tat gilt $\psi' a = \psi' \phi \psi(a) = \psi a$. Wir nennen deshalb ψ den zu ϕ inversen Homomorphismus und benützen die Notation $\psi = \phi^{-1}$.

Definition Zwei Gruppen G, H heissen *isomorph*, $G \cong H$, wenn ein Isomorphismus $\phi : G \to H$ existiert.

Satz 4.3 *Ein Homomorphismus $\phi : G \to H$ ist genau dann ein Isomorphismus, wenn ϕ als Mengenabbildung bijektiv ist.*
Beweis Ist ϕ ein Isomorphismus, so ist ϕ sicher bijektiv. Es sei umgekehrt ϕ bijektiv. Wir zeigen, dass die mengentheoretische Umkehrabbildung ϕ^{-1} homomorph ist. Es gilt

$$\phi^{-1}(a \cdot b) = \phi^{-1}(\phi \circ \phi^{-1}(a) \cdot \phi \circ \phi^{-1}(b)) = \phi^{-1}\phi(\phi^{-1}(a) \cdot \phi^{-1}(b)) = \phi^{-1}(a) \cdot \phi^{-1}(b).$$

Beispiele
(f) Die Abbildung log aus Beispiel (b) ist ein Isomorphismus.

(g) Die Gruppen $\mathbb{Z}_n$ und C_n sind isomorph. Ein Isomorphismus $\phi : Z_n \to C_n$ ist gegeben durch $\phi(r + nZ) = t^r$, wobei t ein erzeugendes Element der Gruppe C_n ist.

(h) Die Gruppe G der Drehungen des dreidimensionalen Euklidischen Vektorraumes und die Gruppe H der reellen orthogonalen 3×3-Matrizen mit Determinante +1 sind isomorph. Ein Isomorphismus $\phi : G \to H$ erhält man, indem man im dreidimensionalen reellen Vektorraum eine Basis wählt und jede Drehung durch die zugehörige 3×3-Matrix darstellt. Man beachte, dass die Wahl einer anderen Basis einen anderen Isomorphismus liefert.

(i) Es sei G eine beliebige Gruppe. Für jedes $a \in G$ betrachten wir die Abbildung $\phi_a : G \to G$, die durch $\phi_a(x) = axa^{-1}$ definiert ist. Diese Abbildung ist offensichtlich homomorph und bijektiv, also ein Isomorphismus von G nach G. Man nennt ϕ_a den *inneren Automorphismus* von G induziert durch das Element a oder auch einfach die *Konjugation* mit a.

Wir merken noch an, dass ein Homomorphismus $\phi : G \to G$ ein *Endomorphismus* von G

heisst. Ein Isomorphismus $\phi : G \to G$ heisst auch *Automorphismus* von G.

Satz 4.4 *Es sei $\phi : G \to H$ ein Homomorphismus. Ist U eine Untergruppe von G, und V eine Untergruppe von H, so gilt*

(i) *$\phi U = \{\phi u \mid u \in U\}$ ist eine Untergruppe von H;*

(ii) *$\phi^{-1}V = \{u \in G \mid \phi u \in V\}$ ist eine Untergruppe von G.*

Die Untergruppe ϕU von H heisst das Bild *von U unter ϕ, und die Untergruppe $\phi^{-1}V$ von G heisst das* Urbild *von V unter ϕ.*

Beweis (i) Es sei $a = \phi u$, $b = \phi v$. Dann gilt $a \cdot b = \phi u \cdot \phi v = \phi(u \cdot v)$, also $a \cdot b \in \phi U$. Ferner gilt $a^{-1} = \phi(u^{-1}) \in \phi U$.
(ii) Es seien $u, v \in \phi^{-1}V$, d.h. es gilt $\phi u,\ \phi v \in V$. Dann folgt $\phi(u \cdot v) = \phi u \cdot \phi v \in V$, d.h. $u \cdot v \in \phi^{-1}V$. Ferner gilt $\phi(u^{-1}) = (\phi u)^{-1} \in V$, d.h. $u^{-1} \in V$. Damit ist $\phi^{-1}V$ eine Untergruppe von G.

Definition Es sei $\phi : G \to H$ homomorph. Der Kern von ϕ, $\ker \phi$ ist definiert durch $\ker \phi = \phi^{-1}(e_H) = \{a \in G \mid \phi a = e\}$.

Korollar 4.5 $\ker \phi$ *ist eine Untergruppe von G.*

Satz 4.6 *Es sei $\phi : G \to H$ homomorph. Genau dann ist ϕ injektiv, wenn* $\ker \phi = \{e_G\}$.

Beweis Es sei $\phi a = \phi(e_G) = e_H$. Da ϕ injektiv ist, folgt $a = e_G$. Damit ist $\ker \phi = \{e_G\}$. Es sei umgekehrt $\ker \phi = \{e_G\}$. Ferner sei $\phi a = \phi b$. Dann gilt $\phi(a^{-1}b) = \phi(a^{-1}) \cdot \phi(b) = (\phi a)^{-1} \cdot \phi(b)) = e_H$, d.h. $a^{-1}b$ ist enthalten in $\ker \phi$. Damit folgt $a^{-1}b = e_G$, d.h. $b = a$, und ϕ ist injektiv.

Definition Es sei $\phi : G \to H$ homomorph. Das Bild von ϕ, $\operatorname{im} \phi$ ist definiert durch $\operatorname{im} \phi = \phi G = \{\phi x \mid x \in G\}$.

Korollar 4.7 $\operatorname{im} \phi$ *ist eine Untergruppe von H.*

Der Homomorphismus ϕ ist genau dann surjektiv, wenn $\phi G = \operatorname{im} \phi = H$.

Beispiele

(k) Es sei $\phi : \mathbb{Z} \to \mathbb{Z}_m$ der Homomorphismus definiert durch $\phi(n) = n + m\mathbb{Z}$. Dann gilt $\ker \phi = m\mathbb{Z}$ und $\operatorname{im} \phi = \mathbb{Z}_m$.

(l) Die Abbildung $\phi : \mathbb{Z} \to G$, $a \in G$ sei definiert durch $\phi(n) = a^n$. Sie besitzt den Kern $\ker \phi = \{k \in \mathbb{Z} \mid a^k = e\} = |a| \cdot \mathbb{Z}$ und das Bild $\operatorname{im} \phi = \{a^k \mid k \in \mathbb{Z}\} = \langle a \rangle$.

Schliesslich fügen wir noch zwei Aussagen über zyklische Gruppen an:

Das Bild einer zyklischen Gruppe ist zyklisch. Wie man leicht zeigt, gilt $\phi\langle a\rangle = \langle \phi a\rangle$.

Satz 4.8 *Es sei V eine Untergruppe der zyklischen Gruppe H. Dann ist V zyklisch.*
Beweis Es sei $H = \langle a\rangle$. Betrachte $\phi : \mathbb{Z} \to H$ definiert durch $\phi(k) = a^k$, $k \in \mathbb{Z}$. Nach obigem ist $\phi^{-1}(V)$ eine Untergruppe von $\mathbb{Z}$. Als solche ist sie unendlich zyklisch, also isomorph zu $\mathbb{Z}$. Die Einschränkung von ϕ auf diese zyklische Untergruppe hat V als Bild. Also ist V zyklisch.

I.5 Nebenklassen

Es sei G eine multiplikative Gruppe und U eine Untergruppe von G.

Definition Für $a \in G$ bezeichnen wir mit aU die Menge $aU = \{au \mid u \in G\} \subseteq G$. Die Menge aU heisst die *Linksnebenklasse* von a modulo U. [Ebenso für Rechtsnebenklassen.]

1. In der additiven Schreibweise heissen Nebenklassen oft *Rest*klassen.

2. Es gilt $aU = bU$ genau dann, wenn $a^{-1}b \in U$.
Beweis Ist $aU = bU$, so existiert $u \in U$ mit $au = be = b$. Somit gilt $a^{-1}b = u \in U$. Ist umgekehrt $a^{-1}b = u \in U$, so folgt $b = au$ für gewisses $u \in G$. Für jedes $v \in U$ gilt dann $bv = auv$ und damit $bU \subseteq aU$. Es gilt aber auch $bu^{-1} = a$, woraus $aU \subseteq bU$ folgt.

3. Gibt es $x \in G$ mit $x \in aU$ und $x \in bU$, so folgt $aU = bU$.
Beweis Es sei $x = au_1 = bu_2$ für $u_1, u_2 \in U$. Daraus folgt $u_1u_2^{-1} = a^{-1}b$, also $a^{-1}b \in U$. Nach 2 folgt dann $aU = bU$.

4. Aus 2 und 3 schliessen wir: *Zwei Nebenklassen sind entweder gleich oder besitzen einen leeren Durchschnitt.* Man kann folglich die Menge G darstellen als disjunkte Vereinigung von Linksnebenklassen modulo U:

$$G = a_1U \cup a_2U \cup a_3U \cup \cdots .$$

Dabei wird üblicherweise $a_1 = e$ genommen.

Definitionen Die Elemente $a_1, a_2, \ldots$ bilden ein *Repräsentantensystem* der Linksnebenklassen.
Die Anzahl der verschiedenen Linksnebenklassen von G modulo U heisst *Index* $[G : U]$ von U in G.

5. In der Nebenklasse aU gibt es höchstens $|U|$ Elemente. Da aus $au_1 = au_2$ stets $u_1 = u_2$ folgt, enthält aU auch mindestens $|U|$ Elemente. Es gilt deshalb: *Jede Linksnebenklasse von G modulo U enthält genau $|U|$ Elemente.*

Satz 5.1 (Satz von Lagrange) *Es sei G endlich und U eine Untergruppe von G. Dann gilt $|G| = |U| \cdot [G : U]$. Insbesondere sind $|U|$ und $[G : U]$ Teiler von $|G|$.*

6. Ist $|G| = p$, p prim, so besitzt G keine echten Untergruppen.

7. Ist $|G| = p$, p prim, $a \in G$, $a \neq e$, dann folgt $\langle a \rangle = G$, das heisst G ist zyklisch.

Satz 5.2 *Eine Gruppe von Primzahlordnung ist zyklisch. Sie wird erzeugt von jedem beliebigen nichttrivialen Element.*

8. Es sei G endlich, $a \in G$. Dann ist $\langle a \rangle$ eine Untergruppe von G. Es folgt: $|a| = |\langle a \rangle|$ ist ein Teiler von G.

Satz 5.3 *Die Ordnung eines Elementes in einer endlichen Gruppe G ist ein Teiler der Gruppenordnung. Insbesondere gilt $a^{|G|} = e$.*

9. Es sei G die multiplikative Gruppe der zu m-teilerfremden Restklassen von $\mathbb{Z}$ modulo m. Die Gruppenordnung haben wir mit Hilfe der Eulerschen Funktion ausgedrückt: $|G| = \phi(m)$. Für das Element $r + m\mathbb{Z} \in G$ folgt also $(r + m\mathbb{Z})^{\phi(m)} = e$ in G. Auf äquivalente Weise können wir dies durch $r^{\phi(m)} \equiv 1 \pmod{m}$ ausdrücken.

Satz 5.4 *Ist r teilerfremd zu m, so folgt $r^{\phi(m)} \equiv 1 \pmod{m}$.*

Im Spezialfall einer Primzahl, $m = p$ prim, erhalten wir wegen $\phi(p) = p - 1$ das folgende Resultat, welches unter dem Namen "Kleiner Satz von Fermat" bekannt ist.

Korollar 5.5 (Kleiner Satz von Fermat) *Es sei p eine Primzahl und a eine Zahl, die p nicht teilt. Dann ist $a^{p-1} \equiv 1 \pmod{p}$.*

10. Statt Linksnebenklassen von G modulo U können auch *Rechts*nebenklassen Ua von G

modulo U betrachtet werden. Es gilt: Ist $a_1, a_2, \ldots$ ein Repräsentantensystem der Linksnebenklassen, so ist $a_1^{-1}, a_2^{-1}, \ldots$ ein Repräsentantensystem der Rechtsnebenklassen.

Beweis Die Zuordnung $aU \to Ua^{-1}$ definiert eine bijektive Abbildung der Menge der Linksnebenklassen in die Menge der Rechtsnebenklassen.

Satz 5.6 *Die Anzahl der Linksnebenklassen stimmt mit der Anzahl der Rechtsnebenklassen überein.*

11. Für abelsche Gruppen ist jede Linksnebenklasse auch eine Rechtsnebenklasse; dies ist aber für nicht abelsche Gruppen im allgemeinen nicht der Fall.

12. Wir machen noch folgende Zusatzbemerkung zum kleinen Satz von Fermat. Ist p eine Primzahl, so gilt für alle Zahlen a

$$a^p \equiv a \pmod{p} .$$

Teilt p die Zahl a nicht, so folgt dies aus dem Satz von Fermat durch Multiplikation beider Seiten mit a. Teilt p die Zahl a, so ist sowohl die linke wie auch die rechte Seite kongruent 0 modulo p.

Es sei nun q eine positive ganze Zahl mit der Eigenschaft

$$a^q \equiv a \pmod{q} .$$

für alle $1 \leq a \leq q$. Man könnte vermuten, dass daraus folgt, dass q eine Primzahl ist. Dies ist aber nicht der Fall: Die Zahl $561 = 3 \cdot 11 \cdot 13$ ist ein (das kleinste!) Gegenbeispiel. Eine derartige Zahl q heisst *Carmichael-Zahl*. Erst vor einigen Jahren konnte man zeigen, dass es davon unendlich viele gibt. Andererseits sind sie doch so selten, dass deren Eigenschaft als Ausgangspunkt von Primzahltests gebraucht werden kann.[1]

I.6 Normalteiler

In diesem Abschnitt führen wir die wichtigen Begriffe *Zentrum* und *Normalteiler* ein. Beide werden durch eine Invarianzeigenschaft bezüglich der der inneren Automorphismen definiert.

[1] Zu diesem Thema vergleiche man den attraktiven Beitrag von A. Granville: *Primality Testing and Carmichael Numbers*, Notices Amer. Math. Soc. **39** (1992), 696-700.

Definition Es sei $x \in G$. Der zu x gehörige *innere Automorphismus* $\phi_x : G \to G$ ist durch die Vorschrift $\phi_x(a) = xax^{-1}$, $a \in G$ definiert.

Definition Das *Zentrum* ZG von G ist die Menge der Elemente von G, die unter allen inneren Automorphismen invariant bleiben:

$$ZG = \{a \in G \mid xax^{-1} = a \text{ für alle } x \in G\} = \{a \in G \mid xa = ax \text{ für alle } x \in G\} \ .$$

Gemäss der zweiten Gleichung kann das Zentrum ZG als die Menge aller Elemente von G beschrieben werden, welche mit allen $x \in G$ kommutieren.

Satz 6.1 *Das Zentrum ZG ist eine abelsche Untergruppe.*
Beweis Es ist $e \in ZG$. Aus $xa = ax$ und $xb = bx$ folgt $xab = axb = abx$. Mit a und b liegt also auch ab in ZG. Ferner folgt aus $xa = ax$ sofort $xa^{-1} = a^{-1}x$. Mit a liegt also auch a^{-1} in ZG. Damit ist ZG eine Untergruppe von G. Die Tatsache, dass ZG abelsch ist, folgt direkt aus der Definition.

Beispiel Ist G abelsch, so gilt $ZG = G$.

Definition Es sei U eine Untergruppe von G. Dann ist $\phi_x U = xUx^{-1}$ wiederum eine Untergruppe. Sie heisst die zu U unter x *konjugierte Untergruppe* von G.

Der innere Automorphismus ϕ_x von G induziert eine Permutation der Untergruppen von G: Die Untergruppe U geht in die unter x konjugierte Untergruppe xUx^{-1} über.

Definition Die Untergruppe U von G heisst ein *Normalteiler* von G, falls $\phi_x(U) = U$ für alle $x \in G$. In diesem Fall benützen wir die Notation $U \lhd G$.

Beispiele
(a) Ist G abelsch, und ist U eine Untergruppe von G, so ist U automatisch auch ein Normalteiler von G.

(b) Das Zentrum ZG ist ein Normalteiler von G. Denn für $a \in ZG$ und $x \in G$ gilt $xax^{-1} = a$. Damit folgt $x(ZG)x^{-1} = ZG$ (und zwar sogar elementweise!).

Satz 6.2 *Ist $\phi : G \to H$ ein Homomorphismus, so ist* $\ker \phi$ *ein Normalteiler von G.*
Beweis Wir wissen bereits, dass $\ker \phi$ eine Untergruppe ist. Es sei $a \in \ker \phi$ dann folgt $\phi(xax^{-1}) = \phi x \cdot \phi a \cdot (\phi x)^{-1} = \phi x \cdot e \cdot (\phi x)^{-1} = e$. Damit gilt $xax^{-1} \in \ker \phi$, also $x(\ker \phi)x^{-1} \subseteq \ker \phi$. Umgekehrt folgt aus $a \in \ker \phi$ nach obigem $x^{-1}ax \in \ker \phi$ und

damit $a = x(x^{-1}ax)x^{-1} \in x(\ker\phi)x^{-1}$. Es gilt also auch $\ker\phi \subseteq x(\ker\phi)x^{-1}$.

Satz 6.3 *Für eine Untergruppe U von G sind die folgenden Aussagen äquivalent:*

(i) $xUx^{-1} \subseteq U$ *für alle* $x \in G$,

(ii) $xUx^{-1} = U$ *für alle* $x \in G$,

(iii) $xU \subseteq Ux$ *für alle* $x \in G$,

(iv) $xU = Ux$ *für alle* $x \in G$.

Beweis (i)⇒(ii): Aus $u \in U$ folgt $u = x(x^{-1}ux)x^{-1} \in xUx^{-1}$.
(ii)⇒(iii): Es sei $xUx^{-1} = U$. Zu $u \in U$ existiert somit $v \in U$ mit $xux^{-1} = v$, also $xu = vx$. Damit gilt $xU \subseteq Ux$.
(iii)⇒(iv): Es sei $xU \subseteq Ux$. Es ist zu zeigen, dass für alle $u \in U$ gilt $ux \in xU$. Wir betrachten $(ux)^{-1} = x^{-1}u^{-1} = vx^{-1}$ für gewisses $v \in U$. Damit folgt $ux = xv^{-1}$ mit $v^{-1} \in U$.
(iv)⇒(i): Es sei $xU = Ux$. Zu $u \in U$ existiert dann $v \in U$ mit $xu = vx$, und es folgt $xux^{-1} = v \in U$. Also gilt $xUx^{-1} \subseteq U$.

Ein weiterer wichtiger Aspekt des Begriffes des Normalteilers wird im folgenden Satz behandelt.

Satz 6.4 *Es sei U eine Untergruppe von G. Genau dann ist U ein Normalteiler von G, wenn die Nebenklasse xyU stets eindeutig durch die Nebenklassen xU und yU bestimmt ist.*

Beweis Es sei zuerst U ein Normalteiler von G. Es ist zu zeigen, dass aus $x_1U = x_2U$ und $y_1U = y_2U$ stets $x_1y_1U = x_2y_2U$ folgt. Es gilt $x_1^{-1}x_2 = u \in U$ und $y_1^{-1}y_2 = v \in U$. Es folgt dann $(x_1y_1)^{-1}x_2y_2 = y_1^{-1}(x_1^{-1}x_2)y_2 = y_1^{-1}uy_2 = (y_1^{-1}uy_1)y_1^{-1}y_2 = u'v \in U$, wobei wir $y_1^{-1}uy_1 = u'$ gesetzt haben. Wegen der Normalteilereigenschaft liegt u' in U, so dass in der Tat $x_1y_1U = x_2y_2U$ gilt.
Umgekehrt folge aus $x_1U = x_2U$ und $y_1U = y_2U$ stets $x_1y_1U = x_2y_2U$. Setzen wir $x_1 = e$, $x_2 = u \in U$, $y_1 = x^{-1}$, $y_2 = x^{-1}$, so erhalten wir $xux^{-1} = (x_1y_1)^{-1}(x_2y_2) \in U$, also $xUx^{-1} \subseteq U$. Damit ist U ein Normalteiler von G.

Die in diesem Satz ausgesprochene Eigenschaft macht es möglich, in der Menge der Nebenklassen von G modulo einem Normalteiler N eine Gruppenstruktur zu definieren.

Definition Es sei N ein Normalteiler von G. Wir definieren die *Quotientengruppe* G/N ("G modulo N") wie folgt:

– Die unterliegende Menge ist die Menge der Nebenklassen von G modulo N,

– die Verknüpfungsvorschrift ist definiert durch $xN \cdot yN = xyN$,

– das Neutralelement ist definiert durch eN,

– das Inverse ist definiert durch $(xN)^{-1} = x^{-1}N$.

Natürlich gilt für die Ordnungen der involvierten Gruppen $|G| = |G/N| \cdot |N|$. Die zur Quotientengruppe gehörige Abbildung $\pi : G \to G/N$ definiert durch $x \mapsto xN$ ist offensichtlich ein Homomorphismus. Wir nennen π die *kanonische Projektion* von G auf G/N.

Beispiele

(a) Es sei G die multiplikative Gruppe der von 0 verschiedenen komplexen Zahlen und N die Untergruppe der positiven reellen Zahlen. Da G abelsch ist, ist N automatisch ein Normalteiler. Die Elemente von G/N lassen sich in der komplexen Zahlebene als Strahlen deuten. In diesem Beispiel können die Repräsentanten der Nebenklassen in besonders geschickter Weise gewählt werden: man wähle als Repräsentanten komplexe Zahlen z mit $|z| = 1$. Diese bilden unter der Multiplikation eine Gruppe, die zu G/N isomorph ist. Offensichtlich ist also G/N isomorph zur Drehgruppe der Ebene SO(2).

(b) Es seien $G = \mathbb{Z}$ und $N = n\mathbb{Z}$. Die Quotientengruppe G/N besteht aus den Elementen $x + n\mathbb{Z}$, also den Restklassen ganzer Zahlen modulo n. Die Verknüpfungsvorschrift (additiv!) in der Quotientengruppe ist gegeben durch $(x + m\mathbb{Z}) + (y + n\mathbb{Z}) = (x + y) + n\mathbb{Z}$, stimmt also mit derjenigen in $\mathbb{Z}_n$ überein. Es ist folglich $G/N = \mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}_n$.

(c) Es sei $G = \mathrm{GL}(n, \mathbb{R})$ und $U = \{aE \mid 0 \neq a \in \mathbb{R}\}$. Es ist leicht zu sehen, dass U in G Normalteiler ist; in der Tat ist U das Zentrum von G. Die Quotientengruppe $G/U = \mathrm{PL}(n, \mathbb{R})$ heisst die *projektive lineare Gruppe* in n Dimensionen über $\mathbb{R}$.

(d) Es sei G eine multiplikativ geschrieben Gruppe. Für $a, b \in G$ definieren wir

$$[a, b] = aba^{-1}b^{-1}$$

und nennen diese Bildung den *Kommutator* von a und b. Die *Kommutatorgruppe* $[G, G]$ von G ist definiert als Untergruppe, die in G von allen Kommutatoren erzeugt wird.
Wegen $[a, b]^{-1} = [b, a]$ lässt sich jedes Element der Kommutatorgruppe als Produkt von Kommutatoren schreiben.

Satz 6.5 *Die Kommutatoruntergruppe $[G, G]$ ist ein Normalteiler in G.*

Beweis Es gilt

$$x([a_1,b_1][a_2,b_2]\cdots[a_n,b_n])x^{-1} = (x[a_1,b_1]x^{-1})(x[a_2,b_2]x^{-1})\cdots(x[a_n,b_n])x^{-1}) \ ,$$

und für einen einzelnen Kommutator erhalten wir

$$x[a,b]x^{-1} = x(aba^{-1}b^{-1})x^{-1} = (xax^{-1})(xbx^{-1})(xa^{-1}x^{-1})(xb^{-1}x^{-1}) = [xax^{-1}, xbx^{-1}] \ .$$

Das Konjugierte eines Produktes von Kommutatoren ist folglich wiederum ein Produkt von Kommutatoren. Damit gilt $x[G,G]x^{-1} \subseteq [G,G]$, und $[G,G]$ ist ein Normalteiler von G.

Satz 6.6 *Genau dann ist G abelsch, wenn gilt $[G,G] = \{e\}$.*

Beweis Es sei G abelsch. Dann gilt $[a,b] = e$ für alle $a, b \in G$. Also ist $[G,G]$ trivial. Ist G nicht abelsch, so existieren $a, b \in G$ mit $ab \neq ba$. Dann folgt $aba^{-1}b^{-1} \neq e$, und $[G,G]$ ist nicht trivial.

Satz 6.7 *Die Quotientengruppe $G/[G,G]$ ist abelsch.*

Beweis Es gilt

$$x[G,G]\cdot y[G,G]\cdot(x[G,G])^{-1}\cdot(y[G,G])^{-1} = xyx^{-1}y^{-1}[G,G] = [G,G] \ .$$

Damit ist jeder Kommutator in $G/[G,G]$ trivial und $G/[G,G]$ ist abelsch.

Satz 6.8 *Ist A eine abelsche Gruppe und $\phi : G \to A$ ein Homomorphismus, dann gilt $[G,G] \subseteq \ker\phi$.*

Beweis Es gilt für alle $a, b \in G$

$$\phi([a,b]) = \phi a \cdot \phi b \cdot \phi(a^{-1}) \cdot \phi(b^{-1}) = e \ .$$

Damit folgt $[G,G] \subseteq \ker\phi$.

I.7 Isomorphiesätze

Es sei $\phi : G \to H$ homomorph, und es sei K ein Normalteiler von G mit $K \subseteq \ker\phi$. Wir betrachten die Nebenklassen $aK = \{au \mid u \in K\}$. Auf allen Elementen von aK nimmt ϕ den gleichen Wert an, nämlich $\phi(a') = \phi(au) = \phi(a)\cdot\phi(u) = \phi(a)\cdot e_H = \phi(a)$. Es gibt deshalb eine Abbildung $\psi : G/K \to H$ definiert durch $\psi(aK) = \phi(a)$.

Behauptung ψ ist homomorph.
Beweis Es gilt $\psi(aK \cdot bK) = \psi(abK) = \phi(a \cdot b) = \phi a \cdot \phi b = \psi(aK) \cdot \psi(bK)$.

$$\begin{array}{lll} G & \stackrel{\phi}{\to} & H \\ \pi \downarrow & \nearrow \psi & \\ G/K & & \end{array} \qquad \begin{array}{l} \phi = \psi \circ \pi \\ \text{“}\phi \text{ faktorisiert über } \pi\text{”} \end{array}$$

Wir stellen fest: Genau dann ist $\psi : G/K \to H$ injektiv, wenn gilt $K = \ker \phi$.

Satz 7.1 (1. Isomorphiesatz) *Es sei $\phi : G \to H$ homomorph. Dann induziert ϕ einen Isomorphismus*

$$\psi : G/\ker \phi \stackrel{\sim}{\to} \operatorname{im} \phi \ , \quad \psi(x \ker \phi) = \phi(x) \ .$$

Beispiele
(a) Es sei $\phi : G \to A$ ein Homomorphismus mit A abelsch. Dann ist, nach einer Bemerkung im Abschnitt 6, die Kommutatoruntergruppe $[G, G]$ in $\ker \phi$ enthalten.

$$\begin{array}{ccc} G & \stackrel{\phi}{\to} & H \\ \pi \downarrow & \nearrow \psi & \\ G/[G,G] & & \end{array}$$

Wir entnehmen dieser Überlegung: *Jeder von G ausgehende Homomorphismus in eine abelsche Gruppe A faktorisiert über die kanonische Projektion $\pi : G \to G/[G, G]$.* Die Gruppe $G/[G, G]$ ist in diesem Sinne der grösste abelsche Quotient von G. Sie heisst deshalb oft auch die “abelsch gemachte Gruppe” von G.

(b) Es sei $x \in H$. Wir definieren $\phi : \mathbb{Z} \to H$ durch $\phi(x) = x^m$. Dann ist $\ker \phi = |x|\mathbb{Z}$, und man erhält den Isomorphismus $\psi : \mathbb{Z}/|x|\mathbb{Z} \stackrel{\sim}{\to} \langle x \rangle$.

(c) Unter der Zusammensetzung bilden die Automorphismen einer Gruppe G ihrerseits eine Gruppe, die wir mit $\operatorname{Aut}(G)$ bezeichnen. Die Zuordnung χ, die einem Gruppenelement x den zu x gehörigen inneren Automorphismus ϕ_x von G zuordnet, also die Abbildung $\chi : G \to \operatorname{Aut}(G)$ definiert durch $\chi(x) = \phi_x$, $\phi_x(a) = xax^{-1}$, ist homomorph. Es gilt nämlich $\chi(xy)(a) = \phi_{xy}(a) = xya(xy)^{-1} = xyay^{-1}x^{-1} = \phi_x(\phi_y(a)) = \phi_x \circ \phi_y(a) = (\chi(x) \circ \chi(y))(a)$.

Wir wenden den Isomorphiesatz auf χ an. Wir definieren $\operatorname{im}\chi = \{\phi_x \mid x \in G\} = \operatorname{Inn} G$. Dies ist die Untergruppe der innern Automorphismen in Aut G. Für den Kern von χ, erhalten wir

$$\begin{aligned}\ker\chi &= \{x \in G \mid \phi_x = 1_G\} = \{x \in G \mid xax^{-1} = a \text{ für alle } \ a \in G\} \\ &= \{x \in G \mid xa = ax \text{ für alle } \ a \in G\} = ZG\ .\end{aligned}$$

Der 1. Isomorphiesatz liefert dann den Isomorphismus $\chi_* : G/ZG \xrightarrow{\sim} \operatorname{Inn} G$.

Es sei N ein Normalteiler in G, $N \lhd G$, $\pi : G \to G/N$ die kanonische Projektion und $H \subseteq G$ eine Untergruppe. Wir betrachten $\pi|_H : H \to G/N$.

$$\begin{aligned}\ker\pi|_H &= \{a \in H \mid aN = N\} = H \cap N\ , \\ \operatorname{im}\pi|_H &= \{bN \mid b \in H\} = HN/N\ .\end{aligned}$$

Die Anwendung des 1. Isomorphiesatzes auf diese Situation liefert den Isomorphismus

$$(\pi|_H)_* : H/H \cap N \xrightarrow{\sim} HN/N\ .$$

Satz 7.2 (2. Isomorphiesatz) *Es sei N ein Normalteiler von G und H eine Untergruppe von G. Dann induziert $\pi : G \to G/N$ einen Isomorphismus*

$$\pi_* : H/H \cap N \xrightarrow{\sim} HN/N\ , \qquad \pi_*(h(H \cap N)) = hN\ .$$

Beispiele

(d) Es sei G die Bewegungsgruppe der Ebene, und es bezeichne O den Ursprung der Ebene. Jedes Element $b \in G$ ist gegeben durch das Bild des Ursprungs $b(O)$ und dem Drehwinkel β. Es sei nun T die Untergruppe der Translationen (Drehwinkel 0), und D die Untergruppe der Drehungen um O. Wir stellen leicht fest, dass T ein Normalteiler in G ist. Ist nämlich $t \in T$, so hat xtx^{-1} den Drehwinkel 0 und ist deshalb eine Translation. Wir behaupten nun $G = T \cdot D$. Um dies einzusehen, betrachten wir $b \in G$ mit $b(O) = P$ und Drehwinkel β. Dann ist $b = t \cdot d$, wo $d \in D$ die Drehung um den Winkel β und $t \in T$ die Translation mit $t(O) = P$ bezeichnet. Ferner gilt, mit Hilfe des zweiten Isomorphiesatzes, angewandt auf die Projektion $\pi : B \to B/T$: $D = D/D \cap T \cong DT/T = B/T$.

(e) Wir klären in diesem Beispiel mit Hilfe der Isomorphiesätze die Struktur der Gruppe S_4 auf. Die Parität liefert einen surjektiven Gruppenhomomorphismus sign: $S_4 \to C_2$. Der

Kern von sign ist definitionsgemäss die alternierende Gruppe A_4. Nach dem 1. Isomorphiesatz gilt dann $S_4/A_4 \cong C_2$. Wir betrachten nun die Konjugationsklasse K in G, die aus allen Doppeltranspositionen besteht, d.h. $K = \{(1,2)(3,4), (1,3)(2,4), (1,4)(2,3)\}$. Natürlich gilt $K \subset A_4$. Es ist nicht schwierig zu zeigen, dass K zusammen mit e eine zur Kleinschen Vierergruppe isomorphe Untergruppe V von A_4 ist. Als Vereinigung von Konjugationsklassen ist V sogar ein Normalteiler von S_4 und damit *a fortiori* auch von A_4. Um die Struktur des Quotienten S_4/V zu bestimmen, betrachten wir die Untergruppe S_3 von S_4. Natürlich ist $S_3 \cap V = \{e\}$. Mit dem 2. Isomorphiesatz, angewandt auf die Projektion $\pi : S_4 \to S_4/V$ und $H = S_3$, erhält man dann

$$S_3 = S_3/S_3 \cap V \xrightarrow{\sim} VS_3/V \ .$$

Wegen $|S_3| \cdot |V| = |VS_3|$ enthält VS_3 24 Elemente. Es gilt folglich $VS_3 = S_4$, und der obige Isomorphismus liefert $S_4/V \cong S_3$. Daraus folgt auch das Resultat $A_4/V = C_3$, welches allerdings auf anderen Wegen einfacher zu erhalten ist.

Es sei N ein Normalteiler in G, $N \lhd G$, und $\pi : G \to G/N$ die zugehörige kanonische Projektion. Es sei M ein weiterer Normalteiler in G mit $N \subseteq M$. Dann ist $\pi M = M/N$ ein Normalteiler in G/N. Für die Zusammensetzung

$$\sigma : G \to G/N \to (G/N)/(M/N)$$

berechnet man $\ker \sigma = M$. Dies liefert den folgenden Satz.

Satz 7.3 (3. Isomorphiesatz) *Es sei $N \lhd G$, $M \lhd G$ und $N \subseteq M$. Dann gilt*

$$\psi : G/M \xrightarrow{\sim} (G/N)/(M/N) \ .$$

I.8 Transformationsgruppen

Es sei Ω eine beliebige Menge. Die Menge der bijektiven Abbildungen von Ω bilden eine Gruppe $S(\Omega)$, die *symmetrische Gruppe* von Ω.

Definition Man sagt, eine Gruppe G *operiere* auf der Menge Ω, wenn ein Homomorphismus $\Phi : G \to S(\Omega)$ gegeben ist.

Es ist dann $\Phi_x = \Omega \to \Omega$ eine bijektive Abbildung von Ω, und es gilt $\Phi_e = 1_\Omega$ und $\Phi_{xy} = \Phi_x \circ \Phi_y$. Man spricht deshalb auch von einer *Permutationsdarstellung* von G.

Beispiele
(a) Natürlich operiert $G = S(\Omega)$ auf Ω via $\Phi = 1_{S(\Omega)}$.

(b) Es seien C die unendliche zyklische Gruppe, t ein erzeugendes Element von C und $\Omega = \{1, 2, 3\}$. Der Homomorphismus $\Phi : C \to S_3 = S(\Omega)$ gegeben durch $t \mapsto (1, 2, 3)$ ist eine Permutationsdarstellung von C: Das Element t operiert auf $\{1, 2, 3\}$ durch zyklische Vertauschung.

Definition Der Kern des Homomorphismus Φ, $\ker \Phi$, heisst *Kern der Permutationsdarstellung*. Ist $\ker \Phi = \{e\}$, so sagt man, G operiere *treu* (oder *effektiv*). Ein solches G heisst auch etwa *Transformationsgruppe*. Natürlich ist $G/\ker \Phi$ eine Transformationsgruppe von Ω.

(c) Es sei $\Omega = V$ ein Vektorraum über dem Körper k. Die Gruppe G der regulären linearen Selbstabbildungen operiert in offensichtlicher Weise auf Ω. Die Operation ist treu.

(d) Es sei $\Omega = X$ ein topologischer Raum. Die Gruppe G der Homöomorphismen von X operiert auf X.

(e) Transformationsgruppen werden oft durch Invarianzbedingungen festgelegt. So ist zum Beispiel $\mathrm{O}(n)$ die Gruppe der linearen Transformationen des Vektorraumes $\mathbb{R}^n$, welche das Standardskalarprodukt invariant lassen. Die Lorentzgruppe, die in der speziellen Relativitätstheorie eine zentrale Rolle spielt, ist die Transformationsgruppe des Vektorraumes $\mathbb{R}^4$, welche das "Skalarprodukt"

$$v_1^2 + v_2^2 + v_3^2 - v_4^2$$

invariant lässt.

Umgekehrt kann man fragen, was für Eigenschaften unter einer gegebenen Transformationsgruppe invariant bleiben. Zum Beispiel bleibt unter der Bewegungsgruppe der Ebene die Kongruenz von ebenen Figuren erhalten, die Eigenschaften, die unter der Gruppe der Kollineationen der Ebene invariant bleiben, bilden den Gegenstand der ebenen projektiven Geometrie, usw. Dies ist die Hauptidee des "Erlanger Programmes" von Felix Klein (1872): "Es ist eine Mannigfaltigkeit[2] und in derselben eine Transformationsgrup-

[2]Es ist hier anzumerken, dass der Begriff 'Mannigfaltigkeit' erst um 1920 herum seine heute übliche Bedeutung erhielt. So benutzte Georg Cantor noch 1880 das Wort 'Mannigfaltigkeit', um im wesentlichen das zu bezeichnen, wofür wir heute das Wort 'Menge' verwenden.

pe gegeben; man solle die der Mannigfaltigkeit angehörigen Gebilde hinsichtlich solcher Eigenschaften untersuchen, die durch die Transformationen der Gruppe nicht geändert werden." (Siehe Felix Klein: Gesammelte Mathematische Abhandlungen. Springer 1921. Erster Band, 460-497. Das Zitat ist auf Seite 463 zu finden.)

(f) Es sei $G = S_3$ und $\Omega = \mathbb{C}^2$. Die Abildung $\Phi : S_3 \to S(\Omega)$ ist wie folgt gegeben. Wir ordnen dem Element $\sigma = (1, 2, 3)$ die durch die Matrix

$$\begin{bmatrix} 0 & -1 \\ 1 & -1 \end{bmatrix}$$

vermittelte lineare Selbstabbildung von $\mathbb{C}^2$ zu, und dem Element $\tau = (1, 2)$ die durch die Matrix

$$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

vermittelte. Wie man leicht sieht, gibt diese Festsetzung Anlass zu einem Homomorphismus $\Phi' : S_3 \to \mathrm{GL}(2, \mathbb{C})$. Die Permutationen der Menge $\Omega = \mathbb{C}^2$ sind in diesem Beispiel also sogar als $\mathbb{C}$-lineare Selbstabbildungen realisiert. Allgemein heisst ein Gruppenhomomorphismus $\rho : G \to \mathrm{GL}(n, \mathbb{C})$ eine (komplexe) Darstellung von G vom Grad n. Auf die wichtige und umfangreiche Theorie derartiger Darstellungen wird in Kapitel V des vorliegenden Textes näher eingegangen.

Definition Es sei $\Phi : G \to S(\Omega)$ gegeben, und es sei $a \in \Omega$. Die Menge $H_a = \{x \in G \mid \Phi_x(a) = a\}$ ist eine Untergruppe von G. Natürlich operiert H_a wiederum auf Ω. Der Punkt a bleibt dabei fest. Die Untergruppe H_a heisst deshalb *Stabilisator* oder *Isotropieuntergruppe* von a.

(g) Die Gruppe $\mathrm{SO}(2)$ operiert auf den regulären Dreiecken mit Schwerpunkt in O. Die Isotropieuntergruppe *eines* Dreiecks ist die Symmetriegruppe dieses Dreiecks, sie ist also isomorph zu $D_{2\cdot 3}$.

(h) Es sei $\Phi : S_3 \to S(\{1, 2, 3\})$ die Identität. Der Stabilisator des Elementes 1 ist $\langle (2, 3) \rangle$.
Definition Es operiere G auf Ω. Wir definieren eine Relation in der Menge Ω wie folgt:

$$a \sim b \Leftrightarrow \text{es existiert } x \in G \text{ mit } \Phi_x(a) = b.$$

Behauptung Die durch "$\sim$"gegebene Relation ist eine Äquivalenzrelation auf Ω.
Beweis (i) $a \sim a$. Denn es gilt $\Phi_e(a) = a$.
(ii) $a \sim b, b \sim a$. Denn aus $\Phi_x a = b$ folgt $\Phi_x^{-1} b = a$.

(iii) $a \sim b, b \sim c$, dann folgt $a \sim c$. Denn aus $\Phi_x(a) = b$ und $\Phi_y(b) = c$ folgt $\Phi_y \circ \Phi_x(a) = \Phi_{yx}(a) = c$.

Definition Die Äquivalenzklassen von Ω unter der Operation von G heissen *Bahnkurven* (englisch: *orbits*) unter G.

Trivialerweise folgt daraus, dass sich die Menge Ω als disjunkte Vereinigung von Bahnkurven schreiben lässt.

(i) Es sei $\Phi : S_3 \to S_4 = S(\{1, 2, 3, 4\})$. Die Bahnkurven dieser Operation sind $\{1, 2, 3\}$ und $\{4\}$.

Definition Die Operation von G auf Ω heisst *transitiv*, wenn Ω selbst eine Bahnkurve ist.

Um die Schreibweise zu vereinfachen, setzen wir im folgenden gewöhnlich $\Phi_x(a) = xa$.

Es seien $a, b \in \Omega$ in der gleichen Bahnkurve. Dann existiert $x \in G$ mit $xa = b$. Ferner sei $y \in H_a$. Dann gilt

$$xyx^{-1}(b) = xy(a) = xa = b \ .$$

Das heisst, es gilt $xyx^{-1} \in H_b$. Die Zuordnung $y \mapsto xyx^{-1}$, also der zu x gehörige innere Automorphismus, bildet H_a in H_b ab. Da die inverse Abbildung durch x^{-1} gegeben ist, ist diese Zuordnung ein Isomorphismus $\phi_x : H_a \xrightarrow{\sim} H_b$.

Satz 8.1 *Es seien a, b Elemente der selben Bahnkurve. Dann gehen die Isotropieuntergruppen von a und b durch einen innern Automorphismus in G auseinander hervor. Insbesondere sind sie isomorph.*

(k) Es sei G die Bewegungsgruppe der Ebene. Der Stabilisator des Punktes P sei D_P. Es gilt $T \circ D_P \circ T^{-1} = D_Q$, wo T die Translation ist, die P in Q überführt (oder irgend eine Bewegung, die P in Q überführt).

Als Nächstes wenden wir uns der Frage zu, wieviele Elemente eine Bahnkurve enthält.

Es sei $c \in \Omega$. Die Bahnkurve, die c enthält, ist die Menge $\{xc \mid x \in G\} \subseteq \Omega$. Es gilt

$$yc = xc \Leftrightarrow x^{-1}y(c) = c \Leftrightarrow x^{-1}y \in H_c \Leftrightarrow xH_c = yH_c \ .$$

Daraus ergibt sich der folgende Satz

Satz 8.2 *Die Punkte in der Bahnkurve, in der c liegt, entsprechen eineindeutig den (Links-) Nebenklassen von G modulo H_c. Ist G endlich, so ist folglich die Anzahl Elemente in einer Bahnkurve ein Teiler der Gruppenordnung von $|G|$.*

Beispiel Es sei W die Symmetriegruppe des Würfels. Dann operiert W transitiv auf der Menge Ω bestehend aus den 8 Ecken des Würfels. Greift man eine Ecke A des Würfels heraus, so gibt es in W offenbar 3 Elemente, die A festlassen, nämlich die Drehungen um 0, $2\pi/3$ und $4\pi/3$ um die Würfeldiagonale durch A. Die Bahnkurve von A besteht folglich aus 8 Elementen und der Stabilisator von A hat die Ordung 3. Aus dieser einfachen Überlegung ergibt sich mit dem Satz 8.2 die Ordnung von G als $|G| = 3 \cdot 8 = 24$. – Auf ganz analoge Weise sieht man, dass die Symmetriegruppe P des Pentagondodekaeders 60 beträgt: Die Gruppe P operiert transitiv auf der Menge der 20 Eckpunkte und der Stabilisator eines Eckpunktes besteht aus den Drehungen um 0, $2\pi/3$ und $4\pi/3$ um die Diagonale des Dodekaeders durch diesen Eckpunkt.

Im Folgenden diskutieren wir noch einige weitere **Beispiele** von Gruppenoperationen, die zu interessanten Folgerungen führen.

(a) Wir betrachten eine Operation der Gruppe G auf der Menge $\Omega = G$. Dem Gruppenelement $x \in G$ wird die Abbildung $\Phi_x : G \to G$ zugeordnet: $\Phi_x(a) = xa$. Offenbar ist Φ_x bijektiv, denn es gilt $x(x^{-1}b) = b$ und aus $xa = xb$ folgt $a = b$. Man sagt, G operiere durch *Linkstranslation* auf sich selbst. Offensichtlich ist $\ker \Phi = \{e\}$. Aus unseren Sätzen über Transformationsgruppen folgt somit

Satz 8.3 (Satz von Cayley) *Jede Gruppe G lässt sich auffassen als Untergruppe von $S(G)$.*

(b) Wie betrachten wiederum eine Operation von G auf der Menge $\Omega = G$: Die Abbildung $\phi_x : G \to G$ ist in diesem Beispiel definiert durch $\phi_x(a) = xax^{-1}$. Wir wissen bereits, dass die Konjugation ϕ_x bijektiv ist und dass die Zuordnung $x \to \phi_x$ homomorph ist.

Die Bahnkurven unter dieser Operation sind definitionsgemäss die Klassen konjugierter Elemente von G:

$$a \sim b <=> \text{ es existiert } x \in G \text{ mit } xax^{-1} = b \ .$$

Es folgt, dass man G als disjunkte Vereinigung von Klassen konjugierter Elemente darstellen kann. Die Anzahl Elemente in einer Bahnkurve ist gleich dem Index in G des

Stabilisators H_a eines Elementes a in dieser Bahnkurve, $H_a = \{x \in G \mid xax^{-1} = a\}$. Die Untergruppe H_a von G heisst der *Zentralisator* von a. Es gilt nun Folgendes:

- Ist $a \in ZG$, so ist $H_a = G$, das heisst $[G : H_a] = 1$.
- Ist $a \notin ZG$, so ist H_a eine *echte* Untergruppe und $[G : H_a]$ ist ein *echter* Teiler von $|G|$.

Für die Menge G erhalten wir die Darstellung $G = ZG \cup K_1 \cup \cdots \cup K_k$, wo K_i die verschiedenen nichttrivialen Konjugationsklassen durchläuft. Für die Ordnung von G liefert dies:

$$|G| = |ZG| + h_1 + h_2 + \cdots + h_k$$

mit $h_i = [G : H_{a_i}]$ für a_i aus der Konjugationsklasse K_i. Es gilt also $h_i \geq 2$. Damit haben wir die sogenannte Klassengleichung bewiesen.

Satz 8.4 (Klassengleichung) *Es sei G endlich. Dann gilt*

$$|G| = |ZG| + \sum h_i \ ,$$

wo $h_i \mid |G|$ und $h_i \geq 2$.

Diese Klassengleichung hat viele interessante Anwendungen; die wohl bekannteste ist die folgende.

Es sei $\{e\} \neq G$ eine p-Gruppe, das heisst, die Ordnung von G ist eine Primzahlpotenz, $|G| = p^n$, p prim. Dann gilt $h_i = p^{n_i}$, $n_i \geq 1$. Folglich erhalten wir

$$p^n = |G| = |ZG| + \sum p^{n_i} = |ZG| + pm \ , \quad m \neq 0 \ .$$

Daraus folgt sofort $p \mid |ZG|$, insbesondere $ZG \neq \{e\}$.

Satz 8.5 *Es sei G eine p-Gruppe, $|G| = p^n$, $n \geq 1$, p prim. Dann ist $ZG \neq \{e\}$; das Zentrum einer p-Gruppe ist nicht trivial.*

(c) Die Sätze von Sylow. Der Satz von Lagrange kann als arithmetische Bedingung für die Existenz von Untergruppen einer endlichen Gruppe G angesehen werden. Ist nämlich H eine Untergruppe von G, so teilt die Ordnung von H die Ordnung von G. Es stellt sich im Anschluss daran die Frage, ob zu jedem Teiler der Gruppenordnung auch eine

entsprechende Untergruppe existiert. Das Beispiel A_4 zeigt, dass dies im allgemeinen nicht der Fall ist, denn A_4 besitzt keine Untergruppe der Ordnung 6. Andererseits gilt – wie leicht zu zeigen ist – diese Aussage für zyklische Gruppen: *Es sei G zyklisch, und d teile die Ordnung von G. Dann existiert eine Untergruppe $U \subseteq G$ mit $|U| = d$.* Die Sätze von Sylow geben für bestimmte Teiler der Gruppenordnung Auskunft über die Existenz, Struktur und Anzahl von Untergruppen.

Wir beweisen als erstes das folgende Lemma, welches einen Spezialfall des sogenannten Satzes von Cauchy beinhaltet. (Letzterer besagt, dass die Aussage des folgenden Lemmas für beliebige Gruppen (nicht nur für abelsche) richtig ist.)

Lemma 8.6 *Es sei p eine Primzahl und A eine abelsche Gruppe deren Ordung $|A|$ von p geteilt werde. Dann existiert $a \in A$ mit $|a| = p$.*

Beweis Wir führen den Beweis mit Induktion. Wähle $a \in A$ mit $a \neq e$. 1. Fall: Ist $p \mid |a|$, so gibt es in der zyklischen Gruppe $\langle a \rangle$ ein Element der Ordnung p. 2. Fall: Ist $p \nmid |a|$, so betrachte man die Faktorgruppe A/N mit $N = \langle a \rangle$. Deren Ordnung wird von p geteilt. Da diese Ordnung auch echt kleiner ist als $|A|$, können wir nach Induktion schliessen, dass ein Element $bN \in A/N$ existiert, dessen Ordnung von p geteilt wird. Daraus folgt, dass p auch die Ordnung von b teilt, und die Aussage des Lemmas ergibt sich wie im Fall 1.

Es sei G eine beliebige Gruppe, deren Ordnung von der Primzahl p geteilt wird; wir schreiben $|G| = p^n q$, wo p und q teilerfremd sind.

Satz 8.7 (1. Satz von Sylow) *Es existiert in G eine Untergruppe P mit $|P| = p^n$. (P heisst eine* p-Sylow Untergruppe *von G.)*

Beweis Wir führen den Beweis mit Induktion nach der Gruppenordnung $|G|$. Dazu benützen wir die Klassengleichung von G; sie lautet $|G| = |ZG| + \sum h_i$ mit $h_i \geq 2$ und $h_i \mid |G|$. Wir unterscheiden die folgenden zwei Fälle.

1. Fall: Es sei p ein Teiler von $|ZG|$. Nach dem Lemma 8.6 existiert $C_p \subseteq ZG$. Als Untergruppe von ZG ist C_p ein Normalteiler in G. Die Gruppe $H = G/C_p$ besitzt die Ordnung $p^{n-1}q$. Nach Induktion gibt es in H eine Untergruppe $\overline{P}$ der Ordnung p^{n-1}. Das volle Urbild P von $\overline{P}$ unter der Projektion $G \to G/C_p$ besitzt die Ordnung p^n.

2. Fall: Es sei p kein Teiler von $|ZG|$. Dann muss ein i existieren, so dass p kein Teiler von h_i ist. Nun ist h_i der Index einer Untergruppe H_a, und daraus folgt $|H_a| = p^n \cdot \overline{q}$ mit $\overline{q} < q$. Nach Induktion existiert $P \subseteq H_a$ mit $|P| = p^n$. Dies war zu beweisen.

Satz 8.8 (2. Satz von Sylow) *Es seien P, Q zwei p-Sylow Untergruppen von G. Dann existiert $y \in G$ mit $y^{-1}Qy = P$.*

Beweis Wir betrachten die Menge Ω der Nebenklassen yP von G bezüglich P und die Operation von Q auf Ω definiert durch

$$x \cdot (yP) = xyP \ , \quad x \in Q \ .$$

Da Q eine p-Gruppe ist, ist die Anzahl der Elemente in einer Bahnkurve eine Potenz von p. Es gilt folglich

$$|\Omega| = \frac{|G|}{|P|} = q = p^{k_1} + p^{k_2} + \cdots + p^{k_l} \ .$$

Da p kein Teiler von q ist, muss mindestens eines der k_i Null sein. Damit existiert eine Nebenklasse yP mit $xyP = yP$ für alle $x \in Q$. Daraus folgt $y^{-1}xy \in P$ für alle $x \in Q$, das heisst $y^{-1}Qy \subseteq P$. Da Q und P beide p^n Elemente enthalten, gilt $y^{-1}Qy = P$. Dies war zu beweisen.

Satz 8.9 (3. Satz von Sylow) *Für die Anzahl N verschiedener p-Sylow Untergruppen von G gilt $N \equiv 1$ modulo p.*

Aus diesem Satz, den wir hier *ohne Beweis* erwähnen, folgt, dass die Anzahl N der p-Sylow Untergruppen von der Form $1 + kp$ ist. Es ist eine bis heute offene Frage, welche Zahlen k in dieser Gleichung wirklich auftreten können.

I.9 Direkte Produkte

Definition Es seien A, B zwei (multiplikativ geschriebene) Gruppen. Die Gruppe $G = A \times B$, das (externe) *direkte Produkt* von A und B ist wie folgt definiert:

Elemente: $(a, b), \quad a \in A, b \in B$

Operation: $(a, b) \cdot (a', b') = (aa', bb'), \quad a, a' \in A, \ b, b' \in B \ .$

Das Neutralelement ist gegeben durch (e_A, e_B) und das Inverse durch $(a, b)^{-1} = (a^{-1}, b^{-1})$.

In $G = A \times B$ gibt es ausgezeichnete Normalteiler, nämlich $H = \{(a, e_B) \mid a \in A\} \cong A$ und $K = \{(e_A, b) \mid b \in B\} \cong B$. Ferner gibt es Projektionen $G \to G/H \cong B$ und

$G \to G/K \cong A$. Jedes Element in $A \times B$ lässt sich in eindeutiger Weise schreiben als $(a, e_B)(e_A, b)$, d.h. als Produkt eines Elementes in H und eines Elementes in K.

Definition Eine Gruppe G heisst (internes) *direktes Produkt* ihrer Untergruppen A und B, wenn es einen Isomorphismus $\psi : G \to A \times B$ gibt mit $\psi|_A : A \to H$ und $\psi|_B : B \to K$.

Satz 9.1 *Genau dann ist G (internes) direktes Produkt ihrer Untergruppen A und B, wenn gilt* (i) $AB = G$, (ii) $A \cap B = \{e\}$, (iii) *A, B sind Normalteiler in G.*

Beweis Die eine Richtung ist nach obigem klar. Es seien also die drei Eigenschaften (i), (ii), (iii) erfüllt. Wir müssen einen Isomorphismus $\psi : G \to A \times B$ konstruieren. Wir zeigen zuerst, dass sich jedes Element $x \in G$ in eindeutiger Weise als Produkt ab schreiben lässt mit $a \in A$ und $b \in B$. Nach (i) existiert eine derartige Darstellung. Ist nun $x = ab = a_1 b_1$ mit $a, a_1 \in A$ und $b, b_1 \in B$, so folgt $a_1^{-1} a = b_1^{-1} b \in A \cap B$. Wegen (ii) impliziert dies $a_1^{-1} a = b_1^{-1} b = e$, also $a_1 = a$ und $b_1 = b$. Wir definieren jetzt $\psi : G \to A \times B$ durch $\psi(x) = \psi(ab) = (a, b)$. Dies ist ein Homomorphismus wegen $ab = ba$ für $a \in A$ und $b \in B$. Letzteres ergibt sich, indem man den Kommutator $aba^{-1}b^{-1}$ betrachtet und (iii) berücksichtigt. In der Tat liegt Kommutator wegen $(aba^{-1})b^{-1}$ in B und wegen $a(ba^{-1}b^{-1})$ in A, und es folgt mit (ii) $[a, b] = e$.

Es ist klar, dass der Begriff des direkten Produktes auf mehr als zwei Faktoren ausgedehnt werden kann. Wir verzichten hier auf die Behandlung der notwendigen Einzelheiten. Anzumerken ist ferner, dass man bei additiv geschriebenen Gruppen nicht von einem direkten *Produkt* sondern von einer direkten *Summe* $A \oplus B$ der beiden Gruppen A und B sprechen wird.

Beispiel
(a) Es sei $G = C_r \times C_s$ mit r, s teilerfremd. Dann gilt $G = C_{rs}$. In der Tat ist $|G| = rs$. Falls c und d erzeugende Elemente der Gruppen C_r bzw. C_s sind, so ist offenbar (c, d) in $C_r \times C_s$ ein Element der Ordnung rs. Es erzeugt also die ganze Gruppe $C_r \times C_s$.

Dieses Beispiel kann man stark verallgemeinern. Es gilt der Satz:

Satz 9.2 *Es sei A eine abelsche (additiv geschriebene) Gruppe der Ordung n. Dann ist A die direkte Summe ihrer Sylowuntergruppen $A(p)$, die zu den Primteilern p von n gehören.*

Beweis Wir beweisen hier nur den Fall, wo n nur zwei Primteiler p und q besitzt, wo also gilt $n = p^r \cdot q^s$. Der allgemeine Fall wird analog bewiesen. Gemäss Satz 8.7 existiert eine

p-Sylowuntergruppe P der Ordung p^r und eine q-Sylowuntergruppe Q der Ordnung q^s. Da A abelsch ist, sind P und Q Normalteiler in A. Ferner gilt offenbar $P \cap Q = 0$, denn ein Element im Durchschnitt muss eine Ordung besitzen, die gleichzeitig eine p- und eine q-Potenz ist. Schliesslich folgt auch $P+Q = A$, denn es gilt $|P+Q| = |P| \cdot |Q| = p^r \cdot q^s = |A|$.

In diesem Zusammenhang ist der wichtige sogenannte *Fundamentalsatz für endliche abelsche Gruppen* zu erwähnen; er ist wesentlich schwieriger zu beweisen als der Satz 9.2. Er besagt, dass sich jede endliche abelsche Gruppe als direktes Produkt von zyklischen Gruppen schreiben lässt (siehe Korollar IV.5.7). Zusammen mit den obigen Ausführungen ergibt sich daraus, dass die zyklischen Faktoren so gewählt werden können, dass sie Primzahlpotenzordnung besitzen.

Im Falle von unendlich vielen Faktoren muss man zwei verschiedene Bildungen auseinanderhalten; darauf wollen wir hier noch kurz hinweisen.

Es sei $\{A_\nu\}_{\nu \in I}$ eine indizierte Familie von Gruppen. Wir definieren die zwei verschiedenen Gruppen X und $\overline{X}$.

$X = \prod_{\nu \in I} A_\nu$: Elemente: $(a_\nu)_{\nu \in I}$, $a_\nu \in A_\nu$ nur *endlich* viele $a_\nu \neq e$.
Gruppenoperation: komponentenweise.

$\overline{X} = \overline{\prod}_{\nu \in I} A_\nu$: Elemente: $(a_\nu)_{\nu \in I}$, $a_\nu \in A_\nu$.
Gruppenoperation: komponentenweise.

Als konkrete **Beispiele** in additiver Schreibweise erwähnen wir die folgenden:

(b) Sei $A_i = \mathbb{Z}$ für $i = 1, 2, \ldots$. Die Gruppe X heisst dann die freie abelsche Gruppe mit abzählbar unendlich vielen Erzeugenden. Die Gruppe $\overline{X}$ ist wesentlich grösser: Sie enthält überabzählbar viele Elemente, und, wie E. Specker[3] 1950 gezeigt hat, gibt es $\overline{X}$ sogar überabzählbar unendlich viele paarweise nicht isomorphe Untergruppen.

(c) Ein rationaler Vektorraum V von abzählbar unendlicher Dimension ist – aufgefasst als abelsche Gruppe – eine Bildung von der Art X für unendlich viele Kopien des Grundkörpers $\mathbb{Q}$. Der zu V duale Vektorraum V^*, also $\mathrm{Hom}_{\mathbb{Q}}(V, \mathbb{Q})$ – wiederum aufgefasst als abelsche Gruppe – ist eine Bildung der Art $\overline{X}$ für abzählbar unendlich viele Kopien von $\mathbb{Q}$.

[3] Ernst Specker war von 1955 bis 1987 Professor an der ETH Zürich.

Kapitel II. Ringe

Einleitung

Ringe sind in der Mathematik ähnlich omnipräsent wie Gruppen. In Anwendungen spielen dabei erfahrungsgemäss Voraussetzungen eine grosse Rolle, die *zusätzlich* zu den Ringaxiomen gefordert werden: kommutativ, nullteilerfrei, Noethersch, faktoriell und andere. Ringe zeigen aus diesem Grund je nach Gebiet, in dem sie auftreten, sehr variable Erscheinungsformen: ein Polynomring und eine Boolesche Algebra haben einen stark unterschiedlichen 'Charakter'. Aufgabe dieses Kapitels ist es, die einfachsten ringtheoretischen Begriffe einzuführen und an einigen Beispielen ihre Relevanz aufzuzeigen.

Prototyp eines Ringes sind die ganzen Zahlen. E.E. Kummer (1810-1893), L. Kronecker (1823-1891), R. Dedekind (1831-1916) machten im Laufe der Entwicklung der algebraischen Zahlentheorie dann Ringe ganzer Zahlen in algebraischen Zahlkörpern zum Untersuchungsgegenstand; diesbezügliche Stichworte sind Ideale (als Abstraktion 'idealer Zahlen'), Hauptideale, Primideale, eindeutige Primfaktorzerlegung, etc. In der Körpertheorie und dann vor allem in der algebraischen Geometrie traten in natürlicher Weise Polynomringe in einer oder mehreren Unbestimmten auf. Dass die aus der Zahlentheorie stammenden Begriffe sich auch hier als nützlich erwiesen, kann die mit Mathematik etwas Vertrauten nicht überraschen.

Auch einfach aussehende Ringe bergen noch viele Geheimnisse. Die vielen offenen Fragen über Primzahlen oder das Fermatproblem handeln im Grunde genommen vom Ring der ganzen Zahlen. Der erst 1983/84 entdeckte Satz von Mason über den komplexen Polynomring ist ein anderes derartiges Beispiel (siehe Abschnitt II.6).

II.1 Definitionen, Beispiele

Definition Ein *Ring* R ist eine (additiv geschriebene) abelsche Gruppe zusammen mit einem Produkt "$\cdot$", so dass für alle $a, b, c \in R$ gilt

(1) $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ (Assoziativität),

(2) $a \cdot (b + c) = a \cdot b + a \cdot c$ und $(a + b) \cdot c = a \cdot c + b \cdot c$ (Distributivität).

Definition Der Ring R heisst ein *Ring mit Eins*, wenn in R ein Element 1, $1 \neq 0$ existiert, so dass für alle $a \in R$ gilt

(3) $1 \cdot a = a = a \cdot 1$.

Folgerungen

1. Es gilt $a \cdot 0 = 0 = 0 \cdot a$ für alle $a \in R$.

Beweis Aus $a \cdot 0 = a \cdot (0 + 0) = a \cdot 0 + a \cdot 0$ folgt sofort $a \cdot 0 = 0$. [Ebenso für $0 \cdot a = 0$.]

2. Es gilt $a \cdot (-b) = -(a \cdot b) = (-a) \cdot b$.

Beweis Für die linke Gleichung ist $a \cdot b + a \cdot (-b) = 0$ zu zeigen. In der Tat ist $a \cdot b + a \cdot (-b) = a \cdot (b + (-b)) = a \cdot 0 = 0$. [Ebenso für $(-a) \cdot b$.]

3. In einem Ring mit Eins ist das Einselement eindeutig bestimmt.

Beweis Es sei $e \in R$ ein Element mit $e \cdot a = a$ für alle $a \in R$. Dann folgt $e = e \cdot 1 = 1$.

Beispiele

(a) Die ganzen Zahlen $\mathbb{Z}$ bilden einen Ring mit Eins; die geraden Zahlen $2\mathbb{Z}$ bilden einen Ring ohne Eins.

(b) $\mathbb{R}$ ($\mathbb{Q}$, $\mathbb{C}$): die reellen (rationalen, komplexen) Zahlen sind Beispiele von Ringen mit Eins.

Definition Ein Ring R heisst *kommutativ*, wenn für alle $a, b \in R$ gilt

(4) $a \cdot b = b \cdot a$.

Beispiele

(c) Die komplexen $n \times n$-Matrizen $\mathbb{M}_n(\mathbb{C})$ bilden einen Ring mit Eins, der für $n \geq 2$ nicht kommutativ ist.

(d) $\mathbb{Z}_m = \mathbb{Z}/m\mathbb{Z}$ zusammen mit der Multiplikation $(a + m\mathbb{Z}) \cdot (b + m\mathbb{Z}) = a \cdot b + m\mathbb{Z}$ ist ein kommutativer Ring mit Eins.

Definition Ein Element $0 \neq a \in R$ heisst ein *Linksnullteiler*, wenn $0 \neq b \in R$ existiert mit $a \cdot b = 0$. Analog wird ein Rechtsnullteiler definiert.

Beispiele

(e) Der Ring $\mathbb{M}_n(\mathbb{C})$ besitzt für $n \geq 2$ sowohl Links- wie auch Rechtsnullteiler.

(f) Es sei $m \geq 2$. Genau dann hat der Ring $\mathbb{Z}_m$ Nullteiler, wenn m keine Primzahl ist.

Definition Ein kommutativer Ring mit Eins und ohne Nullteiler heisst *Integritätsbereich* oder einfach *Bereich*.

4. Es sei R ein Integritätsbereich. Dann folgt aus $a \cdot b = a \cdot b'$ und $a \neq 0$ stets $b = b'$.

Beweis Aus $a \cdot b = a \cdot b'$ folgt $a \cdot (b - b') = 0$, also $b - b' = 0$ und damit $b = b'$.

Definition Es sei R ein Ring mit Eins. Das Element $a \in R$ heisst eine *Einheit*, wenn $b \in R$ existiert mit $a \cdot b = b \cdot a = 1$.

Satz 1.1 *Die Einheiten in einem Ring R bilden unter der Ringmultiplikation eine Gruppe, die wir mit $U(R)$ bezeichnen.*

Beispiele

(g) Die Einheiten in $\mathbb{Z}$ sind $+1, -1$. Das Einselement ist immer eine Einheit. In einem Körper K sind die Nichtnullelemente Einheiten, $U(K) = K^\bullet$.

(h) Die Einheiten in $\mathbb{M}_n(\mathbb{C})$ sind die regulären $n \times n$ Matrizen, also $U(\mathbb{M}_n(\mathbb{C})) = \mathrm{GL}(n, \mathbb{C})$.

(i) Die Einheiten in $\mathbb{Z}_m$ sind die zu m teilerfremden Restklassen modulo m.

Beweis Wir wissen bereits, dass die zu m teilerfremden Restklassen unter der Multiplikation eine Gruppe bilden. Insbesondere existiert also zu jeder solchen Restklasse ein Inverses. Es sei umgekehrt a *nicht* teilerfremd zu m, $(a, m) = d \neq 1$. Dann ist a ein Nullteiler. Setzt man nämlich $b = m/d$, so ist $(a + m\mathbb{Z}) \cdot (b + m\mathbb{Z}) = a \cdot m/d + m\mathbb{Z} = m\mathbb{Z}$. Nun gilt: Ein Nullteiler ist keine Einheit. Wäre nämlich a eine Einheit mit Inversem c und zugleich ein Nullteiler, $a \cdot b = 0$, so hätte man $b = 1 \cdot b = c \cdot a \cdot b = c \cdot 0 = 0$, im Widerspruch zur Voraussetzung $b \neq 0$.

Definition Ein Ring mit Eins, in dem alle von 0 verschiedenen Elemente Einheiten sind, heisst *Schiefkörper* oder *Divisionsring*. Ein kommutativer Divisionsring heisst ein *Körper*.

Beispiele $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ sind Körper, $\mathbb{H}$ (siehe Beispiel (a) unten) ist ein Schiefkörper. $\mathbb{Z}_m$ ist genau dann ein Körper, wenn m eine Primzahl ist.

Ein Körper K mit $\mathbb{Q} \subseteq K \subseteq \mathbb{C}$, dessen additive Gruppe ein endlich dimensionaler Vektorraum über $\mathbb{Q}$ ist, heisst *Zahlkörper*. Ist K ein derartiger Zahlkörper, so ist der *Ring der ganzen Zahlen* in K ein für die algebraische Zahlentheorie zentrales Objekt. Im Rahmen dieses Textes können wir nicht näher auf diese Begriffsbildungen eingehen. Trotzdem erwähnen wir die folgenden Beispiele – man fasse dabei die linken Seiten einfach als abstrakte Bezeichnungen auf:

$$\begin{aligned}\mathbb{Z}[i] &= \{a + ib \mid a, b \in \mathbb{Z}\} \ , \\ \mathbb{Q}(\sqrt{2}) &= \{a + \sqrt{2}b \mid a, b \in \mathbb{Q}\} \ , \\ \mathbb{Z}[\sqrt{2}] &= \{a + \sqrt{2}b \mid a, b \in \mathbb{Z}\} \ .\end{aligned}$$

Man beachte, dass Unterringe eines Körpers immer Integritätsbereiche sind.

Es sei R ein kommutativer Ring mit Eins. Dann bilden die Polynome in x mit Koeffizienten in R unter der üblichen Addition und Multiplikation ebenfalls einen kommutativen Ring mit Eins; er wird mit $R[x]$ bezeichnet. Einem Polynom $f(x) \in R(x)$ ordnet man seinen Grad $\deg(f(x)) \in \mathbb{Z}$ zu, nämlich den Index des höchsten nichtverschwindenden Koeffizienten von $f(x)$. Es gilt offensichtlich,

$$\begin{aligned}\deg(f(x) + g(x)) &\leq \deg f(x) + \deg g(x) \ , \\ \deg(f(x) \cdot g(x)) &\leq \deg f(x) \cdot \deg g(x) \ .\end{aligned}$$

Jedes $f(x) \in R[x]$ definiert eine Funktion $F : R \to R$, die durch Evaluation definiert ist $F(r) = f(r)$. Man beachte, dass es vorkommen kann, dass verschiedene Polynome dieselbe Funktion beschreiben: Es sei $R = \mathbb{F}_2$, dann beschreiben die beiden Polynome $f(x) = x^2 + x$ und $g(x) = 0$ beide die gleiche Funktion.

Definition Ein Ring R, dessen additive Gruppe ein Vektorraum über K und dessen Produkt $(a, b) \mapsto a \cdot b$ bilinear bezüglich K ist, heisst eine *Algebra* über K. Die Bilinearität ist gewährleistet durch das Axiom, $a, b, c \in K$, $\lambda \in K$

$$(\lambda a) \cdot b = \lambda(a \cdot b) = a \cdot (\lambda b) \ .$$

Beispiel Die komplexen Zahlen $\mathbb{C}$ sind eine Algebra über $\mathbb{R}$. Eine Basis ist z.B. $\{1, i\}$.

Ist R eine Algebra über K mit Basis $\{a_i\}$, $i \in I$, so ist die Multiplikation in R vollständig durch die Angabe der Produkte

$$a_i \cdot a_j = \sum_{k \in I} c_{ijk} a_k$$

bestimmt. Die Grössen $c_{ijk} \in K$ heissen manchmal *Strukturkonstanten* der Algebra R.

Beweis Es sei $x = \sum \xi_i a_i$ und $y = \sum \eta_j a_j$. Dann folgt wegen der Bilinearität

$$x \cdot y = \Big(\sum \xi_i a_i\Big) \cdot \Big(\sum \eta_j a_j\Big) = \sum \xi_i \eta_j c_{ijk} a_k \ .$$

Beispiele

(a) Als konkretes Beispiel erwähnen wir die *Quaternionenalgebra* $\mathbb{H}$.[4] Dazu betrachten wir $\{1, i, j, k\}$ als Basis eines vierdimensionalen reellen Vektorraumes. Die Produkte der Basiselemente sind durch die folgende Multiplikationstabelle für die Basiselemente gegeben:

	1	i	j	k
1	1	i	j	k
i	i	-1	k	$-j$
j	j	$-k$	-1	i
k	k	j	$-i$	-1

Man zeigt ohne grosse Schwierigkeiten, dass $\mathbb{H}$ eine assoziative, nichtkommutative Algebra über $\mathbb{R}$ mit Eins ist. Ferner besitzt jedes von Null verschiedene Element in $\mathbb{H}$ ein Inverses: $\mathbb{H}$ ist ein *Schiefkörper*.

(b) Die reellen Zahlen $\mathbb{R}$ können als Algebra über den rationalen Zahlen $\mathbb{Q}$ angesehen werden; die Dimension ist überabzählbar unendlich.

(c) Der Polynomring $K[x]$, K ein Körper, ist eine Algebra über K von abzählbar unendlicher Dimension.

(d) Es sei G eine Gruppe und K ein Körper. Wir definieren die *Gruppenalgebra* KG über K wie folgt. Als K-Vektorraum besitzt KG die Basis $\{x\}$, $x \in G$. Das Produkt zweier Elemente $\sum_{x \in G} a_x x$ und $\sum_{y \in G} b_y y$ ist gegeben durch

$$\left(\sum_{x \in G} a_x x\right) \cdot \left(\sum_{y \in G} b_y y\right) = \sum_{x\, y \in G} a_x b_y \, xy \ .$$

[4] Bezeichnung nach William Rowan Hamilton (1805-1865), der die Quaternionen 1843 erstmals beschrieben hat.

Die Assoziativität der Multiplikation der Gruppe G überträgt sich in offensichtlicher Weise auf die Multiplikation in der Gruppenalgebra KG.

(e) Die $n \times n$ Matrizen über dem Körper K bilden eine Algebra über K der Dimension n^2. Eine Basis ist durch die Matrizen E_{ij} gegeben, wobei E_{ij} die Matrix ist, die in der i-ten Zeile und der j-ten Spalte eine 1 besitzt und sonst überall Nullen. Die Strukturkonstanten ergeben sich durch die Matrizenmultiplikation, also

$$E_{ij} \cdot E_{kl} = \delta_{jk} \cdot E_{il} \ .$$

II.2 Ringhomomorphismen, Ideale

Wie bei Gruppen, so wird man auch bei Ringen vor allem Abbildungen betrachten, welche mit der Struktur verträglich sind.

Definition Es seien R und S zwei Ringe. Die Abbildung $\phi : R \to S$ heisst ein *Ringhomomorphismus*, wenn für alle $a, b \in R$ gilt

(i) $\phi(a + b) = \phi a + \phi b$,

(ii) $\phi(a \cdot b) = \phi a \cdot \phi b$.

Aus (i) folgt, dass ϕ ein Homomorphismus der additiven Gruppe von R ist. Insbesondere gilt $\phi(0_R) = 0_S$ und $\phi(-a) = -\phi(a)$. Im Gegensatz dazu folgt aus den Axiomen aber *nicht*, dass bei einem Ringhomomorphismus $\phi : R \to S$ das Einselement von R ins Einselement von S übergeht.

Definition Es seien R, S Ringe mit Eins. Der Ringhomomorphismus $\phi : R \to S$ heisst *Homomorphismus von Ringen mit Eins*, wenn zusätzlich $\phi(1_R) = 1_S$ gilt.

Es sei $\phi : R \to S$ ein Homomorphismus von Ringen (mit Eins). Wir betrachten

$$I = \ker \phi = \{a \in R \mid \phi a = 0\} \ .$$

Es ist klar, dass I eine Untergruppe der additiven Gruppe von R ist. (Da die additive Gruppe abelsch ist, ist jede Untergruppe auch Normalteiler!) Ferner gilt für $a \in I$ und $b \in R$

$$\phi(a \cdot b) = \phi(a) \cdot \phi(b) = 0 \cdot \phi(b) = 0 \ .$$

Analog folgt $\phi(b \cdot a) = 0$. Mit $a \in I$ und $b \in R$ liegt damit stets auch $a \cdot b$ und $b \cdot a$ in I.

Definition Eine Untergruppe I der additiven Gruppe von R heisst ein (zweiseitiges) *Ideal* von R, wenn aus $a \in I$ und $b \in R$ stets folgt $ab \in I$ und $ba \in I$.

Satz 2.1 *Der Kern eines Ringhomomorphismus ist ein Ideal.*

Definition Es sei I ein Ideal in R. Der Ring S der Restklassen von R modulo I ist wie folgt definiert:

- Die additive Gruppe von S ist die Quotientengruppe R/I.
- Das Produkt in S ist definiert durch $(a + I) \cdot (b + I) = a \cdot b + I$.

Natürlich ist hier zuerst zu zeigen, dass das Produkt wohldefiniert ist, das heisst dass es unabhängig ist von der Auswahl der Repräsentanten. Die Tatsache, dass das Produkt assoziativ und distributiv ist, folgt dann unmittelbar, weil dies bereits für die Repräsentanten gilt.
Es seien $a + I = a' + I$ und $b + I = b' + I$. Dann existieren $u, v \in I$ mit $a' = a + u$ und $b' = b + v$. Also folgt $a'b' + I = (a + u)(b + v) + I = ab + av + ub + uv + I = ab + I$, letzteres wegen $av, ub, uv \in I$. Damit ist das Produkt in R/I wohldefiniert.

Bemerkungen
1. Die kanonische Projektion $\pi : R \to R/I$ ist ein Ringhomomorphismus.

2. Ist R ein Ring mit Eins und I ein Ideal in R mit $I \neq R$, dann besitzt R/I eine Eins, nämlich $1_R + I$.
Beweis Es ist nur zu zeigen, dass $1_R \notin I$. Wäre aber $1_R \in I$, so hätte man für $b \in R$, sofort $b = 1_R \cdot b \in I$, das heisst $I = R$. Dies ist ein Widerspruch.

Satz 2.2 (Isomorphiesatz der Ringtheorie) *Es sei $\phi : R \to S$ ein Ringhomomorphismus. Dann induziert ϕ einen Ringisomorphismus*

$$\phi_* : R/I \xrightarrow{\sim} \phi R \ , \quad \phi_*(a + I) = \phi a$$

mit $I = \ker \phi$.
Beweis Nach dem 1. Isomorphiesatz für Gruppen (siehe Kapitel I, Satz 7.1) ist ϕ_* ein Isomorphismus der additiven Gruppen. Es ist somit nur zu zeigen, dass ϕ_* ein Ringhomomorphismus ist. Dies ist aber klar.

Beispiele
(a) Es sei $R = K$ ein Körper. Dann gibt es ausser $\{0\}$ und K keine Ideale. Ist nämlich $0 \neq a$ eine Element von I, so ist $1_K = a^{-1} \cdot a \in I$ und damit $I = K$. Es folgt, dass jeder von einem Körper ausgehende Homomorphismus von Ringen mit Eins injektiv ist.

(b) Es sei $R = \mathbb{Z}$. Die Ideale in $\mathbb{Z}$ lassen sich explizit beschreiben: einerseits ist $m\mathbb{Z}$ ein Ideal in $\mathbb{Z}$ und andererseits ist jedes Ideal in $\mathbb{Z}$ insbesondere eine Untergruppe der additiven Gruppe von $\mathbb{Z}$, also von der Form $m\mathbb{Z}$ für ein gewisses $m \in \mathbb{Z}$. Jedes Ideal in $\mathbb{Z}$ besteht somit aus den Vielfachen eines Elementes $m \in \mathbb{Z}$; es wird das von m erzeugte Hauptideal genannt und üblicherweise durch (m) bezeichnet.

Definition Es sei R ein kommutativer Ring mit Eins, $a \in R$, dann heisst $(a) = \{r \cdot a \mid r \in R\}$ das von a erzeugte *Hauptideal* in R.

Definition Ein Integritätsbereich R, in dem jedes Ideal ein Hauptideal ist, heisst *Hauptidealbereich.*

Nach obigem gilt:

Satz 2.3 *Der Ring der ganzen Zahlen ist ein Hauptidealbereich.*

Satz 2.4 *Der Ring der Polynome $R = K[x]$, K ein Körper, ist ein Hauptidealbereich.*

Für den Beweis benötigen wir den Divisionsalgorithmus für Polynome.

Lemma 2.5 (Euklidischer Algorithmus) *Es seien $f(x)$ und $g(x)$ Polynome in $K[x]$. Dann existieren Polynome $q(x)$ und $r(x)$ in $K[x]$ mit*

$$f(x) = g(x) \cdot q(x) + r(x) \ , \quad \deg r(x) < \deg g(x) \ .$$

Beweis Falls $\deg f(x) < \deg g(x)$, so ist nichts zu beweisen: $r(x) = f(x)$, $q(x) = 0$. Sei $f(x) = a_0 + a_1 + \cdots + a_n x^n$ und $g(x) = b_0 + b_1 + \cdots + b_m x^m$, $a_n, b_m \neq 0$, $n \geq m$. Setze

$$f_1(x) = f(x) - x^{n-m} \frac{a_n}{b_m} g(x) \ .$$

Dann ist $\deg f_1(x) < \deg f(x)$. Nach Induktion existiert $q_1(x)$ und $r_1(x)$, $\deg r_1(x) < \deg g(x)$ mit

$$f(x) - x^{n-m} \frac{a_n}{b_m} g(x) = f_1(x) = g(x) \cdot q_1(x) + r_1(x) \ .$$

Daraus folgt

$$f(x) = \left(q_1(x) + x^{n-m} \frac{a_n}{b_m} \right) g(x) + r_1(x) \ .$$

Dies war zu beweisen.

Beweis des Satzes Es ist klar, dass $K[x]$ ein Integritätsbereich ist. Es sei $\{0\} \neq I$ ein Ideal in $K[x]$. Dann existiert $0 \neq h(x) \in I$. Sei $0 \neq g(x)$ ein Polynom von kleinstem Grad in I. Dann behaupten wir $I = (g(x))$. Natürlich ist $(g(x)) \subseteq I$. Zu zeigen bleibt somit, dass $I \subseteq (g(x))$. Es sei $f(x) \in I$. Dann gilt $\deg f(x) \geq \deg g(x)$. Somit folgt $f(x) = g(x) \cdot q(x) + r(x)$ mit $\deg r(x) < \deg g(x)$, aber $r(x) = f(x) - g(x) \cdot q(x) \in I$. Wegen der Minimalität von $g(x)$ ergibt sich daraus $r(x) = 0$ und damit $f(x) = g(x) \cdot q(x) \in (g(x))$.

Der Ring der Gaussschen Zahlen $\mathbb{Z}[i]$ ist definiert als Unterring von $\mathbb{C}$, der aus allen komplexen Zahlen $a + ib$ besteht mit $a, b \in \mathbb{Z}$. In diesem Ring spielt die sogenannte Norm N eine grosse Rolle; man definiert $N(a + ib) = a^2 + b^2$. Man weiss aus der Theorie der komplexen Zahlen, dass die Norm multiplikativ ist; es gilt $N(w \cdot z) = N(w) \cdot N(z)$. Wir werden zeigen:

Satz 2.6 *Der Ring $\mathbb{Z}[i]$ ist ein Hauptidealbereich.*

Beweis Klar ist zuerst, dass $\mathbb{Z}[i]$ keine Nullteiler hat. Die Hauptidealeigenschaft leiten wir mit Hilfe des folgenden Euklidischen Algorithmus her. Es gilt:

Zu $z, w \in \mathbb{Z}[i]$ mit $w \neq 0$ gibt es Elemente $q, r \in \mathbb{Z}[i]$ mit $z = w \cdot q + r$ und $N(r) < N(w)$.

Für den Beweis betrachte man die komplexe Zahl $z/w = c_1 + ic_2$ – die c_i sind im allgemeinen natürlich rationale Zahlen. Man schreibe c_i, $i = 1, 2$ als $q_i + s_i$ mit $|s_i| \leq 1/2$ und setze $q = q_1 + iq_2$, $s = s_1 + is_2$ und $r = w \cdot s$. Dann gilt

$$z = w \cdot c = w \cdot (q + s) = w \cdot q + w \cdot s = w \cdot q + r \ .$$

Dabei ergibt sich für die Norm $N(r)$:

$$N(r) = N(w \cdot s) = N(w) \cdot N(s) = N(w) \cdot (s_1^2 + s_2^2) \leq N(w)(1/4 + 1/4) < N(w) \ .$$

Der Beweis für die Hauptidealeigenschaft von $\mathbb{Z}[i]$ verläuft nun ganz analog zum Beweis der entsprechenden Eigenschaft bei Polynomringen über einem Körper (siehe Satz 2.4). Ist I ein Ideal in $\mathbb{Z}$, so nehme man in I ein Element z mit minimaler Norm und zeige mit Hilfe des Euklidischen Algorithmus, dass z das Ideal I erzeugt.

Beispiele

(c) In $\mathbb{R}[x,y]$ gibt es Ideale, die *nicht* Hauptideale sind. Es gibt somit Integritätsbereiche, die *nicht* Hauptidealbereiche sind:

Sei $I = \{f(x,y) \in \mathbb{R}[x,y] \mid f(0,0) = 0\}$. Natürlich ist I ein Ideal, aber I ist offensichtlich kein Hauptideal.

(d) Wir betrachten $\mathbb{R}[x]$ und die Abbildung $\phi : \mathbb{R}[x] \to \mathbb{C}$, die durch $\phi(f(x)) = f(i)$ definiert wird. Dann ist ϕ ein Homomorphismus von Ringen mit Eins, und ϕ ist surjektiv. Der Kern $\ker(\phi) = I$ ist ein Ideal in $\mathbb{R}[x]$, also ein Hauptideal, $I = (h(x))$, wobei $h(x)$ (irgend)ein Polynom in I von minimalem Grad ist. Da es kein Polynom vom Grad 0 oder 1 gibt, das unter ϕ auf Null abgebildet wird, ist dieser minimale Grad 2. Natürlich gilt $\phi(x^2+1) = 0$, so dass wir folgern können $I = (x^2+1)$. Der Isomorphiesatz der Ringtheorie liefert dann

$$\phi_* : \mathbb{R}[x]/(x^2+1) \xrightarrow{\sim} \mathbb{C} \ .$$

Es dürfte klar sein, dass die Technik, die wir hier zur Beschreibung von $\mathbb{C}$ verwendet haben, auch in anderen Fällen nützlich sein wird. Wir werden dies im Kapitel III genauer zu untersuchen haben.

(e) Wir betrachten hier noch einmal $\mathbb{Z}$. Es seien (m) und (n) zwei Ideale in $\mathbb{Z}$ mit $m, n \geq 1$. Es gelte $(m) \subseteq (n)$. Dann existiert $k \in \mathbb{Z}$ mit $m = kn$, d.h. n ist ein Teiler von m, $n \mid m$. Ist umgekehrt n ein Teiler von m, so gilt offensichtlich $(m) \subseteq (n)$. Damit können wir die Teilereigenschaft von natürlichen Zahlen, durch die Inklusion der zugehörigen Hauptideale beschreiben:

$$(m) \subseteq (n) \Leftrightarrow n \mid m \ .$$

Mit dieser Feststellung können wir dann auch folgern, dass $p \in \mathbb{Z}$ genau dann eine Primzahl ist, wenn es in $\mathbb{Z}$ ausser $\mathbb{Z}$ selbst kein (p) echt umfassendes Ideal gibt. Wir führen deshalb die folgende Terminologie ein.

Definition Ein Ideal $I \neq R$ von R heisst *maximal*, wenn aus $I \subseteq J \subseteq R$, J ein Ideal in R, stets folgt $J = I$ oder $J = R$.

Satz 2.7 *Genau dann ist p eine Primzahl, wenn (p) in $\mathbb{Z}$ ein maximales Ideal ist.*

Satz 2.8 *Es sei R ein kommutativer Ring mit Eins. Ein echtes Ideal I in R ist genau dann maximal, wenn R/I ein Körper ist.*

Beweis Es sei zuerst R/I ein Körper. Um zu zeigen, dass I maximal ist, betrachten wir ein Ideal J mit $I \subset J \subseteq R$. Dann existiert $a \in J$ mit $a \notin I$. Zu $a + I$ existiert laut

Voraussetzung ein Inverses in R/I, d.h. es existiert $y \in R$ mit $(a+I)(y+I) = ay + I = 1_R + I$. Daraus folgt aber $1_R = ay + u$ für ein gewisses $u \in I$. Aber dies zieht $1_R \in J$ nach sich, so dass gilt $J = R$.
Es sei umgekehrt I ein maximales Ideal in R. Um zu zeigen, dass $a+I$, $a \notin I$ ein Inverses besitzt, betrachten wir die Menge

$$J = \{ya + u \mid y \in R,\, u \in I\} \ .$$

Es ist leicht zu zeigen, dass J ein Ideal von R ist, das wegen $a \in J$ das Ideal I echt enthält. Damit folgt laut Voraussetzung $J = R$. Es existieren somit $y_0 \in R$ und $u_0 \in I$ mit $1_R = y_0 a + u_0$. Dann ist aber $y_0 + I$ das Inverse von $a + I$ in R/I, denn es gilt $(y_0 + I)(a + I) = y_0 a + I = 1_R + I$.

Beispiele
(f) Der Ring $\mathbb{Z}/m\mathbb{Z}$ ist genau dann ein Körper, wenn m eine Primzahl ist, was seinerseits genau dann der Fall ist, wenn (m) maximal ist.
(g) Wie wir gesehen haben, ist der Ring $\mathbb{R}[x]/(x^2+1)$ ein Körper. Folglich ist (x^2+1) ein maximales Ideal in $\mathbb{R}[x]$.

II.3 Faktorielle Ringe

Wir haben in Abschnitt 2 gesehen, dass für $R = \mathbb{Z}$ gilt $n \mid m \Leftrightarrow (m) \subseteq (n)$. Dieses einfache Resultat lässt sich in offensichtlicher Weise auf jeden kommutativen Ring R mit Eins verallgemeinern.
Im Zusammenhang mit der Teilbarkeit verwenden wir allgemein die folgende *Notation*:

Es sei R ein kommutativer Ring mit Eins, $a, b \in R$. Wir definieren

$$a \mid b \Leftrightarrow \text{es existiert } c \in R \text{ mit } b = ac \ .$$

Wenn zu $a, b \in R$ kein solches $c \in R$ existiert, so schreiben wir $a \nmid b$.

Definition Es sei R ein Integritätsbereich. Ein Element $p \in R$ heisst *irreduzibel* von R, wenn folgendes gilt:

(i) p ist keine Einheit.

(ii) Aus $p = a \cdot b$ folgt stets a ist Einheit oder b ist Einheit.

Beispiele
(a) In $\mathbb{Z}$ sind die die irreduziblen Elemente von der Form p oder $-p$, wo p eine Primzahl ist.

(b) Wegen $0 \cdot 0 = 0$ ist $0 \in R$ nicht irreduzibel.

(c) Ist ϵ eine Einheit, so ist mit p auch ϵp irreduzibel.

(d) Es sei $R = K[x]$, K ein Körper. Genau dann ist $f(x) \in K[x]$ irreduzibel, wenn gilt $\deg f(x) \geq 1$ und wenn $f(x)$ sich nicht als Produkt von zwei Polynomen vom Grad grösser gleich 1 schreiben lässt. Das Polynom $x^2 + 1$ ist ireduzibel in $\mathbb{R}[x]$, aber es ist *reduzibel* in $\mathbb{C}[x]$.

In $\mathbb{Z}$ lässt sich ein jedes Element in "eindeutiger" Weise als Produkt von irreduziblen Elementen, d.h. Primzahlen schreiben. Diese Eigenschaft verallgemeinernd führen wir die folgende Definition ein.

Definition Ein Integritätsbereich R heisst *faktoriell*, wenn folgendes gilt:

(i) Jedes Element $0 \neq a \in R$ besitzt eine Darstellung

$$a = \epsilon p_1 p_2 \dots p_n \ ,$$

wobei ϵ eine Einheit in R ist und p_i, $i = 1, 2, \dots, n$ irreduzible Elemente in R sind.

(ii) Diese Darstellung ist eindeutig; das heisst, aus

$$a = \epsilon p_1 p_2 \cdots p_n = \overline{\epsilon}\, \overline{p}_1 \overline{p}_2 \cdots \overline{p}_m$$

folgt: $n = m$, und nach Umnumerierung der irreduziblen Elemente $\overline{p}_i$ existieren Einheiten $\overline{\epsilon}_i$, $i = 1, 2, \dots, n$ mit $p_i = \overline{\epsilon}_i \overline{p}_i$.

Man sagt in diesem Fall auch, es gelte in R die *eindeutige Faktorzerlegung*.[5]

Beispiel
(e) Im Ring $\mathbb{Z}[\sqrt{-5}]$ existiert die eindeutige Primfaktorzerlegung *nicht*. Es gilt nämlich

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

In $\mathbb{Z}[\sqrt{-5}]$ lässt sich also 6 auf zwei wesentlich verschiedene Arten als Produkt von irreduziblen Elementen darstellen.

[5]Die Geschichte der eindeutigen Faktorzerlegung enthält viele Irrungen und Wirrungen. Man vergleiche dazu U. Stammbach: *Die eindeutige Primfaktorzerlegung*, Math. Semesterber. **56** (2009), 105-122.

Es ist das Hauptziel dieses Abschnittes zu zeigen, dass jeder Hauptidealbereich faktoriell ist. Insbesondere sind also $\mathbb{Z}$ und $K[x]$ faktoriell.

Satz 3.1 *Es sei R ein Hauptidealbereich. Dann gibt es zu $a, b \in R$ einen grössten gemeinsamen Teiler und dieser ist bis auf Multiplikation mit einer Einheit eindeutig bestimmt.*

Definition Das Element $t \in R$ heisst *grösster gemeinsamer Teiler* (ggT) von $a, b \in R$, $t = (a, b)$, wenn Folgendes erfüllt ist: (i) $t \mid a, t \mid b$, (ii) $d \mid a, d \mid b \Rightarrow d \mid t$.

Beweis Setze $I = \{ua + vb \mid u, v \in R\}$. Es ist natürlich I eine Untergruppe der additiven Gruppe von R, und es ist ein Ideal, denn für $c \in R$ gilt

$$c(ua + vb) = (cu)a + (cv)b \in I \ .$$

Da R ein Hauptidealbereich ist, existiert $t \in R$ mit $I = (t)$. Ferner gilt $(a) \subseteq (t), (b) \subseteq (t)$, also $t \mid a$ und $t \mid b$. Das Element t ist somit ein gemeinsamer Teiler von a und b. Wir zeigen, dass es der *grösste* gemeinsame Teiler ist. Es sei d ein gemeinsamer Teiler von a und b. Es ist zu zeigen, dass gilt $d \mid t$. Aus $(a) \subseteq (d)$ und $(b) \subseteq (d)$ folgt $ua + vb \in (d)$ für alle $u, v \in R$. Damit gilt $I = (t) \subseteq (d)$, also $d \mid t$. Es seien schliesslich t_1 und t_2 grösste gemeinsame Teiler von a und b. Dann folgt $t_1 \mid t_2$ und $t_2 \mid t_1$ und damit $t_1 = \epsilon t_2$ mit ϵ eine Einheit. Letzteres ergibt sich aus dem folgenden Lemma.

Lemma 3.2 *Es sei R ein Integritätsbereich. Aus $a \mid b$ und $b \mid a$ folgt, dass eine Einheit ϵ existiert mit $b = \epsilon a$.*

Beweis Aus $ac = b$ und $bd = a$ folgt $bdc = b$, also $dc = 1$. Das Element c ist folglich eine Einheit, $c = \epsilon$, und damit gilt $b = \epsilon a$.

Korollar 3.3 *Es sei R ein Hauptidealbereich. Es sei t der grösste gemeinsame Teiler von a und b. Dann existieren $u, v \in R$ mit $t = ua + vb$.*

Definition Die Elemente $a, b \in R$ heissen *teilerfremd*, wenn ihr ggT eine Einheit ist.

Korollar 3.4 *Es sei R ein Hauptidealbereich. Die Elemente $a, b \in R$ seien teilerfremd. Dann gibt es $u, v \in R$ mit $1 = ua + vb$.*

Korollar 3.5 *Es sei R ein Hauptidealbereich. Dann folgt aus $a \mid bc$ und $(a, b) = 1$ stets $a \mid c$.*

Beweis Es gibt $u, v \in R$ mit $ua + vb = 1$. Folglich gilt $c = c(ua + vb) = (cu)a + (cv)b$. Wegen $a \mid a$ und $a \mid bc$ folgt daraus $a \mid c$. Dies war zu beweisen.

Theorem 3.6 *Es sei R ein Hauptidealbereich. Dann ist R faktoriell.*

Beweis *Existenz* der Faktorzerlegung: Wir gehen indirekt vor. Es sei $0 \neq a \in R$ keine Einheit, nicht irreduzibel und auch kein Produkt von irreduziblen Elementen. Es gibt dann also Nichteinheiten a_1 und b_1 mit $a = a_1 b_1$, wobei mindestens eines der Elemente a_1, b_1 nicht irreduzibel und auch kein Produkt von irreduziblen Elementen ist. Wir dürfen annehmen, dass a_1 von dieser Art ist. Somit gibt es Nichteinheiten a_2 und b_2 mit $a_1 = a_2 b_2$, wobei mindestens eines der Elemente a_2, b_2, sagen wir a_2, nicht irreduzibel und auch kein Produkt von irreduziblen Elementen ist, usw. Wir erhalten auf diese Weise eine unendliche Folge von Elementen $a = a_0, a_1, a_2, \ldots$, die alle keine Einheiten, nicht irreduzibel und auch keine Produkte von irreduziblen Elementen sind. Für jedes $j = 0, 1, \ldots$ gilt ferner $a_{j+1} \mid a_j$, das heisst $(a_j) \subseteq (a_{j+1})$.

Wir setzen nun $I = \cup_{i=0}^{\infty}(a_i)$ und behaupten, dass I ein Ideal von R ist. Um dies zu beweisen, betrachten wir $b, c \in I$. Dann gibt es ein j mit $b, c \in (a_j)$. Da (a_j) ein Ideal ist, folgt $b + c \in (a_j) \subseteq I$ und $-b \in (a_j) \subseteq I$. Ferner gilt auch $x \cdot b \in (a_j) \subseteq I$ für alle $x \in R$. Damit ist I ein Ideal.

Da R ein Hauptidealbereich ist, existiert d mit $I = (d)$. Aus $d \in I$ folgt, dass k existiert mit $d \in (a_k)$. Daraus schliessen wir

$$I = (d) \subseteq (a_k) \subseteq (a_{k+1}) \subseteq I \ .$$

Somit gilt $(a_j) = (a_{j+1})$, so dass y existiert mit $a_{j+1} = y \cdot a_j$. Ferner gilt $a_j = a_{j+1} \cdot b_{j+1}$, so dass folgt $a_j = y \cdot a_j \cdot b_{j+1}$. Dann ist aber $y \cdot b_{j+1} = 1$ und b_{j+1} eine Einheit. Dies ist ein Widerspruch.

Eindeutigkeit der Faktorzerlegung: Induktion nach n. Ist $n = 0$, so gilt $\epsilon = \overline{\epsilon}\,\overline{p}_1\overline{p}_2 \cdots \overline{p}_m$, das heisst $1 = \epsilon^{-1} \cdot \epsilon = \overline{\epsilon} \cdot \epsilon^{-1}\overline{p}_1\overline{p}_2 \cdots \overline{p}_m$. Wäre $m \geq 1$, so wäre $\overline{p}_1$ eine Einheit. Dies ist ein Widerspruch.

Es sei $n \geq 1$. Dann ist $\epsilon p_1 p_2 \cdots p_n = \overline{\epsilon}\,\overline{p}_1\overline{p}_2 \cdots \overline{p}_m$. Folglich gilt $p_1 \mid \overline{\epsilon}\,\overline{p}_1 \cdots \overline{p}_m$. Ist $p_1 \nmid \overline{p}_1$, so ist $(p_1, \overline{p}_1) = 1$ und mit dem obigen Korollar folgt $p_1 \mid \overline{\epsilon}\,\overline{p}_2 \cdots \overline{p}_m$. Mit Induktion schliessen wir, dass $2 \leq k \leq m$ existiert mit $p_1 \mid \overline{p}_k$, das heisst $p_1 = \epsilon_k \overline{p}_k$. Nach Umnumerierung können wir $k = 1$ annehmen. Dann gilt, da R ein Integritätsbereich ist,

$$\epsilon_1 \epsilon p_2 \cdots p_n = \overline{\epsilon}\,\overline{p}_2 \cdots \overline{p}_m \ .$$

Nach Induktion gilt dann $n = m$ und nach Umnumerierung $p_i = \epsilon_i\,\overline{p}_i, i = 2, 3, \cdots, n$. Dies war zu beweisen.

Der wesentliche Schritt im Beweis für die Existenz der eindeutigen Primfaktorzerlegung in einem Hauptidealbereich, bestand darin zu zeigen, dass *jede aufsteigende Folge von Idealen stationär wird*. Auf Grund der zentralen Rolle, die diese Eigenschaft ganz allgemein in der Ringtheorie spielt, nennt man einen Ring R *Noethersch*, wenn jede aufsteigende Folge von Idealen von R stationär wird. Viele natürlich auftretende Ringe sind in der

Tat Noethersch, wie etwa die in der Zahlentheorie wichtigen Ringe der ganz algebraischen Zahlen in einem Zahlkörper. Es hat sich in der Entwicklung der Ringtheorie herausgestellt, dass dieser abstrakten Eigenschaft in ganz verschiedenen konkreten Situation eine Schlüsselrolle zukommt. Leider können wir im Rahmen dieses einführenden Textes nicht weiter auf diesen Punkt eingehen.

Lemma 3.7 *Es sei R faktoriell und $p \in R$ sei irreduzibel. Dann folgt aus $p \mid a \cdot b$, $p \nmid a$ stets $p \mid b$.*

Beweis Laut Voraussetzung existiert c mit $ab = pc$; es sei $c = \epsilon p_1 \cdots p_n$. Folglich gilt $a \cdot b = \epsilon p p_1 \cdots p_n$. Auf der anderen Seite sei $a = \epsilon' \cdot p'_1 \cdots p'_r,\ b = \epsilon'' p''_1 \cdots p''_s$. Dann folgt $ab = \epsilon' \cdot \epsilon'' p'_1 \cdots p'_r\ p''_1 \cdots p''_s$. Wegen der Eindeutigkeit der Primfaktorzerlegung existiert eine Einheit δ mit $p = \delta p'_i$ oder $p = \delta p''_i$ für gewisses i. Wäre $p = \delta p'_i$, so wäre $p \mid a$. Dies ist ein Widerspruch. Folglich gilt $p = \delta p''_i$ und $p \mid b$.

Korollar 3.8 *Es sei R faktoriell, p irreduzibel. Dann folgt aus $a \cdot b \in (p)$ und $a \notin (p)$ stets $b \in (p)$.*

Definition (i) Ein Element $p \in R$ heisst *Primelement*, wenn aus $p \mid a \cdot b$, $p \nmid a$ stets $p \mid b$ folgt.

(ii) Ein Ideal $I \subseteq R$, $I \neq R$ heisst *Primideal*, wenn aus $a \cdot b \in I$ stets $a \in I$ oder $b \in I$ folgt.

Satz 3.9 *Es sei R faktoriell und $0 \neq p \in R$. Dann sind die folgenden Aussagen äquivalent:*

(i) *p ist irreduzibel,*

(ii) *p ist ein Primelement,*

(iii) *(p) ist ein Primideal.*

Beweis Die Implikationen (i) $\Rightarrow$ (ii) $\Rightarrow$ (iii) sind nach obigem klar. Es bleibt, (iii) $\Rightarrow$ (i) zu beweisen. Es sei (p), $p \neq 0$ ein Primideal und es sei $p = a \cdot b$. Dann gilt $a \in (p)$ oder $b \in (p)$. Es sei $a \in (p)$, das heisst $a = c \cdot p$. Dann folgt $p = ab = cp \cdot b$ und damit $c \cdot b = 1$ und b ist eine Einheit. Damit ist p irreduzibel.

Satz 3.10 *Es sei R ein Hauptidealbereich und $0 \neq I = (p)$ ein Hauptideal. Dann sind folgende Aussagen äquivalent:*

(i) *p ist irreduzibel,*

(ii) *$I = (p)$ ist ein Primideal,*

(iii) *$I = (p)$ ist ein maximales Ideal.*

Beweis Nach dem obigen Satz sind die Aussagen (i) und (ii) für faktorielle Ringe, also insbesondere für Hauptidealbereiche äquivalent. Wir haben schon früher gesehen, dass für Hauptidealringe die Ausagen (i) und (iii) äquivalent sind.

II.4 Polynomringe

Wir stellen zuerst einige allgemeine, wohlbekannte Tatsachen über Nullstellen von Polynomen zusammen.

Satz 4.1 *Es sei R ein kommutativer Ring mit* 1. *Ferner sei $f(x) \in R[x]$ mit* $\deg f(x) \geq 1$. *Genau dann ist $\alpha \in R$ eine Nullstelle von $f(x)$, wenn ein Polynom $g(x) \in R[x]$ existiert mit $f(x) = (x - \alpha) \cdot g(x)$.*

Beweis Die eine Richtung ist trivial. Den Beweis in der anderen Richtung führen wir mit Induktion nach $n = \deg f(x)$. Es sei $n = 1$ und $f(x) = a_0 + a_1 x$ mit $a_1 \neq 0$. Aus $f(\alpha) = a_0 + a_1\alpha = 0$ folgt $f(x) = (x - \alpha) \cdot a_1$, da $a_0 = -a_1\alpha$. Es sei nun $\deg f(x) \geq 2$. Wir betrachten für $f(x) = a_0 + a_1 x + \cdots + a_n x^n$, $a_n \neq 0$ das Polynom

$$h(x) = f(x) - (x - \alpha)a_n x^{n-1} \ .$$

Dann gilt $h(\alpha) = 0$ und $\deg h(x) < \deg f(x)$. Folglich gilt entweder $h(x) = 0$, also $f(x) = (x - \alpha) \cdot a_n x^{n-1}$, oder wir können $h(x)$ nach Induktionsvoraussetzung schreiben als

$$h(x) = (x - \alpha) \cdot \overline{g}(x) \ .$$

In diesem Fall folgt aber

$$f(x) = (x - \alpha)\overline{g}(x) + (x - \alpha)a_n x^{n-1} = (x - \alpha)\left(\overline{g}(x) + a_n x^{n-1}\right) = (x - \alpha) \cdot g(x) \ ,$$

wobei wir $g(x) = \overline{g}(x) + a_n x^{n-1}$ gesetzt haben. Dies war zu beweisen.

Korollar 4.2 *Es sei R ein Integritätsbereich, $f(x) \in R[x]$, $n = \deg f(x) \geq 1$. Dann besitzt $f(x)$ höchstens n Nullstellen.*

Beweis Wir beweisen mit Induktion nach n. Es sei $n = 1$, $f(x) = (x - \alpha)a_1$ und $0 = f(\alpha_2) = (\alpha_2 - \alpha_1) \cdot a_1$. Dies impliziert $\alpha_2 = \alpha_1$, da R keine Nullteiler hat. Damit hat $f(x)$ höchstens eine Nullstelle.

Es sei $n = \deg f(x) \geq 2$. Und es seien $\alpha_1, \ldots, \alpha_{n+1}$ Nullstellen von $f(x)$. Dann gilt $f(x) = (x - \alpha_1)g(x)$, und $0 = f(\alpha_i) = (\alpha_i - \alpha_1)g(\alpha_i)$. Es hat also $g(x)$ n Nullstellen, aber $\deg g(x) = n - 1$. Dies ist ein Widerspruch zur Induktionsvoraussetzung.

Wir wenden uns jetzt dem Ring $\mathbb{Z}[x]$ zu. Man beachte dabei, dass $\mathbb{Z}[x]$ *kein* Hauptidealbereich ist. In der Tat ist das Ideal $(2, x)$ kein Hauptideal.

Definition Das Polynom $f(x) \in \mathbb{Z}[x]$ heisst *primitiv*, wenn $\deg f(x) \geq 1$ gilt und wenn der ggT der Koeffizienten 1 ist.

Nichtprimitive Polynome lassen sich in $\mathbb{Z}[x]$ zerlegen in ein Produkt von Nichteinheiten, sind also in $\mathbb{Z}[x]$ reduzibel.
Die Einheiten in $\mathbb{Z}[x]$ sind ± 1. Was sind die irrreduziblen Elemente in $\mathbb{Z}[x]$? Es sind dies einmal die irreduziblen Elemente von $\mathbb{Z}$. Ein echtes Polynom $f(x) \in \mathbb{Z}[x]$ ist irreduzibel, wenn es primitiv ist und wenn aus $f(x) = g(x) \cdot h(x)$ mit $\deg g(x) \geq 1$ stets folgt $\deg h(x) = \pm 1$.

Beispiele
(a) Das Polynom $f(x) = 3x + 3 = 3(x + 1)$ ist reduzibel in $\mathbb{Z}[x]$, aber natürlich irreduzibel in $\mathbb{Q}[x]$.

(b) Das Polynom $f(x) = x^2 + 1$ ist irreduzibel in $\mathbb{R}[x]$, aber reduzibel in $\mathbb{C}[x]$.

Lemma 4.3 *Das Produkt von primitiven Polynomen ist wieder primitiv.*
Beweis Es seien $f(x) = a_0 + a_1 x + \cdots + a_n x^n$ und $g(x) = b_0 + b_1 + \cdots + b_m x^m$ primitive Polynome in $\mathbb{Z}[x]$. Wir führen den Beweis indirekt. Es sei

$$f(x) \cdot g(x) = c_0 + c_1 x + \cdots + c_{n+m} x^{n+m}$$

nicht primitiv. Dann existiert eine Primzahl $p \in \mathbb{Z}$ mit $p \mid c_k$ für $k = 1, 2, \ldots, n + m$. Da p nicht alle a_i's teilen kann, existiert ein kleinstes i mit $p \nmid a_i$, und analog ein kleinstes j mit $p \nmid b_j$. Betrachte $c_{i+j} = a_i b_j + a_{i+1} b_{j-1} + \cdots + a_{i-1} b_{j+1} + \cdots$. Da alle von $a_i b_j$ verschiedenen Terme dieser Gleichung durch p teilbar sind, muss auch $a_i b_j$ durch p teilbar sein. Damit folgt $p \mid a_i$ oder $p \mid b_j$. Dies ist ein Widerspruch.

Satz 4.4 (Satz von Gauss) *Es sei $f(x) \in \mathbb{Z}[x]$, $\deg f(x) \geq 1$ irreduzibel in $\mathbb{Z}[x]$. Dann ist $f(x)$ auch irreduzibel in $\mathbb{Q}[x]$.*
Wir wollen jetzt schon darauf hinweisen, dass wir als Korollar dieses Satzes am Ende dieses Abschnittes beweisen werden, dass der Ring $\mathbb{Z}[x]$ faktoriell ist.
Beweis Das Polynom $f(x)$ ist primitiv, sonst wäre $f(x)$ reduzibel in $\mathbb{Z}[x]$. Wir bewei-

sen indirekt: Wäre $f(x)$ reduzibel in $\mathbb{Q}[x]$, so würden Polynome $g(x)$ und $h(x) \in \mathbb{Q}[x]$ existieren mit $f(x) = g(x) \cdot h(x)$ und $\deg g(x) \geq 1$, $\deg h(x) \geq 1$. Wir schreiben

$$g(x) = \frac{a_0}{b_0} + \frac{a_1}{b_1}x + \cdots + \frac{a_n}{b_n}x^n = \frac{1}{b_0 b_1 \cdots b_n}\,\overline{g}(x); \quad \overline{g}(x) \in \mathbb{Z}[x].$$

Es existiert dann ein primitives Polynom $p(x) \in \mathbb{Z}[x]$ mit $g(x) = \frac{a}{b}p(x)$. Ebenso existiert ein primitives Polynom $q(x) \in \mathbb{Z}[x]$ mit $h(x) = \frac{c}{d}q(x)$. Daraus folgt

$$f(x) = g(x) \cdot h(x) = \frac{ac}{bd}\, p(x) \cdot q(x)$$

also $bd \cdot f(x) = ac \cdot p(x) \cdot q(x)$. Nun sind $f(x)$ und $p(x) \cdot q(x)$ primitiv. Daraus folgt $\epsilon bd = ac$ für eine Einheit ϵ in $\mathbb{Z}$. Es ergibt sich $bdf(x) = \epsilon bd\ p(x)q(x)$ also $f(x) = \epsilon p(x) \cdot q(x)$. Letzteres steht im Widerspruch zur Tatsache, dass $f(x)$ in $\mathbb{Z}[x]$ irreduzibel ist.

Der Satz von Gauss hat weitreichende Anwendungen; zwei davon stellen wir in der Folge dar, nämlich das Irreduziblitätskriterium von Eisenstein (Satz 4.5) und den Satz 4.8, der besagt, dass $R[x]$ faktoriell ist, wenn R faktoriell ist.

Satz 4.5 (Kriterium von Eisenstein) *Es sei $f(x) = a_0 + a_1x + \cdots + a_nx^n$ ein ganzzahliges Polynom mit $a_n \neq 0$. Es existiere eine Primzahl $p \in \mathbb{Z}$ mit $p \mid a_0$, $p^2 \nmid a_0$, $p \mid a_i$ für $i = 1, 2, \ldots, n-1$, $p \nmid a_n$. Dann ist $f(x)$ irreduzibel in $\mathbb{Q}[x]$.*

Beispiele

(a) Es sei $f(x) = x^n - a, a = p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_k^{\alpha_k}$, p_i verschiedene Primzahlen, und mindestens ein $\alpha_i = 1$. Für dieses $p = p_i$ gilt $p \mid a_0$, $p^2 \nmid a_0$, $p \mid a_i$ für $i = 1, 2, \cdots, n-1$, $p \nmid a_n$. Damit ist $x^n - a$ irreduzibel in $\mathbb{Q}[x]$. Insbesondere besitzt $x^n - a$ für $n \geq 2$ keine rationale Nullstelle, oder anders ausgedrückt, $\sqrt[n]{a}$ ist irrational.

(b) Wir betrachten das Polynom

$$f(x) = x^{p-1} + \binom{p}{1}x^{p-2} + \cdots + \binom{p}{p-2}x + \binom{p}{p-1} = \frac{(x+1)^p - 1}{x} \in \mathbb{Z}[x]\ .$$

Nach dem Lemma 4.6 gilt $p \mid a_0$, $p^2 \nmid a_0$, $p \mid a_i$ für $i = 1, 2, \ldots, p-2$ und $p \nmid a_{p-1}$. Nach dem Kriterium von Eisenstein ist $f(x)$ irreduzibel. Dann ist aber auch

$$g(x) = f(x-1) = (x^p - 1)/(x-1) = x^{p-1} + x^{p-2} + \cdots + x + 1$$

irreduzibel.

Lemma 4.6 *Für eine Primzahl $p \in \mathbb{Z}$ gilt für $i = 1, 2, \ldots, p-1$*

$$p \mid \binom{p}{i}\ .$$

Beweis Nach dem kleinen Satz von Fermat (siehe Kapitel I, Korollar 5.5) gilt für a mit $p \nmid a$ stets $a^{p-1} \equiv 1 \pmod{p}$. Also folgt für beliebiges a

$$a^p \equiv a \pmod{p} .$$

Setzen wir $a = b + 1$, so folgt

$$b^p + \binom{p}{1} b^{p-1} + \binom{p}{2} b^{p-2} + \cdots + \binom{p}{p-1} b + 1 = (b+1)^p \equiv (b+1) \pmod{p} .$$

Wegen $b^p \equiv b \pmod{p}$ folgt daraus für alle $b \in \mathbb{Z}$

$$\binom{p}{1} b^{p-1} + \binom{p}{2} b^{p-2} + \cdots + \binom{p}{p-1} b \equiv 0 \pmod{p} .$$

Damit hat das Polynom

$$g(x) = \binom{p}{1} x^{p-1} + \binom{p}{2} x^{p-2} + \cdots + \binom{p}{p-1} x \in \mathbb{Z}/p\mathbb{Z}\,[x]$$

p verschiedene Nullstellen. Dies ist wegen $\deg g(x) = p - 1$ nur möglich, wenn $g(x) = 0$. Dies ist aber genau dann der Fall, wenn gilt

$$\binom{p}{i} \equiv 0 \pmod{p} .$$

für $1 \leq i \leq p - 1$.

Beweis von Satz 4.5 Wir gehen indirekt vor, und nehmen an, dass $f(x)$ über $\mathbb{Q}$ reduzibel ist. Nach dem Satz von Gauss (Satz 4.4) ist es dann auch reduzibel über $\mathbb{Z}$. Es existieren also ganzzahlige Polynome $h(x) = b_0 + b_1 x + \cdots + b_r x^r$, $\deg h(x) = r \geq 1$ und $g(x) = c_0 + c_1 x + \cdots + c_s x^s$, $\deg g(x) = s \geq 1$ mit

$$f(x) = a_0 + a_1 x + \cdots + a_n x^n = g(x)h(x) = (b_0 + b_1 x + \cdots + b_r x^r)(c_0 + c_1 x + \cdots + c_s x^s) .$$

Ausmultiplizieren liefert das Gleichungssystem

$$\begin{aligned} a_0 &= b_0 c_0 \\ a_1 &= b_0 c_1 + b_1 c_0 \\ a_2 &= b_0 c_2 + b_1 c_1 + b_2 c_0 \\ &\vdots \\ a_n &= b_r c_s \end{aligned}$$

Wegen $p \mid a_0$ und $p^2 \nmid a_0$ teilt p entweder b_0 oder c_0 nicht. Ohne Beschränkung der Allgemeinheit dürfen wir annehmen, dass $p \mid b_0$, aber $p \nmid c_0$. Dann folgt der Reihe nach

$$\begin{array}{ccc} p \mid b_1c_0\,, & \text{also} & p \mid b_1\ , \\ p \mid b_2c_0\,, & \text{also} & p \mid b_2\ , \\ & \vdots & \\ p \mid b_rc_0\,, & \text{also} & p \mid b_r\ . \end{array}$$

Aus der letzten Gleichung schliessen wir $p \mid b_rc_s$, also $p \mid a_n$. Dies ist ein Widerspruch zur Voraussetzung $p \nmid a_n$.

Als weitere Anwendung des Satzes von Gauss (Satz 4.4) beweisen wir das folgende Resultat.

Satz 4.7 *Der Ring $\mathbb{Z}[x]$ ist faktoriell.*

Wir erinnern zuerst daran, dass für einen *Körper* K der Ring $K[x]$ ein Hauptidealbereich und deshalb faktoriell ist. Wie wir bereits früher bemerkt haben, ist der Ring $\mathbb{Z}[x]$ *kein* Hauptidealbereich. Der Beweis der faktoriellen Eigenschaft von $\mathbb{Z}[x]$ muss deshalb auf anderen Wegen verlaufen.

Beweis Wir wenden uns zuerst der *Existenz* der Primfaktorzerlegung zu. Die Einheiten im Ring $\mathbb{Z}[x]$ sind ± 1. Die Primelemente sind einerseits die Primelemente von $\mathbb{Z}$ und andererseits die irreduziblen Polynome. Es sei nun $f(x) \in \mathbb{Z}[x]$, und es sei c der ggT der Koeffizienten von $f(x)$. Wir schreiben $f(x) = cg(x)$. Das Polynom $g(x)$ ist dann primitiv. Wir zerlegen nun c in Primfaktoren in $\mathbb{Z}$ und $g(x)$ in ein Produkt von irreduziblen Polynomen. Letzteres ist deshalb möglich, weil in einem Produkt von Polynomen der Grad der Faktoren jeweils echt kleiner ist als der Grad des Produktes. Deshalb muss das Verfahren nach endlich vielen Schritten zu einem Ende kommen. Damit erhalten wir

$$f(x) = \epsilon p_1p_2\cdots p_kh_1(x)h_2(x)\cdots h_l(x)\ ,$$

wo $p_1, p_2, \ldots, p_k$ Primelemente in $\mathbb{Z}$ und $h_1(x), h_2(x), \ldots, h_l(x)$ irreduzible Polynome in $\mathbb{Z}[x]$ sind. Damit ist die Existenz der Primfaktorzerlegung gezeigt.

Um die *Eindeutigkeit* der Zerlegung zu zeigen betrachten wir

$$f(x) = \epsilon p_1p_2\cdots p_kh_1(x)h_2(x)\cdots h_l(x) = \epsilon' p'_1p'_2\cdots p'_mh'_1(x)h'_2(x)\cdots h'_n(x)\ .$$

Da die Polynome $h_i(x)$ und $h_j(x)$ primitiv sind, sind es auch ihre Produkte. Der Faktor $\epsilon p_1p_2\cdots p_k$ und der Faktor $\epsilon' p'_1p'_2\cdots p'_m$ sind also beide ggT's der Koeffizienten von $f(x)$. Aber der ggT ist bis auf Multiplikation mit einer Einheit eindeutig bestimmt. Wegen der Eindeutigkeit der Primfaktorzerlegung in $\mathbb{Z}$ gilt dann $m = k$, und es existiert eine Numerierung und Einheiten ϵ_i mit $p_i = \epsilon_i p'_i$ für $i = 1, 2, \ldots, k$. Damit folgt

$$h_1(x)h_2(x)\cdots h_l(x) = \overline{\epsilon}h'_1(x)h'_2(x)\cdots h'_n(x)\ .$$

Wir betrachten dies als Zerlegung in $\mathbb{Q}[x]$. Nach dem Satz von Gauss (Satz 4.4) sind die Polynome $h_i(x)$ und $h'_j(x)$ auch irreduzibel in $\mathbb{Q}[x]$. Aber in $\mathbb{Q}[x]$ ist die Primfaktorzerlegung eindeutig. Es folgt $n = l$ und es existieren eine Numerierung und Einheiten δ_i in $\mathbb{Q}[x]$ mit $h_i(x) = \delta_i h'_i(x)$. Da die Einheiten in $\mathbb{Q}[x]$ gerade die Nichtnullelemente von $\mathbb{Q}$ sind, gibt es a_i, $b_i \in \mathbb{Z}$ mit $\delta_i = a_i/b_i$. Dann folgt

$$b_i h_i(x) = a_i h'_i(x) \ .$$

Nun sind aber $h_i(x)$ und $h'_i(x)$ primitiv. Also ist a_i bzw. b_i der ggT der Koeffizienten des in dieser Gleichung vorkommenden Polynoms. Folglich existiert eine Einheit μ_i in $\mathbb{Z}$ mit $a_i = \mu_i b_i$, und es ergibt sich

$$h_i(x) = \mu_i h'_i(x) \ .$$

Gerade dies blieb aber noch zu zeigen, um die Eindeutigkeit der Zerlegung nachzuweisen.

Dieser Beweis lässt sich stark verallgemeinern. Eine Analyse zeigt, dass man im wesentlichen die zwei folgenden Dinge benötigt hat:

(a) $\mathbb{Z}$ ist faktoriell,

(b) $\mathbb{Z}$ lässt sich in einen Körper $\mathbb{Q}$ einbetten, so dass jedes Element in $\mathbb{Q}$ in der Form a/b geschrieben werden kann mit a, $b \in \mathbb{Z}$.

Es ist nun nicht schwierig zu zeigen, dass die Konstruktion, die von $\mathbb{Z}$ zu $\mathbb{Q}$ führt in ganz analoger Weise für einen beliebigen Integritätsbereich R anstelle von $\mathbb{Z}$ durchgeführt werden kann. Man gewinnt so den *Quotientenkörper* Q von R. Natürlich gilt, dass Q den Ring R enthält und dass jedes Element von Q in der Form a/b mit $a, b \in R$ geschrieben werden kann.

Ist zusätzlich R faktoriell, so lässt sich der oben gegebene Beweis ohne irgendwelche Schwierigkeiten auf die allgemeinere Situation übertragen. (Die an gewissen Stellen für den betrachteten Spezialfall unnötig komplizierte Formulierung in unserem Beweis wurde im Hinblick auf diese Übertragung gewählt.) Dies liefert dann das folgende Resultat:

Satz 4.8 *Es sei R ein faktorieller Ring. Dann ist $R[x]$ ebenfalls faktoriell.*

Korollar 4.9 *Es sei R ein faktorieller Ring. Dann ist $R[x_1, x_2, \ldots, x_n]$ faktoriell.*

Beweis Wir beweisen mit Induktion nach n. Für $n = 1$ folgt das Korallar direkt aus Satz 4.8. Für $n \geq 2$ schreiben wir

$$R[x_1, x_2, \ldots, x_n] = (R[x_1, x_2, \ldots, x_{n-1}])\,[x_n]$$

und wenden darauf den Satz 4.8 an.

II.5 Der Satz von den zwei Quadraten

Wir behandeln in diesem Abschnitt die Frage, welche Primzahlen sich als Summe von zwei Quadraten schreiben lassen. Es gilt zum Beispiel $5 = 1^2 + 2^2$, $13 = 2^2 + 3^2$, aber 3, 7, 11 haben keine solche Darstellung. Es ist nicht von vorneherein klar und es dürfte in der Tat für manche überraschend sein, dass zur Beantwortung dieser Frage Überlegungen im Ring $\mathbb{Z}[i]$ nützlich sind. Ein erster Zusammenhang ergibt sich aus dem folgenden Tatsache:

Es sei p eine Primzahl mit $p = m^2 + n^2$. Dann gilt im Ring $\mathbb{Z}[i]$ die Zerlegung $p = (m + in)(m - in)$ mit $m, n \in \mathbb{Z}$.

Für das weitere Vorgehen werden einige Eigenschaften des Ringes $\mathbb{Z}[i]$ benötigt. Wir wissen bereits (siehe Satz 2.6), dass $\mathbb{Z}[i]$ ein Hauptidealbereich ist. Beim Beweis dieser Tatsache hat die Norm in $\mathbb{Z}[i]$ eine wichtige Rolle gespielt. Diese ist für das Element $a+ib$, $a, b \in \mathbb{Z}$ definiert durch $N(a+ib) = a^2+b^2$. Aus der Hauptidealeigenschaft folgt mit Theorem 3.6, dass in $\mathbb{Z}[i]$ die eindeutige Primfaktorzerlegung gilt.

Auch die Einheiten in $\mathbb{Z}[i]$ lassen sich mit Hilfe der Norm einfach identifizieren: es sind die Elemente ± 1, $\pm i$. Für eine Einheit ϵ in $\mathbb{Z}[i]$ gilt nämlich:

$$1 = N(\epsilon) \cdot N\left(\frac{1}{\epsilon}\right) = N(\epsilon) \cdot \frac{1}{N(\epsilon)} \ .$$

Daraus folgt $N(\epsilon) = 1$, da die Norm eines Elementes in $\mathbb{Z}[i]$ eine ganze Zahl sein muss, und damit $\epsilon = \pm 1, \pm i$.

Im Lichte dieser zusätzlichen Informationen lässt sich die einleitenden Bemerkung also in der folgenden etwas präziseren Form ausdrücken:

Ist p eine Primzahl, welche Summe von zwei Quadraten ist, so ist p in $\mathbb{Z}[i]$ kein *Primelement.*

Dank der Eigenschaften des Ringes $\mathbb{Z}[i]$ lässt sich davon nun auch die Umkehrung beweisen.

1. Behauptung *Es sei p eine Primzahl. Ist p in $\mathbb{Z}[i]$ kein Primelement, so ist p Summe von zwei Quadraten.*

Beweis Es sei $p = p_1 \cdot p_2 \cdots p_k$ mit Primelementen $p_l \in \mathbb{Z}[i]$ und $k \geq 2$. Dann gilt $1 \neq N(p) = p^2 = N(p_1) \cdot N(p_2) \cdots N(p_k)$. Wegen der eindeutigen Primfaktorzerlegung in $\mathbb{Z}$ schliessen wir daraus $k = 2$ und $N(p_1) = p = N(p_2)$. Ist nun $p_1 = m + in$, so folgt $N(p_1) = m^2 + n^2 = p$.

Im folgenden betrachten wir nur den Fall $p \neq 2$; für $p = 2$ gilt natürlich $p = 1^2 + 1^2$, so dass die Primzahl 2 eine Summe von zwei Quadraten ist. Wir bemerken als nächstes die einfache Tatsache, dass für die ungerade Zahl $t = 2a + 1,\ a \in \mathbb{Z}$ gilt $t^2 = 4a^2 + 4a + 1 \equiv 1 \pmod 4$.

2. Behauptung *Es sei p eine Primzahl mit $p = m^2 + n^2$. Dann ist $p \equiv 1 \pmod 4$.*

Beweis Es sei $p = m^2 + n^2$. Dann folgt nach der obigen Bemerkung $p \equiv 0, 1, 2 \pmod 4$. Da p ungerade ist, muss gelten $p \equiv 1 \pmod 4$.

3. Behauptung *Ist p eine Primzahl mit $p \equiv 1 \pmod 4$, so ist p kein Primelement in $\mathbb{Z}[i]$.*

Beweis Es sei $p = 4k + 1$. Betrachte $d = (\frac{p-1}{2})!$. Dann folgt $d^2 \equiv -1 \pmod p$. Um dies einzusehen gehen wir wie folgt vor: Mit den gegebenen Bezeichnungen lässt sich modulo p die Grösse d^2 wie folgt schreiben:

$$1 \cdot 2 \cdot 3 \cdots (2k)(-2k) \cdots (-2)(-1) \ .$$

Dies ist das Produkt aller Nichtnullelemente im Ring $\mathbb{Z}/(p)$. Diese Nichtnullelemente können andererseits modulo p als die $p - 1 = 4k$ Nullstellen des Polynoms $x^{4k} - 1$ angesehen werden. Aus diesem Grund lässt sich modulo p dieses Polynom in Linearfoktoren aufspalten:

$$(x-1)(x-2) \cdots (x-2k)(x+2k) \cdots (x+2)(x+1) \ .$$

Die explizite Berechnung des konstanten Terms des Polynoms liefert dann

$$d^2 \equiv 1 \cdot 2 \cdot 3 \cdots (2k)(-2k) \cdots (-2)(-1) \equiv -1 \bmod p \ .$$

Nun gilt $(d + i)(d - i) = d^2 + 1 \equiv 0 \pmod p$. Das heisst, es existiert $l \in \mathbb{Z}$ mit

$$(d + i)(d - i) = l \cdot p \ .$$

Wäre nun p ein Primelement in $\mathbb{Z}[i]$, so müsste p wegen der eindeutigen Primfaktorzerlegung in $\mathbb{Z}[i]$ entweder $d + i$ oder $d - i$ teilen. Man hätte dann $a, b, \in \mathbb{Z}$ mit

$$p \cdot (a + ib) = d \pm i \ .$$

Daraus folgt $p \cdot b = \pm 1$. Dies ist aber ein Widerspruch zur Tatsache, dass p eine Primzahl ist.

Mit den Behauptungen 1,2,3 ist der folgende Satz bewiesen:

Satz 5.1 *Es sei p eine ungerade Primzahl. Genau dann ist p eine Summe von zwei Quadraten, wenn $k \in \mathbb{Z}$ existiert mit $p = 4k + 1$.*

II.6 Der Satz von Mason und der grosse Satz von Fermat für komplexe Polynome

Die Fermatsche Vermutung dürfte allgemein bekannt sein:

Für $n \geq 3$ gibt es keine von Null verschiedenen ganzen Zahlen x, y, z mit

$$x^n + y^n = z^n \ .$$

Bekanntlich wurde diese Vermutung, die von P. Fermat (1607-1665) ausgesprochen worden ist, erst vor wenigen Jahren von A. Wiles bewiesen. Es waren dazu technisch ausserordentlich schwierige Überlegungen und ganz neue Beweisideen notwendig.[6]

Man kann die Frage, die mit der Fermatschen Vermutung aufgeworfen wird, natürlich auch für andere Ringe formulieren, z.B. für den Ring der komplexen Polynome $\mathbb{C}[t]$.

Gibt es nichtkonstante, teilerfremde Polynome $x, y, z \in \mathbb{C}[t]$ mit $x(t)^n + y(t)^n = z(t)^n$?

Diese Frage wurde (negativ) um die Jahrhundertwende mit Hilfe von Argumenten aus der algebraischen Geometrie beantwortet; es gilt also der Satz

Satz 6.1 *Für $n \geq 3$ gibt es keine nichtkonstanten, teilerfremden Polynome $x, y, z \in \mathbb{C}[t]$ mit $x(t)^n + y(t)^n = z(t)^n$.*

Hier wollen wir dafür einen elementaren Beweis angeben, der vom Satz von R.C. Mason ausgeht.[7]

Der Satz von Mason, der erst um 1983 entdeckt wurde, handelt von komplexen Polynomen. Wir schreiben die Elemente von $\mathbb{C}[t]$ in der Form

$$f(t) = c_1 \cdot \prod_{i=1}^{r} (t - \alpha_i)^{m_i} \ ,$$

wobei $\alpha_1, \alpha_2, \ldots, \alpha_r$ die (paarweise verschiedenen) Nullstellen des Polynoms $f(t)$ bezeichnen. Der Grad von $f(t)$ ist dann gegeben durch $\deg f = m_1 + m_2 + \cdots + m_r$. Die Anzahl der (verschiedenen) Nullstellen des Polynoms f bezeichnen wir mit $n_0(f)$, also

$$n_0(f) = r \ .$$

[6] Eine Beschreibung des Beweises ist im Rahmen dieses Textes nicht möglich. Ein allgemein verständlicher Text, der auf die Geschichte und die allgemeinen Umstände des Beweises von Wiles eingeht, ist das Buch von Simon Singh: *Fermats letzter Satz*, dtv, München 2000.

[7] Für den Satz von Mason und damit zusammenhängende Fragen, wie die *abc*-Vermutung, vergleiche man den für Studierende verständlich geschriebenen Artikel von Serge Lang: *Die abc-Vermutung.* Elemente der Mathematik, **48** (1993), 89-100.

Es ist offensichtlich, dass $\deg f$ gross sein kann und gleichzeitig $n_0(f)$ klein. Zum Beispiel besitzt $f(t) = (t-\alpha)^{1000}$ den Grad 1000, aber es ist $n_0(f) = 1$. Für Polynome f, g gilt allgemein $n_0(f) + n_0(g) \geq n_0(f \cdot g)$, und wenn sie teilerfremd sind, gilt sogar Gleichheit:

$$n_0(f) + n_0(g) = n_0(f \cdot g) \ .$$

Satz 6.2 (Satz von Mason) *Es seien $f, g, h \in \mathbb{C}[t]$ nichtkonstante, teilerfremde Polynome mit $f + g = h$. Dann gilt*

$$\max(\deg f, \deg g, \deg h) \leq n_0(f \cdot g \cdot h) - 1 \ .$$

Der Satz 6.2 besagt, dass die Relation $f+g = h$ den Grad der Polynome f, g, h beschränkt und zwar durch die Anzahl der verschiedenen Nullstellen der drei Polynome f, g, h.

Wir beweisen zuerst mit Hilfe Satzes 6.2 den grossen Satz den Satz von Fermat für komplexe Polynome, Satz 6.1.

Beweis Wir setzen $f(t) = x(t)^n$, $g(t) = y(t)^n$, $h(t) = z(t)^n$. Dann liefert der Satz von Mason

$$\deg x(t)^n \leq n_0(x(t)^n \cdot y(t)^n \cdot z(t)^n) - 1 \ .$$

Aber $\deg x(t)^n = n \cdot \deg x(t)$, und $n_0(x(t)^n) = n_0(x(t)) \leq \deg x(t)$, so dass folgt

$$n \cdot \deg x(t) \ \leq \ \deg x(t) + \deg y(t) + \deg z(t) - 1 \ .$$

Auf analoge Weise erhalten wir für $y(t)$ und $z(t)$ die Ungleichungen

$$\begin{aligned} n \cdot \deg y(t) &\leq \deg x(t) + \deg y(t) + \deg z(t) - 1 \ , \\ n \cdot \deg z(t) &\leq \deg x(t) + \deg y(t) + \deg z(t) - 1 \ . \end{aligned}$$

Die Addition dieser drei Ungleichungen liefert

$$n \cdot (\deg x(t) + \deg y(t) + \deg \ z(t)) \leq 3 \cdot (\deg x(t) + \deg y(t) + \deg z(t)) - 3 \ .$$

Es folgt

$$(n-3) \cdot (\deg x(t) + \deg y(t) + \deg z(t)) \leq -3 \ ,$$

was für $n \geq 3$ offensichtlich ein Widerspruch ist. Damit ist der "Satz von Fermat für Polynome" bewiesen.

Beweis des Satzes 6.2 In der Aussage des Satzes haben wir links den Grad und rechts n_0, also die Anzahl der verschiedenen Wurzeln eines Polynoms. Wir müssen deshalb einen Weg finden, um die Vielfachheiten der Wurzeln in den Griff zu bekommen. Aus diesem Grunde dividieren wir die Gleichung $f + g = h$ durch h und erhalten

$$\frac{f}{h} + \frac{g}{h} = 1 \ .$$

Setzen wir $R = f/h$, $S = g/h$, so folgt $R + S = 1$ und die Ableitung nach t liefert $R' + S' = 0$. Diese Beziehung schreiben wir in der Form

$$\frac{R'}{R}R + \frac{S'}{S}S = 0 \ . \tag{1}$$

Wir betrachten nun den Quotienten g/f. Mit unseren Bezeichnungen und mit der Beziehung (1) lässt sich dieser durch

$$\frac{g}{f} = \frac{S}{R} = -\frac{R'/R}{S'/S} \tag{2}$$

ausdrücken. Wir haben also g/f als Quotient von logarithmischen Ableitungen $F \rightsquigarrow F'/F$ schreiben können. Es stellt sich heraus, dass wir das mehrfache Auftreten der Wurzeln damit unter Kontrolle gebracht haben. In der Tat hat – wie Sie wissen – die logarithmische Ableitung die angenehme Eigenschaft, Produkte in Summen überzuführen:

$$\frac{(F \cdot G)'}{F \cdot G} = \frac{F'}{F} + \frac{G'}{G} \ .$$

Dies folgt direkt aus der Produktformel für die Ableitung. Dann gilt bekanntlich auch

$$\frac{(F/G)'}{F/G} = \frac{F'}{F} - \frac{G'}{G} \ .$$

Wenn wir unsere Polynome in der am Anfang angegebenen Form schreiben, also

$$\begin{aligned} f(t) &= c_1 \cdot \prod (t - \alpha_i)^{m_i} \ , \\ g(t) &= c_2 \cdot \prod (t - \beta_j)^{n_j} \ , \\ h(t) &= c_3 \cdot \prod (t - \gamma_k)^{l_k} \ , \end{aligned}$$

so erhalten wir für die logarithmischen Ableitungen die folgenden einfachen Ausdrücke

$$\frac{f'}{f} = \sum \frac{m_i}{t-\alpha_i} \ , \quad \frac{g'}{g} = \sum \frac{n_j}{t-\beta_j} \ , \quad \frac{h'}{h} = \sum \frac{l_k}{t-\gamma_k} \ .$$

Mit $R = f/h$ und $S = g/h$ und indem wir die Regeln der logarithmischen Ableitung verwenden, erhalten wir aus (2)

$$\frac{g}{f} = -\frac{f'/f - h'/h}{g'/g - h'/h} = -\frac{\sum \frac{m_i}{t-\alpha_i} - \sum \frac{l_k}{t-\gamma_k}}{\sum \frac{n_j}{t-\beta_j} - \sum \frac{l_k}{t-\gamma_k}} \ . \tag{3}$$

Es sei nun $D(t)$ das Polynom

$$D(t) = \prod (t-\alpha_i) \cdot \prod (t-\beta_j) \cdot \prod (t-\gamma_k) \ .$$

Offensichtlich gilt $\deg D(t) = n_0(f \cdot g \cdot h)$. Daraus folgt

$$\deg \left(\frac{D(t)}{t-\alpha_i} \right) = n_0(f \cdot g \cdot h) - 1 = \deg \left(\frac{D(t)}{t-\beta_j} \right) = \deg \left(\frac{D(t)}{t-\gamma_k} \right) \ .$$

Erweitern wir den Bruch (3) mit $D(t)$, so erhalten wir

$$\frac{g}{f} = -\frac{\sum \frac{m_i}{t-\alpha_i} - \sum \frac{l_k}{t-\gamma_k}}{\sum \frac{n_j}{t-\beta_j} - \sum \frac{l_k}{t-\gamma_k}} \cdot \frac{D(t)}{D(t)} = \frac{\text{Polynom vom Grad} \leq n_0(f \cdot g \cdot h) - 1}{\text{Polynom vom Grad} \leq n_0(f \cdot g \cdot h) - 1} \ .$$

Damit ist g/f als Quotient von zwei Polynomen geschrieben, deren Grad höchstens $n_0(f \cdot g \cdot h) - 1$ ist. Da f und g teilerfremd sind, folgt daraus, dass auch die Grade der Polynome f und g höchstens $n_0(f \cdot g \cdot h) - 1$ sein können. Und schliesslich hat das Polynom h, als Summe $h = f + g$, ebenfalls höchstens diesen Grad. Damit ist der Satz von Mason bewiesen.

Kapitel III. Körper

Einleitung

Die Mathematik hat sich eigentlich mit Körpern beschäftigt, seit ihr rationale Zahlen bekannt sind. Allerdings war dem mathematischen Denken vor Cantor und Dedekind der *Begriff* des Körpers, so wie wir heute kennen, im Grunde genommen fremd. Noch zu Zeiten von N. Abel und E. Galois betrachtete man einfach diejenigen reellen (oder komplexen) Zahlen die sich aus einer Anzahl von gegebenen reellen (oder komplexen) Zahlen durch rationale Operationen gewinnen liessen und mit denen man demzufolge in der *üblichen Art* rechnen konnte. Die *Menge* dieser Elemente wurde erst seit Dedekind als Objekt mathematischer Forschung "begriffen"; der Name "Körper" stammt denn auch von R. Dedekind (1831-1916).[8]

Auf A. L. Cauchy (1789-1857) geht die Beschreibung von $\mathbb{C}$ als $\mathbb{R}[x]/(x^2+1)$ zurück. Erst viele Jahre später zeigte L. Kronecker (1821-1891), dass jeder Körper algebraischer Zahlen (von endlichem Grad) sich als $\mathbb{Q}[x]/(f(x))$ beschreiben lässt, wo $f(x)$ ein irreduzibles rationales Polynom ist. H. Weber (1842-1913)[9] setzte dann axiomatische Denkweisen ein, um Kroneckers Vorgehen auf endliche Erweiterungen eines beliebigen Körpers zu verallgemeinern. Im Jahre 1910 hat E. Steinitz (1871-1928) einer langen, fundamentalen Arbeit die Körpertheorie von Grund auf axiomatisch zu behandeln: Durch diese Arbeit wurde die bis heute gebräuchliche Terminologie der Körpertheorie festgelegt.

Das vorliegende Kapitel dient dazu, die *grundlegendsten* Aspekte der Körpertheorie darzustellen, wobei die Galoistheorie vollständig ausgeklammert bleibt; ihr ist das Kapitel VI des vorliegenden Textes gewidmet. Aufgenommen wurden andererseits Abschnitte über zwei Themenkreise, welche *Anwendungen* der Körpertheorie betreffen: die Unmöglichkeitsbeweise für die klassischen geometrischen Probleme wie die Verdoppelung des Würfels und die Dreiteilung des Winkels (siehe Abschnitt III.3) sowie einige grundlegende Bemerkungen zur Codierungstheorie (siehe Abschnitt III.5).

[8] Erwähnt sei hier, dass Richard Dedekind von 1858 bis 1862 Professor am Eidgenössischen Polytechnikum in Zürich war. Im Jahre 1909 wurde er zum Ehrendoktor der ETH ernannt.

[9] Heinrich Weber war von 1870 bis 1875 Professor am Eidgenössischen Polytechnikum in Zürich. Richard Dedekind hat später eng mit Heinrich Weber zusammengearbeitet.

III.1 Körpererweiterungen

Definition Es seien K, L, $K \subseteq L$ zwei Körper. Dann heisst der Körper L eine *Körpererweiterung* von K. Die Körpermultiplikation von Elementen aus K mit Elementen aus L macht L zu einem Vektorraum über K. Als solcher besitzt L eine bestimmte Dimension $\dim_K L$. Sie heisst *Körpergrad* von L über K und wird mit $[L : K]$ bezeichnet. Eine Körpererweiterung $K \subseteq L$ von endlichem Körpergrad heisst *endlich*.

Satz 1.1 *Es seien $K \subseteq K' \subseteq K''$ drei Körper. Ist K' eine endliche Körpererweiterung von K und K'' eine endliche Körpererweiterung von K', dann ist K'' eine endliche Körpererweiterung K, und es gilt*

$$[K'' : K] = [K'' : K'] \cdot [K' : K] \ .$$

Beweis Es sei $\{\alpha_1, \alpha_2, \ldots, \alpha_r\}$ eine Basis von K' über K und $\{\beta_1, \beta_2, \ldots, \beta_s\}$ eine Basis von K'' über K'. Wir behaupten, dass $\{\alpha_i\beta_j\}$, $i = 1, 2, \ldots, r$, $j = 1, 2, \ldots, s$ eine Basis von K'' über K ist. Dazu beweisen wir *erstens*, dass $\{\alpha_i\beta_j\}$ linear unabhängig ist. Es sei $\sum c_{ij}\alpha_i\beta_j = 0$ mit $c_{ij} \in K$. Dann gilt $\sum_j \left(\sum_i c_{ij}\alpha_i\right)\beta_j = 0$. Wegen $\sum c_{ij}\alpha_i \in K'$ und weil $\{\beta_1, \beta_2, \ldots, \beta_s\}$ eine K'-Basis von K'' ist, folgt daraus $\sum_i c_{ij}\alpha_i = 0$. Da $\{\alpha_1, \alpha_2, \ldots, \alpha_r\}$ eine Basis von K' über K ist, ergibt sich schliesslich $c_{ij} = 0$. *Zweitens* behaupten wir, dass $\{\alpha_i\beta_j\}$ ein Erzeugendensystem von K'' über K ist. Es sei $\gamma \in K''$. Dann existieren $d_j \in K'$ mit $\gamma = \sum d_j\beta_j$. Aber zu d_j existieren $c_{ij} \in K$ mit $d_j = \sum c_{ij}\alpha_i$. Damit folgt $\gamma = \sum c_{ij}\alpha_i\beta_j$.

Korollar 1.2 *Es seien $K \subseteq K' \subseteq K''$ drei Körper. Dann folgt $[K' : K] \mid [K'' : K]$. Insbesondere gilt: Wenn $[K'' : K]$ eine Primzahl ist, so gibt es zwischen K'' und K keinen Zwischenkörper.*

Definition Es sei $K \subseteq L$ eine Körpererweiterung. Das Element $\alpha \in L$ heisst *algebraisch* über K, wenn $f(x) \in K[x]$ existiert mit $f(\alpha) = 0$. Falls kein solches Polynom existiert, so heisst α *transzendent* über K.

Beispiele

(a) Es sei $K = \mathbb{Q}$, $\alpha = \sqrt{2}$. Dann ist $f(x) = x^2 - 2 \in K[x]$ ein Polynom mit $\sqrt{2}$ als Nullstelle. Damit ist $\sqrt{2}$ algebraisch über $\mathbb{Q}$.

(b) Es kann bewiesen werden, dass e transzendent ist (C. Hermite 1822-1901; 1873) und dass π transzendent ist (C.L.F. Lindemann 1852-1939; 1882).

Es sei $K \subseteq L$ und $\alpha \in L$ algebraisch über K. Dann gibt es ein Polynom $0 \neq f(x) \in K[x]$ mit $f(\alpha) = 0$. Wir betrachten die Menge V aller Polynome $f(x) \in K[x]$ mit $f(\alpha) = 0$.

Dann ist mit $f_1(x),\ f_2(x) \in V$ auch $f_1(x)+f_2(x)$ und $-f_1(x) \in V$ und für alle $g(x) \in K[x]$ gilt $g(x) \cdot f_1(x) \in V$. Die Menge $V \subseteq K[x]$ ist folglich ein Ideal.

Wir wissen, dass $K[x]$ ein Hauptidealbereich ist. Deshalb gilt $V = (h(x))$, wobei $h(x)$ ein Polynom von minimalem Grad in V ist. Das Polynom $h(x)$ ist bis auf eine Einheit in $K[x]$, also bis auf ein Element von K eindeutig bestimmt. Wählen wir also $h(x)$ so, dass der höchste Koeffizient 1 ist, so ist $h(x)$ eindeutig bestimmt. Ein Polynom, dessen höchster Koeffizient 1 ist, heisst *normiert*.

Satz 1.3 *Es sei $K \subseteq L$ eine Körpererweiterung, $\alpha \in L$ sei algebraisch über K. Dann gehört zu α ein eindeutig bestimmtes irreduzibles normiertes Polynom $h(x)$ in $K[x]$ mit $h(\alpha) = 0$ und mit der Eigenschaft, dass zu $f(x) \in K[x]$ mit $f(\alpha) = 0$ stets ein Polynom $g(x) \in K[x]$ existiert mit $f(x) = g(x) \cdot h(x)$.*

Beweis Es bleibt nur, die Irreduzibilität von $h(x)$ zu zeigen. Wäre $h(x) = h_1(x) \cdot h_2(x)$ mit $\deg h_i(x) \geq 1$, so hätte man $0 = h(\alpha) = h_1(\alpha) \cdot h_2(\alpha)$. Daraus folgt $h_1(\alpha) = 0$ oder $h_2(\alpha) = 0$, im Widerspruch zur Minimalität von $h(x)$.

Definition Das Polynom $h(x) \in K[x]$, das oben konstruiert worden ist, heisst das *Minimalpolynom* von α; sein Grad heisst *Grad* von α.

Beispiele

(c) Es sei $K \subseteq L$, $\alpha \in L$. Genau für $\alpha \in K$ ist α algebraisch vom Grad 1 über K.

Beweis Es sei α algebraisch von Grad 1. Dann existiert $b \in K$ mit $h(x) = x + b$ und $0 = h(\alpha) = \alpha + b$, und es folgt $\alpha = -b \in K$. Die Umkehrung ist trivial.

(d) Es sei $K = \mathbb{Q}$, $a \in \mathbb{Z}$. Die reelle Zahl $\alpha = \sqrt[n]{a}$ ist Nullstelle von $f(x) = x^n - a \in K[x]$. Für $a = p_1 p_2^{\alpha_2} \cdots p_k^{\alpha_k}$, wo $p_1, p_2, \ldots, p_k$ paarweise verschiedene Primzahlen bezeichnen, ist $f(x)$ irreduzibel (siehe Abschnitt II.4). In diesem Fall ist also $f(x)$ das zu α gehörige Minimalpolynom; der Grad von α ist n.

Definition Ein algebraisches Element über $\mathbb{Q}$ heisst *algebraische Zahl*.

Es gibt höchstens abzählbar unendlich viele rationale Polynome und deshalb nur höchstens abzählbar unendlich viele algebraische Zahlen. Daraus folgt, dass überabzählbar unendlich viele transzendente reelle Zahlen existieren.

Satz 1.4 *Es sei $K \subseteq L$ eine endliche Körpererweiterung mit $[L : K] = n$. Dann ist jedes Element $\alpha \in L$ algebraisch über K und zwar von einem Grad $\leq n$.*

Beweis Wir betrachten $1, \alpha, \alpha^2, \ldots, \alpha^n$. Wegen $\dim_K L = n$ sind diese $n+1$ Elemente von L linear abhängig über K. Deshalb existieren $a_i \in K$, nicht alle gleich Null, mit $0 = \sum_{i=0}^{n} a_i \alpha^i$. Dann ist aber $f(x) = \sum a_i x^i \in K[x]$ ein Polynom mit $f(\alpha) = 0$ und α ist algebraisch von einem Grad $\leq n$.

Definition Eine Körpererweiterung $K \subseteq L$ heisst *algebraisch*, falls jedes Element $\alpha \in L$ über K algebraisch ist.

Nach obigem ist jede endliche Körpererweiterung algebraisch. Das Umgekehrte gilt nicht, wie wir später sehen werden.

III.2 Adjunktion von Nullstellen

Es sei $K \subseteq L$ eine Körpererweiterung, und es sei $\alpha \in L$ algebraisch über K mit Minimalpolynom $h(x) \in K[x]$ vom Grad n. Wir betrachten die Unterkörper K' von L mit $K \subseteq K' \subseteq L$ und $\alpha \in K'$. Es ist klar, dass der Durchschnitt von allen diesen Unterkörpern der kleinste Unterkörper von L ist, der K und α umfasst. Wir bezeichnen diesen mit $K(\alpha)$ und sagen, $K(\alpha)$ entstehe in L durch *Adjunktion* von α zu K.

Als nächstes geben wir eine konstruktive Beschreibung von $K(\alpha)$. Zu diesem Zweck untersuchen wir den Homomorphismus von Ringen mit Eins $\phi : K[x] \to L$, der durch $\phi\,(f(x)) = f(\alpha)$, $f(x) \in K[x]$ definiert ist. Der Kern von ϕ besteht aus allen Polynomen in $K[x]$, die α als Nullstelle besitzen; er ist also gleich dem Hauptideal, das von $h(x)$, dem Minimalpolynom von α erzeugt wird. Da $h(x)$ irreduzibel ist, ist $h(x)$ ein Primelement im Hauptidealbereich $K[x]$, und damit ist $(h(x))$ ein maximales Ideal. Nun ist ein Ring modulo einem maximalen Ideal ein Körper; somit folgt, dass

$$\text{im } \phi \cong K[x]/(h(x))$$

ein Körper ist. Dieser enthält natürlich K (Bilder der Polynome $f(x) = a_0 \in K$) und α (Bild des Polynoms $f(x) = x$). Damit gilt $\text{im}\,\phi \supseteq K(\alpha)$. Anderseits ist natürlich für jedes Polynom $f(x) = \sum a_i x^i$ das Bild $\phi(f(x)) = \sum a_i \alpha^i$ in $K(\alpha)$. Es gilt folglich auch $\text{im}\,\phi \subseteq K(\alpha)$. Damit haben wir den folgenden Satz erhalten.

Satz 2.1 *Es sei $K \subseteq L$, $\alpha \in L$, α algebraisch über K mit Minimalpolynom $h(x) \in K[x]$. Dann ist*

$$\phi_* : K[x]/(h(x)) \xrightarrow{\sim} K(\alpha).$$

Jedes Element von $K[x]$ kann geschrieben werden als $f(x) = q(x) \cdot h(x) + r(x)$ mit

$0 \leq \deg r(x) \leq (\deg h(x)) - 1 = n - 1$. Daraus folgt, dass jedes Element in $K(\alpha)$ von der Form $\sum_{i=0}^{n-1} a_i \alpha^i, a_i \in K$ ist. Es gilt sogar der Satz

Satz 2.2 *Es sei $K \subseteq L$, $\alpha \in L$, α algebraisch über K von Grad n. Dann lässt sich jedes Element in $K(\alpha)$ eindeutig in der Form $\sum_{i=0}^{n-1} a_i \alpha^i$ schreiben mit $a_i \in K$.*

Beweis Gilt

$$\sum_{i=0}^{n-1} a_i \alpha^i = \sum_{i=0}^{n-1} b_i \alpha^i \,,$$

so folgt

$$0 = \sum_{i=0}^{n-1} (a_i - b_i) \alpha^i.$$

Wäre $a_i - b_i \neq 0$ für gewisses i, so wäre $\sum_{i=0}^{n-1} (a_i - b_i) x^i$ ein nichttriviales Polynom in $K[x]$ mit α als Nullstelle und von kleinerem Grad als n. Dies ist ein Widerspruch.

Korollar 2.3 *Es sei α algebraisch über K vom Grad n. Dann ist $K \subseteq K(\alpha)$ eine endliche Körpererweiterung mit $[K(\alpha) : K] = n$.*

Aus obigem ergibt sich, dass $\{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$ eine Basis von $K(\alpha)$ über K ist.

Beispiele

(a) Die reelle Zahl $\sqrt{2}$ ist algebraisch vom Grad 2 über $\mathbb{Q}$; es gilt daher

$$\mathbb{Q}(\sqrt{2}) = \left\{ a_1 + a_2 \sqrt{2} \mid a_i \in \mathbb{Q} \right\} .$$

(b) Die reelle Zahl $\sqrt[5]{2}$ ist algebraisch von Grad 5 über $\mathbb{Q}$, denn $x^5 - 2$ ist irreduzibel. Deshalb gilt

$$\mathbb{Q}(\sqrt[5]{2}) = \left\{ a_0 + a_1 \sqrt[5]{2} + a_2 (\sqrt[5]{2})^2 + \cdots + a_4 (\sqrt[5]{2})^4 \mid a_i \in \mathbb{Q} \right\} .$$

Satz 2.4 *Es sei $K \subseteq L$ eine endliche Körpererweiterung vom Grad n, und es sei $\alpha \in L$ algebraisch vom Grad m über K. Dann gilt $m \mid n$.*

Beweis $K \subseteq K(\alpha) \subseteq L$ impliziert $n = [L : K] = [L : K(\alpha)] \cdot [K(\alpha) : K] = q \cdot m$.

Satz 2.5 *Es sei $K \subseteq L$ eine Körpererweiterung. Die Elemente $\alpha, \beta \in L$ seien algebraisch über K. Dann sind $\alpha \pm \beta$, $\alpha\beta$, α/β (für $\beta \neq 0$) ebenfalls algebraisch über K. Mit andern Worten: die algebraischen Elemente über K bilden einen Unterkörper von L.*

Beweis Es sei α algebraisch über K vom Grad m und β algebraisch über K vom Grad n. Dann ist $K \subseteq K(\alpha)$ eine algebraische Körpererweiterung vom Grad m, und es ist β algebraisch über $K(\alpha)$ vom Grad $\leq n$. Somit ist $K(\alpha) \subseteq (K(\alpha))(\beta) = K'$ eine algebraische Körpererweiterung mit Grad $\leq m$. Die Erweiterung $K \subseteq K'$ ist damit endlich und deshalb algebraisch, insbesondere sind $\alpha \pm \beta$, $\alpha\beta$, α/β, für $\beta \neq 0$, als Elemente von K' algebraisch über K.

Wir betrachten $\mathbb{Q} \subseteq \mathbb{R}$. Die algebraischen Elemente in $\mathbb{R}$ bilden einen Körper A mit $\mathbb{Q} \subseteq A \subseteq \mathbb{R}$. Der Körper A ist eine algebraische Erweiterung von $\mathbb{Q}$, aber *nicht* endlich. Es gibt nämlich in A für jede natürliche Zahl $m \geq 2$ Elemente vom Grad m, z.B. $\sqrt[m]{2}$. Andererseits besitzt in einer endlichen Körpererweiterung vom Grad m jedes Element einen Grad $\leq m$.

Bis anhin haben wir ganz innerhalb eines vorgegebenen Körpers L operiert. Wir stellen aber in der Aussage von Satz 2.1 fest, dass der Körper L nur auf der rechten Seite (implizit) vorkommt: $\phi_* : K[x]/(h(x)) \xrightarrow{\sim} K(\alpha)$. Auf der linken Seite kommt nur K und ein irreduzibles Polynom $h(x) \in K[x]$ vor.

Es ist damit ganz natürlich, sich von der Vorgabe von L zu befreien und nur von K und $h(x)$ auszugehen. Es ist zu fragen, was die Eigenschaften von $K[x]/(h(x))$ sind.

Da $K[x]$ ein Hauptidealbereich und $h(x) \in K[x]$ ein Primelement ist, ist das Ideal $(h(x))$ maximal. Damit ist $K[x]/(h(x))$ ein Körper. Da jedes $g(x) \in K[x]$ geschrieben werden kann als $q(x) \cdot h(x) + r(x)$ mit $0 \leq \deg r(x) \leq (\deg h(x)) - 1$ kann jedes Element in $K[x]/(h(x))$ repräsentiert werden durch ein Polynom $r(x) \in K[x]$ mit $0 \leq \deg r(x) \leq (\deg h(x)) - 1$, und zwar in eindeutiger Weise. Die zu den 'konstanten' Polynomen $r(x) = a \in K$ gehörigen Restklassen in $K[x]/(h(x))$ bilden offensichtlich einen zu K isomorphen Unterkörper von $K[x]/(h(x))$. Identifizieren wir diesen mit K, so wird $K[x]/(h(x))$ zu einer Körpererweiterung von K.

Wir behaupten nun: *Das Polynom $h(y)$ in $K[y]$ besitzt in $K[x]/(h(x))$ die Nullstelle $r(x)+(h(x)) = x + (h(x))$.*

Beweis Es sei $h(y) = a_0 + a_1 y + \cdots + a_n y^n$, $a_i \in K$. Dann ist

$$\begin{aligned} h(x + (h(x))) &= a_0 + a_1(x + h(x)) + \cdots + a_n(x + h(x))^n \\ &= a_0 + a_1 x + \cdots + a_n x^n + (h(x)) = h(x) + (h(x)) \\ &= (h(x)) \ . \end{aligned}$$

Zusammenfassend können wir folgenden Satz aussprechen:

Satz 2.6 *Es sei $h(x)$ ein irreduzibles Polynom in $K[x]$ vom Grad n. Dann ist $L = K[x]/(h(x))$ ein Erweiterungskörper von K, in dem α existiert mit $h(\alpha) = 0$. Ferner gilt $[L : K] = n$.*

Geht man von $K \subseteq K'$, $\alpha \in K'$ mit $h(\alpha) = 0$ aus, so gilt, wie wir oben gesehen haben, $K[x]/(h(x)) \cong K(\alpha)$.

Das oben beschriebene Verfahren heisst *Adjunktion einer symbolischen Nullstelle.*

Korollar 2.7 *Es sei $f(x) \in K[x]$ ein beliebiges Polynom vom Grad n. Dann existiert ein Erweiterungskörper L von K mit $[L : K] \leq n$, in dem $f(x)$ eine Nullstelle besitzt.*

Korollar 2.8 *Es sei $f(x) \in K[x]$ ein beliebiges Polynom vom Grad n. Dann existiert ein Erweiterungskörper L von K mit $[L : K] \leq n!$, über dem $f(x)$ in Linearfaktoren zerfällt.*

Beweis Wir beweisen mit Induktion nach n. Für $n = 1$ ist nichts zu beweisen. Es sei $n \geq 2$. Nach dem obigen Korollar können wir eine Nullstelle α von $f(x)$ adjungieren. Wir erhalten einen Körper $K_1 \supseteq K$, über dem $f(x)$ zerfällt als $(x-\alpha) \cdot g(x)$ mit $g(x) \in K_1[x]$. Nach Induktion existiert ein Erweiterungskörper $L \supseteq K_1$, über dem $g(x)$ in Linearfaktoren zerfällt. Dann zerfällt $f(x)$ über L in Linearfaktoren. Da nach Induktion $[L : K_1] \leq (n-1)!$ gilt, folgt $[L : K] \leq n \cdot (n-1)! = n!$.

Definition Es sei $f(x) \in K[x]$ gegeben. Der Oberkörper L von K von minimalem Grad über K, über dem $f(x)$ in Linearfaktoren zerfällt, heisst *Zerfällungskörper* von $f(x)$ über K. Natürlich gilt $L = K(\alpha_1, \ldots, \alpha_n)$.

Satz 2.9 *Der Zerfällungskörper eines Polynoms $f(x)$ in $K[x]$ ist bis auf Isomorphie eindeutig bestimmt.*

Dieser Satz folgt unmittelbar aus dem folgenden, etwas genauer umschriebenen Resultat.

Satz 2.10 *Es sei $f(x) \in K[x]$, und L ein Zerfällungskörper von $f(x)$ über K. Ferner sei $\iota : K \xrightarrow{\sim} K'$ ein Körperisomorphismus und L', $L' \supseteq K'$ ein Körper über dem $\iota f(x)$ in Linearfaktoren zerfällt. Dann gibt es einen (injektiven) Körperhomomorphismus $\phi : L \to L'$ mit $\phi|_K = \iota$.*

Für den Beweis benötigen wir das folgende Lemma.

Lemma 2.11 *Es sei $K \subseteq L$ eine Körpererweiterungen, und es sei $h(x) \in K[x]$ das Minimalpolynom von $\alpha \in L$. Ferner sei $\iota : K \to K'$ ein Isomorphismus von Körpern und $K' \subseteq L'$ eine weitere Körpererweiterung. Schliesslich besitze das Polynom $\iota h(x) \in K'[x]$ in L' die Nullstelle α'. Dann existiert ein Körperisomorphismus $\phi : K(\alpha) \to K'(\alpha')$ mit $\phi|_K = \iota$ und $\phi(\alpha) = \alpha'$.*

Beweis Der Isomorphismus $\iota : K[x] \xrightarrow{\sim} K'[x]$ induziert einen Isomorphismus

$$\iota' : K[x]/(h(x)) \xrightarrow{\sim} K'[x]/(\iota h(x)).$$

Damit erhält man einen Isomorphismus

$$\begin{array}{ccccccc} K(\alpha) & \stackrel{f^{-1}}{\to} & K[x]/(h(x)) & \stackrel{\iota'}{\to} & K'[x]/(\iota h(x)) & \stackrel{f'}{\to} & K'(\alpha') \\ \alpha & \mapsto & x+(h(x)) & \mapsto & x+(\iota h(x)) & \mapsto & \alpha' \end{array}$$

welcher offensichtlich die verlangten Eigenschaften hat.

Beweis des Satzes 2.10 Wir führen den Beweis mit Induktion nach dem Grad von $f(x)$. Im Falle $\deg(f(x)) = 1$ ist nichts zu beweisen. Es sei $n = \deg(f(x)) > 1$. Dann zerfällt $f(x)$ in $L[x]$ in Linearfaktoren,

$$f(x) = a_n(x-\alpha_1)\cdots(x-\alpha_n)\ ,\ \alpha_1,\ldots,\alpha_n \in L\ .$$

Es sei $m(x)$ das Minimalpolynom von α_1 in $K[x]$. Aus $m(x) \mid f(x)$ folgt $\iota m(x) \mid \iota f(x)$. Da $\iota f(x)$ über L' in Linearfaktoren zerfällt, muss gelten

$$\iota m(x) = (x-\alpha_1')\cdots(x-\alpha_r'),\ \alpha_1',\ldots,\alpha_r' \in L'.$$

Ferner ist $\iota m(x)$ irreduzibel über K', also das Minimalpolynom von (zum Beispiel) α_1' über K'. Nach Lemma 2.11 existiert ein Isomorphismus $\kappa : K(\alpha_1) \stackrel{\sim}{\to} K'(\alpha_1')$ mit $\kappa|_K = \iota$ und $\kappa(\alpha_1) = \alpha_1'$. Nun ist L ein Zerfällungskörper von $g(x) = f(x)/(x-\alpha_1)$ über $K(\alpha_1)$ und $\kappa(g(x)) = \kappa(f(x)/(x-\alpha_1)) = \iota f(x)/(x-\alpha_1')$ zerfällt in $L'[x]$ in Linearfaktoren. Nach Induktion gibt es einen injektiven Körperhomomorphismus $\phi : L \to L'$ mit $\phi|_{K(\alpha_1)} = \kappa$. Also gilt auch $\phi|_K = \iota$.

III.3 Konstruktion mit Zirkel und Lineal

Die Geschichte der Mathematik kennt im Bereich der elementaren Geometrie einige ganz berühmte Probleme:

(a) Winkeldreiteilung,

(b) Würfelverdopplung (Delisches Problem),

(c) Konstruktion von regulären Vielecken, z.B. 7-Eck,

(d) Quadratur des Kreises.

Dabei ist die präzise Frage jeweils die, ob die Aufgabe mit *Zirkel und Lineal* lösbar sei. Einige dieser Probleme haben auch Kreise ausserhalb der Mathematik angesprochen: Humanisten erzählen die Geschichte rund um den Ursprung des Delischen Problems, sogar Journalisten sprechen von der Quadratur des Kreises. Zur Zeit der Blüte der antiken griechischen Geometrie blieben diese Fragen bekanntlich offen; erst in neuerer Zeit wurden sie beantwortet. Dazu trug ganz wesentlich die Einführung der analytischen Geometrie (Descartes 1596-1650) bei, welche die Geometrie insgesamt und damit auch diese Probleme einer algebraischen Behandlung zugänglich machten. Allerdings hatte dann die Algebra die notwendigen Hilfsmittel erst etwa zwei Jahrhunderte später zur Verfügung.

Wir werden in dieser Vorlesung, die Unlösbarkeit von (a), (b), (c) zeigen können, für (d) brauchen wir einen weiteren Satz, den wir ohne Beweis zitieren.

Es sei eine Einheitslänge 1 gegeben.

Definition Eine reelle Zahl α heisst *konstruierbar*, wenn ausgehend von der Einheitslänge mit Zirkel und Lineal eine Strecke der Länge α konstruiert werden kann.

Mit α, β sind auch $\alpha \pm \beta$, $\alpha \cdot \beta$ und α/β mit $\beta \neq 0$ konstruierbar. Die konstruierbaren Zahlen bilden aus diesem Grund einen Unterkörper W der reellen Zahlen, $\mathbb{Q} \subseteq W \subseteq \mathbb{R}$. Der Körper W ist damit eine Körpererweiterung von $\mathbb{Q}$.

Es sei L irgend ein Unterkörper der reellen Zahlen. Wir betrachte alle Punkte (x, y) in $\mathbb{R}^2$, deren Koordinaten beide in L liegen. Wir nennen die Menge dieser Punkte die *Ebene von* L. Eine Gerade, die zwei Punkte in der Ebene von L verbindet, hat eine Gleichung $ax + by + c = 0$ mit $a, b, c \in L$. Ein Kreis mit Mittelpunkt in der Ebene von L und einem Punkt in der Ebene von L auf dem Umfang hat eine Gleichung $x^2 + y^2 + ax + by + c = 0$ mit $a, b, c \in L$. Diese Geraden und Kreise heissen die *Geraden und Kreise* der Ebene von L.

Zwei Geraden in der Ebene von L, die sich in $\mathbb{R}^2$ schneiden, haben einen Schnittpunkt in der Ebene von L. Für eine Gerade und einen Kreis in der Ebene von L, die sich in $\mathbb{R}^2$ schneiden, liegen im allgemeinen die Schnittpunkte *nicht* in der Ebene von L. *Aber*, die Schnittpunkte besitzen Koordinaten, die für ein gewisses $\gamma > 0$ aus L in einer Körpererweiterung $L(\sqrt{\gamma})$ liegen. Zwei Kreise in der Ebene von L, die sich in $\mathbb{R}^2$ schneiden, besitzen Schnittpunkte, deren Koordinaten für ein gewisses $\gamma > 0$ aus L in einem $L(\sqrt{\gamma})$ liegen. Diese Tatsachen sind einfach zu beweisen; wir überlassen die Beweise deshalb dem Leser.

Wir folgern: *Irgend ein Konstruktionsschritt in der Ebene von L liefert einen Punkt in der Ebene einer Erweiterung* $L(\sqrt{\gamma})$ *mit* $\gamma \in L$, $\gamma > 0$.

Umgekehrt lässt sich zeigen: Ist $\gamma \in L$, $\gamma > 0$, dann lässt sich $\sqrt{\gamma}$ und damit jeder Punkt in der Ebene von $L(\sqrt{\gamma})$ konstruieren. Prägnanter ausgedrückt: *Ist L konstruierbar, dann ist auch* $L(\sqrt{\gamma})$ *konstruierbar.*

Eine reelle Zahl α ist folglich genau dann konstruierbar, wenn es positive reelle Zahlen

$\gamma_1, \gamma_2, \ldots, \gamma_n$ gibt, mit $\gamma_i \in \mathbb{Q}\left(\sqrt{\gamma_1}, \sqrt{\gamma_2}, \ldots, \sqrt{\gamma_{i-1}}\right)$ für $i = 1, 2, 3, \ldots, n$ und $\alpha \in K = \mathbb{Q}\left(\sqrt{\gamma_1}, \sqrt{\gamma_2}, \ldots, \sqrt{\gamma_n}\right)$.

Satz 3.1 *Ist $\alpha \in \mathbb{R}$ konstruierbar, so liegt α in einer Erweiterung K von $\mathbb{Q}$ mit $[K : \mathbb{Q}]$ eine 2er Potenz.*

Beweis Es gilt $\left[\left(\mathbb{Q}\left(\sqrt{\gamma_1}, \ldots, \sqrt{\gamma_i}\right)\right)\left(\sqrt{\gamma_{i+1}}\right) : \mathbb{Q}\left(\sqrt{\gamma_1}, \ldots, \sqrt{\gamma_i}\right)\right] \leq 2$. Die Zusammensetzung der Körpererweiterungen liefert dann das Resultat.

Korollar 3.2 *Es sei $\alpha \in \mathbb{R}$ algebraisch über $\mathbb{Q}$ vom Grad k. Ist k keine Potenz von 2, so ist α nicht konstruierbar.*

Beweis Wäre α konstruierbar, so müsste $K \supseteq \mathbb{Q}$ existieren mit $[K : \mathbb{Q}] = 2^r$, $\alpha \in K$. Aber dann müsste wegen $\mathbb{Q} \subseteq \mathbb{Q}(\alpha) \subseteq K$, auch $[\mathbb{Q}(\alpha) : \mathbb{Q}]$ eine 2er Potenz sein.

Satz 3.3 *Es ist unmöglich, mit Zirkel und Lineal einen Würfel zu verdoppeln.*

Beweis Wäre dies möglich, so könnte α mit $\alpha^3 = 2$ konstruiert werden. Aber $f(x) = x^3 - 2$ ist irreduzibel über $\mathbb{Q}$ (siehe Abschnitt II.4), so dass α den Grad 3 über $\mathbb{Q}$ besitzt.

Satz 3.4 *Es ist unmöglich, mit Zirkel und Lineal einen Winkel von $\pi/3$ in drei gleiche Teile zu teilen.*

Beweis Wäre dies möglich, so könnte man $\alpha = \cos \pi/9$ konstruieren. Aber es gilt $4\alpha^3 - 3\,\alpha = \frac{1}{2}(= \cos \pi/3)$, so dass folgt $8\alpha^3 - 6\alpha - 1 = 0$. Aber das Polynom $f(x) = 8x^3 - 6x - 1$ ist irreduzibel über $\mathbb{Q}$. Wäre es nämlich reduzibel über $\mathbb{Q}$, so wäre es nach Satz II.4.4 auch reduzibel über $\mathbb{Z}$. Da es vom Grad 3 ist, müsste es also eine ganzzahlige Nullstelle besitzen. Dies ist offensichtlich nicht der Fall. Es folgt, dass α nicht konstruierbar ist.

Satz 3.5 *Es ist unmöglich, mit Zirkel und Lineal ein reguläres 7-Eck zu konstruieren.*

Beweis Wäre das reguläre 7-Eck konstruierbar, so könnte man $\alpha = 2\cos(2\pi/7)$ konstruieren. Aber α ist Nullstelle des Polynoms $f(x) = x^3 + x^2 - 2x - 1$, und dieses ist irreduzibel über $\mathbb{Q}$. Dies folgt wie im Beweis von Satz 3.4 aus dem Satz II.4.4. Damit ist α nicht konstruierbar.

Bemerkung Man kann zeigen, dass das reguläre 17-Eck konstruierbar ist. Dies wurde 1796 vom damals neunzehnjährigen Gauss bewiesen (C.F. Gauss 1777-1855).

Satz 3.6 *Es ist unmöglich, einen Kreis mit Zirkel und Lineal in ein flächengleiches Quadrat zu verwandeln.*

Beweis Wäre es möglich, so könnte man $\sqrt{\pi}$ und damit π konstruieren. Dann müsste aber π in einer algebraischen Erweiterung von $\mathbb{Q}$ liegen. Dies ist aber unmöglich, da π transzendent ist. Letzteres wurde 1882 von Lindemann bewiesen (C.L.F. Lindemann 1852-1939).

III.4 Endliche Körper

Es sei K ein Körper. Wir betrachten den Ringhomomorphismus $\phi : \mathbb{Z} \to K$ definiert durch $\phi(n) = n \cdot 1_K$, $n \in \mathbb{Z}$. Es sei $\ker \phi = m\mathbb{Z}$, $m \geq 0$. Da K ein Körper ist, darf $\operatorname{im} \phi \cong \mathbb{Z}/m\mathbb{Z}$ keine Nullteiler enthalten. Dies ist genau dann der Fall, wenn m gleich 0 oder eine Primzahl p ist. Die so erhaltene Zahl, $m = 0$ oder $m = p$, heisst die *Charakteristik* des Körpers K, $\operatorname{char} K$. Für $\operatorname{char} K = 0$ enthält K eine Kopie von $\mathbb{Z}$ und damit auch eine Kopie von $\mathbb{Q}$. Für $\operatorname{char} K = p$ enthält K eine Kopie von $\mathbb{Z}/p\mathbb{Z}$. In der Körpertheorie ist es üblich, die Bezeichnung $\mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$ zu verwenden.

Ist K ein *endlicher* Körper, so muss die Charakteristik von K offensichtlich eine Primzahl sein, $\operatorname{char} K = p$. Natürlich ist dann $\mathbb{F}_p \subseteq K$ eine endliche Körpererweiterung. Ist $n = [K : \mathbb{F}_p]$ der Körpergrad, so enthält K gerade p^n Elemente. Damit haben wir das folgende Resultat erhalten:

Satz 4.1 *Es sei K ein endlicher Körper. Dann existiert eine Primzahl p mit $|K| = p^n$.*

Wir werden zeigen, dass es zur Primzahlpotenz p^n bis auf Isomorphie genau einen Körper K gibt mit $|K| = p^n$. Dies verlangt aber einige Vorbereitungen.

Definition Die (formale) Ableitung eines Polynoms $f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n \in K[x]$ ist definiert durch

$$Df(x) = a_1 + 2a_2x + 3a_3x^2 + \cdots + na_nx^{n-1}.$$

Es ist klar, dass diese Ableitung den üblichen elementaren Ableitungsregeln genügt, insbesondere gilt

$$(D(fg))(x) = Df(x) \cdot g(x) + f(x) \cdot Dg(x).$$

Satz 4.2 *Ein Polynom $f(x) \in K[x]$ besitzt genau dann eine mehrfache Nullstelle in einer Körpererweiterung $L \supseteq K$, wenn $f(x)$ und $Df(x)$ einen gemeinsamen Faktor $h(x) \in K[x]$ mit $\deg h(x) \geq 1$ besitzen.*

Beweis Es sei α eine mehrfache Nullstelle von $f(x)$. Dann gilt in $K(\alpha)$ die Gleichung $f(x) = (x - \alpha)^2 \cdot g(x)$ für ein gewisses $g(x) \in K(\alpha)$. Es folgt $Df(x) = 2(x - \alpha) \cdot g(x) + (x - \alpha)^2 \cdot Dg(x)$ und α ist deshalb auch Nullstelle von $Df(x)$. Das Minimalpolynom $h(x)$ von α teilt folglich sowohl $f(x)$ wie $Df(x)$.

Es sei $h(x)$ ein gemeinsamer Faktor von $f(x)$ und $Df(x)$ und α eine Nullstelle von $h(x)$. Dann ist α auch eine Nullstelle von $f(x)$. Wir behaupten, dass sie mehrfach sein muss. In

$K(\alpha)$ gilt $f(x) = (x-\alpha)\cdot g(x)$ und $Df(x) = g(x) + (x-\alpha)\cdot Dg(x)$. Damit muss α auch eine Nullstelle von $g(x)$ sein; es folgt $f(x) = (x-\alpha)\cdot(x-\alpha)\cdot\overline{g}(x)$.

Definition Das Polynom $h(x) \in K[x]$ heisst *separabel*, wenn jeder irreduzible Faktor von $h(x)$ nur einfache Nullstellen besitzt. Andernfalls heisst $h(x)$ *inseparabel*.

Korollar 4.3 *Das Polynom $h(x) \in K[x]$ ist separabel, wenn $h(x)$ und $Dh(x)$ keinen gemeinsamen Faktor $\overline{h}(x)$ mit $\deg \overline{h}(x) \geq 1$ besitzen.*

Korollar 4.4 *Es sei $f(x) = x^{p^n} - x \in \mathbb{F}_p[x]$. Dann ist $f(x)$ separabel.*

Beweis Es gilt $Df(x) = (p^n)\cdot x^{p^n-1} - 1 = -1$. Es gibt folglich keinen nichttrivialen gemeinsamen Faktor von $f(x)$ und $Df(x)$.

Satz 4.5 *Es sei p eine Primzahl und $n \geq 1$ eine natürliche Zahl. Dann gibt es bis auf Isomorphie genau einen endlichen Körper $\mathbb{F}_{p^n}$ mit p^n Elementen. Er besteht gerade aus den Nullstellen von $x^{p^n} - x \in \mathbb{F}_p[x]$.*

Beweis Es ist klar, dass alle Elemente x eines Körpers K mit p^n Elementen die Gleichung $x^{p^n} = x$ erfüllen. Wir werden umgekehrt zeigen, dass der Körper mit p^n Elementen gerade der Zerfällungskörper des Polynoms $x^{p^n} - x \in \mathbb{F}_p[x]$ ist.

Es sei L dieser Zerfällungskörper. Wir behaupten, dass die p^n Nullstellen des Polynoms $x^{p^n} - x$ in L einen Unterkörper K bilden. Dann muss L mit K übereinstimmen. Aus der Eindeutigkeit des Zerfällungskörpers folgt dann die Eindeutigkeit des Körpers mit p^n Elementen.

Es bleibt also zu zeigen, dass die Nullstellen von $x^{p^n} - x$ einen Unterkörper von L bilden. Dazu ist nur nachzuweisen, dass mit α und β auch $\alpha\beta$, α/β (für $\beta \neq 0$) und $\alpha \pm \beta$ Nullstellen sind. Es gilt

$$(\alpha\beta)^{p^n} = \alpha^{p^n}\cdot\beta^{p^n} = \alpha\beta \ ,$$

$$\left(\frac{\alpha}{\beta}\right)^{p^n} = \frac{\alpha^{p^n}}{\beta^{p^n}} = \frac{\alpha}{\beta} \ .$$

Schliesslich rufen wir das Lemma II.4.6 in Erinnerung, welches besagt, dass für eine Primzahl p die Binomialkoeffizienten $\binom{p}{2}, \binom{p}{3}, \ldots, \binom{p}{p-1}$ durch p geteilt werden. Dies impliziert in Charakteristik p die folgende einfache Rechenregel für die p-te Potenz einer Summe bzw. Differenz

$$(a+b)^p = a^p + b^p \ .$$

Wir erhalten daraus durch wiederholtes Anwenden

$$(\alpha \pm \beta)^{p^n} = ((\alpha \pm \beta)^p)^{p^{n-1}} = (\alpha^p \pm \beta^p)^{p^{n-1}} = \cdots = \alpha^{p^n} \pm \beta^{p^n} = \alpha \pm \beta \ .$$

Die Nullstellen von $x^{p^n} - x$ bilden also in der Tat einen Unterkörper von L. Der Beweis des Satzes ist damit vollständig.

Die multiplikative Gruppe $K^\bullet$ des Körpers $K = \mathbb{F}_{p^n}$ hat die Ordung $p^n - 1$. Wir behaupten, dass sie zyklisch ist. Dazu schreiben wir $K^\bullet$ wie in Satz I.9.2 als direkte Summe ihrer Sylowuntergruppen. Sind alle diese Summanden zyklisch, so ist auch ihre direkte Summe zyklisch. Wäre einer der Summanden nicht zyklisch, so würde $k < p^n - 1$ (nämlich ein Teiler von $p^n - 1$) existieren mit $x^k = 1$ für alle Element $0 \neq x \in \mathbb{F}_{p^n}$. Dann wären aber alle nichttrivalen Elemente von $\mathbb{F}_{p^n}$ Nullstellen des Polynoms $x^k - 1$. Davon kann es aber nur k verschiedene geben. Dies ist wegen $k < p^n - 1$ ein Widerspruch.

Aus dieser Tatsache folgt nun sofort, dass es in $K = \mathbb{F}_{p^n}$ ein Element $\alpha \neq 0$ gibt mit $K^\bullet = \langle \alpha \rangle$. Das Element α ist als Element in einer endlichen Körpererweiterung algebraisch und besitzt deshalb ein Minimalpolynom. Es sei $m(x)$ das Minimalpolynom von α. Es ist klar, dass $m(x) \in \mathbb{F}_p[x]$ das Polynom $x^{p^n-1} - 1$ teilt und dass es ausserdem irreduzibel ist. Wegen $\mathbb{F}_p(\alpha) = K$ und $[K : \mathbb{F}_p] = n$ gilt $\deg m(x) = n$. Damit haben wir das folgende Resultat erhalten.

Satz 4.6 *Zur Primzahl p und zur natürlichen Zahl $n \geq 1$ existiert (mindestens) ein irreduzibles Polynom $m(x) \in \mathbb{F}_p[x]$ vom Grad n.*

Kennt man ein irreduzibles Polynom $m(x) \in \mathbb{F}_p[x]$ vom Grad n, so ergibt sich aus unserer allgemeinen Theorie der endlichen algebraischen Körpererweiterungen eine explizite Konstruktion von $\mathbb{F}_{p^n}$, nämlich

$$\mathbb{F}_{p^n} \cong \mathbb{F}_p[x]/(m(x)).$$

Es ist zu erwähnen, dass es im allgemeinen mehrere irreduzible Polynome über $\mathbb{F}_p$ vom Grad n gibt; sie führen aber alle zum 'gleichen' Körper $\mathbb{F}_{p^n}$, da ja letzterer bis auf Isomorphie eindeutig bestimmt ist.

Beispiele

(a) Es sei $p = 2$. Der Primkörper $\mathbb{F}_2$ enthält zwei Elemente 0, 1. Um den Körper $K = \mathbb{F}_4$ zu konstruieren, betrachten wir $x^4 - x = x \cdot (x^3 - 1) = x(x - 1)(x^2 + x + 1)$. Da das Polynom $x^2 + x + 1$ in $\mathbb{F}_2$ keine Nullstelle besitzt, ist es irreduzibel. Es folgt

$$\mathbb{F}_4 \cong \mathbb{F}_2[x]/(x^2 + x + 1) \ .$$

Ausserdem folgt, dass das Polynom $x^2 + x + 1$ das einzige irreduzible Polynom über $\mathbb{F}_2$ vom Grad 2 ist.

(b) Es sei wiederum $p = 2$. Wir behaupten, dass das Polynom $x^4+x+1 \in \mathbb{F}_2[x]$ irreduzibel ist. Wäre es nämlich reduzibel, so müsste es entweder eine Nullstelle in $\mathbb{F}_2$ besitzen oder Produkt von zwei irreduziblen Polynomen vom Grad zwei sein. Nun ist aber x^2+x+1 das einzige irreduzible Polynom vom Grad 2 über $\mathbb{F}_2$, und es gilt $(x^2+x+1)^2 = x^4+x^2+1 \neq x^4+x+1$. Damit ist x^4+x+1 irreduzibel. Wir erhalten

$$\mathbb{F}_{16} \cong \mathbb{F}_2[x]/(x^4+x+1) \ .$$

Diese Beschreibung des endlichen Körpers ist konstruktiv. Die Addition beherrscht man dank der Vektorraumstruktur von $\mathbb{F}_{16}$ über $\mathbb{F}_2$ und der 'natürlichen' Basis gegeben durch 1, x, x^2, x^3 modulo (x^4+x+1). Die Multiplikation wird wie folgt beschrieben: Wir wissen aus der allgemeinen Theorie, dass eine Nullstelle α von x^4+x+1 in $\mathbb{F}_{16}$ durch x modulo (x^4+x+1) repräsentiert wird. Die Potenzen von α können dann ohne Schwierigkeiten berechnet werden:

$$\begin{array}{rcl}
\alpha & = & x \\
(\alpha)^2 & = & x^2 \\
(\alpha)^3 & = & x^3 \\
(\alpha)^4 & = & x+1 \\
(\alpha)^5 & = & x^2+x \\
(\alpha)^6 & = & x^3+x^2 \\
(\alpha)^7 & = & x^3+x+1 \\
(\alpha)^8 & = & x^2+1 \\
(\alpha)^9 & = & x^3+x \\
(\alpha)^{10} & = & x^2+x+1 \\
(\alpha)^{11} & = & x^3+x^2+x \\
(\alpha)^{12} & = & x^3+x^2+x+1 \\
(\alpha)^{13} & = & x^3+x^2+1 \\
(\alpha)^{14} & = & x^3+1 \\
(\alpha)^{15} & = & 1
\end{array}$$

Das Element $\alpha \in \mathbb{F}_{16}$ hat folglich die multiplikative Ordnung 15 und ist damit ein erzeugendes Element der multiplikativen Gruppe $\mathbb{F}_{16}^{\bullet}$.

Es gibt zwei weitere irreduzible Polynome vom Grad 4 über $\mathbb{F}_2$, nämlich x^4+x^3+1 und $x^4+x^3+x^2+x+1$. Der Beweis für die Irreduzibilität verläuft wie oben. Während die Nullstellen von x^4+x^3+1 die multiplikative Ordnung 15 haben, gilt dies *nicht* für das Polynom $x^4+x^3+x^2+x+1$.

Satz 4.7 *Es sei $\beta \in K$ eine Nullstelle des Polynoms $h(x) \in \mathbb{F}_p[x]$. Dann ist auch β^p eine Nullstelle von $h(x)$.*

Beweis Es gilt $0 = (h(\beta))^p = (a_0 + a_1\beta + \cdots + a_n\beta^n)^p = a_0^p + a_1^p\beta^p + \cdots + a_n^p(\beta^p)^n =$

$a_0 + a_1\beta^p + \cdots + a_n(\beta^p)^n$; letzteres, da in $\mathbb{F}_p$ die Gleichung $(a_i)^p = a_i$ gilt.

Korollar 4.8 *Es sei $h(x) \in \mathbb{F}_p$ ein irreduzibles Polynom und β eine Nullstelle von $h(x)$. Dann sind $\beta, \beta^p, \beta^{p^2}, \ldots, \beta^{p^{n-1}}$ gerade die n Nullstellen des Polynoms $h(x)$.*

Beweis Es ist zu zeigen, dass die β^{p^i} für $i = 0, 1, 2, \ldots, n-1$ verschieden sind. Wäre $\beta^{p^i} = \beta^{p^j}$ für $0 \leq i < j \leq n-1$, so würde folgen

$$\beta = \beta^{p^n} = (\beta^{p^i})^{p^{n-i}} = (\beta^{p^j})^{p^{n-i}} = (\beta^{p^n})^{p^{j-i}} = \beta^{p^{j-i}} \ .$$

Es sei $l \geq 1$ die kleinste Zahl mit $\beta = \beta^{p^l}$. Dann sind $\beta, \beta^p, \beta^{p^2}, \ldots, \beta^{p^{l-1}}$ paarweise verschieden. Wir müssen $l = n$ zeigen. Wir definieren

$$g(x) = \prod_{i=0}^{l-1}(x - \beta^{p^i}).$$

Dann folgt einerseits

$$\begin{aligned}(g(x))^p &= (b_0 + b_1 x + \cdots + b_l x^l)^p \\ &= b_0^p + b_1^p x^p + \cdots + b_l^p (x^l)^p \\ &= b_0^p + b_1^p x^p + \cdots + b_l^p (x^p)^l \ .\end{aligned}$$

Andererseits werden die Nullstellen von $g(x)$ durch das Potenzieren nur permutiert, so dass gilt

$$(g(x))^p = g(x^p) = b_0 + b_1 x^p + \cdots + b_l (x^p)^l \ .$$

Für die Koeffizienten b_i, $i = 0, 1, \ldots, l$ des Polynoms $g(x)$ ergibt sich $b_i^p = b_i$, woraus sofort $b_i \in \mathbb{F}_p$ folgt. Damit ist $g(x)$ ein Polynom über $\mathbb{F}_p$. Es wurde aber als Faktor des irreduziblen Polynoms $f(x)$ definiert. Daraus folgt $g(x) = f(x)$, und es gilt in der Tat $l = n$.

Aus den angestellten Überlegungen ergibt sich, dass für jeden Körper K der Charakteristik p die Abbildung $a \mapsto a^p$ einen Endomorphismus von K definiert. Diese Abbildung heisst *Frobeniusabbildung*. Als Körperhomomorphismus ist die Frobeniusabbildung immer injektiv. Für endliche Körper ist sie deshalb auch surjektiv, so dass in diesem Fall sogar ein *Auto*morphismus des Körpers vorliegt. Die Frobeniusabbildung spielt in der Galoistheorie, insbesondere der Galoistheorie der endlichen Körper eine zentrale Rolle.

III.5 Codierungstheorie; Newtonsche Identitäten

Wir fügen hier eine Anwendung der Theorie endlicher Körper in der Codierungstheorie an, wobei wir allerdings die Ideen nur an einem einfachen Beispiel erklären. In natürlicher Weise führen diese Überlegungen schliesslich zu den sogenannten Newtonschen Identitäten, die in vielen Teilen der Mathematik eine grosse Rolle spielen.

Wir erinnern zuerst daran (siehe III.4), dass der Körper $K = \mathbb{F}_{16}$ durch $\mathbb{F}_p[x]/(x^4+x+1)$ beschrieben werden kann. Die Nullstelle α von x^4+x+1 ist ein erzeugendes Element von $K^\bullet$.

Wir betrachten nun den Vektorraum $V = (\mathbb{F}_2)^{15}$, bestehend aus den Null-Eins Folgen der Länge 15. Wir fassen V auf als Raum der Polynome über $\mathbb{F}_2$ vom Grad ≤ 14 und definieren einen Unterraum $U \subseteq V$ wie folgt:

Das Polynom $f(x) \in V$ liege in U, wenn gilt $f(\alpha) = 0$ und $f(\alpha^3) = 0$. Diese Forderung ist natürlich gleichbedeutend damit, dass $f(x)$ ein Vielfaches von $m(x) = x^4 + x + 1$ (Minimalpolynom von α) und $\overline{m}(x) = x^4+x^3+x^2+x+1$ (Minimalpolynom von α^3) ist. Wir bemerken, dass nach Korollar 4.8 das Polynom $f(x)$ auch $\alpha^2, \alpha^4, \alpha^8$ und $\alpha^6, \alpha^{12}, \alpha^{24} = \alpha^9$ als Nullstellen besitzt.

Behauptung *Es seien u, u' zwei verschiedene Elemente von U. Dann unterscheiden sich diese an mindestens 5 Stellen.*

In der Codierungstheorie nennt man U einen *Code*, und die Elemente von U heissen *Codewörter*. Unter dem *Hammingabstand* zweier Elemente u, u' eines endlich dimensionalen $\mathbb{F}_2$-Vektorraums versteht man die Anzahl Stellen, in denen sich die Vektoren u, u' unterscheiden. Man sagt, der *minimale Hammingabstand* des Codes U sei mindestens d, wenn der Hammingabstand von je zwei Elementen $u, u' \in U$, $u \neq u'$ mindestens d ist.

Beweis der Behauptung Da mit u, u' auch $u - u'$ in U liegt, ist zu zeigen, dass ein Polynom $c(x) \in V$ mit $\alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^6, \alpha^8, \alpha^9, \alpha^{12}$ als Nullstellen mindestens 5 von Null verschiedene Koeffizienten besitzen muss.

Wir gehen indirekt vor. Es sei $c(x) = c_1x^{i_1} + c_2x^{i_2} + c_3x^{i_3} + c_4x^{i_4}$ mit $0 \leq i_j < i_k \leq 14$ ein Polynom in V mit höchstens 4 von Null verschiedenen Koeffizienten, und $\alpha, \alpha^2, \alpha^3, \alpha^4$ als Nullstellen. Wir zeigen, dass dann $c_1 = c_2 = c_3 = c_4 = 0$ gilt.

Einsetzen von $\alpha, \alpha^2, \alpha^3, \alpha^4$ liefert die folgenden vier Gleichungen

$$\begin{array}{rcccccccc} 0 &=& c_1\alpha^{i_1} &+& c_2\alpha^{i_2} &+& c_3\alpha^{i_3} &+& c_4\alpha^{i_4} \\ 0 &=& c_1(\alpha^{i_1})^2 &+& c_2(\alpha^{i_2})^2 &+& c_3(\alpha^{i_3})^2 &+& c_4(\alpha^{i_4})^2 \\ 0 &=& c_1(\alpha^{i_1})^3 &+& c_2(\alpha^{i_2})^3 &+& c_3(\alpha^{i_3})^3 &+& c_4(\alpha^{i_4})^3 \\ 0 &=& c_1(\alpha^{i_1})^4 &+& c_2(\alpha^{i_2})^4 &+& c_3(\alpha^{i_3})^4 &+& c_4(\alpha^{i_4})^4 \end{array} .$$

Diese bilden ein homogenes lineares Gleichungssystem für c_1, c_2, c_3, c_4 mit Koeffizienten in K. Die Matrix ist

$$M = \begin{bmatrix} \alpha^{i_1} & \alpha^{i_2} & \alpha^{i_3} & \alpha^{i_4} \\ (\alpha^{i_1})^2 & (\alpha^{i_2})^2 & (\alpha^{i_3})^2 & (\alpha^{i_4})^2 \\ (\alpha^{i_1})^3 & (\alpha^{i_2})^3 & (\alpha^{i_3})^3 & (\alpha^{i_4})^3 \\ (\alpha^{i_1})^4 & (\alpha^{i_2})^4 & (\alpha^{i_3})^4 & (\alpha^{i_4})^4 \end{bmatrix} .$$

Die Determinantenberechnung liefert (Vandermonde)

$$\det M = \alpha^{i_1}\alpha^{i_2}\alpha^{i_3}\alpha^{i_4} \prod_{1\le j<k\le 4} (\alpha^{i_k} - \alpha^{i_j}) .$$

Wegen $\alpha^{i_j} \neq \alpha^{i_k}$ für $j \neq k$ ist die Determinante von Null verschieden. Damit besitzt unser homogenes Gleichungssystem nur die triviale Lösung, und es folgt $c_1 = c_2 = c_3 = c_4 = 0$.

Das obige ist ein Beispiel eines sogenannten BCH-Codes, der zur Fehlerkorrektur von *zwei* Übermittlungsfehlern innerhalb von 15 Übermittlungsbits gebraucht werden kann. Wir erklären kurz, wie dies vonstatten geht.

Die zu übermittelnde Nachricht wird in Blöcke von 7 Bits eingeteilt. Es sei n ein derartiges 7-Tupel (*Nachrichtenwort*), $n = (a_0, a_1, a_2, \ldots, a_6)$. Wie oben fassen wir dieses Wort als Polynom auf: $n(x) = a_0 + a_1 x + \cdots + a_6 x^6$. Die Codierung besteht darin, dass man $n(x)$ mit $m(x) \cdot \overline{m}(x) = x^8 + x^7 + x^6 + x^4 + 1$ multipliziert; die 15 Koeffizienten des resultierenden Polynoms $w(x)$ bilden das Wort w. Dieses wird übermittelt. Es sei $\overline{w}$ das empfangene Wort. Ist *kein* Übermittlungsfehler aufgetreten, so ist $\overline{w} = w$, also ein Codewort. Dies ist genau dann der Fall, wenn α und α^3 Nullstellen von $\overline{w}(x)$ sind. Das Nachrichtenwort n erhält man schliesslich durch Division von $\overline{w}(x)$ durch $m(x) \cdot \overline{m}(x)$.

Wir machen nun die Voraussetzung, dass bei der Übermittlung eines Wortes der Länge 15 *keiner*, *einer* oder höchstens *zwei* Fehler auftreten. Dann haben die Wörter w und $\overline{w}$ einen Hammingabstand ≤ 2. Wir haben festgestellt, dass der minimale Hammingabstand unseres Codes ≥ 5 ist. Aus diesem Grund hat $\overline{w}$ nur von einem einzigen, wohlbestimmten Element u von U einen Hammingabstand ≤ 2. Unter den getroffenen Voraussetzungen über die Anzahl der Übermittlungsfehler stimmt dieses Element u mit w überein. Das Nachrichtenwort n ergibt sich dann wie oben durch Division von $w(x)$ durch $m(x) \cdot \overline{m}(x)$.

Den Fall, wo kein Übermittlungsfehler aufgetreten ist, haben wir oben diskutiert. Er liegt genau dann vor, wenn gilt $\overline{w}(\alpha) = 0 = \overline{w}(\alpha^3)$. In diesem Fall ist $w = \overline{w}$. In den anderen Fällen unterscheidet sich das empfangene Polynom $\overline{w}(x)$ von $w(x)$ durch das sogenannte *Fehlerpolynom* $e(x)$; es gilt $\overline{w}(x) = w(x) + e(x)$. Kennt man das Fehlerpolynom, so lassen sich die Übermittlungsfehler offensichtlich korrigieren: $w(x) = \overline{w}(x) - e(x)$. Laut Voraussetzung wird das Fehlerpolynom nur an einer, beziehungsweise zwei Stellen einen von 0 verschiedenen Koeffizienten 1 aufweisen. Wegen $w(\alpha) = 0 = w(\alpha^3)$ gelten die Gleichungen

$$e(\alpha) = \overline{w}(\alpha)$$

und

$$e(\alpha^3) = \overline{w}(\alpha^3) \ .$$

Aus dieser dem Empfänger bekannten Information soll $e(x)$ bestimmt werden. Dies ist in der Tat möglich, wie wir zeigen werden.

Ist nur *ein* Übermittlungsfehler geschehen, so besitzt $e(x)$ nur einen von Null verschiedenen Koeffizienten, und das Gleichungssystem lautet

$$(*) \qquad \left| \begin{array}{rcl} X & = & \overline{w}(\alpha) \\ X^3 & = & \overline{w}(\alpha^3) \end{array} \right| \ .$$

Man schreibe X in der Form α^i mit $0 \leq i \leq 14$. Dann folgt $e(x) = x^i$.

Sind *zwei* Übermittlungsfehler geschehen, so lässt sich dies am obigen Gleichungssystem erkennen: dieser Fall liegt dann vor, wenn das Gleichungssystem $(*)$ *keine* Lösung besitzt, d.h. wenn

$$(\overline{w}(\alpha))^3 \neq \overline{w}(\alpha^3)$$

gilt. In diesem Fall muss $e(x)$ *zwei* von Null verschiedene Koeffizienten aufweisen; das Gleichungssystem lautet deshalb in diesem Fall

$$\left| \begin{array}{rcl} X+Y & = & \overline{w}(\alpha) \\ X^3+Y^3 & = & \overline{w}(\alpha^3) \end{array} \right| \ .$$

Natürlich lässt sich dieses in unserem Spezialfall direkt lösen; wir skizzieren hier aber ein Verfahren, das analog auch für BCH-Codes mit grösserem minimalem Hammingabstand gangbar ist. Wir müssen allerdings hinzufügen, dass wir die Effizienz des Verfahrens ganz ausser Acht lassen, obschon diese natürlich in der Praxis eine wichtige Rolle spielt. In der Tat gibt es wesentlich effizientere Verfahren der Fehlerkorrektur bei BCH-Codes!

Von den gesuchten Grössen X, Y sind hier die Summen der ersten und der dritten Potenzen bekannt. Daraus lässt sich mit Hilfe der *Newtonschen Identitäten* (siehe unten) das Produkt XY bestimmen. Es gilt nämlich

$$XY \ = \ ((X+Y)^3 - (X^3+Y^3))/3(X+Y) \ . \tag{1}$$

Die Grössen X, Y selbst ergeben sich dann als die beiden Lösungen der quadratischen Gleichung in Z

$$(Z-X)(Z-Y) = Z^2 - (X+Y)Z + XY = 0 \ .$$

Schreiben wir $X = \alpha^i$ und $Y = \alpha^j$ mit $0 \leq i, j \leq 14$, so ist $e(x) = x^i + x^j$.

Die *Newtonschen Identitäten*, auf die wir hier von der Codierungstheorie herkommend gestossen sind, treten in vielen Teilen der Mathematik auf. Sie verknüpfen in enger Weise die sogenannten elementaren symmetrischen Funktionen mit den Potenzsummen.
Wir schreiben

$$\sigma(z) = \prod_{i=1}^{r}(1 - x_i z) = \sum_{i=0}^{r} \sigma_i(x_1, x_2, \ldots, x_r) \cdot z^i \ .$$

Dann gilt

$$\begin{array}{rcl} \sigma_0(x_1, x_2, \ldots, x_r) & = & 1 \\ \sigma_1(x_1, x_2, \ldots, x_r) & = & -(x_1 + x_2 + \cdots + x_r) \\ \sigma_2(x_1, x_2, \ldots, x_r) & = & (x_1x_2 + x_1x_3 + \cdots + x_{r-1}x_r) \\ & \vdots & \\ \sigma_r(x_1, x_2, \ldots, x_r) & = & (-1)^r(x_1x_2x_3 \cdots x_r) \ . \end{array}$$

Die Polynome $\sigma_i(x_1, x_2, \ldots, x_r)$, $i = 1, 2, \ldots, r$ heissen die *elementar symmetrischen Funktionen* in $x_1, x_2, \ldots, x_r$. Für $i > r$ setzen wir $\sigma_i(x_1, x_2, \ldots, x_r) = 0$.
Die i-te Potenzsumme P_i ist definiert durch

$$P_i(x_1, x_2, \ldots, x_r) = \sum_{k=0}^{r} x_k^i \ .$$

Wir schreiben, ähnlich wie oben,

$$P(z) = \sum_{i=1}^{\infty} P_i(x_1, x_2, \ldots, x_r) \cdot z^i \ .$$

Der folgende Satz zeigt eine enge Beziehung zwischen den elementar symmetrischen Funktionen und den Potenzsummen.

Satz 5.1 *Für die formalen Potenzreihen $\sigma(z)$ und $P(z)$ gilt die Beziehung*

$$\sigma(z) \cdot P(z) + z \cdot \sigma'(z) = 0 \ .$$

Beweis Es ist natürlich

$$P(z) = \sum_{i=1}^{\infty} x_1^i z^i + \sum_{i=1}^{\infty} x_2^i z^i + \cdots + \sum_{i=1}^{\infty} x_r^i z^i = \frac{x_1 z}{1 - x_1 z} + \frac{x_2 z}{1 - x_2 z} + \cdots + \frac{x_r z}{1 - x_r z} \ .$$

Damit erhalten wir

$$\sigma(z) \cdot P(z) = \sum_{j=1}^{r} \left(\prod_{i=1,\, i\neq j}^{r} (1 - x_i z) \right) x_j z \ .$$

Andererseits gilt

$$z \cdot \sigma'(z) = z \cdot \left(\sum_{j=1}^{r} \left(-x_j \cdot \left(\prod_{i=1,\, i\neq j}^{r} (1 - x_i z) \right) \right) \right) \ .$$

Damit ist der Satz bewiesen.

Setzt man in die Gleichung in Satz 5.1 die Potenzreihen ein, so erhält man

$$\left(\sum_{i=0}^{r} \sigma_i z^i \right) \left(\sum_{i=1}^{\infty} P_i z^i \right) + z \left(\sum_{i=1}^{r} i \cdot \sigma_i z^{i-1} \right) = 0 \ .$$

Daraus gewinnt man durch Koeffizientenvergleich die *Newtonschen Identitäten* (beachte $\sigma_0 = 1$)

$$\begin{aligned} P_1 + \sigma_1 &= 0 \\ P_2 + \sigma_1 P_1 + 2\sigma_2 &= 0 \\ P_3 + \sigma_1 P_2 + \sigma_2 P_1 + 3\sigma_3 &= 0 \\ &\vdots \\ P_r + \sigma_1 P_{r-1} + \cdots + \sigma_{r-2} P_1 + r\sigma_r &= 0 \end{aligned}$$

sowie für $i > r$

$$P_i + \sigma_1 P_{i-1} + \cdots + \sigma_r P_{i-r} = 0 \ .$$

Mit Hilfe dieses Gleichungssystems lassen sich die P_i aus den σ_i rekursiv bestimmen und zwar sogar über $\mathbb{Z}$. Umgekehrt lassen sich die σ_i aus den $P_1, P_2, \ldots, P_r$ rekursiv bestimmen, wenn die Zahlen $2, 3, \ldots, r$ im Grundring invertierbar sind. Die Gleichung (1) ist auf diesem Weg erhalten worden.

Wir fügen hier noch die folgende *Bemerkung* an. Die hier auftretenden ganzzahligen Polynome $\sigma_i(x_1, x_2, \ldots, x_n)$ und $P_i(x_1, x_2, \ldots, x_n)$ sind Beispiele *symmetrischer* Polynome; ein Polynom heisst symmetrisch, wenn es bei einer beliebigen Permutation der Unbestimmten $x_1, x_2, \ldots, x_n$ invariant bleibt. Es ergibt sich durch rekursive Auflösung der Newtonschen Identitäten, dass sich die Potenzsummen P_i als ganzzahlige Polynome in den elementar

symmetrischen Funktionen schreiben lassen. Dies ist ein spezieller Fall eines ganz allgemeinen Resultates, das wir hier ohne Beweis erwähnen:

Jedes ganzzahlige symmetrische Polynom in $x_1, x_2, \ldots, x_n$ lässt sich als ganzzahliges Polynom in den elementar symmetrischen Funktionen schreiben.

Es gilt sogar noch mehr:

Die ganzzahligen symmetrischen Polynome bilden einen Polynomring über $\mathbb{Z}$ mit Erzeugenden $\sigma_1, \sigma_2, \ldots, \sigma_n$.

Dies bedeutet, dass es zwischen den elementar symmetrischen Polynomen keine nichttrivialen algebraischen Beziehungen gibt.

Kapitel IV. Modultheorie

Einleitung

Der Text des vorliegenden Kapitels ist eine kurze Einführung in die Modultheorie. Beim Begriff des Moduls über einem Ring handelt es sich um eine gemeinsame Verallgemeinerung des Begriffes eines Vektorraumes über einem Körper und des Begriffes einer abelschen Gruppe. Fast in jedem mathematischen Gebiet treten Moduln auf natürliche Weise auf, oft spielen sie bei der Behandlung des betreffenden Gebietes eine zentrale Rolle. Dies gilt insbesondere für die Darstellungstheorie (siehe Kapitel V), die Zahlentheorie, die kommutative Algebra und die homologische Algebra. Das Ziel dieser kurzen Einführung ist es, die grundlegendsten Begriffe und Resultate zusammenzustellen; für weiterführende Aussagen sei auf die entsprechenden Texte verwiesen. Einige Anwendungen allgemeinerer Natur, welche im Rahmen der Modultheorie ihren natürlichen Platz finden, werden im vorliegenden Kapitel allerdings behandelt; es sind dies der Fundamentalsatz für endlich erzeugte abelsche Guppen sowie einige Resultate über Normalformen von Matrizen (siehe Abschnitt IV.5).

IV.1 Definitionen und Beispiele

Es sei Λ ein Ring mit 1.

Definition Ein *Linksmodul* über Λ (auch Λ-*links-Modul* genannt) ist eine abelsche Gruppe A zusammen mit einer Operation $(\lambda, a) \mapsto \lambda a$, $\lambda \in \Lambda$, $a \in A$, welche den Axiomen

$$\begin{aligned} \lambda(a+b) &= \lambda a + \lambda b \ , \\ (\lambda+\mu)a &= \lambda a + \mu a \ , \\ (\lambda\mu)a &= \lambda(\mu a) \ , \\ 1_\Lambda a &= a \ , \end{aligned}$$

$\lambda, \mu \in \Lambda$, $a, b \in A$, genügt.

Gemäss den Axiomen ist für festes $\lambda \in \Lambda$ die Zuordnung $a \mapsto \lambda a$ ein Homomorphismus $T_\lambda : A \to A$ von abelschen Gruppen; insbesondere gilt $\lambda 0 = T_\lambda(0) = 0$. – Für $\lambda = 1_\Lambda$ erhält man die Identität von A: es gilt $T_{1_\Lambda} = 1_A$.

Statt einer "Links"-Operation von Λ kann man auch eine "Rechts"-Operation betrachten. Man erhält auf diese Weise die Definition eines *Rechtsmoduls* über Λ (auch Λ-*rechts-Moduls* genannt). Ist Λ kommutativ, so sind die beiden Begriffe äquivalent, im Allgemeinen sind sie es aber nicht. Wenn nicht explizit etwas anderes gesagt wird, so ist ein Modul im Folgenden immer ein *Links*-Modul.

Definition Es sei A ein Linksmodul über Λ. Ein *Untermodul* B von A ist eine Untergruppe der abelschen Gruppe A mit $\lambda b \in B$ für alle $\lambda \in \Lambda$ und alle $b \in B$. Unter der induzierten Operation ist B ein Linksmodul über Λ.

Es seien A und A' zwei Linksmoduln über Λ. Ein Λ-*Modulhomomorphismus* $f : A \to A'$ ist ein Homomorphismus von abelschen Gruppen mit

$$f(\lambda a) = \lambda(fa)$$

für alle $\lambda \in \Lambda$ und alle $a \in A$.

Beispiele (1) Es sei $\Lambda = k$ ein Körper. Ein Λ-Modul ist nichts anderes als ein Vektorraum über k, ein Λ-Untermodul ist ein k-Unterraum und ein Λ-Modulhomomorphismus ist eine k-lineare Abbildung.

(2) Es sei $\Lambda = \mathbb{Z}$. *Jede abelsche Gruppe A kann als $\mathbb{Z}$-Modul angesehen werden.* Die

Operation des Ringes $\mathbb{Z}$ auf A ist wie folgt definiert, $n \in \mathbb{Z}$, $a \in A$:

$$na = \begin{cases} a + a + \cdots + a \ , & n\text{-fach} \quad n \geq 1 \ , \\ 0 & n = 0 \ , \\ -(a + a + \cdots + a) \ , & -n\text{-fach} \quad n \leq -1 \ . \end{cases}$$

Die Axiome sind leicht zu verifizieren. Die Begriffe "$\mathbb{Z}$-Modul" und "abelsche Gruppe" sind somit gleichbedeutend. Homomorphismen von $\mathbb{Z}$-Moduln sind einfach Homomorphismen von abelschen Gruppen.

(3) Die additive Gruppe des Ringes Λ ist ein Linksmodul (bzw. Rechtsmodul) über Λ unter der Operation, die durch die Λ-Multiplikation von links (bzw. von rechts) induziert wird. Die Axiome sind direkte Folgerungen der Ringaxiome. Man sagt, man fasse Λ *als Linksmodul (bzw. Rechtsmodul) über sich selbst* auf. Die Λ-Untermoduln des Λ-Linksmoduls Λ sind die *Links*ideale im Ring Λ; die Untermoduln des Λ-Rechtsmoduls Λ sind die *Rechts*ideale.

(4) Es sei ein Ring Λ und eine indizierte Menge $S = \{s_i \mid i \in I\}$ gegeben. Der *freie* Λ-*Modul* (Linksmodul) $F(S)$ auf der Menge S ist wie folgt definiert.

Elemente: formale Summen $\sum_{i \in I} \lambda_i s_i$, $\lambda_i \in \Lambda$, wobei nur *endlich viele* der λ_i von Null verschieden sind;

Addition: $$\sum_{i \in I} \lambda_i s_i + \sum_{i \in I} \mu_i s_i = \sum_{i \in I} (\lambda_i + \mu_i) s_i, \quad \lambda_i, \mu_i \in \Lambda;$$

Λ-Operation: $$\lambda \left(\sum_{i \in I} \lambda_i s_i \right) = \sum_{i \in I} (\lambda \lambda_i) s_i, \quad \lambda, \lambda_i \in \Lambda.$$

Die Axiome sind offensichtlich erfüllt. Der Λ-Modul $F(S)$ enthält ausgezeichnete Elemente

$$s_j = \sum_{i \in I} \lambda_i s_i \ , \quad \lambda_i = \begin{cases} 1 & \text{für} \quad i = j \ , \\ 0 & \text{sonst.} \end{cases}$$

Die Menge dieser Elemente in $F(S)$ kann mit S identifiziert werden, so dass S als Teilmenge von $F(S)$ aufgefasst werden kann. Man spricht dann von einer *Basis* von $F(S)$. In der Tat gilt:

- S "erzeugt" $F(S)$: jedes Element von $F(S)$ lässt sich als (endliche) Linearkombination von Elementen in S mit Koeffizienten in Λ schreiben;
- S ist "linear unabhängig": aus $\sum_{i \in I} \lambda_i s_i = 0$ folgt stets $\lambda_i = 0$ für alle $i \in I$.

Satz 1.1 (Universelle Eigenschaft des freien Moduls) *Zu jedem Λ-Modul A und zu jeder Funktion $f : S \to A$ existiert ein eindeutig bestimmter Λ-Modulhomomorphismus $\psi : F(S) \to A$ mit $\psi|_S = f$.*

Beweis Es sei $\phi : F(S) \to A$ ein Λ-Modulhomomorphismus. Dann gilt

$$\phi\left(\sum_{i\in I} \lambda_i s_i\right) = \sum_{i\in I} \lambda_i\, \phi(s_i)\ .$$

Der Homomorphismus ϕ ist somit bestimmt, wenn seine Werte auf der Basis S gegeben sind. Daraus folgt, dass der gesuchte Homomorphismus ψ eindeutig bestimmt ist, falls er existiert. Setzen wir nun

$$\psi\left(\sum_{i\in I} \lambda_i s_i\right) = \sum_{i\in I} \lambda_i f(s_i)\ ,$$

so ist offensichtlich $\psi : F(S) \to A$ ein Λ-Modulhomomorphismus der verlangten Art.

Wir fügen folgende **Bemerkungen** an:

Ist $\Lambda = k$ ein Körper, so ist jeder Λ-Modul A frei, denn, wie aus der linearen Algebra bekannt ist, existiert eine Menge S (Basis) mit $A = F(S)$.

Ist $\Lambda = \mathbb{Z}$, so gibt es $\mathbb{Z}$-Moduln (abelsche Gruppen), die *nicht* frei sind: Für jedes Element s in $A = \mathbb{Z}/n\mathbb{Z}$ gilt $ns = 0$. Damit kann s nicht Element einer Basis sein, denn die Menge $\{s\}$ ist nicht linear unabhängig!

(5) Ist $\phi : \Lambda' \to \Lambda$ ein Ringhomomorphismus und A ein Λ-Modul, so ist A in natürlicher Weise auch ein Λ'-Modul: Die Operation von Λ' in A ist definiert durch $\lambda' a = (\phi(\lambda'))a$, $\lambda' \in \Lambda'$, $a \in A$. Die Axiome sind offensichtlich erfüllt. Man spricht in diesem Zusammenhang etwa vom *Zurückziehen der Operation von Λ auf Λ' via ϕ.*

Ist der Ring Λ eine Algebra über dem Körper k, so liefert die Zuordnung $\kappa \mapsto \kappa 1_\Lambda$, $\kappa \in k$ einen (injektiven) Ringhomomorphismus $\phi : k \to \Lambda$. Daraus folgt, dass jeder Modul M über der k-Algebra Λ automatisch die Struktur eines k-Vektorraums trägt.

(6) Es sei G eine endliche (multiplikativ geschriebene) Gruppe, $G = \{e = x_1, x_2, \ldots, x_n\}$. Die komplexe Gruppenalgebra $\Lambda = \mathbb{C}G$ ist wie folgt definiert (siehe Abschnitt II.1):

Elemente: $\sum_{i=1}^{n} c_i x_i \ , \quad c_i \in \mathbb{C}$;

Addition: $\sum_{i=1}^{n} c_i x_i + \sum_{i=1}^{n} d_i x_i = \sum_{i=1}^{n} (c_i + d_i) x_i, \ \ c_i, d_i \in \mathbb{C};$

Multiplikation: distributive Erweiterung der Gruppenmultiplikation.

Wir werden oft das Gruppenelement $x_i \in G$ mit dem Ringelement

$$0x_1 + 0x_2 + \cdots + 0x_{i-1} + 1x_i + 0x_{i+1} + \cdots + 0x_n \in \mathbb{C}G$$

identifizieren. Unter dieser Identifikation wird das Neutralelement e der Gruppe G zum Einselement 1_Λ des Ringes Λ.

Es sei A ein $\mathbb{C}G$-Linksmodul. Zum Elemente $x_i \in G$, aufgefasst als Ringelement, gehört ein Endomorphismus $T_{x_i} : A \to A$ der abelschen Gruppe A. Dabei gelten gemäss den Modulaxiomen die *Darstellungsbedingungen*, $x_i, x_j \in G$:

$$\begin{aligned} T_{x_i} \cdot T_{x_j} &= T_{x_i x_j} \ , \\ T_e &= 1_A \ . \end{aligned}$$

Da $\mathbb{C}G$ eine Algebra über $\mathbb{C}$ ist, trägt nach obigem der $\mathbb{C}G$-Modul A die Struktur eines $\mathbb{C}$-Vektorraumes. Sie wird erhalten, indem man den Unterring $\mathbb{C} = \mathbb{C}1_{\mathbb{C}G} = \mathbb{C}e$ in A operieren lässt. Der Endomorphismus T_{x_i}, $x_i \in G$, ist mit dieser Vektorraumstruktur verträglich und damit eine $\mathbb{C}$-lineare Selbstabbildungen des $\mathbb{C}$-Vektorraumes A. Er ist sogar regulär. Die Darstellungsbedingungen implizieren nämlich, dass T_{x_i} invertibel ist: $(T_{x_i})^{-1} = T_{x_i^{-1}}$.

Es folgt aus dem Gesagten, dass sich $T : x_i \mapsto T_{x_i}$ als einen Homomorphismus von Gruppen $T : G \to \mathrm{Aut}_{\mathbb{C}}(A)$ auffassen lässt.

Es sei umgekehrt ein Gruppenhomomorphismus $T : G \to \mathrm{Aut}_{\mathbb{C}}(A)$ gegeben, wo A ein beliebiger $\mathbb{C}$-Vektorraum ist. Ist T durch die Angabe der entsprechenden Matrizen gegeben, so spricht man von einer *komplexen Darstellung* im (Darstellungs-)Raum A. Dann lässt sich in A die Struktur eines $\mathbb{C}G$-Linksmoduls definieren, indem man setzt:

$$\lambda a = \left(\sum_{i=1}^{n} c_i x_i \right) (a) = \sum_{i=1}^{n} c_i (T_{x_i}(a)) \ .$$

Die Modulaxiome sind offensichtlich erfüllt. Wir fassen zusammen:

Jede komplexe Darstellung der Gruppe G gibt Anlass zu einem $\mathbb{C}G$-Modul. Umgekehrt liefert jeder $\mathbb{C}G$-Modul (nach einer Basiswahl im Darstellungsraum) eine komplexe Darstellung der Gruppe G.

Ersetzt man in den obigen Überlegungen den Körper $\mathbb{C}$ durch einen anderen Körper k oder durch einen beliebigen kommutativen Ring R, so entsprechen in offensichtlicher Weise Darstellungen von G über k oder R den kG- bzw. RG-Moduln.

IV.2 Quotientenmodul, direkte Summe

Es sei A ein Λ-Modul und B ein Untermodul. Insbesondere ist B eine Untergruppe von A. In der Restklassengruppe A/B kann auf natürliche Weise eine Λ-Modulstruktur definiert werden:

$$\lambda(a+B) = \lambda a + B \ , \quad \lambda \in \Lambda \ , \quad a \in A \ .$$

Dazu ist zu zeigen, dass diese Definition nicht vom gewählten Repräsentanten abhängt. Es sei also $a' = a + b$, $b \in B$. Dann gilt

$$\lambda(a'+B) = \lambda a' + B = \lambda(a+b) + B = \lambda a + \lambda b + B = \lambda a + B = \lambda(a+B) \ .$$

Es ist einfach nachzuweisen, dass diese Operation von Λ auf A/B die Modulaxiome erfüllt. Die kanonische Projektion $\pi : A \to A/B$, von der wir wissen, dass sie ein Homomorphismus von abelschen Gruppen ist, ist wegen

$$\pi(\lambda a) = (\lambda a) + B = \lambda(a+B) = \lambda(\pi(a))$$

automatisch ein Λ-Modulhomomorphismus.

Satz 2.1 *Es sei $\phi : A \to A'$ ein Λ-Modulhomomorphismus. Dann ist*

$$\ker \phi = \{a \in A \mid \phi a = 0\}$$

ein Λ-Untermodul von A, und

$$\phi A = \text{im } \phi = \{\phi(a) \mid a \in A\}$$

ist ein Λ-Untermodul von A'.

Beweis Für $a \in \ker\phi$ gilt $\phi(\lambda a) = \lambda(\phi(a)) = \lambda 0 = 0$. Damit ist $\ker\phi$ ein Untermodul von A. – Es sei $a' = \phi(a)$, $a \in A$. Dann folgt $\lambda a' = \lambda(\phi(a)) = \phi(\lambda a)$, d.h. $\lambda a' \in \text{im}\,\phi$. Damit ist $\text{im}\,\phi$ ein Untermodul von A'.

Satz 2.2 (Isomorphiesatz für Moduln) *Es sei $\phi : A \to A'$ ein Λ-Modulhomomorphismus. Dann faktorisiert ϕ über $\pi : A \to A/\ker\phi$ und die induzierte Abbildung $\psi : A/\ker\phi \to \phi A$, $\psi(a + \ker\phi) = \phi(a)$, ist ein Isomorphismus von Λ-Moduln.*

Beweis Dies folgt direkt aus dem Isomorphiesatz für abelsche Gruppen. Es ist nur nachzuweisen, dass ψ ein Homomorphismus von Λ-Moduln ist. Es gilt aber

$$\psi(\lambda(a + \ker\phi)) = \psi(\lambda a + \ker\phi) = \phi(\lambda a) = \lambda(\phi(a)) = \lambda(\psi(a + \ker\phi)) \ .$$

Aus diesem Isomorphiesatz ergibt sich genau wie im Falle von Gruppen – wir verzichten deshalb darauf, den Beweis ausführlich anzugeben – der folgende Satz:

Satz 2.3 *Es seien B und C Untermoduln des Λ-Moduls A. Es sei $\pi|_C : C \to A/B$ die Restriktion der kanonischen Projektion $\pi : A \to A/B$. Dann induziert $\pi|_C$ einen Isomorphismus von Λ-Moduln*

$$C/B \cap C = C/\ker\pi|_C \xrightarrow{\sim} \text{im}\,\pi|_C = (C + B)/B \ .$$

Als nächstes beschäftigen wir uns mit der direkten Summe von zwei bzw. beliebig vielen Λ-Moduln.

Definition Es seien A und B zwei Λ-Moduln. Die (externe) *direkte Summe* $A \oplus B$ der Moduln A und B ist wie folgt definiert, $a, a' \in A$, $b, b' \in B$, $\lambda \in \Lambda$:

Elemente: (a, b) ;

Addition: $(a, b) + (a', b') = (a + a', b + b')$;

Λ-Operation: $\lambda(a, b) = (\lambda a, \lambda b)$.

Die direkte Summe $A \oplus B$ enthält Untermoduln $A' = \{(a, 0) \mid a \in A\}$ und $B' = \{(0, b) \mid b \in B\}$. Die kanonische Einbettung $\iota_A : A \to A \oplus B$ definiert durch $\iota_A(a) = (a, 0)$ induziert einen Isomorphismus $A \simeq A'$. Ebenso induziert $\iota_B : B \to A \oplus B$, $\iota_B(b) = (0, b)$ einen Isomorphismus $B \simeq B'$.

Zur direkten Summe $A \oplus B$ gehören auch die Projektionen $\pi_A : A \oplus B \to A$ definiert durch $\pi_A(a, b) = a$ und $\pi_B : A \oplus B \to B$ definiert durch $\pi_B(a, b) = b$. Offensichtlich gilt

$\ker \pi_B = A'$, so dass folgt $(A \oplus B)/A' \simeq B$. Ebenso erhält man $\ker \pi_A = B'$, so dass folgt $(A \oplus B)/B' \simeq A$.

Satz 2.4 (Universelle Eigenschaft der direkten Summe) *Zu jedem Λ-Modul M und jedem Paar von Λ-Modulhomomorphismen $\alpha : A \to M$ und $\beta : B \to M$ existiert genau ein Λ-Modulhomomorphismus $\phi : A \oplus B \to M$ mit $\phi \circ \iota_A = \alpha$ und $\phi \circ \iota_B = \beta$.*

Beweis Damit die Gleichungen $\phi \circ \iota_A = \alpha$ und $\phi \circ \iota_B = \beta$ gelten, muss ϕ durch $\phi(a, b) = \alpha(a) + \beta(b)$ definiert werden. Die so definierte Abbildung ist offensichtlich ein Λ-Modulhomomorphismus.

Definition Der Λ-Modul C heisst (interne) *direkte Summe* der beiden Untermoduln A und B, wenn ein Isomorphismus $\phi : A \oplus B \to C$ von Λ-Moduln existiert, so dass ϕ den Untermodul A' von $A \oplus B$ isomorph auf den Untermodul A von C abbildet und den Untermodul B' von $A \oplus B$ isomorph auf den Untermodul B von C.

Satz 2.5 *Der Λ-Modul C ist genau dann interne direkte Summe der beiden Untermoduln A und B, wenn* (i) $C = A + B$ *und* (ii) $A \cap B = \{0\}$ *gilt.*

Beweis Ist C die interne direkte Summe der beiden Untermoduln A und B, so sind die Beziehungen (i) und (ii) offensichtlich erfüllt. Es seien umgekehrt, zwei Untermoduln A und B von C gegeben, die (i) und (ii) erfüllen. Die Einbettungen $\alpha : A \to C$ und $\beta : B \to C$ ergeben mit der universellen Eigenschaft der direkten Summe einen Λ-Modulhomomorphismus $\phi : A \oplus B \to C$ der durch $\phi(a, b) = a + b$ definiert ist. Seine Restriktionen auf A' bzw. B' induzieren offensichtlich Isomorphismen auf A bzw. B. Es bleibt somit zu zeigen, dass ϕ ein Isomorphismus ist. In der Tat ist ϕ wegen (i) surjektiv. Um die Injektivität nachzuweisen betrachten wir $\ker \phi$. Es sei $\phi(a, b) = a + b = 0$ mit $a \in A$ und $b \in B$. Daraus folgt aber $b = -a \in A$. Nach (ii) impliziert dies $b = 0$ und folglich $a = 0$. Der Homomorphismus ϕ ist somit auch injektiv.

In der Folge werden wir manchmal sagen, dass C die *Summe* $A + B$ der beiden Untermoduln A und B ist, wenn die Voraussetzung (i), aber nicht notwendigerweise (ii) erfüllt ist. Ist die Summe direkt, d.h. ist auch (ii) erfüllt, so schreiben wir $A \oplus B$, wie im Falle der externen direkten Summe.

Defintion Es seien A, B, C drei Λ-Moduln und $\alpha : A \to B$ und $\beta : B \to C$ zwei Λ-Modulhomomorphismen. Die Folge

$$A \xrightarrow{\alpha} B \xrightarrow{\beta} C$$

heisst *exakt* in B, wenn gilt im $\alpha = \ker \beta$.

Es ist somit $0 \to A \xrightarrow{\alpha} B$ exakt (in A), wenn α injektiv ist, und es ist $B \xrightarrow{\beta} C \to 0$ exakt (in C), wenn β surjektiv ist.

Die Folge

$$0 \to A \xrightarrow{\alpha} B \xrightarrow{\beta} C \to 0$$

heisst *kurz exakt*, wenn sie in A, B und C exakt ist. In diesem Fall ist α injektiv, β surjektiv, und es gilt $C \simeq B/\operatorname{im}\alpha$.

Satz 2.6 *Es sei* $0 \to A \xrightarrow{\iota} B \xrightarrow{\pi} C \to 0$ *eine kurze exakte Folge von* Λ*-Moduln. Es existiere ein* Λ*-Modulhomomorphismus* $\sigma : C \to B$ *mit* $\pi\sigma = 1_C$*. Dann ist* B *die direkte Summe von* $\ker\pi$ *und* $\operatorname{im}\sigma$*, also* $B \simeq A \oplus C$*.*

Der Homomorphismus σ mit $\pi\sigma = 1_C$ heisst auch etwa ein *Rechtsinverses* von π. Falls π ein Rechtsinverses besitzt, so ist B von der Form $A \oplus A'$. Man sagt in diesem Fall, A *besitze in* B *ein Komplement*, nämlich A', $A' \simeq C$. Oft wird man ι als Einbettung betrachten, d.h. A mit seinem Bild unter ι identifizieren.

Beweis des Satzes 2.6 Es sei $b \in \ker\pi \cap \operatorname{im}\sigma$. Dann existiert $c \in C$ mit $b = \sigma(c)$. Es folgt $0 = \pi(b) = \pi\sigma(c) = 1_C(c) = c$. Damit ist $\ker\pi \cap \operatorname{im}\sigma = \{0\}$ nachgewiesen. Es sei nun $b \in B$. Wir setzen $a = b - \sigma\pi(b)$. Dann gilt $\pi(a) = \pi(b) - \pi\sigma\pi(b) = \pi(b) - \pi(b) = 0$. Damit ist $a \in \ker\pi$. Aus $b = (b - \sigma\pi(b)) + \sigma\pi(b) = a + \sigma\pi(b)$ folgt dann $B = \ker\pi + \operatorname{im}\sigma$. Damit ist B in der Tat direkte Summe der Untermoduln $\ker\pi$ und $\operatorname{im}\sigma$. Schliesslich gilt wegen der Exaktheit $\ker\pi = \operatorname{im}\iota \simeq A$ und wegen $\sigma\pi = 1_C$ ist der Homomorphismus σ injektiv, also $\operatorname{im}\sigma \simeq C$.

Satz 2.7 *Es sei* $0 \to A \xrightarrow{\iota} B \xrightarrow{\pi} F \to 0$ *eine kurze exakte Folge von* Λ*-Moduln, wobei* $F = F(S)$ *frei ist. Dann existiert ein* Λ*-Modulhomomorphismus* $\sigma : F \to B$ *mit* $\pi\sigma = 1_F$*. Insbesondere besitzt* $\ker\pi$ *in* B *ein Komplement, das zu* F *isomorph ist.*

Beweis Zu $s \in S$ wähle man $b_s \in B$ mit $\pi(b_s) = s$. Die Funktion $f : S \to B$ gegeben durch $f(s) = b_s$ gibt wegen der universellen Eigenschaft des freien Moduls $F = F(S)$ Anlass zu einem Λ-Modulhomomorphismus $\sigma : F \to B$ mit $\sigma(s) = b_s$. Es bleibt $\pi\sigma = 1_F$ zu zeigen. Wegen der Wahl von b_s folgt für $s \in S$ sofort $\pi\sigma(s) = \pi(b_s) = s$. Da die Zusammensetzung $\pi\sigma$ und die Identität von F auf den Elementen von S übereinstimmen, folgt $\pi\sigma = 1_F$.

Wir merken noch die folgenden Dinge an:

Im obigen Satz hängt σ, das Rechtsinverse zu π, von der Wahl der Elemente b_s ab. Deshalb ist das Komplement von $\ker\pi$ in B nicht eindeutig bestimmt.

Für $\Lambda = \mathbb{Z}$ besitzt nicht jede Projektion ein Rechtsinverses. Zum Beispiel besitzt die kanonische Projektion $\pi : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ kein Rechtsinverses.

Für $\Lambda = k$, k ein Körper, ist jeder Λ-Modul frei. Zu einer surjektiven linearen Abbildung von Vektorräumen gibt es deshalb immer ein Rechtsinverses. Daraus folgt weiter, dass ein Unterraum U eines Vektorraumes V immer ein Komplement W besitzt. Auch in diesem Spezialfall ist das Komplement W bekanntlich nicht eindeutig bestimmt.

Die Definition der direkten Summe lässt sich ohne grosse Schwierigkeiten auf eine beliebige Familie von Λ-Moduln ausdehnen.

Definition Es sei $\{B_i\}$, $i \in I$ eine Familie von Λ-Moduln. Die *direkte Summe* $\bigoplus_{i\in I} B_i$ ist wie folgt definiert:

Elemente: Familien $(b_i)_{i\in I}$ mit $b_i \in B_i$, wobei nur endlich viele der b_i verschieden von Null sein sollen;

Addition: $(b_i)_{i\in I} + (b'_i)_{i\in I} = (b_i + b'_i)_{i\in I}$, $b_i, b'_i \in B_i$;

Λ-Operation: $\lambda(b_i)_{i\in I} = (\lambda b_i)_{i\in I}$, $\lambda \in \Lambda$, $b_i \in B_i$.

Für jedes $j \in I$ gibt es einen kanonischen injektiven Λ-Modulhomomorphismus $\iota_j : B_j \to \bigoplus_{i\in I} B_i$ definiert durch

$$\iota_j(b_j) = (b_i)_{i\in I} \text{ , wobei } b_i = \begin{cases} b_j & \text{für } i = j\,, \\ 0 & \text{sonst.} \end{cases}$$

Satz 2.8 (Universelle Eigenschaft der direkten Summe) *Zu jedem Λ-Modul M und jeder Familie von $\{\phi_i\}$, $i \in I$ von Λ-Modulhomomorphismen $\phi_i : B_i \to M$ existiert genau ein Λ-Modulhomomorphismus $\phi : \bigoplus_{i\in I} B_i \to M$ mit $\phi \circ \iota_i = \phi_i$ für alle $i \in I$.*

Beweis Offensichtlich ist ϕ durch

$$\phi\left((b_i)_{i\in I}\right) = \sum_{i\in I} \phi_i(b_i)$$

zu definieren. Man beachte, dass diese Formel nur wegen der Endlichkeitsvoraussetzung für die Elemente der direkten Summe sinnvoll ist.

Satz 2.9 *Es sei S die Familie $\{s_i\}$, $i \in I$. Dann ist der freie Λ-Modul $F(S)$ isomorph zur direkten Summe $\bigoplus_{i\in I} \Lambda_i$ mit $\Lambda_i \simeq \Lambda$ für alle $i \in I$.*

Beweis Wir definieren einen Λ-Modulhomomorphismus $\chi : F(S) \to \bigoplus_{i\in I} \Lambda_i$ durch

$$\chi\left(\sum_{i\in I} \lambda_i s_i\right) = (\lambda_i)_{i\in I} \ .$$

Offensichtlich ist χ sowohl injektiv wie auch surjektiv.

IV.3 Linearkombinationen

Es sei $\Phi = \{a_i \in A\}$, $i \in I$ eine Familie von Elementen des Λ-Moduls A. Wir betrachten die Menge $\langle\Phi\rangle$ der Elemente in A, die sich als (endliche) Linearkombinationen der Familie Φ mit Koeffizienten in Λ darstellen lassen:

$$\sum_{i\in I} \lambda_i a_i \in A \ .$$

Die Menge $\langle\Phi\rangle$ ist offensichtlich ein Untermodul von A; es ist der kleinste Untermodul von A, der die Familie Φ enthält. Wir nennen $\langle\Phi\rangle$ den *durch* Φ *erzeugten Untermodul* von A.

Definition Die Familie $\Phi = \{a_i \in A\}$, $i \in I$ heisst *linear unabhängig*, wenn aus $\sum_{i\in I} \lambda_i a_i = 0$ stets $\lambda_i = 0$, $i \in I$ folgt. Die Familie Φ heisst *maximal linear unabhängig*, wenn für jedes $b \in A$ die Familie $\{b\} \cup \Phi$ linear abhängig ist.

Satz 3.1 *In jedem Λ-Modul A gibt es mindestens eine maximale linear unabhängige Familie Φ_m.*

Wir werden den *Beweis des Satzes 3.1* etwas aufschieben und zuerst einige Bemerkungen und Beispiele anschliessen.

(1) Es sei für den Modul A die maximale Familie Φ_m leer. Dann gibt es zu jedem $a \in A$ ein $0 \neq \lambda \in \Lambda$ mit $\lambda a = 0$. Ein derartiger Modul A heisst *Torsionsmodul*.

(2) Ist $F = F(S)$ der freie Λ-Modul auf der Menge S, so ist S eine maximale linear unabhängige Familie in F.

(3) Der Modul A werde durch die Familie $\Phi_m = \{a_i \in A\}$, $i \in I$ erzeugt: $A = \langle\Phi_m\rangle$. Dann lässt sich jedes $a \in A$ als $\sum_{i\in I} \lambda_i a_i$ darstellen. Diese Darstellung ist eindeutig, denn $\sum_{i\in I} \lambda_i a_i = \sum_{i\in I} \mu_i a_i$ impliziert $\sum_{i\in I} (\lambda_i - \mu_i) a_i = 0$, also wegen der linearen Unabhängigkeit $\lambda_i - \mu_i = 0$ für alle $i \in I$.

Satz 3.2 *Es gelte $A = \langle\Phi_m\rangle$. Dann ist A isomorph zum freien Modul F auf der Menge Φ_m.*

Beweis Wir betrachten die Einbettung f von Φ_m in A. Die universelle Eigenschaft des freien Moduls $F = F(\Phi_m)$ liefert dann einen Λ-Modulhomomorphismus $\psi : F \to A$, der

durch

$$\psi\left(\sum_{i\in I}\lambda_i a_i\right)=\sum_{i\in I}\lambda_i f(a_i)=\sum_{i\in I}\lambda_i a_i$$

definiert ist. Dabei ist die Summe auf der linken Seite die formale Summe im freien Modul F, während die Summenbildung in der Mitte und auf der rechten Seite im Modul A stattfindet. Offensichtlich ist ψ surjektiv, da $\langle\Phi_m\rangle$ den Modul A erzeugt; er ist auch injektiv, da Φ_m linear unabhängig ist.

(4) Im Modul A ist der Untermodul $B=\langle\Phi_m\rangle$ isomorph zum freien Modul F auf Φ_m.

Beispiel Es sei $\Lambda=\mathbb{Z}$ und $A=\mathbb{Q}^+$, die additive Gruppe des Körpers der rationalen Zahlen. Ist r/s irgend eine von Null verschiedene rationale Zahl, so ist die Familie $\{r/s\}$ eine maximale linear unabhängige Familie in A. Für jedes Φ_m ist damit $B=\langle\Phi_m\rangle\simeq\mathbb{Z}$.

(5) Es sei $\Lambda=D$ ein Schiefkörper, A ein Λ-Modul und Φ_m eine maximale linear unabhängige Familie in A. Dann ist für jedes $b\in A$ die Familie $\{b\}\cup\Phi_m$ linear abhängig. Es gibt also eine nichttriviale Darstellung der Null: $\lambda b+\sum_{i\in I}\lambda_i a_i=0$. In dieser Darstellung ist $\lambda\neq 0$, denn sonst hätte man eine nichtriviale Darstellung der Null als Linearkombination der Familie Φ_m. Da Λ ein Schiefkörper ist, existiert λ^{-1}, und es folgt

$$b=\lambda^{-1}\lambda b=-\sum_{i\in I}\lambda^{-1}\lambda_i a_i\ .$$

Damit ergibt sich $\langle\Phi_m\rangle=A$. Es gilt also der Satz:

Satz 3.3 *Über einem Schiefkörper D ist jeder Modul frei, d.h. jeder D-Modul besitzt eine Basis.*

(6) Es sei Φ eine beliebige Familie von Elementen des Λ-Moduls A. Gilt $A=\langle\Phi\rangle$, so heisst Φ ein Erzeugendensystem von A. Der Modul A heisst endlich erzeugbar, wenn in A ein endliches Erzeugendensystem existiert.

Es sei $\Phi=\{b_i\}$, $i\in I$ ein Erzeugendensystem des Λ-Moduls A, und es sei F der freie Λ-Modul auf der Menge Φ. Die Einbettung f von Φ in A liefert mit der universellen Eigenschaft des freien Moduls einen Λ-Modulhomomorphismus $\psi: F\to A$ mit

$$\psi\left(\sum_{i\in I}\lambda_i a_i\right)=\sum_{i\in I}\lambda_i f(a_i)=\sum_{i\in I}\lambda_i a_i\ .$$

Dabei ist wie oben die Summe auf der linken Seite die formale Summe im freien Modul F, während die Summenbildung in der Mitte und auf der rechten Seite im Modul A stattfindet. Offensichtlich ist ψ surjektiv. Damit ist A als Quotient $F/\ker\psi$ eines freien Moduls F dargestellt.

Satz 3.4 *Jeder Λ-Modul A lässt sich als Quotienten eines freien Λ-Moduls F darstellen. Ist A endlich erzeugt, so kann F endlich erzeugt gewählt werden.*

Wir wenden uns jetzt dem Beweis des noch nicht bewiesenen Satzes am Anfang des Abschnittes zu. Wir benötigen dazu das sogenannte Lemma von Zorn, das wir hier zuerst in Erinnerung rufen wollen. Es handelt von einer Menge $\mathcal{M}$ von Teilmengen einer Menge E. Eine *Kette* $\mathcal{K}$ von Mengen in $\mathcal{M}$ ist eine Teilmenge von $\mathcal{M}$ mit der Eigenschaft, dass für $\Phi, \Phi' \in \mathcal{K}$ stets $\Phi \subseteq \Phi'$ oder $\Phi' \subseteq \Phi$ gilt. Eine Menge $\Phi_m \in \mathcal{M}$ heisst *maximal*, wenn aus $\Phi_m \subseteq \Psi \subseteq E$ und $\Psi \in \mathcal{M}$ stets folgt $\Psi = \Phi_m$.

Lemma 3.5 (Lemma von Zorn) *Es sei $\mathcal{M}$ eine nicht leere Menge von Teilmengen der Menge E. Es gelte, dass mit jeder Kette $\mathcal{K}$ von Mengen in $\mathcal{M}$ die Vereinigung $\bigcup_{\Phi\in\mathcal{K}} \Phi$ in $\mathcal{M}$ ist. Dann existiert in $\mathcal{M}$ eine maximale Menge Φ_m.*

Mit dem Lemma von Zorn lässt sich unser *Satz* ohne grosse Schwierigkeiten *beweisen*:

Wir betrachten die Menge $\mathcal{M}$ der Teilmengen von A, die linear unabhängig sind. Da die leere Menge linear unabhängig ist, ist $\mathcal{M}$ nicht leer. Ist eine Kette $\mathcal{K}$ von linear unabhängigen Mengen Φ gegeben, so ist die Vereinigung $\mathcal{V} = \bigcup_{\Phi\in\mathcal{K}} \Phi$ wiederum linear unabhängig. Ist nämlich $\sum_{i\in I} \lambda_i a_i = 0$ eine Linearkombination von Elementen aus $\mathcal{V}$, so sind nur *endlich* viele der λ_i verschieden von Null. Deshalb gibt es $\Phi' \in \mathcal{K}$, so dass alle mit nichtrivialem λ_i vorkommenden a_i in Φ' liegen. Aber Φ' ist nach Voraussetzung linear unabhängig, woraus $\lambda_i = 0$ für alle $i \in I$ folgt. Die Vereinigung $\mathcal{V}$ ist somit ebenfalls linear unabhängig. Nach dem Lemma von Zorn existiert dann (mindestens) eine maximale linear unabhängige Menge Φ_m in $\mathcal{M}$. Dies war zu beweisen.

Wie man in der Mengenlehre zeigt, ist die Aussage des Lemmas von Zorn logisch äquivalent zum Auswahlaxiom. Die Sätze in der Algebra, zu deren Beweis man das Lemma von Zorn hinzuziehen muss, brauchen also nicht zu gelten, wenn eine Mengenlehre ohne Auswahlaxiom zugrunde gelegt wird. In der Tat lassen sich Modelle von Mengenlehren angeben, in denen das hier als Konsequenz des Lemmas von Zorn erhaltene Resultat *nicht* gilt. Der Satz, dass jeder Vektorraum eine Basis besitzt, ist in einem solchen Modell der Mengenlehre im allgemeinen falsch: es können dann durchaus Vektorräume existieren, die keine Basen besitzen.

IV.4 Moduln über einem Hauptidealbereich

Wir werden hier in diesem Abschnitt einige Resultate über Moduln über einem Hauptidealbereich kennen lernen, wobei ein Teil davon auch für Moduln über einem Integritätsbereich gültig ist. Da $\mathbb{Z}$ ein Hauptidealbereich ist, gelten alle unsere Resultate insbesondere für abelsche Gruppen.

Satz 4.1 *Es sei Λ ein Integritätsbereich. Es seien S und T endliche Mengen. Der freie Λ-Modul $F(S)$ ist genau dann isomorph zum freien Λ-Modul $F(T)$, wenn $|S| = |T|$ gilt.*

Es folgt aus diesem Satz, dass $|S|$ durch den freien Modul $F(S)$ eindeutig bestimmt ist; die Zahl $|S|$ heisst der *Rang* von $F(S)$, Rang $F(S)$.

Beweis Es sei $S = \{s_1, s_2, \ldots, s_n\}$ und $T = \{t_1, t_2, \ldots, t_m\}$. Ein Λ-Modulhomomorphismus $\phi : F(S) \to F(T)$ wird eindeutig beschrieben durch $\phi(s_k) = \sum_{j=1}^{m} a_{jk} t_j$, $j = 1, 2, \ldots, n$, $a_{jk} \in \Lambda$. Ist ϕ ein Isomorphismus, so existiert $\psi : F(T) \to F(S)$ mit $\psi \circ \phi = 1$ und $\phi \circ \psi = 1$. In analoger Weise wird ψ beschrieben durch $\psi(t_l) = \sum_{i=1}^{n} b_{il} s_i$, $l = 1, 2, \ldots, m$, $b_{il} \in \Lambda$. Für die Matrizen $A = [a_{jk}]$ und $B = [b_{il}]$ folgt dann $AB = I_m$ und $BA = I_n$, wo I_m und I_n die Einheitsmatrizen der Dimension m bzw. n bezeichnen. Betrachtet man A und B jetzt als Matrizen über den Quotientenkörper Q von Λ, so definieren sie Isomorphismen zwischen zwei Vektorräumen über Q der Dimensionen n und m. Damit folgt $n = m$.

Definition Es sei Λ ein Integritätsbereich und A ein Λ-Modul. Der Torsionsuntermodul $T(A)$ von A ist definiert durch

$$T(A) = \{a \in A \mid \text{es existiert } 0 \neq \lambda \in \Lambda \text{ mit } \lambda a = 0\} .$$

Ein Λ-Modul A mit $T(A) = 0$ heisst *torsionsfrei*.

Beispiele (1) Der Modul $A/T(A)$ ist torsionsfrei.

Beweis Es sei $\lambda(a + T(A)) = T(A)$, $0 \neq \lambda$. Dann gilt $\lambda a \in T(A)$. Also existiert $0 \neq \mu \in \Lambda$ mit $\mu\lambda a = 0$. Da Λ ein Integritätsbereich ist, folgt $\mu\lambda \neq 0$. Daraus schliessen wir $a \in T(A)$.

(2) Ist F ein freier Λ-Modul, so ist F torsionsfrei.

Satz 4.2 *Es sei Λ ein Hauptidealbereich, A ein freier Λ-Modul vom Rang n und B ein Untermodul von A. Dann ist B ein freier Λ-Modul, und der Rang m von B ist höchstens n.*

Beweis Wir führen den Beweis mit Induktion nach n. Es sei $n = 1$. Dann ist $A = \Lambda$, und B ist ein Linksideal von Λ. Also existiert $\mu \in \Lambda$ mit $B = (\mu)$. Für $\mu = 0$ ist $B = 0$,

und B ist frei vom Rang 0. Für $\mu \neq 0$ definiert $\lambda \mapsto \lambda\mu$ einen Λ-Modulhomomorphismus $\Lambda \to B$. Dieser ist wegen der Nullteilerfreiheit von Λ ein Isomorphismus. Damit ist B frei vom Rang 1. In beiden Fällen gilt Rang $B \leq$ Rang $A = 1$.

Es sei $n \geq 2$, und $\{a_1, a_2, \ldots, a_n\}$ sei ein linear unabhängiges Erzeugendensystem von A. Jedes Element $a \in A$ lässt sich dann in eindeutiger Weise als $\sum \lambda_i a_i$ schreiben. Wir definieren nun einen Λ-Modulhomomorphismus $\phi : A \to \Lambda$ durch

$$\phi(a) = \phi\left(\sum \lambda_i a_i\right) = \lambda_n \ .$$

Durch Einschränkung auf B erhalten wir einen Λ-Modulhomomorphismus $\psi = \phi|_B : B \to \Lambda$. Das Bild im ψ ist ein Linksideal in Λ. Also existiert $\mu \in \Lambda$ mit im $\psi = (\mu)$. Es sind zwei Fälle zu unterscheiden:

Für $\mu = 0$ ist $B \subseteq \langle a_1, a_2, \ldots, a_{n-1}\rangle$, und nach Induktion ist B frei mit Rang $B \leq n-1 <$ Rang $A = n$.

Für $\mu \neq 0$ ist, wie oben, $(\mu) \simeq \Lambda$. Nach dem Isomorphiesatz ist somit $B/\ker\psi \simeq \Lambda$. Da der Quotient frei ist, hat nach einem früheren Resultat $\ker\psi$ in B ein Komplement, und es gilt $B \simeq \ker\psi \oplus \Lambda$. Aber $\ker\psi \subseteq \langle a_1, a_2, \ldots, a_{n-1}\rangle$. Nach Induktion ist somit $\ker\psi$ frei mit Rang $\ker\psi \leq n-1$. Daraus folgt, dass B frei ist. Ferner gilt Rang $B =$ Rang $\ker\psi + 1 \leq (n-1)+1 = n =$ Rang A.

Bemerkung Der Satz 4.2 gilt – *mutatis mutandis* – auch für Moduln über einem Hauptidealbereich, die nicht endlich erzeugbar sind. Wir beschränken uns hier aber auf den Fall endlich erzeugbarer Moduln, der in den Anwendungen wohl auch häufiger vorkommt.

Satz 4.3 *Es sei Λ ein Hauptidealbereich und A ein endlich erzeugter torsionsfreier Λ-Modul. Dann ist A frei von endlichem Rang.*

Beweis Es sei $\{a_1, a_2, \ldots, a_n\}$ ein Erzeugendensystem von A. Es sei, nach eventueller Umnumerierung, $\{a_1, a_2, \ldots, a_m\}$ eine maximale linear unabhängige Teilmenge. Der Untermodul $B = \langle a_1, a_2, \ldots, a_m\rangle$ ist dann frei.

Für $m < i \leq n$ ist die Menge $\{a_1, a_2, \ldots, a_m, a_i\}$ linear abhängig. Es existieren also $\lambda_1, \lambda_2, \ldots, \lambda_m$, $\lambda_i \in \Lambda$, so dass

$$\lambda_i a_i + \sum_{j=1}^{m} \lambda_j a_j = 0$$

eine nichttriviale Darstellung der Null ist. Da nach Voraussetzung $\{a_1, a_2, \ldots, a_m\}$ linear unabhängig ist, folgt $\lambda_i \neq 0$. Wir setzen $\lambda = \lambda_{m+1}\lambda_{m+2}\cdots\lambda_n$. Da Λ keine Nullteiler hat, folgt $\lambda \neq 0$. Mit Hilfe von λ definieren wir nun einen Λ-Modulhomomorphismus $\phi : A \to B$ wie folgt. Es sei $a = \sum_{k=1}^{n} \mu_k a_k$. Dann folgt

$$\lambda a = \sum_{j=1}^{m} \lambda\mu_j a_j + \lambda\mu_{m+1}a_{m+1} + \lambda\mu_{m+2}a_{m+2} + \cdots + \lambda\mu_n a_n \ .$$

Es ist λ für $i = m+1, m+2, \ldots, n$ ein Vielfaches von λ_i. Wegen der Wahl von λ_i folgt daraus $\lambda\mu_i a_i \in B$ für $i = m+1, m+2, \ldots, n$. Damit ist $\lambda a \in B$. Der Λ-Modulhomomorphismus $\phi : A \to B$ ist definiert durch $\phi(a) = \lambda a$.

Wegen $\ker \phi = \{a \in A \mid \lambda a = 0\} \subseteq T(A)$ und da A torsionsfrei ist, ist ϕ injektiv. Damit ist A isomorph zu einem Untermodul des freien Moduls B, also nach dem vorhergehenden Satz frei mit Rang $A \leq$ Rang B.

Bemerkung Die Aussage des Satzes 4.3 wird falsch, wenn die Voraussetzung über die endliche Erzeugbarkeit von A weggelassen wird: Als $\mathbb{Z}$-Modul ist $\mathbb{Q}^+$ torsionsfrei, aber nicht frei.

Satz 4.4 *Es sei Λ ein Hauptidealbereich und A ein endlich erzeugbarer Λ-Modul. Dann ist $A/T(A)$ isomorph zu einem freien Modul F, und es gilt $A \simeq T(A) \oplus F$.*

Beweis Der Quotient $A/T(A)$ ist torsionsfrei und endlich erzeugbar, also nach dem vorhergehenden Satz isomorph zu einem freien Modul F. Die Projektion $A \to A/T(A)$ besitzt folglich ein Rechtsinverses. Daraus ergibt sich $A \simeq T(A) \oplus F$.

IV.5 Endlich erzeugbare Torsionsmoduln über einem Hauptidealbereich

Es sei Λ ein Hauptidealbereich. Wir haben im letzten Abschnitt die Struktur von endlich erzeugbaren Λ-Moduln zurückgeführt auf die Struktur von endlich erzeugbaren Torsionsmoduln.

Es sei A ein Λ-Modul. Für $a \in A$ betrachten wir den Λ-Modulhomomorphismus $\phi : \Lambda \to A$ gegeben durch $\phi(\lambda) = \lambda a$ und definieren den Annihilator von a durch

$$\mathrm{Ann}\,(a) = \ker \phi = \{\lambda \in \Lambda \mid \lambda a = 0\}\ .$$

Dann gilt $\Lambda/\mathrm{Ann}\,(a) \simeq \langle a \rangle$. Da Λ ein Hauptidealbereich ist, existiert zu a ein bis auf Einheiten eindeutig bestimmtes Element μ_a mit $\mathrm{Ann}\,(a) = (\mu_a)$. Es heisst minimales Annihilatorelement oder kürzer *Exponent* von a.

Es sei nun T ein Torsionsmodul. Wir definieren

$$\mathrm{Ann}\,(T) = \bigcap_{a\in T} \mathrm{Ann}\,(a) = \{\lambda \in \Lambda \mid \lambda a = 0 \text{ für alle } a \in T\}\ .$$

Natürlich ist $\mathrm{Ann}\,(T)$ ein Linksideal von Λ; deshalb existiert ε mit $\mathrm{Ann}\,(T) = (\varepsilon)$. Es heisst minimales Annihilatorelement oder *Exponent* von T.

Lemma 5.1 *Es sei T ein endlich erzeugbarer Torsionsmodul über dem Hauptidealbereich Λ. Dann ist der Exponent ε von T nicht Null.*

Beweis Es sei $T = \langle a_1, a_2, \ldots, a_n\rangle$. Ist μ_{a_i} der Exponent von a_i, so ist das Produkt $\mu_{a_1}\mu_{a_2}\cdots\mu_{a_n}$ ein nichttriviales Element in $\mathrm{Ann}\,(T) = (\varepsilon)$. Daraus folgt $\varepsilon \neq 0$.

Definition Für $\pi \in \Lambda$ bezeichnen wir mit $T(\pi)$ den Untermodul von T, der aus allen Elementen besteht, die einen Exponenten der Form π^r, $r \geq 1$ besitzen. Ferner setzen wir $T_\pi = \ker(\pi : T \to T)$.

Wir machen nun Gebrauch davon, dass im Hauptidealbereich Λ die eindeutige Faktorzerlegung gilt. Es sei $\varepsilon = \pi_1^{r_1}\pi_2^{r_2}\cdots\pi_l^{r_l}$ die Zerlegung von ε, wobei $\pi_1, \pi_2, \ldots, \pi_l$ paarweise verschiedene irreduzible Elemente sind. Dann gilt der folgende Satz:

Satz 5.2 *Es sei $\varepsilon = \pi_1^{r_1}\pi_2^{r_2}\cdots\pi_l^{r_l}$ die Faktorzerlegung des Exponenten ε von T. Dann gilt*

$$T \simeq T(\pi_1) \oplus T(\pi_2) \oplus \cdots \oplus T(\pi_l)\ .$$

Beweis Es gilt für π_i offensichtlich $T(\pi_i) = T_{\pi_i^{r_i}}$. Es sei nun $\varepsilon = \alpha\beta$ mit $(\alpha, \beta) = 1$. Dann gibt es $\mu, \nu \in \Lambda$ mit $1 = \mu\alpha + \nu\beta$. Für $a \in T$ folgt $a = 1a = (\mu\alpha + \nu\beta)a = \mu\alpha a + \nu\beta a$, also $\mu\alpha a \in T_\beta$ und $\nu\beta a \in T_\alpha$. Ausserdem gilt $T_\alpha \cap T_\beta = 0$. Dies liefert die Zerlegung von T in eine direkte Summe $T_\alpha \oplus T_\beta$. Eine Induktion nach der Anzahl l der verschiedenen Faktoren in der Zerlegung von ε liefert schliesslich

$$T = T(\pi_1) \oplus T(\pi_2) \oplus \cdots \oplus T(\pi_l)\ .$$

Dies war zu beweisen.

Satz 5.3 *Es sei $\pi \in \Lambda$ ein irreduzibles Element, und π^r der Exponent von $T(\pi)$. Dann gilt*

$$T(\pi) \simeq \Lambda/(\pi^{s_1}) \oplus \Lambda/(\pi^{s_2}) \oplus \cdots \oplus \Lambda/(\pi^{s_m})$$

mit $r = s_1 \geq s_2 \geq \cdots \geq s_m \geq 1$.

Der *Beweis* des Satzes 5.3 verlangt einige technische Vorbereitungen. Zuerst führen wir den Begriff der Unabhängigkeit von Elementen eines Moduls ein. Die Elemente $y_1, y_2, \ldots, y_m \in T$ heissen *unabhängig*, wenn aus $\lambda_1 y_1 + \lambda_2 y_2 + \cdots + \lambda_m y_m = 0$ mit $\lambda_1, \lambda_2, \ldots, \lambda_m \in \Lambda$ stets folgt $\lambda_i y_i = 0$ für alle $i = 1, 2, \ldots, m$. (Man beachte, dass *unabhängig* nicht dasselbe ist wie *linear unabhängig*.) Die Elemente $y_1, y_2, \ldots, y_m$ sind offenbar genau dann unabhängig, wenn der von ihnen erzeugte Untermodul $\langle y_1, y_2, \ldots, y_m \rangle$ die direkte Summe $\langle y_1 \rangle \oplus \langle y_2 \rangle \oplus \cdots \oplus \langle y_m \rangle$ ist.

Ferner benötigen wir das folgende Lemma.

Lemma 5.4 *Es sei π^r der Exponent von T. Es sei $x \in T$ ein Element mit Exponent π^r. Es seien $\bar{y}_1, \bar{y}_2, \ldots, \bar{y}_m$ unabhängige Elemente in $\bar{T} = T/\langle x \rangle$. Dann existiert für jedes $i = 1, 2, \ldots, m$ ein Repräsentant $y_i \in T$ von $\bar{y}_i \in \bar{T}$, so dass der Exponent von y_i gleich dem Exponent von $\bar{y}_i$ ist. Die Elemente $x, y_1, y_2, \ldots, y_m$ sind unabhängig.*

Beweis Es sei $\bar{y} \in \bar{T}$ ein Element mit Exponent π^t und $y \in T$ ein Repräsentant von $\bar{y}$. Dann gilt $\pi^t y \in \langle x \rangle$. Damit existiert $\lambda \in \Lambda$ mit $\pi \nmid \lambda$ und $s \leq r$, so dass $\pi^t y = \pi^s \lambda x$. Gilt $s = r$, so hat y den gleichen Exponenten wie $\bar{y}$. Es sei $s < r$. Der Exponent von $\pi^s \lambda x$ ist dann π^{r-s}, so dass π^{t+r-s} der Exponent von y ist. Da π^r der Exponent von T ist, gilt $t + r - s \leq r$, und es folgt $t \leq s$. Es zeigt sich, dass $y - \pi^{s-t}\lambda x$ ein Repräsentant von $\bar{y}$ mit Exponent π^t ist.

Es seien nun $\bar{y}_1, \bar{y}_2, \ldots, \bar{y}_m \in \bar{T}$ unabhängige Elemente, und es sei für jedes $i = 1, 2, \ldots, m$ das Element $y_i \in T$ ein Repräsentant von $\bar{y}_i \in \bar{T}$ mit dem gleichen Exponenten. Wir behaupten, dass dann die Elemente $x, y_1, y_2, \ldots, y_m$ unabhängig sind. Gilt nämlich $\lambda x + \lambda_1 y_1 + \lambda_2 y_2 + \cdots + \lambda_m y_m = 0$, so folgt $\lambda_1 \bar{y}_1 + \lambda_2 \bar{y}_2 + \cdots + \lambda_m \bar{y}_m = 0$ und damit $\lambda_i \bar{y}_i = 0$ für $i = 1, 2, \ldots, m$. Es sei π^{s_i} der Exponent von $\bar{y}_i$. Dann folgt $\pi^{s_i} \mid \lambda_i$ und $\lambda_i y_i = 0$ für $i = 1, 2, \ldots, m$, da y_i den gleichen Exponenten wie $\bar{y}_i$ hat. Daraus ergibt sich schliesslich auch $\lambda x = 0$. Damit ist das Lemma bewiesen.

Wir wenden uns jetzt dem *Beweis des Satzes 5.3* zu. Wir stellen zuerst fest, dass mit T auch $T(\pi)$ endlich erzeugt ist. Ferner betrachten wir T_π. Dies ist offensichtlich ein Modul über $\Lambda/(\pi)$. Aber $\Lambda/(\pi)$ ist, wie wir wissen, ein Körper. Damit können wir dem Λ-Modul T die Dimension des Vektorraumes T_π über dem Körper $\Lambda/(\pi)$ zuordnen. Wir führen den Beweis mit Induktion nach dieser Dimension. Es sei $x \in T$ ein Element mit Exponent π^r. Wir betrachten $\bar{T} = T/\langle x \rangle$. Offensichtlich hat $\bar{T}_\pi$ kleinere Dimension als T_π, denn nach unserem Lemma, angewandt auf T_π und $\bar{T}_\pi$ lässt sich eine Basis von $\bar{T}_\pi$ zu einer (linear!) unabhängigen Menge von Elementen aus T_π hochheben. Letztere kann aber T_π nicht erzeugen, denn $x^{\pi^{r-1}}$ liegt im Kern der durch die Projektion induzierten Abbildung $T_\pi \to \bar{T}_\pi$. Nach Induktion existieren in $T/\langle x \rangle$ Elemente $\bar{x}_2, \bar{x}_3, \ldots, \bar{x}_s$ mit Exponent $\pi^{s_2}, \pi^{s_3}, \ldots, \pi^{s_m}$, $s_2 \geq s_3 \geq \cdots \geq s_m$. Nach unserem Lemma 5.4 lassen sich Repräsentanten $x_2, x_3, \ldots, x_m \in T$ finden mit den gleichen Exponenten, und so, dass $x_1 = x, x_2, x_3, \ldots, x_m$ unabhängig sind. Ferner gilt $s_1 = r$ und damit $s_1 \geq s_2$. Dies beweist die Aussage des Satzes.

Satz 5.5 *Es sei T ein endlich erzeugbarer Torsionsmodul über dem Hauptidealbereich Λ. Dann ist T eine direkte Summe $T \simeq A_1 \oplus A_2 \oplus \cdots \oplus A_m$ mit $A_i \simeq \Lambda/(\mu_i)$, $i = 1, 2, \ldots m$, wobei μ_{i+1} ein Teiler von μ_i ist für $i = 1, 2, \ldots, m-1$.*

Beweis Es sei $\mu = \pi_1^{r_1}\pi_2^{r_2}\cdots\pi_m^{r_m}$ die Faktorzerlegung des Exponenten μ von T. Gemäss unserem Satz lässt sich T in die direkte Summe der $T(\pi_j)$, $j = 1, 2, \ldots, m$ zerlegen und jedes $T(\pi_j)$ in eine direkte Summe $A_1^j \oplus A_2^j \oplus \cdots \oplus A_{m_j}^j$ wobei A_k^j von der Form $\Lambda/(\pi_j^s)$ ist. Die Aussage des Satzes ergibt sich nun ohne weiteres, indem man feststellt, dass für $\alpha, \beta \in \Lambda$ mit $(\alpha, \beta) = 1$ der Isomorphismus $\Lambda/(\alpha) \oplus \Lambda/(\beta) \simeq \Lambda/(\alpha\beta)$ gilt.

Korollar 5.6 *Es sei A ein endlich erzeugbarer Modul über dem Hauptidealbereich Λ. Dann ist A isomorph zu einer endlichen direkten Summe von Moduln der Form $\Lambda/(\mu)$. Die direkte Summe der $\Lambda/(\mu)$ mit $\mu = 0$ ist isomorph zu $A/T(A)$, die direkte Summe der $\Lambda/(\mu)$ mit $\mu \neq 0$ ist isomorph zu $T(A)$.*

Korollar 5.7 (Hauptsatz für endlich erzeugte abelsche Gruppen) *Es sei A eine endlich erzeugbare abelsche Gruppe. Dann ist A isomorph zu einer endlichen direkten Summe von zyklischen Gruppen*

$$A \simeq (\mathbb{Z} \oplus \mathbb{Z} \oplus \cdots \oplus \mathbb{Z}) \oplus (\mathbb{Z}/n_1\mathbb{Z} \oplus \mathbb{Z}/n_2\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/n_m\mathbb{Z}) \ .$$

Dabei ist n_{i+1} ein Teiler von n_i für $i = 1, 2, \ldots, m-1$.

Anwendung auf die Theorie der linearen Transformationen

Es sei k ein Körper, V ein Vektorraum endlicher Dimension über k und T eine k-lineare Selbstabbildung von V. Ist $f(T) = a_0 + a_1T + a_2T^2 + \cdots + a_nT^n$ ein Polynom mit Koeffizienten in k, so definiert $f(T)$ in der üblichen Art eine k-lineare Abbildung $f(T) : V \to V$. Mit dieser Operation wird V zu einem Modul über dem Polynomring $k[T]$. Ein $k[T]$-Untermoduln von V ist ein Unterraum U, der unter T invariant ist, $T(U) \subseteq U$.

Nach dem Satz von Cayley-Hamilton induziert das charakteristische Polynom $c(T)$ der linearen Selbstabbildung T die Nullabbildung von V, $0 = c(T) : V \to V$. Dies bedeutet, dass $c(T)$ den Modul V annihiliert. Der Modul V ist somit ein Torsionsmodul, und der Exponent $\mu = \mu(T)$ ist ein Teiler des charakteristischen Polynoms $c(T)$. Aus unserem Satz ergibt sich, dass sich der $k[T]$-Modul V als direkte Summe von $k[T]$-Untermoduln schreiben lässt, die von der Form $k[T]/(\mu(T))$ sind. Dabei ist $\mu(T)$ ein Teiler des charakteristischen Polynoms $c(T)$ der Selbstabbildung T.

Wir betrachten ein einzelnes solches $W = k[T]/(\mu(T))$ etwas näher. Es sei $\mu(T) = b_0 + b_1T + \cdots + b_mT^m$. Als k-Basis von W wählen wir $\beta_1 = 1, \beta_2 = T, \ldots, \beta_m = T^{m-1}$. Die Operation von T auf den Basiselementen ist dann gegeben durch

$$\begin{aligned} T(\beta_i) &= \beta_{i+1} \text{ für } i = 1, 2, \ldots, m-1 \\ T(\beta_m) &= -\frac{b_0}{b_m}\beta_1 - \frac{b_1}{b_m}\beta_2 - \cdots - \frac{b_{m-1}}{b_m}\beta_m \ . \end{aligned}$$

Die Matrix von T bezüglich dieser Basis ist also

$$\begin{bmatrix} 0 & 0 & 0 & \ldots & 0 & -b_0/b_m \\ 1 & 0 & 0 & \ldots & 0 & -b_1/b_m \\ 0 & 1 & 0 & \ldots & 0 & -b_2/b_m \\ 0 & 0 & 1 & \ldots & 0 & -b_3/b_m \\ \vdots & \vdots & \vdots & & \vdots & \vdots \\ 0 & 0 & 0 & \ldots & 1 & -b_{m-1}/b_m \end{bmatrix} .$$

Wählt man in jedem direkten Summanden von V eine derartige Basis, so zerfällt die zugehörige Matrix der Selbstabbildung T in Kästchen der obigen Form.

Meistens ist man daran interessiert, die Kästchen so klein wie möglich zu machen. Um dies zu illustrieren, betrachten wir den Spezialfall $k = \mathbb{C}$. Wir schreiben

$$\mu(T) = (T - c_1)^{\alpha_1}(T - c_2)^{\alpha_2} \cdots (T - c_l)^{\alpha_l}$$

mit $c_i \in \mathbb{C}$ und paarweise verschieden. Es gilt dann

$$\mathbb{C}[T]/(\mu(T)) \simeq \mathbb{C}[T]/((T - c_1)^{\alpha_1}) \oplus \mathbb{C}[T]/((T - c_2)^{\alpha_2}) \oplus \cdots \oplus \mathbb{C}[T]/((T - c_l)^{\alpha_l}) \ .$$

Im Summanden $W = \mathbb{C}[T]/((T - c)^{\alpha})$ kann – etwas anders als im ersten Fall – die Basis

$$\beta_1 = 1, \beta_2 = T - c, \beta_3 = (T - c)^2, \ldots, \beta_l = (T - c)^{\alpha - 1}$$

gewählt werden. Dann gilt für die Selbstabbildung T

$$\begin{aligned} T(\beta_1) &= \beta_2 + c\beta_1 \, , \\ T(\beta_2) &= \beta_3 + c\beta_2 \, , \\ &\cdots \\ T\beta_l &= c\beta_l \ . \end{aligned}$$

Die Matrix, welche T in dieser Basis darstellt, ist also

$$\begin{bmatrix} c & 0 & 0 & \cdots & 0 & 0 \\ 1 & c & 0 & \cdots & 0 & 0 \\ 0 & 1 & c & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & c & 0 \\ 0 & 0 & 0 & \cdots & 1 & c \end{bmatrix}.$$

Durch analoge Basiswahl in jedem direkten Summanden von V kann man somit erreichen, dass die Matrix der Selbstabbildung T in Kästchen dieser Form zerfällt. Dies ist die sogenannte *Jordansche Normalform* einer Matrix.

IV.6 Einfache Moduln

In diesem Abschnitt ist Λ ein beliebiger Ring.

Definition Ein Λ-Modul A, $A \neq 0$ heisst *einfach*, wenn es ausser 0 und A keine weiteren Untermoduln gibt.

Beispiele (a) Es sei $\Lambda = K$ ein Körper. Der (bis auf Isomorphie) einzige einfache Modul ist K.

(b) Es sei $\Lambda = K(T)$. Ein $K(T)$-Modul V ist genau dann einfach, wenn in V keine unter T invarianten Teilräume existieren ausser 0 und V.

(c) Es sei $\Lambda = \mathbb{Z}$. Die einfachen $\mathbb{Z}$-Moduln sind die abelschen Gruppen von Primzahlordnung $\mathbb{Z}/p\mathbb{Z}$, p prim.

(d) Es sei A ein einfacher Λ-Modul. Zu $0 \neq a \in A$ betrachten wir $\phi : \Lambda \to A$ definiert durch $\phi(\lambda) = \lambda a$, $\lambda \in \Lambda$. Wegen $\phi(1) = a$ folgt im $\phi \neq 0$. Damit gilt im $\phi = \langle a \rangle = A$. Nach dem Isomorphisatz folgt dann $A \simeq \Lambda / \ker \phi$ mit $\ker \phi = \{\lambda \in \Lambda \mid \lambda a = 0\} = \text{Ann } (a)$. Es gilt somit:

Satz 6.1 *Es sei A einfach, $0 \neq a \in A$. Dann ist $A = \langle a \rangle$. Ist $\phi : \Lambda \to A$ durch $\phi(\lambda) = \lambda a$, $\lambda \in \Lambda$ definiert, so folgt $A \simeq \Lambda / \text{Ann } (a)$.*

Satz 6.2 *Es sei K ein Linksideal von Λ. Genau dann ist Λ / K einfach, wenn K ein maximales Linksideal ist.*

Beweis Es sei I ein Linksideal mit $K \subseteq I \subseteq \Lambda$. Dann gilt $0 = K/K \subseteq I/K \subseteq \Lambda/K$. Ist Λ/K einfach, so folgt $I/K = 0$ oder $I/K = \Lambda/K$, d.h. $I = K$ oder $I = \Lambda$. Es ist also K maximal. Ist umgekehrt K maximal, so folgt $I = K$ oder $I = \Lambda$. Der Modul Λ/K besitzt folglich keine nichttrivialen Untermoduln.

Genau gleich beweist man den folgenden Satz, auf den wir später zurückgreifen werden.

Satz 6.3 *Es sei C ein Λ-Modul und B ein echter Untermodul. Genau dann ist C/B einfach, wenn es zwischen B und C keine weiteren Untermoduln gibt.*

Beispiele (1) Es sei $\Lambda = \mathbb{Z}$. Eine abelsche Gruppe A ist genau dann einfach, wenn A von der Form $\mathbb{Z}/K$ ist, wobei K ein maximales Ideal ist. Bekanntlich sind in $\mathbb{Z}$ genau die Ideale maximal, die von einer Primzahl p erzeugt werden.

(2) Der Λ-Modul Λ ist genau dann einfach, wenn es in Λ keine echten Linksideale gibt. Man beachte, dass ein Ring Λ *einfach* (als Ring) genannt wird, wenn es in Λ keine nichttrivialen *zwei*seitigen Ideale gibt.

Definition Der Λ-Modul heisst *halbeinfach*, wenn A direkte Summe von einfachen Moduln ist,

$$A = \bigoplus_{i \in I} B_i \ , \quad B_i \text{ einfach} \ .$$

Beispiele (a) Es sei $\Lambda = D$ ein Schiefkörper. Dann ist jeder Λ-Modul halbeinfach.
(b) Es sei $\Lambda = \mathbb{Z}$. Es gibt abelsche Gruppen ($\mathbb{Z}, \mathbb{Z}/p^2\mathbb{Z}$, etc.), die nicht halbeinfach sind.

Man sagt (siehe Abschnitt 2), der Untermodul B von A besitze ein *Komplement*, wenn ein Untermodul C in A existiert mit $A \simeq B \oplus C$.

Satz 6.4 *Genau dann ist A halbeinfach, wenn jeder Untermodul von A ein Komplement besitzt.*
Wir beweisen zuerst zwei Lemmas, die wir im Beweis dieses Satzes benötigen werden.

Lemma 6.5 *Es sei N ein echtes Linksideal von Λ. Dann existiert ein maximales Linksideal M von Λ mit $N \subseteq M \subseteq \Lambda$.*
Beweis Wir betrachten die Menge $\mathcal{M}$ der Linksideale N' von Λ mit $N \subseteq N' \subset \Lambda$. Diese Menge ist wegen $N \in \mathcal{M}$ nicht leer. Ferner enthält sie mit einer Kette $\mathcal{K}$ auch die Vereinigung $\bigcup_{K \in \mathcal{K}} K$. Dazu ist nur zu zeigen, dass diese Vereinigung nicht ganz Λ sein

kann. In diesem Fall wäre aber $1_\Lambda \in \bigcup_{K\in\mathcal{K}} K$, und es würde $K \in \mathcal{K}$ existieren mit $1_\Lambda \in K$. Damit wäre aber $K = \Lambda$, im Widerspruch zur Auswahl der Elemente von $\mathcal{M}$. Nach dem Lemma von Zorn existiert in $\mathcal{M}$ ein maximales Element M, aber dies ist definitionsgemäss ein maximales Linksideal in Λ.

Lemma 6.6 *Es sei A ein Modul, in dem jeder Untermodul ein Komplement besitzt. Dann gilt:*
(i) *Es seien B und D Untermoduln mit $B \subseteq D$. Dann besitzt B in D ein Komplement.*
(ii) *Jeder Untermodul D, $D \neq 0$ enthält einen einfachen Untermodul E.*

Beweis (i) Es sei C ein Komplement von B in A. Man verifiziert ohne grosse Mühe, dass $C \cap D$ ein Komplement von B in D ist.

(ii) Es sei $0 \neq d \in D$. Die übliche Abbildung $\phi : \Lambda \to D$ definiert durch $\phi(\lambda) = \lambda d$ liefert den Isomorphismus $\Lambda/N \simeq \langle d\rangle \subseteq D$, $N = \ker\phi$. Es sei M ein maximales Ideal von Λ mit $N \subseteq M$. Dann ist M/N ein Untermodul von Λ/N. Zu diesem gibt es nach (i) ein Komplement E. Es gilt dann $\Lambda/N = (M/N) \oplus E$ und $E \simeq \Lambda/M$, so dass E einfach ist. Damit ist ein einfacher Untermodul E von D gefunden.

Beweis des Satzes 6.4 Es sei zuerst A halbeinfach, $A = \bigoplus_{i\in I} B_i$, B_i einfach, und B ein Untermodul von A. Wir betrachten die Teilmengen I' der Indexmenge I mit

$$B \cap \sum_{i\in I'} B_i = 0 \ .$$

Wir behaupten, dass die Menge $\mathcal{M}$ der Mengen I' die Voraussetzungen des Lemmas von Zorn erfüllt.

Es ist $\mathcal{M}$ nicht leer, denn die leere Teilmenge von I liegt darin. Es sei in $\mathcal{M}$ eine Kette $\mathcal{K}$ gegeben. Wir müssen zeigen, dass $\bigcup_{K\in\mathcal{K}} K$ eine Menge in $\mathcal{M}$ ist. Zu diesem Zweck betrachten wir

$$a \in B \ \cap \sum_{i\in\bigcup_{K\in\mathcal{K}} K} B_i \ .$$

Dann lässt sich a als *endliche*(!) Summe $b_{i_1} + b_{i_2} + \cdots + b_{i_l}$ mit $b_{i_k} \in B_{i_k}$ schreiben. Da $\mathcal{K}$ eine Kette ist, existiert ein $K \in \mathcal{K}$ mit $i_1, i_2, \ldots, i_l \in K$. Damit folgt aber $a = 0$. Es ist also in der Tat $\bigcup_{K\in\mathcal{K}} K$ eine Menge in $\mathcal{M}$.

Nach dem Lemma von Zorn existiert in $\mathcal{M}$ eine maximale Menge J mit

$$B \cap \sum_{i\in J} B_i = 0 \ .$$

Wir setzen $C = \sum_{i\in J} B_i$ und behaupten, dass C ein Komplement von B in A ist. Nach Konstruktion gilt $B \cap C = 0$. Es bleibt $A = B + C$ zu zeigen. Dazu genügt es nachzuweisen,

dass für alle $j \in I$ gilt $B_j \subseteq B + C$. Für $j \in J$ ist dies klar. Es sei also $j \notin J$. Dann folgt wegen der Maximalität von J

$$B \cap (C + B_j) \neq 0 \ .$$

Damit existiert $0 \neq b = c + b_j$ mit $b \in B$, $c \in C$, $b_j \in B_j$. Wäre $b_j = 0$, so hätte man $B \cap C \neq 0$, was im Widerspruch zur Konstruktion von C stünde. Es gibt somit $0 \neq b_j = b - c$, also $0 \neq b_j \in B + C$. Da B_j einfach ist, folgt $B_j \subseteq B + C$. Dies war zu beweisen.

Es ergibt sich damit $A = B \oplus C$.

Umgekehrt besitze jeder Untermodul von A ein Komplement. Wir betrachten die Menge aller einfachen Untermoduln B_i, $i \in I$ von A. Es sei $\mathcal{M}$ die Menge der Teilmengen I' von I, so dass die Summe $\sum_{i \in I'} B_i$ direkt ist. Wir behaupten, dass $\mathcal{M}$ die Voraussetzungen des Lemmas von Zorn erfüllen. Natürlich ist $\mathcal{M}$ nicht leer, denn die leere Teilmenge von I liegt in $\mathcal{M}$. Es sei $\mathcal{K}$ eine Kette in $\mathcal{M}$. Dann ist auch $\bigcup_{K \in \mathcal{K}} K$ in $\mathcal{K}$. Nach dem Lemma von Zorn existiert somit eine maximale Menge J in $\mathcal{M}$. Wir behaupten nun

$$A = \bigoplus_{i \in J} B_i \ .$$

Die Summe ist laut Konstruktion direkt. Es ist $A = \sum_{i \in J} B_i$ zu zeigen. Wäre $\sum_{i \in J} B_i$ ein echter Untermodul von A, so würde laut Voraussetzung dazu ein Komplement C existieren. Es sei nun B_k ein einfacher Untermodul von C. Dann folgt aber, dass die Summe $B_k + \sum_{i \in J} B_i$ direkt ist, im Widerspruch zur Maximalität von J. Damit ist der Satz vollständig bewiesen.

Satz 6.7 (Krull-Schmidt) *Es sei M halbeinfach und es seien $M = \bigoplus_{i \in I} M_i = \bigoplus_{j \in J} N_j$ zwei Darstellungen von M als direkte Summen von einfachen Moduln. Dann sind die Zerlegungen äquivalent, d.h. es gibt eine Bijektion $f : I \to J$ mit $M_i \simeq N_{f(i)}$.*

Satz 6.7 besagt, dass die Summanden eines halbeinfachen Moduls bis auf Reihenfolge und Isomorphie eindeutig bestimmt sind. Wir verzichten hier auf einen Beweis des Satzes in dieser Allgemeinheit. Für endliche Indexmengen folgt der Beweis aus dem Satz von Jordan-Hölder, der im folgenden Abschnitt bewiesen wird (siehe Korollar 7.4).

IV.7 Kompositionsreihen

Es sei A ein Λ-Modul. Wir betrachten hier eine endliche *Reihe von Untermoduln*

$$0 = A_0 \subseteq A_1 \subseteq A_2 \subseteq \cdots \subseteq A_m = A \ .$$

Die Quotienten A_{i+1}/A_i heissen die *Faktoren* der Reihe und m heisst die *Länge* der Reihe.

Satz 7.1 *Es seien*

$$0 = A_0 \subseteq A_1 \subseteq A_2 \subseteq \cdots \subseteq A_m = A$$

und

$$0 = B_0 \subseteq B_1 \subseteq B_2 \subseteq \cdots \subseteq B_n = A$$

zwei Reihen von Untermoduln des Moduls A der Länge m bzw. n. Dann lassen sich diese Reihen verfeinern, so dass die Verfeinerungen gleiche Länge und isomorphe Faktoren besitzen (aber nicht notwendigerweise in der gleichen Reihenfolge).

Zum Beweis benötigen wir das folgende Lemma:

Lemma 7.2 *Es seien $B' \subseteq B \subseteq A$ und $C' \subseteq C \subseteq A$ gegeben. Dann gilt*

$$(B' + (B \cap C))/(B' + (B \cap C')) \simeq (C' + (B \cap C))/(C' + (B' \cap C)) \ .$$

Beweis Nach dem Isomorphiesatz gilt $X + Y/X \simeq Y/X \cap Y$. Wir wenden diesen Isomorphiesatz auf $X = ((B \cap C') + B')$ und $Y = B \cap C$. Damit erhalten wir

$$\begin{aligned} ((B \cap C') + B') + (B \cap C)/((B \cap C') + B') &\simeq B \cap C/((B \cap C') + B') \cap (B \cap C) \\ &= B \cap C/(B' \cap C) + (B \cap C') \ , \end{aligned}$$

wobei für den letzten Schritt

$$((B \cap C') + B') \cap (B \cap C) = (B' \cap C) + (B \cap C')$$

zu zeigen ist. Es sei $x \in B' \cap C$, $y \in B \cap C'$. Dann folgt $x + y \in B \cap C$ und $x + y \in B' + (B \cap C')$. Ist umgekehrt $x \in B'$, $y \in B \cap C'$, $x + y \in B \cap C$, so ist *a fortiori* $y \in B \cap C$, und es folgt $x \in B \cap C$. Daraus ergibt sich $x \in B' \cap C$, also $x + y \in (B' \cap C) + (B \cap C')$.

Aus Symmetriegründen ist auch der Modul auf der rechten Seite der Behauptung des Lemmas isomorph zu

$$B \cap C/(B' \cap C + B \cap C') \ ,$$

womit das Lemma 7.2 bewiesen ist.

Beweis des Satzes 7.1 Wir schieben zwischen A_i und A_{i+1} die Moduln

$$A_{ij} = A_i + (A_{i+1} \cap B_j) \ , \quad j = 0, 1, \ldots, m$$

ein und zwischen B_j und B_{j+1} die Moduln

$$B_{j,i} = B_j + (B_{j+1} \cap A_i) \ , \quad i = 0, 1, \ldots, n \ .$$

Dann gilt gemäss dem Lemma 7.2

$$\begin{aligned} A_{i,j+1}/A_{i,j} &\simeq (A_i + (A_{i+1} \cap B_{j+1}))/(A_i + (A_{i+1} \cap B_j)) \\ &\simeq (B_j + (B_{j+1} \cap A_{i+1}))/(B_j + (B_{j+1} \cap A_i)) \\ &\simeq B_{i+1,j}/B_{i,j} \ . \end{aligned}$$

Dabei sind natürlich die Gleichungen $A_{i-1,m} = A_i = A_{i,0}$ und $B_{n,j-1} = B_{j+1} = B_{0,j}$ zu beachten. Die verfeinerten Reihen haben somit gleiche Länge und isomorphe Faktoren.

Definition Die echt aufsteigende Reihe von Untermoduln

$$0 = A_0 \subset A_1 \subset A_2 \subset \cdots \subset A_m = A$$

heisst *Kompositionsreihe* des Moduls A, wenn keine echten Verfeinerungen der Reihe existieren. Mit Satz 6.3 folgt sofort:

Genau dann besitzt eine echt aufsteigende Reihe von Untermoduln keine echten Verfeinerungen, wenn alle ihre Faktoren einfach sind.

Beispiele (1) Es sei $A = M_1 \oplus M_2 \oplus \cdots \oplus M_m$ (endlich) halbeinfach. Dann erhält man eine Reihe von Untermoduln von A, indem man setzt

$$A_0 = 0, \ A_1 = M_1, \ A_2 = M_1 \oplus M_2, \ \ldots, \ A_m = M_1 \oplus M_2 \oplus \cdots \oplus M_m \ .$$

Dies ist offensichtlich eine Kompositionsreihe, denn es gilt

$$A_i/A_{i-1} = (M_1 \oplus M_2 \oplus \cdots \oplus M_{i-1} \oplus M_i)/(M_1 \oplus M_2 \oplus \cdots \oplus M_{i-1}) \simeq M_i \ ,$$

und nach Voraussetzung ist M_i, $i = 1, 2, \ldots, m$ ein einfacher Modul.

(2) Nicht jeder Modul besitzt eine Kompositionsreihe: Für $\Lambda = \mathbb{Z}$ besitzt $A = \mathbb{Z}$ keine Kompositionsreihe, denn jede Reihe von Untermoduln lässt sich echt verfeinern.

Korollar 7.3 (Jordan-Hölder) *Es seien*

$$0 = A_0 \subset A_1 \subset A_2 \subset \cdots \subset A_m = A$$

und

$$0 = B_0 \subset B_1 \subset B_2 \subset \cdots \subset B_n = A$$

zwei Kompositionsreihen von A. Dann ist $m = n$, und es existiert eine Permutation π der Zahlen $1, 2, \ldots, m$ mit $A_i/A_{i-1} \simeq B_{\pi(i)}/B_{\pi(i)-1}$ für $i = 1, 2, \ldots, m$.

Korollar 7.4 (Krull-Schmidt) *Es seien $\bigoplus_{i=0}^{m} M_i$ und $\bigoplus_{j=0}^{n} N_i$ zwei Zerlegungen des Moduls A in eine direkte Summe von einfachen Moduln. Dann ist $m = n$, und es existiert eine Permutation π der Zahlen $1, 2, \ldots, m$ mit $M_i \simeq N_{\pi(i)}$.*

IV.8 Tensorprodukt

Ist Λ ein beliebiger Ring, so lässt sich der Begriff des Tensorproduktes eines Λ-Rechtsmoduls A und eines Λ-Linksmoduls B definieren. Wir behandeln hier nicht diesen allgemeinen Fall, sondern beschränken uns auf den Fall eines *kommutativen* Ringes. Dies erlaubt eine etwas einfachere Darstellung: erstens brauchen wir nicht zwischen Links- und Rechtsmoduln zu unterscheiden, und zweitens ist für einen kommutativen Ringe Λ das Tensorprodukt zweier Λ-Moduln wieder ein Λ-Modul.

Es sei Λ ein beliebiger *kommutativer* Ring, und es seien A, B, X drei Λ-Moduln.

Definition Eine Funktion $f : A \times B \to X$ heisst Λ-*bilinear*, wenn für $a, a' \in A$, $b, b' \in B$ und $\lambda \in \Lambda$ gilt

$$\begin{aligned} f(a + a', b) &= f(a, b) + f(a', b) \ , \\ f(a, b + b') &= f(a, b) + f(a, b') \ , \\ f(a\lambda, b) &= f(a, \lambda b) = \lambda f(a, b) \ . \end{aligned}$$

Falls f bilinear ist, so gilt automatisch $f(a,0) = 0 = f(0,b)$, $f(-a,b) = f(a,-b) = -f(a,b)$.

Das Tensorprodukt erlaubt, einer Λ-bilinearen Abbildung in eindeutiger Weise eine Λ-*lineare* Abbildung (Λ-Modulhomomorphismus) zuzuordnen.

Wir konstruieren den Λ-Modul $A \otimes_\Lambda B$ wie folgt. Wir betrachten die Menge S der Paare (a,b) mit $a \in A$ und $b \in B$ und den freien Λ-Modul F auf S. In F betrachten wir den Untermodul L, der von allen Elementen der folgenden Form erzeugt wird, $a, a' \in A$, $b, b' \in B$ und $\lambda \in \Lambda$:

$$(*) \quad \begin{cases} (a,b) + (a',b) - (a+a',b) \ , \\ (a,b) + (a,b') - (a,b+b') \ , \\ (a\lambda,b) - (a,\lambda b) \ , \\ (a\lambda,b) - \lambda(a,b). \end{cases}$$

Definition Das *Tensorprodukt* $A \otimes_\Lambda B$ ist definiert durch

$$A \otimes_\Lambda B = F/L \ .$$

Die Restklasse des Elementes (a,b) bezeichnen wir mit $a \otimes b$.

Die Funktion $\tau : A \times B \to A \otimes_\Lambda B$ definiert durch $\tau(a,b) = a \otimes b$ ist bilinear.
Beweis Es gilt für $a, a' \in A$, $b, b' \in B$

$$\begin{aligned} \tau(a+a',b) &= (a+a') \otimes b \\ &\equiv (a+a',b) \bmod L \\ &\equiv (a+a',b) + (a,b) + (a',b) - (a+a',b) \bmod L \\ &\equiv (a,b) + (a',b) \bmod L \\ &= a \otimes b + a' \otimes b \\ &= \tau(a,b) + \tau(a',b) \ . \end{aligned}$$

Für die anderen Beziehungen verläuft der Beweis analog.

Die Relationen $(*)$ übersetzen sich im Tensorprodukt in die folgenden Rechenregeln, $a, a' \in A$, $b, b' \in B$ und $\lambda \in \Lambda$:

$$a \otimes b + a' \otimes b \quad = \quad (a+a') \otimes b \ ,$$

$$\begin{aligned} a \otimes b + a \otimes b' &= a \otimes (b + b') \ , \\ \lambda(a \otimes b) = a\lambda \otimes b &= a \otimes \lambda b \ . \end{aligned}$$

Satz 8.1 (Universelle Eigenschaft des Tensorproduktes) *Zu jedem Λ-Modul X und zu jeder Λ-bilinearen Abbildung $f : A \times B \to X$ existiert ein eindeutig bestimmter Homomorphismus von Λ-Moduln $\phi : A \otimes_\Lambda B \to X$ mit $\phi \circ \tau = f$.*

Beweis Die Bedingung $\phi \circ \tau(a, b) = f(a, b)$ liefert sofort $\phi(a \otimes b) = f(a, b)$. Wenn also ϕ existiert, so ist es eindeutig bestimmt. Es ist zu zeigen, dass $\phi : A \otimes_\Lambda B \to X$ ein Λ-Modulhomomorphismus ist. Zu diesem Zweck definieren wir einen Λ-Modulhomomorphismus $\Phi : F \to X$ durch die Vorgabe auf der Basis von F, nämlich $\Phi(a, b) = f(a, b)$. Wir behaupten, dass Φ auf dem Untermodul L verschwindet. In der Tat gilt, da f bilinear ist, für $a, a' \in A$, $b \in B$,

$$\begin{aligned} \Phi((a, b) + (a', b) - (a + a', b)) &= \Phi(a, b) + \Phi(a', b) - \Phi(a + a', b) \\ &= f(a, b) + f(a', b) - f(a + a', b) \\ &= 0 \ . \end{aligned}$$

Analoge Überlegungen liefern, dass Φ auch auf den anderen Erzeugenden von L verschwindet. Damit faktorisiert Φ über $\phi : F/L = A \otimes_\Lambda B \to X$, und gemäss Definition ist $\phi(a \otimes b) = f(a, b)$.

Wir erinnern hier daran, dass eine universelle Eigenschaft das Objekt bis auf Isomorphie festlegt. Dies gilt auch hier: die universelle Eigenschaft des Tensorproduktes $A \otimes_\Lambda B$ legt dieses zusammen mit τ bis auf Isomorphie fest.

Beispiele und Bemerkungen (1) Es sei $\Lambda = k$ ein Körper. Es seien A und B k-Vektorräume mit Basen $\{a_i\}$, $i \in I$ bzw. $\{b_j\}$, $j \in J$. Ferner sei C der k-Vektorraum mit Basis $\{c_{ij}\}$, $i \in I$, $j \in J$. Die k-bilineare Abbildung $\sigma : A \times B \to C$ sei durch $\sigma(a_i, b_j) = c_{ij}$ definiert. Wir behaupten, dass C zusammen mit σ die universelle Eigenschaft des Tensorproduktes besitzt und deshalb mit dem oben auf abstrakte Weise definierte Tensorprodukt (bis auf Isomorphie) übereinstimmt.

Um dies zu *beweisen* betrachten wir einen beliebigen k-Vektorraum X und eine beliebige k-bilineare Abbildung $f : A \times B \to X$. Dann definieren wir die k-lineare Abbildung $\phi : C \to X$ durch $\phi(c_{ij}) = f(a_i, b_j)$, $i \in I, j \in J$. Für diese gilt offensichtlich $\phi \circ \sigma = f$. Ausserdem ist ϕ die einzige Abbildung mit dieser Eigenschaft.

Natürlich wird man im k-Vektorraum $C = A \otimes_\Lambda B$ die Basiselemente c_{ij} durch $a_i \otimes b_j$ bezeichnen. Jedes Element $t \in A \otimes_\Lambda B$ lässt sich in eindeutiger Weise als k-Linearkombina-

tion $t = \sum \lambda^{ij}(a_i \otimes b_j)$ darstellen, wobei $\lambda^{ij} \in k$ die Komponenten des Tensors t bezüglich der Basen $\{a_i\}$, $i \in I$ und $\{b_j\}$, $j \in B$ heissen.
Sind $\{a'_k\}$, $k \in I$ und $\{b'_l\}$, $l \in J$ neue Basen mit

$$a_i = \sum A_i^k a'_k \ , \quad b_j = \sum B_j^l b'_l$$

so folgt

$$\begin{aligned} a_i \otimes b_j &= \sum A_i^k a'_k \otimes \sum B_j^l b'_l \\ &= \sum A_i^k B_j^l (a'_k \otimes b'_l) \end{aligned}$$

also

$$t = \sum \lambda^{ij}(a_i \otimes b_j) = \sum \lambda^{ij} A_i^k B_j^l (a'_k \otimes b'_l) = \sum \mu^{kl}(a'_k \otimes b'_l) \ .$$

Daraus liest man die bekannte Transformationsformel für die Tensorkomponenten ab:

$$\mu^{kl} = \sum \lambda^{ij} A_i^k B_i^l \ .$$

(2) *Es gilt* $A \otimes_\Lambda \Lambda \simeq A$ *und* $\Lambda \otimes_\Lambda B \simeq B$.
Beweis Die Zuordnung $a \otimes \lambda \mapsto a\lambda$ definiert eine Abbildung $A \otimes_\Lambda \Lambda \to A$ und $a \to a \otimes 1_\Lambda$ definiert eine Abbildung $A \to A \otimes_\Lambda \Lambda$. Beides sind Λ-Modulhomomorphismen und die Zusammensetzung ist die Identität in A bzw. die Identität in $A \otimes_\Lambda \Lambda$. Der zweite Isomorphismus wird auf analoge Weise bewiesen.

(3) *Es gilt* $(A \oplus A') \otimes_\Lambda B \simeq (A \otimes_\Lambda B) \oplus (A' \otimes_\Lambda B)$.
Beweis Der Isomorphismus ist gegeben durch die Zuordung $(a, a') \oplus b \mapsto ((a \otimes b), (a' \otimes b'))$.

(4) *Es sei* A *ein freier* Λ*-Modul,* $A = \bigoplus \Lambda_i$ *mit* $\Lambda_i \simeq \Lambda$. *Dann gilt* $A \otimes_\Lambda B = \bigoplus (\Lambda_i \otimes_\Lambda B) = \bigoplus B_i$ *mit* $B_i \simeq B$.

(5) *Es sei* A *eine* Λ*-Algebra. Dann besitzt* $A \otimes_\Lambda B$ *automatisch die Struktur eines Linksmoduls über* A. Die Operation von A ist gegeben durch $a'(a \otimes b) = (a'a) \otimes b$. Es ist leicht, die Axiome nachzuprüfen. Durch dieses Verfahren wird, wie man sagt, der *Skalarbereich erweitert*, nämlich von Λ zu A. Als explizite Beispiele erwähnen wir die folgenden.
(a) Es sei $\Lambda = \mathbb{R}$ und $A = \mathbb{C}$. Ist B ein reeller Vektorraum, so ist $\mathbb{C} \otimes_\mathbb{R} B$ ein komplexer Vektorraum. Man nennt $\mathbb{C} \otimes_\mathbb{R} B$ auch etwa die *Komplexifizierung* des Raumes B. Ist $\{b_i\}$,

$i \in I$ eine Basis von B, so ist $\{1 \otimes b_i\}$, $i \in I$ eine Basis von $\mathbb{C} \otimes_{\mathbb{R}} B$. Oft werden diese Basen stillschweigend identifiziert.

(b) Es sei $\Lambda = \mathbb{Z}$ und $A = \mathbb{Q}$. Ist B eine abelsche Gruppe so ist $\mathbb{Q} \otimes_{\mathbb{Z}} B$ ein $\mathbb{Q}$-Vektorraum. Zu dieser Situation gehört offenbar die Abbildung $\mu : B \to \mathbb{Q} \otimes_{\mathbb{Z}} B$. *Es gilt* $\ker \mu = T(B)$.

Beweis Es sei $b \in T(B)$. Dann existiert $0 \neq m \in \mathbb{Z}$ mit $mb = 0$. Dann folgt $\mu b = 1 \otimes b = 1\frac{m}{m} \otimes b = \frac{1}{m} \otimes mb = \frac{1}{m} \otimes 0 = 0$. Daraus folgt $T(B) \subseteq \ker \mu$. Die Umkehrung beweisen wir hier nur für endlich erzeugte abelsche Gruppen. Für diese ist zu beweisen, dass μ eine injektive Abbildung $B/T(B) \to \mathbb{Q} \otimes B$ induziert. Nun ist aber $B/T(B)$ frei, $B/T(B) \simeq \bigoplus \mathbb{Z}_i$, $\mathbb{Z}_i \simeq \mathbb{Z}$. Damit folgt $\mathbb{Q} \otimes_{\mathbb{Z}} \bigoplus \mathbb{Z}_i \simeq \bigoplus \mathbb{Q}_i$ mit $\mathbb{Q}_i \simeq \mathbb{Q}$, und μ bildet eine Basis der freien abelschen Gruppe $B/T(B)$ in eine Basis des $\mathbb{Q}$-Vektorraumes ab. Damit ist μ injektiv.

Die Dimension des $\mathbb{Q}$-Vektorraumes $\mathbb{Q} \otimes_{\mathbb{Z}} B$ heisst *(torsionsfreier) Rang* der abelschen Gruppe B. Diese Zahl ist offensichtlich gleich der Mächtigkeit einer maximal linear unabhängigen Menge Φ_m in B.

(6) Es sei $\Lambda = \mathbb{Z}$. Wir betrachten $A = \mathbb{Z}/m\mathbb{Z}$ und $B = \mathbb{Z}/n\mathbb{Z}$. *Für* $(m, n) = 1$ *gilt* $A \otimes_{\mathbb{Z}} B = 0$.

Beweis Zu $(m, n) = 1$ existieren $u, v \in \mathbb{Z}$ mit $um + vn = 1$. Dann folgt

$$a \otimes b = (um + vn)(a \otimes b) = uma \otimes b + a \otimes vnb = 0 \ .$$

Es ist also in der Tat $A \otimes_{\mathbb{Z}} B = 0$.

(7) Es sei $\alpha : A \to A'$ ein Homomorphismus von Λ-Moduln. Dann induziert α einen Homomorphismus von Λ-Moduln $\phi_* : A \otimes_\Lambda B \to A' \otimes_\Lambda B$ durch $\phi_*(a \otimes b) = \phi(a) \otimes b$.

Dazu bemerken wir noch folgendes: Es sei $\Lambda = \mathbb{Z}$, $A = A' = \mathbb{Z}$ und $B = \mathbb{Z}/2\mathbb{Z}$. Die Abbildung $\phi : \mathbb{Z} \to \mathbb{Z}$ sei durch $\phi(n) = 2n$ definiert. Dann ist ϕ_* durch $\phi_*(n \otimes a) = 2n \otimes a = n \otimes 2a = 0$ gegeben. Es ist also ϕ_* die Nullabbildung; dies obschon ϕ selbst nichttrivial und injektiv war.

Kapitel V. Elemente der Darstellungstheorie

Einleitung

Das vorliegende Kapitel führt in die Darstellungstheorie der Gruppen ein. Im Vordergrund stehen dabei *endliche* Gruppen und *komplexe* Darstellungen. Nur an einigen wenigen Stellen wird der Blick auch auf allgemeinere Situationen geöffnet: auf kompakte topologische bzw. Liegruppen und auf Darstellungen über Körpern, die von den komplexen Zahlen verschieden sind.

Die Darstellungstheorie der Gruppen geht wesentlich auf F.G. Frobenius (1849-1917)[10], W. Burnside (1852-1927) und I. Schur (1875-1941) zurück. Sie beschäftigt sich mit linearen Operationen einer Gruppe auf einem Vektorraum. Überraschenderweise führt dieser eigentlich einfache Ansatz zu tiefliegenden Resultaten. Insbesondere sind der Darstellungstheorie ganz wichtige Resultate zur Strukturtheorie endlicher Gruppen zu verdanken; so lässt sich mit ihrer Hilfe oft die Einfachheit einer Gruppe nachweisen; siehe Abschnitt V.7, Beispiel (e), wo dieser Weg exemplarisch beschritten wird, um die Einfachheit der Gruppe $\mathbf{A}_5$ zu beweisen. Ferner hat die Darstellungstheorie mannigfache weitere Anwendungen in und ausserhalb der Mathematik gefunden, beispielsweise in der Quantentheorie (siehe Abschnitt V.6).

Es können hier nur die grundlegendsten Begriffe und Resultate behandelt werden. Es existiert eine umfangreiche Spezialliteratur, welche die Theorie in den verschiedensten Richtung weiterführt.

[10] Ferdinand Georg Frobenius war von 1875 bis 1892 Professor am Eidgenössischen Polytechnikum.

V.1 $\mathbb{C}[G]$-Moduln und Darstellungen

Es sei G eine multiplikative Gruppe und A ein $\mathbb{C}$-Vektorraum.

Für das ganze Kapitel setzen wir $\dim_{\mathbb{C}} A < \infty$ *voraus.*

Eine **Darstellung** T von G im Darstellungsraum A besteht aus $\mathbb{C}$-linearen Abbildungen $T_x : A \to A$, $x \in G$, wobei die folgenden Bedingungen (*Darstellungsbedingungen*) erfüllt sind

$$T_{xy} = T_x \circ T_y \ , \quad T_e = 1_A \ .$$

Insbesondere ist die Abbildung T_x invertierbar: $(T_x)^{-1} = T_{x^{-1}}$. Aus den Darstellungsbedingungen folgt, dass eine Darstellung von G der Dimension n auch als ein Gruppenhomomorphismus

$$T : \ G \to GL(n, \mathbb{C})$$

aufgefasst werden kann.

Wir haben im Kapitel über die Modultheorie (siehe Kapitel IV) bereits gesehen, dass eine Darstellung von G im Darstellungsraum A Anlass gibt zu einer $\mathbb{C}[G]$-Modulstruktur in A, indem $xa = T_x a$, $x \in G$, $a \in A$ gesetzt wird. Umgekehrt definiert eine $\mathbb{C}[G]$-Modulstruktur in A in eindeutiger Weise eine Darstellung T von G im $\mathbb{C}$-Vektorraum A. Ein Sachverhalt kann deshalb immer sowohl in der Sprache der Modultheorie als auch in der Sprache der Darstellungstheorie beschrieben werden. Wir beginnen mit einer Gegenüberstellung einiger Grundbegriffe, wie sie sich in den beiden Sprachen ausdrücken.

Modulsprache	**Darstellungssprache**
Untermodul $B \subseteq A$	B ist Unterraum von A mit $T_x(B) \subseteq B$ für alle $x \in G$; d.h. ein unter G *invarianter Unterraum* von A.
A einfach	Es gibt keinen invarianten Unterraum in A ausser 0 und A selbst; in diesem Fall heisst die Darstellung T *irreduzibel*.
$A = A_1 \oplus A_2$ direkte Summe von Untermoduln	A_1 und A_2 sind komplementäre invariante Unterräume. Die Darstellung T *zerfällt* in $T^{(1)}$ und $T^{(2)}$. Wir schreiben $T = T^{(1)} \oplus T^{(2)}$.

A halbeinfach, $A = A_1 \oplus A_2 \oplus \cdots \oplus A_m,\ A_i$ einfach	Die Darstellung T zerfällt in Darstellungen $T^{(1)}, T^{(2)}, \cdots, T^{(m)}$, wobei die in A_i stattfindende Darstellung $T^{(i)}$ irreduzibel ist. Die Darstellung T heisst in diesem Fall *vollreduzibel*.
$\mathbb{C}[G]$-Homomorphismus $f : A \to B$	$\mathbb{C}$-lineare Abbildung $f : A \to B$ mit $f(T_x a) = S_x f(a)$. Dabei ist T die Darstellung in A und S die Darstellung in B. Die Abbildung f ist mit den Darstellungen T und S *verträglich*.
$\mathbb{C}[G]$-Isomorphismus $f : A \xrightarrow{\sim} B$	$\mathbb{C}$-lineare Abbildung $f : A \to B$ mit $f(T_x a) = S_x f(a)$ und f ist invertierbar. Die Darstellungen T in A und S in B heissen in diesem Fall *äquivalent*.

Die folgenden Resultate sind direkte Übersetzungen der entsprechenden Sätze IV.64 und IV.6.7 der Modultheorie.

Satz 1.1 *Die Darstellung T von G in A ist genau dann vollreduzibel, wenn in A jeder invariante Unterraum ein invariantes Komplement besitzt.*

Satz 1.2 *Es sei T eine vollreduzible Darstellung von G in A. Die Zerlegung von T in irreduzible Darstellungen $T^{(i)}$ ist bis auf Reihenfolge und Äquivalenz eindeutig.*

Als Vorbereitung auf Abschnitt 3 beweisen wir den folgenden Satz.

Satz 1.3 *Jede unitäre Darstellung ist vollreduzibel.*

Definition Es sei A ein komplexer Vektorraum, und $\langle v, w\rangle$ ein unitäres Skalarprodukt in A. Die Darstellung T in A heisst *unitär* bezüglich $\langle\ ,\ \rangle$, wenn $\langle T_x v,\ T_x w\rangle = \langle v, w\rangle$ gilt für alle $x \in G,\ v, w \in A$. Die Darstellung T heisst *unitär*, wenn in A ein Skalarprodukt existiert, bezüglich dem T unitär ist.

Beweis Es seien $A' \subseteq A$ ein invarianter Unterraum und A'' sein orthogonales Komplement, $A'' = \{\, b \in A \mid \langle b, a'\rangle = 0 \text{ für alle } a' \in A'\}$. Für alle $b \in A''$ gilt dann

$$\langle T_x b,\ a'\rangle = \langle b,\ T_{x^{-1}} a'\rangle = 0\ .$$

Daraus folgt $T_x b \in A''$, d.h. A'' ist invariant. Nach Satz 1.1 ist T vollreduzibel.

Es sei $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ eine Basis von A, $n = \dim_{\mathbb{C}} A$. Dann entspricht der Transformation $T_x : A \to A$ eine reguläre $n \times n$-Matrix $[t_{ij}(x)]$; diese ist durch $T_x(\alpha_j) = \sum_{i=1}^{n} t_{ij}(x)\ \alpha_i$, $i = 1, 2, \ldots, n$ gegeben.

Ist A' ein invarianter Unterraum von A, so kann man die Basis $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ so wählen, dass die Teilfamilie $\{\alpha_1, \alpha_2, \ldots, \alpha_k\}$ eine Basis von A' ist. Die Matrix von T_x hat dann die Form

$$\begin{bmatrix} * & \cdots & * & * & \cdots & * \\ \vdots & & \vdots & \vdots & & \vdots \\ * & \cdots & * & * & \cdots & * \\ 0 & \cdots & 0 & * & \cdots & * \\ \vdots & & \vdots & \vdots & & \vdots \\ 0 & \cdots & 0 & * & \cdots & * \end{bmatrix}$$

und zwar simultan für alle $x \in G$.

Falls die Darstellung zerfällt, $A = A_1 \oplus A_2$, so kann eine Basis so gewählt werden, dass die ersten k Elemente eine Basis von A_1 bilden und die restlichen $(n - k)$ Elemente eine Basis von A_2. Die Matrix von T_x hat dann die Form

$$\begin{bmatrix} * & \cdots & * & 0 & \cdots & 0 \\ \vdots & & \vdots & \vdots & & \vdots \\ * & \cdots & * & 0 & \cdots & 0 \\ 0 & \cdots & 0 & * & \cdots & * \\ \vdots & & \vdots & \vdots & & \vdots \\ 0 & \cdots & 0 & * & \cdots & * \end{bmatrix}$$

und zwar simultan für alle $x \in G$.

Es sei $f : A \to B$ ein $\mathbb{C}[G]$-Homomorphismus. In fest gewählten Basen in A und B werde die Abbildung f durch die Matrix F beschrieben. Bezeichen S_x und T_x für $x \in G$ die Matrizen bezüglich der gegebenen Basen der Darstellungen S in A und T in B, so gilt die Matrizenbeziehung $FS_x = T_xF$ für alle $x \in G$. Ist f ein $\mathbb{C}[G]$-Isomorphismus ($m = n$, $\det f \neq 0$), so ist F invertierbar, und es folgt $FS_xF^{-1} = T_x$. Zu *äquivalenten Darstellungen* gehören folglich *ähnliche Darstellungsmatrizen.*

V.2 Das Lemma von Schur

Der folgende wichtige Satz ist bekannt als *Lemma von Schur*.

Satz 2.1 (I. Schur) *Es sei $f : A \to B$ ein $\mathbb{C}[G]$-Homomorphismus, A, B seien einfach. Dann ist f entweder die Nullabbildung oder ein Isomorphismus.*

Beweis Da f ein Modulhomomorphismus ist, ist $\ker f$ ein Untermodul von A. Da A einfach ist, gilt entweder $\ker f = A$ (d.h. f ist die Nullabbildung) oder $\ker f = 0$ (d.h. f ist injektiv). Ist f injektiv, so ist $\operatorname{im} f \neq 0$. Da B einfach ist, muss gelten $\operatorname{im} f = B$, d.h. f ist surjektiv. Folglich ist in diesem Fall f ein Isomorphismus.

Wir bemerken noch folgendes. Es sei A ein einfacher $\mathbb{C}[G]$-Modul und $f : A \to A$ ein $\mathbb{C}[G]$-Modul*endo*morphismus. Dann ist f die Nullabbildung oder ein Isomorphismus. Da $\mathbb{C}$ algebraisch abgeschlossen ist, existiert ein Eigenwert λ von f. Betrachte $g = f - \lambda 1_A : A \to A$. Dies ist ein $\mathbb{C}[G]$-Homomorphismus. Aus $\ker g \neq 0$ folgt $g = 0$, d.h. $f = \lambda 1_A$. Damit ist der folgende Satz bewiesen.

Satz 2.2 *Es sei A ein einfacher $\mathbb{C}[G]$-Modul. Dann ist jeder $\mathbb{C}[G]$-Endomorphismus von A ein Vielfaches der Identität; es gilt* $\operatorname{End}_{\mathbb{C}[G]} A = \mathbb{C}$.

In Matrizenform lautet dieses Resultat wie folgt: Es sei T eine irreduzible Darstellung von G in A, und es sei $f : A \to A$ eine lineare Abbildung mit $f \circ T_x = T_x \circ f$ für alle $x \in G$. Dann ist f ein komplexes Vielfaches der Identität.

Es sei nun G abelsch und T eine irreduzible Darstellung in A. Dann gilt $T_x \circ T_y = T_{xy} = T_{yx} = T_y \circ T_x$. Wie oben die Abbildung f so vertauscht die lineare Transformation T_y für alle $x \in G$ mit T_x. Aus Satz 2.2 folgt $T_y = \lambda \cdot 1_A$, $\lambda = \lambda(y) \in \mathbb{C}$. Jeder Unterraum von A ist damit unter T invariant. Nun ist aber A irreduzibel, also muss gelten $\dim_{\mathbb{C}} A = 1$.

Satz 2.3 *Jede irreduzible Darstellung einer abelschen Gruppe ist eindimensional.*

Für eine irreduzible und deshalb eindimensionalen Darstellung T der abelschen Gruppe G entspricht T_y der Multiplikation mit einer komplexen Zahl $\lambda(y)$. Die Regel $T_y \circ T_x = T_{yx}$ impliziert $\lambda(y) \cdot \lambda(x) = \lambda(yx)$. Damit ist die Zuordnung $x \mapsto \lambda(x)$ ein Gruppenhomomorphismus $\lambda : G \to \mathbb{C}^\bullet$.

Bemerkung Für $\mathbb{R}$ an Stelle von $\mathbb{C}$ ist die Aussage des Satzes 2.3 im allgemeinen nicht richtig: Betrachtet man die Ebene als zweidimensionalen reellen Vektorraum, so gibt die

Drehung T_t um $2\pi/3$ um den Nullpunkt Anlass zu einer reellen 2-dimensionalen Darstellung der zyklischen Gruppe $C_3 = \langle t \rangle$ der Ordnung 3. Da T_t keinen reellen Eigenwert und damit auch keinen reellen Eigenvektor besitzt, kann kein invarianter Unterraum existieren. Als *reelle* Darstellung ist T deshalb irreduzibel.

V.3 Die Vollreduzibilität der Darstellungen

Satz 3.1 *Es sei G eine endliche Gruppe. Dann ist jede komplexe Darstellung T von G unitär.*

Wir erinnern daran, dass dies bedeutet, dass im Darstellungsraum A ein unitäres Skalarprodukt $\langle\ ,\ \rangle$ existiert mit $\langle T_x a, T_x b\rangle = \langle a, b\rangle$ für alle $a, b \in A$ und alle $x \in G$. Zusammen mit dem Satz 1.3 folgt daraus sofort das folgende grundlegende Resultat, das als *Satz von Maschke* bekannt ist.

Satz 3.2 (H. Maschke) *Jede komplexe Darstellung einer endlichen Gruppe ist vollreduzibel. Jeder $\mathbb{C}[G]$-Modul ist halbeinfach.*

Beweis Es sei $|G|$ die Ordnung der Gruppe G und T eine Darstellung von G in A. Man wähle in A irgendein unitäres Skalarprodukt $[\ ,\ ] : A \times A \to \mathbb{C}$ und definiere ein neues Skalarprodukt $\langle\ ,\ \rangle$ durch

$$\langle a, b\rangle = \frac{1}{|G|} \sum_{x \in G} [T_x a, T_x b]\ .$$

Dass $\langle\ ,\ \rangle$ ein unitäres Skalarprodukt ist, beweist man leicht mit einigen einfachen Rechnungen. Es bleibt zu zeigen, dass die Darstellung T bezüglich $\langle\ ,\ \rangle$ unitär ist. Es gilt für $a, b \in A$ und $y \in G$:

$$\langle T_y a, T_y b\rangle = \frac{1}{|G|} \sum_{x \in G} [T_x \circ T_y(a), T_x \circ T_y(b)] = \frac{1}{|G|} \sum_{x \in G} [T_{xy} a, T_{xy} b] = \langle a, b\rangle\ .$$

Damit ist Satz 3.1 bewiesen.

Bemerkung Der obige Beweis lässt sich verallgemeinern. Die Bildung

$$Mf = \frac{1}{|G|} \sum_{x \in G} f(x)$$

liefert eine "Mittelbildung" für komplexwertige Funktionen $f : G \to \mathbb{C}$. Ist G eine beliebige, nicht notwendigerweise endliche Gruppe und M eine derartige Mittelbildung für eine gewisse Klasse von Funktionen $G \to \mathbb{C}$, so lässt sich der obige Beweis auf diesen Fall übertragen. Die Analyse des Beweises zeigt, dass die Mittelbildung $f \mapsto Mf$ die folgenden Eigenschaften besitzen muss:

(1) *linear*: $M(\lambda f + \mu g) = \lambda Mf + \mu Mg$ für $\lambda, \mu \in \mathbb{C}$.
(Damit wird $\langle\ ,\ \rangle$ eine hermitesche Bilinearform.)

(2) *positiv*: Für eine Funktion f mit $f(x) \geq 0$ für alle $x \in G$ folgt $Mf \geq 0$; und $Mf = 0$ gilt nur für $f \equiv 0$.
(Damit wird $\langle\ ,\ \rangle$ positiv definit.)

(3) *normiert*: Für die Funktion f mit $f(x) = 1$ für alle $x \in G$ folgt $Mf = 1$.
(Die Klasse von Funktionen, für die M definiert ist, enthält mindestens die Funktion $f \equiv 1$.)

(4) *invariant*: Für $y \in G$ sei h definiert durch $h(x) = f(xy)$; dann gilt $Mh(x) = Mf(x)$.
(Damit wird die Darstellung T unitär bezüglich dem neuen Skalarprodukt.)

Wir sagen, G sei eine M-Gruppe, wenn für eine gewisse Klasse von komplexwertigen Funktionen eine Mittelbildung M mit (1), (2), (3), (4) definiert ist.

Beispiele (a) Es sei G endlich. Dann liefert

$$Mf = \frac{1}{|G|} \sum_{x \in G} f(x)$$

für Funktionen $f : G \to \mathbb{C}$ eine derartige Mittelbildung.
(b) Es sei G die Gruppe der Drehungen der komplexen Zahlebene um den Nullpunkt; also $G = \{e^{i\alpha} \mid \alpha \bmod 2\pi\}$. Für $f : G \to \mathbb{C}$ setze man

$$Mf = \frac{1}{2\pi} \int_0^{2\pi} f(e^{i\alpha})\, d\alpha\ .$$

Es ist klar, dass dieses M insbesondere für stetige Funktionen f die verlangten Eigenschaften besitzt.

Satz 3.3 *Jede M-Darstellung T von G ist unitär und somit vollreduzibel.*

Bemerkungen (1) Man muss hier beachten, dass man nur sogenannte M-Darstellungen betrachtet: eine M-Darstellung ist dadurch definiert, dass die Mittelbildung M für die im Beweis zu mittelnden Funktionen definiert ist. Betrachten wir zum Beispiel für die Drehgruppe der Ebene *stetige* Darstellungen, so sind die zu mittelnden Funktionen sicher ebenfalls stetig. Die im obigen Beispiel angegebene Mittelbildung lässt sich also in diesen Fall anwenden und liefert das Resultat, dass *die stetigen Darstellungen der Drehgruppe vollreduzibel sind*.

(2) Ist G eine kompakte topologische Gruppe, so existiert für stetige Funktionen immer eine Mittelbildung der verlangten Art. Es existiert in diesem Fall nämlich ein sogenanntes invariantes Mass auf G (Haar'*sches Mass*); dieses ist sogar eindeutig bestimmt. Somit erhält man das Resultat, dass *die stetigen Darstellungen einer kompakten topologischen Gruppe vollreduzibel sind*. Ganz allgemein kann die Theorie dieser Darstellungen ähnlich entwickelt werden, wie diejenige für endliche Gruppen.

V.4 Orthogonalitätsrelationen

Es sei G eine endliche Gruppe der Ordnung $|G|$. Die folgenden Überlegungen lassen sich im Prinzip auch durchführen, wenn man die Bildung

$$Mf = \frac{1}{|G|}\sum_{x\in G} f(x)$$

durch eine allgemeine Mittelbildung M ersetzt. Der Übersichtlichkeit halber bleiben wir aber bei endlichen Gruppen und bei der zu diesen gehörigen Mittelbildung.

Es seien A und B zwei $\mathbb{C}[G]$-Moduln. Wir *definieren* zu einer $\mathbb{C}$-linearen Abbildung $h : A \to B$ eine $\mathbb{C}$-lineare Abbildung $f : A \to B$ durch

$$f(a) = \frac{1}{|G|}\sum_{x\in G} xh(x^{-1}a)\ , \quad a \in A\ .$$

Wir behaupten: *Die Abbildung $f : A \to B$ ist ein $\mathbb{C}[G]$-Homomorphismus.*

Beweis Für $a \in A$ und $y \in G$ gilt

$$f(ya) \;=\; \frac{1}{|G|}\sum_{x\in G} xh(x^{-1}(ya))$$

$$\begin{aligned} &= \frac{1}{|G|}\sum_{x\in G} y(y^{-1}x)h((y^{-1}x)^{-1}a) \\ &= y\left(\frac{1}{|G|}\sum_{z\in G} zh(z^{-1}a)\right) \\ &= yf(a)\ . \end{aligned}$$

Es seien nun zusätzlich A und B einfach. Dann können nach dem Lemma von Schur nur die folgenden Fälle eintreten: entweder gilt (i) $f = 0$, oder (ii) $m = n$ und $\det f \neq 0$.

(1) Es seien A und B nicht isomorph. Dann muss der Fall (i) eintreten und zwar für jede beliebig gewählte $\mathbb{C}$-lineare Abbildung h. Wir wählen in A und B Basen. Die Abbildung $S_x : a \mapsto xa$ werde durch die Matrix $[s_{ij}(x)]$ beschrieben, die Abbildung $T_x : b \mapsto xb$ durch $[t_{kl}(x)]$ und h durch $[h_{li}]$. Von der Möglichkeit h beliebig zu wählen, machen wir Gebrauch, indem wir h_{li} gleich der Matrix setzen, die nur in der l'-ten Zeile und der i'-ten Spalte eine Eins und sonst überall Nullen aufweist; d.h. $h_{li} = \delta_{ll'}\delta_{i'i}$. Dabei sind $1 \leq l' \leq n$ und $1 \leq i' \leq m$ beliebige, aber fest gewählte Zahlen. Dann folgt

$$\begin{aligned} 0 &= \frac{1}{|G|}\sum_{x\in G}\sum_{l,i} t_{kl}(x)\, h_{li}\, s_{ij}(x^{-1}) \\ &= \frac{1}{|G|}\sum_{x\in G}\sum_{l,i} t_{kl}(x)\, \delta_{ll'}\, \delta_{i'i}\, s_{ij}(x^{-1}) \\ &= \frac{1}{|G|}\sum_{x\in G} t_{kl'}(x)\, s_{i'j}(x^{-1})\ . \end{aligned}$$

Damit haben wir das folgende Resultat erhalten:

Satz 4.1 *Es seien S und T zwei irreduzible, nicht äquivalente Darstellungen der Dimensionen m bzw. n. Dann gilt für alle $1 \leq k, l \leq n$ und $1 \leq i, j \leq m$*

$$\frac{1}{|G|}\sum_{x\in G} t_{kl}(x)\, s_{ij}(x^{-1}) = 0\ .$$

Aus Gründen, die weiter unten klar werden, lassen wir hier den an sich überflüssigen Faktor $1/|G|$ stehen.

(2) Im Lemma von Schur kann der zweite Fall nur auftreten, wenn A und B isomorph sind und f ein Isomorphismus ist. Wir betrachten deshalb den Spezialfall $B = A$. Dann

ist $f : A \to A$ ein Vielfaches der Identität (siehe Satz 2.2) $f = \lambda 1_A$; die Matrix von f ist also $\lambda\delta_{kj}$. Es folgt

$$\lambda\delta_{kj} = \frac{1}{|G|} \sum_{x\in G} \sum_{l,i} s_{kl}(x)\, h_{li}\, s_{ij}(x^{-1}) \ .$$

Um λ aus $[h_{li}]$ zu bestimmen, berechnen wir die Spur:

$$\begin{aligned} m\lambda &= \lambda \sum_k \delta_{kk} \\ &= \frac{1}{|G|} \sum_{x\in G} \sum_{k,l,i} s_{kl}(x)\, h_{li}\, s_{ik}(x^{-1}) \\ &= \frac{1}{|G|} \sum_{x\in G} \sum_{l,i} \left(\sum_k s_{ik}(x^{-1})\, s_{kl}(x) \right) h_{li} \\ &= \frac{1}{|G|} \sum_{x\in G} \sum_{l,i} \delta_{il}\, h_{li} \\ &= \frac{1}{|G|} \sum_{x\in G} \sum_{l} h_{ll} \\ &= \sum_l h_{ll} \ . \end{aligned}$$

Es folgt

$$\lambda = \frac{1}{m} \text{ Spur } h \ .$$

Wählen wir nun wie oben $h_{li} = \delta_{i'i}\, \delta_{ll'}$, so erhalten wir

$$\frac{1}{|G|} \sum_{x\in G} s_{kl'}(x)\, s_{i'j}(x^{-1}) = \left\{ \begin{array}{ll} 0 & \text{für } \ i' \neq l' \\ \\ \dfrac{1}{m}\, \delta_{kj} & \text{für } \ i' = l' \end{array} \right\} = \frac{1}{m}\, \delta_{kj}\, \delta_{i'l'} \ .$$

Damit haben wir das folgende Resultat bewiesen:

Satz 4.2 *Es sei S eine irreduzible Darstellung von G der Dimension m. Dann gilt*

$$\frac{1}{|G|} \sum_{x\in G} s_{kl}(x)\, s_{ij}(x^{-1}) = \frac{1}{m}\, \delta_{kj}\, \delta_{il} \ .$$

Die beiden eben bewiesenen Resultate, Satz 4.1 und Satz 4.2, heissen *Orthogonalitätsrelationen*. Im Folgenden machen wir diese nun noch etwas präziser.

Wir wissen, dass die Darstellungen unitär sind. Wir können also in den obigen Überlegungen orthonormierte Basen zugrunde legen, bezüglich denen S und T durch unitäre Matrizen gegeben sind. Dann gilt

$$S_{x^{-1}} = (S_x)^{-1} = \overline{S_x}^T \ ,$$

wo $\overline{S_x}^T$ die zu S_x konjugierte und transponierte Matrix bezeichnet. Für $S_x = [s_{ij}(x)]$ gilt also $\overline{S_x}^T = [\overline{s_{ji}(x)}]$.

Korollar 4.3 *Es seien S und T zwei irreduzible, nicht äquivalente Darstellungen von G der Dimensionen m bzw n. Sie werden als unitäre Darstellungen angesehen, und man wähle entsprechende orthonormierte Basen. Dann gilt*

$$(t_{kl}, s_{ij}) = \frac{1}{|G|} \sum_{x \in G} t_{kl}(x) \overline{s_{ij}(x)} = 0 \ , \quad 1 \le i, j \le m \ , \quad 1 \le k, l \le n \ ;$$

$$(s_{kl}, s_{ij}) = \frac{1}{|G|} \sum_{x \in G} s_{kl}(x) \, \overline{s_{ij}(x)} = \frac{1}{m} \delta_{ki} \, \delta_{lj} \ , \quad 1 \le i, j, k, l \le m \ .$$

Man beachte, dass wir in diesen Gleichungen aus 'alphabetischen' Gründen gegenüber den Aussagen in den Sätzen 4.1 und 4.2 die Rollen von i und j vertauscht haben.

Bemerkungen (1) Im Vektorraum der komplexwertigen Funktionen $G \to \mathbb{C}$ definiert

$$\frac{1}{|G|} \sum_{x \in G} f(x) \, \overline{g(x)}$$

ein unitäres Skalarprodukt (f, g). Unser Korollar 4.3 sagt, dass die Funktionen $t_{kl}(x)$ und $s_{ij}(x)$ orthogonal sind und dass $s_{kl}(x)$ und $s_{ij}(x)$ ebenfalls orthogonal sind, ausser im Fall $(k, l) = (i, j)$.

(2) Es sei $T^{(1)}, T^{(2)}, \ldots$ eine Liste aller irreduziblen Darstellungen (bis auf Äquivalenz) von G; die Dimension der Darstellung $T^{(\nu)}$ sei n_ν. Dann gibt $T^{(\nu)}$ Anlass zu $(n_\nu)^2$ Funktionen $G \to \mathbb{C}$, die durch die Matrizenkoeffizienten gegeben sind: $x \to t_{ij}^{(\nu)}(x)$. Dieses Funktionensystem ist orthogonal bezüglich des oben eingeführten Skalarproduktes, denn nach Korollar 4.3 gilt

$$(t_{kl}^{(\mu)}, t_{ij}^{(\nu)}) = 0 \quad \text{für } (\mu, k, l) \neq (\nu, i, j) \ ,$$

$$(t_{kl}^{(\mu)}, t_{kl}^{(\mu)}) = \frac{1}{n_\nu} .$$

Für eine endliche Gruppe G bilden die komplexwertigen Funktionen $G \to \mathbb{C}$ einen $|G|$ dimensionalen Vektorraum. Es kann also darin höchstens $|G|$ paarweise zueinander orthogonale Funktionen geben. Es folgt der Satz

Satz 4.4 *Es seien G endlich und $n_1, n_2, \ldots, n_\nu \ldots$ die Dimensionen der irreduziblen Darstellungen von G. Dann gilt*

$$(*) \qquad n_1^2 + n_2^2 + \cdots + n_\nu^2 + \cdots \leq |G| .$$

Insbesondere gibt es höchstens $|G|$ nicht äquivalente irreduzible Darstellungen.

Wir werden später sehen (siehe Korollar 6.2), dass (*) nicht nur eine Ungleichung sondern sogar eine *Gleichung* ist. Man kann dies wie folgt ausdrücken: *Die Funktionen $t_{kl}^{(\nu)} : G \to \mathbb{C}$ bilden eine orthogonale Basis des Vektorraumes der komplexwertigen Funktionen $G \to \mathbb{C}$.*
Dieser Satz – wie auch die meisten Überlegungen dieses Abschnittes – lässt eine Verallgemeinerung auf kompakte topologische Gruppen und M-Darstellungen zu. Dies gilt insbesondere für die letzte Bemerkung (Satz von Peter-Weyl): Die Matrizenkoeffizienten der Liste der irreduziblen stetigen (unitären) Darstellungen einer kompakten topologischen Gruppe G bilden ein vollständiges Orthogonalsystem im Raum der quadratintegrierbaren Funktionen $G \to \mathbb{C}$.

V.5 Gruppencharaktere

Definition Es sei T eine Darstellung in G in A. Der zu T gehörige *Charakter* $\chi : G \to \mathbb{C}$ ist definiert durch $\chi(x) = \text{Spur } T_x$.

Aus der linearen Algebra weiss man, dass die Spur von T_x und damit $\chi(x)$ nicht von der in A gewählten Basis abhängt. Natürlich gilt $\chi(e) = n = \dim A$.
Es seien S und T zwei äquivalente Darstellungen. Dann existiert eine reguläre $n \times n$-Matrix X mit $T_x = X S_x X^{-1}$ für alle $x \in G$. Somit gilt Spur $T_x =$ Spur S_x. Dies beweist das folgende Resultat.

Satz 5.1 *Äquivalente Darstellungen haben denselben Charakter.*

Es sei χ der Charakter der Darstellung T in A. Dann folgt für $x,\ y \in G$ aus den Eigenschaften der Spurbildung: $\chi(yxy^{-1}) = \text{Spur } T_{yxy^{-1}} = \text{Spur } T_y T_x T_{y^{-1}} = \text{Spur } T_y T_x T_y^{-1} = \text{Spur } T_x$.

Satz 5.2 *Der Charakter einer Darstellung T ist eine Funktion auf den Konjugationsklassen von G; für alle $x, y \in G$ gilt* $\chi(x) = \chi(yxy^{-1})$.

Wie wir wissen, existiert zur Darstellung T in A ein Skalarprodukt, so dass T bezüglich diesem unitär ist. Wählen wir in A eine orthonormierte Basis, so folgt für $x \in G$

$$\chi(x^{-1}) = \text{Spur } T_{x^{-1}} = \text{Spur } (T_x^{-1}) = \text{Spur } (\overline{T_x}^T) = \text{Spur } \overline{T_x} = \overline{\chi(x)}\ .$$

Da aber die Spur von der gewählten Basis unabhängig ist, gilt ganz allgemein

Satz 5.3 *Für jede Darstellung T gilt* $\chi(x^{-1}) = \overline{\chi(x)}$ für alle $x \in G$.

Es seien S und T nicht äquivalente, irreduzible Darstellungen. Wir betrachten die Orthogonalitätsrelationen in orthonormierten Basen

$$(t_{kl}, s_{ij}) = \frac{1}{|G|} \sum_{x \in G} t_{kl}(x)\, \overline{s_{ij}(x)} = 0\ ,\quad 1 \le i, j \le m\ ,\quad 1 \le k, l \le n\ ,$$

$$(s_{kl}, s_{ij}) = \frac{1}{|G|} \sum_{x \in G} s_{kl}(x)\, \overline{s_{ij}(x)} = \frac{1}{m} \delta_{ki}\, \delta_{lj}\ ,\quad 1 \le i, j, k, l \le m\ .$$

Setzen wir $j = i$ und $l = k$, und summieren wir, so erhalten wir für den Charakter $\chi : G \to \mathbb{C}$ von T und den Charakter $\psi : G \to \mathbb{C}$ von S

$$(\chi, \psi) = \frac{1}{|G|} \sum_{x \in G} \chi(x)\, \overline{\psi(x)} = 0$$

$$(\psi, \psi) = \frac{1}{|G|} \sum_{x \in G} \psi(x)\, \overline{\psi(x)} = \frac{1}{m} \sum_k \sum_i \delta_{ki}\, \delta_{ki} = 1$$

Damit haben wir das folgende Resultat erhalten:

Satz 5.4 *Es seien S und T zwei irreduzible Darstellungen von G mit Charakter ψ und χ. Dann gilt*

$$(\chi, \psi) = \frac{1}{|G|} \sum_{x \in G} \chi(x)\, \overline{\psi(x)} = \begin{cases} 0\ , & \textit{falls } S \textit{ und } T \textit{ nicht äquivalent sind,} \\ 1\ , & \textit{falls } S \textit{ und } T \textit{ äquivalent sind.} \end{cases}$$

Korollar 5.5 *Die Charaktere der irreduziblen Darstellungen bilden im Raum der Klassenfunktionen $G \to \mathbb{C}$ ein orthonormiertes Funktionensystem bezüglich des Skalarproduktes*

$$(f, g) = \frac{1}{|G|} \sum_{x \in G} f(x)\, \overline{g(x)} \ .$$

Als nächstes stellen wir uns die Frage, inwieweit die Charaktere die Darstellungen charakterisieren. Gilt zum Beispiel die Umkehrung des Satzes 5.1?

Es seien S und T irreduzible Darstellungen mit Charakter ψ und χ. Es gelte $\chi(x) = \psi(x)$ für alle $x \in G$. Dann folgt

$$(\chi(x), \psi(x)) = \frac{1}{|G|} \sum_{x \in G} \chi(x)\, \overline{\psi(x)} = \frac{1}{|G|} \sum_{x \in G} |\chi(x)|^2 \ > \ 0 \ ,$$

da wegen $\chi(e) = n$ der Ausdruck $\sum_{x \in G} |\chi(x)|^2$ *echt* positiv ist. Nach Satz 5.4 können für irreduzible Darstellungen nur die Werte 0 oder 1 auftreten. Damit muss gelten

$$\frac{1}{|G|} \sum_{x \in G} \chi(x) \overline{\psi(x)} = 1 \ ,$$

und es folgt, dass S und T äquivalent sind.

Satz 5.6 *Die Charaktere von zwei irreduziblen Darstellungen sind genau dann gleich, wenn die Darstellungen äquivalent sind.*

Zusammen mit Korollar 5.5 ergibt sich daraus

Korollar 5.7 *Es gibt höchstens so viele nichtäquivalente irreduzible Darstellungen wie es Klassen konjugierter Elemente gibt.*

Ausreduzieren einer Darstellung

Es sei T eine Darstellung von G, und es sei $T^{(1)}, T^{(2)}, \ldots, T^{(l)}$ die Liste der (nicht äquivalenten) irreduziblen Darstellungen von G; ihre Charaktere seien $\chi_1, \chi_2, \ldots, \chi_l$.
Wir wissen, dass T vollreduzibel ist, sich also in eine direkte Summe von irreduziblen Darstellungen zerlegen lässt. Bezeichnen wir die Vielfachheit, mit der die Darstellung $T^{(i)}$ in dieser Zerlegung von T vorkommt, mit c_i, so können wir schreiben

$$T = c_1 T^{(1)} \oplus c_2 T^{(2)} \oplus \cdots \oplus c_l T^{(l)} \ .$$

Für den Charakter χ von T gilt somit

$$\chi(x) = \text{Spur } T_x = \sum \ c_j \text{ Spur } T_x^{(j)} = \sum c_j \, \chi_j(x) \ .$$

Das Ausreduzieren der Darstellung T besteht darin, die Vielfachheiten c_j zu bestimmen, wenn T und $T^{(j)}$ als bekannt vorausgesetzt werden. Dies ist wegen den Orthogonalitätsrelationen (Satz 5.4) sehr einfach! Es gilt

$$\begin{aligned}
(\chi, \chi_j) &= \frac{1}{|G|} \sum_{x \in G} \chi(x) \, \overline{\chi_j(x)} \\
&= \frac{1}{|G|} \sum_{x \in G} \left(\sum_i c_i \, \chi_i(x) \, \overline{\chi_j(x)} \right) \\
&= \sum_i c_i \, \frac{1}{|G|} \sum_{x \in G} \chi_i(x) \, \overline{\chi_j(x)} \\
&= c_j \ .
\end{aligned}$$

Wir stellen fest: Die Berechnung der Vielfachheiten c_j entspricht der Berechnung der Fourierkoeffizienten in einer Fourierreihe. Darauf werden wir später noch einmal zurückkommen.

Satz 5.7 *Es seien $T^{(1)}, T^{(2)}, \ldots, T^{(l)}$ die irreduziblen Darstellungen von G, $\chi_1, \chi_2, \ldots, \chi_l$ ihre Charaktere. Ist χ der Charakter der Darstellung T, so ist die Vielfachheit c_j von $T^{(j)}$ in T gegeben durch $c_j = (\chi, \chi_j)$.*

Satz 5.8 *Zwei beliebige Darstellungen S und T von G sind genau dann äquivalent, wenn ihre Charaktere übereinstimmen.*

Dieser Satz besagt, dass die Charaktere die Darstellungen bis auf Äquivalenz *charakter*isieren!

Beweis Falls S und T äquivalent sind, so sind (Satz 5.1) die Charaktere gleich. Sind die Charaktere gleich, so folgt aus Satz 5.6, dass die Vielfachheiten c_j gleich sind. Damit sind aber S und T äquivalent.

Satz 5.9 *Es sei $\chi_1, \chi_2, \ldots, \chi_l$ die Liste der Charaktere der (nicht äquivalenten) irreduziblen Darstellungen von G, und es gelte $\chi = \sum_j \ c_j \, \chi_j$. Dann folgt $(\chi, \chi) = \sum_i c_i^2$.*

Beweis

$$(\chi,\chi) = \Big(\sum c_i\,\chi_i, \sum c_j\chi_j\Big) = \sum_i\sum_j c_ic_j(\chi_i,\overline{\chi_j}) = \sum_i\sum_j c_ic_j\delta_{ij} = \sum_i c_i^2\ .$$

Dieses Resultat liefert das folgende sehr nützliche *Irreduzibilitätskriterium*. Offensichtlich ist eine Darstellung genau dann irreduzibel, wenn *ein* c_i gleich Eins und alle übrigen gleich Null sind. Folglich gilt

Satz 5.10 *Genau dann ist die Darstellung T von G mit Charakter χ irreduzibel, wenn gilt $(\chi,\chi) = 1$.*

Beispiel Wir betrachten die Gruppe $\mathbf{S}_3$. Die Elemente von $\mathbf{S}_3$ sind (in Zyklenschreibweise)

$$\{(e)\}\ \ \{(12)\ \ (13)\ \ (23)\}\ \ \{(123)\ \ (132)\}\ ,$$

wobei wir die drei Konjugationsklassen durch geschweifte Klammern angedeutet haben. Einige Darstellungen von $\mathbf{S}_3$ liegen auf der Hand:
$T^{(1)}$: *Einsdarstellung*; eindimensional

$$\chi_1(e) = 1,\ \ \chi_1(12) = 1,\ \ \chi_1(123) = 1\ .$$

$T^{(2)}$: *Parität*; eindimensional

$$\chi_2(e) = 1,\ \ \chi_2(12) = -1,\ \ \chi_2(123) = 1\ .$$

Als eindimensionale Darstellungen sind $T^{(1)}$ und $T^{(2)}$ irreduzibel.
$T^{(3)}$: Darstellung im zweidimensionalen (reellen) Raum als *Symmetriegruppe des regulären Dreiecks*:

$$T^{(3)}_e = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}\ ,\ \ T^{(3)}_{(12)} = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}\ ,\ \ T^{(3)}_{(123)} = \begin{bmatrix} -\frac{1}{2} & -\frac{\sqrt{3}}{2} \\ \frac{\sqrt{3}}{2} & -\frac{1}{2} \end{bmatrix}$$

$$\chi_3(e) = 2,\ \ \chi_3(12) = 0,\ \ \chi_3(123) = -1\ .$$

Mit Hilfe von Satz 5.10 können wir am Charakter ablesen, ob $T^{(3)}$ als komplexe Darstellung irreduzibel ist. Es gilt

$$(\chi_3,\chi_3) = \frac{1}{6}(4 + 3\cdot 0 + 2\cdot 1) = 1\ .$$

Die Darstellung $T^{(3)}$ ist somit irreduzibel.

Da es höchstens soviele nicht äquivalente irreduzible Darstellungen gibt, wie es Klassen konjugierter Elemente gibt, haben wir mit $T^{(1)}$, $T^{(2)}$, $T^{(3)}$ bereits alle irreduziblen Darstellungen von $\mathbf{S}_3$ gefunden.

T: *zweidimensionale Darstellung* gegeben durch

$$T_e = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \quad \begin{aligned} T_{(12)} &= \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \\ T_{(13)} &= \begin{bmatrix} -1 & 0 \\ -1 & 1 \end{bmatrix} \\ T_{(23)} &= \begin{bmatrix} 1 & -1 \\ 0 & -1 \end{bmatrix} \end{aligned}, \quad \begin{aligned} T_{(123)} &= \begin{bmatrix} 0 & -1 \\ 1 & -1 \end{bmatrix} \\ T_{(132)} &= \begin{bmatrix} -1 & 1 \\ -1 & 0 \end{bmatrix} \end{aligned} .$$

Der Charakter χ von T ist

$$\chi(e) = 2, \quad \chi(12) = 0, \quad \chi(123) = -1 .$$

Aus $\chi = \chi_3$ folgt, dass die Darstellungen $T^{(3)}$ und T äquivalent sind.

S: die *dreidimensionale Darstellung*, die man erhält, indem man die Basis eines dreidimensionalen Vektorraumes gemäss $\mathbf{S}_3$ permutiert. Die Darstellungsmatrizen sind Permutationsmatrizen, d.h. in jeder Zeile und in jeder Spalte findet sich genau eine Eins; an den übrigen Stellen stehen Nullen. Der Charakter ψ der Darstellung S ist:

$$\psi(e) = 3, \quad \psi(12) = 1, \quad \psi(123) = 0 .$$

Wegen

$$(\psi, \psi) = \frac{1}{6}(3 \cdot 3 + 3 \cdot 1 \cdot 1 + 2 \cdot 0 \cdot 0) = 2$$

ist S nicht irreduzibel. Zum Ausreduzieren berechnet man

$$\begin{aligned} (\psi, \chi_1) &= \frac{1}{6}(3 \cdot 1 + 3 \cdot 1 \cdot 1 + 2 \cdot 0 \cdot 1) = 1 , \\ (\psi, \chi_2) &= \frac{1}{6}(3 \cdot 1 + 3 \cdot 1 \cdot (-1) + 2 \cdot 0 \cdot 1) = 0 , \\ (\psi, \chi_3) &= \frac{1}{6}(3 \cdot 2 + 3 \cdot 1 \cdot 0 + 2 \cdot 0 \cdot (-1)) = 1 . \end{aligned}$$

Es folgt

$$S = T^{(1)} \oplus T^{(3)} .$$

V.6 Die reguläre Darstellung einer endlichen Gruppe

Es sei G eine endliche Gruppe. Der $\mathbb{C}[G]$-Modul $\mathbb{C}[G]$ bestimmt eine endlich dimensionale Darstellung von G; sie heisst die *reguläre Darstellung* von G.
Es seien $T^{(1)}, T^{(2)}, \ldots, T^{(l)}$ die endlich vielen, nicht äquivalenten irreduziblen Darstellungen von G, ihre Charaktere seien $\chi_1, \chi_2, \cdots, \chi_l$. Der Charakter χ der regulären Darstellung lässt sich leicht bestimmen; er ergibt sich zu

$$\chi(e) = |G| \ , \quad \chi(x) = 0 \ , \quad x \neq 0 \ .$$

Nach Satz 5.7 gilt dann für die Vielfachheit c_i von $T^{(i)}$ in der regulären Darstellung

$$c_i = (\chi, \chi_i) = \frac{1}{|G|} \sum_{x \in G} \chi(x)\, \overline{\chi_i(x)} = \frac{1}{|G|} |G|\, \overline{\chi_i(e)} = n_i$$

mit $n_i = \dim T^{(i)}$. Dies beweist den folgenden Satz:

Satz 6.1 *In der regulären Darstellung tritt jede irreduzible Darstellung $T^{(i)}$ genau so oft auf, wie ihre Dimension n_i angibt.*

Beispiel Jede Gruppe besitzt natürlich die 'triviale' irreduzible Darstellung $T^{(1)}_x = 1_{\mathbb{C}}$. Sie tritt in der regulären Darstellung genau einmal auf. Das entsprechende Basiselement lautet $\sum_{x \in G} x \in \mathbb{C}[G]$.

Zählt man die Dimensionen in der Zerlegung der regulären Darstellung, so erhält man

Korollar 6.2

$$|G| = \sum_{i=1}^{l} n_i^2 .$$

Die in Satz 4.4 erwähnte Ungleichung ist also sogar eine Gleichung. Dieses Resultat ist sehr nützlich bei der Suche nach allen irreduziblen Darstellungen: Man hat genau dann alle irreduziblen Darstellungen gefunden, wenn die Quadratsumme ihrer Dimensionen $|G|$ ist. – Am einfachsten ist natürlich der Fall abelscher Gruppen.

Korollar 6.3 *Es sei G abelsch. Dann gilt $l = |G|$.*

Die Charaktertafel

Die Charaktere sind Klassenfunktionen. Aus diesem Grunde genügt es, die Charakterwerte auf einem Repräsentantensystem $e = x_1, x_2, \cdots, x_k$ der Konjugationsklassen von G zu kennen. Die Werte der irreduziblen Charaktere $\chi_1, \chi_2, \ldots, \chi_l$ können dann in eine Matrix eingetragen werden:

$$\begin{array}{cccccc} & e & x_2 & x_3 & \cdots & x_k \\ \\ \chi_1 & 1 & 1 & 1 & \cdots & 1 \\ \chi_2 & n_2 & \chi_2(x_2) & \chi_2(x_3) & \cdots & \chi_2(x_k) \\ \chi_3 & n_3 & \chi_3(x_2) & \chi_3(x_3) & \cdots & \chi_3(x_k) \\ \vdots & \vdots & \vdots & \vdots & & \vdots \\ \chi_l & n_l & \chi_l(x_2) & \chi_l(x_3) & \cdots & \chi_l(x_k) \end{array}$$

Diese $l \times k$-Matrix beschreibt die Charaktere und damit die Darstellungen von G vollständig. Man nennt sie die *Charaktertafel* der Gruppe G.

Wie wir gesehen haben, bilden die Funktionen $\chi_i : G \to \mathbb{C}$, $i = 1, 2, \ldots, l$ im Raum der Klassenfunktionen ein orthonormiertes System bezüglich des Skalarproduktes $(\ ,\ )$. Es folgt somit $l \leq k$, da die Dimension dieses Raumes k ist. Es gilt sogar der Satz

Satz 6.4 *Die Charaktere $\chi_1, \chi_2, \ldots, \chi_l$ der irreduziblen Darstellungen bilden im Raum der Klassenfunktionen eine orthonormierte Basis. Insbesondere gilt $l = k$, d.h. es gibt genau so viele nicht äquivalente irreduzible Darstellungen, wie es Klassen konjugierter Elemente gibt.*

Die Beweise für diesen und den nächsten Satz verlangen eine etwas andere Technik als die früheren Sätze. Wir gehen dabei in Schritten vor. Es sei zuerst $f : G \to \mathbb{C}$ eine beliebige Funktion. Dann definieren wir $c(f) = \sum_{x \in G} f(x)\, x \in \mathbb{C}[G]$.

Lemma 6.5 *Genau dann gilt $y\, c(f)\, y^{-1} = c(f)$ für alle $y \in G$, wenn f eine Klassenfunktion ist.*

Beweis Die Gleichung

$$y\, c(f)\, y^{-1} = \sum_{x \in G} f(x) yxy^{-1} = \sum_{x \in G} f(y^{-1}xy)\, x = \sum_{x \in G} f(x)\, x = c(f)$$

gilt genau dann, wenn $f(x) = f(y^{-1}xy)$ für alle $y \in G$ und alle $x \in G$ erfüllt ist.

Es sei nun T eine Darstellung von G in A. Wir fassen A als $\mathbb{C}[G]$-Modul auf und benützen der Übersichtlichkeit wegen für die Zuordnung $a \mapsto (c(f))a$, $a \in A$ die Notation $T_{c(f)} = \sum_{x \in G} f(x)\, T_x$.

Lemma 6.6 *Es seien T eine irreduzible Darstellung von G der Dimension n mit Charakter χ und f eine Klassenfunktion. Dann gilt*

$$T_{c(f)} = \lambda 1_A \quad \textit{mit} \quad \lambda = \frac{|G|}{n}(\chi, \overline{f}).$$

Beweis Wegen $y\,c(f)\,y^{-1} = c(f)$ gilt $y\,c(f) = c(f)\,y$, d.h. $T_y T_{c(f)} = T_{c(f)} T_y$. Nach dem Lemma von Schur gilt dann $T_{c(f)} = \lambda 1_A$. Spurbildung liefert nun sofort

$$n\lambda = \text{Spur } T_{c(f)} = \sum_{x\in G} f(x) \text{ Spur } T_x = \sum_{x\in G} f(x)\,\chi(x) = |G|\,(\chi, \overline{f})\ .$$

Hieraus folgt $\lambda = \frac{|G|}{n}(\chi, \overline{f})$.

Beweis von Satz 6.4 Es sei f eine Klassenfunktion mit $(\chi_i, f) = 0$ für $i = 1, 2, \ldots, l$. Es ist zu zeigen, dass die Funktion f trivial ist. Wir betrachten die irreduziblen Darstellungen $T^{(i)}, i = 1, 2, \ldots, l$ und die zugehörigen Abbildungen $T^{(i)}_{c(\overline{f})} = \sum_{x\in G} \overline{f(x)}\, T^{(i)}$. Nach Lemma 6.6 sind diese alle trivial. Wegen der Vollreduzibilität folgt dann, dass für jede Darstellung T die Abbildung $T_{c(\overline{f})}$ trivial ist. Wir wenden dies auf die reguläre Darstellung an und berechnen $T_{c(\overline{f})}(e)$. Wir erhalten

$$0 = T_{c(\overline{f})}(e) = \sum_{x\in G} \overline{f(x)}\, T_x(e) = \sum_{x\in G} \overline{f(x)}\, x.$$

Hieraus folgt $\overline{f(x)} = 0$ für alle $x \in G$, also $f \equiv 0$.

Wir schliessen diesen Abschnitt mit dem folgenden überraschenden Satz.

Satz 6.7 *Es sei T eine irreduzible Darstellung von G der Dimension n. Dann ist n ein Teiler von $|G|$.*

Der Beweis von Satz 6.7 verlangt einige Kenntnisse der Zahlentheorie, die wir hier kurz (ohne Beweis) zusammenstellen.

Definition Die komplexe Zahl c heisst *ganz algebraisch*, wenn c Nullstelle eines ganzzahligen Polynoms $f(x) = a_0 + a_1 x + \cdots + a_{n-1}x^{n-1} + x^n$ ist, $a_i \in \mathbb{Z}$ für $i = 1, 2, \ldots, n-1$; der höchste Koeffizient ist 1.

Es gilt dann:

(1) Die Zahl $c \in \mathbb{Q}$ ist genau dann ganz algebraisch, wenn c ganzzahlig ist (Satz II.4.4, Satz von Gauss).

(2) Die Zahl $c \in \mathbb{C}$ ist genau dann ganz algebraisch, wenn es einen Unterring R von $\mathbb{C}$ gibt mit $c \in R$, der als abelsche Gruppe endlich erzeugt ist.

(3) Die ganz algebraischen Zahlen bilden einen Ring.

Lemma 6.8 *Es sei T eine Darstellung von G mit Charakter χ. Dann ist $\chi(x)$ ganz algebraisch.*

Beweis Es sei $x \in G$. Dann ist $x^{|G|} = e$, also $T_x^{|G|} = 1$. Die Eigenwerte ζ von T_x sind somit $|G|$-te Einheitswurzeln. Da jede Einheitswurzel ganz algebraisch ist, ist wegen (3) auch jede Summe von Einheitswurzeln ganz algebraisch. Als Summe der Eigenwerte von T_x ist $\chi(x)$ somit ganz algebraisch.
Es sei T eine irreduzible Darstellung und K eine Klasse konjugierter Elemente von G. Die Funktion $f_K : G \to \mathbb{C}$ sei definiert durch $f_K(x) = 1$ für $x \in K$ und $f(x) = 0$ sonst. Da f_K eine Klassenfunktion ist, gilt $T_{c(f_K)} = \sum_{x \in G} f_K(x)\, T_x = \lambda_K 1_A$ (siehe Lemma 6.6) und

$$\lambda_K = \frac{|G|}{n}\,(\chi, \overline{f_K}) = \frac{1}{n} \sum_{x \in K} \chi(x)\ .$$

Lemma 6.9 *Die Zahl $\dfrac{1}{n} \displaystyle\sum_{x \in K} \chi(x)$ ist ganz algebraisch.*

Wir zeigen zuerst, dass mit diesem Lemma der Satz 6.7 folgt.

Beweis von Satz 6.7 Es gilt

$$1 = (\chi, \chi) = \frac{1}{|G|} \sum_{x \in G} \chi(x)\, \overline{\chi(x)}\ ,$$

also

$$\frac{|G|}{n} = \sum_{x \in G} \overline{\chi(x)}\, \frac{\chi(x)}{n} = \sum_{K} \overline{\chi(x)} \sum_{x \in K} \frac{\chi(x)}{n}\ .$$

Daraus folgt mit Lemma 6.8 und 6.9, dass $|G|/n$ ganz algebraisch ist. Da $|G|/n$ auch rational ist, muss es ganz sein, d.h. n ist ein Teiler von $|G|$.

Zum *Beweis* von Lemma 6.9 betrachten wir zuerst die Untermenge R von $\mathbb{C}[G]$, welche aus allen $c(f)$ besteht, wo f eine ganzzahlige Klassenfunktion ist:

$$R = \{c(f) \in \mathbb{C}[G] \mid f : G \to \mathbb{Z} \text{ Klassenfunktion}\}.$$

Dann gilt:

– Jedes Element von R lässt sich darstellen als ganzzahlige Linearkombination von Elementen $c(f_K)$ mit $f_K : G \to \mathbb{Z}$, wo f definiert ist durch $f(x) = 1$ für $x \in K$ und $f(x) = 0$ sonst. Dabei durchläuft K die Konjugationsklassen von G.

– R ist unter der Addition abgeschlossen.

– R ist unter der Multiplikation abgeschlossen.

Nur die dritte dieser Aussagen ist nicht offensichtlich. Der Beweis ergibt sich wie folgt. Es ist zu zeigen, dass mit $c(f)$ und $c(g) \in R$ auch $c(f)\,c(g) \in R$ liegt. Es gilt $y\,c(f)\,c(g)\,y^{-1} = y\,c(f)\,y^{-1}\,y\,c(g)\,y^{-1} = c(f)\,c(g)$. Nach Lemma 6.5 ist die ganzzahlige Funktion, die zu $c(f)\,c(g)$ gehört, eine Klassenfunktion, d.h. $c(f)\,c(g)$ ist in R.

Damit ist gezeigt, dass R ein Ring ist, dessen additive Gruppe endlich erzeugt ist. Zu jedem $c(f)$ betrachten wir nun die Abbildung $T_{c(f)} : A \to A$. Nach obigem folgt $T_{c(f)} = \lambda(f)1_A$ mit $\lambda(f) \in \mathbb{C}$. Die Zuordnung $c(f) \mapsto \lambda(f)$ ist offensichtlich ein Ringhomomorphismus. Das Bild $\overline{R} = \{\lambda(f) \in \mathbb{C} \mid f : G \to \mathbb{Z} \text{ Klassenfunktion}\}$ ist folglich ein Unterring von $\mathbb{C}$, dessen additive Gruppe endlich erzeugt ist. Jedes Element von $\overline{R}$ ist damit nach der Charakterisierung (2) ganz algebraisch. Dies gilt insbesondere für $\frac{1}{n}\sum_{x\in K}\chi(x)$, denn dieses Element wird für die oben definierte Funktion $f_K : G \to \mathbb{Z}$ erhalten. Dies war zu beweisen.

V.7 Beispiele zur Darstellungstheorie endlicher Gruppen

a. Die zyklische Gruppe der Ordnung n

Es sei $G = C_n$, die zyklische Gruppe der Ordnung n. Da G abelsch ist, ist jede irreduzible Darstellung eindimensional (Satz 2.3), und es gibt n nicht äquivalente irreduzible Darstellungen (Korollar 6.3). Es sei nun t ein erzeugendes Element von G. Für jede eindimensionale Darstellung T von G, gilt dann $T_t = [\chi(t)] = [\lambda(t)]$ und $\lambda(t)$ ist eine n-te Einheitswurzel. Es sei nun ζ eine *primitive* n-te Einheitswurzel, dann lassen sich die nicht äquivalenten irreduziblen Charaktere von G wie folgt angeben.

$$\begin{array}{cccccc} & e & t & t^2 & \cdots & t^{n-1} \\ \\ \chi_1 & 1 & 1 & 1 & \cdots & 1 \\ \chi_2 & 1 & \zeta & \zeta^2 & \cdots & \zeta^{n-1} \\ \chi_3 & 1 & \zeta^2 & \zeta^4 & \cdots & \zeta^{2(n-1)} \\ \vdots & \vdots & \vdots & \vdots & & \vdots \\ \chi_n & 1 & \zeta^{n-1} & \zeta^{2(n-1)} & \cdots & \zeta^{(n-1)(n-1)} \end{array}$$

b. Die Kleinsche Vierergruppe

Es sei $G = \{e, a, b, c\}$ mit $a^2 = b^2 = c^2 = e$, $ab = c$. Da G abelsch ist, ist jede irreduzible Darstellung eindimensional. Ist T eine eindimensionale Darstellung, so gilt $T_x = [\chi(x)] = [\lambda(x)]$, und für $\lambda(x)$ kommen nur die Werte ± 1 in Frage. Die Charaktertafel von G lautet deshalb wie folgt:

$$\begin{array}{cccccc} & e & a & b & c \\ \\ \chi_1 & 1 & 1 & 1 & 1 \\ \chi_2 & 1 & -1 & 1 & -1 \\ \chi_3 & 1 & 1 & -1 & -1 \\ \chi_4 & 1 & -1 & -1 & 1 \end{array}$$

c. Die symmetrische Gruppe auf drei Objekten

Die irreduziblen Charaktere der Gruppe $G = \mathbf{S}_3$ wurden bereits früher berechnet (siehe Abschnitt V.5). Die Charaktertafel lautet wie folgt:

$$\begin{array}{cccc} & e & (12) & (123) \\ \\ \chi_1 & 1 & 1 & 1 \\ \chi_2 & 1 & -1 & 1 \\ \chi_3 & 2 & 0 & -1 \end{array}$$

d. Die symmetrische Gruppe $\mathbf{S}_4$

Es sei $G = \mathbf{S_4}$. Die Konjugationsklassen in $\mathbf{S_4}$ sind durch die Zyklentypen gegeben. Man erhält mit einfachen kombinatorischen Argumenten

	e	(12)	(123)	$(12)(34)$	(1234)
Anzahl Elemente	1	6	8	3	6

Nach Satz 6.4 besitzt G fünf nicht äquivalente irreduzible Darstellungen. Davon sind zwei eindimensional, nämlich die Einsdarstellung und die Darstellung, die durch die Parität gegeben ist. Da eine Gruppe G genau so viele nicht äquivalente *ein*dimensionale Darstellungen besitzt, wie die Gruppenordnung von $G/[G,G]$ angibt – der Beweis ist eine Übungsaufgabe – , haben wir alle eindimensionalen Darstellungen gefunden. Für die Dimensionen n_3, n_4, n_5 der übrigen irreduziblen Darstellungen ergeben sich aus den Korollaren 6.2 und Satz 6.7 die Einschränkungen

$$n_3^2 + n_4^2 + n_5^2 = 22 \quad \text{und} \quad n_i \mid 24,\ i = 3,4,5\ .$$

Daraus lesen wir ohne weiteres $n_3 = 2$, $n_4 = n_5 = 3$ als einzige Möglichkeit ab (bis auf Reihenfolge).

Als nächstes betrachten wir die Permutationsdarstellung von $\mathbf{S}_4$, die dadurch entsteht, dass die Basis eines vierdimensionalen Vektorraumes gemäss $\mathbf{S}_4$ permutiert wird. Der zugehörige Charakter χ ergibt sich sofort zu

$$\chi(e) = 4,\ \chi(12) = 2,\ \chi(123) = 1,\ \chi(12)(34) = 0,\ \chi(1234) = 0\ .$$

Es ist klar, dass diese Darstellung die Einsdarstellung enthält. Um die Vielfachheit zu bestimmen berechnen wir das Skalarprodukt (χ, χ_1). Wir erhalten

$$(\chi, \chi_1) = \frac{1}{24}(4 + 6 \cdot 2 + 8 \cdot 1 + 3 \cdot 0 + 6 \cdot 0) = \frac{1}{24} \cdot 24 = 1\ .$$

Betrachten wir nun den Charakter $\chi_5 = \chi - \chi_1$, also

$$\chi_5(e) = 3,\ \chi_5(12) = 1,\ \chi_5(123) = 0,\ \chi_5(12)(34) = -1,\ \chi_5(1234) = -1\ ,$$

so zeigt die Berechnung des Skalarproduktes (χ_5, χ_5), dass χ_5 irreduzibel ist:

$$(\chi_5, \chi_5) = \frac{1}{24}(3^2 + 6 \cdot 1^2 + 0 + 3 \cdot (-1)^2 + 6 \cdot (-1)^2) = 1\ .$$

Der Charakter χ_4 ergibt sich als Produkt $\chi_4 = \chi_2 \cdot \chi_5$. (Die eindimensionalen Charaktere operieren auf diese Weise *immer* auf der Menge der irreduziblen Charakter. Die zugehörige Operation auf den Darstellungen ist das Kroneckerprodukt bzw. das Tensorprodukt der Moduln (siehe die Abschnitte IV.9 und V.9.)

Der Charakter χ_3 der zweidimensionalen irreduziblen Darstellung lässt sich mit Hilfe der Orthogonalitätsrelationen 'abstrakt' bestimmen. Da es nur *eine* zweidimensionale irreduzible Darstellung gibt, folgt $\chi_2 \cdot \chi_3 = \chi_3$. Daraus ergibt sich $\chi_3(12) = \chi_3(1234) = 0$. Setzen wir schliesslich $\chi_3(123) = \xi$ und $\chi_3(12)(34) = \eta$, so liefert

$$0 = (\chi_5, \chi_3) = \frac{1}{24}(3 \cdot 2 + 8 \cdot 0 \cdot \xi + 3 \cdot (-1) \cdot \eta)$$

sofort $\chi_3(12)(34) = \eta = 2$, und

$$0 = (\chi_1, \chi_3) = \frac{1}{24}(1 \cdot 2 + 8 \cdot 1 \cdot \xi + 3 \cdot 1 \cdot 2)$$

liefert $\chi_3(123) = \xi = -1$. Damit ist die Charaktertafel von $\mathbf{S}_4$ vollständig bestimmt:

	e	(12)	(123)	$(12)(34)$	(1234)
χ_1	1	1	1	1	1
χ_2	1	-1	1	1	-1
χ_3	2	0	-1	2	0
χ_4	3	-1	0	-1	1
χ_5	3	1	0	-1	-1

An der Charaktertafel lassen sich viele Eigenschaften der Gruppe ablesen. Wir wollen dies mit dem folgenden Beispiel deutlich machen. Ist N ein Normalteiler von G, so lässt sich wegen $G \to G/N \to \mathrm{GL}(n, \mathbb{C})$ jede (irreduzible) Darstellung von G/N zu einer (irreduziblen) Darstellung von G 'hochheben'. In einer solchen Darstellung operieren die Elemente von N als Identität, so dass der entsprechende Charakterwert gleich der Dimension der Darstellung ist. (Man beachte dabei, dass ein Normalteiler immer eine Vereinigung von Konjugationsklassen ist.) Es sei nun umgekehrt der Wert $\chi(x)$ eines irreduziblen Charakters auf einem Element $x \in G$ gleich der Dimension n der Darstellung T. Da $\chi(x)$ die Summe der Eigenwerte der Transformation T_x ist und diese Eigenwerte alle Einheitswurzeln sind, kann die Summe nur dann gleich der Dimension n sein, wenn jeder dieser Eigenwerte Eins ist. Schränken wir nun die Darstellung T auf die zyklische (und deshalb abelsche) Untergruppe $\langle x \rangle$ ein, so zerfällt sie in eine Summe von eindimensionalen Darstellungen. Da die Eigenwerte natürlich dieselben bleiben, muss T_x die Einheitsmatrix sein. Dies bedeutet, dass x als Identität operiert, d.h. im Kern N der Abbildung $T : G \to \mathrm{GL}(n, \mathbb{C})$ liegt. Der Normalteiler N enthält (natürlich) mit x die ganze Konjugationsklasse, in der x liegt; in der Tat ist er die Vereinigung aller Konjugationsklassen K, für welche $\chi(K) = n = \chi(e)$ gilt.

Wir haben damit gesehen, *dass sich aus der Charaktertafel einer Gruppe die Existenz von (nichttrivialen) Normalteilern in der Gruppe ablesen lässt.*

Wir illustrieren dies im Falle der Charaktertafel von $\mathbf{S}_4$. (Für diese Gruppe sind die Normalteiler natürlich bereits bekannt.) Die Einsdarstellung χ_1 liefert (wie immer) den (trivialen) Normalteiler $G = \mathbf{S}_4$. Der Charakter χ_2 liefert den Normalteiler $\mathbf{A}_4$, der aus den geraden Permutationen besteht. Am Charakter χ_3 lesen wir ab, dass das Neutralelement und die drei Doppeltranspositionen einen Normalteiler bilden; dieser ist bekanntlich isomorph zur Kleinschen Vierergruppe V. Die Charaktere χ_4 und χ_5 schliesslich liefern den trivialen Normalteiler $\{e\}$.

Wir merken noch an, dass wegen $\mathbf{S}_4/V \cong \mathbf{S}_3$ die zu χ_3 gehörige zweidimensionale Darstellung von $\mathbf{S}_4$ nichts anderes ist als die 'Hochhebung' der zweidimensionalen Darstellung von $\mathbf{S}_3$.

e. Die alternierende Gruppe $\mathbf{A}_5$

Es sei $G = \mathbf{A}_5$. Die Konjugationsklassen von G lassen sich aus den einfach zu erhaltenden Konjugationsklassen von $\mathbf{S}_5$ bestimmen. Jede aus geraden Permutationen bestehende Konjugationsklasse von $\mathbf{S}_5$ spaltet in $\mathbf{A}_5$ in höchstens zwei Klassen auf. Wir erhalten ohne Schwierigkeiten das folgende Resultat:

	e	(123)	$(12)(34)$	(12345)	(13245)
Anzahl Elemente	1	20	15	12	12

Damit wissen wir, dass es fünf nicht äquivalente irreduzible Darstellungen von $\mathbf{A}_5$ gibt. Eine davon ist natürlich die Einsdarstellung. Wir bezeichen den Einscharakter mit χ_1. Um weitere irreduzible Darstellungen zu konstruieren kann man von Permutationsdarstellungen ausgehen. Wir betrachten zuerst die Darstellung, bei der $\mathbf{A}_5$ auf den fünf Basiselementen eines 5-dimensionalen Vektorraumes operiert. Der dazugehörige Charakter χ lässt sich leicht berechnen:

$$\chi(e) = 5,\ \chi(123) = 2,\ \chi(12)(34) = 1,\ \chi(12345) = 0,\ \chi(13245) = 0\ .$$

Es ist klar, dass χ den Einscharakter enthält. Um die Vielfachheit festzustellen berechnen wir das Skalarprodukt (χ, χ_1):

$$(\chi, \chi_1) = \frac{1}{60}(5 \cdot 1 + 20 \cdot 2 \cdot 1 + 15 \cdot 1 \cdot 1) = 1\ .$$

Wir setzen $\chi_4 = \chi - \chi_1$ und behaupten, dass χ_4 irreduzibel ist. In der Tat erhalten wir

$$(\chi_4, \chi_4) = \frac{1}{60}(4^2 + 20 \cdot 1^1 + 15 \cdot 0^2 + 12 \cdot (-1)^2 + 12 \cdot (-1)^2) = 1\ .$$

Nach dem Irreduzibilitätskriterium ist χ_4 irreduzibel.

Eine weitere Permutationsdarstellung erhalten wir, indem wir $\mathbf{A}_5$ auf der Menge der zyklischen Untergruppen der Ordnung 5 durch Konjugation operieren lässt.[11] Die (nichttrivialen) Elemente einer zyklischen Untergruppe der Ordnung 5 lassen sich durch einen Fünferzyklus darstellen. Im ganzen gibt es 24 solche Fünferzyklen, und da zwei zyklische Untergruppen der Ordnung 5 entweder übereinstimmen oder den Durchschnitt $\{e\}$ besitzen, gibt es genau 6 verschiedene zyklische Untergruppen der Ordnung 5. Die Gruppe $\mathbf{A}_5$ operiert auf dieser Menge durch Konjugation. Wir betrachten nun einen 6-dimensionalen Vektorraum, auf dessen Basis $\mathbf{A}_5$ in gleicher Weise operiert. Den Charakter der entsprechenden Darstellung bezeichnen wir mit ψ. Eine nicht allzuschwierige Rechnung liefert

$$\psi(e) = 6,\ \psi(123) = 0,\ \psi(12)(34) = 2,\ \psi(12345) = 1,\ \psi(13245) = 1\ .$$

Natürlich enthält ψ den Einscharakter:

$$(\psi, \chi_1) = \frac{1}{60}(6 \cdot 1 + 20 \cdot 0 \cdot 1 + 15 \cdot 2 \cdot 1 + 12 \cdot 1 \cdot 1 + 12 \cdot 1 \cdot 1) = 1\ .$$

Wir setzen $\chi_5 = \psi - \chi_1$ und stellen fest, dass χ_5 irreduzibel ist:

$$(\chi_5, \chi_5) = \frac{1}{60}(5^2 + 20 \cdot (-1)^2 + 15 \cdot 1^2 + 0 + 0) = 1\ .$$

Das Korollar 6.2 liefert für die Dimensionen n_2 und n_3 der weiteren irreduziblen Darstellungen die Restriktion $n_2^2 + n_3^2 = 60 - 1 - 4^2 - 5^2 = 18$. Daraus ergibt sich sofort $n_2 = n_3 = 3$. Setzen wir nun $\chi_2(123) = \alpha$, $\chi_2(12)(34) = \beta$, $\chi_2(12345) = \gamma$, $\chi(13245) = \delta$. Dann liefern die Orthogonalitätsbedingungen diese Werte ohne Schwierigkeiten. Wir haben

$$\begin{aligned}
0 = (\chi_1, \chi_2) &= \frac{1}{60}(1 \cdot 3 + 20 \cdot 1 \cdot \alpha + 15 \cdot 1 \cdot \beta + 12 \cdot 1 \cdot \gamma + 12 \cdot 1 \cdot \delta)\ , \\
0 = (\chi_4, \chi_2) &= \frac{1}{60}(4 \cdot 3 + 20 \cdot 1 \cdot \alpha + 15 \cdot 0 \cdot \beta + 12 \cdot (-1) \cdot \gamma + 12 \cdot (-1) \cdot \delta)\ , \\
0 = (\chi_5, \chi_2) &= \frac{1}{60}(5 \cdot 3 + 20 \cdot (-1) \cdot \alpha + 15 \cdot 1 \cdot \beta + 0 + 0)\ .
\end{aligned}$$

Dies liefert für $\alpha, \beta, \gamma, \delta$ die Gleichungen

$$\begin{aligned}
3 + 20\alpha + 15\beta + 12\gamma + 12\delta &= 0\ , \\
12 + 20\alpha - 12\gamma - 12\delta &= 0\ , \\
15 - 20\alpha + 15\beta &= 0\ .
\end{aligned}$$

[11] Man könnte - statt diesen etwas abstrakten Weg zu beschreiten - auch davon Gebrauch machen, dass $\mathbf{A}_5$ die Symmetriegruppe des regulären Pentagondodekaeders (oder des regulären Ikosaeders) ist. Dies würde eine dreidimensionale (reelle) Darstellung liefern. Hier beschreiten wir einen anderen Weg, weil dabei die Kraft der Orthogonalitätsrelationen sehr schön zur Geltung kommt.

Die Summation der ersten beiden eliminiert γ und δ, und es ergibt sich $\alpha = 0$ und $\beta = -1$. Ausserdem folgt

$$\gamma + \delta = 1.$$

Wir behaupten als nächstes, dass γ und δ reell sind. Um dies zu beweisen, betrachten wir das Element (12345) und sein Inverses (54321). Diese beiden Elemente sind in der Gruppe $\mathbf{A}_5$ zueinander konjugiert, so dass gemäss Satz 5.3 für jeden Charakter χ gilt

$$\chi(12345) = \chi(54321) = \overline{\chi(12345)} \ .$$

Dies beweist, dass γ reel ist. Ein analoger Schluss liefert, dass δ reell ist.
Aus der Irreduzibilität von χ_2 folgt die Gleichung

$$1 = (\chi_2, \chi_2) = \frac{1}{60}(3^2 + 20 \cdot \alpha^2 + 15 \cdot \beta^2 + 12 \cdot \gamma^2 + 12 \cdot \delta^2) \ .$$

Dies liefert

$$\gamma^2 + \delta^2 = \frac{6}{2} \ .$$

Einsetzen von $\delta = 1 - \gamma$ ergibt

$$\gamma^2 - \gamma - 1 = 0 \ .$$

Damit erhält man

$$\gamma = \frac{1 \pm \sqrt{1+4}}{2} = \frac{1 \pm \sqrt{5}}{2}$$

und

$$\delta = \frac{1 \mp \sqrt{5}}{2} \ .$$

Die Charaktertafel der Gruppe $\mathbf{A}_5$ lautet demnach wie folgt

	e	(123)	(12)(34)	(12345)	(13245)
χ_1	1	1	1	1	1
χ_2	3	0	-1	$\frac{1+\sqrt{5}}{2}$	$\frac{1-\sqrt{5}}{2}$
χ_3	3	0	-1	$\frac{1-\sqrt{5}}{2}$	$\frac{1+\sqrt{5}}{2}$
χ_4	4	1	0	-1	-1
χ_5	5	-1	1	0	0

Als Korollar erhalten wir, dass $\mathbf{A}_5$ keine nicht trivialen Normalteiler enthält, also einfach ist.

V.8 Zur Darstellungstheorie unendlicher Gruppen

Wir wollen in diesem Abschnitt die komplexe Darstellungstheorie von drei kompakten topologischen Gruppen behandeln, die in der Quantenmechanik (Pauli-Ausschliessungsprinzip) eine grosse Rolle spielen. Alle diese drei Gruppen sind sogar kompakte Liegruppen. Die Methode der Wahl zur Behandlung der Darstellungstheorie solcher Gruppen besteht zweifellos darin, von der Liestruktur, also insbesondere von der Liealgebra Gebrauch zu machen. Wir gehen hier einen anderen Weg, indem wir – wie weiter oben bereits angemerkt – die Mittelbildung auf diesen Gruppen heranziehen und dann analog zum Fall endlicher Gruppen vorgehen. Vieles aus der Darstellungstheorie dieser Gruppen lässt sich auf diese einfache und direkte Weise erhalten.

a. Die Gruppe SO(2)**.**

Wir betrachten zuerst die Gruppe der Drehungen des zweidimensionalen reellen Raumes, $\mathrm{SO}(2) = \{\phi \mid 0 \leq \phi < 2\pi\} = \mathbb{R}/(2\pi)$, wobei wir die Gruppenoperation als Addition schreiben. Als topologischer Raum ist SO(2) homöomorph zur Kreislinie und die Gruppenoperation ist stetig. Somit ist SO(2) eine kompakte topologische Gruppe. Eine Funktion $f : \mathrm{SO}(2) \to \mathbb{C}$ kann aufgefasst werden als eine 2π-periodische Funktion auf $\mathbb{R}$. Für stetige Funktionen $f : \mathrm{SO}(2) \to \mathbb{C}$ kann folglich eine Mittelbildung durch das Riemannsche Integral definiert werden (vergleiche dazu auch Abschnitt 3):

$$Mf = \frac{1}{2\pi} \int_0^{2\pi} f(\phi)\, d\phi \; .$$

Diese Mittelbildung ist offensichtlich (1) linear, (2) positiv definit, (3) normiert und (4) invariant. Aus unsern allgemeinen Sätzen über M-Darstellungen ergibt sich somit:

Satz 8.1 *Jede stetige Darstellung von* SO(2) *ist vollreduzibel.*

Da SO(2) abelsch ist, ist jede irreduzible M-Darstellung von SO(2) eindimensional. Eine irreduziblen Darstellung ist somit nichts anderes als ein Gruppenhomomorphismus von SO(2) in die multiplikative Gruppe der komplexen Zahlen. Wie üblich im Falle eindimensionaler Darstellungen identifizieren wir die Darstellung mit ihrem Charakter. Für jedes $\rho \in \mathbb{Z}$ ist die Funktion $\chi_\rho : \mathrm{SO}(2) \to \mathbb{C}$ definiert durch $\chi_\rho(\phi) = e^{i\rho\phi}$ ein derartige

Darstellung bzw. ein derartiger Charakter. Damit haben wir unendlich viele irreduzible M-Darstellungen von SO(2) konstruiert. Es gilt

Satz 8.2 (i) *Die Darstellungen χ_ρ, χ_σ sind genau dann äquivalent, wenn $\rho = \sigma$.*
(ii) *Es gibt keine weiteren irreduziblen Darstellungen.*

Beweis (i) Dies ist aus allgemeinen Sätzen an sich klar. Zur Illustration zeigen wir, worauf der charaktertheoretische Beweis hinausläuft. Es gilt

$$M\chi_\rho\overline{\chi}_\sigma = \frac{1}{2\pi}\int_0^{2\pi} e^{i\rho\phi}e^{-i\sigma\phi}\ d\phi = \frac{1}{2\pi}\int_0^{2\pi} e^{i(\rho-\sigma)\phi}\ d\phi = \delta_{\rho\phi}\ .$$

Die Aussage (i) ist also äquivalent zu den Orthogonalitätsrelationen trigonometrischer Polynome.
(ii) Es sei χ ein stetiger irreduzibler Charakter, der zu allen χ_ρ, $\rho \in \mathbb{Z}$ nicht äquivalent ist. Dann gilt

$$0 = (\chi, \chi_\rho) = \frac{1}{2\pi}\int_0^{2\pi} \chi(\phi)\cdot e^{-i\rho\phi}d\phi = a_\rho\ ,$$

wo a_ρ der ρ-te Fourierkoeffizient von χ ist. Wegen der Vollständigkeit der trigonometrischen Polynome gilt nun

$$\frac{1}{2\pi}\int_0^{2\pi} \chi(\phi)\overline{\chi(\phi)}\ d\phi = \sum_{\rho\in\mathbb{Z}} |a_\rho|^2 = 0\ .$$

Da $\chi(\phi)$ stetig ist, folgt $\chi = 0$. Damit ist (ii) bewiesen; die Aussage ist äquivalent zur Vollständigkeit der trigonometrischen Polynome.

Es folgt aus diesem Satz, dass jede endlich dimensionale M-Darstellung T von SO(2) direkte Summe $T = \sum_{\rho\in\mathbb{Z}} c_\rho\chi_\rho$ von Darstellungen χ_ρ mit gewissen Vielfachheiten c_ρ ist.

Beispiel Es sei T die Darstellung von SO(2) gegeben durch die reelle Drehung der Ebene, d.h.

$$\phi \mapsto T_\phi = \begin{bmatrix} \cos\phi & -\sin\phi \\ \sin\phi & \cos\phi \end{bmatrix}\ .$$

Für den Charakter $\chi : \mathrm{SO}(2) \to \mathbb{C}$ gilt $\chi(\phi) = 2\cos\phi$. Die Ausreduktion ergibt sich mit Hilfe des Skalarproduktes : Ist $T = \sum c_\rho\chi_\rho$, so ist $c_\rho = (\chi, \chi_\rho)$. Damit erhält man

$$c_\rho = (\chi, \chi_\rho) = \frac{1}{2\pi} \int_0^{2\pi} 2\cos\phi \; e^{-i\rho\phi} \; d\phi = \begin{cases} 0 & \text{für} \quad \rho \neq \pm 1 \; , \\ 1 & \text{für} \quad \rho = \pm 1 \; . \end{cases}$$

Damit ist $\chi = \chi_{-1} + \chi_{+1}$, d.h. T ist äquivalent zur Darstellung, die durch

$$\phi \mapsto \begin{bmatrix} e^{i\phi} & 0 \\ 0 & e^{-i\phi} \end{bmatrix}$$

gegeben ist.

b. Die Gruppe $\mathrm{SU}(2)$**, Gruppe der** 2×2**-unitären Matrizen** X **mit** $\det X = 1$**.**

Wir beschreiben $\mathrm{SU}(2)$ wie folgt:

$$\mathrm{SU}(2) = \left\{ X = \begin{bmatrix} \alpha & \beta \\ \overline{\beta} & \overline{\alpha} \end{bmatrix} \mid \alpha, \beta \in \mathbb{C}, \; \alpha\overline{\alpha} + \beta\overline{\beta} = 1 \right\} \; .$$

Setzen wir $\alpha = x_1 + ix_2$, $\beta = x_3 + ix_4$, $x_1, x_2, x_3, x_4 \in \mathbb{R}$, so erhalten wir

$$1 = \det X = \alpha\overline{\alpha} + \beta\overline{\beta} = \sum_{j=1}^{4} x_j^2 \; .$$

Die Elemente von $\mathrm{SU}(2)$ entsprechen somit eineindeutig den Punkten auf der Einheitssphäre $\mathbf{S}^3$ in $\mathbb{R}^4$. Man kann somit $\mathrm{SU}(2)$ als kompakten topologischen Raum betrachten, indem man die Topologie von $\mathbf{S}^3$ überträgt. Man kann zeigen (was wir hier nicht tun), dass in dieser Topologie die Gruppenoperation von $\mathrm{SU}(2)$ stetig ist. Damit ist $\mathrm{SU}(2)$ eine kompakte topologische Gruppe. Wir wissen dann aus allgemeinen Sätzen, dass auf $\mathrm{SU}(2)$ ein invariantes Mass existiert, das eindeutig bestimmt ist. Wir sind in diesem Beispiel in der Lage, die dazugehörige Mittelbildung explizit anzugeben.

Es sei $f : \mathrm{SU}(2) \to \mathbb{C}$ eine stetige Funktion. Mit der obigen Identifikation kann f als stetige Funktion $f : \mathbf{S}^3 \to \mathbb{C}$ angesehen werden. Dann ist die Mittelbildung gegeben durch das Riemannsche Integral

$$Mf = \frac{1}{\mathrm{vol}\; \mathbf{S}^3} \int_{\mathbf{S}^3} f \; .$$

Offensichtlich ist M linear, positiv und normiert. Dass M auch invariant ist, lässt sich ohne allzu grosse Schwierigkeiten ebenfalls zeigen (hier wollen wir dies allerdings nicht beweisen). Aus Satz 3.3 ergibt sich somit:

Satz 8.3 *Jede stetige Darstellung von* $\mathrm{SU}(2)$ *ist vollreduzibel.*

Da diese Gruppen in der Quantentheorie eine grosse Rolle spielt, wollen wir ihre Darstellungstheorie noch etwas näher untersuchen und insbesondere die irreduziblen Darstellungen beschreiben. Zu diesem Zweck ist es nützlich, die Mittelbildung bzw. das zugehörige Skalarprodukt für Klassenfunktionen explizit auszurechnen. Dies verlangt einige Vorarbeit.

Jede Matrix X der Form

$$X = \begin{bmatrix} \alpha & \beta \\ -\overline{\beta} & \overline{\alpha} \end{bmatrix}$$

ist in SU(2) zu einer Diagonalmatrix konjugiert; diese ist von der Form

$$X' = \begin{bmatrix} e^{i\phi} & 0 \\ 0 & e^{-i\phi} \end{bmatrix} \ , \ 0 \leq \phi \leq \pi \ ,$$

d.h. es gilt $\alpha' = \cos\phi + i\sin\phi,\ \beta' = 0$; $x'_1 = \cos\phi$, $x'_2 = \sin\phi$, $0 \leq \phi \leq \pi$ und $x_3 = x_4 = 0$. Damit wird jedem Element von SU(2) ein Element des "nicht negativen x_1, x_2-Äquators" von $\mathbf{S}^3$ zugeordnet.

Wir bestimmen nun diejenigen Elemente von SU(2), welche der Matrix X' zugeordnet sind. Bei dem Übergang zu einer konjugierten Matrix bleibt die Spur invariant. Damit muss gelten

$$\text{Spur}\, X = \alpha + \overline{\alpha} = 2x_1 = \alpha' + \overline{\alpha}' = 2\cos\phi = \text{Spur}\, X' \ .$$

Wie man weiss, ist die Bedingung auch hinreichend für die Konjugiertheit. Die Klasse der zu X' konjugierten Elemente bildet folglich auf $\mathbf{S}^3$ eine Sphäre $\mathbf{S}^2_\phi$ parallel zur x_2, x_3, x_4-Koordinatenebene mit Radius $\sin\phi$.

Es sei nun $f : \text{SU}(2) \to \mathbb{C}$ eine Klassenfunktion. Da f auf $\mathbf{S}^2_\phi$ konstant ist, erhält man für die Mittelbildung

$$\begin{aligned} Mf &= \frac{1}{\text{vol}\ \mathbf{S}^3} \int_{\mathbf{S}^3} f \\ &= \frac{1}{\text{vol}\ \mathbf{S}^3} \int_0^\pi (\text{vol}\ \mathbf{S}^2_\phi)\ f(\phi)\ d\phi \\ &= \frac{1}{\text{vol}\ \mathbf{S}^3} \int_0^\pi (\text{vol}\ \mathbf{S}^2) \sin^2\phi\ f(\phi)\ d\phi \ , \ \mathbf{S}^2 = \text{Einheitssphäre} \\ &= \frac{\text{vol}\ \mathbf{S}^2}{\text{vol}\ \mathbf{S}^3} \int_0^\pi \sin^2\phi\ f(\phi)\ d\phi \ . \end{aligned}$$

Die explizite Berechnung des Faktors vol $\mathbf{S}^2$/vol $\mathbf{S}^3$ liefert $2/\pi$; dieser Wert ergibt sich

aber auch direkt aus der Normierungsbedingung. Für Klassenfunktion $f : \mathrm{SU}(2) \to \mathbb{C}$ erhalten wir somit

$$Mf = \frac{2}{\pi} \int_0^\pi \sin^2 \ f(\phi) \ d\phi \ .$$

Nach diesen Vorbereitungen sind wir in der Lage, die irreduziblen Darstellungen zu bestimmen. Wir kennen natürlich bereits

$T^{(1)}$: Einsdarstellung, $\dim T^{(1)} = 1$,

$T^{(2)}$: die 'natürliche' Darstellung der Gruppe SU(2) im zweidimensionalen Vektorraum über $\mathbb{C}$, $\dim T^{(2)} = 2$.

Die weiteren irreduziblen Darstellungen von SU(2) erhält man, indem man SU(2) auf dem homogenen Polynomen in z_1, z_2 operieren lässt. Es sei

$$f(z_1, z_2) = a_{p,0} z_1^p + a_{p-1,1} z_1^{p-1} z_2 + \cdots + a_{0,p} z_2^p \ , \ a_{i,j} \in \mathbb{C} \ .$$

ein homogenes Polynom vom Grad p. Man betrachtet nun z_1, z_2 als Basis eines zweidimensionalen Vektorraumes und lässt $X \in \mathrm{SU}(2)$ operieren durch

$$X \cdot f(z_1, z_2) = f(Xz_1, Xz_2) \ .$$

Diese Operation definiert eine $p+1$-dimensionale Darstellung von SU(2) im Vektorraum der homogenen Polynome vom Grade p. Wir bezeichen diese Darstellung mit $T^{(p+1)}$. Wir behaupten und werden zeigen, dass alle die Darstellungen $T^{(p)}$, $p = 1, 2, \ldots$ irreduzibel sind.

Beispiel Wir setzen $p = 2$, $1 + p = 3$. Die Polynome $z_1^2, z_1 z_2, z_2^2$ bilden eine Basis des Raumes der homogenen Polynome vom Grad 2. Für

$$X = \begin{bmatrix} \alpha & \beta \\ \overline{\beta} & \overline{\alpha} \end{bmatrix}$$

erhalten wir:

$$\begin{array}{rll} z_1^2 & \text{geht über in} & (Xz_1)^2 = (\alpha z_1 - \overline{\beta} z_2)^2 = \alpha^2 z_1^2 - 2\alpha\overline{\beta} z_1 z_2 + \overline{\beta}^2 z_2^2 \ , \\ z_1 z_2 & \text{geht über in} & (Xz_1)(Xz_2) = (\alpha z_1 - \overline{\beta} z_2)(\beta z_1 + \overline{\alpha} z_2) = \ldots \ , \\ z_2^2 & \text{geht über in} & (Xz_2)^2 = (\beta z_1 + \overline{\alpha} z_2)^2 = \ldots \ . \end{array}$$

Es sei χ_p der Charakter von $T^{(p)}$. Da χ_p eine Klassenfunktion ist, genügt es, χ_p auf den Elementen des nicht negativen x_1, x_2-Äquators von $\mathbf{S}^3$ zu berechnen, d.h. auf den

Elementen der Form X'. Unter X' verhalten sich die homogenen Polynome vom Grad $p-1$ wie folgt:

$$\begin{aligned} z_1^{p-1} &\mapsto (X'z_1)^{p-1} = e^{i(p-1)\phi} z_1^{p-1} \ , \\ z_1^{p-2} z_2 &\mapsto (X'z_1)^{p-2}(X'z_2) = e^{(p-3)\phi} z_1^{p-2} z_2 \ , \\ &\cdots \\ z_2^{p-1} &\mapsto (X'z_2)^{p-1} = e^{-i(p-1)\phi} z_2^{p-1} \ . \end{aligned}$$

Die Darstellungsmatrix von $T^{(p)}_{X'}$ hat also die folgende Form

$$T^{(p)}_x = \begin{bmatrix} e^{i(p-1)\phi} & & & \\ & e^{i(p-3)\phi} & & \\ & & \ddots & \\ & & & e^{-i(p-1)\phi} \end{bmatrix} \ .$$

Damit ergibt sich

$$\chi_p(X') = \chi_p(\phi) = e^{i(p-1)\phi} + e^{i(p-3)\phi} + \cdots + e^{-i(p-1)\phi} \ .$$

Wegen

$$\chi_p(\phi) \cdot \sin\phi = \chi_p \cdot \frac{1}{2i}(e^{i\phi} - e^{-i\phi}) = \frac{1}{2i}(e^{ip\phi} - e^{-ip\phi}) = \sin(p\phi)$$

erhalten wir sofort

$$\chi_p(\phi) = \frac{\sin(p\phi)}{\sin\phi} \ .$$

Es gilt somit der folgende Satz.

Satz 8.4 (i) *Die Darstellungen* $T^{(p)}$, $p = 1, 2, \ldots$ *sind irreduzibel und paarweise nicht äquivalent.*
(ii) *Es gibt keine weiteren irreduziblen stetigen Darstellungen von* $\mathrm{SU}(2)$.

Beweis (i) Da die Dimension von $T^{(p)}$ gerade p ist, ist die paarweise Nichtäquivalenz klar. Um die Irreduzibilität zu beweisen, berechnen wir (χ_p, χ_p). Wir erhalten

$$(\chi_p, \chi_p) = M\chi_p\overline{\chi}_p = \frac{2}{\pi}\int_0^\pi \frac{\sin^2(p\phi)}{\sin^2\phi}\ \sin^2\phi\ d\phi = 1 \ .$$

Damit ist $T^{(p)}$ irreduzibel.

(ii) Es sei T eine endlich dimensionale stetige Darstellung von SU(2), die irreduzibel ist und nicht äquivalent zu einem $T^{(p)}$. Dann gilt für den Charakter χ von T

$$0 = (\chi, \chi_p) = M\chi\overline{\chi_p} = \frac{2}{\pi}\int_0^\pi \chi(\phi)\ \frac{\sin(p\phi)}{\sin\phi}\ \sin^2\phi\ d\phi\ .$$

Die Funktion $\chi : [0,\pi] \to \mathbb{C}$ hat also sämtliche sin-Fourierkoeffizienten Null. Da die Funktionen $\sin(p\phi)$, $p = 1, 2, \ldots$ auf $[0,\pi]$ ein vollständiges Funktionensystem bilden, und da χ stetig ist, folgt $\chi \cdot \sin\phi = 0$. Daraus ergibt sich unmittelbar $\chi \equiv 0$.

Bemerkung Die übliche Notation für $T^{(p)}$ in der theoretischen Physik (Pauli-Prinzip der Quantentheorie) ist

$$T^{(p)} = D_j,\ \ j = \frac{p-1}{2}, j = 0, \frac{1}{2}, 1, \frac{3}{2}, \ldots\ .$$

Der zugehörige Charakter ist dann

$$\psi_j(\phi) = \frac{\sin(2j+1)}{\sin\phi}\ .$$

c. Die Gruppe SO(3)**.**

Wir berechnen zuerst das Zentrum der Gruppe SU(2). Ist $Z \in \mathrm{SU}(2)$ ein Zentrumselement und T eine Darstellung von SU(2) so gilt für $X \in \mathrm{SU}(2)$

$$T_X \circ T_Z = T_{XZ} = T_{ZX} = T_Z \circ T_X\ .$$

Wir wählen nun $T = T^{(2)}$, die natürliche Darstellung von SU(2), für diese gilt $T_X = X$, $X \in \mathrm{SU}(2)$. Da $T^{(2)}$ irreduzibel ist, folgt mit dem Lemma von Schur, dass T_Z ein Vielfaches der Identität ist. Daraus ergibt sich $Z = I$ oder $Z = -I$. Das Zentrum von SU(2) besteht folglich nur aus den beiden Elementen

$$e = I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \text{ und } -I = \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}\ .$$

Es gilt nun der folgende Satz, den wir ohne Beweis zitieren.

Satz 8.5 *Die Gruppe* SO(3) *ist isomorph zu* SU(2)/Zentrum*. Als topologischer Raum ist* SU(2) *eine* 2*-blättrige Überlagerung von* SO(3)*, insbesondere ist die Projektion* π : SU(2) $\to$ SO(3) *stetig.*

Jede (irreduzible) Darstellung T von SO(3) lässt sich deshalb via π als (irreduzible) Darstellung $T \circ \pi$ von SU(2) ansehen. Die Darstellungen von SU(2), die so erhalten werden, sind genau diejenigen, bei denen $-I \in \mathrm{SU}(2)$ als Identität operiert. Für die irreduziblen Darstellungen $T^{(p)}$, $p = 1, 2, \ldots$ ist das genau dann der Fall, wenn p ungerade ist. Daraus folgt, dass die irreduziblen Darstellungen von $T^{(1)}, T^{(3)}, \ldots$, d.h. $D_0, D_1, \ldots$ von SU(2) genau auch die irreduziblen Darstellungen von SO(3) sind.

V.9 Das Kroneckerprodukt von Darstellungen

Es seien V, W zwei Vektorräume über $\mathbb{C}$. Man betrachte $V \otimes_{\mathbb{C}} W$. Sind $f : V \to V'$ und $g : W \to W'$ zwei $\mathbb{C}$-lineare Abbildungen, so gibt es eine $\mathbb{C}$-lineare Abbildung $f \otimes g : V \otimes_{\mathbb{C}} W \to V' \otimes_{\mathbb{C}} W'$ definiert durch $(f \otimes g)(v \otimes w) = fv \otimes gw$, $w, v \in V, w \in W$.

Es sei G eine Gruppe und S eine Darstellung in A und T eine Darstellung in B. Dann definieren wir eine Darstellung R in $A \otimes_{\mathbb{C}} B$ durch

$$R_x = T_x \otimes S_x : A \otimes_{\mathbb{C}} B \to A \otimes_{\mathbb{C}} B \ .$$

Die Darstellung R heisst das *Kroneckerprodukt* der Darstellungen S und T. Die Darstellungsbedingungen sind trivialerweise erfüllt. Die Dimesion von R ist das Produkt der Dimension T und S. Der zugehörige $\mathbb{C}[G]$-Modul ist $A \otimes_{\mathbb{C}} B$, wo die G-Operation durch $x(a \otimes b) = xa \otimes xb$ definiert ist, $x \in G,\ a \in A,\ b \in B$.

Wir berechnen den Charakter von R aus den Charakteren von S und T. Dazu wählen wir mit $\alpha_1, \alpha_2, \ldots, \alpha_m$ eine Basis von A und mit $\beta_1, \beta_2, \ldots, \beta_n$ eine Basis von B. Dann ist $\alpha_k \otimes \beta_l, k = 1, 2, \ldots, m, l = 1, 2, \ldots, n$ eine Basis von $A \otimes_{\mathbb{C}} B$. Ist S_x gegeben durch $[s_{ik}(x)]$ und T_x durch $[t_{jl}(x)]$, so ergibt sich

$$(S_x \otimes T_x)(\alpha_k \otimes \beta_l) = S_x(\alpha_k) \otimes T_x(\beta_l) = \sum_i s_{ik}(x)\alpha_i \otimes \sum_j t_{jl}(x)\beta_j = \sum_{i,j} s_{ik}(x)t_{jl}(x)(\alpha_i \otimes \beta_j) \ .$$

Dabei ist $s_{ik}(x)t_{jl}(x)$ eine $(m \times n) \cdot (m \times n)$ Matrix, (i, j) ist der Spaltenindex, (k, l) ist der Zeilenindex. Durch diese Matrix ist R_x gegeben. Der Charakter χ_R von R berechnet sich nun sehr leicht aus den Charakteren χ_S und χ_T. Es gilt

$$\chi_R(x) = \sum_{k,j} s_{kk}(x) \cdot t_{jj}(x) = \chi_S(x) \cdot \chi_T(x) \ .$$

Beispiel (1) Im Beispiel $G = \mathbf{S}_4$ ist $T^{(5)} = T^{(2)} \otimes T^{(4)}$; der Charakter von $T^{(5)}$ ist gegeben durch $\chi_5 = \chi_2 \cdot \chi_4$.

(2) Es sei $G = \mathrm{SU}(2)$ und es sei $T^{(p)}$ die $(p-1)$-dimensionale irreduzible Darstellung von G in der Schreibweise von Abschnitt 8. Wir betrachten $T^{(p)} \otimes T^{(q)}$. Im folgenden sei $p \leq q$. Der Charakter χ von $T^{(p)} \otimes T^{(q)}$ ist gegeben durch

$$\chi(\phi) = \chi_p(\phi) \cdot \chi_q(\phi) = \frac{\sin(p\phi) \cdot \sin(q\phi)}{\sin^2 \phi} \ .$$

Die Ausreduktion

$$T^{(p)} \otimes T^{(q)} = \sum c_k T^{(k)}$$

liefert für den Koeffizienten c_k

$$c_k = M\chi\overline{\chi_k} = \frac{2}{\pi} \int_0^\pi \frac{\sin(p\phi)\sin(q\phi)}{\sin^2 \phi} \ \sin(k\phi) \ \sin^2 \phi \ d\phi \ .$$

Der Koeffizient c_k ist also nichts anderes als der Fourierkoeffizient zu $\sin(k\phi)$ der Funktion

$$\frac{\sin(p\phi) \cdot \sin(q\phi)}{\sin \phi} = \sin(p+q-1)\phi + \sin(p+q-3)\phi + \cdots + \sin(q-p+1)\phi \ .$$

Folglich gilt

$$c_k = \begin{cases} 1 & \text{für} \quad k = p+q-1, p+q-3, \ldots, q-p+1 \ , \\ 0 & \text{sonst} \ . \end{cases}$$

Damit ist die Darstellung $T^{(p)} \otimes T^{(q)}$ ausreduziert:

$$T^{(p)} \otimes T^{(q)} = T^{(p+q-1)} \oplus T^{(p+q-3)} \oplus \cdots \oplus T^{(q-p+1)} \ ,$$

oder in der Schreibweise der theoretischen Physik

$$D_j \otimes D_l = D_{j+l} \oplus D_{j+l-1} \oplus \cdots \oplus D_{l-j} \ , \quad j = \frac{p-1}{2}, \quad l = \frac{q-1}{2} \ .$$

Dies ist die sogenannte 'Clebsch-Gordan Reihe', die bei der Pauli-Auswahlregel der Quantentheorie eine grosse Rolle spielt.

Die Darstellungen eines **direkten Produktes von Gruppen** lassen sich mit einer Konstruktion behandeln, die dem Kroneckerprodukt eng verwandt ist.

Es sei $G \times H$ das direkte Produkt der Gruppen G und H. Es sei S eine Darstellung G in A und T eine Darstellung von H in B. Dann ist eine Darstellung $R = S \otimes T$ von $G \times H$ in $A \otimes_{\mathbb{C}} B$ gegeben durch

$$R_{(x,y)}(a \otimes b) = S_x a \otimes T_y b \ .$$

Es gilt, ähnlich wie oben, $\chi_R(x,y) = \chi_S(x) \cdot \chi_T(y)$.

Satz 9.1 *Es sei S eine irreduzible Darstellung von G und T eine irreduzible Darstellung von H. Dann ist R eine irreduzible Darstellung von $G \times H$.*

Beweis Wir wenden das Irreduzibilitätskriterium an und berechnen (χ_R, χ_R). Wir erhalten

$$\begin{aligned}
(\chi_R, \chi_R) &= \frac{1}{|G| \cdot |H|} \sum_{(x,y) \in H \times G} \chi_R(x,y) \cdot \overline{\chi_R(x,y)} \\
&= \frac{1}{|G| \cdot |H|} \sum \chi_S(x)\, \overline{\chi_S(x)} \cdot \chi_T(y)\, \overline{\chi_T(y)} \\
&= \frac{1}{|G|} \sum_{x \in G} \chi_S(x) \cdot \overline{\chi_S(x)} \cdot \frac{1}{|H|} \sum_{y \in H} \chi_T(y) \cdot \overline{\chi_T(y)} \\
&= 1 \cdot 1 \\
&= 1 \ .
\end{aligned}$$

Satz 9.2 *Jede irreduzible Darstellung von $G \times H$ ist äquivalent zu einer Darstellung $S \otimes T$, wo S eine irreduzible Darstellung von G und T eine irreduzible Darstellung von H ist.*

Beweis Es sei R eine Darstellung von $G \times H$, deren Charakter χ_R orthogonal ist zu allen $\chi_S \cdot \chi_T$, wo S alle irreduziblen Darstellungen von G und T alle irreduziblen Darstellungen von H durchläuft. Dann hat man

$$0 = (\chi_R, \chi_S \cdot \chi_T) = \frac{1}{|H| \cdot |G|} \sum \chi_R(x,y) \cdot \overline{\chi_S(x)}\ \overline{\chi_T(y)} \ .$$

Setze $\rho(y) = \frac{1}{|G|} \sum\limits_{x \in G} \chi_R(x,y) \cdot \overline{\chi_S(x)}$. Offensichtlich ist ρ eine Klassenfunktion auf H, die auf allen χ_T orthogonal steht. Daraus folgt $\rho \equiv 0$. Für festes $y \in H$ gilt somit

$$0 = \rho(y) = \frac{1}{|G|} \sum_{x \in G} \chi_R(x,y)\, \overline{\chi_S(x)}$$

für alle irreduziblen Darstellungen S von G. Damit ist die Funktion $\chi_R(-, y)$ eine zu allen χ_S orthogonal stehende Funktion. Folglich gilt $\chi_R \equiv 0$.

Kapitel VI. Abriss der Galoistheorie

Einleitung

Es geht in diesem Kapitel um einen kurzen und kompakten Überblick über die Galoistheorie, der das Wesentliche dieser wichtigen Theorie hervortreten lässt.

Die Galoistheorie verbindet die Körpertheorie und die Gruppentheorie; kurz ausgedrückt gründet sie auf der Idee, dass die Gruppe der Automorphismen einer Körpererweiterung in der Lage ist, Information über die Körperstruktur zu liefern. In ihren Grundzügen wurde die Theorie von E. Galois (1811-1832) geschaffen, wobei er allerdings seine Gedanken nur skizzenhaft dargestellt hat. Auch Anwendungen dieser Theorie gehen auf Galois zurück, etwa die Behandlung der Frage, unter welchen Bedingungen die Lösungen einer polynomialen Gleichung durch Radikale darstellbar sind (siehe Abschnitt VI.10). Nach den Resultaten aus Abschnitt III.3 dürfte es keine Überraschung bedeuten, dass die Galoistheorie in der Lage ist, abschliessend zu entscheiden, welche geometrischen Konstruktionsprobleme mit Zirkel und Lineal durchführbar sind und welche nicht (siehe Abschnitt VI.9). Im Laufe der Entwicklung der Mathematik hat die Galoistheorie ferner viele tiefliegende Anwendungen in der algebraischen Zahlentheorie gefunden, auf die hier nicht eingegangen werden kann. Hingegen enthält der Abschnitt VI.11 ein Beispiel, in dem die Galoistheorie herangezogen wird, um ein wichtiges Resultat aus der Darstellungstheorie endlicher Gruppen zu beweisen.

VI.1 Endliche Körpererweiterungen, Zerfällungskörper

Es seien K, L, $K \subseteq L$ zwei Körper. Dann ist der Erweiterungskörper L von K ein Vektorraum über K. Dessen Dimension über K heisst *Körpergrad* von L über K, $[L : K] = \dim_K L$. Die Körpererweiterung heisst *endlich*, wenn der Körpergrad endlich ist. Für $K \subseteq K' \subseteq K''$ gilt $[K'' : K'][K' : K]=[K'' : K]$. Ein Element $\alpha \in L$ heisst *algebraisch* über K, falls $f(x) \in K[x]$ existiert mit $f(\alpha) = 0$; sonst heisst α *transzendent*. Ist L endlich über K, so ist jedes Element $\alpha \in L$ algebraisch über K. Der Körper L heisst dann eine *endliche algebraische* Körpererweiterung von K.

Es sei $\alpha \in L$ algebraisch über K. Dann existiert ein eindeutig bestimmtes normiertes Polynom $h(x) \in K[x]$ mit $h(\alpha) = 0$ und $h(x)$ von minimalem Grad. Wir nennen $h(x)$ das *Minimalpolynom* von $\alpha \in L$. Der Grad von $h(x)$, $\deg h(x)$, heisst *Grad* von α über K. Das Minimalpolynom $h(x)$ ist irreduzibel über K.

Es sei $K \subseteq L$ und $\alpha \in L$ algebraisch über K mit Minimalpolynom $h(x) \in K[x]$. Dann induziert die Zuordnung $x \mapsto \alpha$ einen Isomorphismus $f : K[x]/(h(x)) \xrightarrow{\sim} K(\alpha)$. Insbesondere gilt $[K(\alpha) : K] = \deg h(x) = \deg \alpha$. Dabei bezeichnet $K(\alpha)$ den kleinsten Unterkörper von L, der K und α umfasst. Es sei K gegeben und $h(x)$ ein irreduzibles Polynom in $K[x]$. Dann ist $K[x]/(h(x))$ ein Körper, der K und eine Nullstelle des Polynoms $h(x)$, nämlich $x+(h(x))$ enthält. Diese Konstruktion heisst *Adjunktion einer symbolischen Nullstelle*.

Es sei K ein Körper und $f(x) \in K[x]$ ein Polynom vom Grad n, $n \geq 1$. Da $f(x)$ in irreduzible Faktoren zerfällt, können wir eine Nullstelle α von $f(x)$ adjungieren. Wir erhalten einen Körper K', über dem $f(x)$ in $(x - \alpha)g(x)$ zerfällt. Dabei gilt $[K' : K] \leq n$, $\deg\ g(x) = n - 1$. Eine Wiederholung dieses Verfahrens liefert einen Körper $L \supseteq K$, über dem $f(x)$ in Linearfaktoren zerfällt; es gilt offensichtlich $[L : K] \leq n!$.

Definition Es sei L ein Erweiterungskörper von K, über dem $f(x)$ in Linearfaktoren zerfällt, $f(x) = a_n(x - \alpha_1) \cdots (x - \alpha_n)$. Der Körper $K(\alpha_1, ..., \alpha_n) \subseteq L$ heisst ein *Zerfällungskörper* von $f(x)$ über K.

Definition Es seien $K \subseteq L, K \subseteq L'$ Körpererweiterungen. Ein Körperhomomorphismus $\phi : L \to L'$ mit $\phi|_K = 1$ heisst ein *Körperhomomorphismus* über K.

Es gilt (siehe Kapitel Körper, Abschnitt 2) der folgende Satz:

Satz 1.1 *Es sei $f(x) \in K[x]$. Der Zerfällungskörper von $f(x)$ ist bis auf Isomorphie über K eindeutig bestimmt.*

Dieses Resultat ergab sich aus dem folgenden detaillierteren Resultat, das weiter unten benötigt wird:

Satz 1.2 *Es sei $f(x) \in K[x]$, und L ein Zerfällungskörper von $f(x)$ über K. Ferner sei $\iota : K \xrightarrow{\sim} K'$ ein Körperisomorphismus und L', $L' \supseteq K'$ ein Körper über dem $\iota f(x)$ in Linearfaktoren zerfällt. Dann gibt es einen (injektiven) Körperhomomorphismus $\phi : L \to L'$ mit $\phi|_K = \iota$.*

Beispiel Es sei $K = \mathbb{Q}$, $f(x) = x^5 - 1$. Dann ist $\mathbb{Q}(e^{2k\pi i/5})$ für $k = 1, 2, 3, 4$ ein Zerfällungskörper von $f(x)$ über $\mathbb{Q}$. Man beachte, dass es neben der Identität des Zerfällungskörpers noch weitere Isomorphismen ϕ_k, $k = 2, 3, 4$ über $\mathbb{Q}$ gibt: ϕ_k führt $e^{2\pi i/5}$ in $e^{2k\pi i/5}$ über.

Beispiel Es sei $K = \mathbb{Q}$, $f(x) = x^3 - 2$. Der Körper $\mathbb{Q}(\sqrt[3]{2})$ ist reell und kann deshalb nicht Zerfällungskörper von $f(x)$ über $\mathbb{Q}$ sein.

Beispiel Es sei $K = \mathbb{Q}$, $f(x) = x^2 - 2x - 2$, $g(x) = x^2 - 3$. Über $\mathbb{C}$ zerfällt $f(x)$ in $(x - (1 + \sqrt{3}))(x - (1 - \sqrt{3}))$ und $g(x)$ in $(x - \sqrt{3})(x + \sqrt{3})$. Der Körper $\mathbb{Q}(\sqrt{3})$ ist somit ein Zerfällungskörper sowohl von $f(x)$ wie auch von $g(x)$.

VI.2 Normale Körpererweiterungen

Definition Eine Körpererweiterung $K \subseteq L$ heisst *normal*, falls jedes irreduzible Polynom $f(x) \in K[x]$, welches in L *eine* Nullstelle besitzt, über L vollständig in Linearfaktoren zerfällt.

Beispiel Die Körpererweiterung $\mathbb{R} \subseteq \mathbb{C}$ ist normal.

Beispiel Die Körpererweiterung $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt[3]{2})$ ist nicht normal. Denn das Minimalpolynom $x^3 - 2$ von $\sqrt[3]{2}$ über $\mathbb{Q}$ zerfällt über $\mathbb{Q}(\sqrt[3]{2})$ nicht in Linearfaktoren.

Satz 2.1 *Eine Körpererweiterung $K \subseteq L$ ist genau dann endlich und normal, wenn ein Polynom $f(x) \in K[x]$ existiert, so dass L Zerfällungskörper von $f(x)$ über K ist.*

Beweis Die Körpererweiterung $K \subseteq L$ sei endlich und normal. Dann ist sie auch algebraisch; d.h. es gibt $\alpha_1, \alpha_2, ..., \alpha_s \in L$ mit $L = K(\alpha_1, ..., \alpha_s)$ und $\alpha_i, i = 1, 2, ..., s$ algebraisch über K. Es sei $m_i(x) \in K[x]$ das Minimalpolynom von α_i. Setze $f(x) = m_1(x)m_2(x)\cdots m_s(x)$. Da $m_i(x)$ in L eine Nullstelle, nämlich α_i, besitzt, zerfällt $m_i(x)$,

und damit $f(x)$, über L vollständig in Linearfaktoren. Andererseits ist L erzeugt durch $\alpha_1, \alpha_2, ..., \alpha_s$, so dass L Zerfällungskörper von $f(x)$ über K ist.

Es sei L umgekehrt Zerfällungskörper des Polynoms $f(x) \in K[x]$. Dann ist sicher $[L : K]$ endlich. Es bleibt zu zeigen, dass $K \subseteq L$ normal ist. Es sei also $g(x) \in K[x]$ ein irreduzibles Polynom; es besitze die Nullstelle $\alpha \in L$. Wir betrachten den Zerfällungskörper M, $M \supseteq L \supseteq K$ des Polynoms $f(x) \cdot g(x) \in K[x]$. Es seien ϑ_1, ϑ_2 Nullstellen von $g(x)$ in M. Wir behaupten

$$[L(\vartheta_1) : L] = [L(\vartheta_2) : L]$$

und zeigen zuerst, dass daraus folgt, dass die Erweiterung $K \subseteq L$ normal ist. Ist $\alpha = \vartheta_1$, so ist $[L(\vartheta_1) : L] = 1$. Dann folgt $L(\vartheta_2) = L$ und damit $\vartheta_2 \in L$. Mit α liegt somit jede Nullstelle von $f(x)$ in L.

Um die Behauptung zu beweisen, betrachten wir die folgenden Körpererweiterungen

$$\begin{array}{ccccc} M & = & M & = & M \\ \cup\!| & & \cup\!| & & \cup\!| \\ L(\vartheta_1) & \supseteq & L & \subseteq & L(\vartheta_2) \\ \cup\!| & & \cup\!| & & \cup\!| \\ K(\vartheta_1) & \supseteq & K & \subseteq & K(\vartheta_2) \end{array}$$

Für $j = 1, 2$ gilt dann

$$[L(\vartheta_j) : L][L : K] = [L(\vartheta_j) : K] = [L(\vartheta_j) : K(\vartheta_j)] \cdot [K(\vartheta_j) : K].$$

Da $g(x)$ über K irreduzibel ist, gilt $[K(\vartheta_1) : K] = \deg g(x) = [K(\vartheta_2) : K]$. Es existiert ein Isomorphismus $\iota : K(\vartheta_1) \xrightarrow{\sim} K(\vartheta_2)$ über K. Nun ist $L(\vartheta_i)$ für $i = 1, 2$ Zerfällungskörper von $f(x)$ über $K(\vartheta_i)$, denn in M ist $L(\vartheta_i)$ erzeugt von $K(\vartheta_i)$ und den Nullstellen $\alpha_1, ..., \alpha_n$ von $f(x)$. Nach Satz 1.2 lässt sich ι zu einem Isomorphismus $\phi : L(\vartheta_1) \xrightarrow{\sim} L(\vartheta_2)$ mit $\phi|_{K(\vartheta_1)} = \iota$ erweitern. Somit gilt $[L(\vartheta_1) : K(\vartheta_1)] = [L(\vartheta_2) : K(\vartheta_2)]$, und es folgt $[L(\vartheta_1) : L] = [L(\vartheta_2) : L]$. Damit ist Satz 2.1 bewiesen.

VI.3 Die Charakteristik eines Körpers, separable Polynome, separable Körpererweiterungen

Für den Körper K betrachten wir die Abbildung $\phi : \mathbb{Z} \to K$ definiert durch $\phi(n) = n \cdot 1, n \in \mathbb{Z}$. Dann gibt es eine natürliche Zahl q mit $\operatorname{im} \phi \cong \mathbb{Z}/(q)$. Da K keine Nullteiler enthält, ist q entweder eine Primzahl oder Null.

Definition Die Zahl q heisst die *Charakteristik* von K, $\operatorname{char} K = q$. Ist $q = p$, p eine Primzahl, so enthält K den Körper $\mathbb{F}_p$, $\mathbb{F}_p = \mathbb{Z}/(p)$. Im Falle $q = 0$ enthält K den Ring $\mathbb{Z}$ und damit auch den Körper $\mathbb{Q}$. Der so erhaltene Unterkörper ist offensichtlich der kleinste Unterkörper von K; er heisst *Primkörper* von K.

Beispiel Die Charakteristik von $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ ist 0, die Körper $\mathbb{F}_p$ und $\mathbb{F}_p(x)$ haben Charakteristik p.

Wir erinnern daran, dass in Charakteristik $p \neq 0$ die Gleichung

$$(a \pm b)^p = a^p \pm b^p,$$

gilt (siehe Abschnitt III.4).

Definition Ein irreduzibles Polynom $f(x) \in K[x]$ heisst *separabel* über K, wenn es im Zerfällungskörper L keine mehrfache Nullstellen besitzt, d.h. wenn in der Zerlegung $f(x) = a_n(x-\alpha_1)\cdots(x-\alpha_n)$ die α_i's paarweise verschieden sind. Andernfalls heisst $f(x)$ *inseparabel* über K. Von einem *beliebigen* Polynom sagen wir, es sei *separabel*, wenn jeder seiner irreduziblen Faktoren separabel ist.

Beispiel Das Polynom $x^4 + x^3 + x^2 + x + 1 \in \mathbb{Q}[x]$ hat die Nullstellen

$$\alpha_1 = e^{2\pi i/5}, ..., \alpha_4 = e^{8\pi i/5}.$$

Es ist irreduzibel, wie man mit Hilfe des Eisensteinschen Kriteriums (siehe Satz III.4.5) beweisen kann, und separabel.

Beispiel Es sei $K = \mathbb{F}_p$, und L der Quotientenkörper von $K[u]$. Dann ist das Polynom $x^p - u \in L[x]$ irreduzibel und inseparabel. Den Beweis dieser Behauptung überlassen wir dem Leser als Übungsaufgabe.

Wir erinnern daran, dass ein Polynom $f(x) \in K[x]$ genau dann mehrfache Nullstellen besitzt, wenn $f(x)$ und $Df(x)$ einen nichttrivialen gemeinsamen Faktor besitzen (siehe Satz III.4.2).

Satz 3.1 *Es sei* $\operatorname{char} K = 0$. *Dann ist jedes irreduzible Polynom* $f(x) \in K[x]$ *separabel.*

Beweis Es sei $f(x) = a_0 + a_1x + \cdots + a_nx^n \in K[x]$ mit $a_n \neq 0$. Dann ist $Df(x) = a_1 + 2a_2x + \cdots + na_nx^{n-1}$. Wegen $\operatorname{char} K = 0$ gilt $na_n \neq 0$. Damit ist $Df(x) \neq 0$ und $\deg Df(x) < \deg f(x)$. Da $f(x)$ irreduzibel ist, kann kein nichttrivialer gemeinsamer Faktor von $f(x)$ und $Df(x)$ existieren.

Satz 3.2 *Es sei* char $K = p \neq 0$. *Ein irreduzibles Polynom* $f(x) \in K[x]$ *ist genau dann separabel, wenn es kein Polynom* $g(x) \in K[x]$ *gibt mit* $f(x) = g(x^p)$.

Beweis Es sei $f(x) = g(x^p)$. Dann gilt $Df(x) = Dg(x^p) \cdot p \cdot x^{p-1} \equiv 0$. Damit existiert ein nichttrivialer gemeinsamer Faktor von $f(x)$ und $Df(x)$, nämlich $f(x)$, und es folgt, dass $f(x)$ nicht separabel ist. Es sei umgekehrt $f(x)$ *nicht* von der Form $g(x^p)$. Ist $f(x) = a_0 + a_1 x + \cdots + a_n x^n$, so existiert folglich ein Index j mit $a_j \neq 0$ und $p \nmid j$. Die Ableitung liefert

$$Df(x) = \cdots + j \cdot a_j \cdot x^{j-1} + \cdots .$$

Aus $j \cdot a_j \neq 0$ folgt $Df(x) \neq 0$. Da $f(x)$ irreduzibel ist, gibt es somit keinen nichttrivialen gemeinsamen Faktor von $f(x)$ und $Df(x)$, und es folgt, dass $f(x)$ separabel ist.

Satz 3.3 *In* $\mathbb{F}_p[x]$ *ist jedes irreduzible Polynom* $f(x)$ *separabel.*

Beweis Wir führen den Beweis indirekt. Wir setzen $K = \mathbb{F}_p$ und nehmen an, dass $f(x) \in K[x]$ irreduzibel und nicht separabel sei. Dann folgt nach Satz 3.2 $f(x) = g(x^p) = b_0 + b_1 x^p + b_2 x^{2p} + \cdots + b_n x^{np}$. In $\mathbb{F}_p$ gilt nun $a = a^p$ und $(a+b)^p = a^p + b^p$, woraus sich sofort $f(x) = (b_0 + b_1 x + \cdots + b_n x^n)^p \in K[x]$ ergibt. Dann ist aber $f(x)$ nicht irreduzibel. Dies ist ein Widerspruch.

Es sei $K \subseteq L$ eine Körpererweiterung. Ist $\alpha \in L$ algebraisch, so heisst α *separabel* über K, wenn das Minimalpolynom von α über K separabel ist. Die algebraische Körpererweiterung $K \subseteq L$ heisst *separabel*, wenn jedes Element von L über K separabel ist.

Satz 3.4 *Es sei* $K \subseteq L$ *eine separable Körpererweiterung, und es sei* M *ein Zwischenkörper,* $K \subseteq M \subseteq L$. *Dann sind auch die Körpererweiterungen* $K \subseteq M$ *und* $M \subseteq L$ *separabel.*

Beweis Es ist klar, dass $K \subseteq M$ separabel ist. Sei $\alpha \in L$ mit Minimalpolynom $m(x) \in K[x]$ und $\overline{m}(x) \in M(x)$. Dann ist $m(x) = \overline{m}(x) \cdot h(x),\ h(x) \in M[x]$. Da $m(x)$ separabel ist, ist es auch $\overline{m}(x)$.

Offen bleibt an dieser Stelle die folgende Frage. Es sei $f(x) \in K[x]$ ein irreduzibles und separables Polynom, und α sei eine Nullstelle von $f(x)$ in einem Erweiterungskörper von K. Ist die Körpererweiterung $K \subseteq K(\alpha)$ separabel? Wir werden später (siehe Korollar 7.2) beweisen können, dass dies in der Tat der Fall ist.

VI.4 Einheitswurzeln und endliche Körper

Definition Es sei K ein Körper. Die Nullstellen von $f(x) = x^n - 1 \in K[x]$ heissen n-te *Einheitswurzeln.*

Satz 4.1 *Die n-ten Einheitswurzeln bilden eine multiplikative Gruppe.*

Beweis Es sei $f(x) = x^n - 1$. Mit α, β sind offensichtlich auch $\alpha \cdot \beta$ und α^{-1} Nullstellen von $f(x)$.

Satz 4.2 *Es sei* char $K = 0$ *oder* char $K = p$ *mit* $p \nmid n$. *Dann gibt es genau n paarweise verschiedene Einheitswurzeln.*

Beweis Unter der Voraussetzung des Satzes gilt $Df(x) = n \cdot x^{n-1} \neq 0$. Damit besitzt $Df(x)$ nur die Nullstelle 0. Aber 0 ist *keine* Nullstelle von $f(x)$. Es folgt, dass für $f(x)$ und $Df(x)$ kein nichtrivialer gemeinsamer Faktor existiert, dass also $f(x)$ nur einfache Nullstellen besitzt.

Satz 4.3 *Es sei K ein Körper mit* char $K = 0$ *oder* char $K = p$ *und* $p \nmid n$. *Dann ist die Gruppe der n-ten Einheitswurzeln zyklisch.*

Beweis Die Gruppe der n-ten Einheitswurzeln enthält nach Satz 4.2 n Elemente. Wäre sie nicht zyklisch, so würde $k < n$ existieren mit $\zeta^k = 1$ für alle n-ten Einheitswurzeln ζ. Damit wären alle n-ten Einheitswurzeln Nullstellen des Polynoms $x^k - 1$. Dieses besitzt aber höchstens k verschiedene Nullstellen. Dies ist ein Widerspruch.

Definition Eine n-te Einheitswurzel heisst *primitiv*, wenn sie ein erzeugendes Element der Gruppe der n-ten Einheitswurzeln ist.

Beispiel Es sei $f(x) = x^4 - 1 \in \mathbb{Q}[x]$. Die Nullstellen sind $1, i, -1, -i$. Dies sind die 4-ten Einheitswurzeln über $\mathbb{Q}$; darunter sind i und $-i$ primitiv.

Gilt char $K = 0$ oder char $K = p$ mit $p \nmid n$, so gibt es genau $\phi(n)$ primitive n-te Einheitswurzeln über K, wo ϕ die Eulersche Funktion bezeichnet ($\phi(n)$ = Anzahl der zu n teilerfremden Zahlen modulo n).

Beispiel Es sei q eine Primzahl. Dann gilt $\phi(q) = q - 1$, so dass es $q - 1$ primitive q-te Einheitswurzeln gibt. Wegen $x^q - 1 = (x - 1)(x^{q-1} + \cdots + x + 1)$ sind diese gerade die Nullstellen von $x^{q-1} + \cdots + x + 1$. Im Fall $K = \mathbb{Q}$ können wir noch mehr sagen. Über $\mathbb{Q}$ ist nämlich, wie wir wissen, das Polynom $x^{q-1} + \cdots + x + 1$ irreduzibel. Wir haben damit das Resultat, dass über $\mathbb{Q}$ jede primitive q-te Einheitswurzel, q prim, den Grad $q - 1$ hat.

Beispiel Es sei p eine Primzahl und $q = p^n$. Der Körper $\mathbb{F}_q$ besteht (siehe Abschnitt III.4) genau aus den Nullstellen des Polynoms $x^q - x \in \mathbb{F}_p$. Die Nichtnullelemente von $\mathbb{F}_q$ sind folglich gerade die $(q - 1)$-ten Einheitswurzeln über $\mathbb{F}_p$. Als Gruppe von Einheitswurzeln ist die multiplikative Gruppe des Körpers $\mathbb{F}_q$ zyklisch.

VI.5 Die Galoisgruppe

Definition Es sei $K \subseteq L$ eine endliche Körpererweiterung. Ein Isomorphismus $\sigma : L \to L$ über K heisst ein *Automorphismus* von L über K. Die Automorphismen von L über K bilden unter der Zusammensetzung eine Gruppe; man nennt diese die *Galoisgruppe* $\mathrm{Gal}(L/K)$ von L über K.

Man beachte, dass jeder Automorphismus von L über K insbesondere ein Isomorphismus von K-Vektorräumen ist.

Beispiel In der Körpererweiterung $\mathbb{R} \subseteq \mathbb{C}$ besitzt $\mathbb{C}$ die $\mathbb{R}$-Basis {1,i}. Es sei $\sigma : \mathbb{C} \to \mathbb{C}$ ein Automorphismus von $\mathbb{C}$ über $\mathbb{R}$. Dann muss gelten

$$(\sigma(i))^2 = \sigma(i^2) = \sigma(-1) = -1.$$

Daraus folgt $\sigma(i) = \pm i$ Es gibt folglich genau zwei Automorphismen von $\mathbb{C}$ über $\mathbb{R}$, nämlich die Identität und die Konjugation $\sigma : x + iy \mapsto x - iy$. Die Galoisgruppe $\mathrm{Gal}(\mathbb{C}/\mathbb{R})$ ist isomorph zu C_2.

Satz 5.1 *Es sei $K \subseteq L$ eine Körpererweiterung mit $G = \mathrm{Gal}(L/K)$. Es sei U eine Untergruppe von G. Dann ist*

$$F(U) = \{a \in L \,|\, \sigma(a) = a \text{ für alle } \sigma \in U\} \subseteq L$$

ein Unterkörper von L mit $K \subseteq F(U) \subseteq L$. Ausserdem gilt $U \subseteq \mathrm{Gal}(L/F(U))$.

Definition $F(U)$ heisst der zur Untergruppe U gehörige *Fixkörper*.

Beweis Mit $a, b \in F(U)$ ist auch $a \pm b \in F(U)$, $a^{-1} \in F(U)$ und $ab \in F(U)$. Ausserdem gilt offensichtlich $K \subseteq F(U)$. Da jeder Automorphismus von L über $F(U)$ auch ein Automorphismus über K ist, ist U eine Untergruppe von $\mathrm{Gal}(L/F(U))$.

Satz 5.2 *Es sei $K \subseteq L$ eine Körpererweiterung mit $G = \mathrm{Gal}(L/K)$. Es sei M ein Zwischenkörper, $K \subseteq M \subseteq L$. Dann ist*

$$S(M) = \{\sigma \in G \,|\, \sigma(b) = b \text{ für alle } b \in M\} \subseteq \mathrm{Gal}(L/K)$$

eine Untergruppe von G. Ausserdem gilt $S(M) = \mathrm{Gal}(L/M)$.

Beweis Mit $\sigma, \tau \in S(M)$ ist auch $\sigma \cdot \tau \in S(M)$ und $\sigma^{-1} \in S(M)$. Damit ist $S(M)$ eine Untergruppe von $\mathrm{Gal}(L/K)$. Da jeder Automorphismus von L über M auch ein Automorphismus von L über K ist, folgt $S(M) = \mathrm{Gal}(L/M)$.

Beispiel Wir betrachten die Körpererweiterung $\mathbb{Q} \subseteq \mathbb{Q}(c)$ mit $c = \sqrt[3]{2}$. Für $\sigma \in \mathrm{Gal}(\mathbb{Q}(c)/\mathbb{Q})$ gilt

$$(\sigma(c))^3 = \sigma(c^3) = \sigma(2) = 2.$$

Wegen $\mathbb{Q} \subseteq \mathbb{Q}(c) \subseteq \mathbb{R}$ muss $\sigma(c)$ reell sein. Daraus folgt $\sigma(c) = \sqrt[3]{2}$. Die Galoisgruppe $\mathrm{Gal}(\mathbb{Q}(c)/\mathbb{Q})$ ist also trivial. Insbesondere gilt $S(\mathbb{Q}) = S(\mathbb{Q}(c)) = \{e\}$.

Wir werden im folgenden Voraussetzungen kennen lernen, unter denen $F(-)$ und $S(-)$ eine eineindeutige Beziehung zwischen den Zwischenkörpern der Erweiterung einerseits und den Untergruppen der Galoisgruppe andererseits schaffen; diese Beziehung heisst *Galoiskorrespondenz*. Zuerst wollen wir hier aber die Galoisgruppe einer Körpererweiterung etwas genauer studieren.

Es sei $K \subseteq L$ eine endliche Körpererweiterung, und es sei $f(x) \in K[x]$ vom Grad n das Minimalpolynom von $\alpha \in L$. Für $\sigma \in \mathrm{Gal}(L/K)$ gilt dann

$$0 = \sigma 0 = \sigma(f(\alpha)) = \sigma(a_0 + a_1\alpha + a_2\alpha^2 + \cdots + a_n\alpha^n) =$$

$$= a_0 + a_1\sigma(\alpha) + a_2(\sigma(\alpha))^2 + \cdots + a_n(\sigma(\alpha))^n.$$

Es folgt, dass $\sigma(\alpha)$ ebenfalls eine Nullstelle von $f(x)$ ist. Die Nullstellen des Minimalpolynoms $f(x)$ von α heissen die in L zu α *konjugierten Elemente*. In dieser Terminologie lässt sich unser Resultat wie folgt aussprechen.

Satz 5.3 *Es sei $\sigma \in \mathrm{Gal}(L/K)$, $\alpha \in L$. Dann ist $\sigma(\alpha) \in L$ zu α konjugiert.*

Es sei $L \supseteq K$ der Zerfällungskörper eines Polynoms $g(x) \in K[x]$, d.h. es gelte $L = K(\alpha_1, ..., \alpha_n)$, wo $\alpha_1, ..., \alpha_n$ die Nullstellen des Polynoms $g(x)$ sind. Jedem $\sigma \in \mathrm{Gal}(L/K)$ wird nach Satz 5.3 eine Permutation $\Pi(\sigma)$ von $\alpha_1, ..., \alpha_n$ zugeordnet. Die so definierte Abbildung Π von $\mathrm{Gal}(L/K)$ in die Permutationsgruppe der Nullstellen von $g(x)$ ist natürlich homomorph. Ausserdem ist sie injektiv, denn, weil L durch K und $\alpha_1, ..., \alpha_n$ erzeugt wird, ist σ durch $\Pi(\sigma)$ eindeutig bestimmt. Es folgt, dass $\mathrm{Gal}(L/K)$ unter Π zu einer Untergruppe der Permutationsgruppe der Elemente $\alpha_1, ..., \alpha_n$ isomorph ist.

Satz 5.4 *Es sei L der Zerfällungskörper von $g(x) \in K[x]$. Dann ist* $\mathrm{Gal}(L/K)$ *isomorph zu einer Untergruppe der Permutationsgruppe der Nullstellen von $g(x)$.*

Definition Unter der *Galoisgruppe eines Polynoms $g(x) \in K[x]$* versteht man die Galoisgruppe des Zerfällungskörpers von $g(x)$ über K.

Korollar 5.5 *Es sei $g(x)$ vom Grad n. Dann ist die Ordnung der Galoisgruppe von $g(x)$ höchstens $n!$.*

Im Rest dieses Abschnittes werden wir dieses Resultat schrittweise verschärfen.

Satz 5.6 *Es sei $K \subseteq L$ eine endliche Körpererweiterung. Dann gilt*

$$|\mathrm{Gal}(L/K)| \leq [L : K].$$

Dies ergibt sich unmittelbar aus der etwas allgemeineren und präziseren Aussage des folgenden Satzes.

Satz 5.7 *Es sei $K \subseteq L$ eine endliche Körpererweiterung und $\iota : K \to L'$ ein Körperhomomorphismus. Dann gibt es höchstens $[L : K]$ verschiedene Körperhomomorphismen $\phi : L \to L'$ mit $\phi|_K = \iota$.*

Beweis Wir führen den Beweis zuerst für $L = K(\alpha)$. Es sei $g(x) \in K[x]$ das Minimalpolynom von α, deg $(g(x)) = r$. Das Polynom $\iota g(x)$ habe in L' die Nullstellen $\alpha'_1, ..., \alpha'_s$, $s \leq r$. Zu jedem j, $1 \leq j \leq s$ gibt es einen Homomorphismus $\phi_j : K(\alpha) \to L'$ mit $\phi_j|_K = \iota$ und $\phi(\alpha) = \alpha'_j$. Andererseits führt ein Homomorphismus $\phi : K(\alpha) \to L'$ mit $\phi|_K = \iota$ notwendigerweise α in eine Nullstelle α'_j von $\iota g(x)$ über, d.h. ϕ stimmt mit einem ϕ_j überein. Es gibt also gerade s verschiedene Körperhomomorphismen $\phi : K(\alpha) \to L'$ mit $\phi|_K = \iota$. Wegen $s \leq r = [L : K]$ ist damit in diesem Fall die Aussage des Satzes bewiesen.

$$\begin{array}{ccc} L & \stackrel{\phi}{\to} & L' \\ \cup| & & \| \\ K(\alpha) & \stackrel{\phi_j}{\to} & L' \\ \cup| & & \| \\ K & \stackrel{\iota}{\to} & L' \end{array}$$

Im allgemeinen Fall verwenden wir Induktion nach $[L : K]$. Ist $[L : K] = 1$, so ist nichts zu beweisen. Es sei $[L : K] > 1$. Wir wählen ein Element $\alpha \in L$ mit deg $\alpha = r > 1$. Für einen Körperhomomorphismus $\phi : L \to L'$ mit $\phi|_K = \iota$ betrachten wir dann die Restriktion $\phi|_{K(\alpha)} : K(\alpha) \to L'$. Nach obigem gilt $\phi|_{K(\alpha)} = \phi_j$ für ein gewisses j mit $1 \leq j \leq s$, d.h. ϕ ist eine Erweiterung von ϕ_j. Nach Induktion, angewandt auf die Körpererweiterung $K(\alpha) \subseteq L$ gibt es davon höchstens $[L : K(\alpha)]$ verschiedene. Wegen

$$s \cdot [L : K(\alpha)] \leq [K(\alpha) : K][L : K(\alpha)] = [L : K]$$

folgt daraus die Aussage des Satzes.

Im Falle, wo $K \subseteq L$ eine endliche, normale und separable Körpererweiterung ist, können wir das Resultat von Satz 5.6 noch weiter verschärfen.

Theorem 5.8 *Es sei L der Zerfällungskörper eines separablen Polynoms $f(x) \in K[x]$. Dann gilt*

$$|\mathrm{Gal}(L/K)| = [L : K].$$

Ähnlich wie bei Satz 5.6 beweisen wir eine etwas allgemeinere und präzisere Aussage, aus der Theorem 5.8 direkt folgt.

Satz 5.9 *Es sei L der Zerfällungskörper des separablen Polynoms $f(x) \in K[x]$. Es sei ferner $\iota : K \to L'$ ein Körperhomomorphismus, so dass $\iota f(x)$ über L' in Linearfaktoren zerfällt. Dann gibt es genau $[L : K]$ Körperhomomorphismen $\phi : L \to L'$ mit $\phi|_K = \iota$.*

Beweis Wir führen den Beweis mit Induktion nach $[L : K]$. Für $[L : K] = 1$ ist nichts zu beweisen. Es sei $[L : K] > 1$. Wir wählen einen irreduziblen Faktor $g(x)$ von $f(x)$ mit deg $(g(x)) = r > 1$. Da $f(x)$ separabel ist, sind es auch $g(x)$ und $\iota g(x)$. Es sei α eine Nullstelle von $g(x)$. Für jede Nullstelle $\alpha'_j,\ j = 1, 2, ..., r$ von $\iota g(x)$ existiert ein Körperhomomorphismus $\phi_j : K(\alpha) \to L'$ mit $\phi_j|_K = \iota$ und $\phi_j(\alpha) = \alpha'_j$. Mit Induktion, angewandt auf die Körpererweiterung $K(\alpha) \subseteq L$ folgt, dass sich jedes ϕ_j auf genau $[L : K(\alpha)]$ Arten zu einem Körperhomomorphismus $\phi : L \to L'$ mit $\phi|_{K(\alpha)} = \phi_j$ erweitern lässt. Wegen

$$r \cdot [L : K(\alpha)] = [K(\alpha) : K][L : K(\alpha)] = [L : K]$$

ist damit die Existenz von $[L : K]$ verschiedenen Körperhomomorphismen $\phi : L \to L'$ mit $\phi|_K = \iota$ nachgewiesen. Nach Satz 5.7 gibt es aber höchstens so viele. Damit ist Satz 5.9 vollständig bewiesen.

VI.6 Einige Beispiele von Galoisgruppen

(a) Die reine Gleichung.

Es sei char $K = 0$ oder char $K = p$ und $p \nmid n$. Für das Folgende nehmen wir an, dass die n-ten Einheitswurzeln in K enthalten seien, d.h. wir nehmen an, dass das Polynom $f(x) = x^n - 1$ über K in Linearfaktoren zerfalle. Wir betrachten $0 \neq a \in K$ und das Polynom $g(x) = x^n - a$. (Aus historischen Gründen heisst $x^n - a = 0$ eine *reine Gleichung.*) Dann ist $g(x)$ separabel, denn $Dg(x) = n \cdot x^{n-1}$ hat mit $g(x)$ keinen nichttrivialen gemeinsamen Faktor. Die Galoisgruppe von $g(x)$ ist definitionsgemäss Gal(L/K), wo L der Zerfällungskörper von $g(x)$ ist. Bezeichnet ζ eine primitive n-te Einheitswurzel, so sind offenbar $\alpha,\ \zeta\alpha,\ \zeta^2\alpha, ...,\ \zeta^{n-1}\alpha$ die n verschiedenen Nullstellen von $g(x)$. Damit gilt $L = K(\alpha)$. Man sagt, α sei ein *primitives* Element der Körpererweiterung $K \subseteq L$.

Beispiel Es sei $K = \mathbb{Q}((1 + i)/\sqrt{2})$. Das Element $(1 + i)/\sqrt{2}$ ist eine primitive 8-te Einheitswurzel. Betrachte $g(x) = x^8 - 4 \in K[x]$ und $\alpha = \sqrt[4]{2}$. Dann sind

$$\alpha,\ \alpha\zeta, ...,\ \alpha\zeta^7$$

die 8 Nullstellen des Polynoms $g(x)$. Offensichtlich gilt $[L : K] = 2$.

Es sei $\sigma \in$ Gal(L/K). Dann bildet σ das Element α auf eine Nullstelle von $g(x)$ ab, d.h. es gibt $\nu,\ 0 \leq \nu \leq n - 1$ mit $\sigma(\alpha) = \zeta^\nu\alpha$. Wir behaupten, dass die Zuordnung $\sigma \mapsto \zeta^\nu$ einen injektiven Homomorphismus von Gal(L/K) in die Gruppe der n-ten Einheitswurzeln

definiert. In der Tat folgt aus $\sigma(\alpha) = \zeta^\nu \alpha$, $\tau(\alpha) = \zeta^\mu \alpha$, sofort

$$\sigma \cdot \tau(\alpha) = \sigma(\zeta^\mu \alpha) = \alpha \zeta^\nu \zeta^\mu.$$

Die Zuordnung ist also homomorph. Ausserdem ist σ als Automorphismus von $K(\alpha)$ durch das Bild $\sigma(\alpha)$ festgelegt; das bedeutet, dass die Abbildung injektiv ist.

Die Gruppe $\mathrm{Gal}(L/K)$ ist somit isomorph zu einer Untergruppe der Gruppe der n-ten Einheitswurzeln. Letztere ist unter den oben genannten Bedingungen zyklisch. Damit ist die Gruppe $\mathrm{Gal}(L/K)$ ebenfalls zyklisch, und ihre Ordnung ist ein Teiler von n.

(b) Kreisteilungskörper.

Es sei $\mathrm{char}\, K = 0$ oder $\mathrm{char}\, K = p$ und $p \nmid n$. Betrachte das Polynom $f(x) = x^n - 1 \in K[x]$ und dessen Zerfällungskörper L. Ist ζ eine primitive n-te Einheitswurzel, so ist $L = K(\zeta)$. Körper, die wie L durch Adjunktion einer Einheitswurzel entstehen, heissen *Kreisteilungskörper*. Ein Element $\sigma \in \mathrm{Gal}(L/K)$ bildet ζ in $\sigma(\zeta)$ ab. Wegen $\sigma(\alpha\beta) = \sigma(\alpha) \cdot \sigma(\beta)$ muss σ ein Isomorphismus der Gruppe der n-ten Einheitswurzeln sein; insbesondere muss $\sigma(\zeta)$ wieder eine *primitive* n-te Einheitswurzel sein. Daraus folgt $\sigma(\zeta) = \zeta^k$ für ein gewisses $0 \leq k \leq n-1$ mit $(n, k) = 1$. Die Zuordnung $\sigma \mapsto k$ definiert einen injektiven Homomorphismus von $\mathrm{Gal}(L/K)$ in die multiplikative Gruppe der zu n teilerfremden Restklassen modulo n. In der Tat gilt für σ mit $\sigma(\zeta) = \zeta^k$ und τ mit $\tau(\zeta) = \zeta^h$

$$\sigma(\tau(\zeta)) = \sigma(\zeta^h) = \zeta^{hk},$$

wobei hk modulo n zu nehmen ist. Die Zuordnung ist also homomorph. Ausserdem ist sie injektiv, da σ als Automorphismus von $K(\zeta)$ durch das Bild $\sigma(\zeta)$ festgelegt ist. Damit ist $\mathrm{Gal}(L/K)$ isomorph zu einer Untergruppe der multiplikativen Gruppe der zu n teilerfremden Restklassen modulo n. Insbesondere ist die Gruppe $\mathrm{Gal}(L/K)$ abelsch, und ihre Ordnung ist ein Teiler von $\phi(n)$.

Im Spezialfall, wo n prim ist, $n = q$, gilt $\phi(q) = q - 1$ und die Gruppe der zu n teilerfremden Restklassen modulo n ist zyklisch der Ordnung $q - 1$. In diesem Fall ist also die Galoisgruppe $\mathrm{Gal}(L/K)$ zyklisch, und deren Ordnung teilt $q - 1$.

(c) Endliche Körper.

Wir betrachten die Körpererweiterung $\mathbb{F}_p \subseteq F$, wo F der endliche Körper mit p^n Elementen ist. Als Zerfällungskörper von $x^{p^n} - x$ ist die Körpererweiterung normal. Ausserdem ist sie separabel (Satz 3.5).

Aus Theorem 5.8 folgt $|\mathrm{Gal}(F/\mathbb{F}_p)| = n$. Die Abbildung $\sigma : F \to F$ definiert durch $\sigma(\alpha) = \alpha^p$ ist wegen $\mathrm{char}\, F = p$ ein Körperhomomorphismus, welcher die Elemente von $\mathbb{F}_p$ festhält. Nach dem kleinen Satz von Fermat gilt nämlich $a^p \equiv a \pmod p$. Als

Körperhomomorphismus ist σ injektiv; wegen des endlichen Körpergrades folgt daraus, dass σ auch surjektiv ist. Damit ist σ ein Automorphismus von F über $\mathbb{F}_p$, also ein Element von $\mathrm{Gal}(F/\mathbb{F}_p)$; man nennt σ den *Frobeniusautomorphismus* von F.

Wir behaupten, dass die Gruppe $\mathrm{Gal}(F/\mathbb{F}_p)$ zyklisch ist und von σ erzeugt wird. Um die Behauptung zu beweisen, gehen wir indirekt vor und nehmen an, dass m mit $m < n$ existiert mit $\sigma^m = e$. Dann hätte man für alle $\alpha \in F$

$$\sigma^m(\alpha) = \alpha^{p^m} = \alpha,$$

d.h. jedes Element von F wäre Nullstelle von $x^{p^m} - x$. Der Körper F enthält aber p^n Elemente. Dies ist ein Widerspruch.

VI.7 Der Hauptsatz der Galoistheorie

Satz 7.1 *Es sei L der Zerfällungskörper eines separablen Polynoms $f(x) \in K[x]$. Bezeichnet G die Galoisgruppe* $\mathrm{Gal}(L/K)$*, dann ist $F(G) = K$.*

Beweis Nach Theorem 5.8 gilt $|\mathrm{Gal}(L/K)| = [L : K] = n$. Setze

$$K' = F(G) = \{a \in L \mid \sigma(a) = a \text{ für alle } \sigma \in G\}.$$

Dann ist $K \subseteq K' \subseteq L$ und damit $[L : K'] = m \leq n$. Wir betrachten nun L als Zerfällungskörper des Polynoms $f(x) \in K'[x]$. Dann folgt

$$|\mathrm{Gal}(L/K')| = [L : K'] = m.$$

Aber nach Definition von K' gilt $\mathrm{Gal}(L/K') = \mathrm{Gal}(L/K) = G$. Daraus ergibt sich $n = m$ und $K = K'$. Dies war zu beweisen.

Korollar 7.2 *Es sei L der Zerfällungskörper eines separablen Polynoms $f(x) \in K[x]$. Dann ist die Körpererweiterung $K \subseteq L$ separabel.*

Beweis Es ist zu zeigen, dass $\alpha \in L$ separabel ist. Zu diesem Zweck betrachten wir die Galoisgruppe $G = \mathrm{Gal}(L/K)$ und die in L zu α konjugierten Elemente $\alpha_1, \alpha_2, ..., \alpha_r$,

wobei wir mehrfache Nullstellen nur einmal aufführen. Wir definieren das Polynom $g(x)$ durch

$$g(x) = (x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_r).$$

Laut Definition ist $g(x)$ separabel. Da es unter jedem Element der Galoisgruppe invariant ist, müssen die Koeffizienten von $g(x)$ in $F(G)$ liegen. Nach Satz 7.1 gilt aber $F(G) = K$. Als Nullstelle von $g(x)$ ist somit α separabel über K. Dies war zu beweisen.[12]

Es folgt aus Satz 2.4 und Korollar 7.2, dass eine Körpererweiterung $K \subseteq L$ genau dann endlich, normal und separabel ist, wenn L Zerfällungskörper eines separablen Polynoms über K ist. Solche Körpererweiterungen werden auch etwa *endliche Galoiserweiterungen* genannt.

Satz 7.3 *Es sei L ein Körper und U eine endliche Automorphismengruppe von L. Dann gilt $[L : F(U)] \leq |U|$.*

Beweis Der Einfachheit halber setzen wir $F(U) = K$ und $|U| = m$. Wir gehen indirekt vor. Es sei also $[L : K] > m$. Dann existieren in L Elemente $\alpha_1, \alpha_2, ..., \alpha_{m+1}$, die über K linear unabhängig sind. Für jedes $\sigma \in U$ betrachten wir die folgende lineare Gleichung für $y_1, y_2, ..., y_{m+1}$

$$y_1\sigma(\alpha_1) + y_2\sigma(\alpha_2) + \cdots + y_{m+1}\sigma(\alpha_{m+1}) = 0.$$

Dies liefert ein System von m Gleichungen in $m + 1$ Unbekannten; es hat also in L nichttriviale Lösungen. Wir wählen eine Lösung mit der maximalen Anzahl Nullen und numerieren so, dass $y_1 \neq 0, ..., y_q \neq 0$ und $y_{q+1} = \cdots = y_{m+1} = 0$. Wenden wir $\tau \in U$ auf die Gleichungen unseres Gleichungssystems an, so erhalten wir

$$\tau(y_1)\tau\sigma(\alpha_1) + \cdots + \tau(y_{m+1})\tau\sigma(\alpha_{m+1}) = 0.$$

Die Matrix des Gleichungssystems ist bis auf Vertauschung der Zeilen die gleiche wie vorhin, so dass $(\tau(y_1), ..., \tau(y_{m+1}))$ auch eine Lösung des ursprünglichen Systems ist. Wir betrachten nun die durch

$$y_i' = \tau(y_1)y_i - y_1\tau(y_i)\ ,\ i = 1, 2, ..., m + 1$$

als Linearkombination (über L) gegebene Lösung. Wegen $y_1' = 0$ und $y_{q+1}' = \cdots = y_{m+1}' = 0$. kommt in ihr eine grössere Anzahl Nullen vor als in der ursprünglichen Lösung. Es muss

[12] Man kann diese Beweistechnik mit der Aussage des Satzes 7.3 kombinieren, um das folgende Resultat zu erhalten: Es sei G eine endliche Automorphismengruppe des Körpers L. Dann ist die Körpererweiterung $F(G) \subseteq L$ endlich, normal und separabel.

sich deshalb um die triviale Lösung $0 = y_1' = y_2' = \cdots = y_{m+1}'$ des Gleichungssystems handeln. Für $i = 1, 2, ..., m+1$ folgt daraus

$$\tau(y_1)y_i = y_1\tau(y_i),$$

und damit

$$y_i y_1^{-1} = \tau(y_i y_1^{-1}).$$

Da dies für alle $\tau \in U$ gilt, muss $y_i y_1^{-1}$ im Fixkörper K liegen. Es gibt also Elemente $z_i \in K$ mit $y_i = y_1 z_i$. Im Spezialfall $\sigma = e$ erhalten wir dann

$$y_1(z_1\alpha_1 + z_2\alpha_2 + \cdots + z_{m+1}\alpha_{m+1}) = 0.$$

Die Elemente $\alpha_1, \alpha_2, ..., \alpha_{m+1}$ sind also über K linear abhängig. Dies ist ein Widerspruch.

Theorem 7.4 *Die Körpererweiterung $K \subseteq L$ sei endlich, normal und separabel mit Galoisgruppe* $\mathrm{Gal}(L/K)$. *Die Zuordnung $U \rightsquigarrow F(U),\ F(U) \subseteq L$ ist eine bijektive Funktion zwischen der Menge der Untergruppen von* $\mathrm{Gal}(L/K)$ *und der Menge der Körper M mit $K \subseteq M \subseteq L$. Die inverse Funktion ist gegeben durch $M \rightsquigarrow S(M),\ S(M) \subseteq \mathrm{Gal}(L/K)$.*

Beweis (1) Es sei $K \subseteq M \subseteq L$. Da $K \subseteq L$ endlich, normal und separabel ist, ist auch $M \subseteq L$ endlich, normal und separabel. Damit folgt mit Satz 7.1

$$M \rightsquigarrow S(M) = \mathrm{Gal}(L/M) \rightsquigarrow F(\mathrm{Gal}(L/M)) = M.$$

(2) Es sei $U \subseteq \mathrm{Gal}(L/K)$. Betrachte

$$U \rightsquigarrow F(U) \rightsquigarrow S(F(U)) = \mathrm{Gal}(L/F(U)).$$

Natürlich gilt $U \subseteq \mathrm{Gal}(L/F(U))$. Zusammen mit Satz 5.6 und Satz 7.3 erhalten wir nun

$$|U| \leq |\mathrm{Gal}(L/F(U))| \leq [L : F(U)] \leq |U|.$$

Damit folgt $U = \mathrm{Gal}(L/F(U))$.

Dem Hauptsatz der Galoistheorie lassen wir eine Anzahl von Korollaren folgen. Wir betrachten immer die Situation, wo $K \subseteq L$ eine endliche, normale und separable Körpererweiterung ist.

(1) Es sei M ein Zwischenkörper, $K \subseteq M \subseteq L$, mit $S(M) = U \subseteq G = \mathrm{Gal}(L/K)$. Dann gilt

$$|G| = [L : K]\ ;\ |U| = [L : M].$$

Wegen $[M : K] = [L : K]/[L : M]$ folgt daraus $[M : K] = |G|/|U| = [G : U]$.

Korollar 7.5 *In der Situation $K \subseteq M \subseteq L$ ist der Körpergrad $[M : K]$ gleich dem Index von $S(M)$ in* $\mathrm{Gal}(L/K)$.

(2) Der aufsteigenden Folge von Zwischenkörpern

$$K \subseteq M_0 \subseteq M_1 \subseteq L$$

entspricht die absteigende Folge von Untergruppen der Galoisgruppe $\mathrm{Gal}(L/K)$:

$$\mathrm{Gal}(L/K) \supseteq S(M_0) \supseteq S(M_1) \supseteq \{e\}.$$

$$\mathrm{Gal}(L/K) \supseteq \mathrm{Gal}(L/M_0) \supseteq \mathrm{Gal}(L/M_1) \supseteq \{e\}.$$

Korollar 7.6 *Die Galoiskorrespondenz ist ein Verbandsantiisomorphismus.*

(3) Es sei $K \subseteq M \subseteq L$. Für $\sigma \in \mathrm{Gal}(L/K)$ ist $\sigma(M)$ wiederum ein Körper mit $K \subseteq \sigma(M) \subseteq L$. Es ist dann offensichtlich

$$S(\sigma M) = \sigma(S(M))\sigma^{-1}.$$

Der Körper $\sigma(M)$ heisst üblicherweise der unter σ zu M *konjugierte Körper* .

Korollar 7.7 *Zu konjugierten Zwischenkörpern gehören unter der Galoiskorrespondenz konjugierte Untergruppen.*

(4) Es sei $K \subseteq M \subseteq L$. Ist die Körpererweiterung normal, so liegt jedes zu $a \in M$ konjugierte Element wiederum in M, d.h. für $\sigma \in \mathrm{Gal}(L/K)$ gilt $\sigma(M) = M$. Dann folgt aber aus Korollar 7.7

$$\sigma(S(M))\sigma^{-1} = S(\sigma M) = S(M).$$

Die zu M gehörige Untergruppe $S(M)$ von $\mathrm{Gal}(L/K)$ ist somit ein Normalteiler.

Ist umgekehrt U ein Normalteiler von $\mathrm{Gal}(L/K)$ und M, $M = F(U)$ der zugehörige Zwischenkörper, so gilt für alle $\sigma \in \mathrm{Gal}(L/K)$

$$\sigma(M) = F(\sigma U \sigma^{-1}) = F(U) = M.$$

Der Körper M enthält folglich mit jedem Element auch alle zu diesem konjugierten Elemente, d.h. die Körpererweiterung $K \subseteq M$ ist normal. Damit haben wir das folgende Korollar bewiesen:

Korollar 7.8 *In der Situation $K \subseteq M \subseteq L$ ist die Körpererweiterung $K \subseteq M$ genau dann normal, wenn $S(M)$ in $\mathrm{Gal}(L/K)$ ein Normalteiler ist.*

(7) Es sei $K \subseteq M \subseteq L$ gegeben mit $K \subseteq M$ normal. Dann gilt für $\sigma \in \mathrm{Gal}(L/K)$ stets $\sigma(M) = M$. Es gibt folglich einen Gruppenhomomorphismus $\pi : \mathrm{Gal}(L/K) \to \mathrm{Gal}(M/K)$ der durch die Restriktion von σ auf M definiert ist. Der Kern von π besteht aus allen Automorphismen, die in M die Identität induzieren; es folgt $\ker \pi = S(M)$. Ausserdem gilt

$$|\mathrm{Gal}(M/K)| = [M : K] = |\mathrm{Gal}(L/K)/S(M)|,$$

so dass π einen Isomorphismus

$$\mathrm{Gal}(L/K)/S(M) \xrightarrow{\sim} \mathrm{Gal}(M/K)$$

induziert.

Korollar 7.9 *Es sei $K \subseteq M \subseteq L$ gegeben mit $K \subseteq M$ normal. Dann gilt*

$$\mathrm{Gal}(L/K)/S(M) \cong \mathrm{Gal}(M/K).$$

VI.8 Ein Beispiel[13]

Es sei $K = \mathbb{Q}$. Das Polynom $f(x) = x^4 - 2$ lässt sich über $\mathbb{C}$ wie folgt faktorisieren

$$f(x) = (x - \alpha)(x + \alpha)(x - i\alpha)(x + i\alpha),$$

wobei wir $\alpha = \sqrt[4]{2}$ gesetzt haben. Der Zerfällungskörper von $f(x)$ ist somit $\mathbb{Q}(i, \sqrt[4]{2})$. Die Körpererweiterung ist endlich, normal und separabel. Adjungieren wir zuerst die 4-te Einheitswurzel i und dann α, so erhalten wir

$$[L : K] = [\mathbb{Q}(\alpha) : \mathbb{Q}(i)][\mathbb{Q}(i) : \mathbb{Q}].$$

Da $f(x)$ über $\mathbb{Q}(i)$ irreduzibel ist, folgt $[\mathbb{Q}(\alpha) : \mathbb{Q}(i)] = 4$. Wegen $[\mathbb{Q}(i) : \mathbb{Q}] = 2$ folgt somit $[L : K] = 8$. Nach Abschnitt 6 definiert

$$\sigma(i) = i, \quad \sigma(\alpha) = i\alpha$$

[13]Das detailliert ausgearbeitete Beispiel ist im Buch von I. Stewart, *Galois Theory*, Chapman Hall, 1979, p. 118 ff zu finden. Es wird hier im wesentlichen übernommen.

einen Automorphismus von L über $\mathbb{Q}$. Ebenso induziert die komplexe Konjugation (von $\mathbb{C}$) einen Automorphismus τ von L über $\mathbb{Q}$:

$$\tau(i) = -i \ , \quad \tau(\alpha) = \alpha \ .$$

Die Bilder von i und α unter den Produkten von σ, τ sind in der folgenden Tabelle zusammengestellt.

	i	α
1	i	α
σ	i	$i\alpha$
σ^2	i	$-\alpha$
σ^3	i	$-i\alpha$
τ	$-i$	α
$\sigma\tau$	$-i$	$i\alpha$
$\sigma^2\tau$	$-i$	$-\alpha$
$\sigma^3\tau$	$-i$	$-i\alpha$

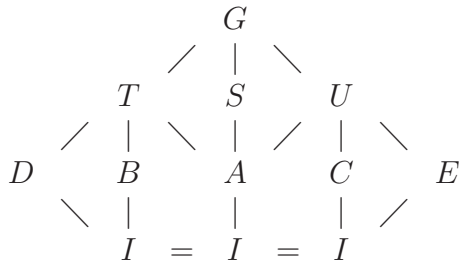
Es gibt keine weiteren Körperhomomorphismen von L über $\mathbb{Q}$, denn jeder Körperhomomorphismus muss i in $\pm i$ und α in $\pm\alpha$ oder $\pm i\alpha$ abbilden. Alle möglichen Kombinationen kommen in der Tabelle vor. In der Tat muss ja die Galoisgruppe $\mathrm{Gal}(L/K)$ die Ordnung 8 besitzen. Damit gilt

$$\mathrm{Gal}(L/K) = \mathbf{D}_8 = \langle\sigma\rangle \rtimes \langle\tau\rangle,$$

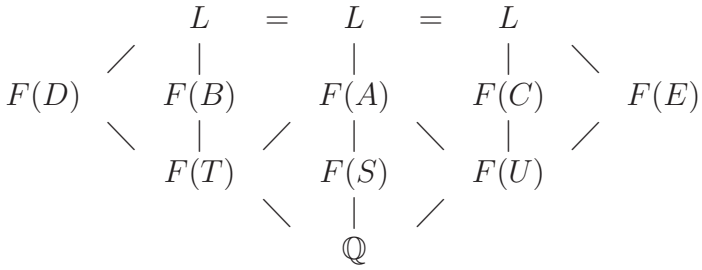
wo $\mathbf{D}_8$ die Diedergruppe der Ordnung 8 bezeichnet, also die Symmetriegruppe des Quadrates. Deren Untergruppen lassen sich leicht aufzählen:

Untergruppe	Ordnung	Struktur
G	8	$C_4 \rtimes C_2$
$S = \{1, \sigma, \sigma^2, \sigma^4\}$	4	C_4
$T = \{1, \sigma^2, \tau, \sigma^2\tau\}$	4	$C_2 \times C_2$
$U = \{1, \sigma^2, \sigma\tau, \sigma^3\tau\}$	4	$C_2 \times C_2$
$A = \{1, \sigma^2\}$	2	C_2
$B = \{1, \tau\}$	2	C_2
$C = \{1, \sigma\tau\}$	2	C_2
$D = \{1, \sigma^2\tau\}$	2	C_2
$E = \{1, \sigma^3\tau\}$	2	C_2
$I = \{1\}$	1	e

Der volle Verband der Untergruppe sieht dann wie folgt aus



Unter der Galoiskorrespondenz liefert dies sämtliche Zwischenkörper der Körpererweiterung $\mathbb{Q} \subseteq L$.



Einige dieser Unterkörper lassen sich in einfacher Weise beschreiben, z.B. $F(S) = \mathbb{Q}(i)$, $F(T) = \mathbb{Q}(\sqrt{2})$, $F(U) = \mathbb{Q}(i\sqrt{2})$. Andere der Unterkörper sind nicht auf so offensichtliche Art gegeben. Wir illustrieren dies an $F(C)$. Jedes Element von L lässt sich schreiben als

$$\xi = a_0 + a_1\alpha + a_2\alpha^2 + a_3\alpha^3 + a_4 i + a_5 i\alpha + a_6 i\alpha^2 + a_7 i\alpha^3$$

mit $a_i \in \mathbb{Q},\ i = 0, 1, ..., 7$. Es sind jetzt Bedingungen zu suchen, welche ausdrücken, dass ξ unter $\sigma\tau$ invariant ist:

$$\begin{aligned} \sigma\tau(\xi) &= a_0 + a_1 i\alpha - a_2\alpha^2 - a_3 i\alpha^3 - a_4 i - a_5 i(i\alpha) - a_6 i(i\alpha)^2 - a_7 i(i\alpha)^3 \\ &= a_0 + a_5\alpha - a_2\alpha^2 - a_7\alpha^3 - a_4 i + a_1 i\alpha + a_6 i\alpha^2 - a_3 i\alpha^3. \end{aligned}$$

Gilt $\xi = \sigma\tau(\xi)$, so folgt

$$a_1 = a_5,\ a_2 = -a_2,\ a_3 = -a_7,\ a_4 = -a_4.$$

Es lässt sich folglich α schreiben als

$$\begin{aligned}\alpha &= a_0 + a_1(1+i)\alpha + a_6 i\alpha^2 + a_3(1-i)\alpha^3 \\ &= a_0 + a_1(1+i)\alpha + \frac{a_6}{2}((1+i)\alpha)^2 - \frac{a_3}{2}((1+i)\alpha)^3.\end{aligned}$$

Daraus liest man sofort $F(C) = \mathbb{Q}((1+i)\alpha)$ ab.

Analog lassen sich die anderen Unterkörper erhalten:

$$\begin{aligned}F(A) &= \mathbb{Q}(i, \sqrt{2}) \\ F(B) &= \mathbb{Q}(\alpha) \\ F(D) &= \mathbb{Q}(i\alpha) \\ F(E) &= \mathbb{Q}((1-i)\alpha)\end{aligned}$$

Schliesslich merken wir an, dass die Untergruppen I, A, S, T, U, G in G Normalteiler sind. Die zugehörigen Zwischenkörper sind normal, d.h. Zerfällungskörper von gewissen Polynomen. Solche Polynome sind der Reihe nach:

$$x^4 - 2,\ x^4 - x^2 - 2,\ x^2 + 1,\ x^2 - 2,\ x^2 + 2,\ x.$$

Die Untergruppe B und damit der Zwischenkörper $F(B)$ ist nicht normal; das irreduzible Polynom $x^4 - 2$ hat die Nullstelle α in $F(B)$, zerfällt aber über $F(B)$ nicht in Linearfaktoren.

VI.9 Konstruktion mit Zirkel und Lineal

In Abschnitt III.3 (siehe Satz III.3.1) wurde gezeigt: Ist die reelle Zahl α aus der Einheitsstrecke mit Zirkel und Lineal konstruierbar, so existiert eine Folge von Erweiterungskörpern L_i von $\mathbb{Q}$

$$\mathbb{Q} = L_0 \subseteq L_1 \subseteq L_2 \subseteq \cdots \quad \subseteq L_n \subseteq \mathbb{R}$$

mit $\alpha \in L_n$ und $[L_i : L_{i-1}] = 2,\ i = 1, 2, ..., n$. Insbesondere existiert zu einem konstruierbaren α ein reeller Erweiterungskörper L von $\mathbb{Q}$, der α enthält und dessen Körpergrad eine Potenz von 2 ist. Von diesem Resultat gilt auch die Umkehrung.

Satz 9.1 *Es sei $\mathbb{Q} \subseteq L$ eine normale Körpererweiterung mit $L \subseteq \mathbb{R}$ und $[L : \mathbb{Q}] = 2^\lambda$. Dann ist jedes $\alpha \in L$ konstruierbar.*

Beweis Da L auch separabel ist, folgt aus Theorem 5.8, dass die Ordnung von $\mathrm{Gal}(L/\mathbb{Q})$ gerade 2^λ ist. Als Gruppe, deren Ordnung eine Potenz der Primzahl 2 ist, besitzt $\mathrm{Gal}(L/\mathbb{Q})$ ein nichttriviales Zentrum (siehe Satz I.8.5) und damit ein zentrales Element der Ordnung 2. Dieses erzeugt einen Normalteiler N der Ordnung 2. Zu N gehört ein Zwischenkörper $M = F(N)$, $\mathbb{Q} \subseteq M \subseteq L$ mit $[M : \mathbb{Q}] = 2^{\lambda-1}$. Da N ein Normalteiler ist, ist die Körpererweiterung $\mathbb{Q} \subseteq M$ normal. Wir können deshalb induktiv annehmen, dass jedes Element in M konstruierbar ist. Die Galoisgruppe $\mathrm{Gal}(L/M)$ ist isomorph zu N. Es sei σ das nichttriviale Element in $\mathrm{Gal}(L/M)$. Für $\alpha \in L$, $\alpha \notin M$ betrachten wir $(\alpha - \sigma(\alpha))^2 \in L$. Dieses Element ist offensichtlich unter σ invariant, und es folgt $(\alpha - \sigma(\alpha))^2 \in M$. Andererseits gilt $\sigma(\alpha - \sigma(\alpha)) = -(\alpha - \sigma(\alpha))$, d.h. $\alpha - \sigma(\alpha)$ ist unter σ *nicht* invariant, liegt also *nicht* in M. Daraus ergibt sich

$$L = M(\alpha - \sigma(\alpha)).$$

Das Element $\alpha - \sigma(\alpha)$ ist aber als Quadratwurzel eines konstruierbaren Elementes konstruierbar, also ist jedes Element in L konstruierbar, insbesondere ist α konstruierbar. Dies war zu beweisen.

Wir wenden dieses Resultat auf die Konstruktion von regulären n-Ecken an. Wir beweisen das folgende Resultat.

Satz 9.2 *Es sei ζ eine primitive n-te Einheitswurzel. Genau dann ist das reguläre n-Eck konstruierbar, wenn $[\mathbb{Q}(\zeta) : \mathbb{Q}]$ eine Potenz von 2 ist.*

Beweis Das reguläre n-Eck ist offenbar genau dann konstruierbar, wenn $\cos(2\pi/n)$ konstruierbar ist. Setzen wir $\alpha = \cos(2\pi/n)$ und $\zeta = e^{2\pi i/n}$, so gilt

$$\alpha = \frac{1}{2}(\zeta + \zeta^{-1})$$

und damit $\zeta^2 - 2\alpha\zeta + 1 = 0$. Daraus folgt, dass der Körpergrad $[\mathbb{Q}(\zeta) : \mathbb{Q}(\alpha)]$ entweder 1 oder 2 ist. Da $\mathbb{Q} \subseteq \mathbb{Q}(\zeta)$ normal und die Galoisgruppe $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$ abelsch ist, ist auch $\mathbb{Q} \subseteq \mathbb{Q}(\alpha)$ normal. Ausserdem ist $[\mathbb{Q}(\alpha) : \mathbb{Q}]$ genau dann eine Potenz von 2, wenn $[\mathbb{Q}(\zeta) : \mathbb{Q}]$ eine Potenz von 2 ist. Aus Satz 9.1 ergibt sich dann die Behauptung.

Beispiel Es sei $n = p$, p prim. Dann ist ζ vom Grad $p - 1$. Aus Satz 9.2 folgt, dass das reguläre p-Eck genau dann konstruierbar ist, wenn p von der Form $2^k + 1$ ist. Das

reguläre p-Eck ist somit für $p = 3, 5, 17, 257, ...$ konstruierbar und für $p = 7, 11, 13, 19, ...$ *nicht* konstruierbar.

Bemerkung Man kann leicht zeigen, dass $2^k + 1$ nur für $k = 2^r$ prim sein kann. Die Primzahlen der Form $2^{2^r} + 1$ heissen *Fermatprimzahlen*. Für $r = 0, 1, 2, 3, 4$, erhält man der Reihe nach die Primzahlen $3, 5, 17, 257, 65'537$. Euler hat 1732 gezeigt, dass $2^{2^5} + 1$ *keine* Primzahl ist. Bis heute konnten keine weiteren Fermatprimzahlen gefunden werden; man weiss auch nicht, ob es unendlich oder nur endlich viele davon gibt.

Bemerkung Es sei n beliebig. Dann gibt es $\phi(n)$ primitive n-te Einheitswurzeln. Man kann zeigen,[14] dass das Polynom, welches gerade die $\phi(n)$ primitiven n-ten Einheitswurzeln als Nullstellen besitzt, rationale Koeffizienten besitzt und irreduzibel ist. Daraus folgt für eine primitive n-te Einheitswurzel ζ

$$[\mathbb{Q}(\zeta) : \mathbb{Q}] = \phi(n).$$

Ist $2^\beta p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ die Primfaktorenzerlegung von n, so gilt bekanntlich

$$\phi(n) = 2^{\beta-1} p_1^{\alpha_1-1} p_2^{\alpha_2-1} \cdots p_r^{\alpha_r-1} (p_1 - 1)(p_2 - 1) \cdots (p_r - 1).$$

Genau dann ist also das reguläre n-Eck konstruierbar, wenn in der Primfaktorenzerlegung von n ausser 2 nur Fermatprimzahlen und diese höchstens in der ersten Potenz vorkommen.

VI.10 Auflösen von Gleichungen durch Radikale

Es sei $f(x)$ ein irreduzibles Polynom über K, wo K ein Körper der Charakteristik 0 ist. Wir nehmen an, dass im Zerfällungskörper L von $f(x)$ die Nullstelle α durch Radikale darstellbar ist, etwa in der Form

$$\alpha = \frac{\sqrt[s]{\sqrt[r]{a}} + \sqrt[p]{\sqrt[q]{b} + \sqrt[t]{c} \pm \cdots}}{\sqrt[u]{d} \pm \cdots}.$$

Dabei dürfen wir offenbar annehmen, dass alle Wurzelexponenten Primzahlen sind. Es seien $p, q, r, ...$ diese endlich vielen Primzahlen. Wir adjungieren zu K der Reihe nach die p-ten, q-ten,... Einheitswurzeln. Dies gibt eine endliche aufsteigende Folge von normalen

[14] Für einen Beweis, siehe z.B. B.L. van der Waerden, *Algebra I*, Springer 1960, p. 180 ff.

und separablen Körpererweiterungen $K = K_0 \subseteq K_1 \subseteq K_2 \subseteq \cdots \subseteq K_m \subseteq M$. Nach den Resultaten in Abschnitt 6 ist in jedem Schritt die Galoisgruppe zyklisch.

Als nächstes adjungieren wir nun der Reihe nach, beginnend mit der innersten, die auftretenden Wurzeln $\sqrt[r]{a}, ...$ und die Wurzeln *der zu a konjugierten Elemente*. Auf diese Weise konstruiert man eine endliche Folge von Körpern

$$M = M_0 \subseteq M_1 \subseteq M_2 \subseteq \cdots \subseteq M_m \subseteq L.$$

Jeder Schritt liefert nach den Resultaten in Abschnitt 6 eine endliche, normale und separable Körpererweiterung mit zyklischer Galoisgruppe. Ferner ist $K \subseteq L$ eine normale Körpererweiterung, weil jeweils auch die Wurzeln der zum Radikanden konjugierten Elemente adjungiert wurden. Setzt man $H_i = \mathrm{Gal}(L/M_i)$ und $\overline{H}_i = \mathrm{Gal}(L/K_i)$, so erhält man in der Galoisgruppe $G = \mathrm{Gal}(L/K)$ eine Folge von Untergruppen

$$\{e\} \subseteq \cdots \subseteq H_2 \subseteq H_1 \subseteq H_0 \subseteq \cdots \subseteq \overline{H}_2 \subseteq \overline{H}_1 \subseteq G\ ,$$

wobei die Quotienten $\overline{H}_i/\overline{H}_{i+1}$ und H_i/H_{i+1} jeweils zyklisch sind. Eine endliche Gruppe, die eine derartige Reihe zulässt heisst in der Gruppentheorie definitionsgemäss auflösbar: Die Galoisgruppe $G = Gal(L/K)$ ist also auflösbar. Da die Körpererweiterung $K \subseteq L$ normal ist, folgt, dass sich *jede* Nullstelle von $f(x)$ durch Radikale ausdrücken lässt; in der Tat lässt sich nach Konstruktion sogar jedes Element von L durch Radikale ausdrücken.

Es sei nun $\overline{L}$ der Zerfällungskörper von $f(x)$. Wegen der Irreduzibilität von $f(x)$ ist $\overline{L}$ ein Unterkörper von L mit $K \subseteq \overline{L} \subseteq L$, und $\mathrm{Gal}(\overline{L}/K)$ ist ein Quotient von $\mathrm{Gal}(L/K)$, also insbesondere auflösbar.

Satz 10.1 *Es sei K ein Körper der Charakteristik 0. Es sei $f(x)$ ein irreduzibles Polynom. Lässt sich eine Nullstelle von $f(x)$ durch Radikale ausdrücken, so ist die Galoisgruppe von $f(x)$ auflösbar, und jede Nullstelle von $f(x)$ lässt sich durch Radikale ausdrücken.*

Satz 10.2 *Die Nullstellen des Polynoms $f(x) = x^5 - 6x + 3 \in \mathbb{Q}[x]$ lassen sich nicht durch Radikale ausdrücken.*

Beweis Mit Hilfe des Kriteriums von Eisenstein lässt sich leicht zeigen, dass $f(x)$ irreduzibel ist. Eine Kurvendiskussion zeigt, dass $f(x)$ drei reelle und zwei komplexe Nullstellen besitzt. Die Galoisgruppe G von $f(x)$ ist eine Untergruppe von $\mathbf{S}_5$. Bei der Konstruktion des Zerfällungskörpers $f(x)$ wird zuerst eine Nullstelle von $f(x)$ adjungiert. Der Körpergrad $[L : \mathbb{Q}]$ ist somit durch 5 teilbar. Wegen $[L : \mathbb{Q}] = |G|$ folgt dann, dass G ein

Element der Ordnung 5 enthalten muss. Aber in $\mathbf{S}_5$ sind nur die 5er Zyklen von der Ordnung 5. Die Gruppe G enthält somit einen 5er Zyklus. Da $f(x)$ auch komplexe Nullstellen besitzt, definiert die komplexe Konjugation einen nichttrivialen Automorphismus von L über $\mathbb{Q}$. Damit enthält G auch eine Transposition. Daraus folgt $G = \mathbf{S}_5$. Aber $\mathbf{S}_5$ ist nicht auflösbar.

Bemerkung Von Satz 9.1 gilt auch die Umkehrung.[15] Es sei K ein Körper der Charakteristik 0. Genau dann ist die Galoisgruppe von $f(x)$ auflösbar, wenn die Gleichung $f(x) = 0$ durch Radikale auflösbar ist. Daraus folgt unter anderem, dass die Gleichungen von Grad $2, 3, 4$ durch Radikale auflösbar sind, denn die Gruppen $\mathbf{S}_2, \mathbf{S}_3, \mathbf{S}_4$ sind auflösbar.

Im Rest dieses Abschnittes untersuchen wir noch die sogenannte *"allgemeine Gleichung"*. Es sei $K \subseteq L$ eine endliche normale separable Körpererweiterung, d.h. es gelte $L = K(\alpha_1, \alpha_2, ..., \alpha_n)$, wo $\alpha_i,\ i = 1, 2, ..., n$ die Nullstellen eines separablen Polynoms $f(x) \in K[x]$ sind.

Definition Eine Funktion $(x_1, x_2, ..., x_n) \to g(x_1, x_2, ..., x_n)$ heisst *symmetrisch* in den Variablen $x_1, x_2, ..., x_n$, wenn $g(x_{\pi(1)}, x_{\pi(2)}, ..., x_{\pi(n)}) = g(x_1, x_2, ..., x_n)$ gilt für alle $\pi \in \mathbf{S}_n$.

Es sei $G = \mathrm{Gal}(L/K)$ und $\sigma \in G$. Ist g eine symmetrische Funktion, so gilt

$$\sigma g(\alpha_1, \alpha_2, ..., \alpha_n) = g(\sigma\alpha_1, \sigma\alpha_2, ..., \sigma\alpha_n),$$

da σ die Nullstellen von $f(x)$ permutiert. Wir erhalten, dass $g(\alpha_1, \alpha_2, ..., \alpha_n)$ im Fixkörper $F(G)$, also in K liegt.

Davon machen wir wie folgt Gebrauch. Wir betrachten $M = K(x_1, x_2, ..., x_n)$, den Körper der rationalen Funktionen in n Unbestimmten $x_1, x_2, ..., x_n$ und Koeffizienten in K. Die Funktionen

$$\begin{aligned} s_1(x_1, x_2, ..., x_n) &= x_1 + x_2 + \cdots + x_n \\ s_2(x_1, x_2, ..., x_n) &= x_1x_2 + x_1x_3 + \cdots + x_{n-1}x_n \\ &\vdots \\ s_n(x_1, x_2, ..., x_n) &= x_1x_2 \cdots x_n. \end{aligned}$$

[15] Für einen Beweis siehe I. Stewart, *Galois Theory*, Chapman and Hall 1973, p. 159 ff. oder B.L. van der Waerden, *Algebra I*, Springer 1960, p. 180 ff. Dort ist auch eine explizite Beschreibung des Auflösungsvorganges für Gleichungen vom Grade 3 und 4 zu finden, wie er sich aus der Galoistheorie ergibt.

heissen die *elementaren symmetrischen* Funktionen in $x_1, x_2, ..., x_n$. Natürlich liegen die Funktionen $s_j,\ j = 1, 2, ..., n$ in M. Es sei $N = K(s_1, s_2, ..., s_n)$ der in M von $s_1, s_2, ..., s_n$ erzeugte Zwischenkörper. Das Polynom

$$f(x) = x^n - s_1 x^{n-1} + \cdots \pm s_n \in N[x]$$

zerfällt offensichtlich über M in Linearfaktoren

$$f(x) = (x - x_1) \cdots (x - x_n) \in M[x].$$

Das Polynom $f(x)$ hat somit n verschiedene Nullstellen und ist separabel. Da M aus N durch Adjunktion der Elemente $x_1, x_2, ..., x_n$ entsteht, ist M gerade der Zerfällungskörper von $f(x)$ über N. Die Körpererweiterung $N \subseteq M$ ist damit endlich, normal und separabel, und es gilt $[M : N] \leq n!$. Jede Permutation π von $x_1, x_2, ..., x_n$ definiert einen Automorphismus von M über K, welcher die Elemente von N festhält. Daraus folgt $\mathbf{S}_n \subseteq \mathrm{Gal}(M/N)$.

Satz 10.3 *Die Galoisgruppe von* $f(x) = x^n - s_1 x^{n-1} + \cdots \pm s_n \in N[x]$ *ist* $\mathbf{S}_n$.

Beweis Wir haben bereits gesehen, dass $\mathbf{S}_n$ eine Untergruppe von $\mathrm{Gal}(M/N)$ ist. Nach Theorem 5.8 gilt aber $|\mathrm{Gal}(M/N)| = [M : N] \leq n!$.

Bemerkung Als Nebenresultat haben wir erhalten, dass sich jede rationale symmetrische Funktion in $x_1, x_2, ..., x_n$ rational in $s_1, s_2, ..., s_n$ ausdrücken lässt, denn sie ist invariant unter allen $\pi \in \mathbf{S}_n$, liegt also in N. Dieses Resultat lässt sich verschärfen. Es gilt der sogenannte Hauptsatz über symmetrische Polynome. Er besagt, dass sich jedes symmetrische Polynom in $x_1, x_2, ..., x_n$, als *Polynom* in $s_1, s_2, ..., s_n$ schreiben lässt.[16]

Es sei P der Quotientenkörper von $K[u_1, u_2, ..., u_n]$. Wir betrachten die sogenannte allgemeine Gleichung n-ten Grades über K:

$$0 = g(x) = x^n - u_1 x^{n-1} + \cdots \pm u_n \in P[x].$$

Es sei R der Zerfällungskörper von $g(x)$ über P. Der Körper R wird durch Adjunktion der n Nullstellen von $g(x)$ erhalten. Es seien $v_1, v_2, ..., v_n$ diese Nullstellen. Dann gilt

$$s_i(v_1, v_2, ..., v_n) = u_i,\ i = 1, 2, ..., n.$$

Wir betrachten als nächstes den Ringhomomorphismus

$$\phi : K[u_1, u_2, ..., u_n] \to K[x_1, x_2, ..., x_n] \subseteq K(x_1, x_2, ..., x_n) = M$$

[16] Siehe dazu das Buch von I.G. Macdonald, *Symmetric functions and Hall polynomials*, Clarendon Press, 1979.

definiert durch

$$\phi(h(u_1, u_2, ..., u_n)) = h(s_1(x_1, x_2, ..., x_n), s_2(x_1, x_2, ..., x_n), ..., s_n(x_1, x_2, ..., x_n)).$$

Genau dann liegt $h(u_1, u_2, ..., u_n)$ in $\ker \phi$, wenn

$$h(s_1(x_1, x_2, ..., x_n), s_2(x_1, x_2, ..., x_n), ..., s_n(x_1, x_2, ..., x_n)) \equiv 0.$$

A fortiori folgt dann aus $h(u_1, u_2, ..., u_n) \in \ker \phi$

$$h(s_1(v_1, v_2, ..., v_n), s_2(v_1, v_2, ..., v_n), ..., s_n(v_1, v_2, ..., v_n)) = 0.$$

Nun ist aber $s_i(v_1, v_2, ..., v_n) = u_i$. Also gilt $h(u_1, u_2, ..., u_n) = 0$, und die Abbildung ϕ ist injektiv.[17] Ferner ist natürlich im $\phi \subseteq K(s_1, s_2, ..., s_n) = N$, so dass ϕ einen Körperhomomorphismus $\psi : P \to N$ induziert. Nun ist R Zerfällungskörper von $g(x)$ über P und M Zerfällungskörper von $f(x)$ über N. Ausserdem gilt $f(x) = \psi g(x)$. Damit folgt $\mathrm{Gal}(R/P) = \mathrm{Gal}(M/N) = \mathbf{S}_n$, womit der folgende Satz bewiesen ist.

Satz 10.4 *Das allgemeine Polynom $g(x) \in P[x]$ besitzt die Galoisgruppe $\mathbf{S}_n$; insbesondere gilt $[R : P] = n!$.*

Ein unmittelbares Korollar ist der berühmte Satz von N.H. Abel.

Korollar 10.5 *Die allgemeine Gleichung $g(x) = 0$ mit $\deg\ g(x) \geq 5$ ist nicht durch Radikale auflösbar, d.h. es gibt für derartige Gleichungen keine allgemeine Lösungsformel mit Radikalen.*

Beweis Die Gruppe $\mathbf{S}_n$ ist für $n \geq 5$ nicht auflösbar. Jede dieser Gruppen enthält nämlich die Gruppe $\mathbf{A}_5$ als Untergruppe. Und $\mathbf{A}_5$ ist einfach (siehe Abschnitt V.7, Beispiel (e)), also nicht auflösbar. Andererseits ergibt sich aus der Definition einer auflösbaren Gruppe sofort, dass jede ihrer Untergruppen wiederum auflösbar ist.

[17] Damit haben wir im Grunde bewiesen, dass die symmetrischen Polynome algebraisch unabhängig sind; d.h. dass es keine algebraische Abhängigkeit unter den s_i's gibt. Siehe dazu I.G. Macdonald, l.c.

VI.11 Galoistheorie und Darstellungstheorie

Es sei $K \subseteq L$ eine Körpererweiterung und G die Galoisgrupe $\mathrm{Gal}(L/K)$. Laut Definition operiert G durch Körperautomorphismen über K, also insbesondere durch K-lineare Transformationen im K-Vektorraum L. Damit trägt L eine K-Darstellung von G, oder, anders ausgedrückt, L ist ein $K[G]$-Modul. Im ersten Teil dieses Abschnittes werden wir für den Fall einer endlichen, normalen und separablen Körpererweiterung die Struktur dieses Moduls aufklären (siehe Korollar 11.3). Dazu benötigen wir den "Satz vom primitiven Element" und den "Satz von der Normalbasis".

Satz 11.1 (Satz vom primitiven Element) *Es seien $\alpha_1, \alpha_2, ..., \alpha_n$ über K separable Elemente. Dann existiert $\delta \in K(\alpha_1, \alpha_2, ..., \alpha_n)$ mit $K(\alpha_1, \alpha_2, ..., \alpha_n) = K(\delta)$.*

Beweis Ist K ein endlicher Körper, so ist die Aussage klar, denn in diesem Fall kann für δ eine entsprechende primitive Einheitswurzel gewählt werden. Wir dürfen also annehmen, dass K ein unendlicher Körper ist. Es genügt, den Satz für $n = 2$ zu beweisen; eine offensichtliche Induktion liefert dann die allgemeine Aussage. Wir setzen also $\beta = \alpha_1, \gamma = \alpha_2$. Es seien $\beta_1, \beta_2, ..., \beta_m$ die zu β und $\gamma_1, \gamma_2, ..., \gamma_n$ die zu γ konjugierten Elemente im Zerfällungskörper des Produktes des Minimalpolynoms $f(x)$ von β und $g(x)$ von γ. Dabei setzen wir $\beta_1 = \beta$ und $\gamma_1 = \gamma$. Für $1 \leq i \leq m$ und $2 \leq k \leq n$ betrachten wir die Gleichung

$$\beta + y\gamma = \beta_i + y\gamma_k.$$

Diese besitzt stets nur *eine* Lösung. Da K unendlich viele Elemente enthält, gibt es ein Element $c \in K$, so dass für alle i mit $1 \leq i \leq m$ und alle k mit $2 \leq k \leq n$ gilt

$$\beta + c\gamma \neq \beta_i + c\gamma_k.$$

Wir wählen ein solches c und setzen $\delta = \beta + c\gamma$. Dann gilt offensichtlich $K(\delta) \subseteq K(\beta, \gamma)$, und es bleibt, die umgekehrte Inklusion zu zeigen.

Die Polynome $g(x)$ und $f(\delta - cx)$ liegen in $K(\delta)[x]$ und haben γ als gemeinsame Nullstelle. Daraus folgt, dass das Minimalpolynom $m(x)$ von γ über $K(\delta)$ ein gemeinsamer Teiler von $g(x)$ und $f(\delta - cx)$ ist. Wir behaupten, dass $m(x)$ den Grad 1 besitzt, so dass gilt $m(x) = x - \gamma$. Dazu stellen wir zuerst einmal fest, dass mit $g(x)$ auch $m(x)$ separabel ist. Wäre nun $\deg m(x) \geq 2$, so müsste $m(x)$ als Teiler von $g(x)$ eines der Elemente $\gamma_2, \gamma_3, ..., \gamma_n$, sagen wir γ_k, als weitere Nullstelle besitzen. Da $m(x)$ auch ein Teiler von $f(\delta - cx)$ ist, müsste für ein gewisses $i = 1, 2, \ldots, m$ gelten $\delta - c\gamma_k = \beta_i$. Gerade dies wurde aber durch die Wahl von c ausgeschlossen. Damit haben wir einen Widerspruch erhalten, und es folgt in der Tat $m(x) = x - \gamma$. Als Koeffizient eines Polynoms in $K(\delta)$ liegt γ in $K(\delta)$ und wegen $\beta = \delta - c\gamma$ auch β. Dies war zu beweisen.

Satz 11.2 (Satz von der Normalbasis) *Es sei $K \subseteq L$ eine endliche, normale und separable Körpererweiterung, und $\sigma_1, \sigma_2, ..., \sigma_n$ bezeichne die Elemente der Galoisgruppe* $\mathrm{Gal}(L/K)$*. Dann existiert ein $\vartheta \in L$, so dass $(\sigma_1(\vartheta), \sigma_2(\vartheta), ..., \sigma_n(\vartheta))$ eine K-Basis von L ist. (Eine solche Basis heisst* Normalbasis*.)*

Beweis Wir führen den Beweis nur für den Fall, wo L ein unendlicher Körper ist. Nach dem Satz vom primitiven Element existiert $\alpha \in L$ mit $K(\alpha) = L$. Es sei $f(x) \in K[x]$ das Minimalpolynom von α. Wir setzen $\sigma_i(\alpha) = \alpha_i$ mit $\alpha_1 = \alpha$ und betrachten das Polynom

$$g(x) = \frac{f(x)}{(x-\alpha)\prod_{l=2}^{n}(\alpha - \alpha_l)} \in L[x]$$

und die dazu konjugierten Polynome

$$\sigma_i g(x) = g_i(x) = \frac{f(x)}{(x-\alpha_i)\prod_{l\neq i}(\alpha_i - \alpha_l)} \in L[x],\ i = 1, 2, ..., n.$$

Daraus folgt unmittelbar

$$g_i(x)g_k(x) \equiv 0 \mod f(x),\ i \neq k, \tag{2}$$

denn offensichtlich sind $\alpha_1, \alpha_2, ..., \alpha_n$ Nullstellen des Polynoms auf der linken Seite der Gleichung. Um auch eine Aussage für $g_i(x)g_i(x)$ zu gewinnen, zeigen wir zuerst

$$g_1(x) + g_2(x) + \cdots + g_n(x) - 1 = 0.$$

In der Tat gilt diese Gleichung für $x = \alpha_j,\ j = 1, 2, ..., n$, und da das Polynom auf der linken Seite höchstens den Grad $n-1$ besitzt, gilt sie allgemein. Multiplizieren wir diese Gleichung mit $g_i(x)$, so folgt zusammen mit der Aussage (1)

$$g_i(x)g_i(x) \equiv g_i(x) \mod f(x). \tag{3}$$

Als nächstes zeigen wir, dass die Determinante $D(x)$

$$D(x) = \det(\sigma_i\sigma_k(g(x)))$$

nicht trivial ist. Dazu betrachten wir das Produkt der Matrix $[\sigma_i\sigma_k(g(x))]$ mit ihrer Transponierten. Modulo $f(x)$ ist dieses Produkt nach (1) und (2) die Einheitsmatrix. Daraus folgt $D(x) \equiv 1 \mod f(x)$, insbesondere $D(x) \neq 0$. Wir wählen nun ein Element $\beta \in L$, welches *keine* Nullstelle des Polynoms $D(x)$ ist. Da L ein unendlicher Körper ist, existiert ein solches. Wir setzen $\vartheta = g(\beta)$, so dass $D(x) = \det(\sigma_i\sigma_k(\vartheta)) \neq 0$.

Es bleibt zu zeigen, dass dies impliziert, dass $\sigma_1(\vartheta), \sigma_2(\vartheta), ..., \sigma_n(\vartheta)$ über K linear unabhängig sind. Es sei

$$x_1\sigma_1(\vartheta) + x_2\sigma_2(\vartheta) + \cdots + x_n\sigma_n(\vartheta) = 0$$

mit $x_1, x_2, ..., x_n \in K$. Wenden wir $\sigma_i,\ i = 1, 2, ..., n$ auf diese Gleichung an, so folgt, dass $x_1, x_2, ..., x_n$ eine Lösung des homogenen Gleichungssystems mit Matrix $[\sigma_i\sigma_k(\vartheta)]$ ist. Da deren Determinante nicht verschwindet, erhalten wir $x_1 = x_2 = \cdots = x_n = 0$. Dies war zu beweisen.

Korollar 11.3 *Es sei $K \subseteq L$ eine endliche, normale und separable Körpererweiterung mit Galoisgruppe G. Dann ist L als $K[G]$-Modul isomorph zu $K[G]$.*

Beweis Es seien $\sigma_1, \sigma_2, ..., \sigma_n$ die Elemente der Galoisgruppe. Nach Satz 11.2 existiert ein Element $\vartheta \in L$, so dass $(\sigma_1(\vartheta), \sigma_2(\vartheta), ..., \sigma_n(\vartheta))$ eine Normalbasis ist. Die Abbildung $\Phi : K[G] \to L$ definiert durch $\sigma_i \mapsto \sigma_i(\vartheta),\ i = 1, 2, ..., n$ ist dann offensichtlich ein Isomorphismus von $K[G]$-Moduln.

Im Folgenden betrachten wir eine Anwendung der Galoistheorie auf die Darstellungstheorie endlicher Gruppen. Gegeben sei eine endliche Gruppe G und ein treuer $\mathbb{C}[G]$-Modul V. Ein $\mathbb{C}[G]$-Modul heisst *treu*, wenn zu $y \in G$ stets ein $v \in V$ existiert mit $yv \neq v$. Wir wählen eine $\mathbb{C}$-Basis $(x_1, x_2, ..., x_n)$ von V und betrachten die Polynomalgebra $\mathbb{C}[x_1, x_2, ..., x_n]$. Die Operation von G auf den Basiselementen $x_1, x_2, ..., x_n$ von V induziert in $\mathbb{C}[x_1, x_2, ..., x_n]$ in offensichtlicher Weise die Struktur eines (unendlich dimensionalen) $\mathbb{C}[G]$-Moduls. Es gilt nun der folgende Satz.

Satz 11.4 *Es sei V ein treuer $\mathbb{C}[G]$-Modul mit $\mathbb{C}$-Basis $(x_1, x_2, ..., x_n)$. Dann kommt jeder einfache $\mathbb{C}[G]$-Modul M als direkter Summand in $\mathbb{C}[x_1, x_2, ..., x_n]$ vor.*

Bevor wir daran gehen, diesen Satz zu beweisen, fügen wir noch die folgende Bemerkung an. Die Aussage des Satzes kann wie folgt etwas verschärft werden. Der $\mathbb{C}$-Unterraum H_i des Polynomringes $\mathbb{C}[x_1, x_2, ..., x_n]$, welcher von den homogenen Polynomen vom Grad i gebildet wird, ist offensichtlich stabil unter der G-Operation und ist deshalb ein $\mathbb{C}[G]$-Untermodul von $\mathbb{C}[x_1, x_2, ..., x_n]$. Dabei gilt

$$\mathbb{C}[x_1, x_2, ..., x_n] = \bigoplus_{i=0}^{\infty} H_i.$$

Aus dieser Tatsache folgt nun sofort, dass der einfache Modul M sogar in einem *homogenen Anteil* H_i als Untermodul vorkommt.

Beweis des Satzes 11.4 Wir werden beweisen, dass $\mathbb{C}[x_1, x_2, ..., x_n]$ eine Kopie der Gruppenalgebra $\mathbb{C}[G]$ enthält. Wegen der Halbeinfachheit der $\mathbb{C}[G]$-Moduln, und weil $\mathbb{C}[G]$

den Modul M als direkten Summand enthält, folgt daraus die Behauptung des Satzes. Wir betrachten den Quotientenkörper L, $L = \mathbb{C}(x_1, x_2, ..., x_n)$ von $\mathbb{C}[x_1, x_2, ..., x_n]$. Die Operation von G auf den Elementen $x_1, x_2, ..., x_n$ definiert auch in L die Struktur eines $\mathbb{C}[G]$-Moduls, und zwar so, dass $\mathbb{C}[x_1, x_2, ..., x_n]$ ein $\mathbb{C}[G]$-Untermodul ist. Da V ein treuer $\mathbb{C}[G]$-Modul ist, operiert jedes nichttriviale Element $\sigma \in G$ durch einen nichttrivialen Körperautomorphismus in L. Es sei K der Fixkörper $F(G)$ in L. Natürlich gilt $\mathbb{C} \subseteq K = F(G) \subseteq L$. Die Körpererweiterung $K \subseteq L$ ist dann endlich, normal und separabel (siehe Fussnote zum Korollar 7.2). Nach dem Satz von der Normalbasis (siehe Satz 11.2) existiert $\vartheta \in L$, so dass die Zuordnung $\sigma \mapsto \sigma(\vartheta),\ \sigma \in G$ einen Isomorphismus $K[G] \to L$ von $K[G]$-Moduln definiert. Es sei

$$\vartheta = \frac{f_1(x_1, x_2, ..., x_n)}{f_2(x_1, x_2, ..., x_n)},\ f_i(x_1, x_2, ..., x_n) \in \mathbb{C}[x_1, x_2, ..., x_n],\ i = 1, 2\ .$$

Dann setzen wir

$$\overline{\vartheta} = (\prod_{\sigma \in G} \sigma(f_2(x_1, x_2, ..., x_n)) f_1(x_1, x_2, ..., x_n).$$

Offensichtlich ist $\overline{\vartheta} \in \mathbb{C}[x_1, x_2, ..., x_n]$. Da $\prod_{\sigma \in G} \sigma(f_2(x_1, x_2, ..., x_n))$ unter der Operation von G invariant bleibt, definiert die Zuordnung $\sigma \mapsto \sigma(\vartheta),\ \sigma \in G$ einen injektiven $K[G]$-Modulhomomorphismus $K[G] \to K[x_1, x_2, ..., x_n]$. Dessen Einschränkung auf $\mathbb{C}[G] \subseteq K(G)$ liefert als Bild einen zu $\mathbb{C}[G]$ isomorphen Untermodul von $\mathbb{C}[x_1, x_2, ..., x_n]$. Dies war zu beweisen.

Korollar 11.5 (R. Steinberg) *Es sei V ein treuer $\mathbb{C}[G]$-Modul. Zu jedem einfachen $\mathbb{C}[G]$-Modul M existiert eine Tensorpotenz $V \otimes V \otimes \cdots \otimes V$, die M als direkten Summanden enthält.*

Beweis Nach Satz 11.4, beziehungsweise nach der anschliessenden Bemerkung kommt M in einem homogenen Anteil H_i von $\mathbb{C}[x_1, x_2, ..., x_n]$ vor. Die offensichtliche Abbildung von der i-fachen Tensorpotenz von V nach H_i, definiert durch

$$x_{j_1} \otimes x_{j_2} \otimes \cdots \otimes x_{j_i} \mapsto x_{j_1} x_{j_2} \cdots x_{j_i}$$

ist, wie man leicht einsieht, ein surjektiver $K[G]$-Modulhomomorphismus. Da M in H_i als direkter Summand vorkommt, muss wegen der Halbeinfachheit M auch als direkter Summand in der i-fachen Tensorpotenz von V vorkommen.

Literatur

Die ersten vier Literaturangaben betreffen Einführungen in das Gebiet der Algebra. Bei den übrigen Angaben handelt es sich um weiterführende Literatur, wobei jeweils angegeben ist, auf welche Kapitel des vorliegenden Textes sie sich beziehen. – Die Liste spiegelt die Präferenzen des Autors; Vollständigkeit ist in keiner Weise angestrebt, viele Bücher herausragender Qualität sind hier nicht aufgeführt.

Michael Artin: *Algebra*. Birkhäuser, 1993.

Nathan Jacobson: *Basic algebra* (two volumes). W.H. Freeman, vol. I 1985 (2^{nd} ed.), vol. II 1989.

Serge Lang: *Algebra*. Addison Wesley, 1993 (3^{rd} ed.).

Bartel L. van der Waerden: *Algebra* (zwei Bände). Springer Verlag, 1993 (9. Aufl.).

Jon L. Alperin, Rowen B. Bell: *Groups and representations*. Springer, 1995. (Kap. I, V)

Emil Artin: *Galois theory*. Dover 1998 (reprint of the 1942 ed.). (Kap. III, VI)

Michael F. Atiyah, Ian G. Macdonald: *Introduction to commutative algebra*. Addison-Wesley, 1969. (Kap. II)

Dave J. Benson: *Representation and cohomology* (two volumes). Cambridge University Press, 1991. (Kap. V)

Peter Hilton, Urs Stammbach: *A course in homological algebra*. Springer, 1996 (2^{nd} ed.). (Kap. IV)

Bertram Huppert: *Endliche Gruppen*. Springer, 1967. (Kap. I)

I. Martin Isaacs: *Character theory of finite groups*. Academic Press, 1976. (Kap.V)

James P. Jans: *Rings and homology*. Holt, Rinehart and Winston, 1964. (Kap. II, IV)

Walter Ledermann: *Introduction to group characters*. Cambridge University Press, 1977. (Kap. V)

Ian D. Macdonald: *The theory of groups*. Clarendon Press, 1968 (Kap. I)

Saunders Mac Lane: *Homology*. Springer, 1995 (4^{th} printing). (Kap. IV)

Derek J.S. Robinson: *A course in the theory of groups*. Springer, 1996 (2nd ed.). (Kap. I)

Jean-Pierre Serre: *Linear representations of finite groups*. Springer 1982 (2^{nd} printing). (Kap. V)

Ian Stewart: *Galois theory*, Chapman and Hall, 2004 (3^{rd} ed.). (Kap. III, VI)

Oscar Zariski, Pierre Samuel: *Commutative algebra* (two volumes). Springer, 1975 (reprint of the 1958-60 ed.). (Kap. II)