Vorlesungen über Algebra

Mainz, Wintersemester 2015

Manfred Lehn

Korrekturstand: 2. Dezember 2015

INHALTSVERZEICHNIS

§1. Polynomgleichungen

1.1. **Nullstellen.** Der Ausgangspunkt für die Entwicklung der modernen Algebra war die Frage, wie man eine algebraische Gleichung der Form

$$f_0x^n + f_1x^{n-1} + \ldots + f_{n-1}x + f_n = 0 \tag{1.1}$$

löst. Dabei stammen die Koeffizienten $f_0, \ldots, f_n$ der Gleichung aus einem Körper K, so daß man die linke Seite als ein Polynom $f = f_0x^n + \ldots + f_n \in K[x]$ auffassen und die Gleichung kürzer $f(x) = 0$ schreiben kann. Lösungen $\alpha \in K$ der Gleichungen heißen Nullstellen oder Wurzeln des Polynoms. Wenn der Leitkoeffizient f_0 nicht 0 ist, spricht man von einer Gleichung vom Grad n und für kleine Werte $n = 1, 2, 3$ und 4 auch von linearen, quadratischen, kubischen und biquadratischen Gleichungen.

Für jedes $\alpha \in K$ erhält man durch Polynomdivision eine Darstellung

$$f(x) = q(x)(x - \alpha) + r,$$

wobei der Rest r ein Polynom vom Grad < 1, also eine Konstante ist. Indem man auf beiden Seiten $x = \alpha$ setzt, erhält man

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

Statt der Polynomdivision kann man auch die Relation

$$x^m - \alpha^m = (x - \alpha)(x^{m-1} + \alpha x^{m-2} + \ldots + \alpha^{m-1})$$

verwenden und erhält so einen Ausdruck für den Quotienten.

$$q(x) = \frac{f(x) - f(\alpha)}{(x - \alpha)} = \sum_{m=1}^{n} f_m(x^{m-1} + \alpha x^{m-2} + \ldots + \alpha^{m-1}).$$

Wenn nun α eine Nullstelle von $f(x)$ ist und damit der Restterm verschwindet, ergibt sich eine Faktorisierung

$$f(x) = (x - \alpha)q(x).$$

Jede weitere von α verschiedene Nullstelle muß dann eine Nullstelle von q sein, die sich in gleicher Weise ausfaktorisieren läßt. Auf diese Weise erhält man eine Zerlegung

$$f(x) = (x - \alpha_1)^{m_1}(x - \alpha_2)^{m_2} \cdot \ldots (x - \alpha_s)^{m_s} g(x)$$

mit Nullstellen $\alpha_1, \ldots, \alpha_s \in K$, Vielfachheiten $m_1, \ldots, m_s \in \mathbb{N}$ und einem (möglicherweise konstanten) Polynom $g(x)$, das keine Nullstellen in K hat. Insbesondere hat ein Polynom f vom Grad n höchstens n verschiedene Nullstellen. Die Zerlegung ist bis auf die Reihenfolge der Faktoren eindeutig. Man sagt, α_i ist eine doppelte Nullstelle, wenn $m_i \geq 2$, eine dreifache Nullstelle, wenn $m_i \geq 3$ usw.

Man kann die Vielfachheit einer Nullstelle mit Hilfe der formalen Ableitungen eines Polynoms messen: Für Polynome $f = \sum_{k=0}^{n} f_k x^k \in R[X]$ mit Koeffizienten in einem beliebigen kommutativen Ring wird durch

$$f' := \sum_{k=1}^{n} k f_k x^{k-1}$$

auf rein algebraischem Wege und ohne Grenzprozeß eine Ableitung definiert. Man verifiziert dann leicht, daß die übliche Summen- und Produktregel gelten:

$$(f + g)' = f' + g', \qquad (fg)' = f'g + fg'.$$

Allerdings kann es vorkommen, daß $f' = 0$, ohne daß f ein Polynom vom Grad 0 ist. Das passiert zum Beispiel für das Polynom $x^p \in \mathbb{F}_p[x]$. Dieses Phänomen wird später noch wichtig werden.

Aus einer Zerlegung $f(x) = (x - \alpha)^m g(x)$, $m > 0$, erhält man durch Ableiten

$$f'(x) = (x - \alpha)^m g'(x) + m(x - \alpha)^{m-1} g(x) = (x - \alpha)^{m-1}((x - \alpha)g'(x) + mg(x)).$$

Wir können deshalb schließen:

Satz 1.1 (Huddesche[1] Regel) — *$\alpha \in K$ ist genau dann eine mehrfache Nullstelle von $f \in K[x]$, wenn α eine gemeinsame Nullstelle von f und f' ist.* □

Wenn der Körper K die Charakteristik 0 hat, d.h. wenn alle natürlichen Zahlen in K invertierbar sind, kann man die Vielfachheit mit Hilfe höherer Ableitungen genau angeben:

Satz 1.2 — *Es sei K ein Körper der Charakteristik 0. Ein Polynom $f \in K[X]$ hat in $\alpha \in K$ eine Nullstelle der Vielfachheit m, wenn*

$$f(\alpha) = f'(\alpha) = \ldots = f^{(m-1)}(\alpha) = 0 \quad \textit{und} \quad f^{(m)}(\alpha) \neq 0.$$

Beweis. Ohne Einschränkung ist f nicht konstant und $\ell \in \mathbb{N}_0$ maximal mit der Eigenschaft, daß es eine Zerlegung $f(x) = (x-\alpha)^\ell g(x)$ gibt. Alle Ableitungen $f^{(k)}$, $k < \ell$, enthalten den Faktor $(x-\alpha)^{\ell-k}$ und damit die Nullstelle α, und

$$f^{(\ell)}(x) = \sum_{i=0}^{\ell-1} \frac{\ell!^2}{i!(\ell-i)!^2} (x-\alpha)^{\ell-i} g^{(\ell-i)}(x) + \ell! g(x).$$

Es folgt $f^{(\ell)}(\alpha) = \ell! g(\alpha) \neq 0$. □

1.2. **Lösungsformeln.**

Wir wollen die klassischen Lösungsformeln für Polynomgleichungen $f(x) = 0$ für reelle Polynome vom Grad ≤ 4 besprechen.

Lineare Gleichungen

$$f_0 x + f_1 = 0$$

mit $f_0 \neq 0$ haben stets die eindeutige Lösung $x = -f_1/f_0$. Allgemeiner kann man in jeder Gleichung $f_0 x^n + \ldots + f_n = 0$ mit nichttrivialem Leitkoeffizienten stets durch f_0 teilen und deshalb ohne Einschränkung annehmen, daß $f_0 = 1$.

Eine quadratische Gleichung

$$x^2 + f_1 x + f_2 = 0$$

wird durch quadratische Ergänzung vereinfacht:

$$\left(x + \frac{f_1}{2}\right)^2 = x^2 + 2\frac{f_1}{2}x + \frac{f_1^2}{4} = \frac{f_1^2}{4} - f_2.$$

Setzt man $y = x + \frac{f_1}{2}$, so hat man die ursprüngliche Gleichung auf eine sogenannte reine Gleichung

$$y^2 = b \qquad \text{mit der Diskriminante} \quad b = \frac{f_1^2}{4} - f_2$$

zurückgeführt. Man erhält die formale Lösung

$$x = -\frac{f_1}{2} \pm \sqrt{\frac{f_1^2}{4} - f_2}$$

der Gleichung $f = 0$. Damit diese formale Lösung für konkrete Zahlenwerte wirklich Lösungen liefert, muß die Diskriminante Wurzeln besitzen.

Das Wissen, wie man quadratische Gleichungen löst, ist uralt. Die berühmte Keilschrifttafel 'Plimpton 322' ist ca 3700 Jahre alt und wird heute als Beispielsammlung für Zahlen verstanden, die in Rechenaufgaben zu quadratischen Gleichungen eingehen.

Dagegen ist die Auflösung kubischer Gleichung ein Ergebnis des 16. Jahrhunderts. Die Entdeckung der im Folgenden erklärten Verfahren geht auf die italienischen Mathmematiker SCIPIONE DEL FERRO (1465 - 1526), HANNIBAL DEL NAVE (1500 - 1558), ANTONIO MARIA FIOR, NICCOLO (FONTANA) TARTAGLIA (ca 1499 - 1557), GEROLAMO CARDANO (1501–1576), LODOVICO

[1] Johan Hudde, ⋆23. April 1628, †15. April 1704 jeweils in Amsterdam.

FERRARI (1522 - 1565) zurück. Für die ebenso spannende wie verwickelte Geschichte verweise ich auf Bücher zur Mathematikgeschichte, insbesondere das Buch 'A History of Algebra: From al-Khwarizmi to Emmy Noether' von VAN DER WAERDEN.

Wir betrachten eine kubische Gleichung

$$x^3 + f_1x^2 + f_2x + f_3 = 0$$

und nehmen der Einfachheit an, der Koeffizientenkörper sei der Körper der reellen Zahlen. Der Vergleich mit dem binomischen Ausdruck

$$\left(x + \frac{f_1}{3}\right)^3 = x^3 + f_1x^2 + \frac{f_1^2}{3}x + \frac{f_1^3}{27}$$

legt nahe, die Substitution

$$y = x + \frac{f_1}{3}, \qquad x = y - \frac{f_1}{3}$$

durchzuführen. Man erhält

$$\begin{aligned} x^3 + f_1x^2 + f_2x + f_3 &= \left(y - \frac{f_1}{3}\right)^3 + f_1\left(y - \frac{f_1}{3}\right)^2 + f_2\left(y - \frac{f_1}{3}\right) + f_3 \\ &= y^3 + \left(f_2 - \frac{1}{3}f_1^2\right)y + \left(f_3 - \frac{1}{3}f_1f_2 + \frac{2}{27}f_1^3\right). \end{aligned}$$

Durch diese Substitution kann man also den quadratischen Term eliminieren, erhält aber nicht sofort eine reine Gleichung vom Typ $y^3 = b$. Wenn wir die Unbestimmte wieder mit x bezeichnen und der Tradition folgend die konstanten und linearen Terme auf der anderen Seite des Gleichungszeichens sammeln, ist das Ausgangsproblem auf eine Gleichung der Form

$$x^3 = ax + b \tag{1.2}$$

zurückgeführt. Wenn $a = 0$, handelt es sich um eine reine Gleichung, die man sofort lösen kann, wenn man weiß, wie man Kubikwurzeln zieht. Wir nehmen also an, daß $a \neq 0$. Mit dem Ansatz $x = u + v$ mit zwei neuen Unbestimmten und der Identität

$$x^3 = (u+v)^3 = (u^3 + v^3) + (3uv)x$$

folgt, daß die Gleichung (1.2) jedenfalls dann gelöst wird, wenn

$$3uv = a \qquad \text{und} \qquad u^3 + v^3 = b \tag{1.3}$$

gilt. Aus $u^3 + v^3 = b$ und $(u^3)(v^3) = \frac{a^3}{27}$ folgt, daß u^3 und v^3 Lösungen der quadratischen Gleichung

$$0 = (t - u^3)(t - v^3) = t^2 - bt + \frac{a^3}{27}$$

sind. Bis auf eine irrelevante Vertauschung der Variablen bedeutet dies:

$$u^3 = \frac{b}{2} + \sqrt{\frac{b^2}{4} - \frac{a^3}{27}}, \quad v^3 = \frac{b}{2} - \sqrt{\frac{b^2}{4} - \frac{a^3}{27}}.$$

Man erhält so die sogenannte *Cardanische Formel*

$$x = \sqrt[3]{\frac{b}{2} + \sqrt{\frac{b^2}{4} - \frac{a^3}{27}}} + \sqrt[3]{\frac{b}{2} - \sqrt{\frac{b^2}{4} - \frac{a^3}{27}}}. \tag{1.4}$$

Dabei ist bei der Bildung der dritten Wurzeln das Folgende zu beachten: Bekanntlich hat jede komplexe Zahl $\neq 0$ nicht eine, sondern drei dritte Wurzeln, die sich um Potenzen der dritten Einheitswurzel $\rho = \frac{1}{2}(-1 + i\sqrt{3})$ unterscheiden. Das Wurzelzeichen ist also auf gefährliche Weise mehrdeutig. Aber nicht jede der 9 Kombinationen der beiden Wurzeln ist zulässig, denn u und v müssen der Nebenbedingung $3uv = a$ genügen. Deshalb legt die Wahl der Wurzel für u die Wahl der Wurzel für v fest.

Zum Beispiel hat die Gleichung

$$x^3 = 18x + 35$$

die Lösung

$$\begin{aligned} x_1 &= \sqrt[3]{\frac{35}{2} + \sqrt{\frac{35^2}{4} - \frac{18^3}{27}}} + \sqrt[3]{\frac{35}{2} - \sqrt{\frac{35^2}{4} - \frac{18^3}{27}}} \\ &= \sqrt[3]{\frac{35}{2} + \frac{19}{2}} + \sqrt[3]{\frac{35}{2} - \frac{19}{2}} \;=\; 3 + 2 = 5, \end{aligned}$$

aber auch die Lösungen

$$x_2 = 3\rho + 2\rho^2 = -2 + \rho \quad \text{und} \quad x_3 = 3\rho^2 + 2\rho = -3 - \rho.$$

(Es ist $\rho^2 + \rho + 1 = 0$!)

Es ist verblüffend, daß zwischen der Entdeckung der Lösungsmethoden für quadratische und für kubische Gleichungen drei Jahrtausende liegen, daß die Lösung für biquadratische Gleichungen fast zeitgleich mit der Lösung für kubische Gleichungen gefunden wurde, und zwar von LUDOVICO FERRARI. Beide Lösungen wurden von CARDANO in seinem Buch *Ars Magna de Regulis Algebraicis* (1545) veröffentlicht.

Mit demselben Trick wie im Falle der quadratischen und kubischen Gleichungen kann man bei allen Polynomgleichungen $f(x) = x^n + f_1 x^{n-1} + \ldots + f_n = 0$ mit der Substitution $y = x + \frac{f_1}{n}$ den Term vom Grad $n-1$ eliminieren:

$$f(x) = F(y) = y^n + (f_2 - \tfrac{n-1}{2n} f_1^2) y^{n-2} + \ldots$$

Bei einer biquadratischen Gleichungen kann man also stets den Term vom Grad 3 eliminieren. Wir gehen gleich von der normalisierten Form

$$x^4 = ax^2 + bx + c \tag{1.5}$$

aus und geben zunächst eine leicht modifizierte Form des ursprünglichen Arguments von FERRARI, natürlich ausgedrückt in der modernen symbolischen Sprache, die FERRARI noch nicht zur Verfügung stand. Die Idee besteht darin, auf beiden Seiten einen quadratischen Ausdruck so zu addieren, daß jede Seite für sich ein Quadrat ist:

$$x^4 + 2px^2 + p^2 = (a + 2p)x^2 + bx + (c + p^2). \tag{1.6}$$

Dabei ist p ein Parameter, über dessen Wert noch zu verfügen ist. Die linke Seite ist offensichtlich $(x^2 + p)^2$. Die rechte Seite ist genau dann ein Quadrat, wenn die Diskriminante des quadratischen Polynoms verschwindet, d.h. wenn

$$4(a + 2p)(c + p^2) - b^2 = 0. \tag{1.7}$$

Dies ist eine kubische Gleichung

$$(2p)^3 + a(2p)^2 + 4c(2p) + (4ac - b^2) = 0 \tag{1.8}$$

für den Parameter p. Diese Gleichung nennt man eine *kubische Resolvente* für die Ausgangsgleichung. Wenn man nun eine Nullstelle p der kubischen Resolventen bestimmt hat und in (1.6) einsetzt, kann man auf beiden Seiten die Wurzel ziehen und erhält

$$x^2 + p = \pm(\sqrt{a + 2p}\, x + \sqrt{c + p^2}),$$

wobei die beiden Wurzeln so zu wählen sind, daß sie die Nebenbedinung

$$2\sqrt{a + 2p}\sqrt{c + p^2} = b$$

erfüllen, was nach Wahl von p stets möglich ist. Auf diese Weise ist die Lösung der biquadratischen Gleichung (1.5) auf das Lösen einer kubischen und mehrerer quadratischer Gleichungen zurückgeführt.

DESCARTES löst die Gleichung

$$x^4 - ax^2 - bx - c = 0$$

mit dem Ansatz

$$x^4 - ax^2 - bx - c = (x^2 - ux + v)(x^2 + ux + w)$$

mit den Unbestimmten u, v, w. Durch Koeffizientenvergleich erhält man die Bedingungsgleichungen

$$\begin{aligned} -a &= -u^2 + v + w \\ -b &= u(v - w) \\ -c &= vw \end{aligned}$$

Aus der ersten Gleichung kann man w eliminieren: $w = -a + u^2 - v$. Wenn $b = 0$, ist die Ausgangsgleichung eine quadratische Gleichung in x^2 und kann sofort mit den üblichen Mitteln gelöst werden. Wir nehmen deshalb ohne Einschränkung an, daß $b \neq 0$ ist. Falls das Gleichungssystem also überhaupt eine Lösung hat, muß jedenfalls auch $u \neq 0$ gelten, und man kann aus der ersten und der zweiten Gleichung auch v elimineren:

$$v = \frac{u^3 - au - b}{2u}, \quad w = \frac{u^3 - au + b}{2u}.$$

Die dritte Bedingungsgleichung liefert dann nach Multiplikation mit dem Hauptnenner

$$\begin{aligned} 0 &= (u^3 - au - b)(u^3 - au + b) + 4cu^2 \\ &= u^6 - 2au^4 + (a^2 + 4c)u^2 - b^2. \end{aligned}$$

Dies ist eine kubische Gleichung für u^2, die im Übrigen durch eine einfache Substitution in (1.8) übergeht.

Ein anderer sehr eleganter Ansatz geht auf EULER zurück: Man setzt

$$x = u + v + w$$

mit drei Unbestimmten u, v, w. Zur Abkürzung führen wir die Bezeichnungen

$$A = u^2 + v^2 + w^2, \quad B = u^2v^2 + v^2w^2 + w^2u^2, \quad T = uvw$$

ein. Dann gilt

$$x^2 = (u^2 + v^2 + w^2) + 2(uv + vw + wu) = A + 2(uv + vw + wu)$$

und

$$\begin{aligned} (x^2 - A)^2 &= 4(uv + vw + wu)^2 \\ &= 4 \cdot \big((u^2v^2 + v^2w^2 + w^2u^2) + 2(u^2vw + v^2uw + w^2uv)\big) \\ &= 4B + 8(u + v + w)uvw \;=\; 4B + 8Tx. \end{aligned}$$

Zusammengenommen heißt das

$$x^4 = 2Ax^2 + 8Tx + (4B - A^2).$$

Substituiert man diesen Ausdruck in (1.5),

$$(2A - a)x^2 + (8T - b)x + (4B - A^2 - c) = 0,$$

so ist diese Gleichung offenbar identisch erfüllt, wenn u, v und w so gewählt werden, daß

$$A = \frac{1}{2}a, \quad T = \frac{1}{8}b, \quad B = \frac{1}{4}c + \frac{1}{16}a^2.$$

Konstruktionsgemäß sind u^2, v^2 und w^2 die Nullstellen des kubischen Polynoms

$$\begin{aligned}(Y-u^2)(Y-v^2)(Y-w^2)&\\ &= Y^3-(u^2+v^2+w^2)Y^2+(u^2v^2+v^2w^2+w^2u^2)Y-u^2v^2w^2\\ &= Y^3-AY^2+BY-T^2\\ &= Y^3-\frac{1}{2}aY^2+\left(\frac{1}{4}c+\frac{1}{16}a^2\right)Y-\frac{1}{64}b^2.\end{aligned}$$

Bezeichnen also λ_1, λ_2, λ_3 die drei Nullstellen dieses Polynoms, so ist

$$x=u+v+w \quad \text{mit} \quad u=\pm\sqrt{\lambda_1}, v=\pm\sqrt{\lambda_2}, w=\pm\sqrt{\lambda_3}$$

eine Lösung der biquadratischen Gleichung (1.5), wobei die Vorzeichen der Wurzeln so zu wählen sind, daß die Nebenbedingung

$$uvw=T=\frac{1}{8}b$$

erfüllt ist. Von den $2^3=8$ denkbaren Vorzeichenwahlen scheiden also 4 aus, und die übrigen liefern vier Lösungen x_1, x_2, x_3, x_4. Im Ausnahmefall, daß $b=0$, verschwindet eine Nullstelle, etwa λ_3, und die vier Lösungen der biquadratischen Gleichung ergeben sich aus $\pm\sqrt{\lambda_1}\pm\sqrt{\lambda_2}$.

In der Folgezeit haben viele Mathematiker vergeblich versucht, auch für Gleichungen vom Grad 5 Lösungsformeln zu finden, bis sich das Verständnis durchgesetzt hat, daß es solche Lösungsformeln vielleicht nicht gibt. Daß es Lösungsformeln für Polynomgleichungen vom Grad ≥ 5 nicht geben kann, wurde 1799 von RUFFINI (mit unvollständigem Argument) und schließlich 1824 von NIELS ABEL bewiesen. Allerdings bedeutet dies nicht, daß es nicht Gleichungen vom Grad 5 gibt, deren Nullstellen man durch Wurzelausdrücke angeben kann. So hat ALEXANDRE-THÉOPHILE VANDERMONDE 1771 gezeigt, daß die Zahlen $2\cos\frac{2\pi k}{11}$, $k=1,\ldots,5$, die die Nullstellen des Polynoms $x^5+x^4-4x^3-3x^2+3x+1$ sind, durch iterierte Wurzelausdrücke angegeben werden können. Es entsteht so das Problem zu bestimmen, für welche Gleichungen man eine oder alle reellen oder komplexen Nullstellen durch iterierte Wurzelausdrücke schreiben kann. Diese Frage wurde von EVARISTE GALOIS 1832 auf ein kombinatorisches Problem zurückgeführt, das in der weiteren Entwicklung zur Entstehung der modernen Gruppentheorie führte. Ich empfehle die Bücher von Tignol *Galois' theory of algebraic equations* und van der Waerden *A history of Algebra* als vertiefende Lektüre zur Entstehungsgeschichte des Gruppenbegriffs.

§2. Ringe

2.1. Grundbegriffe.

Definition 2.1. — Ein *Ring* ist eine Menge A mit zwei Verknüpfungen $+$ und $\cdot$ mit den folgenden Eigenschaften:

(1) $(A, +)$ ist eine kommutative Gruppe. Das Neutralelement der Addition wird mit 0 bezeichnet, das additive Inverse zu a mit $-a$.
(2) Die Multiplikation $\cdot$ ist assoziativ.
(3) Es gelten die Distributivgesetze $(a + b)c = ac + bc$ und $a(b + c) = ab + ac$ für alle $a, b, c \in A$.

Ein Element $1 \in A$ heißt *Einselement*, wenn $1 \cdot a = a = a \cdot 1$ für alle $a \in A$. Falls ein Einselement existiert, ist es eindeutig bestimmt.

Der Nullring 0 ist die Menge $\{0\}$ mit den trivialen Verknüpfungen $0+0 = 0 \cdot 0 = 0$. Im Nullring ist 0 zugleich Null- und Einselement.

Aus den Ringaxiomen folgt, daß $0 \cdot a = 0 = a \cdot 0$ für alle $a \in A$. In der Regel sollten keine Mißverständnisse daraus erwachsen, daß wir alle Nullelemente in allen Ringen mit 0 und alle Einselemente mit 1 bezeichnen. Wenn es darauf ankommt, schreiben wir 0_A und 1_A, um zu betonen, daß es sich um die Neutralelemente der Addition und der Multiplikation in A handelt.

Definition 2.2. — Ein Ring A heißt *kommutativ*, wenn es ein Einselement gibt und die Multiplikation kommutativ ist.

Definition 2.3. — Es sei A ein Ring mit Einselement $1 \neq 0$. Ein Element $b \in A$ ein *Rechtsinverses* von $a \in A$ und a ein *Linksinverses* von b, falls $ab = 1$. Ein Ring A ist ein *Schiefkörper*, wenn jedes von 0 verschiedene Element ein Rechtsinverses besitzt. In diesem Falle hat jedes Element $a \neq 0$ auch ein Linksinverses, und Links- und Rechtsinverse sind gleich und werden mit a^{-1} bezeichnet. Ein kommutativer Schiefkörper heißt *Körper*.

Definition 2.4. — Eine Abbildung $f : A \to B$ von Ringen ist ein Ringhomomorphismus, wenn $f(a + b) = f(a) + f(b)$ und $f(ab) = f(a)f(b)$. Wenn A und B kommutative Ringe sind, wird zusätzlich vorausgesetzt, daß $f(1_A) = 1_B$.

Weil jeder Ringhomomorphismus $f : A \to B$ auch ein Gruppenhomomorphismus der zugrundeliegenden additiven Gruppen ist, gilt stets $f(0_A) = 0_B$ und $f(-a) = -f(a)$ für alle $a \in A$.

Man definiert für alle $a \in A$ und $n \in \mathbb{Z}$ induktiv $0_{\mathbb{Z}} \cdot a = 0_A$, $(n+1) \cdot a = n \cdot a + a$, falls $n \geq 0$, und $n \cdot a = -((-n) \cdot a)$, falls $n < 0$. Für jedes a ist dann die Abbildung $\mathbb{Z} \to (A, +)$, $n \mapsto na$, ein Gruppenhomomorphismus. Wenn es ein Einselement gibt, ist die Abbildung

$$\mathbb{Z} \to A, n \mapsto n_A := n \cdot 1_A,$$

ein Ringhomomorphismus.

Ähnlich definiert man für $n \in \mathbb{N}$ und $a \in A$ rekursiv Potenzen $a^1 := a$, $a^{n+1} := a^n \cdot a$ und, falls A ein Einselement besitzt, $a^0 := 1$. Es gelten dann die Rechenregeln $a^{n+m} = a^n \cdot a^m$ und $(a^n)^m = a^{nm}$ für alle $n, m \in \mathbb{N}$ bzw. $\mathbb{N}_0$.

Definition 2.5. — Es sei A ein kommutativer Ring.

(1) Ein Element $a \in A$ ist invertierbar oder eine *Einheit*, wenn es ein $b \in A$ mit $ab = 1$ gibt. Die Einheiten in A bilden eine Gruppe mit der Ringmultiplikation als Verknüpfung, die mit $A^\times$ bezeichnete *Einheitengruppe* von A.
(2) $a \in A$ ist ein *Nullteiler*, wenn es ein $b \in A \setminus \{0\}$ mit $ab = 0$ gibt. A ist nullteilerfrei oder ein *Integritätsbereich*, wenn $A \neq 0$ und wenn 0 der einzige Nullteiler in A ist. In einem

Integritätsbereich gilt für $a, b, c \in A$ mit $c \neq 0$ die Kürzungsregel: $ac = bc \quad \Rightarrow a = b$.

(3) $a \in A$ ist *nilpotent*, falls $a^n = 0$ für ein $n \in \mathbb{N}$.

(4) $e \in A$ ist *idempotent*, falls $e^2 = e$.

2.2. **Ideale und Faktorringe.**

Definition 2.6. — Es sei A ein kommutativer Ring.

(1) Eine nichtleere Teilmenge $I \subset A$ ist ein *Ideal*, wenn für alle $x, x' \in I$ und alle $a \in A$ gilt: $x + x' \in I$ und $ax \in I$.

(2) Für jedes $a \in A$ ist die Menge $(a) = \{ra \mid r \in A\}$ ein Ideal, das von a erzeugte *Hauptideal*. In jedem Ring gibt es das Nullideal $(0) = \{0\}$ und das Einsideal $(1) = A$. Schließlich ist A ein *Hauptidealring*, wenn jedes Ideal in A ein Hauptideal ist.

(3) Für $S \subset A$ ist $(S) := \{a_1 s_1 + \ldots + a_n s_n \mid n \in \mathbb{N}_0,\ a_i \in A,\ s_i \in S\}$ das von S erzeugte Ideal. (S) ist auch der Durchschnitt aller Ideale in A, die S enthalten. Ist $S = \{s_1, \ldots, s_n\}$, schreibt man $(s_1, \ldots, s_n) := (S)$. Ein Ideal I ist *endlich erzeugt*, wenn es $s_1, \ldots, s_n \in A$ mit $I = (s_1, \ldots, s_n)$ gibt. Der Ring A heißt *noethersch*[2], wenn jedes Ideal endlich erzeugt ist.

Für jeden Ringhomomorphismus $\varphi : A \to A'$ von kommutativen Ringen ist der Kern

$$\ker(\varphi) = \varphi^{-1}(0)$$

ein Ideal in A. Das Bild eines Ringhomomorphismus ist ein Unterring in A', aber im Allgemeinen kein Ideal. Ist $\{I_s\}_{s \in S}$ eine Familie von Ideal in A, so sind auch der Durchschnitt $\bigcap_{s \in S} I_s$ und die Summe $\sum_{s \in S} I_s := \big(\cup_{s \in S}\ I_s\big)$ Ideale in A. Und sind I_1 und I_2 Ideale in A, so ist auch $I_1 I_2 := \big(\{x_1 x_2 \mid x_i \in I_i\}\big)$ ein Ideal in A.

Definition 2.7. — Es sei nun A ein kommutativer Ring mit einem Ideal I. Nach einer von Gauß[3] eingeführten Bezeichnungsweise sagt man, zwei Elemente $a, b \in A$ seien *kongruent modulo* I, in Zeichen

$$a \equiv b \bmod I,$$

wenn $a + I = b + I$, oder äquivalent, wenn $a - b \in I$. Für jedes $a \in A$ bezeichne $\overline{a} := a + I$ die Restklasse von a modulo I, und A/I die Menge aller Restklassen. Die Abbildung $\pi : A \to A/I$, die jedes $a \in A$ auf seine Restklasse $\overline{a} = a + I$ schickt, heißt kanonische Projektion.

Lemma 2.8 — *Es gibt genau eine Ringstruktur auf A/I, bezüglich der π ein Ringhomomorphismus wird, nämlich*

$$\overline{a} + \overline{b} := \overline{a + b}, \quad \overline{a} \cdot \overline{b} := \overline{ab}.$$

Beweis. Es ist klar, daß die Verknüpfungen nur so definiert werden können, weil π surjektiv ist. Man zeigt dann, daß die so definierten Verknüpfungen wohldefiniert sind. Für die Wohldefiniertheit der Addition wird nur benutzt, daß I eine additive Untergruppe ist. Für die Wohldefiniertheit der Multiplikation wird die Idealeigenschaft gebraucht: Es seien a, a' und b, b' Elemente aus A mit $a + I = a' + I$ und $b + I = b' + I$, also $a' = a + x$ und $b' = b + y$ mit $x, y \in I$. Dann hat man

$$a'b' = (a + x)(b + y) = ab + (ay + xb + xy) \in ab + I.$$

Daß die Ringaxiome in A/I erfüllt sind, folgt dann automatisch, weil π surjektiv ist und die Verknüpfungen erhält und weil A ein Ring ist. □

[2] Emmy Noether, ⋆23. März 1882 in Erlangen, †14. April 1935. Begründerin der modernen Algebra.

[3] Carl Friedrich Gauß, ⋆30. April 1777 in Braunschweig, †23. Februar 1855 in Göttingen.

Definition 2.9. — Es sei A ein kommutativer Ring und $I \subset A$ ein Ideal. Der Ring A/I heißt *Restklassenring* von A bezüglich I.

Satz 2.10 (Universelle Eigenschaft des Restklassenrings) — *Es sei A ein kommutativer Ring, $I \subset A$ ein Ideal und $\pi : A \to A/I$ die kanonische Projektion. Zu einem Ringhomomorphismus $\varphi : A \to B$ gibt es genau dann einen Ringhomomorphismus $\overline{\varphi} : A/I \to B$ mit $\varphi = \overline{\varphi} \circ \pi$, wenn $I \subset \ker(\varphi)$. In diesem Falle ist $\overline{\varphi}$ eindeutig bestimmt.*

Man sagt, φ faktorisiere über π und $\overline{\varphi}$.

Beweis. Falls ein solches $\overline{\varphi}$ existiert, so ist es offensichtlich eindeutig bestimmt, weil π surjektiv ist. Außerdem gilt in diesem Falle für jedes $x \in I$, daß $\varphi(x) = \overline{\varphi}(\pi(x)) = \overline{\varphi}(0) = 0$, also $I \subset \ker(\varphi)$. Es gelte nun umgekehrt $I \subset \ker(\varphi)$. Wir definieren $\overline{\varphi}(\pi(a)) := \varphi(a)$. Es genügt zu zeigen, daß $\overline{\varphi}$ wohldefiniert ist. Für $a, b \in A$ mit $\pi(a) = \pi(b)$ folgt $a - b \in I \subset \ker(\varphi)$, also $\varphi(a) - \varphi(b) = \varphi(a - b) = 0$. □

Definition 2.11. — Es sei A ein kommutativer Ring.

(1) Ein Ideal $\mathfrak{p} \subset A$ ist ein *Primideal*, wenn $\mathfrak{p} \neq A$, und wenn für beliebige Ringelemente $a, b \in A$ aus $ab \in \mathfrak{p}$ folgt: $a \in \mathfrak{p}$ oder $b \in \mathfrak{p}$.
(2) Die Menge $\mathrm{Spec}(A) := \{\mathfrak{p} \mid \mathfrak{p} \text{ ist ein Primideal}\}$ heißt das Primspektrum oder kurz das *Spektrum* von A.
(3) Ein Ideal $\mathfrak{m} \subset A$ ist ein *maximales Ideal*, wenn $\mathfrak{m} \neq A$, und wenn für jedes Ideal I mit $\mathfrak{m} \subset I$ gilt $\mathfrak{m} = I$ oder $I = A$.

Lemma 2.12 — *Es sei A ein kommutativer Ring und $\mathfrak{p} \subset A$ ein Ideal.*

(1) *$\mathfrak{p}$ ist ein Primideal $\Leftrightarrow$ $A/\mathfrak{p}$ ist ein Integritätsbereich.*
(2) *$\mathfrak{p}$ ist ein maximales Ideal $\Leftrightarrow$ $A/\mathfrak{p}$ ist ein Körper.*

Beweis. Zu 1: $\mathfrak{p}$ ist genau dann ein Primideal, wenn aus $ab \in \mathfrak{p}$ und $a \notin \mathfrak{p}$ folgt $b \in \mathfrak{p}$. Das ist äquivalent zu der Aussage: Wenn $\overline{ab} = 0 \in A/\mathfrak{p}$ und $\overline{a} \neq 0 \in A/\mathfrak{p}$, so ist $\overline{a} = 0$. Aber das ist genau die Definition der Nullteilerfreiheit von $A/\mathfrak{p}$.
Zu 2: $\mathfrak{p}$ ist genau dann ein maximales Ideal, wenn für alle $x \in A \setminus \mathfrak{p}$ gilt $\mathfrak{p} + (x) = A$ oder äquivalent: $1 - xy \in \mathfrak{p}$ für ein $y \in A$. Das ist äquivalent zu der Aussage: Für alle $\overline{x} \in (A/\mathfrak{p}) \setminus \{0\}$ existiert ein $y \in A$ mit $\overline{xy} = 1 \in A/\mathfrak{p}$. Und das bedeutet genau, daß $A/\mathfrak{p}$ ein Körper ist. □

Satz 2.13 — *Es sei A ein kommutativer Ring und $I \subsetneq A$ ein echtes Ideal. Dann gibt es ein maximales Ideal $\mathfrak{m} \subset A$ mit $I \subset \mathfrak{m}$.*

Beweis. Beweis durch transfinite Induktion: Es sei X die Menge aller echten Ideale $J \subsetneq A$ mit $I \subset J$. Da X das Ideal I enthält, ist X nicht leer. Die Inklusionsordnung ist eine Halbordnung auf X. Jede nichtleere Kette $K \subset X$ besitzt die obere Schranke: Es sei nämlich $J_K := \bigcup_{J \in K} J$. Offensichtlich enthält J_K das Ideal I. Das Ideal J_K ist nicht der ganze Ring, denn andernfalls läge 1 in J_K, und definitionsgemäß müßte es ein $J \in K$ mit $1 \in J$ geben. Deshalb liegt J_K in der Menge X, und nach der Definitions von J_K ist klar, daß J_K eine obere Schrankte von K ist. Damit ist gezeigt, daß X induktiv geordnet ist. Nach dem Zornschen Lemma gibt es ein maximales Element $\mathfrak{m} \in X$. Für jedes $a \in A$ folgt nun: $\mathfrak{m} + (a) = A$ oder $\mathfrak{m} + (a) \in X$. Wegen der Maximalität von $\mathfrak{m}$ muß im zweiten Fall $\mathfrak{m} = \mathfrak{m} + (a)$ gelten. Es gibt also keine Ideale, die echt zwischen $\mathfrak{m}$ und A liegen. □

Eine unmittelbare Folgerung daraus ist, daß jeder Ring $A \neq 0$ wenigstens ein maximales Ideal und damit wenigstens ein Primideal besitzt, d.h. $\mathrm{Spec}(A) = \emptyset$ genau dann, wenn $A = 0$.

2.3. **Lokalisierung und Quotientenringe.**

Weil in den ganzen Zahlen die multiplikativen Inversen fehlen, führt man in der elementaren Arithmetik die rationalen Zahlen ein. Allgemeiner konstruiert man zu einem Integritätsbereich A seinen Quotientenkörper $Q(A)$, in dem alle Elemente aus $A \setminus \{0\}$ invertierbar sind. *Lokalisierung* ist ein Verfahren, zu einem gegebenen kommutativen Ring A einen neuen Ring zu konstruieren, in dem eine vorgegebene Menge von Elementen invertierbar wird.

Definition 2.14. — Es sei A ein kommutativer Ring. Eine Teilmenge $S \subset A$ ist *multiplikativ abgeschlossen*, wenn $1 \in S$ und wenn $f_1 f_2 \in S$ für alle $f_1, f_2 \in S$.

Beispiele 2.15. — Es sei A ein kommutativer Ring.

(1) Für jedes $f \in A$ ist $\{1, f, f^2, \ldots\}$ multiplikativ abgeschlossen.
(2) Für ein Ideal $I \subset A$ ist $A \setminus I$ genau dann multiplikativ abgeschlossen, wenn I ein Primideal ist.
(3) Ist A ein Integritätsbereich, so ist $A \setminus \{0\}$ multiplikativ abgeschlossen.

Es sei nun A ein kommutativer Ring und $S \subset A$ ein multiplikativ abgeschlossene Teilmenge. Wir betrachten auf der Menge $A \times S$ die folgende Relation:

$$(a, s) \sim (a', s') \quad :\Leftrightarrow \quad \text{es gibt ein } t \in S \text{ mit } tas' = ta's.$$

Lemma 2.16 — *Die Relation $\sim$ ist eine Äquivalenzrelation.*

Beweis. Reflexivität und Symmetrie sind offensichtlich. Zum Beweis der Transitivität seien Paare $(a, s) \sim (a', s') \sim (a'', s'')$ vorgegeben. Definitionsgemaß gibt es dann $u, t \in S$ mit $as't = a'st$ und $a's''u = a''s'u$. Nun folgt:

$$as''(s'tu) = (as't)(s''u) = (a'st)(s''u) = (a's''u)(st) = (a''s'u)(st) = (a''s)(s'tu).$$

Weil S multiplikativ ist, ist $s'tu \in S$. Definitionsgemäß folgt $(a, s) \sim (a'', s'')$. □

Wenn A ein Integritätsbereich ist und $0 \notin S$, kann wegen der Gültigkeit der Kürzungsregel in der Definition der Relation stets $t = 1$ gewählt werden. Würde man für einen beliebigen kommutativen Ring diese Definition wählen, also

$$(a, s) \approx (a', s') \quad :\Leftrightarrow \quad as' = a's$$

setzen, so stößt man bei dem Versuch, die Transitivität zu beweisen, auf das folgende Problem:

$$(as'')s' = (as')s'' = (a's)s'' = (a's'')s = (a''s')s = (a''s)s'.$$

Im Ring der ganzen Zahlen und allgemeiner in einem Integritätsbereich kann mit der Kürzungsregel jetzt auf $as'' = a''s$ schließen, in einem allgemeinen kommutativen Ring nicht. Das ist der Grund für den merkwürdigen zusätzlichen Faktor in der Definition von $\sim$.

Wir bezeichnen mit $S^{-1}A := A \times S/\sim$ den Quotienten nach der Relation $\sim$ und mit $\frac{a}{s}$ die Klasse von (a, s).

Satz 2.17 — *Auf $S^{-1}A$ wird durch*

$$\frac{a}{s} + \frac{a'}{s'} := \frac{as' + a's}{ss'} \quad \text{und} \quad \frac{a}{s} \cdot \frac{a'}{s'} := \frac{aa'}{ss'}$$

eine Ringstruktur definiert. Die Abbildung $i : A \to S^{-1}A, a \mapsto a/1$, ist ein Ringhomomorphismus. $S^{-1}A$ ist genau dann der Nullring, wenn $0 \in S$. Der Homomorphismus i ist genau dann injektiv, wenn S keine Nullteiler enthält.

Beweis. Übung □

Der Ring $S^{-1}A$ oder genauer: die Abbildung $i : A \to S^{-1}A$ heißt Lokalisierung von A nach der Menge S. Im Ring $S^{-1}A$ ist das Bild $i(s) = s/1$ von $s \in S$ invertierbar: $i(s)^{-1} = 1/s$. Der Ring $S^{-1}A$ ist durch diese Eigenschaft charakterisiert:

Satz 2.18 (Universelle Eigenschaft der Lokalisierung) — *Es sei A ein kommutativer Ring, $S \subset A$ eine multiplikativ abgeschlossene Menge und $i : A \to S^{-1}A$ die zugehörige Lokalisierung. Ist $\varphi : A \to B$ ein Ringhomomorphismus in einen kommutativen Ring B mit $\varphi(S) \subset B^\times$, dann gibt es einen eindeutig bestimmten Ringhomomorphismus $\psi : S^{-1}A \to B$ mit $\varphi = \psi \circ i$.*

Beweis. Falls ψ existiert, muß wegen $\varphi(a) = \psi(a/1) = \psi(a/s)\psi(s/1) = \psi(a/s)\varphi(s)$ gelten: $\psi(a/s) = \varphi(a)\varphi(s)^{-1}$. Daher ist ψ jedenfalls eindeutig. Definiert man umgekehrt ψ auf diese Weise, dann ist ψ wohldefiniert und ein Homomorphismus. □

In den folgenden Fällen werden spezielle Bezeichnungen verwendet: A sei ein kommutativer Ring.

(1) Für $f \in A$ schreibt man $A_f := \{f^n \mid n \in \mathbb{N}_0\}^{-1}A$.
(2) Für ein Primideal $\mathfrak{p} \subset A$ setzt man $A_\mathfrak{p} := (A \setminus \mathfrak{p})^{-1}A$.
(3) Die Menge $NNT(A)$ der Nichtnullteiler von A ist multiplikativ abgeschlossen. Die zugehörige Lokalisierung $Q(A) := \mathrm{NNT}(A)^{-1}A$ heißt der totale Quotientenring von A. Wenn A ein Integritätsbereich ist, ist $Q(A)$ ein Körper, der sogenannte Quotientenkörper von A.

Beispiele 2.19. — 1. Der Quotientenkörper von $\mathbb{Z}$ ist der Körper der rationalen Zahlen $Q(\mathbb{Z}) = \mathbb{Q}$.
2. $Q(\mathbb{Z}[i]) = \mathbb{Q}(i) := \{a + bi \mid a, b \in \mathbb{Q}\} \subset \mathbb{C}$.
3. Es sei K ein Körper. Der Polynomring $K[X]$ ist ein Integritätsbereich. Der Körper

$$K(X) := Q(K[X])$$

heißt Körper der *rationalen Funktionen* (mit Koeffizienten in K). Im Falle $K = \mathbb{R}$ kann man die formalen Brüche $p(X)/q(X)$ als Funktionen $f : \mathbb{R} \setminus D \to \mathbb{R}$, die außerhalb der Nullstellenmenge D des Nenners definiert sind, auffassen.
4. Es sei $p \in \mathbb{N}$ eine Primzahl und $(p) \subset \mathbb{Z}$ das zugehörige Primideal. Man unterscheide die Lokalisierungen:

$$\mathbb{Z}_p := \left\{ \frac{a}{s} \in \mathbb{Q} \;\middle|\; \text{der einzige Primfaktor von } s \text{ ist } p. \right\}$$

und

$$\mathbb{Z}_{(p)} := \left\{ \frac{a}{s} \in \mathbb{Q} \;\middle|\; \text{kein Primfaktor von } s \text{ ist } p. \right\}$$

Insbesondere ist $\mathbb{Z}_p \cap \mathbb{Z}_{(p)} = \mathbb{Z}$. Der Umgang mit diesen Bezeichnungen wird dadurch erschwert, daß in vielen mathematischen Texten $\mathbb{Z}_p$ für den Restklassenring $\mathbb{Z}/p$ verwendet wird, und in wieder anderen Texten $\mathbb{Z}_p$ den Ring der ganzen p-adischen Zahlen bezeichnet. Da hilft nur: Auf den Kontext achten!

2.4. **Aufgaben.**

Aufgabe 2.20. — Es seien $A_1, \ldots, A_n$ Ringe. Das kartesische Produkt $A = A_1 \times \ldots \times A_n$ mit den komponentenweise definierten Verknüpfungen

$$(a + b)_i = a_i + b_i, \quad (ab)_i = a_i b_i \text{ für alle } i = 1, \ldots, n$$

ist ein Ring. A besitzt genau dann eine Eins bzw. ist kommutativ, wenn dies für alle Faktoren A_1,…,A_n gilt.

Aufgabe 2.21. — Es sei A ein kommutativer Ring mit 1 und einem idempotenten Element e_1. Man zeige:

(1) $e_2 := 1 - e_1$ ist ebenfalls idempotent, und $e_1 e_2 = 0$.
(2) Die Teilmenge $A_i := e_i A = \{e_i a \mid a \in A\}$, $i = 1, 2$, ist ein Unterring mit Einselement e_i.
(3) Die Abbildung $A \to A_1 \times A_2$, $a \mapsto (e_1 a, e_2 a)$ ist ein Ringisomorphismus.

Aufgabe 2.22. — Es sei A ein Ring mit nilpotenten Elementen f und g. Wenn f und g vertauschen, d.h. wenn $fg = gf$, so ist auch $f + g$ nilpotent.

§3. Polynomringe

3.1. Polynomringe in einer Variablen.

Es sei A ein kommutativer Ring. Wir betrachten auf der Menge

$$A^{(\mathbb{N}_0)} = \{(a_0, a_1, \ldots) \mid a_i \in A, \text{ und } a_i = 0 \text{ für alle hinreichend großen } i.\}$$

aller endlichen Folgen in A die folgenden Verknüpfungen:

$$(a+b)_n := a_n + b_n \qquad \text{und} \qquad (ab)_n := \sum_{k=0}^{n} a_k b_{n-k}.$$

Man sieht leicht, daß $a+b$ und ab tatsächlich endliche Folgen sind, so daß $+$ und $\cdot$ wirklich Verknüpfungen auf $A^{(\mathbb{N}_0)}$ sind, und ebenso, daß $(A^{(\mathbb{N}_0)}, +, \cdot)$ ist ein kommutativer Ring mit Nullelement $0 := (0, 0, \ldots)$ und Einselement $1 := (1, 0, 0, \ldots)$ ist. Genauer ist die Abbildung

$$i : A \mapsto A^{(\mathbb{N}_0)}, \quad a \mapsto (a, 0, 0, \ldots)$$

ein injektiver Ringhomomorphismus. Wir identifizieren deshalb jedes $a \in A$ mit seinem Bild in A und fassen A als Unterring von $A^{(\mathbb{N}_0)}$ auf. Es bezeichne nun

$$X := (0, 1, 0, 0, \ldots).$$

Dann ist die Potenz X^m die Folge, die eine einzige 1 an der m-ten Stelle und sonst nur Nulleinträge hat, wenn man die Folgenglieder beginnend mit dem Index 0 zählt. Tatsächlich gilt für beliebige Elemente aus $A^{(\mathbb{N}_0)}$:

$$(a_0, a_1, a_2, \ldots) \quad = \quad a_0 + a_1 X + a_2 X^2 + \ldots,$$

wobei die Summe auf der rechten Seite endlich ist, weil nur endlich viele Folgenterme $\neq 0$ sind. Üblicherweise schreibt man

$$A[X] := (A^{(\mathbb{N}_0)}, +, \cdot)$$

für diesen Ring. Der Name X für die angegebene Folge ist natürlich beliebig austauschbar. Elemente in $A[X]$ heißen *Polynome* in der Unbestimmten X mit Koeffizienten in A. Dieser *Polynomring* hat die folgenden wichtigen Strukturmerkmale: Einen Ringhomomorphismus $i : A \to A[X]$ und ein ausgezeichnetes Element $X \in A[X]$. Er ist durch die folgende universelle Eigenschaft charakterisiert:

Satz 3.1 (Universelle Eigenschaft des Polynomrings) — *Es sei B ein Ring mit Eins und $\psi : A \to B$ ein Ringhomomorphismus mit $\psi(1_A) = 1_B$. Zu jedem $\alpha \in B$, das mit allen Elementen aus dem Bild $\psi(A)$ kommutiert, gibt es genau einen Ringhomomorphismus $\Psi : A[X] \to B$ mit $\Psi(a) = \psi(a)$ für alle $a \in A$ und $\Psi(X) = \alpha$.*

Beweis. Da jedes Polynom eine Linearkombination aus Potenzen von X mit Koeffizienten aus A ist, ist ein Ringhomomorphismus auf $A[X]$ vollständig bestimmt, wenn man seine Werte auf A und auf X kennt. Damit ist Ψ in jedem Falle eindeutig bestimmt und muß wie folgt aussehen:

$$\Psi((a_0, a_1, a_2, \ldots)) := \sum_{n=0}^{\infty} \psi(a_k)\alpha^k.$$

Es bleibt zu verifizieren, daß die so definierte Abbildung ein Homomorphismus ist. Dabei ist klar, daß Ψ additiv ist, und die Null- und Einselemente jeweils ineinander überführt werden. Es bleibt zu zeigen, daß Ψ auch multiplikativ ist. An dieser Stelle geht ein, daß α mit $\psi(A)$ vertauscht: Es seien

$a = (a_0, a_1, \ldots)$, $b = (b_0, b_1, \ldots)$ gegeben und $c = ab$ mit $c_n = \sum_{k=0}^{n} a_k b_{n-k}$. Dann gilt, weil alle Summen endlich sind und beliebig vertausch werden dürfen:

$$\begin{aligned}
\Psi(a)\Psi(b) &= \sum_{k=0}^{\infty} \psi(a_k)\alpha^k \sum_{\ell=0}^{\infty} \psi(b_\ell)\alpha^\ell \\
&= \sum_{k,\ell\geq 0} \psi(a_k)\alpha^k \psi(b_\ell)\alpha^\ell \\
&= \sum_{k,\ell\geq 0} \psi(a_k)\psi(b_\ell)\alpha^k \alpha\ell \\
&\quad \text{(weil } \psi \text{ ein Ringhomomorphismus ist)} \\
&= \sum_{k,\ell\geq 0} \psi(a_k b_\ell)\alpha^{k+\ell} \\
&= \sum_{n\geq 0} \left(\sum_{k=0}^{n} \psi(a_k b_{n-k}) \right) \alpha^n \\
&= \sum_{n\geq 0} \psi(c_n)\alpha^n \;=\; \Psi(c).
\end{aligned}$$

□

Definition 3.2. — Der *Grad* eines nichtverschwindenden Polynoms $f = \sum_{k=0}^{n} f_k X^k$ ist

$$\deg(f) := \max\{k \mid f_k \neq 0\},$$

und $\deg(0) := 0$. Ist $f \in A[X]$ ein nichttriviales Polynom vom Grad d, dann heißt $\mathrm{Lt}(f) := f_d X^d$ der *Leitterm* von f, $\mathrm{Lc}(f) := f_d$ der *Leitkoeffizient* und $\mathrm{Lm}(f) := X^d$ das *Leitmonom*.

Für alle f, g gilt: $\deg(f+g) \leq \max\{\deg(f), \deg(g)\}$ und $\deg(fg) \leq \deg(f)\deg(g)$.

Satz 3.3 (Polynomdivision) — *Es sei $q = q_n X^n + \ldots + q_0$ ein Polynom vom Grad n, dessen Leitkoeffizient q_n eine Einheit in A ist. Dann gibt es zu jedem Polynom $f \in A[X]$ eindeutig bestimmte Polynome $p, r \in A[X]$ mit*

$$f = pq + r \quad \textit{und} \quad \deg(r) < \deg(q) \quad \textit{oder} \quad r = 0.$$

Beweis. Beweis durch vollständige Induktion nach $\deg(f)$. Wenn $\deg(f) < \deg(q)$, ist nichts zu zeigen: Man setzt $p = 0$ und $r = f$ und ist fertig. Es sei also $m := \deg(f) \geq n := \deg(q) \geq 0$ und die Behauptung für alle Polynome kleineren Grades schon gezeigt. Das Polynom $\frac{f_m}{q_n} X^{m-n} q$ hat denselben Leitterm wie f. Deshalb hat die Differenz

$$g = f - \frac{f_m}{q_n} X^{m-n} q$$

einen kleineren Grad als f und besitzt nach Induktionsannahme eine Darstellung $g = bq + r$ mit $\deg(r) < \deg(q)$. Dann hat man

$$f = g + \frac{f_m}{q_n} X^{m-n} q = (b + \frac{f_m}{q_n} X^{m-n})q + r.$$

Mit $p = b + \frac{f_m}{q_n} X^{m-n}$ folgt die Existenz der Darstellung durch Induktion. Zur Eindeutigkeit: Sind $f = pq + r = p'q + r'$ zwei Zerlegungen, so gilt $(p - p')q = r' - r$. Die rechte Seite ist entweder 0 oder hat Grad $< \deg(q)$, während die rechte Seite entweder 0 ist oder einen Grad $\geq \deg(q)$ hat, weil der Leitkoeffizient von q eine Einheit ist und deshalb $\deg((p-p')q) = \deg(p-p') + \deg(q)$ gilt. Aus dem Vergleich folgt: $r = r'$ und $pq = p'q$, und weil der Leitkoeffizient von q invertierbar ist, muß auch $p = p'$ gelten. □

3.2. **Polynomringe in mehreren Variablen.**

Auf analoge Weise können wir Polynomringe mit beliebig vielen Unbestimmten einführen: Dazu bezeichne S eine beliebige Indexmenge, im endlichen Falle etwa die Menge $\{1, \ldots, \ell\}$. Weiter sei $M := \mathbb{N}_0^{(S)}$ die Menge aller Folgen $(n_s)_{s\in S}$ mit $n_s \in \mathbb{N}_0$ und $n_s \neq 0$ für höchstens endlich viele $s \in S$. Durch die Verknüpfung

$$(n + n')_s := n_s + n'_s$$

wird M zu einem abelschen Monoid mit dem Nullelement $0 = (0)_{s\in S}$. Bezeichnet $e_s \in M$ für $s \in S$ die Folge $(e_s)_{s'} = \delta_{s,s'}$, so kann man jedes Element $n \in M$ in der Form $n = \sum_{s\in S} n_s e_s$ schreiben. In der formal unendlichen Summe sind nur endlich viele Summanden ungleich Null. Wir definieren auf

$$B := \{f : M \to A \mid f_m = 0 \text{ für fast alle } m \in M\}$$

wie folgt zwei Verknüpfungen:

$$(f + g)_m := f_m + g_m, \qquad (f \cdot g)_m = \sum_{m'+m''=m} f_{m'} \cdot g_{m''}.$$

Summe und Produkt sind wohldefiniert, weil man aus den endlich vielen Termen $\{m' \mid f_{m'} \neq 0\}$ und den endlich vielen Termen $\{m'' \mid g_{m''} \neq 0\}$ auch nur endlich viele Summen kombinieren kann. Man rechnet sofort nach, daß $(B, +, \cdot)$ ein kommutativer Ring ist. Speziell können wir für jedes $s \in S$ die Abbildung $X_s : M \to A$ mit der Eigenschaft $(X_s)_m = \delta_{e_s,m}$ betrachten, und für jedes $m \in M$ das Monom $X^m := \prod_{s\in S} X_s^{m_s}$. Mit diesen Bezeichnungen gilt nun $X^0 = 1$, $X^m \cdot X^{m'} = X^{m+m'}$ für alle $m, m' \in M$ und

$$f = \sum_{m\in M} f_m X^m \quad \text{für jedes } f \in B.$$

Außerdem ist die Abbildung $A \to B$, $a \mapsto aX^0$, ein injektiver Ringhomomorphismus. Wir identifizieren A mit dem Bild in B und bezeichnen mit $A[\{X_s\}_{s\in S}] := B$ den Polynomring in den Unbestimmten $\{X_s\}_{s\in S}$.

Satz 3.4 (Universelle Eigenschaft des Polynomrings) — *Es sei $\varphi : A \to R$ ein Ringhomomorphismus in einen kommutativern Ring R und $r = (r_s)_{s\in S}$ eine Folge von Elementen in R. Dann gibt es genau einen Ringhomomorphismus*

$$\Phi : A[\{X_s\}_{s\in S}] \longrightarrow R$$

mit $\Phi|_A = \varphi$ und $\Phi(X_s) = r_s$.

Beweis. Falls Φ existiert, muß Φ jedenfalls auf einem Polynom $f = \sum_n f_n X^n$ folgendermaßen aussehen:

$$\Phi(f) = \sum_n \varphi(f_n) \prod_s \Phi(X_s)^{n_s} = \sum_n \varphi(f_n) \prod_s r_s^{n_s}.$$

Definiert man umgekehrt eine Abbildung Φ auf diese Weise, so hat Φ alle gewünschten Eigenschaften. □

Der Ringhomomorphismus Φ heißt Auswertungsabbildung in b. Wir schreiben kurz $f(r) := \Phi(f)$. Die Aussage bleibt auch für nichtkommutative Ringe R mit Eins richtig, solange die Elemente r_s, $s \in S$, untereinander und mit $\varphi(A)$ vertauschen.

Meist hat man mit Polynomringen in endlich vielen Variablen zu tun, etwa

$$A[X_1, \ldots, X_\ell].$$

Wir verwenden dann die folgenden Multiindexbezeichnungen und schreiben

$$X^n := X_1^{n_1} \cdot \ldots \cdot X_\ell^{n_\ell}.$$

für einen Multigrad $n = (n_1, \ldots, n_\ell) \in \mathbb{N}_0^\ell$. Die Summe $|n| = n_1 + \ldots + n_s$ ist der Gesamtgrad oder Totalgrad des Monoms X^n. Jedes $f \in A[X_1, \ldots, X_\ell]$ schreibt sich nun in der Form

$$f = \sum_{n \in \mathbb{N}_0^\ell} f_n X^n,$$

wobei für fast alle $n \in \mathbb{N}_0^\ell$ der Koeffizient f_n verschwindet.

3.3. **(*) Potenzreihenringe.**

Es sei A ein kommutativer Ring. Auf der Menge

$$B := \{f : \mathbb{N}_0 \to A\}$$

wird durch $(f+g)_n := f_n + g_n$ und $(fg)_n := \sum_{d=0}^n f_d g_{n-d}$ die Struktur eines kommutativen Rings mit Eins definiert. Der Unterschied zur Konstruktion des Polynomrings besteht darin, daß von den Abbildungen f nicht verlangt wird, daß fast alle Werte 0 sind. Wir notieren Elemente in B durch

$$f = \sum_{n=0}^{\infty} f_n X^n.$$

Die Summe hat also zunächst lediglich den Charakter einer Notation. Wir werden erst später im Zusammenhang mit der Vervollständigung von Ringen sehen, daß die Summe tatsächlich wie in der Analysis als Grenzwert einer Summation von unendlich vielen Folgentermen aufgefaßt werden kann. Elemente in B heißen *(formale) Potenzreihen* mit Koeffizienten in A, und man nennt den Ring $A[[X]] := B$ den *Potenzreihenring*.

Satz 3.5 — *Eine Potenzreihe $f = \sum_{n=0}^\infty f_n X^n \in A[[X]]$ ist genau dann invertierbar, wenn der konstante Term f_0 eine Einheit in A ist.*

Beweis. Wir machen einen Ansatz $g = \sum_{m=0}^\infty g_m X^m$ für die Identität

$$1 = fg = (f_0 g_0) + (f_1 g_0 + f_0 g_1)X + (f_2 g_0 + f_1 g_1 + f_0 g_2)X^2 + \ldots.$$

Wenn f invertierbar ist, d.h. wenn ein solches g existiert, zeigt der Koeffizientenvergleich, daß $f_0 g_0 = 1$, d.h. f_0 ist eine Einheit in A. Es sei umgekehrt f_0 in A invertierbar und $g_0 := f_0^{-1}$. Für alle $m > 0$ soll die Identität

$$0 = f_0 g_m + f_1 g_{m-1} + \ldots + f_m g_0$$

bestehen. Wir können induktiv annehmen, daß Elemente $g_0, \ldots, g_{n-1}$ bereits so bestimmt sind, daß diese diese Identität für alle $m < n$ tatsächlich gilt. Aber weil f_0 invertierbar ist, kann man die Gleichung für $m = n$ nach g_n auflösen:

$$g_n := -g_0(f_1 g_{n-1} + \ldots + f_n g_0).$$

Mit dieser Wahl ist die Identität auch für $m = n$ richtig. Induktiv kann man so $g = f^{-1}$ konstruieren. □

In diesem Sinne gilt die aus der elementaren Analysis bekannte Identität

$$\frac{1}{1-X} = 1 + X + X^2 + \ldots$$

für die geometrische Reihe auch im Ring $A[[X]]$.

3.4. **Aufgaben.**

Aufgabe 3.6. — Es sei n eine natürliche Zahl und A ein kommutativer Ring, in dem n invertierbar ist. Dann gibt es zu jeder Potenzreihe $F \in A[[X]]$ mit $F \equiv 1 \bmod (X)$ eine eindeutig bestimmte Reihe G mit $G \equiv 1 \bmod (X)$ und $G^n = F$. Man schreibt $\sqrt[n]{F} := G$.

§4. Symmetrische Polynome

Es sei A ein kommutativer Ring. Ein Polynom $f \in A[x_1, \ldots, x_n]$ in n Unbestimmten $x_1, \ldots, x_n$ heißt *symmetrisch*, wenn es invariant unter allen Vertauschungen der Variablen ist. Das bedeutet, daß

$$f(x_1, \ldots, x_n) = f(x_{\pi(1)}, \ldots, x_{\pi(n)}) \tag{4.1}$$

für alle Permutationen $\pi \in S_n$. Es ist klar, daß Summen und Produkte von symmetrischen Polynomen wieder symmetrisch sind. Die symmetrischen Polynome bilden deshalb einen Unterring $A[x_1, \ldots, x_n]^{S_n}$ im Ring aller Polynome.

4.1. Symmetrische Polynome in zwei Variablen.

Wir betrachten zunächst den Fall von zwei Variablen x_1 und x_2. Die Polynome $s_1 = x_1 + x_2$ und $s_2 = x_1 x_2$ sind symmetrisch. Auch die Polynome $x_1^n + x_2^n$ sind für jedes $n \in \mathbb{N}$ symmetrisch. Man sieht sofort:

$$x_1^2 + x_2^2 = (x_1 + x_2)^2 - 2x_1x_2 = s_1^2 - 2s_2$$

und

$$x_1^3 + x_2^3 = (x_1 + x_2)^3 - 3x_1^2x_2 - 3x_1x_2^2 = (x_1 + x_2)^3 - 3(x_1 + x_2)(x_1x_2) = s_1^3 - 3s_1s_2.$$

Tatsächlich gilt allgemein:

Satz 4.1 — *Zu jedem symmetrischen Polynom $f(x, y)$ mit Koeffizienten in einem kommutativen Ring A gibt es ein Polynom $g \in A[z_1, z_2]$ mit der Eigenschaft, daß $f(x, y) = g(x + y, xy)$.*

Beweis. Ein Polynom

$$f(x, y) = f_0x^n + f_1x^{n-1}y + \ldots + f_ny^n$$

ist genau dann symmetrisch, wenn $f_0 = f_n$, $f_1 = f_{n-1}$ usw. Man kann deshalb das Polynom folgendermaßen zusammenfassen:

$$f(x, y) = f_0(x^n + y^n) + f_1(xy)(x^{n-2} + y^{n-2}) + \ldots$$

wobei der letzte Term $f_m(xy)^m$ bzw. $f_m(xy)^m(x + y)$ ist je nachdem, ob $n = 2m$ gerade oder $n = 2m + 1$ ungerade ist. Die Aufgabe $f(x, y)$ als Polynom in $x + y$ und xy zu schreiben, wird also darauf zurückgeführt, dies für die Polynome $x^n + y^n$ zu tun. Nun gilt:

$$x^n + y^n = (x + y)(x^{n-1} + y^{n-1}) - xy(x^{n-2} + y^{n-2}).$$

Induktiv hat man das Problem damit auf die trivialen Fälle $x^1 + y^1$ und $x^0 + y^0$ zurückgeführt. □

Palindromische Gleichungen — Man nennt ein Polynom

$$a(x) = a_nx^n + a_{n-1}x^{n-1} + \ldots + a_1x + a_0 \in \mathbb{C}[x]$$

palindromisch, wenn $a_i = a_{n-i}$ für alle $i = 0, \ldots, n$, d.h. wenn die Koeffizienten symmetrisch zur Mitte des Polynoms sind.

Satz 4.2 — *Gleichungen der Form $a(x) = 0$ mit einem palindromischen Polynom lassen sich immer auf Gleichungen kleineren Grades und ein quadratisches Polynom zurückführen.*

Dazu macht sich zunächst klar:

Lemma 4.3 — *Ist a ein palindromisches Polynom von ungeradem Grad, so ist $a(x)$ durch $x + 1$ teilbar, und der Quotient ist wieder palindromisch.*

Beweis. Übung. □

Deshalb kann man sich auf den Fall von Polynomen geraden Grades beschränken. Es sei also $n = 2m$ gerade und $a_n \neq 0$. Weil dann auch $a_0 \neq 0$, ist 0 jedenfalls keine Lösung der Gleichung $a(x) = 0$. Wir dividieren die Gleichung formal durch x^m und erhalten:

$$a_n x^m + a_{n-1} x^{m-1} + a_{m-1} x + \ldots + a_m + a_{m+1} x^{-1} \ldots + a_0 x^{-m} = 0.$$

Mit einer neuen Variablen $y = x^{-1}$ können wir diese Gleichung wie folgt umschreiben:

$$a_n x^m + a_{n-1} x^{n-2} + \ldots + a_{m-1} x + a_m + a_{m+1} y + \ldots + a_0 y^m = 0.$$

Weil a palindromisch ist, ist die linke Seite ein in x und y symmetrisches Polynom vom Grad $m = \frac{n}{2}$ und kann Satz 4.1 als ein Polynom $a(x)x^{-m} = g(x + y, xy)$ in $u := x + y = x + \frac{1}{x}$ und $xy = 1$ ausgedrückt werden. Das Lösen der Ausgangsgleichung $a(x) = 0$ wird also darauf zurückgeführt, zunächst die Gleichung

$$g(u, 1) = 0$$

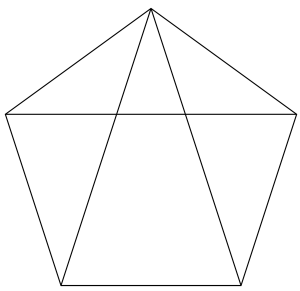
von halbem Grad in der Variablen u und anschließend eine quadratische Gleichung

$$x^2 - ux + 1 = 0$$

für x zu lösen. □

Wir betrachten dazu das folgende Beispiel:

Regelmäßige Fünfecke und fünfte Einheitswurzeln — Wie kann man mit Zirkel und Lineal ein reguläres Fünfeck konstruieren? Man kann sowohl geometrisch wie algebraisch zu einer Konstruktionsmethode kommen. Ich skizziere zunächst einen geometrischen Weg, bevor wir zur algebraischen Methode kommen: Dazu betrachten wir ein reguläres Fünfeck



und bezeichnen die Länge der Diagonale mit d, die einer Seite mit s. Ein Blick auf die Zeichnung zeigt einem ähnliche gleichschenklige Dreiecke mit den Seitenlängen (d, d, s) und $(s, s, d - s)$. Das Seitenverhältnis

$$x := \frac{d}{s} = \frac{s}{d - s} = \frac{1}{x - 1}$$

genügt also der quadratischen Gleichung

$$x^2 - x - 1 = 0,$$

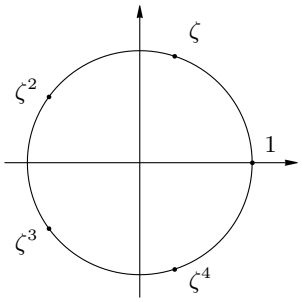
und weil $x > 1$ ist, hat man

$$x = \frac{1}{2}(1 + \sqrt{5}).$$

Gibt man sich also eine Strecke s vor, so genügt es, eine Strecke der Länge $d = xs$ zu konstruieren, was mit Zirkel und Lineal leicht ist, und dann über der Strecke s das entsprechende spitzwinklige Dreieck zu errichten. Es ist dann leicht, das Dreieck zu einem Fünfeck zu vervollständigen.

Das Verhältnis $- - -d : s = \frac{1}{2}(1 + \sqrt{5})$ heißt der Goldene Schnitt. Der numerische Wert ist ungefähr $1,618$.

Algebraisch kann man so vorgehen: Die fünften Einheitswurzeln $e^{2\pi ik/5}$, $k = 0, \ldots, 4$ lassen sich alle als Potenzen einer Wurzel $\zeta = e^{2\pi i/5}$ schreiben. Als Punkte der komplexen Ebene gelesen, bilden sie die Ecken eines regulären Fünfecks, das dem Einheitskreis einbeschrieben ist.



Definitionsgemäß genügt ζ der Gleichung $\zeta^5 - 1 = 0$. Weil $\zeta \neq 1$, können wir durch $\zeta - 1$ teilen. Man erhält

$$\zeta^4 + \zeta^3 + \zeta^2 + \zeta + 1 = 0.$$

Die linke Seite ist das sogenannte fünfte Kreisteilungspolynom $\Phi_5(\zeta)$. Wir werden später allgemeiner Φ_n für beliebige $n \in \mathbb{N}$ definieren. Allerdings gilt nur für Primzahlen p die einfache Beziehung $\Phi_p(X) = (X^p - 1)/(X - 1)$. Die Gleichung $\Phi_5(\zeta) = 0$ ist palindromisch und hat geraden Grad. Mit der oben eingeführten Substitution $u = \zeta + \frac{1}{\zeta}$ wird man auf die quadratischen Gleichungen

$$\frac{\Phi_5(\zeta)}{\zeta^2} = \zeta^2 + \zeta + 1 + \frac{1}{\zeta} + \frac{1}{\zeta^2} = u^2 + u - 1 = 0 \quad \text{und} \quad \zeta^2 - u\zeta + 1 = 0$$

geführt. Also gilt

$$u = \zeta + \frac{1}{\zeta} = 2\cos\tfrac{2\pi}{5} = \frac{1}{4}(-1 + \sqrt{5}).$$

Um den Punkt ζ wirklich zu konstruieren, genügt es, $u/2$ zu kennen, weil man dann ζ und ζ^{-1} als Schnittpunkte der Senkrechten zur x-Achse durch $u/2$ mit dem Einheitskreis gewinnt.

4.2. **Symmetrische Polynome in beliebig vielen Variablen.**

Die Vorüberlegungen zum Falle von zwei Variablen lassen sich wie folgt auf den Fall von n Variablen $x_1, \ldots, x_n$ verallgemeinern:

Die Potenzsummen $p_k := x_1^k + \ldots + x_n^k$, $k > 0$, sind symmetrische Polynome.

Mit einer Hilfvariablen t kann man das folgende Produkt bilden und nach Potenzen von t zusammenfassen:

$$(1 + tx_1) \cdot \ldots \cdot (1 + tx_n) = 1 + s_1 t + s_2 t^2 + \ldots + s_n t^n.$$

Dabei sind $s_1, \ldots, s_n$ gewisse Polynome in den x_i vom Grad $\deg(s_i) = i$. Weil die linke Seite offensichtlich invariant unter Vertauschung der x_i ist, gilt dasselbe für die rechte Seite, d.h. die Polynome $s_1, \ldots, s_n$ sind symmetrisch. Man nennt s_i das i-te elementarsymmetrische Polynom in den Variablen $x_1, \ldots, x_n$. Konstruktionsgemäß ist

$$s_k := \sum_{i_1 < \ldots < i_k} x_{i_1} \cdots x_{i_k},$$

für $0 < k \leq n$. Ausgeschrieben lauten die elementarsymmetrischen Polynome für $n = 4$:

$$\begin{aligned}
s_1 &= x_1 + x_2 + x_3 + x_4 \\
s_2 &= x_1x_2 + x_1x_3 + x_1x_4 + x_2x_3 + x_2x_4 + x_3x_4 \\
s_3 &= x_1x_2x_3 + x_1x_2x_4 + x_1x_3x_4 + x_2x_3x_4 \\
s_4 &= x_1x_2x_3x_4
\end{aligned}$$

Die Bezeichnungen s_k sind nicht ganz befriedigend, weil man nur aus dem Kontext auf die Anzahl der relevanten Variablen schließen kann. Aber zusätzliche Indizierungen würden die Lesbarkeit unnötig erschweren.

Formeln von Girard[4] und Viète[5] — In $A[x_1, \ldots, x_n, t]$ gilt die Beziehung

$$(t - x_1) \cdot \ldots \cdot (t - x_n) = t^n - s_1 t^{n-1} + s_2 t^{n-2} + \ldots + (-1)^n s_n. \tag{4.2}$$

Das liefert die Formeln von Girard und Viète über den Zusammenhang zwischen den Koeffizienten eines Polynoms und seinen Nullstellen: Sind $\lambda_1, \ldots, \lambda_n \in A$ die Nullstellen eines Polynoms

$$f = x^n + f_1 x^{n-1} + f_2 x^{n-2} + \ldots + f_{n-1} x + f_n,$$

so gilt

$$f_k = (-1)^k s_k(\lambda_1, \ldots, \lambda_n).$$

Dabei sind die Nullstellen so häufig einzusetzen, wie es ihrer Vielfachheit entspricht.

Der folgende Satz ist die Verallgemeinerung von Satz 4.1 für beliebig beliebig viele Variablen:

Satz 4.4 (Hauptsatz über symmetrische Polynome, Waring[6] 1762) — *Es sei A ein kommutativer Ring. Jedes symmetrische Polynom $f \in A[x_1, \ldots, x_n]$ läßt sich auf eindeutige Weise als Polynom mit Koeffizienten in A in den elementarsymmetrischen Polynomen $s_1, \ldots, s_n$ ausdrücken.*

Etwas formaler kann man den Satz wie folgt umschreiben: Wir betrachten zwei Polynomringe mit den Unbestimmten $x_1, \ldots, x_n$ bzw. $y_1, \ldots, y_n$. Wenn man $y_1, \ldots, y_n$ in dieser Reihenfolge auf $s_1, \ldots, s_n$ abbildet, setzt sich diese Abbildung auf eindeutige Weise zu einem Ringhomomorphismus

$$\Phi : A[y_1, \ldots, y_n] \to A[x_1, \ldots, x_n], \qquad y_i \mapsto s_i,$$

fort. Es ist klar, daß das Bild von Φ im Invariantenunterring liegt. Man kann den Sachverhalt des Satzes deshalb auch so ausdrücken:

Satz 4.5 — *Der Ringhomomorphismus $\Phi : A[y_1, \ldots, y_n] \to A[x_1, \ldots x_n]^{S_n}$ ist ein Isomorphismus.*

Die Surjektivität von Φ entspricht dann die Darstellbarkeit eines beliebigen symmetrischen Polynoms durch elementarsymmetrische und die Injektivität der Eindeutigkeit einer solchen Darstellung.

Beweis. Der Beweis ist konstruktiv: Wir geben zwei Algorithmen an, die für jedes symmetrische Polynom eine Darstellung als Polynom in elementarsymmetrischen Polynomen liefern.

Algorithmus 1: Der erste Algorithmus verwendet Monomordnungen, wie sie in erweiterter Form heute in der Computeralgebra von zentraler Bedeutung sind. Wir ordnen die Monome $x^d = x_1^{d_1} \cdots x_n^{d_n}$ lexikographisch nach ihren Exponentenfolgen $d = (d_1, \ldots, d_n)$ und $d' = (d'_1, \ldots, d'_n)$, d.h. wir setzen $x^d > x^{d'}$ genau dann, wenn es ein i mit der folgenden Eigenschaft gibt: $d_j = d'_j$ für alle $j < i$ und $d_i > d'_i$. Das Leitmonom eines Polynoms $f = \sum_t f_t x^t$ ist das größte Monom, dessen zugehöriger Koeffizient nicht 0. Das Produkt aus diesem Leitkoeffizienten und dem Leitmonom ist der Leitterm.

Es sei nun $f = \sum f_t x^t$ ein symmetrisches Polynom. Für das Leitmonom x^d von f gilt wegen der Symmetrieannahme, daß $d_1 \geq d_2 \geq \ldots \geq d_n$. Das symmetrische Polynom

$$g := f_d s_1^{d_1 - d_2} s_2^{d_2 - d_3} \cdots s_{n-1}^{d_{n-1} - d_n} s_n^{d_n} \tag{4.3}$$

---

[4] Albert Girard, ⋆1595 in St Mihiel, †8.12.1632 in Leiden.

[5] François Viète, ⋆1540 in Fontenay-le-Comte, †13.12.1603 in Paris.

[6] Edward Waring, ⋆1736 in Old Heath, †15 August 1798 in Pontesbury.

hat denselben Leitterm wie f. Die Differenz $f-g$ hat daher einen strikt kleineren Leitterm bezüglich der Monomordnung als f. Durch Induktion folgt nun die Behauptung.

Ähnlich beweist man die Injektivität: Das Polynom $s_1^{\nu_1}\cdots s_n^{\nu_n}$ hat das Leitmonom

$$x_1^{\nu_1+\ldots+\nu_n}x_2^{\nu_2+\ldots+\nu_n}\cdots x_n^{\nu_n}.$$

Die Bilder verschiedener Monome $y_1^{\nu_1}\cdots y_n^{\nu_n}$ unter dem Ringhomomorphismus $\Phi: y_n\mapsto s_n$ haben verschiedene Leitmonome. Deshalb kann es in $\Phi(\sum_\nu a_\nu y^\nu)$ nicht zu einer vollständigen Auslöschung aller Monome in den Variablen x_i kommen.

Algorithmus 2: Wir argumentieren durch Induktion über die Anzahl der Variablen. Im Falle $n=1$ ist die Aussage trivialerweise richtig. Es sei also $n>1$, und die Aussage sei für alle kleineren Anzahlen von Variablen schon bewiesen. Es sei $f\in A[x_1,\ldots,x_n]$ ein symmetrisches Polynom in n Variablen. Das Polynom

$$\tilde f(x_1,\ldots,x_{n-1}) := f(x_1,\ldots,x_{n-1},0)$$

in $n-1$ Variablen ist ebenfalls symmetrisch. Nach Induktionsannahme gibt es ein Polynom $g\in A[y_1,\ldots,y_{n-1}]$ mit der Eigenschaft, daß

$$\tilde f(x_1,\ldots,x_{n-1})) = g(s'_1,\ldots,s'_{n-1}),$$

wobei $s'_i(x_1,\ldots,x_{n-1}) = s_i(x_1,\ldots,x_{n-1},0)$ für $i=1,\ldots,n-1$ das i-te elementarsymmetrische Polynom in den Variablen $x_1,\ldots,x_{n-1}$ bezeichnet. Das Polynom $F := f-g(s_1,\ldots,s_{n-1})$ verschwindet konstruktionsgemäß, sobald man $x_n=0$ setzt, ist also durch x_n teilbar. Weil F symmetrisch ist, ist es auch durch die anderen Variablen $x_1,\ldots,x_{n-1}$ teilbar und somit auch durch das Produkt $s_n = x_1\cdots x_n$. Es gibt deshalb ein Polynom $h(x_1,\ldots,x_n)$ so, daß $f-g(s_1,\ldots,s_{n-1}) = F = s_nh$. Notwendigerweise ist auch h symmetrisch. Weil h kleineren Grad als f hat, kann man durch Induktion über den Grad annehmen, daß $h=k(s_1,\ldots,s_n)$ für ein gewisses Polynom k. Es folgt:

$$f = g(s_1,\ldots,s_{n-1}) + s_nk(s_1,\ldots,s_n).$$

Das beweist die Existenz. Die Eindeutigkeit kann man ähnlich zeigen: Angnommen, p ist ein Polynom mit $p(s_1,\ldots,s_n)=0$. Setzt man $x_n=0$, so folgt $p(s'_1,\ldots,s'_{n-1},0)=0$. Induktiv kann man annehmen, daß die Injektivität für $n-1$ Variablen schon gezeigt ist. Dann weiß man, daß $p(y_1,\ldots,y_{n-1},0)=0$. Das bedeutet, daß p durch y_n teilbar ist, etwa $p=y_nq$. Nach Voraussetzung ist $0=p(s_1,\ldots,s_n)=s_nq(s_1,\ldots,s_n)$. Aber dann ist schon $q(s_1,\ldots,s_n)=0$. Durch Induktion über den Grad von p schließt man auf $q=0$ und somit $p=0$. □

Eine fundamentale Konsequenz des Hauptsatzes, die wir in der Folge häufig anwenden werden, ist das folgende Prinzip:

Folgerung 4.6 — *Es seien $A\subset B$ Ringe und $f=x^n+a_1x^{n-1}+\ldots+a_n\in A[x]$ ein Polynom, das über B in Linearfaktoren zerfällt:*

$$f(x) = (x-\lambda_1)\cdot\ldots\cdot(x-\lambda_n),\qquad \lambda_i\in B. \tag{4.4}$$

Dann liegt jedes Element $b\in B$, das sich symmetrisch und polynomiell in den Nullstellen $\lambda_1,\ldots,\lambda_n$ ausdrücken läßt, schon in A.

Beweis. Es sei $\varphi: A[x_1,\ldots,x_n]\to B$ der Ringhomomorphismus mit $\varphi: x_i\mapsto\lambda_i$. Die Annahme über b besagt, daß es ein symmetrisches Polynom f mit $\varphi(f)=b$ gibt. Nun gilt nach den Formeln von Girard und Viète, daß $\varphi(s_i)=(-1)^ia_i\in A$. Nach dem Hauptsatz gibt es ein Polynom $g\in A[y_1,\ldots,y_n]$ mit $f=g(s_1,\ldots,s_n)$. Es folgt $b=\varphi(f)=g(\Phi(s_1),\ldots,\varphi(s_n))=g(-a_1,a_2,\ldots)\in A$. □

4.3. **Potenzsummen und Newtonsche Formeln.**

Die Potenzsummen $p_k := x_1^k + \ldots + x_n^k$, $k \in \mathbb{N}$, sind besonders wichtige Beispiele von symmetrischen Polynomen. Deswegen gehen wir näher auf die Frage ein, wie sich denn p_k *konkret* durch $s_1, \ldots, s_n$ ausdrücken läßt. Zum Beispiel gilt für $n = 3$ und $k = 1, 2, 3$:

$$\begin{aligned} p_1 &= s_1 \\ p_2 &= s_1^2 - 2s_2 \\ p_3 &= s_1^3 - 3s_1s_2 + 3s_3 \end{aligned}$$

Im Folgenden setzen wir $s_k = 0$, wenn k größer als die Anzahl der betrachteten Variablen ist.

Newton hat für die Berechung der p_k die folgenden Rekursionsgleichungen angegeben:

Satz 4.7 (Newton[7]) — *Für alle $k \geq 1$ gilt*

$$p_k - s_1p_{k-1} + s_2p_{k-2} - \ldots + (-1)^k k s_k = 0. \tag{4.5}$$

Dabei ist $s_\ell = 0$ zu setzen, wenn ℓ größer als die Anzahl der Variablen ist.

Beweis. Es sei n die Anzahl der Unbestimmten $x_1, \ldots, x_n$. Wertet man Gleichung (4.2) in x_i aus, erhält man

$$0 = x_i^n - s_1x_i^{n-1} + \ldots + (-1)^n s_n. \tag{4.6}$$

Summation über alle $i = 1, \ldots, n$ liefert die Behauptung für den Fall $k = n$. Wenn $k > n$ erhält man zunächst die Gültigkeit der Formel für k Variablen $x_1, \ldots, x_k$. Die Substitution $x_{n+1} = \ldots = x_k = 0$ liefert die Behauptung. Für den Fall $k < n$ kann man so argumentieren: Wir wissen, daß sich alle p_i durch die elementarsymmetrischen Polynome $s_1, \ldots, s_n$ ausdrücken lassen. Aus Gradgründen können in dem Ausdruck für p_k aber aber nur $s_1, \ldots, s_k$ vorkommen. Wenn man nun eine Formel $p_k = \Phi(s_1, \ldots, s_k)$ betrachtet und nun $x_{k+1} = \ldots = x_n = 0$ setzt, erhält man eine gültige Formel derselben Gestalt. Jede Gleichung zwischen symmetrischen Polynomen vom Grad $\leq k$ muß also richtig bleiben, wenn man die Zahl der Variablen von k auf n erhöht. □

Daraus lassen sich die p_i rekursiv durch die s_k, $k \leq n$, ausdrücken, ohne daß man auf den allgemeinen Algorithmus des Hauptsatzes 4.4 zurückgreifen muß. Man beachte den Vorfaktor n vor s_n in der Identität (4.5). Deshalb entstehen beim umgekehrten Auflösen nach den s_n Nenner. Die Formeln

$$\begin{aligned} s_1 &= p_1 \\ s_2 &= \frac{1}{2}(p_1^2 - p_2) \\ s_3 &= \frac{1}{6}p_1^3 - \frac{1}{2}p_1p_2 + \frac{1}{3}p_3 \end{aligned}$$

gelten daher nur in $\mathbb{Q}$-Algebren, d.h. in kommutativen Ringen, in denen alle natürlichen Zahlen invertierbar sind.

Die Umrechnungsformeln zwischen elementarsymmetrischen Polynomen und Potenzsummen lassen sich einigermaßen geschlossen ausdrücken. Um solche Ausdrücke herzuleiten, verwenden wir erzeugende Funktionen. Mit einer Hilfsvariablen t betrachten wir die Identität

$$\prod_{i=1}^{n}(1 + x_it) = \sum_{k=0}^{n} s_k t^k,$$

wobei auf der rechten Seite $s_0 = 1$ ist. Wenn wir wieder $s_k = 0$ für $k > n$ verabreden, können wir den Laufindex k auf der rechten Seite auch gegen ∞ gehen lassen. Das erleichtert das Aufschreiben

[7] Sir Isaac Newton, ⋆1643 †1727

der Formeln. Wir nehmen auf beiden Seiten den Logarithmus, und zwar im Sinne von formalen Potenzreihen in t. Deshalb spielen Konvergenzfragen hier keine Rolle. Man erhält:

$$\sum_{i=1}^{n} \log(1 + x_i t) = \log(1 + \sum_{k=1}^{n} s_k t^k)$$

und somit

$$\sum_{m=1}^{\infty} \frac{(-1)^{m-1}}{m} \left(\sum_{i=1}^{n} x_i^m \right) t^m = \sum_{\ell=1}^{\infty} \frac{(-1)^{\ell-1}}{\ell} \left(\sum_{k=1}^{n} s_k t^k \right)^{\ell}.$$

Der Koeffizientenvergleich für die Monome t^m zeigt:

$$\begin{aligned} (-1)^m \frac{p_m}{m} &= \text{Koeffizient von } t^m \text{ in} \\ &\qquad \sum_{\ell=1}^{\infty} \frac{(-1)^{\ell}}{\ell} \sum_{\ell_1+\ldots+\ell_n=\ell} \frac{\ell!}{\ell_1! \cdots \ell_n!} s_1^{\ell_1} \cdots s_n^{\ell_n} t^{\ell_1+2\ell_2+\ldots+n\ell_n} \end{aligned}$$

Die Summanden auf der rechten Seite, die zum Koeffizienten von t^m beitragen, gehören zu den Indextupeln $(\ell_1, \ldots, \ell_n)$ mit $\ell_1 + 2\ell_2 + \ldots + n\ell_n = m$. Deshalb erhält man schließlich:

Satz 4.8 — *Für alle $m \geq 1$ gilt:*

$$(-1)^m \frac{p_m}{m} = \sum_{\ell_1+2\ell_2+\ldots+n\ell_n=m} (-1)^{\ell_1+\ldots+\ell_n} \frac{(\ell_1 + \ldots + \ell_n - 1)!}{\ell_1! \cdots \ell_n!} s_1^{\ell_1} \cdots s_n^{\ell_n}.$$

□

Analog findet man umgekehrt Formeln, die die elementarsymmetrischen Polynome durch Potenzsummen ausdrücken:

$$\begin{aligned} \sum_{i=0}^{n} s_i t^i &= \exp\left(\log\left(\sum_{j=1}^{n} (1 + x_j t) \right) \right) \\ &= \exp\left(\sum_{m=1}^{\infty} \frac{(-1)^m}{m} p_m t^m \right) \\ &= \sum_{i=0}^{\infty} (-t)^i \sum_{i_1+2i_2+3i_3\ldots=i} \prod_j \frac{1}{i_j!} \left(-\frac{p_j}{j} \right)^{i_j} \end{aligned}$$

Durch Koeffizientenvergleich erhält man also wieder:

Satz 4.9 — *Für alle m gilt:*

$$s_m = (-1)^m \sum_{m_1+2m_2+3m_3\ldots=m} \prod_{j \geq 1} \frac{1}{m_j!} \left(-\frac{p_j}{j} \right)^{m_j}$$

□

Für $m = 4$ ist die Summe über die Tupel $(m_1, m_2, \ldots)$ mit den Werten $(4, \ldots)$, $(2, 1, \ldots)$, $(1, 0, 1, \ldots)$, $(0, 2, \ldots)$, $(0, 0, 0, 1, \ldots)$ zu nehmen, wobei irrelevante Nullen nicht aufgezählt sind. Man findet so, ohne in eine Rekursion einsteigen zu müssen:

$$s_4 = \frac{1}{4!} p_1^4 - \frac{1}{4} p_1^2 p_2 + \frac{1}{3} p_1 p_3 + \frac{1}{8} p_2^2 - \frac{1}{4} p_4. \tag{4.7}$$

4.4. **Aufgaben zu symmetrischen Polynomen.**

Aufgabe 4.10. — Finden Sie eine Konstruktion mit Zirkel und Lineal für ein regelmäßiges Fünfeck, das

(1) auf einer gegebenen Seite errichten werden soll;
(2) einem gegebenen Kreis einbeschrieben werden soll.

Aufgabe 4.11. — Bestimmen Sie ein Polynom vom Grad 3 mit rationalen Koeffizienten, das $2\cos(2\pi/7)$ als Wurzel hat, und zwar

(1) indem Sie die Argument des Textes für siebte Einheitswurzeln anpassen.
(2) Aus den Additionsformeln für die trigonometrischen Funktionen und dem Umstand, daß $\cos(6\pi/7) = \cos(8\pi/7)$.

Aufgabe 4.12. — Leiten Sie aus der Geometrie des regelmäßigen Dreiecks, Vierecks und Fünfecks für die Winkel 30^o, 45^o, 72^o Wurzelausdrücke ihrer Sinus und Cosinus her. Wenn man weiß, wie man Wurzeln aus reellen Zahlen bis zu einer vorgegebenen numerischen Genauigkeit ziehen kann, kann man mit Hilfe der Additionstheoreme für die trigonometrischen Funktionen die Werte $\sin(3^o)$ und $\cos(3^o)$ bis zu jeder vorgegebenen Genauigkeit berechnen. Berechnen Sie diese Werte auf diese Weise bis auf vier Nachkommastellen. Wieder mit den Additionstheoremen erhält man eine grobe Sinus- und Cosinustabelle für alle Winkel der Form $3n^0$, $n \in \mathbb{N}$. Informieren Sie sich über Berechnungsmethoden für Tabellen für Sinus- und Sehnenwerte bei den Griechen bis Ptolemaios und bei den Mathematikern der indischen Keralaschule.

Aufgabe 4.13. — Programmieren Sie einen oder beide Algorithmen in Mupad (oder Maple oder ...). Präzisieren Sie zunächst die Aufgabenstellung: Sie übergeben eine beliebigen Ausdruck, in dem viele Bezeichner vorkommen können, eine Liste von Bezeichnern, die den Unbestimmten im Satz entsprechen, sowie eine Liste von Werten (!), die den elementarsymmetrischen Polynomen entsprechen. Da Sie nicht wissen, *welche* Werte übergeben werden, dürfen Sie nicht zu früh substituieren...

Aufgabe 4.14. — Drücken Sie die folgenden symmetrischen Polynome durch elementarsymmetrische Polynome aus:

(1) $x_1^4 + x_2^4 + x_3^4 + x_4^4$.
(2) Es sei $h_k \in A[x_1, \ldots, x_n]$ die Summe aller Monome vom Grad k. Die h_k heißen vollständige symmetrische Polynome. Schreiben Sie h_k für $n = 3$ und $k = 1, \ldots, 3$ als Polynom in den elementarsymmetrischen Polynomen.
(3) $\Delta := \prod_{1 \le i < j \le 3}(x_i - x_j)^2$.

Aufgabe 4.15. — Das Polynom $\Delta := \prod_{i<j}(x_i - x_j)^2 \in \mathbb{Z}[x_1, \ldots, x_n]$ ist symmetrisch. Deshalb gibt es ein Polynom disc_n, die sogenannte Diskriminante, mit $\Delta = \mathrm{disc}_n(s_1, \ldots, s_n)$, wobei $s_1, \ldots, s_n$ die elementarsymmetrischen Polynome in den x_i bezeichnen.

(1) Bestimmen Sie disc_2 und disc_3.
(2) Es sei $f = x^n - f_1 x^{n-1} + \ldots + (-1)^n f_n$. Zeigen Sie: f hat genau dann eine mehrfache Nullstelle, wenn $\mathrm{disc}(f_1, \ldots, f_n) = 0$.
(3) Wir betrachten den Raum $V = \{f = x^3 - ax - b \mid a, b \in \mathbb{R}\} \cong \mathbb{R}^2$. Bestimmen Sie die Orte $V_1 \subset V$ aller Polynome mit mehrfacher Nullstelle und $V_0 \subset V_1$ aller Polynome mit dreifacher Nullstelle. (Zeichnung).

Aufgabe 4.16. — Betrachten Sie die letzte Frage aus Aufgabe 4.15 auch für Polynome vom Grad 4: Es sei $V = \{f = x^4 + ax^2 + bx + c \mid a, b, c \in \mathbb{R}\}$. Bestimmen Sie die Orte V_2 aller Polynome mit mindestens doppelter Nullstelle, V_{22} mit mindestens zwei doppelten Nullstellen, V_3 mit mindestens einer dreifachen Nullstelle und V_4 mit einer vierfachen Nullstelle.

Aufgabe 4.17. — Wir betrachten den Polynomring $S = \mathbb{C}[x_{ij}, 1 \le i, j \le n]$ in n^2 Unbestimmten. Das charakteristische Polynom $\chi_A(t) = t^n - \chi_1 t^{n-1} + \ldots + (-1)^n \chi_n$ der Matrix $A = (x_{ij}) \in M_n(\mathbb{C})$ hat Koeffizienten $\chi_k \in S$. Für jede Matrix $M \in M_n(\mathbb{C})$ sind $(-1)^i \chi_i(M)$ die Koeffizienten des charakteristischen Polynoms von M.

(1) Es gibt ein Polynom $p \in S$ mit der Eigenschaft, daß jede Matrix $M \in M_n(\mathbb{C})$ genau dann paarweise verschiedene Eigenwerte hat, wenn $p(M) \neq 0$.

(2) Finden Sie für $n = 4$ eine Formel, die die Koeffizienten $\chi_i(M)$, $i = 1, \ldots, n$ durch die Spuren $\mathrm{tr}(M^k)$, $k = 1 \ldots, n$, ausdrückt.

Hinweis zum zweiten Teil: Betrachten Sie zunächst diagonalisierbare Matrizen und verwenden Sie dann ein Stetigkeitsargument.

Aufgabe 4.18. (Invariante Polynome für die alternierende Gruppe) — Die Gruppe S_n operiert auf dem Polynomring $\mathbb{C}[x_1, \ldots, x_n]$ durch $\sigma(x_i) = x_{\sigma(i)}$. Ein Polynom f ist S_n-invariant (oder symmetrisch), wenn $\sigma(f) = f$ für alle $\sigma \in S_n$. Ein Polynom f ist antisymmetrisch, wenn $\sigma(f) = \mathrm{sgn}(\sigma) f$ für alle $\sigma \in S_n$. Schließlich ist f A_n-invariant, wenn $\sigma(f) = f$ für alle σ in der alternierenden Gruppe A_n. Zeigen Sie:

(1) Das Polynom $\delta := \prod_{i<j}(x_i - x_j)$ ist antisymmetrisch.
(2) Ist f antisymmetrisch, so gilt $\delta | f$, und f/δ ist symmetrisch.
(3) f ist genau dann A_n-invariant, wenn sich f als Summe eines symmetrischen und eines antisymmetrischen Polynoms schreiben läßt.
(4) Die Menge A der A_n-invarianten Polynome ist ein Unterring in $\mathbb{C}[x_1, \ldots, x_n]$, der die Menge S der S_n-invarianten Polynome als Unterring enthält.
(5) A wird als $\mathbb{C}$-Algebra von den elementarsymmetrischen Polynome s_1,$\ldots$, s_n und δ erzeugt.
(6) Der Kern des Homomorphismus $\Psi : \mathbb{C}[Y_1, \ldots, Y_n, Z] \to A$, $Y_i \mapsto s_i$, $Z \mapsto \delta$, wird von dem Element $Z^2 - \mathrm{disc}_n(Y_1, \ldots, Y_n)$ erzeugt (cf. Aufgabe 4.15).

§5. Euklidische Ringe

5.1. Allgemeine Teilbarkeitsbegriffe.

Definition 5.1. — Es sei A ein kommutativer Ring.

(1) $a \in A$ ist ein *Teiler* von $b \in A$ und b ein *Vielfaches* von a, wenn es ein $c \in A$ mit $b = ac$ gibt. In Zeichen: $a|b$. Falls a kein Teiler von b ist, schreibt man $a \nmid b$.
(2) $d \in A$ ist ein *gemeinsamer Teiler* von $S \subset A$, wenn $d|a$ für alle $a \in S$, und d ist ein *größter gemeinsamer Teiler* von S, wenn d ein gemeinsamer Teiler ist und wenn für jeden anderen gemeinsamen Teiler x von S gilt $x|d$.
(3) $a, b \in A$ sind *assoziiert*, in Zeichen: $a \sim b$, wenn $a = ub$ für eine Einheit u.
(4) $v \in A$ ist ein *gemeinsames Vielfaches* von S, wenn $a|v$ für alle $a \in S$, und v ist ein *kleinstes gemeinsames Vielfaches* von S, wenn v ein gemeinsames Vielfaches ist und wenn für jedes andere gemeinsame Vielfache y gilt $v|y$.

Für die Teilbarkeitsrelation gelten die folgenden Rechenregeln:

(1) $1|a|0$ für alle $a \in A$.
(2) $a|b$ und $a|c \quad \Rightarrow \quad a|(\lambda b + \mu c)$ für alle $\lambda, \mu \in A$.
(3) $a|b$ und $b|c \quad \Rightarrow \quad a|c$.
(4) $a \sim b \quad \Leftrightarrow \quad a|b$ und $b|a$.
(5) Falls ein größter gemeinsamer Teiler für $S \subset A$ existiert, ist er eindeutig bis auf Einheiten.
(6) Falls ein kleinstes gemeinsames Vielfaches für $S \subset A$ existiert, ist es eindeutig bis auf Einheiten.

Satz 5.2 — *Es sei A ein Hauptidealring. Dann besitzt jede Menge $S \subset A$ einen größten gemeinsamen Teiler d. Außerdem gibt es Elemente $s_1, \ldots, s_n \in S$ und $\alpha_1, \ldots, \alpha_n \in A$ mit*

$$d = \alpha_1 s_1 + \ldots + \alpha_n s_n.$$

Die Koeffizienten $\alpha_1, \ldots, \alpha_n$ heißen Bézout-Koeffizienten von d.

Beweis. Das von S erzeugte Ideal ist ein Hauptideal, etwa $S = (d)$. Dann besitzt d wegen $d \in (S)$ eine additive Darstellung wie angegeben. Wegen $s \in S \subset (S) = (d)$ gilt $d|s$ für alle $s \in S$. Schließlich folgt aus $x|s$ für alle $s \in S$ auch $x|\sum_i \alpha_i s_i = d$. Damit ist d ein größter gemeinsamer Teiler. □

5.2. Euklidische Ringe.

Definition 5.3. — Ein *euklidischer Ring* ist ein Integritätsbereich A mit einer Gradfunktion $\delta : A \setminus \{0\} \to \mathbb{N}_0$ und der Eigenschaft, daß es für alle $a \in A$ und $b \in A \setminus \{0\}$ Elemente $q, r \in A$ mit $a = qb + r$ und $r = 0$ oder $\delta(r) < \delta(b)$ gibt.

Das Element r ist der Rest bei Division von a durch b. Dabei muß man allerdings daran denken, daß das Paar (q, r) im allgemeinen durch (a, b) nicht eindeutig bestimmt ist. Dies ist nicht einmal im Ring $\mathbb{Z}$ der ganzen Zahlen mit $\delta(a) := |a|$ der Fall: $7 = 1 \cdot 5 + 2 = 2 \cdot 5 - 3$.

Beispiel 5.4. — Der Ring der ganzen Zahlen $\mathbb{Z}$ ist ein euklidischer Ring mit Gradfunktion $\delta(a) := |a|$. Die Division mit Rest ist die gewöhnliche ganzzahlige Division. Wenn man zusätzlich vereinbart, daß der Rest grundsätzlich ≥ 0 sein soll, ist die Division sogar eindeutig.

Beispiel 5.5. — Der Ring der sogenannten GAUSSschen Zahlen

$$\mathbb{Z}[i] = \{m + ni \in \mathbb{C} \mid m, n \in \mathbb{Z}\}$$

ist ein euklidischer Ring mit Gradfunktion $\delta(m, ni) = |m + ni|^2 = m^2 + n^2$. Zum Beweis dieser Aussage seien Elemente $a = \alpha + \alpha' i \in \mathbb{Z}[i]$ und $b = \beta + \beta' i \in \mathbb{Z}[i] \setminus \{0\}$ vorgegeben. Wir können

im Körper $\mathbb{C}$ den Quotienten $z = a/b$ bilden und Real- und Imaginärteil von z durch ganze Zahlen approximieren. Es gibt sicher $m, m' \in \mathbb{Z}$ mit

$$|\operatorname{Re}(z) - m| \leq \frac{1}{2}, \quad |\operatorname{Im}(z) - m'| \leq \frac{1}{2}.$$

Es folgt $|z - (m + m'i)|^2 \leq \frac{1}{2}$. Wir setzen nun $q = m + m'i$ und $r = a - bq = b(z - q) \in \mathbb{Z}[i]$. Es folgt:

$$\delta(r) = |r|^2 = |b|^2|z - q|^2 \leq \frac{1}{2}\delta(b) < \delta(b).$$

Wenn man sich die GAUSSschen Zahlen als Gitterpunkte in einem quadratischen Gitter in $\mathbb{C}$ vorstellt, so landet der Quotient z in einem der Gitterquadrate, und q ist die durch die Wahl eines nächstliegenden Gitterpunktes bestimmt. Diese Wahl ist nicht eindeutig.

Beispiel 5.6. — Auf ähnliche Weise zeigt man, daß der Ring der Ring der EISENSTEINzahlen

$$\mathbb{Z}[\rho] = \{m + n\rho \mid m, n \in \mathbb{Z}\}$$

mit $\rho = \exp(2\pi i/3)$ ein euklidischer Ring mit Gradfunktion $\delta(m + n\rho) = |m + n\rho|^2 = m^2 - mn + n^2$ ist.

Beispiel 5.7. — Für jeden Körper K ist der Polynomring $K[X]$ ein euklidischer Ring mit Gradfunktion $\delta(f) = \deg(f)$. Dies ergibt sich unmittelbar aus dem Satz über Polynomdivision 3.3.

Satz 5.8 — *Euklidische Ringe sind Hauptidealringe.*

Beweis. Es sei (A, δ) ein euklidischer Ring und $I \subset A$ ein Ideal. Falls $I = 0$, ist nichts zu zeigen. Es sei also $I \neq 0$ und $b \in I \setminus \{0\}$ ein Element mit

$$\delta(b) = \min\{\delta(c) \mid c \in I \setminus \{0\}\}.$$

Offensichtlich gilt $(b) \subset I$. Es sei $a \in I$ beliebig und $r = a - qb$ ein Rest bei Division von a durch b, so daß also $r = 0$ oder $\delta(r) < \delta(b)$. Da $r = a - qb \in I$, ist die zweite Möglichkeit wegen der Minimalitätsbedingung an b ausgeschlossen. Deshalb bleibt nur Option $r = 0$ und somit $a = qb \in (b)$. Das zeigt die umgekehrte Inklusion $I \subset (b)$. □

Die Umkehrung ist falsch, obwohl es nicht so leicht ist, dies an Gegenbeispielen zu nachzuweisen. RICHARD DEDEKIND zeigt, daß $R = \mathbb{Z}[\frac{1}{2}(1 + \sqrt{-19})]$ ein Hauptidealring ist (vgl. das bekannte Lehrbuch: Dirichlet-Dedekind: *Vorlesungen über Zahlentheorie*. 4. Aufl 1894). THEODORE MOTZKIN zeigt in dem Aufsatz *The Euclidean algorithm*. Bull. Amer. Math. Soc. 55, (1949), pp. 1142–1146, daß R kein euklidischer Ring ist. Eine elementare Darstellung beider Aussagen findet man bei JACK WILSON: *A principal ideal ring that is not a eulidean ring*, Mathematics Magazine vol. 46, No. 1 (1973), pp. 34-38). MOTZKIN und WILSON verwenden eine Definition des Begriffs Euklidischer Ring, die scheinbar enger ist, als die von uns verwendete. Daß dem nicht so ist, zeigt PIERRE SAMUEL: *About Euclidean Rings*. J. Alg. vol. 19 (1971), pp. 282 - 301. Details dazu im Abschnitt 5.7

5.3. **Der euklidische Algorithmus.**

Unter dem euklidischen Algorithmus versteht man das folgende Verfahren, um zu gegebenen a, b in einem euklidischen Ring (A, δ) einen größten gemeinsamen Teiler d und Bézout-Koeffizienten zu berechnen.

Wir setzen $a_0 = a$ und $a_1 = b$ und berechnen a_n rekursiv wie folgt: Es sei $n \geq 1$ und a_n schon berechnet. Falls $a_n = 0$ bricht das Verfahren ab. Andernfalls gibt es Elemente $q_n, a_{n+1} \in A$ mit

$$a_{n-1} = q_n a_n + a_{n+1} \qquad \text{und} \quad a_{n+1} = 0 \quad \text{oder} \quad \delta(a_{n+1}) < \delta(a_n).$$

Dieses Verfahren muß abbrechen, d.h. man muß nach endlich vielen Schritten auf ein Element $a_n = 0$ stoßen, weil andernfalls $(\delta(a_n))$ eine strikt monoton fallende Folge natürlicher Zahlen wäre.

Aus der trivialen Umformung

$$a_{n-1} = q_n a_n + a_{n+1} \qquad \Leftrightarrow \qquad a_{n+1} = a_{n-1} - q_n a_n$$

folgt: Jeder (größte) gemeinsame Teiler von a_{n-1} und a_n ist auch ein (größter) gemeinsamer Teiler von a_n und a_{n+1} und umgekehrt. Wenn das Verfahren mit $a_{N+1} = 0$ abbricht, so gilt offenbar $a_N | a_{N-1}$. Deshalb ist a_N ein größter gemeinsamer Teiler des Paares (a_{N-1}, a_N) und damit auch des Paares $(a_0, a_1) = (a, b)$. Zusammengefaßt:

Das letzte nichtverschwindende Glied der Folge $(a_1, a_2, \ldots)$ ist ein größter gemeinsamer Teiler von a und b.

Zur Berechnung der Bézout-Koeffizienten betrachten wir die Identitäten

$$\begin{aligned} a_0 &= q_1 a_1 + a_2 \\ a_1 &= q_2 a_2 + a_3 \\ &\vdots \\ a_{N-2} &= q_{N-1} a_{N-1} + a_N \\ a_{N_1} &= q_N a_N + 0 \end{aligned}$$

und machen den Ansatz

$$a_i = \alpha_i a + \beta_i b, \tag{5.1}$$

mit $(\alpha_0, \beta_0) = (1, 0)$ und $(\alpha_1, \beta_1) = (0, 1)$. Aus $a_{n+1} = a_{n-1} - q_n a_n$ folgt rekursiv:

$$a_{n+1} = (\alpha_{n-1} a + \beta_{n-1} b) - q_n(\alpha_n a + \beta_n b) = (\alpha_{n-1} - q_n \alpha_n) a + (\beta_{n-1} - q_n \beta_n) b,$$

also

$$\alpha_{n+1} = \alpha_{n-1} - q_n \alpha_n, \quad \beta_{n+1} = \beta_{n-1} - q_n \beta_n.$$

Die Bézoutkoeffizienten genügen also exakt denselben Rekursionsgleichungen wie die a_n selbst, und man erhält für den größten gemeinsamen Teiler die Darstellung

$$a_N = \alpha_N a + \beta_N b.$$

Beispiel 5.9. — Es seien $a = 412$ und $b = 34$ im euklidischen Ring $\mathbb{Z}$ vorgegeben. Der euklidische Algorithmus verläuft dann so:

$$\begin{aligned} 412 &= 12 \cdot 34 + 4 \\ 34 &= 8 \cdot 4 + 2 \\ 4 &= 2 \cdot 2 + 0. \end{aligned}$$

Deshalb ist 2 ein größter gemeinsamer Teiler von 412 und 34 (aber -2 auch!), und die Bézout-Koeffizienten findet man so:

$$\begin{aligned} 412 &= 1 \cdot 412 + 0 \cdot 34 \\ 34 &= 0 \cdot 412 + 1 \cdot 34 \\ 4 &= 1 \cdot 412 - 12 \cdot 34 \\ 2 &= (0 - 8 \cdot 1) \cdot 412 + (1 - 8 \cdot (-12)) \cdot 34, \end{aligned}$$

also $2 = (-8) \cdot 412 + 97 \cdot 34$.

5.4. **Lineare Kongruenzen.** GAUSS hat in den 1801 erschienenen *Disquisitiones Arithmeticae* die folgende Notation eingeführt: Er nennt zwei ganze Zahlen $a, b \in \mathbb{Z}$ kongruent nach dem Modul $m \in \mathbb{N}$, wenn $m|(a-b)$, und schreibt in diesem Falle

$$a \equiv b \bmod m. \tag{5.2}$$

Das Kongruenzzeichen $\equiv$ ist dabei bewußt so gewählt, daß es an ein Gleichheitszeichen erinnert. In moderner Sprache betrachtet man das von m erzeugte Hauptideal (m) und geht zum Faktorring $\mathbb{Z}/(m)$ über, den wir in der Regel kürzer $\mathbb{Z}/m$ schreiben. Die Aussage (5.2) ist dann äquivalent zu der Aussage, daß a und b dieselbe Restklasse in $\mathbb{Z}/m$ haben. Wir erweitern die Begriffsbildung für beliebige Ideale I in kommutativen Ringen A und verwenden mit äquivalenter Bedeutung die Schreibweisen:

$$a \equiv b \bmod I \quad \Leftrightarrow \quad a - b \in I \quad \Leftrightarrow \quad \bar{a} = \bar{b} \in A/I.$$

Unter einer linearen Kongruenz in $\mathbb{Z}$ versteht man eine Gleichung der Form

$$ax \equiv b \bmod m.$$

Dazu sind eigentlich zwei Zahlen $x, y \in \mathbb{Z}$ mit

$$ax + my = b$$

zu bestimmen.

Satz 5.10 — *Es seien $a, b, m \in \mathbb{Z}$, $m \neq 0$, und d ein größter gemeinsamer Teiler von a und m. Die lineare Kongruenz*

$$ax \equiv b \bmod m$$

hat genau dann eine Lösung, wenn b ein Vielfaches von d ist, etwa $b = \ell d$. Gilt $d = \alpha a + \mu m$ mit Bézoutkoeffizienten $\alpha, \mu \in \mathbb{Z}$, so sind alle Lösungen der Kongruenz von der Form

$$x \equiv \ell\alpha \bmod m/d.$$

Beweis. Wenn es eine Darstellung $b = ax + my$ gibt, liegt b definitionsgemäß im Ideal $(a, m) = (d)$ und ist ein Vielfaches von d. Die Bedingung ist also sicher notwendig. Ist umgekehrt $b = \ell d$ und $d = \alpha a + \mu m$, so erhält man durch Multiplikation mit ℓ die Aussage $b = \ell d = (\ell\alpha)a + (\ell\mu)m$. Deshalb ist $x = \ell\alpha$ eine Lösung der Kongruenz. Damit schließlich eine andere Zahl $x' = x + u$ die Kongruenz löst, muß gelten $m|(au)$. Das ist äquivalent zu der Aussage $(m/d)|(a/d)u$, und weil m/d und a/d teilerfremd sind, bedeutet dies $m/d \mid u$, also $x' \equiv x \bmod m/d$. □

Der Satz gilt analog mit identischem Beweis für jeden nullteilerfreien Hauptidealring.

Man beachte, daß die Kongruenz, falls sie überhaupt lösbar ist, eine eindeutige Lösung x_0 nach dem möglicherweise kleineren Modul m/d hat, die aber in mehrere Klassen

$$x_0, \quad x_0 + \frac{m}{d}, \quad \ldots, \quad x_0 + (d-1)\frac{m}{d} \mod m$$

aufspaltet, falls d keine Einheit ist.

Beispiel 5.11. — Die Kongruenz $6x \equiv 4 \bmod 10$ ist lösbar, weil 2 ein ggT von $a = 6$ und $m = 10$ ist und ein Teiler von $b = 4$. Mit $4 = 2 \cdot 2$ und $2 = 2 \cdot 6 + (-1) \cdot 10$ ist $x = 2 \cdot 2 = 4$ eine Lösung, die aber nur eindeutig modulo $10/2 = 5$ ist. Bezüglich dem Ausgangsmodul 10 hat man zwei Lösungen 4 und 9.

Unter einer *simultanen linearen Kongruenz* versteht man ein System von Kongruenzen

$$\begin{aligned} a_1 x &\equiv b_1 \bmod m_1 \\ a_2 x &\equiv b_2 \bmod m_2 \\ &\vdots \\ a_n x &\equiv b_n \bmod m_n \end{aligned}$$

Nach dem gerade beschriebenen Verfahren für lineare Kongruenzen kann man jede einzelne Kongruenz so ersetzen, daß die Koeffizienten a_i der linearen Terme alle gleich 1 werden. Dabei ändern sich aber auch die Koeffizienten b_i und die Moduln m_i. Wir können also der Einfachheit halber von einem System

$$\begin{aligned} x &\equiv b_1 \bmod m_1 \\ &\vdots \\ x &\equiv b_n \bmod m_n \end{aligned} \tag{5.3}$$

ausgehen.

Satz 5.12 (Chinesischer Restklassensatz) — *Es seien $m_1, \ldots, m_n$ paarweise teilerfremde ganze Zahlen $\neq 0$. Dann hat das System* (5.3) *für beliebige $b_1, \ldots, b_n$ eine eindeutige Lösung $x \bmod m_1 \cdot \ldots \cdot m_n$.*

Beweis. Es sei $M = m_1 \cdot \ldots \cdot m_n$ und $M_i = M/m_i = m_1 \ldots m_{i-1} m_{i+1} \cdots m_n$ für alle $i = 1, \ldots, n$. Weil jedes m_i teilerfremd zu allen m_j, $j \neq i$, ist, ist m_i auch teilerfremd zu M_i. Deshalb gibt es Koeffizienten $\alpha_i, \beta_i \in \mathbb{Z}$ mit $1 = \alpha_i m_i + \beta_i M_i$. Dann hat $e_i := \beta_i M_i$ die Eigenschaften

$$e_i \equiv \delta_{ij} \bmod m_j.$$

Folglich erfüllt $x_0 := \sum_i b_i e_i$ die Bedingung

$$x_0 \equiv \sum_i b_i e_i \equiv \sum_i \delta_{ij} b_i \equiv b_j \bmod m_j$$

für alle $j = 1, \ldots, n$. Eine andere Zahl x löst dieselbe Kongruenz, wenn $m_i | (x - x_i)$ für alle i. Und weil die m_i paarweise teilerfremd sind, ist das äquivalent zu $M | (x - x_i)$. Die Lösung $x = x_0$ ist also eindeutig modulo M. □

Satz und Beweis bleiben wieder für beliebige nullteilerfreie Hauptidealringe richtig, und über euklidischen Ringen mit einer effektiven Division mit Rest ist das im Beweis verwendete Verfahren ein effektiver Algorithmus.

Man kann den Satz auch wie folgt umformulieren: Für jeden Index $i = 1, \ldots, n$ hat man eine surjektive Abbildung $\psi_i : \mathbb{Z} \to \mathbb{Z}/m_i$, und diese setzen sich zu einem Ringhomomorphismus

$$\psi = \prod_{i=1}^{n} \psi_i : \mathbb{Z} \to \mathbb{Z}/m_1 \times \ldots \times \mathbb{Z}/m_n$$

zusammen. Unter den Bedingungen des Satzes ist die Abbildung surjektiv und hat als Kern das Ideal $(m_1 \cdots m_n)$. Deshalb kann man den Satz auch so aussprechen:

Satz 5.13 — *Es seien $m_1, \ldots, m_n \in \mathbb{Z} \setminus \{0\}$ paarweise teilerfremde Zahlen. Dann ist die natürliche Abbildung*

$$\psi : \mathbb{Z}/(m_1 \cdots m_n) \longrightarrow \mathbb{Z}/m_1 \times \ldots \times \mathbb{Z}/m_n$$

ein Ringisomorphismus. □

Die im Beweis zum Chinesischen Restklassensatz konstruierten Zahlen $e_1, \ldots, e_n$ besimmen die zu ψ inverse Abbildung

$$\psi^{-1} : (\bar{b}_1, \ldots, \bar{b}_n) \mapsto b_1 e_1 + \ldots + b_n e_n.$$

Man kann den Chinesischen Restklassensatz für beliebige kommutative Ringe verallgemeinern:

Definition 5.14. — Es sei A ein kommutativer Ring. Zwei Ideale $I, J \subset A$ heißen koprim, wenn $I + J = A$.

Offenbar sind I und J genau dann koprim, wenn es $x \in I$ und $y \in J$ mit $x + y = 1$ gibt.

Satz 5.15 — *Es sei A ein kommutativer Ring mit paarweise koprimen Idealen $I_1, \ldots, I_n \to A$. Es sei weiter $p_i : A \to A/I_i$ die kanonische Projektion. Dann ist die zusammengesetzte Abbildung $p = (p_1, \ldots, p_n) : A \to A/I_1 \times \ldots A/I_n$ surjektiv mit Kern $I_1 \cap \ldots \cap I_n = I_1 \cdot \ldots \cdot I_n$. Insbesondere ist die natürliche Abbildung*

$$A/(I_1 \cdots I_n) \to A/I_1 \times \ldots \times A/I_n$$

ein Isomorphismus.

Beweis. Wir wählen für jedes Paar $i \neq j$ Elemente $a_{ij} \in I_i$ mit $a_{ij} + a_{ji} = 1$. Dann gilt $a_{ij} \equiv 0 \bmod I_i$ und $a_{ij} \equiv 1 \bmod I_j$ für alle $j \neq i$. Insbesondere hat

$$e_j := \prod_{i \neq j} a_{ij}$$

die Eigenschaft $e_j \equiv 0 \bmod I_i$ für alle $i \neq j$ und $e_j \equiv 1 \bmod I_j$. Sind also Klassen $[a_j] \in A/I_j$, $j = 1, \ldots, n$ mit Repräsentanten $a_j \in A$ vorgegeben, so hat $a := \sum_j a_j e_j$ die Eigenschaft $a \equiv a_j \bmod I_j$ für alle j. Deshalb ist p surjektiv. Der Kern von p ist offensichtlich das Ideal $I = \bigcap_j I_j$. Es bleibt zu zeigen, daß $I = I_1 \cdots I_n$. Dabei ist die Inklusion $\supset$ offensichtlich. Die Rückrichtung zeigt man durch Induktion: Im Falle $n = 2$ gilt für jedes Element $a \in I_1 \cap I_2$ die Beziehung $a = a(a_{12} + a_{21}) = aa_{12} + aa_{21}$. Weil $a_{12} \in I_2$, ist $aa_{12} \in I_1 I_2$, und weil $a_{21} \in I_2$, ist $aa_{21} \in I_1 I_2$. Das zeigt: $I_1 \cap I_2 \subset I_1 I_2$. Die Behauptung folgt nun induktiv aus der Tatsache, daß I_1 koprim zum Produkt $I_2 \cdots I_n$ ist, sofern I_1 koprim zu jedem einzelnen Ideal $I_2, \ldots, I_n$ ist:

$$A = A \cdots A = (I_1 + I_2) \cdots (I_1 + I_n) \subset I_1 + I_2 \cdots I_n.$$

□

5.5. **Einheiten in $\mathbb{Z}/n$.**

Ein Element $\bar{a} \in \mathbb{Z}/n$ ist eine Einheit, wenn es ein $\bar{x} \in \mathbb{Z}/n$ mit $\bar{a}\,\bar{x} = 1$ gibt. Das ist äquivalent zur Kongruenz $ax \equiv 1 \bmod n$. Bezeichnet wie üblich $(\mathbb{Z}/n)^\times$ die Gruppe der Einheiten in $\mathbb{Z}/n$, so folgt:

$$(\mathbb{Z}/n)^\times = \{\bar{a} \in \mathbb{Z}/n \mid 0 < a < n \text{ und } a \text{ ist teilerfremd zu } n.\}$$

Satz 5.16 — *Sind $A_1, \ldots, A_s$ kommutative Ringe, so gilt*

$$(A_1 \times \ldots \times A_s)^\times = A_1^\times \times \ldots \times A_s^\times.$$

Beweis. Addition und Multiplikation in $A_1 \times \ldots \times A_s$ werden komponentenweise ausgeführt. Deshalb ist ein Element $(a_1, \ldots, a_s)$ genau dann invertierbar, wenn jede Komponente a_i in A_i invertierbar ist. Daraus erhält man die angegebene Bijektion. Aus demselben Grund ist es auch ein Homomorphismus von Gruppen. □

Folgerung 5.17 — *Sind $m_1, \ldots, m_s$ paarweise teilerfremde natürliche Zahlen und $m = m_1 \cdot \ldots \cdot m_s$, so gilt*

$$(\mathbb{Z}/m)^\times \cong (\mathbb{Z}/m_1)^\times \times \ldots \times (\mathbb{Z}/m_s)^\times$$

Beweis. Nach dem Chinesischen Restklassensatz gilt $\mathbb{Z}/m = \mathbb{Z}/m_1 \times \ldots \times \mathbb{Z}/m_s$. Die Behauptung folgt dann aus dem vorigen Satz. □

Definition 5.18. — Die Abbildung $\varphi : \mathbb{N} \to \mathbb{N}$ mit

$$\varphi(n) = |(\mathbb{Z}/n)^\times| = |\{a \in \{1, \ldots, n-1\} \mid a \text{ teilerfremd zu } n.\}|$$

für $n \geq 2$ und $\varphi(1) = 1$ heißt EULERsche phi-Funktion.

Satz 5.19 — *Die φ-Funktion hat die folgenden Eigenschaften:*

(1) *Sind $m_1, \ldots, m_s \in \mathbb{N}$ paarweise teilerfremd, so gilt*

$$\varphi(m_1 \cdots m_s) = \varphi(m_1) \cdots \varphi(m_s).$$

(2) *Für jede Primzahl p gilt $\varphi(p^n) = p^{n-1}(p-1)$.*

(3) *Für jede natürliche Zahl n gilt*

$$\frac{\varphi(n)}{n} = \prod_{p|n \text{ prim}} \left(1 - \frac{1}{p}\right).$$

(4) *Für jede natürliche Zahl n gilt*

$$n = \sum_{d|n} \varphi(d).$$

wobei d durch alle positiven Teiler von n läuft.

Beweis. Die erste Aussage ergibt sich aus Folgerung 5.17 durch Übergang zu den Gruppenordnungen. Die zweite Aussage erhält man durch einfaches Abzählen: Eine Zahl a ist genau dann teilerfremd zu p^n, wenn sie nicht durch p teilbar ist. Die durch p teilbaren Zahlen in $\{1, \ldots, p^n\}$ sind $p, 2p, \ldots, p^{n-1}p$. Die Mächtigkeit des Komplements ist daher $p^n - p^{n-1} = p^{n-1}(p-1)$. Für die dritte Aussage zerlegt man n in Primfaktoren: $n = \prod_{p|n} p^{\nu_p}$ und schließt:

$$\varphi(n) = \prod_{p|n} \varphi(p^{\nu_p}) = \prod_{p|n} p^{\nu_p - 1}(p-1) = n \prod_{p|n} (1 - \tfrac{1}{p}).$$

Die letzte Aussage erhält man so: Jede Zahl $a \in \{1, \ldots, n\}$ hat einen eindeutig bestimmten positiven größten gemeinsamen Teiler d mit n. Weiter ist dann a/d teilerfremd zu n/d. Ist umgekehrt α teilerfremd zu n/d, so hat αd den größten gemeinsamen Teiler d mit n. Deshalb hat die Menge der a, die zum Teiler $d|n$ gehören, die Mächtigkeit $\varphi(\frac{n}{d})$. Da aber jede Zahl a zu irgendeinem Teiler gehören muß, ergibt sich: $n = \sum_{d|n} \varphi(\frac{n}{d}) = \sum_{t|n} \varphi(t)$. Die letzte Gleichung ergibt sich daraus, daß man statt über d über den komplementären Teiler $t = n/d$ summiert. □

Für eine Primzahl p ist $\varphi(p) = p - 1$, so daß $(\mathbb{Z}/p)^\times = (\mathbb{Z}/p) \setminus \{0\}$. Das ist das bekannte Ergebnis, daß

$$\mathbb{F}_p := \mathbb{Z}/p$$

ein Körper ist. Wir wollen die wichtige Aussage herleiten, daß die Einheitengruppe $\mathbb{F}_p^\times$ selbst eine zyklische Gruppe ist. Das bedeutet: Es gibt eine natürliche Zahl $g < p$ mit der Eigenschaft, daß

$$1, g, g^2, \ldots, g^{p-2}$$

ein Vertretersystem für $\mathbb{F}_p^\times$ ist. Solche Zahlen heißen *Primitivwurzeln* modulo p.

Für $p = 7$ ist $g = 3$ eine Primitivwurzel:

$$3^0 \equiv 1, \quad 3^1 \equiv 3, \quad 3^2 \equiv 2, \quad 3^3 \equiv 6, \quad 3^4 \equiv 4, \quad 3^5 \equiv 5 \mod 7.$$

Für $p = 11$ ist $g = 2$ eine Primitivwurzel:

$$2^0 \equiv 1, \quad 2^1 \equiv 2, \quad 2^2 \equiv 4, \quad 2^3 \equiv 8, \quad 2^4 \equiv 5,$$
$$2^5 \equiv 10, \quad 2^6 \equiv 9, \quad 2^7 \equiv 7, \quad 2^8 \equiv 3, \quad 2^9 \equiv 6 \mod 11.$$

Satz 5.20 — *Die Einheitengruppe $\mathbb{F}_p^\times$ ist zyklisch. Insbesondere gibt es zu jeder Primzahl p eine Primitivwurzel g mit der Eigenschaft, daß die Exponentialabbildung*

$$\mathbb{Z}/(p-1) \to (\mathbb{Z}/p)^\times, \quad m \mapsto g^m,$$

ein Gruppenisomorphismus ist. Die Anzahl der Primitivwurzeln modulo p ist $\varphi(p-1)$.

Wir zeigen gleich etwas allgemeiner:

Satz 5.21 — *Es sei K ein Körper und $G < K^\times$ eine endliche Untergruppe der Einheitengruppe von K. Dann ist G zyklisch. Genauer ist die Anzahl der Erzeuger gleich $\varphi(|G|)$. Insbesondere ist für jeden endlichen Körper $\mathbb{F}$ die Einheitengruppe $\mathbb{F}^\times$ zyklisch.*

Beweis. Es sei d die Ordnung eines Elements $a \in G$. Dann gilt $a^d = 1$. Die Potenzen a^i, $i = 0, \ldots, d-1$ sind nach Definition der Ordnung paarweise verschieden, und alle haben die Eigenschaft $(a^i)^d = (a^d)^i = 1$, sind also d verschiedene Nullstellen des Polynoms $X^d - 1 \in K[X]$. Dieses Polynom hat aber nur höchstens d Nullstellen. Deshalb ist *jedes* Element $b \in G$ der Ordnung d in der zyklischen Gruppe $\langle a \rangle \cong \mathbb{Z}/d$ enthalten. Ein Element in der additiven Gruppe $\mathbb{Z}/d$ hat die maximale Ordnung d genau dann, wenn es teilerfremd zu d ist. Deshalb gibt es in G genau $\varphi(d)$ Elemente der Ordnung d. Natürlich ist d ein Teiler der Ordnung $n := |G|$. Es sei nun $\psi(d)$ die Anzahl der Elemente der Ordnung d in G. Die bisherigen Überlegungen sagen: Entweder ist $\psi(d) = 0$ oder $\psi(d) = \varphi(d)$. Da jedes Element in G aber eine Ordnung besitzt, die n teilt, folgt mit Satz 5.19:

$$|G| = \sum_{d|n} \psi(d) \leq \sum_{d|n} \varphi(d) = n.$$

Die Endterme der Ungleichung sind gleich, deshalb muß an jeder Stelle $\psi(d) = \varphi(d)$ gelten. Insbesondere ist die Anzahl der Elemente der Ordnung $|G|$ gleich $\varphi(|G|)$. □

Folgerung 5.22 — *Es sei p eine Primzahl. Die Kongruenz $x^2 \equiv -1 \mod p$ besitzt genau dann eine Lösung, wenn $p = 2$ oder wenn $p \equiv 1 \mod 4$ ist.*

Beweis. Die Behauptung für $p = 2$ ist offensichtlich. Für jede natürliche Zahl x ist $x^2 \equiv 0 \mod 4$, falls x gerade ist, und $x^2 \equiv 1 \mod 4$, falls x ungerade ist. Die quadratische Kongruenz $x^2 \equiv -1 \mod p$ kann also keine Lösung haben, wenn $p \equiv 3 \mod 4$ ist. Es bleibt der Fall zu betrachten, daß p eine ungerade Primzahl der Form $p = 4m + 1$ ist. Es sei g eine Primitivwurzel mod p. Definitionsgemäß hat g die Ordnung $4m$. Also ist $y = g^{2m}$ nicht kongruent zu 1, genügt aber der Kongruenz $y^2 \equiv 1 \mod p$, deren einzige Lösungen 1 und -1 sind. Das bedeutet: $(g^m)^2 = g^{2m} \equiv -1 \mod p$. Somit sind $x = \pm g^m$ Lösungen der Kongruenz $x^2 \equiv -1 \mod p$. □

5.6. (*) Die Einheitengruppe von $\mathbb{Z}/p^m$.

Lemma 5.23 — *1. Es sei p eine ungerade Primzahl. Dann gilt*

$$(1 + gp^m)^p \equiv 1 + gp^{m+1} \mod p^{m+2}$$

für alle $m \geq 1$ und $g \in \mathbb{Z}$.

2. Für die Primzahl $p = 2$ gilt

$$(1 + g2^m)^2 \equiv 1 + g2^{m+1} \mod 2^{m+2}$$

für alle $m \geq 2$ und $g \in \mathbb{Z}$.

Der Unterschied ist also der Geltungsbereich für den Exponenten m. Die Behauptung ist für $p = 2$ und $m = 1$ falsch: $(1 + 2g)^2 = 1 + 8\binom{g+1}{2} \equiv 1 \bmod 2^3$.

Beweis. Für alle Primzahlen p gilt

$$(1 + gp^m)^p = 1 + gp^{m+1} + \sum_{i=2}^{p-1} \binom{p}{i} g^i p^{mi} + g^p p^{pm}.$$

Der Exponent von p in den Summanden zu $2 \leq i < p$ ist $\geq 1 + mi \geq m + 2$ für $i \geq 2$. Der Exponent von p im letzten Term ist pm, und dies ist $\geq m + 2$, sobald $m \geq 2$ oder $p \geq 3$. □

Satz 5.24 — *Es sei p eine ungerade Primzahl. Die Einheitengruppe $(\mathbb{Z}/p^n)^\times$ ist zyklisch von der Ordnung $p^{n-1}(p-1)$.*

Beweis. Jede zu p^n teilerfremde Zahl ist auch zu p teilerfremd. Durch Reduktion modulo p erhält man also eine exakte Sequenz

$$1 \longrightarrow U \longrightarrow (\mathbb{Z}/p^n)^\times \longrightarrow (\mathbb{Z}/p)^\times \longrightarrow 1.$$

Dabei ist

$$U := \{\bar{a} \in \mathbb{Z}/p^n \mid a \equiv 1 \bmod p\} = \{\overline{1 + pg} \mid g = 0, \ldots, p^{n-1}\} \tag{5.4}$$

die sogenannte Gruppe der Einseinheiten. Offenbar ist $U = |p^{n-1}|$. Wir zeigen zunächst:

1. Schritt: *U ist zyklisch mit Erzeuger $1 + p$.*

Die Ordnung von $1 + p$ ist in jedem Falle eine p-Potenz. Andererseits wissen wir aus Lemma 5.23 durch Induktion, daß $(1 + p)^{p^\ell} \equiv 1 + p^{\ell+1} \bmod p^{\ell+2}$ für alle $\ell \geq 0$. Deshalb hat $1 + p$ in U jedenfalls keine Ordnung $< p^{n-1}$.

2. Schritt: *Es gibt eine Element $g \in (\mathbb{Z}/p^n)^\times$ der Ordnung $p - 1$.*

Wir zeigen dies durch Induktion über n, wobei der Induktionsanfang einfach die Existenz einer Primitivwurzel modulo p ist. Wir nehmen also induktiv an, es sei g eine Primitivwurzel modulo p, die der verschärften Bedingung $g^{p-1} \equiv 1 \bmod p^{n-1}$ genügt, d.h. $g^{p-1} \equiv 1 + \ell p^{n-1} \bmod p^n$. Mit dem Ansaz $g' = g + xp^{n-1}$ ist g' sicher wieder eine Primitivwurzel modulo p, und es gilt

$$(g')^{p-1} \equiv 1 + \ell p^{n-1} + (p-1)g^{p-2}xp^{n-1} \bmod p^n.$$

Weil $(p - 1)$ und g Einheiten modulo p sind, kann man die Kongruenz

$$\ell + (p-1)g^{p-2}x \equiv 0 \bmod p$$

nach x auflösen. Mit einem solchen x erfüllt g' die Bedingung $(g')^{p-1} \equiv 1 \bmod p^n$.

3. Schritt: Ist g das im zweiten Schritt konstruierte Element der Ordnung $p - 1$, so erzeugen offenbar g und $1 + p$ eine Untergruppe, deren Ordnung ein Vielfaches von $p - 1$ und von p^{n-1} ist und deshalb mit $(\mathbb{Z}/p^n)^\times$ zusammenfällt. Es gilt also

$$(\mathbb{Z}/p^n)^\times \cong \langle 1 + p\rangle \times \langle g\rangle \cong \mathbb{Z}/(p-1) \times \mathbb{Z}/p^{n-1} \cong \mathbb{Z}/\varphi(p^n),$$

wie behauptet. □

Satz 5.25 — *Für $m \geq 3$ ist die Abbildung*

$$\mathbb{Z}/2 \times \mathbb{Z}/2^{m-2} \longrightarrow (\mathbb{Z}/2^m)^\times, (\varepsilon, \ell) \mapsto (-1)^\varepsilon 5^\ell,$$

ein Isomorphismus.

5.7. **(*) Minimale Euklidische Gradfunktionen.** Es gibt Definitionen des Begriffs des euklidischen Rings, die verschieden von Definition 5.3, aber dazu äquivalent sind.

Definition 5.26. — Es sei A ein Integritätsbereich. Eine Abbildung $\varphi : A \to \mathbb{N}$ ist eine *euklidische Gradfunktion*, wenn es zu $a, b \in A$ mit $b \neq 0$ stets Elemente $q, r \in A$ mit $a = bq + r$ und $0 \leq \varphi(r) < \varphi(b)$ gibt.

Wenn A eine euklidische Gradfunktion φ besitzt, ist A sicher euklidisch im Sinne von Definition 5.3. Ist umgekehrt δ eine Gradfunktion im Sinne von 5.3, genügt es, $\varphi(0) := 0$ und $\varphi(a) := \delta(a)+1$ für alle $a \neq 0$ zu setzen.

Der Grund für unsere frühere Wahl der Definition ist der, daß im Falle eines Polynomrings $K[X]$ der 'natürliche' Grad eines Polynoms die Definition 5.3 erfüllt, aber nicht 5.26. Dafür hat die neue Definition 5.26 Vorteile, die wir in diesem Abschnitt betrachten wollen. Die Ideen dazu gehen auf die folgenden Arbeiten zurück:

Theodore Motzkin: *The Euclidean algorithm*. Bull. Amer. Math. Soc. 55, (1949), pp. 1142–1146

Jack Wilson: *A principal ideal ring that is not a eulidean ring*, Mathematics Magazine vol. 46, No. 1 (1973), pp. 34-38.

Pierre Samuel: *About Euclidean Rings*. J. Alg. vol. 19 (1971), pp. 282 - 301.

Lemma 5.27 — *Es sei A ein Integritätsbereich und S die Menge aller euklidischen Gradfunktionen auf A. Wenn S nicht leer ist, ist*

$$\varphi_0(a) := \min\{\varphi(a) \mid \varphi \in S\}$$

eine euklidische Gradfunktion auf A.

Beweis. Es seien $a, b \in A$ mit $b \neq 0$ gegeben. Es gibt ein $\varphi \in S$ mit $\varphi_0(b) = \varphi(b)$. Es gibt dann $q, r \in A$ mit $a = bq + r$ und $0 \leq \varphi(r) < \varphi(b)$. Definitionsgemäß gilt dann auch $\varphi_0(r) \leq \varphi(r) < \varphi(b) = \varphi_0(b)$. □

Jeder Integritätsbereich, der also überhaupt eine euklidische Gradfunktion besitzt, hat also eine ausgezeichnete minimale solche.

Es sei also A ein Integritätsbereich mit einer minimalen euklidischen Gradfunktion. Für $n \in \mathbb{N}_0$ sei $A_n := \{a \in A \mid \varphi_0(a) = n\}$ und $A'_n = A_0 \cup A_1 \cup \ldots \cup A_n$ gesetzt, so daß $A = \bigcup_{n \geq 0} A_n$. Es gilt dann $A_0 = A'_0 = \{0\}$. Denn einerseits gilt $0 < \varphi_0(b)$ für alle $b \neq 0$ nach Definition 5.26, und andererseits gilt $\varphi_0(0) = 0$, weil man im Falle $\varphi_0(0) > 0$ durch $\varphi'(0) := 0$ und $\varphi'(a) = \varphi_0(a)$ für $a \neq 0$ eine neue Gradfunktion erhielte, die der Minimalität von φ_0 widerspräche.

Lemma 5.28 — *Für alle $n > 0$ gilt:*

$$A_n = \{a \in A \setminus A'_{n-1} \mid \textit{Die Komposition } A'_{n-1} \to A \to A/(a) \textit{ ist surjektiv.}\}.$$

Beweis. Es bezeichne B_n die rechte Seite der Identität im Lemma. Damit φ_0 eine euklische Gradfunktion ist, muß es für $a \neq 0$ in jeder Restklasse $A/(a)$ mindestens einen Vertreter r mit $\varphi(r) < \varphi(a)$ geben. Wenn also $\varphi_0(a) = n$, muß die Zusammensetzung $A'_{n-1} \to A \to A/(a)$ surjektiv sein, d.h. $a \in B_n$. Das zeigt $A_n \subset B_n$. Wenn nun umgekehrt $a \in B_n$ ist, so ist die Abbildung ψ mit $\psi(a) = n$ und $\psi(b) = \varphi_0(b)$ für alle $b \neq a$ wieder eine euklidische Normfunktion. Aus der Minimalität von φ_0 folgt $\psi = \varphi_0$, also $\varphi_0(a) = n$. Damit hat man auch die Umkehrung $B_n \subset A_n$. □

In gewissen Fällen kann man das Lemma zur Berechnung der minimalen Gradfunktion verwenden:

Beispiel 5.29. — Im Ring $\mathbb{Z}$ hat man zunächst $A_0 = \{0\}$. Die Menge A_1 besteht dann aus allen $a \in A$ mit $A/(a) = (0)$, d.h. den Einheiten von $\mathbb{Z}$, also $A_1 = \{\pm 1\}$ und $A'_1 = \{a \mid |a| < 2^1\}$. Tatsächlich gilt allgemein: $A'_n = \{a \mid |a| < 2^n\}$ wie man durch Induktion sieht. Daraus folgt: $\varphi_0(a) = \lfloor \log_2(a) + 1 \rfloor$ für $a \neq 0$. Die minimale Gradfunktion unterscheidet sich also sehr von der 'natürlichen' Gradfunktion $a \mapsto |a|$.

Beispiel 5.30. — Im Polynomring $K[X]$ über einem Körper findet man $A_0 = \{0\}$, $A_1 = K \setminus \{0\}$ und allgemein $A_n = \{f \mid \deg(f) = n+1\}$ für $n > 0$. Die minimale Gradfunktion ist also $\varphi_0(f) = \deg(f) + 1$ für $f \neq 0$.

Man kann das Lemma aber auch verwenden, um zu zeigen, daß ein gegebener Ring nicht euklidisch ist.

Satz 5.31 — *Es sei A ein Integritätsbereich. Die Mengen A_n, A'_n seien rekursiv durch die Festsetzungen $A_0 = A'_0 = \{0\}$,*

$$A_n := \{a \in A \setminus A'_{n-1} \mid A'_{n-1} \to A \to A/(a) \text{ ist surjektiv}\}$$

und $A'_n = A'_{n-1} \cup A_n$ definiert. A ist genau dann euklidisch, wenn $A = \bigcup_{n\geq 0} A_n$.

Beweis. Wenn A euklidisch ist, folgt aus Lemma 5.28, daß $A = \bigcup_{n\geq 0} A_n$. Gilt umgekehrt diese Gleichheit, so wird durch $\varphi(a) := n$ für $a \in A_n$ eine euklidische Gradfunktion definiert. die Behauptung □

Es ist aus der rekursiven Definition der Mengen A_n für einen beliebigen Integritätsbereich klar, daß die Folge $A'_0 \subset A'_1 \subset A'_2 \subset \ldots$ stationär wird, sobald einmal $A'_n = A'_{n+1}$ gilt. Daraus ergibt sich das Kriterium:

Satz 5.32 — *Ist A ein Integritätsbereich und gilt für ein $n \in \mathbb{N}$ die Beziehung $A'_n = A'_{n+1} \subsetneq A$, so ist A nicht euklidisch.* □

5.8. **(*) Der Ring $\mathbb{Z}[\frac{1}{2}(1+\sqrt{-19})]$.**

Wir betrachten den Ring $\mathbb{Z}[\omega] = \{x_0 + x_1\omega \mid x_i \in \mathbb{Z}\}$, wobei zur Abkürzung $\omega := \frac{1}{2}(1+\sqrt{19}i)$ gesetzt sei. $\mathbb{Z}[\omega]$ ist wirklich ein Ring, denn $\omega^2 = \frac{1}{4}1 + 2\sqrt{19}i - 19 = -5 + \omega$. Als Unterring des Körpers $\mathbb{C}$ ist $\mathbb{Z}[\omega]$ nullteilerfrei. Wir zeigen in diesem Unterabschnitt, daß $\mathbb{Z}[\omega]$ ein Hauptidealring, aber nicht euklidisch ist.

Die Normfunktion $N : \mathbb{Z}[\omega] \to \mathbb{R}$, $z \mapsto |z|^2$, nimmt Werte in den ganzen Zahlen, denn

$$N(x_0 + x_1\omega) = x_0^2 + x_0x_1(\omega + \overline{\omega}) + x_1^2\omega\overline{\omega} = x_0^2 + x_0x_1 + 5x_1^2,$$

und ist multiplikativ. Deshalb ist $x_0 + x_1\omega$ genau dann eine Einheit, wenn $N(x_0 + x_1\omega) = 1$. Aber die einzigen ganzzahligen Lösungen der Gleichung $x_0^2 + x_0x_1 + 5x_1^2 = 1$ sind $x_0 = \pm 1$, $x_1 = 0$. Das zeigt:

$$\mathbb{Z}[\omega]^\times = \{\pm 1\}.$$

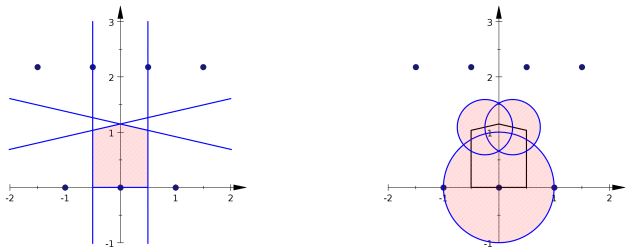
Satz 5.33 — *$\mathbb{Z}[\omega]$ ist ein Hauptidealring.*

Beweis. Es sei dazu $I \subset \mathbb{Z}[\omega]$ ein nichttriviales Ideal und $x \in I \setminus \{0\}$ ein Element mit minimaler Norm $N(x) > 0$. Falls I kein Hauptideal ist, gibt es ein Element $y \in I \setminus (x)$. Es sei y so gewählt, daß $N(y)$ minimal ist. Wir setzen $z = y/x \in \mathbb{C}^*$ und leiten eine Reihe von Ungleichungen für z her, die nicht simultan erfüllbar sind. Das liefert den gesuchten Widerspruch.

(1) Indem man gegebenenfalls y durch $-y$ ersetzt, kann man zunächst ohne Einschränkung annehmen, daß $\mathrm{Im}(z) \geq 0$.

(2) Und weil y von minimaler Norm in $I \setminus (x)$ ist, gilt $N(y) \leq N(y - ux)$ für alle $u \in \mathbb{Z}[\omega]$. Das bedeutet $N(z) \leq N(z - u)$ für alle $u \in \mathbb{Z}[\omega]$, d.h. z liegt vom Ursprung nicht weiter entfernt als von jedem anderen Punkt des Gitters $\mathbb{Z}[\omega]$.

Das läßt für z nur den folgenden schraffierten Bereich zu (linkes Bild):



(3) Weil x ein nichttriviales Element in I von minimaler Norm ist, gilt $N(uy - vx) \geq N(x)$ für alle $u, v \in \mathbb{Z}[\omega]$ mit $uy \neq vx$, also speziell $N(y) \geq N(x)$ sowie $N(2y - \omega x) \geq N(x)$ und $N(2y + \overline{\omega}x) \geq N(x)$. Deshalb muß z *außerhalb* der Vereinigung der offenen Kreisscheiben vom Radius 1 um den Ursprung und vom Radius $\frac{1}{2}$ um die Punkte $\omega/2$ und $(\omega - 1)/2 = -\overline{\omega}/2$ liegen (rechtes Bild).

Da die Kreisscheiben das schraffierte Fünfeck ganz überdecken, gibt es keine Lösungen für z. □

Wir benötigen noch einen Satz aus der Zahlentheorie:

Satz 5.34 — *Für jedes nichttriviale Elemente $u \in \mathbb{Z}[\omega]$ gilt:*

$$|\mathbb{Z}[\omega]/(u)| = N(u).$$

Beweis. 1. Schritt: Wenn $u \in \mathbb{Z}$, ist die Aussage sicher richtig: Ist nämlich $n_1, \ldots, n_{|u|} \in \mathbb{Z}$ ein Restklassensystem von $\mathbb{Z}$ modulo u, so bilden die Elemente $n_i + n_j\omega$ ein Restklassensystem von $\mathbb{Z}[\omega]$ modulo u. Die Anzahl dieser Elemente ist $|\mathbb{Z}[\omega]/(u)| = |u|^2 = N(u)$.

2. Schritt: Weil $\overline{\omega} = -\omega + 1$, geht der Unterring $\mathbb{Z}[\omega] \subset \mathbb{C}$ unter komplexer Konjugation isomorph in sich über. Dabei wird das Ideal (u) auf das Ideal $(\overline{u})$ abgebildet, und man erhält einen Ringisomorphismus $\mathbb{Z}[\omega]/(u) \to \mathbb{Z}[\omega]/(\overline{u})$, $a \bmod u \ \mapsto \overline{a} \bmod \overline{u}$. Das zeigt: $|\mathbb{Z}[\omega]/(u)| = |\mathbb{Z}[\omega]/(\overline{u})|$, und es gilt sowieso $N(u) = N(\overline{u})$.

3. Für beliebige nichttriviale Elemente $u, v \in \mathbb{Z}[\omega]$ gilt $N(uv) = N(u)N(v)$ und

$$|\mathbb{Z}[\omega]/(uv)| = |\mathbb{Z}[\omega]/(u)| \cdot |\mathbb{Z}[\omega]/(v)|.$$

Weil nämlich $(uv) \subset (u)$, hat man einen natürlichen surjektiven Ringhomomorphismus

$$\pi : \mathbb{Z}[\omega]/(uv) \to \mathbb{Z}[\omega]/(u), \quad a \bmod uv \mapsto a \bmod u.$$

Der Kern besteht aus allen Restklassen der Form $tu \bmod vu$ mit $t \in \mathbb{Z}[\omega]$. Deshalb ist die Abbildung $\mathbb{Z}[\omega]/(v) \to \ker(\pi)$, $t \bmod v \mapsto tu \bmod vu$ ein Isomorphismus von Gruppen. Es folgt:

$$|\mathbb{Z}[\omega]/(u)| = [\mathbb{Z}[\omega]/(uv) : \ker(\pi)] = |\mathbb{Z}[\omega]/(uv)| \ / \ |\mathbb{Z}[\omega]/(v)|,$$

wie behauptet.

4. Für ein beliebiges nichttriviales u ist $a := u\overline{u} \in \mathbb{Z}$. Deshalb schließt man wie folgt:

$$\begin{aligned} |\mathbb{Z}[\omega]/(u)|^2 &= |\mathbb{Z}[\omega]/(u)| \cdot |\mathbb{Z}[\omega]/(\overline{u})| = |\mathbb{Z}[\omega]/(u\overline{u})| \\ &= |\mathbb{Z}[\omega]/(a)| = N(a) = N(u\overline{u}) = N(u)N(\overline{u}) = N(u)^2. \end{aligned}$$

Das war zu zeigen. □

Damit haben wir alle Bausteine zusammen, um den letzten Stein der Gesamtargumentation zu setzen:

Satz 5.35 — *$\mathbb{Z}[\omega]$ ist nicht euklidisch.*

Beweis. Wir wollen das Kriterium 5.32 verwenden. Man hat $A_0 = \{0\}$ und $A_1 = \mathbb{Z}[\omega]^\times = \{\pm 1\}$. Deshalb hat $A_1' = \{-1, 0, 1\}$ drei Elemente, und wenn $A_1' \to A/(a)$ für ein $a \in A_2$ surjektiv sein

soll, darf $A/(a)$ höchstens aus 3 Restklassen bestehen. Nach dem vorstehenden Lemma geht das nur, wenn $N(a) \leq 3$. Aber die einzigen ganzzahligen Lösungen der Ungleichung

$$N(x_0 + x_1\omega) = x_0^2 + x_0x_1 + 5x_1^2 = (x_0 + \tfrac{1}{2}x_1)^2 + \tfrac{19}{4}x_1^2 \leq 3$$

sind $x_1 = 0$ und $x_0^2 \leq 1$, also $x_0 + x_1\omega \in A_1'$. Deshalb ist A_2 leer. Aus $A_1' = A_2'$ folgt mit 5.32, daß $\mathbb{Z}[\omega]$ nicht euklidisch ist. □

5.9. **Aufgaben.**

Aufgabe 5.36. (Satz von Wilson) — Man zeige:

(1) Es sei p eine Primzahl. Zeige, daß $(p-1)! \equiv -1 \bmod p$.
(2) Für ungerade Primzahlen der Form $p = 4m + 1$ gilt $\left(\frac{p-1}{2}!\right)^2 \equiv -1 \bmod p$.

[Hinweis: Man kann dies auf verschiedene Weisen angehen: Man gruppiert die Elemente in $(\mathbb{Z}/p)^\times$ zu Paaren $\{x, \frac{1}{x}\}$. Oder man wählt eine Primitivwurzel g modulo p.]

Aufgabe 5.37. (Primfaktorzerlegungen in $\mathbb{Z}[i]$) — Es bezeichne $\overline{\ }$ die komplexe Konjugation. Zeige:

(1) Die Einheiten in $\mathbb{Z}[i]$ sind 1, i, -1, $-i$.
(2) Wenn $\pi = a + bi$ ein Primelement in $\mathbb{Z}[i]$ ist und ein Primfaktor von $n \in \mathbb{Z}$, so ist $\pi\overline{\pi}$ ein Teiler von n.
(3) Alle Primelemente in $\mathbb{Z}[i]$ sind bis auf Einheiten entweder Primzahlen aus $\mathbb{Z}$ oder von der Form $a + bi$ mit natürlichen Zahlen a, b, für die $a^2 + b^2$ eine Primzahl ist.

Zum Beispiel hat die Primfaktorzerlegungen $2 = (-i)(1+i)^2$, $5 = (2+3i)(2-3i)$ in $\mathbb{Z}[i]$, während 3 unzerlegbar ist, weil sich 3 nicht in der Form $a^2 + b^2$ mit ganzen Zahlen $a, b \in \mathbb{Z}$ schreiben läßt. Zeige:

(4) Ist p eine Primzahl mit $p \equiv 3 \bmod 4$, so ist p auch in $\mathbb{Z}[i]$ prim.
(5) Ist $p \equiv 1 \bmod 4$, so gibt es natürliche Zahlen a, b mit $a^2 + b^2 = p$. Insbesondere ist p in $\mathbb{Z}[i]$ nicht prim, sondern besitzt eine Faktorisierung $p = (a + bi)(a - bi)$.

[Hinweise zu (5): Wähle m mit $m^2 \equiv -1 \bmod p$, so daß also $m^2 + 1 = p\ell$, und bestimme einen ggT für p und $m + i$ in $\mathbb{Z}[i]$.]

Aufgabe 5.38. — Bekanntlich gilt die Formel $(a^2+b^2)(c^2+d^2) = (ac-bd)^2+(ad+bc)^2$. Zeige: Eine natürliche Zahl n läßt sich genau dann also Summe von genau zwei Quadratzahlen schreiben, wenn n keinen ungeraden Primfaktor p mit $p \equiv 3 \bmod 4$ hat. (Unter einer Quadratzahl wird hier eine Zahl der Form u^2 mit $u \in \mathbb{Z}$ verstanden.)

Aufgabe 5.39. (Euklidischer Algorithmus im Ring der Hurwitzquaternionen) — Wir betrachen im Ring $\mathbb{H}$ der Quaternionen die Teilmenge

$$\mathcal{H} := \{\tfrac{1}{2}(a + bi + cj + dk) \mid a, b, c, d \in \mathbb{Z}, \text{die alle gerade oder alle ungerade sind.}\}.$$

Zeige:

(1) $\mathcal{H}$ ist ein (nichtkommutativer) Ring mit 1, der $\mathbb{Z}\langle 1, i, j, k\rangle$ als Unterring enthält.
(2) Für alle $z \in \mathcal{H}$ ist $\delta(z) := z\overline{z}$ ganzzahlig, und es gilt $\delta(zw) = \delta(z)\delta(w)$.
(3) Für alle $z \in \mathbb{H}$ gibt es ein $q \in \mathcal{H}$ mit $\delta(z - q) < 1$.

Der Ring $\mathcal{H}$ ist nichtkommutativ. Deshalb müssen wir bei der Division mit Rest eine linke und eine rechte Variante unterscheiden. Zeige:

(4) Sind $a, b \in \mathcal{H}$ mit $b \neq 0$, so gibt es Elemente q_1, r_1 und $q_2, r_2 \in \mathcal{H}$ mit $a = bq_1 + r_1 = q_2b + r_2$ und $\delta(r_1) < \delta(b)$ und $\delta(r_2) < \delta(b)$.

§6. Faktorielle Ringe

6.1. Primfaktorzerlegungen.

Definition 6.1. — Es sei A ein Integritätsbereich und $f \in A \setminus (\{0\} \cup A^\times)$.

(1) $f \in A$ ist irreduzibel, wenn $f = ab \;\Rightarrow\; f \sim a$ oder $f \sim b$.
(2) $f \in A$ ist prim, wenn $f|ab \;\Rightarrow\; f|a$ oder $f|b$.

Lemma 6.2 — *Jedes Primelement ist irreduzibel.*

Beweis. Es sei f prim und $f = ab$. Dann gilt ohne Einschränkung $f|a$, also $a = fc$. Daraus folgt $f = fbc$, also $f(1 - bc) = 0$. Weil A ein Integritätsbereich ist und $f \neq 0$, folgt $1 = bc$, so daß b und c Einheiten sein müssen und $f \sim a$. □

Beispiel 6.3. — Die Umkehrung ist im Allgemeinen falsch, wie das folgende Beispiel zeigt: Wir betrachten den Ring

$$A = \mathbb{Z}[\sqrt{-5}] = \{a + b\sqrt{-5} \mid a, b \in \mathbb{Z}\} \subset \mathbb{C}.$$

Die Normabbildung $N : A \to \mathbb{Z}$, $a + b\sqrt{-5} \mapsto |a + b\sqrt{-5}|^2 = a^2 + 5b^2$, ist multiplikativ, d.h. $N(xy) = N(x)N(y)$ für alle $x, y \in A$. Wenn x eine Einheit mit Inversem y ist, folgt $N(x)N(y) = N(xy) = N(1) = 1$. Umgekehrt hat $x = a + b\sqrt{-5}$ die Norm $N(x) = 1$ nur dann, wenn $a^2 + 5b^2 = 1$, was nur für $b = 0$ und $a = \pm 1$, also $x = \pm 1$ möglich ist. Deshalb sind ± 1 die einzigen Einheiten in A.

Weiter ist $z \in A$ sicher irreduzibel, wenn in jeder nichttrivialen Faktorzerlegung $N(z) = u \cdot v$ wenigstens einer der Faktoren u oder v nicht im Bild von N liegt. Nun gibt es in A die Zerlegung

$$6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5}).$$

Die Normen

$$N(2) = 4, \quad N(3) = 9, \quad N(1 \pm \sqrt{-5}) = 6$$

haben in jeder nichttrivialen Zerlegung wenigstens einen Faktor 2 oder 3, während diese Zahlen in der Menge $\mathrm{im}(N) = \{1, 4, 5, 6, \ldots\}$ nicht vorkommen. Deshalb sind 2, 3 und $1 \pm \sqrt{-5}$ irreduzibel. Aber keiner dieser Faktoren ist prim, denn aus $2 \cdot 3 = (1+\sqrt{-5})(1-\sqrt{-5})$ müßte für einen primen Faktor folgen, daß er einen der beiden Faktoren auf der anderen Seite teilt. Dasselbe müßte dann für ihre Normen gelten. Aber zwischen 4, 6 und 9 gibt es keine Teilbarkeitsbeziehungen.

All das zeigt, daß $2, 3$ und $1 \pm \sqrt{-5}$ irreduzible Elemente in $\mathbb{Z}[\sqrt{-5}]$ sind, die aber nicht prim sind. □

Definition 6.4. — Ein kommutativer Ring A heißt *faktoriell*, wenn A nullteilerfrei ist und wenn jedes Element $a \in A \setminus \{0\}$ eine Produktdarstellung $a = \epsilon \cdot p_1 \cdot \ldots \cdot p_\ell$ mit einer Einheit $\epsilon \in A^\times$ und primen Elementen p_i, $i = 1, \ldots, \ell$, $\ell \in \mathbb{N}_0$, besitzt.

Lemma 6.5 — *Es sei A ein faktorieller Ring und $a \in A \setminus \{0\}$. Die Primfaktorzerlegung $a = \epsilon \cdot p_1 \cdot \ldots \cdot p_\ell$ ist eindeutig bis auf Einheiten und die Reihenfolge der Faktoren, d.h. sind $a = \epsilon \cdot p_1 \cdot \ldots \cdot p_\ell$ und $a = \epsilon' \cdot p'_1 \cdot \ldots \cdot p'_n$ zwei Primfaktorzerlegungen, dann gilt $\ell = n$, und es gibt eine Permutation $\pi \in S_n$ mit der Eigenschaft, daß $p_i \sim p'_{\pi(i)}$ für $i = 1, \ldots, \ell$.*

Beweis. Ohne Einschränkung ist $\ell \leq n$. Wenn $\ell = 0$, ist $a = \varepsilon$ eine Einheit. Dann sind auch alle Faktoren ε' und p'_i Einheiten. Das geht nur, wenn auch $n = 0$.

Es sei also $\ell > 0$. Dann teilt p_1 das Element $a = \varepsilon' p'_1 \cdots p'_n$, also auch einen der Faktoren p'_i. Nach Umordnung kann man annehmen, daß es p'_1 ist. Es gilt nun $p'_1 = p_1 x$ mit einem $x \in A$. Da p'_1 irreduzibel ist und p_1 keine Einheit, ist x eine Einheit, d.h. $p_1 \sim p'_1$. Nach Kürzen von p_1 hat man Zerlegungen

$$\varepsilon p_2 \cdots p_\ell = (\varepsilon' x) p'_2 \cdots p'_n.$$

Induktion nach ℓ zeigt $n = \ell$ und $p_i' \sim p_i$ für $i = 2, \ldots, n$, nach passender Umordnung. □

Satz 6.6 — *Es sei A ein Integritätsbereich. A ist genau dann faktoriell, wenn gilt:*

(1) *Jedes irreduzible Element in A ist prim.*

(2) *Jede aufsteigenden Kette von Hauptidealen in A wird stationär.*

Beweis. Es sei zunächst A faktoriell und f ein irreduzibles Element. Nach Voraussetzung gibt es eine Primfaktorzerlegung $f = \varepsilon p_1 \cdots p_\ell$. Da f irreduzibel ist, gilt $f | p_i$ für ein i. Weil p_i auch irreduzibel ist, hat man $f \sim p_i$ für ein i. Insbesondere ist f prim. Weiter sei $(a_1) \subset (a_2) \subset (a_3) \subset \ldots$ eine aufsteigende Kette von Hauptidealen. Das ist äquivalent dazu, daß $a_2 | a_1$, $a_3 | a_2$, etc. Aus der Eindeutigkeit der Primfaktorzerlegung folgt, daß die Primfaktoren von a_2 bis auf Assoziation eine Teilmenge der Primfaktoren von a_1 sind. Sind die Primfaktoren einschließlich Vielfachheit gleich, unterscheiden sich a_1 und a_2 höchstens um eine Einheit, was $(a_1) = (a_2)$ impliziert. Ist also die Inklusion $(a_2) \subset (a_1)$ echt, so hat a_2 weniger Primfaktoren als a_1. In der Idealkette kann echte Inklusion demnach nur endlich oft vorkommen.

Es gelte umgekehrt die Bedingung (2). Ein Element $a \in A \setminus \{0\}$ heiße zerlegbar, wenn sich a als Produkt aus Einheiten und irreduziblen Elementen darstellen läßt. Offenbar sind alle Einheiten und alle irreduziblen Elemente zerlegbar, ebenso alle Produkte aus zerlegbaren Elementen. Angenommen, es gibt ein unzerlegbares Element $a \in A \setminus \{0\}$. Dann ist a weder eine Einheit noch irreduzibel und besitzt deshalb eine Zerlegung $a = a'a''$ in Faktoren, die beide keine Einheit sind. Wenigstens einer der Faktoren ist ebenfalls unzerlegbar, etwa a'. Wir setzen $a_1 = a$ und $a_2 = a'$ und verfahren mit a' analog. Dies führt auf eine Idealkette $(a_1) \subset (a_2) \subset \ldots$, in der alle Inklusionen echt sind, im Widerspruch zur Annahme. Demnach besitzen alle nichttrivialen Elemente in A eine multiplikative Zerlegung in irreduzible Elemente und Einheiten. Gilt zusätzlich die Bedingung (1), so besitzt jedes nichttriviale Element eine Primfaktorzerlegung. □

Satz 6.7 — *Nullteilerfreie Hauptidealringe sind faktoriell.*

Beweis. Es sei A ein nullteilerfreier Hauptidealring. Dann wird jede aufsteigende Kette von Idealen stationär. Nach Satz 6.6 genügt es zu zeigen, daß jedes irreduzible Element f prim ist. Es gelte dazu $f | ab$ und $f \nmid a$. Das Ideal (f, a) ist ein Hauptideal, etwa $(f, a) = (c)$. Es bestehen dann Gleichungen

$$f = mc, \quad a = nc, \quad c = pf + qa, \quad ab = fr$$

mit geeigneten Koeffizienten $m, n, p, q, r \in A$. Da f irreduzibel ist, ist entweder $c \sim f$ oder $c \sim 1$. Der erste Fall ist wegen $c | a$ und $f \nmid a$ ausgeschlossen. Im zweiten Falle folgt $b = (bc^{-1})c = (bc^{-1})(pf + qa) = c^{-1}(bpf + qfr) = c^{-1}(bp + qr)f$, also $f | b$. □

Es sei A ein faktorieller Ring und $D \subset A$ ein Vertretersystem für die Klassen assoziierter Primelemente, d.h. jedes Primelement ist zu genau einem Primelement in D assoziiert. In manchen Ringen läßt sich ein solches Vertretersystem durch eine einfache Konvention auszeichnen: In $\mathbb{Z}$ unterscheiden sich assoziierte Primelemente höchsten um ein Vorzeichen und wir können $D = \{p \in \mathbb{N} \mid p \text{ Primzahl}\}$ wählen. Im Polynomring $K[X]$ über einem Körper X unterscheiden sich assoziierte Primelemente höchstens um eine nichttriviale Konstante. In jeder Klasse gibt es also genau ein normiertes Polynom, d.h. ein Polynom mit Leitkoeffizienten 1, und wir können $D = \{f \mid f \text{ ist normiert und irreduzibel}\}$ setzen.

Mit einem solchen Vertretersystem D können wir jedes Element $a \in A \setminus \{0\}$ auf eindeutige Weise in der Form

$$a = u \prod_{p \in D} p^{\nu_p}$$

schreiben, wobei $\nu_p = 0$ für fast alle $p \in D$. Man nennt $\mathrm{ord}_p(a) := \nu_p$ die Ordnung von a bezüglich p. Wir setzen formal $\mathrm{ord}_p(0) := \infty$. Man verifiziert leicht die Eigenschaften:

(1) $\mathrm{ord}_p(ab) = \mathrm{ord}_p(a) + \mathrm{ord}_p(b)$ für alle $a, b \in A$ und $p \in D$.
(2) $a|b \quad \Leftrightarrow \quad \mathrm{ord}_p(a) \leq \mathrm{ord}_p(b)$ für alle $p \in D$.

Inbeondere ist für ein Tupel $a_1, \ldots, a_n \in A$, die nicht alle verschwinden, die Zahl

$$d = \prod_{d \in D} p^{\min\{\mathrm{ord}_p(a_i) \mid i=1,\ldots,n\}}$$

ein größter gemeinsamer Teiler von $a_1, \ldots, a_n$.

Zwischen den Begriffen *euklidischer Ring*, *Hauptidealbereich* und *faktorieller Ring* haben wir also die folgenden Beziehungen:

$$\{\text{euklidischer Ringe}\} \subset \{\text{Hauptidealbereiche}\} \subset \{\text{faktorielle Ringe}\} \subset \{\text{Integritätsbereiche}\}$$

In faktoriellen Ringen kann man immer größte gemeinsame Teiler finden. Diese sind aber nur durch die Primfaktorzerlegung, also multiplikativ bestimmt. In Hauptidealbereichen gibt es eine *additive* Darstellung des größten gemeinsamen Teilers, und in euklidischen Ringen kann man die zugehörigen Bézout-Koeffizienten mit dem euklidischen Algorithmus berechnen.

Die Inklusionen sind echt: Wir haben in Abschnitt 5.8 gesehen, daß der Ring $\mathbb{Z}[\frac{1}{2}(1+\sqrt{-19})]$ ein nullteilerfreier Hauptidealring, aber nicht euklidisch ist. Die Ringe $\mathbb{Z}[X]$ und $\mathbb{C}[X,Y]$ sind faktoriell, wie wir bald sehen werden (Folgerung 6.13), aber sicher keine Hauptidealringe, denn die Ideale $(2, X)$ bwz. (X, Y) sind keine Hauptideale. Und der Ring $\mathbb{Z}[\sqrt{-5}]$ ist als Unterring des Körpers $\mathbb{C}$ sicher ein Integritätsbereich, aber nach Beispiel 6.3 nicht faktoriell.

6.2. **Der Satz von Gauß.** Im Folgenden wollen wir für einen faktoriellen Ring A die Eigenschaften von $A[X]$ untersuchen. Dazu betrachten wir auch noch den Quotientenkörper $K = Q(A)$ und den zugehörigen Polynomring, so daß wir die folgenden Inklusionsverhältnisse haben:

$$\begin{array}{ccc} A & \subset & A[X] \\ \cap & & \cap \\ K & \subset & K[X] \end{array}$$

Wir verwenden, daß A nach Voraussetzung faktoriell ist und daß $K[X]$ ein Hauptidealring ist, weil K ein Körper ist.

Zunächst erweitern wir die Primfaktorzerlegung auf den Quotientenkörper: Für $a = b/c \in Q(A)^\times$ mit $b, c \in A$ und $p \in D$ bezeichne

$$\mathrm{ord}_p(a) := \mathrm{ord}_p(b) - \mathrm{ord}_p(c) \in \mathbb{Z}$$

die Ordnung von a. Um die Wohldefiniertheit zu verifizieren, ist zu zeigen, daß aus $b/c = b'/c'$ folgt $\mathrm{ord}_p(b) - \mathrm{ord}_p(c) = \mathrm{ord}_p(b') - \mathrm{ord}_p(c')$ für alle $p \in D$. Aber das folgt aus der Additivität der Ordnung, angewandt auf $bc' = b'c$. Aus der Eindeutigkeit der Primfaktorzerlegung folgt nun, daß

$$\mathrm{ord}_p : Q(A)^\times \to \mathbb{Z}$$

ein Gruppenhomomorphismus ist. Mit diesen Bezeichnungen haben wir dann für jedes $a \in Q(A)^\times$ eine eindeutige Zerlegung

$$a = u \prod_{p \in D} p^{\mathrm{ord}_p(a)}$$

mit einer Einheit $u \in A$.

Definition 6.8. — Es sei A ein faktorieller Ring, $D \subset A$ ein Repräsentantensystem der Klassen assoziierter Primelemente.

(1) Für ein Tupel $\{a_0, \ldots, a_n\}$ von Elementen in $Q(A)$, die nicht alle gleichzeitig verschwinden, heißt

$$\operatorname{Inh}(a_0, \ldots, a_n) = \prod_{p \in D} p^{\min\{\operatorname{ord}_p(a_i) | i=0,\ldots,n\}} \in Q(A)$$

der Inhalt des Tupels.

(2) Für $f = \sum_{i=0}^{n} f_n X^n \in Q(A)[X] \setminus \{0\}$ heißt $\operatorname{Inh}(f) = \operatorname{Inh}(f_0, \ldots, f_n)$ der Inhalt des Polynoms f.

(3) Ein Polynom $f \in Q(A)[X] \setminus \{0\}$ heißt primitiv, wenn $\operatorname{Inh}(f) = 1$.

Im Folgenden gehen wir, wenn von einem faktoriellen Ring A die Rede ist, immer davon aus, daß ein Vertretersystem $D \subset A$ für Primelemente gewählt ist, und die Begriffe 'Inhalt' und 'primitiv' beziehen sich stets auf dieses fest gewählte System. Man verifiziert leicht die folgenden Aussagen:

(1) Für jedes $a \in Q(A)^\times$ ist $a/\operatorname{Inh}(a)$ eine Einheit in A.

(2) Für $a \in Q(A)^\times$ und $f \in Q(A)[X] \setminus \{0\}$ gilt $\operatorname{Inh}(af) = \operatorname{Inh}(a)\operatorname{Inh}(f)$.

(3) Ein nichttriviales Polynom $f \in Q(A)[X]$ ist genau dann primitiv, wenn $f \in A[X]$ und wenn die Koeffizienten von f teilerfremd sind.

(4) Für $f \in Q(A)[X] \setminus \{0\}$ ist $f/\operatorname{Inh}(f)$ primitiv.

Es folgen eine Reihe von Sätzen, die in der Regel nach Gauß benannt werden. Gauß beweist in Disq. Arith. Art. 42 eigentlich den folgenden Satz: *Sind $f, g \in \mathbb{Q}[X]$ normierte Polynome von positivem Grad und ist $fg \in \mathbb{Z}[X]$, dann haben auch f und g ganzzahlige Koeffizienten.* Die Beweismethode verallgemeinert sich auf faktorielle Ringe und führt zu den folgenden Aussagen:

Lemma 6.9 — *Es sei A ein faktorieller Ring. Sind $f, g \in A[X]$ nichttriviale primitive Polynome, so ist auch $fg \in A[X]$ primitiv.*

Beweis. Wir machen den Ansatz

$$f = f_0 + f_1 X + \ldots + f_n X^n, \quad g = g_0 + g_1 X + \ldots + g_m X^m,$$

und $fg =: h = h_0 + h_1 X + \ldots + h_{n+m} X^{n+m}$. Es sei ein Primelement $p \in D$ fixiert. Da f und g primitiv sind, gibt es Indizes i und j mit $\operatorname{ord}_p(f_i) = 0$ und $\operatorname{ord}_p(g_j) = 0$. Es seien i_0 bzw. j_0 die größten Indizes mit dieser Eigenschaft. Das bedeutet, daß $p \not| f_{i_0}$ aber $p | f_i$ für alle $i > i_0$, und analog $p \not| g_{j_0}$ aber $p | g_i$ für alle $j > j_0$. Mit der Bezeichung $k_0 = i_0 + j_0$ gilt dann: Im Ausdruck

$$h_{k_0} = f_{i_0} g_{j_0} + \sum_{i > i_0} f_i g_{k_0 - i} + \sum_{j > j_0} f_{k_0 - j} g_j .$$

ist im zweiten Summanden jeweils der erste Faktor durch p teilbar, und im dritten Summanden jeweils der zweite Faktor. Andererseits ist $f_{i_0} g_{i_0}$ nicht durch p teilbar. Folglich ist $h_{i_0 + j_0}$ nicht durch p teilbar und somit p kein Faktor des Inhalts von h. Da dies für alle $p \in D$ gilt, ist h primitiv. □

Lemma 6.10 — *Es sei A ein faktorieller Ring. Für nichttriviale Polynome $f, g \in Q(A)[X]$ gilt:* $\operatorname{Inh}(fg) = \operatorname{Inh}(f)\operatorname{Inh}(g)$.

Beweis. Die Polynome $f/\operatorname{Inh}(f)$ und $g/\operatorname{Inh}(g)$ sind primitiv, nach Lemma 6.9 also auch der Bruch $fg/(\operatorname{Inh}(f)\operatorname{Inh}(g))$. Daraus folgt

$$1 = \operatorname{Inh}\left(\frac{fg}{\operatorname{Inh}(f)\operatorname{Inh}(g)}\right) = \frac{\operatorname{Inh}(fg)}{\operatorname{Inh}(f)\operatorname{Inh}(g)}.$$

□

Satz 6.11 — *Es sei A ein faktorieller Ring. Ein nichtkonstantes Polynom $f \in A[X]$, das in $A[X]$ irreduzibel ist, ist auch in $Q(A)[X]$ irreduzibel.*

Beweis. Es sei $f \in A[X]$ ein nichtkonstantes irreduzibles Polynom. Dann ist f insbesondere primitiv und $\mathrm{Inh}(f) = 1$. Angenommen, es gibt eine Zerlegung $f = gh$ mit nichtkonstanten Polynomen $g, h \in Q(A)[X]$. Dann gilt $1 = \mathrm{Inh}(f) = \mathrm{Inh}(g)\,\mathrm{Inh}(h)$ und somit

$$f = \frac{g}{\mathrm{Inh}(g)} \frac{h}{\mathrm{Inh}(h)}.$$

Auf der rechten Seite stehen zwei nichtkonstante Polynome in $A[X]$ im Widerspruch zur Irreduzibilität von f. □

Satz 6.12 (Satz von Gauß) — *A faktoriell $\Rightarrow$ $A[X]$ faktoriell.*

Beweis. $A[X]$ genügt der Kettenbedingung für Hauptideale: Hat man $(f_1) \subset (f_2) \subset \ldots$, so fällt der Grad der Polynome f_n monoton und muß konstant werden, etwa für alle $n \geq n_0$. Dann ist $f_n/f_{n_0} =: a_n \in A$ für $n \geq n_0$ eine Folge von Ringelementen mit $(a_n) \subset (a_{n+1}) \subset \ldots$. Weil A der Kettenbedingung für Hauptideale genügt, wird auch diese Kette stationär.

Nach Satz 6.6 genügt es zu zeigen, daß jedes in $A[X]$ irreduzible Element f prim ist. Wenn f konstant ist, ist dies klar. Es sei also f ein nicht konstantes, irreduzibles Polynom, und es gelte $f|ab$ für Polynome $a, b \in A[X]$. Nach Satz 6.11 ist f in $Q(A)[X]$ irreduzibel, und weil $Q(A)[X]$ ein Hauptidealring ist, auch prim. Ohne Einschränkung können wir daher annehmen, daß $f|a$ in $Q(A)[X]$, etwa $a = fc$ mit $c \in Q(A)[X]$. Gemäß Lemma 6.10 hat man

$$\mathrm{Inh}(a) = \mathrm{Inh}(f)\,\mathrm{Inh}(c) = \mathrm{Inh}(c) \in A.$$

Aber dann ist auch $c \in A[X]$. Deshalb ist f schon in $A[X]$ ein Teiler von a. Zusammengenommen zeigt dies, daß f prim ist. □

Durch Induktion über die Anzahl der Variablen erhält man:

Folgerung 6.13 — *Für jeden faktoriellen Ring A ist $A[X_1, \ldots, X_\ell]$ faktoriell. Insbesondere ist $\mathbb{Z}[X_1, \ldots, X_\ell]$ und für jeden Körper K auch $K[X_1, \ldots, X_\ell]$ faktoriell.*

6.3. **Irreduzibilitätskriterien.**

Die folgenden Kriterien erweisen sich als außerordentlich nützlich, wenn man die Irreduzibilität eines Polynoms testen will.

Satz 6.14 — *Es sei K ein Körper. Ein nichtkonstantes Polynom $f \in K[X]$ vom Grad ≤ 3 ist genau dann irreduzibel, wenn es keine Nullstelle hat.*

Beweis. Das ist offensichtlich: In jeder Zerlegung müßte wenigstens ein linearer Faktor vorkommen. □

Satz 6.15 (Eisensteinkriterium) — *Es sei A ein faktorieller Ring und p ein Primelement in A. Gilt für das nichtkonstante primitive Polynom $f = f_0 + \ldots + f_n X^n$, daß*

$$p \nmid f_n, \quad p|f_{n-1}, \quad \ldots, \quad p|f_0, \quad p^2 \nmid f_0,$$

so ist f in $A[X]$ irreduzibel.

Beweis. Es sei $f = gh$ eine Zerlegung mit Polynomen $g = g_0 + \ldots + g_m X^m$, $h = h_0 + \ldots + h_\ell X^\ell \in A[X]$, die keine Einheiten sind. Da f primtiv ist, sind g und h auch nicht konstant. Wir betrachten die kanonische Projektion $A[X] \to A/(p)[X]$ und schreiben $\overline{f}$ für das Bild von f etc. Nach Annahme ist $\overline{g}\overline{h} = \overline{f} = X^n$. Notwendigerweise ist dann $\overline{g} = \overline{g}_m X^m$ und $\overline{h} = \overline{h}_\ell X^\ell$. Das bedeutet, daß p ein Teiler von g_0 und von h_0 ist. Aber dann teilt p^2 das Produkt $g_0 h_0 = f_0$, im Widerspruch zur Annahme. □

Satz 6.16 (Reduktionskriterium) — *Es sei A ein faktorieller Ring und $\mathfrak{p} \subset A$ ein Primideal mit Restklassenring $\overline{A}$. Es sei $f \in A[X]$ ein nichtkonstantes primitives Polynom mit $Lc(f) \notin \mathfrak{p}$. Ist die Reduktion $\overline{f} \in \overline{A}[X]$ irreduzibel, so ist auch f irreduzibel.*

Beweis. Angenommen, f ist nicht irreduzibel und besitzt eine Zerlegung $f = gh$, in der g und h keine Einheiten sind. Da f primitiv ist, können g und h keine Konstanten sein. Die Annahme $Lc(f) \notin \mathfrak{p}$ bedeutet, daß $\overline{f}$ und f denselben Grad haben. Wegen $\overline{f} = \overline{g}\overline{h}$ haben daher auch $\overline{g}$ und $\overline{h}$ denselben Grad wie g bzw. h und sind nichtkonstante Polynome. Das Widerspricht der Annahme, daß $\overline{f}$ irreduzibel ist. □

§7. Grundbegriffe der Gruppentheorie

7.1. Gruppen, Homomorphismen, Erzeuger.

Die folgenden Grundbegriffe der Gruppentheorie sollten aus den Anfängervorlesungen bekannt sein.

Definition 7.1. — Eine Menge G mit einer assoziativen Verknüpfung $\circ : G \times G \to G$ ist eine *Halbgruppe*. Ein Element e einer Halbgruppe G ist ein Neutralelement, wenn $a \circ e = a = e \circ a$ für alle $a \in G$. Falls ein Neutralelement existiert, ist es eindeutig. Eine Halbgruppe mit einem Neutralelement ist ein *Monoid*. Wenn in einem Monoid die Relation $a \circ b = e$ besteht, heißt b ein Rechtsinverses von a und a ein Linksinverses von b. Ein Monoid ist eine *Gruppe*, wenn jedes Element ein Rechtsinverses besitzt. Die Gruppe, die nur aus dem Neutralelement besteht, heißt die triviale Gruppe und wird mit dem Symbol 1 bezeichnet.

Wenn kein anderes spezifisches Symbol für die Gruppenmultiplikation vereinbart ist, schreiben wir $a \cdot b$ und kürzer ab für die Verknüpfung und verwenden wegen der Gültigkeit des Assoziativitätsgesetzes Klammern nur zur graphischen Hervorhebung bestimmter Teile eines Produkts oder lassen sie ganz weg.

Lemma 7.2 — *Ist G eine Gruppe und b ein Rechtsinverses von a, so ist b auch ein Linksinverses von a und eindeutig bestimmt. Es gelten die Rechenregeln $e^{-1} = e$, $(a^{-1})^{-1} = a$ und $(ab)^{-1} = b^{-1}a^{-1}$.*

Man spricht deshalb einfach vom Inversen von a und schreibt es als a^{-1}

Beweis. Es sei also b ein Rechtsinverses von a und c ein Rechtsinverses von b. Dann folgt: $c = ec = (ab)c = a(bc) = ae = a$. Somit ist a ein Links- und ein Rechtsinverses von b. Ist b' ein anderes Rechtsinverses von b, so hat man $b = be = b(ab') = (ba)b' = eb' = b'$. Von den Rechenregeln sind die beiden ersten trivial, und die dritte ergibt sich aus $(ab)(b^{-1}a^{-1}) = a(bb^{-1})a^{-1} = aa^{-1} = e$. □

Definition 7.3. — Eine Halbgruppe, ein Monoid oder eine Gruppe heißt *abelsch*[8], wenn die Verknüpfung kommutativ ist, d.h. wenn $g \circ h = h \circ g$ für je zwei Elemente $g, h \in G$. Häufig wird die Verknüpfung in einer abelschen Gruppe additiv geschrieben, d.h. mit dem Symbol $+$. In diesem Falle wird das Neutralelement meist mit 0 bezeichnet und das Inverse zu g mit $-g$. Die triviale Untergruppe einer abelschen Gruppe wird in der Regel mit dem Symbol 0 bezeichnet.

Definition 7.4. — Eine Teilmenge $H \subset G$ ist eine *Untergruppe*, wenn H nicht leer ist, wenn $h \circ h' \in H$ für alle $h, h' \in H$, und wenn H mit der Einschränkung der Verknüpfung wieder eine Gruppe ist. Eine Untergruppe $H < G$ heißt *normal* oder ein *Normalteiler*, wenn $ghg^{-1} \in H$ für alle $h \in H$ und $g \in G$.

Um zu prüfen, ob eine nichtleere Teilmenge $H \subset G$ eine Untergruppe ist, genügt es zu verifizieren, daß $gh^{-1} \in H$ für alle $g, h \in H$. Gelegentlich schreiben wir $H < G$, um auszudrücken, daß H eine Untergruppe von G ist. Wir schreiben $H \lhd G$ um auszudrücken, daß H ein Normalteiler von G ist.

Beispiele 7.5. — 1. In abelschen Gruppen ist jede Untergruppe ein Normalteiler.
2. Das *Zentrum* einer Gruppe ist die Menge

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

[8]Niels Abel, norwegischer Mathematiker, ⋆5. August 1802 auf Finnøy, †6. April 1829 in Froland.

Das Zentrum ist ein Normalteiler von G.
3. Ist $H \subset G$ eine Untergruppe, so heißt

$$Z_G(H) := \{g \in G \mid ghg^{-1} = h \text{ für alle } h \in H\}$$

der Zentralisator und

$$N_G(N) := \{g \in G \mid ghg^{-1} \in H \text{ für alle } h \in H\}$$

der Normalisator von H in G. Beides sind Untergruppen in G. Es gilt $Z_G(H) \cap H = Z(H)$ und $H \subset N_G(H)$. Dabei ist H ein Normalteiler in $N_G(H)$.

Definition 7.6. — Ein *Gruppenhomomorphismus* $\varphi : G \to G'$ ist eine Abbildung von Gruppen mit $\varphi(gh) = \varphi(g)\varphi(h)$. Für einen solchen Gruppenhomomorphismus gilt stets $\varphi(e) = e'$ und $\varphi(a)^{-1} = \varphi(a^{-1})$ für alle $a \in G$. Ein Gruppenhomomorphismus φ ist ein *Isomorphismus*, wenn φ bijektiv ist. In diesem Falle ist die inverse Abbildung φ^{-1} automatisch ein Homomorphismus. Ein Isomorphismus $\varphi : G \to G$ von einer Gruppe G in sich selbst heißt *Automorphismus* von G. Wir bezeichnen einen trivialen Homomorphismus $\varphi : G \to G'$, der ganz G auf das Neutralelement $e' \in G'$ abbildet, durch $\varphi = e'$.

Ist $\varphi : G \to G'$ ein Gruppenhomomorphismus, so ist der Kern $\ker(\varphi) = \varphi^{-1}(e') \subset G$ stets ein Normalteiler, das Bild $\mathrm{im}(\varphi) = \varphi(G) \subset G'$ in der Regel aber zunächst nur eine Untergruppe.

Definition 7.7. — Eine endliche oder unendliche Folge

$$\ldots \longrightarrow G_{n-1} \xrightarrow{\varphi} G_n \xrightarrow{\psi} G_{n+1} \ldots$$

von Gruppenhomomorphismen heißt *exakt* an der Stelle G_n, wenn $\ker(\psi) = \mathrm{im}(\varphi)$.

Zum Beispiel ist eine Sequenz $1 \to G' \to G$ exakt an der Selle G', wenn $G' \to G$ injektiv ist, und $G \to G'' \to 1$ ist exakt an der Stelle G'', wenn $G \to G''$ surjektiv ist.

Definition 7.8. — Ist S eine Teilmenge einer Gruppe G, so bezeichnet $\langle S\rangle$ die von S *erzeugte Untergruppe*. Definitionsgemäß ist $\langle S\rangle = \bigcap_{S\subset H} H$, wobei H durch die Menge der Untergruppen, die S enthalten, läuft. Alternativ ist

$$\langle S\rangle = \{s_1 \cdot \ldots \cdot s_n \mid n \in \mathbb{N}_0, s_1, \ldots, s_n \in S \cup S^{-1}\}.$$

Im Falle der leeren Menge ist $\langle\emptyset\rangle = \{e\}$ die triviale Untergruppe. S ist ein *Erzeugersystem* von G, wenn $G = \langle S\rangle$. Eine Gruppe heißt *endlich erzeugt*, wenn sie ein endliches Erzeugendensystem besitzt. Eine Gruppe, die von einem Element erzeugt wird, heißt *zyklisch*.

Ist G eine zyklische Gruppe mit einem Erzeuger g, so ist die Abbildung $\varphi : \mathbb{Z} \to G$, $n \mapsto g^n$, ein surjektiver Gruppenhomomorphismus. Der Kern ist entweder die trivialer Untergruppe $\{0\}$, oder die Menge $(m) = \{nm \mid n \in \mathbb{Z}\}$ einer natürlichen Zahl m. Im ersten Fall ist G isomorph zu $\mathbb{Z}$, im zweiten Fall zu $\mathbb{Z}/m$.

7.2. **Nebenklassen, Index, Faktorgruppen.**

Definition 7.9. — Für eine Untergruppe $H < G$ und ein Gruppenelement $a \in G$ bezeichnet

$$aH = \{ah \mid h \in H\}$$

die von a erzeugte *Linksnebenklasse* von H und

$$Ha = \{ha \mid h \in H\}$$

die von a erzeugte *Rechtsnebenklasse* zu H. Die Menge aller Linksnebenklassen wird mit G/H, die Menge aller Rechtsnebenklassen mit $H\backslash G$ bezeichnet.

Das Invertieren von Gruppenelementen $i : G \to G$, $g \mapsto g^{-1}$, bildet die Linksnebenklasse aH bijektiv auf die Rechtsnebenklasse Ha^{-1} ab. Die so definierte Abbildung $G/H \to H\backslash G$, $aH \mapsto Ha^{-1}$, ist eine Bijektion. Dies führt auf den Begriff des Indexes einer Untergruppe:

Definition 7.10. — Es sei $H \subset G$ eine Untergruppe.

$$[G : H] := |G/H| = |H\backslash G|$$

heißt der Index von H in G.

Satz 7.11 (Satz von Lagrange[9]) — *Für jede Untergruppe H von G gilt*

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

Dabei spielt es keine Rolle, ob G oder H endliche oder unendliche Gruppen sind. □

Beweis. Offensichtlich haben alle Nebenklassen dieselbe Mächtigkeit wie H. Außerdem sind je zwei Links- bzw. Rechtsnebenklassen entweder disjunkt oder gleich, d.h. G ist die disjunkte Vereinigung ihrer Links- bzw. Rechtsnebenklassen. Die Mächtigkeit jeder Linksnebenklasse ist $|H|$, die Mächtigkeit der Menge der Linksnebenklassen ist $[G : H]$. Daraus folgt die Behauptung. □

Definition 7.12. — Es sei G eine Gruppe. Für $g \in G$ heißt

$$\mathrm{ord}(g) := \inf\{n \in \mathbb{N} \mid g^n = e\} \in \mathbb{N} \cup \{\infty\}$$

die Ordnung von g.

Es gilt: $\mathrm{ord}(g) = |\langle g \rangle|$. Mit dem Satz von Lagrange folgt, daß die Ordnung jedes Elements $g \in G$ die Gruppenordnung $|G|$ teilt.

Eine Untergruppe N ist genau dann ein Normalteiler, wenn $aN = Na$ für alle $a \in G$. In diesem Falle sind die Mengen G/N und $N\backslash G$ nicht nur gleichmächtig, sondern tatsächlich gleich.

Satz 7.13 (Hölder[10]) — *Es sei $N \lhd G$ ein Normalteiler. Es gibt genau eine Gruppenstruktur auf G/N, bezüglich der die kanonische Projektion $\pi : G \to G/N$ ein Gruppenhomomorphismus ist. G/N mit dieser Gruppenstruktur heißt Faktorgruppe zum Normalteiler N.*

Beweis. Da $\pi : G \to G/N$ surjektiv ist, ist die Gruppenstruktur durch die Forderung

$$g_1N \cdot g_2N = \pi(g_1) \cdot \pi(g_2) = \pi(g_1g_2) = g_1g_2N$$

eindeutig bestimmt. Definiert man umgekehrt die Verknüpfung auf die angegebene Weise, so ist zunächst zu zeigen, daß $\cdot$ wohldefiniert ist. In der Tat, falls $g_1N = g_1'N$ und $g_2N = g_2'N$, so gibt es $n_1, n_2 \in N$ mit $g_1' = g_1n_1$ und $g_2' = g_2n_2$. Daraus folgt

$$g_1'g_2' = g_1n_1g_2n_2 = g_1g_2(g_2^{-1}n_1g_2)n_2.$$

Weil N ein Normalteiler ist, gilt $(g_2^{-1}n_1g_2)n_2 \in N$, was zu zeigen war. Jetzt folgt leicht, daß $\cdot$ eine Gruppenstruktur und π ein Homomorphismus ist. □

Satz 7.14 (Homomorphiesatz) — *Es sei $\varphi : G \to G'$ ein Gruppenhomomorphismus. Dann induziert φ einen Isomorphismus $G/\ker(\varphi) \to \mathrm{im}(\varphi)$.*

Beweis. Indem wir G' durch $\varphi(G)$ ersetzen, können wir ohne Einschränkung annehmen, daß φ surjektiv ist. Es sei $N = \ker(\varphi)$. Nun folgt: $\varphi(g_1) = \varphi(g_2)$ genau dann, wenn $g_1^{-1}g_2 \in N$, d.h. wenn $g_1N = g_2N$. Deshalb ist $\bar{\varphi} : G/N \to G'$, $g_1N \mapsto \varphi(g_1)$, wohldefiniert, ein Gruppenhomomorphismus und bijektiv. □

---

[9] Joseph-Louis Lagrange, italienischer Mathematiker, ⋆25. Januar 1736 Turin, †10. April 1813 Paris.

[10] Otto Ludwig Hölder, ⋆22. Dezember 1859 in Stuttgart, †29. August 1937 in Leipzig.

Satz 7.15 (Universelle Eigenschaft der Faktorgruppe) — *Es sei G eine Gruppe, $N \lhd G$ ein Normalteiler und $\pi : G \to G/N$ die kanonische Projektion. Ein Gruppenhomomorphismus $\varphi : G \to G'$ faktorisiert genau dann über G/N, d.h. es gibt einen Homomorphismus $\bar{\varphi} : G/N \to G'$ mit $\varphi = \bar{\varphi} \circ \pi$, wenn $N \subset \ker(\varphi)$.*

Beweis. Wenn $\bar{\varphi}$ existiert, so gilt $\varphi(N) = \bar{\varphi}(\pi(N)) = \bar{\varphi}(\bar{e}) = e'$, d.h. $N \subset \ker(\varphi)$. Wir nehmen umgekehrt an, die Bedingung $N \subset \ker(\varphi)$ sei erfüllt. Dann gilt für zwei Repräsentanten g_1, g_2 derselben Nebenklasse $g_1 N = g_2 N \in G/N$, daß $g_1^{-1} g_2 \in N$, also $\varphi(g_1)^{-1}\varphi(g_2) = e'$ oder $\varphi(g_1) = \varphi(g_2)$. Das zeigt, daß $\bar{\varphi}(g_1 N) := \varphi(g_1)$ wohldefiniert ist. Es folgt dann sofort, daß $\bar{\varphi}$ ein Gruppenhomomorphismus ist, und nach Konstruktion gilt $\bar{\varphi} \circ \pi = \varphi$. □

7.3. **Konjugationsklassen, Automorphismen, semidirekte Produkte.**

Es sei im Folgenden G eine multiplikativ geschriebene Gruppe mit Neutralelement e.

Definition und Satz 7.16. — Zwei Elemente $a, b \in G$ heißen *konjugiert*, wenn es ein $g \in G$ mit $b = gag^{-1}$ gibt. Konjugiert zu sein, ist eine Äquivalenzrelation. Die zugehörigen Äquivalenzklassen heißen *Konjugationsklassen*.

Beweis. Es bezeichne $a \sim b$ die Relation: Es gibt ein g mit $b = gag^{-1}$. Die Relation $\sim$ ist reflexiv, denn $a = eae^{-1}$ für alle $a \in G$, und symmetrisch, denn aus $b = gag^{-1}$ folgt $a = g^{-1}b(g^{-1})^{-1}$. Sie ist auch transitiv: Aus $b = gag^{-1}$ und $c = hbh^{-1}$ folgt $c = h(gag^{-1})h^{-1} = (hg)a(hg)^{-1}$. □

Lemma 7.17 — *Eine Untergruppe $H \subset G$ ist genau dann ein Normalteiler, wenn H mit jedem Element auch dessen gesamte Konjugationsklasse enthält.* □

Die Komposition zweiter Gruppenisomorphismen $G \to H$ und $H \to K$ ist wieder ein Isomorphismus. Insbesondere ist die Komposition zweiter Automorphismen von G wieder ein Automorphismus.

Definition 7.18. — Die Menge $\mathrm{Aut}(G)$ aller Automorphismen der Gruppe G ist eine Gruppe unter der gewöhnlichen Verknüpfung von Abbildungen und heißt *Automorphismengruppe* von G.

Satz und Definition 7.19 — *Es sei G eine Gruppe.*

(1) *Für jedes $g \in G$ ist die Abbildung $c_g : G \to G$, $a \mapsto gag^{-1}$, ein Gruppenisomorphismus, ein sogenannter innerer Automorphismus von G. Ein Automorphismus, der kein innerer Automorphismus ist, heißt äußerer Automorphismus.*

(2) *Für alle $g, h \in G$ gilt $c_g \circ c_h = c_{gh}$. Deshalb ist die Abbildung $c : G \to \mathrm{Aut}(G)$ ein Gruppenhomomorphismus.*

(3) *Es gilt $\ker(c_g) = Z(G)$. Das Bild $\mathrm{Im}(c_g) = \{c_g \mid g \in G\} =: \mathrm{Int}(G)$ ist die Untergruppe der inneren Automorphismen.*

(4) *Für jeden Automorphismus $\Phi : G \to G$ gilt $\Phi \circ c_g \circ \Phi^{-1} = c_{\Phi(g)}$. Deshalb ist $\mathrm{Int}(G)$ ein Normalteiler in $\mathrm{Aut}(G)$. Die Faktorgruppe $\mathrm{Aut}(G)/\mathrm{Int}(G) =: \mathrm{Out}(G)$ heißt äußere Automorphismengruppe.*

Die Sequenz

$$1 \longrightarrow Z(G) \xrightarrow{i} G \xrightarrow{c} \mathrm{Aut}(G) \xrightarrow{p} \mathrm{Out}(G) \longrightarrow 1$$

wo i die Inklusion und p die kanonische Projektion bezeichnen, ist exakt.

Beweis. Wegen $c_g(ab) = g(ab)g^{-1} = gag^{-1}gbg^{-1} = c_g(a)c_g(b)$ ist $c_g : G \to G$ ein Gruppenhomomorphismus. Wegen $c_g c_h(a) = g(hah^{-1})g = (gh)a(gh)^{-1} c_{gh}(a)$ gilt $c_g \circ c_h = c_{gh}$. Insbesondere ist $c_g \circ c_{g^{-1}} = c_{gg^{-1}} = c_e = \mathrm{id}_G$. Deshalb ist $c_{g^{-1}}$ invers zu c_g und somit c_g eine Bijektion, also ein Automorphismus. Es gilt $c_g = e_{\mathrm{Aut}(G)} = \mathrm{id}_g$ genau dann, wenn $a = c_g(a) = gag^{-1}$

für alle $a \in G$, d.h. wenn $ga = ag$ für alle $a \in G$. Das ist gleichbedeutend damit, daß a im Zentrum von G liegt. Wendet man einen Automorphismus Φ auf eine $c_g(x) = gxg^{-1}$ an, erhält man $(\Phi \circ c_g)(x) = \Phi(gxg^{-1}) = \Phi(g)\Phi(x)\Phi(g^{-1}) = \Phi(g)\Phi(x)\Phi(g)^{-1} = (c_{\Phi(g)} \circ \Phi)(x)$. Das zeigt $\Phi \circ c_g = c_{\Phi(g)} \circ \Phi$ oder $\Phi \circ c_g \circ \Phi^{-1} = c_{\Phi(g)}$. Das die angegebene Sequenz exakt ist, bedeutet genau, daß $Z(G)$ der Kern von c ist, und daß das Bild von c der Kern der Projektion auf $\mathrm{Out}(G)$ ist, was einfach definitionsgemäß so ist. □

Beispiele 7.20. — 1. Wenn G abelsch ist, gilt $Z(G) = G$, und jeder innere Automorphismus ist trivial.
2. Die Kleinsche Vierergruppe $V_4 \cong \mathbb{Z}/2 \times \mathbb{Z}/2$ besteht aus dem Neutralelement und drei weiteren Elementen a, b, c, für die die Relationen

$$a^2 = b^2 = c^2 = e, \quad ab = c, \quad bc = a, \quad ca = b$$

gelten. Jede Bijektion $\Phi : G \to G$, die e in sich abbildet und die übrigen Elemente permutiert, ist ein Automorphismus. Deshalb gilt:

$$\mathrm{Aut}(V_4) \cong \mathrm{Out}(V_4) \cong S_3.$$

Satz 7.21 — *Jeder Automorphismus der zyklischen Gruppe $\mathbb{Z}/n$ hat die Form $\phi_k(a) = ka$ für eine Einheit $k \in (\mathbb{Z}/n)^\times$. Die Abbildung*

$$\Psi : (\mathbb{Z}/n)^\times \longrightarrow \mathrm{Aut}(\mathbb{Z}/n), \quad k \mapsto (a \mapsto ka),$$

ist ein Gruppenisomorphismus.

Beweis. Für jedes $k \in \mathbb{Z}/n$ ist die Abbildung ϕ_k sicher ein Gruppenhomomorphismus von $\mathbb{Z}/n$ in sich. Für zwei Elemente k, ℓ gilt weiter $\phi_{kl} = \phi_k\phi_\ell$. Bezeichnet ℓ speziell das Inverse zu einer Einheit k, so gilt $\phi_k\phi_\ell = \phi_1 = \mathrm{id}$. Deshalb ist ϕ_ℓ eine zu ϕ_k inverse Abbildung. Damit ist einerseits gezeigt, daß, wenn k eine Einheit ist, ϕ_k eine Bijektion und damit ein Isomorphismus von $\mathbb{Z}/n$ ist. Und andererseits ist die Abbildung $(\mathbb{Z}/n)^\times \to \mathrm{Aut}(\mathbb{Z}/n)$, $k \mapsto c_k$, ein Gruppenhomomorphismus.

Es sei nun Φ ein beliebiger Automorphismus von $\mathbb{Z}/n$ und $k := \Phi(1)$. Für jede natürliche Zahl m gilt nun $\Phi(\overline{m}) = \Phi(\bar{1} + \ldots + \bar{1}) = \Phi(\bar{1}) + \ldots + \Phi(\bar{1}) = m\bar{1} = \overline{mk}$. Ist $d > 0$ ein ggT von k und n, so gilt $\Phi_k(n/d) = \overline{n(k/d)} = 0$, d.h. n/d ist ein Element im Kern von Φ_k und deshalb kongruent zu 0. Das ist nur möglich, wenn $d = 1$, d.h. wenn k eine Einheit in $\mathbb{Z}/n$ ist. Deshalb ist Ψ surjektiv. Schließlich ist Ψ offensichtlich injektiv, denn $\Psi(\bar{k})(\bar{1}) = \phi_k(\bar{1}) = \bar{k} \neq \mathrm{id}(\bar{1})$. □

Für eine beliebige Familie $\{G_i\}_{i \in I}$ ist das kartesische Produkt

$$\prod_{i \in I} G_i$$

mit komponentenweise definierter Verknüpfung

$$(g_i)_{i \in I} \circ (h_i)_{i \in I} \ := \ (g_i \circ h_i)_{i \in I}$$

wieder eine Gruppe, das sogenannte *direkte Produkt* der Gruppen G_i. Im Falle einer endlichen Indexmenge $I = \{i_1, \ldots, i_s\}$ schreibt man $G_{i_1} \times \ldots \times G_{i_s}$.

Es seien nun N und H zwei Gruppen und $G = N \times H$. Die Abbildungen

$$i : N \to G, n \mapsto (n, e_H), \quad \text{ und } j : H \to G, h \mapsto (e_G, h),$$

sind injektive Gruppenhomomorphismen. Wenn man N und H auf diese Weise mit ihren Bildern in G identifiziert, werden sie zu Untergruppen in G mit der Eigenschaft, daß jedes $n \in N$ mit jedem $h \in H$ kommutiert, auch wenn N und H selbst nicht abelsch sind.

Diese Konstruktion kann wie folgt variiert werden: Wir fixieren einen Gruppenhomomorphismus $\alpha : H \to \mathrm{Aut}(N)$ und definieren auf $N \times H$ wie folgt eine Verknüpfung:

$$(n, h) \circ (n', h') := (n\alpha(h)(n'), hh').$$

Lemma 7.22 — *Die Verknüpfung $\circ$ definiert eine Gruppenstruktur auf $N \times H$.*

Beweis. 1. Das Element $e = (e_N, e_H)$ ist ein Neutralelement, denn

$$(n, h) \circ (e_N, e_H) = (n\alpha(h)(e_N), he_H) = (ne_N, he_H) = (n, h)$$

weil jeder Automorphismus $\alpha(h) \in \mathrm{Aut}(N)$ das Neutralelement in sich abbildet, und

$$(e_N, e_H)(n, h) = (e_N\alpha(e_H)(n), e_H h) = (e_N n, e_H h) = (n, h),$$

weil $\alpha(e_H) = e_{\mathrm{Aut}(N)} = \mathrm{id}_N$.

2. Die Verknüpfung ist assoziativ, denn

$$\begin{aligned}
(n, h) \circ ((n', h') \circ (n'', h'')) &= (n, h) \circ (n'\alpha(h')(n''), h'h'') \\
&= (n\alpha(h)(n'\alpha(h')(n'')), h(h'h'') \\
&= (n\alpha(h)(n')(\alpha(h) \circ \alpha(h'))(n''), (hh')h'') \\
&= ((n\alpha(h)(n'))\alpha(hh')(n''), (hh')h'') \\
&= (n\alpha(h)(n'), hh') \circ (n'', h'') \\
&= ((n, h) \circ (n', h')) \circ (n'', h'').
\end{aligned}$$

3. (n, h) besitzt ein Inverses, nämlich $(\alpha(h)^{-1}(n^{-1}), h^{-1})$. □

Definition 7.23. — Die Menge $N \times H$ mit der so definierten Verknüpfung heißt ein *semidirektes Produkt* von N und H und wird mit $N \rtimes_\alpha H$ bezeichnet.

Man beachte, daß die Gruppenstruktur von der Wahl von α abhängt. Es gibt also unter Umständen viele verschiedene semidirekte Produkte von N und H.

Satz 7.24 — *Es sei $G = N \rtimes_\alpha H$ das semidirekte Produkt von N und H zum Homomorphismus $\alpha : H \to \mathrm{Aut}(N)$. Die Abbildung $i : N \to N \rtimes_\alpha H$, $n \mapsto (n, e_H)$, ist ein injektiver Gruppenhomomorphismus, dessen Bild ein Normalteiler ist. Die Abbildung $j : H \to N \times_\alpha H$, $h \mapsto (e_N, h)$, ist ein injektiver Gruppenhomomorphismus. Die Komposition $H \xrightarrow{j} G \xrightarrow{p} G/i(N)$ ist ein Isomorphismus.*

Beweis. Daß i und j injektive Homomorphismen sind, ist klar. Ebenso ist $\pi : G \to H$, $(n, h) \mapsto h$, ein surjektiver Homomorphismus mit $\pi \circ j = \mathrm{id}_H$ und $\ker(\pi) = i(N)$. Deshalb ist N ein Normalteiler, und nach dem Homomorphiesatz induziert π einen Isomorphismus $G/i(N) \to H$. □

Wenn man N und H mit ihren Bildern in $N \times_\alpha H$ vermöge i bzw. j identifiziert, kann man für $n \in N$ und $h \in H$ schreiben: $hnh^{-1} = \alpha(h)(n)$.

7.4. **Kommutatoruntergruppen.**

Es sei G eine Gruppe. Der Kommutator zweier Elemente $a, b \in G$ ist

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

Die Kommutatoruntergruppe von G ist die von allen Kommutatoren erzeugte Untergruppe. Übliche Bezeichnungen sind $[G, G]$ oder G', wobei wir die Bezeichnung G' hier meiden, weil diese Notation auch häufig schlicht zur Indizierung einer Reihe $G, G', G'', \ldots$ von Gruppen verwendet wird.

Satz 7.25 — *$[G, G]$ ist ein Normalteiler von G. Die Faktorgruppe $G^{\mathrm{ab}} := G/[G, G]$ ist abelsch.*

Beweis. Die erste Aussage folgt aus der einfachen Relation $g[a,b]g^{-1} = [gag^{-1}, gbg^{-1}]$ für alle $a, b, g \in G$. Die zweite Aussage ergibt sich aus $ab = [a,b]ba$, also $ab = ba \bmod [G,G]$. □

Definition 7.26. — Die Gruppe $G^{\mathrm{ab}} := G/[G,G]$ heißt die *Abelisierung* von G. Eine Gruppe G heißt *perfekt*, wenn $G = [G,G]$.

Satz 7.27 (Universelle Eigenschaft der Abelisierung) — *Es sei G eine Gruppe und $\pi : G \to G^{\mathrm{ab}}$ die kanonische Projektion auf die Abelisierung. Zu jedem Gruppenhomomorphismus $\varphi : G \to A$ in eine abelsche Gruppe A gibt es genau einen Gruppenhomomorphismus $\bar{\varphi} : G^{\mathrm{ab}} \to A$ mit $\varphi = \bar{\varphi} \circ \pi$.*

Beweis. Weil A abelsch ist, gilt für jeden Kommutator $[g,h] \in G$ die Beziehung $\varphi([g,h]) = \varphi(g)\varphi(h)\varphi(g)^{-1}\varphi(h) = \varphi(g)\varphi(g)^{-1}\varphi(h)\varphi(h)^{-1} = e$. Deshalb liegt $[G,G]$ im Kern von φ, und nach der universellen Eigenschaft der Faktorgruppe gibt es genau einen Gruppenhomomorphismus $\bar{\varphi} : G/[G,G] \to A$ mit $\bar{\varphi} \circ \pi = \varphi$. □

Beispiel 7.28. — Weil das Bild des Signaturhomomorphismus $\mathrm{sgn} : S_n \to \{\pm 1\}$ abelsch ist, gilt $[S_n, S_n] \subset \ker(\mathrm{sgn}) = A_n$. Andererseits hat man $[(12),(23)] = (12)(23)(12)(23) = (123)^2 = (132) \in [S_n, S_n]$. Weil A_n von 3-Zykeln erzeugt wird, hat man also auch die umgekehrte Inklusion $A_n \subset [S_n, S_n]$. Zusammengefaßt gilt also $[S_n, S_n] = A_n$ für alle $n \geq 2$.

7.5. **Endliche abelsche Gruppen.**

Definition 7.29. — Es sei G eine Gruppe.

$$\mathrm{ex}(G) := \sup\{\mathrm{ord}(g) \mid g \in G\} \in \mathbb{N} \cup \{\infty\}$$

heißt *Exponent* von G.

Satz 7.30 — *Es sei G eine abelsche Gruppe. Dann gilt $\mathrm{ord}(g) | \mathrm{ex}(G)$ für alle $g \in G$.*

Beweis. Falls $\mathrm{ex}(G) = \infty$, ist nichts zu zeigen. Andernfalls sei $x \in G$ ein Element mit $\mathrm{ord}(x) = \mathrm{ex}(G) =: n$. Jedes andere Element hat dann ebenfalls endliche Ordnung. Angenommen, es gibt ein $a \in G$ mit $\mathrm{ord}(a) \nmid n$. Dann gibt es eine Primzahl p, die die Ordnung von a häufiger teilt als die Ordnung von x. Es sei p^ℓ die maximale p-Potenz, die $\mathrm{ord}(a)$ teilt, und p^k die maximale p-Potenz, die in n aufgeht. Das Element $a' := a^{\mathrm{ord}(a)/p^\ell}$ hat genau die Ordnung p^ℓ und das Element $x' := x^{p^k}$ hat genau die zu p prime Ordnung $n' = n/p^k$.

Wir betrachten das Element $z = a'x'$ und setzen $m = \mathrm{ord}(z)$. Aus $e = z^m = b^m x^m$ folgt $a'^m = x'^{-m} \in \langle a' \rangle \cap \langle x' \rangle$. Deshalb gilt einerseits $\mathrm{ord}(a'^m) | \mathrm{ord}(a') = p^\ell$ und andererseits $\mathrm{ord}(a'^m) | \mathrm{ord}(x') = n'$. Weil p^ℓ und n' teilerfremd sind, ist $\mathrm{ord}(a'^m) = 1$ und somit $a'^m = e = x'^{-m}$. Daraus folgt $p^\ell | m$ und $n' | m$, also auch $p^{\ell-k} n = p^\ell n' | m$. Damit ist $\mathrm{ord}(z) > n = \mathrm{ord}(x)$, im Widerspruch zur Definition des Exponenten von G. □

Satz 7.31 (Hauptsatz über endliche abelsche Gruppen) — *Jede endliche abelsche Gruppe G besitzt eine Zerlegung*

$$G = \mathbb{Z}/d_1 \times \ldots \times \mathbb{Z}/d_s$$

mit natürlichen Zahlen $d_i > 1$, die der Bedingung $d_1 | d_2 | \ldots | d_s$ genügen.

Beweis. Es sei $x \in G$ ein Element mit $\mathrm{ord}(x) = \mathrm{ex}(G) =: d$. Falls $\langle x \rangle = G$ sind wir fertig. Andernfalls ist die zyklische Gruppe $\langle x \rangle$ ein echter Normalteiler in G. Es bezeichne $\varphi : G \to G' := G/\langle x \rangle$ die Projektion auf die Faktorgruppe. Weil G' eine kleinere Ordnung als G hat, können wir durch Induktion über die Gruppenordnung annehmen, daß der Satz für G' schon bewiesen ist und wir eine Zerlegung

$$G' \cong \mathbb{Z}/d_1 \times \ldots \times \mathbb{Z}/d_{s-1}$$

haben. Es seien $y_1, \ldots, y_{s+r'} \in G'$ Erzeuger der zyklischen Faktoren. Wir wählen weiter Urbilder $z_i \in G$ mit $\varphi(z_i) = y_i$ und setzen $n_i = \mathrm{ord}(z_i)$. Weil $\langle z_i \rangle \twoheadrightarrow \langle y_i \rangle$, gilt $d_i | n_i$. Das Element $z_i^{d_i}$ liegt im Kern von φ und läßt sich deshalb in der Form $z_i^{d_i} = x^{m_i}$ mit $0 \leq m_i < d$ schreiben. Aus $e = z_i^{n_i} = (z_i^{d_i})^{n_i/d_i} = x^{m_i n_i/d_i}$ folgt $d | m_i \frac{n_i}{d_i}$. und somit $\frac{d}{n_i} d_i | m_i$. Aber n_i teilt d. Deshalb ist d/n_i eine ganzen Zahl und somit d_i ein Teiler von m_i. Setze $x_i := z_i x^{-m_i/d_i}$. Dann gilt einerseits $\varphi(x_i) = y_i$, also $d_i | \mathrm{ord}(x_i)$ und andererseits $x_i^{d_i} = z_i^{d_i} x^{-m_i} = e$. Demnach haben die Elemente x_i genau die Ordnung d_i. Wir finden so einen Gruppenhomomorphismus

$$\mathbb{Z}/d_1 \times \ldots \times \mathbb{Z}/d_{s-1} \times \mathbb{Z}/d \longrightarrow G, (a_1, \ldots, a_{s_1}, a) \mapsto x_1^{a_1} \cdot \ldots \cdot x_{s_1}^{a_{s-1}} \cdot x^a,$$

der nach Konstruktion surjektiv ist. Weil beide Gruppen die gleiche Ordung haben, ist die Abbildung ein Isomorphismus von Gruppen. □

Man kann jeden Faktor $\mathbb{Z}/d_i$ nach dem chinesischen Restklassensatz weiter in ein Produkt aus zyklischen Gruppen von Primpotenzordnung zerlegen. Damit erhält man insgesamt eine Zerlegung

$$G \cong \mathbb{Z}/p_1^{m_1} \times \ldots \times \mathbb{Z}/p_s^{m_s}$$

mit nicht notwendig verschiedenen Primzahlen $p_1, \ldots, p_s$ und Exponenten $m_1, \ldots, m_s \in \mathbb{N}$.

7.6. **Aufgaben.**

Aufgabe 7.32. — Das Zentrum $Z(G)$ einer Gruppe G ist ein Normalteiler.

Aufgabe 7.33. — Es sei $\{G_i\}_{i \in I}$ eine Familie von Gruppen, $G = \prod_{i \in I} G_i$ das mengentheoretische kartesische Produkt und $\pi_i : G \to G_i$, $g = (g_j)_{j \in I} \mapsto g_i$, die Projektion auf den i-ten Faktor. Man zeige:

(1) Auf G wird für $g = (g_i)$ und $h = (h_i)$ durch $(g \cdot h)_i := g_i h_i$ eine Gruppenstruktur definiert.
(2) Die Projektionen $\pi_i : G \to G_i$ sind Gruppenhomomorphismen.
(3) (Universelle Eigenschaft) Ist H eine beliebige Gruppe mit einer Familie von Gruppenhomomorphismen $\{\psi_i : H \to G_i\}_{i \in I}$, so gibt es genau einen Gruppenhomomorphismus $\psi : H \to G$ mit der Eigenschaft $\pi_i \circ h = h_i$ für alle $i \in I$.

Die Gruppe G heißt das direkte Produkt der Gruppen $\{G_i\}_{i \in I}$.

Aufgabe 7.34. — Es sei G eine Gruppe mit Normalteilern N_1, N_2. Man zeige: $N_1 \cap N_2$ ist ein Normalteiler in G. Wenn $N_1 \cap N_2 = \{e\}$, so gilt $nm = mn$ für alle $n \in N_1$ und $m \in N_2$.

Aufgabe 7.35. — Es sei G eine Gruppe, $N \lhd G$ ein Normalteiler und $H < G$ eine Untergruppe. Man zeige:

(1) Die Menge $NH := \{nh \mid n \in N, h \in H\}$ ist eine Untergruppe in G.
(2) N ist ein Normalteiler in NH, und $N \cap H$ ist ein Normalteiler in H.
(3) Die Abbildung $\varphi : NH/N \to H/(N \cap H)$, $[nh] \mapsto [h]$, ist wohldefiniert. Dabei bezeichnet $[-]$ die Restklasse modulo N bzw. modulo $H \cap H$.
(4) φ ist ein Isomorphismus.

Aufgabe 7.36. — Es seien $N \subset H \subset G$ Normalteiler von G. Man zeige:

(1) H/N ist ein Normalteiler in G/N.
(2) Die Projektion $G \to G/N$ induziert einen Isomorphismus $G/H \to (G/N)/(H/N)$.

Aufgabe 7.37. — Es sei $C = \langle x \rangle$ eine zyklische Gruppe der Ordnung n. Man zeige:

(1) Ist $H \subset G$ eine nichttriviale Untergruppe und $a \in \mathbb{N}$ minimal mit der Eigenschaft $x^a \in H$, so gilt $a | n$, und ist eine von x^a erzeugte zyklische Gruppe der Ordnung n/a.
(2) Zu jedem Teiler $d | n$ gibt es genau eine zyklische Untergruppe $H_d < G$ der Ordnung d. Alle Untergruppen von G haben diese Form, und es gilt $H_d < H_{d'}$ genau dann, wenn $d | d'$.

Aufgabe 7.38. — Es sei $n \in \mathbb{N}$. Die Diedergruppe D_n der Ordnung $2n$ ist die Untergruppe der Gruppe $\mathrm{O}(2)$ der orthogonalen Matrizen vom Rang 2, die von einer Drehung d in der euklidischen Ebene den Winkel $2\pi/n$ und der Spiegelung $s = \left(\begin{smallmatrix} -1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$ an der x-Achse erzeugt wird. Man zeige:

(1) $\mathrm{ord}(d) = n$ und $\mathrm{ord}(s) = 2$. Es gilt $sds = d^{-1}$ und $dsd^{-1} = sd^{-2}$.

(2) Jedes Element in G hat die Form d^m oder $d^m s$ für $m = 0, \ldots, n-1$.

(3) Die von d erzeugte zyklische Untergruppe $C_n \subset D_n$ ist ein Normalteiler.

(4) Man bestimme alle Untergruppen und Normalteiler von D_n.
[Hinweis: ist $H \subset D_n$ eine Untergruppe, so ist $H \cap C_n$ eine Untergruppe in C_n, und H ist entweder gleich $H \cap C_n$ oder wird von $H \cap C$ und einer weiteren Spiegelung $d^m s$ erzeugt.]

§8. Auflösbare Gruppen

8.1. Gruppenwirkungen.

Definition 8.1. — Eine *Linkswirkung* der Gruppe G auf einer Menge X ist eine Abbildung $s : G \times X \to X$ mit der Eigenschaft $s(e,x) = x$ und $s(g, s(h,x)) = s(gh,x)$ für alle $g, h \in G$, $x \in X$. Eine G-Menge ist eine Menge X mit einer G-Wirkung. Wenn die Wirkung aus dem Kontext klar ist, schreibt man kürzer $gx := s(g,x)$. Eine Abbildung $\alpha : X \to Y$ von G-Mengen heißt G-äquivariant, wenn $\alpha(gx) = g\alpha(x)$ für alle $x \in X$ und $g \in G$.

Die Bedingung an die Wirkung liest sich in der verkürzten Notation wie die übliche Assoziativitätsbedingung: $ex = x$, $g(hx) = (gh)x$ für $e, g, h \in G$ und $x \in X$. Man muß aber immer daran denken, daß g, h und x aus ganz verschiedenen Mengen stammen.

Analog definiert man eine Wirkung von rechts als eine Abbildung $t : X \times G \to X$ mit $t(t(x,g),h)) = t(x,gh)$ und $t(x,e) = x$. Man kann auf die folgende Weise stets eine Rechtswirkung t in eine Linkswirkung s umwandeln und umgekehrt:

$$s(g,x) := t(x, g^{-1}).$$

Im Folgenden betrachten wir deshalb der Einfachheit halber nur Linkswirkungen. Alle Begriffe übertragen sich in analoger Weise auf Rechtswirkungen.

Definition 8.2. — Es sei X eine G-Menge. Die *Bahn* (oder der Orbit) von $x \in X$ ist die Menge $\mathcal{O}_x = Gx := \{gx \mid g \in G\}$. Die *Standgruppe* (oder Isotropie- oder Stabilisatorgruppe) von $x \in X$ ist die Untergruppe $G_x := \mathrm{Stab}_G(x) := \{g \in G \mid gx = x\}$. Der *Bahnenraum* ist die Menge aller Bahnen und wird für eine Linkswirkung mit $G\backslash X$ und für eine Rechtswirkung mit X/G bezeichnet. Die kanonische Projektion $\pi : X \to G\backslash X$ bildet jedes $x \in X$ auf seine Bahn ab. Eine Wirkung heißt *transitiv*, wenn alle Elemente von X in einer Bahn liegen. Die Wirkung ist *frei*, wenn alle Standgruppen trivial sind. Schließlich ist $x \in X$ ein *Fixpunkt*, wenn $Gx = \{x\}$, oder anders gesagt, wenn $G_x = G$. Die Menge aller Fixpunkte wird mit X^G bezeichnet.

Das Symbol $G\backslash X$ kann mit der mengentheoretischen Subtraktion $G \setminus X$ ('ohne') verwechselt werden. Deshalb und aus ästhetischen Gründen schreibt man auch bei Linkswirkungen häufig X/G für den Bahnenraum und verwendet die andere Schreibweise nur dann, wenn gleichzeitig Links- und Rechtswirkungen betrachtet und unterschieden werden müssen.

Beispiel 8.3. — Die Gruppe $G = \mathrm{SO}(2)$ wirkt auf der Einheitssphäre $S^2 \subset \mathbb{R}^3$ durch Verdrehung der ersten beiden Koordinaten:

$$\left(\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right), \begin{pmatrix} x \\ y \\ z \end{pmatrix} \right) \mapsto \begin{pmatrix} ax+by \\ cx+dy \\ z \end{pmatrix}.$$

Es gibt zwei Fixpunkte: die beiden Pole $\pm \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}$. Die Bahnen dieser Wirkung sind genau die Pole und die Breitenkreise. Die Standgruppe von $y \in S^2$ ist die volle Gruppe $\mathrm{SO}(2)$, wenn y ein Pol ist, und sonst die triviale Gruppe.

Beispiel 8.4. — Die Symmetrische Gruppe S_n wirkt auf der Menge $[n] = \{1, \ldots, n\}$ durch $(\pi, k) \mapsto \pi(k)$. Die Wirkung ist sicher transitiv: Sind $x, y \in [n]$ verschiedene Elemente, so bildet die Transposition $\tau = (x\,y)$ das Element x auf y ab, d.h. alle Elemente liegen in einer Bahn. Die Standgruppe jedes Elements ist isomorph zur symmetrischen Gruppe S_{n-1}.

Zwischen den Mächtigkeiten von X und seinen Bahnen und den Ordnungen von G und der Standgruppen bestehen Relationen, die durch die Bahnengleichungen präzisiert werden:

Satz 8.5 (Bahnengleichungen) — *Es sei G eine endliche Gruppe und $G \times X \to X$ eine Gruppenwirkung.*

(1) *Es gilt* $|X| = \sum_{B \in G\backslash X} |B|$.
(2) *Für jedes* $x \in X$ *gilt* $|G| = |G_x| \cdot |Gx|$ *und* $|Gx| = [G : G_x]$.

Beweis. Jedes Element von X liegt in genau einer Bahn, d.h. X ist die disjunkte Vereinigung aller Bahnen. Durch Übergang zu Mächtigkeiten folgt die erste Aussage. Es sei nun $x \in X$ beliebig. Wir betrachten die Abbildung $p : G \to Gx$, $g \mapsto gx$. Nach Konstruktion ist p surjektiv. Es sei $y \in Gx$ beliebig und $g_0 \in p^{-1}(y)$. Dann gilt $g \in p^{-1}(y)$ genau dann, wenn $gx = g_0 x$, d.h. $(g_0)^{-1}gx = x$, also $(g_0)^{-1}g \in G_x$ oder $g \in g_0 G_x$. Das bedeutet insbesondere, daß $|p^{-1}(y)| = |G_x|$ für alle $y \in Gx$. Es folgt $|G| = \sum_{y \in Gx} |p^{-1}(y)| = |Gx| \cdot |G_x|$. □

Beispiel 8.6. — Es sei $H < G$ eine Untergruppe. Dann wirkt H durch Multiplikation von links und von rechts auf G. Die Bahnen sind genau die Rechts- bzw. Linksnebenklassen. Man beachte die Vertauschung von links und rechts: die Rechtsnebenklasse von H zu a ist die Menge $Ha = \{ha \mid h \in H\}$. Die Wirkung ist frei. Die Bahnengleichung führt auf den Satz von Lagrange.

Lemma 8.7 — *Es sei* $G \times X \to X$ *eine Gruppenwirkung,* $x \in X$ *und* $g \in G$. *Dann gilt*

$$G_{gx} = gG_x g^{-1}.$$

Beweis. h liegt genau dann in G_{gx}, wenn $hgx = gx$, d.h. wenn $g^{-1}hgx = x$. Das ist genau dann der Fall, wenn $g^{-1}hg \in G_x$, oder äquivalent: wenn $h \in gG_x g^{-1}$. □

Beispiel 8.8. — Jede Gruppe G operiert auf sich selbst durch Konjugation:

$$c : G \times G \to G, \quad (g, h) \mapsto ghg^{-1}.$$

Die Standgruppe eines Elements h ist die Untergruppe

$$Z_G(h) := \{g \in G \mid gh = hg\}$$

aller Elemente, die mit h vertauschen, der sogenannte *Zentralisator* von h in G. Die Bahn von h ist die Menge $\{ghg^{-1} \mid g \in G\}$, d.h. die Konjugationsklasse von h. Schließlich ist h ein Fixpunkt, wenn h mit allen Gruppenelementen vertauscht. Anders gesagt: Die Fixpunktmenge dieser Wirkung ist das Zentrum $Z(G)$ der Gruppe.

8.2. p-Gruppen.

Definition 8.9. — Es sei p eine Primzahl. Eine endliche Gruppe G ist eine p-Gruppe, wenn $|G| = p^n$ für ein $n \in \mathbb{N}$.

Beispiel 8.10. — Es gibt fünf 2-Gruppen der Ordnung 8, die drei abelschen Gruppen $\mathbb{Z}/8$, $\mathbb{Z}/4 \times \mathbb{Z}/2$, $\mathbb{Z}/2 \times \mathbb{Z}/2 \times \mathbb{Z}/2$ und die beiden nichtabelschen Gruppen D_4 und Q_8. Dabei ist D_4 die Diedergruppe der Ordnung 8, also die Symmetriegruppe eines Quadrats, und Q_8 ist die Quaternionengruppe $Q_8 = \{\pm 1, \pm I, \pm J, \pm K\} \subset M_2(\mathbb{C})$, wobei

$$1 = \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right), \quad I = \left(\begin{smallmatrix} i & 0 \\ 0 & -i \end{smallmatrix}\right), \quad J = \left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right), \quad K = IJ.$$

Die zentrale Beobachtung, die der Ausgangspunkt für viele Strukturaussagen über p-Gruppen ist, ist das folgende einfache Lemma:

Lemma 8.11 — *Es sei* G *eine* p*-Gruppe, die auf einer endlichen Menge* X *wirkt. Dann ist* $|X| \equiv |X^G| \bmod p$, *wenn* X^G *die Fixpunktemenge der Wirkung bezeichnet.*

Beweis. Es seien $B_i \subset X$, $i = 1, \ldots, n$, die Bahnen der G-Wirkung und G_i die Standgruppen von ausgewählten Elementen $b_i \in B_i$. Dann gelten die Bahnengleichungen

$$|X| = \sum_i |B_i| \quad \text{und} \quad |B_i| = |G|/|G_i|.$$

Fixpunkte entsprechen bijektiv den Bahnen der Länge 1. Für alle anderen Bahnen ist $|B_i|$ ein nichttrivialer Teiler von $|G|$, also selbst durch p teilbar. Rechnet man modulo p, bleibt von der Bahnengleichung nur

$$|X| \equiv \sum_{x \in X^G} 1 \bmod p$$

übrig. Das war zu zeigen. □

Satz 8.12 — *Es sei G eine p-Gruppe. Dann ist das Zentrum von G nicht trivial. Insbesondere gibt es ein zentrales Element der Ordnung p.*

Beweis. Wir wenden Lemma 8.11 auf die folgende Situation an: Die Gruppe G wirke auf sich durch Konjugation. Ein Element $g \in G$ ist genau dann ein Fixpunkt, wenn es mit allen Elementen in G vertauscht, also im Zentrum liegt. Deshalb gilt $|Z(G)| \equiv |G| \equiv 0 \mod p$. Da das Zentrum aber mindestens das Neutralelement enthält, ist $|Z(G)| \geq p$. Ein beliebiges nichttriviales $x \in Z(G)$ hat die Ordnung p^m für ein $m \geq 1$. Nun ist $y = x^{p^{m-1}}$ ein zentrales Element der Ordnung p. □

Satz 8.13 — *Es sei G eine p-Gruppe. Dann gibt es eine Folge von Untergruppen*

$$\{e\} = G_0 < G_1 < \cdots < G_n = G$$

der Ordnung $|G_i| = p^i$ mit der Eigenschaft, daß G_i für jedes i ein Normalteiler in G ist.

Beweis. Es sei $x \in Z(G)$ ein Element der Ordnung p. Die von x erzeugte zyklische Untergruppe $G_1 = \langle x \rangle$ ist zentral und daher ein Normalteiler in G. Die Faktorgruppe G/G_1 ist ebenfalls eine p-Gruppe. Durch Induktion nach der Ordnung der Gruppe schließen wir auf die Existenz von Normalteilern $1 < \overline{G}_2 < \ldots < \overline{G}_n = G/G_1$ mit $|\overline{G}_k| = p^{k-1}$. Es sei G_k das Urbild von $\overline{G}_k$ unter der Projektion $G \to G/G_1$. Als Urbilder von Normalteilern sind die G_k selbst Normalteiler, und ihre Ordnung ist $|G_k| = |G_1| \cdot |\overline{G}_k| = p^k$. □

Definition 8.14. — Es sei G eine endliche Gruppe, p eine Primzahl und m die Multiplizität von p in der Ordnung von G. Eine p-Untergruppe $S \subset G$ mit $|S| = p^m$ heißt p-Sylowuntergruppe[11].

Satz 8.15 (Sylow) — *Es sei G eine endliche Gruppe und p eine Primzahl.*

(1) *G besitzt p-Sylowuntergruppen.*
(2) *Für die Anzahl s_p der p-Sylowuntergruppen gilt $s_p \mid |G|$ und $s_p \equiv 1 \bmod p$.*
(3) *Jede p-Untergruppe von G liegt in einer p-Sylowuntergruppe.*
(4) *Alle p-Sylowuntergruppen von G sind konjugiert.*

Dieser wichtige Satz wurde von Sylow zuerst in der Arbeit *Théorèmes sur les groupes de substitutions*, Math. Annalen 5 (1872), S. 584-594, bewiesen. Der hier gegebene Beweis folgt späteren Bearbeitungen. Wir variieren dazu den Beweisgedanken von Lemma 8.11:

Beweis. 1. Es sei $|G| = n = p^m u$ mit $p \not| u$. Wir betrachten die Menge X aller p^m-elementigen Teilmengen von G. Die Gruppe G operiere auf X durch Linkstranslation, d.h. für $Y = \{y_1, \ldots, y_{p^m}\} \in X$ und $g \in G$ ist $gY = \{gy_1, \ldots, gy_{p^m}\}$.

Es sei nun $H := G_Y$ die Standgruppe von Y. Definitionsgemäß heißt das, daß H aus allen $h \in G$ mit $hY = Y$ besteht. Insbesondere erhalten wir eine neue Gruppenwirkung $H \times Y \to Y, (h, y) \mapsto hy$, die nicht mit der Wirkung von G auf X zu verwechseln ist. Offensichtlich ist die Wirkung von H auf Y frei, denn H und Y sind Teilmengen von G, und Y zerfällt in eine disjunkte Vereinigung von Rechtsnebenklassen von H. Aber das bedeutet insbesondere: Die Ordnung von H ist ein Teiler der Mächtigkeit von Y, d.h. H ist eine p-Gruppe der Ordnung $p^{m'}$ für ein $m' \leq m$. Und H ist genau

[11] Peter Ludwig Mejdell Sylow, norwegischer Mathematiker, ⋆12. Dezember 1832, †7. September 1918 in Christiana

dann eine p-Sylowuntergruppe, wenn Y aus einer einzigen H-Bahn besteht, also die Form $Y = Hy$ hat.

Gehen wir wieder zur Wirkung von G auf X über, so bedeutet dies: Die Länge der Bahn von Y ist $|G|/|H| = up^{m-m'}$, also genau dann nicht durch p teilbar, wenn $Y = Hy$ für eine p-Sylowuntergruppe H. Es sei $X_0 \subset X$ die Menge aller Teilmengen der Form $Y = Hy$ mit einer p-Sylowuntergruppe H und $y \in G$. Aus der Bahnengleichung folgt:

$$|X| \equiv |X_0| \bmod p.$$

Nun gilt nach Lemma 8.16 die Gleichung

$$|X_0| \equiv |X| = \binom{p^m u}{p^m} \equiv u \not\equiv 0 \bmod p. \tag{8.1}$$

Da u teilerfremd zu p ist, ist X_0 nicht leer, d.h. es gibt p-Sylowuntergruppen.

2. Weiter gibt es zu jeder p-Sylowuntergruppe H genau $u = [G : H]$ verschiedene Nebenklassen Hy in X_0. Andererseits ist H als Standgruppe der Nebenklasse Hy eindeutig bestimmt, d.h. ein Elemente aus X_0 gehört immer nur zu genau einer p-Sylowuntergruppe. Deshalb gilt $|X_0| = us_p$. Zusammen mit der Kongruenz 8.1 erhält man $u \equiv |X| \equiv |X_0| = us_p \bmod p$, also $s_p \equiv 1 \bmod p$.

3. Es sei $S < G$ eine p-Sylowuntergruppe und $H < G$ eine beliebige p-Untergruppe. Wir wenden Lemma 8.11 direkt auf die Wirkung von H auf der Menge G/S durch Linksmultiplikation an. Da

$$|G/S| = |G|/|S| = u \not\equiv 0 \bmod p,$$

gibt es einen Fixpunkt $yS \in G/S$, d.h. eine Nebenklasse yS mit $HyS = yS$. Aber das bedeutet, daß $y^{-1}Hy \subset S$ bzw. $H \subset ySy^{-1}$. Demnach liegt H in der p-Sylowuntergruppe ySy^{-1}, was zu zeigen war.

4. Dieses Argument liefert in dem Spezialfall, daß H selbst schon eine p-Sylowuntergruppe ist, eine Inklusion $H \subset ySy^{-1}$. Da beide Gruppen p-Sylowuntergruppen sind, sind sie gleichmächtig. Die Inklusionsbeziehung ist daher schon eine Gleichheit. Folglich sind je zwei p-Sylowuntergruppen konjugiert.

5. Schließlich betrachten wir die Wirkung von G auf der Menge X_1 der p-Sylowuntergruppen durch Konjugation: $(g, S) \mapsto gSg^{-1}$. Wir haben gerade gesehen, daß alle p-Sylowuntergruppen konjugiert sind. Es gibt deshalb nur eine Bahn. Bezeichnet K die Standgruppe von $S \in X_1$, so folgt: $|G| = |K| \cdot |X_1|$, also ist $s_p = |X_1|$ ein Teiler von $|G|$. □

Im Beweis haben wir die folgende Kongruenz benutzt: Für jede Primzahl p und jede zu p teilerfremde natürliche Zahl u gilt

$$\binom{up^m}{p^m} \equiv u \bmod p.$$

Tatsächlich gilt eine allgemeinere Aussage:

Lemma 8.16 — *Es sei p eine Primzahl, $u \in \mathbb{N}$ und $0 \le k \le u$. Dann gilt*

$$\binom{u}{k} \equiv \binom{up^m}{kp^m} \bmod p$$

für alle $m \in \mathbb{N}$.

Beweis. Im Polynomring $\mathbb{F}_p[x, y]$ gilt $(x+y)^p = x^p + y^p$. Induktiv folgt $(x+y)^{p^m} = x^{p^m} + y^{p^m}$ und schließlich

$$(x+y)^{up^m} = (x^{p^m} + y^{p^m})^u.$$

Indem man auf beiden Seiten nach der binomischen Formel expandiert und die Koeffizienten vergleicht, findet man die behauptete Formel. □

8.3. **Auflösbare Gruppen.**

Definition 8.17. — Unter der *derivierten Reihe* einer Gruppe G versteht man die rekursiv definierte, absteigende Kette von Untergruppen $\mathcal{D}^0(G) = G$ und $\mathcal{D}^{n+1}(G) = [\mathcal{D}^n(G), \mathcal{D}^n(G)]$. Eine Gruppe heißt *auflösbar*, wenn $\mathcal{D}^n(G) = 1$ für ein $n \in \mathbb{N}_0$.

Konstruktionsgemäß ist $\mathcal{D}^{n+1}(G)$ ein Normalteiler in $\mathcal{D}^n G$. Außerdem sind die Faktorgruppen $\mathcal{D}^n(G)/\mathcal{D}^n(G) = \mathcal{D}^n(G)^{\mathrm{ab}}$ abelsch. Wenn G endlich ist, ist G entweder auflösbar, oder es gibt ein n, für das $\mathcal{D}^n(G)$ perfekt, aber nicht trivial ist.

Beispiel 8.18. — Für die symmetrische Gruppe S_4 findet man als derivierte Reihe $S_4 \rhd A_4 \rhd V_4 \rhd 1$, wobei A_4 die alternierende Gruppe der geraden Permutationen bezeichnet und

$$V_4 = \{(1), (12)(34), (13)(24), (14)(23)\}$$

die Kleinsche Vierergruppe. S_4 ist also auflösbar. Die abelschen Faktorgruppen sind

$$S_4/A_4 \cong \mathbb{Z}/2, \quad A_4/V_4 \cong \mathbb{Z}/4, \quad V_4/1 \cong \mathbb{Z}/2 \times \mathbb{Z}/2.$$

In diesem Beispiel sind alle Gruppen der derivierten Reihe tatsächlich Normalteiler der Ausgangsgruppe S_4.

Beispiel 8.19. — Alle abelschen Gruppen sind auflösbar.

Satz 8.20 — *1. Jede Untergruppe einer auflösbaren Gruppe ist auflösbar.*
2. Ist $N \subset G$ ein Normalteiler, so ist G genau dann auflösbar, wenn N und G/N auflösbar sind.

Beweis. Für jede Untergruppe $H \subset G$ gilt $\mathcal{D}^n(H) \subset \mathcal{D}^n(G)$. Ähnlich erhält man aus der Surjektion $G \to G/N$ surjektive Homomorphismen $\mathcal{D}^n(G) \to \mathcal{D}^n(G/N)$ für alle n. Wenn $\mathcal{D}^n(G)$ für ein n trivial wird, gilt dasselbe für $\mathcal{D}^n(H)$ und $\mathcal{D}^n(G/N)$. Es sei umgekehrt N ein Normalteiler mit der Eigenschaft, daß N und G/N auflösbar sind. Es gibt dann ein n mit $\mathcal{D}^n(G/N) = 1$. Demnach liegt $\mathcal{D}^n(G)$ im Kern der Abbildung $G \to G/N$, also in N. Bildet man erneut iterierte Kommutatoren, so gilt $\mathcal{D}^{n+m}(G) \subset \mathcal{D}^m(N)$. Weil $\mathcal{D}^m(N)$ für große m trivial wird, gilt dasselbe für $\mathcal{D}^{n+m}(G)$. □

Als Anwendung der Sylowsätze können wir von vielen Gruppen die Auflösbarkeit aus der Faktorisierung ihrer Gruppenordnung schließen.

Satz 8.21 — *Alle p-Gruppen sind auflösbar.*

Beweis. Nach Satz Satz 8.13 besitzt jede Gruppe G der Ordnung p^n, p prim, einen Normalteiler $G' \subset G$ der Ordnung p^{n-1}. Die Faktorgruppe $G/G' = \mathbb{Z}/p$ ist abelsch, also auflösbar, und wir können durch Induktion über die Gruppenordnung annehmen, daß auch G' auflösbar ist. Damit ist auch G auflösbar. □

Satz 8.22 — *Es seien $p < q$ Primzahlen. Dann ist jede Gruppe der Ordnung pq auflösbar.*

Beweis. Es sei G eine Gruppe der Ordnung pq. Die Anzahl s der q-Sylowgruppen in G ist ein Teiler von p und kongruent 1 modulo q. Weil $p < q$, läßt das nur die Möglichkeit $s = 1$. Deshalb gibt es genau eine q-Sylowuntergruppe U, und die ist ein Normalteiler. Weil U und G/U zyklische Gruppen der Ordnung q bzw. p sind, sind sie auflösbar. Folglich ist auch G auflösbar. □

Satz 8.23 — *Es seien $p < q < r$ Primzahlen. Dann ist jede Gruppe der Ordnung pqr auflösbar.*

Beweis. Es sei G eine Gruppe der Ordnung pqr. Wenn G für eine der Primzahlen genau eine Sylowuntergruppe hat, ist diese ein Normalteiler, und die zugehörige Faktorgruppe ist auflösbar, weil ihre Ordnung ein Produkt aus zwei verschiedenen Primzahlen ist. Dann ist auch G auflösbar.

Andernfalls gibt es mindestens $q+1$ q-Sylowuntergruppen und genau pq r-Sylowuntergruppen. Es gibt dann mindestens $(q+1)(q-1)$ Elemente der Ordnung q in G und genau $pq(r-1)$ Elemente der Ordnung r in G, weil zwei verschiedene Sylowuntergruppen (zur selben Primzahl) nur das neutrale Element gemeinsam haben. Also enthält G mindestens $pq(r-1)+(q^2-1)+1 \geq pqr+(q-p)q > |G|$ Elemente, ein offensichtlicher Widerspruch. □

Wir zitieren ohne Beweis zwei berühmte Sätze aus der Gruppentheorie:

Satz 8.24 (Burnside 1906) — *Jede Gruppe der Ordnung $p^n q^m$ mit Primzahlen p und q ist auflösbar.*

William Burnside: On Groups of Order $p^\alpha q^\beta$. Proc. London Math. Soc(1904), 388 - 392.

Satz 8.25 (Feit - Thompson 1963) — *Jede Gruppe von ungerader Ordnung ist auflösbar.*

Walter Feit, John G. Walter: Solvability of groups of odd order. Pacific J. Math. 13 (1963), 775 - 1029.

8.4. **Kompositionsreihen.**

Definition 8.26. — Eine Gruppe G heißt einfach, wenn G nicht trivial ist, und wenn 1 und G die einzigen Normalteiler in G sind.

Satz 8.27 — *Für jede Primzahl p ist $\mathbb{Z}/p$ eine einfache Gruppe.* □

Bemerkung 8.28. — Die endlichen einfachen Gruppen sind vollständig klassifiziert. Es gibt, wie wir gesehen haben,

- Die zyklischen Gruppen $\mathbb{Z}/p$, p prim.
- Die alternierenden Gruppen A_n, $n \geq 5$.

Darüberhinaus gibt es 16 Serien von Gruppen vom sogenannten Lie-Typ. Schließlich gibt es noch 26 endliche einfache Gruppen, die nicht in Serien auftreten und deshalb sporadische Gruppen genannt werden. Die größte unter den sporadischen Gruppen heißt Monstergruppe M. Sie wurde von Fischer und Griess 1973 vorausgesagt und 1982 von Griess konstruiert. Sie hat

$$\begin{aligned} |M| &= 2^{46}\cdot 3^{20}\cdot 5^9\cdot 7^6\cdot 11^2\cdot 13^3\cdot 17\cdot 19\cdot 23\cdot 29\cdot 31\cdot 41\cdot 47\cdot 59\cdot 71 \\ &= 808017424794512875886459904961710757005754368000000000 \end{aligned}$$

Elemente. Es gibt merkwürdige Beziehungen zwischen der Monstergruppe und gewissen Funktionen, die in der Theorie der Modulformen auftauchen. Diese Beziehungen erschienen bei ihrem ersten Auftreten so verrückt, daß sie seither unter dem Schlagwort Mondschein (moonshine) bekannt sind. Für die Klärung vieler damit verbundener Fragen erhielt Borcherds 1998 die Fields-Medaille.

Definition 8.29. — Es sei G eine Gruppe. Eine Folge von Untergruppen

$$G = G_0 \supset G_1 \supset G_2 \supset \ldots \supset G_n = 1$$

ist eine *Normalreihe*, wenn für alle $i = 0, \ldots, n-1$ die Gruppe G_{i+1} ein Normalteiler in G_i ist. Eine Normalreihe ist eine *Kompositionsreihe*, wenn alle Faktorgruppen G_i/G_{i+1} einfach sind.

Satz 8.30 — *Es sei G eine endliche Gruppe. Jede Normalreihe läßt sich Hinzunahme weiterer Gruppen zu einer Kompositionsreihe verfeinern.*

Beweis. Es sei $G = G_0 \supset G_1 \supset \ldots \supset G_n = 1$ eine Normalreihe. Falls alle Faktoren G_i/G_{i+1} einfach sind, ist nichts zu zeigen. Andernfalls gibt es einen Index i und einen Normalteiler $1 \subsetneq N \subsetneq G_i/G_{i+1}$. Es bezeichne $\pi : G_i \to G_i/G_{i+1}$ die natürliche Projektion. Das Urbild $G' := \pi^{-1}(N)$ ist eine Untergruppe in G_i mit $G_{i+1} \subset G' \subset G_i$. Weil N ein Normalteiler in G_i/G_{i+1} ist, ist G' ein Normalteiler in G_i, und weil 1 ein Normalteiler in N ist, ist G_{i+1} ein Normalteiler in N. Dieser Vorgang läßt sich wiederholen, solange wenigstens eine Faktorgruppe der gegebenen

Normalreihe nicht einfach ist. Da die Länge einer Normalreihe bei einer endlichen Gruppe durch die Gruppenordnung und eigentlich sogar durch $\log_2(|G|)$ beschränkt ist, muß dieses Verfahren nach endlich vielen Schritten mit dem Erreichen einer Kompositionsreihe abbrechen. □

Folgerung 8.31 — *Die folgenden Aussagen über eine endliche Gruppe G sind äquivalent:*

(1) *G ist auflösbar.*
(2) *G besitzt eine Normalreihe mit abelschen Faktoren.*
(3) *G besitzt eine Kompositionsreihe, deren Faktoren zyklisch von Primzahlordnung sind.*

□

Satz 8.32 (Jordan-Hölder) — *Es sei G ein endliche Gruppe. Die Faktorgruppen einer Kompositionsreihe von G hängen bis auf Isomorphie und Reihenfolge nicht von der Wahl der Faktorgruppe ab.*

Beweis. Wir können induktiv annehmen, daß die Behauptung ür alle Gruppen kleinerer Ordnung als $|G|$ schon gezeigt ist. Es seien nun

$$G = G_0 \rhd G_1 \rhd \ldots \rhd G_n = 1 \quad \text{und} \quad G = G'_0 \rhd G'_1 \rhd \ldots \rhd G'_m = 1.$$

zwei Kompositionsreihen, möglicherweise von verschiedener Länge. Die Menge $N = G'_1 \cap G_1$ ist als Durchschnitt zweier Normalteiler selbst ein Normalteiler von G. Das liefert das folgende kommutative Diagramm mit exakten Zeilen und Spalten:

$$\begin{array}{ccccccccc}
 & & 1 & & 1 & & 1 & & \\
 & & \uparrow & & \uparrow & & \uparrow & & \\
1 & \longrightarrow & G_1/N & \longrightarrow & G/G'_1 & \longrightarrow & B & \longrightarrow & 1 \\
 & & \uparrow & & \uparrow & & \uparrow & & \\
1 & \longrightarrow & G_1 & \longrightarrow & G & \longrightarrow & G/G_1 & \longrightarrow & 1 \\
 & & \uparrow & & \uparrow & & \uparrow & & \\
1 & \longrightarrow & N & \longrightarrow & G'_1 & \longrightarrow & G'_1/N & \longrightarrow & 1 \\
 & & \uparrow & & \uparrow & & \uparrow & & \\
 & & 1 & & 1 & & 1 & &
\end{array}$$

mit $B := (G/G'_1)/(G/N) = G/(G'_1G_1) = (G/G_1)/(G'_1/N)$. Weil nach Voraussetzung G/G'_1 eine einfache Gruppe ist, ist entweder B oder G_1/N trivial. Aber G_1/N kann nur trivial sein, wenn $G_1 = G_1 \cap G'_1$, d.h. wenn $G_1 \subset G'_1$. In diesem Falle ist G'_1/G_1 eine echte Untergruppe der einfachen Gruppe G/G_1 und deshalb trivial. Das bedeutet: $G_1 = G'_1$. Die beiden Kompositionsreihen haben also denselben Anfang, und Induktion liefert die Behauptung.

Im anderen Fall ist B trivial, also $G_1/N \cong G/G'_1$ und $G'_1/N \cong G/G_1$. Wir wählen eine Kompositionsreihe $N = N_0 \rhd N_1 \rhd \ldots \rhd N_\ell = 1$ und erhalten so zwei weitere Kompositionsreihen für G:

$$G \rhd G_1 \rhd N \rhd N_1 \rhd \ldots \rhd 1 \quad \text{und} \quad G \rhd G'_1 \rhd N \rhd N_1 \rhd \ldots \rhd 1.$$

Die Faktorgruppen für die neuen Reihen sind:

$$G/G_1, G_1/N \cong G/G'_1, N/N_1, \ldots \quad \text{bzw.} \quad G/G'_1, G'_1/N \cong G/G_1, N/N_1, \ldots.$$

Bis auf die Reihenfolge und Isomorphie sind die Faktorgruppenreihen gleich. Es genügt also, die beiden Reihen

$$G \rhd G_1 \rhd G_2 \rhd \ldots \rhd 1 \quad \text{und} \quad G \rhd G_1 \rhd N \rhd N_1 \rhd \ldots \rhd 1$$

bzw.

$$G \rhd G'_1 \rhd G'_2 \rhd \ldots \rhd 1 \quad \text{und} \quad G \rhd G'_1 \rhd N \rhd N_1 \rhd \ldots \rhd 1$$

zu vergleichen. Der Unterschied zwischen den Reihen beginnt aber jeweils erst bei G_1 bzw. bei G_1'. Die Behauptung folgt also durch Induktion über die Gruppenordnung. □

Camille Jordan zeigte zunächst, daß die Folge der Indizes $[G_i : G_{i+1}]$, $i = 0, \ldots, n-1$, einer Kompositionsreihe bis auf die Reihenfolge unabhängig von der Wahl der Kompositionsreihe ist. Er nannte diese Indizes die *Faktoren* der Gruppe G. Nachdem Otto Hölder später den Begriff der *Faktorgruppe* gebildet und deren Eigenschaften studiert hatte, konnte er die hier diskutierte Verschärfung des Satzes von Jordan beweisen.

8.5. **Aufgaben zur Gruppentheorie.**

Aufgabe 8.33. — Es sei $q = p^s$ eine Primzahlpotenz und $\mathbb{F}_q$ der Körper mit q Elementen. Die Gruppe $\mathrm{GL}_n(\mathbb{F}_q)$ der invertierbaren $n \times n$-Matrizen mit Koeffizienten in $\mathbb{F}_q$ operiert durch Linksmultiplikation auf dem Vektorraum $\mathbb{F}_q^n$. Man zeige:

(1) $\mathbb{F}_q^n$ besteht aus zwei Bahnen: $\{0\}$ und $\mathbb{F}_q^n \setminus \{0\}$.
(2) Die Standgruppe des ersten Standardeinheitsvektors ist
$$H = \left\{ \left(\begin{array}{c|c} 1 & u \\ \hline 0 & A \end{array} \right) \;\middle|\; A \in \mathrm{GL}_{n-1}(\mathbb{F}_q), u \in \mathbb{F}_q^{n-1} \right\}.$$
(3) Man leite aus der Bahnengleichung und den Aussagen (1) und (2) eine rekursive Beziehung für die Gruppenordnungen von $\mathrm{GL}_{n-1}(\mathbb{F}_q)$ und $\mathrm{GL}_n(\mathbb{F}_q)$ her.
(4) $|\mathrm{GL}_n(\mathbb{F}_q)| = q^{\binom{n}{2}} \prod_{k=1}^{n} (q^k - 1)$.

Aufgabe 8.34. — Es sei G eine Gruppe und $S \subset G$ eine Teilmenge und X die Menge aller Untergruppen von G, die S enthalten. Zeigen Sie:

(1) X ist nicht leer.
(2) $\langle S \rangle := \bigcap_{H \in X} H$ ist ein Element in X.

$\langle S \rangle$ heißt die von S erzeugte Untergruppe von G, und G heißt von S erzeugt, wenn $G = \langle S \rangle$.

Aufgabe 8.35. — Es sei G eine Gruppe und $S \subset G$ eine Teilmenge. Es sei H die Menge aller Produkt $s_1 \cdots s_n$ mit $n \in \mathbb{N}_0$ und $s_i \in S$ oder $s_i^{-1} \in S$. Zeigen Sie, daß $H = \langle S \rangle$.

Aufgabe 8.36. — Es sei $n \in \mathbb{N}$ gegeben. Es bezeichne $s = \left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right) \in \mathrm{O}(2)$ die Spiegelung an der x-Achse und $d = \left(\begin{smallmatrix} \cos(2\pi/n) & -\sin(2\pi/n) \\ \sin(2\pi/n) & \cos(2\pi/n) \end{smallmatrix}\right) \in \mathrm{O}(2)$ die Drehung um den Winkel $2\pi/n$.

(1) Die Untergruppe $C_n := \langle d \rangle$ in der orthogonalen Gruppe $\mathrm{O}(2)$ ist zyklisch mit Ordnung n, d.h. $C_n \cong \mathbb{Z}/n$.
(2) Die Untergruppe $D_n := \langle s, d \rangle$ heißt Diedergruppe. Man zeige, daß $|D_n| = 2n$.
(3) Man bestimme alle Konjugationsklassen von D_n. (Vorsicht: Unterscheide die Fälle n gerade und n ungerade.)
(4) Man bestimme alle Untergruppen und Normalteiler in D_n.

Es sei $H < G$ eine Untergruppe. Das Verhältnis $[G : H] := |G/H| = |G|/|H|$ wird als Index von H in G bezeichnet.

Aufgabe 8.37. — Jede Untergruppe $H < G$ vom Index $[G : H] = 2$ ist ein Normalteiler.

Aufgabe 8.38. — Es sei G eine Gruppe, $N \lhd G$ ein Normalteiler und $H < G$ eine Untergruppe.

(1) $N \cap H$ ist ein Normalteiler in H.
(2) Die Menge $NH = \{nh \mid n \in N, h \in H\}$ ist eine Untergruppe in G.
(3) N ist ein Normalteiler in NH.
(4) Die Abbildung $NH \to NH/N$ hat den Kern $N \cap H$.
(5) Die Abbildung $H/(N \cap H) \to NH/N$, $h \bmod (N \cap h) \mapsto h \bmod N$, ist ein Isomorphismus (Erster Isomorphiesatz).

(6) Ist auch H ein Normalteiler, so ist $N \cap H$ ein Normalteiler in G.

Aufgabe 8.39. — Es sei $m : G \times X \to X$ eine Linkswirkung. Dann ist $q(x, g) := m(g^{-1}, x)$ eine Rechtwirkung von G auf X.

Aufgabe 8.40. — Es sei $G \times X \to X$ eine Gruppenwirkung. Liegen x und y in derselben Bahn, so sind ihre Standgruppen $G_x, G_y < G$ konjugierte Untergruppen. Wie hängen G_{gy} und G_y zusammen?

Aufgabe 8.41. — Es sei p eine Partition von n. Man bestimme die Mächtigkeit der Konjugationsklasse aller Permutationen vom Zykeltpy p.

Aufgabe 8.42. — Es sei G eine Gruppe und $g \in G$. Der Zentralisator von g in G ist die Menge $Z_G(g) = \{h \in G \mid hg = gh\}$. Man zeige:

(1) $Z_G(g)$ ist eine Untergruppe von G.
(2) $Z_G(x)$ ist die Standgruppe von x bezüglich der Wirkung $G \times G \to G$, $(g, x) \mapsto gxg^{-1}$.
(3) Es sei speziell $G = S_n$ und $\pi \in S_n$ ein Permutation. Man drücke die Ordnung von $Z_{S_n}(\pi)$ durch den Zykeltyp von π aus.

Aufgabe 8.43. — Es seien N und H Gruppen und $\alpha : H \to \mathrm{Aut}(N)$ ein Gruppenhomomorphismus. Das semidirekte Produkt $N \rtimes_\alpha H$ ist die Menge $N \times H$ mit der folgenden Gruppenstruktur:

$$(n, h) \cdot (n', h') := (n\alpha(h)(n'), hh').$$

Zeigen Sie: 1. Die angegebene Verküpfung definiert tatsächlich eine Gruppenstruktur.
2. Die Abbildungen $N \to N \rtimes_\alpha H$, $n \mapsto (n, e)$, und $H \to N \rtimes_\alpha H$, $h \mapsto (e, h)$, sind injektive Gruppenhomomorphismen.
3. Identifiziert man N und H mit ihren Bildern in $N \rtimes H$, so gilt: N ist ein Normalteiler in $N \rtimes H$, und die Inklusion von H induziert einen Isomorphismus $H \cong (N \rtimes H)/N$.
4. Für $n \in N$ und $h \in H$ gilt: $hnh^{-1} = \alpha(h)(n)$.
5. Es sei $\alpha : \mathbb{Z}/2 \to \mathrm{Aut}(\mathbb{Z}/3)$ ein Homomophismus. Dann gilt $\mathbb{Z}/3 \rtimes_\alpha \mathbb{Z}/2 \cong \mathbb{Z}/6$ oder S_3 je nachdem, ob α die triviale Abbildung ist oder nicht.

Aufgabe 8.44. — Es seien $s_0, s_1 : \mathbb{R} \to \mathbb{R}$ die Punktspiegelungen an den Punkten 0 bzw. 1. Zeigen Sie: Die von s_0 und s_1 erzeugte Gruppe G ist isomorph zu $\mathbb{Z} \rtimes_\alpha \mathbb{Z}/2$, wobei $\alpha : \mathbb{Z}/2 \to \mathrm{Aut}(\mathbb{Z})$ den eindeutigen Gruppenisomorphismus bezeichne

Aufgabe 8.45. — Es sei V ein K-Vektorraum. Die Gruppe $\mathrm{GL}(V)$ der K-linearen Automorphismen von V ist eine Untergruppe in der Gruppe $\mathrm{Aut}(V)$ der Automorphismen von V als abelsche Gruppe. Es sei $\alpha : \mathrm{GL}(V) \to \mathrm{Aut}(V)$ die Inklusionsabbildung. Die Gruppe $\mathrm{Aff}(V) := V \rtimes_\alpha \mathrm{GL}(V)$ heißt *affine Gruppe* von V. Man zeige, daß $\mathrm{Aff}(V) \times V \to V$, $((b, A), v) \mapsto Av+b$, eine Gruppenwirkung von $\mathrm{Aff}(V)$ auf V ist.

Aufgabe 8.46. — Es sei K ein Körper und $G \subset \mathrm{GL}_n(K)$ die Untergruppe der oberen Dreiecksmatrizen. Zeigen Sie, daß G auflösbar ist.

Aufgabe 8.47. — 1. Für alle $n \geq 2$ gilt $[S_n, S_n] = A_n$.
2. $A_2 = \{(1)\}$, $A_3 \cong \mathbb{Z}/3$, also insbesondere $[A_3, A_3] = \{(1)\}$.
3. $[A_4, A_4] = V_4 := \{(12)(34), (13)(24), (14)(23)\}$, und $[V_4, V_4] = \{(1)\}$.
4. Für $n \geq 5$ ist $[A_n, A_n] = A_n$. [Ohne Rückgriff auf die in der Vorlesung bewiesene Einfachheit von A_n.]

Es sei K ein Körper. $\mathrm{GL}_n(K)$ bezeichnet die Gruppe der invertierbaren $n \times n$-Matrizen, $\mathrm{SL}_n(K)$ die Untergruppe der Matrizen mit Determinante 1, und Z_n die Untergruppe der Vielfachen der Einheitsmatrix. Man sieht leicht, daß Z_n ein Normalteiler ist. Wir definieren $\mathrm{PSL}_n(K) := \mathrm{SL}_n(K)/(Z_n \cap \mathrm{SL}_n(K))$ und $\mathrm{PGL}_n(K) := \mathrm{GL}_n(K)/Z_n$.

Aufgabe 8.48. — Es sei $\mathbb{F}_q$ ein[12] endlicher Körper mit q Elementen. Bestimmen Sie die Ordnungen der endlichen Gruppen $\mathrm{GL}_n(\mathbb{F}_q)$, $\mathrm{SL}_n(\mathbb{F}_q)$, $\mathrm{PGL}_n(\mathbb{F}_q)$ and $\mathrm{PSL}_n(\mathbb{F}_q)$.

Aufgabe 8.49. — Es sei K ein Körper und $n \in \mathbb{N}$.
1. Falls $(K,n) \neq (\mathbb{F}_2, 2)$, gilt $[\mathrm{GL}_n(K), \mathrm{GL}_n(K)] = \mathrm{SL}_n(K)$.
2. Falls $(K,n) \neq (\mathbb{F}_2, 2), (\mathbb{F}_2, 3)$, gilt $[\mathrm{SL}_n(K), \mathrm{SL}_n(K)] = \mathrm{SL}_n(K)$
[Elementarmatrizen $E_{ij}(\lambda)$ mit $E_{ij}(\lambda)_{mn} = \delta_{mn} + \lambda\delta_{im}\delta_{jn}$ betrachten.]
3. Was geschieht in den Ausnahmefällen?

Aufgabe 8.50. — Wir betrachten in $\mathrm{GL}_2(\mathbb{C})$ die Untergruppe Q_8, die von den Matrizen

$$I := \left(\begin{smallmatrix} i & 0 \\ 0 & -i \end{smallmatrix}\right) \quad \text{und} \quad J := \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$$

erzeugt wird. Zeigen Sie, daß Q_8 eine endliche Gruppe der Ordnung 8 ist. Q_8 heißt Quaternionengruppe. Bestimmen Sie alle Untergruppen und Normalteiler in Q_8.

Aufgabe 8.51. — Es gibt bis auf Isomorphie genau fünf Gruppen der Ordnung 8, nämlich

$$\mathbb{Z}/8, \quad \mathbb{Z}/4 \times \mathbb{Z}/2, \quad \mathbb{Z}/2 \times \mathbb{Z}/2 \times \mathbb{Z}/2, \quad D_4, \quad Q_8.$$

Dabei ist D_4 die Diedergruppe, die von der Spiegelung $\left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$ und der Drehung $\left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$ erzeugt wird, und Q_8 ist die Quaternionengruppe. Zu welcher dieser Gruppen ist die Gruppe

$$N = \left\{ \left(\begin{smallmatrix} 1 & * & * \\ 0 & 1 & * \\ 0 & 0 & 1 \end{smallmatrix}\right) \right\} \subset \mathrm{GL}_3(\mathbb{F}_2)$$

isomorph?

Aufgabe 8.52. — Es sei G eine endliche Gruppe mit $|G| = pq$ mit Primzahlen $p > q$. Zeigen Sie:

(1) Es gibt genau eine p-Sylowuntergruppe N.
(2) Ist H eine q-Sylowuntergruppe, so ist G isomorph zu einem semidirekten Produkt $N \rtimes_\alpha H$.
(3) Wenn q kein Teiler von $p-1$ ist, ist G zyklisch.

Aufgabe 8.53. — Zeigen Sie:

(1) Es sei G eine Gruppe mit Zentrum Z. Wenn G/Z zyklisch ist, so ist G abelsch.
(2) Es sei p eine Primzahl. Jede Gruppe der Ordnung p^2 ist abelsch. Wie viele Gruppen der Ordnung p^2 gibt es?
(3) Sei p eine Primzahl. Zeigen Sie: In einer nichtabelschen Gruppe der Ordnung p^3 hat das Zentrum die Ordnung p.

Wir wiederholen in den folgenden Aufgaben einige Ergebnisse aus der Vorlesung Elementare Algebra und Zahlentheorie. Es sei G eine abelsche Gruppe. Die Zahl
$e(G) := \sup\{\mathrm{ord}(g) \mid g \in G\} \in \mathbb{N} \cup \{\infty\}$ heißt Exponent von G.

Aufgabe 8.54. — Es sei G eine Gruppe mit kommutierenden Elementen a und b von endlicher Ordnung $m = \mathrm{ord}(a)$ bzw. $n = \mathrm{ord}(b)$. Man zeige:

(1) Sind m und n teilerfremd, so gibt es $k, \ell \in \mathbb{Z}$ mit $(ab)^k = a$ und $(ab)^\ell = b$, und das Element ab hat die Ordnung mn.
(2) Es gibt ein Element $c \in \langle a, b\rangle < G$ mit $\mathrm{ord}(c) = \mathrm{kgV}(m,n)$.

Aufgabe 8.55. — Es sei G eine endliche abelsche Gruppe. Dann gilt $\mathrm{ord}(g) | e(G)$ für alle $g \in G$, und $e(G)$ teilt die Gruppenordnung. [Hinweis: Aufgabe 8.54.]

[12] Wir werden im Laufe der Vorlesung sehen, daß es bis auf Isomorphie genau einen endlichen Körper mit q Elementen gibt, wenn q eine Primzahlpotenz ist.

Aufgabe 8.56. — Es sei K ein Körper und $G < K^\times$ eine endliche Untergruppe der Einheitengruppe. Dann ist G zyklisch. Insbesondere ist für jeden endlichen Körper $\mathbb{F}$ die Einheitengruppe $\mathbb{F}^\times$ zyklisch. [Hinweis: Man zeige, daß alle $g \in G$ Nullstellen des Polynoms $X^{e(G)} - 1 \in K[X]$ sind.]

Die Bestimmung der Einheitengruppe $(\mathbb{Z}/n)^\times$ für eine beliebige natürliche Zahl zerfällt in zwei Teile. Zunächst zerlegt man $n = \prod_i p_i^{m_i}$ in seine Primfaktoren. Nach dem Chinesischen Restklassensatz gilt dann zunächst

$$\mathbb{Z}/n \cong \prod_i \mathbb{Z}/p_i^{m_i}$$

und damit auch

$$(\mathbb{Z}/n)^\times \cong \prod_i (\mathbb{Z}/p_i^{m_i})^\times.$$

Es bleibt das Problem, die Struktur von $(\mathbb{Z}/n)^\times$ für den Fall einer Primzahlpotenz $n = p^m$ zu bestimmen. Das geschieht in den folgenden Aufgaben.

Aufgabe 8.57. — Es sei p eine ungerade Primzahl. Für alle $m \geq 0$ gilt:

$$(1+p)^{p^m} \equiv 1 + p^{m+1} \equiv p^{m+2}.$$

Für alle $m \geq 0$ gilt

$$(1+2^2)^{2^m} \equiv 1 + 2^{m+2} \equiv 2^{m+3}.$$

Aufgabe 8.58. — Es sei p eine ungerade Primzahl und $m \geq 1$. Es sei U der Kern des Homomorphismus $\varphi : (\mathbb{Z}/p^m)^\times \to (\mathbb{Z}/p)^\times$.

(1) U ist eine p-Gruppe.
(2) U wird von $1 + p$ erzeugt.
(3) $(\mathbb{Z}/p^m)^\times$ ist zyklisch der Ordnung $(p-1)p^{m-1}$.

Aufgabe 8.59. — Es sei $m \geq 2$ und U der Kern des Homomorphismus $\varphi : (\mathbb{Z}/2^m)^\times \to (\mathbb{Z}/4)^\times$.

(1) U ist eine 2-Gruppe.
(2) U wird von 5 erzeugt.
(3) $(\mathbb{Z}/2^m)^\times \cong \mathbb{Z}/2 \times \mathbb{Z}/2^{m-2}$, wobei die Faktoren von -1 und 5 erzeugt werden.

§9. Die symmetrische Gruppe

Definition 9.1. — Die symmetrische Gruppe S_n vom Grad $n \in \mathbb{N}$ ist die Menge der Bijektionen der Menge $[n] = \{1, \ldots, n\}$ in sich mit der Komposition als Verknüpfung. Insbesondere ist $|S_n| = n!$.

Permutationen sind also Abbildungen. In einer Verknüpfung $\sigma \circ \pi$ wird nach den üblichen Konventionen für Abbildungen die Permutation π zuerst ausgeführt, danach die Permutation σ. Definitionsgemäß ist S_1 die triviale Gruppe. S_2 besteht aus zwei Elementen und ist somit isomorph zu $\mathbb{Z}/2$.

9.1. Partitionen.

Eine Partition von $n \in \mathbb{N}$ ist eine Zerlegung $n = \lambda_1 + \lambda_2 + \ldots + \lambda_s$ in natürliche Zahlen $\lambda_1, \ldots, \lambda_s$. Dabei kommt es auf die Reihenfolge nicht an. Üblicherweise ordnet man die Partition fallend und schreibt

$$\lambda = [\lambda_1, \ldots, \lambda_s] \qquad \text{mit } \lambda_1 \geq \ldots \geq \lambda_s > 0.$$

Die Zahl 4 besitzt zum Beispiel die folgenden fünf Partitionen:

$$[4], \quad [3,1], \quad [2,2], \quad [2,1,1], \quad [1,1,1,1].$$

Bezeichnet $p(n)$ die Anzahl der Partitionen von n, und vereinbart man noch, daß $p(0) = 1$, weil 0 nur die leere Partition $[]$ besitzt, so kann man die erzeugende Funktion

$$p(t) = \sum_{n=0}^{\infty} p(n)t^n = 1 + t + 2t^2 + 3t^3 + 5t^4 + 11t^5 + \ldots \in \mathbb{Z}[[t]]$$

wie folgt als ein unendliches Produkt schreiben:

$$\sum_{n=0}^{\infty} p(n)t^n = \prod_{m=1}^{\infty} \frac{1}{1-t^m}.$$

9.2. Zykelzerlegung und Konjugationsklassen.

Für jede Folge $(n_1, \ldots, n_k)$ von $k \geq 1$ paarweise verschiedenen Zahlen aus $[n]$ bezeichnet $(n_1 \ \ldots \ n_k) \in S_n$ die Permutation mit der Eigenschaft

$$n_1 \mapsto n_2, \ n_2 \mapsto n_3, \ \ldots, n_k \mapsto n_1 \quad \text{ und } \quad i \mapsto i \quad \text{ für alle } i \notin \{n_1, \ldots, n_k\}.$$

Permutationen dieser Form heißen *k-Zykel* oder Zykel der Länge k. Zykel der Länge 2 heißen *Transpositionen*. Es ist dann klar, daß $(n_1 \ldots n_k) = (n_k\, n_1 \ldots n_{k-1})$ und daß $(n_1 n_2 \ldots n_k)^{-1} = (n_k n_{k-1} \ldots n_1)$. Zwei Zykel $(n_1 \ \ldots \ n_k)$ und $(m_1 \ \ldots \ m_\ell)$ sind *disjunkt* oder *elementfremd*, falls die Mengen $\{n_1, \ldots, n_k\}$ und $\{m_1, \ldots, m_\ell\}$ disjunkt sind. Schließlich bezeichnen wir gelegentlich die Identität auf $[n]$ mit dem 1-Zykel $(1) = (2) = \ldots = (n)$.

Es sei eine Permutation $\pi \in S_n$ gegeben. Die von π erzeugte zyklische Gruppe $\langle \pi \rangle$ operiert auf der Menge $[n]$, und unter dieser Wirkung zerfällt $[n]$ in Bahnen $B_1, \ldots, B_s$. Diese seien so numeriert, daß $|B_1| \geq |B_2| \geq \ldots$. Es gilt $[B_1| + \ldots + |B_s| = n$. Die Partition $Z(\pi) = [|B_1|, |B_2|, \ldots, |B_s|]$ von n heiße der *Zykeltyp* der Permutation π. Zum Beispiel ist der Zykeltyp von $(145)(27) \in S_8$ die Partition $[3,2,1,1,1]$. Man sieht leicht, daß umgekehrt jede Partition von n wirklich als Zykeltyp einer Partition vorkommt.

Satz 9.2 — *Jede Permutation $\pi \in S_n$ läßt sich als Produkt von elementfremden Zykeln schreiben, und diese Produktdarstellung ist eindeutig bis auf die Reihenfolge der Faktoren.*

Beweis. Jede Bahn B von π der Länge $\ell \geq 2$ bestimmt einen eindeutigen ℓ-Zykel ζ wie folgt: Es sei $x \in B$ beliebig gewählt. Wir setzen $\zeta = (x\, \pi(x)\, \pi^2(x) \ldots \pi^{\ell-1}(x))$. Definiert man auf diese Weise zu jeder Bahn B_i der Länge $\ell_i \geq 2$ einen Zykel ζ_i, so sind alle Zykel ζ_1, ζ_2,... paarweise disjunkt und es gilt $\pi = \zeta_1\zeta_2 \ldots$. Nur im Falle $\pi = \mathrm{id}_{[n]}$ gibt es überhaupt keine Bahnen der Länge ≥ 2,

und π ist das leere Produkt. Auf diese Weise läßt sich jede Permutation als Produkt von disjunkten Zykeln schreiben. Die Eindeutigkeit ist klar. □

Lemma 9.3 *— Für Zykel $(a_1 \dots a_s)$ und $(a_s \dots a_m)$ mit paarweise verschiedenen a_i, $i = 1, \dots, m$, gilt*

$$(a_1 \dots a_s)(a_s \dots a_m) = (a_1 \dots a_s \dots a_m).$$

Insbesondere besitzt jeder Zykel $(b_1 \dots b_k)$ eine Zerlegung in Transpositionen:

$$(b_1 \dots b_k) = (b_1 b_2)(b_2 b_3) \dots (b_{k-1} b_k),$$

und allgemein ist jede Permutation ein Produkt von Transpositionen.

Beweis. Man verifiziert die erste Aussage direkt, die zweite Aussage erhält man durch wiederholte Anwendung der ersten Aussage auf das angegebene Produkt von Transpositionen. □

Satz 9.4 (Coxetersystem) *— Die Transpositionen $(12), (23), \dots, (n-1\, n)$ erzeugen S_n.*

Beweis. Es sei $s_i = (i\, i+1)$. Man verfiziert für $k < m$:

$$s_k s_{k+1} \dots s_{m-1} s_m s_{m-1} \dots s_{k+1} s_k = (km).$$

Aus den Transpositionen $s_1, \dots, s_{n-1}$ erhält man auf diese Weise alle Transpositionen, und diese erzeugen S_n. □

Satz 9.5 *— Für jede Permutation π und jeden k-Zykel $(n_1 \ \dots \ n_k)$ in S_n gilt*

$$\pi \cdot (n_1 \ \dots \ n_k) \cdot \pi^{-1} = (\pi(n_1) \ \dots \ \pi(n_k)).$$

Zwei Permutationen $\pi, \pi' \in S_n$ sind genau dann konjugiert, wenn sie denselbe Zykeltyp haben. Insbesondere ist die Abbildung

$$\{\text{Konjugationsklassen von } S_n\} \leftrightarrow \{\text{Partitionen von } n\}, \pi \mapsto \text{Zykeltyp von } \pi,$$

eine Bijektion.

Beweis. Die erste Aussage ergibt sich durch eine einfache Rechnung. Es folgt unmittelbar, daß $\pi\sigma\pi^{-1}$ und σ denselben Zykeltyp haben. Sind umgekehrt σ und σ' Permutationen vom selben Zykeltyp, so kann man die Elemente in $[n]$ so benennen, daß

$$\sigma = (a_1 \dots a_{\ell_1})(a_{\ell_1+1} \dots a_{\ell_s}) \cdots (a_{\ell_{s-1}+1} \dots a_{\ell_s})$$

und

$$\sigma' = (b_1 \dots b_{\ell_1})(b_{\ell_1+1} \dots b_{\ell_2}) \cdots (b_{\ell_{s-1}+1} \dots b_{\ell_s}),$$

wobei auch die Fixpunkte von σ bzw. von σ' in Form von 1-Zykeln aufgenommen sind, so daß $\{1, \dots, n\} = \{a_1, \dots, a_{\ell_s}\} = \{b_1, \dots, b_{\ell_s}\}$. Bezeichnet nun π die Permutation mit $\pi : a_i \mapsto b_i$ für $i = 1, \dots, n$, so gilt $\pi\sigma\pi^{-1} = \sigma'$. Demnach liegen π und π' in derselben Konjugationsklasse. □

Es sei $\lambda = [\lambda_1, \lambda_2, \dots, \lambda_t]$ eine Partition von n, d.h. $\lambda_1 \geq \dots \geq \lambda_t > 0$ und $n = \lambda_1 + \dots + \lambda_t$. Es bezeichne $m_\lambda(i) := \{j \mid \lambda_j = i\}$ die Vielfachheit, mit der i in der Partition λ vorkommt. Wir schreiben dann auch

$$\lambda = (1^{m_\lambda(1)} 2^{m_\lambda(2)} \cdots).$$

Zum Beispiel ist $[4, 2, 2, 1, 1, 1] = (1^3 2^2 4^1)$ eine Partition von 11.

Satz 9.6 — *Es sei $\lambda = (1^{m_1} 2^{m_2} \cdots)$ eine Partition von n. Dann ist die Mächtigkeit der Konjugationsklasse C_λ aller Permutationen in S_n vom Zykeltyp λ gleich*

$$|C_\lambda| = \frac{n!}{\prod_i m_i!\, i^{m_i}}.$$

Beweis. Es gibt insgesamt $\frac{n!}{a!b!\cdots z!}$ Möglichkeiten, aus einer n-elementigen Menge in dieser Reihenfolge erst a, dann b, etc. und schließlich z Elemente ohne Rücksicht auf ihre Anordnung auszuwählen. Wenn dabei m_i-mal jeweils i Elemente auszuwählen sind, ist die Anzahl $n!/\prod_i (i!)^{m_i}$. Wenn es dabei auf die Reihenfolge zwischen den i-elementigen Mengen nicht ankommt, ist die Anzahl der Möglichkeiten $n!/\prod_i m_i!(i!)^{m_i}$. Schließlich ist die Anzahl der i-Zykel, die dieselbe i-elementige Menge permutieren, genau $(i-1)!$. Daraus folgt die Behauptung. □

9.3. **Der Signaturhomomorphismus und die alternierende Gruppe.**

Wir diskutieren, zwei Methoden den Signaturhomomorphismus

$$\operatorname{sgn} : S_n \to \{\pm 1\}$$

zu beschreiben, die natürlich zum selben Ergebnis führen.

Erste Methode:

Satz 9.7 — *Für jede Permutation $\pi \in S_n$ nimmt das Produkt*

$$\operatorname{sgn}(\pi) := \prod_{i<j} \frac{\pi(i) - \pi(j)}{i - j}$$

den Wert 1 oder -1 an. Die Abbildung

$$\operatorname{sgn} : S_n \to \{\pm 1\}$$

ist ein Gruppenhomomorphismus. Für einen Zykel ζ der Länge ℓ gilt

$$\operatorname{sgn}(\zeta) = (-1)^{\ell-1}.$$

□

Beweis. Weil der Quotient $(\pi(i) - \pi(j))/(i-j)$ nicht von der Reihenfolge der Elemente i und j abhängt, kann man das Produkt auch über die Menge U aller zweielementigen Teilmengen $\{i, j\}$ von $[n]$ ausführen, statt über die Menge der Paare (i, j) mit $i < j$. Weil π eine Bijektion ist, kommen in dem Produkt

$$\prod_{\{i,j\}\in U} \frac{\pi(i) - \pi(j)}{i - j}$$

bis auf Vorzeichen dieselben Faktoren vor. Deshalb hat das Produkt den absoluten Wert 1. Sind π und σ Permutationen, so gilt

$$\prod_{\{i,j\}} \frac{\pi(\sigma(i)) - \pi(\sigma(j))}{i - j} = \prod_{\{i,j\}} \frac{\pi(\sigma(i)) - \pi(\sigma(j))}{\sigma(i) - \sigma(j)} \prod_{\{i,j\}} \frac{\sigma(i) - \sigma(j)}{i - j}$$

Im ersten Faktor der rechten Seite können wir nun umindizieren: Wenn $\{i, j\}$ einmal durch T läuft, so gilt dasselbe für $\{k, \ell\} := \{\pi(i), \pi(j)\}$. Deshalb gilt:

$$\prod_{\{i,j\}\in U} \frac{\pi(\sigma(i)) - \pi(\sigma(j))}{i - j} = \prod_{\{k,\ell\}\in U} \frac{\pi(k) - \pi(\ell)}{k - \ell} \prod_{\{i,j\}\in U} \frac{\sigma(i) - \sigma(j)}{i - j}$$

Das zeigt $\operatorname{sgn}(\pi \circ \sigma) = \operatorname{sgn}(\pi)\operatorname{sgn}(\sigma)$. Somit ist sgn ein Gruppenhomomorphismus.

Speziell für die Transposition (12) haben alle Faktoren $(\tau(i)-\tau(j))/(i-j)$ positives Vorzeichen bis auf den Faktor zum Paar $\{i, j\} = \{1, 2\}$. Deshalb gilt $\operatorname{sgn}((12)) = -1$. Weil sgn ein Gruppenhomomorphismus ist, nimmt sgn auch auf allen zu (12) konjugierten Permutationen, d.h. auf allen Transpositionen den Wert -1 an. Schließlich ist jeder ℓ-Zykel ein Produkt aus $\ell - 1$ Transpositionen. Daraus ergibt sich die letzte Aussage. □

Zweite Methode: Wir definieren direkt für eine Permutation π, in deren Zerlegung in elementfremde Zykel genau s Zykel vorkommen, alle 1-Zykel mitgezählt, den Wert

$$\operatorname{sgn}(\pi) := (-1)^{n-s}.$$

Bei einem ℓ-Zykel ζ müssen also alle $n-\ell$ 1-Zykel mitgezählt werden, so daß man auf

$$\operatorname{sgn}(\zeta) = (-1)^{n-(1+n-\ell)} = (-1)^{\ell-1}$$

kommt. Es bleibt aber zu zeigen, daß sgn ein Gruppenhomomorphismus ist. Dazu betrachten wir die Wirkung einer Transposition $(1k)$ auf einem Zykel $(12\dots m)$ mit $k \leq m$:

$$(1k)\cdot(12\dots m) = (12\dots k-1)(k\dots m).$$

Eine erneute Multiplikation mit derselben Transposition gibt

$$(1k)\cdot(12\dots k-1)(k\dots m) = (12\dots m).$$

Durch die Multiplikation mit einer Transposition (ij) auf einer Permutation π wird also die Anzahl der Zykel in der Zykelzerlegung um 1 erhöht bzw. um eins vermindert je nachdem, ob die beiden Elemente i und j zum selben Zykel von π gehören oder nicht. Aber in beiden Fällen ändert sich die Parität modulo 2 um 1. Deshalb gilt

$$\operatorname{sgn}(\tau\cdot\pi) = -\operatorname{sgn}(\pi).$$

Induktiv folgt für ein σ, daß sich als Produkt von ℓ Transpositionen schreiben läßt:

$$\operatorname{sgn}(\sigma\cdot\pi) = (-1)^{\ell}\operatorname{sgn}(\pi).$$

Und indem man dies auf $\pi = \mathrm{id}$ anwendet:

$$\operatorname{sgn}(\sigma) = (-1)^{\ell}.$$

Jetzt ist die Homomorphieeigenschaft von sgn offenkundig: Sind π und σ Produkte von k bzw. ℓ Transpositionen, so ist $\pi\sigma$ ein Produkt von $k+\ell$ Transpositionen, und man erhält:

$$\operatorname{sgn}(\pi\sigma) = (-1)^{k+\ell} = \operatorname{sgn}(\pi)\operatorname{sgn}(\sigma).$$

Definition 9.8. — Der Kern $A_n := \ker(\operatorname{sgn}) \subset S_n$ ist ein Normalteiler vom Index 2, die sogenannte *alternierende Gruppe*. Die Elemente in A_n heißen *gerade* Permutationen, alle übrigen *ungerade* Permutationen.

Transpositionen sind ungerade. Eine Permutationen ist genau dann gerade bzw. ungerade, wenn sie sich als Produkt einer geraden bzw. ungeraden Anzahl von Transpositionen schreiben läßt.

Satz 9.9 — *A_n wird von der Menge der 3-Zykel erzeugt.*

Beweis. Weil alle 3-Zykel gerade sind, ist klar, daß die von diesen erzeugte Untergruppe in A_n liegt. Umgekehrt ist eine Permutation π genau dann gerade, wenn sie sich als Produkt einer geraden Anzahl von Transpositionen schreiben läßt, etwa $\pi = \tau_1\tau_2\cdots\tau_{2m} = (\tau_1\tau_2)\cdots(\tau_{2m-1}\tau_{2m})$. Es genügt deshalb zu zeigen, daß sich Produkte $\tau\tau'$ von zwei Transpositionen mit 3-Zykeln schreiben lassen. Falls $\tau = \tau'$, ist dies trivial. Wenn τ und τ' ein Element gemeinsam haben, etwa $\tau = (ij)$ und $\tau' = (jk)$, hat man $\tau\tau' = (ijk)$. Wenn schließlich τ und τ' elementfremd sind, etwa $\tau = (ij)$ und $\tau' = (k\ell')$, gilt $\tau\tau' = (ij)(jk)(jk)(k\ell) = (ijk)(jk\ell)$. □

Satz 9.10 — *Es gilt* $[S_n, S_n] = A_n$. *Außerdem ist* A_n *ist die einzige Untergruppe in* S_n *vom Index* 2.

Beweis. Weil A_n von der Menge der 3-Zykel erzeugt wird, genügt es zu zeigen, daß jeder 3-Zykel als Kommutator geschrieben werden kann. In der Tat gilt nun $[(12),(23)] = (12)(23)(12)(23) = (123)(123) = (132)$.

Ist $H \subset S_n$ eine Untergruppe vom Index 2, so ist H ein Normalteiler mit abelscher Faktorgruppe $S_n/H \cong \mathbb{Z}/2$. Deshalb muß der Kommutator $[S_n, S_n] = A_n$ in H liegen. Weil beide Untergruppen denselben Index haben, sind sie gleich. □

9.4. **Die Gruppe S_3.** Die Diedergruppe D_3, d.h. die Gruppe der Symmetrien eines ebenen gleichseitigen Dreiecks mit den Ecken p_1, p_2, p_3 permutiert die drei Ecken des Dreiecks. Man erhält so einen Gruppenhomomorphismus $D_3 \to S_3$, und diese Abbildung ist ein Isomorphismus, weil jede Symmetrie, die die Ecken einzeln festläßt, auch die Identität auf der ganze Ebene sein muß. Unter diesem Isomorphismus wird die Untergruppe der Drehungen auf die alternierende Gruppe $A_3 = \langle (123) \rangle$ abgebildet.

9.5. **Die Gruppe S_4.** Die derivierte Reihe der Gruppe S_4 ist

$$S_4 \rhd A_4 \rhd V_4 \rhd 1,$$

wobei

$$V_4 = [A_4, A_4] = \{(1), (12)(34), (13)(24), (14)(23)\}$$

die sogenannte Kleinsche Vierergruppe bezeichnet. Die drei nichttrivialen Elemente von V_4 haben die Ordnung 2, und das Produkt von zwei verschiedenen Elementen der Ordnung 2 ist stets das übrig gebliebene dritte Element. Es gilt $V_4 \cong \mathbb{Z}/2 \times \mathbb{Z}/2$. Um einen Isomorphismus hinzuschreiben, muß man allerdings die Symmetrie zwischen den Elementen $(12)(34)$, $(13)(24)$ und $(14)(23)$ brechen und zwei davon als Erzeuger auswählen. Weil V_4 mit jedem Element auch dessen konjugierte enthält, ist V_4 nicht nur in A_4, sondern auch in S_4 ein Normalteiler. Für die Faktorgruppe gilt

$$S_4/V_4 \cong S_3.$$

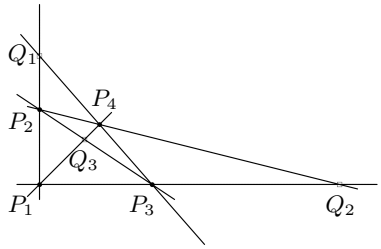
Daß S_4 einen nichttrivialen Homomorphismus $\pi : S_4 \to S_3$ in eine symmetrische Gruppe von kleinerem Grad > 2 zuläßt, ist eine Besonderheit der Zahl 4.

Abstrakt kombinatorisch stellt sich dieser Zusammenhang so dar: Es gibt drei Möglichkeiten, die Mengen $A = \{a_1, a_2, a_3, a_4\}$ in zwei Teilmengen mit je 2 Elementen zu zerlegen:

$$m_1 = \{\{1,2\},\{3,4\}\}, \quad m_2 = \{\{1,3\},\{2,4\}\}, \quad m_3 = \{\{1,4\},\{2,3\}\}.$$

Werden die Elemente der Menge A auf irgendeine Weise vertauscht, so werden auch die Elemente der Menge $M = \{m_1, m_2, m_3\}$ M_1 untereinander vertauscht. Dies definiert einen surjektiven Homomorphismus $S_4 \cong \mathrm{Sym}(A) \to \mathrm{Sym}(M) \cong S_3$.

Diese kombinatorische Situation wird wie folgt geometrisch realisiert: Bezeichnen P_1, P_2, P_3 und P_4 vier Punkte in der Ebene in allgemeiner Lage, so schneiden sich die sechs Geraden durch je zwei Punkte in drei weiteren Punkten Q_1, Q_2 und Q_3. Jede Permutation der vier Punkte P_i führt zu einer Permutation der drei Punkte Q_j.



Der Homomorphismus $S_4 \to S_3$ läßt sich auch mit den Symmetrien eines Würfels realisieren. Es bezeichne W einen Würfel im $\mathbb{R}^3$ mit Mittelpunkt im Koordinatenursprung. Die Untergruppe $\mathrm{SO}(W) \subset \mathrm{SO}(3)$ aller Drehungen, die den Würfel in sich abbilden, hat die Ordnung 24: Die Gruppe operiert transitiv auf den 8 Ecken, und die Standgruppe einer Ecke besteht aus den drei Drehungen um die Achse durch diese Ecke mit den Drehwinkeln 0, $2\pi/3$ und $4\pi/3$. Nach den Bahnengleichungen ist die Ordnung von $\mathrm{SO}(W)$ also $8 \cdot 3 = 24$. Die Gruppe $\mathrm{SO}(W)$ permutiert zum einen die vier Diagonalen durch die acht Ecken des Würfels, was auf einen Homomorphismus $\psi : \mathrm{SO}(W) \to S_4$ führt. Eine Drehung, die alle vier Diagonalen in sich abbildet, muß die Identität sein. Deshalb ist ψ injektiv, und weil die beiden Gruppen dieselbe Mächtigkeit haben, sogar ein Isomorphismus. Färbt man die Ecken des Würfels abwechseln weiß und schwarz ein, werden zwei Tetraeder T' und T'' mit weißen bzw. schwarzen Ecken definiert. Unter ψ entspricht die Untergruppe $\mathrm{SO}(T') = \mathrm{SO}(T') \subset \mathrm{SO}(W)$ genau der Gruppe A_4. Andererseits permutiert $\mathrm{SO}(W)$ auch die drei Achsen durch die sechs Flächenmittelpunkte, und dies führt auf einen Homomorphismus $\mathrm{SO}(W) \to S_3$. Durch Zusammensetzung mit ψ^{-1} erhält man wieder den alten Homomorphismus $S_4 \to S_3$.

9.6. **Einfachheit der alternierenden Gruppen A_n, $n \geq 5$.**

Eine Gruppe G heißt einfach, wenn G nicht trivial ist und wenn G und die triviale Untergruppe die einzigen Normalteiler in G sind.

Satz 9.11 — *Die Gruppen A_n sind für $n \geq 5$ einfach.*

Beweis. Es sei $n \geq 5$ und $N \subset A_n$ ein nichttrivialer Normalteiler. Weil A_n von den 3-Zykeln erzeugt wird, genügt es zu zeigen, daß N alle 3-Zykel enthält. Wenigstens einer der folgenden Fälle muß eintreten:

1. Fall: N enthält einen 3-Zykel, ohne Einschränkung $\pi = (123)$. Ist nun (ijk) irgendein anderer 3-Zykel, so gibt es eine Permutation $\sigma \in S_n$ mit $\sigma(123)\sigma^{-1} = (ijk)$. Aber auch $\sigma' = \sigma(45)$ hat die Eigenschaft $\sigma'(123){\sigma'}^{-1} = (ijk)$. Weil σ und σ' verschiedenes Vorzeichen haben, liegt entweder σ oder σ' in A_n. Damit ist (ijk) in A_n zu (123) konjugiert und liegt in N. Deshalb enthält N alle 3-Zykel und ist gleich A_n.

2. Fall: N enthält eine Permutation π, deren Zykelzerlegung einen Zykel der Länge ≥ 4 enthält, etwa $\pi = (1234\cdots)\cdot\ldots$. Mit π liegt dann auch

$$(123)\pi(123)^{-1}\pi^{-1} = (123)(1234\cdots)(132)(\cdots 4321) = (124)$$

in N. Weiter mit Fall 1.

3. Fall: N enthält eine Permutation π, deren Zykelzerlegung einen 3-Zykel und einen weiteren Zykel der Länge ≥ 2 enthält, etwa $\pi = (123)(45\cdots)\cdot\ldots$. Mit π enthält N auch

$$(124)\pi(124)^{-1}\pi^{-1} = (124)(123)(45)(142)(45)(132) = (12534).$$

Weiter mit Fall 2.

4. Fall: N enthält eine Permutation π, deren Zykelzerlegung wenigstens drei 2-Zykel enthält, etwa $\pi = (12)(34)(56)\cdot\ldots$. Mit π enthält N dann auch

$$(135)\pi(135)^{-1}\pi^{-1} = (135)(12)(34)(56)(153)(56)(34)(12) = (135)(264).$$

Weiter mit Fall 3.

5. Fall: N enthält eine Permutation π, deren Zykelzerlegung genau zwei Faktoren der Länge 2 enthält, etwa $\pi = (12)(34)$. Mit π enthält N dann auch

$$(125)\pi(125)^{-1}\pi^{-1} = (125)(12)(34)(152)(34)(12) = (152).$$

Weiter mit Fall 1. □

Folgerung 9.12 — *Für $n \geq 5$ ist A_n perfekt, d.h. $[A_n, A_n] = A_n$.*

Beweis. Die Kommutatoruntergruppe ist ein Normalteiler und deshalb entweder trivial oder gleich A_n. Da A_n nicht abelsch ist, ist die erste Möglichkeit ausgeschlossen. □

Folgerung 9.13 — *Es sei $n \geq 1$. Die einzigen Normalteiler von S_n sind die triviale Gruppe, A_n und S_n.*

Beweis. Ist N ein Normalteiler von S_n, so ist $N \cap A_n$ ein Normalteiler in A_n. Falls $N \cap A_n = A_n$, hat man $N = A_n$ oder $N = S_n$. Falls $N \cap A_n = 1$, hat N die Ordnung ≤ 2. Aber alle Konjugationsklassen von Elementen der Ordnung 2 bestehen aus mehr als einem Element. Deshalb muß N trivial sein. □

9.7. **(*) Zur Kombinatorik der Zahlen 5 und 6.**

Wenn $m < n$, kann man die Gruppe S_m in natürlicher Weise als eine Untergruppe der Gruppe S_n auffassen, nämlich als die Gruppe derjenigen Permutationen der Menge $[n] = \{1, \ldots, n\}$, die die Elementen $m+1, \ldots, n$ fest lassen. Diese Standardeinbettung sei mit $i : S_m \to S_n$ bezeichnet. Durch Konjugation $\pi i(S_m)\pi^{-1} \subset S_n$ erhält man andere zu S_m isomorphe Untergruppen, die aber kombinatorisch ähnlich gebaut sind: Statt der Elemente $\{m+1, \ldots, n\}$ lassen sie die Elemente $\{\pi(m+1), \ldots, \pi(n)\}$ fest. Für das Paar $(m, n) = (5, 6)$ tritt die Besonderheit ein, daß es eine Einbettung $j : S_5 \to S_6$ gibt, für die die Untergruppe $j(S_5)$ nicht zur Untergruppe $i(S_5)$ konjugiert ist. Das kann man auf verschiedene Weise sehen:

1. Methode: Die Anzahl der 5-Sylowuntergruppen von S_5 ist ein Teiler von $5!/5 = 24$ und kongruent zu 1 modulo 5, was nur die Möglichkeiten 1 und 6 läßt. Der erste Fall ist ausgeschlossen, weil S_5 sonst einen Normalteiler der Ordnung 5 hätte. Es gibt also genau sechs 5-Sylowgruppen U_1,...,U_6. Die Gruppe S_5 operiert auf der Menge $X := \{U_1, \ldots, U_6\}$ durch Konjugation, und diese Wirkung ist nach der Theorie der Sylowgruppen transitiv. Dies definiert einen Homomorphismus $j : S_5 \to \mathrm{Sym}(X) \cong S_6$. Weil die Wirkung transitiv ist, hat der Kern mindestens den Index 6 in S_5. Aber die einzigen Normalteiler in S_5 sind die triviale Gruppe, A_5 und S_5 mit den Indizes 60, 2 und 1. Also ist der Kern die triviale Untergruppe, d.h. j ist injektiv. Alle zu $i(S_5)$ konjugierten Untergruppen lassen ein Element fest, während $j(S_5)$ transitiv operiert. Deshalb kann $j(S_5)$ nicht zu $i(S_5)$ isomorph sein.

Um diesen Gedankengang weiter auszubeuten, betrachten wir irgendeine Gruppe $H \subset S_6$ der Ordnung $|H| = 120$. Dann ist $[S_6 : H] = 6$, und die Menge der Nebenklassen $S_6/j(S_5)$ hat genau sechs Elemente, auf denen S_6 durch Multiplikation von links transitiv operiert. Man erhält einen Homomorphismus

$$\Psi : S_6 \to \mathrm{Sym}(S_6/H) \cong S_6.$$

Der Kern dieses Homomorphismus hat mindestens den Index 6 in S_6, und der einzige Normalteiler mit dieser Eigenschaft ist die triviale Gruppe. Deshalb ist Ψ injektiv und aus Mächtigkeitsgründen ein Isomorphismus. Man erhält also einen Automorphismus $\Psi : S_6 \to S_6$, der die Standgruppe

der Nebenklasse H, also die Untergruppe H selbst, auf die Untergruppe derjenigen Bijektionen von S_6/H abbildet, die die Nebenklasse H fest lassen. Unter dem Isomorphismus $\mathrm{Sym}(S_6/H) \cong S_6$ ist das eine Untergruppe, die zu $i(S_5)$ konjugiert ist! Das zeigt:

Satz 9.14 — *Zu jeder Untergruppe $H \subset S_6$ vom Index $[S_6 : H] = 6$ gibt es einen Automorphismus $\Psi : S_6 \to S_6$, der H isomorph auf $i(S_5)$ abbildet.* □

Speziell für $j(S_5)$ bedeutet dies, daß der Automorphismus $\Psi : S_6 \to S_6$, der $j(S_5)$ auf $i(S_5)$ schickt, kein innerer Automorphismus sein kann. Wir schließen:

Satz 9.15 — *S_6 hat äußere Automorphismen.* □

Nach einem Satz von Hölder ist S_6 die einzige symmetrische Gruppe mit dieser Eigenschaft!

Dieselbe Methode erlaubt auch einen durchsichtigen geometrischen Beweis des Satzes:

Satz 9.16 — $\mathrm{PGL}_2(\mathbb{F}_5) \cong S_5$ *und* $\mathrm{PSL}_2(\mathbb{F}_5) \cong A_5$.

Dabei bezeichnet $\mathrm{GL}_2(\mathbb{F}_5)$ die Gruppe der invertierbaren 2×2-Matrizen mit Werten in dem endlichen Körper $\mathbb{F}_5$ mit 5 Elementen und $\mathrm{SL}_2(\mathbb{F}_5)$ die Untergruppe der Matrizen mit Determinante 1. Diese Gruppen haben die Ordnung 480 bzw. 120. Das Zentrum beider Gruppen besteht aus Vielfachen der Einheitsmatrix:

$$Z(\mathrm{GL}_2(\mathbb{F}_5)) = \{\lambda I_2 \mid \lambda \neq 0\} \cong \mathbb{F}_5^* \quad \text{und} \quad Z(\mathrm{SL}_2(\mathbb{F}_5)) = \{\lambda I_2 \mid \lambda^2 = 1\} = \{\pm 1\}.$$

Die Faktorgruppen

$$\mathrm{PGL}_2(\mathbb{F}_5) = \mathrm{GL}_2(\mathbb{F}_5)/\mathbb{F}_5^* \quad \supset \quad \mathrm{PSL}_2(\mathbb{F}_5) = \mathrm{SL}_2(\mathbb{F}_5)/\{\pm 1\}$$

heißen die projektive lineare bzw. projektive spezielle lineare Gruppe vom Grad 2 über dem Körper $\mathbb{F}_5$. Die Ordnungen sind $|\mathrm{PGL}_2(\mathbb{F}_5)| = 120$ und $|\mathrm{PSL}_2(\mathbb{F}_5)| = 60$.

Beweis. Der projektive Raum

$$\mathbb{P}^1(\mathbb{F}_5) := (\mathbb{F}_5^2 \setminus \{0\})/v \sim \lambda v$$

hat sechs Elemente: $x = [x : 1]$, $x \in \mathbb{F}_5$, und $\infty = [1 : 0]$. Die Gruppe $\mathrm{PGL}_2(\mathbb{F}_5)$ operiert darauf durch Multiplikation von links, $[A] \cdot [v] := [Av]$, und zwar transitiv. Dies definiert einen Homomorphismus $j : \mathrm{PGL}_2(\mathbb{F}_5) \to \mathrm{Sym}(\mathbb{P}^1(\mathbb{F}_5)) \cong S_6$. Wenn $[A]$ im Kern liegt, muß A alle Ursprungsgeraden in der Ebene $\mathbb{F}_5^2$ in sich abbilden. Das geht nur, wenn A ein Vielfaches der Einheitsmatrix ist, also $[A]$ das Neutralelement in der Faktorgruppe $\mathrm{PGL}_2(\mathbb{F}_5)$. Anders gesagt: j ist injektiv. Deshalb ist $j(\mathrm{PGL}_2(\mathbb{F}_5))$ eine Untergruppe vom Index 6 in S_6. Es gibt also einen Automorphismus $\Psi : S_6 \to S_6$, der $j(\mathrm{PGL}_2(\mathbb{F}_5))$ isomorph auf $i(S_5)$ abbildet. Dabei geht die Untergruppe $\mathrm{PSL}_2(\mathbb{F}_5)$ isomorph auf eine Untergruppe von S_5 vom Index 2, also A_5. □

Eine Variation derselben Argumente zeigt auch:

Satz 9.17 — *Eine Gruppe der Ordnung 60 ist entweder isomorph zu A_5 oder auflösbar.*

Beweis. Es sei G eine Gruppe der Ordnung 60. Dann hat G entweder eine oder sechs 5-Sylowgruppen. Im ersten Fall ist die 5-Sylowgruppe $U \subset G$ ein auflösbarer Normalteiler mit einer Faktorgruppe G/U der Ordnung 12, die somit ebenfalls auflösbar ist. In diesem Fall ist auch G auflösbar.

Im zweiten Fall operiert G transitiv auf der Menge $X = \{U_1, \ldots, U_6\}$ der 5-Sylowgruppen, und man erhält einen nichttrivialen Homomorphismus $\varphi : G \to \mathrm{Sym}(X) \cong S_6$. Weil G nach Voraussetzung einfach ist, ist die Abbildung injektiv. Und weil die Komposition $\mathrm{sgn} \circ \varphi : G \to \mathbb{Z}/2$ keinen von 1 und G verschiedenen Kern haben kann, liegt $\varphi(G)$ in A_6. Folglich ist G isomorph zu einer Untergruppe vom Index 6 in A_6.

Die Wirkung von A_6 auf der Menge der Nebenklassen $A_6/\varphi(G)$ definiert einen Homomorphismus $\psi : A_6 \to S_6$, der aus denselben Gründen wie im vorigen Absatz injektiv mit Bild in A_6 sein muß. Also ist $\psi : A_6 \to A_6$ ein Automorphismus, der $\varphi(G)$ isomorph auf A_5 abbildet. □

2. Methode: Wir konstruieren einen äußeren Automorphismus $\Psi : S_6 \to S_6$ kombinatorisch.

Die Gruppe S_6 hat 15 Transpositionen: $(12), (13), \ldots, (56)$. Aus diesen Transpositionen lassen sich auf 15 verschiedene Weisen Tripel von paarweise elementfremden Transpositionen auswählen:

$$(12)(34)(56), (12)(35)(46), (12)(36)(45), (13)(24)(56), \ldots,$$

Und aus diesen Permutationen lassen sich auf genau sechs verschiedene Weisen Quintupel zusammenstellen, die zusammengenommen, alle 15 Transpositionen erhalten:

$$\begin{aligned}
A &= (12)(34)(56), (13)(25)(46), (14)(26)(35), (15)(24)(36), (16)(23)(45)\\
B &= (12)(34)(56), (13)(26)(45), (14)(25)(36), (15)(23)(46), (16)(24)(35)\\
C &= (12)(35)(46), (13)(24)(56), (14)(25)(36), (15)(26)(34), (16)(23)(45)\\
D &= (12)(35)(46), (13)(26)(45), (14)(23)(56), (15)(24)(36), (16)(25)(34)\\
E &= (12)(36)(45), (13)(24)(56), (14)(26)(35), (15)(23)(46), (16)(25)(34)\\
F &= (12)(36)(45), (13)(25)(46), (14)(23)(56), (15)(26)(34), (16)(24)(35)
\end{aligned}$$

Tatsächlich macht man sich leicht klar, daß sich jedes Tripel auf zwei Weisen zu einem Quintupel vervollständigen läßt, und daraus erhält man für die Anzahl der Quintupel die Formel $15 \cdot 2/5 = 6$, ohne alle Quintupel hinschreiben zu müssen. Es seien A, B, C, D, E, F diese sechs Quintupel. Jede Permutation der Ziffern $1, 2, 3, 4, 5, 6$ führt zu einer Permutation der Buchstaben A, B, C, D, E, F. Man erhält so einen Gruppenisomorphismus

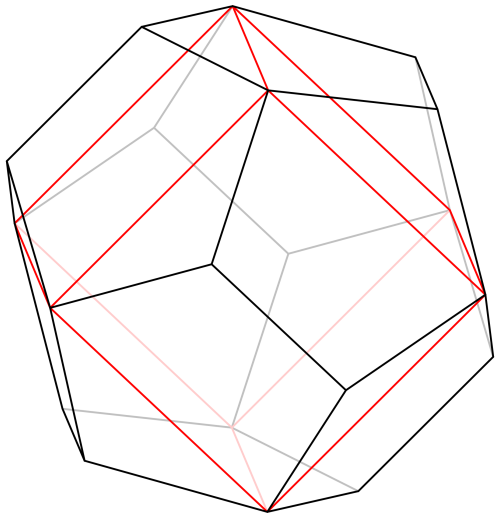
$$\Phi : \mathrm{Sym}(\{1, 2, 3, 4, 5, 6\}) \longrightarrow \mathrm{Sym}(\{A, B, C, D, E, F\}).$$

Jede willkürliche Numerierung der Menge $\{A, B, C, D, E, F\}$, d.h. jede Wahl einer Bijektion

$$\{A, B, C, D, E, F\} \to \{1, 2, 3, 4, 5, 6\}$$

macht aus Φ einen Automorphismus $\Psi \in \mathrm{Aut}(\mathrm{Sym}(\{1, 2, 3, 4, 5, 6\})) = \mathrm{Aut}(S_6)$. Dieser Automorphismus Ψ kann kein innerer Automorphismus sein. Das sieht man so: Die Transposition (12) ist Teil von genau drei Tripeln, und jedes dieser Tripel gehört zu genau zwei verschiedenen Quintupeln. Unter der Permutation (12) werden die drei Tripel auf sich selbst abgebildet, aber die zugehörigen Quintupel jeweils vertauscht. Deshalb wird unter dem Isomorphismus Φ die Transposition (12) vom Zykeltyp $[2, 1, 1, 1, 1]$ auf eine Permutation vom Zykeltyp $[2, 2, 2]$ abgebildet, nämlich $(12) \mapsto (AB)(CD)(EF)$. Deshalb kann Ψ kein innerer Automorphismus sein.

3. Methode: Man kan die außergewöhnliche Einbettung $j : A_5 \to A_6$ geometrisch am Dodekaeder realisieren. In ein Dodekaeder kann man auf fünf verschiedene Weisen einen Würfel so einbeschreiben, daß die Würfelecken eine Teilmenge der Dodekaederecken sind. Jede der zwölf Kanten eines Würfels bildet jeweils eine Diagonale einer Seitenfläche des Dodekaeders.



Die Gruppe $\mathbb{I} \subset \mathrm{SO}(3)$ der orientierungserhaltenden Symmetrien eines Dodekaeders hat die Ordnung 60: Die Gruppe operiert transitiv auf den 20 Ecken, und die Standgruppe einer Ecke besteht aus den drei Drehungen um die Achse durch die Ecke mit den Winkeln 0, $2\pi/3$ und $4\pi/3$. Diese Gruppe muß die eingebetteten Würfel untereinander permutieren. Man erhält so einen Homomorphismus $a : \mathbb{I} \to S_5$. Eine Drehung, die alle Würfel festläßt, muß auch alle Achsen in sich abbilden und ist deshalb ein Vielfaches der Identität. Weil die Abbildung orientierungserhaltend ist, ist es die Identität, d.h. der Homomorphismus ρ ist injektiv. Das Bild ist eine Untergruppe vom Index 2 in S_5 und deshalb gleich der alternierenden Gruppe A_5.

Andererseits gibt es genau 6 Achsen durch die Flächenmittelpunkte der begrenzenden Fünfecke, und diese werden von der Gruppe $\mathbb{I}$ transitiv permutiert. Man erhält einen zusammengesetzten Homomorphismus

$$j : A_5 \xrightarrow{a^{-1}} \mathbb{I} \longrightarrow S_6.$$

Die Abbildung ist nicht trivial und damit sogar injektiv, weil A_5 einfach ist. Und weil die Einschränkung des Signaturhomomorphismus $\mathrm{sgn} : S_6 \to \{\pm 1\}$ trivial sein muß, liegt das Bild in $A_6 \subset S_6$. Schließlich ist j nicht die Standardeinbettung, weil die Wirkung von $\mathbb{I}$ auf den sechs Flächenmittelpunktsachsen transitiv ist.

§10. (*) Lineare Gruppen

10.1. **Matrizengruppen.**

Es sei K ein beliebiger Körper. Die invertierbaren $n \times n$-Matrizen mit Koeffizienten in K bilden die sogenannte *allgemeine lineare Gruppe* $\mathrm{GL}_n(K)$. Die Determinante ist ein surjektiver Homomorphismus

$$\det : \mathrm{GL}_n(K) \to K^\times.$$

Ihr Kern ist die *spezielle lineare Gruppe* $\mathrm{SL}_n(K)$ der Matrizen mit Determinante 1. In der $\mathrm{SL}_n(K)$ liegen unter anderem die *Elementarmatrizen* $E_{ij}(\lambda)$ mit den Einträgen $(E_{ij}(\lambda))_{ab} = \delta_{ab} + \lambda\delta_{ai}\delta_{bj}$. Dabei sind i, j verschiedene Indizes und $\lambda \in K$ ein beliebiger Skalar.

Lemma 10.1 — *$\mathrm{SL}_n(K)$ wird als Gruppe von Elementarmatrizen erzeugt.*

Beweis. Die Multiplikation einer Matrix A von links bzw. rechts mit einer Elementarmatrix entspricht einer elementaren Zeilen- bzw. Spaltentransformation. Bekanntlich läßt sich jede Matrix A durch wiederholte Zeilen- und Spaltentransformationen auf Diagonalgestalt bringen. Es genügt also zu zeigen, daß sich jede Diagonalmatrix als Produkt von Elementarmatrizen schreiben läßt. Nun gilt

$$\begin{pmatrix} a & & & \\ & b & & \\ & & c & \\ & & & d \\ & & & & \ddots \end{pmatrix} = \begin{pmatrix} a & & & \\ & a^{-1} & & \\ & & 1 & \\ & & & 1 \\ & & & & \ddots \end{pmatrix} \begin{pmatrix} 1 & & & \\ & ab & & \\ & & (ab)^{-1} & \\ & & & 1 \\ & & & & \ddots \end{pmatrix} \begin{pmatrix} 1 & & & \\ & 1 & & \\ & & abc & \\ & & & (abc)^{-1} \\ & & & & \ddots \end{pmatrix} \cdots$$

Deshalb kann man sich auf den Fall von 2×2-Matrizen zurückziehen. Für $a \in K^\times$ gilt

$$\begin{pmatrix} 1 & 0 \\ a^{-2} - a^{-1} & 1 \end{pmatrix} \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 1 - a^{-1} & 1 \end{pmatrix} \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix}$$

□

Satz 10.2 — *Von den Ausnahmefällen $\mathrm{SL}_2(\mathbb{F}_2)$ und $\mathrm{SL}_2(\mathbb{F}_3)$ abgesehen, sind alle Gruppen $\mathrm{SL}_n(K)$ für $n \geq 2$ und beliebige Körper K perfekt.*

Beweis. Weil $\mathrm{SL}_n(K)$ von Elementarmatrizen erzeugt wird, genügt es zu zeigen, daß sich jede Elementarmatrix $E_{ij}(\lambda)$ als Kommutator schreiben läßt. Falls $n \geq 3$, kann man k verschieden von i und j wählen. Dann gilt $[E_{ik}(\lambda), E_{kj}(1)] = E_{ij}(\lambda)$.

Im Falle $n = 2$ gilt die Identität:

$$\left[\begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix}, \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \right] = \begin{pmatrix} 1 & (a^2 - 1)b \\ 0 & 1 \end{pmatrix}.$$

Wenn der Körper mehr als 3 Elemente enthält, kann man immer ein $a \neq -1, 0, 1$ finden. Dann sind sowohl a wie $a^2 - 1$ invertierbar, und mit der Wahl $b = \lambda/(a^2 - 1)$ hat man eine Darstellung von $E_{12}(\lambda)$ als Kommutator gefunden. Die Matrix $E_{21}(\lambda)$ erhält man analog.

Demnach ist $\mathrm{SL}_n(K)$ perfekt bis auf die möglichen Ausnahmen $n = 2$ und $|K| \leq 3$. □

Auf der Menge $K^n \setminus \{0\}$, $n \geq 1$, wird durch

$$v \sim v' \quad :\Leftrightarrow \quad v' = \lambda v \text{ für ein } \lambda \in K^\times$$

eine Äquivalenzrelation definiert. Die Menge der Äquivalenzklassen

$$\mathbb{P}^{n-1}(K) := K^n \setminus \{0\} / \sim$$

heißt der $n-1$-dimensionale projektive Raum über dem Körper K. Punkte in $\mathbb{P}^{n-1}$ entsprechen wahlweise Äquivalenzklassen in $K^n \setminus \{0\}$ oder eindimensionale Untervektorräume in K^n, nämlich die von den Äquivalenzklassen aufgespannten Geraden.

Die Gruppen $\mathrm{GL}_n(K)$ und $\mathrm{SL}_n(K)$ operieren auf $\mathbb{P}^{n-1}(K)$ durch Linksmultiplikation: Für zwei nichttriviale Vektoren $v, v' \in K^n$ gilt $v \sim v' \Leftrightarrow Av \sim Av'$. Deshalb ist die Wirkung

$$\mathrm{GL}_n(K) \times \mathbb{P}^{n-1}(K) \to \mathbb{P}^{n-1}(K), \quad (A, [v]) \mapsto [Av],$$

wohldefiniert.

Lemma 10.3 — *Eine Matrix $A \in \mathrm{GL}_n(K)$ wirkt auf $\mathbb{P}^{n-1}(K)$ genau dann trivial, wenn A ein Vielfaches der Einheitsmatrix ist.*

Beweis. Die Wirkung ist genau dann trivial, wenn A jede Gerade in K^n in sich abbildet. Bezüglich der Standardbasis $e_1, \ldots, e_n$ hat A also Diagonalgestalt, etwa $A = \mathrm{diag}(a_1, \ldots, a_n)$. Damit auch $e_1 + \ldots + e_n$ ein Eigenvektor ist, müssen alle Eigenwerte $a_1, \ldots, a_n$ untereinander gleich sein. □

Die Gruppe $Z := \{\lambda I_n \mid \lambda \in K^\times\}$ ist genau das Zentrum von $\mathrm{GL}_n(K)$ und deshalb ein Normalteiler. Als Gruppe ist Z isomorph zur Einheitengruppe $K^\times$. Weil die Elemente des Zentrums trivial auf dem projektiven Raum operieren, steigt die Wirkung von $\mathrm{GL}_n(K)$ auf $\mathbb{P}^{n-1}(K)$ zu einer Wirkung der Faktorgruppe

$$\mathrm{PGL}_n(K) := \mathrm{GL}_n(K)/Z$$

ab. Der Durchschnitt

$$Z_0 = Z \cap \mathrm{SL}_n(K) = \{\lambda I_n \mid \lambda^n = 1\}$$

ist isomorph zur Gruppe $\mu_n(K) = \{\lambda \in K \mid \lambda^n = 1\}$ der n-ten Einheitswurzeln in K. Analog steigt die Wirkung von $\mathrm{SL}_n(K)$ zu einer Wirkung der Faktorgruppe

$$\mathrm{PSL}_n(K) := \mathrm{SL}_n(K)/Z_0$$

ab. Die Gruppen $\mathrm{PGL}_n(K)$ und $\mathrm{PSL}_n(K)$ heißen die *allgemeine* bzw. *spezielle projektive lineare Gruppe* über K. Alle diese Gruppen lassen sich in dem folgenden kommutativen Diagramm mit exakten Zeilen und Spalten anordnen:

$$\begin{array}{ccccccccc}
 & & 1 & & 1 & & 1 & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
1 & \longrightarrow & \mu_n(K) & \longrightarrow & K^\times & \xrightarrow{a \mapsto a^n} & K^{\times n} & \longrightarrow & 1 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
1 & \longrightarrow & \mathrm{SL}_n(K) & \longrightarrow & \mathrm{GL}_n(K) & \xrightarrow{\det} & K^\times & \longrightarrow & 1 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
1 & \longrightarrow & \mathrm{PSL}_n(K) & \longrightarrow & \mathrm{PGL}_n(K) & \xrightarrow{\det} & K^\times/K^{\times n} & \longrightarrow & 1 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & 1 & & 1 & & 1 & &
\end{array}$$

wobei $K^{\times n} = \{a^n \mid a \in K^\times\}$.

Im Folgenden soll die Wirkung

$$\mathrm{PGL}_n(K) \times \mathbb{P}^{n-1}(K) \longrightarrow \mathbb{P}^{n-1}(K)$$

oder in äquivalenter Formulierung der Gruppenhomomorphismus

$$\rho : \mathrm{PGL}_n(K) \to \mathrm{Sym}(\mathbb{P}^{n-1}(K))$$

untersucht werden.

10.2. **Transitive und imprimitive Wirkungen.**

Definition 10.4. — Es sie $G \times X \to X$ eine Gruppenwirkung.

(1) Die Wirkung heißt transitiv, wenn es zu beliebigen $x, y \in X$ ein Gruppenelement $g \in G$ mit $gx = y$ gibt.
(2) Die Wirkung heißt k-fach transitiv, wenn zu beliebigen k-Tupeln von paarweise verschiedenen Punkten $x_1, \ldots, x_k \in X$ und $y_1, \ldots, y_k \in X$ ein Gruppenelement $g \in G$ mit $gx_1 = y_1, \ldots, gx_k = y_k$ gibt.
(3) Eine transitive Wirkung heißt *imprimitiv*, wenn es eine disjunkte Zerlegung

$$X = B_1 \cup B_2 \cup \ldots$$

in echte, mehrelementige Teilmengen von X gibt, die von allen $g \in G$ erhalten wird, d.h. wenn $g(B_i) = B_j$ für jedes i und geeignetes j. Die Mengen B_1, B_2, ... heißen *Imprimitivitätsgebiete*. Eine transitive Wirkung, die nicht imprimitiv ist, heißt *primitiv*.

Satz 10.5 — *Es sei $n \geq 2$. Die Wirkung von $\mathrm{PSL}_n(K)$ auf $\mathbb{P}^{n-1}(K)$ ist zweifach transitiv.*

Beweis. Es seien x_1, x_2 und y_1, y_2 zwei Paare verschiedener Punkte auf $\mathbb{P}^{n-1}(K)$, die von Vektoren v_1, v_2 bzw. w_1, w_2 in K^n repräsentiert werden. Daß x_1 und x_2 verschieden sind bedeutet, daß v_1 und v_2 linear unabhängig sind. Sie lassen sich deshalb zu einer Basis $v_1, \ldots, v_n$ erweitert. Ebenso gibt es eine Erweiterung von w_1 und w_2 zu einer Basis $w_1, \ldots, w_n$ von K^n. Es bezeichne A die eindeutig bestimmte Matrix mit $Av_i = w_i$ für $i = 1, \ldots, n$. Indem man w_n nötigenfalls um einen Skalar abändert, kann man erreichen, daß $\det(A) = 1$. Dann ist $[A] \in \mathrm{PSL}_n(K)$ mit $[A]x_i = y_i$ für $i = 1, 2$. □

Satz 10.6 — *Die Wirkung von $\mathrm{PGL}_2(K)$ auf $\mathbb{P}^1(K)$ ist dreifach transitiv.*

Beweis. Es seien x_1, x_2, x_3 und y_1, y_2, y_3 zwei Tripel von paarweise verschiedenen Punkten auf $\mathbb{P}^1(K)$. Es seien Vektoren v_1, v_2, v_3 und w_1, w_2, w_3 gewählt, die diese Punkte repräsentieren. Weil $x_1 \neq x_2$, sind v_1 und v_2 linear unabhängig und eine Basis von K^2. Schreibt man $v_3 = \alpha v_1 + \beta v_2$, so ist $\alpha \neq 0$, weil $x_3 \neq x_2$, und analog $\beta \neq 0$, weil $x_3 \neq x_1$. Indem man gegebenenfalls v_1 und v_2 durch αv_1 und βv_2 ersetzt, kann man ohne Einschränkung erreichen, daß $v_1 + v_2 = v_3$. Analog verfährt man mit den Vektoren w_1, w_2 und $w_3 = w_1 + w_2$. Die eindeutig bestimmte Matrix A mit $Av_1 = w_1$ und $Av_2 = w_2$ hat dann auch die Eigenschaft $Av_3 = w_3$. Es folgt $[A]x_i = y_i$ für $i = 1, 2, 3$. □

Es sei $G \times X \to X$ eine transitive Wirkung von X, d.h. die Menge X besteht aus einer einzigen Bahn unter G. Dagegen zerfällt X für eine Untergruppe $H \subset G$ möglicherweise in mehrere Bahnen $Hx, x \in R \subset X$. Spezielle für den Fall eines Normalteilers N passiert das Folgende: Wir betrachten eine N-Bahn Nx und den Effekt einer zusätzlichen Wirkung durch ein $g \in G$. Es gilt $gNx = gNg^{-1}(gx) = N(gx)$. Das Element g bildet also die Bahn Nx wieder auf eine Bahn $N(gx)$ ab. Die zweite Bahn stimmt entweder mit der ersten überein oder zu dieser disjunkt. Läßt man g durch die ganze Gruppe G laufen, erhält man wegen der Transitivität der G-Wirkung auf X eine Zerlegung von X in gleichgroße disjunkte G-Bahnen:

Satz 10.7 — *Es sei $G \times X \to X$ eine transitive Gruppenwirkung und $N \lhd G$ ein Normalteiler.*

(1) *Die Menge X zerfällt in gleich große N-Bahnen, die unter der Wirkung von G permutiert werden.*
(2) *Wenn G zweifach transitiv operiert, so ist die Wirkung von N auf X entweder trivial oder ebenfalls transitiv.*

Beweis. Es bleibt die zweite Aussage zu beweisen. Wir nehmen an, die Wirkung von G auf X sei zweifach transitiv, und die Wirkung von N sei weder trivial noch transitiv. Dann gibt es wenigstens zwei verschiedene N-Bahnen B und B' in X, die jeweils aus mehr als einem Element bestehen, etwa $B = \{x, y, \ldots\}$ und $B' = \{x', y', \ldots\}$. Weil die Wirkung von G zweifach transitiv ist, gibt es ein $g \in G$ mit $gx = x$ und $gy = y'$. Dann ist gB weder zu B disjunkt, noch stimmt es mit B überein. Widerspruch. □

10.3. **Endliche lineare Gruppen.**

Im Folgenden betrachten wir speziell die im ersten Abschnitt eingeführten linearen Gruppen für den Fall eines endlichen Körpers $\mathbb{F}_q$ mit q Elementen. Dann sind alle linearen und projektiven linearen Gruppen endlich. Wir besimmten zunächst ihre Ordnungen:

Satz 10.8 — $|\operatorname{GL}_n(\mathbb{F}_q)| = q^{\binom{n}{2}} \prod_{i=1}^{n}(q^i - 1)$ *und* $|\operatorname{SL}_n(\mathbb{F}_q)| = q^{\binom{n}{2}} \prod_{i=2}^{n}(q^i - 1)$.

Beweis. Die Gruppe $\operatorname{GL}_n(\mathbb{F}_q)$ operiert durch Multiplikation von links transitiv auf der Menge der von 0 verschiedenen Vektoren im Vektorraum $\mathbb{F}_q^n$. Die Anzahl dieser Vektoren ist demnach $q^n - 1$. Die Standgruppe des ersten Standardbasisvektors ist

$$H = \left\{ \begin{pmatrix} 1 & u \\ 0 & A \end{pmatrix} \;\middle|\; u \in \mathbb{F}_q^{n-1}, A \in \operatorname{GL}_{n-1}(\mathbb{F}_q) \right\}.$$

Das führt auf die rekursive Beziehung:

$$|\operatorname{GL}_n(\mathbb{F}_q)| = (q^n - 1)|H| = (q^n - 1)q^{n-1}|\operatorname{GL}_{n-1}(\mathbb{F}_q)|.$$

Daraus folgt die erste Behauptung durch Induktion. Die zweite folgt aus der ersten, weil das Bild der Determinante die Ordnung $|\mathbb{F}_q^\times| = q - 1$ hat. □

Weil die Einheitengruppe von $\mathbb{F}_q$ zyklisch von der Ordnung $q - 1$ ist, ist die Gruppe $\mu_n(\mathbb{F}_q)$ der n-ten Einheitswurzeln isomorph zur Untergruppe in $\mathbb{Z}/(q-1)$ aller Elemente $a \bmod (q-1)$ mit $na \equiv 0$. Deren Anzahl ist $\operatorname{ggT}(q-1, n)$. Mit anderen Worten:

Folgerung 10.9 — *Es gilt* $|\mu_n(\mathbb{F}_q)| = \operatorname{ggT}(q-1, n)$ *und*

$$|\operatorname{PSL}_n(\mathbb{F}_q)| = \frac{q^{\binom{n}{2}}}{\operatorname{ggT}(q-1, n)} \prod_{i=2}^{n}(q^i - 1). \quad \square$$

Der $n-1$-dimensionale projektive Raum hat

$$|\mathbb{P}^{n-1}(K)| = \frac{|K^n \setminus \{0\}|}{|\mathbb{F}_q^\times|} = \frac{q^n - 1}{q - 1} = q^{n-1} + \ldots + q + 1$$

Elemente. Insbesondere definiert die Wirkung von $\operatorname{PGL}_n(\mathbb{F}_q)$ einen injektiven Gruppenhomomorphismus

$$\rho : \operatorname{PGL}_n(\mathbb{F}_q) \to S_m, \quad m = \frac{q^n - 1}{q - 1}.$$

$\boxed{\operatorname{PGL}_2(\mathbb{F}_2)}$ Die Gruppen $\operatorname{PGL}_2(\mathbb{F}_2)$, $\operatorname{GL}_2(\mathbb{F}_2)$, $\operatorname{PSL}_2(\mathbb{F}_2)$ und $\operatorname{SL}_2(\mathbb{F}_2)$ sind alle gleich und haben die Mächtigkeit 6. Man hat einen injektiven Gruppenhomomorphismus $\rho : \operatorname{PGL}_2(\mathbb{F}_2) \to S_m$, $m = \frac{2^2-1}{2-1} = 3$. Das zeigt:

$$\operatorname{PSL}_2(\mathbb{F}_2) \cong S_3.$$

Insbesondere ist $\operatorname{PSL}_2(\mathbb{F}_2)$ auflösbar.

$\boxed{\operatorname{PGL}_2(\mathbb{F}_3)}$ Es gilt $|\operatorname{GL}_2(\mathbb{F}_3)| = 48$, und $|\operatorname{PGL}_2(\mathbb{F}_3) = 24$. Aus der Injektivität des Homomorphismus $\rho : \operatorname{PGL}_2(\mathbb{F}_3) \to S_m$, $m = \frac{3^2-1}{3-1} = 4$, folgt:

$$\operatorname{PGL}_2(\mathbb{F}_3) \cong S_4 \quad \text{und} \quad \operatorname{PSL}_2(\mathbb{F}_3) \cong A_4.$$

Insbesondere ist $\operatorname{PSL}_2(\mathbb{F}_3)$ auflösbar.

$\boxed{\mathrm{PGL}_2(\mathbb{F}_4)}$ Man hat $|\,\mathrm{GL}_2(\mathbb{F}_4)| = 180$ und $|\,\mathrm{PGL}_2(\mathbb{F}_4) = 60$. Die Wirkung auf $\mathbb{P}^1(\mathbb{F}_4)$ definiert eine injektiven Homorphismus $\rho : \mathrm{PGL}_2(\mathbb{F}_4) \to S_m$, $m = \frac{4^2-1}{4-1} = 5$, und somit einen Isomorphismus

$$\mathrm{PSL}_2(\mathbb{F}_4) = \mathrm{PGL}_2(\mathbb{F}_4) \cong A_5.$$

$\boxed{\mathrm{PGL}_2(\mathbb{F}_5)}$ Es gilt $|\,\mathrm{GL}_2(\mathbb{F}_5)| = 480$ und $\mathrm{PGL}_2(\mathbb{F}_5) = 120$. Der injektive Homomorphismus $\rho : \mathrm{PGL}_2(\mathbb{F}_5) \to S_m$, $m = \frac{5^2-1}{5-1} = 6$, definiert also Einbettungen $\mathrm{PGL}_2(\mathbb{F}_5) \to S_6$ und $\mathrm{PSL}_2(\mathbb{F}_5) \to A_6$ vom Index 6. Wie in Abschnitt 9.7 ausgeführt folgt hieraus schon:

$$\mathrm{PGL}_2(\mathbb{F}_5) \cong S_5 \quad \text{und} \quad \mathrm{PSL}_2(\mathbb{F}_5) \cong A_5.$$

Insbesondere hat man den merkwürdigen Umstand:

Satz 10.10 — $\mathrm{PSL}_2(\mathbb{F}_4) \cong \mathrm{PSL}_2(\mathbb{F}_5) \cong A_5$.

Satz 10.11 — *Für alle* $(n,q) \neq (2,2),(2,3)$ *sind die Gruppen* $\mathrm{PSL}_n(\mathbb{F}_q)$ *einfach.*

Beweis. Wenn $(n,q) \neq (2,2),(2,3)$, ist die Gruppe $G = \mathrm{SL}_n(\mathbb{F}_q)$ nach Satz 10.2 perfekt und operiert nach Satz 10.5 zweifach transitiv auf $\mathbb{P}^{n-1}(\mathbb{F}_q)$. Insbesondere ist die Wirkung primitiv. Angenommen, G ist nicht einfach. Es sei dann $N \lhd G$ ein maximaler nichttrivialer echter Normalteiler. Weil N nichttrivial und die Wirkung von G auf $\mathbb{P}^{n-1}(\mathbb{F}_q)$ effektiv ist, haben die N-Bahnen eine Länge $n \geq 2$. Nach Satz 10.7 muß N ebenfalls transitiv auf $\mathbb{P}^{n-1}(\mathbb{F}_q)$ operieren. Betrachte die Untergruppe

$$H = \left\{ \left[\begin{array}{c|c} * & * \\ \hline 0 & * \end{array}\right] \right\} < G,$$

nämlich die Standgruppe der vom ersten Standardbasisvektor e_1 aufgespannten Gerade. Weil N transitiv wirkt, hat man

$$G = NH.$$

Die Gruppe

$$U = \left\{ \left[\begin{array}{c|c} 1 & * \\ \hline 0 & I_{n-1} \end{array}\right] \right\}$$

ist eine normale Untergruppe in H. Deshalb ist NU ein Normalteiler in $G = NH$. Weil U alle Elementarmatrizen der Gestalt $E_{1j}(\lambda)$ enthält, erzeugen die konjugierten Untergruppen gUg^{-1}, $g \in G$, zusammen die Gruppe G. Deshalb kann U keine Untergruppe von N sein, so daß $N \subsetneq NU$. Nach Voraussetzung war N aber ein maximaler echter Normalteiler von G, so daß $NU = G$ gelten muß. Wir berechnen die Kommutatoruntergruppe von G aus der Darstellung $G = NU$. Weil G perfekt, N normal und U abelsch ist, hat man:

$$G = [G,G] = [NU,NU] \subset N[U,U] = N,$$

Widerspruch. □

Die nächstgrößeren Gruppen nach $\mathrm{PSL}_2(\mathbb{F}_4)$ und $\mathrm{PSL}_2(\mathbb{F}_5)$ sind die Gruppen $\mathrm{PSL}_2(\mathbb{F}_7)$ und $\mathrm{PSL}_3(\mathbb{F}_2)$. Nach den obigen Regeln findet man leicht

$$|\,\mathrm{PSL}_2(\mathbb{F}_7)| = |\,\mathrm{PSL}_3(\mathbb{F}_2)| = 3 \cdot 7 \cdot 8 = 168.$$

Es ist klar, daß eine Gruppe der Ordnung 168 nicht zu einer alternierenden Gruppe isomorph sein kann. Im Übrigen gilt:

Satz 10.12 — *Es gibt bis auf Isomorphie nur eine einfache Gruppe der Ordnung* 168. *Insbesondere gilt*

$$\mathrm{PSL}_2(\mathbb{F}_7) \cong \mathrm{PSL}_3(\mathbb{F}_2).$$

§11. Körpererweiterungen

11.1. Charakteristik und Grad.

Wir kennen drei prinzipielle Methoden, um aus Ringen Körper zu konstruieren:

(1) Ist A ein kommutativer Ring und $\mathfrak{m}$ ein maximales Ideal, dann ist der Restklassenring $A/\mathfrak{m}$ ein Körper, der *Restklassenkörper* von $\mathfrak{m}$. Aus $\mathbb{Z}$ gewinnt man so für jede Primzahl p den endlichen Körper $\mathbb{F}_p = \mathbb{Z}/p$.

(2) Ist A ein Integritätsbereich, so ist der totale Quotientenring $Q(A)$ ein Körper, der *Quotientenkörper* von A. Das verallgemeinert den Übergang von den ganzen Zahlen $\mathbb{Z}$ zum Körper $\mathbb{Q} = Q(\mathbb{Z})$ der rationalen Zahlen.

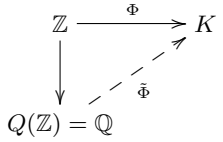
(3) Es sei K ein Körper. Dann ist $K[X]$ ein Integritätsbereich. Sein Quotientenkörper ist der *Funktionenkörper*

$$F(X) := \left\{ \frac{f(X)}{g(X)} \;\middle|\; f, g \in K[X], g \neq 0 \right\}.$$

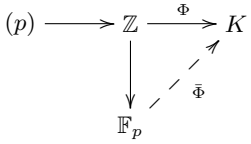
Analog kann man mit einer beliebigen Anzahl von Unbestimmten verfahren.

Eine der wichtigsten Invarianten eines Körpers ist seine *Charakteristik*: Es sei K ein Körper und 1_K das Einselement. Für jedes $n \in \mathbb{N}$ bezeichne n_K die n-fache Summe von 1_K mit sich. Die Abbildung $\mathbb{N} \to K$, $n \to n_K$, setzt sich zu einem Ringhomomorphismus $\Phi : \mathbb{Z} \to K$ fort. Der Kern von Φ ist notwendigerweise ein Primideal. Die Charakteristik $\operatorname{char}(K)$ ist die Zahl 0 oder die Primzahl p je nachdem, ob $\ker(\Phi) = (0)$ oder $\ker(\Phi) = (p)$. Es gibt also zwei fundamental verschiedene Fälle:

(1) $\operatorname{char}(K) = 0$. Dieser Fall tritt genau dann ein, wenn $n_K \neq 0$ für alle $n \in \mathbb{N}$. Der Ring $\mathbb{Z}$ wird durch Φ auf eindeutige Weise in K eingebettet. Jedes Element $\neq 0$ in $\mathbb{Z}$ ist in K invertierbar. Deshalb setzt sich die Abbildung Φ zu einem kanonischen injektiven Homomorphismus $\mathbb{Q} \to K$ des Quotientenkörpers fort.



(2) $\operatorname{char}(K) = (p)$ für eine Primzahl p. Dabei ist p die kleinste natürliche Zahl n mit $n_K = 0$. Nach der universellen Eigenschaft des Restklassenrings induziert $\mathbb{Z} \to K$ einen kanonischen injektiven Homomorphismus $\mathbb{F}_p = \mathbb{Z}/(p) \to K$.



Ein *Unterkörper* in einem Körper K ist eine Teilmenge $k \subset K$, die unter Addition und Multiplikation abgeschlossen und mit diesen ererbten Verknüpfungen ein Körper ist. Der Durchschnitt aller Unterkörper in einem gegebenen Körper ist selbst ein Unterkörper, und zwar der kleinstmögliche. Er heißt der *Primkörper* von K. Offenbar ist der Primkörper eines Körpers auf kanonische Weise zu $\mathbb{Q}$ oder $\mathbb{F}_p$ isomorph je nachdem, ob $\operatorname{char}(K) = 0$ oder p.

Körper der Charakteristik $p > 0$ unterscheiden sich in zahlreichen Punkten von Körpern der Charakteristik 0. Alle endlichen Körper haben positive Charakteristik. Ein Beispiel für einen unendlichen Körper von positiver Charakteristik ist der Körper $\mathbb{F}_p(X)$ der rationalen Funktionen über $\mathbb{F}_p$.

Die Binomialkoeffizienten $\binom{p}{k}$ sind für $0 < k < p$ durch p teilbar. Deshalb gilt in den Körpern der Charakteristik $p > 0$ die Rechenregel

$$(a_1 + \ldots + a_n)^p = a_1^p + \ldots + a_n^p. \tag{11.1}$$

Daraus ergibt sich der Satz:

Satz 11.1 — *Es sei p eine Primzahl und K ein Körper der Charakteristik p. Die Abbildung*

$$F : K \to K, \quad a \mapsto a^p,$$

ist ein injektiver Ringhomomorphismus, der sogenannte Frobeniushomomorphismus.

Definition 11.2. — Es sei K ein Körper. Eine K-Algebra ist ein Ring R zusammen mit einer Verknüpfung $K \times R \to R$, so daß R mit der Ringaddition und dieser skalaren Verknüpfung ein K-Vektorraum ist und die Ringmultiplikation $R \times R \to R$ eine K-bilineare Abbildung ist.

Wenn R ein Einselement besitzt, also insbesondere wenn R ein kommutativer Ring ist, definiert jede K-Algebrenstruktur einen Ringhomomorphismus $K \to R$, $\lambda \mapsto \lambda 1_R$, und umgekehrt definiert jeder solche Ringhomomorphismus auf R die Struktur einer K-Algebra. K-Algebren lassen sich mit Mitteln der linearen Algebra untersuchen.

Definition 11.3. — Es sei K ein Körper. Ein Homomorphismus $K \to L$ in einen Körper L heißt *Körpererweiterung* von K. Die Dimension von L als K-Vektorraum heißt *Grad* der Erweiterung und wird mit $[L : K] := \dim_K(L)$ notiert. Eine Erweiterung $K \to L$ heißt *endlich*, wenn $[L : K] < \infty$.

Da jede Körpererweiterung notwendigerweise injektiv ist, identifizieren wir K häufig mit seinem Bild und betrachten K als einen Unterkörper von L, wenn es ohne Gefahr von Mißverständnissen möglich ist. Man spricht auch von einer Einbettung des Körpers K in den Körper L. Wenn man den Homomorphismus $K \to L$ nicht betonen will, schreibt man L/K für die Erweiterung.

Beispiele 11.4. — 1. Der Körper $K = \mathbb{Q}(\sqrt[3]{2})$ besitzt drei verschiedene Einbettungen in $\mathbb{C}$. Zunächst hat man mit der Abkürzung $\alpha = \sqrt[3]{2}$ die Darstellung

$$K = \{a + b\alpha + c\alpha^2 \mid a, b, c \in \mathbb{Q}\}. \tag{11.2}$$

Um K in $\mathbb{C}$ einzubetten, muß α auf eine komplexe Zahl abgebildet werden, deren dritte Potenz 2 ist. Dazu gibt es genau drei Möglichkeiten: α, $\alpha\rho$ und $\alpha\rho^2$ mit $\rho = \exp(2\pi i/3)$. Die Wahl von α liefert einfach die Standardinklusion $\varphi_1 = \mathrm{id} : K \to \mathbb{C}$, die beiden anderen Wahlen liefern Einbettungen $\varphi_2, \varphi_3 : K \to \mathbb{C}$, deren Bilder nicht einmal in $\mathbb{R}$ landen.

2. Etwas anders ist die Situation im folgenden Fall: Der Körper $\mathbb{Q}(\sqrt{2})$ besitzt zwei verschiedene Einbettungen in $\mathbb{C}$, nämlich $\varphi_1(a + b\sqrt{2}) = a + b\sqrt{2}$ und $\varphi_2(a + b\sqrt{2}) = a - b\sqrt{2}$. In diesem Falle sind die Bilder der beiden Abbildungen gleich, aber die Abbildungen selbst sind verschieden.

3. Die Erweiterungen $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ und $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ sind endlich vom Grad 3 bzw. 2. Ähnlich ist $[\mathbb{C} : \mathbb{R}] = 2$. Die Erweiterung $\mathbb{R}/\mathbb{Q}$ hat unendlichen Grad.

Satz 11.5 — *Es seien $K \to L \to M$ Körpererweiterungen. Dann gilt*

$$[M : K] = [M : L] \cdot [L : K]. \tag{11.3}$$

Beweis. Es sei $\{x_i\}_{i\in I}$ eine K-Basis von L und $\{y_j\}_{j\in J}$ eine L-Basis von M. Wir betrachten die Familie $B := \{x_i y_j\}_{(i,j)\in I\times J}$. Es genügt zu zeigen, daß B eine Basis ist, denn $|I \times J| = |I| \cdot |J|$.

Zunächst läßt sich jedes $m \in M$ als Linearkombination $m = \sum_j \ell_j y_j$ schreiben, wobei fast alle $\ell_j \in L$ verschwinden. Weiter läßt sich jedes $\ell_j \neq 0$ als Linearkombination $\ell_j = \sum_i a_{ij} x_i$ schreiben. Insgesamt sind nur endlich viele $a_{ij} \neq 0$. Nun gilt $m = \sum_{(i,j)} a_{ij} x_i y_j$. Folglich ist B ein Erzeugersystem.

Ist andererseits $0 = \sum_{(i,j)} a_{ij} x_i y_j = \sum_j \left(\sum_i a_{ij} x_i\right) y_j$, so folgt aus der linearen Unabhängigkeit der y_j zunächst, daß $\sum_i a_{ij} x_i = 0$ für alle j, und dann aus der linearen Unabhängigkeit der x_i, daß $a_{ij} = 0$ für alle (i, j). Folglich ist B eine Basis. □

Für den Satz und den Beweis ist es unerheblich, ob die Mengen I und J endlich sind oder nicht.

Satz 11.6 — *Es sei K ein Körper, A eine kommutative nullteilerfreie K-Algebra mit $\dim_K(A) < \infty$. Dann ist A ein Körper.*

Beweis. Der Beweis ist sehr leicht. Wir führen bei der Gelegenheit Bezeichnungen ein, die wir auch später gebrauchen können. Für jedes $a \in A$ ist die Linksmultiplikation

$$\ell_a : A \to A, \quad x \mapsto ax,$$

eine K-lineare Abbildung. Die Nullteilerfreiheit von A impliziert, daß ℓ_a injektiv ist, wenn $a \neq 0$. Da $\dim_K(A) < \infty$, ist jeder injektive Endomorphismus des K-Vektorraums A auch surjektiv. Es gibt also insbesondere zu jedem $a \in A \setminus \{0\}$ ein $b \in A$ mit $ab = \ell_a(b) = 1$. □

Es sei $K \to L$ eine Körpererweiterung und $S \subset L$ eine Menge. Es gibt Unterkörper von L, die das Bild von K und S enthalten, zum Beispiel L selbst. Der Durchschnitt aller dieser Unterkörper hat dieselbe Eigenschaft und ist der kleinste Unterkörper mit dieser Eigenschaft. Er wird mit $K(S)$ bezeichnet und heißt der von S über K erzeugt Unterkörper von L. Er läßt sich auch folgendermaßen beschreiben:

$$K(S) := \left\{ \frac{p(s_1, \ldots, s_n)}{q(s_1, \ldots, s_n)} \;\middle|\; n \in \mathbb{N}_0, p, q \in K[X_1, \ldots, X_n], s_1, \ldots, s_n \in S, q(s) \neq 0. \right\}$$

Falls $S = \{a_1, \ldots, a_\ell\}$ schreiben wir kurz $K(a_1, \ldots, a_\ell)$ statt $K(\{a_1, \ldots, a_\ell\})$.

Definition 11.7. — Es sei L/K eine Körpererweiterung.

(1) Eine Menge $S \subset L$ erzeugt die Erweiterung L/K, wenn $L = K(S)$.
(2) Der Körper L heißt endlich erzeugt über K, wenn es eine endliche Menge $S \subset L$ mit $L = K(S)$ gibt.
(3) Eine Erweiterung L/K heißt einfach, wenn es ein Element $a \in L$ mit $L = K(a)$ gibt.

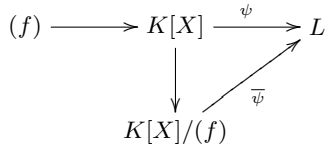
Es ist klar, daß jede endliche Körpererweiterung auch endlich erzeugt ist, denn jede Basis ist erst recht ein Erzeugendensystem. Umgekehrt wird der Funktionenkörper $K(X)$ als Körpererweiterung von K allein von X erzeugt, d.h. $K(X)/K$ ist eine einfache Erweiterung, aber $[K(X) : K] = \infty$.

Man beachte auch, daß es zu jedem $a \in K(S)$ eine *endliche* Teilmenge $S_a \subset S$ mit $a \in K(S_a)$ gibt, weil sich jedes a als Quotient von zwei Polynomen mitEinträgen aus S ausdrücken läßt, die aber jeweils nur von endlich vielen Elementen aus S abhängen können.

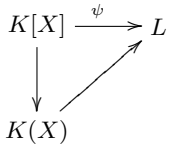
11.2. **Algebraische Erweiterungen.**

Es sei $i : K \to L$ eine Körpererweiterung und $a \in L$. Wegen der universellen Eigenschaft des Polynomrings gibt es genau einen Ringhomomorphismus $\psi : K[X] \to L$ mit $\psi|_K = i$ und $\psi(X) = a$. Wir schreiben kurz $\psi(f) =: f(a)$. Das Bild von ψ ist ein Unter*ring* von L und wird mit $K[a]$ bezeichnet. Weil jeder Unterring eines Körper nullteilerfrei ist, ist der Kern von ψ ein Primideal. Deshalb bestehen zwei Möglichkeiten:

(1) $\ker(\psi) = (f)$ mit einem eindeutig bestimmten normierten irreduziblen Polynom f. Wegen der universellen Eigenschaft des Restklassenrings faktorisiert ψ über eine Einbettung $\overline{\psi} : K[X]/(f) \to L$. Es folgt, daß $K[X]/(f) \cong K(a)$ und $[K(a) : K] = [K[X]/(f) : K] = \operatorname{grad}(f) =: n$. Es gilt dann schon $K[a] = K(a)$. Wir nennen a in diesem Falle *algebraisch* vom Grad n über K. Das Polynom f ist das eindeutig bestimmte normierte Polynom kleinsten Grades mit $f(a) = 0$. Es heißt das *Minimalpolynom* von a über K und wird mit $\operatorname{minpol}_{a/K} := f$ bezeichnet.



(2) $\ker(\psi) = (0)$. In diesem Falle wird $K[X]$ durch ψ in L eingebettet, und setzt sich gemäß der universellen Eigenschaft der Lokalisierung zu einer Einbettung des Körpers der rationalen Funktionen fort: $\Phi : K(X) \to L$. Es folgt, daß $K[X] \cong K[a]$ und $K(X) \cong K(a)$. Insbesondere ist $[K(a) : K] = \infty$. Wir nennen a in diesem Falle *transzendent* über K.



Definition 11.8. — Es sei L/K eine Körpererweiterung und $a \in L$ algebraisch über K. Ein Element $b \in L$ ist *konjugiert* zu a, wenn b Nullstelle des Minimalpolynoms von a ist.

Die Definition erweitert den Begriff der komplex konjugierten Zahl: In der Erweiterung $\mathbb{C}/\mathbb{R}$ ist jedes $z \in \mathbb{C}$ algebraisch über $\mathbb{R}$, und zwar vom Grad 1 oder 2 je nachdem ob z reell ist oder nicht. Die zu z konjugierten Zahlen sind z selbst und $\overline{z}$, die im üblichen Sinne konjugierte komplexe Zahl.

Beispiel 11.9. — Die komplexe Zahl $a = \sqrt{5} - 2$ ist algebraisch über $\mathbb{Q}$: Da $\sqrt{5} = a + 2$, folgt $5 = a^2 + 4a + 4$. Alternativ kann man $\sqrt{5}$ aus $a = \sqrt{5} - 2$ und $a^2 = 9 - 4\sqrt{5}$ eliminieren:

$$\sqrt{5} = a + 2 = \frac{1}{4}(9 - a^2). \tag{11.4}$$

Auch so ergibt sich $a^2 + 4a - 1 = 0$. Das Polynoms $x^2 + 4x - 1$ ist irreduzibel in $\mathbb{Q}[x]$, weil es keine Nullstellen in $\mathbb{Q}$ besitzt: Jede Nullstelle müßte schon ganzzahlig sein und außerdem ein Teiler des konstanten Terms. Die einzigen Teiler sind ± 1, und diese sind keine Nullstellen. Also ist $x^2 + 4x - 1$ das Minimalpolynom von a. Die zu a konjugierte Nullstelle ist $-\sqrt{5} - 2 = -a - 4 \in \mathbb{Q}(a)$.

Beispiel 11.10. — Es sei $a = \sqrt[3]{2} \in \mathbb{R}$. Dann ist $b = a^2 + a$ algebraisch über $\mathbb{Q}$: Wir finden $b^2 = (a^2 + a)^2 = a^4 + 2a^3 + a^2 = a^2 + 2a + 4$ und $b^3 = a^6 + 3a^5 + 3a^4 + a^3 = 6a^2 + 6a + 6$. Durch Elimination von a^2 und a aus diesen Gleichungen findet man $b^3 - 6b - 6 = 0$. Nach dem Eisensteinkriterium ist $x^3 - 6x - 6 \in \mathbb{Q}[X]$ irreduzibel und daher das Minimalpolynom von b. Die zu b konjugierten Elemente in $\mathbb{C}$ sind $\rho a^2 + \rho^2 a$ und $\rho^2 a^2 + \rho a$, wobei $\rho = \exp(2\pi i/3)$, wie man durch Ausmultiplizieren verifiziert:

$$(X - a^2 - a)(X - \rho a^2 - \rho a)(X - \rho^2 a^2 - \rho a) = \ldots = X^3 - 6X - 6. \tag{11.5}$$

Beachte: $a^3 = 2$, $\rho^2 + \rho + 1 = 0$. Die zu b konjugierten Zahlen sind nicht reell und liegen sicher nicht in $\mathbb{Q}(b)$.

Beispiel 11.11. — Um das reguläre Siebeneck in den Einheitskreis zeichnen zu können, bräuchte man eine Strecke der Länge $u = \cos(\alpha)$, $\alpha = 2\pi/7$. Aus dem Additionstheorem für den Kosinus folgt für beliebige $a, b \in \mathbb{R}$:

$$\cos(a + b) + \cos(a - b) = 2\cos(a) \cdot \cos(b). \tag{11.6}$$

Daraus ergibt sich:

$$\cos(2\alpha) = 2u^2 - 1, \quad \cos(3\alpha) = 2u(2u^2 - 1) - u = 4u^3 - 3u \tag{11.7}$$

und

$$\cos(4\alpha) = 2(2u^2 - 1)^2 - 1 = 8u^4 - 8u^2 + 1. \tag{11.8}$$

Da $\cos(3\alpha) = \cos(4\alpha)$ für diese spezielle Wahl von α, liefert der Vergleich die Identität

$$8u^4 - 8u + 1 = 4u^3 - 3u \tag{11.9}$$

oder

$$8u^4 - 4u^3 - 8u^2 + 3u + 1 = 0. \tag{11.10}$$

Das Polynom $8x^4 - 4x^3 - 8x^2 + 3x + 1$ ist aber nicht irreduzibel, es hat die Nullstelle 1. Division durch $x - 1$ liefert das kubische Polynom:

$$8x^3 + 4x^2 - 4x - 1 \in \mathbb{Q}[x]. \tag{11.11}$$

Es liegt nahe, die Substitution $z = 2u = e^{i\alpha} + e^{-i\alpha}$ vorzunehmen. z ist dann Nullstelle des Polynoms $f = x^3 + x^2 - 2x - 1$. Da ± 1 keine Nullstellen von f sind, ist f irreduzibel. Also ist z algebraisch über $\mathbb{Q}$ mit Minimalpolynom f. Die zu $z = 2\cos(\alpha)$ konjugierten Elemente sind $2\cos(2\alpha) = z^2 - 2$ und $2\cos(3\alpha) = z^3 - 3z$ und liegen, wie die Formeln zeigen, in $\mathbb{Q}(z)$.

Man kann dasselbe Polynom f auch wie folgt herleiten: Es sei $\zeta = \exp(2\pi i/7)$. Dann genügt ζ der Gleichung

$$\zeta^6 + \zeta^5 + \zeta^4 + \zeta^3 + \zeta^2 + \zeta + 1 = 0. \tag{11.12}$$

Außerdem ist $z = \zeta + \zeta^{-1}$. Wir teilen (11.12) durch ζ^3 und entwickeln nach Potenzen von z:

$$\begin{aligned} \zeta^3 + \zeta^2 + \zeta + 1 + \zeta^{-1} + \zeta^{-2} + \zeta^{-3} &= z^3 + \zeta^2 + \zeta^{-2} - 2\zeta - 2\zeta^{-1} + 1 \\ &= z^3 + z^2 - 2\zeta - 2\zeta^{-1} - 1 \\ &= z^3 + z^2 - 2z - 1. \end{aligned}$$

Definition 11.12. — Eine Körpererweiterung $K \to L$ heißt algebraisch, wenn jedes $a \in L$ algebraisch über K ist, und andernfalls transzendent.

Satz 11.13 — *Die folgenden Aussagen über eine Körpererweiterung L/K sind äquivalent:*

(1) *L/K ist endlich.*
(2) *L/K ist algebraisch und endlich erzeugt.*
(3) *L/K ist erzeugt von endlich vielen algebraischen Elementen.*

Beweis. $1 \Rightarrow 2$: Es sei L/K endlich vom Grad n. Jede Vektorraumbasis ist ein Erzeugersystem. Deshalb ist L/K sicher endlich erzeugt. Für jedes $a \in L$ sind die Elemente 1, a, …, a^n linear abhängig über K. Es gelte etwa $f_0 + f_1 a + \ldots + f_n a^n = 0$. Dann ist a Nullstelle des Polynoms $f = \sum_k f_k X^k$ und deshalb algebraisch.
$2 \Rightarrow 3$: Trivial.
$3 \Rightarrow 1$: Es seien $s_1, \ldots, s_n \in L$ Elemente, die algebraisch über K sind und L erzeugen. Wir zeigen durch Induktion über n, daß der Körper $K_i = K(s_1, \ldots, s_i)$ endlich über K ist. Für $i = 1$ ist dies klar. Angenommen, $i > 1$ und $[K_{i-1} : K] < \infty$. Nach Annahme ist s_i algebraisch über K, also erst recht über K_{i-1}. Es folgt mit dem Gradsatz: $[K_i : K] = [K_i : K_{i-1}] \cdot [K_{i-1} : K] < \infty$. Mit $L = K_n$ hat man die Behauptung. □

Satz 11.14 — *Die folgenden Aussagen über eine Erweiterung L/K sind äquivalent:*

(1) *L ist algebraisch über K.*
(2) *L wird von Elementen erzeugt, die algebraisch über K sind.*
(3) *Jede endliche Menge $S \subset L$ liegt in einem Zwischenkörper M von endlichem Grad über K.*

Beweis. $1 \Rightarrow 2$: Trivial.
$2 \Rightarrow 3$: Es sei T ein Erzeugendensystem von L über K aus algebraischen Elementen und $S \subset L$ eine endliche Teilmenge. Zu jedem Element $s \in S$ gibt es eine endliche Menge $T_s \subset T$ mit $s \in K(T_s)$. Es sei T' die Vereinigung aller T_s. Dann ist $M = K(T')$ ein von endlich vielen algebraischen Elementen erzeugter Zwischenkörper und nach Satz 11.13 algebraisch über K von endlichem Grad.

$3 \Rightarrow 1$: Jedes Element $a \in L$ liegt in einem Zwischenkörper von endlichem Grad über K und ist deshalb nach Satz 11.13 algebraisch über K.

□

Eine unmittelbare Folgerung des Satzes ist die folgende: Ist L/K eine Körpererweiterung, so ist die Menge aller Elemente in L, die algebraisch über K sind, ein Zwischenkörper.

Definition 11.15. — 1. Es sei L/K eine Körpererweiterung. Der Zwischenkörper aller Elemente in L, die algebraisch über K sind, heißt *algebraischer Abschluß* von K in L.
2. Der algebraische Abschluß von $\mathbb{Q}$ in $\mathbb{C}$ wird mit $\overline{\mathbb{Q}}$ bezeichnet und heißt der *Körper der algebraischen Zahlen*.

Satz 11.16 — *Es sei L/K eine algebraische und M/L eine beliebige Körpererweiterung. Ein Element $a \in M$ ist genau dann algebraisch über L, wenn a algebraisch über K ist.*

Beweis. Wenn a algebraisch über K ist, ist es trivialerweise auch algebraisch über L. Es sei also umgekehrt a algebraisch über L und $f = X^n + f_{n-1}X^{n-1} + \ldots + f_0$ das Minimalpolynom. Dann ist der von den Koeffizienten von f erzeugte Zwischenkörper $L' := K(f_0, \ldots, f_{n-1}) \subset L$ nach Satz 11.13 endlich über K, und nach Konstruktion ist a algebraisch über L'. Daher ist $[L'(a) : K] = [L'(a) : L'][L' : K] < \infty$ und somit a algebraisch über K. □

Man kann diesen Satz auch so ausdrücken, daß die Eigenschaft, eine algebraische Erweiterung zu sein, transitiv ist:

Folgerung 11.17 — *Sind $M/L/K$ Körpererweiterungen, so ist M/K genau dann algebraisch, wenn M/L und L/K algebraisch sind.* □

11.3. **Nullstellen und algebraisch abgeschlossene Körper.** Im letzten Abschnitt sind wir *analytisch* vorgegangen: Die Körpererweiterung $K \to L$ war gegeben, und zu einem algebraischen Element $a \in L$ haben wir das zugehörige Minimalpolynom betrachtet. In diesem Abschnitt gehen wir den umgekehrten *synthetischen* Weg: Wir starten mit einem Körper K und einem irreduziblen Polynom $f \in K[X]$ und konstruieren eine Erweiterung $K \to L$, in der f eine Nullstelle besitzt. Indem wir diesen Weg zu Ende gegen, können wir zu jedem Körper K eine algebraisch abgeschlossene Erweiterung $\overline{K}$ konstruieren.

Es sei $i : K \to L$ eine Körpererweiterung. Diese Abbildung erweitert sich zu einer Inklusion von Polynomringen $i' : K[X] \to L[X]$ durch $i'|_K = i$ und $i'(X) = X$. Solange keine Gefahr von Mehrdeutigkeiten besteht, schreiben wir wieder f statt $i'(f)$ für Polynome $f \in K[X]$. Ein Polynom $f \in K[X]$ kann in L Nullstellen bekommen oder über L in Faktoren zerfallen, die es über K noch nicht gab. Zum Beispiel ist $X^4 + 1 \in \mathbb{Q}[X]$ irreduzibel, besitzt aber über $\mathbb{R}$ bzw. $\mathbb{C}$ die Faktorisierungen

$$\begin{aligned} X^4 + 1 &= (X^2 + \sqrt{2}X + 1)(X^2 - \sqrt{2}X + 1) \\ &= (X - \varepsilon)(X - \varepsilon^3)(X - \varepsilon^5)(X - \varepsilon^7) \end{aligned}$$

mit der primitiven 8-ten Einheitswurzel $\varepsilon = \exp(2\pi i/8)$.

Satz 11.18 (Kronecker) — *Es sei K ein Körper und $f \in K[X]$ ein irreduzibles normiertes Polynom vom Grad n. Dann ist $M := K[X]/(f)$ eine Körpererweiterung von K vom Grad n. Die Restklasse $\overline{X} \in M$ von X ist eine Nullstelle von f.*

Beweis. Weil f ein irreduzibles Polynom ist, ist das von f erzeugte Hauptideal (f) ein maximales Ideal und deshalb $K[X]/(f)$ ein Körper. Daß $f(X) \equiv 0 \bmod (f)$, kann man auch so lesen, daß für die Restklasse $\overline{X} := X \bmod (f)$ gilt: $f(\bar{X}) = 0$. □

Man beachte, daß man — mit den Bezeichnungen des Satzes — zu jedem Element $0 \neq \bar{g} = g_0 + g_1\overline{X} + \ldots + g_{n-1}\overline{X}^{n-1} \in M$ mit dem euklidischen Algorithmus ein Inverses explizit berechnen kann: Da f irreduzibel ist, sind f und $g = g_0 + g_1 X + \ldots + g_{n-1}X^{n-1}$ in $K[X]$ teilerfremd. Man bestimmt dann mit dem euklidischen Algorithmus Polynome α und β mit $1 = \alpha f + \beta g$. Die Restklasse von β in M ist ein Inverses zu $\bar{g}$.

Folgerung 11.19 — *Es seien K ein Körper und $f_1, \ldots, f_n \in K[X] \setminus \{0\}$ Polynome. Dann gibt es eine Körpererweiterung L/K derart, daß alle f_i über L in Linearfaktoren zerfallen.*

Beweis. Man kann sich sofort auf den Fall $n = 1$ zurückziehen, indem man die Polynome durch ihr Produkt ersetzt. Es sei also f ein nichttriviales Polynom. Wir argumentieren mit Induktion über den Grad von f. Falls f den Grad 0 oder 1 hat, kann man $L = K$ wählen. Andernfalls sei $g|f$ ein irreduzibler normierter Faktor. Der Satz 11.18 garantiert die Existenz einer Erweiterung $K \to M$ und eines Elements $\beta_1 \in M$ mit $g(\beta_1) = 0$. Es sei $h := f/(X - \beta_1) \in M[X]$. Da $\operatorname{grad}(h) < \operatorname{grad}(f)$, folgt induktiv die Existenz einer Erweiterung $M \to L$ derart, daß h in $L[X]$ in Linearfaktoren zerfällt: $h = c(X - \beta_2)\cdots(X - \beta_\ell)$ mit $\beta_i \in M$ und $c \in K$. Damit hat man auch $f = c(X - \beta_1)\cdots(X - \beta_\ell)$. □

Definition 11.20. — Ein Körper K heißt algebraisch abgeschlossen, wenn die folgenden äquivalenten Bedingungen erfüllt sind:

(1) Jedes nichtkonstante Polynome $f \in K[X]$ besitzt eine Nullstelle in K.
(2) Jedes nichtkonstante Polynom $f \in K[X]$ zerfällt in ein Produkt aus Linearfaktoren.
(3) Jedes irreduzible Polynom $f \in K[X]$ hat Grad 1.

Der Beweis der Äquivalenz der Bedingungen ist einfach.

Satz 11.21 (Fundamentalsatz der Algebra) — *$\mathbb{C}$ ist algebraisch abgeschlossen.*

Da der Körper $\mathbb{C}$ als Erweiterung von $\mathbb{R}$ definiert ist und die Konstruktion von $\mathbb{R}$ analytische Elemente enthält, nämlich die Vervollständigung von $\mathbb{Q}$ bezüglich des Betrages, kommt man nicht ganz ohne analytische Hilfsaussagen aus. Man kann sie im Kern auf das folgende Lemma reduzieren:

Lemma 11.22 — *Jedes Polynom in $\mathbb{R}[X]$ von ungeradem Grad hat in $\mathbb{R}$ eine Nullstelle. Für jede positive reelle Zahl a hat $X^2 - a$ eine positive Nullstelle in $\mathbb{R}$.*

Beweis. Zwischenwertsatz. □

Aus der zweiten Aussage des Lemmas ergibt sich zunächst:

Lemma 11.23 — *Jedes quadratische Polynom in $\mathbb{C}[X]$ hat in $\mathbb{C}$ eine Nullstelle.*

Beweis. Durch quadratische Ergänzung führt man das Problem auf die Aussage zurück, daß jede komplexe Zahl eine komplexe Quadratwurzel besitzt. Ist nun $a + bi \neq 0$ vorgegeben, so führt der Ansatz $(x + iy)^2 = (a + bi)$ auf die Gleichungen

$$x^2 + y^2 = \sqrt{a^2 + b^2}, \quad x^2 - y^2 = a \tag{11.13}$$

mit den Lösungen

$$x = \pm\sqrt{\frac{1}{2}\left(a + \sqrt{a^2 + b^2}\right)}, \quad y = \pm\sqrt{\frac{1}{2}\left(-a + \sqrt{a^2 + b^2}\right)}. \tag{11.14}$$

Dabei sind die Vorzeichen so zu wählen, daß $2xy = b$. □

Beweis des Hauptsatzes der Algebra. Es genügt zu zeigen, daß jedes nichtkonstante reelle Polynom in $\mathbb{C}$ eine Nullstelle besitzt. Denn ist f ein beliebiges komplexes Polynom, so ist $g = f\overline{f}$ reell, und ist α eine Nullstelle von g, so ist entweder α oder $\overline{\alpha}$ eine Nullstelle von f.

Es sei nun ein normiertes Polynom $f \in \mathbb{R}[X]$ vom Grad n vorgelegt. Wir schreiben $n = 2^m u$ mit einer ungeraden Zahl u und einem Exponenten $m \in \mathbb{N}_0$. Wir führen den Beweis durch Induktion über m. Der Induktionsanfang $m = 0$ ist gerade der Fall eines Polynoms von ungeradem Grad $n = u$ und wird durch den Zwischenwertsatz erledigt.

Es sei also $m \geq 1$ und die Behauptung für alle Polynome vom Grad $2^{m'}u'$ mit $m' < m$ schon gezeigt. Wir wählen eine algebraische Erweiterung $\mathbb{R} \subset \mathbb{C} \subset L$ so, daß f über L in Linearfaktoren zerfällt, $f = \prod_{i=1}^{n}(X - x_i)$. Wir betrachten für einen noch näher zu bestimmenden Parameter $t \in \mathbb{R}$ und für jedes Paar von Indizes $1 \leq i < j \leq n$ die Elemente $c_{ij} = x_i + x_j + t x_i x_j$, sowie das Polynom

$$F_t := \prod_{i<j}(X - c_{ij}). \tag{11.15}$$

Offensichtlich ist F_t symmetrisch unter Permutation der x_i. Die Koeffizienten von F_t lassen sich nach dem Hauptsatz über symmetrische Polynome polynomiell durch t und die Koeffizienten von f ausdrücken, sind also insbesondere reell. Das Polynom $F_t \in \mathbb{R}[X]$ hat den Grad

$$\deg(F_t) = \binom{n}{2} = 2^{m-1}u(2^m u - 1) = 2^{m-1}u' \text{ mit ungeradem } u'. \tag{11.16}$$

Nach Induktionsannahme ist eine der Nullstellen c_{ij} von F_t komplex, d.h. es gibt ein von der Wahl von t abhängiges Paar $(i(t), j(t))$ mit $u(t) := x_{i(t)} + x_{j(t)} + t x_{i(t)} x_{j(t)} \in \mathbb{C}$. Da es mehr reelle Zahlen als Paare (i, j) gibt, gibt es zwei verschiedene reelle Parameter s, t mit $(i(s), j(s)) = (i(t), j(t)) =: (i, j)$. Wir haben also erreicht, daß

$$(x_i + x_j) + s x_i x_j = u(s) \in \mathbb{C}, \quad (x_i + x_j) + t x_i x_j = u(t) \in \mathbb{C}. \tag{11.17}$$

Dieses lineare Gleichungssystem für $x_i + x_j$ und $x_i x_j$ hat eine eindeutige Lösung, weil die Determinante gleich $t - s \neq 0$ ist. Deshalb gilt

$$x_i + x_j, \quad x_i x_j \in \mathbb{C}. \tag{11.18}$$

Damit sind x_i und x_j die beiden Lösungen einer quadratischen Gleichung mit komplexen Koeffizienten. Wir wissen, daß diese quadratische Gleichung komplexe Lösungen besitzt. □

Satz 11.24 — *Jeder Körper K besitzt eine Einbettung $K \to \tilde{K}$ in einen algebraisch abgeschlossenen Körper.*

Beweis. 1. Schritt: Wir imitieren die Konstruktion einer Nullstelle zu einem gegebenen Polynom, nur daß wir Nullstellen für alle Polynome auf einen Schlag konstruieren.

Es sei dazu $\{f_i\}_{i \in I}$ die Familie aller normierten irreduziblen Polynome $f_i \in K[X]$. Wir betrachten den Polynomring $R := K[\{X_i\}_{i \in I}]$ mit einer eigenen Unbestimmten X_i zu jedem irreduziblen Polynom f_i. Es sei $\mathfrak{a} \subset R$ das Ideal, das von allen Elementen $f_i(X_i)$, $i \in I$, erzeugt wird. Wir zeigen zunächst, daß $\mathfrak{a}$ nicht der ganze Ring ist. Wäre nämlich $1 \in \mathfrak{a}$, so gäbe es eine Darstellung $1 = \sum_i u_i f_i(X_i)$ mit irgendwelchen Elementen $u_i \in R$, von denen aber nur endlich viele ungleich 0 sind. In diesem Falle bezeichne $J \subset I$ die Menge der Indizes mit $u_i \neq 0$. Es gibt eine Körpererweiterung K'/K, über der das Polynom $\prod_{j \in J} f_j(X)$ vollständig in Linearfaktoren zerfällt. Wir wählen eine Nullstelle $\beta_j \in K'$ für jedes f_j, $j \in J$. Nach der universellen Eigenschaft des Polynomrings R gibt es genau einen K-linearen Ringhomomorphismus $\Phi : R \to K'$ mit $\Phi(X_j) = \beta_j$ für $j \in J$ und $\Phi(X_i) = 0$ für $i \in I \setminus J$. Wendet man Φ auf die Relation $1 = \sum_j u_j f_j(X_j)$ an, erhält man den Widerspruch

$$1 = \sum_j \Phi(u_j)\Phi(f_j(X_j)) = \sum_j \Phi(u_j) f_j(\Phi(X_j)) = \sum_j \Phi(u_j) f_j(\beta_j) = \sum_j \Phi_j(u_j) 0 = 0.$$

Damit ist gezeigt, daß $\mathfrak{a} \subset R$ ein echtes Ideal ist, und wir können ein maximales Ideal $\mathfrak{m}$ wählen, das $\mathfrak{a}$ enthält. Der Restklassenring $L := R/\mathfrak{m}$ ist eine Körpererweiterung von K. Bezeichnet $\alpha_i \in L$ die Restklasse von X_i, so gilt $f_i(\alpha_i) = 0$, weil $f(X_i) \in \mathfrak{a} \subset \mathfrak{m}$. In L hat also jedes Polynom von K eine Nullstelle. Außerdem ist L algebraisch über K, weil L von den Restklassen der X_f erzeugt wird, die nach Konstruktion algebraisch über K sind. Wir haben also gezeigt:

Zu jedem Körper K gibt es eine algebraische Erweiterung $K \to L$ mit der Eigenschaft, daß jedes nichtkonstante Polynom aus $K[X]$ eine Nullstelle in L besitzt.

Wir werden später sehen (Satz 12.39), daß L bereits algebraisch abgeschlossen ist. Bis dahin müssen wir anders argumentieren.

2. Schritt: Wir iterieren die Konstruktion und erhalten eine Folge von Körpererweiterungen

$$K_0 := K \to K_1 := L \to K_2 \to K_3 \to \dots \tag{11.19}$$

mit der Eigenschaft: Jedes irreduzible Polynom in $K_n[X]$ besitzt in K_{n+1} eine Nullstelle. Daraus folgt durch Induktion über den Grad: Jedes Polynom in $K_n[X]$ vom Grad $m > 0$ zerfällt in $K_{n+m}[X]$ in Linearfaktoren.

Wären die Abbildungen $K_n \to K_{n+1}$ wirklich Inklusionen, so würden wir einfach $K_\infty := \bigcup K_n$ setzen. Jedes Polynom in $K_\infty[X]$ vom Grad ℓ hat nur endlich viele Koeffizienten und liegt daher schon in $K_N[X]$ für hinreichend groß gewähltes N und zerfällt in $K_{N+\ell}[X]$ in Linearfaktoren. Also ist K_∞ algebraisch abgeschlossen (und sicher auch algebraisch über K).

Da die iterativ konstruierten Erweiterungen $u_n : K_n \to K_{n+1}$ zwar injektiv, aber keine Inklusionen sind, müssen wir anders vorgehen: Es sei $A := \bigoplus_{n\geq 0} K_n$ mit komponentenweise definierten Verknüpfungen und $i_n : K_n \to A$ die Inklusionsabbildung. Elemente in A sind also Folgen $(a_0, a_1, \dots)$ von Elementen $a_i \in K_i$, wobei höchstens endlich viele Komponenten a_i nicht 0 sind. Deshalb ist A zwar ein Ring mit kommutativer Multiplikation, hat aber kein Einselement, weil ein solches an allen Stellen eine 1 haben müßte, also nicht in A liegen kann. Es bezeichne $J \subset A$ das Ideal, das von allen Elementen der Form

$$i_{n+1}(u_n(x)) - i_n(x) = (\dots, 0, -x, u_n(x), 0, \dots)$$

erzeugt wird. Modulo J sind alle Elementen $i_n(1)$, $n \in \mathbb{N}_0$, untereinander kongruent. Deshalb ist $K_\infty := A/J$ ein kommutativer Ring mit Einselement $1 := i_n(1) \bmod J$ für alle $n \in \mathbb{N}_0$. Bezeichnet j_n den zusammengesetzten Ringhomomorphismus $K_n \to A \to K_\infty$, so gilt:

(1) $j_n : K_n \to A$ ist injektiv, also $K_n \cong K'_n := j_n(K_n) \subset A$.
(2) $j_{n+1} \circ u_n = j_n$ für alle n, d.h. $K'_n \subset K'_{n+1}$.
(3) $\bigcup_{n\geq 0} K'_n = K_\infty$.

Wie bereits ausgeführt, ist K_∞ ein algebraisch abgeschlossener Körper, und konstruktionsgemäß ist $K = K_0 \cong K'_0 \subset K_\infty$ eine algebraische Erweiterung. □

Die im zweiten Beweisschritt durchgeführte Konstruktion ist ein Beispiel für eine allgemeine Konstruktion, die einem *direkten System* von Ringen einen sogenannten *direkten Limes* oder *Kolimes* zuordnet.

Definition 11.25. — Eine Erweiterung $K \to \overline{K}$ ist ein *algebraischer Abschluß* von K, wenn $\overline{K}$ algebraisch abgeschlossen und algebraisch über K ist.

Zum Beispiel ist $\mathbb{C}$ algebraisch abgeschlossen, aber nicht der algebraische Abschluß von $\mathbb{Q}$.

11.4. **Fortsetzungen von Einbettungen.**

Zu jeder Körpererweiterung $\psi : K \to L$ gehört ein injektiver Ringhomomorphismus

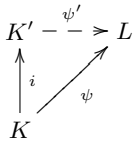
$$\psi : K[X] \to L[X]$$

mit

$$\psi : f = f_n X^n + \ldots + f_1 X + f_0 \quad \mapsto \quad \psi(f) = \psi(f_n) X^n + \ldots + \psi(f_1) X + \psi(f_0).$$

Verschiedene Einbettungen $\psi : K \to L$ derselben Körper K und L geben notwendigerweise auch verschiedene Abbildungen der Polynomringe. Solange aber keine Mißverständnisse zu erwarten sind, schreiben wir weiter f statt $\psi(f)$, so als wäre ψ einfach eine Inklusion, um die Bezeichnungen lesbar zu halten.

Definition 11.26. — Es seien $i : K \to K'$ und $\psi : K \to L$ Körpererweiterungen. Eine *Fortsetzung* von ψ auf K' ist ein Ringhomomorphismus $\psi' : K' \to L$ mit $\psi' \circ i = \psi$. Jede solche Fortsetzung ist K-linear. Umgekehrt ist jeder K-lineare Homomorphismus von Ringen $K' \to L$ eine Fortsetzung von ψ.



Satz 11.27 — *Es sei $K(a)/K$ eine einfache algebraische Erweiterung mit Minimalpolynom $f = \mathrm{minpol}_{a/K}$. Jede Fortsetzung einer gegebenen Einbettung $\psi : K \to L$ auf $K(a)$ bildet a auf eine Nullstelle von $\psi(f)$ in L ab. Umgekehrt gibt es zu jeder Nullstelle β von $\psi(f)$ in L genau eine Fortsetzung $\psi' : K(a) \to L$ mit $\psi'(a) = \beta$. Insbesondere ist die Anzahl der verschiedenen Fortsetzungen von ψ genau die Anzahl der verschiedenen Nullstellen von f in L.*

Beweis. Da $f(a) = 0$, ist zunächst klar, daß jede Fortsetzung $\psi' : K(a) \to L$ das Element a auf eine Nullstelle von $\psi(f)$ in L abbilden muß: $0 = \psi'(f(a)) = \psi(f)(\psi(a))$. Und da $K(a)$ von a erzeugt ist, liegt ψ' durch den Wert auf a fest.

Es sei nun umgekehrt eine Nullstelle $\beta \in L$ von $\psi(f)$ vorgegeben. Es ist $K(a) = K[X]/(f)$. Wegen der universellen Eigenschaft des Polynomrings gibt es genau einen Homomorphismus $\tilde{\psi} : K[X] \to L$ mit $X \mapsto \beta$, der die Erweiterung $\psi : K \to L$ fortsetzt. Dabei geht f auf $\tilde{\psi}(f(X)) = \psi(f)(\tilde{\psi}(X)) = \psi(f)(\beta) = 0$. Insbesondere faktorisiert $\tilde{\psi}$ nach der universellen Eigenschaft des Restklassenrings über einen Homomorphismus $\psi' : K(a) = K[X]/(f) \to L$. □

Satz 11.28 (Existenz von Fortsetzungen) — *Es sei L/K eine algebraische Erweiterung. Dann läßt sich jede Einbettung $j : K \to M$ in einen algebraisch abgeschlossenen Körper M zu einer Einbettung $i : L \to M$ fortsetzen.*

Beweis. Wir betrachten die Menge $X = \{(L', i')\}$ aller Paare aus einem Zwischenkörper L', $K \subset L' \subset L$, und einer Einbettung $i' : L' \to M$ mit $i'|_K = j$. Dann enthält X wenigstens das Element (K, j) und ist deshalb nicht leer. Die Menge X ist halbgeordnet durch die Relation

$$(L', i') \leq (L'', i'') :\Leftrightarrow L' \subset L'' \text{ und } i''|_{L'} = i'. \tag{11.20}$$

Ist nun $Y \subset X$ eine Kette, so setzen wir $L_Y := \bigcup_{L' \in Y} L'$ und definieren $i_Y : L_Y \to M$ durch $i_Y|_{L'} := i'$. Dann liegt das Paar (L_Y, i_Y) wieder in X und ist nach Konstruktion eine obere Schranke von Y. Mit anderen Worten: $(X, \leq)$ ist induktiv geordnet. Nach dem Zornschen Lemma existiert in X ein maximales Element (L_0, i_0).

Angenommen, die Inklusion $L_0 \subset L$ ist echt. Jedes Element $a \in L \setminus L_0$ ist algebraisch über K, also erst recht über L_0. Das Minimalpolynom g von a über L_0 besitzt in M eine Nullstelle, weil M algebraisch abgeschlossen ist. Folglich gibt es eine Fortsetzung $i_0' : L_0(a) \to M$ von i_0. Das Paar $(L_0(a), i_0')$ widerspräche der Maximalität von (L_0, i_0). Daher gilt in der Tat $L_0 = L$, und $i := i_0$ ist eine Fortsetzung von j, wie verlangt. □

Satz 11.29 (Eindeutigkeit des algebraischen Abschlusses) — *Es seien $i : K \to K'$ und $j : K \to K''$ algebraische Abschlüsse. Dann gibt es eine Fortsetzung $\psi : K' \to K''$ von j auf K', und jede solche Fortsetzung ist ein Isomorphismus.*

Beweis. Die Existenz von ψ ist eine Konsequenz des Satzes 11.28. Es sei nun $\psi : K' \to K''$ irgendeine Fortsetzung. Es ist nur zu zeigen, daß ψ surjektiv ist. Es sei $a \in K''$ vorgegeben mit Minimalpolynom h über K. Weil K' algebraisch abgeschlossen ist, zerfällt h über K' vollständing in Linearfaktoren $i(h) = (X - a_1) \cdots (X - a_q)$. Es folgt $j(h) = (X - \psi(a_1)) \cdots (X - \psi(a_1))$ in $K''[X]$. Da a eine Nullstelle von $j(h)$ ist, gilt $a = \psi(a_i)$ für ein i. □

11.5. **Endliche Körper.**

Satz 11.30 — *Es sei p eine Primzahl, K ein Körper der Charakteristik p, und $F : K \to K$ der Frobeniushomomorphismus. Falls K endlich oder algebraisch abgeschlossen ist, ist F surjektiv.*

Beweis. In jedem Falle ist F injektiv. Injektive Abbildungen einer endlichen Menge in sich selbst sind stets auch surjektiv. Das erledigt die Behauptung für endliche Körper. Falls K algebraisch abgeschlossen ist, hat die Gleichung $X^p - a = 0$ für jedes $a \in K$ eine Lösung, etwa $\beta \in K$. Es folgt $F(\beta) = \beta = a$. Also ist F auch in diesem Falle surjektiv. □

Satz 11.31 — *Es sei p eine Primzahl und $\overline{\mathbb{F}}_p$ ein algebraischer Abschluß von $\mathbb{F}_p$.*

(1) *Für jedes $\ell \in \mathbb{N}$ gibt es in $\overline{\mathbb{F}}_p$ genau einen Unterkörper mit p^ℓ Elementen. Dieser wird mit $\mathbb{F}_{p^\ell}$ bezeichnet.*
(2) *Ist K ein endlicher Körper der Charakteristik p und vom Grad ℓ über seinem Primkörper, so gilt $K \cong \mathbb{F}_{p^\ell}$.*

Beweis. Die Frobeniusabbildung $F : x \mapsto x^p$ ist ein Automorphismus von $\overline{\mathbb{F}}_p$. Dasselbe gilt dann für die ℓ-te Potenz F^ℓ. Die Menge

$$\mathbb{F}_{p^\ell} := \{u \in \overline{\mathbb{F}}_p \mid u = F^p(u) = u^{p^\ell}\}$$

der Fixpunkte von F^ℓ ist ein Unterkörper von $\overline{\mathbb{F}}_p$. Nun besteht $\mathbb{F}_{p^\ell}$ genau aus den Elementen u mit der Eigenschaft $u^{p^\ell} = u$, also den Nullstellen des Polynoms $f = X^{p^\ell} - X$. Wegen $f' = -1$ hat f keine mehrfachen Nullstellen. Da $\overline{K}$ aber algebraisch abgeschlossen ist und f deshalb in Linearfaktoren zerfällt, hat f genau p^ℓ verschiedene Nullstellen. Folglich hat $\mathbb{F}_{p^\ell}$ genau p^ℓ Elemente.

Es sei nun K irgendein endlicher Körper der Charakteristik p und vom Grad ℓ über seinem Primkörper $\mathbb{F}_p$. Nach Satz 11.28 gibt es eine Einbettung $\psi : K \to \overline{\mathbb{F}}_p$. Die Einheitengruppe $K^\times$ hat die Ordnung $p^\ell - 1$. Für jedes Element $x \in K^\times$ gilt deshalb $x^{p^\ell - 1} = 1$. Insbesondere gilt für jedes Element $x \in K$ die Gleichung $x^{p^\ell} = x$. Aber das bedeutet $\psi(K) \subset \mathbb{F}_{p^\ell}$. Da die beiden Körper gleich viele Elemente enthalten, ist $\psi : K \to \mathbb{F}_{p^\ell}$ ein Isomorphismus. □

Folgerung 11.32 — *Es sei p eine Primzahl. Zu jeder natürlichen Zahlen n gibt es genau einen Zwischenkörper $\mathbb{F}_p \subset \mathbb{F}_{p^\ell} \subset \overline{\mathbb{F}}_p$. Dabei gilt*

$$\mathbb{F}_{p^m} \subset \mathbb{F}_{p^n} \quad \Leftrightarrow \quad m|n.$$

Beweis. Jede endliche Erweiterung eines endlichen Körpers mit $q = p^m$ Elementen vom Grad ℓ enthält $q^\ell = p^{m\ell}$ Elemente. Das zeigt die Notwendigkeit der Teilbarkeitsrelation. Die Umkehrung folgt aus der Charakterisierung von $\mathbb{F}_{p^n}$ als Fixpunktmenge von F^n. □

Wir haben schon früher einen Beweis des folgenden Satzes gesehen. Der Beweis hier unterscheidet sich nur in einer Nuance von dem früheren:

Satz 11.33 — *Es sei K ein Körper. Jede endliche Untergruppe $G \subset K^\times$ ist zyklisch.*

Beweis. G ist abelsch. Wir wissen, daß in endlichen abelschen Gruppen die Ordnung jedes Elements ein Teiler des Exponenten $\mathrm{ex}(G) = \max\{\mathrm{ord}(g) \mid g \in G\}$ ist (Satz 7.30). Für die Gruppe G heißt das, daß alle Gruppenelemente von G Nullstellen des Polynoms $X^{\mathrm{ex}(G)} - 1$ sind. Dieses Polynom hat höchstens $\mathrm{ex}(G)$ Nullstellen, d.h. $|G| \leq \mathrm{ex}(G)$. Da trivialerweise auch die umgekehrte Ungleichung besteht, gilt sogar Gleichheit. Folglich gibt es ein $g \in G$ mit $\mathrm{ord}(g) = |G|$, und dieses g erzeugt G. □

Folgerung 11.34 — *Ist K ein endlicher Körper, $|K| = p^\ell$, so ist $K^\times$ zyklisch von der Ordnung $p^\ell - 1$. Insbesondere gibt es ein Element $\theta \in K$ mit der Eigenschaft, daß $K = \mathbb{F}_p(\theta)$. Das Minimalpolynom von θ ist ein Teiler des Polynoms $x^{p^\ell - 1} - 1$ und zerfällt über K in paarweise verschiedene Linearfaktoren.*

Genauer ist θ eine Nullstelle des $(p^{\ell-1} - 1)$-ten Kreisteilungspolynoms $\Phi_{p^{\ell-1}-1}$ (cf. Abschnitt **§13**). Dieses Polynom ist irreduzibel über $\mathbb{Z}$, zerfällt aber im allgemeinen über $\mathbb{F}_p$.

Beispiel 11.35. — Wir betrachten die Erweiterung $\mathbb{F}_5 \subset \mathbb{F}_{25}$. Über $\mathbb{Z}$ hat man eine Faktorisierung $X^{24} - 1 = \prod_{n|24} \Phi_n$ mit irreduziblen Faktoren.

$$\begin{array}{llll} \Phi_1 = X - 1, & \Phi_2 = X + 1, & \Phi_4 = X^2 + 1, & \Phi_8 = X^4 + 1, \\ \Phi_3 = X^2 + X + 1, & \Phi_6 = X^2 - X + 1, & \Phi_{12} = X^4 - X^2 + 1, & \Phi_{24} = X^8 - X^4 + 1. \end{array}$$

Ein Element α in $\mathbb{F}_{25}^\times$ hat die Ordnung m genau dann, wenn α eine Nullstelle von Φ_m ist. Die Elemente der Ordnungen 1, 2 und 4 liegen schon in $\mathbb{F}_5^\times$. Die entsprechenden zyklotomischen Polynome zerfallen über $\mathbb{F}_5$ in Linearfaktoren:

$$\Phi_1 \equiv X + 4, \quad \Phi_2 \equiv X + 1, \quad \Phi_4 \equiv (X + 2)(X + 3).$$

Die übrigen zyklotomischen Polynome Φ_m, $m|24$, zerfallen über $\mathbb{F}_5$ in quadratische Polynome:

$$\begin{array}{ll} \Phi_3 \equiv X^2 + X + 1 & \Phi_8 \equiv (X^2 + 2)(X^2 + 3) \\ \Phi_6 \equiv X^2 + 4X + 1 & \Phi_{12} \equiv (X^2 + 2X + 4)(X^2 + 3X + 4) \end{array}$$

und

$$\begin{aligned} \Phi_{24} &\equiv X^8 + 4X^4 + 1 \\ &\equiv (X^4 + 2X^2 + 4)(X^4 + 3X^2 + 4) \\ &\equiv (X^2 + 3X + 3)(X^2 + 2X + 3)(X^2 + X + 2)(X^2 + 4X + 2) \mod 5. \end{aligned}$$

Die Nullstellen der Polynome Φ_3, Φ_6, Φ_{12} und Φ_{24} erzeugen alle den Körper $\mathbb{F}_{25}$ als Erweiterung von $\mathbb{F}_5$, aber nur die acht Nullstellen von Φ_{24} erzeugen $\mathbb{F}_{25}^\times$ als Gruppe.