Algebra I

Vorlesung Wintersemester 2004/05
Peter Müller

9. Februar 2005

Inhaltsverzeichnis

1 Einführung

Die Algebra hat ihre Wurzeln in der Geometrie und Zahlentheorie.

Klassische Beispiele

- Kann man mit Zirkel und Lineal beliebige Winkel dritteln, oder Würfel verdoppeln?
- Kann man die Nullstellen von Polynomen stets durch Wurzeln und die vier Grundrechenarten ausdrücken?
- Kann man für Funktionen wie e^{-x^2} explizite Stammfunktionen angeben?
- Wie findet man rationale oder ganzzahlige Lösungen von Systemen von Polynomen in mehreren Veränderlichen, z.B. (für festes $n \in \mathbb{N}$) $X^n + Y^n = Z^n$ mit $X, Y, Z \in \mathbb{Z}$ (Fermat-Problem)?

Moderne Beispiele

- Wie überträgt man digitale Daten, bei deren Übertragung Fehler auftreten können, durch Einbau von möglichst wenig Redundanz, aber mit möglichst guter Fehlererkennungs- und -korrekturmöglichkeit? Dies führt zur Kodierungstheorie.
- Wie überträgt man verschlüsselte Daten öffentlich, so dass nur der vorgesehene Empfänger sie entschlüsseln kann? Das geht sogar, ohne dass Sender und Empfänger vorher geheime Schlüssel austauschen müssen, selbst die dürfen öffentlich mitgeteilt werden (public key cryptography)! Dies führt zur Kryptographie.

In der Algebra haben sich wichtige Begriffe herauskristallisiert, nämlich Gruppen, Ringe, Moduln (der Spezialfall der Vektorräume ist aus der Linearen Algebra bekannt) und Körper. Diesen vier Begriffen ist die Vorlesung Algebra I gewidmet.

Die Algebra II wird mit der Galoistheorie, einer reizvollen Kombination aus Gruppen- und Körpertheorie, beginnen. Danach ...?

2 Gruppen

2.1 Definitionen, Beispiele

Definition 2.1. Eine Menge G mit einer zweistelligen Verknüpfung $G \times G \to G$, $(x, y) \mapsto x \cdot y$, heißt *Halbgruppe*, wenn das *Assoziativgesetz* gilt, d.h. $(x \cdot y) \cdot z = x \cdot (y \cdot z)$ für alle $x, y, z \in G$. Häufig schreibt man xy statt $x \cdot y$.

Beispiele von Halbgruppen

- $(\mathbb{N}, +)$, $(\mathbb{N}, \cdot)$, $(\mathbb{Z}, +)$, $(\mathbb{Z}, \cdot)$.
- $\mathrm{Abb}(X, X)$ = Menge der Abbildungen von X auf sich. Das Produkt $f \cdot g$ für $f, g \in \mathrm{Abb}(X, X)$ ist als die Komposition definiert, also $(f \cdot g)(x) = f(g(x))$ für $x \in X$. In der Gruppentheorie werden wir häufig x^f statt $f(x)$ schreiben.
- Sei G die Potenzmenge einer Menge. Dann sind $(G, \cap)$ und $(G, \cup)$ Halbgruppen.

Definition 2.2. Eine Halbgruppe heißt *abelsch* oder *kommutativ*, wenn $xy = yx$ für alle $x, y \in G$ gilt.

Definition 2.3. Die Halbgruppe G ist ein *Monoid*, wenn es ein *Einselement* e (oder auch *neutrales Element* genannt) gibt, d.h. es gilt $ex = xe = x$ für alle $x \in G$. Man schreibt dann $x^0 = e$.

Beispiel. Die Halbgruppe $(\mathbb{N}, +)$ ist kein Monoid, $(\mathbb{N}, \cdot)$ aber schon.

Wir kommen nun zum zentralen Begriff dieses Kapitels.

Definition 2.4. Ein Monoid G heißt *Gruppe*, wenn es für alle $x \in G$ ein $y \in G$ gibt mit $xy = yx = e$.

Bemerkung. In der Definition ist y eindeutig. Denn aus $y'x = xy' = e$ folgt $y' = y'e = y'(xy) = (y'x)y = ey = y$.

Man schreibt x^{-1} für y, und $x^{-n} := (x^{-1})^n$ für $n \in \mathbb{N}$. Mit diesen Festsetzungen gilt dann $x^m x^n = x^{m+n}$ und $(x^m)^n = x^{mn}$ für alle $m, n \in \mathbb{Z}$.

Einfache Folgerungen für eine Gruppe G

- Seien $a, b \in G$. Dann sind die Gleichungen $ax = b$ und $ya = b$ eindeutig durch $x = a^{-1}b$ und $y = ba^{-1}$ lösbar. Im allgemeinen gilt $x \neq y$, so dass eine Bruchschreibweise $\frac{b}{a}$ nur für abelsche Gruppen sinnvoll ist.

- Es gelten Kürzungsregeln: Aus $ax = ay$ (oder $xa = ya$) folgt $x = y$.

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

Beispiele von Gruppen

- $(V, +)$ mit Vektorraum V.

- $(K \setminus \{0\}, \cdot)$ mit Körper K.

- S_X = Teilmenge der Bijektionen aus $\mathrm{Abb}(X, X)$, wieder mit Komposition als Verknüpfung. Für $X = \{1, 2, \ldots, n\}$ schreibt man S_n statt S_X. Man nennt S_n die *symmetrische Gruppe* vom Grad n.

- $\mathrm{GL}_n(K) = \{A \in M_n(K) | \ \det A \neq 0\}$, K Körper.

- $\mathrm{SL}_n(\mathbb{Z}) = \{A \in M_n(\mathbb{Z}) | \ \det A = 1\}$.

Bemerkung. Häufig schreibt man 1 für das neutrale Element e. Ist die Gruppe abelsch, so verwendet man oft eine additive Notation, also $a + b$ und $-a$ statt $a \cdot b$ und a^{-1}. Natürlich verwendet man dennoch z.B. für multiplikative Gruppen von Körpern die multiplikative Notation.

2.2 Untergruppen und zyklische Gruppen

Definition 2.5. Eine nichtleere Teilmenge U einer Gruppe G heißt *Untergruppe* von G, wenn aus $a, b \in U$ schon $a \cdot b \in U$ und $a^{-1} \in U$ folgt. (In diesem Fall ist $(U, \cdot)$ eine Gruppe.) Man schreibt $U \leq G$.

Es folgt sehr einfach, dass Untergruppen von Untergruppen wieder Untergruppen sind. Auch Schnitte von Untergruppen sind wieder Untergruppen. (Was ist mit Vereinigungen?)

Beispiele

- $G = \mathbb{Z}$, $U = 2\mathbb{Z} = \{2m |\ m \in \mathbb{Z}\}$
- $G = S_5$, $U = \{g \in G |\ g(5) = 5\} = S_4$
- $G = \mathrm{GL}_n(K)$, $U = \mathrm{SL}_n(K)$

Definition 2.6. Sei $M \subseteq G$ eine Teilmenge der Gruppe G. Die von M *erzeugte Untergruppe* $<M>$ ist die kleinste M enthaltende Untergruppe von G.

Wichtige Beispiele von (Unter)gruppen sind solche, die von einem Element erzeugt werden.

Definition 2.7. Eine *zyklische Gruppe* ist eine von einem Element erzeugte Gruppe.

Beispiele zyklischer Gruppen

- $G = \mathbb{Z} = <1>$
- $G = \{e^{\frac{2\pi i k}{n}} |\ k = 0, 1, \ldots, n-1\} = <e^{\frac{2\pi i}{n}}>$ für $n \in \mathbb{N}$
- $G = \mathbb{Z}/n\mathbb{Z} = <1 + n\mathbb{Z}>$ für $n \in \mathbb{N}$

Definition 2.8. Ist G eine Gruppe, dann heißt $|G| \in \mathbb{N} \cup \{\infty\}$ die *Ordnung* von G.

Für $a \in G$ heißt $\mathrm{ord}(a) = |<a>| \in \mathbb{N} \cup \{\infty\}$ die *Ordnung* von a.

Lemma 2.9. *Ist* $\mathrm{ord}(a) = n \in \mathbb{N}$*, dann ist* n *die kleinste natürliche Zahl* m *mit* $a^m = e$*. Ferner gilt* $<a> = \{e = a^0, a^1, \ldots, a^{n-1}\}$*, und* $a^i = a^j$ *ist äquivalent zu* $i \equiv j \pmod{n}$*.*

Beweis. Zunächst müssen wir sehen, dass es überhaupt eine natürliche Zahl m gibt $a^m = e$. Das folgende Argument unter Verwendung des Schubfachprinzips wird uns in vielen Varianten noch öfters begegnen: Unter den $n+1$ Elementen $\{a^0, a^1, \ldots, a^n\}$ muss es zwei gleiche geben, da die Menge eine Teilmenge einer n-Elementigen Menge ist. Sei etwa $a^i = a^j$ mit $0 \leq i < j \leq n$. Dann gilt $j - i \in \mathbb{N}$ und $a^{j-i} = e$.

Sei nun $m \in \mathbb{N}$ minimal mit $a^m = e$. Dann gilt $<a> = \{a^0, a^1, \ldots, a^{m-1}\}$. Ferner gilt $a^i \neq a^j$ für $0 \leq i < j \leq m-1$, denn andernfalls folgte $a^{j-i} = e$, im Widerspruch zur Minimalität von m. Es folgt $m = n$ und der Rest der Behauptung. □

Definition 2.10. Ein Element der Ordnung 2 nennt man *Involution*.

Wir werden später sehen, dass die Struktur der Untergruppen selbst in endlichen Gruppen sehr kompliziert sein kann. Übersichtlich ist das hingegen in zyklischen Gruppen.

Satz 2.11. *Die Gruppe G sei zyklisch. Dann ist jede Untergruppe von G zyklisch. Hat G endliche Ordnung n, dann hat G für jeden Teiler r von n genau eine Untergruppe der Ordnung r. (Ferner ist die Ordnung jeder Untergruppe ein Teiler von n.)*

Beweis. Sei U eine Untergruppe von $G = <a>$. Wähle $s \in \mathbb{N}$ minimal mit $a^s \in U$. Wir behaupten $U = <a^s>$. Dazu sei $m \in \mathbb{Z}$ mit $a^m \in U$. Schreibe $m = us + v$ mit $0 \leq v \leq s-1$ (Division mit Rest). Wegen $(a^s)^u a^v = a^m \in U$ und $a^s \in U$ folgt $a^v \in U$, also $v = 0$ wegen der Minimalität von s. Aber $a^m = a^{us} \in <a^s>$. Hieraus folgt der erste Teil der Behauptung.

Sei nun $n \in \mathbb{N}$ die Ordnung von a. Wegen $a^n = e \in U$ folgt wie eben, dass s ein Teiler von n ist, also $n = rs$ mit $r \in \mathbb{N}$. Offenbar gilt $<a^s> = \{a^0, a^s, a^{2s}, \ldots, a^{(r-1)s}\}$, also $|U| = \mathrm{ord}(a^s) = r$. Umgekehrt ist für jeden Teiler r von n die Menge $<a^s> = \{a^0, a^s, a^{2s}, \ldots, a^{(r-1)s}\}$ mit $s = n/r$ eine Untergruppe der Ordnung r. □

2.3 Nebenklassen

Sei U eine Untergruppe der Gruppe G. Für $g \in G$ nennt man die Menge $Ug := \{ug |\ u \in U\}$ eine *Rechtsnebenklasse*. Analog ist gU eine *Linksnebenklasse*. Die Menge der Rechts- bzw. Linksnebenklassen bezeichnen wir mit $U\backslash G$ bzw. G/U.

In diesem Abschnitt verstehen wir unter Nebenklassen, wenn nichts anderes gesagt wird, Rechtsnebenklassen. Mit entsprechenden Modifikationen gelten die folgenden Aussagen auch für Linksnebenklassen.

Lemma 2.12. *Für zwei Nebenklassen Ug und Uh gilt entweder $Ug = Uh$, oder $Ug \cap Uh = \emptyset$.*

Beweis. Sei $x \in Ug \cap Uh$, also $x = u_1 g = u_2 h$ für $u_1, u_2 \in U$. Es folgt $g = u_3 h$ mit $u_3 = u_1^{-1} u_2 \in U$, also $Ug = Uu_3 h = Uh$. □

Da die Inversenabbildung $g \mapsto g^{-1}$ eine Bijektion von G ist, ist auch die Abbildung $Ug \mapsto (Ug)^{-1} = g^{-1}U^{-1} = g^{-1}U$ eine Bijektion zwischen $U\backslash G$ und G/U. Insbesondere gilt $|G/U| = |U\backslash G|$. Man nennt $[G : U] := |U\backslash G|$ den *Index* von U in G.

Definition 2.13. Aus obigem Lemma gewinnt man eine disjunkte Zerlegung $G = \biguplus_i Ug_i$ für geeignete $g_i \in G$, die *Nebenklassenzerlegung*. Die Menge der g_i nennt man *Rechtstransversale* oder *Vertretersystem* von $U\backslash G$.

Bemerkung. Eine Rechtstransversale ist im allgemeinen keine Linkstransversale. Dennoch kann man z.B. für endliche Gruppen G zeigen, dass es zu jeder Untergruppe U eine simultane Rechts- und Linkstransversale gibt.

Für alle $g \in G$ gilt $|Ug| = |U|$; zusammen mit der Nebenklassenzerlegung folgt der fundamentale Satz von Lagrange:

Satz 2.14 (Lagrange). *Sei U eine Untergruppe der Gruppe G. Dann gilt $|G| = [G : U]|U|$. Insbesondere ist (falls $|G| < \infty$) $|U|$ ein Teiler von $|G|$.*

Bemerkung. Die Umkehrung des Satzes von Lagrange gilt im allgemeinen nicht, es muss nicht für jeden Teiler r von $|G|$ eine Untergruppe der Ordnung r existieren. Ist hingegen r eine Primpotenz, so werden wir später sehen, dass es stets Untergruppen der Ordnung r gibt.

Der Satz von Lagrange hat einige bemerkenswerte Folgen:

Korollar 2.15. *Sei G eine endliche Gruppe. Für alle $g \in G$ ist* $\mathrm{ord}(g)$ *ein Teiler von $|G|$.*

Beweis. Klar, da $<g>$ eine Untergruppe der Ordnung $\mathrm{ord}(g)$ ist. □

Korollar 2.16 (Kleiner Satz von Fermat). *$a \in \mathbb{Z}$ sei nicht durch die Primzahl p teilbar. Dann ist $a^{p-1} - 1$ durch p teilbar.*

Beweis. Die Gruppe der invertierbaren Elemente im Monoid $(\mathbb{Z}/p\mathbb{Z}, \cdot)$ hat Ordnung $p - 1$. □

Korollar 2.17. *Gruppen von Primzahlordnung sind zyklisch.*

Beweis. Sei $e \neq g \in G$. Dann ist $\mathrm{ord}(g) > 1$ ein Teiler der Primzahl $|G|$, also $\mathrm{ord}(g) = |G|$ und daher $G = <g>$. □

2.4 Normalteiler und Faktorgruppen

Sind A und B Teilmengen einer Halbgruppe G, dann schreiben wir $AB := \{ab|\ a \in A, b \in B\}$.

Auf den Begriff des Normalteilers stößt man, wenn man versucht, auf dem Quotientenraum $U\backslash G$ auf sinnvolle Weise ein Produkt einzuführen. Es sollte $(Ug) \cdot (Uh) = Ugh$ für alle $g, h \in G$ gelten. Speziell für $h = 1$ folgt $gU \subseteq (Ug)U = Ug$, und daraus (durch Inversenbildung und Ersetzen von g durch g^{-1}) $gU = Ug$. Diese spezielle Eigenschaft von Untergruppen kennzeichnet Normalteiler.

Definition 2.18. Eine Untergruppe $N \leq G$ heißt *Normalteiler* von G, wenn $Ng = gN$ für alle $g \in G$ gilt. Man sagt auch, N ist *normal* in G, und schreibt $N \trianglelefteq G$.

Zur Überprüfung der Normalteilereigenschaft ist folgende Aussage oft nützlich.

Lemma 2.19. *Die Untergruppe N von G ist genau dann ein Normalteiler, wenn $g^{-1}Ng \subseteq N$ gilt für alle $g \in G$.*

Beweis. Aus $g^{-1}Ng \subseteq N$ folgt $Ng \subseteq gN$. Mit g^{-1} statt g gilt $Ng^{-1} \subseteq g^{-1}N$, also $gN = (Ng^{-1})^{-1} \subseteq (g^{-1}N)^{-1} = Ng$, und die eine Richtung der Behauptung folgt. Die andere Richtung ist sowieso klar. □

Beispiele

- Untergruppen abelscher Gruppen sind normal.
- Sei $U \leq G$ mit $[G : U] = 2$. Für $g \in G$ gilt entweder $g \in U$, und daher $Ug = U = gU$, oder $g \notin U$, und dann ist $Ug = gU$, da G die disjunkte Vereinigung von U und Ug bzw. von U und gU ist. Daher sind Untergruppen vom Index 2 stets Normalteiler.
- Es gilt $\mathrm{SL}_n(K) \trianglelefteq \mathrm{GL}_n(K)$. Dazu seien $A \in \mathrm{SL}_n(K)$ und $B \in \mathrm{GL}_n(K)$ beliebig. Wegen $\det(B^{-1}AB) = \det(B)^{-1}\det(A)\det(B) = 1$ gilt $B^{-1}AB \in \mathrm{SL}_n(K)$, und die Behauptung folgt aus Lemma 2.19.
- Die Untergruppe U der oberen Dreiecksmatrizen in $\mathrm{GL}_n(K)$ ist für $n \geq 2$ nicht normal in $\mathrm{GL}_n(K)$. Dazu sei D die Antidiagonalmatrix mit Einträgen 1. Dann besteht $D^{-1}UD$ aus den unteren Dreiecksmatrizen.

Der folgende Satz bildet aus einer Gruppe G und einem Normalteiler N eine kleinere Gruppe G/N. Dieses Prinzip ist wichtig, um über eine eventuell komplizierte Gruppe G Informationen aus den kleineren Gruppen N und G/N gewinnen zu können.

Satz 2.20. *Sei $N \trianglelefteq G$. Dann gilt $(Ng)(Nh) = Ngh$ für alle $g, h \in G$. Mit diesem Produkt wird G/N zu einer Gruppe, der* Faktorgruppe *von G modulo N.*

Beweis. Durch Verwendung von $Nx = xN$ und der Assoziativität folgt $NgNh = NNgh = Ngh$. Wir müssen zeigen, dass wir ein wohldefiniertes Produkt auf G/N bekommen. Dazu sei $Ng = Ng'$ und $Nh = Nh'$. Dies liefert $g' = ug$ und $h' = vh$ mit $u, v \in N$. Wegen $gvg^{-1} = w \in N$ und $uw \in N$ gilt $g'h' = ugvh = u(gvg^{-1})gh = uwgh$ und daher $Ng'h' = Ngh$.

Assoziativität des Produkt auf G/N ist klar, das neutrale Element ist N, und das inverse Element von Ng ist Ng^{-1}. □

Definition 2.21. Eine Gruppe $G > \{e\}$ heißt *einfach*, wenn sie außer G und $\{e\}$ keine Normalteiler hat.

Einfache Gruppen spielen eine ähnliche Rolle wie die Primzahlen für die natürlichen Zahlen. Nach dem Satz von Lagrange ist z.B. eine Gruppe von Primzahlordnung einfach. Weniger triviale Beispiele werden uns in den folgenden Abschnitten begegnen.

2.5 Symmetrische und alternierende Gruppen

Sei $n \in \mathbb{N}$ und S_n die Gruppe der Permutationen von $\{1, 2, \ldots, n\}$. Wir verwenden die Exponentialnotation a^ϕ für das Bild von a unter ϕ. Das hat den Vorteil der bequemen Notation wie z.B. $a^{\phi\psi} = (a^\phi)^\psi$ für $\phi, \psi \in S_n$. Man kann Permutationen $\phi \in S_n$ durch eine Wertetabelle $\phi = \begin{pmatrix} 1 & 2 & \cdots & n \\ 1^\phi & 2^\phi & \cdots & n^\phi \end{pmatrix}$ angeben. Transparenter, und für praktische wie auch theoretische Zwecke geeigneter, ist die Zykelnotation. Dabei heißt $\psi \in S_n$ ein *m-Zykel*, wenn es eine Folge $a_1, a_2, \ldots, a_m$ verschiedener Zahlen aus $\{1, 2, \ldots, n\}$ gibt mit $a_i^\phi = a_{i+1}$ für $1 \leq i \leq m-1$, $a_m^\phi = a_1$ und $a^\phi = a$ für alle $a \notin \{a_1, a_2, \ldots, a_m\}$. Die *Zykelnotation* für ψ ist $\psi = (a_1, a_2, \ldots, a_m)$, wobei man auch häufig $\psi = (a_1\, a_2\, \ldots\, a_m)$ schreibt. In den folgenden Beweisen erspart man sich Fallunterscheidungen, wenn man $a_{m+1} = a_1, a_{m+2} = a_2, \ldots$ setzt.

Ist $\phi \in S_n$ eine Permutation, so nennt man die Menge der von ϕ bewegten Elemente den Träger von ϕ; er besteht also aus den a mit $a^\phi \neq a$.

Jedes Element ϕ aus S_n ist ein Produkt von Zykeln ψ_i mit disjunkten Trägern. Diese Zykel kommutieren paarweise, also $\psi_i\psi_j = \psi_j\psi_i$ für alle i, j. Das Produkt diser Zykel in Zykelnotation ist die *Zykelnotation* für ϕ. Kommt in ϕ ein trivialer Zykel (a) vor, so lässt man den Faktor (a) häufig weg.

Beispiele

- $n = 3$, $\phi = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = (13)(2) = (13)$.
- $n = 5$, $\phi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 1 & 2 & 4 \end{pmatrix} = (13)(254)$, $\phi^{-1} = (13)(245)$, $\phi^2 = (1)(3)(245) = (245)$.
- $n = 5$, $\phi = (1234)$, $\psi = (23)(45)$, $\phi\psi = (1354)$.

Ein wichtiger Begriff der Gruppentheorie ist die *Konjugiertheit*, den wir hier am Beispiel der symmetrischen Gruppe näher kennenlernen wollen. Die Konjugiertheit ist eine Verallgemeinerung des Begriffs der Ähnlichkeit für die Gruppe der invertierbaren Matrizen $\mathrm{GL}_n(K)$.

Definition 2.22. Sei G eine Gruppe. Die Elemente $a, b \in G$ heißen *konjugiert*, wenn es ein $g \in G$ gibt mit $b = g^{-1}ag$. Statt $g^{-1}ag$ schreibt man auch a^g, was die eingängigen Beziehungen $a^{gh} = (a^g)^h$ und $(ab)^g = a^g b^g$ liefert.

Die Konjugiertheit schreibt sich in Zykelnotation sehr übersichtlich:

Satz 2.23. *Sei $\phi = (a_1\, a_2 \ldots)(b_1\, b_2 \ldots) \cdots \in S_n$ und $\psi \in S_n$. Dann gilt $\phi^\psi = (a_1^\psi\, a_2^\psi \ldots)(b_1^\psi\, b_2^\psi \ldots) \ldots$.*

Beweis. Wir müssen sehen, wohin z.B. das Element a_i^ψ von ϕ^ψ abgebildet wird. Wir rechnen

$$\begin{aligned}(a_i^\psi)^{\phi^\psi} &= (a_i^\psi)^{\psi^{-1}\phi\psi} \\ &= a_i^{\psi\psi^{-1}\phi\psi} \\ &= a_i^{\phi\psi} \\ &= (a_i^\phi)^\psi \\ &= a_{i+1}^\psi\end{aligned}$$

und die Behauptung folgt. □

Die Zykellängen von α sind die Längen der in der Zykelschreibweise von α auftretenden Zykel. Obiger Satz zeigt, dass sich die Zykellängen unter Konjugation nicht ändern. Es gilt auch die Umkehrung:

Satz 2.24. *Seien $\alpha, \beta \in S_n$ Permutationen mit den gleichen Zykellängen. Dann sind α und β in S_n konjugiert.*

Beweis. Seien $m_1, m_2, \ldots$ die Zykellängen. Schreibe

$$\begin{aligned}\alpha &= (a_{1,1}\, a_{1,2} \ldots a_{1,m_1})(a_{2,1}\, a_{2,2} \ldots a_{2,m_2}) \ldots \\ \beta &= (b_{1,1}\, b_{1,2} \ldots b_{1,m_1})(b_{2,1}\, b_{2,2} \ldots b_{2,m_2}) \ldots,\end{aligned}$$

wobei wir auch die Zykel der Längen 1 mit aufschreiben. Jedes Element aus $\{1, 2, \ldots, n\}$ kommt daher genau einmal sowohl unter den $a_{i,j}$, als auch

unter den $b_{i,j}$, vor. Sei $\psi \in S_n$ definiert durch $b_{i,j} = a_{i,j}^{\psi}$. Aus der folgenden Rechnung ergibt sich $\beta = \alpha^{\psi}$:

$$\begin{aligned} b_{i,j}^{\beta} &= b_{i,j+1} \\ &= a_{i,j+1}^{\psi} \\ &= a_{i,j}^{\alpha\psi} \\ &= a_{i,j}^{\psi\psi^{-1}\alpha\psi} \\ &= b_{i,j}^{\psi^{-1}\alpha\psi} \end{aligned}$$

□

Eine wichtige Klasse von Permutationen sind die 2-Zykel. Man nennt sie auch *Transpositionen*. Die folgende Aussage zeigt, dass die symmetrischen Gruppen von Transpositionen erzeugt werden.

Satz 2.25. *Jede Permutation $\phi \in S_n$ ist ein Produkt von Transpositionen, und jeder Zykel der Länge m ist ein Produkt von $m-1$ Transpositionen.*

Beweis. Da jede Permutation ein Produkt von Zykeln ist, genügt es, die Aussage für einen Zykel zu beweisen. Die Behauptung folgt induktiv wegen $(a_1\, a_2 \ldots a_m) = (a_2\, a_3 \ldots a_m)(a_1\, a_2)$. □

Sind $m_1, m_2, \ldots, m_r$ die Zykellängen eines Elements $\phi \in S_n$, so nennt man $\ell(\phi) := \sum_{i=1}^{r}(m_i - 1)$ die *Länge* von ϕ. Obiger Satz zeigt, dass sich ϕ als Produkt von $\ell(\phi)$ Transpositionen schreiben lässt.

Satz 2.26. *Für $\phi, \psi \in S_n$ gilt $\ell(\phi\psi) \equiv \ell(\phi) + \ell(\psi) \pmod 2$.*

Beweis. Schreibt man ϕ und ψ jeweils als Produkt von Transpositionen, so sieht man, dass die Behauptung aus folgender Aussage folgt: Sei $\alpha = \tau_1\tau_2 \ldots \tau_m$ ein Produkt von m Transpositionen. Dann gilt $\ell(\alpha) \equiv m \pmod 2$. Das beweisen wir durch Induktion über m. Die Behauptung ist trivial für $m = 1$. Wir nehmen nun an, dass sie richtig ist für m. Sei τ eine Transposition. Die Richtigkeit der Aussage für $m+1$ folgt, wenn wir zeigen, dass $\ell(\alpha\tau) = \ell(\alpha) + \delta$ gilt mit $\delta \in \{-1, 1\}$. Wir schreiben $\tau = (u\, v)$, und unterscheiden zwei Fälle:

(i) u und v sind in einem Zykel $\beta = (a_1\, a_2 \cdots a_r)$ von α enthalten, also etwa $a_i = u$ und $a_j = v$ mit $i < j$. Zur Bestimmung der Zykeldarstellung von $\alpha\tau$ muss man lediglich $\beta\tau$ bestimmen. Man erhält $\beta\tau = (a_1\, a_2 \cdots a_r)(a_i\, a_j) = (a_1\, a_2 \ldots a_{i-1}\, a_j\, a_{j+1} \ldots a_r)(a_i\, a_{i+1} \ldots a_{j-1})$, also $\ell(\beta\tau) = (r - j + i - 1) + (j - i - 1) = r = \ell(\beta) - 1$, und daher $\ell(\alpha\tau) = \ell(\alpha) - 1$

(ii) u und v liegen in verschiedenen Zykeln $(a_1 \dots a_r)$ und $(b_1 \dots b_s)$ von α, wobei wir $a_1 = u$ und $b_1 = v$ annehmen dürfen. Aus $(a_1 \dots a_r)(b_1 \dots b_s)(a_1\, b_1) = (a_1\, a_2 \dots a_r\, b_1\, b_2 \dots b_s)$ folgt $\ell(\alpha\tau) = \ell(\alpha) + 1$.

□

Definition 2.27. Permutationen ϕ mit $\ell(\phi) \equiv 0 \pmod 2$ heißen gerade, und solche mit $\ell(\phi) \equiv 1 \pmod 2$ heißen ungerade.

Satz 2.28. *Sei $1 < n \in \mathbb{N}$. Die Menge der geraden Permutationen aus S_n bildet eine Gruppe A_n mit $[S_n : A_n] = 2$. Man nennt A_n die* alternierende Gruppe *vom Grad n.*

Beweis. Aus obigem Satz folgt die multiplikative Abgeschlossenheit von A_n, somit ist A_n eine Untergruppe von S_n. Sei $\tau \in S_n$ eine Transposition, und $\phi \in S_n$, aber $\phi \notin A_n$. Da τ und ϕ ungerade Permutationen sind, ist nach dem obigen Satz $\phi\tau$ gerade, also $\phi\tau \in A_n$, und daher $\phi \in A_n\tau$. Somit ist $S_n = A_n \cup A_n\tau$ eine Nebenklassenzerlegung, und die Behauptung folgt. □

Unser Ziel ist es zu zeigen, dass die alternierenden Gruppen A_n für $n \geq 5$ einfach sind. Hierfür benötigen wir noch einige Vorbereitungen:

Satz 2.29. *Jede gerade Permutation ist ein Produkt von 3-Zykeln. Insbesondere wird A_n von den 3-Zykeln aus S_n erzeugt.*

Beweis. Da jede gerade Permutation das Produkt einer geraden Anzahl von Transpositionen ist, genügt es zu zeigen, dass das Produkt von zwei Transpositionen $\sigma = (a\, b)$ und $\tau = (c\, d)$ ein Produkt von 3-Zykeln ist. Wir unterscheiden zwei Fälle: (i) σ und τ bewegen einen gemeinsamen Punkt. Sei also etwa $a = c$ (und $b \neq d$, da es sonst nichts zu beweisen gibt). Dann gilt $\sigma\tau = (a\, b)(a\, d) = (a\, b\, d)$. (ii) σ und τ bewegen keinen gemeinsamen Punkt. In diesem Fall gilt $\sigma\tau = (a\, b)(c\, d) = (a\, b)(b\, c)(b\, c)(c\, d) = (a\, c\, b)(b\, d\, c)$. □

Lemma 2.30. *Sei $n \geq 5$. Dann sind alle 3-Zykel aus A_n konjugiert.*

Beweis. Seien α und β zwei 3-Zykel. Nach Satz 2.24 gibt es $\gamma \in S_n$ mit $\beta = \alpha^\gamma$. Liegt γ in A_n, dann sind wir fertig. Das sei also nicht der Fall. Wegen $n \geq 5$ gibt es eine Transposition τ, die zwei Fixpunkte von β vertauscht. Somit gilt $\beta = \alpha^\gamma = \alpha^{\gamma\tau}$, und die Behauptung folgt wegen $\gamma\tau \in A_n$. □

Satz 2.31. *Für $n \geq 5$ ist die Gruppe A_n einfach.*

Proof. Sei $N > 1$ ein Normalteiler von A_n. Unser Ziel ist es zu zeigen, dass N einen 3-Zykel ρ enthält. Für alle $\gamma \in A_n$ folgt dann nämlich $\rho^\gamma \in N^\gamma = N$,

und wegen obigem Lemma enthält N dann alle 3-Zykel aus A_n. Diese aber erzeugen nach Satz 2.29 die Gruppe A_n, und somit gilt $N = A_n$.

Es bleibt die Existenz eines 3-Zykels $\rho \in N$ zu zeigen. Dazu starten wir mit einem beliebigen Element $1 \neq \phi \in N$. Ist σ ein 3-Zykel, dann liegt das Produkt der 3-Zykel σ^{-1} und $\phi^{-1}\sigma\phi$ in N, da $\sigma^{-1}\phi^{-1}\sigma$ und ϕ in N liegen. Unser Ziel ist es, σ geschickt zu wählen, so dass ρ ein 3-Zykel wird. Das gelingt nicht immer in einem Schritt, aber da das Produkt von zwei 3-Zykeln höchstens 6 Elemente bewegt, hat ρ schon mal mindestens $n-6$ Fixpunkte.

Ist ϕ ein 3-Zykel, dann sind wir sowieso fertig. Da ϕ gerade ist, kann ϕ keine Transposition sein. Somit bleibt der Fall zu betrachten, dass ϕ mindestens 4 Punkte bewegt.

Hierzu unterscheiden wir drei Fälle:

(i) ϕ hat eine Zykellänge ≥ 4. Dann können wir $\phi := (a\,b\,c\,d\dots)\dots$ schreiben. Wir setzen $\sigma := (a\,b\,c)$. Wegen $\phi^{-1}\sigma\phi = (a^\phi\,b^\phi\,c^\phi) = (b\,c\,d)$ gilt $\rho = \sigma^{-1}\phi^{-1}\sigma\phi = (a\,c\,b)(b\,c\,d) = (a\,d\,b)$ ist $\rho \in N$ ein 3-Zykel.

(ii) ϕ enthält einen 3-Zykel $(a\,b\,c)$. Da ϕ kein 3-Zykel ist, wird mindestens ein weiteres Element d bewegt, also $\phi = (a\,b\,c)(d\,e\dots)\dots$. Wir setzen $\sigma = (a\,b\,d)$. Es folgt $\phi^{-1}\sigma\phi = (a\,b\,d)^\phi = (b\,c\,e)$ und $\rho = (a\,d\,b)(b\,c\,e) = (a\,d\,c\,e\,b)$. Somit sind wir im Fall (i), und können so wie dort einen 3-Zykel konstruieren.

(iii) ϕ hat nur Zykellängen 2. Dann gilt $\phi = (a\,b)(c\,d)\dots$, und wir setzen $\sigma = (a\,c\,e)$, wobei e von a, b, c, d verschieden ist. (Das geht wegen $n \geq 5$!) Es gilt $\phi^{-1}\sigma\phi = (a\,c\,e)^\phi = (b\,d\,f)$ mit $f = e^\phi$. Ist $e = f$, dann gilt $\rho = (a\,e\,c)(b\,d\,e) = (a\,b\,d\,e\,c)$, und wir fahren fort wie im Fall (i). Ist hingegen $e \neq f$, dann ist $\rho = (a\,e\,c)(b\,d\,f)$ das Produkt zweier disjunkter 3-Zykel, und wir fahren fort wie im Fall (ii).

Wie wir sehen, gelangen wir stets nach endlich vielen Schritten zu einem 3-Zykel aus N. Die Behauptung folgt. □

2.6 Homomorphismen

Strukturerhaltende Abbildungen spielen in der gesamten Mathematik eine wichtige Rolle. In der Algebra heißen sie meist Homomorphismen. Eine Abbildung $\Phi : X \to Y$ zwischen zwei Mengen schreiben wir entweder in der gewöhnlichen oder der Exponentialnotation, d.h. das Bild von x unter Φ ist $\Phi(x)$ oder x^Φ.

Definition 2.32. Eine Abbildung $\Phi : G \to H$ von der Gruppe G in die Gruppe H heißt ein *Homomorphismus*, wenn $(xy)^\Phi = x^\Phi y^\Phi$ gilt für alle $x, y \in G$.

Einfache Folgerungen Die folgenden Aussagen für einen Homomorphismus $\Phi : G \to H$ erhält man direkt aus den Definitionen

- Ein Homomorphismus bildet das neutrale Element auf das neutrale Element ab, das folgt aus der Kürzungsregel und $e^\Phi = (ee)^\Phi = e^\Phi e^\Phi$.
- Es gilt $(x^{-1})^\Phi = (x^\Phi)^{-1}$, man schreibt dafür auch manchmal $x^{-\Phi}$.
- Die Komposition von Homomorphismen ist ein Homomorphismus.
- Das Bild $U^\Phi = \{u^\Phi | \, u \in U\}$ einer Untergruppe $U \leq G$ ist eine Untergruppe von H.
- Das Urbild $V^{\Phi^{-1}}$ einer Untergruppe $V \leq H$ ist eine Untergruppe von G. Ist dabei V normal in H, dann ist $V^{\Phi^{-1}}$ normal in G. (Sind auch Bilder von Normalteilern normal?)
- Sind x, y in G konjugiert, so sind x^Φ, y^Φ in H konjugiert.
- Φ ist bereits durch seine Werte auf einem Erzeugendensystem von G festgelegt.

Homomorphismen $\Phi : G \to H$ mit speziellen Eigenschaften haben noch weitere Bezeichnungen:

Monomorphismus:	Φ ist injektiv
Epimorphismus:	Φ ist surjektiv
Isomorphismus:	Φ ist bijektiv
Endomorphismus:	$G = H$
Automorphismus:	$G = H$ und Φ ist bijektiv

Die Umkehrabbildung eines Isomorphismus Φ bezeichnet man mit Φ^{-1}. Aus $xy = (x^{\Phi^{-1}})^\Phi (y^{\Phi^{-1}})^\Phi = (x^{\Phi^{-1}} y^{\Phi^{-1}})^\Phi$, folgt, nach Anwenden von Φ^{-1}, dass auch Φ^{-1} ein Homomorphismus und damit ein Isomorphismus ist. Insbesondere ist die Menge der Automorphismen einer Gruppe G selber eine Gruppe, man bezeichnet sie mit $\mathrm{Aut}(G)$. Besteht zwischen den Gruppen G und H ein Isomophismus, dann nennt man G und H *isomorph*, und schreibt $G \cong H$.

Beispiele von Homomorphismen

- $G = (\mathbb{C}, +)$, $H = (\mathbb{C} \setminus \{0\}, \cdot)$, $x^\Phi := e^x$.
- $G = \mathrm{GL}_n(K)$, $H = (K \setminus \{0\}, \cdot)$, $x^\Phi := \det(x)$.
- $G = S_n$, $H = (\{-1, 1\}, \cdot)$, $x^\Phi := (-1)^{l(x)}$.

- $G = H$ abelsch, $n \in \mathbb{Z}$, $x^\Phi := x^n$.
- $N \trianglelefteq G$, $H = G/N$, $x^\Phi := Nx$.

Definition 2.33. Der *Kern* eines Homomorphismus $\Phi : G \to H$ ist die Menge der $g \in G$ mit $g^\Phi = e$, man schreibt auch Kern(Φ) für diese Menge. Als Urbild des Normalteilers $\{e\}$ von H ist Kern(Φ) ein Normalteiler von G. Mit Bild(Φ) bezeichnen wir das Bild G^Φ von G unter Φ.

Bemerkung. Man rechnet sofort nach, dass ein Homomorphismus Φ genau dann injektiv ist, wenn Kern(Φ) = $\{e\}$ gilt.

Analog zu einem Satz der linearen Algebra erhalten wir den folgenden wichtigen Homomorphiesatz:

Satz 2.34. *Sei $\Phi : G \to H$ ein Homomorphismus. Dann ist die Abbildung $\Psi : G/Kern(\Phi) \to Bild(\Phi)$, $Kern(\Phi)x \mapsto x^\Phi$ wohldefiniert, und liefert einen Isomorphismus $G/Kern(\Phi) \cong Bild(\Phi)$.*

Beweis. Die Wohldefiniertheit und Surjektivität folgen direkt aus der Definition. Setze $N :=$ Kern(Φ). Wegen $NxNy = Nxy$ gilt $(NxNy)^\Psi = (Nxy)^\Psi = (xy)^\Phi = x^\Phi y^\Phi = (Nx)^\Psi (Ny)^\Psi$. Somit ist Ψ ein Homomorphismus. Ferner ist Ψ injektiv, denn aus $e_H = (Nx)^\Psi = x^\Phi$ folgt $x = e_G$. (e_G und e_H bezeichnen die neutralen Elemente von G bzw. H.) □

Es war wohl schon früher klar, dass es "im Prinzip" nur die zyklischen $\mathbb{Z}$ und $\mathbb{Z}/n\mathbb{Z}$ gibt. Mit den jetzigen Begriffen können wir das präzise formulieren und beweisen:

Korollar 2.35. *Bis auf Isomorphie gibt es nur die folgenden zyklischen Gruppen: $(\mathbb{Z}, +)$ und $(\mathbb{Z}/n\mathbb{Z}, +)$ für ein $n \in \mathbb{N}$.*

Beweis. Sei g ein Erzeuger einer zyklischen Gruppe. Die Abbildung $\mathbb{Z} \to G$, $m \mapsto g^m$ ist ein Epimorphismus. Sei N der Kern. Dann gilt nach obigem Satz $G \cong \mathbb{Z}/N$. Ist $N = \{0\}$, dann gilt natürlich $\mathbb{Z}/N \cong \mathbb{Z}$. Sei nun $N \neq \{0\}$, und n die kleinste natürliche Zahl in N. Dann gilt $N = n\mathbb{Z}$, und die Behauptung folgt. □

Eine weitere wichtige Erkenntnis ist der Satz, dass jede Gruppe isomorph ist zu einer Untergruppe einer symmetrischen Gruppe.

Satz 2.36 (Cayley). *Jede Gruppe G ist isomorph zu einer Untergruppe von $Sym(G)$.*

Beweis. Für $g \in G$ sei g^Φ die Permutation der Elemente von G, welche $x \in G$ auf xg abbildet. Aus $x^{(gh)^\Phi} = xgh = (x^{g^\Phi})^{h^\Phi} = x^{g^\Phi h^\Phi}$ folgt, dass $\Phi : G \to \mathrm{Sym}(G)$ ein Homomorphismus ist. Der Kern von Φ besteht offenbar nur aus dem neutralen Element, somit ist G isomorph zu G^Φ. □

Wie in der Linearen Algebra folgen aus dem Homomorphiesatz einige Isomorphiesätze. Beachte, dass wenn N ein Normalteiler und U eine Untergruppe einer Gruppe G sind, dann ist UN eine Untergruppe von G.

Satz 2.37. *(a) Sei G eine Gruppe mit Untergruppe U und Normalteiler N. Dann gilt $U/U \cap N \cong UN/N$.*

(b) Seien G eine Gruppe mit Normalteilern $N \subseteq M$. Dann gilt $(G/N)/(M/N) \cong G/M$.

Beweis. (a) Sei Φ der natürliche Homomophismus $G \to G/N$. Das Bild von U besteht aus den Nebenklassen uN für $u \in U$, ist also UN/N. Der Kern der Einschränkung von Φ auf U ist $U \cap N$, die Behauptung folgt nun aus dem Homomorphiesatz.

(b) Die Abbildung $G/N \to G/M$, $gN \mapsto gM$ ist ein wohldefinierter Epimorphismus mit Kern M/N, die Behauptung folgt wiederum aus dem Homomorphiesatz. □

2.7 Gruppenoperationen

In diesem Abschnitt wollen wir Operationen von Gruppen auf Mengen betrachten. Einige grundlegende Aussagen werden später als Hilfsmittel zum Beweis interner Aussagen über endliche Gruppen dienen, die nichts mit Gruppenoperationen zu tun haben.

Definition 2.38. Eine *Operation* einer Gruppe G auf einer Menge M ist eine Abbildung $M \times G \to M$, $(m, g) \mapsto m^g$, für die $m^e = m$ und $(m^g)^h = m^{gh}$ gilt für alle $m \in M$, $g \in G$.

Bemerkung. G operiere auf M wie oben. Sei $\Phi : G \to \mathrm{Sym}(M)$ die Abbildung, die $g \in G$ auf die Permutation $M \to M$, $m \mapsto m^g$ abbildet. Dann ist Φ ein Homomorphismus. Umgekehrt liefert jeder Homomorphismus $G \to \mathrm{Sym}(G)$ eine Operation von G auf M.

Operiert die Gruppe G auf der Menge M, so erhält man auf natürliche Weise eine Äquivalenzrelation auf M: Zwei Elemente $m_1, m_2 \in M$ sind äquivalent genau dann, wenn es ein Element $g \in G$ gibt mit $m_2 = m_1^g$. (Man verifiziere die drei Eigenschaften Reflexivität, Symmetrie und Transitivität.)

Die Äquivalenzklassen nennt man *Bahnen*. Die Bahn durch m besteht offenbar aus den Elementen m^g, $g \in G$, und wird daher mit m^G bezeichnet.

Eine Operation von G auf M heißt *transitiv*, wenn M nur aus einer Bahn besteht. In diesem Fall wird M gelegentlich auch *homogener Raum* genannt.

Beispiele

- Sei U eine Untergruppe der Gruppe G. Dann operiert G auf dem Nebenklassenraum $U\backslash G$: Hierbei schickt g die Nebenklasse Ux auf die Nebenklasse Uxg. Diese Operation ist offensichtlich transitiv. Gleich werden wir sehen, dass jede transitive Operation auf einer Menge M, bis auf Umbenennung der Elemente von M, eine solche Operation auf einem Nebenklassenraum ist.

  Diese Operation liefert einen Homomorphismus $G \to \mathrm{Sym}(U\backslash G)$. Es ist natürlich interessant, den Kern N zu bestimmen. Dabei besteht N aus genau den Elementen $g \in G$, die jede Nebenklasse Ux festlassen, also $Uxg = Ux$ für alle $x \in G$ erfüllen. Aber $Uxg = Ux$ ist äquivalent zu $xgx^{-1} \in U$, und das ist äquivalent zu $g \in U^x$. Daher besteht N aus dem Schnitt der Konjugierten von U. Gilt $[G : U] = n < \infty$, dann ist nach dem Homomorphiesatz G/N isomorph zu einer Untergruppe der symmetrischen Gruppe auf n Elementen, insbesondere ist $[G : N]$ endlich und ein Teiler von $n!$.

- Die Gruppe G operiert auf sich selbst durch Konjugation. Dabei schickt g das Element x auf $g^{-1}xg = x^g$. Für $|G| > 1$ ist diese Operation nicht transitiv, da $\{e\}$ eine Bahn ist.

- Die lineare Gruppe $\mathrm{GL}_n(K)$ operiert auf dem Vektorraum K^n, aber sie operiert zum Beispiel auch auf der Menge der 1-dimensionalen Unterräume von K^n.

- Sei G die Gruppe der gleichsinnigen Symmetrien eines Würfels. Diese Gruppe hat Ordnung 24, denn eine Seitenfläche lässt sich auf 6 mögliche Flächen abbilden, und danach hat man noch 4 mögliche Drehungen dieser Fläche. Diese Gruppe hat verschiedene transitive Operationen auf Objekten, die zum Würfel gehören: G operiert transitiv auf den 8 Ecken, transitiv auf den 6 Flächen, transitiv auf den 12 Kanten, aber auch transitiv auf den 4 Raumdiagonalen.

Operiert G auf M, so nennt man $G_m := \{g \in G |\ m^g = m\}$ den *Stabilisator* von $m \in M$. Andere gebräuchliche Bezeichnungen sind *Punktstabilisator*, *Standgruppe* oder *Isotropiegruppe*. Man rechnet sofort nach, dass G_m eine Untergruppe von G ist.

Definition 2.39. Die Gruppe G operiere auf den Mengen M und N. Eine Abbildung $\phi : M \to N$ nennen wir *G-äquivariant*, wenn $(m^g)^\phi = (m^\phi)^g$ gilt für alle $m \in M$, $g \in G$.

Satz 2.40. *Die Gruppe G operiere transitiv auf der Menge M. Sei U der Stabilisator eines Elements $m \in M$. Dann wird durch $\phi : U\backslash G \to M$, $Ux \mapsto m^x$ eine G-äquivariante Bijektion definiert.*

Beweis. Zunächst müssen wir sehen, dass ϕ wohldefiniert ist. Dazu sei etwa $Ux = Uy$. Dann gilt $y = ux$ mit $u \in U$, und wegen $m^u = m$ folgt $m^x = m^{ux} = m^y$.

ϕ ist offenbar surjektiv. Ferner ist ϕ injektiv, denn aus $m^x = m^y$ folgt $m^{yx^{-1}} = m$, also $yx^{-1} \in U$ und dann $Ux = Uy$.

Die G-Äquivarianz folgt aus $((Ux)^\phi)^g = (m^x)^g = m^{xg} = (Uxg)^\phi = ((Ux)^g)^\phi$. □

Eine wichtige Konsequenz ist

Korollar 2.41. *Die Gruppe G operiere auf M. Die Länge der Bahn durch m berechnet sich durch $|m^G| = [G : G_m]$.*

Beweis. G operiert transitiv auf der Bahn m^G. Nach obigem Satz besteht eine Bijektion zwischen m^G und $\mathrm{St}_G(m)\backslash G$. □

Folgende einfache Aussage wird häufig ohne Kommentar verwendet:

Lemma 2.42. *G operiere auf M. Die Elemente $u, v \in M$ seien in einer gemeinsamen Bahn. Dann sind die Stabilisatoren G_u und G_v in G konjugiert. Genauer: Ist $v = u^g$, dann gilt $G_v = g^{-1}G_u g = G_u^g$.*

Beweis. Sei $v = u^g$. Dann ist $h \in G_v \iff v^h = v \iff u^{gh} = u^g \iff u^{ghg^{-1}} = u \iff ghg^{-1} \in G_u \iff h \in g^{-1}G_u g$. □

An einigen Beispielen wollen wir die Anwendbarkeit der neuen Resultate und Konzepte verdeutlichen. Vorher benötigen wir noch einige Begriffe.

Definition 2.43. Die Gruppe G operiere durch Konjugation auf sich selbst. Den Stabilisator eines Elements x unter dieser Operation nennt man den *Zentralisator* von x in G, und schreibt dafür $C_G(x)$. Die Menge $C_G(x)$ besteht also aus allen $g \in G$ mit $gx = xg$.

Die Bahn $x^G = \{g^{-1}xg |\ g \in G\}$ nennt man *Konjugationsklasse* von x in G.

Ist X eine Teilmenge von G, so nennt man $C_G(X) := \{g \in G |\ x^g = x \text{ für alle } x \in X\}$ den Zentralisator von X in G. Offenbar ist $C_G(X)$ der Schnitt der Zentralisatoren $C_G(x)$ für alle $x \in X$.

Ist speziell $X = G$, so nennt man $Z(G) := C_G(G)$ das *Zentrum* von G.

G operiert auch durch Konjugation auf der Menge der Teilmengen von G. Ist X eine Teilmenge, dann nennt man den Stabilisator von X den *Normalisator* von X in G, und schreibt dafür $N_G(X)$. Es gilt also $N_G(X) = \{g \in G |\ X^g = X\}$.

Da Stabilisatoren Untergruppen sind, folgt sofort, dass $N_G(X)$, $C_G(x)$, $C_G(X)$ und $Z(G)$ Untergruppen von G sind, was man aber auch direkt nachrechnen kann. Für $x \in X$ folgt aus der Definition sofort $Z(G) \leq C_G(X) \leq C_G(x)$ und $C_G(X) \leq N_G(X)$.

Satz 2.44 (Bahnengleichung). *Die Gruppe G operiere auf der endlichen Menge M. Seien $m_1, m_2, \ldots, m_r$ Repräsentanten der Bahnen. Dann gilt*

$$|M| = \sum_{i=1}^{r} [G : G_{m_i}].$$

Beweis. M ist die disjunkte Vereinigung der Bahnen durch die m_i, die Behauptung folgt dann aus Satz 2.41. □

Satz 2.45 (Klassengleichung). *Sind $x_1, x_2, \ldots, x_r$ die Repräsentanten der Konjugationsklassen der endlichen Gruppe G, dann gilt*

$$|G| = \sum_{i=1}^{r} [G : C_G(x_i)].$$

Beweis. Dies ist obiger Satz, angewandt auf die Operation von G auf sich durch Konjugation. □

Korollar 2.46. *Sei p eine Primzahl, $n \in \mathbb{N}$, und G eine Gruppe der Ordnung p^n. Dann gilt $|Z(G)| > 1$.*

Beweis. Seien $1 = x_1, x_2, \ldots, x_r$ die Repräsentanten der Konjugationsklassen von G. Dann gilt $p^n = \sum_{i=1}^{r} [G : C_G(x_i)]$. Nach dem Satz von Lagrange sind die Indizes $[G : C_G(x_i)]$ Potenzen von p. Die linke Seite der Klassengleichung ist durch p teilbar, aber $[G : C_G(x_1)] = 1$ ist es nicht. Daher muss es einen Index $i > 1$ geben, so dass auch $[G : C_G(x_i)]$ nicht durch p teilbar ist. Als Potenz von p muss dann $[G : C_G(x_i)] = 1$ gelten, also $G = C_G(x_i)$ und somit $1 \neq x_i \in Z(G)$. □

Die folgende Formel wird manchmal die Burnsidesche Bahnenformel genannt, obwohl sie schon früher bei Cauchy und Frobenius auftaucht.

Satz 2.47 (Cauchy-Frobenius Bahnenformel). *Die endliche Gruppe G operiere auf der endlichen Menge M. Für $g \in G$ sei $\chi(g)$ die Anzahl der Fixpunkte $m \in M$ mit $m^g = m$. Dann ist*

$$\frac{1}{G}\sum_{g\in G}\chi(g)$$

die Anzahl der Bahnen von G auf M.

Beweis. Es genügt die Aussage für transitive Operationen zu beweisen, da die Anzahl der Fixpunkte von g die Summe der Anzahlen der Fixpunkte auf den einzelnen Bahnen ist. Sei S die Menge der Paare $(m, g) \in M \times G$ mit $m^g = m$. Wir zählen S einmal über die Elemente g, und einmal über die Elemente m ab. Die erste Abzählung liefert $|S| = \sum_{g\in G}\chi(m)$, und die zweite Abzählung ergibt $|S| = \sum_{m\in M}|G_m|$. Wegen der Transitivität gilt $|M| = [G : G_m]$ für alle $m \in M$, also $|G_m| = |G|/|M|$, und die Behauptung folgt. □

Wir notieren zwei Folgerungen.

Korollar 2.48. *Die Gruppe G operiere transitiv auf der endlichen Menge M. Es gelte $|M| > 1$. Dann enthält G ein fixpunktfreies Element.*

Beweis. Wir dürfen G ersetzen mit seinem homomorphen Bild in $\mathrm{Sym}(M)$, insbesondere ist dann G endlich. Nach obigem Satz haben die Elemente von G durchschnittlich einen Fixpunkt. Aber e hat $|M| > 1$ Fixpunkte, daher muss es zum Ausgleich ein Element mit weniger als einem Fixpunkt geben. □

Korollar 2.49. *Die echte Untergruppe U von G habe endlichen Index. Dann ist G nicht die Vereinigung der Konjugierten von U.*

Beweis. Betrachte die Operation von G auf $U\backslash G$. Nach obigem Korollar hat G ein fixpunktfreies Element g. Das heißt $Uxg \neq Ux$ für alle $x \in G$, und somit $g \notin U^x$ für alle $x \in G$. □

Bemerkung. Diese Aussage wird falsch, wenn man die Voraussetzung des endlichen Index weglässt. In der Theorie der sogenannten algebraischen Gruppen spielen gerade gewisse Untergruppen (die Borelgruppen) eine wichtige Rolle, deren Konjugierte im zusammenhängenden Fall die Gruppe ausfüllen. Ein Spezialfall davon ist z.B. die bekannte Aussage aus der Linearen Algebra, dass sich jede Matrix aus $\mathrm{GL}_n(\mathbb{C})$ auf obere Dreiecksgestalt transformieren lässt.

2.8 Produkte

Sei I eine Indexmenge, und für alle $i \in I$ sei G_i eine Gruppe. Die Menge der Tupel $(g_i)_{i\in I}$ mit $g_i \in G_i$ wird mit der komponentenweise Multiplikation $(g_i)_{i\in I}(h_i)_{i\in I} := (g_i h_i)_{i\in I}$ zu einer Gruppe. Man nennt diese Gruppe das *direkte Produkt* der Gruppen G_i, und schreibt dafür $\prod_{i\in I} G_i$. Ist I die endliche Menge $\{1, 2, \ldots, n\}$, dann schreibt man dafür auch $G_1 \times G_2 \times \cdots \times G_n$, und stellt die Elemente durch n-Tupel $(g_1, g_2, \ldots, g_n)$ dar.

Das *eingeschränkte direkte Produkt* ist der Normalteiler bestehend aus all den Tupeln $g_i \in G_i$, in denen für alle bis auf endlich viele Indizes i das Element g_i das neutrale Element ist. Man nennt das manchmal auch *direkte Summe*. Gebräuchliche Schreibweisen sind $\bigoplus_{i\in I} G_i$ und $\coprod_{i\in I} G_i$. Ist die Indexmenge I endlich, dann stimmen natürlich direkte Summe und direktes Produkt überein.

Lemma 2.50. *Seien A und B Normalteiler der Gruppe G mit $A \cap B = \{e\}$ und $G = AB$. Dann gilt $G \cong A \times B$.*

Beweis. Sei $a \in A$, $b \in B$. Wegen $a^{-1}b^{-1}a \in B$ und $b \in B$ gilt $a^{-1}b^{-1}ab \in B$. Wegen $a^{-1} \in A$ und $b^{-1}ab \in A$ gilt aber auch $a^{-1}b^{-1}ab \in A$, also $a^{-1}b^{-1}ab \in A \cap B = \{e\}$ und somit $ab = ba$. Folglich ist die Abbildung $A \times B \to G$, $(a, b) \mapsto ab$ ein Homomorphismus. Gemäß Voraussetzung ist dieser Homomorphismus surjektiv. Er ist aber auch injektiv, denn aus $ab = e$ folgt $a, b \in A \cap B$, also $a = b = e$. □

Bemerkung. Das Produkt AB im Lemma nennt man auch das *interne direkte Produkt* der Normalteiler A und B. Im Gegensatz dazu bezeichnet man $A \times B$ manchmal als das *externe direkte Produkt* von A und B.

Eine Verallgemeinerung des obigen Lemmas auf mehrere Faktoren ist

Satz 2.51. *Sei I eine Indexmenge, und G_i, $i \in I$ seien Untergruppen einer Gruppe G. Auf I wähle man eine Totalordnung $<$. Die folgenden Aussagen sind äquivalent.*

(a) $G_i \trianglelefteq G$ für alle i, die G_i erzeugen G, und $G_i \cap \hat{G}_i = \{e\}$, wo $\hat{G}_i$ das Erzeugnis der Gruppen G_j mit $j \in I \setminus \{i\}$ ist.

(b) $G_i \trianglelefteq G$ für alle i, und für jedes $g \in G$ gibt es, bis auf Faktoren e, genau eine Darstellung $g = g_{i_1} g_{i_2} \ldots g_{i_n}$ mit $g_i \in G_i$ und $i_1 < i_2 < \ldots i_n$.

(c) Für alle $i \neq j$, $i, j \in I$ gilt $g_i g_j = g_j g_i$ für $g_i \in G_i$, $g_j \in G_j$, und für jedes $g \in G$ gibt es, bis auf Faktoren e, genau eine Darstellung $g = g_{i_1} g_{i_2} \ldots g_{i_n}$ mit $g_i \in G_i$ und $i_1 < i_2 < \ldots i_n$.

Gilt eine der Aussagen, dann ist G ist isomorph zur direkten Summe der G_i.

Beweis. Aus $G_i \trianglelefteq G$ folgt, wie im Beweis des obigen Lemmas, dass $a^{-1}b^{-1}ab \in G_i \cap G_j$ liegt für $a \in G_i$, $b \in G_j$.

"(a) $\Longrightarrow$ (b)": Für $i \neq j$ gilt $G_j \leq \hat{G}_i$, also $G_i \cap G_j = \{e\}$. Daher vertauschen die Elemente aus G_i mit denen aus G_j. Da die G_i ganz G erzeugen, hat jedes Element $g \in G$ eine Darstellung $g = g_{i_1} g_{i_2} \dots g_{i_n}$ mit $g_i \in G_i$ und $i_1 < i_2 < \dots i_n$. Sei eine weitere solche Darstellung für g gegeben. Durch Ergänzung der Indexmengen durch Einfügen der Faktoren e dürfen wir $g = h_{i_1} h_{i_2} \dots h_{i_n}$ mit $h_i \in G_i$ annehmen. Es folgt $h_{i_1}^{-1} g_{i_1} = h_{i_2} h_{i_3} \dots h_{i_n} g_{i_n}^{-1} \dots g_{i_3}^{-1} g_{i_2}^{-1} \in G_{i_1} \cap \hat{G}_{i_1}$ und daraus $g_{i_1} = h_{i_1}$. Fortsetzen des Verfahrens liefert nacheinander $g_{i_2} = h_{i_2}$, $\dots$, $g_{i_n} = h_{i_n}$. Die Eindeutigkeitsaussage folgt.

"(b) $\Longrightarrow$ (c)": Dies folgt aus dem Beginn des Beweises.

"(c) $\Longrightarrow$ (a)": Aus der Vertauschbarkeitsvoraussetzung folgt $G_i \trianglelefteq G$ für alle i. Wegen der eindeutigen Elementdarstellung aus den G_i folgt $G_i \cap \hat{G}_i = \{e\}$.

Es gelte nun (a), (b) und (c). Dann ist die natürliche Abbildung $\bigoplus_{i \in I} G_i \to G$, die durch multiplikative Fortsetzung der Einbettungsabbildungen $G_i \to G$ definiert ist, ein Epimorphismus. Sei $(g_{i_1}, g_{i_2}, \dots, g_{i_n})$ im Kern, also $g_{i_1} g_{i_2} \dots g_{i_n} = e$. Wegen der eindeutigen Darstellbarkeit von e folgt $g_{i_1} = g_{i_2} = \dots = g_{i_n} = e$, und die Abbildung ist somit auch injektiv. Die Behauptung folgt. □

Beispiele von Produkten

- Seien m und n teilerfremde natürliche Zahlen, und G eine zyklische Gruppe der Ordnung mn. Dann hat G Untergruppen A der Ordnung m und B der Ordnung n. Nach dem Satz von Lagrange gilt $A \cap B = \{e\}$. Nach obigem Satz gilt $AB \cong A \times B$. Die rechte Seite hat Ordnung mn, daher auch die linke Seite und es folgt $G = AB \cong A \times B$.

- Sei $\mathbb{C}^\star$ die multiplikative Gruppe der komplexen Zahlen, und S^1 die Untergruppe der komplexen Zahlen vom Betrag 1. Sei P die Gruppe der positiven reellen Zahlen. Dann gilt $\mathbb{C}^\star \cong S^1 \times P$.

- Sei V ein Vektorraum über einem Körper K, und $\{e_i | i \in I\}$ eine (eventuell unendliche) Basis. Dann ist $(V, +)$ die interne direkte Summe der Unterräume Ke_i, und isomorph zur externen direkten Summe $\bigoplus_{i \in I} K$.

In obigem Beispiel hatten wir ein etwas indirektes Argument zur Bestimmung der Ordnung von AB. Die Größe von Produkten AB lässt sich ganz allgemein bestimmen. Man beachte, dass AB im allgemeinen keine Gruppe sein muss.

Satz 2.52. *Seien A und B Untergruppen der endlichen Gruppe G. Dann gilt* $|AB| = \frac{|A||B|}{|A\cap B|}$.

Beweis. 1. Beweis: Sei $\{b_1, b_2, \ldots, b_n\}$ ein Vertretersystem der Rechtsnebenklassen $(A \cap B)\backslash B$. Dann sind die Nebenklassen Ab_i disjunkt, denn aus $Ab_i = Ab_j$ folgt $b_i b_j^{-1} \in A \cap B$, also $(A \cap B)b_i = (A \cap B)b_j$. Ferner hat jedes Element aus AB die Form ab_i mit $a \in A$: Dazu sei $a' \in A$, $b \in B$. Schreibe $b = a''b_i$ für geeignetes $a'' \in A \cap B$. Dann gilt $a'b = a'a''b_i$, und die Behauptung folgt mit $a = a'a''$.

2. Beweis: Betrachte die Operation von G auf $A\backslash G$. Die Bahn der Untergruppe B durch A besteht aus den Nebenklassen Ab, $b \in B$. Die Vereinigung dieser Nebenklassen ist AB, und jede Nebenklasse besteht aus $|A|$ Elementen. Daher hat die Bahn die Länge $|AB|/|A|$. Der Stabilisator in B von A ist $A \cap B$. Nach Korollar 2.41 wird die Bahnlänge durch $[B : A \cap B]$ gegeben, und die Behauptung folgt. □

Wir kommen nun zum wichtigen Begriff des *semidirekten Produkts*, einer Verallgemeinerung des direkten Produkts zweier Faktoren. Hierzu sei U eine Untergruppe der Gruppe G, und N ein Normalteiler von G, so dass $U \cap N = \{e\}$ und $G = UN$ gelten. In dieser Situation sagt man, G sei das *semidirekte Produkt* des Normalteilers N mit der Untergruppe H. Ferner nennt man H ein *Komplement* von N in G. Im folgenden konstruieren wir aus dieser Situation eine Verallgemeinerung des externen direkten Produkts. Dazu beobachten wir, dass jedes Element aus G eine eindeutige Darstellung der Form un mit $u \in U$, $n \in N$ hat. Das Ziel ist es, das Produkt zweier solcher Elemente u_1n_1 und u_2n_2 wieder in dieser Form darzustellen. Wir rechnen

$$u_1n_1u_2n_2 = u_1u_2u_2^{-1}n_1u_2n_2 = u_1u_2n_1^{u_2}n_2.$$

Man beachte, dass $u_1u_2 \in U$ und $n_1^{u_2}n_2 \in N$ gilt. Um also solche Produkte zu berechnen, muss man Produkte innerhalb U und N berechnen, und die Konjugationswirkung von H aud N kennen. Das führt direkt auf den Begriff des (externen) semidirekten Produkts.

Satz 2.53. *Seien N und U Gruppen, und $\phi : U \to \mathrm{Aut}(N)$ ein Homomorphismus. Auf der Menge G der Paare (u, n), $u \in U$, $n \in N$ definiere man ein Produkt durch $(u_1, n_1)(u_2, n_2) = (u_1u_2, n_1^{u_2^\phi}n_2)$. Mit diesem Produkt ist G eine Gruppe. G hat die zu U und N isomorphen Untergruppen $\tilde{U} = \{(u, e)|u \in U\}$ und $\tilde{N} = \{(e, n)|n \in N\}$. G ist ein semidirektes Produkt des Normalteilers $\tilde{N}$ mit $\tilde{U}$. Es gilt $(e, n)^{(u,e)} = (e, n^{u^\phi})$.*

Beweis. Die Aussagen ergeben sich alle durch direktes Nachrechnen. □

Bemerkung. Dir erste Teil des Satzes liefert eine wichtige Konstruktionsmethode für Gruppen. Gelegentlich schreibt man für G auch $U \ltimes_\phi N$. Ist ϕ der triviale Homomorphismus, dann ist $U \ltimes_\phi N$ einfach das direkte Produkt $U \times N$.

Beispiele semidirekter Gruppen

- Sei S_n die symmetrische Gruppe auf n Punkten, A_n die alternierende Gruppe, und C die von einer Transposition erzeugte Untergruppe von S_n. Dann gilt $S_n = C \ltimes A_n$, aber nicht $S_n = C \times A_n$.

- Sei C_n eine zyklische Gruppe der Ordnung, $C = <c>$ eine Gruppe der Ordnung 2, und $\phi : C \to \mathrm{Aut}(C_n)$ definiert durch $g^{c^\phi} := g^{-1}$. Die Gruppe $G := C \ltimes_\phi C_n$ ist die *Diedergruppe* D_n der Ordnung $2n$. Für $n \geq 3$ kann man sich diese Gruppe geometrisch veranschaulichen, sie besteht aus den Kongruenzabbildungen eines regulären n-Ecks. Die Gruppe C_n besteht dabei aus den gleichsinnigen Kongruenzen, und c ist eine Spiegelung.

- Es gilt $\mathrm{GL}_n(K) = U \ltimes \mathrm{SL}_n(K)$, wo U die Untergruppe der Diagonalmatrizen ist, die außer links oben nur 1er enthält.

2.9 Endliche abelsche Gruppen

Das Ziel dieses Abschnitts ist die Bestimmung der endlichen abelschen Gruppen. Wir beginnen mit einem einfachen

Lemma 2.54. *Seien a, b Elemente einer Gruppe mit teilerfremden Ordnungen. Ferner gelte $ab = ba$. Dann gilt* $\mathrm{ord}(ab) = \mathrm{ord}(a)\,\mathrm{ord}(b)$.

Beweis. Sei $r = \mathrm{ord}(a)$, $s = \mathrm{ord}(b)$. Es gilt $(ab)^{rs} = (a^r)^s(b^s)^r = e$, daher ist die Ordnung von ab höchstens rs. Sei nun $m \in \mathbb{N}$ mit $(ab)^m = e$. Dann gilt $a^m = (b^{-1})^m$. Nach dem Satz von Lagrange haben die beiden Gruppen $<a>$ und $<b>$ trivialen Schnitt. Es folgt $a^m = b^m = e$, und somit sind r und s Teiler von m. Es folgt $rs = m$. □

Lemma 2.55. *Sei G eine endliche abelsche Gruppe, und U eine zyklische Untergruppe maximaler Ordnung. Dann ist* $\mathrm{ord}(g)$ *ein Teiler von $|U|$ für alle $g \in G$.*

Beweis. Sei $g \in G$, p eine Primzahl, und p^r ein Teiler von $\mathrm{ord}(g)$. Wir werden zeigen, dass p^r ein Teiler von $|U|$ ist. Da das für alle p gilt folgt daraus die Behauptung.

Da p^r ein Teiler von ord(g) ist gibt es ein Element $a \in <g>$ der Ordnung p^r. Sei $|U| = p^e m$ mit ggT$(p, m) = 1$, und $b \in U$ mit Ordnung m. Nach obigem Lemma hat ab die Ordnung $p^r m$, wegen der Maximalität von $|U|$ folgt $p^r m \leq p^e m$, also $r \leq e$ und die Behauptung folgt. □

Als Vorbereitung des Hauptsatzes benötigen wir

Lemma 2.56. *Sei G eine endliche abelsche Gruppe, und U eine zyklische Untergruppe maximaler Ordnung. Dann hat U ein Komplement in G.*

Beweis. Wir beweisen die Aussage durch vollständige Induktion über $|G|$.

Ist $G = U$, dann gibt es nichts zu beweisen. Sei also $|U| < |G|$. Wir wählen $g \in G \setminus U$ von minimaler Ordnung. Sei u ein Erzeuger von U. Nach obigem Lemma besitzt U eine Untergruppe W der Ordnung ord(g). Sei w ein Erzeuger von W. Sei p ein Primteiler von ord(g). Dann gilt $g^p \in U$ (wegen der Minimalität von ord(g) mit $g \notin U$), aber $<g^p> = <w^p>$, da die Untergruppen der zyklischen Gruppe U schon durch ihre Ordnungen eindeutig bestimmt sind. Es gibt also $i \in \mathbb{N}$ mit $g^p = w^{pi}$, und daher $(gw^{-i})^p = e$. Aber $gw^{-i} \notin U$ ist somit ein Element der Ordnung p.

Somit ist $N := <g>w^{-i}$ eine Untergruppe mit $|N| > 1$ und $U \cap N = \{e\}$. Sei $\phi : G \to G/N$, $g \mapsto Ng$ der natürliche Epimorphismus. Für $x \in G$ folgt aus $x^n = e$ natürlich $(x^\phi)^n = e^\phi$, also ord$(x^\phi) \leq$ ord(x). Wegen $UN/N \cong U/(U \cap N) \cong U$ gilt $|U^\phi| = |U|$. Somit ist U^ϕ die größte zyklische Untergruppe von G^ϕ. Nach Induktionsannahme hat U^ϕ in G^ϕ ein Komplement. Sei $V \geq N$ das Urbild in G dieses Komplements in G. Dann gilt $UN \cap V \leq N$, also $U \cap V \leq U \cap N = \{e\}$. Ferner gilt $G^\phi = U^\phi V^\phi$, also $G = (UN)V = U(NV) = UV$, und die Behauptung folgt. □

Aus diesem Lemma folgt nun, wiederum durch Induktion über $|G|$, das Hauptergebnis dieses Abschnitts.

Satz 2.57. *Jede endliche abelsche Gruppe ist eine direkte Summe zyklischer Untergruppen.*

Im folgenden wollen wir noch die Eindeutigkeit solcher Zerlegungen in zyklische Gruppen klären. In einem früheren Beispiel sahen wir schon, dass jede endliche zyklische Gruppe eine direkte Summe zyklischer Gruppen von Primpotenzordnung ist. An obigem Satz sehen wir schon, dass es zu jedem Teiler m der Ordnung einer endlichen abelschen Gruppe auch eine Untergruppe der Ordnung m gibt. Diese Untergruppe muss nicht eindeutig sein, aber es gilt

Lemma 2.58. *Sei p eine Primzahl, und p^m die höchste Potenz von p, die die Ordnung einer endlichen abelschen Gruppe teilt. Dann gibt es genau eine Untergruppe der Ordnung p^m.*

Beweis. Seien A und B Untergruppen der Ordnung p^m. Wegen $|AB| = |A|[B : A \cap B]$ ist auch die Ordnung der Untergruppe AB eine Potenz von p, die aber p^m teilen muss. Daher gilt $B = A \cap B$, also $B \leq A$ und aus Symmetriegründen $A = B$. □

Hieraus folgt

Lemma 2.59. *Sei $n = \prod p_i^{e_i}$ die Primfaktorzerlegung der Ordnung einer endlichen abelschen Gruppe G, und G_{p_i} die Untergruppe der Ordnung $p_i^{e_i}$. Dann ist $G \cong \bigoplus G_{p_i}$.*

Um eine bis auf Isomorphie eindeutige Darstellung einer abelschen Gruppe zu bekommen müssen wir nur noch zyklische Gruppen von Primpotenzordnung betrachten. Wir wissen schon, dass solche Gruppen direkte Summen zyklischer Gruppen sind. Im folgenden erhalten wir auch eine Eindeutigkeitsaussage.

Lemma 2.60. *Sei G eine abelsche Gruppe von Primpotenzordnung, und $G = G_1G_2 \dots G_n \cong G_1 \times G_2 \times \dots \times G_n$ ein direktes Produkt zyklischer Untergruppen G_i der Ordnung > 1. Dann sind bis auf Reihenfolge die Ordnungen $|G_1|$, $|G_2|$, $\dots$, $|G_n|$ eindeutig gegeben.*

Beweis. Sei $|G|$ eine Potenz von p. Wir zeigen die Aussage durch vollständige Induktion über die Gruppenordnung. Sei $N = \{g \in G | \, g^p = 1\}$. Man sieht sofort, dass N eine Untergruppe ist. Ferner besteht N aus genau den Elementen $g_1g_2 \dots g_n$ mit $g_i \in G_i$, für die $g_i^p = 1$ gilt. Insbesondere ist N das direkte Produkt der Gruppen $N_i := G_i \cap N$, und da die Gruppen G_i zyklisch sind, gilt $|N_i| = p$ für alle i.

Der natürliche Epimorphismus $G \to \bigoplus G_i/N_i$, der $(g_1, \dots, g_n)$ auf $(N_1g_1, \dots, N_ng_n)$ abbildet, hat Kern N. Daher gilt $G/N \cong \bigoplus G_i/N_i$. Nach Induktionsannahme sind die Ordnungen $|G_i/N_i|$ eindeutig gegeben, und wegen $|G_i| = p|G_i/N_i|$ gilt das dann auch für die Ordnungen $|G_i|$. □

Wir fassen die Ergebnisse zusammen

Satz 2.61. *Eine endliche abelsche Gruppe ist isomorph zu einem direkten Produkt zyklischer Gruppen von Primpotenzordnung, und die Ordnungen dieser zyklischer Gruppen sind bis auf Reihenfolge eindeutig gegeben.*

Beispiele

- Um (bis auf Isomorphie) die abelschen Gruppen der Ordnung 8 zu bestimmen müssen wir alle Darstellungen $\bigoplus_{i=1}^{r} C_{m_i}$ betrachten, wo C_{m_i}

eine zyklische Gruppe der Ordnung m_i ist und $m_1 m_2 \dots m_r = 8$ gilt. Da es auf die Reihenfolge nicht ankommt, können wir ferner $m_1 \leq m_2 \leq m_r$ annehmen. Wir sehen, dass es für diese Tupel $(m_1, m_2, \dots, m_r)$ genau die Möglichkeiten $(2,2,2)$, $(2,4)$, und (8) gibt. Bis auf Isomorphie gibt es also genau 3 abelsche Gruppen der Ordnung 8.

- Ist n quadratfrei, dann ist die zyklische Gruppe der Ordnung n die einzige abelsche Gruppe dieser Ordnung. (Das ist auch schon ohne obigen Hauptsatz klar.)

Bemerkung. Der Beweis des Strukturs atzes für abelsche Gruppen (oder auch obiger Satz) liefert eine andere Form der Darstellung abelscher Gruppen: Jede endliche abelsche Gruppe ist isomorph zu einem direkten Produkt zyklischer Gruppen der Ordnungen n_1, n_2, …, n_k mit $n_i > 1$, so dass n_i ein Teiler von n_{i+1} ist für alle n_i. Diese n_i sind durch die Gruppe eindeutig gegeben.

2.10 Der Satz von Jordan-Hölder

Ist N ein Normalteiler der Gruppe G, so entsprechen die Normalteiler von G/N bijektiv den Normalteilern M von G mit $M \geq N$. Wir nennen N einen maximalen Normalteiler von G, wenn $N < G$ normal in G ist, und es keinen Normalteiler von G gibt, der echt zwischen N und G liegt. Somit ist N genau dann ein maximaler Normalteiler von G, wenn G/N einfach ist. Ist N ein maximaler Normalteiler von G, dann kann man in N wieder einen maximalen Normalteiler von N wählen, und das Verfahren fortsetzen. Dies führt auf den folgenden Begriff.

Definition 2.62. Sei G eine Gruppe, und $G = G_0 > G_1 > G_2 > \dots > G_n = \{e\}$ eine Kette von Untergruppen, so dass G_{i+1} ein maximaler Normalteiler von G_i ist. Eine solche Kette heißt *Kompositionsreihe*, und die einfachen Gruppen G_i/G_{i+1} heißen *Kompositionsfaktoren*.

Bemerkung. Ist G endlich, dann existiert trivialerweise eine Kompositionsreihe. Für unendliche Gruppen muss es das aber nicht geben. Man überlege sich, dass z.B. $(\mathbb{Z}, +)$ keine Kompositionsreihe besitzt.

Das Beispiel $C_6 > C_3 > \{e\}$ und $C_6 > C_2 > \{e\}$ zeigt schon, dass Kompositionsreihen und die Reihenfolge der Kompositionsfaktoren nicht eindeutig sein müssen. Die symmetrische Gruppe S_3 hat die Kompositionsreihe $S_3 > A_3 > \{e\}$, also die gleichen Kompositionsfaktoren wie C_6. Hieran sehen wir, dass die Kompositionsfaktoren den Isomorphietyp einer Gruppe nicht festlegen. Sie liefern aber dennoch wertvolle Informationen. Wenigstens

hängen aber die Kompositionsfaktoren einer Gruppe nicht wesentlich von der gewählten Kompositionsreihe ab, wie der folgende Satz zeigt.

Satz 2.63 (Jordan-Hölder). *Sei G eine endliche Gruppe. Dann haben alle Kompositionsreihen von G die gleiche Länge, und die Kompositionsfaktoren stimmen bis auf Reihenfolge und Isomorphie überein.*

Beweis. Wir zeigen die Behauptung durch vollständige Induktion über die Ordnung von G. Seien $G = G_0 > G_1 > G_2 > \cdots > G_m = \{e\}$ und $G = H_0 > H_1 > H_2 > \cdots > H_n = \{e\}$ Kompositionsreihen. Ist $G_1 = H_1$, so folgt die Behauptung durch Induktion.

Sei also von nun an $G_1 \neq H_1$. Dann ist G_1H_1 ein Normalteiler von G, der die maximalen und verschiedenen Normalteiler G_1 und H_1 enthält. Es folgt $G = G_1H_1$.

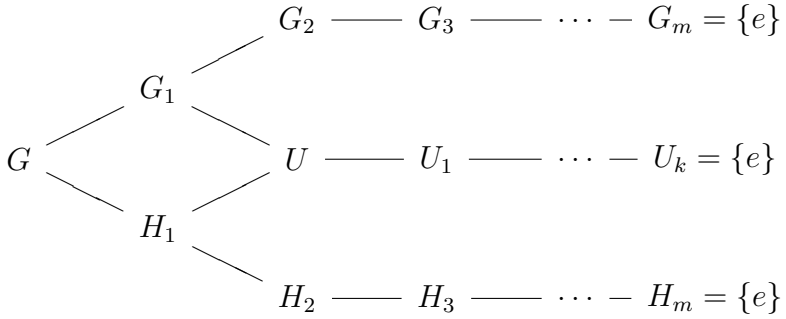
Setze $U = G_1 \cap H_1$, und $U > U_1 > U_2 > \cdots > U_k = \{e\}$ eine Kompositionsreihe von U.

Wegen

$$G_1/U = G_1/G_1 \cap H_1 \cong G_1H_1/H_1 = G/H_1$$

ist U ein maximaler Normalteiler von G_1, insbesondere ist $G_1 > U > U_1 > U_2 > \cdots > U_k = \{e\}$ eine Kompositionsreihe von G_1. Aber G_1 besitzt auch die Kompositionsreihe $G_1 > G_2 > \cdots > G_m = \{e\}$. Nach Induktionsannahme stimmen Länge und Kompositionsfaktoren dieser beiden Kompositionsreihen überein.

Analog gilt die Behauptung auch für die Kompositionsreihen $H_1 > U > U_1 > U_2 > \cdots > U_k = \{e\}$ und $H_1 > H_2 > \cdots > H_n = \{e\}$. Es folgt zunächst $m = n$. Oben sahen wir bereits $G/H_1 \cong G_1/U$, und analog $G/G_1 \cong H_1/U$, und daraus folgt schließlich die Behauptung, wobei zur besseren Orientierung folgendes Diagramm dient:



□

Beispiele von Kompositionsfaktoren

- Ist G eine abelsche Gruppe der Ordnung $\prod p_i^{e_i}$, dann bestehen die Kompositionsfaktoren aus den zyklischen Gruppen der Ordnung p_i, wobei die Gruppe der Ordnung p_i genau e_i Male auftritt.

- Für eine Primzahl p sei G eine Gruppe der Ordnung $p^m > 1$. Wir behaupten, dass alle Kompositionsfaktoren Ordnung p haben (und damit zyklisch sind). Dazu muss man lediglich sehen, dass eine einfache Gruppe mit p-Potenzordnung > 1 zyklisch der Ordnung p ist. Wegen Korollar 2.46 hat eine solche Gruppe ein nichtriviales Zentrum. Eine Untergruppe der Ordnung p des Zentrums ist aber ein Normalteiler der Gruppe, und die Behauptung folgt.

- Ist die Gruppe G ein direktes Produkt einfacher Gruppen G_1, G_2, ..., G_n, dann sind diese einfachen Gruppen gerade die Kompositionsfaktoren von G. (Man beweise diese Aussage!)

In der Theorie der Lösbarkeit von Polynomen spielt eine wichtige Eigenschaft gewisser Gruppen eine große Rolle.

Definition 2.64. Sei G eine Gruppe. Elemente der Form $a^{-1}b^{-1}ab$ für $a, b \in G$ heißen *Kommutatoren*. Die von den Kommutatoren erzeugte Gruppe G' heißt die *Kommutatorgruppe* von G. Die *höheren Kommutatorgruppen* $G^{(i)}$ werden rekursiv durch $G^{(0)} = G$, $G^{(i+1)} = (G^{(i)})'$ definiert. Die Gruppe G heißt *auflösbar*, wenn es ein $n \in \mathbb{N}$ gibt mit $G^{(n)} = \{e\}$.

Sind A und B Normalteiler einer Gruppe G, so dass G/A und G/B abelsch sind, dann ist $G/A \cap B$ abelsch, da diese Gruppe isomorph ist zu einer Untergruppe von $G/A \times G/B$. Daher gibt es genau einen kleinsten Normalteiler N von G, so dass G/N abelsch ist.

Die Kommutatorgruppe G' ist nicht nur normal in G, sondern hat eine stärkere Eigenschaft: Es gilt $(G')^\sigma = G'$ für jeden Automorphismus von G. Das liegt daran, dass ein Automorphismus die Menge der Kommutatoren permutiert, also das Erzeugnis der Kommutatoren nicht ändert. Induktiv folgt, dass auch die höheren Kommutatorgruppen unter Automorphismen σ invariant, also insbesondere auch normal in G sind.

Die wichtigste Eigenschaft der Kommutatorgruppe ist

Satz 2.65. *Sei G eine Gruppe. Dann ist G' der kleinste Normalteiler N von G, für den G/N abelsch ist.*

Beweis. Sei N der kleinste Normalteiler mit G/N abelsch. Sei $\phi : G \to G/N$ der natürliche Epimorphismus. Wegen $(a^{-1}b^{-1}ab)^\phi = a^{-\phi}b^{-\phi}a^\phi b^\phi = e$ ist $(G')^\phi$ die triviale Gruppe, also $G' \leq N$. Umgekehrt liegt jedes Element $a^{-1}b^{-1}ab$ in G', d.h. modulo G' ist G abelsch, und somit $N \leq G'$. Die Behauptung folgt. □

Lemma 2.66. *Sei N ein Normalteiler von G. Dann ist G genau dann auflösbar, wenn N und G/N auflösbar sind.*

Beweis. Ist $\phi : G \to H$ ein Epimorphismus, dann bestehen die Kommutatoren von H gerade aus den Bildern der Kommutatoren von G, und somit gilt $(G')^\phi = H'$. Per Induktion folgt daraus $(G^{(n)})^\phi = H^{(n)}$ für alle $n \in \mathbb{N}$. Speziell für den Epimorphismus $G \to G/N$ folgt daraus $G^{(n)}N/N = (G/N)^{(n)}$.

Ist nun G auflösbar, so sieht man, dass auch G/N auflösbar ist. Wegen $N^{(n)} \leq G^{(n)}$ ist dann auch N auflösbar.

Seien nun G/N und N auflösbar. Wegen der Auflösbarkeit von G/N folgt zunächst die Existenz von n mit $G^{(n)} \leq N$. Daraus folgt dann induktiv $G^{(n+k)} \leq N^{(n+k)}$ für $k \geq 0$. Aus der Auflösbarkeit von N ergibt sich dann die Behauptung. □

Bei endlichen Gruppen lässt sich die Auflösbarkeit an den Kompositionsfaktoren ablesen.

Satz 2.67. *Sei G eine endliche Gruppe. Dann ist G genau dann auflösbar, wenn alle Kompositionsfaktoren von G zyklisch (von Primzahlordnung) sind.*

Beweis. Ist G auflösbar, so sind die Quotienten aufeinanderfolgender Terme in der Kommutatorreihe abelsch. Insbesondere lässt sich die Kommutatorreihe durch Einfügen weiterer Untergruppen zu einer Kompositionsreihe mit zyklischen Quotienten verfeinern.

Die Umkehrung folgt unmittelbar per Induktion aus Lemma 2.66. □

Beispiele auflösbarer Gruppen

- Abelsche Gruppen sind auflösbar.
- Gruppen von Primpotenzordnung sind auflösbar.
- Homomorphe Bilder und direkte Produkte auflösbarer Gruppen sind auflösbar.

Bemerkung. Für $n \geq 5$ sind die Gruppen A_n und S_n wegen der Einfachheit von A_n nicht auflösbar. Man überlege sich, dass für alle $n \in \mathbb{N}$ stets $S_n' = A_n$ gilt.

2.11 Die Sätze von Sylow

Sei p eine Primzahl. Eine endliche Gruppe heißt *p-Gruppe*, wenn die Ordnung der Gruppe eine Potenz von p ist (evtl. auch 1). Wir kommen nun zu einer wichtigen Klasse von Untergruppen.

Definition 2.68. Sei G eine endliche Gruppe, und p eine Primzahl. Eine Untergruppe H von G heißt *p-Sylowgruppe* von G, wenn $|U|$ eine p-Gruppe ist, und $[G : U]$ nicht durch p teilbar ist.

Ist also p^r die höchste Potenz von p, die $|G|$ teilt, dann sind die p-Sylowgruppen gerade die Untergruppen der Ordnung p^r. Für abelsche Gruppen haben wir gesehen, dass es für jedes p genau eine p-Sylowgruppe gibt. Der wichtigste Satz in diesem Zusammenhang liefert die Existenz von Sylowgruppen auch für nicht abelsche Gruppen.

Satz 2.69 (Sylow). *Sei G eine endliche Gruppe, und p eine Primzahl. Dann besitzt G eine p-Sylowgruppe.*

Für diesen wichtigen Satz geben wir drei Beweise.

1. Beweis. Sei Z das Zentrum von G, und $g_1, g_2, \ldots, g_h$ Repräsentanten der Konjugationsklassen. Die Klassengleichung liefert

$$|G| = \sum_{i=1}^{h} [G : C_G(g_i)] = |Z| + \sum_{g_i \notin Z} [G : C_G(g_i)].$$

Man beachte, dass in der zweiten Summe die Gruppen $C_G(g_i)$ echte Untergruppen von G sind. Nach Induktion besitzen diese Gruppen p-Sylowgruppen. Ist einer der Indizes $[G : C_G(g_i)]$ teilerfremd zu p, dann ist eine p-Sylowgruppe von $C_G(g_i)$ auch eine von G. Wir sind also fertig, außer wenn alle Indizes durch p teilbar sind. In diesem Fall aber ist $|Z|$ durch p teilbar. Z besitzt also eine Untergruppe N der Ordnung p, diese ist normal in G. Nach Induktion besitzt G/N eine p-Sylowgruppe P/N, aber dann ist P eine p-Sylowgruppe von G. □

Für den zweiten Beweis benötigen wir ein kleines

Lemma 2.70. *Sei $n \in \mathbb{N}$, und p^r die höchste Potenz der Primzahl p, die n teilt. Dann ist der Binomialkoeffizient $\binom{n}{p^r}$ nicht durch p teilbar.*

Beweis. Schreibe $n = p^r m$. Somit ist m nicht durch p teilbar. $\binom{n}{p^r} = \binom{p^r m}{p^r}$ ist das Produkt der rationalen Zahlen $\frac{p^r m - k}{p^r - k}$ für $k = 0, 1, \ldots, p^r - 1$. Wir zeigen, dass in der gekürzten Darstellung Zähler und Nenner nicht durch p

teilbar sind. Das ist klar für $k = 0$. Sei daher $0 < k = p^l e$ mit e nicht durch p teilbar. Wegen $k < p^r$ gilt $l < r$, daher ist p^{r-l} durch p teilbar und die Behauptung folgt aus $\frac{p^r m - k}{p^r - k} = \frac{p^{r-l} m - e}{p^{r-l} - e}$. □

2. Beweis von Satz 2.69. Sei p^r wieder die höchste p-Potenz, die $|G|$ teilt. Sei M die Menge der p^r-elementigen Teilmengen von G. Die Mächtigkeit $|M| = \binom{|G|}{p^r}$ ist nach obigem Lemma nicht durch p teilbar. Wir lassen nun G von rechts auf M operieren, $g \in G$ schickt also die Teilmenge $S \in M$ nach Sg. Da $|M|$ nicht durch p teilbar ist, muss eine Bahn dabei sein, deren Länge nicht durch p teilbar ist. Sei $S \in M$ in dieser Bahn, und P der Stabilisator von S. Die Bahn durch S hat Länge $[G : P]$, und da das nicht durch p teilbar ist, ist $|P|$ durch p^r teilbar. Sei $s \in S$. Die Abbildung $P \to S$, $x \mapsto sx$ ist injektiv, daher gilt $|P| \leq |S| = p^r$, und somit $|P| = p^r$, und die Behauptung folgt. □

3. Beweis von Satz 2.69. Diesen Beweis zerlegen wir in eine Serie von Übungsaufgaben.

(a) Sei S eine endliche Gruppe mit p-Sylowgruppe P, und G eine Untergruppe von S. Dann gibt es ein $s \in S$, so dass $G \cap P^s$ eine p-Sylowgruppe von G ist. Hierzu betrachte man die Operation von G auf dem Nebenklassenraum $P \setminus S$.

Um den Satz zu beweisen, genügt es also, zu unserer gegebeben Gruppe G eine Gruppe S zu finden, die eine zu G isomorphe Untergruppe enthält, und für die es eine p-Sylowgruppe P gibt. Das wird in den folgenden Schritten erreicht.

(b) Die Gruppe G ist isomorph zu einer Untergruppe der symmetrischen Gruppe S_n. Sei $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ der Körper mit p Elementen. In $\mathrm{GL}_n(\mathbb{F}_p)$ betrachte man die Menge U der Matrizen, die in jeder Zeile und jeder Spalte genau eine 1, und sonst nur 0er besitzen. Zeige, dass U eine zu S_n isomorphe Untergruppe von $\mathrm{GL}_n(\mathbb{F}_p)$ ist. Somit hat $\mathrm{GL}_n(\mathbb{F}_p)$ eine zu G isomorphe Untergruppe.

(c) Zeige, dass die Gruppe der echten oberen Dreiecksmatrizen von $\mathrm{GL}_n(\mathbb{F}_p)$ eine p-Sylowgruppe ist durch direkte Berechnung der Ordnung dieser Gruppe und der höchsten p-Potenz, die die Ordnung von $\mathrm{GL}_n(\mathbb{F}_p)$ teilt.

□

Bevor wir zu weiteren Aussagen von Sylow kommen, wollen wir eine einfache Eigenschaft von p-Gruppen beweisen.

Lemma 2.71. *Sei U eine echte Untergruppe der p-Gruppe G. Dann gilt $N_G(U) > U$. Ferner hat G für jeden Teiler m der Gruppenordnung eine Untergruppe der Ordnung m, und Untergruppen vom Index p sind normal.*

Beweis. U operiere auf dem Nebenklassenraum $U \setminus G$. Da U eine p-Gruppe ist, hat jede Bahn eine Länge, die eine Potenz von p ist. Ferner ist die Summe $|U\backslash G|$ durch p teilbar. Da die Bahn durch U Länge 1 hat, muss es eine weitere Bahn $Ux \neq U$ der Länge 1 geben. Es gilt also $Uxu = Ux$ für alle $u \in U$, und daraus folgt $U^x = U$, d.h. x liegt nicht in U, normalisiert aber U.

Die letzte Aussage ist aus Ordnungsgründen klar, und die Existenz der Untergruppen der Ordnung m folgt induktiv aus der ersten Aussage, oder alternativ aus der bereits gesehenen Tatsache, dass die Kompositionsfaktoren von G alle Ordnung p haben. □

Das Hauptergebnis von Sylow, das wir im folgenden Abschnitt ständig verwenden werden, ist

Satz 2.72 (Sylow). *Sei G eine endliche Gruppe, und p eine Primzahl. Dann gilt:*

(a) Jede p-Untergruppe von G liegt in einer p-Sylowgruppe von G.

(b) Die p-Sylowgruppen von G sind konjugiert.

(c) Die Anzahl der p-Sylowgruppen ist von der Form $1 + kp$ mit $k \in \mathbb{N}_0$, und gleich $[G : N_G(P)]$, wobei P eine p-Sylowgruppe von G ist.

Beweis. Sei P eine p-Sylowgruppe von G, und S die Menge der zu P konjugierten Untergruppen von P. Natürlich ist jede Gruppe aus S wieder eine p-Sylowgruppe. G operiert auf S durch Konjugation. Wegen $|S| = [G : N_G(P)]$ ist die $|S|$ nicht durch p teilbar. Sei $U \leq G$ eine p-Gruppe. Auch U operiert durch Konjugation auf S. Da jede Bahnlänge von U eine p-Potenz ist, und $|S|$ nicht durch p teilbar ist, muss U eine Bahn $\{Q\}$ der Länge 1 haben. Dann gilt $uQ = Qu$ für alle $u \in U$, insbesondere ist QU eine Gruppe mit Normalteiler Q. Wegen $QU/Q \cong U/Q\cap U$ ist QU eine p-Gruppe der Ordnung $|Q|[U : Q \cap U]$. Aber Q ist schon eine p-Untergruppe von G größtmöglicher Ordnung, daher gilt $U = Q \cap U$, also $U \leq Q$. Hieraus folgt (a), und damit auch (b).

Um (c) zu zeigen, verwenden wir obiges Argument mit $U = P$. Ein Fixpunkt von P ist P selber. Weitere Fixpunkte Q kann es nicht geben, denn wie oben folgt $P \leq Q$, also $P = Q$ aus Ordnungsgründen. Alle anderen Bahnen von p haben also eine Länge der Form p^r mit $r \geq 1$, insbesondere sind diese Längen durch p teilbar. Daher hat $|S|$ die Form $1 + kp$.

Der Stabilisator von P in G ist $N_G(P)$, daher gilt $|S| = [G : N_G(P)]$, und alles ist gezeigt. □

2.12 Gruppen kleiner Ordnung

In diesem Abschnitt sollen examplarisch einige Anwendungen der Sylow-Sätze und der Techniken der Gruppenoperationen vorgestellt werden, die dem Studium von Gruppen dienen, die klein sind oder deren Ordnungen nur wenige Teiler besitzen.

Ist p eine Primzahl, dann sind die Gruppen der Ordnung p natürlich zyklisch. Eine Gruppe der Ordnung der Ordnung p^2 hat ein nicht triviales Zentrum, wird also vom Zentrum und einem weiteren Element erzeugt, und ist somit abelsch. Daher ist jede Gruppe der Ordnung p^2 isomorph zu C_{p^2} oder $C_p \times C_p$.

Wenn man in einer Gruppe G mit wenigen Teilern von $|G|$ nach Normalteilern sucht, dann ist häufig folgendes Vorgehen erfolgreich:

Man nimmt den größten Primteiler p von $|G|$, oder die Primzahl p mit der größten p-Sylowgruppe P. Nun versucht man mittels der Teilbarkeitseigenschaften aus den Sätzen von Sylow zu zeigen, dass P normal in G ist. Gelingt das nicht, sollte man andere Primzahlen probieren. Funktioniert auch das nicht, so kann man versuchen, die Nichtnormalität einer p-Sylowgruppe P dadurch zu einem Widerspruch zu führen, dass P zu viele Konjuguierte hat. Ich nämlich P nicht normal, dann hat P mindestens $1 + p$ Konjugierte. Hat beispielsweise P die Ordnung p, dann schneiden sich die Konjugierten trivial, man erhält also mindestens $(p-1)(p+1)$ Elemente der Ordnung p. Wenn man das auch noch für andere Sylowgruppen macht, kann es beispielsweise passieren, dass man durch solche Zählungen mehr Elemente bekommt als die Gruppenordnung ist.

Hilft auch das nicht weiter, kann man probieren, kleine Permutationsoperationen zu finden. Ist z.B. P nicht normal, dann erhält man einen nicht trivialen Homomorphismus $G \to \mathrm{Sym}(P \setminus G)$. Oft muss aus Anzahl- oder Teilbarkeitsgründen ein nicht-trivialer Kern vorhanden sein. Manchmal weiß man schon, dass $N_G(P) > P$ gilt, dann bekommt man meist bessere Aussagen, wenn man $G \to \mathrm{Sym}(N_G(P) \setminus G)$ betrachtet.

Natürlich muss man sich oft auch, abhängig von der Situation, andere Tricks einfallen lassen. Beispielsweise kann man aus der Klassengleichung oft nützliche Informationen gewinnen.

Die folgenden Beispiele sollen einige dieser Prinzipien verdeutlichen.

2.12.1 $|G| = pq$, $p < q$ Primzahlen.

Sei P und Q eine p-Sylow- bzw. q-Sylowgruppe von G, und n_p und n_q die Anzahl der p-Sylow- bzw. q-Sylowgruppen. Ist Q nicht normal in G, dann gilt $N_G(Q) = Q$, es folgt $n_q = [G : N_G(Q)] = [G : Q] = \frac{pq}{q} = p$. Anderseits

ist q ein Teiler von $n_q - 1 = p - 1$, also insbesondere $q < p$, im Widerspruch zu $p < q$.

Daher ist Q ein Normalteiler, und G ein semidirektes Produkt von Q mit P.

Ist P auch normal in G, dann ist G ein direktes Produkt von P und Q, also $G \cong C_p \times C_q \cong C_{pq}$.

Allerdings, wie das Beispiel S_3 schon zeigt, muss P nicht normal sein. In diesem Fall folgt analog wie oben, dass p ein Teiler von $q-1$ sein muss. Wenn also p kein Teiler von $q-1$ ist, dann ist $G \cong C_{pq}$.

Als nächstes wollen wir den Fall von 3 verschiedenen Primfaktoren studieren. Zur Einstimmung erst mal ein einfaches Beispiel.

2.12.2 $|G| = 1001 = 7 \cdot 11 \cdot 13$.

Seien n_7, n_{11} und n_{13} die Anzahlen der 7-, 11- und 13-Sylowgruppen. Nun ist n_{13} ein Teiler von $7 \cdot 11$, also gleich $1, 7, 11$ oder 77. Aber außer 1 hat keine dieser Zahlen die Form $1+13k$, es folgt $n_{13} = 1$. Analog ist n_7 gleich $1, 11, 13$ oder $11 \cdot 13 = 143$ und von der Form $1 + 7k$, also $n_7 = 1$, und genauso folgt $n_{11} = 1$. Damit sind alle Sylowgruppen normal, und G ist somit ein direktes Produkt dieser zyklischen Normalteiler mit teilerfremden Ordnungen. Daher ist G zyklisch.

2.12.3 $|G| = pqr$, $p < q < r$ Primzahlen.

Seien nun P, Q und R Untergruppen der Ordnungen p, q, und r. Natürlich sind P, Q und R Sylowgruppen. Für eine Primzahl s sei n_s wieder die Anzahl der s-Sylowgruppen.

Zunächst wollen wir sehen, dass eine der Gruppen P, Q oder R normal in G ist. Dazu nehmen wir an, das sei nicht der Fall. Wegen $R \leq N_G(R) < G$ gilt $n_r = p, q$ oder pq. Die ersten beiden Fälle treten aber nicht auf, da r ein Teiler von $n_r - 1$ ist, aber $r > p-1$ und $r > q-1$ nach Voraussetzung. Daher gilt $n_r = pq$. Ferner ist $1 < n_p$ ein Teiler von qr, also $n_p \geq q$, und analog $n_q \geq p$. Die Konjugierten der Gruppen P, Q und R schneiden sich paarweise trivial. Daher gibt es $n_r(r-1)$ Elemente der Ordnung r, $n_p(p-1)$ Elemente der Ordnung p und $n_q(q-1)$ Elemente der Ordnung q. Es folgt

$$pqr - 1 \geq n_r(r-1) + n_p(p-1) + n_q(q-1) \geq pq(r-1) + q(p-1) + p(q-1),$$

also $(p-1)(q-1) \leq 0$, was Unsinn ist. Damit ist eine der Gruppen P, Q oder R normal in G.

Wir wollen sehen, dass R normal in G ist. Nach obigem ist P oder Q normal in G, sei z.B. P normal in G. Nach Beispiel 2.12.1 ist dann PR/P

normal in G/P, also PR normal in G. Aber wiederum nach Beispiel 2.12.1 ist R normal in PR. Somit ist R die einzige r-Sylowgruppe in PR, und daher muss R in G normal sein.

Damit ist R als Normalteiler erkannt. Nach Beispiel 2.12.1 ist QR/R normal in G/R, und somit ist QR normal in G. Es folgt

$$G \cong P \ltimes (Q \ltimes R).$$

Führt man diese etwas technischen Betrachtungen noch weiter, so sieht man, dass stets $G \cong C_p \ltimes C_{qr}$ oder $G \cong C_{pq} \ltimes C_r$ gilt.

2.12.4 $|G| = p^a q^b$, $p < q$ Primzahlen, $0 \leq a, b \leq 2$.

Sei wieder P und Q eine p- und q-Sylowgruppe. Ist Q normal in G, dann ist G ein semidirektes Produkt von Q mit P. Wir wollen den Fall analysieren, dass Q nicht normal ist. Mit den gewohnten Bezeichnungen folgt, dass $1 < n_q$ ein Teiler von p^2 ist, und q ein Teiler von $n_q - 1$ ist. Wegen $q > p$ kann nicht $n_q = p$ gelten, daher gilt $n_q = p^2$, und q ist ein Teiler von $p^2 - 1 = (p-1)(p+1)$. Daher ist $p-1$ oder $p+1$ durch q teilbar. Wegen $q > p$ folgt $q = p+1$, also $p = 2$, $q = 3$.

Somit gilt $n_3 = 4$ und $|G| = 12$ oder $|G| = 36$. Wegen $n_3 = 2^2$ gilt $N_G(Q) = Q$. Betrachte die Operation durch Konjugation auf den vier 3-Sylowgruppen. Wir erhalten $G \to S_4$, und der Kern ist der Schnitt der 3-Sylowgruppen. Im Fall $|G| = 12$ ist dieser Schnitt trivial, es folgt $G \leq S_4$. Aber A_4 ist die einzige Untergruppe der Ordnung 12 in S_4, und es folgt $G \cong A_4$. Insbesondere ist P normal in G.

Im zweiten Fall ist der Kern von $G \to S_4$ eine Gruppe Z der Ordnung 3, wie eben folgt $G/Z \cong A_4$. Somit ist PZ/Z normal in G/Z, also PZ normal in G der Ordnung 12. Es folgt schnell, dass P normal in G ist.

Bemerkung. Für beliebige natürliche Zahlen a, b gilt der Satz von Burnside, dass eine Gruppe der Ordnung $p^a q^b$ auflösbar ist. Auch bis heute ist der einfachste Beweis mittels Darstellungstheorie. Hierbei untersucht man die möglichen Homomorphismen $G \to \mathrm{GL}_n(\mathbb{C})$.

2.12.5 Auflösbarkeit von G für $|G| < 60$.

Wir haben bereits die Gruppe A_5 der Ordnung 60 kennengelernt, die einfach aber nicht abelsch ist. Hier wollen wir sehen, dass es keine kleinere einfache und nicht abelsche Gruppen gibt. Insbesondere sind dann alle Gruppen der Ordnung < 60 auflösbar.

Sei G einfach und nicht abelsch mit $|G| < 60$. Wegen der bisherigen Fälle bleiben nur noch die Gruppenordnungen $2 \cdot 3^3$, $2^3 \cdot 3$, $2^3 \cdot 5$, $2^3 \cdot 7$ und $2^4 \cdot 3$

zu untersuchen. G kann keine echte Untergruppe U vom Index ≤ 4 besitzen, denn dann bettet G ein in $\mathrm{Sym}(U \setminus G) \leq S_4$, aber S_4 ist auflösbar. Damit bleiben nur noch die Ordnungen $2^3 \cdot 5$ und $2^3 \cdot 7$. Im ersten Fall folgt aus den Sylowsätzen sofort, dass die 5-Sylowgruppe normal ist, ein Widerspruch. Bleibt $|G| = 8 \cdot 7$. Es folgt $n_7 = 8$, daher hat G genau $8(7-1) = 48$ Elemente der Ordnung 7. Die Menge der restlichen 8 Elemente ist unter Konjugation invariant. Aber auch die 2-Sylowgruppe von G hat Ordnung 8, und stimmt daher mit dieser Menge überein. Sie ist also normal.

3 Ringe und Moduln

3.1 Definitionen, Beispiele

Ein *Ring* ist eine Menge R mit zwei zweistelligen Verknüpfungen $+$ und $\cdot$ und Elementen $0, 1 \in R$, so dass die folgenden Ringaxiome gelten:

- $(R, +)$ ist eine (additiv geschriebene) abelsche Gruppe mit neutralem Element 0.
- $(R, \cdot)$ ist ein Monoid mit neutralem Element 1.
- Es gelten die beiden Distributivgesetze $x \cdot (y + z) = x \cdot y + x \cdot z$ und $(y + z) \cdot x = y \cdot x + z \cdot x$ für alle $x, y, z \in R$.

Um Klammern zu sparen gelten die üblichen Konventionen, dass Potenzbildung vor Multiplikation, und diese vor Addition geht. Bei Produkten schreibt man oft xy statt $x \cdot y$.

Zur Gewöhnung an die Axiome beginnen wir mit einigen einfachen Aussagen:

Lemma 3.1. *In einem Ring R gelten die folgenden Aussagen:*

(a) $0a = a0 = 0$.

(b) $(-a)b = -ab = a(-b)$.

(c) $a(b - c) = ab - ac$, $(a - b)c = ac - bc$.

(d) Gilt $0 = 1$, *so folgt* $R = \{0\}$.

(e) Gilt $ab = ba$, *so folgt* $(a + b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}$ *für* $n \in \mathbb{N}$.

Beweis. Aus $0 = 0+0$ folgt $a0 = a(0+0) = a0+a0$, also $a0 = 0$, und analog $0a = 0$. Ähnlich einfach folgen die Aussagen (b) und (c). Aussage (d) folgt aus (a) und $a = a \cdot 1 = a \cdot 0 = 0$. Der Beweis von (e) ist wie in der Analysis mittels vollständiger Induktion, bei der Rechnung bemerkt man, dass man neben den Ringaxiomen noch die multiplikative Vertauschbarkeit von a und b benötigt. □

Soweit im folgenden nichts anderes gesagt wird, sei stillschweigend $0 \neq 1$ vorausgesetzt.

Beispiele von Ringen

- Die ganzen Zahlen $\mathbb{Z}$ bilden einen Ring.
- Ist $n \in \mathbb{N}$, so bildet die Menge der Restklassen $\mathbb{Z}/n\mathbb{Z}$ mit den Festsetzungen $(a + n\mathbb{Z}) + (b + n\mathbb{Z}) = (a + b) + n\mathbb{Z}$ und $(a + n\mathbb{Z}) \cdot (b + n\mathbb{Z}) = (ab) + n\mathbb{Z}$ einen Ring mit n Elementen.
- Ist K ein Körper, so bildet die Menge der Matrizen $M_n(K)$ einen Ring.
- Für eine abelsche Gruppe A ist die Menge der Endomophismen von A ein Ring, wobei $f + g$ durch $a^{f+g} := a^f + a^g$ und $a^{f \cdot g} := a^{fg} = (a^f)^g$ erklärt werden. (Was passiert, wenn A nicht abelsch ist?)
- Ist M eine Menge, und R ein Ring, so bildet die Menge der Abbildungen von M nach R unter elementweiser Addition und Multiplikation ein Ring.

Nach diesen Beispielen wollen wie einige nachfolgend häufig benutzte Begriffe definieren.

Definition 3.2. Ein Element $a \in R$ heißt *invertierbar* oder *Einheit*, wenn es $b, c \in R$ gibt mit $ab = ca = 1$. (Dann folgt automatisch $c = c1 = cab = 1b = b$.) Die Menge $R^\times$ der Einheiten bilden eine Gruppe, die *Einheitengruppe* von R.

Ein Element $a \in R$ heißt *Nullteiler*, wenn es ein $b \neq 0$ gibt mit $ab = 0$.

Ein Element $a \in R$ heißt *nilpotent*, wenn es ein $n \in \mathbb{N}$ gibt mit $a^n = 0$.

Ein Ring R heißt *kommutativ*, wenn $ab = ba$ gilt für alle $a, b \in R$.

Der Ring R ($\neq \{0\}$) heißt *Integritätsbereich* oder *Integritätsring*, wenn R nullteilerfrei und kommutativ ist.

Sind alle Elemente $\neq 0$ eines Ringes ($\neq \{0\}$) Einheiten, so heißt der Ring ein *Schiefkörper*.

Kommutative Schiefkörper heißen *Körper*.

Typische Integritätsbereiche sind etwa die ganzen Zahlen $\mathbb{Z}$. Die Einheitengruppe von $\mathbb{Z}$ besteht allerdings nur aus ± 1. Natürlich ist auch jeder Körper ein Integritätsbereich. Als einfache Anwendung der Begriffe zeigen wir

Lemma 3.3. *Ein endlicher Integritätsbereich ist ein Körper.*

Beweis. Sei R ein endlicher Integritätsbereich, und $a \neq 0$. Wir müssen zeigen, dass a invertierbar ist. Dazu betrachten wir die Abbildung $R \to R$, $x \mapsto ax$. Diese Abbildung ist injektiv, denn aus $ax = ay$ folgt $a(x - y) = 0$, also $x - y = 0$, da 0 der einzige Nullteiler von R ist. Da aber R endlich ist, folgt aus der Injektivität dieser Abbildung schon die Surjektivität. Insbesondere gibt es $x \in R$ mit $ax = 1$. Analog folgt die Existenz von y mit $ya = 1$, die Behauptung folgt. □

Eine wichtige Folgerung ist

Korollar 3.4. *Sei $n \in \mathbb{N}$. Dann ist $\mathbb{Z}/n\mathbb{Z}$ genau dann ein Körper, wenn n eine Primzahl ist.*

Beweis. Sei $R = \mathbb{Z}/n\mathbb{Z}$. Im Falle $n = 1$ gilt $R = \{0\}$. Sei nun $n = ab$ mit $a, b \in \mathbb{N}$ und $a, b > 1$. Dann gilt $(a + n\mathbb{Z})(b + n\mathbb{Z}) = n\mathbb{Z} = 0_R$, aber $a + n\mathbb{Z}, b + n\mathbb{Z} \neq 0_R$. Damit ist R kein Körper.

Nun sei n eine Primzahl. Nach obigem Lemma bleibt zu zeigen, dass R ein Integritätsbereich ist, d.h, dass R keine Nullteiler außer 0_R hat. Seien $a + n\mathbb{Z}, b + n\mathbb{Z} \neq 0_R$ mit $(a + n\mathbb{Z})(b + n\mathbb{Z}) = ab + n\mathbb{Z} = 0_R$. Damit ist n ein Teiler von ab, und da n prim ist, gilt z.B., dass n ein Teiler von a ist. Aber dann gilt $a + n\mathbb{Z} = 0_R$, ein Widerspruch. □

Ein *Teilring* eines Ringes R ist eine Teilmenge S von R mit $0, 1 \in S$, so dass S mit den von R auf S eingeschränkten Operationen wieder einen Ring bildet. Hierzu genügt es zu zeigen, dass mit $s, t \in S$ auch $s - t$ und st wieder in S liegen. Ist M eine Teilmenge von R, und R_0 ein Teilring von R, dann bezeichnet $R_0[M]$ den von R_0 und M erzeugten Teilring von R. Das ist der kleinste Teilring von R, der R_0 und M enthält.

3.2 Homomorphismen und Ideale

Definition 3.5. Eine Abbildung $\phi : R \to S$ zwischen Ringen R und S heißt *Ringhomomorphismus*, wenn $1_R^\phi = 1_S$ gilt, und $(x + y)^\phi = x^\phi + y^\phi$ und $(xy)^\phi = x^\phi y^\phi$ gelten für alle $x, y \in R$.

Ähnlich einfach wie bei Gruppen rechnet man nach, dass R^ϕ ein Teilring von S ist, und dass Urbilder von Teilringen von S wieder Teilringe von R sind. Die Kerne von Gruppenhomomorphismen waren gerade die Normalteiler von Gruppen. Der Kern eines Ringhomomorphismus $R \to S$ ist natürlich eine Untergruppe von $(R, +)$, aber es gilt eine weitere Eigenschaft.

Definition 3.6. Eine Untergruppe I von $(R, +)$ heißt *Ideal* von R, wenn für alle $r \in R$, $i \in I$ gilt: $ri, ir \in I$. Man schreibt dann auch $I \trianglelefteq R$.

Sei I der Kern eines Ringhomomorphismus $\phi : R \to S$. Wie schon bemerkt, ist I eine Untergruppe von $(R, +)$. Sei $r \in R$, $i \in I$. Wegen $(ri)^\phi = r^\phi i^\phi = r^\phi 0 = 0$ gilt $ri \in I$, und analog $ir \in I$. Damit ist I ein Ideal. In Kürze werden wir sehen, dass umgekehrt jedes Ideal der Kern eines geeigneten Homomorphismus ist.

Man beachte, dass Ideale im allgemeinen keine Teilringe sind. Gilt nämlich $1 \in R$, so folgt bereits $I = R$.

Ist M eine Teilmenge von R, so bildet die Menge der endlichen Summen $\sum r_i m_i s_i$ mit $r_i, s_i \in R$, $m_i \in M$ offenbar das kleinste Ideal von R, welches M enthält. Man nennt das auch das von M erzeugte Ideal. Ein *Hauptideal* ist ein von einem einzigen Element erzeugtes Ideal. Ist R kommutativ, dann hat das von m erzeugte Hauptideal die Form mR. Man schreibt dafür auch häufig (m). Ist jedes Ideal eines Ringes ein Haupideal, dann nennt man den Ring *Hauptidealring*.

Wir wissen bereits, dass die Untergruppen von $(\mathbb{Z}, +)$ alle die Form $n\mathbb{Z}$ mit $n \in \mathbb{N}_0$ haben. Insbesondere haben alle Ideale von $\mathbb{Z}$ diese Form, somit ist $\mathbb{Z}$ ein Hauptidealring.

Sei nun I ein Ideal des Rings R. Da $(I, +)$ eine normale Untergruppe von $(R, +)$ ist, erhalten wir eine natürliche Abbildung $\phi : R \to R/I$ via $x \mapsto x+I$. Wir wollen sehen, dass durch $(x + I)(y + I) := xy + I$ ein wohldefiniertes Produkt auf R/I gegeben wird. Dazu sei $x = x' + i$, $y = y' + j$ mit $i, j \in I$. Wir müssen sehen, dass $xy + I = x'y' + I$ gilt. Das gilt aber wegen

$$xy - x'y' = (x' + i)(y' + j) - x'y' = x'j + iy' + ij \in I.$$

Damit ist R/I offenbar ein Ring mit Nullelement I und Einselement $1 + I$, da sich die Ringaxiome direkt von R auf R/I übertragen. Wir erhalten

Satz 3.7. *Sei I ein Ideal des Rings R. Dann ist $R \to R/I$, $x \mapsto x + I$ ein Epimorphismus von Ringen mit Kern I.*

Das zeigt, dass jedes Ideal der Kern eines Ringhomomorphismus ist. Fast wörtlich genauso wie in der Gruppentheorie (oder linearen Algebra) beweist man nun

Satz 3.8 (Homomorphiesatz). *Sei $\phi : R \to S$ ein Homomorphismus von Ringen mit Kern I. Dann gilt $R/I \cong$ Bild(ϕ).*

Auch die Isomorphiesätze der Gruppentheorie haben ein Analogon in der Ringtheorie.

Satz 3.9 (Isomorphiesätze). *(a) Sei R ein Ring mit Teilring S und Ideal I. Dann gilt $S/S \cap I \cong S + I/I$.*

(b) Seien I und J Ideale des Rings R mit $J \subseteq I$. Dann ist I/J ein Ideal von R/J, und es gilt $R/I \cong (R/J)/(I/J)$.

3.3 Chinesischer Restsatz

Es seien I und J Ideale eines Rings R. Offenbar sind auch $I + J$ und $I \cap J$ Ideale von R. Die multiplikative Struktur von R erlaubt es uns, aus I und J ein weiteres Ideal zu konstruieren. Mit IJ bezeichnen wir die Menge der endlichen Summen mit Summanden der Form ij mit $i \in I$, $j \in J$. Offenbar ist IJ ein Ideal von R. Man beachte, dass nicht jedes Element aus IJ die Form ij haben muss. Es gilt $IJ \subseteq I \cap J$.

Um die nächsten Begriffe zu motivieren, beweisen wir zunächst

Lemma 3.10. *Es seien $m, n \in \mathbb{Z}$, und nicht beide gleich 0. Ferner sei $d \in \mathbb{N}$ der größte gemeinsame Teiler von m und n. Dann gilt $(m) + (n) = (d)$.*

Beweis. Da $\mathbb{Z}$ ein Haupidealring ist, und $(m) + (n)$ nicht das Nullideal ist, gibt es $d \in \mathbb{N}$ mit $(m) + (n) = (d)$. Daher gibt es $a, b \in \mathbb{Z}$ mit $d = am + bn$. Wegen $(m) \subseteq (d)$ ist d ein Teiler von m, und analog ist d ein Teiler von n. Aber die Darstellung $d = am + bn$ zeigt, dass jeder gemeinsame Teiler von m und n auch ein Teiler von d ist, und die Behauptung folgt. □

Wir sehen also, dass insbesondere m und n genau dann teilerfremd sind, wenn $(m) + (n) = \mathbb{Z}$ gilt. Das motiviert (hoffentlich) die folgende

Definition 3.11. Die Ideale I und J des Rings R heißen *teilerfremd*, wenn $R = I + J$ gilt.

Sind $R_1, R_2, \ldots, R_n$ Ringe, dann ist das direkte Produkt $R_1 \times R_2 \times \cdots \times R_n$ mit den komponentenweisen Operationen wieder ein Ring. Im folgenden wollen wir in gewissen Situationen komplizierte Ringe als direkte Produkte einfacherer Ringe schreiben.

Zuvor benötigen wir noch ein

Lemma 3.12. *Es sei I ein Ideal des Rings R, das teilerfremd ist zu den Idealen J und K. Dann gilt*

(a) $IJ + JI = I \cap J$.

(b) I *ist teilerfremd zu* JK *und* $J \cap K$.

Beweis. Wegen $IJ, JI \subseteq I \cap J$ folgt $IJ + JI \subseteq I \cap J$. Sei nun umgekehrt $x \in I \cap J$. Wegen $I + J = R$ gibt es $i \in I$, $j \in J$ mit $1 = i + j$. Es folgt

$$x = (i + j)x = ix + jx \in IJ + JI,$$

und damit (a). Sei nun weiter $1 = i' + k$ mit $i' \in I$, $k \in K$. Wir erhalten

$$1 = (i + j)(i' + k) = ii' + ik + ji' + jk \in I + jk \subseteq I + JK,$$

und die Behauptung folgt. □

Induktiv folgt aus (b)

Lemma 3.13. *Das Ideal* I_1 *des Rings* R *sei teilerfremd zu den Idealen* $I_2, \ldots, I_n$. *Dann ist* I_1 *teilerfremd zu* $I_2 \cap \cdots \cap I_n$.

Das Hauptergebnis dieses Abschnitts ist

Satz 3.14 (Chinesischer Restsatz). *Seien* $I_1, I_2, \ldots, I_n$ *paarweise teilerfremde Ideale eines Rings* R. *Sei* I *der Schnitt der Ideale* I_i. *Dann ist die Abbildung*

$$\begin{aligned} R/I &\to R/I_1 \times R/I_2 \times \cdots \times R/I_n \\ r + I &\mapsto (r + I_1, r + I_2, \ldots, r + I_n) \end{aligned}$$

ein Isomorphismus von Ringen.

Beweis. Offenbar ist I der Kern der Abbildung $R \to R/I_1 \times R/I_2 \times \cdots \times R/I_n$, $r \mapsto (r + I_1, r + I_2, \ldots, r + I_n)$, die Behauptung folgt also aus dem Homomorphiesatz, sobald wir die Surjektivität der Abbildung nachgewiesen haben. Für $n = 1$ ist nichts zu zeigen.

Sei nun $n = 2$. Wegen $R = I_1 + I_2$ gibt es $i_1 \in I_1$, $i_2 \in I_2$ mit $1 = i_1 + i_2$. Seien $x, y \in R$ beliebig, und setze $r = xi_2 + yi_1$. Es gilt $r = x(1 - i_1) + yi_1 = x + (y - x)i_1 \in x + I_1$ und $r = xi_2 + y(1 - i_2) \in y + I_2$. Das Element r wird also auf $(x + I_1, y + I_2)$ abgebildet. Da x und y beliebig waren, folgt die Behauptung für $n = 2$.

Für $n \geq 3$ benutzen wir vollständige Induktion, wobei wir für den Induktionsschritt den Fall $n = 2$ benutzen: Nach Lemma 3.13 ist I_1 teilerfremd zum Schnitt I_1' der I_i mit $2 \leq i \leq n$. Beachte, dass $I = I_1 \cap I_1'$ gilt. Wegen des Falls $n = 2$ ist $R/I_1 \to R/I_1 \times R/I_1'$ ein Isomorphismus, und $R/I_1' \to R/I_2 \times \cdots \times R/I_n$ ist ein Isomorphismus nach der Induktionsannahme für $n - 1$. Die Behauptung folgt. □

Die häufigste Anwendung des chinesischen Restsatzes ist für kommutative Ringe R. In diesem Fall lässt sich der Schnitt paarweiser teilerfremder Ideale noch anders ausdrücken:

Lemma 3.15. *Seien $I_1, I_2, \ldots, I_n$ paarweise teilerfremde Ideale eines kommutativen Rings. Dann gilt $I_1 I_2 \ldots I_n = I_1 \cap I_2 \cap \cdots \cap I_n$.*

Beweis. Für $n = 2$ folgt das aus Lemma 3.12(a), und allgemein per Induktion. □

Eine wichtiger Spezialfall des chinesischen Restsatz ist

Satz 3.16. *Sei $n = \prod p_i^{e_i}$ die natürliche Primfaktorzerlegung von $n \in \mathbb{N}$. Dann ist der Ring $\mathbb{Z}/n\mathbb{Z}$ isomorph zum direkten Produkt der Ringe $\mathbb{Z}/p_i^{e_i}\mathbb{Z}$.*

3.4 Anwendungen der Kongruenzrechnung

Ein klassisches und wichtiges Gebiet der Mathematik ist die Frage der ganzzahligen Lösbarkeit z.B. polynomialer Gleichungen oder Gleichungssysteme. Hier sind Restklassenbetrachtungen häufig von großem Nutzen. Wir betrachten exemplarisch einige Beispiele:

- $4x - 1 = y^2 + z^2$ hat keine ganzzahligen Lösungen. Dazu sei $\mathbb{Z} \to \mathbb{Z}/4\mathbb{Z}$ der natürliche Homomorphismus, und $\bar{a}$ sei das Bild von $a \in \mathbb{Z}$. Ist x, y, z eine Lösung der gegebenen Gleichung, dann gilt auch $\bar{3} = -\bar{1} = \overline{4x - 1} = \bar{y}^2 + \bar{z}^2$. Für $a \in \mathbb{Z}$ gilt aber $\bar{a}^2 = \bar{0}$ oder $\bar{1}$, also $\bar{3} = u + v$ mit $u, v \in \{\bar{0}, \bar{1}\}$, ein Widerspruch.

- Die natürliche Zahl n enthalte in der Dezimaldarstellung nur die Ziffern 6 und 0. Kann n eine Quadratzahl sein? Wir nehmen an, n ist eine Quadratzahl. Dann endet n auf eine gerade Anzahl von 0ern. Streicht man diese, dann erhält man eine Quadratzahl, die mit 6 endet, also modulo 4 den Rest 2 hat, was aber nicht geht, da die Reste der Quadrate modulo 4 nur 0 und 1 sind.

- $15x^2 - 7y^2 = 9$ ist in $\mathbb{Z}$ nicht lösbar: Sei x, y, z eine Lösung. Man sieht, dass $7y^2$ durch 3 teilbar ist. Dann ist y durch 3 teilbar, also $7y^2$ durch 9 teilbar. Somit ist $15x^2$ durch 9 teilbar, also x durch 3 teilbar. Wir setzen also $x = 3a$, $y = 3b$ mit $a, b \in \mathbb{Z}$. Es folgt $15a^2 - 7b^2 = 1$. Eine Betrachtung modulo 4 bringt hier keinen Widerspruch, sie liefert $\bar{b}^2 - \bar{a}^2 = bar1$ in $\mathbb{Z}/4\mathbb{Z}$, aber das ist natürlich lösbar. In $\mathbb{Z}/3\mathbb{Z}$ hingegen erhalten wir $-\bar{b}^2 = \bar{1}$, aber $\bar{b}^2 \in \{\bar{0}, \bar{1}\}$, ein Widerspruch.

- Für welche natürlichen Zahlen n ist $a = 2^n + 65$ eine Quadratzahl? Ist $n = 2m + 1$ ungerade, dann ist $2^n = 2 \cdot 4^m$ stets kongruent ± 2 modulo 5, ferner ist a ungerade, also endet a auf 3 oder 7. Aber ungerade Quadratzahlen enden auf 1, 5 oder 9, ein Widerspruch. Daher ist $n = 2m$ gerade, und 2^n eine Quadratzahl. Wegen $a > 2^n = (2^m)^2$ ist a mindestens so groß wie die nächste Quadratzahl nach 2^n, also $2^{2m}+65 = 2^n + 65 = a \geq (2^m + 1)^2$, und somit $65 \geq 2^{m+1} + 1$, also $2^m \leq 32$ und daher $m \leq 5$. Durchprobieren liefert die einzigen Lösungen $2^4+65 = 9^2$ und $2^{10} + 65 = 33^2$.

- Die Kongruenzmethode führt nicht immer zum Ziel: Man kann zeigen, dass $3x^3 + 4y^3 + 5z^3 = 0$ modulo jedem $n \in \mathbb{Z}$ nicht trivial lösbar ist, und dennoch hat diese Gleichung keine ganzzahlige Lösung außer $x = y = z = 0$. Beide Aussagen sind aber nicht einfach zu beweisen, und liegen jenseits dieser Vorlesung.

3.5 Maximale Ideale

Sei R ein kommutativer Ring. Ein *maximales Ideal* ist ein Ideal I von R mit $I \neq R$, so dass kein Ideal J von R existiert mit $I \subsetneq J \subsetneq R$. Die wichtige Aussage in diesem Zusammenhang ist.

Satz 3.17. *Sei I ein Ideal eines kommutativen Ringes R. Dann ist I genau dann maximal, wenn R/I ein Körper ist.*

Beweis. Sei I maximal, und $a + I \neq 0$ in R/I. Damit ist $a \neq I$. Da $Ra + I$ ein Ideal ist, welches I echt enthält, muss $Ra + I = R$ gelten. Daher gibt es $r \in R$ mit $1 \in ra + I$, also $1 + I = (a + I)(r + I)$, und $a + I$ ist daher multiplikativ invertierbar in R/I. Somit ist R ein Körper.

Sei nun I nicht maximal, und J ein Ideal echt zwischen I und R. Für $a \in J$ und $r \in R$ gilt dann $(a + I)(r + I) = ar + I \subseteq J$, also $1 \neq ar + I$, und somit ist $a + I$ nicht invertierbar. □

Beispiele maximaler Ideale

- Die Ideale I von $\mathbb{Z}$ haben die Form $n\mathbb{Z}$ mit $n = 0, 1, \ldots$. Ein solches Ideal ist genau dann maximal, wenn n eine Primzahl ist.

- Sei R die Menge der reellwertigen Abbildungen $M \to \mathbb{R}$ für eine Menge M. Offenbar ist R ein Ring. Für $m \in M$ ist die Abbildung $R \to \mathbb{R}$, $f \mapsto f(m)$ ein Epimorphismus von Ringen. Der Kern I ist das Ideal der reellwertigen Abbildungen f mit $f(m) = 0$. Wegen $R/I \cong \mathbb{R}$ ist R/I ein Körper, und I damit ein maximales Ideal.

Direkt aus dem Zornschen Lemma folgt

Satz 3.18 (Krull). *Sei $I \subsetneq R$ ein Ideal eines kommutativen Rings R. Dann ist I in einem maximalen Ideal von R enthalten.*

3.6 Primideale

Sei R wieder ein kommutativer Ring. Ein Ideal I von R heißt *Primideal*, wenn R/I ein Integritätsring ist. Ist also $ab \in I$, dann ist $(a+I)(b+I) \subseteq ab + I = 0$ in R/I, und wegen der Nullteilerfreiheit gilt $a \in I$ oder $b \in I$. Da Körper Integritätsringe sind, sind maximale Ideale automatisch Primideale. Das einizige nichtmaximale Primideal von $\mathbb{Z}$ ist $\{0\}$.

Induktiv sieht man sofort, dass nilpotente Elemente in allen Primidealen liegen. Wir wollen die Umkehrung beweisen.

Lemma 3.19. *Sei R ein kommutativer Ring (mit $0 \neq 1$) und S eine multiplikativ abgeschlossene Teilmenge von S mit $0 \neq S$. Dann hat R ein Primideal mit $S \cap I = \emptyset$.*

Beweis. Sei M die Menge der Ideale von R, welche disjunkt sind zu S. Wegen $\{0\} \in M$ ist M nicht leer. Die Vereinigung von Ketten aus M liegt wieder in M, nach dem Zornschen Lemma hat M daher ein maximales Element I. Wir wollen sehen, dass I ein Primideal ist. Dazu seien $x, y \in R \setminus I$. Wir müssen sehen, dass auch $xy \in R \setminus I$ gilt.

Da die Ideale $Rx + I$ und $Ry + I$ echt größer als I sind, enthalten sie Elemente s_x und s_y aus S. Es bestehen also Gleichungen $s_x = r_x x + i_x$, $s_y = r_y y + i_y$ mit $r_x, r_y \in R$, $i_x, i_y \in I$. Es gilt $s_x s_y + I = (s_x + I)(s_y + I) = (r_x x + I)(r_y y + I) = (r_x r_y xy + I)$. Da S multiplikativ abgeschlossen ist gibt es $i \in I$ mit $r_x r_y xy + i \in S$. Wäre $xy \in I$, dann gälte auch $r_x r_y xy + i \in I$, im Widerspruch zu $I \cap S = \emptyset$. Die Behauptung folgt. □

Satz 3.20. *Sei R ein kommutativer Ring (mit $0 \neq 1$). Die Menge der nilpotenten Elemente besteht aus dem Durchschnitt der Primideale.*

Beweis. Sei $x \in R$ nicht nilpotent. Wir müssen sehen, dass es ein Primideal I gibt, das x nicht enthält. Da x nicht nilpotent ist, ist $S = \{x^n | n \in \mathbb{N}\}$ eine multiplikativ abgeschlossene Menge mit $0 \notin S$. Die Behauptung folgt aus dem vorigen Lemma. □

3.7 Polynome

In diesem Abschnitt sei R stets ein kommutativer Ring. Sei X ein Symbol. Ein *Polynom* in der *Variablen* X ist eine formale Summe $r_0 + r_1 X + r_2 X^2 +$

$\cdots + r_n X^n$ für ein $n \in \mathbb{N}_0$. Hierbei trifft man die Festsetzung $X^0 = 1$. Die Menge der Polynome bildet einen Ring unter koeffizientenweiser Addition, und den Festsetzungen $rX = Xr$ und $X^m X^n = X^{m+n}$. Man schreibt $R[X]$ für diesen Ring. Man fasst R als Teilring von $R[X]$ auf, indem man $r \in R$ mit dem Polynom $r = rX^0$ identifiziert. Die Elemente $r_0, r_1, \ldots$ heißen die *Koeffizienten* des Polynoms $f := \sum r_i X^i$. Sei $f \neq 0$, und $n \in \mathbb{N}_0$ maximal mit $r_n \neq 0$. Dann heißt n der *Grad* von f, und r_n der *Leitkoeffizient*. Man schreibt $n = \operatorname{grad} f$. Man nennt f *normiert*, wenn $r_n = 1$ gilt. Der Koeffizient r_0 wird *konstanter Term* oder *Absolutglied* genannt. Für $f = 0$ setzt man $\operatorname{grad} f = -\infty$.

Aus den Definitionen folgt unmittelbar

Lemma 3.21. *Seien $f, g \in R[X]$ Polynome. Dann gilt* $\operatorname{grad}(f+g) \leq \max(\operatorname{grad} f, \operatorname{grad} g)$ *und* $\operatorname{grad}(f \cdot g) \leq \operatorname{grad} f + \operatorname{grad} g$. *Ist R ein Integritätsbereich, dann gilt* $\operatorname{grad}(f \cdot g) = \operatorname{grad} f + \operatorname{grad} g$

An der letzten Aussage sieht man, dass wenn R ein Integritätsbereich ist, dann gilt das auch für $R[X]$.

Wie bei ganzen Zahlen hat man auch für Polynome über Körpern eine Division mit Rest. Genauer gilt:

Satz 3.22. *Sei $g \in R[X]$ ein Polynom mit invertierbarem Leitkoeffizienten, und $f \in R[X]$ beliebig. Dann gibt es eindeutig gegebene Polynome $q, r \in R[X]$ mit $f = q \cdot g + r$ und* $\operatorname{grad} r < \operatorname{grad} g$.

Beweis. Wir wollen zunčhst die Eindeutigkeit beweisen. Dazu sei $f = q' \cdot g + r'$ eine weitere Darstellung der gegebenen Form. Dann folgt $(q - q')g = r' - r$. Da der Leitkoeffizient von g kein Nullteiler ist, gilt $\operatorname{grad}(r' - r) = \operatorname{grad}(q - q') + \operatorname{grad} g$. Wegen $\operatorname{grad}(r' - r) < \operatorname{grad} g$ folgt $q = q'$ und $r' = r$.

Es bleibt die Existenz zu zeigen. Sei a die Inverse des Leitkoeffizienten g, und $g' = ag$. Ist $f = q'g' + r$ eine Division durch g' mit Rest der verlangten Art, dann gilt das auch für $f = qg + r$ mit $q = aq'$. Wir dürfen also annehmen, dass g normiert ist.

Ist $\operatorname{grad} f < \operatorname{grad} g$, dann gibt es nichts zu zeigen, da wir $q = 0$ und $r = f$ setzen können. Wir verwenden nun vollständige Induktion über $\operatorname{grad} f$. Sei $n = \operatorname{grad} f \geq \operatorname{grad} g$, und a der Leitkoeffizient von f. Setze $f' = f - aX^{\operatorname{grad} f - \operatorname{grad} g} g$. Dann gilt $\operatorname{grad} f' < \operatorname{grad} f$. Nach Induktionsvoraussetzung gibt es also eine Darstellung $f' = q'g + r$ mit $\operatorname{grad} r < \operatorname{grad} g$. Die Behauptung folgt nun aus $f = f' + aX^{\operatorname{grad} f - \operatorname{grad} g} g = q'g + r' + aX^{\operatorname{grad} f - \operatorname{grad} g} g = (q' + aX^{\operatorname{grad} f - \operatorname{grad} g})g + r$. □

Eine wichtige Folgerung ist

Satz 3.23. *Sei R ein Körper, und $I \neq \{0\}$ ein Ideal von $R[X]$. Sei $g \neq 0$ ein Polynom kleinsten Grades aus I. Dann ist g bis auf einen Faktor $0 \neq r \in R$ eindeutig, und es gilt $I = (g)$. Insbesondere ist $R[X]$ ein Hauptidealring.*

Beweis. Ist $0 \neq r \in R$ und $g \in R[X]$, dann gilt $g \in I$ genau dann wenn $rg \in I$. Die Differenz zweier normierter Polynome von gleichem Grad n hat Grad $< n$, daraus folgt die Eindeutigkeitsaussage. Sei nun $0 \neq g \in I$ von kleinstem Grad, und $f \in I$ beliebig. Sei $f = qg + r$ eine Division mit Rest. Aus $r \in I$ und $\operatorname{grad} r < \operatorname{grad} g$ folgt $r = 0$, also $I \subseteq (g)$. Die umgekehrte Inklusion ist sowieso klar. □

Bemerkung. Obige Aussage wird im allgemeinen falsch, wenn R kein Körper mehr ist. Sogar ein Integritätsbereich zu sein ist zu schwach, wie das von 2 und X in $\mathbb{Z}[X]$ erzeugte Ideal zeigt.

Ist $a \in R$ und $f = \sum r_i X^i \in R[X]$ ein Polynom, dann bedeutet $f(a)$ die Summe $\sum r_i a^i$, mit der Konvention $a^0 = 1$ auch dann, wenn $a = 0$ gilt. Offenbar ist $R[X] \to R$, $f \mapsto f(a)$ ein Ringhomomorphismus. Man nennt a eine *Nullstelle* von f, wenn $f(a) = 0$ gilt.

Satz 3.24. *Ist a eine Nullstelle des Polynoms f, dann gibt es $g \in R[X]$ mit $f = (X - a)g$.*

Beweis. Schreibe $f = (X - a)g + r$ mit $\deg r < \deg(X - a) = 1$. Daher gilt $r \in R$. Einsetzen von a für X liefert $0 = f(0) = (a - a)g(a) + r = r$, und die Behautptung folgt. □

Eine wichtige Folgerung ist

Satz 3.25. *Sei R ein Integritätsring, und $0 \neq f \in R[X]$. Dann hat f höchstens* $\operatorname{grad} f$ *Nullstellen.*

Beweis. Für $\operatorname{grad} f \leq 1$ ist die Aussage klar. Wir beweisen sie allgemein durch vollständige Induktion. Seien $a_1, \ldots, a_r$ Nullstellen von f. Wir schreiben $f = (X - a_1)g$. Wegen $0 = f(a_i) = (a_i - a_1)g(a_i)$ und der Nullteilerfreiheit von R ist a_i eine Nullstelle von g für $i \geq 2$. Daher gilt $r - 1 \leq \operatorname{grad} g = \operatorname{grad} f - 1$, und die Behauptung folgt. □

Bemerkung. Man überlege sich ein Gegenbeispiel zum Satz, wenn R ein geeigneter Ring mit Nullteilern ist.

Eine überraschende Folgerung obigen Satzes ist

Satz 3.26. *Sei G eine endliche Untergruppe der multiplikativen Gruppe eines Körpers. Dann ist G zyklisch.*

Beweis. Sei n die Ordnung von G. Ist die abelsche Gruppe G nicht zyklisch, dann gibt es nach dem Struktursatz für abelsche Gruppen eine Primzahl p und eine zu $C_p \times C_p$ isomorphe Untergruppe H von G. Aber für alle Elemente $h \in H$ gilt $h^p = 1$. Daher sind die p^2 Elemente aus H Nullstellen des Polynoms $X^p - 1$, im Widerspruch zu vorigem Satz. □

Korollar 3.27. *Sei p eine Primzahl. Dann ist die multiplikative Gruppe des Körpers $\mathbb{Z}/p\mathbb{Z}$ zyklisch.*

Bemerkung. Das Korollar ist eine reine Existenzaussage in dem Sinne, dass man weiß dass $(\mathbb{Z}/p\mathbb{Z})^\times$ zyklisch ist, aber keinen Erzeuger explizit geliefert bekommt. In der Tat ist keine explizite Formel oder guter Algorithmus zum Auffinden solcher Erzeuger bekannt.

Ist R ein kommutativer Ring, und a eine Nullstelle eines Polynoms $0 \neq f \in R[X]$. Sei $e \in \mathbb{N}$ mit $f = (X - a)^e g$ für ein $e \in \mathbb{N}$. Wegen $e + \operatorname{grad} g = \operatorname{grad} f$ gilt $e \leq \operatorname{grad} f$. Insbesondere gibt es ein maximales e mit obiger Darstellung. Man nennt e die *Vielfachheit* der Nullstelle a. Man überlegt sich sofort, dass Satz 3.25 auch dann noch gilt, wenn man die Nullstellen mit Vielfachheit zählt. Ist die Vielfachheit 1, dann nennt man die Nullstelle *einfach*. Die Ableitung ist ein einfaches Hilfsmittel, um Polynome auf vielfache Nullstellen zu testen.

Definition 3.28. Auf dem Polynomring $R[X]$ definiert man durch $r' := 0$, $(rX^i)' := riX^{i-1}$ $(r \in R,\ i \geq 1)$ eine additive Abbildung $R[X] \to R[X]$, $f \mapsto f'$. Man nennt diese Abbildung eine *Ableitung* oder *Differentiation*.

Man rechnet sofort nach, dass die aus der Analysis gewohnte Produktregel $(fg)' = f'g + fg'$ gilt. Allerdings ist Vorsicht angebracht: Gilt $f' = 0$, dann muss f nicht ein konstantes Polynom sein. Ist beispielsweise $R = \mathbb{Z}/p\mathbb{Z}$, dann gilt $(X^p)' = pX^{p-1} = 0X^{p-1} = 0$.

Satz 3.29. *Sei R ein Integritätsbereich, und a eine Nullstelle des Polynoms $f \in R[X]$. Dann ist a eine einfache Nullstelle genau dann, wenn $f'(a) \neq 0$ gilt.*

Beweis. Sei $f = (X-a)g$. Ableiten liefert $f' = (X-a)g' + g$, also $f'(a) = g(a)$. Die Behauptung folgt. □

3.8 Einheitengruppe von $\mathbb{Z}/n\mathbb{Z}$

Als Anwendung des Korollars 3.27 wollen wir allgemein die Einheitengruppe von $\mathbb{Z}/n\mathbb{Z}$ bestimmen. Sei $n = \prod p_e^{e_i}$ die Primfaktorzerlegung von $n \in \mathbb{N}$.

Nach dem Chinesischen Restsatz ist $\mathbb{Z}/n\mathbb{Z}$ isomorph zum direkten Produkt der Ringe $\mathbb{Z}/p_i^{e_i}\mathbb{Z}$, und damit ist die Einheitengruppe $(\mathbb{Z}/n\mathbb{Z})^\times$ isomorph zum direkten Produkt der Einheitengruppen $(\mathbb{Z}/p_i^{e_i}\mathbb{Z})^\times$. Der folgende Satz klärt die Struktur dieser Gruppen.

Satz 3.30. *(a) Sei p eine ungerade Primzahl und $l \in \mathbb{N}$. Dann ist $(\mathbb{Z}/p^l\mathbb{Z})^\times$ zyklisch. Sei $w \in \mathbb{Z}$, so dass $w+p\mathbb{Z}$ ein Erzeuger von $(\mathbb{Z}/p\mathbb{Z})^\times$ ist. Dann ist $w^{p^{l-1}}(1+p) + p^l\mathbb{Z}$ ein Erzeuger von $(\mathbb{Z}/p^l\mathbb{Z})^\times$.*

(b) Für $l \geq 2$ ist $(\mathbb{Z}/2^l\mathbb{Z})^\times$ isomorph zu einem direkten Produkt zweier zyklischer Gruppen der Ordnungen 2 und 2^{l-2}, mit Erzeugern -1 und 5.

Dem Beweis schicken wir einige Lemmata voraus.

Lemma 3.31. *Sei p eine Primzahl, und $1 \leq k \leq p-1$. Dann ist $\binom{p}{k}$ durch p teilbar.*

Beweis. Wegen $\binom{p}{k} = \frac{p(p-1)\ldots(p-k+1)}{1\cdot 2\ldots k}$ ist der Zähler durch p teilbar, aber nicht der Nenner. □

Lemma 3.32. *Sei p eine Primzahl, $l \in \mathbb{N}$, und für $a, b \in \mathbb{Z}$ sei $a-b$ durch p^l teilbar. Dann ist $a^p - b^p$ durch p^{l+1} teilbar.*

Beweis. Schreibe $a = b + cp^l$. Dann gilt

$$\begin{aligned} a^p - b^p &= (b+cp^l)^p - b^p \\ &= \sum_{k=1}^{p} \binom{p}{k} b^{p-k}(cp^l)^k \\ &= b^{p-1}cp^{l+1} + \sum_{k=2}^{p} \binom{p}{k} b^{p-k}(cp^l)^k. \end{aligned}$$

Aber für $k \geq 2$ gilt $kl \geq 2l \geq l+1$, und die Behauptung folgt. □

Lemma 3.33. *Sei $l \geq 2$, und $p \neq 2$ eine Primzahl. Dann ist $(1+p)^{p^{l-2}} - (1+p^{l-1})$ durch p^l teilbar.*

Beweis. Wir benutzen vollständige Induktion über l. Die Aussage ist klar für $l = 2$.

Sie gelte nun für l. Nach obigem Lemma ist $(1+p)^{p^{l-1}} - (1+p^{l-1})^p$ durch p^{l+1} teilbar. Wegen

$$(1+p^{l-1})^p = (1+p^l) + \sum_{k=2}^{p} \binom{p}{k} (p^{l-1})^k$$

ist zu zeigen, dass die Summe durch p^l teilbar ist. Wegen Lemma 3.31 ist das klar für jeden Summanden außer dem für $k = p$. Hierfür benötigen wir $(l-1)p \geq l+1$. Das gilt aber wegen $p \geq 3$ und $l \geq 2$. □

Bemerkung. Man sieht, dass der letzte Schritt im Beweis für $p = 2$ nicht funktioniert. In der Tat ist die entsprechende Aussage falsch. Dies führt dazu, daß die Primzahl 2 hier und in der Zahlen- und Gruppentheorie oft eine (unangenehme) Sonderrolle spielt.

Lemma 3.34. *Für $l \geq 3$ ist $5^{2^{l-3}} - (1 + 2^{l-1})$ durch 2^l teilbar.*

Beweis. Die Behauptung ist klar für $l = 3$. Sie gelte für l. Nach Lemma 3.32 ist dann $5^{2^{l-2}} - (1+2^{l-1})^2$ durch 2^{l+1} teilbar. Wegen $(1+2^{l-1})^2 = 1+2^l+2^{2l-2}$ und $2l - 2 \geq l + 1$ folgt die Behauptung. □

Beweis von Satz 3.30. Die Gruppe $(\mathbb{Z}/p^l\mathbb{Z})^\times$ besteht aus den Restklassen $i + p^l\mathbb{Z}$, mit $0 \leq i \leq p^l - 1$ und i teilerfremd zu p. Daher hat $(\mathbb{Z}/p^l\mathbb{Z})^\times$ die Ordnung $p^{l-1}(p-1)$.

(a) Wir zeigen zunächst, dass $1 + p$ die Ordnung p^{l-1} hat. Wäre das nicht der Fall, dann wäre die Ordnung von $1 + p$ ein echter Teiler von p^{l-1}. Insbesondere wäre $(1 + p)^{p^{l-2}} - 1$ durch p^l teilbar. Nach Lemma 3.33 wäre dann p^{l-1} durch p^l teilbar, was natürlich Unsinn ist.

Da w modulo p die Ordnung $p - 1$ hat, ist die Ordnung von w modulo p^l ein Vielfaches von $p - 1$. Diese Ordnung teilt $p^{l-1}(p-1)$, daher hat $w^{p^{l-1}}$ die Ordnung $p-1$, und nach obigem hat $w^{p^{l-1}}(1+p)$ modulo p^l die Ordnung $(p-1)p^{l-1}$, die Behauptung folgt.

(b) Die Ordnung von $(\mathbb{Z}/2^l\mathbb{Z})^\times$ ist 2^{l-1}. Lemma 3.34 zeigt, dass die Ordnung von $5 + 2^l\mathbb{Z}$ gerade 2^{l-2} ist. Zum Beweis der Aussage ist also zu zeigen, dass $-1 + 2^l\mathbb{Z}$ nicht in der von $5 + 2^l\mathbb{Z}$ erzeugten zyklischen Gruppe liegt. Wir nehmen das Gegenteil an. Dann gibt es $m \in \mathbb{N}$, so dass 2^l ein Teiler von $5^m - (-1) = 5^m + 1$ ist. Insbesondere ist 4 ein Teiler von $5^m + 1$, ein Widerspruch. □

3.9 Quotientenkörper

Es sei R ein Integritätsbereich. Analog wie man den Körper $\mathbb{Q}$ aus $\mathbb{Z}$ konstruiert, werden wir zu R einen kleinsten Körper K konstruieren, in dem R enthalten ist. Auf der Menge der Paare (r, s) mit $r, s \in R$, $s \neq 0$ führen wir eine Äquivalenzrelation ein. Dabei sind zwei solche Paare (r, s) und (r', s') genau dann äquivalent, wenn $rs' = r's$ gilt. Man rechnet sofort nach, dass man tatsächlich eine Äquivalenzrelation erhält. Die Äquivalenzklasse von (r, s)

bezeichnet man mit $\frac{r}{s}$. Sei K die Menge der Äquivalenzklassen. Man rechnet ebenso schnell nach, dass man durch

$$\frac{r}{s} + \frac{r'}{s'} = \frac{rs' + r's}{ss'}$$

und

$$\frac{r}{s} \cdot \frac{r'}{s'} = \frac{rr'}{ss'}$$

eine wohldefinierte Addition und Multiplikation auf K bekommt. Ferner verifiziert man, dass K ein Ring ist, der via $r \mapsto \frac{r}{1}$ den Ring R als Teilring enthält.

Diw wichtigste Eigenschaft von K ist, dass K ein Körper ist: Sei $\frac{r}{s} \neq 0$. Dann gilt $r \neq 0$, also $\frac{s}{r} \in K$. Wegen $\frac{r}{s}\frac{s}{r} = 1$ ist $\frac{r}{s}$ multiplikativ invertierbar. Man nennt daher K den *Quotientenkörper* von R.

3.10 Teilbarkeit

Im folgenden sei R wieder ein Integritätsbereich. Wir wollen einige von $\mathbb{Z}$ bekannte Eigenschaften über Teilbarkeit auf R übertragen, aber auch sehen, dass man mit Verallgemeinerungen vorsichtig sein muss.

Sind $r, s \in R$, dann sagt man, r *teilt* s (oder r ist ein *Teiler* von s), wenn es $x \in R$ gibt mit $s = xr$. Insbesondere ist 1 ein Teiler von allen $r \in R$, und 0 wird von allen $r \in R$ geteilt. Ist $K \supseteq R$ der Quotientenkörper von R, und $s \neq 0$, dann ist s ein Teiler von r genau dann, wenn $\frac{r}{s} \in R$ gilt.

Ist s ein Teiler von r, dann schreibt man $r \mid s$, und wenn das nicht der Fall ist, so schreibt man $r \nmid s$.

Ist $0 \neq s \in R$, so besitzt s gewisse triviale Teiler. So ist z.B. jede Einheit u ein Teiler von s, denn ist $uu' = 1$, so gilt $s = u(u's)$. Ferner ist wegen $s = (su)u'$ auch su ein Teiler von s. Ist s keine Einheit, und hat s außer diesen trivialen Teilern keine weiteren Teiler, dann heißt s *unzerlegbar* oder *irreduzibel*. Ist r nicht irreduzibel, dann ist r *reduzibel*.

Die irreduziblen Elemente aus $\mathbb{Z}$ sind die Zahlen $\pm p$, wobei p eine Primzahl ist. Man hat sich daran gewöhnt, dass man in $\mathbb{Z}$ eine (bis auf Vorzeichen) eindeutige Primfaktorzerlegung hat. Erst Gauß hat erkannt, dass diese Aussage nicht trivial ist und einen Beweis benötigt, den er auch gegeben hat.

Beispiel für Versagen der eindeutigen Zerlegung in irreduzible Faktoren Sei $R = \mathbb{Z}[\sqrt{-5}] = \{a + b\sqrt{-5} | a, b \in \mathbb{Z}\}$. Man rechnet sofort nach, dass R ein Ring ist. Wir betrachten die Abbildung $N : R \to \mathbb{N}_0$, $a + b\sqrt{-5} \mapsto a^2 + 5b^2$. Dabei ist also $N(x)$ das Quadrat des Betrags der komplexen Zahl x. Man weiß, oder rechnet sofort nach, dass $N(xy) = N(x)N(y)$

gilt für alle $x, y \in R$. Ist r eine Einheit, dann gibt es r' mit $rr' = 1$. Hieraus folgt $1 = N(1) = N(rr') = N(r)N(r')$, also $N(r) = 1$. Ist umgekehrt $1 = N(a + b\sqrt{-5}) = a^2 + 5b^2$, dann gilt $b = 0$ und $a = \pm 1$. Somit ist r genau dann eine Einheit, wenn $N(r) = 1$ gilt.

Ist $0 \neq r$ keine Einheit und reduzibel, dann gibt es $x, y \in R$ mit $r = xy$, so dass x und y keine Einheiten sind. Es folgt $N(r) = N(x)N(y)$. Da es in R keine Nichteinheiten $s \neq 0$ mit $N(s) = 2$ oder $N(s) = 3$ gibt, folgt $N(r) \geq 16$. Wegen $N(2) = 4$, $N(3) = 9$, und $N(1 \pm \sqrt{-5}) = 6$ sind die Elemente 2, 3 und $1 \pm \sqrt{-5}$ daher irreduzibel, und 2 unterscheidet sich weder von $1 + \sqrt{-5}$, noch von $1 - \sqrt{-5}$ um eine Einheit. Daher sind $6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$ zwei grundsätzlich verschiedene Zerlegungen in irreduzible Faktoren.

Ein mit der Irreduzibilität verwandter Begriff ist der eines primen Elements. Dabei heißt eine Nichteinheit $0 \neq r \in R$ *prim*, wenn aus $r \mid ab$ stets $r \mid a$ oder $r \mid b$ folgt. Die letzte Bedingung ist äquivalent dazu, dass das Hauptideal (p) ein Primideal von R ist.

Eine erste einfache Beobachtung ist

Lemma 3.35. *Jedes Primelement ist irreduzibel.*

Beweis. Sei r prim, aber nicht irreduzibel. Dann gibt es Nichteinheiten $x, y \in R$ mit $r = xy$. Da r prim ist, teilt r einen der Faktoren x und y. Wir nehmen $r \mid x$ an. Es gibt also $x' \in R$ mit $x = rx'$. Es folgt $r = rx'y$, also $r(1 - x'y) = 0$. Wegen der Nullteilerfreiheit gilt $x'y = 1$, daher ist y eine Einheit, ein Widerspruch. □

Obiges Beispiel zeigt, dass die Umkehrung im allgemeinen nicht gilt. Die Elemente 2, 3 und $1 \pm \sqrt{-5}$ sind alle irreduzibel in $\mathbb{Z}[\sqrt{-5}]$, aber keines davon ist prim. Unter Zusatzvoraussetzungen allerdings stimmt die Umkehrung:

Satz 3.36. *Jedes irreduzible Element eines Hauptidealrings ist ein Primelement.*

Beweis. Sei p ein irreduzibles Element, welches das Produkt ab teilt, aber nicht a teilt. Das von a und p erzeugte Ideal ist ein Hauptideal (d), es gibt also $u, v \in R$ mit $ua + vp = d$. Wegen $(p) \subset (d)$ gilt $d \mid p$. Damit ist d eine Einheit, oder von der Form up mit einer Einheit u. Aber $d \mid a$, und somit $p \mid a$, im Widerspruch zur Voraussetzung an a. Daher ist d eine Einheit, und ohne Einschränkung $d = 1$. Multiplikation mit b liefert die Behauptung. □

Wir kommen nun zum wichtigen Begriff des faktoriellen Rings.

Definition 3.37. Ein Integritätsbereich R heißt *faktoriell*, wenn jedes Element $\neq 0$ entweder eine Einheit ist, oder ein Produkt endlich vieler Primelemente ist.

Natürlich ist in einem faktoriellen Ring jedes irreduzible Element ein Primelement. Die wichtigste Eigenschaft eines faktoriellen Rings ist die eindeutige Primfaktorzerlegung.

Satz 3.38. *Sei R ein faktorieller Ring, $0 \neq a \in R$ keine Einheit, und $a = p_1 p_2 \dots p_r = q_1 q_2 \dots q_s$ zwei Zerlegungen in Primelemente p_i, q_i. Dann gilt $r = s$, und die p_i bzw. q_i stimmen bis auf Reihenfolge und Multiplikation mit Einheiten überein. (D.h., es gibt eine Permutation σ von $\{1, 2, \dots, r\}$ und Einheiten $u_1, \dots, u_r$ mit $p_i = u_i q_{i^\sigma}$ für alle i.)*

Beweis. Ohne Einschränkung gilt $r \geq s$. Wir beweisen die Aussage durch vollständige Induktion über r. Für $r = 1$ gibt es nichts zu beweisen. Wir schließen nun von $r - 1$ auf r. Da p_r das Produkt $q_1 q_2 \dots q_s$ teilt, folgt durch mehrfache Anwendung der Primeigenschaft von p_r, dass p_r einen der Faktoren $q_1, q_2, \dots, q_s$ teilt. Durch Umbenennung der q_i dürfen wir annehmen, dass $p_r \mid q_s$, also $q_s = u p_r$. Als Primelement ist q_s irreduzibel, daher ist u eine Einheit. Die Behauptung folgt nun aus der Richtigkeit für $r - 1$, angewandt auf $p_1 p_2 \dots p_{r-1} = q_1 q_2 \dots q_{s-2}(u q_{s-1})$. □

Natürlich hat jede ganze Zahl eine Zerlegung in irreduzible Zahlen. Da $\mathbb{Z}$ ein Hauptidealring ist, stimmen irreduzible und Primelemente überein, und obiger Satz liefert die eindeutige Primfaktorzerlegung in $\mathbb{Z}$.

Die Primeigenschaft der Primzahlen hatten wir schon früher verwendet (Korollar 3.4). Ferner machten wir mehrfach von der eindeutigen Primfaktorzerlegung in $\mathbb{Z}$ Gebrauch. Man mache sich klar, dass der gerade nachgetragene Beweis nicht auf einem Zirkelschluss beruht!

Wir wissen auch, dass Polynomringe über einem Körper Hauptidealringe sind. Ferner beweist man mittels der Gradfunktion, dass jedes Polynom ein Produkt irreduzibler Polynome ist. Das liefert das wichtige

Korollar 3.39. *Sei $R = \mathbb{Z}$, oder R der Polynomring $K[X]$ für einen Körper K. Dann stimmen in R irreduzible Elemente und prime Elemente überein. Insbesondere ist R faktoriell.*

3.11 Inhalt von Polynomen, Lemma von Gauß

Im folgenden sei R ein faktorieller Integritätsbereich, und K der Quotientenkörper von R. Es mag das Verständnis erleichtern, wenn man stets das Beispiel $R = \mathbb{Z}$, $K = \mathbb{Q}$ im Auge behält.

Sei $0 \neq a \in K$, und $p \in R$ ein Primelement von R. Aus der eindeutigen Primfaktorzerlegung folgt schnell, dass man eine Darstellung $a = p^m \frac{u}{v}$ mit $m \in \mathbb{Z}$, $u \in R$, $0 \neq v \in R$ finden kann, so dass p weder u noch v teilt. Dabei

ist m unabhängig von der Wahl des Paares u, v. Wir schreiben $v_p(a) := m$, und setzen $v_p(0) := \infty$. Es gilt $v_p(ab) = v_p(a)v_p(b)$. Ist $0 \neq f = a_0 + a_1^X + \ldots a_n X^n \in K[X]$, dann setzen wir $v_p(f) := \min_i v_p(a_i)$. Sei P eine Menge von Primelementen von R, so dass jedes Primelement aus R sich von genau einem Element aus P nur um eine Einheit unterscheidet. Ist $0 \neq f \in K[X]$, dann nennt man

$$I(f) := \prod_{p \in P} p^{v_p(f)}$$

den *Inhalt* von f.

Ist beispielsweise $R = \mathbb{Z}$, und $P \subset \mathbb{N}$ die Menge der Primzahlen, dann ist für $f \in \mathbb{Z}[X]$ der Inhalt $I(f)$ gerade der größte gemeinsame Teiler der Koeffizienten von f.

Der Inhalt $I(f)$ hängt von der Wahl von P ab, und ist nur bis auf Einheiten eindeutig bestimmt.

Ist $0 \neq a \in K$ und $0 \neq f \in K[X]$, dann gilt $I(af) = I(a)I(f)$. Hieraus folgt $I(\frac{1}{I(f)}f) = \frac{1}{I(f)}I(f) = 1$. Es gibt also $\gamma \in K$ mit $f = \gamma g$, so dass $I(g) = 1$ gilt. Polynome mit Inhalt 1 nennt man *primitiv*. Man beachte, dass ein primitives Polynom Koeffizienten aus R hat.

Satz 3.40 (Gauß Lemma). *Seien $0 \neq f, g \in K[X]$. Dann gilt $I(fg) = I(f)I(g)$.*

Beweis. Schreibe $f = \alpha f_1$, $g = \beta g_1$ mit $\alpha, \beta \in K$ und f_1, g_1 primitiv. Wegen $I(\alpha\beta) = I(\alpha)I(\beta)$ bleibt zu zeigen, dass auch $f_1 g_1$ primitiv ist. Wegen $f_1 g_1 \in R[X]$ ist das gleichbedeutend damit, das $f_1 g_1$ für jedes Primelement $p \in R$ einen nicht durch p teilbaren Koeffizienten hat. Der Faktorring $\bar{R} = R/(p)$ ist ein Integritätsbereich. Der natürliche Homomorphismus $\bar{}: R \to R/(p)$ setzt sich fort zu einem Homomorphismus $\bar{}: R[X] \to \bar{R}[X]$. Wären alle Koeffizienten von $f_1 g_1$ durch p teilbar, dann folgte $\overline{f_1 g_1} = 0$, also $\bar{f}_1 \bar{g}_1 = 0$. Da $\bar{R}$ ein Integritätsbereich ist, folgt ohne Einschränkung $\bar{f}_1 = 0$. Das bedeutet aber, dass alle Koeffizienten von f_1 durch p teilbar sind, im Widerspruch zu $I(f_1) = 1$. □

Das Gauß Lemma hat eine Reihe von Konsequenzen. Wenn zum Beispiel ein Polynom $f \in R[X]$ in Faktoren aus $K[X]$ zerfällt, dann bekommt man im wesentlichen eine gleiche Faktorisierung über R. Genauer gilt.

Korollar 3.41. *Sei $f = gh$ mit $f \in R[X]$ und $g, h \in K[X]$. Setze $\gamma_g = I(g)$, $\gamma_h = I(h)$, also $g = \gamma_g g_1$, $h = \gamma_h h_1$ mit g_1, h_1 primitiv. Dann gilt $f = (\gamma_g \gamma_h) g_1 h_1$ mit $\gamma_g \gamma_h \in R$. Insbesondere gilt: Ist ein primitives Polynom irreduzibel in $R[X]$, dann ist es auch irreduzibel in $K[X]$.*

Eine wichtige Folgerung ist

Korollar 3.42. *Sei R ein faktorieller Ring. Dann ist $R[X]$ faktoriell. Die Primelemente von $R[X]$ bestehen aus den Primelementen von R, zusammen mit den irreduziblen und primitiven Polynomen aus $R[X]$.*

Beweis. Wir müssen zeigen, dass jedes irreduzible Element $f \in R[X]$ prim ist, und die angebene Form besitzt. Wir schreiben $f = \gamma g$ mit $\gamma \in R$ und g primitiv. Da f irreduzibel ist, ist entweder g irreduzibel und γ eine Einheit, oder g ein konstantes Polynom, und wegen $I(g) = 1$ eine Einheit, und γ ein Primelement.

Es bleibt zu zeigen, dass f prim ist. Sei also f ein irreduzibles Element in $R[X]$, und ein Teiler von uv mit $u, v \in R[X]$. Wir unterscheiden zwei Fälle: f ist ein Primelement aus R. Dann ist $I(f)$ auch prim in R, und $I(f)$ teilt $I(u)I(v)$. Ohne Einschränkung ist dann $I(f)$ ein Teiler von $I(u)$. Dann ist aber $I(\frac{u}{f}) \in R$, also $\frac{u}{f} \in R[X]$, und somit $f \mid u$.

Im zweiten Fall ist f irreduzibel und primitiv. Wegen obigen Korollars ist f auch irreduzibel in $K[X]$, also auch ein Primelement in $K[X]$, da $K[X]$ faktoriell ist. In $K[X]$ ist also f ein Teiler von uv, also auch von u oder v. Sei $v = hf$ mit $h \in K[X]$. Wegen $I(v) = I(h)I(f) = I(h)$ gilt $h \in R[X]$, somit ist u in $R[X]$ durch f teilbar, und die Behauptung folgt. □

Durch $K[X_1, X_2, \ldots, X_n] := K[X_1, X_2, \ldots, X_{n-1}][X_n]$ definiert man iterativ einen Polynomring in n Variablen. Ein Folge des obigen Satzes ist

Korollar 3.43. *Sei K ein Körper. Dann ist der Polynomring $K[X_1, X_2, \ldots, X_n]$ in n Variablen faktoriell.*

Bemerkung. Der Polynomring $K[X_1, X_2, \ldots, X_n]$ ist für $n \geq 2$ kein Hauptidealring, z.B. weil das von $X_1, \ldots, X_n$ erzeugte Ideal kein Hauptideal ist.

3.12 Kryptographie

Eine wichtige moderne Anwendung der Algebra ist die vertrauliche Übertragung von Nachrichten. Während das früher fast nur militärisch verwendet wurde, wäre unser heutiger Alltag ohne kryptographische Methoden nicht denkbar. Das Bezahlen mit Geld- oder Kreditkarten, Mobilfunktelefonie, Kauf und Verkauf über das Internet, elektronische Steuererklärung und vieles mehr basiert auf kryptographischen Methoden. Dabei geht es stets darum, dass zwei Partner S und E Nachrichten austauschen, und diese vorher so verschlüsseln, dass nur der Partner sie entschlüsseln kann. Bei den modernen Anwendungen kommt noch eine weitere wichtige Forderung hinzu: S und E sollten sich **öffentlich** auf eine Methode einigen können, also ohne erst mal über einen sicheren Kanal einen Code festzulegen. Es sieht auf den

ersten Blick sicher so aus, dass so etwas unmöglich ist, und bis in die 70er Jahre glaubte man das auch. Dennoch veröffentlichten 1976 Diffee und Hellman eine raffinierte Idee, die diese beiden Wünsche erfüllt. Eine Variante gaben 1977 **R**ivest, **S**hamir und **A**dleman an, das heute so genannten *RSA-Verfahren*. Mittlerweile weiß man, dass beide diese Durchbrüche schon wenige Jahre vorher gefunden wurden, aber ihre Bedeutung nicht erkannt wurde, und zusätzlich noch zur Verschlusssache erklärt wurden. Das RSA-Verfahren z.B. entdeckte bereits 1973 der britische Mathematiker Clifford Cocks. Da beim RSA-Verfahren der Empfänger die Parameter zur Verschlüsselung öffentlich macht, nennt man die Methode auch ein *public key cryptosystem*.

Im folgenden bedeutet $a \equiv b \pmod{m}$ stets, dass $a - b$ durch m teilbar ist. Für $n \in \mathbb{N}$ sei $\varphi(n)$ die Ordnung der Einheitengruppe von $\mathbb{Z}/n\mathbb{Z}$. Ist $n = \prod p_i^{e_i}$, so wissen wir bereits, dass $\varphi(n) = \prod (p_i - 1) p_i^{e_i - 1}$.

Zur Vorbereitung beweisen wir ein kleines

Lemma 3.44. *Sei $n \in \mathbb{N}$ quadratfrei, und $k \in \mathbb{N}$. Für alle $a \in \mathbb{Z}/n\mathbb{Z}$ gilt dann $a^{k\varphi(n)+1} = a$.*

Beweis. Sei $A \in \mathbb{Z}$ ein Repräsentant von a. Sei $p \mid n$. Falls $p \mid A$, dann gilt natürlich $A^{k\varphi(n)+1} \equiv A \pmod{p}$. Im Fall $p \nmid A$ gilt $A^{p-1} \equiv 1 \pmod{p}$, also $A^{k\varphi(n)} \equiv 1 \pmod{p}$, da $p - 1$ ein Teiler von $\varphi(n)$ ist. Es folgt $A^{k\varphi(n)+1} \equiv A \pmod{p}$. Daher ist $A^{k\varphi(n)+1} - A$ durch alle Primteiler von n teilbar, und die Behauptung folgt aus der Quadratfreiheit von n. □

Das RSA-Verfahren. Im folgenden beschreiben wir das RSA-Verfahren. Ein Sender S möchte einem Empfänger E eine Nachricht schicken. Dazu wählt E zwei große verschiedene Primzahlen p und q, und setzt $n = pq$. Ferner wählt E eine natürliche Zahl $s \leq \varphi(n)$, die teilerfremd zu $\varphi(n)$ ist. Da s teilerfremd ist zu $\varphi(n)$, ist s in $\mathbb{Z}/\varphi(n)\mathbb{Z}$ invertierbar, es gibt also $t \in \mathbb{Z}$ mit $st \equiv 1 \pmod{\varphi(n)}$. Das Paar (n, s) macht E öffentlich (zum Beispiel auf seiner privaten Homepage), die Primfaktoren p und q von n sowie t hält E geheim. Aus Sicherheitsgründen kann E sogar p und q nach der Berechnung von t löschen.

S verwendet zum Versenden seiner Nachricht als "Wörter" die Elemente aus dem Restklassenring $\mathbb{Z}/n\mathbb{Z}$, sowohl für den Klartext, als auch für die Verschlüsselung. Das Klartextwort $a \in \mathbb{Z}/n\mathbb{Z}$ verschlüsselt S hierbei zu a^s, der Empfänger E (und jeder, der die Nachricht eventuell mitliest) erhält also $b = a^s$. Der Empfänger E berechnet nun b^t in $\mathbb{Z}/n\mathbb{Z}$.

Wegen des Lemmas gilt in $\mathbb{Z}/n\mathbb{Z}$ also

$$b^t = a^{st} = a,$$

E erhält also den Klartext a zurück.

Warum nun hält man das Verfahren bei geeigneter Wahl der Parameter für sicher? Ein Zuhöher, der das Wort $b = a^s$ abfängt, und auch n und s kennt, müsste t kennen um a aus b zu rekonstruieren. Wegen $st \equiv 1 \pmod{\varphi(n)}$ kann man t bestimmen, wenn man $\varphi(n)$ kennt. Umgekehrt vermutet man, konnte das aber noch nicht beweisen, dass es keine bessere Methode gibt t zu bestimmen als vorher erst mal $\varphi(n)$ zu ermitteln. Wegen $\varphi(n) = \varphi(pq) = (p-1)(q-1) = n - p - q + 1$ ist die Bestimmung von $\varphi(n)$ äquivalent zur Bestimmung von p und q, also der Faktorisierung von n.

Man kennt bis heute keine Methode, allgemein Zahlen mit über 150 Ziffern (Dezimaldarstellung) zu faktorisieren, auch dann nicht, wenn man schon a priori wie in unserem Fall weiß, dass genau zwei Primfaktoren auftreten.

Andererseits kann man heutzutage von Zahlen mit einigen tausend Stellen schnell entscheiden, ob sie Primzahlen sind. Diese Methoden beruhen nicht darauf, dass man versucht, die gegebene Zahl zu faktorisieren, sondern benutzen z.B. die Tatsache, dass $n \in \mathbb{N}$ genau dann prim ist, wenn die Einheitengruppe von $\mathbb{Z}/n\mathbb{Z}$ die Ordnung $n-1$ hat.

Beim RSA-Verfahren sind Potenzen a^s und b^t mit eventuell sehr großen Exponenten zu berechnen. Allgemein kann man in einem Monoid eine Potenz r^n mit deutlich weniger als $n-1$ Multiplikationen berechnen: Dazu schreibt man n in der Binärentwicklung, also $n = \sum 2^{e_i}$ mit verschiedenen $e_i \in \mathbb{N}_0$. Dabei ist $2^{e_i} \leq n$, also $e_i \leq \log n / \log 2$. Die Potenz r^{2^e} lässt sich durch e-faches Quadrieren berechnen, und wegen $r^n = \prod r^{2^{e_i}}$ lässt sich r^n im wesentlichen mit höchstens $2 \log n / \log 2$ Multiplikationen bestimmen.

Diese einfache Beobachtung liefert im übrigen auch einen schnellen Test, mit dem man in den meisten Fällen schnell feststellen kann, wenn eine Zahl nicht prim ist: Für Primzahlen p gilt ja $a^{p-1} \equiv 1 \pmod{p}$, wenn a nicht durch p teilbar ist. Möchte man eine Zahl n auf Primeigenschaft testen, dann überprüft man, ob $a^{n-1} \equiv 1 \pmod{n}$ gilt z.B. für $a = 2$. Ist das nicht der Fall, dann kann n keine Primzahl sein. Ist es jedoch der Fall, dann kann man weitere Werte für a ausprobieren. Leider gibt es Nicht-Primzahlen n, die $a^{n-1} \equiv 1 \pmod{n}$ für alle zu n teilerfremde $a \in \mathbb{Z}$ erfüllen, das kleinste Beispiel ist $561 = 3 \cdot 11 \cdot 17$.

4 Körper

Index