Algebra

Skript für eine zweisemestrige Vorlesung

Florian Möller
Universität Würzburg

7. Dezember 2022

Inhaltsverzeichnis

Literatur

[Bos20] S. Bosch, Algebra (9. Auflage), Springer (2020),
ISBN: 9783662616499,
DOI: https://doi.org/10.1007/978-3-662-61649-9,
URL: https://bibliothek.uni-wuerzburg.de/permalink/bv/BV046747166

[KM17] C. Karpfinger, K. Meyberg, Algebra (4. Auflage), Springer (2017),
ISBN: 9783662547229,
DOI: https://dx.doi.org/10.1007/978-3-662-54722-9,
URL: https://bibliothek.uni-wuerzburg.de/permalink/bv/BV044432504

[MüP11] S. Müller-Stach, J. Piontkowski, Elementare und algebraische Zahlentheorie (2. Auflage), Vieweg+Teubner (2011),
ISBN: 9783834812568,
DOI: https://doi.org/10.1007/978-3-8348-8263-9,
URL: https://bibliothek.uni-wuerzburg.de/permalink/bv/BV039156152

[Wil73] J. C. Wilson, A principal ideal ring that is not a Euclidean ring,
Math. Mag. 46 (1973), pp. 34–38,
DOI: https://doi.org/10.2307/2688577

Teil I.
Grundlagen

In diesem Abschnitt stellen wir wichtige Begriffe und Techniken der Algebra dar. Meist beschreiben wir diese zunächst abstrakt und zeigen im Anschluss dann die konkrete Umsetzung für *Gruppen*, *Ringe* und *Körper*. Auf diese Weise rückt die eigentliche algebraische Idee in den Vordergrund, ohne aber die wichtigen Anwendungen auf Gruppen, Ringe und Körper zu überdecken.

Beim Durcharbeiten dieses Abschnitts sollten Sie versuchen, eine Verbindung des jeweils betrachteten Konzepts zur Linearen Algebra herzustellen (falls dies sinnvoll möglich ist). Versuchen Sie, folgende Fragen zu beantworten:
Kennen Sie das betrachtete Konzept bereits aus der Linearen Algebra? Falls ja, welche Notationen und Begriffe wurden dort verwendet? Welche Resultate wurden bewiesen? Falls nein, wie sähe die Übersetzung des Konzepts in die Lineare Algebra aus?

Inhaltlich werden wir uns zunächst mit *algebraischen Strukturen*, und hier insbesondere mit Gruppen, Ringen und Körpern, beschäftigen. Wir klären, was wir unter *Unterstrukturen* verstehen wollen und stellen mit den *Unterstrukturkriterien* Sätze bereit, mit denen man Mengen auf Unterstruktureigenschaft prüfen kann. Als direkte Konsequenz erhalten wir den Begriff des *Erzeugnisses*, das Unterstrukturen, die gewissen Minimalitätseigenschaften genügen, beschreibt.
Anschließend zeigen wir einige Grundaussagen über die ganzen Zahlen $\mathbb{Z}$. Wir werden in der Ringtheorie in Abschnitt III hierauf zurückkommen und einige der Beweisideen verallgemeinern.
Für die Darstellung von *Faktorgruppen* und *Faktorringen* nehmen wir uns viel Zeit. Wir motivieren diese Begriffe durch Konstruktion der *Restklassenringe* $\mathbb{Z}_n$. Anschließend abstrahieren wir unser Vorgehen auf allgemeine Gruppen und Ringe. Hierbei werden wir auf die wichtigen Begriffe des *Normalteilers* und des *Ideals* stoßen.
Zuletzt beschäftigen wir uns mit strukturerhaltenden Abbildungen, den *Homomorphismen*. Wir beweisen den *Homomorphiesatz*, der Faktorstrukturen mit Homomorphismen verbindet. Als Abschluss des Abschnitts zeigen wir einen Spezialfall des *chinesischen Restsatzes*, der für die Zahlentheorie enorm wichtig ist.

1. Algebraische Strukturen

Worum geht es? Wir definieren, was wir unter einer *Verknüpfung* und, hierauf aufbauend, unter einer *algebraischen Struktur* verstehen. Anschließend stellen wir mit der *Gruppe*, dem *Ring* und dem *Körper* diejenigen algebraischen Strukturen vor, die wir in diesem Semester genauer untersuchen werden. ⋇

Verknüpfungen und algebraische Strukturen

Sind A und M zwei Mengen, so bezeichnen wir jede Abbildung der Form $A \times M \to M$ als **Verknüpfung (auf M)**. Oft benutzt man die Symbole $+$ bzw. $\cdot$ bzw. $\circ$ als Bezeichnung für Verknüpfungen.
Man notiert das Bild eines Elements $(a, m) \in A \times M$ unter einer Verknüpfung, indem man die Bezeichnung der Verknüpfung *zwischen* a und m schreibt. Man schreibt also

$$a + m \qquad \text{bzw.} \qquad a \cdot m \qquad \text{bzw.} \qquad a \circ m$$

für das Bild von (a, m) unter der Verknüpfung $+$ bzw. $\cdot$ bzw. $\circ$. Diese sogenannte **Infixnotation** imitiert die aus $\mathbb{R}$ gewohnten Rechennotationen. Speziell beim Verknüpfungszeichen $\cdot$ schreibt man statt $a \cdot b$ oft nur ab.
Die Eigenschaft, dass eine Verknüpfung wieder nach M abbildet, nennt man die **Abgeschlossenheit der Verknüpfung**.
Sind auf einer Menge M Verknüpfungen $f_i : A_i \times M \to M$ (mit $1 \leq i \leq n$) definiert, so bezeichnen wir das Tupel $(M, f_1, \dots, f_n)$ als **algebraische Struktur**. Ist aus dem Kontext klar, welche Verknüpfungen gemeint sind, so schreiben wir für die algebraische Struktur nur M statt $(M, f_1, \dots, f_n)$.

Beispiel 1.1 (a) Jeder Vektorraum V ist eine algebraische Struktur. Die auftretenden Verknüpfungen sind die Vektoraddition $+ : V \times V \to V$ sowie die skalare Multiplikation $\cdot : K \times V \to V$. Beide Verknüpfungen werden durch die Vektorraumaxiome miteinander gekoppelt. Die Menge K bezeichnet den dem Vektorraum V zugrunde liegenden Skalarenkörper.

(b) Weitere Beispiele für algebraische Strukturen werden im Folgenden mit der Gruppe, dem Ring und dem Körper gegeben. Die hier auftretenden Verknüpfungen sind immer von der Form $M \times M \to M$. ⋇

Gruppen

Definition 1.2 *Seien G eine Menge und $\cdot : G \times G \to G$ eine Verknüpfung. G heißt **Gruppe**, falls die folgenden **Gruppenaxiome** erfüllt sind:*

Assoziativität *Für alle $a, b, c \in G$ gilt $(ab)c = a(bc)$.*

Existenz eines Neutralen *Es existiert $e \in G$, so dass $eg = g = ge$ für alle $g \in G$ gilt.*

Existenz von Inversen *Zu jedem $g \in G$ existiert $g' \in G$, so dass $gg' = e = g'g$ gilt.*

*Man nennt G **abelsch** oder **kommutativ**, falls zusätzlich $ab = ba$ für alle $a, b \in G$ gilt.*
*Unter der **Ordnung einer Gruppe G** versteht man die Mächtigkeit $|G| \in \mathbb{N} \cup \{\infty\}$ von G.*

Bemerkung 1.3 Sei G eine Gruppe.

(a) Die Assoziativität in G lässt sich per Induktion auf Produkte beliebiger (endlicher) Länge ausdehnen. Man klammert in Gruppen daher meist überhaupt nicht.

(b) In G existiert nur ein Neutrales; denn sind $e, \tilde{e} \in G$ beide neutral, so gilt

$$e \overset{\tilde{e}\text{ neutral}}{=} e \cdot \tilde{e} \overset{e\text{ neutral}}{=} \tilde{e}.$$

Man spricht daher von **dem Neutralen der Gruppe G**.

(c) Das zu $g \in G$ inverse Element ist eindeutig bestimmt; denn sind $g', \tilde{g}$ beide invers zu g, so gilt

$$g' = g'e = g'(g\tilde{g}) = (g'g)\tilde{g} = e\tilde{g} = \tilde{g}.$$

Man spricht daher von **dem Inversen zu $g \in G$**.

(d) Seien g' das Inverse zu $g \in G$ und g'' das Inverse zu g'. Dann gelten die Gleichungen

$$g \cdot g' = e = g' \cdot g \qquad \text{und} \qquad g'' \cdot g' = e = g' \cdot g''.$$

Diese zeigen: Sowohl das Element g als auch das Element g'' sind invers zu g'. Mit (c) erhalten wir $g = g''$. ⁉

Anders formuliert: Das Inverse eines Inversen ist das ursprüngliche Element; doppeltes Invertieren liefert das Ausgangselement.

(e) Seien $g, h \in G$. Das Inverse zu g sei mit g', das zu h mit h' bezeichnet. Dann ist $h'g'$ das Inverse zu gh, denn es gilt

$$(h'g')(gh) = e = (gh)(h'g').$$

Induktiv sieht man, dass $g'_n g'_{n-1} \cdots g'_1$ das Inverse zu $g_1 g_2 \cdots g_n$ ist. ⁂

Vereinbarung zur Schreibweise 1.4 Man überträgt die aus $\mathbb{R}$ gewohnten Notation wie folgt auf Gruppen:
Ist die Verknüpfung in einer Gruppe G mit $\cdot$ bezeichnet, so nennt man das Neutrale von G **die Eins in G** und schreibt 1 für es. Für das zu $g \in G$ inverse Element schreibt man g^{-1}.
Ist die Verknüpfung in einer Gruppe G mit $+$ bezeichnet, so nennt man das Neutrale von G **die Null in G** und schreibt 0 für es. Für das zu $g \in G$ inverse Element schreibt man $-g$.
Beachten Sie, dass, trotz aller Schreibweisenkonventionen, die Gleichungen $a \cdot b = b \cdot a$ bzw. $a + b = b + a$ in nicht-abelschen Gruppen im Allgemeinen *falsch* sind. ⁂

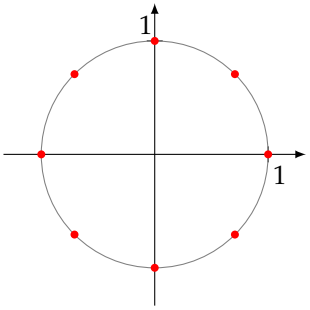
Vereinbarung zur Schreibweise 1.5 Sofern wir nicht explizit ein anderes Gruppenverknüpfungszeichen definieren, benutzen wir das Multiplikationszeichen. ⋇

Die folgenden (Nicht-)Beispiele für Gruppen sollten Ihnen im Laufe Ihres Studiums bereits begegnet sein. Versuchen Sie dennoch, in den einzelnen Beispielen die Gruppenaxiome nachzuweisen oder zu widerlegen:

Beispiel 1.6 (a) Für jeden Vektorraum V ist $(V,+)$ eine abelsche Gruppe. Auch $(\mathbb{Z},+)$, $(\mathbb{R},+)$ und $(\mathbb{C},+)$ sind abelsche Gruppen.

Keine Gruppen sind $(\mathbb{N},+)$ und $(\mathbb{Z}\setminus\{0\},\cdot)$.

(b) Für $n\in\mathbb{N}$ setzen wir $C_n := \left\{\exp\left(\frac{2\pi i}{n}\cdot k\right) \mid k\in\{0,1,\dots,n-1\}\right\}\subseteq\mathbb{C}$.



C_n besteht genau aus den komplexen Zahlen mit Betrag Eins, deren Argument ein ganzzahliges Vielfaches von $\frac{2\pi}{n}$ ist. Alternativ kann man C_n charakterisieren als Lösungsmenge der Gleichung $X^n = 1$ in $\mathbb{C}$. In der Gaußschen Zahlenebene bilden die Elemente von C_n die Ecken eines regelmäßigen n-Ecks, dessen Mittelpunkt im Ursprung liegt und das Eins als Ecke besitzt.
Links sehen Sie in rot die Menge C_8 in die Gaußsche Zahlenebene eingezeichnet.

Mit der Multiplikation $\cdot$ aus $\mathbb{C}$ als Verknüpfung wird C_n zur abelschen Gruppe. (Hierzu ist unter anderem die Abgeschlossenheit von $\cdot$ nachzuweisen, d. h. es ist zu zeigen, dass aus $g,h\in C_n$ auch $g\cdot h\in C_n$ folgt.)

Man nennt C_n auch die **Gruppe der n-ten Einheitswurzeln**. C_n hat Ordnung n.

(c) Für eine nicht-leere Menge M bezeichnen wir mit

$$\mathrm{Sym}(M) := \{f : M\to M \mid f \text{ ist bijektiv}\}$$

die Menge aller Bijektionen von M auf M. Da die Verkettung zweier Bijektionen wieder bijektiv ist, ist die Verkettung $\circ$ von Abbildungen eine Verknüpfung auf $\mathrm{Sym}(M)$. Mit dieser Verknüpfung wird $\mathrm{Sym}(M)$ zu einer Gruppe, der sogenannten **symmetrischen Gruppe auf M**. Die Elemente von $\mathrm{Sym}(M)$ nennt man **Permutationen von M**.

Speziell für $M=\{1,2,\dots,n\}$ mit $n\in\mathbb{N}$ schreibt man S_n statt $\mathrm{Sym}(M)$ und nennt diese Gruppe die **symmetrische Gruppe vom Grad n**. Ihre Ordnung beträgt $n!$

(d) Für jeden Vektorraum V ist

$$\mathrm{GL}(V) := \{f : V\to V \mid f \text{ ist eine bijektive lineare Abbildung}\}$$

mit der Verkettung $\circ$ von Abbildungen eine Gruppe. Man nennt $\mathrm{GL}(V)$ die **allgemeine lineare Gruppe von V**.

Gilt speziell $V=K^n$ mit einem Körper K und $n\in\mathbb{N}$, so schreibt man statt $\mathrm{GL}(V)$ auch $\mathrm{GL}(n,K)$.

(e) Sind G und H zwei Gruppen, so wird durch die Festsetzung

$$(g,h)\cdot(g',h') := (g\cdot g', h\cdot h') \qquad \text{für beliebige } g,g'\in G \text{ und } h,h'\in H$$

eine Verknüpfung auf $G\times H$ definiert, die die Menge $G\times H$ zur Gruppe macht. Man nennt $G\times H$ das **(externe) direkte Produkt von G und H**.

Beachten Sie, dass in der definierenden Gleichung oben das Zeichen $\cdot$ in drei verschiedenen Bedeutungen vorkommt. ⁉

In analoger Weise kann man das direkte Produkt $G_1\times G_2\times\cdots\times G_n$ von $n\in\mathbb{N}$ Gruppen G_i definieren. Man verknüpft dann zwei Elemente aus $G_1\times\cdots\times G_n$ durch komponentenweise Multiplikation.

Direkte Produkte von Gruppen treten beispielsweise in der linearen Algebra auf: Die additive Struktur der n-dimensionalen K-Vektorräume K^n ist gerade das (additiv geschriebene) direkte Produkt $K\times K\times\cdots\times K$ (mit n Faktoren).

Man sieht leicht: Ein direktes Produkt ist genau dann abelsch, wenn jeder Faktor abelsch ist. ⁉ ⁕

Das folgenden Lemma bildet die Grundlage für das Lösen von Gleichungen in Gruppen:

Lemma 1.7 *Multiplikation von links oder rechts mit einem Gruppenelement ist eine Äquivalenzumformung. Genauer: Sind G eine Gruppe und $a,b,c\in G$ Gruppenelemente, so gelten*

$$a=b \iff ac=bc \qquad \textit{sowie} \qquad a=b \iff ca=cb.$$

Beweis. Wir beweisen nur die erste Äquivalenz. Der Beweis der zweiten Äquivalenz erfolgt analog.

„$\Longrightarrow$“ Aus $a=b$ folgt, dass $(a,c)=(b,c)$ für die Paare $(a,c),(b,c)\in G\times G$ gilt. Die Gruppenverknüpfung ist eine Abbildung $G\times G\to G$, ordnet daher gleichen Elementen aus $G\times G$ dasselbe Bild zu. Daher folgt (in Infixnotation) $ac=bc$.

„$\Longleftarrow$“ Aus $ac=bc$ folgt $(ac,c^{-1})=(bc,c^{-1})$. Mit derselben Begründung wie in „$\Longrightarrow$“ folgt $ac\cdot c^{-1}=bc\cdot c^{-1}$, also $a=b$. ■

Bemerkung 1.8 Seien a,b,x,y Gruppenelemente. Mit 1.7 folgt, dass die Gleichungen $ax=b$ bzw. $ya=b$ die eindeutigen Lösungen $x=a^{-1}b$ bzw. $y=ba^{-1}$ besitzen. Im Allgemeinen gilt $x\neq y$. ⁉ ⁕

Wir definieren die Potenzschreibweise:

Vereinbarung zur Schreibweise 1.9 (a) Ist die Verknüpfung in einer Gruppe G mit $\cdot$ bezeichnet, so definiert man für beliebige $g\in G$

$$g^0 := 1 \qquad \text{sowie} \qquad g^n := g\cdot g^{n-1} \text{ und } g^{-n} := (g^{-1})^n \text{ für } n\in\mathbb{N}.$$

Auf diese Weise ist der Ausdruck g^z für alle $z \in \mathbb{Z}$ definiert. Man sieht induktiv, dass für alle $m, n \in \mathbb{Z}$ gilt

$$g^{m+n} = g^m \cdot g^n \qquad \text{sowie} \qquad g^{m \cdot n} = (g^m)^n.$$

Ist G abelsch, so gilt für alle $g, h \in G$ und alle $n \in \mathbb{Z}$ zudem $(gh)^n = g^n \cdot h^n$.

(b) Ist die Verknüpfung in einer Gruppe G mit $+$ bezeichnet, so definiert man für beliebige $g \in G$

$$0 \cdot g := 0 \qquad \text{sowie} \qquad n \cdot g := g + (n-1) \cdot g \text{ und } -n \cdot g := n \cdot (-g) \text{ für } n \in \mathbb{N}.$$

Auf diese Weise ist der Ausdruck $z \cdot g$ für alle $z \in \mathbb{Z}$ definiert. Wieder folgt induktiv für alle $m, n \in \mathbb{Z}$

$$(m+n) \cdot g = m \cdot g + n \cdot g \qquad \text{sowie} \qquad (m \cdot n) \cdot g = m \cdot (n \cdot g).$$

Ist G abelsch, so gilt für alle $n \in \mathbb{Z}$ zudem $n \cdot (g + h) = n \cdot g + n \cdot h$.

(Machen Sie sich klar, was das Zeichen $-$ in den obigen Zeilen bedeutet!) ⁂ ⁉

Ringe und Körper

Definition 1.10 *Seien R eine Menge und $+, \cdot : R \times R \to R$ Verknüpfungen. $(R, +, \cdot)$ heißt* (***kommutativer***) ***Ring*** (***mit Eins***)*, falls die folgenden* ***Ringaxiome*** *gelten:*

additive Gruppe *$(R, +)$ ist eine abelsche Gruppe. Ihr Neutrales bezeichnet man mit 0.*

multiplikative Struktur *$(R, \cdot)$ ist assoziativ und kommutativ, d. h. es gilt $(ab)c = a(bc)$ und $ab = ba$ für alle $a, b, c \in R$. Zudem existiert eine Eins in R, d. h. es gibt ein Element $1 \in R$ mit $1 \cdot r = r = r \cdot 1$ für alle $r \in R$.*

Distributivgesetze *Für alle $a, b, c \in R$ gelten die Distributivgesetze*

$$(a+b) \cdot c = (ac) + (bc) \qquad \textit{und} \qquad a \cdot (b+c) = (ab) + (ac).$$

Ist zusätzlich $(R \setminus \{0\}, \cdot)$ eine Gruppe, so heißt R ***Körper****. Wegen der Kommutativität von $\cdot$ ist $(R \setminus \{0\}, \cdot)$ in diesem Fall abelsch.*

Bemerkung 1.11 (a) In Ringen vereinbart man „Punkt vor Strich“. Mit dieser Konvention sind beispielsweise die Klammern auf den rechten Seiten der obigen Distributivgesetze überflüssig.

(b) In der Literatur wird der Begriff „Ring“ nicht einheitlich verwendet: Manche Autoren verzichten in der Ring-Definition auf die Kommutativität der Multiplikation, andere auf die Existenz der Eins. Achten Sie daher beim Lesen mathematischer Texte darauf, was der Begriff „Ring“ tatsächlich meint.

Für uns ist ein „Ring“ stets ein kommutativer Ring mit Eins in obigem Sinne.

(c) Wie in 1.3 (b) folgt, dass die Eins in Ringen eindeutig ist.

(d) Die Schreibweisen, die wir für Gruppen definiert haben, überträgt man sinngemäß auch auf Ringe. Für ein Ringelement r ist die Potenz r^z im Allgemeinen jedoch nur für $z \in \mathbb{N}_0$ definiert. ⁂ ⁉

Aus den Ringaxiomen folgen zahlreiche Rechenregeln, beispielsweise:

Lemma 1.12 *Seien R ein Ring und $a, b, c \in R$. Dann gelten:*

(a) $0 \cdot a = 0$,

(b) $(-a) \cdot b = -(ab) = a \cdot (-b)$,

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

(d) $(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}$ *für alle $n \in \mathbb{N}_0$. Hierbei bezeichnet $\binom{n}{k}$ den Binomialkoeffizienten n über k.*

Teilweiser Beweis. Die Beweise der obigen Aussagen sind technisch und finden sich beispielsweise in [KM17, Lemma 13.1 auf S. 172]. Wir zeigen beispielhaft die Aussage in (a): Es gilt $0 \cdot a = (0+0) \cdot a = 0 \cdot a + 0 \cdot a$. Wir addieren nun $-0 \cdot a$ auf diese Gleichung und erhalten $0 = 0 \cdot a$. ■

Bemerkung 1.13 In Ringen kann $1 = 0$ gelten. Ist R ein Ring mit dieser Eigenschaft, so gilt $R = \{0\}$, denn für alle $r \in R$ gilt

$$r = 1 \cdot r \overset{1=0}{=} 0 \cdot r \overset{1.12\,(a)}{=} 0.$$

Dies bedeutet umgekehrt: Enthält ein Ring R mehr als ein Element, so gilt $1 \neq 0$ in R.
In Körpern K gilt stets $1 \neq 0$; denn wäre $1 = 0$ in K, so folgte nach obigem $K = \{0\}$. Dies widerspräche aber der Körperdefinition, denn die leere Menge $K \setminus \{0\} = \emptyset$ ist keine Gruppe bezüglich der Multiplikation. ⁉
Körper enthalten also mindestens zwei Elemente, nämlich Null und Eins. ⁂

Weiß man bereits, dass eine algebraische Struktur K ein Ring ist, so müssen zum Nachweis der Körperstruktur von K nicht alle Gruppenaxiome für $(K \setminus \{0\}, \cdot)$ gezeigt werden:

Lemma 1.14 *Für einen Ring K sind äquivalent:*

(a) *K ist ein Körper.*

(b) *In K gilt $1 \neq 0$, und zu jedem $k \in K \setminus \{0\}$ existiert ein $k' \in K$ mit $kk' = 1$.*

Beweis.

(a)$\Longrightarrow$(b) folgt direkt aus der Definition des Körperbegriffs.

(b)$\Longrightarrow$(a) Wir zeigen, dass $(K \setminus \{0\}, \cdot)$ eine abelsche Gruppe ist:

Aufgrund der Ringaxiome ist $\cdot$ kommutativ und assoziativ. Ferner ist $1 \in K \setminus \{0\}$ multiplikativ neutral. Es ist noch zu zeigen, dass jedes $k \in K \setminus \{0\}$ ein multiplikativ Inverses **in $K \setminus \{0\}$** besitzt und dass durch $\cdot$ eine Verknüpfung der Form $K \setminus \{0\} \times K \setminus \{0\} \to K \setminus \{0\}$ gegeben wird.

Wir starten mit der Existenz von Inversen: Zu $k \in K \setminus \{0\}$ existiert nach Voraussetzung $k' \in K$ mit $kk' = 1$. Wäre $k' \notin K \setminus \{0\}$, so wäre $k' = 0$ und daher $kk' = 0 \neq 1$, was widersprüchlich ist. Also gilt $k' \in K \setminus \{0\}$.

Nun zeigen wir, dass das Produkt zweier Elemente aus $K \setminus \{0\}$ wieder in $K \setminus \{0\}$ liegt. Hierzu nehmen wir an, dass $a \cdot b = 0$ für zwei Elemente $a, b \in K \setminus \{0\}$ gelte. Sei $a' \in K \setminus \{0\}$ das Inverse von a. Dann folgt der Widerspruch

$$ab = 0 \Longrightarrow a' \cdot ab = a' \cdot 0 \overset{1.12\,(a)}{\Longrightarrow} b = 0.$$

Dies beendet den Beweis. ■

Beispiel 1.15 (a) Die ganzen Zahlen $\mathbb{Z}$ bilden einen Ring, $\mathbb{Q}$, $\mathbb{R}$ und $\mathbb{C}$ sind Körper.

(b) In Vorlesung 4 lernen wir mit den Ringen $\mathbb{Z}_n$ eine wichtige Klasse von Ringen kennen.

(c) Man definiert das **(externe) direkte Produkt $R_1 \times \cdots \times R_n$ der Ringe R_i** analog zu 1.6 (e); man verknüpft wieder komponentenweise.

(d) Sei K ein Körper. Die Menge aller Folgen auf K bezeichnen wir mit $K^{\mathbb{N}}$. Für Elemente $a = (a_1, a_2, \ldots)$ und $b = (b_1, b_2, \ldots)$ aus $K^{\mathbb{N}}$ setzen wir

$$a + b := (a_1 + b_1, a_2 + b_2, \ldots) \qquad \text{sowie} \qquad a \cdot b := (a_1 \cdot b_1, a_2 \cdot b_2, \ldots).$$

Mit diesen Verknüpfungen wird $K^{\mathbb{N}}$ zum Ring. Man kann $K^{\mathbb{N}}$ als ein direktes Produkt mit unendlich vielen Faktoren auffassen, vgl. (c).

Können Sie die Null bzw. die Eins in $K^{\mathbb{N}}$ angeben? Welche Elemente aus $K^{\mathbb{N}}$ sind multiplikativ invertierbar? ⁉

(e) Der Vollständigkeit halber geben wir Beispiele für algebraische Strukturen, die – je nach Autor – als Ring bezeichnet werden, vgl. 1.11 (b):

Die Menge $2\mathbb{Z} := \{2z \mid z \in \mathbb{Z}\}$ bildet mit der gewöhnlichen Addition und Multiplikation einen kommutativen Ring ohne Eins.

Für jeden Körper K und jedes $n \geq 2$ bildet die Menge $K^{n \times n}$ aller $(n \times n)$-Matrizen mit Einträgen aus K zusammen mit der gewöhnlichen Matrixaddition und -multiplikation einen nicht-kommutativen Ring mit Eins. Die Nicht-Kommutativität bezieht sich hierbei auf die Ringmultiplikation. Die Einheitsmatrix ist die Eins des Rings. ⁕

2. Unterstrukturen, Erzeugnisse

Worum geht es? Wir beschäftigen uns mit *Unterstrukturen* einer algebraischen Struktur und stellen Kriterien bereit, mit denen man Mengen auf Unterstruktur-Eigenschaft testen kann. Als Vorbild dient uns hierbei das aus der linearen Algebra bekannte Konzept der Untervektorraums.
Danach definieren wir, was wir unter einem *Erzeugnis* verstehen wollen. Speziell im Falle von Gruppenerzeugnissen klären wir zudem, wie die Elemente in einem Erzeugnis aussehen. Wir lernen zudem den wichtigen Begriff der *zyklischen Gruppe* kennen. ⋇

Unterstrukturen und Unterstrukturkriterien

Sei $(M, f_1, \dots, f_n)$ eine algebraische Struktur. Wir nennen eine Teilmenge $U \subseteq M$ eine **Unterstruktur von M**, wenn die folgenden Bedingungen erfüllt sind:

Abgeschlossenheit Das Verknüpfen zweier Elemente aus U mit den Verknüpfungen f_i der Struktur M führt nicht aus U heraus. Wir können äquivalent formulieren: Durch Einschränkung der f_i auf U entstehen Verknüpfungen $f_i|_U$ auf U.

gleiche Axiome Die algebraischen Strukturen $(M, f_1, \dots, f_n)$ und $(U, f_1|_U, \dots, f_n|_U)$ genügen denselben Axiomen.

gleiche Neutrale Alle Neutralen aus M sind auch in U enthalten (und dort natürlich ebenfalls neutral). ⁉

Ist U eine Unterstruktur von M, so schreiben wir $U \leq M$.

Beispiel 2.1 (a) Sei V ein K-Vektorraum. Die Vektoraddition in V bezeichnen wir mit $+$, mit $\cdot$ notieren wir die skalare Multiplikation. Ein Untervektorraum von V ist eine Teilmenge $U \subseteq V$, so dass

Abgeschlossenheit die Einschränkungen $+|_U : U \times U \to U$ und $\cdot|_U : K \times U \to U$ Verknüpfungen auf U sind,

gleiche Axiome U mit diesen Verknüpfungen zu einem K-Vektorraum wird und

gleiche Neutrale $0 \in U$ gilt, wobei 0 den Nullvektor aus V bezeichnet.

(b) Jede algebraische Struktur ist Unterstruktur von sich selbst. ⁉

(c) Unterstrukturbildung ist **transitiv** im folgenden Sinne: Sind A, B, C algebraische Strukturen und gelten $A \leq B$ sowie $B \leq C$, so gilt auch $A \leq C$. ⋇

Wir interessieren uns speziell für Unterstrukturen von Gruppen, Ringen und Körpern. Für diese Spezialfälle konkretisieren wir die allgemeine Unterstruktur-Beschreibung:

Definition 2.2 *Sei G eine Gruppe mit Neutralem 1_G. Eine Teilmenge $U \subseteq G$ heißt **Untergruppe von G**, falls die Einschränkung $\cdot|_U : U \times U \to U$ zu einer Verknüpfung auf U wird, die U zu einer Gruppe mit Einselement 1_G macht. Hieraus folgt insbesondere, dass $1_G \in U$ gilt.* ⁉

*Die Begriffe **Unterring** und **Unterkörper** definieren wir analog.*

Zum Nachweis der Unterstruktur-Eigenschaft muss man einige der obigen Punkte nicht vollständig überprüfen, denn typischerweise „vererben“ sich Eigenschaften der Ausgangsstruktur auf Teilmengen. Die nachstehenden Unterstruktur-Kriterien zeigen, was zum Unterstruktur-Nachweis tatsächlich noch zu tun ist:

Satz 2.3 (Untergruppenkriterium) *Seien G eine Gruppe und $U \subseteq G$ eine Teilmenge von G. Dann sind äquivalent:*

(a) *U ist eine Untergruppe von G.*

(b) *Das **Untergruppenkriterium** ist erfüllt: U ist nicht-leer, und für alle $g, h \in U$ gelten $g \cdot h \in U$ sowie $g^{-1} \in U$.*

Die hierbei auftretenden Verknüpfungen sind die Verknüpfungen aus G.

Beweis.

(a)$\Longrightarrow$(b) Sei U eine Untergruppe von G. Wir bezeichnen das Neutrale von G und U mit 1.

Es ist $1 \in U$ und somit $U \neq \emptyset$. Weiter ist die Einschränkung der Gruppenverknüpfung $\cdot$ von G auf U eine Verknüpfung auf U, d. h. es gilt $g \cdot h \in U$ für alle $g, h \in U$. Zuletzt gilt $g^{-1} \in U$ für alle $g \in U$, denn g muss in U ein Inverses besitzen. Für dieses kommt aber aufgrund der Eindeutigkeit in 1.3 (c) nur das Inverse g^{-1} von g in G in Frage. Also gilt $g^{-1} \in U$.

(b)$\Longrightarrow$(a) U erfülle nun das Untergruppenkriterium. Wir müssen zeigen, dass U eine Untergruppe von G ist:

Da für alle $g, h \in U$ auch $gh \in U$ gilt, lässt sich die Verknüpfung $\cdot$ von G zu einer Verknüpfung $U \times U \to U$ einschränken.

Weil U nach Voraussetzung nicht-leer ist, existiert $g \in U$. Wir wissen, dass ebenfalls $g^{-1} \in U$ gilt. Wegen der Abgeschlossenheit von U folgt $1 = g \cdot g^{-1} \in U$. Also enthält U das Neutrale aus G.

Zuletzt ist zu zeigen, dass U die Gruppenaxiome erfüllt. Offenbar enthält U ein Neutrales sowie ein Inverses zu jedem Element. Es ist also nur noch zu zeigen, dass die Verknüpfung auf U assoziativ ist. Dies folgt aber aus der Assoziativität der Verknüpfung auf G: Für alle $a, b, c \in G$ gilt $(ab)c = a(bc)$. Dies gilt sicherlich auch noch, wenn wir $a, b, c \in U$ fordern.

Insgesamt ist damit gezeigt, dass U eine Untergruppe von G ist. ■

Beispiel 2.4 (a) Sei G eine Gruppe mit Neutralem 1. Dann ist $\{1\}$ eine Untergruppe von G. Man nennt $\{1\}$ auch die **triviale Untergruppe von G**. Aus 2.1 (b) wissen wir bereits, dass auch G eine Untergruppe von G ist.

(b) Aus dem Untergruppenkriterium folgt direkt $2\mathbb{Z} < \mathbb{Z} < \mathbb{Q} < \mathbb{R} < \mathbb{C}$.

Welche Gruppenverknüpfung haben wir hierbei betrachtet? ⁉

(c) Jeder Untervektorraum eines Vektorraums V ist eine Untergruppe von V.
Ist auch jede Untergruppe von V ein Untervektorraum von V? ⁉

(d) Für jeden Vektorraum V gilt $\mathrm{GL}(V) \leq \mathrm{Sym}(V)$.

(e) Für einen Körper K und $n \in \mathbb{N}$ verstehen wir unter der **speziellen linearen Gruppe von K^n** die Menge

$$\mathrm{SL}(n, K) := \{A \in K^{n \times n} \mid \det(A) = 1\}$$

aller $(n \times n)$-Matrizen mit Einträgen aus K und Determinante Eins. $\mathrm{SL}(n, K)$ ist tatsächlich eine Gruppe, denn es gilt $\mathrm{SL}(n, K) \leq \mathrm{GL}(n, K)$; für den Nachweis dieser Behauptung benötigt man den Determinantenmultiplikationssatz. ⁉ ⁂

Bemerkung 2.5 In Teil (e) des Beispiels haben wir die Gruppenstruktur von $\mathrm{SL}(n, K)$ gezeigt, indem wir gesehen haben, dass $\mathrm{SL}(n, K)$ eine *Untergruppe* der Gruppe $\mathrm{GL}(n, K)$ ist. Statt die Gruppenaxiome direkt nachzuweisen (was oft arbeitsintensiv ist), haben wir eine uns bekannte Obergruppe gewählt und dann das deutlich einfachere Untergruppenkriterium verifiziert.
Diese Strategie sollten Sie möglichst oft verwenden: Statt direkt zu beweisen, dass eine Menge U eine algebraische Struktur ist und gewissen Axiomen genügt, sollten Sie zuerst versuchen, U als *Unterstruktur* einer passenden Struktur nachzuweisen. ⁂

Mit ähnlichen Schlussweisen wie im Untergruppenkriterium folgt:

Satz 2.6 (Unterringkriterium) *Seien R ein Ring und $U \subseteq R$ eine Teilmenge von R. Dann sind äquivalent:*

(a) *U ist ein Unterring von R.*

(b) *Das **Unterringkriterium** ist erfüllt: U enthält die Null und die Eins aus R, und für alle $r, s \in U$ gilt $r + s, rs, -r \in U$.*
Die hierbei auftretenden Verknüpfungen sind die Verknüpfungen aus R.

Beispiel 2.7 (a) Sei R ein Ring. Gilt $R \neq \{0\}$, so ist $\{0\}$ kein Unterring von R, da diese Menge die Eins aus R nicht enthält.

(b) Die Menge $\{(z, 0) \mid z \in \mathbb{Z}\}$ ist zwar ein Ring, aber kein Unterring von $\mathbb{Z} \times \mathbb{Z}$. ⁉

(c) Sei K ein Körper. Die Menge aller fast immer konstanten Folgen auf K ist ein Unterring von $K^{\mathbb{N}}$.
Für $K = \mathbb{R}$ oder $K = \mathbb{C}$ ist auch die Menge der konvergenten Folgen auf K ein Unterring von $K^{\mathbb{N}}$. Kein Unterring, aber eine Untergruppe von $K^{\mathbb{N}}$ ist die Menge der Nullfolgen auf K. ⁉ ⁂

Aus dem Unterringkriterium folgt:

Satz 2.8 (Unterkörperkriterium) *Seien K ein Körper und $U \subseteq K$ eine Teilmenge von K. Dann sind äquivalent:*

(a) *U ist ein Unterkörper von K.*

(b) *Das **Unterkörperkriterium** ist erfüllt: U enthält die Null und die Eins aus K, für alle $r, s \in U$ gilt $r + s, rs, -r \in U$ und, falls $r \neq 0$, auch $r^{-1} \in U$.*

Die hierbei auftretenden Verknüpfungen sind die Verknüpfungen aus K.

Beispiel 2.9 Die Menge $K := \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$ ist ein Unterkörper von $\mathbb{R}$. Können Sie nachweisen, dass $(a + b\sqrt{2})^{-1}$ für $(a, b) \neq (0, 0)$ in K liegt? ⁉

Erzeugnisse

Seien $(M, f_1, \ldots, f_n)$ eine algebraische Struktur und $A \subseteq M$ eine beliebige Teilmenge von M. Unter einem **Erzeugnis von A in M** verstehen wir jede minimale Unterstruktur von M, die A als Teilmenge enthält. Der Begriff „minimal" bezieht sich hierbei auf die Mengeninklusion: Ist E ein Erzeugnis von A in M, so gibt es keine Unterstruktur U von M, die eine *echte Teilmenge* von E ist und A enthält. Anders formuliert: Gilt $A \subseteq U \leq E$, so folgt $U = E$.
Erzeugnisse von A in M sind daher die (bezüglich Mengeninklusion) kleinsten Unterstrukturen von M, die A enthalten.

Im Allgemeinen müssen Erzeugnisse einer Teilmenge A weder existieren noch, im Falle ihrer Existenz, eindeutig bestimmt sein. In Gruppen, Ringen und Körpern existiert zu jeder Teilmenge A jedoch genau ein Erzeugnis. Der Beweis dieser Tatsache beruht auf der folgenden Beobachtung:

Lemma 2.10 *Seien G eine Gruppe, I eine Indexmenge und U_i mit $i \in I$ Untergruppen von G. Dann ist auch $\bigcap_{i \in I} U_i$ eine Untergruppe von G.*
Dies können wir kürzer formulieren: Der Schnitt von Untergruppen ist wieder eine Untergruppe.

Eine analoge Aussage gilt auch für den Schnitt von Unterringen eines Rings bzw. Unterkörpern eines Körpers.

Beweis. Wir zeigen nur die Gruppenaussage. Der Beweis im Ring- bzw. Körperfall funktioniert ähnlich.
Setze $U := \bigcap_{i \in I} U_i$. Wir zeigen mit dem Untergruppenkriterium, dass $U \leq G$ gilt:
Da die U_i Untergruppen von G sind, gilt $1 \in U_i$ für alle $i \in I$. Daher gilt auch $1 \in U$, was $U \neq \emptyset$ zeigt.
Seien nun $g, h \in U$. Dann folgt $g, h \in U_i$ für alle $i \in I$. Aus der Gruppenstruktur der U_i folgt $gh, g^{-1} \in U_i$ für alle $i \in I$. Somit gilt $gh, g^{-1} \in U$. ■

Aus 2.10 folgt die nachstehende Beschreibung für Erzeugnisse in Gruppen, Ringen und Körpern:

Definition/Satz 2.11 *Seien M eine Gruppe, ein Ring oder ein Körper und $A \subseteq M$ eine Teilmenge von M. Wir bezeichnen die Schnittmenge aller Unterstrukturen von M, die A enthalten, mit $\langle A \rangle$, setzen also*

$$\langle A \rangle = \bigcap_{\substack{U \text{ ist Unterstruktur von } M \\ \text{mit } A \subseteq U}} U.$$

*Dann gilt $\langle A \rangle \leq M$. Zudem ist $\langle A \rangle$ in jeder Unterstruktur von M, die A enthält, enthalten. Dies zeigt, dass $\langle A \rangle$ ein Erzeugnis von A in M ist, und zwar das einzige. **Das** Erzeugnis von A in M ist also eindeutig durch $\langle A \rangle$ gegeben.*
*Gilt $\langle A \rangle = M$, so nennen wir A ein **Erzeugendensystem für M**. Besitzt M ein Erzeugendensystem A, das nur endlich viele Elemente enthält, so nennen wir M **endlich erzeugt**.*

Beweis. Wegen 2.10 ist $\langle A \rangle$ eine Unterstruktur von M. Weil $A \subseteq U$ für alle Mengen U, über die geschnitten wird, gilt, folgt $A \subseteq \langle A \rangle$. Daher ist $\langle A \rangle$ eine Unterstruktur von M, die A enthält.
Da $\langle A \rangle$ als Schnitt über *alle* Unterstrukturen von M, die A enthalten, entsteht, ist $\langle A \rangle$ eine Teilmenge aller dieser Strukturen. $\langle A \rangle$ ist daher die bezüglich Mengeninklusion kleinste Unterstruktur, die A enthält, und durch obige Formel eindeutig gegeben, also *das* Erzeugnis von A in M. ■

Aus 2.11 folgt sofort:

Korollar 2.12 *Seien M eine Gruppe, ein Ring oder ein Körper und $A, B \subseteq M$ Teilmengen von M. Dann gilt: Ist A eine Teilmenge von B, so ist $\langle A \rangle$ eine Unterstruktur von $\langle B \rangle$.*

2.11 liefert zwar eine konkrete Beschreibung von $\langle A \rangle$, jedoch erkennt man anhand dieser Beschreibung nicht, wie die Elemente aus $\langle A \rangle$ aussehen. Für Gruppenerzeugnisse klärt dies der folgende Satz:

Satz 2.13 (Explizite Beschreibung des Gruppenerzeugnisses) *Seien G eine Gruppe und A eine Teilmenge von G. Dann gilt*

$$\langle A \rangle = \{a_1^{e_1} \cdot a_2^{e_2} \cdots a_n^{e_n} \mid n \in \mathbb{N}_0, a_i \in A \text{ und } e_i \in \{\pm 1\} \text{ für } 1 \leq i \leq n\}.$$

$\langle A \rangle$ besteht also aus allen endlichen Produkten von Elementen aus A und den Inversen von Elementen aus A.
Konvention: Leere Produkte, d. h. Produkte, bei denen $n = 0$ gilt, haben Wert Eins. Es gilt also insbesondere $\langle \emptyset \rangle = \{1\}$.

Beweis. Wir bezeichnen mit U die Menge auf der rechten Seite der obigen Gleichung und zeigen $\langle A \rangle = U$ durch Nachweis der Inklusionen $\langle A \rangle \subseteq U$ und $U \subseteq \langle A \rangle$:

$\langle A \rangle \subseteq U$ Das Untergruppenkriterium zeigt, dass $U \leq G$ gilt. Weiter gilt $A \subseteq U$ (für $n = 1$ und $e_1 = 1$). U ist daher eine Untergruppe, die A enthält. Mit 2.11 folgt $\langle A \rangle \subseteq U$. ⁉

$U \subseteq \langle A \rangle$ Nach Definition ist $A \subseteq \langle A \rangle$. Da in der Gruppe $\langle A \rangle$ invertiert werden kann, gilt $a^{-1} \in \langle A \rangle$ für alle $a \in A$. Zudem ist $\langle A \rangle$ multiplikativ abgeschossen, was zeigt, dass $\langle A \rangle$ alle endlichen Produkte von Elementen aus A oder deren Inversen enthält. Dies sind aber genau die Elemente, aus denen U besteht, was $U \subseteq \langle A \rangle$ zeigt. ■

Bemerkung 2.14 Wird G additiv geschrieben, so gilt

$$\langle A\rangle = \{e_1 \cdot a_1 + e_2 \cdot a_2 + \cdots + e_n \cdot a_n \mid n \in \mathbb{N}_0, a_i \in A \text{ und } e_i \in \{\pm 1\} \text{ für } 1 \leq i \leq n\}.$$

Leere Summen haben den Wert Null. ⁜

Speziell für abelsche Gruppen und endliche Mengen A lässt sich 2.13 vereinfachen:

Korollar 2.15 *Seien G eine abelsche Gruppe und $A = \{a_1, \dots, a_n\}$ eine endliche Menge. Dann gilt*

$$\langle A\rangle = \{a_1^{z_1} \cdot a_2^{z_2} \cdots a_n^{z_n} \mid z_1, \dots, z_n \in \mathbb{Z}\}.$$

Beweisskizze. Aufgrund der Kommutativität von G können wir die in 2.13 auftretenden Produkte sortieren und die Faktoren nach 1.9 zusammenfassen. Nicht-vorkommende Elemente aus A fügen wir hinzu, indem wir Null als Exponenten wählen. ■

Ein wichtiger Spezialfall von 2.13 ist das Erzeugnis einer einelementigen Menge:

Korollar 2.16 *Sei g ein Gruppenelement. Dann gilt*

$$\langle g\rangle = \{g^z \mid z \in \mathbb{Z}\} = \{\dots, g^{-2}, g^{-1}, 1, g, g^2, \dots\}.$$

Man schreibt hierfür auch kürzer $\langle g\rangle = g^{\mathbb{Z}}$.

Bemerkung 2.17 Wird G additiv geschrieben, so gilt in den beiden obigen Korollaren

$$\langle A\rangle = \{z_1 \cdot a_1 + \cdots + z_n \cdot a_n \mid z_i \in \mathbb{Z}\} \qquad \text{bzw.} \qquad \langle g\rangle = \{z \cdot g \mid z \in \mathbb{Z}\}.$$

Im Falle des rechten Erzeugnisses schreibt man oft kürzer $\langle g\rangle = \mathbb{Z}g$. ⁜

Gruppen, die ein einelementiges Erzeugendensystem besitzen, sind für die Gruppentheorie grundlegend. Man gibt ihnen einen eigenen Namen:

Definition 2.18 *Eine Gruppe G heißt **zyklisch**, wenn sie ein einelementiges Erzeugendensystem besitzt, d.h. wenn $g \in G$ mit $G = \langle g\rangle$ existiert. Jedes solche g heißt **Erzeuger von G**. Aufgrund der Potenzrechenregeln 1.9 sind zyklische Gruppen stets abelsch.*

Beispiel 2.19 (a) Für jede Gruppe G gilt $\langle G\rangle = G$. Jede Gruppe besitzt also mindestens ein Erzeugendensystem.

(b) Die Gruppe $(\mathbb{R}, +)$ ist nicht endlich erzeugt, denn $\mathbb{R}$ ist überabzählbar. ⁉

Auch $(\mathbb{Q}, +)$ ist nicht endlich erzeugt; denn ansonsten gäbe es eine endliche Menge von Brüchen $\left\{\frac{p_1}{q_1}, \frac{p_2}{q_2}, \dots, \frac{p_n}{q_n}\right\}$ mit $p_i \in \mathbb{Z}$ und $q_i \in \mathbb{N}$, die $\mathbb{Q}$ erzeugte. Dann wäre

$$\left\langle \frac{p_1}{q_1}, \frac{p_2}{q_2}, \dots, \frac{p_n}{q_n}\right\rangle \overset{2.15}{=} \left\{z_1 \cdot \frac{p_1}{q_1} + \cdots + z_n \cdot \frac{p_n}{q_n} \mid z_i \in \mathbb{Z}\right\}$$

$$\overset{\text{auf Hauptnenner bringen}}{=} \left\{\frac{z}{q_1 \cdot q_2 \cdots q_n} \mid \text{für gewisse } z \in \mathbb{Z}\right\}.$$

Dieses Erzeugnis ist aber eine echte Teilmenge von $\mathbb{Q}$; beispielsweise liegt der Bruch $\frac{1}{q_1 \cdots q_n + 1}$ nicht in obigem Erzeugnis. ⁉

(c) Es gilt $\mathbb{Z} = \langle 1 \rangle = \langle -1 \rangle$. Die Gruppe $\mathbb{Z}$ ist daher zyklisch. Sie besitzt genau die beiden Erzeuger ± 1.

Es gilt ebenfalls $\mathbb{Z} = \langle 2, 3 \rangle$, denn es ist $1 = 3 - 2 \in \langle 2, 3 \rangle$. Weiter folgt $\langle 2 \rangle \neq \mathbb{Z} \neq \langle 3 \rangle$.

Somit sind die Mengen $\{1\}$ und $\{2, 3\}$ jeweils minimale (bezüglich Mengeninklusion) Erzeugendensysteme für $\mathbb{Z}$. Allerdings besitzen sie eine unterschiedliche Anzahl von Elementen. Dies zeigt, dass sich der Dimensions- und der Basisbegriff aus der linearen Algebra nicht in die Gruppentheorie übertragen: Verschiedene minimale Erzeugendensysteme haben in der Gruppentheorie im Allgemeinen unterschiedliche Mächtigkeiten.

(d) Die Gruppen C_n aus 1.6 (b) sind zyklisch. Es ist $C_n = \langle \exp(\frac{2\pi i}{n}) \rangle$.

Hieraus können wir folgern, dass $C_m \leq C_n$ genau dann gilt, wenn m ein Teiler von n ist. Der Übersichtlichkeit halber schreiben wir im Folgenden $\zeta_n := \exp(\frac{2\pi i}{n})$. Es gilt also $C_n = \langle \zeta_n \rangle$.

ζ
Zeta

$\Longrightarrow$ Es gelte $C_m \leq C_n$. Dann ist ζ_m ein Element des Erzeugnisses $\langle \zeta_n \rangle = \zeta_n^{\mathbb{Z}}$. Es existiert also $k \in \mathbb{Z}$ mit

$$\zeta_m = \zeta_n^k, \quad \text{also mit } \exp\Big(\frac{2\pi i}{m}\Big) = \exp\Big(\frac{2\pi i k}{n}\Big), \quad \text{also mit } \frac{1}{m} = \frac{k}{n}.$$

Es folgt $n = km$, was zeigt, dass m ein Teiler von n ist.

$\Longleftarrow$ Sei nun m ein Teiler von n. Dann existiert ein $k \in \mathbb{N}$ mit $km = n$, also mit $\frac{1}{m} = \frac{k}{n}$. Die gleiche Schlussweise wie in der Hinrichtung zeigt $\zeta_m = \zeta_n^k$ und somit $\zeta_m \in C_n$. Mit 2.12 erhalten wir $C_m = \langle \zeta_m \rangle \leq \langle C_n \rangle = C_n$. ⋇

Auch für die Elemente in Ring- und Körpererzeugnissen gibt es explizite Darstellungen, die man ähnlich wie 2.13 beweist. Nachstehend geben wir eine explizite Beschreibung des Ringerzeugnisses:

Satz 2.20 *Seien R ein Ring und A eine Teilmenge von R. Dann gilt*

$$\langle A \rangle = \left\{ \sum_{i=1}^{n} \Big(e_i \cdot \prod_{k=1}^{s_i} a_{i,k} \Big) \mid n \in \mathbb{N}_0, s_1, \ldots, s_n \in \mathbb{N}_0, e_i \in \{\pm 1\} \text{ und } a_{i,k} \in A \right\}.$$

$\langle A \rangle$ besteht also aus allen endlichen Summen bzw. Differenzen von endlichen Produkten von Elementen aus A.
Konvention: Leere Produkte haben Wert Eins, leere Summen den Wert Null. Stets gilt $0 \in \langle A \rangle$ (für $n = 0$) und $1 \in \langle A \rangle$ (für $n = 1$, $e_1 = 1$ und $s_1 = 0$).

3. Die ganzen Zahlen

Worum geht es? Wir beschäftigen und zunächst mit den Eigenschaften der Multiplikation in $\mathbb{Z}$ und zeigen, dass in $\mathbb{Z}$ eine *Division mit Rest* existiert. Hieraus leiten wir das *Lemma von Bézout* her, klassifizieren die Untergruppen von $\mathbb{Z}$ und zeigen die Existenz einer eindeutigen Primfaktorzerlegung in $\mathbb{Z}$. ⁜

Die multiplikative Struktur von $\mathbb{Z}$

Mit Hilfe der folgenden Begriffe lässt sich die multiplikative Struktur von $\mathbb{Z}$ beschreiben:

Definition 3.1 *Seien $a, b \in \mathbb{Z}$.*

(a) *a heißt **Teiler von b**, falls $k \in \mathbb{Z}$ existiert, so dass $ak = b$ gilt. In diesem Fall nennt man b auch ein **Vielfaches von a**.*

Ist a ein Teiler von b, so schreiben wir $a \mid b$, ansonsten $a \nmid b$.

(b) *a heißt **Primzahl**, falls $a \geq 2$ gilt und 1 und a die einzigen positiven Teiler von a sind.*

Die Menge der Primzahlen bezeichnen wir mit $\mathbb{P}$. Es gilt $\mathbb{P} \subseteq \mathbb{N}$ und $1 \notin \mathbb{P}$.

Bemerkung 3.2 (a) Gilt $a \mid b$ für $a \neq 0$, so ist die ganze Zahl k mit $ak = b$ eindeutig durch a und b bestimmt. Man nennt k oft den **Koteiler zu a**. Es gilt $k \mid b$.

(b) Teilt a jede der Zahlen $b_1, \dots, b_n \in \mathbb{Z}$, so teilt a auch jede der $\mathbb{Z}$-Linearkombinationen $\sum_{i=1}^{n} \lambda_i b_i$ mit $\lambda_i \in \mathbb{Z}$.

(c) Für alle $a \in \mathbb{Z}$ gilt $a \mid 0$. Umgekehrt gilt $0 \mid a$ genau dann, wenn $a = 0$ ist.

(d) Für $a, b \in \mathbb{Z}$ gilt $a \mid b$ und $b \mid a$ genau dann, wenn $b = \pm a$ ist. ⁉

(e) Die zyklische Untergruppe $\langle a \rangle = a\mathbb{Z}$ von $\mathbb{Z}$ besteht genau aus den Vielfachen von a. Für $a, b \in \mathbb{Z}$ folgt hieraus

$$\langle a \rangle \subseteq \langle b \rangle \iff a \in \langle b \rangle \iff b \mid a.$$

Dies umschreibt man manchmal mit der Formulierung *Teilen heißt Umfassen*. ⁉

(f) Mit (e) und 3.4 können wir eine alternative Charakterisierung von Primzahlen angeben: Eine natürliche Zahl $a \geq 2$ ist eine Primzahl genau dann, wenn $\mathbb{Z}$ die einzige echte Obergruppe von $\langle a \rangle$ ist. ⁜

Eine wichtige Eigenschaft des Rings der ganzen Zahlen ist, dass dort eine Division mit Rest möglich ist:

Satz 3.3 *Auf $\mathbb{Z}$ existiert eine Division mit Rest in folgendem Sinne: Zu beliebigen $a \in \mathbb{Z}$ und $n \in \mathbb{N}$ existieren $q \in \mathbb{Z}$ und $r \in \{0, 1, \dots, n-1\}$, so dass $a = q \cdot n + r$ gilt. q und r sind durch a und n eindeutig festgelegt.*
*Man schreibt $a \operatorname{div} n$ für q und nennt q den **Ganzzahlquotienten von a und n**. Für r schreibt man $a \bmod n$ und nennt r den **Rest von a modulo n**.*

Beweis.

Existenz Es bezeichne $\lfloor\cdot\rfloor : \mathbb{R} \to \mathbb{Z}$ das Abrunden auf die nächstkleinere ganze Zahl. Wir setzen $q := \lfloor \frac{a}{n} \rfloor$ und $r := n\cdot(\frac{a}{n} - q)$. Wegen $q \in \mathbb{Z}$ gilt $r = n\cdot(\frac{a}{n} - q) = a - qn \in \mathbb{Z}$. Weiter gilt $\frac{a}{n} - q \in [0,1[$ und daher $r = n \cdot (\frac{a}{n} - q) \in [0,n[$. Zusammen folgt $r \in \mathbb{Z} \cap [0,n[= \{0,1,\dots,n-1\}$. Umstellen der definierenden Gleichung für r liefert $a = q \cdot n + r$ und zeigt die Existenz einer Division mit Rest auf $\mathbb{Z}$.

Eindeutigkeit Gilt $qn + r = a = q'n + r'$ mit $q, q' \in \mathbb{Z}$ und $r, r' \in \{0,\dots,n-1\}$, so folgt $(q - q') \cdot n = r' - r$.

Es ist $r' - r \in \{-(n-1),\dots,n-1\}$. Die Differenz $r - r'$ wird daher genau dann von n geteilt, wenn $r' - r = 0$ gilt. Dies zeigt $q - q' = 0$. Insgesamt folgt die Eindeutigkeit im Satz auftauchenden Parameter q und r. ■

Wir können nun alle Untergruppen von $(\mathbb{Z}, +)$ klassifizieren:

Satz 3.4 *Die Untergruppen von $\mathbb{Z}$ sind von der Form $\langle n\rangle$, wobei $n \in \mathbb{N}_0$ beliebig ist; insbesondere sind alle Untergruppen von $\mathbb{Z}$ zyklisch.*
Die Untergruppe $\langle n\rangle$ von $\mathbb{Z}$ besitzt genau die Erzeuger $\pm n$. Bis auf die triviale Untergruppe $\{0\}$ haben daher alle Untergruppen von $\mathbb{Z}$ genau zwei Erzeuger.

Beweis. Sei $U \leq \mathbb{Z}$ eine beliebige Untergruppe von $\mathbb{Z}$. Gilt $U = \{0\}$, so können wir U schreiben in der Form $U = \langle 0\rangle$. Offenbar ist Null der einzige Erzeuger dieser Gruppe. Der Satz gilt also in diesem Fall.
Sei nun $U \neq \{0\}$. Dann existiert eine kleinste Zahl $n \in U \cap \mathbb{N}$. Es gilt $\langle n\rangle \subseteq U$.
Wir zeigen jetzt die umgekehrte Inklusion $U \subseteq \langle n\rangle$ und damit die behauptete Gleichheit $U = \langle n\rangle$. Sei hierzu $a \in U$ beliebig. Wegen 3.3 existieren $q \in \mathbb{Z}$ und $r \in \{0,1,\dots,n-1\}$ mit $a = qn + r$. Es gilt $r = a - qn \in U$, denn U ist bezüglich Differenzbildung abgeschlossen und es ist $a \in U$ sowie $qn \in \langle n\rangle \subseteq U$. Die Minimalität von n und $r < n$ erzwingen $r = 0$, also $a = qn \in \langle n\rangle$. Dies zeigt $U \subseteq \langle n\rangle$.
Wir zeigen nun noch, dass U genau die Erzeuger n und $-n$ besitzt. Hierzu sei $z \in \mathbb{Z}$ beliebig mit $\langle z\rangle = U = \langle n\rangle$. Da die Gleichheit von Mengen äquivalent zu beiden Inklusionen ist, liefert 3.2 (e), dass $n \mid z$ und $z \mid n$ gilt. Aus 3.2 (d) folgt $z = \pm n$. ■

Mit Hilfe der Klassifizierung der Untergruppen von $\mathbb{Z}$ können wir zeigen, dass in $\mathbb{Z}$ größte gemeinsame Teiler existieren. Zunächst definieren wir diesen Begriff:

Definition 3.5 *Für $z_1,\dots,z_k \in \mathbb{Z}$ versteht man unter einem **größten gemeinsamen Teiler von $z_1,\dots,z_k$** ein Element $g \in \mathbb{N}_0$, das den folgenden beiden Bedingungen genügt:*

gemeinsamer Teiler *Es gilt $g \mid z_i$ für alle $i \in \{1,\dots,k\}$.*

Maximalität *Ist $t \in \mathbb{Z}$ ein gemeinsamer Teiler der z_i, so gilt $t \mid g$.*

*Existiert ein größter gemeinsamer Teiler von $z_1,\dots,z_k$, so ist dieser aufgrund der Maximalitätseigenschaft eindeutig festgelegt. Man spricht in diesem Fall daher von **dem** größten gemeinsamen Teiler von $z_1,\dots,z_k$ und bezeichnet ihn mit $\mathrm{ggT}(z_1,\dots,z_k)$.*

Wir kommen zur Existenz des ggT:

Satz 3.6 *Seien $z_1, \dots, z_k \in \mathbb{Z}$ beliebig. Dann existiert $\mathrm{ggT}(z_1, \dots, z_k)$; und zwar gilt genauer: Ist $n \in \mathbb{N}_0$ das nach 3.4 existierende Element mit $\langle n \rangle = \langle z_1, \dots, z_k \rangle$, so ist $n = \mathrm{ggT}(z_1, \dots, z_k)$.*

Beweis. Es gelte $\langle z_1, \dots, z_k \rangle = \langle n \rangle$. Dann liegt jedes der z_i in $\langle n \rangle$ und ist somit nach 3.2 (e) ein Vielfaches von n. Dies zeigt, dass n ein gemeinsamer Teiler aller z_i ist.
Sei nun $t \in \mathbb{Z}$ ein weiterer gemeinsamer Teiler der z_i. Da alle z_i Vielfache von t sind, folgt $z_i \in \langle t \rangle$ und somit $\langle z_1, \dots, z_k \rangle \subseteq \langle t \rangle$, also $\langle n \rangle \subseteq \langle t \rangle$. Mit 3.2 (e) folgt $t \mid n$.
Da zudem n aus $\mathbb{N}_0$ stammt, gilt $n = \mathrm{ggT}(z_1, \dots, z_k)$ nach Definition. ■

Bemerkung 3.7 (a) Es gilt $\mathrm{ggT}(z_1, \dots, z_k) = 0$ genau dann, wenn alle z_i gleich Null sind. Dies bedeutet umgekehrt: Gilt $z_i \neq 0$ für ein i, so ist $\mathrm{ggT}(z_1, \dots, z_k) > 0$.

(b) Aus der ggT-Definition folgt direkt, dass für alle $z_1, \dots, z_k \in \mathbb{Z}$ gilt

$$\mathrm{ggT}(z_1, \dots, z_k) = \mathrm{ggT}(\mathrm{ggT}(z_1, \dots, z_{k-1}), z_k).$$

Durch mehrmaliges Anwenden dieser Identität lässt sich das Berechnen des ggT von k Zahlen auf $k-1$ ggT-Berechnungen von zwei Zahlen reduzieren. Hierfür existieren effiziente Algorithmen, vgl. 3.14.

Wollen wir beispielsweise $\mathrm{ggT}(10, 12, 24, 60)$ berechnen, so bestimmen wir zunächst $g_1 := \mathrm{ggT}(10, 12)$, danach $g_2 := \mathrm{ggT}(g_1, 24)$ und zuletzt $g_3 := \mathrm{ggT}(g_2, 60)$. Dann ist g_3 der gesuchte ggT, denn

$$g_3 = \mathrm{ggT}\big(\mathrm{ggT}(\mathrm{ggT}(10, 12), 24), 60\big) = \mathrm{ggT}\big(\mathrm{ggT}(10, 12, 24), 60\big) = \mathrm{ggT}(10, 12, 24, 60).$$

(c) Ein mit dem ggT verwandtes Konzept, das **kleinste gemeinsame Vielfache (kgV)**, werden wir in den Übungen und in Vorlesung 17 einführen. ⋇ → Übung

Nach 2.17 besteht die Gruppe $\langle z_1, \dots, z_k \rangle$ genau aus den $\mathbb{Z}$-Linearkombinationen der z_i und enthält den ggT der z_i. Es folgt:

Korollar 3.8 (Lemma von Bézout) *Seien $z_1, \dots, z_k \in \mathbb{Z}$ beliebig. Dann ist $\mathrm{ggT}(z_1, \dots, z_k)$ eine $\mathbb{Z}$-Linearkombination der z_i, d. h. es existieren ganze Zahlen $\lambda_i \in \mathbb{Z}$, so dass gilt*

$$\mathrm{ggT}(z_1, \dots, z_k) = \sum_{i=1}^{k} \lambda_i z_i.$$

Unser nächstes Ziel ist, die Existenz einer eindeutigen Primfaktorzerlegung in $\mathbb{Z}$ zu beweisen. Hierzu benötigen wir den Begriff der Teilerfremdheit sowie eine alternative Charakterisierung der Primzahlen.

Definition 3.9 *Zwei ganze Zahlen a und b heißen **teilerfremd**, wenn $\mathrm{ggT}(a, b) = 1$ gilt. In diesem Fall existieren nach Bézout $\lambda, \mu \in \mathbb{Z}$, so dass $\lambda a + \mu b = 1$ gilt.*

In 3.1 (b) haben wir Primzahlen mit Hilfe ihrer positiven Teiler charakterisiert. In vielen Beweisen ist die folgende Primeigenschaft nützlicher:

Satz 3.10 *Sei p eine natürliche Zahl mit $p \geq 2$. Dann sind äquivalent.*

(a) *p ist eine Primzahl.*

(b) *Sind $a, b \in \mathbb{Z}$ beliebig und gilt $p \mid ab$, so folgt $p \mid a$ oder $p \mid b$.*
*Man nennt diese Aussage die **Primeigenschaft**.*

(c) *Sind $a, b \in \mathbb{Z}$ beliebig und gilt $ab \in \langle p \rangle$, so folgt $a \in \langle p \rangle$ oder $b \in \langle p \rangle$.*

Beweis.

(b)$\iff$(c) Beide Aussagen sind äquivalent, denn (c) entsteht durch Umformulierung von (b) mit Hilfe der Äquivalenz in 3.2 (e).

(c)$\implies$(a) Wir zeigen die Behauptung per Kontraposition.
Sei p keine Primzahl. Dann existieren $a, b \in \{2, 3, \dots, p-1\}$ mit $p = ab$. In der Gruppe $\langle p \rangle = p\mathbb{Z} = \{\dots, -2p, -p, 0, p, 2p, \dots\}$ liegen aber weder a noch b.

(a)$\implies$(c) Seien $p \in \mathbb{P}$ und $a, b \in \mathbb{Z}$, so dass gilt $ab \in \langle p \rangle$ gilt. Wir können $a \notin \langle p \rangle$ annehmen, denn ansonsten ist die Aussage in (c) bereits erfüllt. Zu zeigen ist $b \in \langle p \rangle$.
Wegen $a \notin \langle p \rangle$ ist $\langle p, a \rangle \supsetneq \langle p \rangle$ und daher $\langle p, a \rangle = \mathbb{Z}$ nach 3.2 (f). Somit ist $1 \in \langle p, a \rangle$ und daher $b \in \langle pb, ab \rangle$. Wir erhalten

$$b \in \langle pb, ab \rangle \overset{ab \in \langle p \rangle}{\subseteq} \langle pb, p \rangle \overset{pb \in \langle p \rangle}{\subseteq} \langle p \rangle.$$

(Können Sie die Implikationen (a)$\implies$(b) und (b)$\implies$(a) auch direkt zeigen?) ■ ⁉

Bemerkung 3.11 Die Primeigenschaft lässt sich induktiv auf Produkte beliebiger endlicher Länge ausdehnen: Genau dann ist p eine Primzahl, wenn für alle $a_1, \dots, a_n \in \mathbb{Z}$ gilt

$$p \mid a_1 a_2 \cdots a_n \implies p \mid a_i \text{ für mindestens ein } i \in \{1, \dots, n\}.$$

Primzahlen sind daher genau diejenigen Elemente aus $\mathbb{N} \setminus \{1\}$, die mit einem Produkt auch einen dessen Faktoren teilt. ⁂

Wir können nun die Existenz eindeutiger Primfaktorzerlegungen in $\mathbb{Z}$ beweisen. Das folgende Resultat wird in der Literatur manchmal als *Fundamentalsatz der Arithmetik* bezeichnet.

Satz 3.12 (eindeutige Primfaktorzerlegung) *Zu jeder ganzen Zahl $a \in \mathbb{Z} \setminus \{0\}$ existieren eindeutig ein $e \in \{\pm 1\}$, ein $n \in \mathbb{N}_0$ und Primzahlen $p_1 \leq p_2 \leq \cdots \leq p_n$, so dass gilt $a = e \cdot p_1 \cdot p_2 \cdots p_n$.*
*Man nennt diese Darstellung von a die **eindeutige Primfaktorzerlegung (PFZ) von a**.*
Konvention: Das leere Produkt hat den Wert 1.

Beweis. Es gilt $e = \operatorname{sgn}(a)$, wobei sgn die Signumsfunktion bezeichnet. Da man durch Multiplikation mit (-1) Aussagen über positive a auf Aussagen über negative a und umgekehrt übersetzen kann, reicht es, Existenz und Eindeutigkeit für positive a zu zeigen. Sei also $a \geq 1$. Im Falle $a = 1$ gibt es nur eine einzige PFZ von a, nämlich das leere Produkt mit $n = 0$. Sei daher $a \geq 2$.

Existenz der PFZ Angenommen, nicht alle Elemente aus $\mathbb{N} \setminus \{1\}$ besäßen eine PFZ. Dann gäbe ein kleinstes Element $a \geq 2$ ohne PFZ. a ist keine Primzahl, denn sonst wäre a eine PFZ von a. Somit existieren $b, c \in \{2, \dots, a-1\}$ mit $a = bc$. Da b und c kleiner als a sind, besitzen sie eine PFZ aufgrund unserer Voraussetzung an a. Das Produkt der PFZen von b und c ist dann eine PFZ von a — Widerspruch.

Eindeutigkeit der PFZ Angenommen, es gäbe Elemente aus $\mathbb{N} \setminus \{1\}$ mit verschiedenen PFZen. Dann gäbe es ein kleinstes Element $a \geq 2$ mit verschiedenen PFZen. Wir könnten also schreiben

$$p_1 \cdots p_m = a = q_1 \cdots q_n \qquad \text{mit } m, n \in \mathbb{N}_0, p_i, q_j \in \mathbb{P}, p_i \leq p_{i+1} \text{ und } q_j \leq q_{j+1}. \quad (\star)$$

Wäre $p_1 = q_1$, so könnten wir in $(\star)$ durch p_1 teilen. Da die PFZ von $\frac{a}{p_1}$ nach Voraussetzung an a eindeutig ist, folgte $m = n$ und $p_i = q_i$ für alle $i \in \{1, \dots, n\}$. Dies widerspricht aber der Voraussetzung an die Verschiedenheit der PFZen von a.

Daher gilt $p_1 \neq q_1$. Wir können ohne Einschränkung $p_1 < q_1$ annehmen. Dann gilt $p_1 < q_i$ und folglich $p_1 \nmid q_i$ für alle i. Dies widerspricht aber 3.11, da p_1 das Produkt $q_1 \cdots q_n$ teilt. ∎

Bemerkung 3.13 (a) Oft fasst man die einzelnen Faktoren in der PFZ von a zusammen und erhält so Faktorisierungen der Form

$$a = e \cdot \prod_{i=1}^{n} p_i^{n_i} \qquad \text{mit } n_i \in \mathbb{N} \text{ und paarweise verschiedenen } p_i \in \mathbb{P}.$$

$t \in \mathbb{N}$ ist genau dann ein Teiler von a, wenn sich t schreiben lässt in der Form

$$t = \prod_{i=1}^{n} p_i^{s_i} \qquad \text{mit } 0 \leq s_i \leq n_i \text{ für alle } i \in \{1, \dots, n\}.$$

a hat aufgrund der Eindeutigkeit der PFZ daher genau $\prod_{i=1}^{n}(n_i + 1)$ positive und somit insgesamt $2 \cdot \prod_{i=1}^{n}(n_i + 1)$ Teiler.

(b) Lässt man in (a) auch den Exponenten Null zu, so können beliebige $a, b \in \mathbb{Z} \setminus \{0\}$ als Produkt über *dieselben* Primzahlen geschrieben werden, d. h. es gibt paarweise verschiedene Primzahlen $p_1, \dots, p_n$ und Exponenten $m_i, n_i \in \mathbb{N}_0$, so dass gilt

$$a = e_1 \prod_{i=1}^{n} p_i^{n_i} \qquad \text{und} \qquad b = e_2 \prod_{i=1}^{n} p_i^{m_i}.$$

Gemeinsame positive Teiler von a und b sind dann genau die Zahlen $\prod_{i=1}^{n} p_i^{s_i}$ mit $0 \leq s_i \leq \min(n_i, m_i)$ für alle $i \in \{1, \dots, n\}$. ⋇

Berechnung des ggT zweier Zahlen

In 3.7 (b) haben wir die Berechnung des ggTs mehrerer ganzer Zahlen auf die (mehrfache) Berechnung des ggTs zweier ganzer Zahlen reduziert. In diesem Abschnitt stellen wir nun zwei Möglichkeiten vor, wie dies praktisch geschehen kann.

Seien $a, b \in \mathbb{Z}$ beliebig. Ziel ist die Berechnung von $\operatorname{ggT}(a, b)$. Aus 3.5 folgt $\operatorname{ggT}(a, b) = \operatorname{ggT}(|a|, |b|)$. Zudem gilt $\operatorname{ggT}(a, 0) = |a|$ bzw. $\operatorname{ggT}(0, b) = |b|$. Wir können daher für das Folgende $a, b \in \mathbb{N}$ annehmen.

Berechnung mittels PFZ Sind die PFZen von a und b bekannt, so lässt sich aus diesen nach 3.13 (b) sehr einfach $\operatorname{ggT}(a, b)$ berechnen: Gilt $a = \prod_{i=1}^{n} p_i^{n_i}$ und $b = \prod_{i=1}^{n} p_i^{m_i}$, so ist

$$\operatorname{ggT}(a, b) = \prod_{i=1}^{n} p_i^{\min(n_i, m_i)}.$$

Diese Formel ist in der Praxis oft weniger nützlich als es auf den ersten Blick scheint, da keine effizienten Algorithmen zur Berechnung von PFZen bekannt sind. Für Beweise kann obige Darstellung des ggTs allerdings sehr wertvoll sein.

Berechnung mittels Euklidischem Algorithmus Der Euklidische Algorithmus berechnet $\operatorname{ggT}(a, b)$ durch wiederholte Division mit Rest. Hierzu definiert man rekursiv

$$r_0 := a, \quad r_1 := b \quad \text{sowie} \quad r_{i+2} := r_i \bmod r_{i+1} \text{ für } i \in \mathbb{N}_0 \text{ und } r_{i+1} \neq 0.$$

Mit diesen Bezeichnungen gilt:

Satz 3.14 *Es gibt ein $n \in \mathbb{N}$ mit $r_{n+1} = 0$. Dann ist $\operatorname{ggT}(a, b) = r_n$.*

Beweisskizze.

Existenz von n Die r_i sind als Reste nicht-negativ. Angenommen, es gelte $r_i > 0$ für alle $i \in \mathbb{N}_0$. Dann ist $(r_i)_{i \in \mathbb{N}_0}$ eine streng monoton fallende Folge auf $\mathbb{N}$, denn es gilt $r_{i+2} = r_i \bmod r_{i+1} \in \{1, 2, \dots, r_{i+1} - 1\}$, also $r_{i+2} < r_{i+1}$. Dies ist widersprüchlich, denn solche Folgen existieren auf $\mathbb{N}$ nicht.

ggT-Aussage Sei $t := \operatorname{ggT}(a, b)$. Wir zeigen, dass die Aussagen $t \mid r_n$ und $r_n \mid t$ gelten. Da $r_n > 0$ ist, folgt $t = r_n$ aus 3.2 (d).

t ist ein gemeinsamer Teiler von a und b und teilt daher auch r_2, denn r_2 lässt sich nach 3.3 schreiben in der Form $r_2 = r_0 - q \cdot r_1 = a - qb$ mit einem $q \in \mathbb{Z}$. Dieses Argument lässt sich induktiv fortsetzen und zeigt $t \mid r_i$ für alle $i \in \{1, \dots, n + 1\}$.

Wegen $r_{n+1} = 0$ ist $r_{n-1} = q \cdot r_n$ mit einem $q \in \mathbb{Z}$ nach 3.3. Also ist $r_n \mid r_{n-1}$. Wieder mit 3.3 gilt $r_{n-2} = q' \cdot r_{n-1} + r_n$ mit einem $q' \in \mathbb{Z}$. Nach 3.2 (b) folgt hieraus $r_n \mid r_{n-2}$. Dieses Argument lässt sich induktiv fortsetzen und zeigt $r_n \mid r_i$ für alle $i \in \{0, 1, \dots, n + 1\}$. Somit ist r_n ein gemeinsamer Teiler von a und b und nach Definition somit auch ein Teiler von $\operatorname{ggT}(a, b) = t$. ■

Bemerkung 3.15 (a) Der Euklidische Algorithmus ist einer der wichtigsten Algorithmen der angewandten Zahlentheorie. Er ist auch noch für größte Zahlen $a, b \in \mathbb{N}$ mit vertretbarem Zeitaufwand durchführbar, denn die benötigten Rechenoperationen zur Bestimmung der Reste r_i lassen sich sehr effizient implementieren.

(b) Berechnet man im Euklidischen Algorithmus nicht nur die Reste, sondern auch die auftretenden Ganzzahlquotienten, so spricht man vom *erweiterten Euklidischen Algorithmus*. Mit ihm kann man die Bézout-Koeffizienten λ_i aus 3.8 konkret berechnen. Wir gehen in den Übungen genauer darauf ein. ※ → Übung

Beispiel 3.16 Wir wollen $\mathrm{ggT}(3\,434, -5\,555)$ berechnen. Wegen $\mathrm{ggT}(3\,434, -5\,555) = \mathrm{ggT}(3\,434, 5\,555)$ führen wir den Euklidischen Algorithmus mit den Startwerten 3 434 und 5 555 aus. Zur kompakten Darstellung des Algorithmus benutzen wir folgende Tabelle:

$i =$	r_i	r_{i+1}	Berechnung $r_{i+2} = r_i \bmod r_{i+1}$
0	3434	5555	3434
1	5555	3434	$5555 \bmod 3434 = 2121$
2	3434	2121	$3434 \bmod 2121 = 1313$
3	2121	1313	$2121 \bmod 1313 = 808$
4	1313	808	$1313 \bmod 808 = 505$
5	808	505	$808 \bmod 505 = 303$
6	505	303	$505 \bmod 303 = 202$
7	303	202	$303 \bmod 202 = 101$
8	202	101	$202 \bmod 101 = 0$

Wir sehen, dass $r_{10} = 0$ ist. Daher ist $\mathrm{ggT}(3434, -5555) = r_9 = 101$.

Beachten Sie die Systematik in obiger Tabelle: Die r_i wandern von rechts nach links durch die Spalten. Wir haben dies am Beispiel des Restes r_3 und r_8 durch Einfärbungen kenntlich gemacht. ※

4. Nebenklassen, Restklassenringe, Einheiten und Nullteiler

Worum geht es? In dieser Vorlesung konstruieren wir die Ringe $\mathbb{Z}_n$ und beweisen einige ihrer grundlegenden Eigenschaften. Hierzu führen wir eine ganze Reihe neuer Konzepte und Begriffe ein; beispielsweise setzen wir Verknüpfungen auf Potenzmengen fort und beschäftigen uns mit *Partitionen*, *Nebenklassen*, *Einheiten* und *Nullteilern*. ⁂

Fortsetzung von Verknüpfungen auf die Potenzmenge

Seien M eine Menge und $\cdot : M \times M \to M$ eine Verknüpfung auf M. Für Teilmengen $A, B \subseteq M$ setzen wir

$$A \cdot B := \{a \cdot b \mid a \in A,\, b \in B\}.$$

Dann ist $AB \subseteq M$, so dass obige Festsetzung eine Verknüpfung $\mathfrak{P}(M) \times \mathfrak{P}(M) \to \mathfrak{P}(M)$ auf der Potenzmenge $\mathfrak{P}(M)$ von M liefert. Die auf diese Weise auf $\mathfrak{P}(M)$ fortgesetzte Verknüpfung bezeichnen wir ebenfalls mit $\cdot$ (mathematisch ungenau).
Der Übersichtlichkeit halber schreiben wir beim Verknüpfen mit einelementigen Mengen keine Mengenklammern: Für $a, b \in M$ schreiben wir also aB statt $\{a\}B$ und Ab statt $A\{b\}$. Das Produkt ab interpretieren wir, je nach Kontext, als Element von M oder als Teilmenge $\{ab\} \subseteq M$.

Beispiel 4.1 (a) Die Menge der geraden Zahlen lässt sich schreiben als $2\mathbb{Z}$, die der ungeraden Zahlen als $1 + 2\mathbb{Z}$. Es gilt $\mathbb{P} \setminus \{2, 3\} \subseteq \{1, 5\} + 6\mathbb{Z}$.

(b) In der Gruppe $(\mathbb{C} \setminus \{0\}, \cdot)$ stellt die Menge $\exp(\frac{\pi i}{4}) \cdot C_4$ die Eckpunkte eines Quadrats dar, dessen Seiten parallel zu den Koordinatenachsen liegen.

(c) Sind G eine nicht-abelsche Gruppe und $A, B \subseteq G$, so gilt i. A. $AB \neq BA$.

(d) Sei U Untergruppe irgendeiner Gruppe. Dann gilt $u \cdot U = U$ für jedes $u \in U$; die Inklusion $\subseteq$ folgt aus der Abgeschlossenheit von U, die Inklusion $\supseteq$ aus der Gleichheit $x = u \cdot u^{-1}x$ für $x \in U$.

Wir erhalten insbesondere, dass $U \cdot U = \bigcup_{u \in U} uU = \bigcup_{u \in U} U = U$ gilt.

(e) Seien G eine Gruppe, $U \leq G$ und $g \in G$. Dann gilt $gU = U$ genau dann, wenn $g \in U$ ist. Die Rückrichtung der Aussage folgt aus (d), die Hinrichtung folgt wegen $g = g \cdot 1 \in gU = U$. ⁂

Viele Rechenregeln übertragen sich beim Fortsetzen einer Verknüpfung auf die Potenzmenge. Man sieht sehr schnell, dass dies beispielsweise für die Kommutativität, die Assoziativität und, im Falle von zwei Verknüpfungen, die Distributivität gilt. Für einelementige Mengen gilt zudem ein Analogon zu 1.8:

Lemma 4.2 *Seien G eine Gruppe, $g \in G$ und $A, B \subseteq G$. Dann gelten die folgenden Äquivalenzen:*

$$gA = B \iff A = g^{-1}B \qquad \text{sowie} \qquad Ag = B \iff A = Bg^{-1}.$$

Diese Äquivalenzen zeigen, dass man durch einelementige Mengen „teilen“ kann.

Teilweiser Beweis. Wir zeigen nur, dass aus $gA = B$ die Aussage $A \subseteq g^{-1}B$ folgt. Die übrigen Mengeninklusionen und Implikationen zeigt man analog.
Es gelte also $gA = B$. Sei $a \in A$ beliebig. Dann existiert ein $b \in B$ mit $ga = b$. Mit 1.8 folgt $a = g^{-1}b$. Also ist $a \in g^{-1}B$. Weil $a \in A$ beliebig war, folgt $A \subseteq g^{-1}B$. ■

Für die Gruppentheorie sind Produkte aus einer einelementigen Menge und einer Untergruppe besonders wichtig. Wir geben ihnen einen eigenen Namen:

Definition 4.3 (Nebenklassen) *Seien G eine Gruppe, $g \in G$ und $U \leq G$. Dann nennen wir die Menge $gU = \{gu \mid u \in U\}$ die **Nebenklasse von U in G durch g**. In additiver Schreibweise ist diese Nebenklasse durch $g + U = \{g + u \mid u \in U\}$ gegeben.*
*Mit $G/U := \{gU \mid g \in G\}$ bezeichnen wir die **Menge aller Nebenklassen von U in G**. Das Objekt G/U ist eine Menge von Teilmengen von G, also eine Teilmenge von $\mathfrak{P}(G)$.*

Eine der wichtigsten Aussagen über die Menge der Nebenklassen G/U ist deren Partitionierungseigenschaft:

Satz 4.4 (Nebenklassenzerlegung) *Seien G eine Gruppe und $U \leq G$ eine Untergruppe von G. Dann **partitioniert** G/U die Menge G, d. h. G/U besteht aus lauter nicht-leeren Teilmengen von G, so dass jedes $g \in G$ in **genau einer** solchen Teilmenge liegt.*
Anders formuliert: G/U ist eine Zerlegung von G in nicht-leere paarweise disjunkte Teilmengen.

Beweis. G/U besteht genau aus den Mengen der Form gU mit $g \in G$. Es gilt $g \in gU$. Dies zeigt, dass kein Element von G/U leer ist und dass jedes $g \in G$ in einem Element von G/U enthalten ist. Es ist daher nur noch zu zeigen, dass zwei *verschiedene* Elemente von G/U disjunkt sind. Wir beweisen dies per Kontraposition, indem wir nachweisen, dass zwei nicht-disjunkte Elemente aus G/U bereits gleich sind:
Seien also Nebenklassen $gU, hU \in G/U$ gegeben mit $gU \cap hU \neq \emptyset$. Dann existiert $x \in gU \cap hU$, und wir können x schreiben in der Form $x = gu_1 = hu_2$ mit $u_1, u_2 \in U$. Es folgt

$$gU \overset{4.1\,(d)}{=} gu_1U = xU = hu_2U \overset{4.1\,(d)}{=} hU.$$

Damit ist gezeigt, dass G/U eine Partition von G ist. ■

Bemerkung 4.5 (a) Sei $g \in G$. Dann zeigt 4.4, dass es in G/U *genau eine* Nebenklasse gibt, die g enthält, nämlich gU.

(b) Sei h ein beliebiges Element der Nebenklasse gU. Dann ist $h \in gU \cap hU$ und somit $gU = hU$ nach 4.4. Gilt umgekehrt $gU = hU$, so ist $h \in gU$.

Dies zeigt, dass sich die Nebenklasse gU auf verschiedene Weisen schreiben lässt; und zwar gilt $gU = hU$ genau dann, wenn $h \in gU$ ist. Jedes $h \in gU$ nennen wir einen **Vertreter der Nebenklasse gU**.

Ein Gruppenelement h ist genau dann ein Vertreter der Nebenklasse gU, wenn $h = gu$ mit einem $u \in U$ gilt, also wenn $g^{-1}h \in U$ ist.

(c) Die Mehrdeutigkeiten in (b) stellen keinen Widerspruch zu (a) dar: Nebenklassen sind gewisse Teilmengen einer Gruppe G, und es gibt genau eine solche Teilmenge, die g enthält. Für diese Teilmenge gibt es aber verschiedene Möglichkeiten der Darstellung. ⁜

Definition 4.6 (Index) *Seien G eine Gruppe und $U \leq G$. Unter dem **Index von U in G** versteht man die Anzahl der verschiedenen Nebenklassen von U in G, also die Anzahl der Elemente der Menge G/U. Man schreibt $[G : U]$ für ihn. Es ist $[G : U] \in \mathbb{N} \cup \{\infty\}$.*

Die Restklassenringe $\mathbb{Z}_n$

In diesem Abschnitt bezeichnet n eine fest gewählte natürliche Zahl. Ist $a \in \mathbb{Z}$, so schreiben wir für die Nebenklasse von $n\mathbb{Z}$ durch a abkürzend $\overline{a}$. Es ist also

$$\overline{a} = a + n\mathbb{Z} = \{a + nz \mid z \in \mathbb{Z}\}.$$

Das folgende Lemma liefert eine alternative Darstellung der Menge $\overline{a}$:

Lemma 4.7 *Sei $a \in \mathbb{Z}$ beliebig. Dann gilt*

$$\overline{a} = \{x \in \mathbb{Z} \mid x \bmod n = a \bmod n\}.$$

Die Menge $\overline{a}$ besteht also genau aus den ganzen Zahlen x, die modulo n denselben Rest haben wie a.

Beweis. Dividieren wir a mit Rest durch n, so erhalten wir $q \in \mathbb{Z}$ und $r \in \{0, \dots, n-1\}$ mit $a = r + nq$. Dann ist

$$\overline{a} = a + n\mathbb{Z} = r + nq + n\mathbb{Z} = r + n(q + \mathbb{Z}) \overset{q+\mathbb{Z}=\mathbb{Z} \text{ nach } 4.1 \text{ (e)}}{=} r + n\mathbb{Z} = \overline{r}.$$

$\overline{a}$ besteht also genau aus den ganzen Zahlen der Form $r + nz$ mit $z \in \mathbb{Z}$. Dies sind genau die ganzen Zahlen, die bei Division durch n den Rest r lassen. ■ ⁇

Wir bezeichnen ab jetzt mit $\mathbb{Z}_n$ die Menge der Nebenklassen von $n\mathbb{Z}$ in $\mathbb{Z}$, d. h. wir setzen $\mathbb{Z}_n := \mathbb{Z}/n\mathbb{Z}$.
Bei der Division durch n treten genau die n Reste $0, 1, \dots, n-1$ auf. Das Lemma zeigt, dass die Nebenklassen $\overline{0}, \overline{1}, \dots, \overline{n-1}$ paarweise verschieden sind. Es folgt:

Satz 4.8 *Es gilt $\mathbb{Z}_n = \{\overline{0}, \dots, \overline{n-1}\}$ und die Elemente $\overline{0}, \overline{1}, \dots, \overline{n-1}$ sind paarweise verschieden. Dies zeigt, dass $|\mathbb{Z}_n| = n$ ist, also dass die Untergruppe $n\mathbb{Z}$ den Index n in $\mathbb{Z}$ hat.*

Wir wollen nun Verknüpfungen auf $\mathbb{Z}_n$ definieren, so dass $\mathbb{Z}_n$ zum Ring wird. Hierzu betrachten wir die auf $\mathfrak{P}(\mathbb{Z})$ fortgesetzten Verknüpfungen von $\mathbb{Z}$:

Lemma 4.9 *Seien $a, b \in \mathbb{Z}$. Dann gelten $\overline{a} + \overline{b} = \overline{a+b}$ sowie $\overline{a} \cdot \overline{b} \subseteq \overline{a \cdot b}$.*

Beweis. Für beliebige $a, b \in \mathbb{Z}$ gilt

$$\begin{array}{rcl} \overline{a} + \overline{b} & = & (a + n\mathbb{Z}) + (b + n\mathbb{Z}) \overset{\text{+ assoziativ}}{=} a + (n\mathbb{Z} + b) + n\mathbb{Z} \\ & \overset{\text{+ kommutativ}}{=} & a + (b + n\mathbb{Z}) + n\mathbb{Z} \overset{\text{+ assoziativ}}{=} a + b + (n\mathbb{Z} + n\mathbb{Z}) \\ & \overset{4.1\,(d)}{=} & a + b + n\mathbb{Z} = \overline{a + b}. \end{array}$$

Weiter ist

$$\begin{array}{rcl} \overline{a} \cdot \overline{b} & = & (a + n\mathbb{Z}) \cdot (b + n\mathbb{Z}) = \{a + nx \mid x \in \mathbb{Z}\} \cdot \{b + ny \mid y \in \mathbb{Z}\} \\ & \overset{\text{Distributivität}}{=} & \{ab + n(ay + bx + nxy) \mid x, y \in \mathbb{Z}\} \subseteq ab + n\mathbb{Z} = \overline{a \cdot b}. \end{array}$$

■

Das Lemma zeigt, dass die auf $\mathfrak{P}(\mathbb{Z})$ fortgesetzte Addition eine Verknüpfung auf $\mathbb{Z}_n$ liefert. Für die auf $\mathfrak{P}(\mathbb{Z})$ fortgesetzte Multiplikation gilt dies nicht; das Produkt $\overline{a} \cdot \overline{b}$ ist im Allgemeinen keine Nebenklasse mehr. Allerdings „verschmiert" $\overline{a} \cdot \overline{b}$ auch nicht über mehrere Nebenklassen hinweg, sondern ist komplett in der Nebenklasse $\overline{ab}$ enthalten. Dies motiviert die folgende Definition:

Definition/Satz 4.10 *Für beliebige $a, b \in \mathbb{Z}$ setzen wir*

$$\overline{a} + \overline{b} := \overline{a + b} \qquad \textit{sowie} \qquad \overline{a} \cdot \overline{b} := \overline{a \cdot b}.$$

*Mit diesen Verknüpfungen wird $\mathbb{Z}_n$ zu einem Ring, dem **Restklassenring modulo n**. In $\mathbb{Z}_n$ ist die Null durch $\overline{0}$ gegeben, die Eins durch $\overline{1}$.*

Teilweiser Beweis. Wir müssen zeigen, dass $\mathbb{Z}_n$ mit den oben definierten Verknüpfungen ein Ring ist. Dies folgt aber sofort aus der Ringstruktur von $\mathbb{Z}$. Wir zeigen beispielhaft, dass $\overline{0}$ neutral ist. Sei hierzu $a \in \mathbb{Z}$ beliebig. Dann ist

$$\overline{0} + \overline{a} \overset{\text{Def. +}}{=} \overline{0 + a} \overset{\text{Rechnen in } \mathbb{Z}}{=} \overline{a} \overset{\text{Rechnen in } \mathbb{Z}}{=} \overline{a + 0} \overset{\text{Def. +}}{=} \overline{a} + \overline{0}.$$ ■

Beispiel 4.11 (a) In $\mathbb{Z}_{25}$ gilt $\overline{2} \cdot \overline{13} = \overline{26} = \overline{1}$. Das Element $\overline{2}$ besitzt in $\mathbb{Z}_{25}$ daher das multiplikativ Inverse $\overline{13}$.

(b) Für jedes $\overline{a} \in \mathbb{Z}_n$ gilt $-\overline{a} = \overline{-a}$, denn es ist $\overline{0} = \overline{a + (-a)} = \overline{a} + \overline{-a}$.

(c) In $\mathbb{Z}_9$ gilt $\overline{3} \cdot \overline{3} = \overline{0} = \overline{6} + \overline{3}$. ※

Bemerkung 4.12 (a) Aus Gründen der Lesbarkeit lässt man die Querstriche über den Elementen aus $\mathbb{Z}_n$ gerne weg. In $\mathbb{Z}_2$ würde man also schreiben $2 = 1 + 1 = 0$. Beachten Sie, dass hier dennoch mit *Mengen* gerechnet wird.

(b) In der Herleitung des Rings $\mathbb{Z}_n$ tauchen die Symbole $+$ bzw. $\cdot$ in drei verschiedenen Bedeutungen auf:

Die auf $\mathbb{Z}$ gegebene Addition haben wir zunächst auf $\mathfrak{P}(\mathbb{Z})$ fortgesetzt und dann auf $\mathbb{Z}_n$ eingeschränkt.

$$+ : \mathbb{Z}^2 \to \mathbb{Z} \overset{\text{Fortsetzen}}{\dashrightarrow} + : \mathfrak{P}(\mathbb{Z})^2 \to \mathfrak{P}(\mathbb{Z}) \overset{\text{Einschränken}}{\dashrightarrow} + : \mathbb{Z}_n^2 \to \mathbb{Z}_n$$

Die auf $\mathbb{Z}$ gegebene Multiplikation haben wir ebenfalls zunächst auf $\mathfrak{P}(\mathbb{Z})$ fortgesetzt. Wir haben dann gesehen, dass ein Produkt $\overline{a} \cdot \overline{b}$ komplett in der Nebenklasse $\overline{ab}$ enthalten ist und haben eine neue Multiplikation auf $\mathbb{Z}_n$ durch $\overline{a} \cdot \overline{b} := \overline{ab}$ definiert.

$$\cdot : \mathbb{Z}^2 \to \mathbb{Z} \overset{\text{Fortsetzen}}{\dashrightarrow} \cdot : \mathfrak{P}(\mathbb{Z})^2 \to \mathfrak{P}(\mathbb{Z}) \overset{\text{neue Definition}}{\dashrightarrow} \cdot : \mathbb{Z}_n^2 \to \mathbb{Z}_n$$

(c) Die Restklassenringe $\mathbb{Z}_n$ zeigen: Zu jeder natürlichen Zahl $n \in \mathbb{N}$ gibt es einen Ring der Ordnung n. ⁜

Einheiten und Nullteiler

Mit den folgenden Begriffen werden wichtige Typen von Ringelementen beschrieben:

Definition 4.13 *Sei R ein Ring.*

(a) *Ein Element $a \in R$ heißt **Nullteiler**, wenn $a \neq 0$ ist und ein $b \in R \setminus \{0\}$ existiert, so dass $ab = 0$ gilt. In diesem Fall ist auch b ein Nullteiler. Man nennt b oft einen **Ko-Nullteiler zu a**.*

*Enthält R keine Nullteiler, so sagt man, dass R **nullteilerfrei** sei.*

(b) *Lässt sich ein Element $a \in R$ multiplikativ invertieren, d. h. existiert ein $b \in R$ mit $ab = 1$, so nennt man a eine **Einheit des Rings R**. In diesem Fall ist auch b eine Einheit.*

Die Menge aller Einheiten von R bezeichnen wir mit $R^\times$. Wegen $1 \in R^\times$ ist $R^\times$ stets nicht-leer.

Beispiel 4.14 (a) $\mathbb{Z}$ ist nullteilerfrei. Es gilt $\mathbb{Z}^\times = \{\pm 1\}$.

(b) Aus 1.14 folgt: Ein Ring R ist genau dann ein Körper, wenn $1 \neq 0$ in R gilt und $R^\times = R \setminus \{0\}$ ist.

(c) In 4.11 haben wir gesehen, dass $\overline{2}$ und $\overline{13}$ Einheiten in $\mathbb{Z}_{25}$ sind und dass $\overline{3}$ ein Nullteiler in $\mathbb{Z}_9$ ist. ⁜

Die Begriffe *Einheit* und *Nullteiler* schließen sich gegenseitig aus:

Satz 4.15 *Kein Ringelement $a \in R$ ist zugleich Einheit und Nullteiler.*

Beweis. Es sei $a \in R$ Einheit und Nullteiler. Dann existieren Elemente $b \in R$ und $c \in R \setminus \{0\}$ mit $ab = 1$ und $ac = 0$. Dann folgt für das Produkt abc der Widerspruch

$$c = 1 \cdot c = (ab) \cdot c = abc = b \cdot (ac) = b \cdot 0 = 0.$$ ■

Bemerkung 4.16 (a) 4.15 schließt nicht aus, dass ein Ringelement *weder* Einheit *noch* Nullteiler ist. Tatsächlich gibt es solche Elemente, beispielsweise $2 \in \mathbb{Z}$.

In den Übungen werden wir allerdings zeigen: Jedes Nicht-Null-Element eines *endlichen* Rings ist *entweder* Einheit *oder* Nullteiler. → Übung

(b) Ist K ein Körper, so gilt $K^\times = K \setminus \{0\}$. Körper sind daher wegen 4.15 stets nullteilerfrei. ※

Durch Überprüfen der Gruppenaxiome zeigt man, dass die Menge der Einheiten eines Rings eine multiplikative Gruppe bildet:

Satz 4.17 *Sei R ein Ring. Dann ist die Menge $R^\times$ der Einheiten von R zusammen mit der Multiplikation von R eine abelsche Gruppe. Man nennt $R^\times$ daher die* ***Einheitengruppe des Rings R****. Wegen 1.3 (c) haben Einheiten in Ringen stets eindeutige Inverse.*

Knobelfrage. Bildet auch die Menge der Nullteiler eines Rings eine Gruppe? ⁉

In Gruppen kann man durch Elemente teilen, indem man mit ihrem Inversen multipliziert. Ebenso kann man in Ringen durch Einheiten teilen. Der nächste Satz sagt, dass in Ringen darüber hinaus durch Nicht-Nullteiler „geteilt“ werden kann:

Satz 4.18 (Kürzen in Ringen) *Seien R ein Ring und $a \in R \setminus \{0\}$. Dann sind die folgenden Aussagen äquivalent:*

(a) *Für beliebige $b, c \in R$ kann in der Gleichung $ab = ac$* ***durch a gekürzt*** *werden, d. h. es gilt die Implikation*

$$ab = ac \Longrightarrow b = c.$$

(b) *a ist* ***kein*** *Nullteiler in R.*

Beweis.

(a)⟹(b) Wir zeigen die Behauptung per Kontraposition. Sei a ein Nullteiler in R. Dann existiert $b \in R$ mit $b \neq 0$ und $ab = 0$. Setzen wir $c := 0$, so gilt $ab = ac$, aber $b \neq c$.

(b)⟹(a) Es gilt

$$ab = ac \iff ab - ac = 0 \iff a \cdot (b - c) = 0.$$

Da a kein Nullteiler ist, folgt $b - c = 0$, also $b = c$. ■ ⁉

Wir wollen die Einheiten von $\mathbb{Z}_n$ bestimmen. Als Vorbereitung dient das folgende Lemma:

Lemma 4.19 *Seien $a, b \in \mathbb{Z}$, so dass $\overline{a} = \overline{b}$ in $\mathbb{Z}_n$ gelte. Dann ist $\mathrm{ggT}(a, n) = \mathrm{ggT}(b, n)$. Dies zeigt, dass alle Vertreter der Nebenklasse $\overline{a}$ denselben ggT mit n besitzen.*

Beweis. Wir berechnen $\mathrm{ggT}(a, n)$ und $\mathrm{ggT}(b, n)$ mit Hilfe des Euklidischen Algorithmus. Da $a \bmod n = b \bmod n$ nach 4.7 gilt, tauchen im Algorithmus nach dem ersten Schritt in beiden ggT-Berechnungen dieselben Reste auf. Beide ggT sind daher gleich. ■

Satz 4.20 *Sei $a \in \mathbb{Z}$ beliebig. Dann ist $\overline{a}$ eine Einheit in $\mathbb{Z}_n$ genau dann, wenn $\mathrm{ggT}(a, n) = 1$.*
*(Das obige Lemma garantiert hierbei, dass die ggT-Bedingung unabhängig vom gewählten Vertreter der Nebenklasse ist. Man sagt auch, dass die ggT-Bedingung **wohldefiniert** ist.)*

Beweis.

$\Longrightarrow$ Sei $\overline{a} \in \mathbb{Z}_n^\times$. Dann existiert $\overline{b} \in \mathbb{Z}_n$ mit $\overline{ab} = \overline{1}$, also mit $ab \in \overline{1}$. Es gibt dann also $z \in \mathbb{Z}$ mit $ab = 1 + nz$, also mit $ab - nz = 1$. Jeder gemeinsame Teiler d von a und n teilt auch $ab - nz$ und somit 1. Es folgt $|d| = 1$ und daher $\mathrm{ggT}(a, n) = 1$.

$\Longleftarrow$ Sei nun $\mathrm{ggT}(a, n) = 1$. Mit Bézout existieren dann $\alpha, \beta \in \mathbb{Z}$ mit $\alpha a + \beta n = 1$, also mit $\alpha a = 1 - \beta n$. Offenbar gilt $1 - \beta n \in \overline{1}$. Dies zeigt $\overline{\alpha a} = \overline{1 - \beta n} = \overline{1}$ und somit $\overline{\alpha} \cdot \overline{a} = \overline{1}$. Dies zeigt, dass $\overline{a}$ eine Einheit in $\mathbb{Z}_n$ ist. ■

Wegen $\mathbb{Z}_n = \{\overline{0}, \ldots, \overline{n-1}\}$ folgt:

Korollar 4.21 *Die Ordnung der Gruppe $|\mathbb{Z}_n^\times|$ entspricht der Anzahl der zu n teilerfremden Zahlen aus der Menge $\{0, 1, \ldots, n-1\}$. Es gilt also $|\mathbb{Z}_n^\times| = |\{z \in \{0, 1, \ldots, n-1\} : \mathrm{ggT}(z, n) = 1\}|$. Für $n \in \mathbb{N}$ setzt man $\varphi(n) := |\mathbb{Z}_n^\times|$ und nennt $\varphi : \mathbb{N} \to \mathbb{N}$ die **Eulersche φ-Funktion**.*

Es gilt $\varphi(n) = n - 1$ genau für $n \in \mathbb{P}$. In diesem Fall ist $\mathbb{Z}_n^\times = \mathbb{Z}_n \setminus \{0\}$. Zusammen mit 4.14 (b) ergibt sich die folgende erstaunliche Konsequenz: ⁉

Korollar 4.22 *Genau für $n \in \mathbb{P}$ ist $\mathbb{Z}_n$ ein Körper. In diesem Fall folgt aus dem Beweis zu 4.20: Ist $\overline{a} \neq \overline{0}$ und ist $\alpha \in \mathbb{Z}$ der Bézout-Faktor in der Gleichung $\alpha a + \beta n = 1$, so ist $\overline{a}^{-1} = \overline{\alpha}$.*

Bemerkung 4.23 Die Ringe $\mathbb{Z}_n$ liefern also unendlich viele Beispiele für Körper. Die Körper $\mathbb{Z}_p$ mit $p \in \mathbb{P}$ sind in der Algebra äußerst wichtig: Sie bilden die Grundbausteine für alle endlichen Körper. ※

5. Faktorgruppen und Faktorringe

Worum geht es? Wir übertragen das Konstruktionsprinzip von $\mathbb{Z}_n$ aus der letzten Vorlesung auf allgemeine Gruppen und Ringe. Dies liefert, neben der Unterstrukturbildung aus Vorlesung 2, eine weitere Möglichkeit, aus einer gegebenen algebraischen Struktur eine neue algebraische Struktur zu bilden. ⋇

Faktorgruppen

Seien G eine beliebige Gruppe und $U \leq G$ eine Untergruppe von G. Für die Nebenklasse gU schreiben wir $\overline{g}$. Diese Schreibweise nennt man die **Querstrichnotation**.

Um G/U zur Gruppe machen zu können, benötigen wir ein Analogon zu 4.9, d. h. wir müssen zeigen, dass das Produkt $\overline{g} \cdot \overline{h}$ mit Elementen $g, h \in G$ in nur einer Nebenklasse enthalten ist. Die einzige Nebenklasse, die hierfür in Frage kommt, ist $\overline{gh}$, denn es ist $g \in \overline{g}$ und $h \in \overline{h}$ und somit $gh \in \overline{g} \cdot \overline{h}$.

Im Beweis zu 4.9 haben wir die Kommutativität der Gruppe $(\mathbb{Z}, +)$ ausgenutzt und konnten deshalb $n\mathbb{Z} + b$ durch $b + n\mathbb{Z}$ ersetzen. Diese Schlussweise fällt bei der beliebig gewählten (und daher i. A. nicht-abelschen) Gruppe G weg. Wir benötigen also ein anderes Argument, um die Aussage

$$gUhU \subseteq ghU \qquad \text{für beliebige } g, h \in G \tag{$\star$}$$

zu zeigen.

Tatsächlich gibt es ein solches Argument nicht. Wir werden in den Übungen ein Beispiel für eine Gruppe G und eine Untergruppe U sehen, für die $(\star)$ nicht erfüllt ist. Damit $(\star)$ erfüllt ist, muss die Bedingung $gU = Ug$ für alle $g \in G$ an die Untergruppe U gestellt werden. Dann ist wörtlich derselbe Beweis wie in 4.9 möglich:

→ Übung

Lemma 5.1 *Seien G eine Gruppe und $U \leq G$. Dann sind äquivalent:*

(a) *Es gilt $gU = Ug$ für alle $g \in G$.*

(b) *Es gilt $gUhU \subseteq ghU$ für alle $g, h \in G$.*

Ist eine der beiden oberen Bedingungen erfüllt, so gilt in (b) sogar die Gleichheit $gUhU = ghU$.

Beweis.

(a)$\Longrightarrow$(b) Es gelte $gU = Ug$ für alle $g \in G$. Dann ist für beliebige $g, h \in G$

$$gUhU \overset{\text{Assoziativität}}{=} g(Uh)U \overset{Uh=hU}{=} g(hU)U \overset{\text{Assoziativität}}{=} gh(UU) \overset{4.1\,(e)}{=} ghU.$$

Obige Umformungen zeigen auch, dass unter Annahme von (a) Gleichheit in Aussage (b) gilt.

(b)$\Longrightarrow$(a) Wir wählen in (b) zunächst speziell $g = 1$ und erhalten $UhU \subseteq hU$. Offenbar gilt $Uh \subseteq UhU$. Zusammen folgt $Uh \subseteq UhU \subseteq hU$ und daher insbesondere $Uh \subseteq hU$ für jedes $h \in G$.

Zum Beweis der anderen Inklusion invertieren wir jedes Element der in (b) auftretenden Mengen. Wir erhalten

$$(gUhU)^{-1} = \{(guhv)^{-1} \mid u, v \in U\} \overset{1.3\,(e)}{=} \{v^{-1}h^{-1}u^{-1}g^{-1} \mid u, v \in U\} = Uh^{-1}Ug^{-1}.$$

Im letzten Schritt haben wir ausgenutzt, dass $U = \{u^{-1} \mid u \in U\}$ gilt. Analog folgt $(ghU)^{-1} = Uh^{-1}g^{-1}$. Weiterhin bleibt die Mengeninklusion in (b) bestehen. Wir erhalten also

$$Uh^{-1}Ug^{-1} \subseteq Uh^{-1}g^{-1} \qquad \text{für alle } g, h \in G.$$

Wir setzen wieder $g = 1$, argumentieren analog zum ersten Teil und erhalten $h^{-1}U \subseteq Uh^{-1}U \subseteq Uh^{-1}$ für alle $h \in G$.

Da h in den beiden gezeigten Inklusionen frei wählbar ist, ist die Aussage in (a) gezeigt. ■

Untergruppen, die die Eigenschaft (a) aus obigem Lemma erfüllen, sind so wichtig für die Gruppentheorie, dass sie einen eigenen Namen bekommen:

Definition 5.2 (Normalteiler) *Eine Untergruppe N einer Gruppe G heißt **Normalteiler von G**, wenn $gN = Ng$ für alle $g \in G$ gilt.*
*Stets sind $\{1\}$ und G Normalteiler von G. Man nennt $\{1\}$ den **trivialen Normalteiler von G**. Ist N ein Normalteiler von G, so schreiben wir $N \trianglelefteq G$. Gilt verschärfend $N \neq G$, so schreiben wir $N \triangleleft G$ und nennen N einen **echten Normalteiler von G**.*

Das folgende Lemma liefert einige nützliche Äquivalenzen zur Normalteilereigenschaft:

Lemma 5.3 *Seien G eine Gruppe und $N \leq G$. Dann sind äquivalent:*

(a) *N ist Normalteiler von G, d. h. es gilt $gN = Ng$ für alle $g \in G$.*

(b) *Es gilt $gNg^{-1} = N$ für alle $g \in G$.*

(c) *Es gilt $gNg^{-1} \subseteq N$ für alle $g \in G$.*

(d) *Es gilt $gng^{-1} \in N$ für alle $g \in G$ und $n \in N$.*

Beweisskizze. Die Äquivalenz von (a) und (b) folgt durch Multiplikation mit g bzw. g^{-1} von rechts, vgl. 4.2.
Die Äquivalenz von (c) und (d) folgt durch den Übergang von Teilmengen von G auf Elemente dieser Teilmengen und umgekehrt.
Es ist daher nur noch die Äquivalenz von (b) und (c) zu zeigen, wobei die Implikation (b)$\Longrightarrow$(c) klar ist. Wir zeigen (c)$\Longrightarrow$(b): Sei $g \in G$ beliebig. Nach (c) ist bereits $gNg^{-1} \subseteq N$. Wir müssen daher nur noch $N \subseteq gNg^{-1}$ zeigen. Dies folgt aber wegen

$$N = gg^{-1}Ngg^{-1} = g(g^{-1}Ng)g^{-1} \overset{g^{-1}Ng \subseteq N \text{ nach (c)}}{\subseteq} gNg^{-1}.$$ ■

Beispiel 5.4 (a) In abelschen Gruppen ist jede Untergruppe ein Normalteiler. Dort fallen also die Begriffe Normalteiler und Untergruppe zusammen.

(b) Seien K ein beliebiger Körper und $n \in \mathbb{N}$. Wir betrachten die allgemeine lineare Gruppe $\mathrm{GL}(n,K)$ aus 1.6 (d). Dann ist die Menge $Z := \{\lambda \cdot 1 \in \mathrm{GL}(n,K) \mid \lambda \in K^\times\}$ aller Vielfachen der Einheitsmatrix ein Normalteiler von $\mathrm{GL}(n,K)$.

Können Sie diese Behauptung zeigen? Worauf beruht der Beweis?

(c) Wir betrachten wieder $\mathrm{GL}(n,K)$. Die Untergruppe $\mathrm{SL}(n,K)$ aus 2.4 (e) ist ein Normalteiler von $\mathrm{GL}(n,K)$. Dies folgt mit Hilfe des Determinantenmultiplikationssatzes aus 5.3 (d), denn für beliebige $A \in \mathrm{GL}(n,K)$ und $S \in \mathrm{SL}(n,K)$ gilt

$$\det(ASA^{-1}) = \det(A) \cdot \det(S) \cdot \det(A^{-1}) \overset{\det(S)=1}{=} \det(A) \cdot \det(A^{-1}) = \det(1) = 1,$$

also $ASA^{-1} \in \mathrm{SL}(n,K)$.

(d) Für Normalteiler gilt ein Analogon von 2.10: Sind N_i mit $i \in I$ Normalteiler einer Gruppe G, so ist auch $N := \bigcap_{i\in I} N_i$ ein Normalteiler von G. Die Untergruppeneigenschaft von N folgt aus 2.10, die Normalität von N aus 5.3 (d), denn für beliebiges $g \in G$ gilt

$$n \in N \Longrightarrow \forall i \in I : n \in N_i \overset{N_i \trianglelefteq G}{\Longrightarrow} \forall i \in I : gng^{-1} \in N_i \Longrightarrow gng^{-1} \in N. \qquad \text{※}$$

Wir können nun den Begriff der Faktorgruppe definieren. Die Gruppenaxiome für G/N folgen wieder direkt aus der Gruppenstruktur von G, vgl. den Beweis zu 4.10. Dass die in (b) definierte Multiplikation tatsächlich eine Verknüpfung auf G/N ist, folgt direkt aus 5.1 und der dortigen Vorbemerkung.

Definition/Satz 5.5 *Seien G eine Gruppe und $N \leq G$. Dann sind äquivalent:*

(a) *N ist ein Normalteiler.*

(b) *Die Menge der Nebenklassen G/N von N in G wird durch die Verknüpfung*

$$\begin{array}{rll} & gN \cdot hN & := ghN \\ \textit{in Querstrichnotation:} & \overline{g} \cdot \overline{h} & := \overline{gh} \\ \textit{in additiver Schreibweise:} & (g+N)+(h+N) & := g+h+N \end{array}$$

*zu einer Gruppe, der **Faktorgruppe von G nach N**. Die Ordnung von G/N entspricht dem Index $[G : N]$.*

Beispiel 5.6 (a) Für $n \in \mathbb{N}$ ist $(\mathbb{Z}_n, +)$ die Faktorgruppe von $(\mathbb{Z}, +)$ nach $n\mathbb{Z}$. Da $\mathbb{Z}$ abelsch ist, ist auch $\mathbb{Z}_n$ eine abelsche Gruppe. $\mathbb{Z}$ ist zyklisch und wird von Eins erzeugt, $\mathbb{Z}_n$ ist zyklisch und wird von $\overline{1}$ erzeugt.

(b) Ist G eine beliebige Gruppe, so ist $G/G = \{\overline{1}\}$ die triviale Gruppe, die nur aus dem neutralen Element besteht.

(c) Wir führen 5.4 (c) fort. Der Übersichtlichkeit halber setzen wir $G := \mathrm{GL}(n, K)$ und $S := \mathrm{SL}(n, K)$. Wir wissen bereits, dass $S \trianglelefteq G$ gilt. Sei A eine beliebige Matrix aus G. Die Nebenklasse durch A, also das Gruppenelement $\overline{A} \in G/S$, ist dann gegeben durch die Menge $\overline{A} = AS = \{A \cdot X \mid X \in S\}$; die auftretende Multiplikation bezeichnet die Verknüpfung auf G, d. h. die Matrixmultiplikation. Die Elemente aus der Menge $\overline{A}$ haben nach Determinantenmultiplikationssatz dieselbe Determinante.

Um die Gruppe G/S besser beschreiben zu können, wollen wir einen besonders schönen Vertreter in $\overline{A}$ finden. Hierzu betrachten wir für $\lambda \in K^\times$ die Diagonalmatrix

$$D_\lambda := \mathrm{diag}(\lambda, \underbrace{1, 1, \dots, 1}_{n-1 \text{ Mal}}) \in G.$$

Für $\lambda, \mu \in K^\times$ gilt $D_\lambda \cdot D_\mu = D_{\lambda \cdot \mu}$ und somit $D_\lambda^{-1} = D_{\lambda^{-1}}$. ⁉

Wir setzen $a := \det(A)$. Dann gilt $A = D_a \cdot D_{a^{-1}} A$, und der Determinantenmultiplikationssatz zeigt $\det(D_{a^{-1}} A) = 1$ und somit $D_{a^{-1}} A \in S$. Wir erhalten

$$\overline{A} = \overline{D_a \cdot D_{a^{-1}} A} = D_a \cdot D_{a^{-1}} AS \overset{D_{a^{-1}} A \in S,\ 4.1\ (e)}{=} D_a S = \overline{D_a}.$$

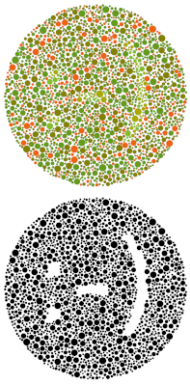
Wir können somit alle Elemente aus G/S in der Form $\overline{D_a}$ mit $a \in K^\times$ schreiben, kompliziertere Vertreter sind nicht vonnöten. Es gilt also $G/S = \{\overline{D_\lambda} \mid \lambda \in K^\times\}$.

Zudem ist $|G/S| = [G : S] = |K^\times|$, da die D_λ für verschiedene λ verschiedene Determinanten haben. G/S ist abelsch wegen ⁉

$$\overline{D_\lambda} \cdot \overline{D_\mu} = \overline{D_{\lambda \cdot \mu}} \overset{D_{\lambda\mu} = D_{\mu\lambda}}{=} \overline{D_{\mu \cdot \lambda}} = \overline{D_\mu} \cdot \overline{D_\lambda}. \qquad ⁂$$

Bemerkung 5.7 Seien G eine Gruppe und N ein Normalteiler von G. Beim Übergang von G zu G/N betrachtet man nicht mehr die einzelnen Elemente von G, sondern die von N induzierten Nebenklassen in G. Liegen zwei Elemente $g, h \in G$ in derselben Nebenklasse, so sind g und h in G/N nicht mehr unterscheidbar: Es gilt $\overline{g} = \overline{h}$ in G/N.
Beim Übergang von G zu G/N wird daher die Struktur von G „vergröbert“, man verliert Informationen. Dieser Informationsverlust kann gewünscht sein, beispielsweise wenn die Ausgangsgruppe G derart kompliziert ist, dass man „den Wald vor lauter Bäumen nicht mehr sieht“.
Nachfolgend noch ein visuelles Beispiel für einen vorteilhaften Informationsverlust[1]:

[1] Die farbige Grafik wurde mit dem *Ishihara Plate Generator* auf https://franciscouzo.github.io/ishihara/ erzeugt.



In der oberen Grafik ist ein Symbol versteckt.

Die untere Grafik entsteht aus der oberen Grafik durch „Zusammenfassen“ von Farben: Alle Farben der oberen Grafik, die einen gewissen Grünanteil unterschreiten, werden zusammengefasst und schwarz dargestellt, alle übrigen weiß. Im unteren Bild sind also fast alle Farbinformationen des oberen Bildes verloren gegangen.

Wo erkennen Sie das versteckte Symbol besser?

⋇

Faktorringe

Wir übertragen die Konstruktion von Faktorgruppen auf Ringe. Dazu gehen wir analog zum vorherigen Abschnitt und der vorherigen Vorlesung vor. Allerdings ist im Ringkontext auf Folgendes zu achten:

Bemerkung 5.8 Ringe sind nur bezüglich der *Addition* Gruppen. Beim Übertragen der Ergebnisse aus dem Abschnitt über Faktorgruppen müssen wir die dort vorkommenden Multiplikationszeichen daher gedanklich durch Additionszeichen ersetzen. Auch die von uns oft benötigten Aussagen 4.1 (d) und (e) gelten im Ring-Fall nur bezüglich der Addition.
Betrachten wir beispielsweise die Untergruppe $U := \langle \frac{2}{3} \rangle = \frac{2}{3}\mathbb{Z}$ des Rings $\mathbb{Q}$ und setzen $u := \frac{2}{3} \in U$, so folgt $\frac{4}{9} \in uU$. Allerdings ist $\frac{4}{9} \notin U$, was $uU \not\subseteq U$ zeigt. Zudem ist $1 \cdot U = U$, obwohl $1 \notin U$ gilt.
Dies zeigt, dass Untergruppen von Ringen im Allgemeinen nicht multiplikativ abgeschlossen sind. ⋇

Seien R ein Ring und $U \leq R$ eine Untergruppe von R. Für die Nebenklasse $r + U$ durch $r \in R$ schreiben wir $\overline{r}$. Da R eine abelsche Gruppe ist, ist U ein Normalteiler von R. Der Faktor R/U ist nach 5.5 eine abelsche Gruppe. Um zu einem Faktor*ring* zu gelangen, müssen wir daher nur noch eine geeignete Multiplikation auf R/U definieren. Hierzu untersuchen wir, unter welcher Bedingung an U das Produkt $\overline{r} \cdot \overline{s}$ für beliebige $r, s \in R$ in nur einer Nebenklasse enthalten ist. Wegen $r \in \overline{r}$ und $s \in \overline{s}$ gilt $rs \in \overline{r} \cdot \overline{s}$. Da $\overline{rs}$ die einzige Nebenklasse ist, die das Produkt rs enthält, kann höchstens $\overline{r} \cdot \overline{s} \subseteq \overline{rs}$ gelten.

Lemma 5.9 *Seien R ein Ring und $U \leq (R, +)$. Dann sind äquivalent:*

(a) *U ist **stark abgeschlossen** in folgendem Sinne: Für alle $u \in U$ und alle $r \in R$ gilt $ru \in U$. Die Multiplikation eines Elements aus U mit einem **beliebigen Ringelement** führt nicht aus U heraus.*

(b) *Es gilt $(r + U) \cdot (s + U) \subseteq rs + U$ für alle $r, s \in R$.*

Im Allgemeinen gilt in (b) keine Gleichheit.

Beweis.

(a)$\Longrightarrow$(b) U sei stark abgeschlossen. Dann gilt für beliebige $r, s \in R$

$$(r+U)\cdot(s+U) \overset{\text{Distributivität}}{\subseteq} rs + rU + sU + U\cdot U$$

Wegen (a) gelten $rU \subseteq U$ sowie $sU \subseteq U$ und $U \cdot U \subseteq U$. Wie gewünscht folgt $(r+U)\cdot(s+U) \subseteq rs + U + U + U = rs + U$.

(b)$\Longrightarrow$(a) Es gelte die Aussage in (b). Seien $r \in R$ und $u \in U$ beliebig gewählt. Dann ist

$$ru \in (r+U)\cdot(u+U) \overset{u+U=0+U}{=} (r+U)\cdot(0+U) \overset{\text{(b)}}{\subseteq} r\cdot 0 + U = 0 + U = U.$$

Damit ist U stark abgeschlossen. ■

Die Untergruppen aus (a) spielen in der Ringtheorie eine wichtige Rolle. Sie bekommen einen eigenen Namen:

Definition 5.10 (Ideal) *Sei R ein Ring. Eine Untergruppe $\mathfrak{a} \leq (R,+)$ heißt **Ideal von R**, wenn $\mathfrak{a}$ stark abgeschlossen ist, wenn also $ra \in \mathfrak{a}$ gilt für alle $r \in R$ und $a \in \mathfrak{a}$.*
*Stets sind $\{0\}$ und R Ideale von R. Man nennt $\{0\}$ das **triviale Ideal von R**.*
*Ist $\mathfrak{a}$ ein Ideal von R, so schreiben wir $\mathfrak{a} \trianglelefteq R$. Gilt verschärfend $\mathfrak{a} \neq R$, so schreiben wir $\mathfrak{a} \triangleleft R$ und nennen $\mathfrak{a}$ ein **echtes Ideal von R**.*

$\mathfrak{a}$ Fraktur-a

Beispiel 5.11 (a) Jede Untergruppe von $(\mathbb{Z},+)$ ist ein Ideal des Rings $\mathbb{Z}$:

Jede Untergruppe von $\mathbb{Z}$ lässt sich nach 3.4 schreiben in der Form $n\mathbb{Z}$ mit einem $n \in \mathbb{N}_0$. Seien $z \in \mathbb{Z}$ und $a \in n\mathbb{Z}$ beliebig. Dann gilt $n \mid a$ und somit auch $n \mid za$. Damit ist $za \in n\mathbb{Z}$ und $n\mathbb{Z}$ ist stark abgeschlossen.

(b) In 5.8 haben wir eine Untergruppe von $\mathbb{Q}$ gesehen, die kein Ideal von $\mathbb{Q}$ ist. Die Ideal-Bedingung ist daher stärker als die Untergruppen-Bedingung.

(c) Analog zu 5.4 (d) folgt, dass der Schnitt von Idealen wieder ein Ideal ist. Man kann daher wie in 2.11 ein Idealerzeugnis definieren, vgl. Vorlesung 17. ※

Der folgende Satz liefert ein einfaches Kriterium, um zu entscheiden, wann ein Ideal dem gesamten Ring entspricht:

Satz 5.12 *Seien R ein Ring und $\mathfrak{a}$ ein Ideal von R. Dann sind äquivalent:*

(a) $\mathfrak{a} = R$.

(b) $\mathfrak{a} \cap R^\times \neq \emptyset$, *d.h. $\mathfrak{a}$ enthält mindestens eine Einheit.*

(c) $1 \in \mathfrak{a}$.

Beweis. Wir zeigen den Satz per Ringschlussprinzip. Die Implikationen (a)$\Longrightarrow$(c) und (c)$\Longrightarrow$(b) sind klar. Zu zeigen ist noch (b)$\Longrightarrow$(a):
Sei $a \in \mathfrak{a}$ eine Einheit von R. Dann existiert $b \in R$ mit $ba = 1$. Für beliebiges $r \in R$ gilt dann $r = r \cdot 1 = rb \cdot a \in \mathfrak{a}$ aufgrund der starken Abgeschlossenheit von $\mathfrak{a}$. Also ist $R \subseteq \mathfrak{a}$ und somit $R = \mathfrak{a}$. ■

Wir können jetzt den Begriff des Faktorrings definieren. Die Ringaxiome für $R/\mathfrak{a}$ folgen wieder direkt aus der Ringstruktur von R, vgl. den Beweis zu 4.10. Dass die in (b) definierte Addition bzw. Multiplikation eine Verknüpfung auf $R/\mathfrak{a}$ ist, folgt aus 5.5 bzw. 5.9.

Definition/Satz 5.13 *Seien R ein Ring und $\mathfrak{a}$ eine Untergruppe von $(R, +)$. Dann sind äquivalent:*

(a) *$\mathfrak{a}$ ist ein Ideal.*

(b) *Die Menge der Nebenklassen $R/\mathfrak{a}$ von $\mathfrak{a}$ in R wird durch die Verknüpfungen*

$$(r + \mathfrak{a}) + (s + \mathfrak{a}) := r + s + \mathfrak{a} \qquad \text{bzw. in Querstrichnotation:} \quad \overline{r} + \overline{s} := \overline{r + s},$$

$$(r + \mathfrak{a}) \cdot (s + \mathfrak{a}) := rs + \mathfrak{a} \qquad \text{bzw. in Querstrichnotation:} \quad \overline{r} \cdot \overline{s} := \overline{rs}$$

*zu einem Ring, dem **Faktorring von R nach $\mathfrak{a}$**. Die Ordnung von $R/\mathfrak{a}$ entspricht dem Index $[R : \mathfrak{a}]$.*

Beispiel 5.14 (a) Für $n \in \mathbb{N}$ ist $\mathbb{Z}_n$ der Faktorring von $\mathbb{Z}$ nach dem Ideal $n\mathbb{Z}$. Da in $\mathbb{Z}$ wegen 5.11 die Begriffe Ideal und Untergruppe zusammenfallen, konnten wir in Vorlesung 4 diese Ringe definieren, ohne den Idealbegriff zu verwenden.

(b) Ist R ein beliebiger Ring, so ist $R/R = \{\overline{0}\}$ der Nullring. Es gilt $\overline{0} = \overline{1}$.

(c) Seien K ein Körper und $\mathfrak{a}$ ein nicht-triviales Ideal von K. Dann enthält $\mathfrak{a}$ eine Einheit von K, und es gilt $\mathfrak{a} = K$ nach 5.12. Somit besitzt K nur die beiden Ideale K und $\{0\}$. Die möglichen Faktorringe von K sind daher der Nullring K/K oder der Ring

$$K/\{0\} = \{k + \{0\} \mid k \in K\} = \{\{k\} \mid k \in K\}.$$

Beim Übergang von K auf $K/\{0\}$ ersetzt man also nur Elemente von K durch einelementige Teilmengen von K. Hierbei geht keinerlei Information verloren. Mit dem Isomorphie-Konzept aus der nächsten Vorlesung können wir sagen: K und $K/\{0\}$ sind isomorph.

Faktorringe eines Körpers sind also entweder Nullringe oder isomorph zum ursprünglichen Körper und daher algebraisch uninteressant. Dies ist der Grund, warum in der Algebra der Begriff des „Faktorkörpers“ nicht auftritt. ⋇

6. Homomorphismen

Worum geht es? Wir beschäftigen uns mit *Homomorphismen*. Dies sind Abbildungen zwischen zwei algebraischen Strukturen desselben Typs, die mit deren Verknüpfungen „verträglich“ sind. Typische Beispiele für Homomorphismen sind die linearen Abbildungen aus der Linearen Algebra. Wir beweisen den für die Algebra äußerst wichtigen *Homomorphiesatz* und als Anwendung desselben unter anderem den *chinesischen Restsatz für Restklassenringe*. ⁜

Homomorphismen

Homomorphismen sind Abbildungen zwischen zwei Strukturen gleichen Typs, die die Verknüpfungen der beiden Strukturen respektieren: Man fordert, dass die Elemente aus der einen Struktur so in die anderen Struktur abgebildet werden, dass sich Verknüpfungen der Bilder so verhalten wie die entsprechenden Verknüpfungen der Urbilder. Dies bedeutet unter anderem, dass Homomorphismen neutrale Elemente wieder auf neutrale Elemente abbilden müssen und dass das Bild eines Produktes dem Produkt der Bilder entspricht.
Genauer fordert man (siehe 6.3 (d) für die grau eingefärbten Textbestandteile):

Definition 6.1 (Homomorphismus)

(a) *Seien $(G,\cdot)$ und $(H,\odot)$ Gruppen mit Neutralem 1_G bzw. 1_H. Eine Abbildung $\varphi: G \to H$ heißt* ***(Gruppen-)Homomorphismus****, wenn φ den nachstehenden Bedingungen genügt:*

φ Phi

Verträglichkeit *Für alle $a,b \in G$ gilt $\varphi(a\cdot b) = \varphi(a)\odot\varphi(b)$.*

Neutrale auf Neutrale *Es gilt $\varphi(1_G) = 1_H$.*

(b) *Seien $(R,+,\cdot)$ und $(S,\oplus,\odot)$ Ringe mit Neutralen 0_R und 1_R bzw. 0_S und 1_S. Eine Abbildung $\varphi: R \to S$ heißt* ***(Ring-)Homomorphismus****, wenn φ den nachstehenden Bedingungen genügt:*

Verträglichkeit *Für alle $a,b \in R$ gelten $\varphi(a+b) = \varphi(a)\oplus\varphi(b)$ sowie $\varphi(a\cdot b) = \varphi(a)\odot\varphi(b)$.*

Neutrale auf Neutrale *Es gilt $\varphi(0_R) = 0_S$ sowie $\varphi(1_R) = 1_S$.*

(c) *Einen Ringhomomorphismus $R \to S$ nennt man* ***(Körper-)Homomorphismus****, wenn R und S Körper sind.*

Beispiel 6.2 (a) Für beliebige Gruppen G,H ist die Abbildung $G \to H$ mit $g \mapsto 1$ ein Homomorphismus.

Sind R,S Ringe, so ist die Abbildung $R \to S$ mit $r \mapsto 0$ genau dann ein Ringhomomorphismus, wenn $S = \{0\}$ gilt. ⁉

Die Abbildung $\mathbb{Z} \to \mathbb{Z}$ mit $z \mapsto 0$ ist ein Gruppen-, aber kein Ringhomomorphismus.

(b) Jede lineare Abbildung zwischen Vektorräumen ist ein (additiv geschriebener) Gruppenhomomorphismus.

(c) Seien $r \in \mathbb{N}$, $A, B_1, \dots, B_r$ Gruppen oder Ringe und $\varphi_i : A \to B_i$ Gruppen- bzw. Ringhomomorphismen. Dann folgt aus der Definition der Verknüpfungen in direkten Produkten, dass auch die Abbildung

$$\varphi : A \to B_1 \times \cdots \times B_r, \qquad a \mapsto (\varphi_1(a), \dots, \varphi_r(a))$$

ein Gruppen- bzw. Ringhomomorphismus ist. ※

Bemerkung 6.3 (a) Ist aus dem Kontext klar, welcher Homomorphismentyp gemeint ist, so werden wir meist nur von einem *Homomorphismus* sprechen und seinen Typ nicht explizit erwähnen.

(b) Die Verknüpfungen der algebraischen Strukturen, zwischen denen ein Homomorphismus definiert ist, können völlig unterschiedlich bezeichnet sein. Wir haben dies in 6.1 durch Verwenden unterschiedlicher Verknüpfungszeichen verdeutlicht.

(c) Die Bedingungen, die in obiger Definition an die Abbildung φ gestellt werden, werden von Mal zu Mal immer spezieller: Ein Körperhomomorphismus ist daher stets auch ein Ringhomomorphismus, ein Ringhomomorphismus stets auch ein Gruppenhomomorphismus. Aussagen, die sich auf Gruppenhomomorphismen beziehen, übertragen sich somit auf Ringhomomorphismen und daher dann auch auf Körperhomomorphismen.

(d) Sind G, H Gruppen und $\varphi : G \to H$ ein Homomorphismus, so folgt aus der Verträglichkeitsbedingung, dass $\varphi(1) = \varphi(1 \cdot 1) = \varphi(1) \cdot \varphi(1)$ ist. Kürzen durch $\varphi(1)$ liefert $1 = \varphi(1)$.

Dies zeigt, dass die Forderung *Neutrale auf Neutrale* in 6.1 (a) überflüssig ist. Im Ringhomomorphismen-Fall liefert die Verträglichkeit stets $\varphi(0) = 0$.

Auf die grau eingefärbten Bedingungen in 6.1 kann also verzichtet werden.

(e) Hingegen kann auf die Forderung $\varphi(1) = 1$ in 6.1 (b) *nicht* verzichtet werden. Dies haben wir bereits in 6.2 (a) gesehen. ※

Die folgenden grundlegenden Aussagen über Gruppenhomomorphismen haben Sie teilweise bereits in der Linearen Algebra gesehen. Man zeigt sie mit Hilfe von Induktion, dem Untergruppenkriterium und den Äquivalenzen aus 5.3, vgl. [KM17, Lemma 2.11 auf S. 26] und [KM17, Lemma 4.3 auf S. 51].

Satz 6.4 *Seien G, H Gruppen und $\varphi : G \to H$ ein Homomorphismus. Dann gelten:*

(a) *Für alle $g \in G$ und $z \in \mathbb{Z}$ gilt $\varphi(g^z) = \varphi(g)^z$.*

(b) *Aus $U \leq G$ folgt $\varphi(U) \leq H$, d.h. Homomorphismen bilden Untergruppen auf Untergruppen ab. Man sagt hierzu auch, dass* ***homomorphe Bilder*** *von Untergruppen wieder Untergruppen sind.*

(c) *Aus $V \leq H$ folgt $\varphi^{-1}(V) \leq G$, d.h. Urbilder von Untergruppen unter Homomorphismen sind wieder Untergruppen. Man sagt hierzu auch, dass* ***homomorphe Urbilder*** *von Untergruppen wieder Untergruppen sind.*

(d) *Aus $N \trianglelefteq H$ folgt $\varphi^{-1}(N) \trianglelefteq G$, d.h. homomorphe Urbilder von Normalteilern sind wieder normal.*

Knobelfrage. Sind auch homomorphe Bilder von Normalteilern normal? Falls nein, woran scheitert ein Beweis der Aussage? ⁉

Der nachstehende Satz liefert einige Aussagen über Ringhomomorphismen.

Satz 6.5 *Seien R, S Ringe und $\varphi : R \to S$ ein Homomorphismus. Dann gelten:*

(a) *Für alle $r \in R$ und $n \in \mathbb{N}_0$ gilt $\varphi(r^n) = \varphi(r)^n$. Ist r eine Einheit von R, so ist $\varphi(r)$ eine Einheit von S und die Aussage gilt sogar für $n \in \mathbb{Z}$.*

(b) *Homomorphe Bilder von Unterringen sind wieder Unterringe. Homomorphe Urbilder von Unterringen sind wieder Unterringe.*

(c) *Homomorphe Urbilder von Idealen sind wieder Ideale.* (*Sind homomorphe Bilder von Idealen wieder Ideale?*) ⁉

Die Aussage, dass Ringhomomorphismen Einheiten auf Einheiten abbilden, können wir auch wie folgt formulieren:

Korollar 6.6 *Seien R, S Ringe und $\varphi : R \to S$ ein Homomorphismus. Dann ist die Einschränkung $\varphi|_{R^\times} : R^\times \to S^\times$ ein Gruppenhomomorphismus.*

Durch Überprüfen der Definition sieht man:

Satz 6.7 *Die Verkettung von Homomorphismen ist wieder ein Homomorphismus.*

Mit den nachstehenden Bezeichnungen fordern wir gewisse Zusatzeigenschaften für Homomorphismen:

Definition 6.8 *Es sei $\varphi : A \to B$ ein Homomorphismus.*
Ist φ injektiv bzw. surjektiv bzw. bijektiv, so nennt man φ einen ***Monomorphismus*** *bzw.* ***Epimorphismus*** *bzw.* ***Isomorphismus****. Gilt $A = B$, so nennt man φ einen* ***Endomorphismus****. Ein bijektiver Endomorphismus heißt* ***Automorphismus****.*

Vereinbarung zur Schreibweise 6.9 Existiert zwischen zwei algebraischen Strukturen A und B ein Isomorphismus, so schreiben wir $A \cong B$. ⁕

Isomorphismen besitzen Umkehrabbildungen. Auch diese sind wieder Homomorphismen. Einen Beweis dieser Aussage finden Sie beispielsweise in [KM17, Lemma 1.6, S. 12] bzw. [KM17, Lemma 13.2, S. 176].

Satz 6.10 *Die Umkehrabbildung eines Isomorphismus ist wieder ein Isomorphismus.*

Im folgenden Beispiel verzichten wir oft auf den Nachweis der Homomorphie. Um ein Gespür für Homomorphismen zu bekommen, sollten Sie dennoch versuchen, den (meist einfachen) Beweis zu führen.

Beispiel 6.11 (a) Für jede abelsche Gruppe G und jedes $z \in \mathbb{Z}$ ist die Abbildung

$$G \to G, \qquad g \mapsto g^z \qquad \text{(additiv geschrieben: } g \mapsto z \cdot g\text{)}$$

nach 1.9 ein Endomorphismus.

(b) Die Exponentialfunktion $\exp : \mathbb{R} \to \mathbb{R}^+$ ist ein Isomorphismus; die Homomorphie von exp folgt aus der Funktionalgleichung.

(c) Seien G eine Gruppe und $g \in G$. Unter der **Konjugation mit g** verstehen wir die Abbildung

$$k_g : G \to G, \qquad x \mapsto gxg^{-1}.$$

k_g ist ein Automorphismus von G: Die Homomorphie von k_g folgt wegen

$$k_g(xy) = gxyg^{-1} = gxg^{-1} \cdot gyg^{-1} = k_g(x) \cdot k_g(y) \qquad \text{für alle } x, y \in G.$$

k_g ist zudem bijektiv; die Umkehrabbildung zu k_g ist durch $k_{g^{-1}}$ gegeben. ⁉

Können Sie abelsche Gruppen mit Hilfe der Konjugation charakterisieren? ⁉

(d) Sei M eine Gruppe, ein Ring oder ein Körper. Aus 6.7 und 6.10 folgt, dass die Menge $\mathrm{Aut}(M)$ aller Automorphismen von M eine Untergruppe von $\mathrm{Sym}(M)$ bildet. Man nennt $\mathrm{Aut}(M)$ die **Automorphismengruppe von M**.

Was ist die Eins in $\mathrm{Aut}(M)$? ⁂ ⁉

Mit Hilfe des Kerns kann man Homomorphismen auf Injektivität untersuchen:

Definition 6.12 (Kern) *Sei $\varphi : G \to H$ ein Gruppenhomomorphismus. Dann bezeichnet man das Urbild $\ker \varphi := \varphi^{-1}(\{1\})$ als **Kern von φ**. Wegen 6.4 (d) ist $\ker \varphi$ ein Normalteiler von G.*

Bemerkung 6.13 Obige Definition gilt auch für *Ring*homomorphismen $\varphi : R \to S$. Hier ist $\ker \varphi = \varphi^{-1}(\{0\})$. Nach 6.5 (c) ist $\ker \varphi$ ein Ideal von R. ⁂

Satz 6.14 *Ein Homomorphismus φ ist genau dann injektiv, wenn sein Kern mit dem trivialen Normalteiler $\{1\}$ bzw. dem trivialen Ideal $\{0\}$ übereinstimmt.*

Beweis. Es reicht, die Behauptung für einen Gruppenhomomorphismus $\varphi : G \to H$ nachzuweisen. ?

$\Longrightarrow$ Wegen $\varphi(1) = 1$ ist $1 \in \ker \varphi$. Die Injektivität von φ liefert $\ker \varphi = \{1\}$.

$\Longleftarrow$ Sei $\ker \varphi = \{1\}$. Seien $g, h \in G$ mit $\varphi(g) = \varphi(h)$ gegeben. Dann gilt $\varphi(gh^{-1}) = 1$, also $gh^{-1} \in \ker \varphi$, also $gh^{-1} = 1$ und somit $g = h$. Also ist φ injektiv. ? ■

Beispiel 6.15 (a) Sei $\varphi : K \to L$ ein Körperhomomorphismus. Dann ist $\varphi(1) = 1 \neq 0$ und somit $1 \notin \ker \varphi$. Nach 5.14 (c) folgt $\ker \varphi = \{0\}$ und daher die Injektivität von φ. Körperhomomorphismen sind also stets injektiv.

(b) Sind G eine Gruppe und N ein Normalteiler von G, so folgt aus der Definition der Multiplikation in Faktorgruppen, dass die Abbildung $\varphi : G \to G/N$ mit $\varphi(g) := \overline{g}$ ein Epimorphismus ist. Es gilt $\ker \varphi = N$.

Analog gilt für Ringe: Sind R ein Ring und $\mathfrak{a}$ ein Ideal von R, so ist die Abbildung $\varphi : R \to R/\mathfrak{a}$ mit $\varphi(r) := \overline{r}$ ein Epimorphismus mit $\ker \varphi = \mathfrak{a}$.

Die oben definierten Abbildungen φ nennt man den **kanonischen Epimorphismus von G auf G/N** bzw. **von R auf $R/\mathfrak{a}$**. ⁜

Der Homomorphiesatz

Wir kommen zu einem der wichtigsten Sätze der Algebra. Zur Vorbereitung benötigen wir das nachstehende, etwas technische Lemma, in dem der Begriff der Wohldefiniertheit eine zentrale Rolle spielt.

Lemma 6.16 *Seien A, B Gruppen oder Ringe und $\varphi : A \to B$ ein Homomorphismus. Dann ist durch die Festsetzung*

$$\psi : A/\ker \varphi \to B, \qquad \overline{a} \mapsto \varphi(a)$$

ψ Psi

ebenfalls ein Homomorphismus gegeben. Beide Homomorphismen haben dasselbe Bild, d.h. es gilt $\varphi(A) = \psi(A/\ker \varphi)$.

Vorbemerkung zum Beweis. Homomorphismen sind Abbildungen, die den Homomorphiebedingungen genügen. Im obigen Lemma ist nicht einmal klar, ob ψ überhaupt eine Abbildung ist. (Bevor Sie weiterlesen: Wo liegt das Problem?) ?

Das Bild $\psi(\overline{a})$ haben wir mit Hilfe des Vertreters a definiert. Allerdings darf $\psi(\overline{a})$ nur von der *Menge* $\overline{a}$, nicht jedoch von einem einzelnen Vertreter $a \in \overline{a}$ abhängen. Wir müssen daher sicherstellen, dass $\psi(\overline{a})$ **vertreterunabhängig** definiert ist: Ist b ein beliebiger Vertreter von $\overline{a}$, gilt also $\overline{a} = \overline{b}$, so muss $\psi(\overline{a}) = \psi(\overline{b})$ sein. Diese Vertreterunabhängigkeit nennt man **Wohldefiniertheit**.

Beweis. Wir zeigen zunächst, dass ψ eine Abbildung ist. Hierzu ist nachzuweisen, dass ψ *jedem* Element aus $A/\ker\varphi$ *genau einen Wert* zuordnet.
Die erste Bedingung ist klar: Ein Element aus $A/\ker\varphi$ lässt sich schreiben in der Form $\bar{a}$ mit einem Vertreter $a \in A$. Diesem Element wird der Wert $\varphi(a)$ zugeordnet.
Zum Nachweis der zweiten Bedingung zeigen wir die Wohldefiniertheit von ψ: Sei ein beliebiges Element aus $A/\ker\varphi$ vorgelegt. Seien $a, b \in A$ Vertreter dieses Elements. Nach 4.5 (b) existiert dann ein $k \in \ker\varphi$ mit

$$b = ak \text{ (im Gruppenfall)} \qquad \text{bzw.} \qquad b = a + k \text{ (im Ringfall)}.$$

Im Gruppenfall gilt dann:

$$\psi(\bar{b}) = \varphi(b) = \varphi(ak) \overset{\varphi \text{ homomorph}}{=} \varphi(a)\cdot\varphi(k) \overset{k\in\ker\varphi}{=} \varphi(a)\cdot 1 = \varphi(a) = \psi(\bar{a}).$$

Im Ringfall folgt $\psi(\bar{b}) = \psi(\bar{a})$ auf ähnliche Weise. Dies zeigt, dass jedem Element aus $A/\ker\varphi$ stets nur genau ein Wert zugeordnet wird und dass ψ eine Abbildung ist.
Wir zeigen nun die Homomorphiebedingungen im Gruppenfall; der Beweis im Ringfall verläuft analog. Seien $\bar{a}, \bar{b} \in A/\ker\varphi$ beliebig gegeben. Dann ist

$$\psi(\bar{a}\cdot\bar{b}) \overset{\text{Def. }\cdot}{=} \psi(\overline{ab}) \overset{\text{Def. von }\psi}{=} \varphi(ab) \overset{\varphi \text{ homomorph}}{=} \varphi(a)\cdot\varphi(b) \overset{\text{Def. von }\psi}{=} \psi(\bar{a})\cdot\psi(\bar{b}).$$

Die Aussage über die Bilder beider Homomorphismen folgt wegen

$$\varphi(A) = \{\varphi(a) \mid a \in A\} = \{\psi(\bar{a}) \mid a \in A\} = \psi(A/\ker\varphi). \qquad \blacksquare$$

Knobelfrage. Hätten wir die Wohldefiniertheit bei der Definition des kanonischen Epimorphismus in 6.15 (b) nicht auch zeigen müssen? ⁉

Satz 6.17 (Homomorphiesatz) *Seien A, B Gruppen oder Ringe und $\varphi : A \to B$ ein Homomorphismus. Dann ist die Abbildung*

$$\psi : A/\ker\varphi \to \varphi(A), \qquad \bar{a} \mapsto \varphi(a)$$

ein Isomorphismus. Es gilt also $A/\ker\varphi \cong \varphi(A)$.
Man sagt oft kürzer: Definitionsbereich modulo Kern ist isomorph zum Bild.

Beweis. Aufgrund des Lemmas ist nur noch die Injektivität von ψ zu zeigen. Hierzu bestimmen wir den Kern von ψ und benutzen 6.14. Im Gruppenfall ist $\bar{a} \in \ker\psi$ genau dann, wenn $\psi(\bar{a}) = \varphi(a) = 1$ gilt, also wenn $a \in \ker\varphi$ ist. Dies gilt genau für $\bar{a} = \bar{1}$, was $\ker\psi = \{\bar{1}\}$ und damit die Injektivität von g liefert. Im Ringfall schließt man analog. $\blacksquare$ ⁉

Beispiel 6.18 Für jedes $n \in \mathbb{N}$ und jeden Körper K ist die Determinantenabbildung $\det : \mathrm{GL}(n,K) \to K^\times$ mit $A \mapsto \det(A)$ ein Epimorphismus. Es gilt $\ker\det = \mathrm{SL}(n,K)$. Der Homomorphiesatz liefert ⁉

$$\mathrm{GL}(n,K)/\mathrm{SL}(n,K) \cong \det(\mathrm{GL}(n,K)) = K^\times.$$

Vergleichen Sie dies mit 5.6 (c). Wir haben dort $\mathrm{GL}(n,K)/\mathrm{SL}(n,K) = \{\overline{D}_\lambda \mid \lambda \in K^\times\}$ gezeigt. Können Sie einen Isomorphismus $\{\overline{D}_\lambda \mid \lambda \in K^\times\} \to K^\times$ angeben? ⁂ ⁉

Der chinesische Restsatz für Restklassenringe

Wir stellen eine etwas kompliziertere Anwendung des Homomorphiesatzes vor. Diese erlaubt es uns, den Ring $\mathbb{Z}_n$ als direktes Produkt von Restklassenringen kleinerer Ordnung zu schreiben. Das folgende Resultat nimmt in der elementaren Zahlentheorie eine zentrale Rolle ein:

Satz 6.19 (Chinesischer Restsatz für Restklassenringe) *Die natürliche Zahl n sei zerlegt in der Form $n = n_1 \cdots n_r$ mit paarweise teilerfremden $n_i \in \mathbb{N}$. Dann ist die Abbildung*

$$\varphi : \mathbb{Z} \to \mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_r}, \qquad z \mapsto (\bar{z}, \bar{z}, \dots, \bar{z})$$

ein Epimorphismus mit Kern $n\mathbb{Z}$. Der Homomorphiesatz liefert $\mathbb{Z}_n \cong \mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_r}$.

Beweis. Wegen 6.15 (b) und 6.2 (c) ist φ ein Ringhomomorphismus. Es gilt $z \in \ker \varphi$ genau dann, wenn $z \in n_k\mathbb{Z}$ ist für alle $k \in \{1, \dots, r\}$. Da die n_i paarweise teilerfremd sind, ist dies gleichbedeutend damit, dass $z \in n_1 \cdot n_2 \cdots n_r\mathbb{Z} = n\mathbb{Z}$ gilt. Nach Homomorphiesatz ist dann $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z} = \mathbb{Z}/\ker\varphi \cong \varphi(\mathbb{Z})$.
Wegen $|\mathbb{Z}_n| = n$ liefert die eben gezeigte Isomorphie, dass $|\varphi(\mathbb{Z})| = n$ ist. Die Surjektivität von φ folgt, weil $|\mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_r}| = n_1 \cdots n_r = n$ ist. ■

Der chinesische Restsatz liefert zusammen mit 6.6

Korollar 6.20 *Die natürliche Zahl n sei zerlegt in der Form $n = n_1 \cdots n_r$ mit paarweise teilerfremden $n_i \in \mathbb{N}$. Dann gilt $\mathbb{Z}_n^\times \cong \mathbb{Z}_{n_1}^\times \times \cdots \times \mathbb{Z}_{n_r}^\times$.*

Obiges Korollar lässt sich in eine Aussage über die Eulersche φ-Funktion übersetzen:

Korollar 6.21 *Sind die natürlichen Zahlen $n_1, \dots, n_r$ paarweise teilerfremd, so gilt*

$$\varphi(n_1 \cdots n_r) = \varphi(n_1) \cdots \varphi(n_r).$$

Gilt diese Aussage auch für nicht-teilerfremde Zahlen? ?

Bemerkung 6.22 (a) Die feinste Zerlegung von $n \in \mathbb{N}$ in paarweise teilerfremde Faktoren ist durch die Primfaktorzerlegung von n gegeben. Meist wird 6.19 auf diese Zerlegung von n angewandt.

(b) Die Aussage in 6.21 nennt man auch die **Multiplikativität der φ-Funktion**. Um $\varphi(n)$ für beliebige $n \in \mathbb{N}$ zu berechnen, reicht es wegen (a) aus, die φ-Funktion für beliebige Primzahlpotenzen ausrechnen zu können. Für diesen Spezialfall liegen explizite Formeln vor, die wir in den Übungen beweisen werden. → Übung

(c) Beachten Sie, dass die Objekte $\bar{z}$ in der Definition von φ in 6.19 paarweise verschieden sind: Die Nebenklasse $\bar{z}$ an der i-ten Stelle bezeichnet die Menge $z + n_i\mathbb{Z}$. ⁜

Knobelfrage. Gibt es eine ganze Zahl z mit $z \in 17 + 23\mathbb{Z}$ und $z \in 12 + 101\mathbb{Z}$? Falls ja, gibt es auch ein solches z mit $z \in \{0, 1, \dots, 23 \cdot 101 - 1\}$? ?

Teil II.
Gruppen

In diesem Abschnitt fokussieren wir uns vorwiegend auf endliche Gruppen.

Mit Hilfe der Nebenklassen-Partition beweisen wir zunächst den *Satz von Lagrange*, führen *Elementordnungen* ein und untersuchen zyklische Gruppen genauer; insbesondere werden wir, bis auf Isomorphie, alle zyklischen Gruppen inklusive deren Untergruppenstruktur beschreiben.
Diese Resultate werden vom *Struktursatz* auf endliche abelsche Gruppen verallgemeinert. Wir zitieren den Satz und geben einige Beispiele an.
Im Anschluss beschäftigen wir uns mit der wichtigen Klasse der symmetrischen Gruppen. Wir untersuchen das Abbildungsverhalten ihrer Elemente und leiten mit der *Zykeldarstellung* eine für algebraische Zwecke besonders geeignete Schreibweise für Permutationen her. Mit Hilfe von *Transpositionszerlegungen* definieren wir das *Signum* einer Permutation und schließlich die *alternierenden Gruppen* A_n. Unsere Untersuchung von S_n und A_n auf Normalteiler liefert schließlich den Begriff der *einfachen Gruppe*.

Wir motivieren und behandeln ausführlich den für die Gruppentheorie zentralen Begriff der *Gruppenoperation*. Hier betrachtet man eine Gruppe nicht mehr als Menge von abstrakten Elementen, sondern fasst die Gruppenelemente als bijektive Funktionen auf. Wir klären, wie dies genau geschieht und welches Abbildungsverhalten die Gruppenelemente aufweisen. Dies führt auf das wichtige Konzept der *Bahn*.
Mit Hilfe von Gruppenoperationen beweisen wir die äußerst wichtigen *Sylowsätze*, die die Existenz gewisser Untergruppen in endlichen Gruppen sicherstellen. Wir zeigen an vielen Beispielen typische Anwendungen der Sylowsätze.

Zuletzt beschäftigen wir uns mit der Konstruktion von Untergruppen innerhalb von Gruppen. Hier fokussieren wir uns zunächst auf *Komplexprodukte* und anschließend auf die Sonderfälle des *internen direkten* und des *internen semidirekten Produkts*. Anschließend behandeln wir auch die externe Variante des semidirekten Produkts und diskutieren einige Anwendungsfälle; wir geben beispielsweise ein Kriterium für die Nicht-Kommutativität von Gruppen der Ordnung pq mit Primzahlen p und q an.

7. Lagrange, Elementordnung, zyklische Gruppen

Worum geht es? Wir beweisen den *Satz von Lagrange*, eines der grundlegendsten Resultate der endlichen Gruppentheorie. Als Anwendung klassifizieren wir alle Gruppen von Primzahlordnung.
Anschließend beschäftigen wir uns mit der *Ordnung von Gruppenelementen*. Dieser Begriff ist nahe mit dem Begriff der zyklischen Gruppe verwandt und erlaubt es, tiefe Resultate über zyklische Gruppen zu beweisen; wir werden beispielsweise alle *Isomorphietypen* sowie den *Untergruppenverband* zyklischer Gruppen klassifizieren. ⁜

Der Satz von Lagrange

Der Satz von Lagrange ist für die endliche Gruppentheorie von äußerster Bedeutung. Wir benötigen als Vorbereitung für seinen Beweis das nachstehende Lemma, das für einen Großteil der Teilbarkeitsbedingungen, die man in der endlichen Gruppentheorie an vielen Stellen vorfindet, verantwortlich ist:

Lemma 7.1 *Sei G eine Gruppe mit Untergruppe $U \leq G$. Dann sind alle Nebenklassen von U in G gleichmächtig, d. h. zu beliebigen $g, h \in G$ existiert eine Bijektion $gU \to hU$.*

Beweis. Seien $g, h \in G$ beliebig. Dann ist die Abbildung $gU \to hU$ mit $x \mapsto hg^{-1}x$ bijektiv (mit Umkehrabbildung $hU \to gU$ mit $x \mapsto gh^{-1}x$). ■ ⁉

Speziell für *endliches* G sagt obiges Lemma aus, dass jede Nebenklasse aus G/U dieselbe Anzahl an Elementen enthält. Es gilt also $|gU| = |1 \cdot U| = |U|$ für alle $g \in G$. Dies liefert:

Satz 7.2 (Lagrange) *Sei G eine endliche Gruppe mit Untergruppe $U \leq G$. Dann ist der Index $[G : U]$ von U in G gegeben durch $[G : U] = \frac{|G|}{|U|}$.*

Beweis. Es sei $n := [G : U]$. Da die Nebenklassen von U in G die Gruppe G partitionieren, existieren Elemente $g_1, \dots, g_n \in G$ mit $G = g_1U \cup g_2U \cup \cdots \cup g_nU$. Das Symbol $\cup$ bedeutet hierbei, dass die Mengen g_iU paarweise disjunkt sind. Es folgt

$$|G| \overset{\text{paarw. Disjunktheit}}{=} \sum_{i=1}^{n} |g_iU| \overset{|g_iU|=|U|}{=} \sum_{i=1}^{n} |U| = n \cdot |U|.$$

Umstellen dieser Gleichung zeigt die Behauptung $n = \frac{|G|}{|U|}$. ■

Nach obigem Satz ist $|G| = [G : U] \cdot |U|$. Da $[G : U]$ eine natürliche Zahl ist, folgt:

Korollar 7.3 (Lagrange) *Sei G eine endliche Gruppe. Dann teilt die Ordnung jeder Untergruppe $U \leq G$ die Ordnung von G, d. h. es gilt $|U| \,\big|\, |G|$ für alle $U \leq G$.*

Bemerkung 7.4 (a) Der Satz von Lagrange liefert eine Einschränkung, welche Ordnungen für Untergruppen einer endlichen Gruppe überhaupt möglich sind. Diese Einschränkung ist umso stärker, je weniger Teiler die Gruppenordnung besitzt. Die stärkste Einschränkung liegt im Fall $|G| = p$ mit einer Primzahl p vor. Diese Situation analysieren wir im nächsten Satz.

(b) In 7.3 gilt im Allgemeinen nicht die Rückrichtung: Es gibt endliche Gruppen, die zu einem Teiler t ihrer Gruppenordnung keine Untergruppe U mit $|U| = t$ besitzen. Ein Beispiel für eine solche Gruppe werden wir in 9.11 sehen.

Endliche Gruppen, die zu jedem Teiler ihrer Ordnung (mindestens) eine Untergruppe besitzen, nennt man **Lagrangegruppen**. Wir werden in 7.22 sehen, dass endliche zyklische Gruppen Lagrangegruppen sind. ⁜

Direkt aus Lagrange folgt, dass Gruppen mit Primzahlordnung zyklisch sind:

Satz 7.5 (Gruppen von Primzahlordnung) *Sei G eine Gruppe mit Ordnung $p \in \mathbb{P}$. Dann ist jedes $g \in G$ mit $g \neq 1$ ein Erzeuger von G. Insbesondere ist G zyklisch.*

Beweis. Für beliebiges $g \in G \setminus \{1\}$ betrachten wir die Untergruppe $U := \langle g \rangle \neq \{1\}$. Da G nach Lagrange nur die Untergruppen $\{1\}$ und G besitzt, gilt $U = G$. ■

Eine weitere Folgerung aus Lagrange ist die folgende Aussage über Indizes:

Satz 7.6 (Indexmultiplikativität) *Sei G eine endliche Gruppe mit Untergruppen $U, V \leq G$. Gilt $U \leq V \leq G$, so ist $[G : U] = [G : V] \cdot [V : U]$.*

Beweis. Mit 7.2 folgt $[G : V] \cdot [V : U] = \frac{|G|}{|V|} \cdot \frac{|V|}{|U|} = \frac{|G|}{|U|} = [G : U]$. ■

Ordnung von Gruppenelementen

Für ein Gruppenelement g betrachten wir die Potenzen g^z mit $z \in \mathbb{Z}$. Es ergeben sich zwei Fälle: Die Potenzen sind entweder paarweise verschieden, oder es gibt ganze Zahlen $x \neq y$ mit $g^x = g^y$.
Im ersten Fall gilt $g^z = 1$ genau für $z = 0$; insbesondere ist $g^n \neq 1$ für alle $n \in \mathbb{N}$.
Im zweiten Fall folgt nach Multiplikation mit g^{-x} bzw. g^{-y}, dass $g^{x-y} = 1 = g^{y-x}$ gilt. Da einer der beiden Exponenten positiv ist, existiert somit ein $n \in \mathbb{N}$ mit $g^n = 1$. Wegen der Wohlordnung von $\mathbb{N}$ gibt es dann auch eine kleinste natürliche Zahl mit dieser Eigenschaft. ⁉
Diese Überlegungen motivieren die folgende Definition:

Definition 7.7 (Elementordnung) *Sei g ein Gruppenelement. Gilt $g^n \neq 1$ für alle $n \in \mathbb{N}$, so sagen wir, dass g **unendliche Ordnung** hat, und schreiben $\operatorname{ord}(g) = \infty$.*
*Andernfalls existiert ein kleinstes $n \in \mathbb{N}$ mit $g^n = 1$. Dieses n nennen wir die **Ordnung von g** und setzen $\operatorname{ord}(g) := n$.*

Zentral für die meisten Aussagen über Elementordnungen ist folgende Beobachtung:

Lemma 7.8 *Sei g ein Gruppenelement. Dann ist die Abbildung $\varphi : \mathbb{Z} \to \langle g \rangle$ mit $\varphi(z) := g^z$ ein Epimorphismus.*

Beweisskizze. Es gilt $\langle g \rangle = g^{\mathbb{Z}}$ nach 2.16. Dies zeigt die Surjektivität von φ. Die Homomorphie von φ folgt aus der Kommutativität von $\langle g \rangle$, vgl. 6.11 (a). ■

In der Vorbemerkung zu 7.7 haben wir gesehen, dass die Potenzen g^z paarweise verschieden sind, falls $\operatorname{ord}(g) = \infty$ gilt. Dies bedeutet, dass der Epimorphismus aus 7.8 in diesem Fall injektiv und somit sogar ein Isomorphismus ist:

Satz 7.9 *Das Gruppenelement g habe unendliche Ordnung. Dann ist die Abbildung φ aus 7.8 ein Isomorphismus. Es gilt also $\mathbb{Z} \cong \langle g \rangle$.*

Im Falle einer endlichen Elementordnung erhalten wir eine Isomorphie zu einer Gruppe des Typs $(\mathbb{Z}_n, +)$ mit $n \in \mathbb{N}$:

Satz 7.10 *Für das Gruppenelement g gelte $\operatorname{ord}(g) = n \in \mathbb{N}$. Dann ist die Abbildung $\mathbb{Z}_n \to \langle g \rangle$ mit $\overline{z} \mapsto g^z$ ein Isomorphismus. Es gilt also $\mathbb{Z}_n \cong \langle g \rangle$.*

Beweis. Wir betrachten den Epimorphismus φ aus 7.8 und bestimmen dessen Kern. Nach 7.7 ist n das kleinste positive Element, das in $\ker \varphi$ liegt. Da $\ker \varphi$ eine Untergruppe von $\mathbb{Z}$ ist, folgt mit 3.4, dass $\ker \varphi = n\mathbb{Z}$ gilt. Die Aussage im Satz folgt nun mit dem Homomorphiesatz. ■

Betrachten wir die in 7.9 und 7.10 auftretenden Gruppenordnungen, so erhalten wir eine alternative Charakterisierung der Ordnung eines Gruppenelements:

Korollar 7.11 *Für jedes Gruppenelement g gilt $\operatorname{ord}(g) = |\langle g \rangle|$. Die Ordnung eines Gruppenelements stimmt also mit der Ordnung der von diesem Element erzeugten zyklischen Gruppe überein.*

Da ein Erzeuger einer zyklischen Gruppe eine gewisse Elementordnung hat, liefern 7.9 und 7.10 alle Möglichkeiten für zyklischen Gruppen (bis auf Isomorphie):

Korollar 7.12 (Isomorphietypen zyklischer Gruppen) *Eine zyklische Gruppe G ist durch die Angabe ihrer Ordnung bereits eindeutig (bis auf Isomorphie) bestimmt: Falls $|G| < \infty$ ist, so gilt $G \cong \mathbb{Z}_{|G|}$. Ansonsten ist $G \cong \mathbb{Z}$.*

Speziell für endliche zyklische Gruppen steht uns mit den Gruppen C_n auch ein multiplikativer Isomorphietyp zur Verfügung:

Korollar 7.13 *Jede zyklische Gruppe der Ordnung $n \in \mathbb{N}$ ist isomorph zu C_n.*

Bemerkung 7.14 (Warum Isomorphie?) Homomorphismen $\varphi : A \to B$ übertragen Identitäten zwischen den Elementen aus A auf die Bilder dieser Elemente. Ist φ ein Isomorphismus, so gilt hier auch die Rückrichtung. Zusammengenommen heißt dies: Sind zwei Strukturen A, B isomorph zueinander, so gilt eine Identität zwischen Elementen aus A genau dann, wenn diese Identität auch zwischen den entsprechenden Elementen aus B gilt. ⁉
Dies können wir anders interpretieren, indem wir sagen, dass sich die Verknüpfungen auf A und B gleich verhalten: Betrachten wir in A und B die jeweils passenden Elemente

(der Begriff „passend“ wird hierbei vom betrachteten Isomorphismus bestimmt), so laufen sämtliche Rechnungen in A bzw. B identisch ab. Zwei isomorphe Strukturen unterscheiden sich daher zwar in ihren Elementen, die zugrunde liegenden Verknüpfungen verhalten sich aber gleich.
Der Isomorphie-Begriff erlaubt es daher, sich von den konkreten Elementen einer algebraischen Struktur zu lösen und sich auf die Eigenschaften der jeweiligen Verknüpfungen zu fokussieren. Beispielsweise sagt 7.12, dass es zu vorgegebenem $n \in \mathbb{N}$ bis auf Umbenennung der Elemente nur genau eine Verknüpfung gibt, die die Menge zur zyklischen Gruppe macht. ⁕

Der nächste Satz stellt einige grundlegende Aussagen über Elementordnungen zusammen:

Satz 7.15 *Für das Gruppenelement g mit $\operatorname{ord}(g) = n \in \mathbb{N}$ gelten die folgenden Aussagen:*

(a) *Für jedes $z \in \mathbb{Z}$ ist $g^z = g^{z \bmod n}$.*

(b) *Es gilt $g^z = 1$ genau dann, wenn $n \mid z$ ist.*

(c) *Für jedes $z \in \mathbb{Z}$ ist $\operatorname{ord}(g^z) = \frac{n}{\operatorname{ggT}(n,z)}$.*

Beweis. Für das Folgende sei $\varphi : \mathbb{Z}_n \to \langle g \rangle$ mit $\varphi(\bar{z}) := g^z$ der Isomorphismus aus 7.10.

zu (a) φ ist als Abbildung wohldefiniert. Damit hat die Potenz g^z für alle Vertreter derselben Nebenklasse denselben Wert. Da in $\mathbb{Z}_n$ für alle $z \in \mathbb{Z}$ gilt $\bar{z} = \overline{z \bmod n}$, folgt $g^z = g^{z \bmod n}$.

zu (b) Genau dann gilt $g^z = 1$, wenn $\bar{z} \in \ker \varphi = \{\bar{0}\}$ ist, also wenn $z \in n\mathbb{Z}$ gilt, d. h. wenn $n \mid z$ ist.

zu (c) Sei $t := \operatorname{ggT}(n, z)$. Dann existieren $z' \in \mathbb{Z}$ und $n' \in \mathbb{N}$ mit $z = tz'$ und $n = tn'$. Es gilt $\operatorname{ggT}(n', z') = 1$, denn jedes $p \in \mathbb{P}$ mit $p \mid \operatorname{ggT}(z', n')$ ist ein gemeinsamer Teiler von z und n und wäre daher schon in t enthalten.

Gesucht ist die Ordnung von g^z, also das minimale $s \in \mathbb{N}$ mit $(g^z)^s = 1$. Wegen $\operatorname{ord}(g) = n$ und $1 = (g^z)^s = g^{zs} = g^{tz's}$ ist s die minimale natürliche Zahl mit $n \mid tz's$, also mit $tn' \mid tz's$, also mit $n' \mid z's$. Wegen $\operatorname{ggT}(n', z') = 1$ folgt $s = n'$. Dies liefert ?

$$\operatorname{ord}(g^z) = s = n' = \frac{n}{t} = \frac{n}{\operatorname{ggT}(n, z)}.$$ ■

Bemerkung 7.16 Sei g ein Gruppenelement der Ordnung $n \in \mathbb{N}$.

(a) Die Gruppe $\langle g \rangle$ hat nach 7.11 genau n Elemente. Jede Potenz g^z lässt sich nach 7.15 (a) schreiben in der Form g^r mit $r \in \{0, 1, \ldots, n-1\}$. Zusammen folgt, dass

$$\langle g \rangle = \{g^0, g^1, \ldots, g^{n-1}\}$$

gilt und dass diese n Elemente paarweise voneinander verschieden sind.

Können Sie anhand obiger Darstellung für $\langle g \rangle$ eine Vermutung aufstellen, woher der Name *zyklische Gruppe* kommt? ⁉

(b) Für $x, y \in \mathbb{Z}$ gilt $g^x = g^y \iff n \mid x - y$.

Dies sieht man, indem man die linke Gleichung mit g^{-y} multipliziert und 7.15 (b) anwendet. ⁂

Das nächste Resultat folgt aus Lagrange und klärt, welche Elementordnungen in endlichen Gruppen überhaupt möglich sind:

Satz 7.17 (Lagrange) *Sei G eine endliche Gruppe. Dann ist* $\operatorname{ord}(g)$ *ein Teiler von $|G|$ für jedes $g \in G$. Mit 7.15 (b) folgt hieraus insbesondere, dass $g^{|G|} = 1$ ist für alle $g \in G$.*

Beweis. Nach Lagrange ist $\operatorname{ord}(g) = |\langle g \rangle|$ ein Teiler von $|G|$. ■

Das folgende Resultat untersucht, welche Auswirkung das Abbilden mit einem Homomorphismus auf Elementordnungen hat:

Satz 7.18 *Seien G, H Gruppen und $\varphi : G \to H$ ein Homomorphismus. Hat $g \in G$ die Ordnung $n \in \mathbb{N}$, so ist* $\operatorname{ord}(\varphi(g))$ *ein Teiler von n.*

Beweis. Aus $g^n = 1$ folgt $\varphi(g)^n = 1$. Mit 7.15 (b) folgt $\operatorname{ord}(\varphi(g)) \mid n$. ■

Zyklische Gruppen

In diesem Abschnitt leiten wir einige wichtige Aussagen über zyklische Gruppen her. Ein wichtiges Beweismittel sind hierbei unsere Resultate über Elementordnungen. Die Übersetzung zwischen Elementordnungen und zyklischen Gruppen erfolgt mit 7.11: Zyklische Gruppen der Ordnung $n \in \mathbb{N} \cup \{\infty\}$ werden genau von Elementen der Ordnung n erzeugt.
Als Konsequenz hieraus ergibt sich eine Aussage, die zyklische Gruppen mit der Eulerschen φ-Funktion verbindet:

Satz 7.19 *Eine zyklische Gruppe der Ordnung $n \in \mathbb{N}$ hat genau $\varphi(n)$ Erzeuger.*

Beweis. Sei G zyklisch von Ordnung $n \in \mathbb{N}$ mit Erzeuger $g \in G$. Nach 7.15 (c) und 7.16 (a) ist g^z ein Erzeuger von G genau dann, wenn $z \in \{0, 1, \dots, n-1\}$ teilerfremd zu n ist. Es gibt aber genau $\varphi(n)$ solche z, vgl. 4.21. ■

Das nächste Resultat zeigt, dass die Eigenschaft, zyklisch zu sein, recht „robust“ ist: Sie bleibt unter den algebraischen Standardkonstruktionen erhalten. Man sagt daher auch, dass zyklische Gruppen **gute Vererbungseigenschaften** besitzen.

Satz 7.20 *Untergruppen, Faktorgruppen und homomorphe Bilder zyklischer Gruppen sind wieder zyklisch.*

Beweis. Seien G eine zyklische Gruppe und $g \in G$ ein Erzeuger von G.

Faktorgruppen Sei U eine beliebige Untergruppe von G. Dann ist U normal, und es gilt

$$G/U = \{\overline{x} \mid x \in G\} \overset{G=g^{\mathbb{Z}}}{=} \{\overline{g^z} \mid z \in \mathbb{Z}\} = \{\overline{g}^z \mid z \in \mathbb{Z}\} = \langle \overline{g} \rangle.$$

G/U wird also von der Nebenklasse $\overline{g}$ erzeugt und ist zyklisch.

homomorphe Bilder Nach dem Homomorphiesatz sind homomorphe Bilder von G isomorph zu einer Faktorgruppe der zyklischen Gruppe G. Diese sind nach Obigem aber zyklisch.

Untergruppen Für $G \cong \mathbb{Z}$ wurde die Aussage bereits in 3.4 gezeigt. Wir müssen also nur noch den Fall $|G| = r < \infty$ behandeln.

Sei $U \leq G$ beliebig. Die Gruppenelemente von U lassen sich nach 7.16 (a) schreiben in der Form g^{n_i} mit gewissen $n_i \in \{0, \dots, r-1\}$. Wir setzen $t := \mathrm{ggT}(n_1, \dots, n_r)$ und zeigen, dass $U = \langle g^t \rangle$ gilt.

Wegen $t \mid n_i$ gilt $g^{n_i} \in \langle g^t \rangle$ für alle i. Daher ist $U \leq \langle g^t \rangle$. Umgekehrt existieren mit Bézout $\lambda_i \in \mathbb{Z}$, so dass $t = \sum_{i=1}^{r} \lambda_i n_i$ gilt. Dies zeigt $\langle g^t \rangle \subseteq U$ wegen

$$g^t = g^{\sum_{i=1}^{r} \lambda_i n_i} = \prod_{i=1}^{r} g^{\lambda_i n_i} = \prod_{i=1}^{r} (\underbrace{g^{n_i}}_{\in U})^{\lambda_i} \in U. \qquad \blacksquare$$

Die Untergruppenstruktur von zu $\mathbb{Z}$ isomorphen zyklischen Gruppen haben wir bereits in 3.4 und 4.8 geklärt:

Satz 7.21 *Sei G eine zyklische Gruppe mit $|G| = \infty$. Dann besitzt G zu jedem $n \in \mathbb{N} \cup \{\infty\}$ genau eine (nach 7.20 zyklische) Untergruppe mit Index n.*

Wir kommen zur Untergruppenstruktur endlicher zyklischer Gruppen:

Satz 7.22 *Seien G eine zyklische Gruppe der Ordnung $n \in \mathbb{N}$ und $g \in G$ ein Erzeuger von G. Dann besitzt G zu jedem Teiler t von n genau eine (nach 7.20 zyklische) Untergruppe der Ordnung t, nämlich $\langle g^{n/t} \rangle$.*

Beweis.

Existenz Aus $t \mid n$ folgt $\frac{n}{t} \mid n$. Es gilt daher $\mathrm{ggT}(\frac{n}{t}, n) = \frac{n}{t}$, und 7.15 (c) zeigt $\mathrm{ord}(g^{n/t}) = \frac{n}{n/t} = t$. Also ist $\langle g^{n/t} \rangle$ eine Untergruppe der Ordnung t.

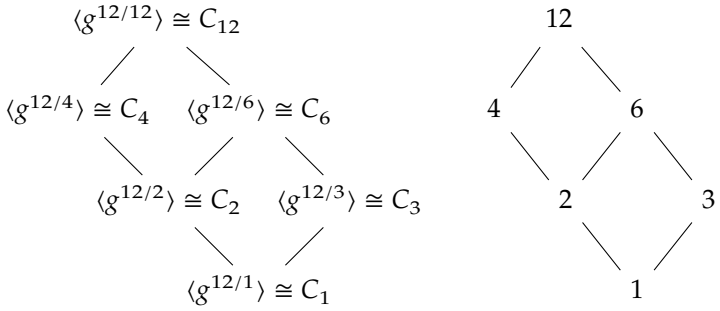
Eindeutigkeit Wir zeigen, dass $g^{n/t}$ in jeder Untergruppe U der Ordnung t von G enthalten ist. Aus Ordnungsgründen folgt dann $\langle g^{n/t} \rangle = U$, was die zu zeigende Eindeutigkeit beweist.

Sei $U \leq G$ von Ordnung t. Nach 7.20 ist U zyklisch. Wir können daher $U = \langle g^z \rangle$ mit einem $z \in \mathbb{Z}$ schreiben. Nach 7.15 (c) gilt $t = \mathrm{ord}(g^z) = \frac{n}{\mathrm{ggT}(n,z)}$ und daher

$\operatorname{ggT}(n,z) = \frac{n}{t}$. Mit Bézout existieren $\lambda, \mu \in \mathbb{Z}$ mit $\frac{n}{t} = \lambda n + \mu z$. Dies beendet den Beweis wegen

$$g^{n/t} = g^{\lambda n + \mu z} = (g^n)^\lambda \cdot (g^z)^\mu \overset{\operatorname{ord}(g)=n}{=} (g^z)^\mu \in \langle g^z \rangle = U. \qquad \blacksquare$$

Bemerkung 7.23 Obiger Satz klärt nicht nur, welche Untergruppenordnungen bei einer zyklischen Gruppe der Ordnung $n \in \mathbb{N}$ überhaupt möglich sind (alle, die der Satz von Lagrange zulässt; daher ist G eine Lagrange-Gruppe), sondern auch, wie diese bezüglich Mengeninklusion angeordnet sind: Sind $U, V \leq G$ und ist $|U|$ ein Teiler von $|V|$, so gilt $U \leq V$; denn nach 7.22 besitzt V eine Untergruppe der Ordnung $|U|$ und G besitzt genau eine solche.
Der Untergruppenverband von G stimmt daher mit dem Teilerdiagramm von n überein. Dies haben wir in der folgenden Grafik für $n = 12$ verdeutlicht. Im linken Bild symbolisieren die Verbindungsstriche eine Untergruppenbeziehung, im rechten eine Teilbarkeitsbeziehung.



※

Aus 7.22 folgt eine nette Identität für die φ-Funktion:

Korollar 7.24 *Für alle $n \in \mathbb{N}$ gilt $n = \sum_{t \text{ teilt } n} \varphi(t)$.*

Beweis. Für Teiler t von n definieren wir die Mengen $M_t := \{g \in C_n \mid \operatorname{ord}(g) = t\}$ aller Elemente von C_n mit Ordnung t. Dann gilt $C_n = \bigcup_{t \text{ teilt } n} M_t$. Jedes Element aus M_t erzeugt nach 7.22 *dieselbe* zyklische Gruppe von Ordnung t. Mit 7.19 folgt $|M_t| = \varphi(t)$. Durch Abzählen von Elementen erhalten wir daher

$$n = |C_n| = \sum_{t \text{ teilt } n} |M_t| = \sum_{t \text{ teilt } n} \varphi(t). \qquad \blacksquare$$

Mit Hilfe dieses Korollars werden wir in den Übungen den folgenden *Hauptsatz über endliche zyklische Gruppen* beweisen, der 7.22 teilweise umkehrt: → Übung

Satz 7.25 (Hauptsatz über endliche zyklische Gruppen) *Für eine endliche Gruppe G sind äquivalent:*

(a) *G ist zyklisch.*

(b) *G enthält zu jedem Teiler t von $|G|$ genau eine Untergruppe der Ordnung t.*

(Beachten Sie, dass wir in (b) nicht gefordert haben, dass diese Untergruppen zyklisch sein sollen.)

8. Endliche abelsche Gruppen, symmetrische Gruppen

Worum geht es? Wir besprechen den *Struktursatz für endliche abelsche Gruppen*, der die Isomorphietypen endlicher abelscher Gruppen vollständig klassifiziert.
Danach beschäftigen wir uns mit endlichen symmetrischen Gruppen. Wir behandeln zuerst spezielle Permutationen, die *Zykel*. Danach zeigen wir, dass sich jede Permutation eindeutig als Produkt von Zykeln schreiben lässt. Als Konsequenz hieraus stellen wir ein Kriterium vor, mit dem man entscheiden kann, ob zwei Permutationen zueinander konjugiert sind. ⋇

Endliche abelsche Gruppen

Das Hauptresultat in der Theorie der endlichen abelschen Gruppen ist der Struktursatz. Wir werden den umfangreichen Beweis dieses Satzes nicht führen, weil die hierfür benötigten Techniken eher in der Linearen Algebra anzusiedeln sind und wir sie in dieser Vorlesung nicht mehr benötigen werden. Sie finden einen Beweis des Satzes beispielsweise in [KM17, Abschnitt 32.6 auf S. 440 ff.].

Satz 8.1 (Struktursatz für endliche abelsche Gruppen) *Jede endliche abelsche Gruppe G ist isomorph zu einem direkten Produkt von zyklischen Gruppen von Primzahlpotenzordnung, d.h. es existieren $r \in \mathbb{N}_0$ sowie Primzahlpotenzen $1 < q_1 \leq q_2 \leq \cdots \leq q_r$, so dass gilt*

$$G \cong C_{q_1} \times C_{q_2} \times \cdots \times C_{q_r}.$$

Konvention: Das leere direkte Produkt, das im Fall $r = 0$ auftritt, fassen wir als die triviale Gruppe $\{1\}$ auf.
Sowohl r als auch das Tupel $(q_1, \ldots, q_r)$ der Primpotenzen sind eindeutig durch G bestimmt.

Bemerkung 8.2 (a) Der Struktursatz enthält sowohl eine Existenz- als auch eine Eindeutigkeitsaussage: Ist G eine endliche abelsche Gruppe, so existiert für den durch G bestimmten Isomorphietyp eine Schreibweise als direktes Produkt zyklischer Gruppen von Primpotenzordnung. Die Anzahl r der Faktoren wird dabei eindeutig von G vorgegeben. Sortiert man die Ordnungen der einzelnen Faktoren aufsteigend, so ist auch die Ordnung q_i jedes einzelnen Faktors eindeutig bestimmt.

(b) Mit Hilfe des Struktursatzes kann man alle Isomorphietypen für abelsche Gruppen mit vorgegebener Ordnung $n \in \mathbb{N}$ aufzählen. Hierzu sucht man alle $r \in \mathbb{N}_0$ und alle Primpotenzen $1 < q_1 \leq \cdots \leq q_r$, so dass $n = \prod_{i=1}^{r} q_i$ gilt. ⋇

Beispiel 8.3 Eine abelsche Gruppe der Ordnung $72 = 2^3 \cdot 3^2$ ist isomorph zu genau einer der folgenden sechs Gruppen:

$$\begin{aligned}
r = 2: &\quad C_8 \times C_9 \\
r = 3: &\quad C_2 \times C_4 \times C_9,\ C_3 \times C_3 \times C_8 \\
r = 4: &\quad C_2 \times C_2 \times C_2 \times C_9,\ C_2 \times C_3 \times C_3 \times C_4 \\
r = 5: &\quad C_2 \times C_2 \times C_2 \times C_3 \times C_3.
\end{aligned}$$ ⋇

Eine alternative Zerlegung zu der im Struktursatz lässt sich mit dem folgenden Satz gewinnen:

Satz 8.4 *Seien $a, b \in \mathbb{N}$. Genau dann gilt $C_a \times C_b \cong C_{ab}$, wenn a und b teilerfremd sind.*

Beweis.

$\Longrightarrow$ Wir zeigen die Kontraposition der Aussage. Sei $\mathrm{ggT}(a, b) > 1$. Dann existiert eine Primzahl p mit $p \mid a$ und $p \mid b$. Daher besitzt die Gruppe $C_a \times C_b$ eine Untergruppe, die zu $C_p \times C_p$ isomorph und nach Struktursatz nicht zyklisch ist. Da Untergruppen zyklischer Gruppen stets zyklisch sind, kann $C_a \times C_b$ nicht zyklisch sein. ⁉

$\Longleftarrow$ Die *Gruppen* C_n und $\mathbb{Z}_n$ sind für jedes $n \in \mathbb{N}$ isomorph. Da a und b teilerfremd sind, folgt aus dem chinesischen Restsatz $\mathbb{Z}_a \times \mathbb{Z}_b \cong \mathbb{Z}_{ab}$. Diese Ringisomorphie übersetzt sich in die Gruppenisomorphie $C_a \times C_b \cong C_{ab}$. ■

Beispiel 8.5 (a) Wir betrachten 8.3 erneut. Ein möglicher Isomorphietyp für abelsche Gruppen der Ordnung 72 ist C_{72}. Mit 8.4 folgt, dass dieser genau durch die Zerlegung $C_8 \times C_9$ gegeben ist.

(b) Es gilt $30 = 2 \cdot 3 \cdot 5$. Der einzige Isomorphietyp für abelsche Gruppen dieser Ordnung ist nach Struktursatz $C_2 \times C_3 \times C_5$. Allerdings bestehen die Isomorphien

$$C_2 \times C_3 \times C_5 \cong C_6 \times C_5 \cong C_{10} \times C_3 \cong C_2 \times C_{15} \cong C_{30}.$$

Dies sieht man, indem man die Faktoren des direkten Produkts permutiert (dies ändert den Isomorphietyp nicht) und dann mit 8.4 zusammenfasst. ⁉

Bei der Verwendung von 8.4 geht zwar die Eindeutigkeit der Zerlegung verloren, man kann jedoch oft aussagekräftigere Darstellungen des jeweiligen Isomorphietyps erhalten. Wir haben oben beispielsweise gezeigt, dass jede abelsche Gruppe der Ordnung 30 zyklisch ist.

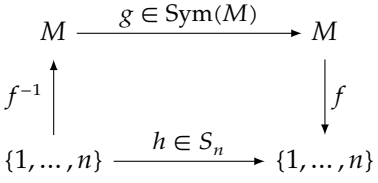
(c) Endliche abelsche Gruppen G sind Lagrangegruppen:

Aufgrund des Struktursatzes können wir davon ausgehen, dass G in der Form $G = C_{q_1} \times \cdots \times C_{q_r}$ mit Primpotenzen q_i zerlegt ist. Es gilt $|G| = \prod_{i=1}^{r} q_i$. Ist t ein Teiler von $|G|$, so existieren Primpotenzen s_i mit $s_i \mid q_i$ und $t = \prod_{i=1}^{r} s_i$. Sei U_i die Untergruppe der Ordnung s_i in C_{q_i}. Dann ist $U := U_1 \times \cdots \times U_r$ eine Untergruppe von G von Ordnung t.

Warum existieren die U_i? ⁂ ⁉

Endliche symmetrische Gruppen

Die symmetrische Gruppe $\mathrm{Sym}(M)$ besteht aus allen Bijektionen der Menge $M \neq \emptyset$, vgl. 1.6 (c). Genau dann ist $\mathrm{Sym}(M)$ endlich, wenn M endlich ist. In diesem Fall existiert ein $n \in \mathbb{N}$, so dass M und $\{1, \dots, n\}$ dieselbe Anzahl an Elementen besitzen. Wir finden dann eine Bijektion $f : M \to \{1, \dots, n\}$ und können mit ihrer Hilfe zeigen, dass $\mathrm{Sym}(M)$ zu S_n isomorph ist.



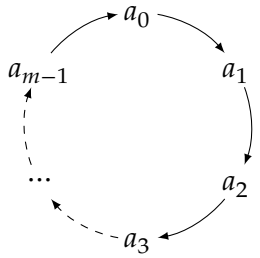
Um $\mathrm{Sym}(M) \cong S_n$ zu zeigen, bildet man $g \in \mathrm{Sym}(M)$ auf dasjenige $h \in S_n$ ab, das die Menge $\{1, \dots, n\}$ auf gleiche Weise permutiert wie g die Menge M. Der Begriff „gleiche Weise“ wird hierbei durch f definiert. Man gelangt dann zu der Beziehung $h = f \circ g \circ f^{-1}$ und zeigt, dass die Abbildung $\mathrm{Sym}(M) \to S_n$ mit $g \mapsto f \circ g \circ f^{-1}$ ein Isomorphismus ist, vgl. [KM17, Abschnitt 2.3.2, S. 27 f.].

Bei der Behandlung endlicher symmetrischer Gruppen können wir uns mit obiger Überlegung auf die Behandlung der Gruppen S_n beschränken. Als Verknüpfungszeichen in S_n schreiben wir $\cdot$ oder $\circ$ und meinen in beiden Fällen die Komposition von Abbildungen. Wir bezeichnen das Bild eines Elements $x \in \{1, \dots, n\}$ unter einer Permutation $g \in S_n$ mit $g(x)$ oder, falls wir aus Gründen der Übersichtlichkeit auf die Klammersetzung verzichten wollen, als $g \bullet x$. Zudem führen wir folgende nützliche Sprechweise ein:

Definition 8.6 *Unter einem **Fixpunkt einer Permutation** $g \in S_n$ verstehen wir jedes Element $x \in \{1, \dots, n\}$, das von g fixiert wird, für das also $g(x) = x$ gilt.*

Eine Permutation $g \in S_n$ kann man mit Hilfe einer Wertetabelle $\begin{pmatrix} 1 & 2 & \cdots & n \\ g(1) & g(2) & \cdots & g(n) \end{pmatrix}$ darstellen. Aus dieser Repräsentation lassen sich algebraische Eigenschaften von g aber oft nur schwer ablesen. Wir wollen daher eine geeignetere Darstellungsform für Permutationen finden. Hierbei helfen spezielle Permutationen, die *Zykel*, die man sehr kompakt notieren kann:

Definition 8.7 *Für $m \geq 2$ heißt eine Permutation $z \in S_n$ ein **m-Zykel** (für $m = 2$ auch **Transposition**), wenn es m paarweise verschiedene Elemente $a_0, a_1, \dots, a_{m-1} \in \{1, \dots, n\}$ gibt, so dass $z(a_i) = a_{(i+1) \bmod m}$ gilt und z die übrigen Elemente aus $\{1, \dots, n\} \setminus \{a_0, \dots, a_{m-1}\}$ fixiert.*



In der Grafik links stellen die Pfeile das Anwenden des Zykels z auf das jeweilige Element a_i dar.
Für $i \in \{0, 1, \dots, m-2\}$ gilt $z(a_i) = a_{i+1}$. Weiter ist $z(a_{m-1}) = a_0$, so dass sich links ein geschlossener Kreis ergibt. Das Anwenden von z entspricht dann einer „zyklischen“ Bewegung im Uhrzeigersinn auf diesem Kreis.

Die übrigen Elemente aus $\{1, \dots, n\}$ werden von z fixiert.

*Wir notieren z in der Kurznotation $z = (a_0\ a_1\ \cdots\ a_{m-1})$. Unter dem **Träger** $\mathbb{T}(z)$ **von** z verstehen wir die Menge $\{a_0, \dots, a_{m-1}\}$. Es gilt $|\mathbb{T}(z)| = m$.*

Bemerkung 8.8 (a) Der Träger eines Zykels z ist genau die Menge, die vom Zykel bewegt wird. Genau die Elemente der Menge $\{1, \dots, n\} \setminus \mathbb{T}(z)$ sind Fixpunkte von z.

(b) Aus (a) und der Forderung $m \geq 2$ in 8.7 folgt, dass jeder Zykel mindestens zwei Nicht-Fixpunkte besitzt.

(c) Ein Zykel z bildet genau die Elemente seines Trägers wieder auf Elemente seines Trägers ab; es gilt $z(\mathbb{T}(z)) = \mathbb{T}(z)$. Die Einschränkung $z|_{\mathbb{T}(z)}$ kann daher als Element aus $\mathrm{Sym}(\mathbb{T}(z)) \cong S_{|\mathbb{T}(z)|}$ aufgefasst werden ❓

(d) Ein Zykel ist allein durch die Reihenfolge, in der die Elemente seines Trägers aufeinander abgebildet werden, definiert. Das Trägerelement, bei dem der Zykel „beginnt“, ist irrelevant. Der m-Zykel $(a_0\ a_1\ \dots\ a_{m-1})$ besitzt daher genau die weiteren Notationen

$$(a_1\ a_2\ \cdots\ a_{m-1}\ a_0)\ ,\ (a_2\ a_3\ \cdots\ a_0\ a_1)\ ,\ \dots\ ,\ (a_{m-1}\ a_0\ a_1 \cdots\ a_{m-2}).$$

Insgesamt besitzt ein m-Zykel also genau m verschiedene Notationen. Das links stehende „Startelement“ legt die Notation eindeutig fest. ⁜ ❓

Wir stellen einige grundlegende Eigenschaften von Zykeln zusammen:

Lemma 8.9 (a) *Haben zwei Zykel $y, z \in S_n$ disjunkte Träger, d. h. gilt $\mathbb{T}(y) \cap \mathbb{T}(z) = \emptyset$, so gilt $yz = zy$. Induktiv folgt: Endlich viele Zykel mit paarweise disjunkten Trägern kommutieren.*

(b) *Sind $z_1, \dots, z_r \in S_n$ Zykel mit paarweise disjunkten Trägern und ist $x \in \mathbb{T}(z_i)$ für ein $i \in \{1, \dots, r\}$, so ist $z_1 \cdots z_r \bullet x = z_i(x)$.*

(c) *Seien $z \in S_n$ ein m-Zykel und $x \in \mathbb{T}(z)$. Dann gilt $z = (z^0(x)\, z^1(x)\, z^2(x)\, \cdots\, z^{m-1}(x))$.*

(d) *Die Ordnung eines m-Zykels ist m.*

(e) *Sei $z := (a_0 \cdots a_{m-1})$ ein m-Zykel. Dann gilt $z^{-1} = (a_{m-1}\, a_{m-2} \cdots a_2\, a_1\, a_0)$.*

Man invertiert einen Zykel also, indem man seine Kurznotation rückwärts niederschreibt.

Beweis.

zu (a) Wir zeigen, dass die Funktionen $yz, zy : \{1, \dots, n\} \to \{1, \dots, n\}$ übereinstimmen. Hierzu sei eine Stelle $x \in \{1, \dots, n\}$ beliebig gegeben. Sei beispielsweise $x \in \mathbb{T}(y)$. Dann ist $x \notin \mathbb{T}(z)$ aufgrund der Trägerdisjunktheit. Ferner gilt $y \bullet x \in \mathbb{T}(y)$ nach 8.8 (c) und somit ebenfalls $y \bullet x \notin \mathbb{T}(z)$. Es folgt daher

$$yz \bullet x = y \bullet (z \bullet x) \overset{x \notin \mathbb{T}(z)}{=} y \bullet x \overset{y \bullet x \notin \mathbb{T}(z)}{=} z \bullet (y \bullet x) = zy \bullet x.$$

Damit stimmen die Funktionen yz und zy auf $\mathbb{T}(y)$ überein. Man zeigt ähnlich, dass diese Gleichheit auch auf den restlichen Stellen gilt.

zu (b) Sei $x \in \mathbb{T}(z_i)$ für ein $i \in \{1, \dots, r\}$. Die Trägerdisjunktheit liefert $z_j(x) = x$ für alle $j \neq i$. Daher ist

$$z_1 \cdots z_r \bullet x \overset{\text{(a)}}{=} z_i \cdot z_1 \cdots z_{i-1} z_{i+1} \cdots z_r \bullet x \overset{z_j(x)=x}{=} z_i(x).$$

(c) folgt direkt aus der grafischen Zykeldarstellung in 8.7: Wir wählen ein beliebiges Element x auf dem Kreis und schreiben z in der Form $z = (x \cdots)$. Dann ist der k-te Eintrag in der Notation gerade dasjenige Element auf dem Kreis, das man von x aus in k Schritten, also durch k-faches Anwenden von z erreicht.

zu (d) Sei $z \in S_n$ ein m-Zykel. Mit (c) ist $z = (z^0(x)\, z^1(x)\, z^2(x) \cdots z^{m-1}(x))$, wobei x ein beliebiges Trägerelement von z bezeichne. Dann ist $z^k(x) \neq x$ für alle $k \in \{1, 2, \dots, m-1\}$. Die Ordnung von z ist also mindestens m. Umgekehrt folgt aus 8.7, dass z^m das Neutrale in S_n ist. Dies zeigt $\operatorname{ord}(z) = m$.

zu (e) Das Inverse von z entsteht, indem man in der grafischen Darstellung aus 8.7 die Pfeile im Kreis umkehrt. Dies erreicht man dadurch, dass man die Kurznotation des Zykels rückwärts niederschreibt. ■

Zykel spielen in der Theorie der endlichen symmetrischen Gruppen eine zentrale Rolle:

Satz 8.10 (Zykeldarstellung) *Jede Permutation $g \in S_n$ lässt sich als Produkt $g = z_1 \cdots z_r$ von Zykeln $z_1, \dots, z_r$ mit paarweise disjunkten Trägern schreiben. Diese Zerlegung ist eindeutig bis auf die Reihenfolge der z_i, vgl. 8.9 (a), und die verschiedenen Darstellungen der z_i, vgl. 8.8 (d). Man nennt sie die **Zykeldarstellung von g**.*
Konvention: Das leere Produkt identifizieren wir mit dem Neutralen aus S_n.

Beweisskizze. Sei $g \in S_n$ eine beliebige Permutation.

Existenz Wir zeigen, dass es zu jedem Nicht-Fixpunkt x von g eine Menge M_x gibt, so dass die Einschränkung $g|_{M_x}$ ein Zykel ist.

Sei hierzu ein beliebiges $x \in \{1, \dots, n\}$ mit $g(x) \neq x$ gegeben. Da die Bilder $g^k(x)$ für $k \in \mathbb{N}_0$ nicht alle voneinander verschieden sein können, existiert ein minimales $m \in \mathbb{N}$ mit $g^m(x) \in \{g^k(x) \mid 0 \leq k \leq m-1\}$. Es gilt also $g^m(x) = g^k(x)$ für ein $k \in \{0, \dots, m-1\}$ und somit $g^{m-k}(x) = g^0(x)$. Die Minimalität von m erzwingt $k = 0$. Es ist daher $g^m(x) = g^0(x)$. Setzen wir $M_x := \{g^k(x) \mid 0 \leq k \leq m-1\}$, so stimmt die Einschränkung $g|_{M_x}$ gerade mit dem Zykel $z_x := (g^0(x)\ g^1(x)\ \cdots\ g^{m-1}(x))$ überein.

Obige Konstruktion können wir für jeden Nicht-Fixpunkt durchführen. Wir erhalten Mengen $M_{x_1}, \dots, M_{x_r}$, die die Menge der Nicht-Fixpunkte von g partitionieren. Dann gilt $g = z_{x_1} \cdots z_{x_r}$ nach 8.9 (b).

Eindeutigkeit Seien $g = y_1 \cdots y_s$ und $g = z_1 \cdots z_r$ zwei Zykeldarstellungen von g. Wir zeigen, dass y_1 mit einem der Zykel z_i übereinstimmt. Sei hierzu $x \in \mathbb{T}(y_1)$ beliebig. Dann ist x kein Fixpunkt von g, und es existiert aufgrund der Trägerdisjunktheit

genau ein $i \in \{1, \dots, r\}$ mit $x \in \mathbb{T}(z_i)$. Wegen 8.9 (b) gilt $y_1(x) = g(x) = z_i(x)$ und somit $y_1^k(x) = g^k(x) = z_i^k(x)$ für alle $k \in \mathbb{N}_0$. Aus 8.9 (c) folgt $y_1 = z_i$.

Obiger Beweis funktioniert analog auch für alle anderen y_k; jedes der y_k stimmt daher mit einem der z_j überein. Durch Vertauschen der Rollen von y_k und z_j folgt auch die Rückrichtung: Jedes der z_j stimmt mit einem der y_k überein.

Damit ist gezeigt, dass die Mengen $\{y_1, \dots, y_s\}$ und $\{z_1, \dots, z_r\}$ gleich sind. Dies liefert die Eindeutigkeit der Zykeldarstellung im Sinne des Satzes. ■

Beispiel 8.11 (a) Wir wollen die Zykeldarstellung der Permutation $g \in S_5$ mit Wertetabelle $\left(\begin{smallmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 1 & 2 & 4 \end{smallmatrix}\right)$ bestimmen. Wir arbeiten hierzu den Algorithmus aus obigem Existenzbeweis ab:

Eins ist kein Fixpunkt von g. Es gilt $1 \overset{g}{\mapsto} 3 \overset{g}{\mapsto} 1$. Daher stimmt die Einschränkung $g|_{\{1,3\}}$ mit dem Zykel $(1\ 3)$ überein.

Zwei ist ebenfalls kein Fixpunkt von g. Es gilt $2 \overset{g}{\mapsto} 5 \overset{g}{\mapsto} 4 \overset{g}{\mapsto} 2$. Damit stimmt die Einschränkung $g|_{\{2,5,4\}}$ mit dem Zykel $(2\ 5\ 4)$ überein.

Damit haben wir das Abbildungsverhalten von g auf allen Nicht-Fixpunkten mit Hilfe von Zykeln beschrieben bestimmt. Wir erhalten die Zykeldarstellung von g als Produkt der obigen Zykel: Es gilt $g = (1\ 3)(2\ 5\ 4)$.

(b) Um die Zykeldarstellung der Permutation $g := (1234)(23)(45) \in S_5$ zu bestimmen, gehen wir wie in (a) vor. Der Unterschied zu (a) ist, dass g nicht in Form einer Wertetabelle gegeben ist.

Eins ist kein Fixpunkt von g, denn es ist $g(1) = 2$. Es folgt $1 \overset{g}{\mapsto} 2 \overset{g}{\mapsto} 4 \overset{g}{\mapsto} 5 \overset{g}{\mapsto} 1$. Daher ist $g|_{\{1,2,4,5\}} = (1\ 2\ 4\ 5)$.

Zu überprüfen ist noch das Element Drei. Es gilt $g(3) = 3$. Wir erhalten daher keinen Beitrag zur Zykeldarstellung von g, vgl. 8.8 (b).

Wir haben damit das Abbildungsverhalten von g auf allen Nicht-Fixpunkten durch Zykel beschrieben und erhalten $g = (1\ 2\ 4\ 5)$. ⁜

Ein Vorteil der Zykelnotation ist deren Kürze: Fixpunkte einer Permutation treten in der Zykeldarstellung nicht auf. Ein weiterer Vorteil ist, dass man mit Zykeln recht einfach rechnen kann. Insbesondere sind Potenzen von Permutationen in Zykeldarstellung leicht berechenbar. Dies erlaubt es, die Ordnung einer solchen Permutation direkt abzulesen.

Satz 8.12 *Die Permutation $g \in S_n$ habe die Zykeldarstellung $g = z_1 \cdots z_r$. Dann gelten:*

(a) *Für jedes $k \in \mathbb{Z}$ ist $g^k = z_1^k \cdots z_r^k$. Man potenziert g also, indem man jeden Zykel in der Zykeldarstellung von g potenziert.*

(b) *Der Zykel z_i habe Länge m_i. Dann gilt* $\operatorname{ord}(g) = \operatorname{kgV}(m_1, \dots, m_r)$.

Beweis. zu (a) Da die Zykel in der Zykeldarstellung von g nach 8.9 (a) beliebig vertauschen, folgt die Behauptung aus 1.9 (a).

zu (b) Wegen 8.9 (b) gilt $g^k = \mathrm{id}$ genau dann, wenn $z_i^k = \mathrm{id}$ gilt für alle $i \in \{1, \dots, r\}$. Dies ist nach 8.9 (d) genau dann der Fall, wenn $m_i \mid k$ für alle i gilt. Die kleinste natürliche Zahl, die dieser Bedingung genügt, ist $\mathrm{kgV}(m_1, \dots, m_r)$, das kleinste gemeinsame Vielfache aller m_i. ■

Beispiel 8.13 (a) Wir führen 8.11 (a) fort: Sei $g := (1\ 3)(2\ 5\ 4) \in S_5$. Dann ist $\mathrm{ord}(g) = \mathrm{kgV}(2,3) = 6$. Ferner ist

$$g^2 = (1\ 3)^2 \cdot (2\ 5\ 4)^2 = \mathrm{id} \cdot (2\ 5\ 4)^2 \overset{\mathrm{ord}((\dots))=3}{=} (2\ 5\ 4)^{-1} = (4\ 5\ 2).$$

(b) Wir führen 8.11 (b) fort: Sei $g := (1\ 2\ 4\ 5) \in S_5$. Dann gilt $\mathrm{ord}(g) = 4$. Es gelten $g^{-1} = (5\ 4\ 2\ 1)$ sowie

$$g^2 = (1\ 2\ 4\ 5)^2 = (1\ 2\ 4\ 5) \cdot (1\ 2\ 4\ 5) = (1\ 4)(2\ 5).$$

(c) Die Gruppe S_7 enthält Elemente der Ordnungen sieben, zehn und zwölf, aber keine der Ordnungen acht, neun oder elf. (Warum? Wie sehen die entsprechenden Elemente aus?) ⁂ ⁉

Die nächsten Resultate beschreiben die Konjugation in endlichen symmetrischen Gruppen. Wir führen zunächst noch einen hilfreichen Begriff ein:

Definition 8.14 (Zykeltyp) *Unter dem **Zykeltyp einer Permutation** $g \in S_n$ verstehen wir das aufsteigend geordnete Tupel der in der Zykelnotation für g auftretenden Zykellängen. Der Zykeltyp ist durch die Permutation eindeutig bestimmt.*

Beispiel 8.15 Die Permutation $(3\ 5\ 6)(1\ 2)(4\ 7\ 8) \in S_8$ liegt in Zykelnotation vor und hat den Zykeltyp $(2,3,3)$. ⁂

Lemma 8.16 *Seien $z := (a_0 \cdots a_{m-1}) \in S_n$ ein m-Zykel und $g \in S_n$ beliebig. Dann gilt*

$$g \cdot (a_0 \cdots a_{m-1}) \cdot g^{-1} = (g(a_0)\ g(a_1)\ \cdots\ g(a_{m-1})).$$

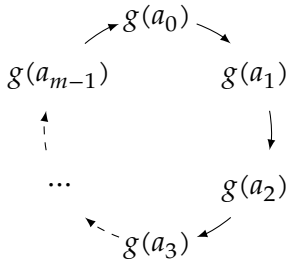
Konjugiert man einen m-Zykel z mit einer beliebigen Permutation g, so ist auch das Konjugat gzg^{-1} ein m-Zykel. Die Einträge im konjugierten Zykel sind die Bilder der Einträge des Ursprungszykels unter g. Es gilt $\mathbb{T}(gzg^{-1}) = g(\mathbb{T}(z))$.

Beweis. Wir untersuchen das Abbildungsverhalten von gzg^{-1}. Sei hierzu zunächst $x \in \{1, \dots, n\} \setminus \{a_0, \dots, a_{m-1}\}$ beliebig. Dann gilt für das Element $g(x)$:

$$gzg^{-1} \bullet g(x) = gzg^{-1}g \bullet x = g \bullet (z \bullet x) \overset{z(x)=x}{=} g(x).$$

Daher ist $g(x)$ ein Fixpunkt von gzg^{-1}. Nun untersuchen wir, wohin gzg^{-1} das Element $g(a_i)$ abbildet. Es gilt

$$gzg^{-1} \bullet g(a_i) = gzg^{-1}g \bullet a_i = g \bullet (z \bullet a_i) = g(a_{i+1 \bmod m}).$$



Insgesamt folgt, dass gzg^{-1} die Elemente $g(a_i)$ zyklisch wie in der Grafik links permutiert. Die übrigen Elemente aus $\{1, \dots, n\}$ werden fixiert. Also stimmt gzg^{-1} mit dem Zykel

$$(g(a_0)\ g(a_1)\ g(a_2)\ \cdots\ g(a_{m-1}))$$

überein.

■

Satz 8.17 (Konjugation in S_n) *Genau dann sind zwei Permutationen $p, q \in S_n$ in S_n konjugiert zueinander, d. h. es existiert ein $g \in S_n$ mit $q = gpg^{-1}$, wenn p und q denselben Zykeltyp besitzen.*

Beweis.

$\Longrightarrow$ Es gelte $q = gpg^{-1}$ mit einem $g \in S_n$. Sei $p = z_1 \cdots z_r$ die Zykeldarstellung von p. Setzen wir $y_i := gz_ig^{-1}$, so gilt

$$q = gpg^{-1} = gz_1g^{-1} \cdot gz_2g^{-1} \cdots gz_rg^{-1} = y_1 \cdots y_r.$$

Nach 8.16 sind z_i und y_i Zykel derselben Länge. Weiter gilt $\mathbb{T}(y_i) \cap \mathbb{T}(y_j) = \emptyset$ für $i \neq j$, denn es gilt

$$\mathbb{T}(y_i) \cap \mathbb{T}(y_j) \overset{8.16}{=} g(\mathbb{T}(z_i)) \cap g(\mathbb{T}(z_j)) \overset{\mathbb{T}(z_i)\cap\mathbb{T}(z_j)=\emptyset}{=} \emptyset.$$

Dies zeigt, dass $y_1 \cdots y_r$ die Zykelzerlegung von q ist und dass diese denselben Typ wie die Zykelzerlegung von p hat.

$\Longleftarrow$ Nun mögen p und q denselben Zykeltyp haben. Da sich die einzelnen Zykel nach 8.9 (a) beliebig vertauschen lassen, können wir schreiben

$$\begin{aligned} p &= (a_{1,1}\ \cdots\ a_{1,n_1})(a_{2,1}\ \cdots\ a_{2,n_2}) \cdots (a_{r,1}\ \cdots\ a_{r,n_r}) \\ q &= (b_{1,1}\ \cdots\ b_{1,n_1})(b_{2,1}\ \cdots\ b_{2,n_2}) \cdots (b_{r,1}\ \cdots\ b_{r,n_r}) \end{aligned}$$

Da die $a_{i,j}$ und die $b_{i,j}$ paarweise verschieden sind, wird durch die Festsetzung $g(a_{i,j}) := b_{i,j}$ eine Bijektion von einer Teilmenge von $\{1, \dots, n\}$ auf eine Teilmenge von $\{1, \dots, n\}$ gegeben. Diese lässt sich zu einer Bijektion $g : \{1, \dots, n\} \to \{1, \dots, n\}$ fortsetzen. Mit 8.16 folgt nun $gpg^{-1} = q$. ■ ⁉

Beispiel 8.18 Für $n \geq 2$ ist jede Transposition von S_n in S_n konjugiert zur Transposition $(1\ 2)$. Allgemeiner gilt: Für $n \geq m$ ist jeder m-Zykel von S_n in S_n konjugiert zum m-Zykel $(1\ 2\ \cdots\ m)$. ※

9. Alternierende Gruppen, Normalteiler von S_n und A_n

Worum geht es? Wir definieren die *alternierende Gruppe* A_n, eine wichtige Untergruppe der Gruppe S_n. Hierzu betrachten wir *Transpositionszerlegungen* von Permutationen und führen den Begriff des *Signums* ein. Anschließend stellen wir einige Erzeugendensysteme der A_n vor und bestimmen die Normalteiler von A_n und S_n für $n \geq 5$. ⁂

Transpositionszerlegungen, Signum

Wir kennen bereits die Zykeldarstellung einer Permutation. Diese wird beim praktischen Umgang mit Permutationen gern benutzt. Das folgende Lemma ist die Basis für eine weitere Darstellung von Permutationen, die eher theoretisch interessant ist:

Lemma 9.1 *Jeder m-Zykel aus S_n lässt sich als Produkt von $m-1$ Transpositionen schreiben.*

Beweis. Konkretes Nachrechnen zeigt, dass

$$(1\ 2\ \cdots\ m) = (1\ 2)(2\ 3)(3\ 4)\cdots(m-1\ m)$$

gilt, wobei auf der rechten Seite der Gleichung genau $m-1$ Transpositionen stehen. Für den m-Zykel $(1\ 2\ \cdots\ m)$ ist daher die Aussage des Lemmas bewiesen.
Sei nun $z \in S_n$ ein beliebiger m-Zykel. Mit 8.18 gilt $z = g(1\ 2\ \cdots\ m)g^{-1}$ für ein $g \in S_n$. Dann folgt die Behauptung wegen

$$z = g(1\ 2)g^{-1}\cdots g(m-1\ m)g^{-1} \overset{8.16}{=} (g(1)\ g(2))\cdots(g(m-1)\ g(m)). \qquad \blacksquare$$

Da jede Permutation eine Zykeldarstellung besitzt und Zykel Produkte von Transpositionen sind, erhalten wir:

Satz 9.2 *Die Gruppe S_n wird von allen ihren Transpositionen erzeugt. Es gilt also*

$$S_n = \langle t \mid t \in S_n \text{ ist eine Transposition}\rangle.$$

*Ist $g \in S_n$ eine Permutation, so nennen wir jede Zerlegung von g in ein Produkt von Transpositionen eine **Transpositionszerlegung von g**.*

Bemerkung 9.3 (a) Wir fordern bei Transpositionszerlegungen keine paarweise disjunkten Träger. Transpositionszerlegungen sind daher im Allgemeinen keine Zykeldarstellungen; 9.2 widerspricht der Eindeutigkeitsaussage aus 8.10 somit nicht.

(b) In Transpositionszerlegungen kommutieren die einzelnen Faktoren im Allgemeinen nicht. Beispielsweise gilt

$$(1\ 2)(2\ 3) = (1\ 2\ 3) \neq (1\ 3\ 2) = (2\ 3)(1\ 2).$$

Daher ist insbesondere 8.12 nicht auf Transpositionszerlegungen anwendbar.

(c) Eine Permutation besitzt im Allgemeinen mehrere verschiedene Transpositionszerlegungen. Beispielsweise gilt

$$\begin{aligned}(1\,2\,3) &= (1\,2)(2\,3) = (1\,3)(1\,2) = (2\,3)(1\,3)\\ &= (1\,2)(1\,3)(1\,2)(1\,3) = (1\,3)(2\,3)(1\,3)(2\,3).\end{aligned}$$

⁜

Die Bedeutung von Transpositionszerlegungen in der Theorie der symmetrischen Gruppen beruht auf dem folgenden Resultat, das einen (schwachen) Ersatz für die nach 9.3 (c) fehlende Eindeutigkeit liefert. Für einen Beweis des Lemmas verweisen wir auf [KM17, Abschnitt 9.2, S. 126] oder die Lineare Algebra.

Lemma 9.4 *Keine Permutation $g \in S_n$ ist Produkt von einer ungeraden Anzahl von Transpositionen und auch Produkt von einer geraden Anzahl von Transpositionen.*

Eine Permutation ist also entweder stets Produkt einer geraden Anzahl von Transpositionen oder stets Produkt einer ungeraden Anzahl an Transpositionen. Dies legt die folgenden Bezeichnungen nahe:

Definition 9.5 (Signum) *Wir nennen $g \in S_n$ **gerade** und setzen $\operatorname{sgn}(g) := 1$, wenn g eine Transpositionszerlegung in eine gerade Anzahl an Faktoren zulässt. Ansonsten nennen wir g **ungerade** und setzen $\operatorname{sgn}(g) := -1$. Den Ausdruck $\operatorname{sgn}(g)$ nennen wir das **Vorzeichen** oder das **Signum von g**.*
Wegen 9.4 sind diese Bezeichnungen sinnvoll; sie hängen nicht von der konkret betrachteten Transpositionszerlegung von g ab.

Beispiel 9.6 Nach 9.1 lässt sich ein m-Zykel als Produkt von $m-1$ Transpositionen schreiben. Dies zeigt, dass Zykel gerader Länge ungerade und Zykel ungerader Länge gerade sind. Insbesondere sind alle Transpositionen ungerade und alle Dreizykel gerade.

Zusammenfassend gilt für einen m-Zykel z also $\operatorname{sgn}(z) = (-1)^{m-1}$. ⁜ ⁉

Wir kommen zur wichtigsten Eigenschaft des Signums:

Satz 9.7 *Für jedes $n \in \mathbb{N}$ ist die **Signumsfunktion***

$$\operatorname{sgn}: S_n \to C_2, \qquad g \mapsto \operatorname{sgn}(g)$$

ein Homomorphismus. Für $n \geq 2$ ist sgn *surjektiv.*

Beweis. Wir zeigen die Homomorphie von sgn. Seien $g, h \in S_n$ transpositionszerlegt in der Form $g = s_1 \cdots s_a$ bzw. $h = t_1 \cdots t_b$. Wegen $gh = s_1 \cdots s_a \cdot t_1 \cdots t_b$ kennen wir dann auch eine Transpositionszerlegung von gh.
Es gilt $\operatorname{sgn}(g) = (-1)^a$, $\operatorname{sgn}(h) = (-1)^b$ und $\operatorname{sgn}(gh) = (-1)^{a+b}$. Dann folgt ⁉

$$\operatorname{sgn}(gh) = (-1)^{a+b} = (-1)^a \cdot (-1)^b = \operatorname{sgn}(g) \cdot \operatorname{sgn}(h).$$

Für $n \geq 2$ gilt $\mathrm{id}, (1\,2) \in S_n$. Die Signumsfunktion nimmt daher nach 9.6 die Werte ± 1 an und ist surjektiv. ■

Beispiel 9.8 Mit Hilfe von 9.6 und 9.7 können wir das Signum einer beliebigen Permutation g einfach berechnen: Wir bestimmen die Zykeldarstellung $z_1 \cdots z_r$ von g. Besitzt der Zykel z_i die Länge m_i, so gilt

$$\operatorname{sgn}(g) = \operatorname{sgn}(z_1) \cdots \operatorname{sgn}(z_r) = (-1)^{m_1-1} \cdots (-1)^{m_r-1} = (-1)^{\sum_{i=1}^{r}(m_i-1)}. \qquad \text{※}$$

Die alternierenden Gruppen A_n

Mit Hilfe der Signumsfunktion definiert man die alternierenden Gruppen A_n:

Definition 9.9 *Für $n \in \mathbb{N}$ bezeichne* $\operatorname{sgn} : S_n \to C_2$ *die Signumsfunktion. Dann setzen wir* $A_n := \ker \operatorname{sgn}$ *und nennen A_n die* ***alternierende Gruppe vom Grad n****.*

Bemerkung 9.10 (a) Im Kern der Signumsfunktion sind genau die geraden Permutationen der S_n enthalten. Daher gilt $A_n = \{g \in S_n \mid g \text{ ist gerade}\}$.

(b) Als Kern ist A_n ein Normalteiler von S_n. Es gilt mit dem Homomorphiesatz

$$S_n/A_n \cong \operatorname{sgn}(S_n) = \begin{cases} \{1\} & \text{falls } n = 1, \\ \{\pm 1\} & \text{falls } n > 1. \end{cases}$$

Es gilt somit $S_n = A_n$ genau für $n = 1$. Für $n > 1$ ist A_n eine Index-2-Untergruppe von S_n. Für diese n gilt $|A_n| = \frac{1}{2} \cdot n!$

(c) Es ist $A_2 = \{\mathrm{id}\}$. Dies folgt aus der Mächtigkeitsformel in (b) oder alternativ aus (a), weil $S_2 = \{\mathrm{id}, (1\,2)\}$ keine nicht-triviale gerade Permutation enthält. Ähnlich sieht man $A_3 \cong C_3$. ※

Beispiel 9.11 (Die Gruppe A_4) Die Gruppe A_4 besteht aus $\frac{1}{2} \cdot 4! = 12$ Elementen. Nichttriviale Elemente aus A_4 können nur die Zykeltypen (3) oder $(2,2)$ besitzen; letztere Elemente nennt man auch **Doppeltranspositionen**. Daher ist

$$\begin{aligned} A_4 \;=\; \{&\mathrm{id}, (12)(34), (13)(24), (14)(23), \\ &(123), (132), (124), (142), (234), (243), (134), (143)\}. \end{aligned}$$

Mit dem Untergruppenkriterium folgt, dass die Menge

$$V_4 := \{\mathrm{id}, (12)(34), (13)(24), (14)(23)\}$$

eine Untergruppe von A_4 ist. Man nennt V_4 die **Kleinsche Vierergruppe**. Es gilt $gh = hg$ für alle $g, h \in V_4$, so dass V_4 abelsch ist. Da V_4 mehr als $\varphi(2) = 1$ Element der Ordnung Zwei enthält, folgt nach Struktursatz $V_4 \cong C_2 \times C_2$.

V_4 ist ein Normalteiler von A_4: Seien $v \in V_4$ und $g \in A_4$. Dann ist entweder $v = \mathrm{id}$ und somit $gvg^{-1} = \mathrm{id} \in V_4$ oder v hat Zykeltyp $(2,2)$. In diesem Fall hat wegen 8.17 auch

gvg^{-1} den Zykeltyp $(2,2)$. Da V_4 alle Elemente aus A_4 mit Zykeltyp $(2,2)$ enthält, folgt $gvg^{-1} \in V_4$. Konjugation mit Elementen aus A_4 führt also nie aus V_4 heraus.

A_4 ist keine Lagrangegruppe; hierzu zeigen wir, dass A_4 keine Untergruppe der Ordnung sechs enthält. Angenommen, $U \leq A_4$ sei eine solche.
Dann muss U mindestens ein Element mit Zykeltyp $(2,2)$ enthalten, denn ansonsten bestünde U aus der Identität und fünf Dreizykeln. Die Anzahl der Dreizykel in einer endlichen Gruppe ist aber stets gerade, denn mit dem Dreizykel (abc) ist auch sein Inverses (cba) enthalten.
Durch Umbenennen der Elemente $1,2,3,4$ können wir daher ohne Einschränkung davon ausgehen, dass $(12)(34) \in U$ gilt. Dann liegt auch jedes in A_4 zu $(12)(34)$ konjugierte Element in U, denn U ist als Index-2-Untergruppe normal in A_4, vgl. die Übungen. → Übung
Wegen

$$(123)\cdot(12)(34)\cdot(123)^{-1} = (14)(23) \quad \text{und} \quad (124)\cdot(12)(34)\cdot(124)^{-1} = (13)(24)$$

liegen daher *alle* Elemente mit Zykeltyp $(2,2)$ in U. Es folgt $V_4 \leq U$. Dies widerspricht aber Lagrange, denn $4 \nmid 6$. ※

Erzeugendensysteme der A_n

Wir versuchen, 9.2 nachzustellen und „schöne“ Erzeugendensysteme der A_n zu finden. Das im folgenden Lemma angegebene Erzeugendensystem bildet die Grundlage für die nächsten beiden Resultate:

Lemma 9.12 *Es gilt $A_n = \langle st \mid s,t \in S_n$ sind Transpositionen$\rangle$, d. h. A_n wird von allen Produkten von zwei Transpositionen der S_n erzeugt.*

Beweis.

$\subseteq$ Sei $g \in A_n$ beliebig. Dann besitzt g eine Transpositionszerlegung gerader Länge, d. h. wir können schreiben $g = t_1 \cdots t_{2r}$ mit einem $r \in \mathbb{N}_0$ und Transpositionen $t_i \in S_n$. Durch die Klammerung

$$g = t_1 \cdots t_{2r} = (t_1 t_2)\cdot(t_3 t_4)\cdot(t_5 t_6)\cdots(t_{2r-1}t_{2r})$$

sieht man, dass g ein Produkt von Produkten von zwei Transpositionen aus S_n ist. Dies zeigt $g \in \langle st \mid s,t \in S_n$ sind Transpositionen$\rangle$. ⁉

$\supseteq$ Produkte von zwei Transpositionen aus S_n sind gerade und liegen somit in A_n. Dies zeigt $\langle st \mid s,t \in S_n$ sind Transpositionen$\rangle \subseteq A_n$. ■

Wir können nun zeigen, dass A_n von allen Dreizykeln erzeugt wird:

Satz 9.13 *Es gilt $A_n = \langle d \mid d \in S_n$ ist ein Dreizykel$\rangle$, d. h. A_n wird von allen Dreizykeln der S_n erzeugt.*

Beweis. Die $\supseteq$-Aussage folgt analog zu obigem Beweis, da Dreizykel gerade sind. Wir zeigen „$\subseteq$“, indem wir nachweisen, dass sich ein Produkt aus zwei Transpositionen als Produkt von Dreizykeln schreiben lässt. Hierzu seien Transpositionen $s := (a\ b) \in S_n$ und $t = (c\ d) \in S_n$ gegeben.
Im Fall $|\mathbb{T}(s) \cap \mathbb{T}(t)| = 0$ sind die Elemente a, b, c, d paarweise verschieden. Es gilt $st = (ab)(cd) = (acb)(acd)$. Die paarweise Verschiedenheit stellt sicher, dass (acb) und (acd) tatsächlich Dreizykel sind. ?
Sei nun $|\mathbb{T}(s) \cap \mathbb{T}(t)| = 1$. Wegen $(ab) = (ba)$ und $(cd) = (dc)$ können wir ohne Einschränkung davon ausgehen, dass $a = c$ gilt und die Elemente a, b, d paarweise voneinander verschieden sind. Dann ist $st = (ab)(ad) = (adb)$ ein Dreizykel.
Im Fall $|\mathbb{T}(s) \cap \mathbb{T}(t)| = 2$ gilt $s = t$ und somit $st = \mathrm{id}$. Aufgrund unserer Konventionen stimmt id mit dem leeren Produkt von Dreizykeln überein. ■

Mit diesem Satz können wir die Aussage aus 9.12 für $n \geq 5$ verschärfen:

Korollar 9.14 *Für $n \geq 5$ gilt $A_n = \langle st \mid s, t \in S_n$ sind **trägerdisjunkte** Transpositionen$\rangle$, d. h. für diese n wird A_n von allen Elementen der S_n mit Zykeltyp $(2, 2)$, also allen Doppeltranspositionen der S_n erzeugt.*

Beweisskizze. Sei $g := (abc)$ ein beliebiger Dreizykel aus A_n. Da wir $n \geq 5$ vorausgesetzt haben, existieren $x, y \in \{1, \dots, n\}$ mit $x \neq y$ und $x, y \notin \mathbb{T}(g)$. Daher ist durch

$$(abc) = (ac)(xy) \cdot (xy)(ab)$$

eine Zerlegung von g in zwei Doppeltranspositionen gegeben. Die Aussage des Korollars folgt nun mit 9.13. ■

Knobelfrage. Ist die Schranke $n \geq 5$ in obigem Korollar scharf? Wird A_n für $n \in \{1, 2, 3, 4\}$ stets von allen Doppeltranspositionen der S_n erzeugt?

Normalteiler von S_n

In diesem Abschnitt untersuchen wir die Gruppen S_n auf Normalteiler. Wir zeigen zunächst, dass ein nicht-trivialer Normalteiler der S_n eine Doppeltransposition oder einen Dreizykel enthält:

Lemma 9.15 *Seien $n \geq 3$ und $N \trianglelefteq S_n$ mit $N \neq \{\mathrm{id}\}$. Dann enthält N eine Doppeltransposition oder einen Dreizykel.*

Beweis. N enthält ein Element $g \neq \mathrm{id}$. Durch Umbenennen der Elemente $1, 2, \dots, n$ können wir ohne Einschränkung annehmen, dass $g(1) = 2$ gilt. Wir betrachten nun das Element $h := g(13)g^{-1}(13)$. Es ist $h \in N$, denn aufgrund der Normalität von N ist $(13)g^{-1}(13) \in N$. Mit Hilfe von 8.16 folgt

$$h = g(13)g^{-1} \cdot (13) = (g(1)\ g(3))(13) = (2\ g(3))(13).$$

Gilt $g(3) \notin \{1, 3\}$, so ist h eine Doppeltransposition. Gilt $g(3) = 1$, so ist $h = (21)(13) = (132)$ ein Dreizykel. Gilt $g(3) = 3$, so ist $h = (23)(13) = (123)$ ebenfalls ein Dreizykel. Dies zeigt die Aussage im Lemma. (Warum tritt der Fall $g(3) = 2$ nicht auf?) ■ ?

Mit den Erzeugenden-Resultaten aus dem letzten Abschnitt erhalten wir nun:

Satz 9.16 *Seien $n \geq 5$ und $N \trianglelefteq S_n$ ein Normalteiler der S_n mit $N \neq \{\mathrm{id}\}$. Dann gilt $N = A_n$ oder $N = S_n$. Beide Fälle treten auf.*

Beweis. Da N normal in S_n ist, enthält N nach 9.15 *alle* Doppeltranspositionen der S_n bzw. *alle* Dreizykel der S_n. Somit ist $A_n \leq N$ aufgrund von 9.14 bzw. 9.13. Da A_n eine Index-2-Untergruppe von S_n ist, folgt $N = A_n$ oder $N = S_n$.
Umgekehrt sind A_n und S_n natürlich Normalteiler von S_n. ■

Knobelfrage. Ist die Schranke $n \geq 5$ im obigen Satz scharf? Hat S_n für $n \in \{1, 2, 3, 4\}$ stets nur die Normalteiler $\{\mathrm{id}\}$, A_n und S_n?

Normalteiler der A_n

Um die Normalteiler der A_n zu bestimmen, geht man wie im vorherigen Abschnitt vor und sucht „schöne“ Elemente in nicht-trivialen Normalteilern der A_n. Das nächste Lemma sagt, dass für $n \geq 5$ jeder nicht-triviale Normalteiler der A_n einen Dreizykel enthält. Sein Beweis benutzt ähnliche Techniken wie der Beweis zu 9.15, ist aber deutlich länger und benötigt einige Fallunterscheidungen. Wir führen ihn nicht und verweisen beispielsweise auf [KM17, Satz 9.10, S. 128].

Lemma 9.17 *Seien $n \geq 5$ und $N \trianglelefteq A_n$ ein Normalteiler der A_n mit $N \neq \{\mathrm{id}\}$. Dann enthält N einen Dreizykel.*

Wir wissen aus 8.17, dass *in* S_n alle Dreizykel zueinander konjugiert sind. Wir zeigen, dass diese Aussage für $n \geq 5$ bereits schon *in* A_n gilt:

Lemma 9.18 *Seien $n \geq 5$ und $d, e \in S_n$ zwei beliebige Dreizykel. Dann sind d und e in A_n zueinander konjugiert, d. h. es gibt $g \in A_n$ mit $gdg^{-1} = e$.*

Beweis. Wegen 8.17 sind d und e in S_n konjugiert, d. h. es existiert eine Permutation $h \in S_n$ mit $hdh^{-1} = e$.
Gilt zufälligerweise $h \in A_n$, so setzen wir $g := h$ und sind fertig.
Ansonsten existieren $x, y \in \{1, \dots, n\}$ mit $x \neq y$ und $x, y \notin \mathbb{T}(e)$, denn es ist $n \geq 5$ und $|\mathbb{T}(e)| = 3$. Wir setzen $g := (x\ y)h$. Dann gilt $g \in A_n$, und es ist

$$gdg^{-1} = (x\ y) \cdot hdh^{-1} \cdot (x\ y) = (x\ y) \cdot e \cdot (x\ y) \overset{x,y \notin \mathbb{T}(e)}{=} (x\ y)(x\ y) \cdot e = e.$$ ■

Wir können nun leicht das Hauptresultat über alternierende Gruppen beweisen:

Satz 9.19 *Für $n \geq 5$ besitzt A_n keine weiteren Normalteiler neben $\{\mathrm{id}\}$ und A_n.*
*Gruppen G, die nur die beiden Normalteiler $\{1\}$ und G besitzen, heißen **einfach**.*
Die Aussage dieses Satzes ist daher: Für $n \geq 5$ ist A_n einfach.

Beweis. Sei $N \trianglelefteq A_n$ ein Normalteiler von A_n mit $N \neq \{\mathrm{id}\}$. Dann enthält N wegen 9.17 einen und wegen 9.18 alle Dreizykel der S_n. Es folgt $N = A_n$ nach 9.13. ■

Bemerkung 9.20 Eine beliebte Beweismethode in der Gruppentheorie ist, Aussagen über eine Gruppe G dadurch zu zeigen, dass man Resultate über einen Normalteiler $\{1\} \lhd N \lhd G$ mit Resultaten über die Faktorgruppe G/N kombiniert. Oft haben N und G/N eine deutlich leichtere Struktur als G, so dass diese Technik den Beweis stark vereinfacht oder sogar erst ermöglicht.
Dieses Vorgehen lässt sich induktiv fortsetzen: Sind N oder G/N noch zu kompliziert, so sucht man einen Normalteiler M in N bzw. in G/N und beweist dann Aussagen in den Gruppen M und N/M bzw. in den Gruppen M und $(G/N)/M$. Klappt dies auch nicht, so sucht man Normalteiler in diesen Normalteilern bzw. Faktorgruppen, etc.

Das Verfahren stoppt, sobald man bei einer einfachen Gruppe G angekommen ist; hier treten als Faktorgruppen nur die triviale Gruppe $\{\overline{1}\}$ oder die Ausgangsgruppe G selbst auf. Der Umgang mit einfachen Gruppen ist daher aus beweistechnischer Sicht oft unangenehm, was erklärt, warum Gruppentheoretiker schon früh begonnen haben, einfache Gruppen intensiv zu studieren.
Diese Untersuchungen haben zur **Klassifikation der endlichen einfachen Gruppen** geführt, einer Auflistung aller möglichen Isomorphietypen endlicher einfacher Gruppen. Dieses Resultat stellt einen Höhepunkt der Gruppentheorie des 20. Jahrhunderts dar: Über 100 Gruppentheoretiker haben über einen Zeitraum von grob 50 Jahren an diesem Satz gearbeitet; sein Beweis ist auf mehrere Hundert Journale verteilt und umfasst mehr als 10 000 gedruckte Seiten.
Grob gesprochen sagt die Klassifikation aus, dass eine endliche einfache Gruppe zur Gruppe C_p mit $p \in \mathbb{P}$, zu A_n mit $n \geq 5$, zu gewissen geometrisch definierten Untergruppen von $\mathrm{GL}(n, \mathbb{Z}_p)$ oder zu einer von 26 **sporadischen Gruppen** isomorph ist. Man hat bisher keine zufriedenstellende Erklärung für die Existenz der sporadischen Gruppen gefunden; sie scheinen mit den anderen möglichen Isomorphietypen nicht zusammenzuhängen. Die größte sporadische Gruppe ist die **Monstergruppe**, deren Ordnung

808 017 424 794 512 875 886 459 904 961 710 757 005 754 368 000 000 000

beträgt. (Können Sie diese Zahl vorlesen?) ⁎ ☺

10. Gruppenoperationen

Worum geht es? Wir fassen Elemente einer Gruppe G als Bijektionen auf einer Menge M auf und lassen G auf diese Weise auf M *operieren*. Mit dem Begriff des *Operationshomomorphismus* lernen wir eine alternative Darstellung einer solchen *Gruppenoperation* kennen. Wir führen den Begriff der *treuen Operation* ein und lernen mit der *Operation durch Konjugation* und der *Nebenklassenoperation* zwei wichtige Operationen kennen. ⁜

Gruppen als Mengen von Bijektionen, Gruppenoperationen

Der abstrakte Gruppenbegriff, den wir in 1.2 kennengelernt haben, klärt nicht, wie Elemente einer Gruppe aussehen, sondern normiert nur, dass sie durch Verknüpfung aufeinander einwirken und dabei gewissen Regeln zu gehorchen haben. Dieser Gruppenbegriff ist relativ jung; er taucht um 1882 das erste Mal in der Literatur auf und setzte sich nur langsam durch.
Gruppentheorie wurde aber schon viel früher betrieben. Die damals behandelten Objekte waren Mengen von *Symmetrien* oder *Substitutionen*. Beide Begriffe würde man mit dem Wort *Bijektion* in die heutige Sprache übersetzen. Zu einer Gruppe G im klassischen Sinn gehört daher eine Menge M; jedes Gruppenelement $g \in G$ ist eine Bijektion $M \to M$. Die betrachtete Verknüpfung ist die Komposition von Abbildungen. Im heutigen Sprachgebrauch würde man G als Untergruppe der $\mathrm{Sym}(M)$ bezeichnen.

Beispiel 10.1 Ein Beispiel für eine Klasse von klassischen Gruppen sind die **Symmetriegruppen ebener Objekte**: Hier ist M die Ebene $\mathbb{R}^2$. Für eine gegebene Teilmenge $S \subseteq \mathbb{R}^2$ setzt man

$$G := \{f \in \mathrm{Sym}(M) \mid f(S) = S\}.$$

G besteht also aus allen Bijektionen $M \to M$, die die Menge S wieder auf sich selbst abbilden. Man sieht mit dem Untergruppenkriterium leicht, dass G eine Gruppe im modernen Sinne ist. ⁉
Oft fordert man zusätzlich, dass die Bijektionen $f \in G$ „geometrisch motiviert" sind, sich also aus geometrischen Grundabbildungen wie Rotationen, Spiegelungen, Verschiebungen, etc. zusammensetzen.
Die Diedergruppen sowie die Gruppe $\mathrm{GL}(2, \mathbb{R})$ sind typische Beispiele für Symmetriegruppen ebener Objekte. (Welche Mengen S werden jeweils fixiert?) ⁜ ⁉

Vorteilhaft am klassischen Gruppenbegriff ist, dass neben der reinen Gruppenstruktur auch die Abbildungsnatur der Gruppenelemente zur Verfügung steht. Dies liefert Zusatzinformationen über die Gruppe, die allein aus dem abstrakten Gruppenbegriff vielleicht gar nicht oder nur sehr schwierig gefolgert werden können.

Gruppenoperationen stellen den klassischen Gruppenbegriff nach, indem die Elemente einer im modernen Sinn gegebenen Gruppe G als Elemente der $\mathrm{Sym}(M)$ für eine Menge M aufgefasst werden. Für $g, h \in G$ interpretiert man dann das Produkt $g \cdot h$ als Verkettung von Abbildungen. Außerdem ermöglicht man es, Elemente $m \in M$ in Gruppenelemente $g \in G$ einzusetzen; man schreibt allerdings üblicherweise $g \bullet m$ statt

$g(m)$. Zuletzt überträgt man die Bedeutung des Neutralen in G, indem man es mit der identischen Abbildung id_M identifiziert.
Aus diesen Schreibweisen folgen für beliebige $g, h \in G$ und $m \in M$ die Rechenregeln $1 \bullet m = m$ sowie

$$gh \bullet m = (g \cdot h)(m) = (g \circ h)(m) = g(h(m)) = g(h \bullet m) = g \bullet (h \bullet m).$$

Die folgende Definition formalisiert obige Überlegungen und klärt, was gemeint ist, wenn wir sagen, dass Gruppenelemente als Bijektionen aufgefasst werden.

Definition 10.2 (Gruppenoperation) *Wir sagen, dass **die Gruppe G auf der Menge M operiert**, wenn M nicht-leer ist und eine Abbildung*

$$\bullet : G \times M \to M, \qquad (g, m) \mapsto g \bullet m$$

*existiert, so dass die folgenden **Operationsaxiome** erfüllt sind:*

Neutrales operiert identisch *Für das Neutrale $1 \in G$ und beliebiges $m \in M$ gilt $1 \bullet m = m$.*

Verträglichkeit von $\cdot$ und $\bullet$ *Für alle $g, h \in G$ und alle $m \in M$ gilt $gh \bullet m = g \bullet (h \bullet m)$.*

Bemerkung 10.3 (a) Operiert eine Gruppe G auf einer Menge M, so steht für $g \in G$ und $m \in M$ die Notation $g \bullet m$ zur Verfügung. Sei g fixiert. Wir betrachten die Abbildung

$$f_g : M \to M, \qquad m \mapsto g \bullet m.$$

Die Schreibweise $g \bullet m$ bedeutet gerade das Einsetzen von m in die Abbildung f_g, also das Berechnen des Ausdrucks $f_g(m)$.

Das weiter oben in der Einleitung beschriebene Identifizieren von Gruppenelementen mit Abbildungen meint, dass man, gedanklich und mathematisch unsauber, $g = f_g$ setzt.

(b) Die Operationsaxiome stellen sicher, dass die Sonderrolle des Neutralen auch beim Übergang auf die Abbildungen gewahrt bleibt und dass sich die Gruppenmultiplikation genauso verhält wie die Komposition der jeweiligen Abbildungen.

(c) Aus den Operationsaxiomen folgt, dass die Abbildungen f_g aus (a) tatsächlich *Bijektionen* sind (Dies haben wir in der Definition nicht gefordert!), denn für alle $m \in M$ gilt

$$(f_g \circ f_{g^{-1}})(m) = gg^{-1} \bullet m \overset{1 \bullet m = m}{=} m \overset{1 \bullet m = m}{=} g^{-1}g \bullet m = (f_{g^{-1}} \circ f_g)(m).$$

Damit sind die Abbildungen f_g und $f_{g^{-1}}$ invers zueinander (und beide bijektiv). ⋇

Wir starten mit Beispielen für Gruppenoperationen, bei denen die Gruppen *in natürlicher Weise* operieren. Hier sind die Gruppenelemente von vornherein Bijektionen; eine zusätzliche Übersetzung von Gruppenelementen in Abbildungen findet nicht statt. Machen Sie sich klar, dass in den folgenden Beispielen die Operationsaxiome erfüllt sind! ?

Beispiel 10.4 (a) Sei M eine nicht-leere Menge. Dann operiert jede Untergruppe U von $\mathrm{Sym}(M)$ auf M durch die Festsetzung $g \bullet m := g(m)$ für $g \in U$ und $m \in M$.

Speziell operiert jede Untergruppe von S_n auf der Menge $\{1, \dots, n\}$. Außerdem operieren die Gruppen aus 10.1 sowohl auf $\mathbb{R}^2$ als auch auf S. ⁉

(b) Seien K ein Körper, $n \in \mathbb{N}$ und $V := K^n$ der n-dimensionale Vektorraum über K. Dann operiert jede Untergruppe U von $\mathrm{GL}(n, K)$ auf V durch die Festsetzung

$$A \bullet v := A \cdot v \qquad \text{für } A \in U \text{ und } v \in V;$$

mit $\cdot$ ist die Matrix-Vektor-Multiplikation gemeint.

(c) Wir führen das Beispiel aus (b) fort: Für $k \in \{0, \dots, n\}$ sei V_k die Menge der k-dimensionalen Unterräume von V. Wir setzen $\bullet$ auf V_k fort, indem wir für einen Unterraum $W \in V_k$ und $A \in U$ definieren

$$A \bullet W := \{A \bullet w \mid w \in W\} = \{A \cdot w \mid w \in W\}.$$

Da reguläre Matrizen linear unabhängige Vektoren auf linear unabhängige Vektoren abbilden, ist $A \bullet W$ ebenfalls Vektorraum der Dimension k. Dies zeigt, dass $\bullet$ abgeschlossen ist. Ähnlich wie in (b) folgt dann, dass U auf V_k operiert. ⁉ ⁂

Wir stellen einen weiteren Zusammenhang zwischen Gruppenelementen g und den zugehörigen Abbildungen f_g aus 10.3 (a) her. Beachten Sie, dass f_g wegen 10.3 (c) in $\mathrm{Sym}(M)$ liegt.

Satz 10.5 *Die Gruppe G operiere auf der Menge M. Zu $g \in G$ definieren wir die Bijektion $f_g : M \to M$ durch $f_g(m) := g \bullet m$. Dann gilt: Die Abbildung*

$$\varphi : G \to \mathrm{Sym}(M), \qquad g \mapsto f_g,$$

die einem Gruppenelement die durch es bewirkte Bijektion auf M zuordnet, ist ein Homomorphismus.

Beweis. Seien $g, h \in G$ beliebig. Es ist zu zeigen, dass $\varphi(gh) = \varphi(g) \circ \varphi(h)$ gilt, also dass $f_{gh} = f_g \circ f_h$ erfüllt ist. Sei hierzu $m \in M$ beliebig. Dann gilt

$$f_{gh}(m) \overset{\text{Def. } f_{gh}}{=} gh \bullet m \overset{10.2}{=} g \bullet (h \bullet m) \overset{\text{Def. } f_g}{=} f_g(h \bullet m) \overset{\text{Def. } f_h}{=} f_g(f_h(m)) = (f_g \circ f_h)(m).$$

Die Abbildungen f_{gh} und $f_g \circ f_h$ bilden M also auf gleiche Weise ab und sind identisch. ■

In 10.5 gilt auch die Rückrichtung: Homomorphismen der Form $G \to \mathrm{Sym}(M)$ liefern Operationen auf M:

Satz 10.6 *Seien G eine Gruppe, M eine nicht-leere Menge und $\varphi : G \to \mathrm{Sym}(M)$ ein Homomorphismus. Dann ist durch die Abbildung*

$$\bullet : G \times M \to M, \qquad g \bullet m := \varphi(g)(m)$$

eine Operation von G auf M gegeben.

Beweis. Das Neutrale von G operiert identisch auf M, denn für beliebiges $m \in M$ gilt $1 \bullet m = \varphi(1)(m) = \mathrm{id}_M(m) = m$.
Ferner sind die Gruppenmultiplikation und $\bullet$ verträglich; für alle $g, h \in G$ und $m \in M$ ist nämlich

$$gh \bullet m = \varphi(gh)(m) \overset{\varphi \text{ homom.}}{=} (\varphi(g) \circ \varphi(h))(m) = \varphi(g)(\varphi(h)(m)) = \varphi(g)(h \bullet m) = g \bullet (h \bullet m).$$

Damit ist gezeigt, dass durch $\bullet$ eine Operation von G auf M gegeben ist. ■

Bemerkung 10.7 (a) Beachten Sie, dass die auf den ersten Blick seltsam anmutende Schreibweise $\varphi(g)(m)$ in 10.6 definiert ist: $\varphi(g)$ ist ein Element aus $\mathrm{Sym}(M)$ und daher eine Funktion. Der Ausdruck $\varphi(g)(m)$ beschreibt also das Einsetzen von m in die Funktion $\varphi(g)$.

(b) Wendet man auf eine Operation $\bullet$ zuerst 10.5 und anschließend 10.6 auf den erhaltenen Homomorphismus φ an, so erhält man eine Operation $\overline{\bullet}$:

$$\text{Operation } \bullet \overset{10.5}{\longrightarrow} \text{Homomorphismus } \varphi \text{ zu } \bullet \overset{10.6}{\longrightarrow} \text{Operation } \overline{\bullet} \text{ zu } \varphi.$$

Dann ist $\bullet = \overline{\bullet}$, denn für beliebige $g \in G$ und $m \in M$ gilt

$$g \mathbin{\overline{\bullet}} m \overset{\text{Def. } \overline{\bullet}, \text{ vgl. } 10.6}{=} \varphi(g)(m) \overset{\text{Def. } \varphi, \text{ vgl. } 10.5}{=} f_g(m) = g \bullet m.$$

Nun starten wir mit einem Homomorphismus $\varphi : G \to \mathrm{Sym}(M)$, erzeugen aus diesem mit 10.6 eine Operation $\bullet$ und aus $\bullet$ mit Hilfe von 10.5 einen Homomorphismus $\overline{\varphi}$:

$$\text{Homomorphismus } \varphi \overset{10.6}{\longrightarrow} \text{Operation } \bullet \text{ zu } \varphi \overset{10.5}{\longrightarrow} \text{Homomorphismus } \overline{\varphi} \text{ zu } \bullet.$$

Dann folgt, ähnlich wie oben, $\varphi = \overline{\varphi}$.

Dies zeigt, dass die Konstruktionen aus den obigen Sätzen invers zueinander sind. Beim Übergang von Operation auf Homomorphismus bzw. von Homomorphismus auf Operation gehen keine Informationen verloren.

(c) In 10.2 haben wir eine Möglichkeit gesehen, wie man eine Identifikation von Gruppenelementen mit Bijektion mathematisch modellieren kann.

Teil (b) liefert eine Alternative: Wir können jedem Gruppenelement $g \in G$ mittels einer Abbildung $\varphi : G \to \mathrm{Sym}(M)$ eine Bijektion $f_g \in \mathrm{Sym}(M)$ zuordnen. Um sicherzustellen, dass die Menge der Abbildungen $\{\varphi(g) \mid g \in G\}$ eine „ähnliche Struktur“ wie G besitzt, fordern wir zusätzlich, dass φ homomorph ist.

Wegen (b) entsteht auf diese Weise ebenfalls eine Gruppenoperation. Welche Sichtweise auf Operationen man bevorzugt, ist letztlich Geschmackssache. ⋇

Wegen Teil (b) und (c) der obigen Bemerkung vereinbaren wir:

Vereinbarung zur Schreibweise 10.8 Sind G eine Gruppe und M eine nicht-leere Menge, so bezeichnen wir auch jeden Homomorphismus vom Typ $G \to \mathrm{Sym}(M)$ als eine Operation von G auf M. ⁜

Bemerkung 10.9 Untergruppen von symmetrischen Gruppen nennt man **Permutationsgruppen**; ihre Elemente sind Bijektionen. Der klassische Gruppenbegriff, den wir am Anfang der Vorlesung vorgestellt haben, umfasst nur Permutationsgruppen.
Operiert eine Gruppe G auf einer Menge, so wird G durch den Operationshomomorphismus φ in eine Permutationsgruppe $\varphi(G)$ überführt. Man nennt $\varphi(G)$ auch die **durch die Operation gegebene Permutationsgruppe**. ⁜

Kern einer Operation, Treue

Operationen von G auf M und Homomorphismen von $G \to \mathrm{Sym}(M)$ sind äquivalente Konzepte. Die folgenden Sprechweisen sind daher sinnvoll:

Definition 10.10 *Die Gruppe G operiere auf der Menge M durch $\bullet$. Dann nennen wir den nach 10.5 gewonnen Homomorphismus $G \to \mathrm{Sym}(M)$ den **Operationshomomorphismus zu $\bullet$**. Seinen Kern bezeichnen wir als **Kern der Operation**.*

Bemerkung 10.11 (a) Der Kern einer Operation besteht genau aus denjenigen $g \in G$, die vom Operationshomomorphismus auf id_M abgebildet werden, für die also gilt:

$$g \bullet m = \mathrm{id}_M(m) = m \qquad \text{für alle } m \in M.$$

Kernelemente sind also genau die Gruppenelemente, die *jedes* $m \in M$ fixieren.

(b) Sind zwei Gruppenelemente $g, h \in G$ verschieden, so können die ihnen zugeordneten Permutationen $f_g, f_h \in \mathrm{Sym}(M)$ dennoch gleich sein. Dieser Fall tritt nach (a) beispielsweise auf, wenn g und h beide im Kern der Operation liegen.

Die durch die Operation gegebene Permutationsgruppe kann also „kleiner“ als die Ausgangsgruppe sein. ⁜

Teil (b) der obigen Bemerkung motiviert die folgende Definition:

Definition 10.12 (Treue) *Eine Operation einer Gruppe G auf einer Menge M heißt **treu**, wenn verschiedenen Elementen aus G stets verschiedene Bijektionen zugeordnet werden, wenn also mit der Notation aus 10.5 für alle $g, h \in G$ gilt: $g \neq h \Longrightarrow f_g \neq f_h$.*

Das folgende Lemma liefert einige Äquivalenzen zur Treue einer Operation:

Lemma 10.13 *Die Gruppe G operiere auf der Menge M durch $\bullet$. Sei φ der zugehörige Operationshomomorphismus. Dann sind äquivalent:*

(a) *G operiert treu, d. h. für alle $g, h \in G$ mit $g \neq h$ folgt $f_g \neq f_h$.*

(b) $\ker \varphi = \{1\}$, *d. h. φ ist injektiv.*

(c) *Nur* $1 \in G$ *fixiert alle* $m \in M$.

(d) $\varphi : G \to \varphi(G)$ *ist ein Isomorphismus.*

(e) *Zu jedem* $g \in G \setminus \{1\}$ *gibt es ein* $m \in M$ *mit* $g \bullet m \neq m$.

Beweisskizze. Wir zeigen die Äquivalenz von (a) und (b): Genau dann liegt eine treue Operation vor, wenn aus $g \neq h$ stets $f_g \neq f_h$ folgt, d. h. wenn $\varphi(g) \neq \varphi(h)$ gilt. Dies bedeutet aber, dass φ injektiv ist. Hierzu äquivalent ist $\ker \varphi = \{1\}$.
Die restlichen Äquivalenzen folgen direkt aus den Definitionen. ■

Bemerkung 10.14 Die Aussage in 10.13 (d) lässt sich wie folgt interpretieren: Operiert G treu, so ist $\varphi(G)$ isomorph zu G. Wir verlieren also keine Informationen über die Struktur von G, wenn wir statt G die durch die Operation gegebene Permutationsgruppe betrachten. ⁜

Beispiel 10.15 (a) Die Gruppe S_n operiert treu auf $\{1, \dots, n\}$, denn nur $\mathrm{id}_{\{1,\dots,n\}}$ fixiert jedes der Elemente $1, \dots, n$.

(b) Seien G eine Gruppe und M eine Menge. Durch die Festsetzung $g \bullet m := m$ für alle $g \in G$ und $m \in M$ ist eine Operation von G auf M gegeben. Diese Operation ist treu genau dann, wenn $G = \{1\}$ gilt. ⁉

(c) Die Operation der $\mathrm{GL}(n, K)$ auf dem Vektorraum K^n aus 10.4 (b) ist treu, denn nur die Einheitsmatrix fixiert alle Vektoren des K^n. ⁜

Knobelfrage. Ist die Operation der $\mathrm{GL}(n, K)$ auf der Menge der eindimensionalen Unterräume des K^n aus 10.4 (c) treu? Was ist der Kern der Operation? ⁉

Konjugations- und Nebenklassenoperation

Wir stellen zwei wichtige Gruppenoperationen vor.

Operation per Konjugation Seien G eine Gruppe und $N \trianglelefteq G$ ein Normalteiler. Wir setzen

$$g \bullet n := g \cdot n \cdot g^{-1} \qquad \text{für alle } g \in G \text{ und } n \in N.$$

Dies liefert eine Operation von G auf N, denn für alle $g, h \in G$ und $n \in N$ gelten $g \bullet n \in N$ sowie $1 \bullet n = 1 \cdot n \cdot 1^{-1} = n$ und

$$gh \bullet n = ghn(gh)^{-1} = g \cdot hnh^{-1} \cdot g^{-1} \overset{hnh^{-1} \in N}{=} g \bullet (hnh^{-1}) = g \bullet (h \bullet n).$$

Man sagt auch, dass G **durch Konjugation** auf N operiere. (Wo geht $N \trianglelefteq G$ ein?) ⁉
Diese Operation ist im Allgemeinen nicht treu, beispielsweise, wenn G abelsch ist. Der Kern der Operation ist gegeben durch ⁉

$$C_G(N) := \{g \in G \mid gng^{-1} = n \text{ für alle } n \in N\} = \{g \in G \mid gn = ng \text{ für alle } n \in N\}.$$

Man nennt $C_G(N)$ den **Zentralisator von N in G**. Er ist als Kern ein Normalteiler von G. ⁉

Ein besonders wichtiger Normalteiler von G ist der Zentralisator von G in G, der der Kern der Operation von G auf sich selbst per Konjugation ist:

Definition 10.16 (Zentrum) *Sei G eine Gruppe. Dann nennt man den Zentralisator*

$$C_G(G) = \{g \in G \mid gng^{-1} = n \text{ für alle } n \in G\} = \{g \in G \mid gn = ng \text{ für alle } n \in G\}$$

*von G in G das **Zentrum von G** und schreibt $Z(G)$ für es. $Z(G)$ ist ein Normalteiler von G und besteht genau aus den Elementen von G, die mit jedem beliebigen Element aus G kommutieren.*

Nebenklassenoperation Seien G eine Gruppe, $U \leq G$ eine Untergruppe von G und $M := G/U$ die Menge der Nebenklassen von U in G. Dann operiert G auf M durch

$$g \bullet mU := g \cdot mU = gmU \qquad \text{für alle } g, m \in G.$$

(Können Sie die Operationsaxiome verifizieren?) Man nennt diese Operation die **Nebenklassenoperation von G auf den Nebenklassen von U**. ⁉
Diese Operation ist im Allgemeinen nicht treu; denn ist beispielsweise $U \trianglelefteq G$, so gilt für jedes $g \in U$ und jedes $mU \in G/U$

$$g \bullet mU = gmU = m \cdot \underbrace{m^{-1}gm}_{\in U \trianglelefteq G} \cdot U = mU.$$

In diesem Fall fixiert also jedes $g \in U$ jedes Element aus M.

Als erste Anwendung der Theorie der Gruppenoperationen zeigen wir den Satz von Cayley; die verwendeten Schlussweisen sind typisch für Gruppenoperationsbeweise.

Satz 10.17 (Cayley) *Jede Gruppe G ist isomorph zu einer Untergruppe von* $\mathrm{Sym}(G)$.

Beweis. Wir betrachten die Nebenklassenoperation von G auf $M := G/\{1\}$. Die Operation ist treu, denn für $g \in G$ mit $g \neq 1$ gilt $g \bullet \{1\} = \{g\} \neq \{1\}$. Nach 10.13 (d) ⁉ enthält $\mathrm{Sym}(M)$ eine zu G isomorphe Untergruppe.
Wir können M durch die Bijektion $\{g\} \mapsto g$ mit der Menge G identifizieren und erhalten daher die Isomorphie $\mathrm{Sym}(M) \cong \mathrm{Sym}(G)$. Daher besitzt auch $\mathrm{Sym}(G)$ eine zu G isomorphe Untergruppe. ■

Cayley zeigt, dass der moderne, abstrakte Gruppenbegriff nicht allgemeiner als der klassische Gruppenbegriff ist. Haben Sie eine Vermutung, warum sich der moderne Begriff dennoch durchgesetzt hat? ⁉

11. Bahnen

Worum geht es? Wir bauen die Theorie der Gruppenoperationen aus, führen den Begriff der *Bahn* ein und zeigen, dass die Menge M von den Bahnen von G partitioniert wird. Dies liefert die *Bahnengleichung* und, als wichtigen Spezialfall, die *Klassengleichung*.⁂

Erreichbarkeit, Bahnen, Transitivität

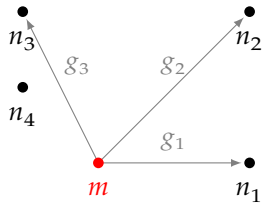
Wir wollen genauer untersuchen, wie Gruppenoperationen Elemente der Menge M permutieren. Hierzu führen wir die folgenden Sprechweisen ein:

Definition 11.1 *Die Gruppe G operiere auf der Menge M.*

(a) *Gilt die Gleichung $n = g \bullet m$ für Elemente $n, m \in M$ und $g \in G$, so sagen wir, dass **n von m aus erreichbar** ist.*

(b) *Sei $m \in M$. Dann bezeichnen wir die Menge $G \bullet m := \{g \bullet m \mid g \in G\}$ aller von m aus erreichbaren Elemente als **Bahn von G durch m**.*

Bemerkung 11.2 Sei $G \to \mathrm{Sym}(M)$ eine Gruppenoperation. Die Begriffe aus 11.1 klären, wohin ein Element $m \in M$ durch die Elemente aus G abgebildet werden kann:



n ist von m aus erreichbar, wenn ein $g \in G$ existiert, so dass m durch g auf n abgebildet wird.
In der linken Grafik betrachten wir den roten Punkt $m \in M$. Durch Anwenden der Gruppenelemente g_1, g_2, g_3 auf m erreichen wir die Punkte $n_1, n_2, n_3 \in M$. Das Element n_4 ist von m aus nicht erreichbar; es existiert kein $g \in G$ mit $g \bullet m = n_4$.

Die Bahn $G \bullet m$ durch $m \in M$ fasst alle Elemente, die von m aus erreichbar sind, in einer Menge zusammen. Sie entsteht, indem man für alle $g \in G$ die Elemente $g \bullet m$ berechnet und diese dann in einer Menge zusammenfasst. ⁂

Wir stellen einige grundlegende Eigenschaften des Erreichbarkeitsbegriffs zusammen. Können Sie diese Eigenschaften grafisch analog zu oben interpretieren? ⁇

Lemma 11.3 *Die Gruppe G operiere auf der Menge M. Für Elemente $m, n, p \in M$ gelten dann:*

(a) *m ist von sich selbst aus erreichbar. Insbesondere folgt $m \in G \bullet m$.*

(b) *Ist n von m aus erreichbar, so ist auch m von n aus erreichbar.*

(c) *Sind p von n und n von m aus erreichbar, so ist p von m aus erreichbar.*

Beweisskizze. Es gilt $m = 1 \bullet m$; dies zeigt (a). Aus $n = g \bullet m$ folgt $g^{-1} \bullet n = m$, was (b) zeigt. Gelten $p = g \bullet n$ und $n = h \bullet m$, so ist $p = gh \bullet m$. Dies beweist (c). ■

Der folgende Satz bildet die Grundlage für die wichtige Bahnengleichung:

Satz 11.4 *Die Gruppe G operiere auf der Menge M. Dann bildet die Menge der Bahnen eine Partition von M, d. h. es gibt eine Indexmenge I und Vertreter m_i der einzelnen Bahnen, so dass gilt*

$$M = \dot{\bigcup_{i\in I}} G \bullet m_i \qquad (\textit{disjunkte Vereinigung}).$$

Man nennt diese Partition von M die ***Bahnenzerlegung von M****.*

Beweis. Wir wissen aus 11.3 (a), dass für alle $m \in M$ gilt $m \in G \bullet m$. Dies zeigt, dass keine Bahn leer ist und dass jedes $m \in M$ in einer Bahn enthalten ist, beispielsweise in $G \bullet m$. Zu zeigen ist also nur noch, dass je zwei Bahnen entweder identisch oder disjunkt sind. Hierzu betrachten wir zwei nicht-disjunkte Bahnen $G \bullet m$ und $G \bullet n$. Dann existiert $x \in G \bullet m \cap G \bullet n$, und wir finden $g_1, g_2 \in G$ mit $x = g_1 \bullet m$ bzw. mit $x = g_2 \bullet n$. Aufgrund der Verträglichkeit von $\cdot$ und $\bullet$ erhalten wir

$$G \bullet m = Gg_1 \bullet m = G \bullet (g_1 \bullet m) = G \bullet x = G \bullet (g_2 \bullet n) = Gg_2 \bullet n = G \bullet n.$$

Damit ist der Satz gezeigt. ■

Beispiel 11.5 (a) Wir betrachten die Operationen von $\mathrm{GL}(n, K)$ aus 10.4 (b) und (c).

Für $k \in \{0, \dots, n\}$ sei $E_k := \{e_1, \dots, e_k\}$ die Menge der ersten k Einheitsvektoren des K^n. Es gilt $\dim \operatorname{span}(E_k) = k$. Seien $b_1, \dots, b_k \in K^n$ linear unabhängig. Wir zeigen, dass $A \in \mathrm{GL}(n, K)$ existiert mit $A \cdot e_i = b_i$. Hierzu setzen wir die Menge der b_i zu einer Basis $B = \{b_1, \dots, b_n\}$ des K^n fort. Dann existiert eine lineare Abbildung $K^n \to K^n$ mit $e_i \mapsto b_i$ für alle $i \in \{1, \dots, n\}$. Die zugehörige Darstellungsmatrix A bezüglich der Basis E_n erfüllt dann $A \in \mathrm{GL}(n, K)$ und $A \cdot e_i = b_i$.

Diese Überlegung zeigt, dass $V_k = \mathrm{GL}(n, K) \bullet \operatorname{span}(E_k)$ gilt. Die Mengen V_k sind also Bahnen von $\mathrm{GL}(n, K)$; jeder k-dimensionale Untervektorraum von K^n lässt sich durch eine reguläre Matrix auf jeden anderen k-dimensionalen Untervektorraum des K^n abbilden.

Weiter folgt, dass die Bahnenzerlegung der Operation aus 10.4 (b) gegeben ist durch $V = \{0\} \cup (V \setminus \{0\})$.

(b) Die Gruppe G operiere per Konjugation auf sich selbst. Die Bahnen dieser Operation nennt man die **Konjugationsklassen von G**; die Konjugationsklasse durch ein Element $x \in G$ ist die Menge $\{gxg^{-1} \mid g \in G\}$ aller zu x konjugierten Elemente.

Wegen 8.17 enthält eine Konjugationsklasse von S_n genau die Permutationen desselben Zykeltyps.

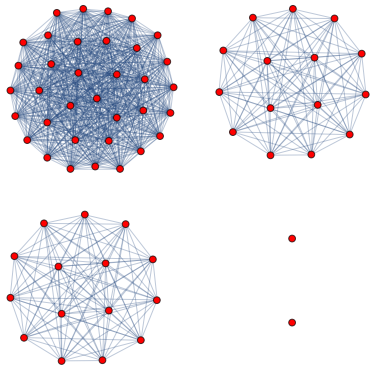
Normalteiler von G sind genau diejenigen Untergruppen von G, die sich als disjunkte Vereinigung von Konjugationsklassen von G schreiben lassen. ⁂

Bemerkung 11.6 Operiert G auf der Menge M, so ist M nach 11.4 eine disjunkte Vereinigung von Bahnen. Sind umgekehrt $M_1, \dots, M_n$ disjunkte Bahnen von G mit zugehörigen Operationen $\bullet_1, \dots, \bullet_n$, so operiert G auf der Menge $M := \bigcup_{i=1}^{n} M_i$ durch

$$g \bullet m := \begin{cases} g \bullet_1 m & \text{falls } m \in M_1, \\ \vdots & \vdots \\ g \bullet_n m & \text{falls } m \in M_n. \end{cases}$$

Bahnen stellen daher die Grundbausteine für Mengen M dar, auf denen Gruppen operieren. ※

Beispiel 11.7 Wir betrachten nochmals die Operation von $\mathrm{GL}(n, K)$ aus 10.4 (c). Mit obiger Bemerkung folgt, dass $\mathrm{GL}(n, K)$ auch auf der Menge M aller Unterräume des K^n operiert. Mit 11.5 folgt die Bahnenzerlegung $M = V_0 \dot\cup V_1 \dot\cup \cdots \dot\cup V_n$.



Wir setzen konkret $K = \mathbb{Z}_2$ und $n = 4$. Dann besitzt $V = \mathbb{Z}_2^4$ jeweils einen null- und einen vierdimensionalen, jeweils 15 ein- und dreidimensionale und 35 zweidimensionale Unterräume. Es gilt $|M| = 67$, und M zerfällt in fünf Bahnen.
Um die Bahnenzerlegung grafisch zu veranschaulichen, verbinden wir zwei verschiedene Elemente aus M, wenn eines vom anderen aus erreichbar ist. Es entsteht das linke Bild; die roten Punkte stellen die Elemente aus M, also die Unterräume des $\mathbb{Z}_2^4$ dar.

※

Bahnen sind die kleinsten Mengen, auf denen eine Gruppe operieren kann. Die folgende Definition dient dazu, diese kleinsten Mengen sprachlich besser zu fassen:

Definition 11.8 *Eine Gruppenoperation von G auf M heißt **transitiv**, wenn M eine Bahn von G ist, d. h. wenn zu je zwei Elementen $m, n \in M$ ein $g \in G$ existiert mit $n = g \bullet m$.*

Wir stellen einige Äquivalenzen zum Transitivitätsbegriff vor. Besonders die Aussagen in (b) und (c) werden in der Praxis gern benutzt: Zum Transitivitätsnachweis reicht es aus, ein *beliebiges* $m \in M$ zu wählen und $M = G \bullet m$ zu zeigen.

Lemma 11.9 *Die Gruppe G operiere auf der Menge M. Dann sind äquivalent:*

(a) *G operiert transitiv auf M, d. h. M ist eine Bahn von G.*

(b) *Es gibt ein $m \in M$ mit $M = G \bullet m$.*

(c) *Für jedes $n \in M$ gilt $M = G \bullet n$.*

Beweisskizze. Wir zeigen nur (b)$\Longrightarrow$(c); die restlichen Implikationen sind leicht: Sei $n \in M$ beliebig. Dann ist $n \in G \bullet m \cap G \bullet n$. Mit 11.4 folgt $G \bullet m = G \bullet n$. ■

Beispiel 11.10 (a) Wegen 11.5 (a) operiert $\mathrm{GL}(n, K)$ transitiv auf jeder der Mengen V_k.

(b) Die Operation einer Gruppe G auf sich selbst per Konjugation ist im Allgemeinen nicht transitiv, denn es gilt $G \bullet 1 = \{1\}$. Sie ist aber transitiv auf jeder Konjugationsklasse von G. ⁉

(c) Sei U eine Untergruppe einer Gruppe G. Dann ist die Nebenklassenoperation von G auf G/U transitiv wegen 11.9 (b), denn jede Nebenklasse gU ist von $1 \cdot U = U$ aus erreichbar: Es gilt $gU = g \bullet U$. ⋇

Die folgende Aussage ist besonders aufgrund ihres Beweises interessant; hier geht das erste Mal eine Transitivitäts-Schlussweise ein.

Satz 11.11 *Seien $n \geq 5$ und U eine Untergruppe der A_n mit $[A_n : U] < n$. Dann gilt $U = A_n$. Dies zeigt, dass A_n für diese n keine „großen" echten Untergruppen hat.*

Beweis. Sei $U \leq A_n$ mit $[A_n : U] < n$. Wir betrachten die Nebenklassenoperation von A_n auf $M := A_n/U$. Sei $\varphi : A_n \to \mathrm{Sym}(M)$ der zugehörige Operationshomomorphismus. Es gilt

$$|\mathrm{Sym}(M)| \overset{|M|=[A_n:U]}{=} [A_n : U]! \overset{[A_n:U]<n}{\leq} (n-1)! = \frac{1}{n} \cdot n! = \frac{1}{n} \cdot |S_n| \overset{n\geq 5}{<} |A_n|.$$

Der Definitionsbereich von φ besitzt also mehr Elemente als der Zielbereich. φ ist somit nicht injektiv. Die Einfachheit der A_n zeigt $\ker \varphi = A_n$. Aufgrund der Transitivität von φ nach 11.10 (c) muss $|M| = 1$ gelten. Dies liefert $U = A_n$. ■

Bahnlänge und Bahnengleichung

Wir betrachten in diesem Abschnitt speziell Operationen endlicher Gruppen. Dann sind auch alle Bahnen endlich. Wir können daher nach der Anzahl der Elemente in einer Bahn, der sogenannten **Bahnlänge**, fragen. Um diese bequem berechnen zu können, benötigen wir einen weiteren Begriff:

Definition 11.12 (Stabilisator) *Die Gruppe G operiere auf der Menge M. Für $m \in M$ bezeichnen wir die Menge*

$$G_m := \{g \in G \mid g \bullet m = m\}$$

*aller Gruppenelemente, die m fixieren, als den **Stabilisator von m in G**. Mit dem Untergruppenkriterium folgt, dass G_m eine Untergruppe von G ist. Aus Gründen der Übersichtlichkeit schreiben wir statt G_m manchmal auch $\mathrm{Stab}_G(m)$.*

Beispiel 11.13 (a) Seien G eine Gruppe und $U \leq G$. Wir betrachten die Nebenklassenoperation von G auf G/U. Dann ist $G_{1U} = U$, denn nach 4.1 (e) gilt $g \bullet 1U = gU = 1U$ genau dann, wenn $g \in U$ ist.

Sei $g \in G$ beliebig. Können Sie G_{gU} berechnen?

(b) Für $n > 1$ ist $\mathrm{Stab}_{S_n}(n) = \{p \in S_n \mid p(n) = n\}$. Diese Gruppe ist isomorph zu S_{n-1}. Wie sieht der Isomorphismus aus?

(c) Der Schnitt aller Stabilisatoren ist gerade der Kern der Operation.

(d) Die Gruppe G operiere auf der Menge M. Seien $m \in M$ und $g \in G$. Dann gilt $G_{g\bullet m} = g \cdot G_m \cdot g^{-1}$, denn es ist

$$\begin{aligned} G_{g\bullet m} &= \{s \in G \mid s \bullet (g \bullet m) = g \bullet m\} = \{s \in G \mid sg \bullet m = g \bullet m\} \\ &= \{s \in G \mid g^{-1}sg \bullet m = m\} = \{s \in G \mid g^{-1}sg \in G_m\} \\ &= \{s \in G \mid s \in g \cdot G_m \cdot g^{-1}\} = g \cdot G_m \cdot g^{-1}. \end{aligned}$$

Dies zeigt insbesondere: Operiert G transitiv auf M, so sind alle Stabilisatoren konjugiert zueinander, vgl. (a). ⋇

Das folgende Lemma stellt einen Zusammenhang zwischen der Bahn durch ein Element m und dem Stabilisator G_m her.

Lemma 11.14 *Die Gruppe G operiere auf der Menge M. Sei $m \in M$. Dann ist die Abbildung*

$$f : G/G_m \to G \bullet m, \qquad gG_m \mapsto g \bullet m$$

bijektiv.

Beweis. Wir müssen zunächst zeigen, dass f wohldefiniert ist (Warum?). Hierzu seien $g, h \in G$ gegeben mit $gG_m = hG_m$. Dann existiert $s \in G_m$ mit $g = hs$. Die Wohldefiniertheit von f folgt nun wegen

$$g \bullet m = hs \bullet m = h \bullet (s \bullet m) \overset{s\in G_m}{=} h \bullet m.$$

f ist surjektiv; denn jedes Element aus $G \bullet m$ lässt sich schreiben in der Form $g \bullet m$ und besitzt das Urbild gG_m.
f ist auch injektiv; denn gilt $f(gG_m) = f(hG_m)$ für Gruppenelemente $g, h \in G$, so folgt $g \bullet m = h \bullet m$, also $h^{-1}g \bullet m = m$. Dies liefert $h^{-1}g \in G_m$ und daher $gG_m = hG_m$. ■

Ist G eine endliche Gruppe, so ist G/G_m eine endliche Menge. Die Bijektion aus 11.14 zeigt, dass auch $G \bullet m$ endlich ist und dass $|G/G_m| = |G \bullet m|$ gilt. Dies können wir mit Lagrange umschreiben und erhalten:

Satz 11.15 (Bahnlängenformel) *Die **endliche** Gruppe G operiere auf der Menge M. Es sei $m \in M$. Dann stimmt die Länge der Bahn von G durch m mit dem Index von G_m in G überein, d.h. es gilt*

$$|G \bullet m| = [G : G_m] = \frac{|G|}{|G_m|}.$$

Man sagt oft kürzer: Bahnlänge = Stabilisatorindex.

Beispiel 11.16 (a) Keine Operation der A_4 besitzt Bahnen der Länge Zwei, denn A_4 hat nach 9.11 keine Untergruppe der Ordnung 6, also vom Index Zwei. Dies zeigt insbesondere, dass A_4 nicht transitiv auf zwei Elementen operieren kann.

(b) Seien p eine Primzahl und G eine Gruppe von p-Potenzordnung. Dann ist wegen Lagrange die Länge einer Bahn von G stets eine p-Potenz. ⁂ ⁉

Bemerkung 11.17 Die Bahnlängenformel liefert lediglich eine Einschränkung an die möglichen Bahnlängen einer endlichen Gruppe G: Wenn G (bei irgendeiner Operation) eine Bahn der Länge k besitzt, so muss G eine Untergruppe vom Index k besitzen.
Mit der Nebenklassenoperation folgt aber eine Umkehrung der obigen Aussage: Besitzt G eine Untergruppe U vom Index k, so ist die Nebenklassenoperation von G auf G/U eine transitive Operation auf k Elementen. Es gibt also eine Operation von G mit einer Bahn der Länge k. ⁂

Wir setzen nun G und M als endlich voraus. Dann liefern die Bahnenzerlegung nach 11.4 und die Bahnlängenformel einen Zusammenhang zwischen $|G|$ und $|M|$:

Satz 11.18 (Bahnengleichung) *Die **endliche** Gruppe G operiere auf der **endlichen** Menge M. Seien $B_1, \dots, B_r$ die Bahnen von G und $b_i \in B_i$ Vertreter der einzelnen Bahnen. Dann gilt aufgrund der Bahnenzerlegung $|M| = \sum_{i=1}^{r} |B_i|$.*
Mit der Bahnlängenformel folgt hieraus

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

Im Spezialfall, in dem die endliche Gruppe G auf sich selbst per Konjugation operiert, folgt:

Korollar 11.19 (Klassengleichung) *Seien G eine endliche Gruppe und $K_1, \dots, K_r$ die Konjugationsklassen von G von Länge mindestens Zwei. Dann gilt*

$$G = Z(G) \cup \dot{\bigcup_{i=1}^{r}} K_i \qquad \textit{und somit} \qquad |G| = |Z(G)| + \sum_{i=1}^{r} |K_i|,$$

wobei wir mit $Z(G)$ das Zentrum von G bezeichnen.

Beweis. Wir betrachten die Operation von G auf sich selbst per Konjugation und bezeichnen mit $B_1, \dots, B_k$ die Konjugationsklassen der Länge Eins. Dann existieren $b_i \in G$ mit $B_i = \{b_i\}$. Es gilt $Z(G) = \dot{\bigcup}_{i=1}^{k} B_i = \{b_1, \dots, b_k\}$; denn für ein Gruppenelement $g \in G$ sind die Aussagen $g \in Z(G)$ sowie $x \bullet g = g$ für alle $x \in G$ äquivalent. Mit der Bahnenzerlegung von G erhalten wir

$$G = \dot{\bigcup_{i=1}^{k}} B_i \cup \dot{\bigcup_{i=1}^{r}} K_i = Z(G) \cup \dot{\bigcup_{i=1}^{r}} K_i.$$

Betrachten der Ordnungen in dieser Gleichung liefert $|G| = |Z(G)| + \sum_{i=1}^{r} |K_i|$. ■

Die Klassengleichung erlaubt es, eine wichtige Aussage über p-Gruppen zu beweisen. Wir klären zunächst, was eine p-Gruppe überhaupt ist:

Definition 11.20 *Für eine Primzahl $p \in \mathbb{P}$ nennen wir jede Gruppe von p-Potenzordnung eine* ***p-Gruppe****.*

Beispiel 11.21 Die triviale Gruppe $\{1\}$ ist eine p-Gruppe zu jedem $p \in \mathbb{P}$. Die Kleinsche Vierergruppe ist eine 2-Gruppe. ⋇

Der Beweis des nächsten Satzes stellt eine typische Anwendung der Klassengleichung vor:

Satz 11.22 *Sei G eine p-Gruppe mit $|G| > 1$. Dann gilt $|Z(G)| > 1$.*
Man sagt auch kürzer: Nicht-triviale p-Gruppen besitzen nicht-triviale Zentren.

Beweis. Seien $K_1, \dots, K_r$ die Konjugationsklassen von G von Länge mindestens Zwei. Wegen 11.16 (b) ist $|K_i|$ eine p-Potenz, die größer als Eins ist. Daher teilt p die Länge einer jeden Konjugationsklasse $|K_i|$.
Mit der Klassengleichung folgt

$$|G| - \sum_{i=1}^{r} |K_i| = |Z(G)|.$$

Die linke Seite dieser Gleichung wird von p geteilt. Daher muss auch die Ordnung von $Z(G)$ von p geteilt werden. Dies zeigt $|Z(G)| \geq p > 1$. ■

12. Mehr zu p-Gruppen, Sylowtheorie

Worum geht es? Wir setzen unsere Beschäftigung mit p-Gruppen fort und zeigen, dass p-Gruppen stets Lagrangegruppen sind. Außerdem bestimmen wir die Isomorphietypen von Gruppen der Ordnung p^2.
Danach beschäftigen wir uns mit den für die endliche Gruppentheorie immens wichtigen *Sylowsätzen* und stellen typische Beispiele für ihre Anwendung vor. Für den Beweis der Sylowsätze nehmen wir uns viel Zeit; hier gehen viele Schlüsse aus der Theorie der Gruppenoperationen ein. ⋇

Mehr zu p-Gruppen

Wir wissen bereits, dass nicht-triviale p-Gruppen nicht-triviale Zentren besitzen. Mit Hilfe dieser Aussage folgt, dass p-Gruppen „viele“ Normalteiler besitzen. Der Beweis dieses Resultats beruht, wie in vielen p-Gruppen-Beweisen, auf Induktion.

Satz 12.1 *Sei G eine p-Gruppe. Dann besitzt G zu jedem Teiler t seiner Ordnung einen Normalteiler der Ordnung t. Dies zeigt insbesondere, dass jede p-Gruppe eine Lagrangegruppe ist.*

Vorbemerkung zum Beweis. Seien G eine endliche Gruppe und $N \trianglelefteq G$ ein Normalteiler von G. Wir betrachten den kanonischen Epimorphismus

$$\varphi : G \to G/N, \qquad g \mapsto gN$$

und eine Untergruppe $U \leq G/N$. Wir schreiben $U = \{g_1N, g_2N, \dots, g_rN\}$ und nehmen an, dass die Nebenklassen g_iN paarweise verschieden sind, also dass $|U| = r$ ist.
Es gilt $\varphi(g) \in U$ genau dann, wenn $gN = g_iN$ für ein $i \in \{1, \dots, r\}$ gilt. Dies ist genau dann der Fall, wenn $g = g_in$ für ein $i \in \{1, \dots, r\}$ und $n \in N$ gilt. Somit ist

$$\varphi^{-1}(U) = g_1N \cup \dots \cup g_rN = g_1N \dot\cup \dots \dot\cup g_rN.$$

Aufgrund der Disjunktheit der Vereinigung folgt $|\varphi^{-1}(U)| = r \cdot |N| = |U| \cdot |N|$.

Beweis. Sei $p \in \mathbb{P}$. Wir weisen per Induktion nach $n \in \mathbb{N}_0$ nach, dass die Behauptung im Satz für alle Gruppen der Ordnung p^n gilt.
Für $n = 0$ ist $G = \{1\}$. In diesem Fall stimmt der Satz offensichtlich. Sei nun die Aussage im Satz bereits für alle Gruppen der Ordnung p^n bewiesen. Dann gilt sie auch für jede Gruppe G der Ordnung p^{n+1}, denn:
Wir betrachten das Zentrum $Z(G)$ von G. Dieses ist wegen 11.22 nicht-trivial, nach Definition abelsch und besitzt somit aufgrund von 8.5 (c) eine Untergruppe N von Ordnung p. Es gilt $N \trianglelefteq G$, denn für alle $g \in G$ und $n \in N$ ist $gng^{-1} = n$ nach Definition des Zentrums. Wir betrachten nun die Faktorgruppe G/N mit Ordnung p^n und den kanonischen Epimorphismus ⁉

$$\varphi : G \to G/N, \qquad g \mapsto gN.$$

Ist U ein Normalteiler von G/N, so ist $\varphi^{-1}(U)$ nach 6.4 (d) ein Normalteiler von G. Die Vorbemerkung zeigt, dass $\varphi^{-1}(U)$ die Ordnung $|N| \cdot |U| = p \cdot |U|$ hat.

G/N hat nach Induktionsvoraussetzung Normalteiler der Ordnungen $p^0, \dots, p^n$. Daher hat G mit obiger Urbild-Schlussweise Normalteiler der Ordnungen $p^1, \dots, p^{n+1}$. Außerdem ist $\{1\}$ ein Normalteiler von G. Damit hat G zu jedem Teiler seiner Ordnung einen Normalteiler dieser Ordnung. ■

Zur Klassifikation der Isomorphietypen von Gruppen der Ordnung p^2 benötigen wir folgendes Hilfsresultat:

Lemma 12.2 *Sei G eine Gruppe. Dann gilt: Ist die Zentrumsfaktorgruppe $G/Z(G)$ zyklisch, so ist G abelsch. In diesem Fall folgt $G = Z(G)$ und somit $G/Z(G) = \{1\}$.*
Man sagt oft kürzer: Die Zentrumsfaktorgruppe ist nie nicht-trivial zyklisch.

Beweis. Seien $g, h \in G$ beliebig. Wir müssen zeigen, dass $gh = hg$ gilt. Hierzu benutzen wir die Nebenklassenzerlegung $G/Z(G)$:
Da $G/Z(G)$ zyklisch ist, existiert ein $x \in G$, so dass $G/Z(G) = \langle xZ(G)\rangle = (xZ(G))^{\mathbb{Z}}$ gilt. Nach 4.4 liegen g und h in Nebenklassen von G nach $Z(G)$. Es existieren also $n, m \in \mathbb{Z}$ und $y, z \in Z(G)$ mit $g = x^n y$ bzw. $h = x^m z$. Da Zentrumselemente mit allen anderen Elementen kommutieren, gilt

$$gh = x^n y \cdot x^m z \overset{y \in Z(G)}{=} x^{n+m} zy = x^{m+n} zy \overset{z \in Z(G)}{=} x^m z \cdot x^n y = hg.$$

Die restlichen Behauptungen folgen direkt aus der Definition des Zentrums: Genau dann gilt $G = Z(G)$, wenn G abelsch ist. ■

Satz 12.3 (Gruppen der Ordnung p^2) *Seien p eine Primzahl und G eine Gruppe der Ordnung p^2. Dann ist G abelsch. Mit dem Struktursatz folgt $G \cong C_{p^2}$ bzw. $G \cong C_p \times C_p$.*

Beweis. Wir betrachten das Zentrum von G. Da G eine nicht-triviale p-Gruppe ist, gilt $|Z(G)| = p$ oder $|Z(G)| = p^2$. Der Fall $|Z(G)| = p$ ist aber nach 12.2 und 7.5 unmöglich. Somit ist $|Z(G)| = p^2$, also $G = Z(G)$. Dies liefert die Kommutativität von G. ■

Die Sätze von Sylow

Die Sylow-Sätze sind, neben Lagrange, die wahrscheinlich wichtigsten Sätze in der Theorie der endlichen Gruppen. Sie stellen eine teilweise Umkehrung des Satzes von Lagrange dar, garantieren also die Existenz gewisser Untergruppen.

Satz 12.4 (Sylow; Existenz) *Seien G eine endliche Gruppe, $p \in \mathbb{P}$ eine Primzahl und $i \in \mathbb{N}_0$. Dann gilt: Teilt p^i die Gruppenordnung $|G|$, so besitzt G eine Untergruppe der Ordnung p^i.*

Beweis. Wir beweisen den Satz per Induktion nach der Gruppenordnung $|G|$.
Für $|G| = 1$ ist die Aussage im Satz offenbar richtig, denn hier ist nur der Fall $i = 0$, d. h. $p^i = 1$ zu betrachten. Sei der Satz nun bereits für alle Gruppen mit Ordnung höchstens n bewiesen. Wir zeigen, dass er dann auch für jede Gruppe G der Ordnung $n + 1$ gilt:

Seien $p \in \mathbb{P}$ eine beliebige Primzahl und p^m mit $m \in \mathbb{N}$ (der Fall $m = 0$ ist trivial) die maximale p-Potenz, die $|G| = n + 1$ teilt, d. h. es gelte $p^m \mid n + 1$, aber $p^{m+1} \nmid n + 1$. Wir

zeigen, dass G eine Untergruppe der Ordnung p^m besitzt. Dann folgt wegen 12.1, dass G auch Untergruppen der Ordnungen p^i mit $i \in \{0, \dots, m\}$ besitzt. (Sind diese normal in G?) Damit ist der Satz bewiesen.
Wir zeigen die Existenz einer Untergruppe der Ordnung p^m mit Hilfe der Klassengleichung und benutzen die Bezeichnungen aus 11.19. Da die K_i Bahnen von G sind, existieren nach Bahnlängenformel Untergruppen $U_i \leq G$ mit $|K_i| = \frac{|G|}{|U_i|}$. Wegen $|K_i| \geq 2$ gilt $U_i < G$. Wir erhalten

$$|G| = |Z(G)| + \sum_{i=1}^{r} \frac{|G|}{|U_i|}.$$

Angenommen, G besäße keine Untergruppe der Ordnung p^m. Dann ist p^m kein Teiler einer der Gruppen U_i, denn per Induktion hätte sonst eines der U_i und damit auch G eine Untergruppe der Ordnung p^m. Daher teilt p jeden der Quotienten $\frac{|G|}{|U_i|}$. Da p auch $|G|$ teilt, folgt, dass p auch $|Z(G)|$ teilt. Nun schließen wir wie im Beweis zu 12.1:
G hat einen Normalteiler $N \subseteq Z(G)$ der Ordnung p. In der Faktorgruppe G/N existiert nach Induktionsvoraussetzung eine Untergruppe der Ordnung p^{m-1}. Ihr Urbild unter dem kanonischen Epimorphismus $G \to G/N$ ist dann eine Untergruppe von G der Ordnung $p \cdot p^{m-1} = p^m$. Dieser Widerspruch beweist den Satz. ■

Bemerkung 12.5 (a) Die Existenzaussage der Sätze von Sylow sagt, dass endliche Gruppen bezüglich ihrer p-Anteile lagrangesch sind: Zu jedem *Primpotenzteiler* ihrer Ordnung besitzen sie eine Untergruppe dieser Ordnung.

(b) Wegen 12.1 hat es in obigem Beweis ausgereicht, die Existenz von Untergruppen zu *maximalen* Primpotenzteilern zu zeigen. Diese für die Sylowtheorie sehr wichtigen Untergruppen nennt man auch die **Sylowuntergruppen von G**, vgl. 12.7.

(c) Obiger Satz gilt auch im Falle, dass die Primzahl p die Ordnung von G *nicht* teilt. Hier reduziert sich seine Aussage aber auf die Trivialität, dass $\{1\}$ eine Untergruppe von G ist. ⁜

Aus dem Existenzsatz von Sylow folgt direkt der nachstehende Satz von Cauchy. Die Bedeutung des Satzes von Cauchy für die Gruppentheorie liegt darin, dass dieser Satz ca. 30 Jahre *vor* den Sylowsätzen bewiesen wurde.

Korollar 12.6 (Cauchy) *Seien G eine endliche Gruppe und $p \in \mathbb{P}$ eine Primzahl, die die Ordnung von G teilt. Dann besitzt G eine Untergruppe von Ordnung p und, da diese nach 7.5 zyklisch ist, auch ein Element der Ordnung p.*

Definition 12.7 (Sylowgruppe) *Seien G eine endliche Gruppe und p eine Primzahl. Ist p^m mit $m \in \mathbb{N}_0$ die maximale p-Potenz, die $|G|$ teilt, so nennen wir jede Untergruppe von G mit Ordnung p^m eine **p-Sylowgruppe** oder **Sylow-p-Gruppe von G**.*
Nach 12.4 besitzt G zu jedem $p \in \mathbb{P}$ eine p-Sylowgruppe.

Beispiel 12.8 A_4 besitzt nach 9.11 acht Elemente der Ordnung drei und daher $8/\varphi(3) = 8/2 = 4$ Untergruppen der Ordnung 3. Wegen $|A_4| = 2^2 \cdot 3$ haben 3-Sylowgruppen in A_4 die Ordnung drei. A_4 besitzt also vier Sylow-3-Gruppen. ⁜

Bemerkung 12.9 (a) Sind P und Q Sylowgruppen von G zu *verschiedenen Primzahlen*, so gilt nach Lagrange $P \cap Q = \{1\}$.

(b) Ist P eine p-Sylowgruppe von G, so ist auch gPg^{-1} eine p-Sylowgruppe von G; denn da Konjugation ein Automorphismus ist, haben P und gPg^{-1} dieselbe Ordnung und die Sylowgruppen-Eigenschaft ist über die Gruppenordnung definiert.

Konjugation bildet mithin Sylowgruppen auf Sylowgruppen *zur selben Primzahl* ab. ⋇

Um die restlichen Sylow-Sätze zu zeigen, benötigen wir das folgende Lemma:

Lemma 12.10 *Seien G eine endliche Gruppe, $p \in \mathbb{P}$ eine Primzahl und P eine p-Sylowgruppe von G. Dann gilt: Ist U eine Untergruppe von G von p-Potenzordnung, so gilt $U \leq gPg^{-1}$ für ein $g \in G$.*
Man kann die p-Sylowgruppe P also so konjugieren, dass sie die p-Untergruppe U enthält.

Beweis. Wir betrachten die Operation von U auf den Nebenklassen $M := G/P$ von P in G, die durch

$$u \bullet gP := ugP \qquad \text{für beliebige } u \in U \text{ und } g \in G$$

gegeben ist. Da U eine p-Gruppe ist, treten nach Bahnlängenformel nur p-Potenz-Bahnlängen auf. Da aber $|M| = |G|/|P|$ kein Vielfaches von p ist, muss es eine Bahn der Länge $p^0 = 1$ geben. Es gibt also $g \in G$ mit $u \bullet gP = gP$ für alle $u \in U$. Für alle $u \in U$ ist also ⁉

$$u \bullet gP = gP \iff g^{-1}u \bullet gP = P \iff g^{-1}ugP = P \iff g^{-1}ug \in P \iff u \in gPg^{-1}.$$

Dies zeigt $U \leq gPg^{-1}$. ■

Satz 12.11 (Sylow; „Eindeutigkeit“) *Für jede endliche Gruppe G und jede Primzahl $p \in \mathbb{P}$ gelten:*

(a) *Jede p-Untergruppe von G ist in einer p-Sylowgruppe von G enthalten.*

(b) *Je zwei p-Sylowgruppen von G sind konjugiert zueinander.*

Beweis.

zu (a) Seien U eine p-Untergruppe und P eine p-Sylowgruppe von G. Nach 12.10 existiert dann ein $g \in G$ mit $U \leq gPg^{-1}$. Mit 12.9 (b) folgt die Behauptung.

zu (b) Seien P, Q zwei p-Sylowgruppen. Dann existiert $g \in G$ mit $Q \leq gPg^{-1}$. Mit 12.9 (b) folgt $|Q| = |gPg^{-1}|$, also $Q = gPg^{-1}$. Dies zeigt (b). ■

Bemerkung 12.12 (a) Teil (b) des obigen Satzes liefert einen Ersatz für die fehlende Eindeutigkeit von p-Sylowgruppen: Diese sind eindeutig *bis auf Konjugation*.

Da Konjugation ein Automorphismus ist, folgt insbesondere, dass alle Sylowgruppen zur selben Primzahl isomorph zueinander sind.

(b) Seien G eine endliche Gruppe M die Menge aller p-Sylowgruppen von G. Bereits aus 12.9 (b) folgt, dass durch

$$g \bullet P := gPg^{-1} \qquad \text{für beliebige } g \in G \text{ und } P \in M$$

eine Operation von G auf M gegeben ist. Mit 12.11 (b) folgt nun, dass die Operation sogar *transitiv* ist. Diese Feststellung ist die Basis für viele Beweistechniken in der Theorie der endlichen Gruppen.

Der Stabilisator einer Sylowgruppe P bezüglich der obigen Operation ist die Gruppe

$$N_G(P) := \{g \in G \mid gPg^{-1} = P\},$$

die man auch den **Normalisator von P in G** nennt. Offenbar gilt $P \leq N_G(P)$ und daher auch $P \trianglelefteq N_G(P)$. ⁂

Knobelfrage. Was ist der Unterschied zwischen dem Zentralisator $C_G(P)$ und dem Normalisator $N_G(P)$?

Eine wichtige Folgerung aus dem Eindeutigkeitsresultat der Sylowsätze ist

Korollar 12.13 *Seien G eine endliche Gruppe, $p \in \mathbb{P}$ eine Primzahl und P eine p-Sylowgruppe von G. Dann gilt: Genau dann ist P normal in G, wenn P die einzige p-Sylowgruppe von G ist.*

Beweis. Seien M die Menge der p-Sylowgruppen von G und $N := \{gPg^{-1} \mid g \in G\}$ die Menge aller zu P konjugierten Untergruppen von G. Wegen 12.11 (b) gilt $M = N$. Hieraus folgt die Behauptung wegen

$$P \trianglelefteq G \iff |N| = 1 \overset{M=N}{\iff} |M| = 1 \overset{P \in M}{\iff} P \text{ ist einzige } p\text{-Sylowgruppe von } G. \qquad \blacksquare$$

Der nächste Satz liefert Beschränkungen an die Anzahl der p-Sylowgruppen einer endlichen Gruppe:

Satz 12.14 (Sylow; Anzahlbeschränkungen) *Für eine endliche Gruppe G und eine Primzahl $p \in \mathbb{P}$ bezeichnen wir mit n_p die Anzahl der p-Sylowgruppen von G. Dann gelten:*

(a) *Es ist $n_p = \frac{|G|}{|N_G(P)|}$.*

(b) *n_p teilt den Index $[G : P]$, d. h. gilt $|G| = p^r \cdot s$ mit $p \nmid s$, so ist $n_p \mid s$.*

(c) *Es gilt $n_p \bmod p = 1$, d. h. es gilt $n_p = k \cdot p + 1$ mit einem $k \in \mathbb{N}_0$.*

Beweis. (a) folgt direkt aus der Transitivität der Operation in 12.12 (b) und der Bahnlängenformel, denn $N_G(P)$ ist der Stabilisator von P.

zu (b) Da $P \leq N_G(P)$ gilt, folgt mit (a)

$$n_p = \frac{|G|}{|N_G(P)|} \;\Big|\; \frac{|G|}{|N_G(P)|} \cdot \frac{|N_G(P)|}{|P|} = \frac{|G|}{|P|} = [G : P].$$

zu (c) Seien P eine p-Sylowgruppe von G und M die Menge aller p-Sylowgruppen von G. Dann operiert P per Konjugation auf M durch die Festsetzung

$$p \bullet Q := pQp^{-1} \qquad \text{für beliebige } p \in P \text{ und } Q \in M.$$

Wegen $pPp^{-1} = P$ für alle $p \in P$ besitzt diese Operation eine Bahn der Länge Eins. Wir zeigen, dass keine weitere Bahn der Länge Eins existiert. Da P eine p-Gruppe ist, haben die übrigen Bahnen nach Bahnlängenformel dann eine Länge, die durch p teilbar ist. Die Bahnengleichung liefert dann

$$|M| = 1 + \sum \text{gewisse Vielfache von } p = 1 + kp,$$

was die Behauptung zeigt.

Sei also $Q \in M$ mit $Q \neq P$. Angenommen, es sei $|P \bullet Q| = 1$. Wir betrachten die Untergruppe $U := \langle P, Q\rangle$ von G. Aufgrund unserer Annahme ist $pQp^{-1} = Q$ für alle $p \in P$. Dies zeigt, dass $Q \trianglelefteq U$ gilt, denn jedes Element aus U lässt sich als Produkt von Elementen aus P und Q schreiben. Nach 12.13 ist Q dann die einzige p-Sylowgruppe von U. Wegen $|P| = |Q|$ folgt hieraus $P = Q$ im Widerspruch zu unserer Annahme. ■

Beispiele zu Sylow-Beweistechniken

Staatsexamensaufgabe (F2017T2A1; Typ: Elemente zählen) *Wie viele Elemente der Ordnung* 11 *gibt es in einer einfachen Gruppe G der Ordnung* 660*?*

Es ist $660 = 2^2 \cdot 3 \cdot 5 \cdot 11$. Wir bezeichnen mit n_{11} die Anzahl der 11-Sylowgruppen von G. Nach 12.14 gilt

$$n_{11} \in \underbrace{\{1, 2, 3, 4, 5, 6, 10, 12, 15, 20, 30, 60\}}_{\text{Teiler von } |G|/11 = 60} \cap \underbrace{\{1, 12, 23, 34, 45, 56, 67, \cdots\}}_{\text{Elemente der Form } 1 + k \cdot 11} = \{1, 12\}.$$

Der Fall $n_{11} = 1$ tritt nach 12.13 nicht auf, da G einfach ist. Somit besitzt G genau $n_{11} = 12$ Untergruppen der Ordnung 11. Diese sind zyklisch und werden von jeweils $\varphi(11) = 10$ Elementen der Ordnung 11 erzeugt. Da ein Erzeuger einer solchen Untergruppe nur in genau einer solchen Untergruppe liegt, folgt, dass G genau $12 \cdot 10 = 120$ Elemente der Ordnung 11 enthält. ⁜

Staatsexamensaufgabe (F2018T3A3 (b) (i); Typ: Elemente zählen) *Es sei G eine Gruppe der Ordnung* 12*. Für $p \in \mathbb{P}$ sei mit n_p die Anzahl der p-Sylowgruppen von G bezeichnet. Zeigen Sie, dass nicht gleichzeitig $n_2 = 3$ und $n_3 = 4$ gelten kann.*

Angenommen, es wäre $n_2 = 3$ und $n_3 = 4$.
3-Sylowgruppen von G besitzen die Ordnung 3, sind zyklisch und haben $\varphi(3) = 2$ Erzeuger. Jedes Element der Ordnung 3 von G liegt in genau einer 3-Sylowgruppe von G und erzeugt diese. Daher besitzt G genau $n_3 \cdot \varphi(3) = 4 \cdot 2 = 8$ Elemente der Ordnung 3.

Seien P und Q zwei 2-Sylowgruppen von G. Es gilt $|P| = |Q| = 4$. In der Vereinigung $|P \cup Q|$ liegen mindestens vier Elemente der Ordnungen 2 oder 4; P steuert drei Elemente bei und Q mindestens eines, da $P \neq Q$ gilt.
Insgesamt folgt der Widerspruch

$$|G| = 12 \geq \underbrace{1}_{\text{Neutrales}} + \underbrace{8}_{\text{Elemente der Ordnung 3}} + \underbrace{4}_{\text{Elemente mit Ordnung 2 oder 4 aus } P \cup Q} = 13. \qquad ⁂$$

Staatsexamensaufgabe (H2016T3A3; Typ: Operation) *Zeigen Sie, dass eine Gruppe G der Ordnung $|G| = 392 = 2^3 \cdot 7^2$ nicht einfach ist.*

Für eine Primzahl p bezeichnen wir mit n_p die Anzahl der p-Sylowgruppen von G. Es gilt nach 12.14

$$n_7 \in \underbrace{\{1,2,4,8\}}_{\text{Teiler von } |G|/7^2 = 8} \cap \underbrace{\{1,8,\ldots\}}_{\text{Elemente der Form } 1+7k} = \{1,8\}.$$

Im Fall $n_7 = 1$ ist G nach 12.13 nicht einfach. Wir betrachten daher den Fall $n_7 = 8$ genauer. Hier operiert G nach 12.12 per Konjugation transitiv auf der Menge M der 7-Sylowgruppen von G. Sei

$$\varphi : G \to \mathrm{Sym}(M) \cong S_8$$

der Operationshomomorphismus. Da $|G| \nmid |S_8|$ ist (in der PFZ von 8! tritt der Primfaktor 7 nur einmal auf), ist $\ker \varphi = \{1\}$ nicht möglich. Aber auch der Fall $\ker \varphi = G$ tritt nicht auf, da eine transitive Operation auf acht Elementen vorliegt. Somit ist $\ker \varphi$ ein echter, nicht-trivialer Normalteiler von G, was die Nicht-Einfachheit von G zeigt. ⁂ ⁉ ⁉

13. Konstruktion neuer Untergruppen

Worum geht es? Wir stellen eine Methode vor, um aus bekannten Untergruppen einer Gruppe neue Untergruppen zu erzeugen. Dies führt insbesondere auf den *Satz vom internen direkten Produkt*, der in vielen Aufgaben zur Sylowtheorie eine Rolle spielt. ⋇

Wir haben in Vorlesung 2 den Begriff des Gruppenerzeugnisses kennengelernt. Mit seiner Hilfe können wir aus bereits bekannten Untergruppen einer Gruppe neue Untergruppen erzeugen: Gilt beispielsweise $U, V \leq G$ für eine Gruppe G, so ist auch $\langle U, V\rangle$ eine Untergruppe von G.
Problematisch an dieser Untergruppenkonstruktion ist, dass wir keine Kontrolle über die Größe der entstehenden Untergruppe haben:

Beispiel 13.1 (a) Die alternierende Gruppe A_4 besitzt nach Sylow Untergruppen der Ordnungen 2 und 3, jedoch keine der Ordnung $2 \cdot 3 = 6$. Es ist $\langle U, V\rangle = A_4$ für alle Untergruppen $U, V \leq A_4$ mit $|U| = 2$ und $|V| = 3$.

(b) Betrachten wir in S_{10} Untergruppen U, V der Ordnung 4, so kann man nachrechnen, dass für die Ordnung von $\langle U, V\rangle$ folgende Möglichkeiten existieren:

$$|\langle U, V\rangle| \in \{4, 8, 16, 24, 32, 48, 64, 72, 96, 128, 144, 192, 256, 288, 336, 384, 672, 768, 1152, 1440, 2304, 2880, 40320, 80640\}.$$

⋇

Wir stellen nun eine Methode zur Untergruppenerzeugung vor, die mehr Kontrolle über die Größe der sich ergebenden Untergruppe zulässt. Ihr Nachteil ist, dass sie nur unter gewissen Bedingungen an die Ausgangsgruppen U und V funktioniert. Sie beruht auf der Idee der Fortsetzung von Verknüpfungen auf die Potenzmenge aus Vorlesung 4.

Komplexprodukte

Definition 13.2 *Seien G eine Gruppe und U, V Untergruppen von G. Dann nennen wir die Menge*

$$UV = \{uv \mid u \in U, v \in V\}$$

das ***Komplexprodukt von U und V***.

Das folgende Resultat zeigt, dass wir die Größe von Komplexprodukten exakt bestimmen können:

Satz 13.3 *Seien U, V endliche Untergruppen einer Gruppe G. Dann gilt $|UV| = \frac{|U|\cdot|V|}{|U\cap V|}$.*

Beweis. Wir zählen Elemente im Komplexprodukt UV. Hierzu schauen wir zunächst, auf wie viele Weisen sich ein Element aus UV als Produkt eines Elements aus U mit einem aus V schreiben lässt. Seien hierzu $u, u' \in U$ und $v, v' \in V$ mit $uv = u'v'$. Es gilt

$$uv = u'v' \iff u^{-1}u' = v(v')^{-1} =: c \in U \cap V.$$

Somit ist $uv = u'v'$ genau dann, wenn $u' = uc$ und $v' = c^{-1}v$ mit einem beliebigen $c \in U \cap V$ gilt. Da die Produkte uc bzw. $c^{-1}v$ paarweise verschieden sind, gibt genau $|U \cap V|$ viele verschiedene Möglichkeiten, ein Element aus UV als Produkt eines Elements aus U mit einem aus V zu schreiben. Es folgt die Behauptung

$$|UV| = \frac{\overbrace{|U| \cdot |V|}^{\text{Anzahl aller möglichen Produkte in } UV}}{\underbrace{|U \cap V|}_{\text{Anzahl verschiedener Schreibweisen pro Element aus } UV}}.$$

■

Bemerkung 13.4 Komplexprodukte sind im Allgemeinen keine Untergruppen. Betrachten wir beispielsweise die Untergruppen $U := \langle (1\ 2)(3\ 4) \rangle$ und $V := \langle (1\ 2\ 3) \rangle$ von A_4, so gilt $|U \cap V| = 1$ und daher $|UV| = 6$. Allerdings besitzt A_4 keine Untergruppe der Ordnung 6. ※

Der folgende Satz charakterisiert, wann Komplexprodukte Untergruppen sind:

Satz 13.5 *Seien G eine Gruppe und U, V Untergruppen von G. Dann sind äquivalent:*

(a) *UV ist eine Untergruppe von G.*

(b) *Es gilt $UV = VU$.*

Beweisskizze.

(a)$\Longrightarrow$(b) Wegen $UV \leq G$ liegen alle Produkte der Form $v^{-1}u^{-1} = (uv)^{-1}$ mit $u \in U$ und $v \in V$ in UV. Somit ist $V^{-1}U^{-1} = UV$. Weil U und V Gruppen sind, folgt $U^{-1} = U$ bzw. $V^{-1} = V$. Wir erhalten somit $VU = UV$.

(b)$\Longrightarrow$(a) Wir benutzen das Untergruppenkriterium. Seien $uv, u'v' \in UV$ beliebig. Dann gilt

$$uv \cdot u'v' = u \cdot vu' \cdot v' \overset{UV=VU}{=} u \cdot \tilde{u}\tilde{v} \cdot v' = u\tilde{u} \cdot \tilde{v}v' \in UV.$$

Die Abgeschlossenheit bezüglich Invertierung zeigt man ähnlich. ■

Das Kriterium in 13.5 (b) ist insbesondere erfüllt, wenn U oder V Normalteiler in G sind:

Korollar 13.6 *Seien G eine Gruppe und U, V Untergruppen von G.*

(a) *Sind U **oder** V normal in G, so ist UV eine Untergruppe von G.*

(b) *Sind U **und** V normal in G, so ist UV sogar ein Normalteiler von G.*

Beweis.

zu (a) Wir nehmen $U \trianglelefteq G$ an. Der Beweis funktioniert im Fall $V \trianglelefteq G$ ähnlich. Dann gilt:

$$UV = \bigcup_{v \in V} Uv \overset{Uv=vU \text{ nach } 5.3 \text{ (a)}}{=} \bigcup_{v \in V} vU = VU.$$

Nach 13.5 ist daher UV eine Untergruppe von G.

zu (b) Wegen (a) ist klar, dass UV eine Untergruppe von G ist. Zum Nachweis der Normalität sei $g \in G$ beliebig. Dann gilt für alle $u \in U$ und $v \in V$

$$g \cdot uv \cdot g^{-1} = gug^{-1} \cdot gvg^{-1} \overset{U,V \text{ normal}}{=} u' \cdot v' \in UV.$$

Damit ist $UV \trianglelefteq G$. ■

Tatsächlich ist die Gruppenkonstruktion aus 13.5 keine neue Methode zur Untergruppenkonstruktion, sondern stimmt mit dem am Anfang der Vorlesung betrachteten Erzeugnis $\langle U, V \rangle$ überein. Durch den Umweg über das Komplexprodukt erhalten wir jedoch eine andere Sichtweise auf das Erzeugnis $\langle U, V \rangle$ und können seine Ordnung bestimmen.

Satz 13.7 *Seien G eine Gruppe und U, V Untergruppen von G, so dass UV selbst eine Untergruppe von G ist. Dann gilt $UV = \langle U, V \rangle$.*

Beweis. Nach 2.13 liegt jedes der Produkte uv mit $u \in U$ und $v \in V$ auch in $\langle U, V \rangle$. Dies zeigt $UV \subseteq \langle U, V \rangle$.
UV enthält U und V als Teilmengen und ist eine Untergruppe von G. Weil $\langle U, V \rangle$ die (bezüglich Mengeninklusion) kleinste Untergruppe von G ist, die U und V enthält, folgt $\langle U, V \rangle \subseteq UV$ und somit die zu zeigende Gleichheit. ■

Ist UV eine Gruppe, so ist es im Allgemeinen schwierig, Aussagen über den Isomorphietyp von UV zu treffen. Dies ändert sich, wenn $U \cap V = \{1\}$ gilt. Wir untersuchen diesen Fall im nächsten Abschnitt und der nächsten Vorlesung genauer.
Die eher speziell anmutende Situation $U \cap V = \{1\}$ tritt in Aufgaben häufig auf, beispielsweise wenn U und V Sylowgruppen zu verschiedenen Primzahlen sind.

Das interne direkte Produkt

Wir untersuchen den Fall, in dem U und V beide Normalteiler von G sind und zudem $U \cap V = \{1\}$ gilt. Dann können wir den Isomorphietyp von UV explizit angeben:

Satz 13.8 (internes direktes Produkt) *Seien G eine Gruppe und U, V Normalteiler von G mit $U \cap V = \{1\}$. Dann ist die Abbildung $U \times V \to UV$ mit $(u, v) \mapsto uv$ ein Isomorphismus. Der Normalteiler $UV \trianglelefteq G$ ist also isomorph zum direkten Produkt $U \times V$.*
*Man nennt UV in diesem Fall auch das **interne direkte Produkt von U und V**. Der Begriff „intern“ kommt daher, dass der Isomorphietyp „direktes Produkt“ nicht durch das kartesische Produkt $U \times V$ dargestellt wird, sondern als Teilmenge der bereits bekannten Menge G auftritt.*

Beweis. Wir zeigen, dass die Abbildung

$$\varphi : U \times V \to UV, \qquad (u,v) \mapsto uv$$

ein Isomorphismus ist.
Zum Nachweis der Homomorphie von φ benötigen wir als Hilfsresultat, dass $uv = vu$ für beliebige $u \in U$ und $v \in V$ gilt. (Beachten Sie, dass diese Vertauschbarkeit innerhalb von U bzw. V nicht gilt; im Allgemeinen ist $uu' \neq u'u$ bzw. $vv' \neq v'v$.)
Seien also $u \in U$ und $v \in V$ beliebig. Es gilt $uv = vu \iff uvu^{-1}v^{-1} = 1$. Die rechte Seite der Äquivalenz ist korrekt, denn es gelten

$$u \cdot \underbrace{vu^{-1}v^{-1}}_{\in U,\ \text{da } U \trianglelefteq G} \in U \qquad \text{sowie} \qquad \underbrace{uvu^{-1}}_{\in V,\ \text{da } V \trianglelefteq G} \cdot v^{-1} \in V.$$

Es folgt $uvu^{-1}v^{-1} \in U \cap V = \{1\}$ und somit $uvu^{-1}v^{-1} = 1$.
Wir zeigen nun die Homomorphie von φ: Für beliebige $u, u' \in U$ und $v, v' \in V$ gilt

$$\varphi(\,(u,v)\cdot(u',v')\,) = \varphi(\,(uu',vv')\,) = u \cdot u'v \cdot v' \overset{\text{s.o.}}{=} u \cdot vu' \cdot v' = \varphi(\,(u,v)\,) \cdot \varphi(\,(u',v')\,).$$

Die Surjektivität von φ ist klar. Zum Nachweis der Injektivität von φ bestimmen wir den Kern von φ. Sei hierzu $(u,v) \in \ker\varphi$. Dann gilt

$$\varphi(\,(u,v)\,) = uv = 1, \qquad \text{also} \qquad u = v^{-1} \in U \cap V = \{1\}.$$

Dies zeigt $u = 1 = v$ und somit $\ker\varphi = \{(1,1)\}$. Also ist φ auch injektiv. ■

Wir stellen einige typische Beispiele vor, in denen der Satz über interne direkte Produkte eine Rolle spielt.

Beispiel Jede Gruppe G der Ordnung 15 ist zyklisch.

Für $p \in \mathbb{P}$ sei mit n_p die Anzahl der p-Sylowgruppen von G bezeichnet. Man sieht wie in der letzten Vorlesung, dass $n_3 = n_5 = 1$ gilt. Seien P_3 *die* 3-Sylowgruppe und P_5 *die* 5-Sylowgruppe von G. Wegen $|P_3|, |P_5| \in \mathbb{P}$ gilt $P_3 \cong C_3$ und $P_5 \cong C_5$. Nach 12.13 sind $P_3, P_5 \trianglelefteq G$, Lagrange zeigt $P_3 \cap P_5 = \{1\}$.
Aufgrund von 13.3 folgt $|P_3P_5| = 3 \cdot 5 = 15$ und somit $P_3P_5 = G$. Der Satz über das interne direkte Produkt liefert $P_3P_5 \cong P_3 \times P_5$. Insgesamt haben wir daher

$$G = P_3P_5 \cong P_3 \times P_5 \cong C_3 \times C_5 \overset{8.4}{\cong} C_{15}.$$ ※

Staatsexamensaufgabe (H2014T3A1) *Es sei G eine Gruppe mit* 2014 *Elementen. Zeigen Sie, dass G einen zyklischen Normalteiler der Ordnung* $1007 = 19 \cdot 53$ *enthält.*

Wieder bezeichne n_p die Anzahl der p-Sylowgruppen von G. Direkt aus den Sylowsätzen folgt $n_{19} = 1 = n_{53}$. Nun schließt man wie im obigen Beispiel:
P_{19} und P_{53} sind beide normal in G und schneiden sich in der trivialen Gruppe. Die Untergruppe $U := P_{19}P_{53}$ hat daher Ordnung $19 \cdot 53 = 1007$ und ist wegen 13.6 ein

Normalteiler von G. Da P_{19} und P_{53} beide Primzahlordnung haben, folgt $P_{19} \cong C_{19}$ bzw. $P_{53} \cong C_{53}$. Mit dem Satz über das interne direkte Produkt ergibt sich

$$U \cong C_{19} \times C_{53} \overset{8.4}{\cong} C_{1007}.$$

Mit U ist daher ein Normalteiler gefunden, der der Aufgabenstellung genügt. (Gibt es weitere solche Normalteiler?) ⁂ ⁉

Staatsexamensaufgabe (H2010T2A1) *Zeigen Sie, dass es bis auf Isomorphie genau zwei Gruppen der Ordnung 99 gibt.*

Die Lösung der Aufgabe läuft im Wesentlichen wie in den beiden obigen Beispielen ab: Es gilt $99 = 3^2 \cdot 11$, und sowohl 3- als auch 11-Sylowgruppe sind normal. Wieder folgt $G \cong P_3 \times P_{11}$.
Es gilt $|P_{11}| = 11$ und somit $P_{11} \cong C_{11}$. Wegen $|P_3| = 3^2$ folgt aus 12.3, dass $P_3 \cong C_9$ oder $P_3 \cong C_3 \times C_3$ gilt. Wir erhalten daher

$$G \cong C_9 \times C_{11} \cong C_{99} \qquad \text{oder} \qquad G \cong C_3 \times C_3 \times C_{11}.$$

Nach Struktursatz werden hierdurch tatsächlich zwei verschiedene Isomorphietypen für G beschrieben. ⁂

Beispiel Jede Gruppe G der Ordnung 6 ist isomorph zu C_6 oder S_3.

Wir benutzen die Bezeichnung n_p wie in den vorherigen Beispielen. Die Sylowsätze zeigen $n_3 = 1$ und $n_2 \in \{1, 3\}$.
Im Fall $n_2 = 1$ schließt man wie oben und erhält $G \cong C_6$ aus dem Satz über das interne direkte Produkt.
Im Fall $n_2 = 3$ operiert G transitiv auf den drei Sylow-2-Untergruppen P, P', P'' per Konjugation. Sei $\varphi : G \to S_3$ der Operationshomomorphismus (Wir haben hier die Isomorphie $\mathrm{Sym}(\{P, P', P''\}) \cong S_3$ ausgenutzt.). Der Stabilisator von P hat nach 12.14 (a) Ordnung $\frac{6}{3} = 2$, stimmt also mit P überein. Nach 11.13 (c) gilt $\ker\varphi \leq P$. Der Fall $\ker\varphi = P$ ist nicht möglich, denn wegen $n_2 = 3$ ist P nicht normal in G. Daher ist $\ker\varphi$ eine echte Untergruppe von $P \cong C_2$. Somit gilt $\ker\varphi = \{1\}$. Wegen $|G| = |S_3|$ folgt, dass φ ein Isomorphismus ist. Wir sehen also, dass $G \cong S_3$ gilt. ⁂ ⁉

Interne direkte Produkte mit mehreren Faktoren

In 13.8 und den obigen Beispielen traten nur interne direkte Produkte mit zwei Faktoren auf. Im nachstehenden Resultat betrachten wir nun interne direkte Produkte mit mehr Faktoren. Sein Beweis beruht auf mehrfachem Anwenden von 13.8.

Korollar 13.9 (internes direktes Produkt mit mehreren Faktoren) *Seien G eine endliche Gruppe, $k \in \mathbb{N}$ und $N_1, \ldots, N_k$ Normalteiler von G. Die Ordnungen der N_i seien paarweise teilerfremd, d. h. es gelte $\mathrm{ggT}(|N_i|, |N_j|) = 1$ für alle $1 \leq i, j \leq n$ mit $i \neq j$.*
Dann ist das Komplexprodukt $N_1 N_2 \cdots N_k$ ein Normalteiler von G, und es gilt

$$N_1 N_2 \cdots N_k \cong N_1 \times N_2 \times \cdots \times N_k.$$

Beweis. Wir zeigen die Behauptung per Induktion nach k.
Der Fall $k = 1$ ist klar. Sei die Aussage für $k \in \mathbb{N}$ und alle in Frage kommenden Gruppen und Normalteiler N_i bereits gezeigt. Wir beweisen, dass sie auch für $k+1$ gilt:

Seien G eine endliche Gruppe und $N_1, \dots, N_{k+1}$ Normalteiler von G mit paarweise teilerfremder Ordnung. Wir setzen $N := N_1 N_2 \cdots N_k$. Die Induktionsvoraussetzung zeigt, dass

$$N \trianglelefteq G \qquad \text{und} \qquad N \cong N_1 \times N_2 \times \cdots \times N_k$$

gelten. Hieraus folgt

$$|N| = |N_1 \times N_2 \times \cdots \times N_k| = |N_1| \cdot |N_2| \cdots |N_k| = \prod_{i=1}^{k} |N_i|.$$

Die paarweise Teilerfremdheit der Ordnungen der N_i zeigt, dass $\mathrm{ggT}(|N|, |N_{k+1}|) = 1$ ist. (Warum?) Mit Lagrange ergibt sich, dass $N \cap N_{k+1} = \{1\}$ ist, denn die Ordnung der Gruppe $N \cap N_{k+1}$ ist ein gemeinsamer Teiler der teilerfremden Zahlen $|N|$ und $|N_{k+1}|$. Damit sind alle Voraussetzungen des Satzes über das interne direkte Produkt erfüllt. 13.8 liefert nun, dass $NN_{k+1} = N_1 N_2 \cdots N_{k+1}$ ein Normalteiler von G ist und dass

$$N_1 N_2 \cdots N_{k+1} = NN_{k+1} \cong N \times N_{k+1} \cong (N_1 \times \cdots \times N_k) \times N_{k+1} \cong N_1 \times \cdots \times N_{k+1}$$

gilt. ■

Bemerkung 13.10 (a) Um im obigen Beweis den Satz über das interne direkte Produkt anwenden zu können, müssen wir sicherstellen, dass sich die Gruppen N und N_{k+1} trivial schneiden. Dies wird durch die Voraussetzung der paarweisen Teilerfremdheit der Ordnungen der N_i garantiert. Damit diese Begrifflichkeiten definiert sind, setzen wir G als *endliche* Gruppe voraus.

(b) Eine direkte Verallgemeinerung der Schnittbedingung aus 13.8 wäre beispielsweise

> *Die N_i mögen sich paarweise trivial schneiden, d. h. es gelte $N_i \cap N_j = \{1\}$ für alle $1 \leq i, j \leq n$ mit $i \neq j$.*

Diese Bedingung ist allerdings zu schwach. Können Sie ein Beispiel für eine Gruppe G mit sich paarweise trivial schneidenden Normalteilern N_1, N_2, N_3 angeben, so dass aber $N_1 N_2 \cap N_3 \neq \{1\}$ und $G \ncong N_1 \times N_2 \times N_3$ ist? ⁂

Beispiel Jede Gruppe G der Ordnung $1001 = 7 \cdot 11 \cdot 13$ ist zyklisch.

Mit Hilfe der Sylowsätze folgt, dass G zu jedem $s \in \{7, 11, 13\}$ genau eine s-Sylowgruppe P_s enthält. Die P_s sind daher Normalteiler von G. Es gilt $|P_s| = s \in \mathbb{P}$. Damit sind die Ordnungen der Gruppen P_s paarweise teilerfremd, ferner ist $P_s \cong C_s$. Aus 13.9 folgt somit

$$P_7 P_{11} P_{13} \cong C_7 \times C_{11} \times C_{13} \cong C_{1001}.$$

Da $|G| = 1001$ ist, stimmt der Normalteiler $P_7 P_{11} P_{13}$ mit G überein. Wir erhalten also $G \cong C_{1001}$. ⁂

14. Semidirekte Produkte

Worum geht es? Wir führen unsere Untersuchungen über Komplexprodukte UV mit $U \cap V = \{1\}$ aus der letzten Vorlesung fort, setzen diesmal aber nur die Normalität der Gruppe U voraus. Dies führt auf den Begriff des *internen semidirekten Produkts*. Anschließend beschäftigen wir uns mit einer verwandten Konstruktion, dem *externen semidirekten Produkt*.
Um semidirekte Produkte genauer untersuchen zu können, beschäftigen wir uns mit Homomorphismen von zyklischen Gruppen und bestimmen die Automorphismengruppen von zyklischer Gruppen. ⋇

Interne semidirekte Produkte

Seien G eine Gruppe und $U, V \leq G$ Untergruppen von G mit $U \cap V = \{1\}$. Der Fall, in dem U und V beide normal in G sind, führt auf das interne direkte Produkt und wurde ausgiebig in der letzten Vorlesung behandelt.
Wir setzen im Folgenden daher nur voraus, dass U ein Normalteiler von G ist; weitere Annahmen über V treffen wir nicht. Nach 13.6 (a) ist UV dann eine Untergruppe von G, allerdings typischerweise kein Normalteiler von G. Man nennt die Gruppe UV das **(interne) semidirekte Produkt aus U und V**. Sie ist eine Untergruppe von G, was die Bezeichnung *intern* erklärt.

Beispiel 14.1 (a) Für $n \geq 2$ ist die Gruppe S_n ein internes semidirektes Produkt aus dem Normalteiler A_n und der Untergruppe $V := \langle(1\ 2)\rangle$; dies folgt, da $U \cap V = \{\mathrm{id}\}$ gilt und somit $|A_n V| = |A_n| \cdot |V| = n!/2 \cdot 2 = n! = |S_n|$ ist.

(b) Jedes interne direkte Produkt ist auch ein internes semidirektes Produkt. ⁉

(c) Ein internes semidirektes Produkt UV mit $U \cong C_3$ und $V \cong C_2$ kann zu C_6 oder zu S_3 isomorph sein.

Den ersten Fall können wir innerhalb der Gruppe C_6 realisieren, indem wir U bzw. V als die eindeutige 3- bzw. 2-Sylowgruppe der C_6 wählen.

Den zweiten Fall können wir innerhalb der Gruppe S_3 realisieren, indem wir U als die eindeutige 3-Sylowgruppe und V als eine der 2-Sylowgruppen wählen. ⋇

Teil (c) des obigen Beispiels zeigt, dass der Isomorphietyp des semidirekten Produkts UV nicht durch die Isomorphietypen von U und V festgelegt ist. Hier unterscheiden sich semidirekte Produkte vom direkten Produkt. ⁉
Wir untersuchen die Multiplikation in semidirekten Produkten, um herauszufinden, welche zusätzlichen Informationen man benötigt, um deren Isomorphietyp festzustellen. Seien hierzu $u, u' \in U$ und $v, v' \in V$. Da UV eine Gruppe ist, lässt sich das Produkt $uv \cdot u'v'$ in die Form $x \cdot y$ mit $x \in U$ und $y \in V$ bringen. Hierbei nutzt man die Normalität von U aus:

$$uv \cdot u'v' = uvu' \cdot v^{-1}v \cdot v' = \overbrace{u \cdot \underbrace{vu'v^{-1}}_{\in U}}^{\in U} \cdot vv' \in UV.$$

Es folgen also $x = u \cdot vu'v^{-1} \in U$ und $y = vv' \in V$.
Bezeichnen wir mit

$$k_v : U \to U, \qquad u \mapsto vuv^{-1}$$

die Konjugation von Elementen aus U mit dem Element $v \in V$, so können wir die eben hergeleitete Multiplikation umschreiben in die Form

$$uv \cdot u'v' = uk_v(u') \cdot vv'. \tag{ISP}$$

Bemerkung 14.2 (a) Gleichung (ISP) zeigt, dass die Multiplikation im semidirekten Produkt UV nicht nur von der Multiplikation in U bzw. in V, sondern auch von der Konjugation von V auf U abhängt: Um den Isomorphietyp von UV zu bestimmen, muss man also wissen, wie V auf U (per Konjugation) operiert.

Hat man umgekehrt diese drei Informationen, so ist die Multiplikation in UV und damit auch der Isomorphietyp von UV eindeutig festgelegt.

(b) Diese Beobachtung erklärt den Effekt aus 14.1 (c):

Dort kannten wir ausschließlich die Struktur von U bzw. von V, wir wussten allerdings nicht, wie V auf U operiert. Daher war die Multiplikation im semidirekten Produkt UV nicht festgelegt, so dass mehrere Isomorphietypen für UV möglich waren. ⋇

Externe semidirekte Produkte

Im oberen Abschnitt haben wir semidirekte Produkte *innerhalb* einer gegebenen Gruppe G konstruiert. Wir wollen nun für zwei beliebig vorgegebene Gruppen U, V ein semidirektes Produkt definieren. Beachten Sie, dass U und V hierbei typischerweise nicht Untergruppen einer gemeinsamen Obergruppe sind.
Ausgangspunkt für die Definition des externen semidirekten Produkts ist die Darstellung der Multiplikation aus Gleichung (ISP). Da allerdings Produkte von Elementen aus U mit Elementen aus V nicht definiert sind, benötigen wir einen Ersatz für die Konjugation $k_v(u')$. Hier helfen die folgenden beiden Beobachtungen:

- Für jedes $v \in V$ ist die Abbildung k_v ein Automorphismus von U.
- Die Abbildung

  $$\varphi : V \to \mathrm{Aut}(U), \qquad v \mapsto k_v$$

  ist ein Homomorphismus. (Können Sie dies nachweisen?)

Mit diesen Notationen lässt sich (ISP) umschreiben in die Form

$$uv \cdot u'v' = u\varphi(v)(u') \cdot vv'. \tag{$\star$}$$

(Machen Sie sich klar, was die Notation $\varphi(v)(u')$ bedeutet!)

Im folgenden Resultat übertragen wir die Multiplikation aus $(\star)$ auf die Menge $U \times V$ und erhalten auf diese Weise eine Gruppe. Der Beweis der Aussage ist einfach: Man muss lediglich die Gruppenaxiome nachprüfen. Allerdings führt er auf lange und technische Rechnungen, weshalb wir ihn nicht führen.

Definition/Satz 14.3 *Seien U, V Gruppen und $\varphi : V \to \mathrm{Aut}(U)$ ein Homomorphismus. Dann wird die Menge $U \times V$ durch die Festsetzung*

$$(u,v) \cdot (u',v') := (u\varphi(v)(u'), vv') \qquad \text{für beliebige } u,u' \in U \text{ und } v,v' \in V \qquad \text{(ESP)}$$

zu einer Gruppe, dem ***(externen) semidirekten Produkt von U mit V unter φ****, das man üblicherweise mit $U \rtimes_\varphi V$ bezeichnet.*
(Machen Sie sich klar, dass der Ausdruck $u\varphi(v)(u')$ tatsächlich ein Element aus U ist.) ⁉

Bemerkung 14.4 (a) Der Ausdruck $U \times V$ kann in der Algebra mehrere Bedeutungen haben: In obiger Definition ist damit das kartesische Produkt von U mit V gemeint, also die *Menge* aller Paare (u,v) mit $u \in U$ und $v \in V$. In dieser Bedeutung trägt $U \times V$ keine Gruppenstruktur. Erst durch die explizite Angabe der Verknüpfung (ESP) wird die Menge $U \times V$ zur Gruppe.

$U \times V$ kann aber auch für das direkte Produkt von U mit V stehen. Dann ist mit $U \times V$ das kartesische Produkt $U \times V$ *zusammen mit der Verknüpfung aus 1.6 (e)* gemeint. In diesem Fall trägt $U \times V$ Gruppenstruktur.

Wann $U \times V$ welche Bedeutung hat, muss man aus dem Kontext schließen. Dies ist nicht immer einfach.

(b) Aus (a) folgt: Das direkte Produkt $U \times V$ hat dieselben Elemente wie das semidirekte Produkt $U \rtimes_\varphi V$. Sind U und V endlich, so gilt

$$|U \times V| = |U| \cdot |V| = |U \rtimes_\varphi V|.$$

Direktes und semidirektes Produkt unterscheiden sich also nur in ihren Multiplikationen. ⋇

Der nächste Satz liefert einen Zusammenhang zwischen externem und internem semidirekten Produkt. Kurz gesprochen sagt er aus, dass jedes externe semidirekte Produkt $U \rtimes_\varphi V$ als internes semidirektes Produkt gewisser Untergruppen geschrieben werden kann. Diese Untergruppen sind dabei isomorph zu den Ausgangsgruppen U bzw. V.

Satz 14.5 *Seien U, V zwei Gruppen mit Neutralem 1_U bzw. 1_V und $\varphi : V \to \mathrm{Aut}(U)$ ein Homomorphismus. Wir betrachten das externe semidirekte Produkt $G := U \rtimes_\varphi V$ und setzen*

$$U' := \{(u, 1_V) \in G \mid u \in U\} \qquad \text{bzw.} \qquad V' := \{(1_U, v) \in G \mid v \in V\}.$$

Dann gelten die folgenden Aussagen:

(a) *U' ist ein Normalteiler von G. Die Abbildung*

$$f : U \to U', \qquad u \mapsto (u, 1_V)$$

ist ein Isomorphismus zwischen U und U'. Es gilt also $U \cong U'$.

(b) *V' ist eine Untergruppe von G. Die Abbildung*

$$g : V \to V', \qquad v \mapsto (1_U, v)$$

ist ein Isomorphismus zwischen V und V'. Es gilt also $V \cong V'$.

(c) *Es gelten $U' \cap V' = \{(1_U, 1_V)\}$ und $G = U'V'$.*

Das externe semidirekte Produkt $U \rtimes_\varphi V$ ist daher das interne semidirekte Produkt $U'V'$ mit den zu U bzw. V isomorphen Gruppen U' bzw. V'.

Teilweiser Beweis. Wir zeigen nur die Aussage in (b). Die restlichen Aussagen lassen sich auf ähnliche Weise begründen.
Offenbar ist die Abbildung g bijektiv. Um zu zeigen, dass g ein Isomorphismus ist, muss nur noch die Homomorphie-Eigenschaft überprüft werden. Seien hierzu $x, y \in V$ beliebig. Dann gilt

$$\begin{aligned} f(x) \cdot f(y) &= (1_U, x) \cdot (1_U, y) \overset{\text{Mult. in } G}{=} (1_U \cdot \varphi(x)(1_U), xy) \\ &\overset{(\star)}{=} (1_U \cdot 1_U, xy) = (1_U, xy) = f(xy). \end{aligned}$$

In $(\star)$ haben wir ausgenutzt, dass Gruppenhomomorphismen Neutrale wieder auf Neutrale abbilden. Der Gruppenhomomorphismus $\varphi(x)$ bildet also 1_U auf 1_U ab.

Es folgt $V \cong V'$. Insbesondere ist gezeigt, dass die Menge V' eine Untergruppe von G ist. ■

Wir haben in 14.1 (b) gesehen, dass das direkte Produkt ein Spezialfall des semidirekten Produkts ist. Der nächste Satz charakterisiert, wann beide Produkte zusammenfallen:

Satz 14.6 *Seien U, V zwei Gruppen und $\varphi : V \to \mathrm{Aut}(U)$ ein Homomorphismus. Dann sind äquivalent:*

(a) *Es gilt $U \rtimes_\varphi V = U \times V$, d.h. das semidirekte Produkt von U und V unter φ entspricht dem direkten Produkt von U mit V.*

(b) *Der Homomorphismus φ ist konstant, d.h. es gilt $\varphi(v) = \mathrm{id}_U$ für alle $v \in V$.*

Beweis.

(a)$\Longrightarrow$(b) Es gelte $U \rtimes_\varphi V = U \times V$. Seien $u' \in U$ und $v \in V$ beliebig. Wir berechnen das Produkt $(1, v) \cdot (u', 1)$ einmal mit der Multiplikation in $U \rtimes_\varphi V$ und einmal mit der Multiplikation in $U \times V$. Da beide Multiplikationen gleich sind, erhalten wir

$$(1 \cdot \varphi(v)(u'), v \cdot 1) \overset{\text{in } U \rtimes_\varphi V}{=} (1, v) \cdot (u', 1) \overset{\text{in } U \times V}{=} (u', v).$$

Es folgt $u' = \varphi(v)(u')$ für jedes $u' \in U$ und jedes $v \in V$. Dies bedeutet, dass $\varphi(v) = \mathrm{id}_U$ für jedes $v \in V$ ist. Damit ist φ konstant.

(b)$\Longrightarrow$(a) Sei nun $\varphi(v) = \mathrm{id}_U$ für alle $v \in V$. Dann gilt in $U \rtimes_\varphi V$ für beliebige $u, u' \in U$ und $v, v' \in V$

$$(u,v) \cdot (u',v') = (u\varphi(v)(u'), vv') = (u\,\mathrm{id}_U(u'), vv') = (uu', vv').$$

Damit folgt $U \rtimes_\varphi V = U \times V$. ■

Wir untersuchen nun den Fall, in dem der Homomorphismus φ nicht konstant ist:

Satz 14.7 *Seien U, V zwei Gruppen und $\varphi : V \to \mathrm{Aut}(U)$ ein nicht-konstanter Homomorphismus. Dann ist das semidirekte Produkt $U \rtimes_\varphi V$ nicht abelsch.*

Beweis. Nach Voraussetzung existiert ein $v \in V$ mit $\varphi(v) \neq \mathrm{id}_U$. Somit finden wir $u \in U$ mit $\varphi(v)(u) \neq u$. Dann gilt

$$(1,v) \cdot (u,1) = (1 \cdot \varphi(v)(u), v \cdot 1) = (\varphi(v)(u), v) \neq (u,v).$$

Allerdings ist

$$(u,1) \cdot (1,v) = (u \cdot \varphi(1)(1), 1 \cdot v) \overset{\varphi(1)=\mathrm{id}_U}{=} (u \cdot \mathrm{id}_U(1), v) = (u,v).$$

Dies zeigt, dass $U \rtimes_\varphi V$ nicht abelsch ist. ■

Homomorphismen und Automorphismen zyklischer Gruppen

Um semidirekte Produkte genauer zu studieren, muss man Homomorphismen $\varphi : V \to \mathrm{Aut}(U)$ analysieren. Dies geht besonders einfach, wenn U und V zyklische Gruppen sind. Wir bestimmen in den folgenden Resultaten zunächst alle möglichen Homomorphismen $C \to G$ mit einer endlichen zyklischen Gruppe C und einer beliebigen Gruppe G. Hiermit können wir dann $\mathrm{Aut}(C)$ bestimmen.
Seien C eine endliche zyklische Gruppe, c ein Erzeuger von C und G eine beliebige Gruppe. Ist $\varphi : C \to G$ ein Homomorphismus und kennen wir das Bild $g := \varphi(c) \in G$, so liegt φ bereits fest: Da sich jedes Element von C in der Form c^k mit $k \in \mathbb{N}$ darstellen lässt, liefert 6.4 (a), dass $\varphi(c^k) = g^k$ ist. Wir müssen also nur noch klären, welche $g \in G$ als Bilder des Erzeugers c in Frage kommen:

Satz 14.8 (Homomorphismen mit zyklischem Definitionsbereich) *Seien C eine endliche zyklische Gruppe, c ein Erzeuger von C und G eine beliebige Gruppe. Für $g \in G$ sind äquivalent:*

(a) *Durch die Festsetzung $\varphi(c) := g$ entsteht ein Homomorphismus $\varphi : C \to G$.*

(b) *Die Ordnung von g ist endlich und es gilt* $\mathrm{ord}(g) \mid \mathrm{ord}(c)$.

Beweis. Der Übersichtlichkeit halber setzen wir $n := \mathrm{ord}(c)$. Es ist also $C \cong C_n$.

(a)$\Longrightarrow$(b) Es ist

$$1 = \varphi(1) = \varphi(c^n) = \varphi(c)^n = g^n.$$

7.15 (b) liefert nun $\operatorname{ord}(g) \mid n$. Insbesondere ist $\operatorname{ord}(g)$ endlich.

(b)$\Longrightarrow$(a) Es sei nun $\operatorname{ord}(g) < \infty$ mit $\operatorname{ord}(g) \mid n$. Wir setzen $\varphi(c) := g$. Die Homomorphie von φ erzwingt dann $\varphi(c^k) = g^k$ für alle $k \in \mathbb{N}$. Wir überprüfen, ob φ wohldefiniert ist. (Bevor Sie weiterlesen: Warum? Welche Probleme treten auf?) ⁉

Da C endlich ist, lässt sich ein Element aus C auf unendlich viele Weisen als Potenz von c schreiben. Seien $k, s \in \mathbb{N}$ mit $c^k = c^s$. Nach 7.16 (b) ist dann $n \mid s - k$, also $s = k + z \cdot n$ mit $z \in \mathbb{Z}$. Es folgt

$$\varphi(c^s) \overset{\text{Def. } \varphi}{=} g^s = g^k \cdot (g^n)^z \overset{\operatorname{ord}(g) \mid n}{=} g^k \cdot 1 = g^k \overset{\text{Def. } \varphi}{=} \varphi(c^k).$$

Damit ist nachgewiesen, dass φ eine Abbildung $C \to G$ ist. φ ist homomorph, denn für beliebige $k, s \in \mathbb{N}$ gilt

$$\varphi(c^{k+s}) \overset{\text{Def.}}{=} g^{k+s} = g^k \cdot g^s \overset{\text{Def.}}{=} \varphi(c^k) \cdot \varphi(c^s).$$ ■

Bemerkung 14.9 (a) Die Hauptschwierigkeit in obigem Beweis ist, zu erkennen, dass φ auf Wohldefiniertheit zu überprüfen ist. Der Nachweis der Homomorphie ist dann sehr einfach.

(b) Im Beweis reicht es, die Zahlen k und s aus $\mathbb{N}$ zu wählen: Da C endlich ist, lässt sich jedes Element von C als positive Potenz von c schreiben. Negative Exponenten werden also nicht benötigt.

Knobelfrage: Wie können Sie c^{-1} als positive Potenz von c schreiben? ⁉ ⋇

Beispiel 14.10 Die Gruppe S_5 enthält $\frac{5!}{5} = 4! = 24$ Elemente der Ordnung Fünf und genau ein Element der Ordnung Eins. Daher existieren genau 25 Homomorphismen $C_5 \to S_5$. ⁉ ⋇

Wir können nun die Automorphismengruppen endlicher zyklischer Gruppen bestimmen:

Korollar 14.11 *Seien $n \in \mathbb{N}$ und c ein Erzeuger der zyklischen Gruppe C_n. Für $k \in \mathbb{N}_0$ bezeichnen wir den Endomorphismus, der durch die Festsetzung $c \mapsto c^k$ entsteht, mit φ_k. Dann gilt*

$$\operatorname{Aut}(C_n) = \{\varphi_k \mid 0 \leq k \leq n-1 \text{ mit } \operatorname{ggT}(k, n) = 1\}.$$

Anders formuliert: Genau dann entsteht durch die Festsetzung $c \mapsto c^k$ ein Automorphismus von C_n, wenn c^k ein Erzeuger von C_n ist. Da C_n genau $\varphi(n)$ Erzeuger besitzt, gilt $|\operatorname{Aut}(C_n)| = \varphi(n)$.

Beweis. Da die Ordnung von c^k ein Teiler von n ist, ist jede der Abbildungen φ_k ein Endomorphismus von C_n. Wir müssen also nur noch diejenigen k finden, für die φ_k bijektiv ist. Da Definitions- und Zielbereich von φ_k dieselbe endliche Anzahl an Elementen besitzen, ist die Bijektivität von φ_k äquivalent zur Surjektivität von φ_k. Nun ist

$$\varphi_k(C_n) = \varphi_k(c^{\mathbb{N}}) = (c^k)^{\mathbb{N}} = \langle c^k \rangle.$$

Genau dann ist φ_k also surjektiv, wenn $\langle c^k \rangle = C_n$ gilt, also wenn c^k ein Erzeuger von C_n ist. Dies ist genau dann der Fall, wenn $k \in \{0, 1, \dots, n-1\}$ teilerfremd zu n ist, vgl. den Beweis zu 7.19. ■

Bemerkung 14.12 Obiges Korollar gibt die Elemente und die Ordnung von $\mathrm{Aut}(C_n)$ konkret an. In den Übungen werden wir zeigen, dass die Abbildung → Übung

$$\mathrm{Aut}(C_n) \to \mathbb{Z}_n^\times, \qquad \varphi_k \mapsto k$$

ein Isomorphismus ist. Der Isomorphietyp von $\mathrm{Aut}(C_n)$ ist also durch $\mathbb{Z}_n^\times$ gegeben. ※

Beispiel 14.13 Seien p, q Primzahlen mit $p < q$. Wir untersuchen, wann es nicht-abelsche Gruppen G der Ordnung pq geben kann.
Sei n_q die Anzahl der q-Sylowgruppen von G. Es gilt

$$n_q \in \{1, p\} \cap \{1, q+1, \dots\} \overset{p<q}{=} \{1\}.$$

Sei U *die* q-Sylowgruppe von G. Dann ist U normal in G. Sei V eine p-Sylowgruppe von G. Es gelten $U \cong C_q$ und $V \cong C_p$ und $U \cap V = \{1\}$. Daher ist $G = UV$, und 14.5 (c) zeigt

$$G \cong C_q \rtimes_\varphi C_p \qquad \text{mit einem Homomorphismus } \varphi : C_p \to \mathrm{Aut}(C_q).$$

Wir konstruieren die möglichen Homomorphismen φ. Sei c ein Erzeuger von C_p; dann gilt $\mathrm{ord}(c) = p \in \mathbb{P}$. Nach 14.8 können wir c auf genau diejenigen $g \in \mathrm{Aut}(C_q)$ mit $\mathrm{ord}(g) \mid p$, also mit $\mathrm{ord}(g) \in \{1, p\}$ abbilden. Dies führt auf die folgenden beiden Fälle:

Fall $\mathrm{ord}(g) = 1$ Dann wird c und somit auch jede Potenz von c auf das Neutrale in $\mathrm{Aut}(C_q)$, also auf id_{C_q} abgebildet. Der Homomorphismus φ ist dann konstant; nach 14.6 ist G isomorph zum direkten Produkt

$$G \cong C_q \times C_p \cong C_{pq}$$

und damit zyklisch (und abelsch).

Fall $\mathrm{ord}(g) = p$ Dieser Fall kann nur eintreten, wenn $\mathrm{Aut}(C_q)$ ein Element der Ordnung p enthält, also nach Cauchy 12.6 genau dann, wenn $|\mathrm{Aut}(C_q)| = \varphi(q) = q-1$ ein Vielfaches von p ist. In diesem Fall entsteht durch Abbilden von c auf ein Element der Ordnung p in $\mathrm{Aut}(C_q)$ tatsächlich ein nicht-konstanter Homomorphismus φ. Die Gruppe G ist dann wegen 14.7 nicht abelsch.

Zusammenfassend können wir also sagen: Genau dann gibt es nicht-abelsche Gruppen der Ordnung pq, wenn $p \mid q-1$ gilt. ※

Teil III.
Integritätsbereiche

Wir beschäftigen uns mit *Polynomringen* und ihren Elementen, den *Polynomen*, für die wir die wichtigen *Gradformeln* beweisen. Wir zeigen, dass unter gewissen Voraussetzungen eine *Polynomdivision mit Rest* existiert. Konsequenzen hieraus sind Einschränkungen an die Anzahl von Nullstellen eines Polynoms sowie die Aussage, dass endliche Untergruppen der Einheitengruppe eines nullteilerfreien Rings zyklisch sind.

Im Anschluss untersuchen wir die multiplikative Struktur von Ringen genauer. Unser Ziel ist es, Ringe anzugeben, die sich aus algebraischer Sicht ähnlich wie die ganzen Zahlen verhalten und in denen Resultate analog zu Vorlesung 3 gelten.
Hierzu diskutieren wir zuerst, wie sich die zahlentheoretischen Begriffe aus Vorlesung 3 auf Ringe verallgemeinern lassen. Diese Überlegungen führen uns schnell auf einen ersten Typ von Ring, den *Integritätsbereich*.
Nach Definition einer *eindeutigen Primfaktorzerlegung für Integritätsbereiche* erhalten wir einen weiteren Ringtyp, den *faktoriellen Ring*. Wir zeigen, dass dort die Begriffe des *größten gemeinsamen Teilers* und des *kleinsten gemeinsamen Vielfachen* zur Verfügung stehen.
Trotz der Existenz dieser vertrauten Begriffe verhalten sich faktorielle Ringe oft anders als $\mathbb{Z}$; dies werden wir an einigen Beispielen sehen.
Wir fordern daher weitere Bedingungen und erhalten so die Ringtypen *Hauptidealring* und *euklidischer Ring*; letzterer verhält sich aus algebraischer Sicht wie $\mathbb{Z}$.

Als Abschluss des Abschnitts und Überleitung zur Körpertheorie beschäftigen wir uns mit Zerlegungen von Polynomen und lernen Techniken kennen, mit denen man Unzerlegbarkeit und, darauf aufbauend, Irreduzibilität von Polynomen nachweist.

15. Adjunktion von Elementen, Polynomringe

Worum geht es? Wir beschreiben eine Standardtechnik, das *Adjungieren von Elementen an einen Ring*. Hierbei wird ein gegebener Ring vergrößert, indem Elemente zu ihm hinzugefügt werden. Die Ringstruktur bleibt dabei erhalten.
Danach beschäftigen wir uns mit einer wichtigen Klasse von Ringen, den *Polynomringen*. Wir zeigen die *Gradformeln*, dividieren mit Rest, definieren das *Einsetzen von Elementen in Polynome* und geben Schranken für die Anzahl von Nullstellen eines Polynoms an. ⋇

Adjunktion von Elementen

Wir haben in Vorlesung 2 den Begriff des Ringerzeugnisses kennengelernt. Wir wollen jetzt auf einen Spezialfall dieses Erzeugnisses eingehen, der in der Ring- und Körpertheorie oft verwendet wird. Hier liegen ein Ring R sowie eine Menge M von Elementen aus einem Oberring S von R vor. Man ist am kleinsten Unterring von S interessiert, der M und R enthält, d. h. am Ringerzeugnis $\langle R \cup M\rangle$. In der oben geschilderten speziellen Situation führt man eine eigene Schreibweise ein:

Definition 15.1 *Seien R ein Ring und M eine Teilmenge eines Oberrings S von R. Mit $R[M]$ (gelesen: **R adjungiert M**) bezeichnen wir den (per Mengeninklusion) kleinsten Unterring von S, der R und M als Teilmengen enthält. Es gilt nach 2.11 also $R[M] = \langle R \cup M\rangle$.*

Mit Hilfe von 2.20 können wir die Elemente aus $R[M]$ konkret angeben:

Satz 15.2 *Seien R ein Ring und M eine Teilmenge irgendeines Oberrings von R. Dann gilt*

$$R[M] = \left\{ \sum_{i=0}^{n} r_i m_i : n \in \mathbb{N}_0, r_i \in R, m_i \text{ ist Produkt endlich vieler Elemente aus } M \right\}.$$

Konvention: Leere Produkte haben den Wert Eins, leere Summen den Wert Null.

Beweis. Sei $A := R \cup M$. Dann gilt $R[M] = \langle A\rangle$. Nach 2.20 erhalten wir

$$\begin{aligned}
\langle A\rangle &= \left\{ \sum_{i=1}^{n} \left(e_i \prod_{k=1}^{s_i} a_{i,k} \right) : n \in \mathbb{N}_0, s_1, \dots, s_n \in \mathbb{N}_0, e_i \in \{\pm 1\} \text{ und } a_{i,k} \in A \right\} \\
&\overset{(\star)}{=} \left\{ \sum_{i=1}^{n} \left(r_i \prod_{k=1}^{t_i} m_{i,k} \right) : n \in \mathbb{N}_0, t_1, \dots, t_n \in \mathbb{N}_0 \text{ und } m_{i,k} \in M \right\} \\
&\overset{(\star\star)}{=} \left\{ \sum_{i=0}^{n} r_i m_i : n \in \mathbb{N}_0, r_i \in R, m_i \text{ ist Produkt endlich vieler Elemente aus } M \right\}.
\end{aligned}$$

Zu $(\star)$: Wir haben für festes i das Element e_i und alle der $a_{i,k}$ mit $a_{i,k} \in R$ zu einem Element $r_i \in R$ zusammengefasst.
Zu $(\star\star)$: Das Produkt $\prod_{k=1}^{t_i} m_{i,k}$ haben wir mit m_i bezeichnet. ■

Bemerkung 15.3 Die obigen Rechnungen finden im vorausgesetzten Oberring S von R statt. Die Produkte $r_i m_i$ und die anschließende Summation sind also definiert. ⁜

Beispiel 15.4 (a) Wir betrachten den (oft auftretenden) Fall einer einelementigen Menge $M = \{m\}$. Produkte endlich vieler Elemente aus M sind dann von der Form m^k mit $k \in \mathbb{N}_0$. Es folgt

$$\begin{aligned} R[M] = R[m] &= \left\{ \sum_{k=0}^{n} r_k m^{i_k} \mid n \in \mathbb{N}_0, i_k \in \mathbb{N}_0, r_k \in R \right\} \\ &\overset{\text{Sortieren nach Potenzen von } m}{=} \left\{ \sum_{k=0}^{n} r_k m^k : n \in \mathbb{N}_0, r_k \in R \right\}. \end{aligned}$$

(b) Wir bezeichnen mit $i \in \mathbb{C}$ die imaginäre Einheit. Im Oberring $\mathbb{C}$ ist die Adjunktion $\mathbb{R}[i]$ definiert. Mit (a) erhält man

$$\mathbb{R}[i] = \left\{ \sum_{k=0}^{n} r_k i^k : n \in \mathbb{N}_0, r_k \in \mathbb{R} \right\} = \{ r_0 + r_1 \cdot i \mid r_0, r_1 \in \mathbb{R} \} = \mathbb{C}.$$

Warum werden keine höheren Potenzen i^k mit $k \geq 2$ benötigt? ⁉

Analog folgt $\mathbb{Q}[i] = \{q_0 + q_1 \cdot i \mid q_0, q_1 \in \mathbb{Q}\}$ und $\mathbb{Z}[i] = \{z_0 + z_1 \cdot i \mid z_0, z_1 \in \mathbb{Z}\}$.

(c) Sei $\alpha \in \mathbb{C}$ eine Nullstelle des Polynoms $X^s - a \in \mathbb{Z}[X]$. Dann kann, ähnlich wie in (b), auf Potenzen α^k mit $k \geq s$ verzichtet werden. Es gilt also: ⁉

$$\mathbb{Z}[\alpha] = \left\{ \sum_{k=0}^{n} z_k \alpha^k : n \in \mathbb{N}_0, z_k \in \mathbb{Z} \right\} = \{ z_0 + z_1 \alpha + \cdots + z_{s-1} \alpha^{s-1} \mid z_k \in \mathbb{Z} \}.$$

⁂

Bemerkung 15.5 In Teil (a) des obigen Beispiels haben wir die Ringadjunktion eines einzigen Elements m untersucht. In den Fällen (b) und (c) konnten wir Zusatzinformationen über m ausnutzen, um einfachere Darstellungen für $R[m]$ zu finden.
Die Frage nach einfachen Darstellungen für Adjunktionen wird uns in der Körpertheorie wieder begegnen und dort systematisch untersucht werden. ⁂

Polynomringe

Ein für die Algebra sehr wichtiges Objekt ist das Polynom. Beispielsweise ist die Körpertheorie über weite Strecken eine Theorie der Polynome.
Wir werden Polynome in naiver Weise definieren, d. h. nicht genau klären, was die Polynomvariable X eigentlich ist; hierzu verweisen wir beispielsweise auf [KM17, Kapitel 14, S. 187]. Eine exakte Behandlung von Polynomen ist umfangreich, für konkrete Rechnungen mit Polynomen nicht erforderlich und liefert im Wesentlichen nur Aussagen, die man für Polynome erwartet und die von vornherein schon „klar“ waren.

Für uns gilt daher: Eine **Polynomvariable** ist ein nicht näher bestimmtes Objekt X,

(a) mit dem wie mit einem Ringelement gerechnet werden kann und das daher insbesondere mit allen anderen Ringelementen kommutiert und

(b) dessen Potenzen „linear unabhängig“ sind, d. h. aus $\sum_{k=0}^{n} r_k X^k = 0$ soll $r_k = 0$ für alle $k \in \{0, \dots, n\}$ folgen. Wie in 1.9 setzen wir $X^0 := 1$.

Wir können nun definieren, was wir unter einem Polynomring verstehen wollen:

Definition 15.6 *Seien R ein Ring und X eine Polynomvariable. Dann zeigt man durch Überprüfung der Ringaxiome, dass die Menge*

$$R[X] := \left\{ \sum_{k=0}^{n} r_k X^k : n \in \mathbb{N}_0, r_k \in R \right\}$$

*ein (wegen obiger Eigenschaft (a) kommutativer) Ring ist. Man nennt $R[X]$ den **Polynomring über R in der Polynomvariablen X**, seine Elemente heißen **Polynome über R in der Polynomvariablen X**. Die Null in $R[X]$ nennt man das **Nullpolynom**.*

Bemerkung 15.7 15.1 und 15.6 beschreiben dieselbe Vorstellung, nämlich das Bilden des kleinsten Oberrings von R nach Hinzufügen gewisser Elemente zu R. Aus mathematischer Sicht sind 15.1 und 15.6 aber völlig verschieden:
In 15.1 steht uns bereits ein passender Oberring zur Verfügung, innerhalb dessen die Konstruktion von $R[M]$ vonstatten geht. Dies ist mathematisch unkritisch.
In 15.6 haben wir jedoch keinen Zugriff auf einen Oberring von R, der X enthält. Somit muss der Ring $R[X]$ von R aus mit Hilfe der Eigenschaften, die wir für Polynomvariablen gefordert haben, aufgebaut werden. Erst durch Nachweis der Ringaxiome wird klar, dass so tatsächlich ein Ring entstanden ist. ⁂ ⁉

Definition 15.8 *Seien R ein Ring und $f := \sum_{k=0}^{n} r_k X^k \in R[X]$ ein Polynom über R. Für $k \in \{0, \dots, n\}$ nennen wir r_k den **k-ten Koeffizienten von f**. Für $k > n$ definieren wir den k-ten Koeffizienten von f als Null.*

Bemerkung 15.9 (a) Wegen der Polynomvariablen-Eigenschaft (b) sind zwei Polynome genau dann gleich, wenn ihre k-ten Koeffizienten für alle $k \in \mathbb{N}_0$ übereinstimmen. Dies zeigt insbesondere, dass die Darstellung eines Polynoms als Summe $\sum_{k=0}^{n} r_k X^k$ eindeutig ist bis auf führende Nullsummanden, d. h. wir können für dieses Polynom auch $\sum_{k=0}^{m} r_k X^k$ mit $m > n$ schreiben, wobei wir die neu auftretenden Koeffizienten r_k mit $k > n$ alle auf Null setzen.

(b) Seien $f := \sum_{i=0}^{a} r_i X^i$ und $g := \sum_{j=0}^{b} s_j X^j$ zwei Polynome aus $R[X]$. Wegen der Polynomvariablen-Eigenschaft (a) können wir $f+g$ und $f \cdot g$ wie üblich ausrechnen:

Zur Berechnung von $f+g$ füllen wir f bzw. g mit Nullsummanden auf und erhalten

$$f + g = \sum_{i=0}^{a} r_i X^i + \sum_{j=0}^{b} s_j X^j = \sum_{i=0}^{\max(a,b)} r_i X^i + \sum_{i=0}^{\max(a,b)} s_i X^i = \sum_{i=0}^{\max(a,b)} (r_i + s_i) X^i.$$

Für das Produkt $f \cdot g$ erhalten wir mit dem Distributivgesetz:

$$f \cdot g = r_a s_b X^{a+b} + (r_{a-1} s_b + r_a s_{b-1}) X^{a+b-1} + \cdots + a_0 b_0.$$

(c) In der Algebra muss streng zwischen einem *Polynom* im Sinne von 15.6 und der durch ein Polynom beschriebenen *Polynomfunktion* unterschieden werden.

So sind die Polynome $f := X \in \mathbb{Z}_2[X]$ und $g := X^2 \in \mathbb{Z}_2[X]$ nach 15.9 (a) verschieden, denn der erste Koeffizient von f ist Eins, der erste Koeffizient von g hingegen Null. Allerdings stimmen die Polynomfunktionen

$$F : \mathbb{Z}_2 \to \mathbb{Z}_2, \quad a \mapsto f(a) = a \qquad \text{bzw.} \qquad G : \mathbb{Z}_2 \to \mathbb{Z}_2, \quad a \mapsto g(a) = a^2$$

überein. ⁂ ⁉

Wegen der Eindeutigkeit in 15.9 (a) können wir definieren:

Definition 15.10 *Seien R ein Ring und $f := \sum_{k=0}^{n} r_k X^k \in R[X]$ ein Polynom mit $f \neq 0$. Dann existiert ein größter Index $k \in \mathbb{N}_0$ mit $a_k \neq 0$. Dieses a_k nennt man den **Leitkoeffizienten von f**. Man nennt k den **Grad von f** und schreibt* $\deg f$ *für ihn.*
Das Nullpolynom $0 \in R[X]$ besitzt als einziges Polynom keinen Leitkoeffizienten. Wir setzen $\deg(0) := -\infty$.
Konvention: Für alle $n \in \mathbb{N}_0 \cup \{-\infty\}$ ist $-\infty + n := -\infty$.

Für die weitere Ring- und Körpertheorie ist das Einsetzen von Elementen in Polynome wesentlich. Man kann so beispielsweise mathematisch sauber den Übergang von Polynom auf Polynomfunktion beschreiben.

Definition 15.11 *Seien R ein Ring, S ein Oberring von R und $f := \sum_{k=0}^{n} r_k X^k$ ein Polynom aus $R[X]$. Für $a \in S$ definiert man das **Einsetzen von a** durch $f(a) := \sum_{k=0}^{n} r_k a^k$.*
*Gilt $f(a) = 0$, so nennt man a eine **Nullstelle von f (in S)**. Die Abbildung*

$$e_a : R[X] \to S, \qquad f \mapsto f(a)$$

*ist ein Homomorphismus (Warum?) und heißt **Einsetzhomomorphismus**.* ⁉

Bemerkung 15.12 Beachten Sie, dass beim Einsetzhomomorphismus nicht die einzusetzenden Elemente a, sondern die betrachteten Polynome f variieren.
Es gilt $\ker e_a = \{f \in R[X] \mid f(a) = 0\}$. Der Kern von e_a besteht also aus allen Polynomen aus $R[X]$, die in a eine Nullstelle besitzen. ⁂

Ein weiteres wichtiges Resultat über Polynome sind die Gradformeln. Sie stellen Zusammenhänge zwischen dem Grad zweier Polynome und dem Grad des Produkt bzw. der Summe dieser Polynome her:

Satz 15.13 (Gradformeln) *Seien R ein Ring und $f, g \in R[X]$.*

(a) *Es gilt* $\deg(f+g) \leq \max(\deg f, \deg g)$.

Ist $\deg f \neq \deg g$, *so gilt sogar* $\deg(f+g) = \max(\deg f, \deg g)$.

(b) *Es gilt* $\deg(f \cdot g) \leq \deg f + \deg g$.

Ist eines der beiden Polynome das Nullpolynom oder besitzt eines der beiden Polynome einen Nicht-Nullteiler als Leitkoeffizienten, so gilt sogar $\deg(f \cdot g) = \deg f + \deg g$. *Diese Oder-Bedingung ist stets erfüllt, wenn R nullteilerfrei ist.* ⁉

Beweis. Wir zeigen nur (b); der Beweis von (a) ist ähnlich.
Für $f = 0$ oder $g = 0$ gilt $\deg(f \cdot g) = \deg f + \deg g$ gemäß der Konvention in 15.10. Seien nun f und g beide nicht das Nullpolynom. Wir können schreiben

$$f = r_n X^n + \cdots + r_0 \qquad \text{und} \qquad g = s_m X^m + \cdots + s_0 \qquad \text{mit } r_n, s_m \neq 0.$$

Dann gilt $f \cdot g = r_n s_m X^{n+m} + h$ mit $h \in R[X]$ und $\deg h < n+m$. Dies zeigt, dass $\deg(fg) \leq n+m = \deg f + \deg g$ gilt. ⁉
Unter der Zusatzannahme, dass r_n oder s_m kein Nullteiler ist, folgt $r_n s_m \neq 0$. Wir erhalten dann die Gleichheit $\deg(fg) = n+m = \deg f + \deg g$. ■

Wir geben zwei Beispiele an, in denen die Gradformeln besonders schlecht abschätzen:

Beispiel 15.14 (a) Für beliebiges $n \in \mathbb{N}$ setzen wir $f := X^n \in \mathbb{Z}[X]$ und $g := -f$. Dann gilt $-\infty = \deg 0 = \deg(f+g) \leq \max(\deg f, \deg g) = n$.

(b) Wir setzen $f := \overline{2}X + \overline{2} \in \mathbb{Z}_4[X]$ und $g := f$. Dann ist

$$f \cdot g = (\overline{2}X + \overline{2})^2 = \overline{4}X^2 + \overline{8}X + \overline{4} = \overline{0}.$$

Somit ist $-\infty = \deg(fg) \leq \deg f + \deg g = 4$. ※

Aus den Gradformeln folgen wichtige Resultate in der Theorie der Polynome:

Korollar 15.15 *Ist R ein nullteilerfreier Ring, so ist auch der Polynomring R[X] nullteilerfrei.*

Beweis. Seien $f, g \in R[X]$ mit $fg = 0$. Mit 15.13 (b) folgt $\deg f + \deg h = -\infty$. Dies zeigt, dass f oder g das Nullpolynom ist. $R[X]$ besitzt also keine Nullteiler. ■

Korollar 15.16 *Ist R ein nullteilerfreier Ring, so sind die Einheitengruppen von R und R[X] gleich, d.h. es gilt* $R[X]^\times = R^\times$.

Beweis. Die Aussage ist klar, wenn $R = \{0\}$ ist. Sei nun R nicht der Nullring. Dann ist $\deg 1 = 0$. Ist f eine Einheit von $R[X]$, so existiert $g \in R[X]$ mit $fg = 1$. Wegen der Nullteilerfreiheit liefert die Gradformel $0 = \deg f + \deg g$. Dies zeigt $\deg f, \deg g \in \mathbb{N}_0$ und daher $\deg f = \deg g = 0$. Es folgt $f, g \in R$ und somit $R[X]^\times \subseteq R^\times$.
Die umgekehrte Inklusion $R^\times \subseteq R[X]^\times$ ist klar. ■ ⁉

Korollar 15.17 (Division mit Rest) *Seien R ein Ring und $f, g \in R[X]$ mit $g \neq 0$. Der Leitkoeffizient von g möge eine Einheit sein. Dann ist eine* ***Division von f durch g mit Rest*** *in folgendem Sinne möglich: Es existieren eindeutige $q, r \in R[X]$, so dass $f = qg + r$ und $\deg r < \deg g$ gelten.*

Beweis.

Existenz Sei

$$g = eX^n + \textit{Terme mit deg} < n \qquad \text{mit } e \in R^\times.$$

Wir wählen $q \in R[X]$ derart, dass $r := f - qg$ einen minimalen Grad besitzt. (Warum existiert ein solches q?) Angenommen, es gilt $\deg r \geq n = \deg g$. Wir zeigen, dass dann ein Polynom $\tilde{q} \in R[X]$ existiert, so dass $\deg(f - \tilde{q} \cdot g) < \deg r$ gilt. Dieser Widerspruch zur Minimalität von $\deg r$ beweist die zu zeigende Existenz.

Aufgrund der Annahme $\deg r \geq n$ können wir schreiben

$$r = s_m X^m + \textit{Terme mit deg} < m \qquad \text{mit } m \geq n \text{ und } s_m \neq 0.$$

Dann ist $m - n \geq 0$, und es gilt $e^{-1} s_m X^{m-n} \cdot g = s_m X^m + \textit{Terme mit deg} < m \in R[X]$. Setzen wir $\tilde{q} := q + e^{-1} s_m X^{m-n}$, so folgt

$$\begin{aligned} \deg(f - \tilde{q} \cdot g) &= \deg(f - qg - e^{-1} s_m X^{m-n} g) = \deg(r - e^{-1} s_m X^{m-n} g) \\ &= \deg(s_m X^m + \textit{Terme mit deg} < m \; - s_m X^m - \textit{Terme mit deg} < m) \\ &< m = \deg r. \end{aligned}$$

Eindeutigkeit Seien $q, q', r, r' \in R[X]$ mit $f = qg + r = q'g + r'$ und $\deg r, \deg r' < \deg g$. Dann gilt $r - r' = g \cdot (q' - q)$. Da der Leitkoeffizient von g eine Einheit und somit kein Nullteiler ist, gilt Gleichheit in der Gradformel aus 15.13 (b). Es folgt

$$\deg g \overset{\deg g > \deg r, \deg r'}{>} \deg(r - r') = \deg(g \cdot (q' - q)) \overset{15.13\,(b)}{=} \deg g + \deg(q' - q).$$

Dies liefert $0 > \deg(q' - q)$ und somit $\deg(q' - q) = -\infty$. Also folgt $q' = q$ und hieraus $r' = r$. ∎

Auf die Einheitenvoraussetzung bei der Division mit Rest für Polynomringe kann im Allgemeinen nicht verzichtet werden:

Beispiel 15.18 Wir betrachten die Polynome $f := X$ und $g := 2$ in $\mathbb{Z}[X]$; der Leitkoeffizient von g ist keine Einheit in $\mathbb{Z}$.
Die Bedingung $\deg r < \deg g$ aus 15.17 liefert $\deg r \leq 0$, also $r \in \mathbb{Z}$. Mit dieser Einschränkung ist die Gleichung $f = qg + r$ für kein $q \in \mathbb{Z}[X]$ lösbar: Aus Gradgründen muss $q \neq 0$ sein. Dann haben linke und rechte Seite der Gleichung aber verschiedene Leitkoeffizienten. ⁂

Mit Hilfe der Division mit Rest können wir Nullstellen von Polynomen abspalten:

Korollar 15.19 *Seien R ein Ring, $f \in R[X]$ und $a \in R$ eine Nullstelle von f. Dann existiert ein $g \in R[X]$, so dass $f = (X - a) \cdot g$ gilt.*

Beweis. Die Behauptung ist klar, wenn $R = \{0\}$ ist. Ansonsten dividieren wir f mit Rest durch $X - a$; dies ist möglich, da der Leitkoeffizient von $X - a$ eine Einheit ist. Nach 15.17 existieren dann $q, r \in R[X]$ mit $f = (X-a)q+r$, wobei $\deg r < \deg(X-a) = 1$ gilt. Es folgt $r \in R$. Einsetzen zeigt nun

$$0 = f(a) \overset{\text{Einsetzen ist Homom.}}{=} (a - a) \cdot q(a) + r(a) = r(a).$$

Wegen $r \in R$ folgt aus $r(a) = 0$, dass $r = 0$ ist. Somit ist $f = (X - a) \cdot q$. ■

Satz 15.20 *Seien R ein nullteilerfreier Ring und $f \in R[X]$ nicht das Nullpolynom. Dann hat f höchstens* $\deg f$ *Nullstellen.*

Beweis. Der Beweis erfolgt per Induktion nach $\deg f$. Die Aussage ist für $\deg f = 0$ offenbar wahr.
Gilt sie für alle Polynome vom Grad n für ein bestimmtes $n \in \mathbb{N}_0$, so gilt sie auch für alle Polynome vom Grad $n + 1$; denn:
Ist $f \in R[X]$ ein beliebiges Polynom vom Grad $n+1$, so kann f entweder keine Nullstellen haben – in diesem Fall gilt die Behauptung – oder f hat mindestens eine Nullstelle $a \in R$. Dann können wir nach 15.19 schreiben $f = (X - a) \cdot g$, wobei für das Polynom $g \in R[X]$ nach Gradformel $\deg g = n$ gilt. Nullstellen von f sind nun Nullstellen von $X - a$ oder von g. Nach Induktionsvoraussetzung hat g höchstens n Nullstellen. Insgesamt hat f daher höchstens $n + 1$ Nullstellen. ■

Aus der Anzahlbeschränkung für Nullstellen eines Polynoms über nullteilerfreien Ringen folgt ein wichtiges Resultat:

Korollar 15.21 *Jede **endliche** Untergruppe G der Einheitengruppe eines nullteilerfreien Rings R ist zyklisch.*
*Insbesondere gilt: Ist K ein **endlicher** Körper, so ist $K^\times$ eine zyklische Gruppe.*

Beweis. Wäre die endliche abelsche Gruppe G nicht zyklisch, so hätte sie nach Struktursatz eine zu $C_p \times C_p$ isomorphe Untergruppe für eine Primzahl $p \in \mathbb{P}$. Die p^2 Elemente dieser Untergruppe wären aber Nullstellen des Polynoms $X^p - 1 \in R[X]$. Dies widerspricht 15.20. ■

Bemerkung 15.22 Nach 15.9 (c) muss man zwischen Polynom und Polynomfunktion unterscheiden: Verschiedene Polynome können dieselbe Polynomfunktion liefern.
Ist R allerdings ein *unendlicher* nullteilerfreier Ring, so liefern verschiedene Polynome $f, g \in R[X]$ stets auch verschiedene Polynomfunktionen: Aus der Verschiedenheit von f und g folgt, dass $f - g$ nicht das Nullpolynom ist und daher nach 15.20 nur endlich viele Nullstellen hat. Wegen $|R| = \infty$ gibt es daher $a \in R$ mit $(f - g)(a) \neq 0$. Die von f und g induzierten Polynomfunktionen sind also verschieden.
Im Falle unendlicher nullteilerfreier Ringe kann man daher ein Polynom eindeutig aus seiner Polynomfunktion rekonstruieren. In diesem Fall kann man also Polynome und Polynomfunktionen miteinander identifizieren. ⁜

16. Integritätsbereiche, Assoziiertheit, prime und (ir-)reduzible Elemente

Worum geht es? In der nächsten Vorlesung behandeln wir *eindeutige Primfaktorzerlegungen* in der Ringtheorie. In dieser Vorlesung stellen wir die hierzu benötigten Begrifflichkeiten bereit, indem wir die vertrauten Begriffe von $\mathbb{Z}$, mit denen wir uns in Vorlesung 3 beschäftigt haben, auf einen speziellen Typus von Ring, den *Integritätsbereich*, übertragen.
Als wesentliches Problem wird sich die fehlende Anordnung in Integritätsbereichen herausstellen. Dieses Problem gehen wir an, indem wir an vielen Stellen nur *Eindeutigkeit bis auf Assoziiertheit* fordern. ⁜

Ringe sind algebraische Strukturen mit sehr schöner additiver Struktur, aber möglicherweise recht unangenehmer multiplikativer Struktur – für diese fordern die Ringaxiome kaum Eigenschaften. Die ganzen Zahlen $\mathbb{Z}$ bilden hier zum Teil eine Ausnahme: Es gibt zwar eine ganze Reihe offener zahlentheoretischer Fragestellungen, beispielsweise die Goldbach-Vermutung oder die Fragen nach der Anzahl von Mersenne- oder Fermat-Primzahlen, allerdings lassen sich mit Hilfe der eindeutigen Primfaktorzerlegung viele Aussagen über $\mathbb{Z}$ beweisen.
Ziel der nächsten Vorlesungen ist es, den Begriff der eindeutigen Primfaktorzerlegung zu verallgemeinern und für Ringe zur Verfügung zu stellen.
Hierbei beschränken wir uns von vornherein auf nullteilerfreie Ringe; denn ist a ein Nullteiler mit Ko-Nullteiler b, so gilt wegen $ab = 0$

$$ac = ac + 0 = ac + ab = a \cdot (c + b) \qquad \text{für jedes Ringelement } c.$$

Faktorisierungen in Ringen mit Nullteilern sind also prinzipiell nicht immer eindeutig. Um Trivialitäten auszuschließen, fordern wir zusätzlich $1 \neq 0$. Dies führt auf den Begriff des Integritätsbereichs:

Definition 16.1 *Einen nullteilerfreien Ring mit* $1 \neq 0$ *nennen wir einen* ***Integritätsbereich****.*

Beispiel 16.2 (a) Die ganzen Zahlen $\mathbb{Z}$ sowie jeder Körper sind Integritätsbereiche.

(b) Wegen 15.15 ist der Polynomring $R[X]$ ein Integritätsbereich genau dann, wenn R ein Integritätsbereich ist.

(c) Jeder Unterring eines Körpers ist ein Integritätsbereich. ⁜ ⁉

Integritätsbereiche

Aus der Kürzungsregel für Ringe 4.18 erhalten wir die folgende Charakterisierung von Integritätsbereichen:

Satz 16.3 *Für einen Ring* R *mit* $1 \neq 0$ *sind äquivalent:*

(a) *R ist ein Integritätsbereich.*

(b) *In R kann durch beliebige $a \neq 0$ gekürzt werden.*

Obiger Satz klärt, warum man beispielsweise die Gleichung $2x = 8$ über $\mathbb{Z}$ nach x auflösen kann: Man schreibt $2x = 2 \cdot 4$ und *kürzt* dann durch 2 (man *teilt* nicht, da $2 \notin \mathbb{Z}^\times$). Alternativ kann man die Gleichung nach x auflösen, indem man sie als Gleichung über $\mathbb{Q}$ auffasst, dort durch 2 *teilt* und nachweist, dass der Wert, den man für x erhält, tatsächlich in $\mathbb{Z}$ liegt. Man hat hierbei ausgenutzt, dass $\mathbb{Q}$ ein Oberkörper von $\mathbb{Z}$ ist, und sogar der (per Mengeninklusion) kleinste.
Ein ähnlicher Übergang auf einen kleinsten Oberkörper ist für jeden Integritätsbereich R möglich. Hierzu stellt man den Übergang von $\mathbb{Z}$ auf $\mathbb{Q}$ durch Brüche nach: Man bildet die Menge $Q(R) := \{\frac{r}{s} \mid r, s \in R \text{ mit } s \neq 0\}$ aller Brüche mit Zählern aus R und Nennern aus $R \setminus \{0\}$, identifiziert gekürzte und erweiterte Brüche miteinander, definiert eine Addition und Multiplikation für Brüche und weist dann nach, dass $Q(R)$ so zum Körper wird. Wir führen die langen und relativ technischen Beweise nicht vor, sondern verweisen beispielsweise auf [KM17, Abschnitt 13.8].

Definition/Satz 16.4 *Seien R ein Integritätsbereich und $Q(R) := \{\frac{r}{s} \mid r, s \in R \text{ und } s \neq 0\}$ die Menge der Symbole $\frac{r}{s}$ mit $r \in R$ und $s \in R \setminus \{0\}$. Jedes solche Symbol bezeichnen wir als **Bruch**.*
Zwei Brüche $\frac{r}{s}$ und $\frac{r'}{s'}$ identifizieren wir miteinander und schreiben $\frac{r}{s} = \frac{r'}{s'}$, wenn $rs' = r's$ gilt. Auf $Q(R)$ definieren wir Verknüpfungen $\cdot$ und $+$ durch

$$\frac{r}{s} \cdot \frac{r'}{s'} := \frac{r \cdot r'}{s \cdot s'} \qquad \text{und} \qquad \frac{r}{s} + \frac{r'}{s'} := \frac{rs' + r's}{s \cdot s'} \qquad \text{für alle } r, r' \in R \text{ und } s, s' \in R \setminus \{0\}.$$

*Dann wird $Q(R)$ mit diesen Verknüpfungen zu einem Körper, dem **Quotientenkörper von R**. Die Null in $Q(R)$ ist $\frac{0}{1}$, die Eins in $Q(R)$ ist $\frac{1}{1}$. Die Abbildung*

$$\varphi : R \to Q(R), \qquad r \mapsto \frac{r}{1}$$

ist ein Monomorphismus. Nach Homomorphiesatz enthält $Q(R)$ daher den zu R isomorphen Unterring $\varphi(R) = \{\frac{r}{1} \mid r \in R\}$.

Bemerkung 16.5 (a) Für zwei Brüche $\frac{r}{s}$ und $\frac{r'}{s'}$ gilt $rs' = r's$ genau dann, wenn sie durch Kürzen oder Erweitern auseinander hervorgehen. Durch die Identifikation der Brüche miteinander stellen wir sicher, dass Kürzen oder Erweitern den Wert eines Bruches nicht ändert.

(b) Wegen (a) müssen die Verknüpfungen im Beweis von 16.4 auf Wohldefiniertheit überprüft werden.

(c) Oft identifiziert man den zu R isomorphen Unterring $\varphi(R)$ mit R und schreibt $\frac{r}{1} = r$ für alle $r \in R$. Dann wird $Q(R)$ zu einer Obermenge von R. Dies zeigt, dass jeder Integritätsbereich in einem Körper enthalten ist. Zusammen mit 16.2 (c) folgt, dass Integritätsbereiche genau die Unterringe von Körpern sind.

(d) Für $s \in R \setminus \{0\}$ übernimmt der Bruch $\frac{1}{s}$ die Rolle des Inversen von s; mit (c) gilt nämlich $s \cdot \frac{1}{s} = \frac{s}{1} \cdot \frac{1}{s} = \frac{s}{s} = \frac{1}{1} = 1$.

$Q(R)$ besteht daher aus allen Produkten der Form $r \cdot s^{-1}$ mit $r \in R$ und $s \in R \setminus \{0\}$ und ist daher der (per Mengeninklusion) kleinste Oberkörper von R. ⁜

Beispiel 16.6 (a) Es gilt $Q(\mathbb{Z}) = \mathbb{Q}$.

(b) Sei K ein Körper. Wegen 16.2 (b) ist der Polynomring $K[X]$ ein Integritätsbereich. Sein Quotientenkörper

$$Q(K[X]) = \left\{ \frac{f}{g} : f, g \in K[X], g \neq 0 \right\}$$

besteht aus allen Quotienten von Polynomen mit Koeffizienten aus K. Man nennt ihn auch den **rationalen Funktionenkörper über K** und bezeichnet ihn mit $K(X)$. Diese Körper spielen in der *algebraischen Geometrie* eine wichtige Rolle. ⁜

Knobelfrage. Wo wird in 16.4 benötigt, dass R ein Integritätsbereich ist? ⁇

Teilbarkeit und Assoziiertheit, prime und (ir-)reduzible Elemente

In Vorlesung 3 haben wir Begriffe kennengelernt, mit deren Hilfe man multiplikative Eigenschaften von $\mathbb{Z}$ beschreiben kann. Einige dieser Begriffe übertragen wir nun auf allgemeine Integritätsbereiche.
Die Teilbarkeitsdefinition aus 3.1 können wir wörtlich übernehmen:

Definition 16.7 *Seien R ein Integritätsbereich und $r, s \in R$. Wir nennen r einen **Teiler von s** und schreiben $r \mid s$, falls ein $x \in R$ existiert mit $rx = s$. In diesem Fall heißt s ein **Vielfaches von r**.*

Bei den meisten anderen Begriffen aus Vorlesung 3 funktioniert die Übersetzung nicht so glatt; wir haben dort in einigen Definitionen gefordert, dass Elemente in $\mathbb{N}$ liegen, also positiv sind. Dieses Konzept steht uns in allgemeinen Integritätsbereichen nicht zur Verfügung.
Die Beobachtung in 3.2 (d) gibt einen Anhaltspunkt, wie dieses Positivitätsproblem angegangen werden kann: Gilt $a \mid b$ und $b \mid a$ für Elemente $a, b \in \mathbb{Z}$, so ist $a = \pm b$, d. h. es gilt $|a| = |b|$. Anders interpretiert: Unter dieser Teilbarkeitsbedingung sind die Vorzeichen von a und b egal. Wir geben dieser Bedingung einen eigenen Namen:

Definition 16.8 *Wir nennen zwei Elemente r, s eines Integritätsbereichs R **zueinander assoziiert**, falls $r \mid s$ und $s \mid r$ gelten. In diesem Fall schreiben wir $r \sim s$.*
*Unter der **Assoziiertheitsklasse von r** verstehen wir die Menge $[r] := \{x \in R \mid x \sim r\}$ aller zu r assoziierten Elemente.*

Das nächste Lemma liefert eine Äquivalenz zur Assoziiertheit zweier Elemente:

Lemma 16.9 *Seien R ein Integritätsbereich und $r, s \in R$. Dann gilt $r \sim s$ genau dann, wenn $r = e \cdot s$ mit einer Einheit $e \in R^\times$ ist.*
Assoziierte Elemente unterscheiden sich also nur durch Multiplikation mit einer Einheit. Für jedes $r \in R$ gilt daher $[r] = R^\times \cdot r$.

Beweis.

$\Longrightarrow$ Es gelte $r \mid s$ und $s \mid r$. Dann existieren Elemente $x, y \in R$ mit $rx = s$ und $sy = r$. Gilt $s = 0$, so ist auch $r = 0$ und wir können $r = 1 \cdot s$ schreiben. Sei daher $s \neq 0$. Einsetzen der zweiten in die erste Gleichung liefert $syx = s$. Kürzen durch $s \neq 0$ liefert $yx = 1$ und daher $x, y \in R^\times$.

$\Longleftarrow$ Sei nun $r = e \cdot s$ mit einer Einheit $e \in R^\times$. Durch Multiplikation mit $e^{-1} \in R$ folgt $s = e^{-1}r$. Die erste Gleichung liefert $s \mid r$, die zweite $r \mid s$. Insgesamt folgt $r \sim s$. ■

Beispiel 16.10 (a) Sei R ein Integritätsbereich. Dann gilt $[0] = \{0\}$ und $[1] = R^\times$.

(b) Ein Körper hat genau zwei Assoziiertheitsklassen, nämlich $[0]$ und $[1]$. ※

Für $z \in \mathbb{Z}$ gilt $[z] = \{z, -z\}$ und daher $\mathbb{Z} = [0] \cup [1] \cup [2] \cup \cdots$. Die Assoziiertheitsklassen partitionieren $\mathbb{Z}$ also. Dies ist auch in allgemeinen Integritätsbereichen korrekt. Wie auch in den Beweisen zu 4.4 und 11.4 ist im Wesentlichen zu zeigen, dass zwei Assoziiertheitsklassen entweder gleich oder disjunkt sind. Können Sie den Beweis führen? ⁉

Satz 16.11 *Sei R ein Integritätsbereich. Dann bildet die Menge der Assoziiertheitsklassen eine Partition von R, d.h. es gibt eine Indexmenge I und Vertreter $r_i \in R$ der einzelnen Assoziiertheitsklassen, so dass gilt*

$$R = \dot{\bigcup_{i \in I}} [r_i].$$

Wir formulieren nun 3.1 (b) und die Primeigenschaft aus 3.10 (b) für allgemeine Integritätsbereiche. Wir haben uns in beiden Fällen auf Elemente aus $\mathbb{N} \setminus \{1\}$ beschränkt, also Null und Eins ausgeschlossen. Dies übertragen wir, indem wir nur Ringelemente betrachten, die außerhalb von $[0]$ und $[1]$ liegen. Wir führen für solche Elemente eine neue Sprechweise ein:

Vereinbarung zur Schreibweise 16.12 Sei R ein Integritätsbereich. Wegen 16.10 (a) sind Elemente aus $[0] \cup [1]$ entweder gleich Null oder Einheiten. Wir bezeichnen jedes Element aus R, das nicht in $[0] \cup [1]$ liegt, als **Nicht-Einheit ungleich Null** und kürzen dies mit dem Begriff NEuN ab. ※

Die Primeigenschaft wird nun zu:

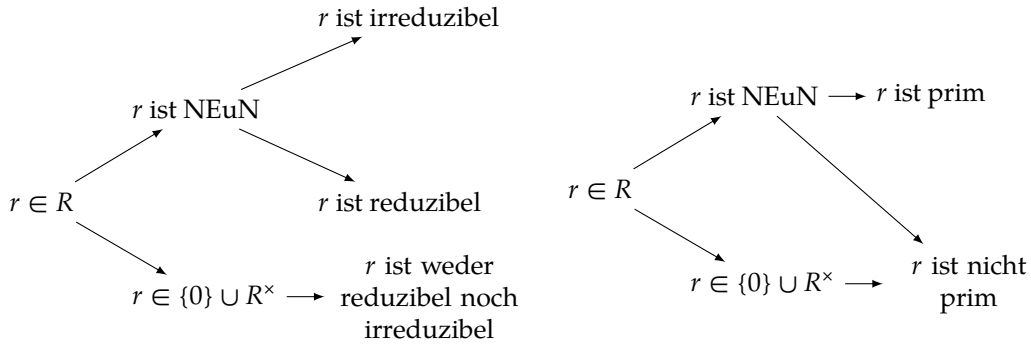
Definition 16.13 *Seien R ein Integritätsbereich und $p \in R$. Wir nennen p **prim**, wenn p eine NEuN ist und für alle $r, s \in R$ gilt: $p \mid rs \Longrightarrow p \mid r$ oder $p \mid s$.*

Aus der Primzahldefinition wird:

Definition 16.14 *Seien R ein Integritätsbereich und $r \in R$. Wir nennen r **irreduzibel**, wenn r eine NEuN ist und jeder Teiler von r in der Menge $[1]$ oder der Menge $[r]$ liegt.*
*Ist r eine NEuN und nicht irreduzibel, so nennen wir r **reduzibel**.*

Bemerkung 16.15 (a) Wie auch in 3.11 lässt sich die Primeigenschaft induktiv auf Produkte beliebiger endlicher Länge ausdehnen. Primelemente sind daher genau diejenigen NEuNen, die mit einem Produkt auch einen Faktor des Produkts teilen.

(b) Durch die beiden obigen Definition werden die Elemente eines Integritätsbereichs R in verschiedene Klassen eingeteilt, nämlich:



Beachten Sie, dass die Begriffe *reduzibel* und *irreduzibel* keine Gegenteile voneinander sind; es gibt Ringelemente, die weder reduzibel noch irreduzibel sind. Beispielsweise ist kein Element eines Körpers reduzibel oder irreduzibel. Innerhalb der Menge der NEuNen sind die Begriffe aber Gegenteile voneinander.

(c) Die Zahl $-2 \in \mathbb{Z}$ ist prim und irreduzibel, aber keine Primzahl. ⁂

Wir geben eine alternative, oft nützlichere Charakterisierung der Irreduzibilität an, die zudem etwas mehr an 16.13 angelehnt ist:

Lemma 16.16 *Seien R ein Integritätsbereich und $r \in R$ eine NEuN. Dann sind äquivalent:*

(a) *r ist irreduzibel.*

(b) *Gilt $r = ab$ für $a, b \in R$, so ist a oder b eine Einheit.*

Irreduzible Elemente sind also nie Produkt zweier Nicht-Einheiten.

Beweis.

(a)$\Longrightarrow$(b) Sei r irreduzibel und zerlegt in der Form $r = ab$ mit $a, b \in R$. Nach 16.14 gilt $a, b \in [1] \cup [r]$. Wir zeigen, dass der Fall $a, b \in [r]$ nicht auftritt. Dann muss $a \in [1] = R^\times$ oder $b \in [1] = R^\times$ gelten, was die Aussage zeigt.

Es gelte $a, b \in [r]$. Dann existieren $e, e' \in R^\times$ mit $a = er$ und $b = e'r$. Es folgt $r = ab = ee'r^2$. Kürzen durch r zeigt $1 = ee'r$ und somit $r \in R^\times$. Dies ist widersprüchlich, denn r ist eine NEuN.

(b)$\Longrightarrow$(a) Sei r beliebig multiplikativ zerlegt in der Form $r = ab$ mit $a, b \in R$. Wegen (b) können wir ohne Einschränkung davon ausgehen, dass $a \in R^\times$ gilt. Dann gilt $a \in [1]$ nach 16.10 (a) und $b = a^{-1}r \in [r]$ nach 16.9. Dies zeigt, dass die Teiler der NEuN r Elemente der Menge $[1] \cup [r]$ sind. r ist also irreduzibel. ■

Wegen 3.10 fallen die Begriffe „irreduzibel“ und „prim“ in $\mathbb{Z}$ zusammen. Dies gilt in allgemeinen Integritätsbereichen nicht. Hier ist „prim“ der stärkere Begriff:

Satz 16.17 *Prime Elemente eines Integritätsbereichs sind stets irreduzibel.*
Kürzer: Aus prim folgt irreduzibel.

Beweis. Das prime Element p des Integritätsbereichs R sei multiplikativ zerlegt in der Form $p = ab$ mit $a, b \in R$. Dann gilt insbesondere $p \mid ab$ und, aufgrund der Prim-Eigenschaft, $p \mid a$ oder $p \mid b$. Wir nehmen ohne Einschränkung den Fall $p \mid a$ an. Dann existiert $x \in R$ mit $px = a$. Es folgt

$$p = ab \overset{a=px}{=} pxb \overset{\text{Kürzen durch } p}{\Longrightarrow} 1 = xb.$$

b ist also eine Einheit von R. Die Irreduzibilität von p folgt aus 16.16 (b). ■

Die Rückrichtung in 16.17 gilt im Allgemeinen nicht:

Beispiel 16.18 Wir betrachten die komplexe Nullstelle $\sqrt{-5} := i \cdot \sqrt{5} \in \mathbb{C}$ des Polynoms $X^2 + 5 \in \mathbb{Z}[X]$ und den Ring $R := \mathbb{Z}[\sqrt{-5}]$. Nach 15.4 (c) ist

$$R = \{a + b \cdot \sqrt{-5} : a, b \in \mathbb{Z}\}. \qquad (\star)$$

R ist als Teilring von $\mathbb{C}$ ein Integritätsbereich. Wir zeigen, dass R irreduzible Elemente enthält, die nicht prim sind, indem wir ein speziell auf Teilringe von $\mathbb{C}$ zugeschnittenes Beweisverfahren, den **Norm-Trick**, benutzen. Hierzu definieren wir die Abbildung

$$N : R \to \mathbb{R}, \qquad r \mapsto |r|^2 = r \cdot \bar{r} = \mathrm{Re}(r)^2 + \mathrm{Im}(r)^2,$$

die man in diesem Kontext oft als **Norm** bezeichnet. (N ist allerdings keine Norm im Sinne der Analysis.) N ist verträglich mit der Multiplikation in R in folgendem Sinne: Für $r, s \in R$ gilt

$$N(rs) = rs \cdot \overline{rs} \overset{\text{Rechnen mit kompl. Konjug.}}{=} rs \cdot \bar{r} \cdot \bar{s} = r\bar{r} \cdot s\bar{s} = N(r) \cdot N(s).$$

Man nennt diese Rechenregel auch die **Multiplikativität der Norm**. Wegen $(\star)$ existieren zu beliebigem $r \in R$ Elemente $a, b \in \mathbb{Z}$ mit $r = a + b\sqrt{-5}$. Daher ist

$$N(r) = N(a + b\sqrt{-5}) = N(a + b\sqrt{5} \cdot i) = a^2 + (b\sqrt{5})^2 = a^2 + 5b^2 \in \mathbb{N}_0.$$

Mit Hilfe der Norm können wir die Einheiten in R charakterisieren, und zwar gilt

$$r \text{ ist eine Einheit von } R \iff N(r) = 1. \qquad (\star\star)$$

$\Longrightarrow$ Ist $r \in R^\times$, so existiert $s \in R^\times$ mit $rs = 1$. Anwendung von N liefert $1 = N(1) = N(rs) = N(r)N(s)$. Wegen $N(r), N(s) \in \mathbb{N}_0$ folgt $N(r) = 1 = N(s)$.

$\Longleftarrow$ Sei nun $N(r) = r \cdot \bar{r} = 1$. Beachten Sie, dass aus $r \in R$ auch $\bar{r} \in R$ folgt. Dann ist aber $\bar{r}$ multiplikativ invers zu r und somit $r \in R^\times$. ⁉

Weiter zeigt die Multiplikativität der Norm, dass für beliebige $r, s \in R$ gilt

$$r \mid s \Longrightarrow N(r) \mid N(s). \qquad (\star\star\star)$$

Mit diesen Vorarbeiten zeigen wir nun, dass das Element $2 \in R$ irreduzibel, aber nicht prim ist:
Offenbar gilt $2 \neq 0$. Wegen $N(2) = 4$ folgt $2 \notin R^\times$ nach $(\star\star)$. Somit ist 2 eine NEuN in R. Wir betrachten nun die in R gültige Gleichung

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

2 ist nicht prim Es gilt $2 \mid (1 + \sqrt{-5}) \cdot (1 - \sqrt{-5})$. Wegen $N(2) = 4$ und $N(1 \pm \sqrt{-5}) = 6$ ist jedoch $N(2) \nmid N(1 \pm \sqrt{-5})$. Nach $(\star\star\star)$ ist somit $2 \nmid 1 \pm \sqrt{-5}$. Das Ringelement 2 teilt ein Produkt, aber keinen der Faktoren und ist somit nicht prim.

2 ist irreduzibel Es gelte $2 = rs$ mit beliebigen $r, s \in R$. Dann gilt

$$4 = N(2) = N(rs) = N(r) \cdot N(s).$$

Da N nach $\mathbb{N}_0$ abbildet, muss $(N(r), N(s)) \in \{(4,1), (2,2), (1,4)\}$ gelten. Allerdings gibt es wegen $N(a + b\sqrt{-5}) = a^2 + 5b^2$ keine Ringelemente mit Norm 2. Somit gilt $N(r) = 1$ oder $N(s) = 1$. Mit $(\star\star)$ und 16.16 (b) folgt, dass 2 irreduzibel ist. ⋇

17. Faktorielle Ringe, Prim-, Haupt- und maximale Ideale

Worum geht es? Wir beschäftigen uns mit *faktoriellen Ringen*, also Integritätsbereichen, in denen eine *eindeutige Primfaktorzerlegung* existiert. Wir definieren für diese Ringe zudem ggT und kgV und zeigen deren Existenz.
Danach führen wir wichtige Ideal-Typen ein und untersuchen Faktorringe genauer. ⁜

Faktorielle Ringe

Mit Hilfe der Begriffe aus der letzten Vorlesung definieren wir, was wir unter einer *eindeutigen Primfaktorzerlegung in Integritätsbereichen* verstehen wollen. Wir starten mit zwei vorbereitenden Resultaten.
Wir zeigen zuerst die Invarianz von Irreduzibilität und Primeigenschaft unter Assoziiertheit:

Lemma 17.1 *Seien R ein Integritätsbereich, $r, s \in R$ Ringelemente und $e \in R^\times$ eine Einheit. Gilt $r \mid s$, so gilt auch $er \mid s$. Aus $r \mid s$ folgt also, dass jedes Element der Assoziiertheitsklasse $[r]$ ein Teiler von s ist.*
Dies liefert insbesondere: Ist $r \in R$ irreduzibel bzw. prim, so ist auch jedes Element aus $[r]$ irreduzibel bzw. prim.

Beweis. Es gelte $r \mid s$. Dann existiert $x \in R$ mit $r \cdot x = s$. Für jede Einheit $e \in R^\times$ ist dann $er \cdot e^{-1}x = s$ und somit $er \mid s$.
Wir zeigen den Insbesondere-Teil nur für irreduzibles r; der Beweis für primes r funktioniert ähnlich.
Seien $r \in R$ irreduzibel, er mit $e \in R^\times$ ein beliebiges zu r assoziiertes Element und $t \in R$ ein Teiler von er. Aus $t \mid er$ folgt nach Multiplikation mit e^{-1}, dass $e^{-1}t \mid r$ gilt. Das Lemma liefert $t \mid r$. Die Irreduzibilität von r zeigt $t \in [1]$ oder $t \in [r] = [er]$. Also ist er irreduzibel. ■ ⁉

Wir zeigen nun, dass Faktorisierungen in Primelemente bis auf Anordnung und Assoziiertheit eindeutig sind:

Satz 17.2 *Seien R ein Integritätsbereich, $m, n \in \mathbb{N}_0$ und $p_1, \dots, p_m, q_1, \dots, q_n \in R$ prim. Ist*

$$p_1 \cdot p_2 \cdots p_m = q_1 \cdot q_2 \cdots q_n,$$

*so folgt $m = n$. Weiter lassen sich die Indizes der Elemente q_i so umbenennen, dass $p_i \sim q_i$ für alle $i \in \{1, \dots, m\}$ gilt. Man sagt, dass die beiden Produkte **bis auf Anordnung und Assoziiertheit übereinstimmen**.*
Kürzer gilt: Lässt sich ein Element $r \in R$ in Primelemente faktorisieren, so stimmen alle solchen Zerlegungen von r bis auf Anordnung und Assoziiertheit überein.
Konvention: Leere Produkte haben den Wert Eins.

Beweis. Wir beweisen die Aussage des Satzes per Induktion nach m.
Für $m = 0$ gilt $1 = q_1 \cdots q_n$. Da die q_i keine Einheiten sind, ist diese Gleichung nur für $n = 0$ per Konvention erfüllt. Die Aussage im Satz gilt dann trivialerweise. Sei die Behauptung nun bereits für $m \in \mathbb{N}_0$ gezeigt. Dann gilt sie auch für $m+1$:
Sei $p_1 \cdots p_m \cdot p_{m+1} = q_1 \cdots q_n$. Da p_{m+1} prim ist, teilt p_{m+1} nach 16.15 (a) eines der q_i, nach Umbenennen ohne Einschränkung q_n. Aus $p_{m+1} \mid q_n$ folgt $q_n = p_{m+1} \cdot e$ mit einer Einheit $e \in R^\times$, da q_n nach 16.17 irreduzibel ist. Kürzen wir in der ursprünglichen Gleichung durch p_{m+1} und setzen wir $\tilde{q_1} := e \cdot q_1$, so erhalten wir

$$p_1 \cdots p_m = \tilde{q_1} \cdot q_2 \cdots q_{n-1}.$$

Nach 17.1 ist auch $\tilde{q_1}$ prim. Aus der Induktionsvoraussetzung ergibt sich, dass $m = n-1$ ist und durch Umbenennen $p_1 \sim \tilde{q_1}$ sowie $p_i \sim q_i$ für alle $i \in \{2, \dots, m\}$ erreichbar ist. Da $\tilde{q_1} \sim q_1$ ist, gilt natürlich auch $p_1 \sim q_1$. Insgesamt haben wir daher $p_i \sim q_i$ für alle $i \in \{1, \dots, m\}$.
Multiplizieren wir die obige Gleichung wieder mit p_{m+1} und fassen e mit p_{m+1} zusammen, so erhalten wir die ursprüngliche Gleichung. Offenbar ist $p_{m+1} \sim p_{m+1}e = q_{m+1}$. Zusammen mit der zuvor gefundenen Umordnung der $q_1, \dots, q_m$ gilt nun $p_i \sim q_i$ für alle $i \in \{1, \dots, m+1\}$. Dies zeigt den Satz. ■

Wir können nun den Begriff der eindeutigen Primfaktorzerlegung definieren:

Definition 17.3 (a) *Seien R ein Integritätsbereich und $r \in R$. Existieren Primelemente $p_1, \dots, p_n \in R$, so dass $r = p_1 \cdots p_n$ gilt, so sagen wir, dass r **primfaktorzerlegbar** ist, und nennen das Produkt $p_1 \cdots p_n$ eine **Primfaktorzerlegung (PFZ) von r**.*

*Wegen 17.2 stimmen alle Primfaktorzerlegungen von r bis auf Anordnung und Assoziiertheit überein. Man spricht daher in obigem Fall (mathematisch ungenau) auch von **der eindeutigen Primfaktorzerlegung von r**.*

(b) *Ein Ring R heißt **faktoriell**, wenn R ein Integritätsbereich ist und jede NEuN aus R primfaktorzerlegbar ist.*

Obige Definition sieht zunächst deutlich anders aus als die eindeutige PFZ in $\mathbb{Z}$ nach 3.12. Wir klären, dass die Unterschiede nicht wesentlich sind:

Bemerkung 17.4 (a) In faktoriellen Ringen R lässt sich jedes Element $r \in R$ mit $r \neq 0$ zerlegen in der Form

$$r = e \cdot p_1 \cdots p_n \qquad \text{mit einer Einheit } e \in R^\times \text{ und Primelementen } p_i \in R,$$

wobei wir, wie üblich, dem leeren Produkt den Wert Eins zuordnen:

Ist r eine Einheit, so erhalten wir obige Darstellung, indem wir $e = r$ und $n = 0$ setzen. Die Wahl der Parameter e und n ist hierbei eindeutig.

Ist r eine NEuN, so setzen wir beispielsweise $e = 1$ und wählen für die Primelemente die nach 17.3 existierende PFZ von r.

Wir erhalten auf diese Weise für alle $r \in R \setminus \{0\}$ eine zu 3.12 analoge Zerlegung von r.

(b) Die starken Eindeutigkeitsresultate aus 3.12 können wir in faktoriellen Ringen allerdings nicht erwarten. Beispielsweise können wir für NEuNen r die Einheit e in der Zerlegung nach (a) frei wählen, denn es gilt

$$r \overset{r \text{ hat PFZ}}{=} p_1 \cdots p_n = e \cdot \underbrace{(e^{-1}p_1)}_{\text{prim nach } 17.1} \cdot p_2 \cdots p_n \qquad \text{mit beliebigem } e \in R^\times.$$

(c) Aus (a) und (b) folgt eine alternative Charakterisierung faktorieller Ringe: Ein Integritätsbereich R ist faktoriell genau dann, wenn jedes $r \in R \setminus \{0\}$ assoziiert zu einem Produkt von Primelementen ist. ⁂ ⁉

Ein wichtiges Ergebnis in faktoriellen Ringen ist, dass dort die Begriffe *prim* und *irreduzibel* zusammenfallen. Dies ist der Grund, warum man in $\mathbb{Z}$ nicht zwischen diesen beiden Eigenschaften unterscheiden muss.

Satz 17.5 *Seien R ein faktorieller Ring und $i \in R$ irreduzibel. Dann ist i prim.*
Zusammen mit 16.17 folgt: In faktoriellen Ringen sind Elemente genau dann irreduzibel, wenn sie prim sind.

Beweis. Sei i primfaktorzerlegt in der Form $i = p_1 \cdots p_n$ mit $n \in \mathbb{N}$. Gilt $n \geq 2$, so ist $i = p_1 \cdot (p_2 \cdots p_n)$ ein Produkt von zwei Nicht-Einheiten, was 16.16 widerspricht. Also gilt $n = 1$. Dann ist $i = p_1$ prim. ■

Beispiel 17.6 (a) $\mathbb{Z}$ ist ein faktorieller Ring.

(b) Jeder Körper ist ein faktorieller Ring. ⁉

(c) Der Integritätsbereich $\mathbb{Z}[\sqrt{-5}]$ ist nicht faktoriell, denn nach 16.18 existieren dort irreduzible Elemente, die nicht prim sind.

Allgemeiner gilt: Ist p eine ungerade Primzahl, so ist der Integritätsbereich $\mathbb{Z}[\sqrt{-p}]$ nicht faktoriell. Dies sieht man, indem man ausnutzt, dass $p + 1$ gerade ist, die Zerlegung

$$p + 1 = 2 \cdot \frac{p+1}{2} = (1 + \sqrt{-p})(1 - \sqrt{-p})$$

betrachtet und bezüglich des Elements 2 ähnlich wie in 16.18 schließt.

(d) Man kann zeigen, dass Polynomringe über faktoriellen Ringen wieder faktoriell sind, vgl. [KM17, Satz 19.5 auf S. 256]. Die Polynomringe $\mathbb{Z}[X]$ und $K[X]$ mit beliebigen Körpern K sind daher faktoriell. ⁂

ggT und kgV

Der ggT-Begriff aus 3.5 lässt sich auf Integritätsbereiche übertragen:

Definition 17.7 *Seien R ein Integritätsbereich und $r_1, \dots, r_k \in R$. Unter einem **größten gemeinsamen Teiler von $r_1, \dots, r_k$** versteht man ein Element $g \in R$, das den folgenden beiden Bedingungen genügt:*

gemeinsamer Teiler *Es gilt $g \mid r_i$ für alle $i \in \{1, \dots, k\}$.*

Maximalität *Ist $t \in R$ ein gemeinsamer Teiler aller r_i, so gilt $t \mid g$.*

Im Allgemeinen muss ein größter gemeinsamer Teiler g von $r_1, \dots, r_k$ nicht existieren. Im Falle der Existenz sind die größten gemeinsamen Teiler von $r_1, \dots, r_k$ aber genau die Elemente der Assoziiertheitsklasse $[g]$; dies folgt aus obiger Maximalitätseigenschaft. ⁉

Jeden größten gemeinsamen Teiler von $r_1, \dots, r_k$ bezeichnen wir (mathematisch ungenau) mit $\operatorname{ggT}(r_1, \dots, r_k)$. Diese Notation ist nur bis auf Assoziiertheit eindeutig.

*Gilt $\operatorname{ggT}(r_1, \dots, r_k) = 1$, so nennen wir die Ringelemente $r_1, \dots, r_k$ **teilerfremd**.*

Bemerkung 17.8 Im Existenzfall folgt wie in 3.7 (b), dass $\operatorname{ggT}(\operatorname{ggT}(r_1, \dots, r_{k-1}), r_k) = \operatorname{ggT}(r_1, \dots, r_k)$ gilt. Die Berechnung des ggT von k Elementen kann also stets auf mehrfache Berechnung des ggT von zwei Elementen zurückgeführt werden. ⁕

In faktoriellen Ringen existieren ggT:

Satz 17.9 *Ist R ein faktorieller Ring, so existiert ein ggT beliebiger Elemente $r_1, \dots, r_k \in R$.*

Beweisskizze. Wegen obiger Bemerkung müssen wir nur zeigen, dass $\operatorname{ggT}(r, s)$ für beliebige $r, s \in R$ existiert.
Gilt $r = 0$ bzw. $s = 0$, so ist $\operatorname{ggT}(r, s) = s$ bzw. $\operatorname{ggT}(r, s) = r$. ⁉
Sei nun $r \neq 0 \neq s$. Dann lassen sich r und s in der in 17.4 (a) beschriebenen Form zerlegen. Durch Wahl geeigneter führender Einheiten und Exponenten aus $\mathbb{N}_0$ können wir in den Zerlegungen dieselben Primelemente erreichen, also schreiben

$$r = e_1 \cdot \prod_{i=1}^{n} p_i^{a_i} \qquad \text{bzw.} \qquad s = e_2 \cdot \prod_{i=1}^{n} p_i^{b_i} \qquad \text{mit } e_1, e_2 \in R^\times,\ n, a_i, b_i \in \mathbb{N}_0,$$

wobei die p_i paarweise nicht-assoziiert seien. Dann ist durch $\prod_{i=1}^{n} p_i^{\min(a_i, b_i)}$ ein ggT von r und s gegeben. ⁉ ■

Auch die Definition des kgV aus den Übungen lässt sich übertragen: → Übung

Definition 17.10 *Seien R ein Integritätsbereich und $r_1, \dots, r_n \in R$. Unter einem **kleinsten gemeinsamen Vielfachen von $r_1, \dots, r_n$** versteht man ein Element $k \in R$, das den folgenden beiden Bedingungen genügt:*

gemeinsames Vielfaches *Es gilt $r_i \mid k$ für alle $i \in \{1, \dots, n\}$.*

Minimalität *Ist $v \in R$ ein gemeinsames Vielfaches aller r_i, so gilt $k \mid v$.*

Im Allgemeinen ist ein kleinstes gemeinsames Vielfaches nicht eindeutig bestimmt. Wegen 17.1 und obiger Minimalitätseigenschaft sind im Falle ihrer Existenz aber alle kleinsten gemeinsamen Vielfachen zueinander assoziiert. ⁉
Jedes kleinste gemeinsame Vielfache von $r_1, \dots, r_n$ bezeichnen wir (mathematisch ungenau) mit $\mathrm{kgV}(r_1, \dots, r_n)$. Diese Notation ist nur bis auf Assoziiertheit eindeutig.

Bemerkung 17.11 Im Falle der Existenz gilt $\mathrm{kgV}(\mathrm{kgV}(r_1, \dots, r_{n-1}), r_n) = \mathrm{kgV}(r_1, \dots, r_n)$; dies sieht man wie in den Übungen. Die Berechnung des kgV von n Elementen kann also stets auf mehrfache Berechnung des kgV von zwei Elementen zurückgeführt werden. ⁕ → Übung

In faktoriellen Ringen existieren kgV:

Satz 17.12 *Ist R ein faktorieller Ring, so existiert ein kgV beliebiger Elemente $r_1, \dots, r_n \in R$.*

Beweis. Wir gehen wie im Beweis zu 17.9 vor und benutzen die dortigen Bezeichnungen.
Gilt $r = 0$ oder $s = 0$, so ist $\mathrm{kgV}(r, s) = 0$.
Für $r \neq 0 \neq s$ ist ein kgV von r und s durch $\prod_{i=1}^{n} p_i^{\max(a_i, b_i)}$ gegeben. ■ ⁉

Bemerkung 17.13 Man kann in faktoriellen Ringen zwar die Existenz von ggT und kgV zeigen, allerdings kann man diese im Allgemeinen nicht effizient berechnen. Dies liegt daran, dass keine schnellen Algorithmen für Primfaktorzerlegungen bekannt sind, man also die Zerlegung nach 17.4 (a) nicht ausrechnen kann. (Nicht einmal über $\mathbb{Z}$ kennt man schnelle PFZ-Algorithmen.) ⁕

Mehr zu Idealen

Nach 5.11 (c) ist der Schnitt von Idealen wieder ein Ideal. Analog zu 2.11 können wir daher ein Ideal-Erzeugnis definieren: Seien R ein Ring und $A \subseteq R$ eine Teilmenge von R. Dann bezeichnen wir mit (A) das (bezüglich Mengeninklusion) kleinste Ideal von R, das A als Teilmenge enthält.
Ist $A = \{a_1, \dots, a_n\}$ eine endliche Menge, so gilt

$$(A) = (a_1, \dots, a_n) = a_1R + a_2R + \cdots + a_nR = \Big\{\sum_{i=1}^{n} a_i r_i \mid r_i \in R\Big\}.$$

Dies sieht man ähnlich wie im Beweis zu 2.13: Man zeigt, dass die rechte Menge ein Ideal von R ist, das alle der Elemente a_i enthält. Danach überlegt man sich, dass jedes Element der rechten Menge in $(a_1, \dots, a_n)$ enthalten sein muss, und erhält so die behauptete Gleichheit.
Besonders interessant sind die Ideale, die von nur einem Element erzeugt werden:

Definition 17.14 *Sei R ein Ring. Wir nennen ein Ideal $\mathfrak{a} \trianglelefteq R$ ein **Hauptideal**, wenn ein $a \in R$ existiert, so dass $\mathfrak{a} = (a)$ gilt. Jedes $a \in R$ mit $(a) = \mathfrak{a}$ nennen wir einen **Erzeuger von** $\mathfrak{a}$.*
Die Hauptideale von R sind genau die Teilmengen von R der Form aR mit $a \in R$.

Der Umgang mit Hauptidealen ist besonders angenehm, weil diese durch Angabe eines einzigen Elements bereits vollständig beschrieben sind und sich Eigenschaften des Ideals oft in Eigenschaften dieses Elements übersetzen:

Lemma 17.15 *Seien R ein Integritätsbereich und $a, b \in R$. Dann gelten:*

(a) *Genau dann gilt $a \mid b$, wenn $(b) \subseteq (a)$ ist.*
Man sagt auch kürzer: Teilen heißt Umfassen, vgl. 3.2 (e).

(b) *Genau dann gilt $(a) = (b)$, wenn a und b assoziiert sind.*
Die Erzeuger eines Hauptideals bilden also eine Assoziiertheitsklasse.

Beweis.

zu (a) Es gilt: $a \mid b \iff \exists r \in R : ar = b \iff b \in (a) \iff (b) \subseteq (a)$.

zu (b) Es gilt: $(a) = (b) \iff (a) \subseteq (b) \wedge (b) \subseteq (a) \overset{\text{(a)}}{\iff} b \mid a \wedge a \mid b \overset{16.8}{\iff} a \sim b.$ ■

Wir stellen zwei wichtige Typen von Idealen vor:

Definition 17.16 *Sei R ein Ring.*

(a) *Ein Ideal $\mathfrak{p} \trianglelefteq R$ heißt **Primideal**, wenn $\mathfrak{p} \neq R$ ist und für alle $a, b \in R$ gilt:* $\mathfrak{p}$ Fraktur-p

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

(Diese Eigenschaft ist uns in $\mathbb{Z}$ bereits in 3.10 (c) begegnet.)

(b) *Ein Ideal $\mathfrak{m} \trianglelefteq R$ heißt **maximales Ideal**, wenn $\mathfrak{m} \neq R$ ist und R das einzige Ideal von R ist, das eine echte Obermenge von $\mathfrak{m}$ ist, d. h. wenn aus $\mathfrak{a} \trianglelefteq R$ mit $\mathfrak{m} \subsetneq \mathfrak{a}$ stets $\mathfrak{a} = R$ folgt.* $\mathfrak{m}$ Fraktur-m

Beispiel 17.17 (a) Die maximalen Ideale in $\mathbb{Z}$ sind genau die Ideale (p) mit $p \in \mathbb{P}$.

(b) Das Nullideal ist genau in nullteilerfreien Ringen ein Primideal. ※

Mit Hilfe der Idealtypen aus der obigen Definition lässt sich die Struktur von Faktorringen klassifizieren:

Satz 17.18 *Seien R ein Ring und $\mathfrak{a} \trianglelefteq R$ ein Ideal von R. Dann gelten:*

(a) *$R/\mathfrak{a}$ ist ein Integritätsbereich genau dann, wenn $\mathfrak{a}$ ein Primideal ist.*

(b) *$R/\mathfrak{a}$ ist ein Körper genau dann, wenn $\mathfrak{a}$ ein maximales Ideal ist.*

(c) *Ist $\mathfrak{a}$ ein maximales Ideal, so ist $\mathfrak{a}$ auch ein Primideal.*

Beweis.

zu (a) Integritätsbereiche sind nullteilerfreie Ringe mit $1 \neq 0$. Wir übersetzen zunächst die Nullteilerfreiheit von $R/\mathfrak{a}$ in Eigenschaften von $\mathfrak{a}$. Es gilt:

$$\begin{aligned} R/\mathfrak{a} \text{ nullteilerfrei} &\iff \forall \overline{r}, \overline{s} \in R/\mathfrak{a} : \ \overline{r} \cdot \overline{s} = \overline{0} \Longrightarrow \overline{r} = \overline{0} \text{ oder } \overline{s} = \overline{0} \\ &\iff \forall r, s \in R : \ rs + \mathfrak{a} = \mathfrak{a} \Longrightarrow r + \mathfrak{a} = \mathfrak{a} \text{ oder } s + \mathfrak{a} = \mathfrak{a} \\ &\iff \forall r, s \in R : \ rs \in \mathfrak{a} \Longrightarrow r \in \mathfrak{a} \text{ oder } s \in \mathfrak{a}. \end{aligned}$$

Ferner gilt in $R/\mathfrak{a}$ genau dann $\overline{1} \neq \overline{0}$, wenn $1 \notin \mathfrak{a}$ ist. Dies ist nach 5.12 genau dann der Fall, wenn $\mathfrak{a} \neq R$ ist. Insgesamt folgt die Aussage in (a). ?

zu (b) Ist $R/\mathfrak{a}$ ein Körper, so gilt $\overline{1} \neq \overline{0}$. Wie oben folgt die Äquivalenz dieser Bedingung zu $\mathfrak{a} \neq R$. Nun übersetzen wir die multiplikative Invertierbarkeit eines Elements aus $R/\mathfrak{a}$ in eine Eigenschaft von $\mathfrak{a}$. Es gilt:

$$\begin{aligned} \overline{0} \neq \overline{r} \in R/\mathfrak{a} \text{ mult. inv.bar} &\iff \exists s \in R/\mathfrak{a} : \ \overline{r} \cdot \overline{s} = \overline{1} \\ &\iff \exists s \in R : \ rs + \mathfrak{a} = 1 + \mathfrak{a} \\ &\iff \exists s \in R : \ rs - 1 \in \mathfrak{a} \\ &\overset{(\star)}{\iff} 1 \in (r, \mathfrak{a}) \overset{5.12}{\iff} (r, \mathfrak{a}) = R. \end{aligned}$$

Zu $(\star)$: Gilt $rs-1 \in \mathfrak{a}$, so existiert $a \in \mathfrak{a}$ mit $rs-1 = a$, also mit $1 = rs-a$. Somit ist $1 \in (r, a)$, und wegen $(r, a) \subseteq (r, \mathfrak{a})$ folgt auch $1 \in (r, \mathfrak{a})$. Gilt umgekehrt $1 \in (r, \mathfrak{a}) = (r) + \mathfrak{a}$, so existieren $s \in R$ und $a \in \mathfrak{a}$ mit $1 = rs + a$, also mit $rs - 1 = -a \in \mathfrak{a}$.

Wegen $\mathfrak{a} \neq R$ ist $\mathfrak{a}$ maximal genau dann, wenn $(\mathfrak{a}, r) = R$ gilt für alle $r \in R \setminus \mathfrak{a}$. Dies ist genau dann der Fall, wenn für alle $r \in R \setminus \mathfrak{a}$ gilt, dass $\overline{r}$ in $R/\mathfrak{a}$ multiplikativ invertierbar ist. Dies ist aber äquivalent dazu, dass $R/\mathfrak{a}$ ein Körper ist, denn die Bedingung $r \in R \setminus \mathfrak{a}$ beschreibt genau die Aussage $\overline{r} \neq \overline{0}$.

zu (c) Ist $\mathfrak{a}$ maximal, so ist $R/\mathfrak{a}$ nach (b) ein Körper. Da Körper stets auch Integritätsbereiche sind, ist $R/\mathfrak{a}$ ein Integritätsbereich. Also ist $\mathfrak{a}$ nach (a) ein Primideal. ■

Für Hauptideale lässt sich die Primideal-Eigenschaft einfach charakterisieren:

Satz 17.19 *Seien R ein Integritätsbereich und $a \in R$ mit $a \neq 0$. Dann ist (a) genau dann ein Primideal, wenn a prim ist.*

Beweis. Für $a \neq 0$ gilt

$$\begin{aligned} (a) \text{ ist Primideal} &\overset{17.16\,(a)}{\iff} (a) \neq R \text{ und } \forall r, s \in R : \ rs \in (a) \Longrightarrow r \in (a) \text{ oder } s \in (a) \\ &\iff a \notin R^\times \text{ und } \forall r, s \in R : \ a \mid rs \Longrightarrow a \mid r \text{ oder } a \mid s \\ &\overset{16.13}{\iff} a \text{ ist prim.} \end{aligned}$$

■

Eine Charakterisierung für die Maximalität eines Hauptideals gibt es in allgemeinen Integritätsbereichen nicht; zum Nachweis der Maximalität eines Ideals müssen nämlich auch Nicht-Hauptideale betrachtet werden. Man kann aber das folgende schwächere Resultat beweisen: ⁉

Satz 17.20 *Seien R ein Integritätsbereich und $a \in R$ mit $a \neq 0$. Dann sind äquivalent:*

(a) *Das einzige **Hauptideal**, das eine echte Obermenge von (a) ist, ist $(1) = R$.*

(b) *a ist irreduzibel.*

Beweis.

(a)$\Longrightarrow$(b) Gilt (a), so sind Teiler von a wegen 17.15 assoziiert zu Eins oder zu a. Da a eine NEuN ist, folgt die Irreduzibilität von a. ⁉

(b)$\Longrightarrow$(a) Gilt (b), so sind Teiler von a assoziiert zu Eins oder zu a. Nach 17.15 sind daher R und (a) die einzigen Hauptideale, die (a) enthalten. Somit folgt (a). ■

18. Hauptideal- und euklidische Ringe

Worum geht es? Wir lernen zwei weitere Ringtypen kennen, den *Hauptidealring* und den *euklidischen Ring*. Speziell euklidische Ringe verhalten sich aus algebraischer Sicht wie $\mathbb{Z}$: Fast alle Resultate aus Vorlesung 3 gelten auch in euklidischen Ringen.
Wir beenden diese Vorlesung mit einer Übersichtsseite über die verschiedenen Ringtypen. ※

Hauptidealringe

Definition 18.1 *Unter einem **Hauptidealring** verstehen wir einen Integritätsbereich, dessen sämtliche Ideale Hauptideale sind: Zu jedem Ideal $\mathfrak{a}$ eines Hauptidealrings existiert ein Ringelement a, so dass $\mathfrak{a} = (a)$ gilt.*

Wir haben in 17.19 und 17.20 Eigenschaften von Hauptidealen in Eigenschaften ihrer Erzeuger übersetzt. Wir haben hierbei stets vorausgesetzt, dass das betrachtete Hauptideal nicht das Nullideal ist. Aus diesen Resultaten folgern wir nun Aussagen über Hauptidealringe. Beachten Sie, dass die Nicht-Nullideal-Voraussetzung auch im Folgenden stets eine Rolle spielt.

In Hauptidealringen lassen sich maximale Ideale charakterisieren; die Problematik, die in der Vorbemerkung zu 17.20 angesprochen wird, tritt nämlich nicht auf.

Satz 18.2 *Ein Ideal $(a) \neq (0)$ eines Hauptidealrings R ist genau dann maximal, wenn a irreduzibel ist.*

Beweis. Nach 17.20 ist a genau dann irreduzibel, wenn R das einzige Hauptideal ist, das eine echte Obermenge von (a) ist. Da R ein Hauptidealring ist, heißt dies, dass R das einzige Ideal ist, das (a) echt enthält. Dies bedeutet, dass (a) ein maximales Ideal ist. ■

Beispiel 18.3 (a) Aus 17.19 und der Nullteilerfreiheit folgt, dass ein Ideal (a) eines Hauptidealrings genau dann prim ist, wenn a prim ist oder $a = 0$ gilt.

(b) Das Nullideal ist in einem Hauptidealring R genau dann maximal, wenn R keine irreduziblen Elemente besitzt. ※

Aus 18.2 folgt, dass in Hauptidealringen die Begriffe *prim* und *irreduzibel* zusammenfallen:

Korollar 18.4 *Seien R ein Hauptidealring und $i \in R$ irreduzibel. Dann ist i prim.*
Zusammen mit 16.17 folgt: In Hauptidealringen sind Elemente genau dann irreduzibel, wenn sie prim sind.

Beweis. Nach 18.2 ist $(i) \neq (0)$ maximal und nach 17.18 (c) ein Primideal. 17.19 zeigt, dass i prim ist. ■

Aus 18.4 und den Charakterisierungen 17.19 bzw. 18.2 der Erzeuger von Prim- und maximalen Idealen folgt:

Korollar 18.5 *Ein nicht-triviales Ideal eines Hauptidealrings ist genau dann maximal, wenn es ein Primideal ist.*

Hauptidealringe erfüllen die folgende *aufsteigende Kettenbedingung für Ideale*. Diese auf Emmy Noether zurückgehende Bedingung taucht an einigen Stellen in der Ringtheorie auf und ist die Grundlage für viele Beweise.

Lemma 18.6 *Seien R ein Hauptidealring und $\mathfrak{a}_1, \mathfrak{a}_2, \mathfrak{a}_3, \ldots \trianglelefteq R$ eine **aufsteigende Kette von Idealen von R**, d.h. es gelte $\mathfrak{a}_1 \subseteq \mathfrak{a}_2 \subseteq a_3 \subseteq \cdots$. Dann sind fast alle der $\mathfrak{a}_i$ identisch, d.h. es existiert ein Grenzindex $N \in \mathbb{N}$, so dass $\mathfrak{a}_n = \mathfrak{a}_N$ für alle $n \geq N$ gilt.*
Man sagt oft kürzer: In Hauptidealringen werden aufsteigende Ketten von Idealen stationär.

Beweisskizze. Wir setzen $\mathfrak{a} := \bigcup_{i \in \mathbb{N}} \mathfrak{a}_i$.

$\mathfrak{a}$ ist ein Ideal Wir zeigen nur, dass $\mathfrak{a}$ additiv abgeschlossen ist. Die restlichen Aussagen beweist man mit derselben Technik. Seien $r, s \in \mathfrak{a}$. Da die $\mathfrak{a}_i$ eine aufsteigende Kette bilden, existiert ein Index $m \in \mathbb{N}$ mit $r, s \in \mathfrak{a}_m$. Es gilt $r + s \in \mathfrak{a}_m$, denn $\mathfrak{a}_m$ ist ein Ideal von R. Daher ist auch $r + s \in \mathfrak{a}$. ?

Idealkette wird stationär Da R ein Hauptidealring ist, existiert ein $a \in R$ mit $(a) = \mathfrak{a}$. Dieses $a \in \mathfrak{a}$ liegt in einem der Ideale $\mathfrak{a}_i$, beispielsweise in $\mathfrak{a}_N$ mit $N \in \mathbb{N}$. Da die Idealkette aufsteigt, gilt $a \in \mathfrak{a}_n$ für alle $n \geq N$. Wegen $(a) = \mathfrak{a}$ folgt $\mathfrak{a} \subseteq \mathfrak{a}_n$ für diese n. Da aber auch $\mathfrak{a}_n \subseteq \mathfrak{a}$ gilt, haben wir $\mathfrak{a}_n = \mathfrak{a}$ für alle $n \geq N$. Die Idealkette wird also stationär. ■

Mit Hilfe der aufsteigenden Kettenbedingung können wir zeigen, dass Hauptidealringe faktoriell sind:

Satz 18.7 *Hauptidealringe sind faktoriell.*

Beweis. Sei R ein Hauptidealring. Wir müssen zeigen, dass sich jede NEuN aus R als Produkt von Primelementen schreiben lässt. Hierzu betrachten wir die Menge

$$M := \{(a) \trianglelefteq R \mid a \in R \text{ ist eine NEuN und nicht Produkt von Primelementen}\}$$

aller Ideale von R, die von nicht-primfaktorzerlegbaren NEuNen erzeugt werden. Wir zeigen im Folgenden, dass M leer ist. Dies liefert die Behauptung.

Nicht-leeres M enthält maximales Element (m) Sei $M \neq \emptyset$. Wir zeigen, dass ein Element $(m) \in M$ existiert, so dass $(m) \subseteq (a) \Longrightarrow (m) = (a)$ für alle $(a) \in M$ gilt. Es gibt also keine Elemente aus M, die (m) als *echte* Teilmenge enthalten.

Angenommen, M enthielte kein solches Element. Sei $\mathfrak{a}_1 \in M$ beliebig. Dann ist $\mathfrak{a}_1$ nicht maximal. Wir finden daher $\mathfrak{a}_2 \in M$ mit $\mathfrak{a}_1 \subsetneq \mathfrak{a}_2$. Derselbe Schluss liefert $\mathfrak{a}_3 \in M$ mit $\mathfrak{a}_2 \subsetneq \mathfrak{a}_3$. Induktiv erhalten wir auf diese Weise eine aufsteigende Kette von Idealen, die nicht stationär wird. Dies widerspricht 18.6 und zeigt, dass M im Falle $M \neq \emptyset$ ein maximales Element enthält.

Maximale Elemente in M sind widersprüchlich Wir zeigen, dass die Existenz maximaler Elemente in M widersprüchlich ist. Sei hierzu $(m) \in M$ ein maximales Element aus M.

m ist nicht irreduzibel; ansonsten wäre m nach 18.4 prim und damit primfaktorzerlegbar. Dann wäre nach Definition von M aber $(m) \notin M$.

Also ist m reduzibel. Es existieren somit NEuNen $r, s \in R$ mit $m = rs$. Es gilt $(m) \subsetneq (r)$ und $(m) \subsetneq (s)$. Die Maximalität von (m) zeigt $(r), (s) \notin M$. Somit sind r und s primfaktorzerlegbar. Wir können also schreiben $r = \prod_i p_i$ und $s = \prod_j q_i$ mit Primelementen $p_i, q_j \in R$. Dann ist aber auch $m = rs = \prod_i p_i \cdot \prod_j q_j$ ein Produkt von Primelementen, was $(m) \notin M$ zeigt.

Insgesamt folgt $(m) \notin M$ für jedes maximale Element $(m) \in M$. Dieser Widerspruch zeigt, dass M kein maximales Element enthält, was $M = \emptyset$ liefert. ■

Aus diesem Resultat folgt, dass in Hauptidealringen ggT und kgV existieren. Tatsächlich gilt sogar das Lemma von Bézout, vgl 3.8. Sein Beweis ist beinahe wörtlich derselbe wie der Beweis von 3.6.

Satz 18.8 (Bézout) *Seien R ein Hauptidealring und $r_1, \dots, r_k \in R$ beliebig. Sei g ein Element von R, so dass $(r_1, \dots, r_k) = (g)$ gelte. Dann ist g ein ggT der r_i.*
Ferner ist g eine R-Linearkombination der r_i, d.h. es existieren $\lambda_i \in R$, so dass $g = \sum_{i=1}^{k} \lambda_i r_i$ erfüllt ist.

Beweis. Nach Voraussetzung gilt $(r_1, \dots, r_k) = (g)$. Dann liegt jedes der r_i in (g) und ist somit ein Vielfaches von g. Dies zeigt, dass g ein gemeinsamer Teiler aller r_i ist.
Sei nun $t \in R$ ein weiterer gemeinsamer Teiler der r_i. Da alle r_i Vielfache von t sind, folgt $r_i \in (t)$ und somit $(r_1, \dots, r_k) \subseteq (t)$, also $(g) \subseteq (t)$. Es folgt $t \mid g$. Damit sind die Bedingungen aus 17.7 für g nachgewiesen: g ist also ein ggT der r_i.
Die Darstellung von g als R-Linearkombination folgt aus der Darstellung des Idealerzeugnisses auf Seite 120. ■

Beispiel 18.9 (a) $\mathbb{Z}$ und jeder Körper K sind Hauptidealringe.

(b) Der Ring $\mathbb{Z}[X]$ ist nach 17.6 (d) faktoriell. Allerdings ist er kein Hauptidealring:

Wir betrachten das Ideal $(2, X) \trianglelefteq \mathbb{Z}[X]$; dieses ist eine Obermenge des Ideals (2), und zwar eine *echte* Obermenge wegen $X \in (2, X)$ und $X \notin (2)$.

Weiter ist $(2, X) \neq (1)$; denn ansonsten gäbe es $a, b \in \mathbb{Z}[X]$ mit $1 = 2a + bX$. Setzen wir für X den Wert Null ein, so folgt, weil Einsetzen ein Homomorphismus ist, der Widerspruch $1 = 2 \cdot a(0) \in 2\mathbb{Z}$.

Das Element $2 \in \mathbb{Z}[X]$ ist irreduzibel, denn die Zerlegung $2 = rs$ mit $r, s \in \mathbb{Z}[X]$ liefert $r, s \in \mathbb{Z}$ aufgrund der Gradformel. Daher ist $r = \pm 1$ oder $s = \pm 1$.

Insgesamt haben wir gezeigt, dass $(2) \trianglelefteq \mathbb{Z}[X]$ kein maximales Ideal ist, obwohl es von einem irreduziblen Element erzeugt wird. Dies ist nach 18.2 in Hauptidealringen unmöglich. ※

Euklidische Ringe

Die nächste Definition stellt die in den ganzen Zahlen verfügbare Division mit Rest nach. Beachten Sie, dass wir keine Eindeutigkeit für die Elemente q und r fordern.

Definition 18.10 *Wir nennen einen Integritätsbereich R einen **euklidischen Ring**, wenn eine **Bewertung** $\beta : R \setminus \{0\} \to \mathbb{N}_0$ existiert, bezüglich derer eine **Division mit Rest** in folgendem Sinne möglich ist:*
Zu beliebigen $a, b \in R$ mit $b \neq 0$ existieren $q, r \in R$, so dass $a = b \cdot q + r$ gilt und entweder $r = 0$ oder $\beta(r) < \beta(b)$ ist.

Das für uns wichtigste Resultat über euklidische Ringe ist:

Satz 18.11 *Jeder euklidische Ring ist ein Hauptidealring (und daher faktoriell).*

Beweis. **(vgl. Beweis zu 3.4)** Seien R ein euklidischer Ring mit Bewertung β und $\mathfrak{a} \trianglelefteq R$ ein Ideal von R. Ziel des Beweises ist es, einen Erzeuger für $\mathfrak{a}$ zu finden. Im Fall $\mathfrak{a} = \{0\}$ können wir $0 \in R$ als Erzeuger wählen. Sei daher für das Folgende $\mathfrak{a} \neq \{0\}$.
Da β nach $\mathbb{N}_0$ abbildet, existiert ein Element $b \in \mathfrak{a} \setminus \{0\}$ mit minimaler Bewertung. Wegen $b \in \mathfrak{a}$ folgt $(b) \subseteq \mathfrak{a}$.
Wir zeigen nun die umgekehrte Inklusion $\mathfrak{a} \subseteq (b)$ und weisen b auf diese Weise als Erzeuger von $\mathfrak{a}$ nach. Sei hierzu $a \in \mathfrak{a}$ beliebig. Da $b \neq 0$ ist, können wir a mit Rest durch b teilen und erhalten $q, r \in R$ mit $a = qb + r$ und $r = 0$ oder $\beta(r) < \beta(b)$.
Die Idealeigenschaften von $\mathfrak{a}$ zeigen, dass $r = a - qb \in \mathfrak{a}$ ist. Die Minimalität von $\beta(b)$ zeigt die Unmöglichkeit von $\beta(r) < \beta(b)$. Es folgt $r = 0$ und somit $a = qb$, also $a \in (b)$. Dies liefert $\mathfrak{a} \subseteq (b)$. ∎

Der nächste Satz klassifiziert die euklidischen Polynomringe:

Satz 18.12 *Für einen Integritätsbereich R sind äquivalent:*

(a) *R ist ein Körper.*

(b) *$R[X]$ ist ein euklidischer Ring.*

(c) *$R[X]$ ist ein Hauptidealring.*

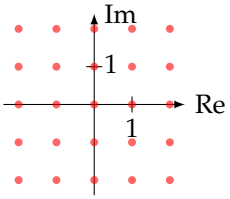
Beweis. Die Aussage (a)$\Longrightarrow$(b) folgt aus 15.17; die Bewertung β, die $R[X]$ zum euklidischen Ring macht, ist für $f \in R[X]$ mit $f \neq 0$ gegeben durch $\beta(f) := \deg f$. Die Aussage (b)$\Longrightarrow$(c) folgt aus 18.11. Zu zeigen ist daher nur noch (c)$\Longrightarrow$(a):
Seien $R[X]$ ein Hauptidealring und $a \in R \setminus \{0\}$ beliebig. Wir müssen zeigen, dass a invertierbar ist. Hierzu betrachten wir das Ideal (a, X), setzen $g := \mathrm{ggT}(a, X)$ und schließen ähnlich wie in 18.9 (b).
Da $a \in R$ ist und daher $\deg a = 0$ gilt, folgt $\deg g \leq 0$, also $g \in R$. Zudem ist $g \mid X$. Betrachten von Leitkoeffizienten liefert $g \mid 1$. Daher ist g eine Einheit in R. Somit ist $(a, X) = (g) = (1)$. Bézout zeigt, dass $\lambda_1, \lambda_2 \in R[X]$ existieren mit $1 = \lambda_1 \cdot a + \lambda_2 \cdot X$. Setzen wir für X den Wert Null ein, so erhalten wir $1 = \lambda_1(0) \cdot a$, was $a \in R^\times$ zeigt. Dies beendet den Beweis. ∎

Beispiel 18.13 (a) Wegen 3.3 ist $\mathbb{Z}$ euklidisch; als Bewertung kann $\beta(z) := |z|$ für alle $z \in \mathbb{Z} \setminus \{0\}$ gewählt werden. ⁉

(b) Nach 18.12 ist $K[X]$ für jeden Körper K ein euklidischer Ring. Als Bewertung wählt man $\beta(f) := \deg f$ für alle $f \in K[X] \setminus \{0\}$. Auf diese Weise ergibt sich als Division mit Rest gerade die aus der Schule bekannte **Polynomdivision mit Rest**.

(c) Der Ring $\mathbb{Z}\left[\frac{1}{2}(1+\sqrt{-19})\right]$ ist ein Hauptidealring, aber nicht euklidisch. Wir führen den länglichen Beweis dieser Aussage nicht und verweisen auf [Wil73].

(d) Wir zeigen mit Hilfe des Norm-Tricks aus 16.18, dass der Ring $\mathbb{Z}[i]$ euklidisch ist; das Element $i \in \mathbb{C}$ bezeichnet hierbei die imaginäre Einheit.



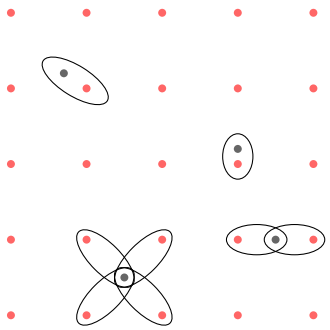
Nach 15.4 (b) gilt $\mathbb{Z}[i] = \{x + y \cdot i \mid x, y \in \mathbb{Z}\} = \mathbb{Z} + i\mathbb{Z}$.
Betrachten wir die Menge $\mathbb{Z}[i]$ in der Gaußschen Zahlenebene, so entsteht das linke Bild: Genau die Punkte mit ganzzahligen Koordinaten gehören zu $\mathbb{Z}[i]$; wir haben sie rot eingezeichnet.

Wir betrachten die Norm

$$N : \mathbb{Z}[i] \to \mathbb{N}_0, \qquad r = x + yi \mapsto |r|^2 = r \cdot \bar{r} = x^2 + y^2,$$

definieren die Bewertung $\beta := N|_{R\setminus\{0\}}$ als Einschränkung der Norm auf $R \setminus \{0\}$ und zeigen, dass $\mathbb{Z}[i]$ mit dieser Bewertung zum euklidischen Ring wird:

Seien $a, b \in \mathbb{Z}[i]$ mit $b \neq 0$ beliebig gegeben. Wir müssen $q, r \in \mathbb{Z}[i]$ finden, so dass $a = bq + r$ ist und für r entweder $r = 0$ oder $\beta(r) < \beta(b)$ gilt. Hierzu vergessen wir zunächst die Ringstruktur und berechnen in $\mathbb{C}$ den Quotienten a/b. Nun definieren wir q als ein Ringelement mit minimalem euklidischen Abstand zu a/b:



Sie sehen links wieder die Gaußsche Zahlenebene mit den roten Ringelementen. Die schwarzen Punkte sind Beispiele für die Quotienten a/b. Beachten Sie, dass a/b irgendeine komplexe Zahl ist; typischerweise gilt $a/b \notin \mathbb{Z}[i]$.
Für q können wir jedes Ringelement wählen, das einen minimalen Abstand zum jeweiligen schwarzen Punkt hat. Links sind die möglichen Kandidaten für q und das jeweils betrachtete Element a/b zusammen eingekreist. Im Allgemeinen ist q nicht eindeutig durch a/b festgelegt; Eindeutigkeit haben wir in 18.10 aber auch nicht gefordert.

Der größte euklidische Abstand zwischen q und a/b tritt auf, wenn a/b exakt in der Mitte zwischen vier roten Punkten liegt, also wenn $a/b \in \frac{1}{2} + \mathbb{Z} + i(\frac{1}{2} + \mathbb{Z})$ ist. ⁉
In diesem Fall gilt

$$|a/b - q| = \sqrt{\left(\frac{1}{2}\right)^2 + \left(\frac{1}{2}\right)^2} = \sqrt{\frac{1}{2}} \qquad \text{und daher} \qquad N(a/b - q) = |a/b - q|^2 = \frac{1}{2}.$$

Aus der Beziehung $a = bq+r$ erhalten wir $r = a-bq$. Wir zeigen nun, dass entweder $r = 0$ oder $\beta(r) < \beta(b)$ gilt:

Im Fall $a/b \in \mathbb{Z}[i]$ folgt $q = a/b$ und daher $r = 0$.

Im Fall $a/b \notin \mathbb{Z}[i]$ folgt $q \neq a/b$ und daher $r \neq 0$. Dann ist

$$\begin{aligned} \beta(r) &\overset{\text{Def. } \beta}{=} N(r) = N(a-bq) = N(b \cdot a/b - bq) = N(b \cdot (a/b - q)) \\ &\overset{(\star)}{=} N(b) \cdot N(a/b - q) \overset{(\star\star)}{\leq} \frac{1}{2} \cdot N(b) \overset{N(b)>0}{<} N(b) \overset{\text{Def. } \beta}{=} \beta(b). \end{aligned}$$

(In $(\star)$ haben wir die Multiplikativität der Norm ausgenutzt, in $(\star\star)$ die oben gezeigte Abschätzung $N(a/b - q) \leq \frac{1}{2}$.)

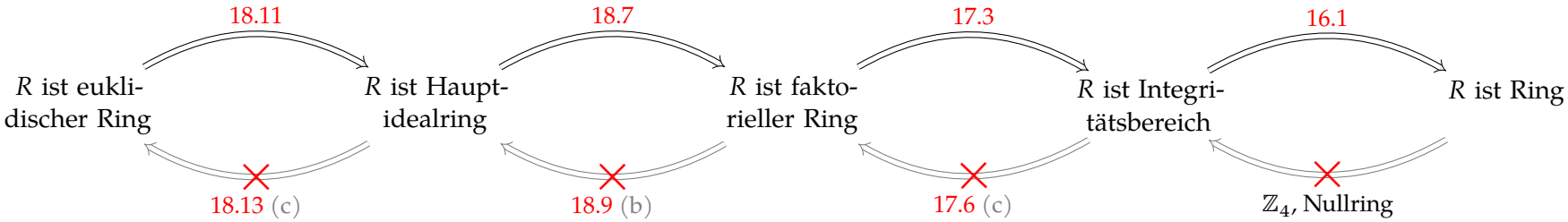
Damit ist gezeigt, dass $\mathbb{Z}[i]$ ein euklidischer Ring ist. ※

Bemerkung 18.14 Der Euklidische Algorithmus, mit dem wir uns auf Seite 21 beschäftigt haben, überträgt sich (samt Beweis) beinahe wörtlich auf euklidische Ringe. In euklidischen Ringen lässt sich somit der ggT zweier Elemente konkret berechnen.
Allgemeine Aussagen über die Effizienz des Algorithmus lassen sich aber nicht treffen; hierzu müsste man beispielsweise wissen, wie aufwendig die Durchführung der Division mit Rest im betrachteten Ring ist.
Auch 3.15 (b) überträgt sich in euklidische Ringe; wir können also auch die Bézout-Koeffizienten λ_i aus 18.8 berechnen.
In den Übungen werden wir auf die ggT- und Koeffizienten-Berechnung in euklidischen Ringen näher eingehen. → Übung ※

Als Abschluss unserer Beschäftigung mit den unterschiedlichen Ringtypen stellen wir diese knapp auf der nächsten Seite zusammen und listen die jeweiligen Haupteigenschaften auf.

Der Zoo der Ringtypen

In der unteren Grafik sehen Sie die Beziehungen zwischen den einzelnen von uns behandelten Ringtypen. Je weiter links ein Ringtyp steht, desto mehr ähnelt er dem Ring $\mathbb{Z}$ aus algebraischer Sicht.
Die Ringtypen werden von rechts nach links echt spezieller: Ein Ring ist i. A. kein Integritätsbereich, ein Integritätsbereich ist i. A. nicht faktoriell, etc.
Umgekehrt beinhalten weiter rechts stehenden Ringtypen stets den weiter links stehenden Typ: Ein euklidischer Ring ist auch ein Hauptidealring, ein Hauptidealring ist auch ein faktorieller Ring, etc.



Was gilt in welchem Ringtyp?

Wir listen auf, welcher Ringtyp welche „Features“ mit sich bringt:

Ring	Addition und Multiplikation existieren und sind verträglich
Integritätsbereich	zusätzlich: Quotientenkörper kann gebildet werden, Kürzen durch Nicht-Null-Elemente ist möglich
faktorieller Ring	zusätzlich: eindeutige Primfaktorzerlegungen für NEuNen existieren, prim=irreduzibel, ggT und kgV existieren
Hauptidealring	zusätzlich: maximale Ideale lassen sich charakterisieren, Lemma von Bézout gilt
euklidischer Ring	zusätzlich: Division mit Rest existiert, euklidischer Algorithmus erlaubt ggT- und Bézout-Koeffizienten-Berechnung

19. Zerlegbarkeit von Polynomen, Primitivität, Eisenstein

Worum geht es? Polynome spielen in der Körpertheorie eine große Rolle. Als Vorbereitung auf die Körpertheorie untersuchen wir in dieser Vorlesung Polynome auf multiplikative Zerlegbarkeit und stellen Techniken und Resultate vor, mit denen man Polynome zerlegen oder die Unzerlegbarkeit von Polynomen zeigen kann. ⁜

Die Ergebnisse dieser Vorlesung werden wir hauptsächlich in der Körpertheorie benötigen. Da Unterringe von Körpern stets Integritätsbereiche sind, werden wir im Folgenden nur Polynome über Integritätsbereichen (oder sogar faktoriellen Ringen) betrachten.

Mit Hilfe der Begriffe *(ir-)reduzibel* kann das multiplikative Zerlegungsverhalten von Ringelementen, also insbesondere auch das von Polynomen beschrieben werden:

Beispiel 19.1 (a) Das Polynom $2X + 2 = 2(X + 1)$ ist irreduzibel in $\mathbb{Q}[X]$, aber reduzibel in $\mathbb{Z}[X]$ (denn Zwei ist eine Einheit in $\mathbb{Q}$, aber nicht in $\mathbb{Z}$).

(b) Das Polynom $2 = 2 \cdot X^0$ ist irreduzibel in $\mathbb{Z}[X]$. Es ist allerdings keine NEuN in $\mathbb{Q}[X]$ und somit nicht irreduzibel in $\mathbb{Q}[X]$.

Ähnlich folgt, dass 4 in $\mathbb{Z}[X]$ reduzibel, aber nicht reduzibel in $\mathbb{Q}[X]$ ist. ⁜

Oft untersucht man ein Polynom auf (Ir-)Reduzibilität, indem man versucht, das Polynom als Produkt von zwei Polynomen mit Grad ≥ 1 zu schreiben. Um diese Faktorisierungseigenschaft eleganter zu formulieren, führen wir den folgenden Begriff ein:

Definition 19.2 *Seien R ein Integritätsbereich und $f \in R[X]$ ein Polynom über R. Wir nennen f* ***zerlegbar in $R[X]$****, wenn Polynome $g, h \in R[X]$ mit $\deg g \geq 1$ und $\deg h \geq 1$ existieren, so dass $f = gh$ gilt. Ansonsten nennen wir f* ***unzerlegbar in $R[X]$****.*

Im Vergleich zu *(Ir-)Reduzibilität* ist *(Un-)Zerlegbarkeit* der einfachere und intuitivere Begriff:

Beispiel 19.3 (a) Aus der Gradformel folgt, dass zerlegbare Polynome (mit Koeffizienten aus einem Integritätsbereich) mindestens Grad Zwei haben müssen.

Das Polynom aus 19.1 (a) ist daher sowohl über $\mathbb{Z}$ als auch über $\mathbb{Q}$ unzerlegbar. Abhängig vom betrachteten Polynomring kann es aber reduzibel oder irreduzibel sein.

(b) Ist ein Polynom $f \in R[X]$ zerlegbar, so ist es auch in jedem Oberring von $R[X]$ zerlegbar, denn die über R mögliche Zerlegung existiert auch im Oberring.

Reduzibilität hingegen bleibt i. A. nicht in Oberringen erhalten, vgl 19.1 (b). ⁜

(Un-)Zerlegbarkeit vs. (Ir-)Reduzibilität

In diesem Abschnitt vergleichen wir *(Un-)Zerlegbarkeit* mit *(Ir-)Reduzibilität* und stellen Übersetzungen zwischen diesen Begriffen bereit.

Besonders elegant funktioniert dies für Polynomringe über Körpern. Hier bedeuten die jeweiligen Begriffspaare für Polynome mit Mindestgrad Eins dasselbe:

Satz 19.4 *Seien K ein Körper und $f \in K[X]$ ein Polynom mit $\deg f \geq 1$. Dann gelten:*

(a) *f ist reduzibel in $K[X]$ $\iff$ f ist zerlegbar in $K[X]$.*

(b) *f ist irreduzibel in $K[X]$ $\iff$ f ist unzerlegbar in $K[X]$.*

Beweis. Aufgrund der Körpervoraussetzung und 15.16 gilt $K[X]^\times = K^\times = K \setminus \{0\}$. Ein Polynom aus $K[X]$ ist also genau dann eine NEuN, wenn sein Grad mindestens Eins beträgt. Insbesondere ist das gegebene Polynom f eine NEuN.

zu (a) f ist reduzibel genau dann, wenn f ein Produkt von zwei NEuNen ist. Mit obiger Klassifikation der NEuNen bedeutet dies, dass $f = gh$ mit $g, h \in K[X]$ und $\deg g, \deg h \geq 1$ gilt. Dies ist äquivalent zur Zerlegbarkeit von f.

zu (b) Da f eine NEuN ist, sind die Eigenschaften *reduzibel in $K[X]$* und *irreduzibel in $K[X]$* Gegenteile voneinander. (b) entsteht daher als Kontraposition aus (a) und ist durch die Gültigkeit von (a) bereits gezeigt. ■

Aus diesem Satz folgt eine erste Aussage zur Irreduzibilität von Polynomen:

Korollar 19.5 *Seien K ein Körper und $f \in K[X]$.*

(a) *Gilt $\deg f = 1$, so ist f unzerlegbar und daher irreduzibel in $K[X]$.*

(b) *Gilt $\deg f \in \{2, 3\}$, so ist f zerlegbar und daher reduzibel in $K[X]$ genau dann, wenn f eine Nullstelle in K besitzt.*

Beweis.

zu (a) Nach 19.3 (a) ist f unzerlegbar und nach 19.4 (b) irreduzibel.

zu (b) Nach 19.4 (a) ist f reduzibel genau dann, wenn f zerlegbar ist.

$\Longleftarrow$ Besitzt f eine Nullstelle in K, so ist f nach 15.19 zerlegbar.

$\Longrightarrow$ Ist f reduzibel, so tritt wegen $\deg f \in \{2, 3\}$ nach Gradformel in einer Zerlegung von f ein Grad-Eins-Polynom auf. f besitzt also einen Teiler der Form $aX + b$ mit $a, b \in K$ und $a \neq 0$ und daher eine Nullstelle $-b/a \in K$. ■ ?

Über Integritätsbereichen gilt immerhin noch die „Hälfte“ von 19.4:

Satz 19.6 *Seien R ein Integritätsbereich und $f \in R[X]$ mit $\deg f \geq 1$. Dann gelten:*

(a) *f ist zerlegbar in $R[X] \Longrightarrow f$ ist reduzibel in $R[X]$.*

(b) *f ist irreduzibel in $R[X] \Longrightarrow f$ ist unzerlegbar in $R[X]$.*

Beweis. Es gilt $R[X]^\times = R^\times$ nach 15.16. Polynome mit Mindestgrad Eins sind also sicherlich NEuNen; insbesondere ist f eine NEuN. (Allerdings kann es NEuNen mit Grad Null geben; im Vergleich zu 19.4 charakterisiert die Grad-Bedingung die NEuNen nicht.)

zu (a) Da f zerlegbar ist, existieren $g, h \in R[X]$ mit $f = gh$ und $\deg g, \deg h \geq 1$. Somit ist die NEuN f ein Produkt von NEuNen und daher reduzibel.

(b) ist die Kontraposition von (a). ■

Die Rückrichtungen in obigem Satz sind im Allgemeinen falsch; ein Gegenbeispiel ist durch das reduzible, aber unzerlegbare Polynom $2X + 2 \in \mathbb{Z}[X]$ aus 19.1 (a) gegeben.

Primitivität

Das Gegenbeispiel zu den Rückrichtungen in 19.6 nutzt aus, dass eine Grad-Null-NEuN existiert, die alle Koeffizienten des Polynoms teilt und daher ausgeklammert werden kann. Um solche Gegenbeispiele auszuschließen, können wir auf zwei Weisen vorgehen: Wir können fordern, dass NEuNen in $R[X]$ mindestens Grad Eins haben müssen. Dann folgt, dass R bereits ein Körper ist. Diese Forderung ist somit sehr restriktiv.
Alternativ können wir nur solche Polynome betrachten, aus denen keine Grad-Null-NEuN ausgeklammert werden kann. Diese Bedingung lässt sich besonders elegant in faktoriellen Ringen formulieren; man betrachtet hierzu den ggT der Koeffizienten des Polynoms. Der folgende Begriff und viele Resultate dieses Abschnitts gehen auf Gauß zurück.

Definition 19.7 (Gauß) *Sei R ein faktorieller Ring. Das Polynom $f := \sum_{i=0}^{n} a_i X^i \in R[X]$ heißt **primitiv**, wenn $\operatorname{ggT}(a_0, a_1, \ldots, a_n) = 1$ gilt, d. h. wenn nur Einheiten aus R gemeinsame Teiler aller Koeffizienten a_i sind.*

Beispiel 19.8 (a) Das Nullpolynom ist nicht primitiv.

(b) Ist (mindestens) ein Koeffizient eines Polynoms f eine Einheit, so ist f primitiv.

Hieraus folgt insbesondere: **Normierte Polynome**, also Polynome, deren Leitkoeffizient gleich Eins ist, sind primitiv.

(c) Über Körpern ist jedes Polynom $f \neq 0$ nach (b) primitiv. ⁂

Für *primitive* Polynome gelten die Rückrichtungen in 19.6. Wir erhalten daher die nachstehenden Äquivalenzen:

Satz 19.9 *Seien R ein faktorieller Ring und $f \in R[X]$ ein **primitives** Polynom mit $\deg f \geq 1$. Dann gelten:*

(a) *f ist zerlegbar in $R[X] \iff f$ ist reduzibel in $R[X]$.*

(b) *f ist irreduzibel in $R[X]$* $\iff$ *f ist unzerlegbar in $R[X]$.*

Beweisskizze.

zu (a) Wegen 19.6 brauchen wir nur „$\Longleftarrow$“ zu zeigen: Sei f reduzibel. Dann lässt sich f als Produkt $f = gh$ von NEuNen $g, h \in R[X]$ schreiben. Wegen der Primitivitätsvoraussetzung an f gilt $g, h \notin R$, denn ansonsten würde die NEuN g bzw. h alle Koeffizienten von f teilen. Somit ist $\deg g, \deg h \geq 1$. Also ist f zerlegbar. ?

(b) ist die Kontraposition von (a). ■

Unter Zuhilfenahme des Primitivitätsbegriffs haben sich Beweistechniken etabliert, mit denen man von Zerlegungen eines Polynoms über dem Quotientenkörper auf Zerlegungen über dem Ring schließen kann. Wir stellen im Folgenden einige Sätze vor, die auf diesen Beweistechniken beruhen. Die meist recht technischen Beweise führen wir nicht.

Der folgende Satz wird bei der Untersuchung von Polynomen auf (Un-)Zerlegbarkeit oft benötigt. Sie finden seinen Beweis beispielsweise in [KM17, Lemma 19.4 auf S. 256].

Satz 19.10 (Gauß) *Seien R ein faktorieller Ring und $f \in R[X]$. Sei $K := Q(R)$ der Quotientenkörper von R. Es gelte $f = g \cdot h$ mit $\boldsymbol{g, h \in K[X]}$. Dann existiert ein $k \in K^\times$, so dass kg und $k^{-1}h$ Polynome **aus** $\boldsymbol{R[X]}$ sind.*
*Die Zerlegung $f = gh$ **über** $\boldsymbol{K}$ liefert daher eine Zerlegung $f = (kg) \cdot (k^{-1}h)$ **über** $\boldsymbol{R}$.*

Bemerkung 19.11 (a) $K[X]$ ist ein Oberring von $R[X]$. Ist f in $R[X]$ zerlegbar, dann wegen 19.3 (b) auch in $K[X]$.

19.10 liefert die Rückrichtung: Ist $f = gh$ in $K[X]$ zerlegbar, so existiert ein $k \in K^\times$, so dass die Produkte kg und $k^{-1}h$ zu Polynomen aus $R[X]$ werden. Da k ein Grad-Null-Polynom ist, ändern sich durch diese Multiplikation die Polynomgrade nicht. Aus der Zerlegung von f über K haben wir somit eine Zerlegung von f über R mit denselben Polynomgraden gewonnen.

(b) Oft wird 19.10 im Fall $R = \mathbb{Z}$ und (daher) $K = \mathbb{Q}$ angewendet: Ist f ein Polynom mit ganzzahligen Koeffizienten und sucht man Zerlegungen von f in $\mathbb{Q}[X]$, so reicht es aus, nach Zerlegungen in $\mathbb{Z}[X]$ zu suchen. Dies ist rechnerisch deutlich einfacher. ⋇

Wir formulieren 19.11 (a) als eigenständiges Resultat:

Korollar 19.12 (Gauß) *Seien R ein faktorieller Ring, $K := Q(R)$ der Quotientenkörper von R und $f \in R[X]$. Dann gilt:*

$$f \text{ ist zerlegbar in } K[X] \iff f \text{ ist zerlegbar in } R[X].$$

Wir benutzen 19.10 und zeigen, dass sich die *rationalen* Nullstellen eines normierten *ganzzahligen* Polynoms einfach bestimmen lassen (die kursiven Einschränkungen hängen mit der Forderung $(R, K) = (\mathbb{Z}, \mathbb{Q})$ zusammen).

Korollar 19.13 *Seien $f \in \mathbb{Z}[X]$ ein normiertes Polynom und $a \in \mathbb{Q}$ eine Nullstelle von f. Dann gilt $a \in \mathbb{Z}$ und $a \mid f(0)$.*

Beweis. Wir betrachten f im Ring $\mathbb{Q}[X]$, dividieren mit 15.19 die Nullstelle a ab und erhalten die Faktorisierung $f = (X - a) \cdot g$ mit einem $g \in \mathbb{Q}[X]$. Mit Gauß können wir diese Zerlegung nach $\mathbb{Z}[X]$ zurückführen: Es existiert $q \in \mathbb{Q}^\times$, so dass $q \cdot (X - a)$ und $q^{-1} \cdot g$ beides Polynome aus $\mathbb{Z}[X]$ sind.
Der Leitkoeffizient von $q \cdot (X - a)$ ist q. Da $q \cdot (X - a) \in \mathbb{Z}[X]$ gilt, folgt $q \in \mathbb{Z}$.
Da f und $X - a$ normiert sind, ist auch g normiert. Der Leitkoeffizient von $q^{-1} \cdot g$ ist somit q^{-1}. Da $q^{-1} \cdot g \in \mathbb{Z}[X]$ gilt, folgt $q^{-1} \in \mathbb{Z}$.
Zusammen erhalten wir $q = 1$ oder $q = -1$. Dies zeigt, dass die ursprünglichen Polynome $X - a$ und g bereits Polynome aus $\mathbb{Z}[X]$ waren und dass somit $a \in \mathbb{Z}$ ist. Einsetzen von Null liefert $f(0) = -a \cdot g(0)$, also $a \mid f(0)$. ∎

Beispiel 19.14 (a) Es gibt kein $a \in \mathbb{Q}$, das eine Nullstelle von $f := X^4 - X - 1 \in \mathbb{Z}[X]$ ist; denn nach 19.12 ist $a \in \mathbb{Z}$ und $a \mid f(0) = -1$, also $a \in \{\pm 1\}$. Jedoch ist $f(\pm 1) \neq 0$.

(b) Die einzige rationale Nullstelle von $f := X^5 - 8X^4 - 2X^3 + 16X^2 + 9X - 72 \in \mathbb{Z}[X]$ ist 8; man schließt hierzu analog zu (a). Dies zeigt die Zerlegbarkeit und wegen 19.6 auch die Reduzibilität von f in $\mathbb{Z}[X]$. ⁂

Knobelfrage. Das Polynom $X^2 - 2 \in \mathbb{Z}[X]$ hat wegen $f(\pm 1) \neq 0 \neq f(\pm 2)$ nach 19.13 keine Nullstellen. Allerdings gilt $f(\sqrt{2}) = 0$. Wie passt das zusammen?

Staatsexamensaufgabe (H2013T3A2 (b)) *Zeigen Sie, dass das Polynom $f := X^4 - X - 1$ irreduzibel in $\mathbb{Q}[X]$ ist.*

Wegen 19.4 (b) reicht es, die Unzerlegbarkeit von f in $\mathbb{Q}[X]$ zu zeigen. Hierzu nehmen wir an, dass f in $\mathbb{Q}[X]$ zerlegbar sei, und führen einen Widerspruchsbeweis.
Sei $f = g \cdot h$ mit $g, h \in \mathbb{Q}[X]$ und $\deg g, \deg h \geq 1$. Da f nach 19.14 (a) keine Nullstelle in $\mathbb{Q}$ besitzt, ist weder g noch h ein Grad-Eins-Polynom. Es folgt $\deg g = \deg h = 2$.
Gauß 19.10 erlaubt es, g und h als Polynome in $\mathbb{Z}[X]$ anzunehmen. Es gilt also

$$X^4 - X - 1 = (a_2X^2 + a_1X + a_0) \cdot (b_2X^2 + b_1X + b_0) \qquad \text{mit } a_i, b_i \in \mathbb{Z}.$$

Ausmultiplizieren und Koeffizientenvergleich führt auf das Gleichungssystem

$$\left\{ \begin{array}{rcl} 1 & = & a_2b_2 \\ 0 & = & a_2b_1 + a_1b_2 \\ 0 & = & a_2b_0 + a_1b_1 + a_0b_2 \\ -1 & = & a_1b_0 + a_0b_1 \\ -1 & = & a_0b_0 \end{array} \right\}.$$

Eine längere Rechnung zeigt, dass dieses keine Lösung hat. Hierbei ist sehr vorteilhaft, dass sämtliche Variablen aus $\mathbb{Z}$ stammen: Die erste Gleichung liefert beispielsweise direkt $a_2 = b_2 = \pm 1$, die letzte $a_0 = -b_0 = \pm 1$.
Dieser Widerspruch zur Zerlegbarkeit von f zeigt die Irreduzibilität von f. ⁂

(Un-)Zerlegbarkeitsnachweis mit Hilfe von Homomorphismen

In den Beweisen der folgenden Resultate spielen Homomorphismen zwischen Polynomringen eine Rolle. Diese sind mit Produkten verträglich und übertragen daher Polynomzerlegungen von einem Ring in einen anderen.
Wir konstruieren den Ringhomomorphismus, auf dem die Beweise der nächsten beiden Sätze beruhen: Seien R ein Integritätsbereich und $\mathfrak{a}$ ein Ideal von R. Mit Hilfe des kanonischen Epimorphismus $R \to R/\mathfrak{a}$, $r \mapsto \overline{r}$ definieren wir die Abbildung

$$\varphi : R[X] \to (R/\mathfrak{a})[X], \qquad \sum_{i=0}^{n} a_i X^i \mapsto \sum_{i=0}^{n} \overline{a_i}\, X^i.$$

Man kann direkt nachrechnen, dass φ ein Ringhomomorphismus ist. Da φ nur die Koeffizienten des eingesetzten Polynoms verändert, bezeichnet man φ manchmal auch als **Koeffizientenreduktion nach $R/\mathfrak{a}$**.
Ein sehr bekanntes Unzerlegbarkeitskriterium ist das **Eisensteinkriterium**:

Satz 19.15 (Eisenstein) *Seien R ein Integritätsbereich und $p \in R$ ein Primelement. Das Polynom $f := \sum_{i=0}^{n} a_i X^i$ erfülle die folgende **Eisensteinbedingung bezüglich p**:*

$$p \nmid a_n \quad \textit{und} \quad p^2 \nmid a_0 \quad \textit{und} \quad p \mid a_i \textit{ für } i \in \{0, 1, \dots, n-1\}.$$

(Beachten Sie, dass diese Bedingung $a_n \neq 0$ und $a_0 \neq a_n$ erzwingt. Es folgt also $n = \deg f \geq 1$.) ⁉
Dann ist f unzerlegbar in $R[X]$.

Beweis. Sei $\varphi : R[X] \to (R/(p))[X]$ die Koeffizientenreduktion nach $R/(p)$. Wegen der Eisensteinbedingung gilt $\varphi(f) = \overline{a_n}\, X^n \neq 0$.
Angenommen, f sei zerlegbar in $R[X]$. Dann existieren Polynome $g := \sum_{i=0}^{s} g_i X^i$ und $h := \sum_{j=0}^{t} h_j X^j$ aus $R[X]$ mit $\deg g = s \geq 1$ und $\deg h = t \geq 1$ und $s + t = n$. Anwenden von φ auf diese Zerlegung zeigt

$$0 \neq \overline{a_n}\, X^n = \varphi(g) \cdot \varphi(h) = \left(\sum_{i=0}^{s} \overline{g_i}\, X^i \right) \cdot \left(\sum_{j=0}^{t} \overline{h_j}\, X^j \right). \qquad (\star)$$

Es folgt $\overline{g_s} \cdot \overline{h_t} = \overline{a_n} \neq 0$ und somit $\overline{g_s} \neq 0 \neq \overline{h_t}$. Wir zeigen, dass die Polynome $\varphi(g)$ und $\varphi(h)$ keine weiteren Nicht-Null-Koeffizienten besitzen. Seien hierzu $\alpha \in \{0, \dots, s\}$ bzw. $\beta \in \{0, \dots, t\}$ der minimale Index mit $\overline{g_\alpha} \neq \overline{0}$ bzw. $\overline{h_\beta} \neq \overline{0}$. Dann ist

$$\begin{aligned} \varphi(g) \cdot \varphi(h) &= \left(\overline{g_\alpha} X^\alpha + \text{Terme mit höherem Grad} \right) \cdot \left(\overline{h_\beta} X^\beta + \text{Terme mit höherem Grad} \right) \\ &= \overline{g_\alpha} \cdot \overline{h_\beta} \cdot X^{\alpha+\beta} + \text{Terme mit höherem Grad} \overset{(\star)}{=} \overline{a_n} X^n. \end{aligned}$$

Da p als prim vorausgesetzt war, ist (p) ein Primideal und somit $R/(p)$ nach 17.18 (a) ein Integritätsbereich. Daher ist $\overline{g_\alpha} \cdot \overline{h_\beta} \neq \overline{0}$, und es folgt $\alpha + \beta = n$, also $\alpha = s$ und $\beta = t$. ⁉
Es gilt also $\varphi(g) = \overline{g_s} X^s$ und $\varphi(h) = \overline{h_t} X^t$. Insbesondere folgt $\overline{g_0} = \overline{0} = \overline{h_0}$, also $p \mid g_0$ und $p \mid h_0$ und somit $p^2 \mid h_0 g_0 = a_0$. Dies widerspricht der Eisensteinbedingung und zeigt, dass die angenommene Zerlegbarkeit von f falsch gewesen ist. ■

Beispiel 19.16 Das Polynom $f := 3X^{2018} + 18X^{512} + 6 \in \mathbb{Z}[X]$ genügt einer Eisensteinbedingung bezüglich der Primzahl $2 \in \mathbb{Z}$. Es ist daher unzerlegbar in $\mathbb{Z}[X]$. Mit Gauß ist es auch unzerlegbar in $\mathbb{Q}[X]$. Nach 19.4 ist f irreduzibel in $\mathbb{Q}[X]$. Allerdings ist f nicht primitiv und daher reduzibel in $\mathbb{Z}[X]$. ⁜

Knobelfrage. Das Polynom $f := X^3 - \overline{2} \in \mathbb{Z}_3[X]$ genügt einer Eisensteinbedingung bezüglich des Primelements $\overline{2} \in \mathbb{Z}_3$ und ist daher nach Eisenstein unzerlegbar in $\mathbb{Z}_3[X]$. Allerdings gilt $f(\overline{2}) = \overline{0}$, was die Zerlegbarkeit von f in $\mathbb{Z}_3[X]$ zeigt. Wie passt das zusammen? ⁉

Speziell für Polynome aus $\mathbb{Z}[X]$ ist auch das folgende **Reduktionskriterium** gebräuchlich:

Satz 19.17 *Seien $p \in \mathbb{P}$ eine Primzahl und $f \in \mathbb{Z}[X]$ ein Polynom, so dass p nicht den Leitkoeffizienten von f teile. Es bezeichne $\varphi : \mathbb{Z}[X] \to \mathbb{Z}_p[X]$ die Koeffizientenreduktion nach $\mathbb{Z}_p$. Gilt dann $f = f_1 \cdots f_r$ mit Polynomen $f_i \in \mathbb{Z}[X]$, so ist $\varphi(f) = \varphi(f_1) \cdots \varphi(f_r)$, wobei $\deg f_i = \deg \varphi(f_i)$ ist.*
Die Koeffizientenreduktion überträgt also Zerlegungen in $\mathbb{Z}[X]$ in den Ring $\mathbb{Z}_p[X]$ ***und erhält dabei die Grade der auftretenden Faktoren****.*

Beweisskizze. Die Aussage $\varphi(f) = \varphi(f_1) \cdots \varphi(f_r)$ folgt aus der Homomorphie von φ. Da der Leitkoeffizient von f nicht durch p teilbar ist, sind auch die Leitkoeffizienten aller f_i nicht durch p teilbar, denn der Leitkoeffizient von f ist das Produkt der Leitkoeffizienten der f_i. ■

Korollar 19.18 *Mit den Bezeichnungen aus obigem Satz sei $\varphi(f) \in \mathbb{Z}_p[X]$ unzerlegbar. Dann ist auch $f \in \mathbb{Z}[x]$ unzerlegbar.*

Beweisskizze. Wäre f zerlegbar, so wäre nach 19.17 auch $\varphi(f)$ zerlegbar. ■

Beispiel 19.19 (a) Das Polynom $f := X^3 + X + 1 \in \mathbb{Z}[X]$ ist unzerlegbar, denn die Reduktion $\varphi(f) = X^3 + X + \overline{1} \in \mathbb{Z}_2[X]$ nach $\mathbb{Z}_2$ besitzt keine Nullstellen und ist nach 19.5 (b) somit unzerlegbar. Da f primitiv ist, ist f irreduzibel in $\mathbb{Z}[X]$.

(b) Wir betrachten das Polynom $f := X^4 - X - 1 \in \mathbb{Z}[X]$ aus der Staatsexamensaufgabe auf Seite 135. Die Reduktion $\varphi(f) = X^4 + X + \overline{1} \in \mathbb{Z}_2[X]$ ist nullstellenfrei. Wäre $\varphi(f)$ zerlegbar, so wäre $\varphi(f)$ nach Gradformel ein Produkt von zwei nullstellenfreien Grad-Zwei-Polynomen aus $\mathbb{Z}_2[X]$.

$\mathbb{Z}_2[X]$ enthält genau vier Grad-Zwei Polynome. Von diesen ist nur das Polynom $X^2 + X + \overline{1} \in \mathbb{Z}_2[X]$ nullstellenfrei. Es müsste also gelten ⁉

$$\varphi(f) = (X^2 + X + \overline{1}) \cdot (X^2 + X + \overline{1}) \overset{\text{Ausmultiplizieren}}{=} X^4 + X^2 + \overline{1}.$$

Allerdings ist $\varphi(f) \neq X^4 + X^2 + \overline{1}$. Dieser Widerspruch zeigt, dass $\varphi(f)$ unzerlegbar in $\mathbb{Z}_2[X]$ ist. Somit ist auch f unzerlegbar in $\mathbb{Z}[X]$ und daher nach Gauß unzerlegbar und irreduzibel in $\mathbb{Q}[X]$. ⁜

Teil IV.
Körper

Die Grundfrage in der Körpertheorie ist, welche Aussagen man über einen Körper L *relativ zu einem Unterkörper* K treffen kann. Um dies mathematisch zu modellieren und um *Ober-* und *Unterkörper* zu fixieren, führt man den Begriff der *Körpererweiterung* ein. Man misst die Größe einer Erweiterung mit Hilfe des *Erweiterungsgrads*, den man mit Methoden der Linearen Algebra definiert.
Der Begriff „Erweiterung“ beschreibt ziemlich treffend eine Grundstrategie, auf die man in der Körpertheorie immer wieder trifft: Ausgehend vom Unterkörper K fügt man so lange Elemente zu K hinzu, bis man beim Oberkörper L angekommen ist. Mathematisch beschreibt man dies mit Hilfe von *Körperadjunktionen*, einem Konzept, das uns in ähnlicher Form bereits bei den Ringadjunktionen in Vorlesung 15 begegnet ist.

Die Adjunktion eines Elements a an einen Körper K liefert zwei verschiedene Typen von Ergebniskörpern: Falls a *transzendent über* K war, hat der Ergebniskörper unendlichen Grad über K, falls a *algebraisch über* K war, nur endlichen.
Wir diskutieren vorwiegend die algebraische Situation. Dann besitzt a ein *Minimalpolynom über* K, das alle algebraischen Eigenschaften von a codiert. Man kann beispielsweise allein mit Hilfe des Minimalpolynoms die Adjunktion von a an K beschreiben, ohne a konkret zu kennen. Auf diese als *Kronecker-Adjunktion* bekannte Technik werden wir sehr detailliert eingehen. Wichtige Konsequenzen der Technik sind die Existenz von *Zerfällungskörpern* und das *Fortsetzungslemma*.

Das Fortsetzungslemma erlaubt zudem das genauere Studium von *K-Automorphismen*, was letztlich zur *Galoistheorie* führt. Diese Theorie liefert eine Übersetzung von Eigenschaften gewisser Körpererweiterungen in die Gruppentheorie. Wir stellen einige Anwendungen der Galoistheorie vor und geben viele Beispiele. Das Themengebiet runden wir ab, indem wir uns mit dem *Umkehrproblem* beschäftigen und gewisse endliche Gruppen als Galoisgruppen *realisieren*. Hierzu benutzen wir Methoden der *Kreisteilungstheorie* und der Theorie der *symmetrischen Polynome*.

Als vielleicht überraschende Anwendung der Körpertheorie diskutieren wir *Konstruktionen mit Zirkel und Lineal*. Wir motivieren, wie diese geometrische Fragestellung in eine Aussage über Körpererweiterungen übersetzt werden kann, und leiten Bedingungen her, aus denen die Nicht-Konstruierbarkeit gewisser Punkte folgt. Damit können wir beweisen, dass die klassischen Konstruierbarkeitsprobleme, das *Delische Problem der Würfelverdoppelung*, die *Quadratur des Kreises* und die *Winkeldreiteilung*, im Allgemeinen nicht lösbar sind.

20. Körperadjunktion, Körpererweiterungen

Worum geht es? Wir beschäftigen uns mit der Adjunktion von Elementen an einen Körper. Die Idee ist hierbei dieselbe wie in Vorlesung 15.
Danach definieren wir den für die Körpertheorie grundlegenden Begriff der *Körpererweiterung*. Mit Hilfsmitteln der Linearen Algebra stellen wir ein Maß für die Größe einer Körpererweiterung, den *Erweiterungsgrad*, bereit. Die *Gradformel* verknüpft dann die Erweiterungsgrade von Teilerweiterungen mit dem der Gesamterweiterung.
Zuletzt beschäftigen wir uns mit *algebraischen Körperelementen* und führen den Begriff des *Minimalpolynoms* ein. ※

Körperadjunktion

Wir haben uns in 15.1 mit der Adjunktion von Elementen an Ringe beschäftigt. Wir stellen nun den analogen Begriff für Körper bereit:

Definition 20.1 *Seien K ein Körper und M eine Teilmenge eines Oberkörpers L von K. Mit $K(M)$ (gelesen: **K adjungiert M**) bezeichnen wir den (per Mengeninklusion) kleinsten Unterkörper von L, der K und M als Teilmengen enthält. Es gilt nach 2.11 also $K(M) = \langle K \cup M \rangle$.*

20.1 bildet 15.1 nach, jedoch gibt es Unterschiede:

Bemerkung 20.2 (a) Ringadjunktionen werden mit eckigen Klammern notiert, Körperadjunktionen mit runden.

(b) Bei der Körperadjunktion muss die zugrunde liegende algebraische Struktur ein Körper sein. Bei der Ringadjunktion reicht ein Ring aus.

Mit den Bezeichnungen aus 20.1 ist daher auch der *Ring* $K[M]$ definiert; im Allgemeinen ist $K[M]$ eine *echte* Teilmenge von $K(M)$. ※

Man kann die Körperadjunktion leicht mit Hilfe der Ringadjunktion ausdrücken:

Satz 20.3 *Seien K ein Körper und M eine Teilmenge eines Oberkörpers von K. Dann ist $K(M)$ der Quotientenkörper des Integritätsbereichs (Warum Integritätsbereich?) $K[M]$, d. h. es gilt* ⁉

$$K(M) = Q(K[M]) = \left\{ \frac{a}{b} : a, b \in K[M], b \neq 0 \right\}.$$

Beweisskizze. $Q(K[M])$ ist ein Körper, der K und M enthält. Weil $K(M)$ diesbezüglich minimal ist, folgt $K(M) \subseteq Q(K[M])$.
Wegen 20.2 (b) ist $K[M] \subseteq K(M)$. Da $K(M)$ ein Körper ist, folgt $Q(K[M]) \subseteq K(M)$. ■

Bemerkung 20.4 In 15.2 haben wir eine explizite Beschreibung für die Elemente aus $K[M]$ hergeleitet. Mit dieser folgt eine explizite Beschreibung der Elemente aus $K(M)$:

$$K(M) = \left\{ \frac{\sum_{i=0}^{n} k_i m_i}{\sum_{j=0}^{s} r_j n_j} : n, s \in \mathbb{N}_0, k_i, r_j \in K, \begin{array}{l} m_i \text{ und } n_j \text{ sind Produkt endlich vieler} \\ \text{Elemente aus } M, \text{ Nenner ist} \neq 0 \end{array} \right\}.$$ ※

Beispiel 20.5 Wir betrachten den wichtigen Fall einer einelementigen Menge $M = \{m\}$. Dann gilt

$$K(m) \overset{15.4\,(a)}{=} Q\left(\left\{\sum_{i=0}^{n} k_i m^i : n \in \mathbb{N}_0, k_i \in K\right\}\right) = Q(\{f(m) \mid f \in K[X]\})$$
$$= \left\{\frac{f(m)}{g(m)} : f, g \in K[X], g(m) \neq 0\right\}.$$

$K(m)$ entsteht also durch Einsetzen von m in den Quotienten f/g mit beliebigen Polynomen $f, g \in K[X]$, wobei wir $g(m) \neq 0$ fordern müssen. Mit Hilfe des rationalen Funktionenkörpers $K(X)$ aus 16.6 (b) können wir dies umformulieren:

$$K(m) = \{r(m) \mid r \in K(X), \text{ sofern das Einsetzen von } m \text{ in } r \text{ definiert ist}\}. \quad ⁜$$

Bemerkung 20.6 In 2.9 trat der Körper $\{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$ auf. Diesen können wir nun als den Körper $\mathbb{Q}(\sqrt{2})$ interpretieren. In der Darstellung von $\mathbb{Q}(\sqrt{2})$ tritt $\sqrt{2}$ nie im Nenner auf. Es gilt also $\mathbb{Q}(\sqrt{2}) = \mathbb{Q}[\sqrt{2}]$. ⁉
Nennerfreie Darstellungen von Körperadjunktionen sind in der Körpertheorie häufig. Wir charakterisieren sie im Abschnitt über algebraische Körperelemente am Ende dieser Vorlesung. ⁜

Körpererweiterungen, Gradformel

In der Körpertheorie gibt es eine ganze Reihe an Begriffen, die relativ zu einem Unterkörper definiert sind, vgl. beispielsweise den Begriff des algebraischen Elements aus 20.17. Um solche Abhängigkeiten von einem Unterkörper mathematisch elegant beschreiben zu können, führt man den Begriff der Körpererweiterung ein:

Definition 20.7 *Seien K, L Körper. Gilt $K \subseteq L$, so schreiben wir $L|K$ und sprechen von der **Körpererweiterung L über K**. Durch die Körpererweiterung $L|K$ werden ein **Oberkörper L** und ein **Unterkörper K** fixiert.*
*Sind $L|K$ eine Körpererweiterung und Z ein Körper mit $K \subseteq Z \subseteq L$, so nennen wir Z einen **Zwischenkörper von $L|K$**. Man bezeichnet $L|Z$ als eine **obere Teilerweiterung von $L|K$** und $Z|K$ als eine **untere Teilerweiterung von $L|K$**.*

$$\begin{array}{c} L \\ | \\ Z \\ | \\ K \end{array}$$

Beispiel 20.8 $\mathbb{R}|\mathbb{Q}$ ist eine Körpererweiterung mit Unterkörper $\mathbb{Q}$ und Oberkörper $\mathbb{R}$. Zwischenkörper dieser Erweiterung sind beispielsweise $\mathbb{Q}$, $\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(\pi)$ und $\mathbb{R}$. ⁜

Aus der Linearen Algebra ist bekannt, dass Oberkörper L Vektorräume über jedem Unterkörper K sind. ⁉

Beispiel 20.9 $\mathbb{C}$ ist ein Oberkörper von $\mathbb{R}$ und daher ein $\mathbb{R}$-Vektorraum. Eine $\mathbb{R}$-Basis von $\mathbb{C}$ ist beispielsweise durch $\{1, i\} \subseteq \mathbb{C}$ gegeben. Das Element $1 + i \in \mathbb{C}$ besitzt bezüglich dieser Basis die Darstellung

$$1 + i = 1 \cdot 1 + 1 \cdot i.$$

Welche Elemente in obiger Gleichung sind Skalare, welche Vektoren? ⁜ ⁉

Mit Hilfe dieser Vektorraum-Interpretation können wir die Größe einer Körpererweiterung messen:

Definition 20.10 *Sei $L|K$ eine Körpererweiterung. Dann nennen wir die Dimension von L als K-Vektorraum den* ***Grad der Körpererweiterung $L|K$*** *und schreiben $[L : K]$ für ihn. Wir setzen also*

$$[L : K] := \dim_K L \in \mathbb{N} \cup \{\infty\}.$$

$L|K$ heißt ***endlich****, falls $[L : K] \in \mathbb{N}$ gilt, ansonsten* ***unendlich****. Körpererweiterungen des Grades Zwei nennen wir* ***quadratisch****.*

Beispiel 20.11 (a) Die Erweiterung $\mathbb{C}|\mathbb{R}$ ist quadratisch. Ebenso ist die Erweiterung $\mathbb{Q}(\sqrt{2})|\mathbb{Q}$ quadratisch. Können Sie eine $\mathbb{Q}$-Basis für $\mathbb{Q}(\sqrt{2})$ angeben? ⁉

(b) Sei K ein Körper. Der rationale Funktionenkörper $K(X)$ ist eine unendliche Körpererweiterung über K, denn die Potenzen $X^0, X^1, \ldots$ sind linear unabhängig.

Ebenso ist die Erweiterung $\mathbb{R}|\mathbb{Q}$ unendlich, denn $\mathbb{R}$ ist überabzählbar.

(c) Jeder Körper K besitzt einen (bzgl. Mengeninklusion) kleinsten Unterkörper P, nämlich den Durchschnitt aller seiner Unterkörper (alternativ: Körpererzeugnis von $1 \in K$). Man nennt P den **Primkörper von K**.

Es gilt $P \cong \mathbb{Q}$, falls K Charakteristik Null hat: $1 \in P$ hat dann unendliche additive Ordnung. Somit ist $\mathbb{Z} \cong \langle 1 \rangle_{\text{Ring}} \subseteq P$ und, da P ein Körper ist, auch $\mathbb{Q} \cong Q(\langle 1 \rangle_{\text{Ring}}) \subseteq P$. Da $\mathbb{Q}$ selbst ein Körper ist, folgt $P \cong \mathbb{Q}$.

Ansonsten ist die Charakteristik von K eine Primzahl $p \in \mathbb{P}$, vgl. die Übungen. Die additive Ordnung von $1 \in P$ ist dann p, und es gilt $P \cong \mathbb{Z}_p$. → Übung

Jeder Körper ist Erweiterung seines Primkörpers.

(d) Für eine Körpererweiterung $L|K$ gilt $L = K$ genau dann, wenn $[L : K] = 1$ ist. ⁉ ⁕

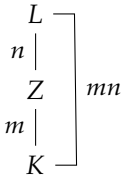
Beispiel 20.12 Sei $L|K$ eine Körpererweiterung mit Zwischenkörper Z.
Es gilt $[L : Z] \leq [L : K]$, denn jede über Z linear unabhängige Teilmenge von L bleibt auch über dem (kleineren) Körper K linear unabhängig.
Weiter ist $[Z : K] \leq [L : K]$, denn der K-Vektorraum L ist ein Oberraum des K-Vektorraums Z. ⁕

Speziell für endliche Körpererweiterungen lässt sich 20.12 präzisieren:

Satz 20.13 (Gradformel) *Sei $L|K$ eine endliche Körpererweiterung mit Zwischenkörper Z. Dann sind nach 20.12 auch $L|Z$ und $Z|K$ endlich. Es gilt $[L : K] = [L : Z] \cdot [Z : K]$.*

Beweis. Sei $n := [L : Z]$ und $m := [Z : K]$. Seien $\{a_1, \ldots, a_n\}$ eine Z-Basis von L und $\{b_1, \ldots, b_m\}$ eine K-Basis von Z. Jedes $v \in L$ lässt sich dann darstellen in der Form

$$v \overset{\substack{\text{Zerlege bzgl. } \{a_1,\ldots,a_n\} \\ \text{mit } \lambda_i \in Z}}{=} \sum_{i=1}^{n} \lambda_i a_i \overset{(\star)}{=} \sum_{i=1}^{n} \left[\Big(\sum_{j=1}^{m} \mu_{i,j}\, b_j \Big) a_i \right] = \sum_{\substack{1 \leq i \leq n \\ 1 \leq j \leq m}} \mu_{i,j}\, a_i b_j.$$



(Zu $(\star)$): Jeder Skalar $\lambda_i \in Z$ lässt sich bzgl. der Basis $\{b_1, \dots, b_m\}$ darstellen: Es existieren Skalare $\mu_{i,j} \in K$ mit $\lambda_i = \sum_{j=1}^{m} \mu_{i,j} b_j$.)

Somit erzeugt die Menge $B := \{a_i b_j \mid 1 \leq i \leq n, 1 \leq j \leq m\}$ den K-Vektorraum L. ⁉
B ist linear unabhängig über K, denn gilt $v = 0$, so folgt aus der linearen Unabhängigkeit der a_i, dass alle λ_i gleich Null sind. Aus der linearen Unabhängigkeit der b_j folgt dann $\mu_{i,j} = 0$ für alle i, j.
Dies zeigt, dass B eine K-Basis von L ist. Da B genau mn Elemente besitzt, ergibt sich $[L : K] = mn = [L : Z] \cdot [Z : K]$, was die Gradformel beweist. ■

Einfache Körpererweiterungen, algebraische Elemente

In 20.5 haben wir eine explizite Darstellung für einelementige Körperadjunktionen hergeleitet. Die so entstehenden Körpererweiterungen spielen in der Körpertheorie eine wichtige Rolle. Man führt für sie eine eigene Bezeichnung ein:

Definition 20.14 *Eine Körpererweiterung $L|K$ heißt **einfach**, wenn ein $a \in L$ existiert, so dass $L = K(a)$ gilt. Jedes solche a bezeichnet man als ein **primitives Element für $L|K$**.*

Beispiel 20.15 (a) Sei $L|K$ eine quadratische Körpererweiterung. Dann ist L ein echter Oberkörper von K, so dass $a \in L$ mit $a \notin K$ existiert. Der Zwischenkörper $K(a)$ ist ein echter Oberkörper von K und stimmt wegen der Gradformel mit L überein. Die Erweiterung $L|K$ ist also einfach; jedes $a \in L \setminus K$ kann als primitives Element gewählt werden. Es gilt $L = K(a) = \operatorname{span}\{1, a\} = \{k_0 + k_1 \cdot a \mid k_i \in K\} = K[a]$. Quadratische Erweiterungen lassen sich also stets nennerfrei darstellen.

$$\begin{array}{c} L \\ | \\ K(a) \\ \neq 1 \; | \\ K \end{array} \Big\} 2$$

(b) Die Erweiterung $\mathbb{R}|\mathbb{Q}$ ist nicht einfach, denn $\mathbb{R}$ ist überabzählbar. ⁉

(c) Der *Satz vom primitiven Element* sagt aus, dass endliche Körpererweiterungen bereits unter schwachen Bedingungen einfach sind, vgl. 25.21 und 25.22. ※

Nach Teil (a) des obigen Beispiels fallen in quadratischen Körpererweiterungen Ring- und Körperadjunktion zusammen; der Oberkörper lässt sich nennerfrei darstellen. Wir untersuchen genauer, wann dieser Effekt eintritt:

Lemma 20.16 *Seien $L|K$ eine Körpererweiterung und $a \in L$ mit $K(a) = K[a]$. Dann existiert ein Polynom $f \in K[X]$ mit $f \neq 0$ und $f(a) = 0$.*

Beweis. Für $a = 0$ können wir $f = X$ wählen. Sei daher $a \neq 0$. Aufgrund der Voraussetzungen gilt $a^{-1} \in K[a]$. Nach 15.4 (a) existieren also Elemente $k_0, \dots, k_n \in K$, so dass $a^{-1} = \sum_{i=0}^{n} k_i a^i$ gilt. Da $a^{-1} \neq 0$ ist, ist mindestens eines der k_i ungleich Null.
Es gilt

$$a^{-1} = \sum_{i=0}^{n} k_i a^i \overset{\text{Mult. mit } a}{\Longrightarrow} 1 = \sum_{i=0}^{n} k_i a^{i+1} \Longrightarrow 0 = -1 + \sum_{i=0}^{n} k_i a^{i+1}.$$

Setzen wir $f := -1 + \sum_{i=0}^{n} k_i X^{i+1} \in K[X]$, so gilt $f(a) = 0$. Weiter ist f nicht das Nullpolynom, da mindestens eines der k_i ungleich Null ist. Damit ist das Lemma gezeigt. ■

Die Nullstellenbedingung aus obigem Lemma ist fundamental für die Körpertheorie. Wir geben Körperelementen, die ihr genügen, einen eigenen Namen:

Definition 20.17 *Sei $L|K$ eine Körpererweiterung. Ein Element $a \in L$ heißt* ***algebraisch über K****, wenn ein Polynom $f \in K[X]$ mit $f(a) = 0$ und $f \neq 0$ existiert. Jedes solche Polynom und auch das Nullpolynom nennen wir ein* ***annullierendes Polynom für a****.*
Elemente aus L, die nicht algebraisch über K sind, nennen wir ***transzendent über K****.*

Beispiel 20.18 Wir betrachten die Körpererweiterung $\mathbb{C}|\mathbb{Q}$. Dann sind $\sqrt{2}$ und i algebraisch über $\mathbb{Q}$. Nach Lindemann (1882) ist die Kreiszahl π transzendent über $\mathbb{Q}$; nach Hermite (1873) ist die eulersche Zahl e transzendent über $\mathbb{Q}$. ⁂

Ein algebraisches Element besitzt viele annullierende Polynome: Ist f annullierend für a, so ist auch jedes Vielfache von f annullierend für a. Insbesondere kann $f \neq 0$ durch Teilen durch den Leitkoeffizienten zu einem *normierten* annullierenden Polynom für a umgeformt werden. Fordert man dann zusätzlich noch minimalen Grad für f, so ist f eindeutig bestimmt:

Definition/Satz 20.19 *Seien $L|K$ eine Körpererweiterung und $a \in L$. Dann sind äquivalent:*

(a) *a ist algebraisch über K.*

(b) *Es existiert ein normiertes, annullierendes Polynom $m \in K[X]$, das minimalen Grad besitzt. Aufgrund der Normiertheit ist* $\deg m \geq 1$. ⁉

Das Polynom m aus (b) ist durch das Körperelement a eindeutig festgelegt und heißt ***das Minimalpolynom von a über K****.*

Beweis.

(b)$\Longrightarrow$(a) folgt per Definition, denn m ist annullierend für a.

(a)$\Longrightarrow$(b) Es sei $A := \{f \in K[X] : f(a) = 0 \text{ und } f \neq 0\}$ die Menge aller annullierenden Nicht-Null-Polynome von a. Da a algebraisch über K ist, ist A nicht-leer. Somit existiert ein Polynom mit minimalem Grad und daher auch ein normiertes Polynom mit minimalem Grad in A, vgl. die Ausführungen vor dem Satz. ⁉

Eindeutigkeit Die Polynome m und μ mögen beide den Bedingungen aus (b) genügen. Dann ist $\deg m = \deg \mu$, denn ansonsten hätte eines der Polynome nicht minimalen Grad. Die Differenz $d := m - \mu$ ist annullierend für a. Da m und μ beide normiert sind und denselben Grad besitzen, gilt $\deg d < \deg m$. Wäre $d \neq 0$, so könnten wir d normieren und erhielten ein Minimalpolynom von a mit kleinerem Grad als m. Dies widerspricht der Minimalität von $\deg m$ und zeigt $d = 0$, also $m = \mu$. ⁉ ■

Die Minimalitätsbedingung aus 20.19 ist oft schwer zu überprüfen. Hier hilft die folgende Charakterisierung für Minimalpolynome, die für einen großen Teil der Irreduzibilitätsforderungen und -untersuchungen in der Körpertheorie verantwortlich ist:

Satz 20.20 *Seien $L|K$ eine Körpererweiterung und $a \in L$ algebraisch über K. Dann sind äquivalent:*

(a) *$m \in K[X]$ ist das Minimalpolynom von a.*

(b) *$m \in K[X]$ ist normiert, irreduzibel und annullierend für a.*

Beweis.

(a)$\Longrightarrow$(b) Es ist nur die Irreduzibilität von m zu zeigen, die wir per Widerspruch beweisen: Sei m reduzibel. Nach 19.4 ist m dann zerlegbar in der Form $m = fg$ mit $f, g \in K[X]$ und $\deg f, \deg g \geq 1$. Wegen $m(a) = 0 = f(a) \cdot g(a)$ und der Nullteilerfreiheit in Körpern folgt $f(a) = 0$ (ggf. nach Umbenennen). Dies ist widersprüchlich, denn nur das Nullpolynom annulliert a und hat kleineren Grad als m.

(b)$\Longrightarrow$(a) Sei $m \in K[X]$ normiert, irreduzibel und annullierend für a. Sei $\mu \in K[X]$ das Minimalpolynom von a. Dividieren wir m durch μ mit Rest, so können wir schreiben $m = q \cdot \mu + r$ mit $q, r \in K[X]$ und $\deg r < \deg \mu$. Es gilt

$$r(a) = (m - q \cdot \mu)(a) \overset{\text{Einsetzen ist Homom.}}{=} m(a) - q(a) \cdot \mu(a) \overset{m(a)=0=\mu(a)}{=} 0.$$

r ist somit ein annullierendes Polynom für a, dessen Grad kleiner als der des Minimalpolynoms μ ist. Es folgt $r = 0$ und somit $m = q \cdot \mu$. Da m irreduzibel und $\deg \mu \geq 1$ ist, folgt $\deg q = 0$, also $q \in K^\times$. Weil m und μ beide normiert sind, erhalten wir $q = 1$, also $m = \mu$. ∎

Wir können jetzt alle annullierenden Polynome eines algebraischen Elements angeben:

Satz 20.21 *Seien $L|K$ eine Körpererweiterung und $a \in L$ algebraisch über K mit Minimalpolynom $m \in K[X]$. Gilt $f(a) = 0$ für ein $f \in K[X]$, so ist $m \mid f$.*
Das Minimalpolynom von a teilt also jedes annullierende Polynom für a.
Anders formuliert: Die Menge der annullierenden Polynome für a ist gerade das von m erzeugte Hauptideal $(m) \trianglelefteq K[X]$. ?

Beweisskizze. Der Beweis ist ähnlich zum Schluss „(b)$\Longrightarrow$(a)“ in 20.20: Wir schreiben $f = q \cdot m + r$, sehen $r(a) = 0$ und folgern $r = 0$. Dies zeigt $f = q \cdot m$, also $m \mid f$. ∎

Im folgenden Satz klassifizieren wir die Elemente a, für die $K(a) = K[a]$ gilt:

Satz 20.22 *Seien $L|K$ eine Körpererweiterung und $a \in L$. Dann sind äquivalent:*

(a) *$K(a) = K[a]$.*

(b) *a ist algebraisch über K.*

Beweis.

(a)$\Longrightarrow$(b) folgt aus 20.16 und 20.17.

(b)$\Longrightarrow$(a) Die Aussage $K[a] \subseteq K(a)$ ist klar. Wir zeigen die Inklusion $K(a) \subseteq K[a]$ unter Verwendung von 20.5: Sei $f(a)/g(a)$ mit $f, g \in K[X]$ und $g(a) \neq 0$ ein beliebiges Element aus $K(a)$. Wir konstruieren ein Polynom $h \in K[X]$ mit $1/g(a) = h(a)$. Dann gilt $f(a)/g(a) = f(a) \cdot h(a) \in K[a]$, was den Beweis beendet.

Sei $m \in K[X]$ das Minimalpolynom von a. Wegen $g(a) \neq 0$ gilt $m \nmid g$. Da m irreduzibel ist, folgt $\operatorname{ggT}(m, g) = 1$. Bézout liefert $1 = s \cdot m + h \cdot g$ mit gewissen Polynomen $s, h \in K[X]$. Einsetzen von a in diese Gleichung zeigt

$$1 = s(a) \cdot m(a) + h(a) \cdot g(a) \overset{m(a)=0}{=} h(a) \cdot g(a), \qquad \text{also} \qquad h(a) = 1/g(a). \qquad \blacksquare$$

Mit diesen Vorarbeiten können wir den *Körper* $K[a]$ für ein algebraisches Element a konkret beschreiben. Das folgende Resultat verallgemeinert und systematisiert unsere Suche nach einfacheren Darstellungen für Adjunktionen, vgl. 15.4 und 15.5.

Korollar 20.23 *Seien $L|K$ eine Körpererweiterung, $a \in L$ algebraisch über K, $m \in K[X]$ das Minimalpolynom von a und $n := \deg m$. Dann gilt*

$$K(a) = K[a] = \Big\{ \sum_{i=0}^{n-1} k_i a^i \mid k_i \in K \Big\} = \{k_0 + k_1 \cdot a + \cdots + k_{n-1} a^{n-1} \mid k_i \in K\}.$$

Die Menge $\{a^0, a^1, \ldots, a^{n-1}\}$ ist eine K-Basis von $K(a)$. Die Darstellung von Elementen aus $K(a)$ in der Form $\sum_{i=0}^{n-1} k_i a^i$ ist daher eindeutig. Es gilt $[K(a) : K] = n$.
(Dies zeigt, dass keine „knappere" Darstellung für $K(a)$ existiert.)

Beweis.

Darstellung von $K(a)$ Wir wissen aus 20.22, dass $K(a) = K[a]$ gilt. Weiter ist klar, dass die beiden im Korollar rechts stehenden Mengen gleich und in $K[a]$ enthalten sind. Es ist noch zu zeigen, dass sich jedes Element $b \in K[a]$ tatsächlich in der Form $\sum_{i=0}^{n-1} k_i a^i$ schreiben lässt:

Sei $b \in K[a]$ beliebig. Nach 15.4 (a) gilt $b = f(a)$ mit einem Polynom $f \in K[X]$. Division mit Rest liefert $q, r \in K[X]$ mit $f = q \cdot m + r$ und $\deg r < n$. Es folgt

$$b = f(a) = (qm + r)(a) = q(a) \cdot m(a) + r(a) \overset{m(a)=0}{=} r(a).$$

Da $\deg r < n$ gilt, finden sich $k_i \in K$, so dass $r = \sum_{i=0}^{n-1} k_i X^i$ gilt. Somit ist, wie gefordert, $b = r(a) = \sum_{i=0}^{n-1} k_i a^i$.

Grad von $[K(a) : K]$ Wir zeigen, dass die Menge $B := \{a^0, a^1, \ldots, a^{n-1}\}$ eine Basis des K-Vektorraums $K(a)$ ist. Wegen $|B| = n$ folgt dann $[K(a) : K] = |B| = n$.

Wir haben oben bereits gesehen, dass B erzeugend für $K(a)$ ist. Es ist daher nur noch die lineare Unabhängigkeit von B zu beweisen. Dies geschieht per Widerspruch: Wäre B linear abhängig, so könnten wir $0 = \sum_{i=0}^{n-1} k_i a^i$ mit $k_i \in K$ schreiben,

wobei mindestens eines der k_i ungleich Null ist. Das Polynom $f := \sum_{i=0}^{n-1} k_i X^i \in K[X]$ wäre dann nicht das Nullpolynom, annullierend für a und hätte einen kleineren Grad als das Minimalpolynom m. Dies ist widersprüchlich. ■

Wir zeigen eine letzte Äquivalenz zur Algebraizität von a:

Satz 20.24 *Seien $L|K$ eine Körpererweiterung und $a \in L$. Dann sind äquivalent:*

(a) *a ist algebraisch über K.*

(b) *Die Erweiterung $K(a)|K$ ist endlich.*

Beweis.

(a)$\Longrightarrow$(b) haben wir in 20.23 gesehen.

(b)$\Longrightarrow$(a) Wegen $[K(a) : K] < \infty$ sind die Potenzen $a^0, a^1, \ldots$ nicht linear unabhängig. Es existieren daher ein $n \in \mathbb{N}$ und $k_0, \ldots, k_n \in K$ mit $\sum_{i=0}^{n} k_i a^i = 0$, wobei mindestens eines der k_i ungleich Null ist. Das Polynom $f := \sum_{i=0}^{n} k_i X^i \in K[X]$ ist dann nicht das Nullpolynom und annulliert a. Dies zeigt, dass a algebraisch ist. ■

21. Anwendung: Konstruktionen mit Zirkel und Lineal

Worum geht es? Wir konstruieren Punkte mit Zirkel und Lineal. Dies führt auf geometrische Fragestellungen.
Danach „algebraisieren“ wir unsere Konstruktionen, indem wir die konstruierten Punkte mit gewissen Erweiterungskörpern von $\mathbb{Q}$ in Verbindung bringen. Auf diese Weise ergeben sich Einschränkungen daran, welche Punkte mit Zirkel und Lineal konstruierbar sind.
Eine Konsequenz hieraus ist, dass die drei klassischen Konstruierbarkeitsprobleme, die *Würfelverdoppelung*, die *Quadratur des Kreises* und die allgemeine *Winkeldreiteilung*, unlösbar sind. ⋇

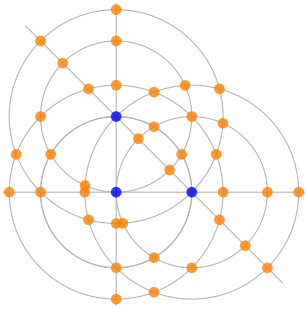
Geometrie: Was sind Konstruktionen mit Zirkel und Lineal?

Wir haben einen Zirkel, ein unbeschriftetes Lineal und ein unendlich großes Blatt Papier zur Verfügung und konstruieren Punkte, indem wir Kreise und/oder Geraden mit Kreisen und/oder Geraden schneiden.
Uns interessieren hierbei nur die so gewonnenen Schnittpunkte; die eingezeichneten Kreise und Geraden fassen wir als Hilfsobjekte auf, die wir anschließend wegradieren.

Unsere Konstruktionen sollen wiederholbar und exakt beschreibbar sein. Wir dürfen daher unser Lineal bzw. unseren Zirkel nicht wahllos irgendwo auf dem Papier platzieren, sondern richten Lineal bzw. Zirkel an bereits konstruierten Punkten aus:
Wir dürfen das Lineal nur so in die Ebene legen, dass die zu zeichnende Gerade durch zwei bereits konstruierte Punkte verläuft.
Den Zirkel dürfen wir in zwei bereits konstruierte Punkte stechen und so dessen Öffnungswinkel definieren. Mit dieser Zirkelöffnung dürfen wir dann einen Kreis um einen bereits konstruierten Punkt zeichnen. Dies bedeutet, dass wir nur solche Kreise zeichnen dürfen, die einen bereits konstruierten Punkt als Mittelpunkt und als Radius den Abstand zweier bereits konstruierter Punkte besitzen.
Damit wir mit unseren Konstruktionen überhaupt beginnen können, geben wir uns Startpunkte vor, die wir als bereits konstruiert auffassen.

Diese Überlegungen mathematisieren wir jetzt:

Das unendlich große Blatt Papier modellieren wir durch die Ebene $\mathbb{R}^2$. Die Punkte dort beschreiben wir mit Hilfe von kartesischen Koordinaten. Als Menge der Startpunkte definieren wir die Menge $S := \{(0,0),(1,0),(0,1)\} \subseteq \mathbb{R}^2$.
Beginnen wir mit unseren Konstruktionen, so stehen uns nur die Startpunkte zur Verfügung. Wir können daher genau drei Geraden und sechs Kreise einzeichnen: ⁇



In der linken Grafik sind die drei Startpunkte blau, die zu Beginn zulässigen Hilfsobjekte grau eingezeichnet. Beachten Sie, dass insbesondere die x- und die y-Achse zulässig sind.

Die grauen Hilfsobjekte schneiden sich 37 neuen, orange eingezeichneten Punkten. Diese Punkte sind nun konstruiert.

Für die nun folgenden Konstruktionen können wir zusätzlich die in obiger Grafik orange eingezeichneten neuen Punkte benutzen. Hierdurch können wir weitere neue Punkte konstruieren, die weitere Möglichkeiten für Konstruktionen liefern, etc.
Die Anzahl der konstruierten Punkte wächst also nach jedem Konstruktionsschritt. Dies führt auf die folgende rekursive Definition der Konstruierbarkeit:

Definition 21.1 (a) *Jedes Element der Startmenge S nennen wir **konstruierbar**. Weiterhin nennen wir jeden Schnittpunkt zulässiger Hilfsobjekte **konstruierbar**.*

(b) *Wir nennen ein Hilfsobjekt **zulässig**, wenn dieses Objekt*

- *ein Kreis ist, dessen Mittelpunkt konstruierbar ist und dessen Radius dem Abstand zweier konstruierbarer Punkte entspricht, oder*
- *eine Gerade ist, die durch zwei konstruierbare Punkte verläuft.*

Bemerkung 21.2 (a) Nach obiger Definition konstruiert man einen Punkt $P \in \mathbb{R}^2$ rekursiv: Ausgehend von den Startpunkten konstruiert man so lange Schnittpunkte zulässiger Hilfsobjekte, bis man P selbst als Schnittpunkt zulässiger Hilfsobjekte konstruiert hat. Die Möglichkeiten für zulässige Hilfsobjekte nehmen dabei in jedem Schritt zu.

Die für die Konstruktion von P notwendigen konstruierten Punkte bezeichnen wir als **Hilfspunkte**.

(b) Ist ein Punkt $P \in \mathbb{R}^2$ konstruierbar, so existiert wegen (a) eine **Konstruktionsbeschreibung für P**: Wir können exakt angeben, welche Hilfspunkte durch Schnitt welcher Hilfsobjekte erzeugt wurden und wie aus diesen P konstruiert wurde.

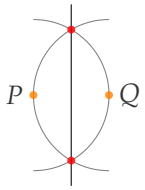
Aufgrund dieser Beschreibung ist die Konstruktion von P wiederholbar. Ferner folgt, dass die Konstruktion von P ein *endlicher* Prozess ist: P ist nach endlich vielen Schritten konstruiert. ⋇

Wir gießen obige Bemerkung in Satzform:

Satz 21.3 *Ein Punkt ist genau dann konstruierbar, wenn er Element der Startpunktmenge S ist oder sich nach endlich vielen Schritten als Schnittpunkt zulässiger Hilfsobjekte ergibt.*

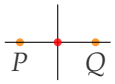
Wir stellen einige Grundkonstruktionen vor:

Beispiel 21.4 (a) Sind P und Q konstruierbare Punkte, so ist die Mittelsenkrechte der Strecke PQ zulässig:



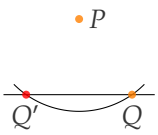
Man zeichnet Kreise mit Radius $|PQ|$ und Mittelpunkt P bzw. Q. In der Grafik links sind Teile dieser Kreise grau eingezeichnet, ihre Schnittpunkte rot.
Die Gerade durch roten Punkte ist dann zulässig und die gesuchte Mittelsenkrechte.

(b) Sind P und Q konstruierbare Punkte, so ist der Mittelpunkt der Strecke PQ konstruierbar:



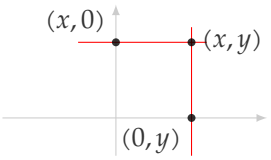
Man schneidet die Mittelsenkrechte der Strecke PQ mit der Verbindungsgeraden von P und Q.

(c) Das Lot durch einen konstruierbaren Punkt P auf eine zulässige Gerade ist zulässig:



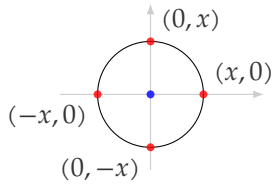
Da die Gerade zulässig ist, liegt auf ihr ein konstruierbarer Punkt Q mit $Q \neq P$. (Warum?) Wir schneiden nun die Gerade mit dem Kreis mit Mittelpunkt P und Radius $|PQ|$ und erhalten den roten Punkt Q'.
Das gesuchte Lot ist die Mittelsenkrechte der Strecke QQ'.

(d) Ein Punkt (x, y) ist genau dann konstruierbar, wenn die Punkte $(x, 0)$ und $(0, y)$ konstruierbar sind:



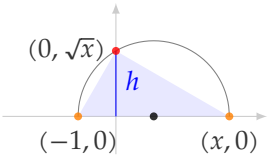
Ist (x, y) konstruierbar, so erhält man $(x, 0)$ bzw. $(0, y)$ als Schnittpunkt der Lote (rot gezeichnet) auf die (zulässige) x- bzw. y-Achse.
Sind umgekehrt $(x, 0)$ und $(0, y)$ konstruierbar, so sind die roten Geraden die Lote durch $(x, 0)$ bzw. $(0, y)$ auf die x- bzw. y-Achse. Sie schneiden sich in (x, y).

(e) Die Konstruierbarkeit der Punkte $(x, 0)$, $(-x, 0)$, $(0, x)$ und $(0, -x)$ ist zueinander äquivalent:



x- und y-Achse sind zulässig, der blau eingezeichnete Ursprung ist als Startpunkt konstruierbar.
Ist einer der rot eingezeichneten Punkte konstruierbar, so sind auch die übrigen roten Punkte konstruierbar.

(f) Ist der Punkt $(x, 0) \in \mathbb{R}^2$ mit $x > 0$ konstruierbar, so ist auch $(0, \sqrt{x})$ konstruierbar:



$(-1, 0)$ ist nach (e) konstruierbar, $(x, 0)$ nach Voraussetzung. (b) liefert die Konstruierbarkeit des schwarzen Mittelpunkts. Der grau eingezeichnete Thaleskreis ist zulässig.
Nach dem Höhensatz folgt $h^2 = 1 \cdot x$. Der rote Punkt hat daher die Koordinaten $(0, \sqrt{x})$.

※

Algebra: Wie übersetzt man Konstruktionen in algebraische Objekte?

Nach 21.3 ist ein Punkt $(x, y) \in \mathbb{R}^2$ genau dann konstruierbar, wenn es eine Konstruktionsbeschreibung für (x, y) gibt. Dies bedeutet, dass $n \in \mathbb{N}$ und Hilfspunkte

$$(x_1, y_1), (x_2, y_2), \dots, (x_n, y_n) \in \mathbb{R}^2$$

existieren, so dass

- der Hilfspunkt (x_k, y_k) nur unter Verwendung der vorherigen Hilfspunkte (x_i, y_i) mit $i < k$ oder der Startpunkte konstruiert werden kann und
- $(x_n, y_n) = (x, y)$ gilt.

Mit Hilfe der Koordinaten der Hilfspunkte definieren wir nun Erweiterungskörper von $\mathbb{Q}$: Wir setzen $K_0 := \mathbb{Q}$ und $K_{i+1} := K_i(x_{i+1}, y_{i+1})$ für $i \in \{0, \dots, n-1\}$. Es ist also

$$K_i = \mathbb{Q}(x_1, y_1,\ x_2, y_2,\ \dots,\ x_i, y_i) \qquad \text{für } i \in \{0, \dots, n\}.$$

Die Körper K_i sind ineinander enthalten: Es gilt $K_0 \subseteq K_1 \subseteq \cdots \subseteq K_n \subseteq \mathbb{R}$. Im Schritt $K_i \to K_{i+1}$ wurden zwei zulässige Objekte miteinander geschnitten und die Koordinaten des Schnittpunkts an K_i adjungiert. Wir untersuchen, wie sich dies auf den Körpergrad $[K_{i+1} : K_i]$ auswirkt:

Lemma 21.5 *Mit den obigen Bezeichnungen gilt* $[K_{i+1} : K_i] \in \{1, 2\}$ *für alle* i.

Beweisskizze. Es gilt $K_{i+1} = K_i(x_{i+1}, y_{i+1})$. Der Punkt $P := (x_{i+1}, y_{i+1})$ ist Schnittpunkt zweier zulässiger Objekte. Wir können daher P als Element der Lösungsmenge eines Gleichungssystems auffassen. Durch genaue Analyse, wie man dieses Gleichungssystem löst, erhält man Aussagen über die Grade von x_{i+1} bzw. y_{i+1} über K_i und beweist so den Satz. ?
Wir führen den Beweis für den schwierigsten Fall vor: Sei P Schnittpunkt zweier zulässiger Kreise. Dann ist P eine Lösung eines Gleichungssystems der Form

$$\text{(I)}:\ (X - a_1)^2 + (Y - b_1)^2 = r_1^2 \qquad \text{und} \qquad \text{(II)}:\ (X - a_2)^2 + (Y - b_2)^2 = r_2^2,$$

wobei $a_1, a_2, b_1, b_2, r_1^2, r_2^2 \in K_i$ sind. ?
Die Gleichung (I)-(II) ist eine in X und Y lineare Gleichung, da sich die quadratischen Terme X^2 und Y^2 wegheben. Löst man (I)-(II) beispielsweise nach X auf und setzt in (I) ein, so ergibt sich eine quadratische Gleichung in Y. Es folgt $[K_i(y_{i+1}) : K_i] \in \{1, 2\}$, je nachdem, ob bei der Lösung der quadratischen Gleichung ein Quadrat aus K_i unter der Wurzel stand oder nicht.
x_{i+1} erhält man nun, indem man y_{i+1} in die lineare Gleichung (I)-(II) einsetzt und nach X auflöst. Es folgt daher $K_{i+1} = K_i(x_{i+1}, y_{i+1}) = K_i(y_{i+1})$ und somit $[K_{i+1} : K_i] \in \{1, 2\}$. ■

Wir erhalten aus dem Lemma ein notwendiges Kriterium für die Konstruierbarkeit eines Punkts. Beachten Sie, dass der Fall $[K_{i+1} : K_i] = 1$ aus obigem Lemma die Gleichheit $K_{i+1} = K_i$ liefert und daher im folgenden Satz vernachlässigt werden kann.

Satz 21.6 *Der Punkt $(x,y) \in \mathbb{R}^2$ sei konstruierbar. Dann existieren ein $n \in \mathbb{N}_0$ und Körper $K_0 := \mathbb{Q} \subseteq K_1 \subseteq \cdots \subseteq K_n \subseteq \mathbb{R}$ mit $[K_{i+1} : K_i] = 2$ für alle i, so dass $x, y \in K_n$ gilt.*

K_n
| 2
⋮
| 2
K_1
| 2
$K_0 = \mathbb{Q}$

Bemerkung 21.7 Im obigen Satz tauchen Körper K_i auf, die $K_i \subseteq K_{i+1}$ erfüllen. Zudem ist stets $[K_{i+1} : K_i] = 2$. Man nennt eine solche Anordnung von Körpern einen **(reellen) 2-Körperturm**. Die Bezeichnung *Turm* kommt von grafischen Darstellung, die Sie am Rand sehen.
Wir können 21.6 nun sehr knapp formulieren:
Ist ein Punkt $(x,y) \in \mathbb{R}^2$ konstruierbar, so liegen x und y in einem reellen 2-Körperturm über $\mathbb{Q}$. ⁜

Mit Hilfe der folgenden Definition übertragen wir den Begriff des Konstruierens auf reelle Zahlen:

Definition 21.8 *Wir nennen eine reelle Zahl x **konstruierbar**, wenn der Punkt $(x,0) \in \mathbb{R}^2$ konstruierbar ist.*

Bemerkung 21.9 (a) Wegen 21.4 (e) ist $x \in \mathbb{R}$ genau dann konstruierbar, wenn einer (und damit alle) der Punkte $(\pm x, 0)$ bzw. $(0, \pm x)$ konstruierbar ist.

(b) Wegen 21.4 (d) ist ein Punkt $P \in \mathbb{R}^2$ genau dann konstruierbar, wenn beide Koordinaten von P konstruierbar sind.

Die Frage nach der Konstruierbarkeit eines Punkts P lässt sich also auf die Frage nach der Konstruierbarkeit der Koordinaten von P reduzieren. ⁜

Aus 21.6 und Teil (b) der obigen Bemerkung folgt ein weiteres notwendiges Kriterium für Konstruierbarkeit:

Korollar 21.10 *Ist die reelle Zahl $x \in \mathbb{R}$ konstruierbar, so ist der Grad $[\mathbb{Q}(x) : \mathbb{Q}]$ eine Zweierpotenz. Insbesondere ist x algebraisch über $\mathbb{Q}$.*

Beweis. Nach 21.6 ist x in einem endlichen 2-Körperturm über $\mathbb{Q}$ enthalten. Bezeichnen wir den Oberkörper des Turms mit K_n, so gilt nach Gradformel $[K_n : \mathbb{Q}] = 2^n$ und $\mathbb{Q}(x) \subseteq K_n$. Wieder mit Gradformel folgt $[\mathbb{Q}(x) : \mathbb{Q}] = 2^r$ mit einem $r \leq n$.
Der „Insbesondere"-Teil folgt aus 20.24. ■

Die Unmöglichkeit der klassischen Konstruktionsprobleme

Die Quadratur des Kreises Zu einem gegebenen Kreis soll ein flächeninhaltsgleiches Quadrat konstruiert werden.
Für manche Kreise ist dieses Problem lösbar, z. B. für Kreise mit Radius $\frac{1}{\sqrt{\pi}}$. Im Allgemeinen ist das Problem aber unlösbar; beispielsweise ist die Quadratur des Einheitskreises nicht zu bewerkstelligen:
Wäre der Einheitskreis quadrierbar, so könnte man ein Quadrat mit Flächeninhalt π, also mit Seitenlänge $\sqrt{\pi}$ konstruieren. Dann wäre aber auch die reelle Zahl $\sqrt{\pi}$ konstruierbar, was 21.10 widerspricht, denn mit π ist auch $\sqrt{\pi}$ transzendent.

Die Würfelverdoppelung / Das Delische Problem Einer Legende nach befragten die Einwohner der Insel Delos um 430 v. Chr. ihr Orakel, wie eine Pestepidemie zu bekämpfen sei. Dieses riet, den würfelförmigen Altar im Tempel des Apollon im Volumen zu verdoppeln, ohne aber seine würfelförmige Geometrie zu verändern. (Ebenfalls legendär: Man verdoppelte daraufhin die *Seitenlänge* des Altars, woraufhin sich die Pest verschlimmerte.)
Es gibt würfelförmige Altäre, die sich konstruktiv im Volumen verdoppeln lassen, z. B. solche der Seitenlänge $\sqrt[3]{4}$. Im Allgemeinen ist das Problem aber nicht lösbar, beispielsweise für einen würfelförmigen Altar der Seitenlänge Eins: ?
In diesem Fall ist ein würfelförmiger Altar des Volumens Zwei, also eine Strecke der Länge $\sqrt[3]{2}$ zu konstruieren. Dies gelingt genau dann, wenn die reelle Zahl $\sqrt[3]{2} \in \mathbb{R}$ konstruierbar ist. Da $\sqrt[3]{2}$ das Minimalpolynom $X^3 - 2 \in \mathbb{Q}[X]$ besitzt (Eisenstein mit $p = 2$), hat $\sqrt[3]{2}$ jedoch Grad drei über $\mathbb{Q}$ und ist nach 21.10 nicht konstruierbar.

Winkeldreiteilung Sei $P := (\cos\varphi, \sin\varphi)$ ein konstruierbarer Punkt auf dem Einheitskreis. Gefragt wird, ob auch der Punkt $Q := (\cos\frac{\varphi}{3}, \sin\frac{\varphi}{3})$ konstruierbar ist. (Was hat diese Fragestellung mit dem Begriff *Winkeldreiteilung* zu tun?) ?
Es gibt Winkel, für die die Winkeldreiteilung möglich ist, z. B. für $\varphi = \pi = 180°$. Im Allgemeinen ist das Problem aber nicht lösbar, beispielsweise für $\varphi = \frac{\pi}{3} = 60°$:
Für $\varphi = \frac{\pi}{3}$ ist P ein konstruierbarer Punkt, denn gleichseitige Dreiecke sind konstruierbar. (Wie? Und warum folgt hieraus die Konstruierbarkeit von P?) ?
Wir setzen $\alpha := \frac{\varphi}{3}$. Die Konstruierbarkeit von Q ist äquivalent zur Konstruierbarkeit der reellen Zahl $\cos\alpha$: Ist Q konstruierbar, so auch $\cos\alpha$ nach 21.4 (d). Ist $\cos\alpha$ konstruierbar, so auch Q als Schnittpunkt des Lots durch $(\cos\alpha, 0)$ auf die x-Achse mit dem Einheitskreis.
Wir bestimmen das Minimalpolynom von $\cos\alpha$. Es gilt $\exp(\varphi i) = \exp(3\alpha i)$ und somit

$$\begin{aligned}\exp(\varphi i) = \exp(\alpha i)^3 \quad \Longleftrightarrow \quad \cos\varphi + i\cdot\sin\varphi &= (\cos\alpha + i\cdot\sin\alpha)^3 \\ &= \cos^3\alpha - 3\sin^2\alpha\cos\alpha + i\cdot(3\sin\alpha\cos^2\alpha - \sin^3\alpha).\end{aligned}$$

Wir betrachten nun die Realteile der letzten Gleichung, setzen $X := \cos\alpha$ und benutzen die Identitäten $X^2 = 1 - \sin^2\alpha$ und $\cos\varphi = \frac{1}{2}$. Dann ist $\frac{1}{2} = X^3 - 3(1 - X^2)X$. Es folgt, dass

$$f := 4X^3 - 3X - \frac{1}{2} \in \mathbb{Q}[X]$$

ein annullierendes Polynom für $\cos\alpha$ ist. Mit den Methoden aus Vorlesung 19 kann man zeigen, dass f irreduzibel ist. Damit hat die Erweiterung $\mathbb{Q}(\cos\alpha)|\mathbb{Q}$ den Grad Drei. Nach 21.10 sind $\cos\alpha$ und daher Q nicht konstruierbar. Ein 60°-Winkel ist also nicht drittelbar.

Charakterisierung der konstruierbaren Punkte

Wir haben 21.6 nur als notwendiges Kriterium formuliert. Tatsächlich gilt aber im Satz eine Äquivalenz:

Satz 21.11 *Der Punkt $(x, y) \in \mathbb{R}^2$ ist **genau dann** konstruierbar, wenn ein reeller 2-Körperturm $K_0 := \mathbb{Q} \subseteq K_1 \subseteq \cdots \subseteq K_n \subseteq \mathbb{R}$ existiert, so dass $x, y \in K_n$ gilt.*

Wir geben eine grobe Skizze des Beweises, die Feinarbeit erledigen wir dann in den Übungen. → Übung

Beweisskizze. Wegen 21.6 ist nur noch die Rückrichtung zu zeigen: Gegeben sei ein reeller 2-Körperturm $K_0 := \mathbb{Q} \subseteq K_1 \subseteq \cdots \subseteq K_n \subseteq \mathbb{R}$. Wir beweisen, dass alle Elemente aus K_n konstruierbar sind. Dann folgt die Behauptung direkt aus 21.9 (b).
Wir argumentieren in zwei Schritten:

Schritt 1: Konstruierbarkeit der Grundrechenarten Seien $a, b \in \mathbb{R}$ konstruierbar. Wir zeigen, dass dann auch $a \pm b$, $a \cdot b$ und, falls $b \neq 0$, auch $\frac{a}{b}$ konstruierbar sind. Dies erfolgt mit Hilfe geometrischer Überlegungen, beispielsweise mit Hilfe des Strahlensatzes.

Schritt 2: Induktion Wir zeigen, dass alle Elemente aus K_i mit $i \in \{0, 1, \ldots, n\}$ konstruierbar sind.

Der Fall $i = 0$ folgt direkt aus Schritt 1: Da 0 und 1 konstruierbar sind, ist $\mathbb{Z}$ konstruierbar. Mit Hilfe von Division folgt, dass alle Elemente aus $\mathbb{Q} = K_0$ konstruierbar sind.

Sei nun bereits gezeigt, dass alle Elemente aus K_i konstruierbar sind. Da die Erweiterung $K_{i+1}|K_i$ quadratisch ist, folgt nach 20.15 (a) die Existenz eines $a \in K_{i+1}$ mit

$$K_{i+1} = \{r \cdot 1 + s \cdot a \mid r, s \in K_i\}$$

a hat ein Minimalpolynom vom Grad Zwei über K_i. Die Lösungsformel für quadratische Gleichungen und 21.4 (f) zeigen, dass a konstruierbar ist. Aus Schritt 1 ergibt sich nun, dass jedes Element aus K_{i+1} konstruierbar ist. ■

Bemerkung 21.12 Die Aussage in 21.10 lässt sich nicht zu einer Äquivalenz ausbauen: Um die Rückrichtung

$$\mathbb{Q}(x)|\mathbb{Q} \text{ hat 2-Potenz} \Longrightarrow x \text{ ist konstruierbar}$$

zu zeigen, müsste man nach obigem Satz in der Erweiterung $\mathbb{Q}(x)|\mathbb{Q}$ passende Zwischenkörper K_i finden, so dass ein 2-Körperturm

$$K_0 := \mathbb{Q} \subseteq K_1 \subseteq \cdots \subseteq K_n = \mathbb{Q}(x)$$

entsteht. Wir werden später im Rahmen der Galoistheorie sehen, dass dies typischerweise nicht möglich ist. ※

22. Kronecker-Adjunktion, Zerfällungskörper

Worum geht es? Wir beschäftigen uns nochmals mit algebraischen und transzendenten Elementen und geben Beispiele. Danach stellen wir mit der *Kronecker-Adjunktion* eine Technik vor, mit der man Oberkörper eines gegebenen Körpers „aus dem Nichts" heraus konstruieren kann. Diese Technik benutzen wir dann, um zu zeigen, dass jedes Polynom $f \in K[X]$ mit $f \neq 0$ in einer endlichen Erweiterung von K vollständig in Linearfaktoren zerfällt. Minimale solche Erweiterungen werden wir *Zerfällungskörper* nennen. ⋇

Nochmals Körpererweiterungen, Transzendenz

Wir fassen unsere Ergebnisse über einfache Körpererweiterungen und algebraische Elemente zusammen:

Satz 22.1 (Charakterisierung algebraischer Elemente) *Seien $L|K$ eine Körpererweiterung und $a \in L$. Dann sind äquivalent:*

(a) *a ist algebraisch, d.h. es existiert $f \in K[X]$ mit $f(a) = 0$ und $f \neq 0$.*

(b) *$K[a] = K(a)$.*

(c) *a besitzt ein Minimalpolynom über K; sein Grad stimmt mit $[K(a) : K]$ überein.*

(d) *$K(a)|K$ ist eine endliche Erweiterung.*

Durch Verneinen der Aussagen in obigem Satz erhalten wir eine Charakterisierung transzendenter Elemente:

Satz 22.2 (Charakterisierung transzendenter Elemente) *Seien $L|K$ eine Körpererweiterung und $a \in L$. Dann sind äquivalent:*

(a) *a ist transzendent, d.h. aus $f(a) = 0$ mit $f \in K[X]$ folgt $f = 0$.*

(b) *$K[a]$ ist eine echte Teilmenge von $K(a)$; insbesondere ist $K[a]$ **kein** Körper.* ⁉

(c) *a besitzt kein Minimalpolynom über K.*

(d) *$K(a)|K$ ist eine unendliche Erweiterung.*

Wir stellen einige typische Techniken im Umgang mit Körpererweiterungen vor:

Beispiel 22.3 (a) Sei $L|K$ eine Körpererweiterung. Für $a, b \in L$ gilt $K(a, b) = K(a)(b)$, denn sowohl $K(a, b)$ als auch $K(a)(b)$ ist ein (bzgl. Mengeninklusion) minimaler Körper, der die Menge $K \cup \{a, b\}$ enthält.

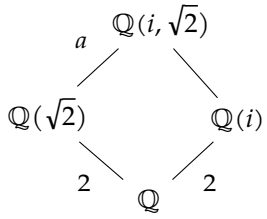
Induktiv folgt $K(a_1, \dots, a_n) = K(a_1)(a_2) \cdots (a_n)$ für beliebige $a_1, \dots, a_n \in L$. Den Körper $K(a_1, \dots, a_n)$ kann man also schrittweise durch Adjunktionen von jeweils nur einem einzigen Element aufbauen. ⁉

(b) Seien $p \in \mathbb{P}$ eine Primzahl und $n \in \mathbb{N}$. Das Element $\sqrt[n]{p} \in \mathbb{R}$ ist algebraisch über $\mathbb{Q}$. Sein Minimalpolynom ist $m := X^n - p \in \mathbb{Q}[X]$; dies folgt aus 20.20, denn m annulliert $\sqrt[n]{p}$, ist normiert und nach Eisenstein irreduzibel. Mit 20.23 folgen $[\mathbb{Q}(\sqrt[n]{p}) : \mathbb{Q}] = n$ und

$$\mathbb{Q}(\sqrt[n]{p}) = \left\{q_0 + q_1 \cdot \sqrt[n]{p} + \cdots + q_{n-1} \cdot \sqrt[n]{p^{n-1}} : q_i \in \mathbb{Q}\right\}.$$

Beispielsweise ist $\mathbb{Q}(\sqrt[3]{2}) = \left\{q_0 + q_1 \cdot \sqrt[3]{2} + q_2 \cdot \sqrt[3]{4} : q_i \in \mathbb{Q}\right\}$ eine Grad-3-Erweiterung.

(c) Es gilt $[\mathbb{Q}(i) : \mathbb{Q}] = 2 = [\mathbb{Q}(\sqrt{2}) : \mathbb{Q}]$. Wir berechnen den Grad der Erweiterung $\mathbb{Q}(i, \sqrt{2})|\mathbb{Q}$ mit Hilfe der Gradformel:



Links haben wir die Erweiterung $\mathbb{Q}(i, \sqrt{2})|\mathbb{Q}$ zusammen mit den Zwischenkörpern $\mathbb{Q}(i)$ und $\mathbb{Q}(\sqrt{2})$ gezeichnet. Die Striche bedeuten eine Teilmengen-Beziehung, die Zahlen bzw. Buchstaben an den Strichen stehen für den Körpergrad. Nach Gradformel gilt

$$[\mathbb{Q}(i, \sqrt{2}) : \mathbb{Q}] = [\mathbb{Q}(i, \sqrt{2}) : \mathbb{Q}(\sqrt{2})] \cdot [\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2a.$$

Um den gesuchten Körpergrad zu berechnen, benötigen wir a. Hierzu betrachten wir die einfache Erweiterung $\mathbb{Q}(\sqrt{2})(i)|\mathbb{Q}(\sqrt{2})$. Das Polynom X^2+1 ist über $\mathbb{Q}(\sqrt{2})$ definiert und annulliert i. Daher gilt $a \leq 2$. (Warum folgt noch nicht $a = 2$?)

Allerdings ist $\mathbb{Q}(i, \sqrt{2})$ ein echter Oberkörper von $\mathbb{Q}(\sqrt{2})$ wegen $\mathbb{Q}(\sqrt{2}) \subseteq \mathbb{R}$ und $\mathbb{Q}(i, \sqrt{2}) \not\subseteq \mathbb{R}$. Dies zeigt $a > 1$ nach 20.11 (d).

Insgesamt ergibt sich $a = 2$ und somit $[\mathbb{Q}(i, \sqrt{2}) : \mathbb{Q}] = 4$.

(d) Sei $L|\mathbb{Q}$ eine quadratische Körpererweiterung. Wir wissen bereits aus 20.15 (a), dass jedes $a \in L \setminus \mathbb{Q}$ ein primitives Element der Erweiterung $L|\mathbb{Q}$ ist. Wir suchen nun besonders „schöne“ primitive Elemente für $L|\mathbb{Q}$ und klassifizieren so alle quadratischen Erweiterungen von $\mathbb{Q}$:

Sei $a \in L \setminus \mathbb{Q}$ beliebig. Es ist $L = \mathbb{Q}(a)$. Wegen $[\mathbb{Q}(a) : \mathbb{Q}] = 2$ ist das Minimalpolynom von a von der Form $m = X^2 + pX + q \in \mathbb{Q}[X]$. Die Lösungsformel für quadratische Gleichungen zeigt $a \in x \pm \sqrt{y}$ mit gewissen $x, y \in \mathbb{Q}$, wobei $\sqrt{y} \notin \mathbb{Q}$ ist. Nun gilt

$$L = \mathbb{Q}(a) = \mathbb{Q}(x \pm \sqrt{y}) \overset{x \in \mathbb{Q}}{=} \mathbb{Q}(\pm\sqrt{y}) \overset{\pm 1 \in \mathbb{Q}}{=} \mathbb{Q}(\sqrt{y}).$$

L entsteht also, indem man an $\mathbb{Q}$ einen Ausdruck der Form $\sqrt{y}$ mit $y \in \mathbb{Q}$ und $\sqrt{y} \notin \mathbb{Q}$ adjungiert. Umgekehrt ist die Erweiterung $\mathbb{Q}(\sqrt{y})|\mathbb{Q}$ unter diesen Voraussetzungen an y quadratisch.

Damit folgt: Die quadratischen Erweiterungen von $\mathbb{Q}$ sind genau von der Form $\mathbb{Q}(\sqrt{y})|\mathbb{Q}$ mit $y \in \mathbb{Q}$ und $\sqrt{y} \notin \mathbb{Q}$. ⁂

Aus den Äquivalenzen in 22.1 lassen sich viele Beweistechniken für algebraische Elemente ableiten. Mit algebraischen Elementen lässt sich daher recht bequem arbeiten. Dies ist bei transzendenten Elementen anders; hier sind viele Fragestellungen offen. Die folgende Bemerkung illustriert dies:

Bemerkung 22.4 (a) Seien a, b algebraische Elemente über einem Körper K. Dann gilt

$$[K(a,b):K] = [K(a,b):K(a)]\cdot[K(a):K] \overset{22.3\,(a)}{=} [K(a)(b):K(a)]\cdot[K(a):K]$$
$$\overset{(\star)}{=} \underbrace{[K(a)(b):K(a)]}_{<\infty,\text{ siehe }(\star)}\cdot\underbrace{[K(a):K]}_{<\infty\text{ nach }22.1\,(d)} < \infty.$$

(Zu $(\star)$: b besitzt ein Minimalpolynom m über K. Es gilt $m \in K(a)[X]$. Somit besitzt b ein annullierendes Polynom (Ist m auch minimal?) über $K(a)$ und ist algebraisch über $K(a)$.) ?

Hieraus folgt die Algebraizität von $a+b$ über K: Der Körper $K(a+b)$ ist ein Zwischenkörper der Erweiterung $K(a,b)|K$ und somit endlich über K. Nach 22.1 (d) ist $a+b$ algebraisch über K.

Dieselbe Schlussweise funktioniert auch für die Elemente $a-b$, ab und, falls $b \neq 0$, auch für a/b. Dies zeigt, dass Summen, Differenzen, Produkte und Quotienten (falls definiert) von algebraischen Elementen wieder algebraisch sind.

(b) Sei $L|K$ eine Körpererweiterung. Wir bezeichnen mit A die Menge aller Elemente aus L, die algebraisch über K sind. Dann ist A wegen (a) ein Zwischen*körper* der Erweiterung $L|K$. ?

(c) Der Umgang mit transzendenten Elementen ist oft schwierig; Summen und Produkte transzendenter Elemente sind i. A. nicht transzendent. ?

Über $\mathbb{Q}$ stehen mit den Sätzen von Lindemann-Weierstraß[2] und Gelfond-Schneider[3] Techniken zur Verfügung, mit denen man die Transzendenz gewisser Zahlen zeigen kann. Aus diesen Sätzen folgt beispielsweise, dass π, e und e^π über $\mathbb{Q}$ transzendent sind. Offen ist hingegen, ob $e+\pi$ oder π^e transzendent über $\mathbb{Q}$ sind. Es ist nicht einmal geklärt, ob diese beiden Zahlen in $\mathbb{Q}$ liegen!

Aufgrund der fehlenden Abschlusseigenschaften lässt sich (b) nicht nachstellen: Eine Menge von transzendenten Elementen ist *nie* ein Körper. ⁂

Teil (b) der obigen Bemerkung sagt, dass Mengen von algebraischen Elementen Körperstruktur haben können. Dies motiviert die folgende Definition:

Definition 22.5 *Eine Körpererweiterung $L|K$ heißt **algebraisch**, wenn jedes Element aus L algebraisch über K ist.*

Beispiel 22.6 (a) Jede endliche Erweiterung $L|K$ ist algebraisch:

Sei $a \in L$ beliebig. Dann ist $K(a)$ ein Zwischenkörper von $L|K$ und endlich über K, vgl. 20.12. Nach 22.1 (d) ist a algebraisch über K.

[2] https://de.wikipedia.org/wiki/Satz_von_Lindemann-Weierstraß
[3] https://de.wikipedia.org/wiki/Satz_von_Gelfond-Schneider

(b) Seien K ein Körper und M eine Menge von über K algebraischen Elementen. Dann ist die Erweiterung $K(M)|K$ algebraisch:

Die Elemente aus $K(M)$ sind Summen, Produkte, Differenzen und Quotienten von Elementen aus $K \cup M$. Da jedes Element aus $K \cup M$ algebraisch über K ist, ist jedes Element aus $K(M)$ algebraisch über K, vgl. 22.4 (a).

(c) Seien $L|K$ eine Körpererweiterung und Z ein beliebiger Zwischenkörper. Wir werden in den Übungen zeigen, dass $L|K$ genau dann algebraisch ist, wenn die beiden Teilerweiterungen $L|Z$ und $Z|K$ algebraisch sind. → Übung

(d) Es sei $M := \{\sqrt{p} \mid p \in \mathbb{P}\} \subseteq \mathbb{R}$. Die Körpererweiterung $\mathbb{Q}(M)|\mathbb{Q}$ ist nach (b) algebraisch. Man kann zeigen, dass M linear unabhängig über $\mathbb{Q}$ ist und somit $[\mathbb{Q}(M) : \mathbb{Q}] = \infty$ gilt.

Dies zeigt, dass durch (a) die algebraischen Erweiterungen nicht charakterisiert werden: Endliche Erweiterungen sind stets algebraisch, es gibt aber unendliche algebraische Erweiterungen. ⁜

Kronecker-Adjunktion

Wir haben in der Körpertheorie bis jetzt stets die Existenz passender Oberkörper L vorausgesetzt: Körperadjunktionen finden in gegebenen Oberkörpern L statt, algebraische Elemente liegen in gegebenen Körpern L, usw.
Diese Herangehensweise ist äußerst bequem: Von vornherein weiß man, dass alle Überlegungen, Rechnungen, Beweise, etc. in L stattfinden werden. Man muss diese Menge nie verlassen, alle Schlussweisen sind problemlos möglich.

In der Praxis sieht die Situation oft anders aus:

Beispiel 22.7 Wir betrachten das normierte und irreduzible (da nullstellenfrei, vgl. 19.5) Polynom $m := X^2 + X + 1 \in \mathbb{Z}_2[X]$. Wegen 20.20 (b) könnte m ein Minimalpolynom sein. Hierzu müssten wir aber die Existenz einer Nullstelle von m in irgendeinem Erweiterungskörper von $\mathbb{Z}_2$ nachweisen. Dies ist uns momentan nicht möglich, weil wir keinen Erweiterungskörper von $\mathbb{Z}_2$ kennen. ⁜

Das Beispiel verdeutlicht eine große Schwachstelle unserer bisherigen Körpertheorie: Wir haben Körpererweiterungen studiert, kennen allerdings keine Methoden zur Konstruktion von Oberkörpern.

Abhilfe schaffen der Einsetzhomomorphismus aus 15.11 und folgende Beobachtungen von Kronecker:

Satz 22.8 (Kronecker) *Seien K ein Körper, a ein über K algebraisches Element (aus irgendeinem Oberkörper von K) und $m \in K[X]$ das Minimalpolynom von a über K. Dann ist die Abbildung*

$$\varphi : K[X]/(m) \to K(a), \qquad \overline{f} \mapsto f(a)$$

ein Körperisomorphismus mit Umkehrabbildung

$$\varphi^{-1}: K(a) \to K[X]/(m), \quad \sum_{i=0}^{\deg m-1} k_i a^i \mapsto \overline{\sum_{i=0}^{\deg m-1} k_i X^i}.$$

Beweis. Es sei $e_a : K[X] \to K(a)$ der Einsetzhomomorphismus mit $f \mapsto f(a)$. Da $K(a) = K[a]$ nach 22.1 (b) gilt, ist e_a surjektiv. Wegen 15.12 und 20.21 stimmt der Kern von e_a mit dem vom Minimalpolynom m erzeugten Hauptideal (m) überein. Der Homomorphiesatz zeigt, dass die im Satz angegebene Abbildung $\varphi : K[X]/(m) \to K(a)$ mit $\overline{f} \mapsto e_a(f) = f(a)$ ein Ringisomorphismus ist. Da $K(a)$ ein Körper ist, folgt, dass auch $K[X]/(m)$ ein Körper ist. φ ist somit ein Körperisomorphismus.
Wir leiten nun die Abbildungsvorschrift für φ^{-1} her. Hierzu betrachten wir ein beliebiges Element $y \in K(a)$. Nach 20.23 lässt sich y schreiben in der Form $\sum_{i=0}^{\deg m-1} k_i a^i$. Wegen $\varphi\big(\overline{\sum_{i=0}^{\deg m-1} k_i X^i}\big) = \sum_{i=0}^{\deg m-1} k_i a^i$ ist somit $\overline{\sum_{i=0}^{\deg m-1} k_i X^i} \in K[X]/(m)$ das eindeutige Urbild von y. ■

Bemerkung 22.9 Wir untersuchen die Körperisomorphismen φ und φ^{-1} aus obigem Satz genauer:

(a) Es gilt $K \cong \varphi^{-1}(K) = \{\overline{k} \mid k \in K\}$. Somit enthält $K[X]/(m)$ den Unterkörper $\varphi^{-1}(K)$, der zu K isomorph ist. Wir fassen daher $K[X]/(m)$ zukünftig als Oberkörper von K auf (mathematisch nicht ganz exakt).

(b) Nach 20.23 lässt sich jedes Element aus $K(a)$ eindeutig als K-Linearkombination in den Potenzen $a^0, a^1, \ldots, a^{\deg m-1}$ schreiben. Dies überträgt sich durch den Isomorphismus φ^{-1} auf $K[X]/(m)$: Jede Nebenklasse aus $K[X]/(m)$ lässt sich darstellen in der Form $\overline{\sum_{i=0}^{\deg m-1} k_i X^i}$, wobei die Koeffizienten $k_i \in K$ eindeutig durch die Nebenklasse bestimmt sind. Diese Darstellung der Elemente aus $K[X]/(m)$ nennen wir auch ihre **Standarddarstellung**.

Aus der Tatsache, dass jede Nebenklasse eine eindeutige Standarddarstellung besitzt, folgt, dass die Potenzen $\overline{X^0}, \overline{X^1}, \ldots, \overline{X^{\deg m-1}}$ eine K-Basis von $K[X]/(m)$ bilden und dass $[K[X]/(m) : K] = \deg m$ ist.

(c) Wir betrachten das Polynom m über dem Körper $K[X]/(m)$, also im Polynomring $K[X]/(m)[T]$. Die Polynomvariable bezeichnen wir hierbei mit T, weil der Variablenname X bereits benutzt wurde. Dann ist $\overline{X}$ eine Nullstelle von m, denn es ist

$$m(\overline{X}) = \overline{m} \overset{\overline{m} \in (m)}{=} \overline{0}.$$

(d) Insgesamt haben wir mit dem Körper $K[X]/(m)$ einen Erweiterungskörper von K konstruiert, der eine Nullstelle von m enthält und minimal möglichen Grad (nämlich $\deg m$) über K besitzt.

22.8 sagt also aus, dass $K[X]/(m)$ eine alternative Darstellung für den Körper $K(a)$ ist, der durch die Adjunktion einer Nullstelle von m an K entsteht. Man spricht hier auch von der Technik der **Kronecker-Adjunktion**.

Beachten Sie, dass die Kronecker-Adjunktion eine **oberkörperfreie** Technik ist: Die auftretenden Objekte $K[X]$, $m \in K[X]$ und $K[X]/(m)$ erfordern nur die Kenntnis von K bzw. des Polynomrings über K. ⁜

Beispiel 22.10 Wir betrachten das Polynom $m = X^2 + X + 1 \in \mathbb{Z}_2[X]$ aus 22.7. Der Körper

$$L := \mathbb{Z}_2[X]/(m) = \{\overline{a_0 + a_1 X} : a_0, a_1 \in \mathbb{Z}_2\}$$

ist eine quadratische Erweiterung von $\mathbb{Z}_2$ und hat Ordnung vier. Das Element $\overline{X} \in L$ ist eine Nullstelle von m. Nach 15.21 gilt $K^\times \cong C_3$. Tatsächlich hat das Element $\overline{X} \in K$ multiplikative Ordnung drei wegen

$$\begin{aligned}
\overline{X} &\overset{22.9\,(b)}{\neq} \overline{1}, \\
\overline{X^2} &= \overline{X^2} + \overline{0} = \overline{X^2} + \overline{X^2 + X + 1} = \overline{2X^2 + X + 1} \overset{2=0}{=} \overline{X + 1} \overset{22.9\,(b)}{\neq} \overline{1}, \\
\overline{X^3} &= \overline{X} \cdot \overline{X^2} \overset{\text{s.o.}}{=} \overline{X} \cdot \overline{X + 1} = \overline{X^2 + X} + \underbrace{\overline{X^2 + X + 1}}_{=\overline{0}} = \overline{2X^2 + 2X + 1} \overset{2=0}{=} \overline{1}.
\end{aligned}$$

In ähnlicher Weise lassen sich auch endliche Körper mit höheren Ordnungen konstruieren. Wir gehen hierauf in Vorlesung 24 näher ein. ⁜

Eine erstaunliche Konsequenz der Kronecker-Adjunktion ist, dass der Isomorphietyp des Körpers $K(a)$ nur vom Minimalpolynom von a abhängt:

Korollar 22.11 *Seien K ein Körper, a ein über K algebraisches Element und $m \in K[X]$ das Minimalpolynom von a über K. Sei b eine beliebige Nullstelle von m. Dann gilt $K(a) \cong K(b)$, wobei der zugehörige Isomorphismus die Abbildungsvorschriften $k \mapsto k$ für alle $k \in K$ und $a \mapsto b$ erfüllt.*

Die Adjunktion einer Nullstelle eines irreduziblen Polynoms an K liefert also stets denselben Isomorphietyp, unabhängig davon, welche Nullstelle genau adjungiert wurde.

Beweis. a und b haben dasselbe Minimalpolynom m. Es sei $\deg m = r$. Kronecker liefert $K(a) \cong K[X]/(m) \cong K(b)$ mit den Abbildungsvorschriften

$$\sum_{i=0}^{r-1} k_i a^i \mapsto \overline{\sum_{i=0}^{r-1} k_i X^i} \mapsto \sum_{i=0}^{r-1} k_i b^i.$$

■

Bemerkung 22.12 Nach obigem Korollar ist die Struktur des Körpers $K(a)$ vollständig durch das Minimalpolynom $m \in K[X]$ von a festgelegt. Dies ist der Grund, warum wir in 20.17 nur von einem algebraischen Element *a über K* sprechen und L nicht erwähnen: In welchem Oberkörper a genau liegt, ist irrelevant. Wir können alle algebraisch wichtigen Eigenschaften von a aus dem von Oberkörpern unabhängigen Körper $K[X]/(m)$ herauslesen. ⁜

Zerfällungskörper

Zerfällungskörper sind (per Mengeninklusion) minimale Oberkörper, die alle Nullstellen eines gegebenen Polynoms enthalten:

Definition 22.13 (Zerfällungskörper) *Seien K ein Körper und $f \in K[X]$ mit Grad $n \in \mathbb{N}_0$. Ein Oberkörper L von K heißt **Zerfällungskörper von f über K**, falls*

(a) *f über L zerfällt in der Form $f = c \cdot \prod_{i=1}^{n}(X - a_i)$ mit $c \in K^\times$ und $a_1, \dots, a_n \in L$ und*

(b) *$L = K(a_1, \dots, a_n)$ gilt.*

In L zerfällt f in Linearfaktoren. Wegen (b) ist L diesbezüglich minimal: Kein echter Zwischenkörper von $L|K$ enthält alle Nullstellen $a_1, \dots, a_n$ von f. (Wofür wird das $c \in K$ in Teil (a) gebraucht?) Da alle der a_i algebraisch über K sind, ist $L|K$ eine endliche Erweiterung. ? ?

Mit Hilfe der Kronecker-Adjunktion können wir zeigen, dass jedes Polynom $f \in K[X]$ mit $f \neq 0$ einen Zerfällungskörper besitzt:

Satz 22.14 (induktiver Kronecker) *Seien K ein Körper und $f \in K[X]$ mit $f \neq 0$. Dann besitzt f einen Zerfällungskörper über K.*

Beweis. Wir wenden Kronecker mehrfach an und fügen so, nach und nach, alle Nullstellen von f zu K hinzu:
Zunächst zerlegen wir f in der Form $f = c \cdot \prod_{i=1}^{r} f_i$ mit $c \in K$ und irreduziblen, normierten Polynomen $f_i \in K[X]$. Gilt $\deg f_i = 1$ für alle i, so ist K ein (sogar *der*) Zerfällungskörper von f über K und wir sind fertig. ?
Andernfalls gibt es unter den f_i eines von Grad ≥ 2, z. B. f_1. Wir setzen $K_1 := K[X]/(f_1)$ und betrachten f ab jetzt über K_1:
Wir zerlegen f in der Form $f = c \cdot \prod_{i=1}^{s} g_i$ mit $c \in K$ und irreduziblen, normierten Polynomen $g_i \in K_1[X]$. Da in K_1 mindestens eine Nullstelle von f enthalten ist, ist diese Zerlegung feiner als die vorherige, d. h. es gilt $s > r$. Gilt $\deg g_i = 1$ für alle i, so ist K_1 ein Zerfällungskörper von f über K. Andernfalls gibt es unter den g_i eines von Grad ≥ 2, beispielsweise g_1. Wir setzen $K_2 := K_1[X_1]/(g_1)$ und betrachten f ab jetzt über K_2, etc.
Dies setzen wir induktiv fort und erhalten eine aufsteigende Kette

$$K \subset K_1 \subset K_2 \subset \cdots$$

von Körpern. In jedem Schritt erhöht sich die Anzahl der enthaltenen Nullstellen von f. Spätestens im Körper $K_{\deg f}$ sind dann alle Nullstellen von f enthalten.
Da wir nur Nullstellen von f an den Körper K adjungieren, erhalten wir so nach endlich vielen Schritten einen minimalen Oberkörper von K, der alle Nullstellen von f enthält, also einen Zerfällungskörper von f über K. ■

23. Fortsetzungslemma, Isomorphie von Zerfällungskörpern

Worum geht es? Wir setzen Körperhomomorphismen auf gewisse Oberkörper fort und zeigen, dass alle Zerfällungskörper eines Polynoms zueinander isomorph sind. Wir stellen eine Verallgemeinerung der hierbei verwendeten Beweisideen vor, mit der die Existenz und Isomorphie von *algebraischen Abschlüssen* gezeigt werden kann. Zuletzt beschäftigen wir uns mit *Mehrfachnullstellen von Polynomen*. ⁜

Das Fortsetzungslemma

Wir haben in der letzten Vorlesung mit Kronecker eine Nullstelle eines normierten, irreduziblen Polynoms $m \in K[X]$ konstruiert, ohne auf (potentiell unbekannte) Oberkörper von K zurückzugreifen. Eine Konsequenz hieraus war 22.11: Zwei beliebige Nullstellen a, b von m erzeugen isomorphe Körpererweiterungen $K(a)$ bzw. $K(b)$; der Isomorphismus φ entsteht hierbei, indem man $\varphi(k) := k$ für alle $k \in K$ und $\varphi(a) := b$ setzt und diese Zuordnung dann homomorph fortsetzt. Man erhält

$$\varphi : K(a) \to K(b), \qquad \sum_{i=0}^{n} k_i a^i \mapsto \sum_{i=0}^{n} k_i b^i.$$

Dies lässt sich auch anders interpretieren:

$$\begin{array}{ccc} K(a) & \xrightarrow{\varphi} & K(b) \\ | & & | \\ K & \xrightarrow{\mathrm{id}_K} & K \end{array}$$

Die identische Abbildung id_K ist ein Isomorphismus zwischen K und K. Die Abbildung φ ist ein Isomorphismus zwischen $K(a)$ und $K(b)$. Für die Einschränkung $\varphi|_K$ von φ auf K gilt $\varphi|_K = \mathrm{id}_K$.

Anders formuliert: Der Isomorphismus $\mathrm{id}_K : K \to K$ lässt sich zu einem Isomorphismus $\varphi : K(a) \to K(b)$ **fortsetzen**.

Fragen über die Fortsetzbarkeit von Isomorphismen spielen in der Körpertheorie eine große Rolle, beispielsweise in der *Galoistheorie*, die wir später behandeln werden.

22.11 lässt sich als Resultat über die Fortsetzbarkeit des (sehr speziellen) Isomorphismus id_K auffassen. Das folgende Lemma ist allgemeiner und ein wichtiges Grundresultat der Körpertheorie. Es behandelt eine ähnliche Situation wie in der Grafik oben, nur wird statt id_K ein beliebiger Körperisomorphismus $\varphi : K \to F$ betrachtet.
Im Allgemeinen gilt $K \neq F$; das normierte, irreduzible Polynom $m \in K[X]$ ist daher kein Element von $F[X]$. Wir übersetzen daher m in ein Polynom aus $F[X]$, indem wir die Koeffizienten von m mit Hilfe von φ in F übertragen. Eine ähnliche Technik haben wir bereits mit der Koeffizientenreduktion auf Seite 136 kennengelernt.

Lemma 23.1 (Fortsetzungslemma) *Seien K und F Körper, $\varphi : K \to F$ ein Körperisomorphismus, $m \in K[X]$ ein normiertes, irreduzibles Polynom und a eine Nullstelle von m (in irgendeinem Zerfällungskörper von m).*
φ liefert eine Abbildung $\varphi_X : K[X] \to F[X]$ durch Übertragen von Koeffizienten, d. h. es ist

$$\varphi_X : K[X] \to F[X], \qquad \sum_{i=0}^{n} k_i X^i \mapsto \sum_{i=0}^{n} \varphi(k_i) X^i \qquad \text{mit } n \in \mathbb{N}_0 \text{ und } k_i \in K.$$

Setzen wir $\mu := \varphi_X(m)$, so ist μ ein normiertes, irreduzibles Polynom aus $F[X]$. Sei b eine Nullstelle von μ (in irgendeinem Zerfällungskörper von μ). Dann ist die Abbildung

$$\hat{\varphi}: K(a) \to F(b), \qquad \sum_{i=0}^{r-1} k_i a^i \mapsto \sum_{i=0}^{r-1} \varphi(k_i) b^i \qquad \text{mit } r := \deg m \text{ und } k_i \in K$$

ein Isomorphismus; es gilt daher $K(a) \cong F(b)$. Ferner stimmt die Einschränkung $\hat{\varphi}|_K : K \to F$ mit φ überein. $\hat{\varphi}$ setzt den Isomorphismus $\varphi : K \to F$ also als Isomorphismus $K(a) \to F(b)$ fort.

Beweisskizze. Der Beweis des Lemmas ist ziemlich technisch und läuft in mehreren Schritten ab:

Schritt 1: Man zeigt, dass φ_X ein Isomorphismus ist.

Die Bijektivität von φ_X ist klar, denn das eindeutige Urbild von $\sum_{i=0}^{n} f_i X^i \in F[X]$ ist durch $\sum_{i=0}^{n} \varphi^{-1}(f_i) X^i \in K[X]$ gegeben. Die Homomorphie von φ_X lässt sich durch (längliches) Rechnen nachweisen.

Schritt 2: μ ist normiert und irreduzibel.

Die Normiertheit von μ folgt aus der Normiertheit von m, da $\varphi(1_K) = 1_F$ ist. Wäre $\mu = f \cdot g$ zerlegbar, so wäre auch m wegen $m = \varphi_X^{-1}(\mu) = \varphi_X^{-1}(f) \cdot \varphi_X^{-1}(g)$ zerlegbar. Dies widerspricht aber der vorausgesetzten Irreduzibilität von m.

Schritt 3: Die Abbildung $\psi : K[X] \to F(b)$ mit $\sum_{i=0}^{n} k_i X^i \mapsto \sum_{i=0}^{n} \varphi(k_i) b^i$ ist ein Ringepimorphismus.

ψ ist gerade die Verkettung des Isomorphismus φ_X mit dem Einsetzhomomorphismus $e_b : F[X] \to F(b)$. Da b algebraisch über F ist, ist e_b surjektiv.

Schritt 4: $\hat{\varphi}$ ist ein Isomorphismus.

Wir betrachten den Epimorphismus ψ aus Schritt 3. Es gilt $\psi(f) = 0$ genau dann, wenn das Polynom $\varphi_X(f)$ die Nullstelle b besitzt. Dies gilt nach 20.21 genau dann, wenn $\mu \mid \varphi_X(f)$ ist, also wenn $m \mid f$ gilt. Daher ist $\ker \psi = (m) \trianglelefteq K[X]$.

Mit Homomorphiesatz folgt $K[X]/(m) \cong F(b)$. Kronecker zeigt $K(a) \cong K[X]/(m)$. Zusammengesetzt folgt $K(a) \cong K[X]/(m) \cong F(b)$, wobei das Element a in der Form $a \overset{\tau}{\mapsto} \overline{X} \overset{\psi}{\mapsto} b$ abgebildet wird, wobei τ die Umkehrabbildung des Isomorphismus $K[X]/(m) \to K(a)$ aus 22.8 bezeichne. Dies zeigt die im Lemma behauptete Abbildungsvorschrift für $\hat{\varphi}$. ■

Bemerkung 23.2 Grob gesprochen sagt das Fortsetzungslemma aus, dass sich ein Körperisomorphismus $\varphi : K \to F$ zu einem Isomorphismus $\hat{\varphi} : K(a) \to F(b)$ fortsetzen lässt, wenn das Minimalpolynom μ von b in der „richtigen Beziehung“ zum Minimalpolynom m von a steht. Diese „richtige Beziehung“ wird vom Fortsetzungslemma spezifiziert: Gilt $m = \sum_{i=0}^{r} k_i X^i$, so ist $\mu = \sum_{i=0}^{r} \varphi(k_i) X^i$. ※

Beispiel 23.3 Durch Überprüfen der entsprechenden Abschlusseigenschaften sieht man, dass die Menge $K := \left\{ \left(\begin{smallmatrix} a & b \\ -b & a \end{smallmatrix}\right) : a, b \in \mathbb{R} \right\}$ ein Unterkörper des Matrizenrings $\mathbb{R}^{2\times 2}$ ist. Wir definieren die Teilmenge $F := \left\{ \left(\begin{smallmatrix} a & 0 \\ 0 & a \end{smallmatrix}\right) : a \in \mathbb{R} \right\} \subseteq K$ und betrachten die Abbildung

$$\varphi : \mathbb{R} \to F, \qquad x \mapsto \left(\begin{smallmatrix} x & 0 \\ 0 & x \end{smallmatrix}\right).$$

φ ist ein Körperisomorphismus. Sei $m := X^2 + 1 \in \mathbb{R}[X]$ das Minimalpolynom von $i \in \mathbb{C}$. Durch Übertragen der Koeffizienten von m mit Hilfe von φ entsteht das Polynom

$$\mu := \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right) \cdot X^2 + \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right) \in F[X],$$

das beispielsweise die Nullstelle $j := \left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right) \in K$ besitzt. Das Fortsetzungslemma liefert nun die Isomorphie

$$\mathbb{C} = \{a + bi \mid a, b \in \mathbb{R}\} = \mathbb{R}(i) \cong F(j) = \left\{ \left(\begin{smallmatrix} a & 0 \\ 0 & a \end{smallmatrix}\right) + \left(\begin{smallmatrix} 0 & b \\ -b & 0 \end{smallmatrix}\right) : a, b \in \mathbb{R} \right\} = K.$$

Der Körper $\mathbb{C}$ lässt sich somit durch (2×2)-Matrizen mit reellen Einträgen darstellen, die imaginäre Einheit wird zu $\left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)$. ⋇

Isomorphie von Zerfällungskörpern

Kronecker 22.8 erlaubt die Adjunktion einer einzigen Nullstelle eines Polynoms an einen Körper. Per Induktion lässt sich mit dieser Technik ein Zerfällungskörper eines Polynoms konstruieren.
Auch das Fortsetzungslemma lässt sich induktiv anwenden und liefert die Isomorphie von Zerfällungskörpern:

Satz 23.4 *Seien K und F Körper, $\varphi : K \to F$ ein Körperisomorphismus, $f \in K[X]$ mit $f \neq 0$ und Z ein Zerfällungskörper von f. Wir setzen $g := \varphi_X(f) \in F[X]$, wobei φ_X den Isomorphismus $K[X] \to F[X]$ aus dem Fortsetzungslemma bezeichnet. Sei S ein Zerfällungskörper von g. Dann hat φ eine Fortsetzung zu einem Isomorphismus $Z \to S$.*

Beweisskizze. Es seien $n := \deg f$ der Grad von f und $a_1, \dots, a_n$ die Nullstellen von f in Z. Wir setzen $K_i := K(a_1, \dots, a_i)$. Dann ist

$$K = K_0 \subseteq K_1 \subseteq \cdots \subseteq K_n = Z \qquad \text{sowie} \qquad K_{i+1} = K_i(a_{i+1}).$$

$$\begin{array}{ccc}
Z = K_{n-1}(a_n) & \xrightarrow{\varphi_n} & F_n := F_{n-1}(b_n) \\
\vdots & & \vdots \\
K_3 = K_2(a_3) & \xrightarrow{\varphi_3} & F_3 := F_2(b_3) \\
| & & | \\
K_2 = K_1(a_2) & \xrightarrow{\varphi_2} & F_2 := F_1(b_2) \\
| & & | \\
K_1 = K_0(a_1) & \xrightarrow{\varphi_1} & F_1 := F_0(b_1) \\
| & & | \\
K_0 = K & \xrightarrow{\varphi = \varphi_0} & F_0 := F
\end{array}$$

Ausgehend vom Isomorphismus $\varphi : K \to F$ konstruieren wir Körper $F_i \subseteq S$ und Isomorphismen $\varphi_i : K_i \to F_i$. Sei hierzu $\varphi_0 := \varphi$ und $F_0 := F$. Wir zeigen beispielhaft den Schritt $i = 1 \to i = 2$:
Sei m das Minimalpolynom von a_2 **über K_1**. Wegen $f(a_2) = 0$ gilt $m \mid f$ über K_1 nach 20.21.
Wir setzen $\mu := \varphi_{1,X}(m)$, wobei $\varphi_{1,X} : K_1[X] \to F_1[X]$ den Isomorphismus aus dem Fortsetzungslemma bezeichne. Da $m \mid f$ über K_1 gilt, ist $\mu \mid \varphi_{1,X}(f) = g$ über F_1. Es existiert daher ein Element $b_2 \in S$ mit $\mu(b_2) = 0$. Wir setzen $F_2 := F_1(b_2)$.
Nach Fortsetzungslemma lässt sich nun φ_1 zu einem Isomorphismus $\varphi_2 : K_1(a_2) \to F_1(b_2)$, also zu einem Isomorphismus $K_2 \to F_2$ fortsetzen.

Um den Satz zu beweisen, zeigen wir nun noch, dass $F_n = S$ gilt:
Die Aussage $F_n \subseteq S$ folgt, weil $F \subseteq S$ gilt und wir in jedem der Schritte $F_i \to F_{i+1}$ nur Elemente aus S adjungiert haben.
Da f über Z in Linearfaktoren zerfällt, zerfällt auch g über F_n in Linearfaktoren; der Isomorphismus $\varphi_{n,X} : Z[X] \to F_n[X]$ überträgt die Zerfällung von f. Daher ist F_n ein Unterkörper eines Zerfällungskörpers von g, in dem g bereits vollständig zerfällt. Aufgrund der Minimalität von Zerfällungskörpern gilt $F_n = S$. ■

Obiger Satz wird oft im Fall $K = F$ und $\varphi = \mathrm{id}_K$ benutzt. Man erhält:

Korollar 23.5 (Isomorphie von Zerfällungskörpern) *Seien K ein Körper und $f \in K[X]$ mit $f \neq 0$. Dann sind alle Zerfällungskörper von f isomorph zueinander.*

Beispiel 23.6 (a) Wir führen 23.3 fort: $\mathbb{C}$ ist ein Zerfällungskörper des Polynoms $m := X^2 + 1 \in \mathbb{R}[X]$. Ein Zerfällungskörper von $\mu := \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right) \cdot X^2 + \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$ über F ist durch K gegeben. Die Isomorphie $\mathbb{C} \cong K$ folgt nun sowohl aufgrund des Fortsetzungslemmas als auch aufgrund der Isomorphie von Zerfällungskörpern.

(b) Wir betrachten das Polynom $f := (X^2 + X + 1)(X^2 + 1) \in \mathbb{Q}[X]$. Es hat die Nullstellen

$$a_\pm := -\frac{1}{2} \pm \frac{1}{2} i\sqrt{3} \qquad \text{und} \qquad b_\pm := \pm i.$$

Die Körper

$$\mathbb{Q}(a_\pm, b_\mp),\ \mathbb{Q}(a_+, b_+),\ \mathbb{Q}(i, \sqrt{3}),\ \mathbb{Q}(a_-, i),\ (\mathbb{Q}[X]/(X^2 + X + 1))[Y]/(Y^2 + 1)$$

sind Zerfällungskörper von f. Obiger Satz garantiert, dass sie alle isomorph zueinander sind. ⁂

Vereinbarung zur Schreibweise 23.7 Aufgrund von 23.5 identifizieren wir zukünftig alle Zerfällungskörper desselben Polynoms miteinander (mathematisch etwas ungenau) und sprechen von **dem** Zerfällungskörper eines Polynoms.
$\mathbb{C}$ ist beispielsweise **der** Zerfällungskörper von $X^2 + 1 \in \mathbb{R}[X]$. ⁂

Algebraische Abschlüsse

Induktive Anwendung von Kronecker lieferte die Existenz von Zerfällungskörpern, induktive Anwendung des Fortsetzungslemmas die Isomorphie von Zerfällungskörpern. Beide Schlüsse können wir problemlos für endlich viele Polynome durchführen. Wir erhalten dann:

Satz 23.8 *Sind K ein Körper und $f_1, \ldots, f_r \in K[X]$ Polynome mit $f_i \neq 0$ für alle i, so existiert ein kleinster Oberkörper Z von K, der alle Nullstellen aller f_i enthält. Alle solchen kleinsten Oberkörper sind isomorph zueinander.*

Beweisskizze. Wende 22.14 und 23.5 auf das Polynom $f := \prod_{i=1}^{r} f_i \in K[X]$ an. ■

Durch mengentheoretische Tricks (Lemma von Zorn, transfinite Induktion) lässt sich der obige Satz auf *unendlich viele* Polynome verallgemeinern. Besonders interessant ist hierbei der Fall, bei dem man alle normierten Polynome über einem Körper betrachtet:

Satz 23.9 (Steinitz; Existenz algebraischer Abschlüsse) *Sei K ein Körper. Dann existiert ein (bezüglich Mengeninklusion) kleinster Oberkörper $\overline{K}$ (gelesen: K quer) von K, der alle Nullstellen aller normierten Polynome aus $K[X]$ enthält. Man nennt $\overline{K}$ einen **algebraischen Abschluss von K**.*
Da $\overline{K}$ ausschließlich durch Adjunktion von Nullstellen von Polynomen, also über K algebraischen Elementen entsteht, ist die Erweiterung $\overline{K}|K$ algebraisch.

Satz 23.10 (Steinitz; Isomorphie algebraischer Abschlüsse) *Alle algebraischen Abschlüsse eines Körpers K sind isomorph zueinander.*
*Man spricht daher (mathematisch ungenau) auch von **dem** algebraischen Abschluss von K.*

Beispiel 23.11 Der algebraische Abschluss von $\mathbb{R}$ ist $\mathbb{C}$, denn nach dem Fundamentalsatz zerfällt jedes nicht-konstante Polynom über $\mathbb{C}$ vollständig in ein Produkt von Linearfaktoren. $\mathbb{C}$ enthält daher alle Nullstellen aller normierten reellen Polynome. Wegen $[\mathbb{C} : \mathbb{R}] = 2$ ist $\mathbb{C}$ gleichzeitig auch minimal bezüglich dieser Eigenschaft. ⁜

Bemerkung 23.12 Algebraische Abschlüsse sind ein Hilfsmittel, um die Existenz von Nullstellen beliebiger Polynome sicherzustellen. Dies kann Beweise deutlich vereinfachen und lesbarer machen.
Diesen Vorteil bezahlt man allerdings mit der komplizierten Struktur algebraischer Abschlüsse: Es sind kaum explizite Darstellungen von algebraischen Abschlüssen bekannt. Arbeitet man mit algebraischen Abschlüssen, so befindet man sich fast immer in einem abstrakten Körper, dessen Elemente man nicht kennt. ⁜

Knobelfrage. Ist $\mathbb{C}$ der algebraische Abschluss von $\mathbb{Q}$? ⁇

Um zum algebraischen Abschluss $\overline{K}$ eines Körpers K zu gelangen, adjungieren wir alle Nullstellen aller normierten Polynome aus $K[X]$ an K. Daher enthält $\overline{K}$ alle über K algebraischen Elemente und ist daher die größtmögliche algebraische Erweiterung von K. Es gilt jedoch mehr: $\overline{K}$ enthält sogar alle *über $\overline{K}$ algebraischen* Elemente! Dies bedeutet, dass $\overline{K}$ die einzige algebraische Erweiterung von $\overline{K}$ ist.

Satz 23.13 *Seien K ein Körper, $\overline{K}$ sein algebraischer Abschluss und a ein algebraisches Element über $\overline{K}$ (aus einem geeigneten Oberkörper von $\overline{K}$). Dann gilt $a \in \overline{K}$.*
Es gibt also keine echte algebraische Erweiterung von $\overline{K}$.

Beweis. Die Erweiterungen $\overline{K}(a)|\overline{K}$ und $\overline{K}|K$ sind algebraisch. Nach 22.6 (c) ist dann auch $\overline{K}(a)|K$ algebraisch. Daher ist a algebraisch über K, was $a \in \overline{K}$ zeigt. ■

Bemerkung 23.14 Obiger Satz sagt, dass das Adjungieren von algebraischen Elementen mit dem algebraischen Abschluss $\overline{K}$ sein Ende gefunden hat: Es gibt keine weiteren algebraischen Elemente, weder über K noch über $\overline{K}$ noch über einem beliebigen Zwischenkörper der Erweiterung $\overline{K}|K$, die noch nicht in $\overline{K}$ enthalten sind.
Anders formuliert: Ist a ein Element eines echten Oberkörpers von $\overline{K}$, so ist a transzendent über $\overline{K}$. ⁜

Mit der folgenden Sprechweise lässt sich 23.13 eleganter formulieren:

Definition 23.15 *Wir nennen einen Körper K **algebraisch abgeschlossen**, falls jedes normierte irreduzible Polynom aus $K[X]$ vom Grad Eins ist. Äquivalent hierzu ist, dass sich jedes nichtkonstante Polynom aus $K[X]$ über K als Produkt von Linearfaktoren schreiben lässt.*

23.13 sagt nun:

Korollar 23.16 *Jeder algebraische Abschluss eines Körpers ist algebraisch abgeschlossen.*

Beispiel 23.17 $\mathbb{C}$ ist algebraisch abgeschlossen. ⁜

Mehrfachnullstellen

In der Körpertheorie tritt häufig die Frage auf, ob ein Polynom $f \neq 0$ in seinem Zerfällungskörper Z (oder im algebraischen Abschluss des Grundkörpers) Mehrfachnullstellen besitzt, d. h. ob in der Zerlegung

$$f = c \cdot (X - a_1)^{n_1} \cdots (X - a_r)^{n_r}$$

über Z ein Exponent n_i mit $n_i \geq 2$ existiert. Dies kann man, wie in der Analysis, durch Ableiten entscheiden.

Definition 23.18 *Seien K ein Körper und $f := \sum_{i=0}^{n} k_i X^i \in K[X]$ ein Polynom über K. Wir setzen $f' := \sum_{i=1}^{n} i k_i X^{i-1}$ und nennen dieses Polynom die **Ableitung von f**.*

Bemerkung 23.19 (a) Obige Definition überträgt die Formel für die Ableitung eines Polynoms aus der Analysis in die Algebra. Analytische Sätze übertragen sich jedoch nicht, sofern nicht gerade $\mathbb{R}$ als Grundkörper betrachtet wurde.

(b) Wir betrachten das Polynom $f := \sum_{i=0}^{n} k_i X^i \in K[X]$. Das Element i im Exponenten der Potenz X^i ist eine *nicht-negative ganze Zahl* und gibt an, wie oft X mit sich selbst multipliziert wird.

In der Ableitung f' taucht i auch als Koeffizient auf und wird zu einem *Element aus K* uminterpretiert. Dies führt dazu, dass der algebraische Ableitungsbegriff körperabhängig ist: Sei $f := X^6 + X^4 + X^2 + 1 \in K[X]$. Für $K = \mathbb{Z}_2$ gilt $f' = 0$, für $K = \mathbb{Z}_3$ ist $f' = X^3 - X$.

Für jedes Polynom f mit $f \neq 0$ gilt jedoch $\deg f' < \deg f$. ⁜

Durch Nachrechnen kann man die folgende *Produktregel* zeigen:

Satz 23.20 *Seien K ein Körper und $f, g \in K[X]$ Polynome. Dann gilt $(fg)' = f'g + fg'$.*

Wir können nun die Eingangsfrage nach Mehrfachnullstellen auflösen:

Satz 23.21 *Seien K ein Körper, $f \in K[X]$ mit $f \neq 0$ ein Polynom und Z der Zerfällungskörper von f. Genau dann ist $a \in Z$ eine Mehrfachnullstelle von f, wenn $f(a) = f'(a) = 0$ gilt.*

Beweis. Über Z lässt sich f schreiben in der Form $f = (X-a)^n \cdot g$ mit $n \in \mathbb{N}_0, g \in Z[X]$ und $g(a) \neq 0$.

„$\Longrightarrow$“ Ist a eine Mehrfachnullstelle von f, so ist $n \geq 2$. Es folgt $f(a) = 0$ und

$$f' = n(X-a)^{n-1} \cdot g + (X-a)^n \cdot g'. \qquad (\star)$$

Wegen $n \geq 2$ ist $n-1 \geq 1$ und somit $f'(a) = 0$.

„$\Longleftarrow$“ Aus $f(a) = 0$ folgt $n \geq 1$. Die Ableitung von f hat dann die Gestalt $(\star)$. Einsetzen von a liefert $0 = f'(a) = n \cdot (a-a)^{n-1} \cdot g(a)$. Da nach Voraussetzung $g(a) \neq 0$ ist, folgt $n \cdot (a-a)^{n-1} = 0$. Diese Gleichung ist für $n = 1$ falsch. Folglich muss $n \geq 2$ und a damit eine mehrfache Nullstelle von f sein. ■

Obiges Kriterium überprüft, ob ein konkretes Element $a \in Z$ eine mehrfache Nullstelle von f ist. Hierzu muss man über dem (komplizierten) Körper Z arbeiten. Das folgende Resultat entscheidet, ob $f \in K[X]$ Mehrfachnullstellen im Zerfällungskörper besitzt. Es gibt diese Mehrfachnullstellen nicht konkret an, arbeitet dafür aber ausschließlich über dem Grundkörper K:

Korollar 23.22 *Seien K ein Körper, $f \in K[X]$ mit $f \neq 0$ ein Polynom und Z der Zerfällungskörper von f. Genau dann besitzt f in Z Mehrfachnullstellen, wenn f und f' nicht teilerfremd sind, also wenn $\deg(\mathrm{ggT}(f, f')) \geq 1$ ist.*
Der ggT kann hierbei effizient mit dem Euklidischen Algorithmus in $K[X]$ berechnet werden; der Körper Z wird hierbei nicht benötigt.

Beweisskizze. Sei $t := \mathrm{ggT}(f, f')$. Da $f \neq 0$ ist, gilt $t \neq 0$. Daher besitzt t genau dann eine Nullstelle in Z, wenn $\deg t \geq 1$ ist. ?

„$\Longrightarrow$“ f besitze die Mehrfachnullstelle $a \in Z$. Da $K[X]$ euklidisch ist, existieren nach Bézout $\alpha, \beta \in K[X]$ mit $t = \alpha \cdot f + \beta \cdot f'$. Nach 23.21 gilt $f(a) = f'(a) = 0$ und somit auch

$$0 = \alpha(a) \cdot f(a) + \beta(a) \cdot f'(a) = t(a).$$

Damit gilt $\deg t \geq 1$ und f und f' sind nicht teilerfremd.

„$\Longleftarrow$“ Sei $\deg t \geq 1$. Wegen $t \mid f$ besitzen dann t und f eine Nullstelle $a \in Z$. Wegen $t \mid f'$ folgt auch $f'(a) = 0$. Nach 23.21 ist a dann eine Mehrfachnullstelle von f. ■

24. Anwendung: Endliche Körper

Worum geht es? Wir beschäftigen uns mit *endlichen Körpern*, d. h. mit Körpern endlicher Ordnung. Wir gehen zunächst auf Existenzresultate ein und klären, welche Ordnungen für endliche Körper überhaupt möglich sind. Danach untersuchen wir die Struktur endlicher Körper und zeigen, dass der Isomorphietyp eines endlichen Körpers bereits eindeutig durch seine Ordnung festgelegt ist. Ferner klären wir, welche Unterkörper ein endlicher Körper gegebener Ordnung besitzt. ⁜

Existenz und Isomorphie

Wir kennen bereits die endlichen Körper $\mathbb{Z}_p$ mit $p \in \mathbb{P}$. Zudem haben wir in 22.10 ein Konstruktionsprinzip für endliche Körper kennengelernt, das sich verallgemeinern lässt: Ist $m \in \mathbb{Z}_p[X]$ mit $p \in \mathbb{P}$ ein irreduzibles, normiertes Polynom vom Grad r, so ist der Körper $L := \mathbb{Z}_p[X]/(m)$ eine Grad-r-Erweiterung von $\mathbb{Z}_p$ und hat daher p^r Elemente. ⁉
Unklar ist noch, ob sich auf diese Weise alle endlichen Körper konstruieren lassen:

- Sind die Ordnungen endlicher Körper stets von der Form p^r mit $(p, r) \in \mathbb{P} \times \mathbb{N}$?
- Gibt es für alle $(p, r) \in \mathbb{P} \times \mathbb{N}$ ein irreduzibles, normiertes Polynom $m \in \mathbb{Z}_p[X]$ mit $\deg m = r$? Existiert für alle $(p, r) \in \mathbb{P} \times \mathbb{N}$ ein endlicher Körper der Ordnung p^r?
- Gibt es endliche Körper L, die *nicht* durch Kronecker-Adjunktion aus einem der Körper $\mathbb{Z}_p$ entstehen?
- Können Sie die obigen Fragen nach Durcharbeiten der Vorlesung beantworten? ⁉

Unser erstes Resultat klärt, dass endliche Körper einen der Körper $\mathbb{Z}_p$ enthalten:

Satz 24.1 *Sei L ein endlicher Körper. Dann existiert genau eine Primzahl $p \in \mathbb{P}$, so dass L eine endliche Erweiterung eines Körpers P mit $P \cong \mathbb{Z}_p$ ist.*
Obige Primzahl p entspricht der additiven Ordnung von $1 \in L$. Man nennt p die ***Charakteristik von L****, vgl. die Übungen.* → Übung

Beweis. Sei P der Primkörper von L, vgl. 20.11 (c). P ist durch L eindeutig bestimmt und isomorph zu $\mathbb{Z}_p$ für eine Primzahl $p \in \mathbb{P}$. In $\mathbb{Z}_p$ hat Eins die additive Ordnung p. Dies gilt aufgrund der Isomorphie $P \cong \mathbb{Z}_p$ auch in P und wegen $1 \in P \subseteq L$ auch in L.
Da P und L beide endliche Körper sind, gilt $\dim_P L < \infty$. Die Erweiterung $L|P$ ist also endlich. ■

Vereinbarung zur Schreibweise 24.2 Nach obigem Satz sind die in der Theorie endlicher Körper auftretenden Primkörper P isomorph zu $\mathbb{Z}_p$ für ein $p \in \mathbb{P}$. Die Struktur von P hängt daher nur von der Ordnung von P ab und ist durch $\mathbb{Z}_{|P|}$ gegeben.
Wir identifizieren zukünftig alle Primkörper gleicher Ordnung miteinander und schreiben $\mathbb{F}_p$ für den Primkörper der Ordnung p. (Das $\mathbb{F}$ steht für *field*, was die englische Bezeichnung für *Körper* ist).
Für jedes $p \in \mathbb{P}$ gilt also $\mathbb{F}_p = \mathbb{Z}_p$. Hat ein endlicher Körper L die Charakteristik p, so ist $\mathbb{F}_p \subseteq L$. ⁜

24.1 hat eine Reihe schöner Konsequenzen:

Korollar 24.3 *Sei L ein endlicher Körper. Dann gilt $|L| = p^r$, wobei p die Charakteristik von L und r den Erweiterungsgrad $[L : \mathbb{F}_p]$ bezeichnen.*
Kurz: Die Ordnungen endlicher Körper sind Potenzen ihrer primen Charakteristik.

Beweis. Es sei $[L : \mathbb{F}_p] = r$. Dann ist L ein r-dimensionaler $\mathbb{F}_p$-Vektorraum und somit isomorph zum Vektorraum $\mathbb{F}_p^r$. Es folgt $|L| = |\mathbb{F}_p^r| = p^r$. ■

Korollar 24.4 *Sei L ein endlicher Körper der Ordnung p^r mit $(p, r) \in \mathbb{P} \times \mathbb{N}$. Dann existiert ein irreduzibles, normiertes Polynom $m \in \mathbb{F}_p[X]$ mit $\deg m = r$, so dass L isomorph zum Körper $\mathbb{F}_p[X]/(m)$ ist.*
Bis auf Isomorphie lassen sich also alle endlichen Körper durch Kronecker-Adjunktion eines einzigen Elements an $\mathbb{F}_p$ wie in 22.10 erzeugen. Die Erweiterung $L|\mathbb{F}_p$ ist einfach.

Beweis. Die Einheitengruppe $L^\times = L \setminus \{0\}$ ist nach 15.21 zyklisch. Sei a ein Erzeuger von $L^\times$. Der Körper $\mathbb{F}_p(a)$ enthält dann alle Potenzen von a und somit die Menge $L \setminus \{0\}$. Daher ist $L = \mathbb{F}_p(a)$.
Da $L|\mathbb{F}_p$ nach 24.1 endlich ist, besitzt a ein Minimalpolynom $m \in \mathbb{F}_p[X]$. Nach Kronecker ist $L = \mathbb{F}_p(a) \cong \mathbb{F}_p[X]/(m)$. Dies zeigt $\deg m = [L : \mathbb{F}_p] = r$. ■

Wir wissen bereits, dass endliche Körper Primpotenzordnung haben. Offen ist noch, ob es zu *jeder* Primpotenz auch einen endlichen Körper dieser Ordnung gibt. Dies klären wir in den nächsten Resultaten:

Satz 24.5 (Fermat) *Sei L ein endlicher Körper. Für jedes $a \in L$ gilt dann $a^{|L|} = a$.*

Beweis. Die Aussage stimmt sicher für $a = 0$. Sei daher $a \neq 0$. Dann ist a ein Element der Gruppe $L^\times$. Wegen $|L^\times| = |L \setminus \{0\}| = |L| - 1$ folgt mit Lagrange $a^{|L|-1} = 1$, vgl. 7.17. Multiplikation dieser Gleichung mit a liefert $a^{|L|} = a$.
Die zu zeigende Gleichung gilt daher für alle $a \in L$, was den Satz beweist. ■

Das nachstehende Korollar drückt Fermat mit Hilfe von Polynomen aus:

Korollar 24.6 (Fermat) *Sei L ein endlicher Körper der Charakteristik p. Dann ist jedes Element $a \in L$ eine Nullstelle des Polynoms $X^{|L|} - X \in \mathbb{F}_p[X]$.*

Fermat sagt, dass endliche Körper die Nullstellenmengen von Polynomen der Form $X^{p^r} - X \in \mathbb{F}_p[X]$ für gewisse $(p, r) \in \mathbb{P} \times \mathbb{N}$ sind.
Wir zeigen nun, dass die Nullstellenmenge des Polynoms $X^{p^r} - X \in \mathbb{F}_p[X]$ für *jedes* $p \in \mathbb{P}$ und *jedes* $r \in \mathbb{N}$ ein Körper ist. Dies zeigt, dass zu *jeder* Primzahlpotenz ein endlicher Körper dieser Ordnung existiert.
Für den Beweis benötigen wir eine ungewohnte Rechenregel, die in Körpern mit primer Charakteristik zusätzlich zur Verfügung steht:

Lemma 24.7 (Frobenius) *In Körpern K der Charakteristik p gilt $(a+b)^p = a^p + b^p$ für alle $a, b \in K$. Die Abbildung*

$$\varphi : K \to K, \qquad x \mapsto x^p$$

*ist daher ein injektiver Endomorphismus von K. Man nennt φ den **Frobenius-Endomorphismus von K**.*

Beweis. K hat Charakteristik p. Somit ist $p = 0$ in K.
Für $i \in \{0, 1, \dots, p\} \subseteq \mathbb{N}_0$ lässt sich der Binomialkoeffizient $\binom{p}{i}$ darstellen in der Form $\binom{p}{i} = \frac{p!}{i! \cdot (p-i)!}$. Der Zähler dieses Bruchs ist stets durch p teilbar. Der Nenner des Bruchs ist genau dann durch p teilbar, wenn eine der beiden Fakultäten mit $p!$ übereinstimmt, wenn also $i = 0$ oder $i = p$ gilt. Dies zeigt: Für $i \in \{1, 2, \dots, p-1\}$ ist $p \mid \binom{p}{i}$.
Fügen wir diese beiden Überlegungen zusammen, so erhalten wir für alle $a, b \in K$ mit Hilfe des binomischen Lehrsatzes:

$$(a+b)^p \overset{1.12\,(\mathrm{d})}{=} \sum_{i=0}^{p} \binom{p}{i} a^i b^{p-i} = \underbrace{\binom{p}{p}}_{=1} a^p + \underbrace{\binom{p}{0}}_{=1} b^p + \sum_{i=1}^{p-1} \underbrace{\binom{p}{i}}_{\text{Vielfaches von } p} a^i b^{p-i}$$

$$\overset{p=0 \text{ in } K}{=} a^p + b^p.$$

Die Homomorphie-Eigenschaften von φ lassen sich nun einfach nachrechnen; die einzige Schwierigkeit ist die additive Verträglichkeit, die aber aus Obigem folgt. Damit ist $\varphi : K \to K$ ein Endomorphismus. Zudem ist φ wegen 6.15 (a) injektiv. ■

Wir können jetzt zeigen:

Satz 24.8 *Zu jeder Primpotenz p^r existiert ein Körper der Ordnung p^r, nämlich die Nullstellenmenge des Polynoms $f := X^{p^r} - X \in \mathbb{F}_p[X]$ (in irgendeinem Zerfällungskörper Z von f).*

Beweis. Es sei Z ein Zerfällungskörper von f und $N \subseteq Z$ die Menge der Nullstellen von f. Für die Ableitung von f gilt

$$f' = p^r \cdot X^{p^r-1} - 1 \overset{p=0 \text{ in } \mathbb{F}_p}{=} -1.$$

Daher sind f und f' teilerfremd. Nach 23.22 besitzt f in Z keine Mehrfachnullstellen. Es ist also $|N| = \deg f = p^r$.
Wir zeigen, dass N ein Unterkörper von Z ist, und beweisen so den Satz:
Für die Elemente $0, 1 \in Z$ gilt $f(0) = 0 = f(1)$. Null und Eins sind daher Elemente aus N. Seien nun $a, b \in N$ beliebig. Wir zeigen, dass auch $a + b \in N$ ist, also dass $f(a+b) = 0$ gilt. Wir dürfen hierzu $f(a) = 0 = f(b)$, also $a^{p^r} = a$ und $b^{p^r} = b$ benutzen.
Aus 24.7 folgt per Induktion $(a+b)^{p^i} = a^{p^i} + b^{p^i}$ für alle $i \in \mathbb{N}_0$. Daher ist

$$(a+b)^{p^r} \overset{\text{induktiver Frobenius}}{=} a^{p^r} + b^{p^r} \overset{a^{p^r}=a,\, b^{p^r}=b}{=} a + b.$$

Dies liefert $f(a+b) = (a+b)^{p^r} - (a+b) = 0$.
Die übrigen Abgeschlossenheiten folgen ähnlich. ■

24.8 klärt, dass es zu jeder Primzahlpotenz einen endlichen Körper dieser Ordnung gibt; wir haben ihn als Nullstellenmenge eines gewissen Polynoms (innerhalb eines Zerfällungskörpers) konstruiert.
Diese Nullstellenmenge ist aber gerade der Zerfällungskörper selbst:

Korollar 24.9 *Zu jeder Primpotenz p^r existiert ein Körper der Ordnung p^r, nämlich der Zerfällungskörper Z des Polynoms $f := X^{p^r} - X \in \mathbb{F}_p[X]$.*
Z besteht genau aus den Nullstellen von f.

Beweis. Sei $N \subseteq Z$ die Nullstellenmenge von f. Nach 24.8 ist N ein Unterkörper von Z, der alle Nullstellen von f enthält. Da Z minimal bezüglich dieser Eigenschaft ist, folgt $N = Z$. ■

Die Interpretation endlicher Körper als Zerfällungskörper liefert:

Korollar 24.10 *Alle endlichen Körper derselben Ordnung sind isomorph zueinander.*

Beweis. Seien K und L endliche Körper gleicher Ordnung p^r. Dann sind K und L beide Zerfällungskörper des Polynoms $X^{p^r} - X \in \mathbb{F}_p[X]$. Aufgrund der Isomorphie von Zerfällungskörpern 23.5 gilt $K \cong L$. ■

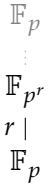
Vereinbarung zur Schreibweise 24.11 Nach 24.10 wird der Isomorphietyp eines endlichen Körpers allein durch seine Ordnung bestimmt. Wir übertragen daher 23.7 auf endliche Körper und identifizieren alle endlichen Körper gleicher Ordnung miteinander (mathematisch etwas ungenau). Zukünftig sprechen wir also von **dem** endlichen Körper der Ordnung p^r. Wir bezeichnen ihn mit $\mathbb{F}_{p^r}$. ※

Endliche Erweiterungen von $\mathbb{F}_p$

Sei L eine endliche Erweiterung von $\mathbb{F}_p$. Dann ist L ein endlicher Körper und stimmt somit mit $\mathbb{F}_{p^r}$ für ein $r \in \mathbb{N}$ überein. Ferner ist L nach 24.8 die Nullstellenmenge eines Polynoms. Hierin unterscheidet sich L deutlich von den uns vertrauteren endlichen Erweiterungen von $\mathbb{Q}$. ⁉

Wir fixieren für das Folgende einen algebraischen Abschluss $\overline{\mathbb{F}_p}$ von $\mathbb{F}_p$. Algebraische Erweiterungskörper von $\mathbb{F}_p$ sehen wir immer als Unterkörper von $\overline{\mathbb{F}_p}$ an. Auf diese Weise fixieren wir das „Universum“, innerhalb dessen wir endliche Erweiterungen von $\mathbb{F}_p$ studieren. Isomorphe Körper außerhalb dieses Universums, die sich nur in der Darstellung der Elemente unterscheiden, betrachten wir nicht mehr.

Aus 24.8 folgt, dass es nur „wenige“ endliche Körper gibt: Ist p^r eine Potenz von p, so existiert nur *genau ein* Erweiterungskörper von $\mathbb{F}_p$ mit p^r Elementen, nämlich die Nullstellenmenge des Polynoms $X^{p^r} - X \in \mathbb{F}_p[X]$.

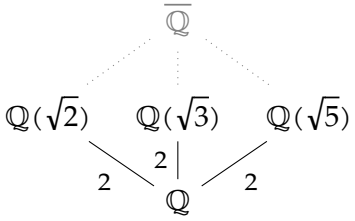


Innerhalb des fixierten algebraischen Abschlusses $\overline{\mathbb{F}_p}$ ist der Körper $\mathbb{F}_{p^r}$ eindeutig gegeben als Menge aller $a \in \overline{\mathbb{F}_p}$ mit $a^{p^r} = a$. In diesem Fall ist $\mathbb{F}_{p^r}$ also nicht nur bis auf Isomorphie, sondern komplett festgelegt.
Zu jedem $r \in \mathbb{N}$ besitzt die Erweiterung $\overline{\mathbb{F}_p}|\mathbb{F}_p$ *genau einen* Zwischenkörper mit Grad r über $\mathbb{F}_p$, nämlich den eindeutig bestimmten Körper $\mathbb{F}_{p^r}$.

Wir gießen diese Erkenntnis in Satzform:

Satz 24.12 *Seien $p \in \mathbb{P}$ und $\overline{\mathbb{F}_p}$ ein algebraischer Abschluss von $\mathbb{F}_p$. Dann besitzt die Erweiterung $\overline{\mathbb{F}_p}|\mathbb{F}_p$ zu jedem $r \in \mathbb{N}$ **genau einen** Zwischenkörper der Ordnung p^r, nämlich die Menge $\{a \in \overline{\mathbb{F}_p} \mid a^{p^r} = a\}$.*

Bemerkung 24.13 Im Kontrast zu obigem Satz besitzt die Erweiterung $\overline{\mathbb{Q}}|\mathbb{Q}$ für jede natürliche Zahl $r > 1$ **unendlich viele** Zwischenkörper vom Grad r über $\mathbb{Q}$; beispielsweise enthält $\overline{\mathbb{Q}}|\mathbb{Q}$ unendlich viele quadratische Erweiterungen von $\mathbb{Q}$:



Die Körper $\mathbb{Q}(\sqrt{p})$ mit $p \in \mathbb{P}$ sind paarweise verschiedene quadratische Erweiterungen von $\mathbb{Q}$.

Es gilt hier sogar schärfer: Für $p, q \in \mathbb{P}$ mit $p \neq q$ sind $\mathbb{Q}(\sqrt{p})$ und $\mathbb{Q}(\sqrt{q})$ nicht isomorph zueinander. Dies zeigt, dass $\overline{\mathbb{Q}}|\mathbb{Q}$ sogar unendlich viele, paarweise nichtisomorphe quadratische Körpererweiterungen über $\mathbb{Q}$ enthält.

⋇

Beispiel 24.14 Sei $p \in \mathbb{P}$ eine beliebige Primzahl. Wir zeigen, dass jedes Element aus $\mathbb{F}_p$ in $\mathbb{F}_{p^2}$ eine Quadratwurzel besitzt, d. h. dass zu jedem $a \in \mathbb{F}_p$ ein $\alpha \in \mathbb{F}_{p^2}$ existiert mit $a = \alpha^2$.

Sei hierzu ein algebraischer Abschluss $\overline{\mathbb{F}_p}$ von $\mathbb{F}_p$ fixiert. Sei $a \in \mathbb{F}_p$ beliebig. Besitzt a bereits eine Quadratwurzel in $\mathbb{F}_p$, so sind wir fertig, denn es ist $\mathbb{F}_p \subseteq \mathbb{F}_{p^2}$.

Nun möge a keine Quadratwurzel in $\mathbb{F}_p$ besitzen. Dann ist $m := X^2 - a \in \mathbb{F}_p[X]$ normiert und irreduzibel. Im Körper $\mathbb{F}_p[X]/(m) = \mathbb{F}_{p^2}$ besitzt m nach Kronecker eine Nullstelle. Dort existiert also ein α mit $\alpha^2 = a$.

Nach 24.12 existiert in der Erweiterung $\overline{\mathbb{F}_p} \mid \mathbb{F}_p$ nur ein einziger Körper der Ordnung p^2. Alle Quadratwurzeln aller Elemente aus $\mathbb{F}_p$ liegen somit in diesem Körper $\mathbb{F}_{p^2}$. ⋇

Eine weitere Konsequenz aus 24.8 ist das folgende Resultat über normierte, irreduzible Polynome:

Satz 24.15 *Seien $p \in \mathbb{P}$ eine beliebige Primzahl und $m \in \mathbb{F}_p[X]$ ein normiertes, irreduzibles Polynom vom Grad $r \in \mathbb{N}$. Dann teilt m das Polynom $f := X^{p^r} - X \in \mathbb{F}_p[X]$.*

Beweis. Sei $a \in \overline{\mathbb{F}_p}$ eine beliebige Nullstelle von m. Dann gilt $\mathbb{F}_p(a) = \mathbb{F}_{p^r}$ nach 24.4. Mit 24.8 folgt $f(a) = 0$. Da m das Minimalpolynom von a über $\mathbb{F}_p$ ist, gilt $m \mid f$. ■

Mit Hilfe dieses Satzes kann man alle normierten, irreduziblen Polynome eines bestimmten Grades finden:

Beispiel 24.16 Wir wollen alle normierten, irreduziblen Polynome vom Grad Zwei in $\mathbb{F}_3[X]$ bestimmen. Nach 24.15 teilen solche Polynome das Polynom $f := X^{3^2} - X \in \mathbb{F}_3[X]$. Eine Zerlegung von f in irreduzible Faktoren liefert

$$f = X \cdot (X+1) \cdot (X+2) \cdot (X^2+1) \cdot (X^2+X+2) \cdot (X^2+2X+2).$$

Die normierten, irreduziblen Polynome vom Grad Zwei in $\mathbb{F}_3[X]$ sind daher genau die letzten drei Polynome in obiger Zerlegung. ⋇

Zwischenkörperstruktur von $\mathbb{F}_{p^r}|\mathbb{F}_p$

Der folgende Satz beschreibt die Zwischenkörper der Erweiterung $\mathbb{F}_{p^r}|\mathbb{F}_p$:

Satz 24.17 *Seien $p \in \mathbb{P}$ und $r \in \mathbb{N}$. Der Körper $\mathbb{F}_{p^s}$ ist genau dann ein Unterkörper von $\mathbb{F}_{p^r}$, wenn $s \mid r$ gilt.*

Beweis.

$\Longrightarrow$ Sei $\mathbb{F}_{p^s}$ ein Unterkörper von $\mathbb{F}_{p^r}$. Dann lässt sich $\mathbb{F}_{p^r}$ als $\mathbb{F}_{p^s}$-Vektorraum auffassen. Gilt $[\mathbb{F}_{p^r} : \mathbb{F}_{p^s}] = n$, so ist $\mathbb{F}_{p^r}$ als Vektorraum isomorph zu $\mathbb{F}_{p^s}^n$. Wir erhalten

$$p^r = |\mathbb{F}_{p^r}| = |\mathbb{F}_{p^s}^n| = (p^s)^n = p^{ns}, \qquad \text{also} \qquad s \mid r.$$

$\Longleftarrow$ Sei nun $s \mid r$, d. h. $r = ns$ mit einem $n \in \mathbb{N}$. Sei $a \in \mathbb{F}_{p^s}$ beliebig. Dann gilt $a^{p^s} = a$ nach 24.8. Induktiv folgt hieraus $a^{p^{k \cdot s}} = a$ für alle $k \in \mathbb{N}$. Somit ist $a^{p^r} = a^{p^{ns}} = a$, was $a \in \mathbb{F}_{p^r}$ zeigt.

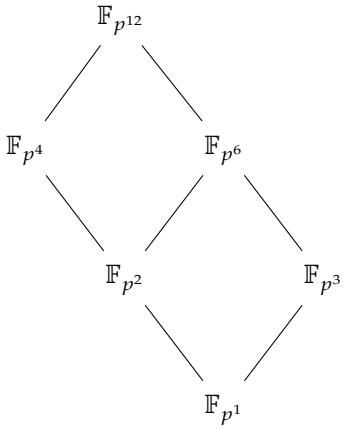
Da a beliebig aus $\mathbb{F}_{p^s}$ gewählt war, folgt $\mathbb{F}_{p^s} \subseteq \mathbb{F}_{p^r}$. Dies war zu zeigen. ■

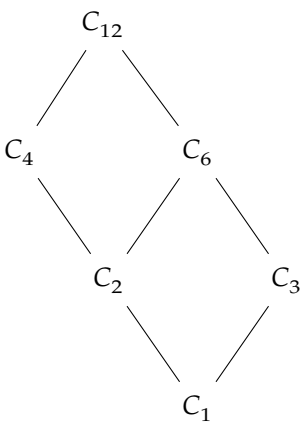
Bemerkung 24.18 (a) Um zu entscheiden, ob $\mathbb{F}_{p^s} \subseteq \mathbb{F}_{p^r}$ gilt, sind die **Exponenten** r und s zu untersuchen. Die Primzahl p ist völlig egal.

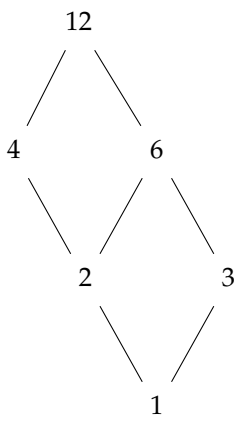
Für *jedes* $p \in \mathbb{P}$ ist $\mathbb{F}_{p^2}$ *kein* Unterkörper von $\mathbb{F}_{p^3}$, denn $2 \nmid 3$. Allerdings ist $\mathbb{F}_{p^2}$ ein Unterkörper von $\mathbb{F}_{p^4}$. Dies zeigt: $\mathbb{F}_4$ ist kein Unterkörper von $\mathbb{F}_8$, aber von $\mathbb{F}_{16}$.

(b) Obiger Satz und die Klassifizierung der Untergruppen einer endlichen zyklischen Gruppe 7.22 ähneln sich: In beiden Resultaten treten dieselben Teilbarkeitsbedingungen auf, einmal angewendet auf Exponenten von Primpotenzen, das andere Mal angewendet auf Gruppenordnungen. Daher überträgt sich 7.23 dem Sinn nach auf endliche Erweiterungen endlicher Körper, vgl. das folgende Beispiel. ⋇

Beispiel 24.19 Wegen Teil (b) der obigen Bemerkung stimmt der Zwischenkörperverband der Erweiterung $\mathbb{F}_{p^r}|\mathbb{F}_p$ mit dem Untergruppenverband der zyklischen Gruppe C_r und dem Teilerdiagramm von r überein. Für das Beispiel $r = 12$ erhalten wir (für beliebiges $p \in \mathbb{P}$):


$\mathbb{F}_{p^{12}}$
$\mathbb{F}_{p^4}$
$\mathbb{F}_{p^6}$
$\mathbb{F}_{p^2}$
$\mathbb{F}_{p^3}$
$\mathbb{F}_{p^1}$


C_{12}
C_4
C_6
C_2
C_3
C_1


12
4
6
2
3
1

※

25. K-Automorphismen, Normalität und Separabilität

Worum geht es? Für eine Körpererweiterung $L|K$ führen wir den Begriff eines *K-Automorphismus von L* ein und untersuchen, wie viele solche Automorphismen eine einfache Körpererweiterung hat. Dies führt auf die Begriffe der *normalen* und der *separablen Körpererweiterung*. Wir stellen die wichtigsten Resultate im Zusammenhang mit diesen beiden Begriffen vor. ⋇

Warum braucht man Normalität und Separabilität?

In den nachfolgenden Vorlesungen werden wir uns mit *Galoistheorie* beschäftigen. Mit Hilfe dieser Theorie lassen sich tiefe Aussagen über gewisse Körpererweiterungen beweisen; insbesondere beschreibt sie alle Zwischenkörper dieser Körpererweiterungen.
Interessanterweise untersucht man in der Galoistheorie nicht die gegebene Körpererweiterung $L|K$ selbst, sondern man ordnet der Erweiterung $L|K$ die Menge der *K-Automorphismen von L* zu. Mit Hilfe des *Hauptsatzes der Galoistheorie* lassen sich dann Aussagen über diese Automorphismen zurück in Aussagen über $L|K$ übersetzen.
Nicht zuletzt aufgrund der Galoistheorie spielen Automorphismen in der Körpertheorie eine große Rolle.

Wir klären zunächst, was ein K-Automorphismus eines Körpers ist:

Definition 25.1 *Sei $L|K$ eine Körpererweiterung. Unter einem **K-Automorphismus von L** versteht man einen Körperautomorphismus $\varphi : L \to L$, der $\varphi(k) = k$ für alle $k \in K$ erfüllt. Die Einschränkung $\varphi|_K$ von φ auf K ist also vom Typ $K \to K$ und stimmt mit id_K überein.*
Wir bezeichnen die Menge aller K-Automorphismen von L mit $\mathrm{Aut}_K(L)$.

Bemerkung 25.2 Einen K-Automorphismus von L kann man als Fortsetzung von id_K zu einem Automorphismus $L \to L$ auffassen. $\mathrm{Aut}_K(L)$ wird dann zur Menge aller möglichen Fortsetzungen von id_K zu Automorphismen von L.
Dies erklärt, warum das Fortsetzungslemma 23.1 in der Körpertheorie eine so zentrale Rolle einnimmt und warum Beweise von Aussagen, die K-Automorphismen involvieren, meist recht technisch sind. ⋇

Die Menge der K-Automorphismen eines Körpers L besitzt eine schöne algebraische Struktur:

Satz 25.3 *Sei $L|K$ eine Körpererweiterung. Dann ist $\mathrm{Aut}_K(L)$ eine Gruppe; die Gruppenverknüpfung ist hierbei die Komposition von Abbildungen.*

Beweisskizze. Wir wissen aus 6.11, dass die Menge $\mathrm{Aut}(L)$ aller Automorphismen von L eine Gruppe bildet.
Mit Hilfe des Untergruppenkriteriums sieht man nun, dass $\mathrm{Aut}_K(L)$ eine Untergruppe von $\mathrm{Aut}(L)$ ist. Dies zeigt den Satz. ■ ⁉

K-Automorphismen haben ein sehr eingeschränktes Abbildungsverhalten:

Satz 25.4 *Seien $L|K$ eine Körpererweiterung, $f \in K[X]$ und $a \in L$ eine Nullstelle von f. Für jeden K-Automorphismus $\varphi \in \mathrm{Aut}_K(L)$ gilt dann $f(\varphi(a)) = 0$.*
K-Automorphismen von L bilden daher Nullstellen eines Polynoms aus $K[X]$ wieder auf Nullstellen desselben Polynoms ab.

Beweis. Schreiben wir $f = \sum_{i=0}^{n} k_i X^i$ mit $k_i \in K$, so folgt

$$\begin{aligned} 0 &= \varphi(0) = \varphi(f(a)) = \varphi\Big(\sum_{i=0}^{n} k_i a^i\Big) \\ &\overset{\varphi \text{ ist Kö.autom.}}{=} \sum_{i=0}^{n} \varphi(k_i) \cdot \varphi(a)^i \overset{\varphi|_K = \mathrm{id}_K}{=} \sum_{i=0}^{n} k_i \varphi(a)^i = f(\varphi(a)). \end{aligned}$$

Damit ist der Satz gezeigt. ■

Beispiel 25.5 (a) Für jede Körpererweiterung $L|K$ gilt $\mathrm{id}_L \in \mathrm{Aut}_K(L)$. Speziell für $K = L$ gilt $\mathrm{Aut}_K(K) = \{\mathrm{id}_K\}$.

(b) Sei $L := \mathbb{Q}(\sqrt[3]{2})$. Wir zeigen, dass es nur einen $\mathbb{Q}$-Automorphismus von L gibt, nämlich id_L:

Das Polynom $m := X^3 - 2 \in \mathbb{Q}[X]$ hat die Nullstelle $\sqrt[3]{2}$. Es besitzt keine weiteren reellen Nullstellen. Nach 25.4 bildet $\varphi \in \mathrm{Aut}_{\mathbb{Q}}(L)$ das Element $\sqrt[3]{2}$ auf eine Nullstelle von m ab, die in L liegt. Da $L \subseteq \mathbb{R}$ gilt, muss daher $\varphi(\sqrt[3]{2}) = \sqrt[3]{2}$ sein. Es folgt $\varphi = \mathrm{id}_L$. Nach (a) ist id_L tatsächlich ein $\mathbb{Q}$-Automorphismus von L. ⁜ ⁉

Wir abstrahieren Teil (b) des obigen Beispiels und klassifizieren alle K-Automorphismen für *einfache* algebraische Erweiterungen $L|K$. Wir kommen in Vorlesung 28 auf das folgende Beispiel zurück und führen es genauer aus.

Beispiel 25.6 Sei $L|K$ eine einfache, algebraische Körpererweiterung. Dann existiert ein $a \in L$ mit $L = K(a)$. Da $L|K$ algebraisch ist, besitzt a ein Minimalpolynom $m \in K[X]$.
Sei $\varphi \in \mathrm{Aut}_K(L)$ beliebig. φ ist durch die Angabe des Bildes $\varphi(a) \in L$ festgelegt.
Nach 25.4 gilt $m(\varphi(a)) = 0$. Somit muss a durch φ auf eine Nullstelle von m, die in L liegt, abgebildet werden.
Nach 22.11 bzw. Fortsetzungslemma wird durch die Festsetzung $\varphi(a) := b$, wobei b eine beliebige Nullstelle von m in L bezeichnet, tatsächlich ein K-Automorphismus von L definiert. Für verschiedene b erhält man verschiedene K-Automorphismen.

Insgesamt haben wir damit gezeigt: Die Anzahl der K-Automorphismen von L entspricht der Anzahl der **verschiedenen** Nullstellen von m, die **in L** liegen. Insbesondere folgt $|\mathrm{Aut}_K(L)| \leq [L : K]$. ⁜ ⁉

Galoistheorie ist nur auf endliche Körpererweiterungen $L|K$ anwendbar, für die die in 25.6 hergeleitete Abschätzung $|\mathrm{Aut}_K(L)| \leq [L : K]$ scharf ist. Für das obige Beispiel bedeutet dies:

(a) Das Minimalpolynom m von a muss $\deg m$ viele verschiedene Nullstellen in seinem Zerfällungskörper besitzen. m darf also keine Mehrfachnullstellen haben.

(b) Der Körper $K(a)$ muss neben der Nullstelle a auch alle weiteren Nullstellen von m enthalten.

Die Bedingung aus (a) führt auf den Begriff der Separabilität, die aus (b) auf den Begriff der Normalität.

Normale Körpererweiterungen

Definition 25.7 *Wir nennen eine endliche Körpererweiterung $L|K$* ***normal****, wenn jedes normierte, irreduzible Polynom $m \in K[X]$, das in L eine Nullstelle besitzt, in $L[X]$ bereits vollständig in Linearfaktoren zerfällt.*

Bemerkung 25.8 (a) Normale Körpererweiterungen sind endlich und somit stets algebraisch.

(b) Ist $L|K$ normal und ist $m \in K[X]$ das Minimalpolynom eines Elements aus L, so zerfällt m über L vollständig. Der Zerfällungskörper von m ist daher ein Zwischenkörper der Erweiterung $L|K$. ⁜

Beispiel 25.9 Die Erweiterung $\mathbb{Q}(\sqrt[3]{2})|\mathbb{Q}$ ist nicht normal: $X^3 - 2 \in \mathbb{Q}[X]$ ist das Minimalpolynom von $\sqrt[3]{2}$ und hat zwei echt komplexe Nullstellen. Diese liegen nicht im Körper $\mathbb{Q}(\sqrt[3]{2})$. ⁜

25.7 eignet sich gut, um die Normalität einer Körpererweiterung $L|K$ zu widerlegen: Hierzu muss man nur ein Element $a \in L$ finden, so dass eine weitere Nullstelle des Minimalpolynoms von a nicht in L liegt, vgl. das obige Beispiel.
Der Nachweis der Normalität mit Hilfe von 25.7 ist schwieriger. Hier hilft die folgende Charakterisierung der Normalität, deren Beweis Sie beispielsweise in [KM17, Satz 24.13 auf S. 321] finden.

Satz 25.10 *Für eine endliche Körpererweiterung $L|K$ sind äquivalent:*

(a) *$L|K$ ist normal.*

(b) *L ist Zerfällungskörper eines Polynoms aus $K[X]$.*

Teil (b) des Satzes erleichtert den Normalitätsnachweis enorm:

Beispiel 25.11 (a) Jede quadratische Körpererweiterung $L|K$ ist normal.

Nach 20.15 (a) existiert $a \in L$ mit $L = K(a)$. Sei $m \in K[X]$ das Minimalpolynom von a; es gilt $\deg m = 2$. Polynomdivision durch $X - a$ zeigt, dass m über L in Linearfaktoren zerfällt. Daher ist L der Zerfällungskörper von m über K. Nach 25.10 (b) ist $L|K$ normal. ⁉

(b) Normalität setzt sich nicht von Teilerweiterungen auf die Gesamterweiterung fort:

$\mathbb{Q}(\sqrt[4]{2})$
$|\,2$
$\mathbb{Q}(\sqrt{2})$
$|\,2$
$\mathbb{Q}$

Beispielsweise sind die Erweiterungen $\mathbb{Q}(\sqrt[4]{2})|\mathbb{Q}(\sqrt{2})$ und $\mathbb{Q}(\sqrt{2})|\mathbb{Q}$ als Grad-Zwei-Erweiterungen beide normal, die Erweiterung $\mathbb{Q}(\sqrt[4]{2})|\mathbb{Q}$ ist jedoch *nicht* normal. Dies sieht man ähnlich wie in 25.9, denn $X^4 - 2 \in \mathbb{Q}[X]$ hat zwei echt komplexe Nullstellen.

(c) Normalität setzt sich nicht von der Gesamterweiterung auf die untere Teilerweiterung fort:

$\mathbb{Q}(\sqrt[3]{2}, \xi)$
$|\,2$
$\mathbb{Q}(\sqrt[3]{2})$
$|\,3$
$\mathbb{Q}$

Wir setzen $\xi := \exp(2\pi i/3)$ und $L := \mathbb{Q}(\sqrt[3]{2}, \xi)$. Dann ist die Erweiterung $L|\mathbb{Q}$ normal, denn L ist der Zerfällungskörper des Polynoms $X^3 - 2 \in \mathbb{Q}[X]$. Die Teilerweiterung $\mathbb{Q}(\sqrt[3]{2})|\mathbb{Q}$ ist jedoch nicht normal, vgl. 25.9. ⁜

Knobelfrage. Setzt sich Normalität auf obere Teilerweiterungen fort, d. h. folgt aus der Normalität von $L|K$, dass auch $L|Z$ für jeden Zwischenkörper Z normal ist? ?

Separabilität

Definition 25.12 *Sei $L|K$ eine algebraische Körpererweiterung. Wir nennen ein Element $a \in L$ **separabel über K**, wenn sein Minimalpolynom über K keine Mehrfachnullstellen in seinem Zerfällungskörper besitzt. Andernfalls nennen wir a **inseparabel über K**.*
*Sind alle Elemente aus L separabel über K, so nennen wir die Erweiterung $L|K$ **separabel**. Andernfalls nennen wir $L|K$ **inseparabel**.*

Beispiel 25.13 Sei $L|K$ eine separable Körpererweiterung.

(a) Sei $m \in K[X]$ das Minimalpolynom zu einem beliebigen Element $a \in L$. Dann gilt $\deg \operatorname{ggT}(m, m') = 0$ nach 23.22, d. h. m und m' sind teilerfremd.

(b) Separabilität vererbt sich auf Teilerweiterungen: Ist Z ein Zwischenkörper von $L|K$, so sind auch $L|Z$ und $Z|K$ separabel:

Nach Voraussetzung ist jedes Element aus L separabel über K. Daher ist auch jedes Element aus Z separabel über K, denn Z ist eine Teilmenge von L. Dies zeigt die Separabilität von $Z|K$.

Seien $a \in L$ beliebig und $m_Z \in Z[X]$ bzw. $m_K \in K[X]$ das Minimalpolynom von a über Z bzw. über K. In $Z[X]$ gilt $m_Z \mid m_K$, denn m_K annulliert a, vgl. 20.21. Da a nach Voraussetzung separabel über K ist, sind die Nullstellen von m_K paarweise verschieden. Weil m_Z ein Teiler von m_K ist, gilt dies auch für m_Z. Also ist a separabel über Z. Da dies für alle $a \in L$ gilt, ist die Erweiterung $L|Z$ separabel. ⁜

Wir untersuchen inseparable Körpererweiterungen genauer. Das Ergebnis der nächsten Resultate ist, dass Inseparabilität „selten“ ist und recht spezielle Anforderungen an die auftretenden Körper stellt.

Satz 25.14 *Sei $L|K$ eine Körpererweiterung. Das Element $a \in L$ sei inseparabel über K. Dann gilt $m' = 0$ für das Minimalpolynom $m \in K[X]$ von a über K.*

Beweis. Da a inseparabel über K ist, besitzt m in seinem Zerfällungskörper Mehrfachnullstellen. Nach 23.22 besitzen m und m' dann einen gemeinsamen Teiler $t \in K[X]$ mit $\deg t \geq 1$.
m ist als Minimalpolynom irreduzibel. Bis auf Assoziiertheit, also Multiplikation mit Elementen aus $K^\times$, besitzt m daher nur die Teiler 1 und m. Wegen $\deg t \geq 1$ ist t assoziiert zu m, d. h. es gilt $t = c \cdot m$ mit einem $c \in K^\times$. Insbesondere ist $\deg t = \deg m$.
t teilt auch m'. Da $\deg m' < \deg m = \deg t$ gilt, ist dies nur möglich, wenn $m' = 0$ ist.
Dies zeigt den Satz. ■

Korollar 25.15 *Der Körper K habe Charakteristik Null. Dann ist jede algebraische Körpererweiterung $L|K$ separabel.*
Insbesondere sind alle algebraischen Erweiterungen $L|\mathbb{Q}$ separabel.

Beweis. Sei $m := \sum_{i=0}^{n} k_i X^i \in K[X]$ das Minimalpolynom eines beliebigen Elements $a \in L$. Dann gelten $n \geq 1$ und $k_n = 1$. Es ist $m' = \sum_{i=1}^{n} i k_i X^{i-1}$.
Der $(n-1)$-te Koeffizient von m' ist $nk_n = n \in K$. Da K Charakteristik Null hat und $n \geq 1$ ist, folgt $n \neq 0$ in K. Daher ist $\deg m' = n - 1 \geq 0$ und somit $m' \neq 0$. Nach 25.14 folgt die Separabilität von a über K.
Da $a \in L$ beliebig gewählt war, folgt die Separabilität von $L|K$. ■

Korollar 25.16 *Sei $L|K$ eine inseparable Erweiterung. Dann ist die Charakteristik von K eine Primzahl $p \in \mathbb{P}$ und K ist eine **transzendente** Erweiterung von $\mathbb{F}_p$.*

Beweis. Wegen 25.15 hat K nicht die Charakteristik Null, also Charakteristik p für ein $p \in \mathbb{P}$, und ist somit eine Erweiterung von $\mathbb{F}_p$.
Zum Nachweis der Transzendenz von $K|\mathbb{F}_p$ führen wir einen Widerspruchsbeweis und nehmen an, dass $K|\mathbb{F}_p$ algebraisch sei. Dann ist nach 22.6 (c) auch die Gesamterweiterung $L|\mathbb{F}_p$ algebraisch.
Sei $a \in L$ beliebig. Da a algebraisch über $\mathbb{F}_p$ ist, ist $\mathbb{F}_p(a)|\mathbb{F}_p$ eine endliche Erweiterung. Somit gilt $\mathbb{F}_p(a) = \mathbb{F}_{p^r}$ mit $r = [\mathbb{F}_p(a) : \mathbb{F}_p] \in \mathbb{N}$.
a ist Nullstelle des Polynoms $f := X^{p^r} - X \in \mathbb{F}_p[X]$. Dieses Polynom hat genau die p^r Elemente aus $\mathbb{F}_{p^r}$ als Nullstellen und besitzt somit keine Mehrfachnullstellen. Das Minimalpolynom $m \in \mathbb{F}_p[X]$ von a über $\mathbb{F}_p$ teilt f und hat ebenfalls keine Mehrfachnullstellen. a ist daher separabel über $\mathbb{F}_p$.
Da dies für jedes $a \in L$ gilt, folgt die Separabilität der Erweiterung $L|\mathbb{F}_p$. Aus 25.13 (b) folgt die Separabilität von $L|K$, was der Voraussetzung widerspricht. $K|\mathbb{F}_p$ kann also nicht algebraisch gewesen sein. ■

Bemerkung 25.17 Obiges Korollar sagt, dass inseparable Körpererweiterungen transzendente Elemente über $\mathbb{F}_p$ enthalten. Dies bedeutet im Umkehrschluss, dass alle algebraischen Erweiterungen der Körper $\mathbb{F}_p$ mit $p \in \mathbb{P}$ stets separabel sind.
Da wir hauptsächlich mit algebraischen Erweiterungen von $\mathbb{Q}$ oder $\mathbb{F}_p$ arbeiten, spielen inseparable Körpererweiterungen für uns also kaum eine Rolle. ※

Wir geben ein Beispiel für eine inseparable Körpererweiterung:

Beispiel 25.18 Seien p eine Primzahl und t ein über $\mathbb{F}_p$ transzendentes Element. Wir betrachten das Polynom $f := X^p - t \in \mathbb{F}_p(t)[X]$.
Wir zeigen zunächst, dass f irreduzibel ist. Hierzu wenden wir das Eisensteinkriterium an: Aufgrund der Transzendenz von t ist der Ring $R := \mathbb{F}_p[t]$ isomorph zum Polynomring über $\mathbb{F}_p$ und daher euklidisch. Das Element t lässt sich als Grad-Eins-Polynom in R auffassen und ist nach 19.5 (a) irreduzibel und somit prim. f erfüllt als Polynom in $R[X]$ eine Eisensteinbedingung bezüglich t. Nach 19.15 ist f daher unzerlegbar in $R[X]$. Mit Gauß 19.12 ist es auch unzerlegbar und daher irreduzibel in $Q(R)[X]$, also in $\mathbb{F}_p(t)[X]$.

Da $p = 0$ in $\mathbb{F}_p$ gilt, folgt $f' = pX^{p-1} = 0$. Daher ist $\mathrm{ggT}(f, f') = \mathrm{ggT}(f, 0) = f$. Nach 23.22 besitzt f Mehrfachnullstellen in seinem Zerfällungskörper Z.
Sei $a \in Z$ eine solche Mehrfachnullstelle von f. Dann ist $a^p = t$. Es gilt $\mathbb{F}_p(t, a) = \mathbb{F}_p(a)$ und dieser Körper hat Grad p über $\mathbb{F}_p(t)$. In $\mathbb{F}_p(a)[X]$ gilt

$$f = X^p - t = X^p - a^p \overset{\text{Frobenius}}{=} (X - a)^p.$$

Dies zeigt, dass $\mathbb{F}_p(a) = Z$ der Zerfällungskörper von f ist und dass das irreduzible Grad-p-Polynom f dort nur genau eine Nullstelle besitzt.
Die Grad-p-Erweiterung $\mathbb{F}_p(a)|\mathbb{F}_p(t)$ ist algebraisch. Das Element a ist inseparabel über $\mathbb{F}_p(t)$. Die Erweiterung $\mathbb{F}_p(a)|\mathbb{F}_p(t)$ ist daher ebenfalls inseparabel. ⋇

Bemerkung 25.19 25.18 liefert das einfachste Beispiel für eine inseparable Körpererweiterung:
Ist $L|K$ eine inseparable Erweiterung, so ist K nach 25.16 eine transzendente Erweiterung einer der Körper $\mathbb{F}_p$. Das minimale Beispiel für K ist daher $\mathbb{F}_p(t)$ mit einem transzendenten Element t.
Nach 25.14 muss $K[X]$ ein normiertes, irreduzibles Polynom f mit $f' = 0$ enthalten. Der kleinste Grad, den ein solches Polynom besitzen kann, ist p, denn ansonsten wäre $\deg f' = \deg f - 1 \geq 0$ und somit $f' \neq 0$. ⋇

Der folgende Satz sagt aus, dass die Frage nach der Separabilität einer Körpererweiterung durch Untersuchung von nur wenigen Körperelementen entschieden werden kann. Da die von uns betrachteten Körpererweiterungen nach 25.17 sowieso fast immer separabel sind, hat der Satz für uns kaum einen Nutzen. Wir führen daher seinen recht technischen Beweis nicht und verweisen auf [KM17, Lemma 25.9 auf S. 325].

Satz 25.20 *Sei $L|K$ eine Körpererweiterung. Der Körper L möge sich schreiben lassen in der Form $K(M)$ mit einer geeigneten Teilmenge $M \subseteq L$. Dann gilt: Sind alle Elemente aus M separabel über K, so ist $L|K$ separabel.*
Die (komplizierte) Frage nach der Separabilität der Erweiterung $L|K$ lässt sich also auf die Frage reduzieren, ob die (wenigen) Elemente aus M separabel über K sind.

Ein wichtiger Satz in der Theorie separabler Körpererweiterungen ist der folgende *Satz vom primitiven Element*. Es gibt viele verschiedene Beweise für diesen Satz, leider keinen kurzen und leicht verständlichen; wir verweisen auf [KM17, Satz 25.6 auf S. 333].

Satz 25.21 (Satz vom primitiven Element) *Sei $L|K$ eine endliche, separable Körpererweiterung. Dann ist $L|K$ einfach, d. h. es gibt ein Element $a \in L$ mit $L = K(a)$.*

Da endliche Erweiterungen von $\mathbb{Q}$ nach 25.15 stets separabel sind, folgt:

Korollar 25.22 *Jede endliche Erweiterung von $\mathbb{Q}$ ist einfach.*

Bemerkung 25.23 (a) Der Satz vom primitiven Element wird gerne in Beweisen verwendet. Er erlaubt es, gewisse Körpererweiterungen $L|K$ in der Form $K(a)|K$ zu schreiben. Die Untersuchung der Erweiterung $L|K$ lässt sich dann oft auf die Untersuchung des Elements a reduzieren.

Im praktischen Umgang mit Körpererweiterungen spielt der Satz vom primitiven Element allerdings kaum eine Rolle. So lässt sich beispielsweise relativ einfach zeigen, dass die Erweiterung $\mathbb{Q}(\sqrt{2}, \sqrt{3}, i) \mid \mathbb{Q}$ den Grad 8 hat. Nach obigem Korollar gibt es daher ein primitives Element a für diese Erweiterung, dessen Minimalpolynom über $\mathbb{Q}$ den Grad 8 hat. Der praktische Umgang mit a ist daher komplizierter und schwerfälliger als der Umgang mit den drei Grad-2-Elementen $\sqrt{2}$, $\sqrt{3}$ und i.

(b) Im Beweis des Satzes vom primitiven Element betrachtet man eine endliche, separable Erweiterung $K(a, b)|K$ mit unendlichem Unterkörper K und zeigt, dass die Linearkombination $a + \lambda b$ für unendlich viele $\lambda \in K$ primitiv ist.

Genauer gilt: Für λ kann jedes Element aus K gewählt werden, das *nicht* von der Form $\frac{a'-a}{b-b'}$ ist, wobei a' die Nullstellen des Minimalpolynoms von a über K und b' die Nullstellen des Minimalpolynoms von b über K durchläuft und $b \neq b'$ gilt.

Wir setzen beispielhaft $L := \mathbb{Q}(\sqrt{2}, \sqrt{3})$ und betrachten die Erweiterung $L|\mathbb{Q}$. Die Nullstellen des Minimalpolynoms von $\sqrt{2}$ über $\mathbb{Q}$ sind $\pm\sqrt{2}$, die des Minimalpolynoms von $\sqrt{3}$ über $\mathbb{Q}$ sind $\pm\sqrt{3}$. Jede Linearkombination der Form $\sqrt{2} + \lambda \cdot \sqrt{3}$ ist ein primitives Element der Erweiterung $L|\mathbb{Q}$, sofern $\lambda \in \mathbb{Q}$ nicht die Werte

$$\frac{\sqrt{2} - \sqrt{2}}{\sqrt{3} - (-\sqrt{3})} = 0 \qquad \text{oder} \qquad \frac{-\sqrt{2} - \sqrt{2}}{\sqrt{3} - (-\sqrt{3})} = -\sqrt{\frac{2}{3}}$$

annimmt. Wir können daher $\lambda \in \mathbb{Q} \setminus \{0\}$ beliebig wählen. Es folgt beispielsweise $L = \mathbb{Q}(\sqrt{2} + \sqrt{3})$. ※

Wir kommen zurück auf 25.6 und können nun zeigen:

Satz 25.24 *Die Erweiterung $L|K$ sei normal und separabel. Dann gilt $|\operatorname{Aut}_K(L)| = [L : K]$.*

Beweis. Nach dem Satz vom primitiven Element ist $L|K$ einfach. Sei $a \in L$ ein primitives Element der Erweiterung mit Minimalpolynom $m \in K[X]$. Nach 25.6 stimmt $|\operatorname{Aut}_K(L)|$ mit der Anzahl der verschiedenen Nullstellen von m, die in L liegen, überein. Aufgrund der Normalität von $L|K$ liegen *alle* Nullstellen von m in L. Aufgrund der Separabilität von $L|K$ hat m nur einfache Nullstellen.
Es ist daher $|\operatorname{Aut}_K(L)| = \deg m = [L : K]$. ■

26. Der Hauptsatz der Galoistheorie

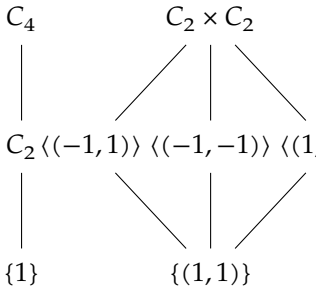
Worum geht es? Wir beschäftigen uns mit *Galoiserweiterungen*. Für diese definieren wir den Begriff der *Galoisgruppe*. Der *Hauptsatz der Galoistheorie* liefert dann eine Bijektion zwischen den Untergruppen der Galoisgruppe und den Zwischenkörpern der betrachteten Galoiserweiterung.
Die Elemente der Galoisgruppe fassen wir in dieser Vorlesung primär als Körperautomorphismen auf. In dieser Darstellung ist der Umgang mit ihnen sehr mühselig, was die geringe Anzahl an Beispielen, die wir in dieser Vorlesung geben, erklärt. In der nächsten Vorlesung lernen wir eine praktischere Darstellung der Galoisautomorphismen kennen; dann werden wir auch mehr Beispiele besprechen. ⋇

Mit Hilfe der Galoistheorie lassen sich normale, separable Körpererweiterungen $L|K$ untersuchen. Die Galoistheorie arbeitet nicht direkt mit der Erweiterung $L|K$, sondern mit der Gruppe $\mathrm{Aut}_K(L)$ der K-Automorphismen von L. Dem Hauptsatz kommt hierbei eine zentrale Rolle zu: Er übersetzt zwischen Aussagen über $\mathrm{Aut}_K(L)$ und Aussagen über $L|K$. Anstatt (schwere) *körpertheoretische* Probleme zu lösen, können mit Hilfe der Galoistheorie äquivalente *gruppentheoretische* Probleme angegangen werden. Diese sind beweistechnisch und algorithmisch oft besser zugänglich.

Beispiel 26.1 Sei $L := \mathbb{Q}(\sqrt{2}, \sqrt{3})$. Wir sind an den Zwischenkörpern Z der Erweiterung $L|\mathbb{Q}$ interessiert. Jede der Erweiterungen $Z|\mathbb{Q}$ ist endlich und separabel, also nach 25.22 einfach. Die Zwischenkörper von $L|\mathbb{Q}$ sind daher die Körper $\mathbb{Q}(a)$ mit $a \in L$. Es gilt

$$\begin{aligned} L &= \mathbb{Q}[\sqrt{2}][\sqrt{3}] = \{q_0 + q_1\sqrt{3} : q_i \in \mathbb{Q}[\sqrt{2}]\} \\ &= \{(\alpha_0 + \alpha_1\sqrt{2}) + (\beta_0 + \beta_1\sqrt{2})\sqrt{3} : \alpha_i, \beta_i \in \mathbb{Q}\} \\ &= \{\alpha + \beta\sqrt{2} + \gamma\sqrt{3} + \delta\sqrt{6} : \alpha, \beta, \gamma, \delta \in \mathbb{Q}\}. \end{aligned}$$

Die Zwischenkörper von $L|\mathbb{Q}$ sind daher in der Form $\mathbb{Q}(\alpha + \beta\sqrt{2} + \gamma\sqrt{3} + \delta\sqrt{6})$ mit $\alpha, \beta, \gamma, \delta \in \mathbb{Q}$ darstellbar. Erst weitere, genauere Untersuchungen zeigen, ob es endlich oder unendlich viele solche Zwischenkörper gibt.
Im Kontrast zu dieser mühseligen Arbeit sagt der Hauptsatz der Galoistheorie, dass es eine Bijektion zwischen den Zwischenkörpern von $L|\mathbb{Q}$ und den Untergruppen von $G := \mathrm{Aut}_K(L)$ gibt. Die Erweiterung $L|\mathbb{Q}$ ist normal (Warum?) und separabel. Es gilt $[L : \mathbb{Q}] = 4$. Nach 25.24 ist $|G| = 4$.



Nach 12.3 gilt $G \cong C_4$ oder $G \cong C_2 \times C_2$. Links sehen Sie die Untergruppenstruktur der beiden Möglichkeiten für G.
Von vornherein ist klar, dass $L|\mathbb{Q}$ nur endlich viele Zwischenkörper besitzen kann. Außerdem sehen wir der Erweiterung $L|\mathbb{Q}$ die Zwischenkörper L, $\mathbb{Q}$, $\mathbb{Q}(\sqrt{2})$ und $\mathbb{Q}(\sqrt{3})$ an. Es folgt $G \cong C_2 \times C_2$. Der noch fehlende Zwischenkörper ist $\mathbb{Q}(\sqrt{6})$.
(Für eine vollständige Argumentation ist noch zu zeigen, dass die gefundenen Zwischenkörper paarweise verschieden sind. Dies funktioniert mit Standardmethoden der Körpertheorie.)
⋇

Galoiserweiterungen

Wir definieren die Grundbausteine der Galoistheorie, die Galoiserweiterungen:

Definition 26.2 *Unter einer* ***Galoiserweiterung*** *verstehen wir jede normale, separable Körpererweiterung.*
Ist $L|K$ eine Galoiserweiterung, so schreiben wir $\mathrm{Gal}(L|K)$ *statt* $\mathrm{Aut}_K(L)$ *und nennen diese Gruppe die* ***Galoisgruppe der Galoiserweiterung $L|K$****.*

Bemerkung 26.3 (a) Aufgrund der Definition der Normalität ist eine Galoiserweiterung stets endlich.

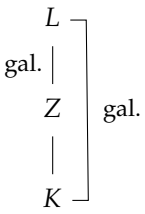
(b) Für jede Galoiserweiterung $L|K$ gilt $[L : K] = |\mathrm{Gal}(L|K)|$ nach 25.24. Die Ordnung der Galoisgruppe stimmt also immer mit dem Grad der zugehörigen Galoiserweiterung überein. Nach (a) sind Galoisgruppen stets endlich.

(c) Ist K ein Charakteristik-Null-Körper, so ist die Erweiterung $L|K$ wegen 25.15 genau dann galoissch, wenn L normal über K ist. Dies trifft insbesondere im (für uns wichtigen) Fall $K = \mathbb{Q}$ zu. Die Überprüfung der Erweiterung $L|K$ auf Separabilität kann dann entfallen. ⋇

Aus 25.10 und 25.20 folgt

Satz 26.4 *Seien K ein Körper und $f \in K[X]$ mit $f \neq 0$ ein Polynom, das in seinem Zerfällungskörper Z keine Mehrfachnullstellen besitze. Dann ist $Z|K$ eine Galoiserweiterung.*

Ist $L|K$ eine Galoiserweiterung mit Zwischenkörper Z, so folgt aus 25.13 (b), dass auch die Teilerweiterung $L|Z$ separabel ist. Außerdem ist die Erweiterung $L|Z$ normal, vgl. die Knobelfrage auf Seite 178. Dies zeigt, dass obere Teilerweiterungen von Galoiserweiterungen wieder galoissch sind.
Der folgende Satz sagt, dass in dieser Situation die Galoisgruppe von $L|Z$ zudem eine Untergruppe der Galoisgruppe von $L|K$ ist. Hier tritt eine erste schwache Verbindung zwischen der Untergruppeneigenschaft und der Zwischenkörpereigenschaft auf.



Satz 26.5 *Sei $L|K$ eine Galoiserweiterung mit Zwischenkörper Z. Dann ist auch $L|Z$ eine Galoiserweiterung. Es gilt* $\mathrm{Gal}(L|Z) \leq \mathrm{Gal}(L|K)$.

Beweis. Aufgrund der Vorbemerkung zum Satz ist nur noch die Untergruppeneigenschaft zu zeigen. Aus 25.3 ist zudem bekannt, dass $\mathrm{Gal}(L|Z)$ eine Gruppe ist. Wir müssen daher nur noch $\mathrm{Gal}(L|Z) \subseteq \mathrm{Gal}(L|K)$ zeigen. Sei hierzu $\varphi \in \mathrm{Gal}(L|Z)$. Dann ist φ ein Automorphismus von L mit $\varphi|_Z = \mathrm{id}_Z$. Da $K \subseteq Z$ gilt, folgt $\varphi|_K = \mathrm{id}_K$. Damit ist $\varphi \in \mathrm{Gal}(L|K)$. ■

Knobelfrage. Ist auch $Z|K$ eine Galoiserweiterung? Falls nein, warum nicht? ?

Der Hauptsatz der Galoistheorie

In 26.5 haben wir aus Zwischenkörpern einer Galoiserweiterung Untergruppen der ursprünglichen Galoisgruppe erzeugt. Wir beschreiben nun die umgekehrte Konstruktion:

Definition/Satz 26.6 *Sei $L|K$ eine Galoiserweiterung mit Galoisgruppe $G := \mathrm{Gal}(L|K)$. Für $U \leq G$ definieren wir die Menge*

$$\mathrm{Fix}(U) := \{a \in L \mid \varphi(a) = a \text{ für alle } \varphi \in U\}.$$

*Dann ist $\mathrm{Fix}(U)$ ein Zwischenkörper der Erweiterung $L|K$. Man nennt $\mathrm{Fix}(U)$ den **Fixkörper der Untergruppe U**.*

Beweisskizze. Die Elemente aus G und damit auch die aus U sind K-Automorphismen. Daher ist $K \subseteq \mathrm{Fix}(U)$. Ferner ist klar, dass $\mathrm{Fix}(U) \subseteq L$ gilt. Es ist daher nur noch die Körperstruktur von $\mathrm{Fix}(U)$ zu zeigen. Seien hierzu $a, b \in \mathrm{Fix}(U)$ gegeben. Wir zeigen, dass auch $a + b \in \mathrm{Fix}(U)$ gilt, indem wir $\varphi(a + b) = a + b$ für alle $\varphi \in U$ zeigen. Es gilt

$$\varphi(a+b) \overset{\varphi \text{ ist Kö.aut.}}{=} \varphi(a) + \varphi(b) \overset{a,b \in \mathrm{Fix}(U)}{=} a + b.$$

Damit ist $a + b \in \mathrm{Fix}(U)$ gezeigt. Die restlichen Abgeschlossenheiten folgen ähnlich. ■

Bemerkung 26.7 (a) Der Fixkörper $\mathrm{Fix}(U)$ besteht genau aus denjenigen Elementen $a \in L$, die von keinem Homomorphismus $\varphi \in U$ bewegt werden.

Anders formuliert: Für jedes $\varphi \in U$ gilt $\varphi|_{\mathrm{Fix}(U)} = \mathrm{id}_{\mathrm{Fix}(U)}$.

(b) Seien U und V Untergruppen der Galoisgruppe. Dann gilt

$$U \leq V \iff \mathrm{Fix}(U) \supseteq \mathrm{Fix}(V),$$

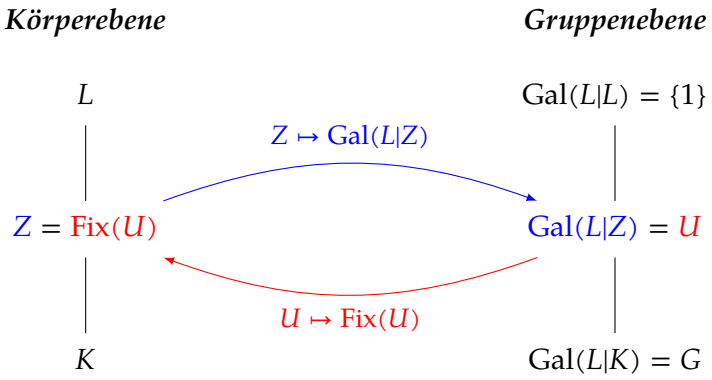
denn die Elemente von $\mathrm{Fix}(V)$ werden nicht nur von den Automorphismen aus U, sondern auch denen aus $V \setminus U$ fixiert. Diese Anforderung ist restriktiver und verkleinert den Körper $\mathrm{Fix}(V)$. ⁂ ⁉

Wir können nun einen der wichtigsten Sätze der Körpertheorie formulieren:

Satz 26.8 (Hauptsatz der Galoistheorie) *Sei $L|K$ eine Galoiserweiterung mit Galoisgruppe $G := \mathrm{Gal}(L|K)$. Dann gelten die folgenden Aussagen:*

(a) *Zwischen der Menge $\mathcal{Z}$ der Zwischenkörper von $L|K$ und der Menge der Untergruppen $\mathcal{U}$ von G wird durch die Abbildung $\mathcal{Z} \to \mathcal{U}$ mit $Z \mapsto \mathrm{Gal}(L|Z)$ eine Bijektion gegeben.*

Ihre Umkehrabbildung ist $\mathcal{U} \to \mathcal{Z}$ mit $U \mapsto \mathrm{Fix}(U)$.



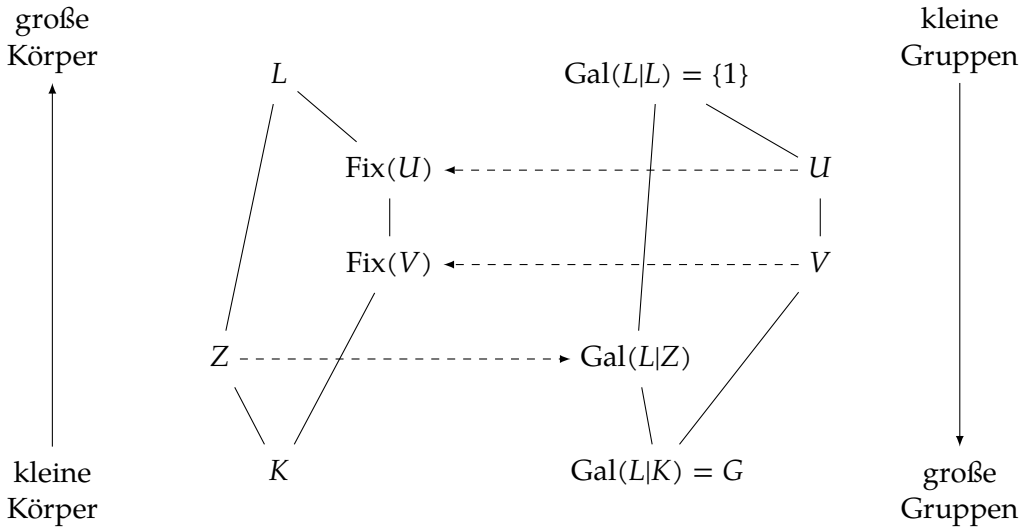
(b) *Für jeden Zwischenkörper Z gilt die Gleichheit $[L : Z] = |\mathrm{Gal}(L|Z)|$. Mit der Gradformel folgt dann*

$$[Z : K] = [\mathrm{Gal}(L|K) : \mathrm{Gal}(L|Z)] = \frac{|\mathrm{Gal}(L|K)|}{|\mathrm{Gal}(L|Z)|}.$$

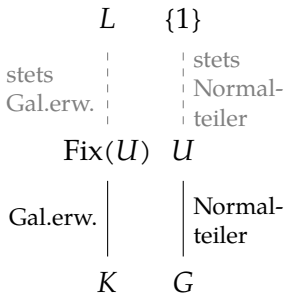
(c) *Sei Z ein Zwischenkörper von $L|K$. Dann ist die untere Teilerweiterung $Z|K$ genau dann normal, wenn $\mathrm{Gal}(L|Z) \trianglelefteq G$ gilt. In diesem Fall ist*

$$\mathrm{Gal}(Z|K) \cong \mathrm{Gal}(L|K)/\mathrm{Gal}(L|Z).$$

Bemerkung 26.9 (a) Nach 26.7 (b) gilt $U \leq V \iff \mathrm{Fix}(U) \supseteq \mathrm{Fix}(V)$ für Untergruppen U und V. Dies bedeutet, dass die Bijektionen im Hauptsatz die $\subseteq$-Relation umkehren. Sie erhalten zwar die Struktur von Zwischenkörper und Untergruppendiagramm, drehen aber eines von beiden um. Typischerweise zeichnet man in Galois-Schaubildern große Körper weiter oben, große Gruppen jedoch weiter unten ein:



(b) Teil (c) des Hauptsatzes heißt in der Literatur oft auch *Zusatz zum Hauptsatz*. Er charakterisiert, wann untere Teilerweiterungen galoissch sind.



Genau dann ist die untere Teilerweiterung $\mathrm{Fix}(U)|K$ eine Galoiserweiterung, wenn zwischen G und U eine Normalteilerbeziehung besteht, d. h. wenn $U \trianglelefteq G$ ist.

Beachten Sie, dass diese Aussage auch für *obere* Teilerweiterungen gilt (und dann trivial ist): Obere Teilerweiterungen sind *stets* galoissch; die Gruppe $\{1\}$ ist *stets* normal in U.

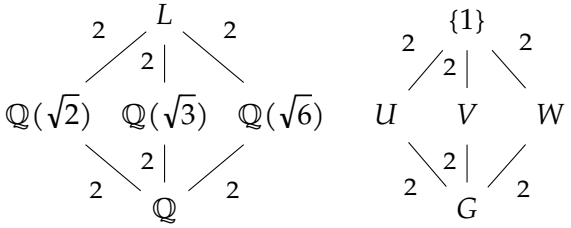
⋇

Teil (c) des Hauptsatzes liefert die folgende, in manchen Aufgaben zur Galoistheorie nützliche Aussage:

Korollar 26.10 *Sei $L|K$ eine Galoiserweiterung mit abelscher Galoisgruppe G. Dann ist die Erweiterung $Z|K$ für jeden Zwischenkörper Z von $L|K$ normal.*
Dies bedeutet umgekehrt: Besitzt eine Galoiserweiterung eine nicht-normale untere Teilerweiterung, so kann ihre Galoisgruppe nicht abelsch sein.

Beispiel 26.11 Sei L der Zerfällungskörper des Polynoms $X^3 - 2 \in \mathbb{Q}[X]$. Die Erweiterung $L|\mathbb{Q}$ ist dann galoissch und enthält den Zwischenkörper $Z := \mathbb{Q}(\sqrt[3]{2})$. Die Erweiterung $Z|\mathbb{Q}$ ist nicht normal, vgl. 25.9. Daher ist $\mathrm{Gal}(L|\mathbb{Q})$ nicht abelsch. ⋇

Beispiel 26.12 Wir führen 26.1 fort, setzen $L := \mathbb{Q}(\sqrt{2}, \sqrt{3})$ und betrachten die Erweiterung $L|\mathbb{Q}$ genauer. Sei $G := \mathrm{Gal}(L|\mathbb{Q})$. Wir wissen bereits, dass $G \cong C_2 \times C_2$ gilt.



Ferner kennen wir die Zwischenkörper von $L|\mathbb{Q}$. Die drei echten, nicht-trivialen Zwischenkörper von $L|\mathbb{Q}$ sind Fixkörper der drei echten, nicht-trivialen Untergruppen U, V, W von G.
Die Zahlen links geben den Körpererweiterungsgrad bzw. den Gruppenindex an.

Wir wollen die Automorphismen in G konkret bestimmen. Hierzu reicht es aus, wenn wir für $\varphi \in G$ die Bilder $\varphi(\sqrt{2})$ und $\varphi(\sqrt{3})$ bestimmen, denn dies legt φ fest. ⁉
Das Minimalpolynom von $\sqrt{2}$ ist $m := X^2 - 2 \in \mathbb{Q}[X]$. Die Nullstellen von m sind $\pm\sqrt{2}$. Nach 25.4 gilt für $\varphi \in G$ also $\varphi(\sqrt{2}) = \pm\sqrt{2}$. Ähnlich sieht man, dass $\varphi(\sqrt{3}) = \pm\sqrt{3}$ ist. Wir erhalten daher die folgenden vier Kandidaten für Elemente von G:

Kandidat für Automorphismus	$\sqrt{2} \mapsto$	$\sqrt{3} \mapsto$
$\varphi_1 = \mathrm{id}_L$	$\sqrt{2}$	$\sqrt{3}$
φ_2	$\sqrt{2}$	$-\sqrt{3}$
φ_3	$-\sqrt{2}$	$\sqrt{3}$
φ_4	$-\sqrt{2}$	$-\sqrt{3}$

Da $|G| = 4$ ist, sind damit alle Elemente von G gefunden: Es gilt $G = \{\varphi_1, \dots, \varphi_4\}$. Insbesondere beschreiben alle der oben gefundenen Kandidaten tatsächlich K-Automorphismen von L.
Man kann nachrechnen, dass $\operatorname{ord}(\varphi_2) = \operatorname{ord}(\varphi_3) = \operatorname{ord}(\varphi_4) = 2$ gilt und $\varphi_i \circ \varphi_j = \varphi_j \circ \varphi_i$ für alle $i, j \in \{1, \dots, 4\}$ ist. G ist damit wirklich isomorph zu $C_2 \times C_2$. ⁉
Das Körperelement $\sqrt{2}$ wird genau von φ_1 und φ_2 fixiert. Die Menge $\{\varphi_1, \varphi_2\} = \langle \varphi_2 \rangle$ ist eine Untergruppe von G und stimmt mit der oben definierten Gruppe U überein. Es gelten also $U = \langle \varphi_2 \rangle$ und $\mathbb{Q}(\sqrt{2}) = \operatorname{Fix}(U)$. Analog sieht man, dass $V = \langle \varphi_3 \rangle$ und $W = \langle \varphi_4 \rangle$ ist.
Die Gruppen U, V, W sind als Index-2-Untergruppen von G normal in G. Daher sind die Erweiterungen $\mathbb{Q}(\sqrt{2}) \mid \mathbb{Q}$, $\mathbb{Q}(\sqrt{3}) | \mathbb{Q}$ und $\mathbb{Q}(\sqrt{6}) | \mathbb{Q}$ galoissch. ⁕

Der Beweis des Hauptsatzes

Teil (b) des Hauptsatzes haben wir bereits in 25.24 gezeigt. Wir beweisen im Folgenden mehrere Resultate, deren Zusammenspiel Teil (a) des Hauptsatzes zeigt.

Die Aussage des folgenden Lemmas ist, dass sich jeder Zwischenkörper einer Galoiserweiterung als Fixkörper einer Untergruppe der Galoisgruppe darstellen lässt.

Lemma 26.13 *Seien $L|K$ eine Galoiserweiterung und Z ein beliebiger Zwischenkörper von $L|K$. Dann gilt $Z = \operatorname{Fix}(\operatorname{Gal}(L|Z))$.*

Beweis.

„$\subseteq$“ Die Elemente aus $\operatorname{Gal}(L|Z)$ sind Z-Automorphismen, fixieren also jedes $z \in Z$. Es gilt daher $z \in \operatorname{Fix}(\operatorname{Gal}(L|Z))$ für jedes $z \in Z$ und somit $Z \subseteq \operatorname{Fix}(\operatorname{Gal}(L|Z))$.

„$\supseteq$“ Sei $a \in \operatorname{Fix}(\operatorname{Gal}(L|Z))$ beliebig gewählt. Sei $f \in Z[X]$ das Minimalpolynom von a über Z. Die Erweiterung $L|Z$ ist nach 26.5 galoissch und daher insbesondere normal. Aus 25.7 folgt, dass alle Nullstellen von f in L enthalten sind. Sei $b \in L$ eine solche.

Nach Kronecker existiert der Z-Isomorphismus $Z(a) \to Z(b)$ mit $a \mapsto b$, der sich nach 23.4 zu einem Automorphismus $\varphi \in \operatorname{Gal}(L|Z)$ fortsetzt. Nun folgt ⁉

$$b = \varphi(a) \overset{\substack{a \in \operatorname{Fix}(\operatorname{Gal}(L|Z)), \\ \text{d.h. } \varphi \in \operatorname{Gal}(L|Z) \text{ fixiert } a}}{=} a.$$

Da b eine beliebige Nullstelle von f war, folgt, dass f nur die Nullstelle a besitzt. Weil $L|Z$ als Galoiserweiterung insbesondere separabel ist, folgt $f = X - a \in Z[X]$, also $a \in Z$. ■

Bemerkung 26.14 In Teil (a) des Hauptsatzes treten die Abbildungen

$$f : \mathcal{Z} \to \mathcal{U}, \quad Z \mapsto \operatorname{Gal}(L|Z) \qquad \text{sowie} \qquad g : \mathcal{U} \to \mathcal{Z}, \quad U \mapsto \operatorname{Fix}(U)$$

auf. Die Aussage des obigen Lemmas ist nun, dass $g \circ f = \mathrm{id}_Z$ gilt. Diese Beziehung zeigt, dass g surjektiv und f injektiv ist. (Dies stimmt ganz allgemein für Abbildungen: Aus $g \circ f = \mathrm{id}$ folgt die Surjektivität von g und die Injektivität von f, vgl. Vorkurs.) ⁂

Um Teil (a) des Hauptsatzes zu beweisen, ist, mit den Bezeichnungen aus der Bemerkung, noch $f \circ g = \mathrm{id}_U$ zu zeigen. Dies geschieht mit Hilfe der folgenden drei Resultate:

Lemma 26.15 *Sei $L|K$ eine separable Körpererweiterung. Existiert $n \in \mathbb{N}$, so dass das Minimalpolynom eines jeden Elements aus L über K höchstens Grad n hat, so ist $[L : K] \leq n$.*

Beweis. Sei $a \in L$ ein Element, dessen Minimalpolynom $m \in K[X]$ maximalen Grad besitzt. Wir setzen $g := \deg m$. Für jedes $b \in L$ ist $K(a,b)|K$ endlich und separabel. Es existiert nach dem Satz vom primitiven Element also $c \in L$ mit $K(a,b) = K(c)$. Wir erhalten

$$g = [K(a) : K] \leq [K(a,b) : K] = [K(c) : K] \overset{g \text{ maximal}}{\leq} g.$$

Dies zeigt $K(a,b) = K(a)$ und somit $b \in K(a)$.
Da dies für alle $b \in L$ stimmt, erhalten wir $L \subseteq K(a)$, also $L = K(a)$. Es ergibt sich also $[L : K] = [K(a) : K] = g \leq n$. ■

Satz 26.16 (E. Artin) *Seien L ein Körper und U eine endliche Gruppe von Automorphismen von L. Sei $K := \mathrm{Fix}(U)$ der Fixkörper von U. Dann ist $L|K$ galoissch und es gilt $\mathrm{Gal}(L|K) = U$.*

Beweis. Sei $a \in L$. Sei $S_a \subseteq U$ eine (bzgl. Elementanzahl; U ist endlich) maximale Teilmenge von U, so dass die Elemente der Menge $A := \{\varphi(a) \mid \varphi \in S_a\}$ paarweise verschieden sind. Wir können ohne Einschränkung $\mathrm{id}_L \in S_a$ annehmen; ansonsten betrachten wir statt S_a die Menge $\varphi^{-1} \circ S_a$ mit einem beliebigen $\varphi \in S_a$.
Zu jedem Automorphismus $\alpha \in U$ existiert ein $\varphi \in S_a$ mit $\alpha(a) = \varphi(a)$, denn ansonsten wäre mit $S_a \cup \{\alpha\}$ eine größere Menge gefunden, was der Maximalität von S_a widerspricht. Es ist also $\alpha(a) \in A$ für alle Automorphismen $\alpha \in U$.
Hieraus folgt, dass $\alpha|_A$ die Elemente der Menge A permutiert, also als bijektive Abbildung $A \to A$ aufgefasst werden kann:

$\alpha|_A$ ist vom Typ $A \to A$ Sei $x \in A$ beliebig. Wir müssen zeigen, dass $\alpha(x) \in A$ gilt. Hierzu führen wir einen Widerspruchsbeweis und nehmen an, dass $\alpha(x) \notin A$ sei.

Nach Definition von A existiert ein $\varphi \in S_a$ mit $x = \varphi(a)$. Es ist also $(\alpha \circ \varphi)(a) \notin A$. Da U als *Gruppe* von Automorphismen vorausgesetzt wurde, gilt $\alpha \circ \varphi \in U$. Dies widerspricht aber der bereits gezeigten Aussage, dass a von jedem Automorphismus aus U, also insbesondere auch von $\alpha \circ \varphi$, in die Menge A abgebildet wird.

$\alpha|_A : A \to A$ ist bijektiv Die Abbildung $\alpha : L \to L$ ist als Automorphismus injektiv. Daher ist auch die Einschränkung $\alpha|_A : A \to A$ injektiv. Da U eine endliche Gruppe ist, ist auch A endlich. Da injektive Selbstabbildungen endlicher Mengen stets bijektiv sind, folgt die Bijektivität von $\alpha|_A$.

Wir betrachten nun das Polynom

$$f_a := \prod_{\varphi \in S_a} (X - \varphi(a)) \in L[X].$$

Aufgrund der Definition von S_a besitzt f_a für kein $a \in L$ Mehrfachnullstellen. Wegen $\mathrm{id}_L \in S_a$ folgt $f_a(a) = 0$. Da jedes $\alpha \in U$ die Nullstellen von f_a permutiert, folgt $\alpha(f_a) = f_a$ für alle $\alpha \in U$. Daher gilt $f_a \in K[X]$.
Dies zeigt: Jedes Element $a \in L$ wird durch das mehrfachnullstellenfreie Polynom $f_a \in K[X]$ annulliert. Die Erweiterung $L|K$ ist daher separabel. Für alle $a \in L$ gilt zudem $\deg f_a = |S_a| \leq |U|$. Nach 26.15 folgt $[L : K] \leq |U|$. Der Satz vom primitiven Element sagt nun, dass $L|K$ einfach ist.
Sei $p \in L$ ein primitives Element für $L|K$. Dann zerfällt f_p über L in Linearfaktoren. $L|K$ ist also auch normal, also insgesamt galoissch. Mit 25.24 ist $|\mathrm{Gal}(L|K)| = [L : K] \leq |U|$. Umgekehrt ist jedes $\alpha \in U$ ein K-Automorphismus von L, was $U \leq \mathrm{Gal}(L|K)$ zeigt. Es folgt $U = \mathrm{Gal}(L|K)$. ■

Aus dem Satz von Artin folgt direkt die zu 26.13 analoge Aussage für Untergruppen: Jede Untergruppe der Galoisgruppe ist Galoisgruppe einer oberen Teilerweiterung der Galoiserweiterung.

Korollar 26.17 *Seien $L|K$ eine Galoiserweiterung und U eine beliebige Untergruppe von $\mathrm{Gal}(L|K)$. Dann gilt $U = \mathrm{Gal}(L \mid \mathrm{Fix}(U))$.*

Bemerkung 26.18 Mit den Bezeichnungen aus 26.14 sagt dieses Korollar, dass $f \circ g = \mathrm{id}_{\mathcal{U}}$ ist. Insgesamt folgt, dass f und g beide bijektiv und invers zueinander sind. Dies ist genau die Aussage von Teil (a) des Hauptsatzes. ※

Wir zeigen jetzt noch Teil (c) des Hauptsatzes:

Satz 26.19 *Sei $L|K$ eine Galoiserweiterung mit Zwischenkörper Z. Dann gilt: Die untere Teilerweiterung $Z|K$ ist galoissch genau dann, wenn $\mathrm{Gal}(L|Z) \trianglelefteq \mathrm{Gal}(L|K)$ gilt.*
In diesem Fall liefert die Einschränkung auf Z einen Epimorphismus

$$\mathrm{Gal}(L|K) \to \mathrm{Gal}(Z|K), \qquad \varphi \mapsto \varphi|_Z$$

mit Kern $\mathrm{Gal}(L|Z)$. Mit Homomorphiesatz folgt

$$\mathrm{Gal}(Z|K) \cong \mathrm{Gal}(L|K) / \mathrm{Gal}(L|Z).$$

Beweis. Wir setzen zur besseren Lesbarkeit $G := \mathrm{Gal}(L|K)$ und $N := \mathrm{Gal}(L|Z)$.

(„$\Longleftarrow$“) Sei N normal in G. Für jedes $\varphi \in G$ gilt

$$\begin{aligned}
\mathrm{Gal}(L|\varphi(Z)) &= \text{Menge aller } \varphi(Z)\text{-Automorphismen von } L \\
&= \{\alpha \in G \mid \alpha(y) = y \text{ für alle } y \in \varphi(Z)\} \\
&= \{\alpha \in G \mid \alpha(\varphi(x)) = \varphi(x) \text{ für alle } x \in Z\} \\
&= \{\alpha \in G \mid (\varphi^{-1} \circ \alpha \circ \varphi)(x) = x \text{ für alle } x \in Z\} \\
&= \{\alpha \in G \mid \varphi^{-1} \circ \alpha \circ \varphi \in \mathrm{Gal}(L|Z) = N\} \\
&= \varphi \cdot N \cdot \varphi^{-1} \\
&\overset{N \trianglelefteq G}{=} N.
\end{aligned}$$

Die Erweiterungen $L|\varphi(Z)$ haben also alle dieselbe Galoisgruppe wie die Erweiterung $L|Z$. Wegen der bereits gezeigten Bijektion zwischen Zwischenkörpern von $L|K$ und Untergruppen der Galoisgruppe folgt $Z = \varphi(Z)$ für alle $\varphi \in G$.

Die Einschränkung $\varphi|_Z$ von $\varphi \in G$ auf Z ist also ein Automorphismus von Z. Die Menge $\{\varphi|_Z : \varphi \in G\}$ ist daher eine endliche Gruppe von Automorphismen von Z; ihr Fixkörper ist

$$Z \cap \mathrm{Fix}(G) = Z \cap K = K.$$

Der Satz von Artin 26.16 zeigt, dass $Z|K$ galoissch ist.

(„$\Longrightarrow$“) Sei nun $Z|K$ galoissch.

Der Satz vom primitiven Element liefert dann $s \in Z$ mit $Z = K(s)$. Sei $f \in K[X]$ das Minimalpolynom von s über K. Wegen der Normalität von $Z|K$ zerfällt f in $Z[X]$ in Linearfaktoren.

Sei $\varphi \in G$ beliebig. Nach 25.4 ist $\varphi(s)$ wieder eine Nullstelle von f, liegt also ebenfalls in Z. Es folgt $\varphi(Z) \subseteq Z$ für alle $\varphi \in G$.

Für jedes $\varphi \in G$ gilt ferner

$$[Z : K] = [K(\varphi(s)) : K] = \deg f;$$

die K-Vektorräume Z und $K(\varphi(s))$ haben daher dieselbe Dimension und stimmen wegen $\varphi(Z) \subseteq Z$ sogar überein. Somit ist durch die Vorschrift

$$\pi : \ G \to \mathrm{Gal}(Z|K), \qquad \varphi \mapsto \varphi|_Z$$

ein Homomorphismus definiert. (Kritisch ist hier, dass φ_Z tatsächlich wieder nach Z abbildet.)

Nach 23.4 lässt sich jeder Homomorphismus aus $\mathrm{Gal}(Z|K)$ zu einem aus $\mathrm{Gal}(L|K)$ fortsetzen. Dies zeigt die Surjektivität von π. Der Kern von π ist offenbar $\mathrm{Gal}(L|Z)$, also N. Die restlichen Behauptungen folgen nun aus dem Homomorphiesatz. ■

27. Operation der Galoisgruppe auf Nullstellen

Worum geht es? Wir leiten eine knappere und für das praktische Rechnen angenehmere Darstellung der Galoisautomorphismen her. Als Ergebnis erhalten wir eine Operation der Galoisgruppe, die wir anschließend untersuchen und in vielen Beispielen illustrieren. ⁕

„Schöne“ Darstellung für Galoisautomorphismen

Sei $L|K$ eine Galoiserweiterung mit Galoisgruppe G. Die Elemente von G sind K-Automorphismen von L und daher vom Typ $L \to L$. Falls L ein unendlicher Körper ist, müssen wir uns überlegen, wie wir die Elemente aus G beschreiben und angeben können; Wertetabellen scheiden aus.
Hierzu wählen wir endlich viele Elemente $a_1, \dots, a_n \in L$, so dass $L = K(a_1, \dots, a_n)$ gilt. Dies ist immer möglich; der Satz vom primitiven Element garantiert sogar, dass wir stets $n = 1$ wählen können. Alternativ folgt die Aussage, weil L wegen $[L : K] < \infty$ ein endlichdimensionaler K-Vektorraum ist und sich somit durch endlich viele Elemente über K erzeugen lässt.
Die a_i sind algebraisch über K; daher gilt sogar $L = K[a_1, \dots, a_n]$. 15.2 zeigt, dass L aus Summen von Produkten von Elementen der Menge $K \cup \{a_1, \dots, a_n\}$ besteht.
Wir zeigen nun: Sind für einen Galoisautomorphismus $\varphi \in G$ die Bilder $\varphi(a_i)$ bekannt, so lässt sich $\varphi(a)$ für alle $a \in L$ berechnen. Die Kenntnis der Bilder der *endlich vielen* Elemente a_i reicht also aus, um φ auf der (potentiell unendlich großen) Menge L komplett festzulegen.

Satz 27.1 *Seien $L|K$ eine Galoiserweiterung und $a_1, \dots, a_n \in L$ mit $L = K[a_1, \dots, a_n]$. Die Bilder $\varphi(a_i)$ des Galoisautomorphismus $\varphi \in \mathrm{Gal}(L|K)$ seien bekannt. Dann lässt sich $\varphi(a)$ für jedes $a \in L$ berechnen.*
Die Kenntnis der Bilder aller a_i legt φ also vollständig fest.

Beweis. Sei $a \in L$ beliebig. Aufgrund der Vorbemerkung ist a Summe von Produkten der Menge $K \cup \{a_1, \dots, a_n\}$, d. h. es gilt $a = \sum_{i=1}^{n} \left(k_i \prod_{j=1}^{s_i} x_{i,j} \right)$ mit $n, s_1, \dots, s_n \in \mathbb{N}_0, k_i \in K$ und $x_{i,j} \in \{a_1, \dots, a_n\}$. Es folgt

$$\varphi(a) \overset{\varphi \text{ ist Autom.}}{=} \sum_{i=1}^{n} \left(\varphi(k_i) \prod_{j=1}^{s_i} \varphi(x_{i,j}) \right) \overset{\varphi \text{ ist } K\text{-Autom.}}{=} \sum_{i=1}^{n} \left(k_i \prod_{j=1}^{s_i} \varphi(x_{i,j}) \right).$$

Da die Bilder $\varphi(x_{i,j})$ nach Voraussetzung bekannt sind, lässt sich der Wert des rechten Terms ausrechnen. ■

Beispiel 27.2 Ein Galoisautomorphismus φ der Erweiterung $\mathbb{Q}(\sqrt{2}, \sqrt{3})|\mathbb{Q}$ ist durch die Kenntnis der Bilder von $\sqrt{2}$ und $\sqrt{3}$ bereits vollständig festgelegt.
φ ist aber auch durch die Kenntnis des Bildes von $\sqrt{2} + \sqrt{3}$ bereits eindeutig bestimmt, denn $\sqrt{2} + \sqrt{3}$ ist nach 25.23 ein primitives Element der betrachteten Erweiterung. ⁕

Wir bringen nun Galoisautomorphismen mit Nullstellen gewisser Polynome in Verbindung und erhalten so eine schönere Darstellung der Automorphismen. Hierzu geben wir eine alternative Interpretation der Voraussetzung $L = K[a_1, \dots, a_n]$ aus 27.1:

Satz 27.3 *Seien $L|K$ eine Galoiserweiterung und $a_1, \dots, a_n \in L$ mit $L = K[a_1, \dots, a_n]$. Das Minimalpolynom von a_i über K bezeichnen wir mit $m_i \in K[X]$. Dann ist L der Zerfällungskörper des Polynoms $f := m_1 \cdots m_n \in K[X]$.*

Beweis. Sei Z der Zerfällungskörper von f über K. Da jedes der a_i eine Nullstelle von f ist, gilt $L \subseteq Z$.
Sei nun $a \in Z$ eine beliebige Nullstelle von f. Dann gilt $m_i(a) = 0$ für ein i. Da a_i in L liegt und $L|K$ normal ist, zerfällt m_i in $L[X]$ in Linearfaktoren. L enthält daher alle Nullstellen von m_i, insbesondere ist $a \in L$. Dies zeigt $Z \subseteq L$ und beendet den Beweis. ■

Obiger Satz beschreibt, wie man aus einer Galoiserweiterung ein Polynom erhält.
Ist umgekehrt $f \in K[X]$ mit $\deg f \geq 1$ ein beliebiges Polynom und ist der Zerfällungskörper L von f separabel über K, so ist $L|K$ eine Galoiserweiterung.
Diese Überlegungen zeigen, dass man durch Zerfällungskörperbildung eine Übersetzung zwischen Galoiserweiterungen und Polynomen erhält. Dies motiviert die folgende Definition:

Definition 27.4 *Seien K ein Körper, $f \in K[X]$ ein Polynom und L der Zerfällungskörper von f über K. Wir nennen die Erweiterung $L|K$ die **durch f gegebene Galoiserweiterung**, falls $\deg f \geq 1$ gilt und $L|K$ separabel ist. Für die Galoisgruppe von $L|K$ schreibt man statt $\mathrm{Gal}(L|K)$ auch $\mathrm{Gal}(f|K)$.*
Speziell für $K = \mathbb{Q}$ ist die Erweiterung $L|K$ stets separabel; die durch f gegebene Galoiserweiterung existiert daher zu jedem $f \in \mathbb{Q}[X]$ mit $\deg f \geq 1$.

Bemerkung 27.5 Definiert man eine Galoiserweiterung $L|K$ mit Hilfe eines Polynoms f wie in obiger Definition, so erzeugen die Nullstellen $a_1, \dots, a_n$ von f den Körper L, d. h. es gilt $L = K(a_1, \dots, a_n)$. In dieser Situation greift wieder 27.1: Kennt man alle Bilder $\varphi(a_i)$ für einen Automorphismus $\varphi \in \mathrm{Gal}(f|K)$, so ist dieser eindeutig bestimmt. ⁜

Beispiel 27.6 (a) Für $m, n \in \mathbb{N}$ liefert das Polynom $(X^2-2)^m \cdot (X^2-3)^n \in \mathbb{Q}[X]$ die Galoiserweiterung $\mathbb{Q}(\sqrt{2}, \sqrt{3})|\mathbb{Q}$. ⁉

(b) Das Polynom $X^p - t \in \mathbb{F}_p(t)[X]$ aus 25.18 liefert keine Galoiserweiterung. ⁜

Nach 27.5 erhalten wir bei Definition einer Galoiserweiterung mit Hilfe eines Polynoms stets eine Menge, aus deren Abbildungsverhalten sich ein Galoisautomorphismus eindeutig rekonstruieren lässt. Es gilt aber sogar mehr:

Satz 27.7 *Seien K ein Körper und $f \in K[X]$ ein Polynom, durch das eine Galoiserweiterung gegeben werde. Es bezeichne N die Menge der Nullstellen von f im Zerfällungskörper von f. Für jedes $\varphi \in \mathrm{Gal}(f|K)$ ist dann die Einschränkung $\varphi|_N$ von φ auf N vom Typ $N \to N$ und bijektiv. $\varphi|_N$ ist daher ein Element der endlichen Gruppe $\mathrm{Sym}(N)$.*

Beweis. Sei $\varphi \in \mathrm{Gal}(f|K)$ beliebig. Wir zeigen zunächst, dass $\varphi(N) \subseteq N$ ist. Dies zeigt, dass $\varphi|_N$ vom Typ $N \to N$ ist.
Sei $a \in N$. Dann ist a eine Nullstelle von f. Nach 25.4 ist auch $\varphi(a)$ eine Nullstelle von f. Daher gilt auch $\varphi(a) \in N$.
Nun zeigen wir, dass $\varphi|_N$ bijektiv ist: $\varphi : L \to L$ ist als Automorphismus eine injektive Abbildung. Die Einschränkung $\varphi|_N$ ist dann ebenfalls injektiv. Da N eine endliche Menge ist (Warum?) und $\varphi|_N$ vom Typ $N \to N$ ist, ist $\varphi|_N$ auch surjektiv und daher bijektiv. ■

Bemerkung 27.8 $f \in K[X]$ möge eine Galoiserweiterung definieren. Sei N die Menge der Nullstellen von f im Zerfällungskörper von f.

(a) Aus 27.1 und 27.7 folgt, dass beim Übergang von $\varphi \in \mathrm{Gal}(f|K)$ zu $\varphi|_N \in \mathrm{Sym}(N)$ keine Informationen verloren gehen: φ legt die Permutation $\varphi|_N$ eindeutig fest, aus der Permutation $\varphi|_N$ lässt sich der Galoisautomorphismus φ eindeutig rekonstruieren.

In etwas algebraischerer Formulierung sagen 27.1 und 27.7 aus, dass die Abbildung

$$\mathrm{Gal}(f|K) \to \mathrm{Sym}(N), \qquad \varphi \mapsto \varphi|_N$$

ein Gruppenmonomorphismus ist.

(b) Sei $n := |N|$. Dann ist $\mathrm{Sym}(N) \cong S_n$, vgl. Seite 54 oben. Oft identifiziert man die Nullstellen $a_1, \dots, a_n$ von f mit den Symbolen $1, \dots, n$ und fasst dann einen Galoisautomorphismus als Element von S_n auf, vgl. das nächste Beispiel. ※

Beispiel 27.9 Wir betrachten wieder die Galoiserweiterung $\mathbb{Q}(\sqrt{2}, \sqrt{3})|\mathbb{Q}$, die vom Polynom $f := (X^2-2)(X^2-3) \in \mathbb{Q}[X]$ gegeben wird. Die Nullstellen von f sind $\pm\sqrt{2}$ und $\pm\sqrt{3}$. Wir nehmen die folgenden Identifizierungen vor:

$$\sqrt{2} \leftrightarrow 1\,, \qquad -\sqrt{2} \leftrightarrow 2\,, \qquad \sqrt{3} \leftrightarrow 3\,, \qquad -\sqrt{3} \leftrightarrow 4.$$

Dann gilt für die Automorphismen φ_i aus 26.12

$$\varphi_1 = \mathrm{id}\,, \qquad \varphi_2 = (3\,4)\,, \qquad \varphi_3 = (1\,2)\,, \qquad \varphi_4 = (1\,2)(3\,4);$$

mit dem Gleichheitszeichen deuten wir an, dass wir die Gruppe $\mathrm{Gal}(f|K)$ mit der entsprechenden Untergruppe von S_4 identifiziert haben. Mit dieser Identifikation folgt dann $\mathrm{Gal}(f|K) = \langle (1\,2),\, (3\,4) \rangle \leq S_4$. ※

Die Nullstellenoperation der Galoisgruppe

In 27.8 (b) haben wir einen Gruppenmonomorphismus $\mathrm{Gal}(f|K) \to \mathrm{Sym}(N)$ gefunden. Dies können wir mit 10.8 anders formulieren:

Satz 27.10 *Seien K ein Körper und $f \in K[X]$ ein Polynom, durch das eine Galoiserweiterung gegeben werde. Dann operiert* $\mathrm{Gal}(f|K)$ *auf den Nullstellen von f. Diese Operation ist treu.*

Beweis. Wegen 10.8 ist nur noch die Treue zu zeigen. Diese folgt direkt aus 10.13 (b), denn Monomorphismen sind injektiv. ■

Vereinbarung zur Schreibweise 27.11 Wenn wir zukünftig von einer Operation der Galoisgruppe $\mathrm{Gal}(f|K)$ sprechen, ohne die Operation genauer zu spezifizieren, so ist immer die obige Operation von $\mathrm{Gal}(f|K)$ auf den Nullstellen von f gemeint. ⁜

Wir untersuchen die Bahnen von $\mathrm{Gal}(f|K)$:

Satz 27.12 *Seien K ein Körper und $f \in K[X]$ ein Polynom, durch das eine Galoiserweiterung gegeben werde. Sei $f = f_1 \cdots f_r$ die Zerlegung von f in irreduzible Faktoren $f_i \in K[X]$. Wir bezeichnen die Menge der Nullstellen von f_i mit N_i. Dann gilt: Die Bahnen der Operation von* $\mathrm{Gal}(f|K)$ *sind genau die Mengen N_i.*

Beweis. Seien $G := \mathrm{Gal}(f|K)$ und L der Zerfällungskörper von f über K. Wir führen den Beweis in zwei Schritten.

$\varphi(N_i) \subseteq N_i$ Wir zeigen zuerst, dass das Anwenden eines beliebigen Galoisautomorphismus auf Elemente aus N_i nicht aus N_i herausführt:

Seien $\varphi \in G$ beliebig und a irgendein Element irgendeiner der Mengen N_i. Dann wird a von f_i annulliert. Nach 25.4 wird auch $\varphi(a)$ von f_i annulliert. Dies zeigt $\varphi(a) \in N_i$.

G* ist transitiv auf jedem der *N_i Seien a und b beliebige Elemente aus irgendeiner der Mengen N_i. Wir konstruieren mit Hilfe von 23.4 einen Automorphismus $\varphi \in G$ mit $\varphi(a) = b$. Dies zeigt den Satz.

a und b werden von demselben irreduziblen Polynom $f_i \in K[X]$ annulliert. Daher besitzen a und b dasselbe Minimalpolynom $m \in K[X]$; es gilt $m = c^{-1} \cdot f_i$, wobei c den Leitkoeffizienten von f_i bezeichnet. Nach 22.11 existiert daher ein K-Automorphismus $K(a) \to K(b)$ mit $a \mapsto b$. Dieser K-Automorphismus lässt sich nach 23.4 auf den Zerfällungskörper von f über $K(a)$ fortsetzen. Dieser Zerfällungskörper stimmt aber gerade mit L überein. Wir haben somit einen K-Automorphismus von L, also ein Element von G konstruiert, was $\varphi(a) = b$ erfüllt. ■ ⁉

Beispiel 27.13 Wir führen 27.9 fort. Dort haben wir die Galoiserweiterung untersucht, die vom Polynom $f := (X^2 - 2)(X^2 - 3) \in \mathbb{Q}[X]$ gegeben wird. f ist Produkt der beiden irreduziblen Polynome $f_1 := X^2 - 2$ und $f_2 := X^2 - 3$. Obiger Satz sagt, dass die Galoisgruppe zwei Bahnen besitzt, nämlich die Nullstellenmengen von f_i für $i = 1$ und $i = 2$.
Mit der Identifikation der Nullstellen aus 27.9 gilt $\mathrm{Gal}(f|K) = \{\mathrm{id}, (1\,2), (3\,4), (1\,2)(3\,4)\}$. Diese Gruppe hat die Bahnen $\{1,2\}$ und $\{3,4\}$. Rückübersetzen auf Nullstellen von f liefert die Bahnen $\{\sqrt{2}, -\sqrt{2}\}$ und $\{\sqrt{3}, -\sqrt{3}\}$. Dies ist genau das nach 27.12 zu erwartende Ergebnis. ⁜

Genau dann operiert $\mathrm{Gal}(f|K)$ transitiv, wenn die Operation nur eine Bahn besitzt. 27.12 sagt, dass dann alle Nullstellen von f zum selben irreduziblen Faktor von f gehören müssen. Wir erhalten:

Korollar 27.14 *Seien K ein Körper und $f \in K[X]$ ein Polynom, durch das eine Galoiserweiterung gegeben werde. Dann gilt: Genau dann operiert $\mathrm{Gal}(f|K)$ transitiv, wenn sich f schreiben lässt in der Form $f = g^r$ mit einem irreduziblen Polynom $g \in K[X]$ und $r \in \mathbb{N}$.*
Dies ist insbesondere dann erfüllt, wenn $f = g$ selbst irreduzibel ist.

Beispiel 27.15 Wir betrachten die Galoiserweiterung $L|\mathbb{Q}$ mit $L := \mathbb{Q}(\sqrt{2}, \sqrt{3})$. (Dies wird das letzte Mal sein – versprochen!) Das Element $a := \sqrt{2} + \sqrt{3}$ ist primitiv für $L|\mathbb{Q}$. Nachrechnen zeigt, dass das Polynom $m := X^4 - 10X^2 + 1 \in \mathbb{Q}[X]$ ein annullierendes Polynom für a ist. Da $L = \mathbb{Q}(a)$ und $[L : \mathbb{Q}] = 4$ gelten, folgt $[\mathbb{Q}(a) : \mathbb{Q}] = 4$. Dies zeigt, dass m das *Minimalpolynom von a* ist. m ist also insbesondere irreduzibel. ⁉
Wir bestimmen nun die Bahnen von $G := \mathrm{Gal}(m|K)$ und zeigen, dass G transitiv ist. Dieses Ergebnis ist aufgrund von 27.14 zu erwarten.
Nachrechnen zeigt, dass die Nullstellen von m durch $\pm\sqrt{2} \pm \sqrt{3}$ und $\pm\sqrt{2} \mp \sqrt{3}$ gegeben sind. Wir identifizieren sie mit den Symbolen $1, 2, 3, 4$ wie folgt:

$$\sqrt{2} + \sqrt{3} \leftrightarrow 1\,, \qquad -\sqrt{2} + \sqrt{3} \leftrightarrow 2\,, \qquad \sqrt{2} - \sqrt{3} \leftrightarrow 3\,, \qquad -\sqrt{2} - \sqrt{3} \leftrightarrow 4.$$

Für den Galoisautomorphismus φ_1 aus 26.12 gilt nun $\varphi_1 = \mathrm{id} \in S_4$.
Der Automorphismus φ_2 fixiert $\sqrt{2}$ und daher auch $-\sqrt{2}$; er ändert das Vorzeichen vor $\sqrt{3}$ und daher auch vor $-\sqrt{3}$. Es gilt daher $\varphi_2 = (1\,3)(2\,4)$.
Analog sieht man $\varphi_3 = (1\,2)(3\,4)$ und $\varphi_4 = (1\,4)(2\,3)$.
Es gilt daher $\mathrm{Gal}(m|\mathbb{Q}) = \{\mathrm{id}, (1\,2)(3\,4), (1\,3)(2\,4), (1\,4)(2\,3)\}$. Diese Gruppe entspricht der Kleinschen Vierergruppe aus 9.11, ist isomorph zu $C_2 \times C_2$ und transitiv. ⁉ ⁂

Bemerkung 27.16 Eine Galoiserweiterung $L|K$ lässt sich stets durch viele verschiedene Polynome $f \in K[X]$ beschreiben. Je nach betrachtetem f ändert sich das Operationsverhalten von $\mathrm{Gal}(f|K)$. Der Isomorphietyp von $\mathrm{Gal}(f|K)$ ist jedoch stets derselbe: Es gilt stets $\mathrm{Gal}(f|K) \cong \mathrm{Gal}(L|K)$. ⁂

Weitere Beispiele

Staatsexamensaufgabe (ähnlich zu F2018T1A4) *Gegeben sei das Polynom $f := X^5 - 4X + 2 \in \mathbb{Q}[X]$. Zeigen Sie, dass durch f eine Galoiserweiterung gegeben ist und dass $G := \mathrm{Gal}(f|\mathbb{Q})$ ein Element der Ordnung 5 enthält.*

Da wir über $\mathbb{Q}$ arbeiten, wird durch f eine Galoiserweiterung gegeben, vgl. 27.4. Seien L der Zerfällungskörper von f über $\mathbb{Q}$ und $a \in L$ eine Nullstelle von f.
f ist irreduzibel nach Eisenstein (mit $p = 2$). Es gilt daher $[\mathbb{Q}(a) : \mathbb{Q}] = \deg f = 5$. Da $\mathbb{Q}(a)$ ein Zwischenkörper der Erweiterung $L|\mathbb{Q}$ ist, gilt nach Gradformel $5 \mid [L : \mathbb{Q}]$. Die Primzahl 5 teilt dann auch die Ordnung von G, denn nach 26.3 (b) ist $[L : \mathbb{Q}] = |G|$. Nach Sylow 12.4 oder Cauchy 12.6 folgt, dass G eine zu C_5 isomorphe Untergruppe besitzt. Daher besitzt G auch ein Element der Ordnung 5. ⁂

Staatsexamensaufgabe (H2017T2A5) *Das irreduzible Polynom $f \in \mathbb{Q}[X]$ besitze eine Nullstelle $\alpha \in \mathbb{R}$ und eine Nullstelle $\beta \in \mathbb{C} \setminus \mathbb{R}$. Sei $L \subseteq \mathbb{C}$ der Zerfällungskörper von f. Zeigen Sie, dass die Galoisgruppe $G := \mathrm{Gal}(L|\mathbb{Q})$ nicht abelsch ist.*

Wir beweisen per Widerspruch und nehmen an, dass G abelsch sei. Dann ist jede untere Teilerweiterung von $L|K$ normal, vgl. 26.10; insbesondere ist die Erweiterung $\mathbb{Q}(\alpha)|\mathbb{Q}$ normal. Da das irreduzible Polynom f in $\mathbb{Q}(\alpha)$ die Nullstelle α besitzt, zerfällt f in $\mathbb{Q}(\alpha)$ bereits vollständig. Es gilt also $\mathbb{Q}(\alpha) = L$.
Dies ist widersprüchlich, denn die Nullstelle β ist echt komplex und liegt somit nicht im Körper $\mathbb{Q}(\alpha) \subseteq \mathbb{R}$. Es ist daher $\mathbb{Q}(\alpha) \neq L$. ⁂

Staatsexamensaufgabe (ähnlich zu F2017T2A4) *Die Galoiserweiterung $L|K$ habe Grad 55 und nicht-abelsche Galoisgruppe. Zeigen Sie: Es gibt genau einen echten Zwischenkörper Z von $L|K$, so dass $Z|K$ eine Galoiserweiterung ist. Berechnen Sie $[Z : K]$.*

L	$\{1\} = \mathrm{Gal}(L\|L)$	Wir setzen $G := \mathrm{Gal}(L\|K)$ und $U := \mathrm{Gal}(L\|Z)$. Dann ist $U \leq G$. Für die Indizes bzw. Erweiterungsgrade r und s im linken Bild gilt $rs = 55$.
$s \Big\vert$	$\Big\vert s$	
Z	$U := \mathrm{Gal}(L\|Z)$	Nach Hauptsatz der Galoistheorie ist die untere Teilerweiterung $Z\|K$ genau dann normal, wenn $U \trianglelefteq G$ ist.
$r \Big\vert$	$\Big\vert r$	Z ist genau dann ein echter Zwischenkörper von $L\|K$, wenn $s \neq 1$ und $r \neq 1$ gelten, also wenn $\{1\} < U < G$ gilt.
K	$G := \mathrm{Gal}(L\|K)$	

Die Aufgabe ist daher gelöst, wenn wir zeigen können, dass eine nicht-abelsche Gruppe G der Ordnung 55 nur genau einen echten, nicht-trivialen Normalteiler U besitzt. Nach Lagrange sind für U nur die Ordnungen 5 und 11 möglich. Damit hat sich die Fragestellung auf eine Standard-Sylowaufgabe reduziert.
Können Sie die Aufgabe lösen? ⁂ ⁉

Beispiel 27.17 Sei $f := X^3 - 5 \in \mathbb{Q}[X]$. Dann ist durch f eine Galoiserweiterung gegeben. Wir sind am Isomorphietyp der Gruppe $G := \mathrm{Gal}(f|\mathbb{Q})$ interessiert.
Wegen $\deg f = 3$ ist G isomorph zu einer Untergruppe von S_3, vgl. 27.8. Da $|S_3| = 6$ ist, folgt $|G| \in \{1, 2, 3, 6\}$.
f ist nach Eisenstein irreduzibel. Mit 27.14 operiert G daher transitiv auf $\deg f = 3$ Elementen. Aus der Bahnlängenformel 11.15 folgt, dass G eine Untergruppe vom Index 3 besitzt. Dies zeigt, dass die Ordnung von G durch Drei teilbar ist. Es folgt $|G| \in \{3, 6\}$ ⁉
und mit $G \leq S_3$ schließlich $G \cong C_3$ oder $G \cong S_3$. Wir zeigen, dass $G \cong S_3$ gilt:
f besitzt nur eine einzige reelle Nullstelle, nämlich $a := \sqrt[3]{5} \in \mathbb{R}$. Daher ist die Erweiterung $\mathbb{Q}(a)|\mathbb{Q}$ nicht normal. Da f das Minimalpolynom von a ist, gilt $[\mathbb{Q}(a) : \mathbb{Q}] = \deg f = 3$. Da $\mathbb{Q}(a)|\mathbb{Q}$ nicht normal ist, muss die durch f gegebene Galoiserweiterung einen größeren Grad haben. Es ist daher $|G| > 3$ und somit $G \cong S_3$. ⁂ ⁉

28. Konstruktion von Galoisautomorphismen

Worum geht es? Wir haben in den vergangenen Vorlesungen bereits in einfachen Beispielen Galoisautomorphismen konstruiert. In dieser Vorlesung gehen wir hierauf genauer ein. Weiter beschäftigen wir uns mit der komplexen Konjugation und zeigen, dass sie als Galoisautomorphismus auftritt, sobald der Unterkörper einer Galoiserweiterung in $\mathbb{R}$ enthalten ist. ⁜

Sei $L|K$ eine Galoiserweiterung. Wir wissen aus der letzten Vorlesung, dass endlich viele Elemente $a_1, \dots, a_n \in L$ existieren, so dass $L = K(a_1, \dots, a_n)$ gilt. Um Galoisautomorphismen von $L|K$ zu konstruieren, gehen wir schrittweise vor: Zunächst legen wir das Bild von a_1 fest, danach das von a_2, dann das von a_3, etc. Nachdem wir schließlich auch das Bild von a_n festgelegt haben, ist der Galoisautomorphismus nach 27.1 vollständig bestimmt.
27.12 schränkt unsere Bilder-Auswahl ein: Bezeichnen wir mit $m_i \in K[X]$ das Minimalpolynom von a_i über K und setzen dann $f := \prod_{i=1}^{n} m_i$, so wird die Galoiserweiterung $L|K$ durch f gegeben. Definieren wir $N_i \subseteq L$ als Menge der Nullstellen von m_i in L, so folgt, dass die Bilder der a_i aus den jeweiligen N_i stammen müssen. Konkret heißt dies:

Erster Schritt: Das Bild von a_1 wählen wir aus den Elementen von N_1. Da die Operation der Galoisgruppe von $L|K$ *transitiv* auf jedem der N_i ist und bisher kein Bild eines anderen a_i gewählt wurde, können wir sogar ein *beliebiges* Element aus N_1 als Bild von a_1 wählen. ⁉

Nachfolgende Schritte: Hier sind für einige der a_i die Bilder bereits gewählt. Dies hat meist zur Folge, dass wir die Bilder für die a_i in den weiteren Schritten nicht mehr frei aus N_i wählen können: Durch die vorhergehenden Festsetzungen entstehen Nebenbedingungen, die in den weiteren Wahlen beachtet werden müssen.

Man sagt auch, dass die Wahl der Bilder der a_i in den weiteren Schritten **verträglich** geschehen muss oder dass **Verträglichkeitsbedingungen** einzuhalten sind.

Beispiel 28.1 $L := \mathbb{Q}(\sqrt{2}, \sqrt{8})$ ist Zerfällungskörper von $f := (X^2 - 2)(X^2 - 8) \in \mathbb{Q}[X]$ über $\mathbb{Q}$; die Erweiterung $L|\mathbb{Q}$ ist galoissch.
Galoisautomorphismen von $L|\mathbb{Q}$ können $\sqrt{2}$ nur auf $\pm\sqrt{2}$ und $\sqrt{8}$ nur auf $\pm\sqrt{8}$ abbilden, denn dies sind die Nullstellen der jeweiligen Minimalpolynome $X^2 - 2 \in \mathbb{Q}[X]$ bzw. $X^2 - 8 \in \mathbb{Q}[X]$. Wir konstruieren nun einen Galoisautomorphismus $\varphi \in \mathrm{Gal}(L|\mathbb{Q})$ und setzen $\varphi(\sqrt{2}) := -\sqrt{2}$. Dies ist möglich, denn es sind noch keine Verträglichkeitsbedingungen einzuhalten.
Nun folgt

$$\begin{aligned} \varphi(\sqrt{8}) &= \varphi(2 \cdot \sqrt{2}) \overset{\text{Kö.autom.}}{=} \varphi(2) \cdot \varphi(\sqrt{2}) \\ &\overset{\mathbb{Q}\text{-Autom.}}{=} 2 \cdot \varphi(\sqrt{2}) \overset{\sqrt{2} \mapsto -\sqrt{2}}{=} -2\sqrt{2} = -\sqrt{8}. \end{aligned}$$

Das Bild von $\sqrt{8}$ ist also durch die Wahl im ersten Schritt bereits bestimmt, d. h. wir haben im zweiten Schritt überhaupt keine Wahlfreiheit mehr. Die Verträglichkeitsbedingungen erzwingen $\varphi(\sqrt{8}) := -\sqrt{8}$. ⁜

Verträglichkeitsbedingungen kommen zustande, wenn gewisse „Beziehungen“ zwischen den a_i bestehen, d. h. wenn verschiedene a_i durch Gleichungen miteinander gekoppelt sind. In 28.1 gilt beispielsweise $\sqrt{8} = 2 \cdot \sqrt{2}$. Im nächsten Beispiel sind diese „Beziehungen“ nicht ganz so offensichtlich:

Beispiel 28.2 Sei $f := X^4 + 6X^2 - 2 \in \mathbb{Q}[X]$. Dann ist f nach dem Eisensteinkriterium irreduzibel und hat die Nullstellen

$$a_1 := \sqrt{-3 + \sqrt{11}}, \quad a_2 := \sqrt{-3 - \sqrt{11}}, \quad a_3 := -a_1, \quad a_4 := -a_2.$$

Ein Zerfällungskörper von f über $\mathbb{Q}$ ist $L := \mathbb{Q}(a_1, a_2)$.
Beachten Sie, dass $a_1 \in \mathbb{R}$ und $a_2 \notin \mathbb{R}$ ist. Dies zeigt, dass $[L : \mathbb{Q}] > [\mathbb{Q}(a_1) : \mathbb{Q}] = 4$ ist. Es müssen daher tatsächlich *beide* Elemente an $\mathbb{Q}$ adjungiert werden, um L zu erreichen.
Wir konstruieren nun einen Galoisautomorphismus φ von $L|\mathbb{Q}$ und setzen im ersten Schritt $\varphi(a_1) := a_3$; dies ist möglich, da f irreduzibel ist. Durch diese Festsetzung ist auch schon das Bild von $\sqrt{11}$ bestimmt: Es gilt $\varphi(\sqrt{11}) = \varphi(a_1^2 + 3) = a_3^2 + 3 = \sqrt{11}$. Diese Bedingung erzwingt, dass $\varphi(a_2) \in \{a_2, a_4\}$ gelten muss. ⁜

Wegfall von Verträglichkeitsbedingungen

Die folgenden Resultate stellen sicher, dass bei der Konstruktion von Galoisautomorphismen keine Verträglichkeitsbedingungen zu beachten sind. In diesem Fall können die a_i tatsächlich völlig beliebig aus den jeweiligen N_i gewählt werden. Dabei spielt die Erweiterung $L|K$ an sich keine große Rolle, es kommt auf die Darstellung von L in der Form $K(a_1, \dots, a_n)$, also auf die Elemente a_i an.
Das erste Resultat ergibt sich im Fall $n = 1$, also für Galoiserweiterungen, die als einfache Körpererweiterungen dargestellt sind:

Satz 28.3 *Seien K ein Körper und $K(a)|K$ eine Galoiserweiterung. Wir bezeichnen das Minimalpolynom von a über K mit $m \in K[X]$ und die Menge der Nullstellen von m in $K(a)$ mit N. Dann gelten die folgenden Aussagen:*

(a) *Es ist* $|N| = \deg m = [K(a) : K] = |\mathrm{Gal}(K(a)|K)|$.

(b) *Für jedes $z \in N$ wird durch homomorphe Fortsetzung von id_K und der Festsetzung $\varphi(a) := z$ ein Galoisautomorphismus $\varphi_z : K(a) \to K(a)$ der Erweiterung $K(a)|K$ gegeben.*

Diese Automorphismen sind paarweise verschieden.

(c) *Es ist* $\mathrm{Gal}(K(a)|K) = \{\varphi_z \mid z \in N\}$.

Beweisskizze.

zu (a) Die Körpererweiterung $K(a)|K$ ist galoissch und daher separabel. Somit hat m keine Mehrfachnullstellen, was $|N| = \deg m$ zeigt. Die restlichen Gleichheiten folgen aus 22.1 (c) und dem Hauptsatz der Galoistheorie.

zu (b) Um einen Galoisautomorphismus von $K(a)|K$ zu konstruieren, müssen wir ein Bild für a wählen. Weitere Schritte sind nicht nötig, daher treten auch keine Verträglichkeitsbedingungen auf. Das Bild von a kann also völlig frei aus N gewählt werden.

Für verschiedene z sind die Bilder $\varphi_z(a)$ und damit auch die Abbildungen φ_z verschieden.

(c) folgt aus Anzahlgründen wegen $|\operatorname{Gal}(K(a)|K)| = |N| = |\{\varphi_z \mid z \in N\}|$. ■

In der folgenden Staatsexamensaufgabe tritt eine einfache Galoiserweiterung auf, so dass obiges Resultat direkt benutzt werden kann:

Staatsexamensaufgabe (H2015T2A5) *Sei* $a := \sqrt{2+\sqrt{2}} \in \mathbb{R}$.

(a) *Berechnen Sie das Minimalpolynom* m *von* a *über* $\mathbb{Q}$.

(b) *Zeigen Sie, dass die Körpererweiterung* $\mathbb{Q}(a)|\mathbb{Q}$ *galoissch ist und berechnen Sie ihre Galoisgruppe.*

zu (a) Es ist $a^2 = 2 + \sqrt{2}$ und daher $(a^2-2)^2 = 2$. Ausmultiplizieren und Umsortieren liefert die Gleichheit $a^4 - 4a^2 + 2 = 0$. Also ist das Polynom $f := X^4 - 4X^2 + 2 \in \mathbb{Q}[X]$ annullierend für a. Weiter ist f normiert und nach Eisenstein irreduzibel. Wir setzen $m := f$ und haben das gesuchte Minimalpolynom gefunden.

zu (b) Die Nullstellen von m sind

$$a = a_1 := \sqrt{2+\sqrt{2}}, \quad a_2 := \sqrt{2-\sqrt{2}}, \quad a_3 := -a_1, \quad a_4 := -a_2.$$

Somit ist $L := \mathbb{Q}(a_1,a_2,a_3,a_4) = \mathbb{Q}(a_1,a_2)$ ein Zerfällungskörper von f. Wegen

$$a_1 \cdot a_2 = \sqrt{(2+\sqrt{2})\cdot(2-\sqrt{2})} = \sqrt{4-2} = \sqrt{2}$$

und aufgrund von $\sqrt{2} \in \mathbb{Q}(a_1)$ gilt sogar ?

$$L = \mathbb{Q}(a_1,a_2) \overset{\text{s.o.}}{=} \mathbb{Q}\Big(a_1, \frac{\sqrt{2}}{a_1}\Big) = \mathbb{Q}(a_1,\sqrt{2}) \overset{\sqrt{2}\in\mathbb{Q}(a_1)}{=} \mathbb{Q}(a_1) = \mathbb{Q}(a).$$

Folglich ist die Erweiterung $\mathbb{Q}(a)|\mathbb{Q}$ galoissch. Ihre Galoisgruppe $G := \operatorname{Gal}(\mathbb{Q}(a)|\mathbb{Q})$ ist nach 28.3 gegeben durch die vier Automorphismen

$$\varphi_i : \ \mathbb{Q}(a) \to \mathbb{Q}(a), \qquad a \mapsto a_i \qquad \text{mit } i \in \{1,2,3,4\}.$$

Wir bestimmen nun noch den Isomorphietyp von G. Hierzu setzen wir $\varphi := \varphi_2$ und berechnen $\varphi^2(a)$. Es gilt:

$$\begin{aligned} \varphi^2(a) &= \varphi(\varphi(a)) \overset{a\mapsto a_2}{=} \varphi(a_2) = \varphi\Big(\frac{\sqrt{2}}{a}\Big) \\ &\overset{\text{Kö.autom.}}{=} \frac{\varphi(\sqrt{2})}{\varphi(a)} \overset{(\star)}{=} \frac{-\sqrt{2}}{a_2} \\ &= -\sqrt{2+\sqrt{2}} = a_3 \neq a. \end{aligned}$$

In $(\star)$ haben wir ausgenutzt, dass $\varphi(a) = a_2$ gilt; dies liefert

$$\varphi(\sqrt{2}) = \varphi(a^2 - 2) = a_2^2 - 2 = (2 - \sqrt{2}) - 2 = -\sqrt{2}.$$

Die Rechnung zeigt $\varphi^2 \neq \mathrm{id}_L$. Die Gruppe G der Ordnung Vier enthält somit ein Element, dessen Ordnung größer als Zwei ist. Also gilt $G \cong C_4$. ⁂ ⁉

Bemerkung 28.4 Die Einschränkung auf einfache Körpererweiterungen in 28.3 sieht auf den ersten Blick sehr restriktiv aus. Allerdings lässt sich mit Hilfe des Satzes vom primitiven Element *jede* Galoiserweiterung $L|K$ in der Form $K(a)|K$ schreiben.
Für praktische Rechnung ist diese Darstellung von $L|K$ allerdings oft nicht gut geeignet. (Haben Sie eine Ahnung, warum?) ⁂ ⁉

Der folgende Satz stellt eine Verallgemeinerung von 28.3 dar. Er garantiert ebenfalls, dass bei der Konstruktion von Galoisautomorphismen keine Verträglichkeitsbedingungen auftreten.

Satz 28.5 *Seien K ein Körper und $L := K(a_1, \dots, a_n)|K$ eine Galoiserweiterung. Für $i \in \{1, \dots, n\}$ bezeichnen wir mit m_i das Minimalpolynom von a_i über K und mit N_i die Menge der Nullstellen von m_i in L. Es gelte zudem*

$$\prod_{i=1}^{n} \deg m_i = [L : K].$$

Dann existiert zu jedem Tupel $(z_1, \dots, z_n) \in N_1 \times \cdots \times N_n$ genau ein Galoisautomorphismus $\varphi \in \mathrm{Gal}(L|K)$ mit $\varphi(a_i) = z_i$ für alle i.
Anders formuliert: Unter den obigen Voraussetzungen kann das Bild von a_i beliebig aus der Nullstellenmenge N_i gewählt werden, und zwar für jedes $i \in \{1, \dots, n\}$. Es treten keine Verträglichkeitsbedingungen auf, die diese Auswahlen einschränken.

Beweis. Wir konstruieren Elemente aus $\mathrm{Gal}(L|K)$, indem wir nacheinander die Bilder von $a_1, a_2, a_3, \dots$ aus den jeweiligen Nullstellenmengen $N_1, N_2, N_3, \dots$ wählen, dabei aber gegebenenfalls auftretende Verträglichkeitsbedingungen beachten. Uns stehen daher für a_i maximal $|N_i|$ Wahlmöglichkeiten zur Verfügung. Somit können wir höchstens $\prod_{i=1}^{n} |N_i|$ Galoisautomorphismen von $L|K$ konstruieren.

Da $L|K$ separabel ist, gilt $\deg m_i = |N_i|$ für alle i. Daher gilt mit der Voraussetzung im Satz

$$|\operatorname{Gal}(L|K)| = [L:K] = \prod_{i=1}^{n} \deg m_i = \prod_{i=1}^{n} |N_i|.$$

Diese Anzahl an Galoisautomorphismen erreichen wir nur, wenn wir bei unseren obigen Auswahlen in den N_i frei und ohne Einschränkungen wählen dürfen, wenn wir also auf keinerlei Verträglichkeitsbedingungen Rücksicht nehmen müssen. ■

Bemerkung 28.6 Durch geschickte Darstellung des Oberkörpers lassen sich Galoiserweiterungen stets so umschreiben, dass 28.5 anwendbar ist. Speziell in Staatsexamensaufgaben treten solche Umschreibungen oft auf. ⁜

Beispiel 28.7 Wir führen 28.2 fort. Es gilt

$$a_1 \cdot a_2 = \sqrt{(-3+\sqrt{11})\cdot(-3-\sqrt{11})} = \sqrt{9-11} = i\sqrt{2}.$$

Damit folgt

$$L = \mathbb{Q}(a_1, a_2) = \mathbb{Q}\Big(a_1, \frac{i\sqrt{2}}{a_1}\Big) = \mathbb{Q}(a_1, i\sqrt{2}).$$

Da $a_1 \in \mathbb{R}$ ist, folgt aus dieser Darstellung von L, dass $[L:\mathbb{Q}] = 8$ ist. Das Minimalpolynom von a_1 ist f, das von $i\sqrt{2}$ ist $g := X^2 + 2 \in \mathbb{Q}[X]$ und hat die Nullstellen $\pm i\sqrt{2}$. Es gilt

$$[L:\mathbb{Q}] = 8 = 4 \cdot 2 = \deg f \cdot \deg g,$$

so dass 28.5 anwendbar ist. Damit besteht die Galoisgruppe $\operatorname{Gal}(L|\mathbb{Q})$ aus den acht Automorphismen

$$\varphi_{s,t} : L \to L, \quad \begin{cases} a_1 \mapsto a_s, \\ i\sqrt{2} \mapsto (-1)^t \cdot i\sqrt{2}, \end{cases}$$

wobei $s \in \{1,2,3,4\}$ und $t \in \{0,1\}$ beide beliebig wählbar sind. ⁜

Die komplexe Konjugation als Galoisautomorphismus

Ist der Unterkörper einer Galoiserweiterung eine Teilmenge der reellen Zahlen, so ist die komplexe Konjugation ein Galoisautomorphismus der Erweiterung:

Satz 28.8 *Seien $K \subseteq \mathbb{R}$ ein Unterkörper der reellen Zahlen und $L|K$ eine Galoiserweiterung. Dann ist die Einschränkung der komplexen Konjugation auf L ein Element von $\operatorname{Gal}(L|K)$, d. h. die Abbildung $\varphi : L \to L$ mit $\varphi(x) := \overline{x}$ ist ein Element von $\operatorname{Gal}(L|K)$.*
(Die Notation $\overline{x}$ steht hierbei für das komplex Konjugierte von x. Wegen $L \subseteq \mathbb{C}$ ist $\overline{x}$ definiert.)

Beweis. Mit dem Satz vom primitiven Element können wir $L = K(a)$ mit einem $a \in L$ schreiben. Da a algebraisch über K ist, folgt $a \in \mathbb{C}$ und daher auch $L \subseteq \mathbb{C}$. Die Abbildung φ ist daher für jedes Element aus L definiert.

Sei $m \in K[X]$ das Minimalpolynom von a. Da m nur reelle Koeffizienten besitzt, ist auch $\varphi(a) = \overline{a}$ eine Nullstelle von m und daher ein Element von L. Es folgt, dass φ auf L abbildet, denn es gilt

$$\varphi(L) = \overline{L} = \overline{K(a)} \overset{K \subseteq \mathbb{R}}{=} K(\overline{a}) \overset{[K(a):K]=\deg m=[K(\overline{a}):K]}{=} K(a) = L.$$

Dies zeigt, dass φ tatsächlich eine Abbildung vom Typ $L \to L$ ist. Die Rechenregeln für die komplexe Konjugation zeigen, dass φ ein Automorphismus von L ist, der den reellen Unterkörper K elementweise fixiert. Damit ist $\varphi \in \mathrm{Gal}(L|K)$. ■

Genau dann stimmt der Automorphismus φ aus obigem Satz mit der Identität überein, wenn $L \subseteq \mathbb{R}$ gilt. Sobald aber L kein reeller Körper ist, ist durch φ ein Galoisautomorphismus der Ordnung Zwei gegeben:

Korollar 28.9 *Seien $K \subseteq \mathbb{R}$ ein Unterkörper der reellen Zahlen und $L|K$ eine Galoiserweiterung mit $L \not\subseteq \mathbb{R}$. Dann enthält die Galoisgruppe von $L|K$ ein Element der Ordnung Zwei, hat also insbesondere gerade Ordnung.*

Staatsexamensaufgabe (Teil (c) von F2018T1A4) *Gegeben sei das Polynom $P := X^5 - 4X + 2 \in \mathbb{Q}[X]$. Weiter sei $Z \subseteq \mathbb{C}$ ein Zerfällungskörper von P über $\mathbb{Q}$. Zeigen Sie, dass die Galoisgruppe $G := \mathrm{Gal}(Z|\mathbb{Q})$ ein Element der Ordnung 5 und ein Element der Ordnung 2 hat.*

Den Ordnung-5-Fall haben wir bereits auf Seite 195 behandelt. Zum Beweis der Existenz eines Elements der Ordnung Zwei benutzen wir 28.9:
Der Unterkörper der Erweiterung $Z|\mathbb{Q}$ ist reell; wir müssen also nur noch nachweisen, dass Z echt komplex ist. Dies geschieht mit analytischen Mitteln, nämlich mit Hilfe einer Kurvendiskussion des Polynoms P. Man sieht dann, dass P genau drei reelle Nullstellen hat. P muss also zwei echt komplexe Nullstellen besitzen. ?
Nach 28.9 ist die Einschränkung der komplexen Konjugation auf Z nun ein Galoisautomorphismus von $Z|\mathbb{Q}$ von Ordnung Zwei. ⋇

29. Frobenius, Galoistheorie endlicher Körper

Worum geht es? Wir untersuchen den Frobenius-Endomorphismus von Körpern primer Charakteristik genauer und stellen einen Zusammenhang zur Separabilität von Körpererweiterungen her.
Diese Untersuchungen erlauben es uns zudem, die Galoisgruppen endlicher Erweiterungen endlicher Körper konkret anzugeben. Wir beenden die Vorlesung mit einer ersten Anmerkung zum *Umkehrproblem das Galoistheorie*.
Viele Resultate dieser Vorlesung sind bereits in früheren Vorlesungen vorgestellt und bewiesen worden. Wir leiten sie hier nochmals, aber mit anderen Mitteln her. ⁜

Der Frobenius

Ist K ein Körper der Charakteristik $p \in \mathbb{P}$, so ist die Abbildung

$$\varphi : K \to K, \qquad a \mapsto a^p$$

ein injektiver Körperendomorphismus, vgl. 24.7. Man bezeichnet φ oft recht knapp als **den Frobenius von K**.

Bemerkung 29.1 Beachten Sie, dass der Exponent in der Abbildungsvorschrift des Frobenius der Charakteristik von K entspricht. Wenn man von „dem Frobenius" des Körpers K spricht, ist die Abbildung also eindeutig festgelegt. ⁜

Falls K endlich ist, fallen für φ die Eigenschaften „injektiv" und „surjektiv" zusammen. ⁉
In diesem Fall ist φ ein Körper*auto*morphismus:

Lemma 29.2 *Sei K ein endlicher Körper. Dann ist der Frobenius von K ein Automorphismus von K.*

Bemerkung 29.3 Es gibt Körper der Charakteristik $p \in \mathbb{P}$, deren Frobenius nicht surjektiv ist. Ein Beispiel für einen solchen Körper ist $K := \mathbb{F}_p(t)$ mit einem beliebigen transzendenten Element t. Bezeichnen wir mit φ den Frobenius von K, so besitzt t kein Urbild unter φ:
Hätte t ein Urbild $a \in K$ unter φ, so wäre $\varphi(a) - t = a^p - t = 0$, d. h. das Polynom

$$f := X^p - t \in K[X]$$

hätte eine Nullstelle in K. Dies ist ein Widerspruch, denn in 25.18 haben wir die Irreduzibilität von f nachgewiesen. ⁜

Der folgende Satz verallgemeinert die polynomiale Methode aus obiger Bemerkung:

Satz 29.4 *Seien K ein Körper der Charakteristik $p \in \mathbb{P}$ und φ sein Frobenius. Dann sind die folgenden Aussagen äquivalent:*

(a) *φ ist surjektiv.*

(b) *Jedes Polynom $f \in K[X]$ mit $f' = 0$ ist eine p-te Potenz, d.h. es gibt ein Polynom $g \in K[X]$, so dass $f = \underbrace{g \cdot g \cdots g}_{p \text{ Mal}} = g^p$ gilt.*

Beweis.

(b)$\Longrightarrow$(a) Sei $a \in K$ beliebig. Wir setzen $f := a$. Dann ist $f' = 0$. Nach Voraussetzung existiert ein Polynom $g \in K$ mit $f = g^p$. Die Gradformel zeigt $\deg g \leq 0$, also $g \in K$. Somit ist g ein Urbild von a unter φ. Da $a \in K$ beliebig gewählt war, ist φ surjektiv. ⁉

(a)$\Longrightarrow$(b) Sei $f := \sum_{i=0}^{n} a_i X^i \in K[X]$. Dann ist

$$\begin{aligned} f' = 0 \quad &\Longleftrightarrow \quad \sum_{i=1}^{n} i \cdot a_i \cdot X^{i-1} = 0 \\ &\Longleftrightarrow \quad i \cdot a_i = 0 \text{ für alle } i \in \{1, 2, \ldots, n\}. \end{aligned}$$

Wir betrachten die letzte Bedingung genauer: $a_0 \in K$ kann beliebig sein. Gilt $p \mid i$ in $\mathbb{Z}$, so ist $i = 0$ in K. Damit gibt es auch keine Einschränkungen an die a_i mit $p \mid i$. Ansonsten ist $i \neq 0$ in K. Es folgt zwingend $a_i = 0$.

Insgesamt treten in der Darstellung von f also nur Koeffizienten a_i mit $p \mid i$ auf. Wir können also schreiben $f = \sum_{j=0}^{r} b_j X^{p \cdot j}$. ⁉

Da φ surjektiv ist, finden wir Elemente $\beta_j \in K$ mit $\varphi(\beta_j) = \beta_j^p = b_j$. Dann folgt

$$\begin{aligned} f \quad &= \quad \sum_{j=0}^{r} b_j X^{p \cdot j} = \sum_{j=0}^{r} \beta_j^p (X^j)^p = \sum_{j=0}^{r} (\beta_j X^j)^p \\ &\overset{\substack{\text{Frobenius:} \\ (a+b)^p = a^p + b^p}}{=} \quad \Big(\sum_{j=0}^{r} \beta_j X^j \Big)^p. \end{aligned}$$

Wir können also $g := \sum_{j=0}^{r} \beta_j X^j$ setzen; dann ist $f = g^p$. ■

Das folgende Korollar führt überraschenderweise in die Theorie der separablen Körpererweiterungen:

Korollar 29.5 *Seien K ein Körper der Charakteristik p und φ sein Frobenius. Dann sind die folgenden Aussagen äquivalent:*

(a) *φ ist surjektiv.*

(b) *Für **jede** algebraische Körpererweiterung $L|K$ gilt: $L|K$ ist separabel.*

Beweis.

(a)$\Longrightarrow$(b) Wir beweisen per Widerspruch und nehmen an, wir hätten einen Oberkörper L von K gefunden, so dass die algebraische Körpererweiterung $L|K$ inseparabel sei. Dann gibt es ein $a \in L$, das über K inseparabel ist. Nach 25.14 gilt dann $m' = 0$ für das Minimalpolynom $m \in K[X]$ von a.

Da φ surjektiv ist, folgt mit dem vorherigen Satz, dass sich m in der Form $m = g^p$ mit einem Polynom $g \in K[X]$ schreiben lässt. Dies widerspricht aber der Irreduzibilität von m.

(b)$\Longrightarrow$(a) Sei $a \in K$ beliebig. Wir setzen $f := X^p - a \in K[X]$ und bezeichnen den Zerfällungskörper von f über K mit L. Sei $n \in L$ eine Nullstelle von f. Dann zerlegt sich f über L in der Form $f = (X - n)^p$. ?

Es sei $f = f_1 \cdots f_s$ die Zerlegung von f in irreduzible Polynome über K. Jedes der f_i besitzt ausschließlich die Nullstelle n. Wäre $\deg f_i > 1$ für ein i, so hätte das irreduzible Polynom f_i die Nullstelle n als Mehrfachnullstelle. Damit wäre das Element $n \in L$ inseparabel über K. Also wäre auch die Erweiterung $L|K$ inseparabel, was der Voraussetzung widerspricht. ?

Also haben alle f_i den Grad Eins. Daher liegt n in K und ist ein Urbild von a unter φ. Dies zeigt, dass φ surjektiv ist. ■

Für Körper, die der Aussage (b) aus dem Korollar genügen, führt man eine eigene Bezeichnung ein:

Definition 29.6 *Der Körper K heißt **vollkommen** oder **perfekt**, wenn jede algebraische Erweiterung L von K separabel ist.*
Anders formuliert: Perfekte Körper besitzen keine inseparablen algebraischen Erweiterungen.

Bemerkung 29.7 (a) Die Aussage aus 25.15 lässt sich nun knapper fassen: Jeder Körper der Charakteristik Null ist perfekt.

(b) Die perfekten Körper in positiver Charakteristik werden von 29.5 klassifiziert: Genau die Körper mit primer Charakteristik und surjektivem Frobenius sind perfekt.

(c) Mit (b) und 29.2 folgt, dass alle endlichen Körper perfekt sind. Dies hatten wir bereits in 25.17 angemerkt.

Mit (b) und 29.3 folgt, dass der Körper $\mathbb{F}_p(t)$ mit transzendentem t imperfekt ist. Dies hatten wir bereits in 25.18 gesehen. ⁕

Wir kommen auf den Fall endlicher Körper zurück. Hier ist der Frobeniusendomorphismus ein Automorphismus. Durch Verknüpfen mit sich selbst erhalten wir dann weitere Automorphismen. Wir klären, wie deren Abbildungsvorschrift aussieht:

Definition/Satz 29.8 *Seien K ein endlicher Körper der Charakteristik $p \in \mathbb{P}$ und φ sein Frobenius. Für $r \in \mathbb{N}$ setzen wir*

$$\varphi^r := \underbrace{\varphi \circ \varphi \circ \cdots \circ \varphi}_{r \text{ Mal}}.$$

Für $r = 0$ definieren wir per Konvention $\varphi^0 := \mathrm{id}_K$.
Dann ist φ^r für alle $r \in \mathbb{N}_0$ ein Automorphismus von K. Es gilt $\varphi^r(a) = a^{p^r}$ für alle $a \in K$.

Beweis. Aus 6.11 (d) folgt, dass φ^r ein Automorphismus ist. Die explizite Darstellung von φ^r zeigen wir per Induktion nach r. Sei hierzu $a \in K$ beliebig.
Für $r = 0$ ist

$$\varphi^0(a) = \mathrm{id}_K(a) = a = a^1 = a^{p^0}.$$

Ist die Darstellung $\varphi^r(a) = a^{p^r}$ bereits gezeigt, so folgt

$$\begin{aligned} \varphi^{r+1}(a) &= \varphi\Big(\varphi^r(a)\Big) = \varphi\Big(a^{p^r}\Big) = \Big(a^{p^r}\Big)^p \\ &= a^{p^r \cdot p} = a^{p^{r+1}}. \end{aligned}$$

■

Das folgende Korollar drückt den Satz von Fermat 24.5 mit Hilfe des Frobenius aus:

Korollar 29.9 *Seien $p \in \mathbb{P}$, $r \in \mathbb{N}$ und φ der Frobenius des endlichen Körpers $\mathbb{F}_{p^r}$. Dann gilt $\varphi^r = \mathrm{id}_{\mathbb{F}_{p^r}}$.*

Beweis. Für jedes $a \in \mathbb{F}_{p^r}$ gilt

$$\varphi^r(a) \overset{29.8}{=} a^{p^r} \overset{24.5}{=} a.$$

■

24.8 erlaubt es, die Elemente des endlichen Körpers $\mathbb{F}_p^r$ mit Hilfe des Frobenius zu charakterisieren:

Satz 29.10 *Seien p eine Primzahl, K der algebraische Abschluss von $\mathbb{F}_p$ und φ der Frobenius von K. Dann gilt für jedes $r \in \mathbb{N}$*

$$\mathbb{F}_{p^r} = \{a \in K \mid \varphi^r(a) = a\}.$$

Der endliche Körper $\mathbb{F}_{p^r}$ besteht also gerade aus den Fixpunkten der r-ten Potenz des Frobenius von K.

Bemerkung 29.11 Das Korollar zeigt, dass der algebraische Abschluss von $\mathbb{F}_p$ zu jeder Potenz von p *genau einen* Körper dieser Ordnung enthält. Dies haben wir bereits in 24.12 gesehen, hier aber mit einer leicht anderen Herangehensweise begründet. ※

29.9 zeigt, dass der Frobenius eines endlichen Körpers $\mathbb{F}_{p^r}$ eine endliche Ordnung besitzt, die r teilt. Das nächste Resultat zeigt, dass sogar Gleichheit gilt:

Satz 29.12 *Seien $p \in \mathbb{P}$, $r \in \mathbb{N}$ und φ der Frobenius des endlichen Körpers $\mathbb{F}_{p^r}$. Dann gilt $\mathrm{ord}(\varphi) = r$.*

Beweis. Angenommen, die Ordnung von φ wäre ungleich r. Aufgrund des obigen Korollars wäre dann $s := \operatorname{ord}(\varphi) < r$.
Sei a ein Erzeuger der nach 15.21 zyklischen Gruppe $\mathbb{F}_{p^r}$. Dann ist

$$\varphi^s(a) \overset{\varphi^s=\mathrm{id}}{=} a, \quad \text{also} \quad a^{p^s} = a, \quad \text{also} \quad a^{p^s} - a = 0.$$

Daher ist a eine Nullstelle des Polynoms $f := X^{p^s} - X$ und liegt nach 24.8 im Körper $\mathbb{F}_{p^s}$. Nun ist aber

$$|\langle a \rangle| = |\mathbb{F}_{p^r}^\times| = p^r - 1 \overset{r>s}{>} p^s - 1 = |\mathbb{F}_{p^s}^\times|.$$

Das Erzeugnis von a „passt“ also gar nicht in den kleineren Körper $\mathbb{F}_{p^s}$ hinein. Dies ist widersprüchlich und zeigt $\operatorname{ord}(\varphi) = r$. ∎

Galoistheorie endlicher Körper

Wir haben nun alle Vorarbeiten geleistet, um uns mit der Galoistheorie endlicher Körper zu beschäftigen. Seien hierzu $p \in \mathbb{P}$ eine Primzahl und r, n natürliche Zahlen. Wir betrachten die Körpererweiterung $\mathbb{F}_{p^{nr}} | \mathbb{F}_{p^r}$ vom Grad n.

?

$\mathbb{F}_{p^{nr}}$ ist Zerfällungskörper des Polynoms $X^{p^{nr}} - X \in \mathbb{F}_{p^r}[X]$ und damit normal über $\mathbb{F}_{p^r}$. Wegen der Perfektheit von $\mathbb{F}_p$ ist die Erweiterung $\mathbb{F}_{p^{nr}} | \mathbb{F}_{p^r}$ auch separabel und somit galoissch. Wir setzen $G := \operatorname{Gal}(\mathbb{F}_{p^{nr}} | \mathbb{F}_{p^r})$.

$\mathbb{F}_{p^{nr}}$
$| n$
$\mathbb{F}_{p^r}$

Sei φ der Frobenius von $\mathbb{F}_{p^{nr}}$. Nach 29.10 fixiert φ^r jedes $a \in \mathbb{F}_{p^r}$. Daher ist φ^r ein $\mathbb{F}_{p^r}$-Automorphismus von $\mathbb{F}_{p^{nr}}$ und somit ein Element von G. Es gilt also

$$\langle \varphi^r \rangle \leq G.$$

φ als Frobenius des Körpers $\mathbb{F}_{p^{nr}}$ hat Ordnung nr, vgl. 29.12. Hieraus folgt $\operatorname{ord}(\varphi^r) = n$; die Gruppe $\langle \varphi^r \rangle$ enthält also n Elemente.
Aus dem Hauptsatz der Galoistheorie ergibt sich $|G| = [\mathbb{F}_{p^{nr}} : \mathbb{F}_{p^r}] = n$, so dass die Gleichheit

$$\langle \varphi^r \rangle = G$$

folgt. Die Galoisgruppe der Erweiterung $\mathbb{F}_{p^{nr}} | \mathbb{F}_{p^r}$ wird also von der r-ten Potenz des Frobenius des Oberkörpers erzeugt.
Diese Erkenntnis formulieren wir als Satz:

Satz 29.13 *Seien p eine Primzahl und $r, n \in \mathbb{N}$ natürliche Zahlen. Wir bezeichnen den Frobenius von $\mathbb{F}_{p^{nr}}$ mit φ. Dann gelten die folgenden Aussagen:*

(a) *Die Körpererweiterung $\mathbb{F}_{p^{nr}} | \mathbb{F}_{p^r}$ ist galoissch und besitzt Grad n.*

Da p, r, n völlig beliebig gewählt waren, heißt dies, dass endliche Erweiterungen endlicher Körper stets galoissch sind.

(b) *Es ist*

$$\operatorname{Gal}(\mathbb{F}_{p^{nr}} | \mathbb{F}_{p^r}) = \langle \varphi^r \rangle = \{\varphi^r, \varphi^{2r}, \ldots, \varphi^{nr} = \mathrm{id}\}.$$

Die Galoisgruppe einer endlichen Erweiterung eines endlichen Körpers ist also stets zyklisch. Es ist $\operatorname{Gal}(\mathbb{F}_{p^{nr}} | \mathbb{F}_{p^r}) \cong C_n$. Der Isomorphietyp der Galoisgruppe einer endlichen Erweiterung endlicher Körper hängt nur vom Grad der Erweiterung ab.

Bemerkung 29.14 (a) In der Praxis tritt der Fall $r = 1$, also der Fall, in dem die Galoiserweiterung über dem Grundkörper $\mathbb{F}_p$ betrachtet wird, besonders häufig auf. Hier wird die Galoisgruppe vom Frobenius selbst erzeugt. Es gilt

$$\mathrm{Gal}(\mathbb{F}_{p^n}|\mathbb{F}_p) = \{\varphi, \varphi^2, \dots, \varphi^n = \mathrm{id}\} \cong C_n.$$

(b) Ist ein $n \in \mathbb{N}$ vorgegeben, so gibt es in jeder Charakteristik $p \in \mathbb{P}$ unendlich viele Körpererweiterungen endlicher Körper, deren Galoisgruppe isomorph zu C_n ist. Beispielsweise gilt für jedes $p \in \mathbb{P}$

$$C_n \cong \mathrm{Gal}(\mathbb{F}_{p^n}|\mathbb{F}_p) \cong \mathrm{Gal}(\mathbb{F}_{p^{2n}}|\mathbb{F}_{p^2}) \cong \mathrm{Gal}(\mathbb{F}_{p^{3n}}|\mathbb{F}_{p^3}) \cong \cdots.$$

(c) Da zyklische Gruppen zu jedem Teiler t ihrer Ordnung genau eine Untergruppe dieser Ordnung t besitzen, zeigt die Galoisdualität: Die Galoiserweiterung $\mathbb{F}_{p^{nr}}|\mathbb{F}_{p^r}$ besitzt zu jedem Teiler t von n genau einen Zwischenkörper Z mit $[\mathbb{F}_{p^{nr}} : Z] = t$.

Dies haben wir im Spezialfall $r = 1$ bereits auf Seite 173 gesehen, jetzt aber mit völlig anderen Hilfsmitteln hergeleitet.

Können Sie Z in der Form $\mathbb{F}_{p^{???}}$ angeben? ⁂ ⁉

Das Umkehrproblem, Realisierung von Galoisgruppen

In der Galoistheorie ist das **Umkehrproblem** ein aktives Forschungsgebiet. Grob gesprochen geht es um die Frage, welche Gruppen als Galoisgruppen auftreten. Etwas genauer: Man fragt sich, welche Gruppen G **über dem Körper K realisierbar** sind, also für welche Gruppen G ein galoisscher Erweiterungskörper L von K existiert, so dass $\mathrm{Gal}(L|K) \cong G$ ist.
Wir haben in 29.13 das Umkehrproblem für endliche Körper komplett gelöst: Über jedem endlichen Körper sind genau die endlichen zyklischen Gruppen realisierbar.

30. Kreisteilungstheorie, Teil 1

Worum geht es? Wir beschäftigen uns in dieser Vorlesung mit den Elementen aus $\mathbb{C}^\times$, die endliche multiplikative Ordnung haben, den sogenannten *Einheitswurzeln*. Diese haben interessante algebraische Eigenschaften, liefern Beispiele für Galoiserweiterungen mit abelschen Galoisgruppen und vertiefen die Beziehung zwischen Gruppen- und Körpertheorie. ⁂

Ein zentraler Begriff in dieser Vorlesung ist der der Einheitswurzel:

Definition 30.1 (Einheitswurzeln) *Unter einer **Einheitswurzel** verstehen wir eine komplexe Zahl $\xi \in \mathbb{C} \setminus \{0\}$, die eine endliche multiplikative Ordnung hat.*
*Gilt $\operatorname{ord}(\xi) = n \in \mathbb{N}$, so bezeichnen wir die Einheitswurzel ξ genauer als **n-te primitive Einheitswurzel**.*
*Wissen wir nur, dass $\xi^n = 1$ für ein $n \in \mathbb{N}$ gilt, so nennen wir ξ eine **n-te Einheitswurzel**.*

ξ Xi

Einheitswurzeln sind uns bereits in 1.6 (b) begegnet: Die zyklische Gruppe C_n besteht genau aus den n-ten Einheitswurzeln. Wir fassen einige grundlegende und uns schon bekannte Aussagen über Einheitswurzeln zusammen:

Bemerkung 30.2 (a) Zu jedem $n \in \mathbb{N}$ gibt es genau $|C_n| = n$ verschiedene n-te Einheitswurzeln. Dies sind genau die Elemente ξ aus $\mathbb{C}^\times$, deren Ordnung ein Teiler von n ist. Die primitiven n-ten Einheitswurzeln sind genau die Erzeuger von C_n. Es gibt daher genau $\varphi(n)$ verschiedene primitive n-te Einheitswurzeln.

(b) Einheitswurzeln lassen sich mit Hilfe der komplexen Exponentialfunktion darstellen: Die n-ten Einheitswurzeln sind genau durch die komplexen Zahlen

$$\exp\Big(\frac{2\pi i}{n} \cdot k\Big) = \exp\Big(\frac{2\pi i}{n}\Big)^k$$

mit $k \in \mathbb{Z}$ gegeben. Man kann den Bereich, aus dem k gewählt wird, weiter einschränken, beispielsweise auf $k \in \{0, 1, \dots, n-1\}$ oder $k \in \{1, 2, \dots, n\}$.

?

(c) Für jedes $n \in \mathbb{N}$ ist die n-te Einheitswurzel $\xi := \exp(\frac{2\pi i}{n})$ eine primitive n-te Einheitswurzel, denn nach 2.19 (d) erzeugt ξ die Gruppe C_n und hat daher Ordnung n.

Die primitiven n-ten Einheitswurzeln sind nach 7.15 (c) genau die komplexen Zahlen der Form

$$\xi^k = \exp(\frac{2\pi i}{n} \cdot k) \qquad \text{mit zu } n \text{ teilerfremden } k \in \mathbb{Z}.$$

Auch hier kann man k weiter einschränken, beispielsweise auf $k \in \{0, \dots, n-1\}$ oder auf $k \in \{1, \dots, n\}$.

(d) Die n-ten Einheitswurzeln liegen auf dem Einheitskreis und teilen ihn gleichmäßig in n Stücke auf. Aus dieser geometrische Eigenschaft folgt der Name **Kreisteilungstheorie** für die Theorie der Einheitswurzeln.

(e) Ist ξ eine n-te Einheitswurzel, so gilt $\xi^n - 1 = 0$. Daher sind n-te Einheitswurzeln genau die komplexen Nullstellen des Polynoms $X^n - 1 \in \mathbb{Q}[X]$.

(f) Für jedes $n \in \mathbb{N}$ ist die Menge der n-ten Einheitswurzeln die disjunkte Vereinigung der Menge der primitiven d-ten Einheitswurzeln, wobei d alle Teiler von n durchläuft. Anders formuliert: Bezeichnen wir mit P_d die Menge der d-ten primitiven Einheitswurzeln (für $d \in \mathbb{N}$), so folgt

$$C_n = \bigcup_{d|n}^{\cdot} P_d.$$

Können Sie dies begründen? ⁂ ⁉

Beispiel 30.3 (a) Die komplexe Zahl i ist eine 16-te Einheitswurzel und eine primitive vierte Einheitswurzel. Sie ist insbesondere eine Einheitswurzel, aber weder dritte noch primitive dritte Einheitswurzel. Sie ist auch keine primitive 16-te Einheitswurzel.

(b) Sei ξ eine Einheitswurzel. Dann ist ξ für unendlich viele $n \in \mathbb{N}$ eine n-te Einheitswurzel und für genau ein $s \in \mathbb{N}$ eine primitive s-te Einheitswurzel. Die möglichen n sind genau die Vielfachen von s. ⁂

Knobelfrage. Ist jedes Element des Einheitskreises eine Einheitswurzel? ⁉

Wir betrachten nun die körpertheoretischen Aspekte der Kreisteilungstheorie. Ein erstes Resultat ist, dass die Adjunktion von Einheitswurzeln stets Galoiserweiterungen erzeugt:

Satz 30.4 *Sei K ein Körper der Charakteristik Null, also ein Oberkörper von $\mathbb{Q}$. Sei ξ eine beliebige primitive n-te Einheitswurzel. Dann ist die Erweiterung $K(\xi)|K$ galoissch. Insbesondere ist die Körpererweiterung $\mathbb{Q}(\xi)|\mathbb{Q}$ galoissch.*
Man nennt $\mathbb{Q}(\xi)$ auch ***den n-ten Kreisteilungskörper*** *und die Erweiterung $\mathbb{Q}(\xi)|\mathbb{Q}$ die* ***n-te Kreisteilungserweiterung****.*

Beweis. ξ ist eine Nullstelle des Polynoms $f := X^n - 1 \in K[X]$ und ein Erzeuger der Gruppe C_n. Es gilt daher $C_n = \{\xi^0, \xi^1, \dots, \xi^{n-1}\} \subseteq K(\xi)$, und wir können $K(\xi)$ als Zerfällungskörper von f über K auffassen. 26.4 liefert nun die Behauptung. ■

Bemerkung 30.5 Um die Bezeichnung *n-ter Kreisteilungskörper* in obigem Satz zu rechtfertigen, muss man sich überlegen, dass $\mathbb{Q}(\xi)$ nur von n, nicht aber von der Wahl der primitiven n-ten Einheitswurzel ξ abhängt.
Dies folgt, da *jede* primitive n-te Einheitswurzel *dieselbe* Gruppe C_n aller n-ten Einheitswurzeln erzeugt. Es gilt daher $\mathbb{Q}(\xi) = \mathbb{Q}(\xi^0, \xi^1, \dots, \xi^{n-1}) = \mathbb{Q}(C_n)$ für jede primitive n-te Einheitswurzel ξ. ⁂ ⁉

Wir wollen die Galoisgruppe von $\mathbb{Q}(\xi)|\mathbb{Q}$ beschreiben. Dies kann mit Hilfe von 28.3 geschehen; jedoch benötigen wir hierzu das Minimalpolynom von ξ. Dessen Bestimmung ist das Ziel des nächsten Abschnitts.

Kreisteilungspolynome

Die im Folgenden definierten Polynome spielen in der Algebra an vielen Stellen eine wichtige Rolle. Wir werden sehen, dass sie gerade die Minimalpolynome der primitiven n-ten Einheitswurzeln über $\mathbb{Q}$ sind.

Φ
Phi

Definition 30.6 (Kreisteilungspolynom) *Sei $n \in \mathbb{N}$. Dann nennen wir das Polynom*

$$\Phi_n := \prod_{\substack{\xi \text{ ist primitive} \\ n\text{-te Einheitswurzel}}} (X - \xi) = \prod_{\substack{0 \le k \le n-1 \\ \mathrm{ggT}(k,n)=1}} \left(X - \exp\left(\frac{2\pi i}{n} \cdot k\right)\right)$$

*das **n-te Kreisteilungspolynom**. Es hat genau die primitiven n-ten Einheitswurzeln als Nullstellen und daher Grad $\varphi(n)$.*

Mit Hilfe der Kreisteilungspolynome kann man das Polynom $X^n - 1$ faktorisieren:

Lemma 30.7 *Für jedes $n \in \mathbb{N}$ gilt*

$$X^n - 1 = \prod_{d|n} \Phi_d.$$

Beweis. Der Beweis der Aussage erfolgt mit ähnlichen Überlegungen wie in 30.2 (f). Es gilt

$$X^n - 1 = \prod_{\substack{\xi \text{ ist } n\text{-te} \\ \text{Einheitswurzel}}} (X - \xi) = \prod_{d|n} \prod_{\substack{\xi \text{ ist primitive} \\ d\text{-te Einheitswurzel}}} (X - \xi) = \prod_{d|n} \Phi_d.$$

■

Die Kreisteilungspolynome Φ_n sind über ihre *komplexen* Nullstellen definiert. Wir müssen daher im Moment noch davon ausgehen, dass die Φ_n Elemente aus $\mathbb{C}[X]$ sind. Die obige Faktorisierung ist vor diesem Hintergrund noch kein großer Wurf: Dass man über $\mathbb{C}$ Polynome in Linearfaktoren zerlegen, diese dann umsortieren und neu klammern kann, ist nahezu trivial.
Wir zeigen im Folgenden aber, dass $\Phi_n \in \mathbb{Z}[X]$ für alle $n \in \mathbb{N}$ gilt. Beim Umgang mit Kreisteilungspolynomen können wir zukünftig also über den ganzen Zahlen arbeiten. Dem eigentlichen Beweis stellen wir einige Hilfslemmata voran.

Lemma 30.8 *Sei $f \in \mathbb{Q}[X]$ ein irreduzibles Polynom, das eine primitive n-te Einheitswurzel ξ als Nullstelle besitze. Dann sind alle Nullstellen von f primitive n-te Einheitswurzeln.*

Beweis. Wir wissen aus 30.4, dass die Erweiterung $\mathbb{Q}(\xi)|\mathbb{Q}$ galoissch ist. f zerfällt daher vollständig in $\mathbb{Q}(\xi)$. Sei $a \in \mathbb{Q}(\xi)$ irgendeine Nullstelle von f. Wegen der Irreduzibilität von f gibt es nach 28.3 einen Galoisautomorphismus φ von $\mathbb{Q}(\xi)|\mathbb{Q}$ mit $\varphi(\xi) = a$. Dieser erhält nach 6.6 multiplikative Ordnungen. Es ist also $\mathrm{ord}(\xi) = n = \mathrm{ord}(a)$.
Also ist a ebenfalls eine primitive n-te Einheitswurzel. ■

Lemma 30.9 *Das normierte, ganzzahlige Polynom $f \in \mathbb{Z}[X]$ sei zerlegt in der Form $f = g \cdot h$ mit $g, h \in \mathbb{Q}[X]$. Dann gilt: Ist g normiert, so sind g und h bereits Elemente aus $\mathbb{Z}[X]$.*

Beweis. Der Beweis beruht auf Gauß 19.10: Wir finden ein $k \in \mathbb{Q}^\times$, so dass die Polynome $G := k^{-1} \cdot g$ und $H := k \cdot h$ ganzzahlig sind. Der Leitkoeffizient von G ist k^{-1}. Da f und g normiert sind, ist auch h normiert. Daher ist k der Leitkoeffizient von H. Weil G und H beide aus $\mathbb{Z}[X]$ stammen, folgt $k, k^{-1} \in \mathbb{Z}$ und daher $k = \pm 1$. Multiplikation mit k^{-1} bzw. k ändert somit nur die Vorzeichen der Koeffizienten von Polynomen. Es gilt also $g = k \cdot G \in \mathbb{Z}[X]$ sowie $h = k^{-1} \cdot H \in \mathbb{Z}[X]$. ■

Wir können nun die Ganzzahligkeit der Kreisteilungspolynome beweisen:

Satz 30.10 *Für alle $n \in \mathbb{N}$ gilt $\Phi_n \in \mathbb{Z}[X]$.*

Beweis. Sei $n \in \mathbb{N}$ beliebig. Wir bezeichnen die primitiven n-ten Einheitswurzeln (in irgendeiner Anordnung) mit $\xi_1, \xi_2, \dots, \xi_{\varphi(n)}$. Für alle i sei $m_i \in \mathbb{Q}[X]$ das Minimalpolynom von ξ_i; die Menge der komplexen Nullstellen von m_i nennen wir N_i.
Wir wissen aus 30.8, dass die N_i nur primitive n-te Einheitswurzeln enthalten. Die Irreduzibilität der m_i zeigt, dass für $i, j \in \{1, \dots, \varphi(n)\}$ entweder $N_i = N_j$ oder $N_i \cap N_j = \emptyset$ gilt.
Durch geeignete Umnummerierung der ξ_i (und dann, nachfolgend, der m_i und N_i) erreichen wir, dass wir die Menge der n-ten primitiven Einheitswurzeln als disjunkte Vereinigung der ersten r der Mengen N_i schreiben können, also dass gilt

$$\{\xi_1, \dots, \xi_{\varphi(n)}\} = N_1 \cup N_2 \cup \dots \cup N_r.$$

Das Polynom $f := m_1 \cdots m_r$ besitzt dann genau die primitiven n-ten Einheitswurzeln als Nullstellen, hat Grad $\varphi(n)$ und ist normiert. Somit ist $f = \Phi_n$. Als Produkt von Polynomen aus $\mathbb{Q}[X]$ ist $f = \Phi_n \in \mathbb{Q}[X]$. Dies zeigt, dass alle Kreisteilungspolynome in $\mathbb{Q}[X]$ liegen.
Nun benutzen wir 30.7 und schreiben

$$X^n - 1 = \prod_{d|n} \Phi_d = \Phi_n \cdot \prod_{\substack{d|n \\ d \neq n}} \Phi_d = \Phi_n \cdot g \qquad \text{mit } g := \prod_{\substack{d|n \\ d \neq n}} \Phi_d.$$

Wir haben bereits gezeigt, dass alle Kreisteilungspolynome in $\mathbb{Q}[X]$ liegen. Daher gilt $\Phi_n, g \in \mathbb{Q}[X]$. Zudem sind $X^n - 1$ und Φ_n normiert. Mit 30.9 folgt nun $\Phi_n \in \mathbb{Z}[X]$. ■

Die wahrscheinlich wichtigste Aussage über Kreisteilungspolynome ist deren Irreduzibilität. Diese beweisen wir im Folgenden, schicken aber wieder einige Hilfsaussagen vorweg.
Das nachstehende Lemma ist ein typisches Reduktionsresultat: Um zu zeigen, dass ein Polynom alle primitiven n-ten Einheitswurzeln als Nullstellen besitzt, reicht es aus, die oft leichtere Aussage (R) zu beweisen. Man reduziert die schwierige Aussage also auf eine leichter zu zeigende.

Lemma 30.11 *Seien K ein Körper der Charakteristik Null, $n \in \mathbb{N}$ und $f \in K[X]$ ein Polynom, das die primitive n-te Einheitswurzel ξ als Nullstelle besitze. Zudem gelte für alle primitiven n-ten Einheitswurzeln a:*

$$\text{Ist } p \in \mathbb{P} \text{ mit } \operatorname{ggT}(n, p) = 1 \text{ und gilt } f(a) = 0, \text{ so ist auch } f(a^p) = 0. \qquad \text{(R)}$$

Dann besitzt f jede primitive n-te Einheitswurzel als Nullstelle.

Beweisskizze. Die primitive n-te Einheitswurzel ξ ist nach Voraussetzung eine Nullstelle von f. Sei z eine weitere primitive n-te Einheitswurzel. Dann existiert nach 30.2 (c) ein zu n teilerfremdes $k \geq 2$ mit $z = \xi^k$. Sei $k = p_1 \cdots p_r$ die Primfaktorzerlegung von k. Wegen $\mathrm{ggT}(k, n) = 1$ ist auch $\mathrm{ggT}(p_i, n) = 1$ für alle i. Sukzessives Anwenden von (R) zeigt, dass die Elemente

$$\xi^{p_1}, \quad \xi^{p_1 \cdot p_2}, \quad \xi^{p_1 \cdot p_2 \cdot p_3}, \quad \ldots, \quad \xi^{p_1 \cdots p_r} = \xi^k = z$$

Nullstellen von f sind. Dies liefert die Behauptung. ■

Lemma 30.12 *Seien $p \in \mathbb{P}$ eine Primzahl und $f \in \mathbb{Z}_p[X]$. Dann gilt*

$$f(X^p) = \underbrace{f \cdot f \cdots f}_{p \text{ Mal}} = f^p.$$

Beweis. Sei $f = \sum_{i=0}^{n} a_i X^i$ mit $a_i \in \mathbb{Z}_p$. Mit Fermat folgt $a_i^p = a_i$. Wir erhalten

$$\begin{aligned} f(X^p) &= \sum_{i=0}^{n} a_i (X^p)^i \overset{\text{Fermat}}{=} \sum_{i=0}^{n} a_i^p X^{pi} = \sum_{i=0}^{n} \left(a_i X^i\right)^p \\ &\overset{\substack{\text{Frobenius:} \\ (a+b)^p = a^p + b^p}}{=} \left(\sum_{i=0}^{n} a_i X^i\right)^p = f^p. \end{aligned}$$

■

Lemma 30.13 *Seien K ein beliebiger Körper, $n \in \mathbb{N}$ und $f := X^n - 1 \in K[X]$.*
Genau dann besitzt f Mehrfachnullstellen in seinem Zerfällungskörper, wenn $n = 0$ in K gilt, also wenn die Charakteristik von K ein Teiler von n ist.

Beweis. Wir bezeichnen mit p die Charakteristik von K. Es gilt $p \in \mathbb{P} \cup \{0\}$. Weiter ist $f' = n \cdot X^{n-1}$. Wir führen den Beweis mit Hilfe des Kriteriums aus 23.21:

$\Longrightarrow$ Sei a eine Mehrfachnullstelle von f. Dann gilt $f(a) = 0 = f'(a)$. Aus $f(a) = 0$ folgt $a \neq 0$. Damit $f'(a) = n \cdot a^{n-1} = 0$ erfüllt sein kann, muss $n = 0$ in K gelten. Dies erzwingt $p \mid n$. ?

$\Longleftarrow$ Sei p ein Teiler von n. Dann ist $f' = n \cdot X^{n-1} = 0$. Jede Nullstelle a von f ist damit auch eine Nullstelle von f'. Also besitzt f Mehrfachnullstellen. ■

Nun können wir die Irreduzibilität der Kreisteilungspolynome beweisen:

Satz 30.14 *Für jedes $n \in \mathbb{N}$ ist das n-te Kreisteilungspolynom Φ_n ein irreduzibles, normiertes Polynom aus $\mathbb{Z}[X]$. Dies bedeutet, dass $\Phi_n \in \mathbb{Z}[X]$ das Minimalpolynom **jeder** primitiven n-ten Einheitswurzel über $\mathbb{Q}$ ist.*

Beweis. Offenbar ist Φ_n normiert. 30.10 zeigt $\Phi_n \in \mathbb{Z}[X]$. Es ist daher nur noch die Irreduzibilität von Φ_n zu zeigen:
Sei $m \in \mathbb{Q}[X]$ das Minimalpolynom der n-ten primitiven Einheitswurzel $\xi := \exp(\frac{2\pi i}{n})$. Wegen $\Phi_n(\xi) = 0$ folgt $m \mid \Phi_n$, und wir erhalten eine Zerlegung der Form

$$\Phi_n = m \cdot g \qquad \text{mit normiertem } g \in \mathbb{Z}[X] \text{ nach 30.9.} \qquad (\star)$$

Können wir zeigen, dass m alle primitiven n-ten Einheitswurzeln als Nullstellen besitzt, dann folgt $\Phi_n = m$ und somit die Irreduzibilität von Φ_n.
Wir führen den Beweis, indem wir die Bedingung (R) aus 30.11 per Widerspruch nachweisen. Sei also eine zu n teilerfremde Primzahl $p \in \mathbb{P}$ mit $m(\xi^p) \neq 0$ gegeben.
Da ξ^p eine primitive n-te Einheitswurzel ist, gelten $\Phi_n(\xi^p) = 0$ und mit $(\star)$ somit $g(\xi^p) = 0$. Also ist ξ eine Nullstelle des Polynoms $g(X^p)$. Da m das Minimalpolynom von ξ ist, faktorisiert sich $g(X^p)$ in der Form

$$g(X^p) = m \cdot h \qquad \text{mit normiertem } h \in \mathbb{Z}[X] \text{ nach 30.9.} \qquad (\star\star)$$

Wir kennzeichnen im Folgenden die Koeffizientenreduktion modulo p mit einem Querstrich. Diese Reduktionstechnik ist uns bereits beim Eisensteinkriterium auf Seite 136 begegnet. Durch sie wird ein Polynom $f \in \mathbb{Z}[X]$ in ein Polynom $\overline{f} \in \mathbb{Z}_p[X]$ überführt.
Sei z eine Nullstelle von $\overline{m}$ aus einem Zerfällungskörper von $\overline{m}$. Dann ist z nach $(\star\star)$ auch eine Nullstelle von $\overline{g(X^p)}$ und mit 30.12 auch von $\overline{g}^p$. Es folgt, dass z auch eine Nullstelle von $\overline{g}$ ist. Die Zerlegung $(\star)$ zeigt, dass z eine *doppelte* Nullstelle von $\overline{\Phi_n}$ ist.
Nun ist aber Φ_n ein Teiler von $X^n - 1$. Damit ist auch $\overline{\Phi_n}$ ein Teiler von $\overline{X^n - 1}$, und $\overline{X^n - 1}$ besitzt Mehrfachnullstellen. Aus 30.13 folgt $p \mid n$. Dies widerspricht aber der vorausgesetzten Teilerfremdheit von p und n.
Dieser Widerspruch zeigt, dass eine Primzahl $p \in \mathbb{P}$ mit $\mathrm{ggT}(p, n) = 1$ und $m(\xi^p) \neq 0$ nicht existiert und beendet den Beweis. ■

Wir können die Zerlegung von $X^n - 1$ aus 30.7 nun als Zerlegung über $\mathbb{Z}$ interpretieren:

Korollar 30.15 *Sei $n \in \mathbb{N}$ beliebig. Dann ist die Zerlegung von $X^n - 1$ in normierte irreduzible Polynome über $\mathbb{Z}$ gegeben durch*

$$X^n - 1 = \prod_{d \mid n} \Phi_d.$$

Bemerkung 30.16 Dies ist ein starkes Resultat. Man kennt nur wenige Polynomklassen, deren Zerfällungsverhalten über $\mathbb{Q}$ bzw. $\mathbb{Z}$ man vollständig beschreiben kann. ※

31. Kreisteilungstheorie, Teil 2

Worum geht es? Wir benutzen die Zerlegung $X^n - 1 = \prod_{d|n} \Phi_d$ zur Berechnung der Kreisteilungspolynome.
Danach bestimmen wir die Galoisgruppen der n-ten Kreisteilungserweiterungen. Wir nutzen hier im Wesentlichen die in der letzten Vorlesung gezeigte Irreduzibilität der Kreisteilungspolynome aus.
Weiter zeigen wir eine schwache Version des Satzes von Kronecker-Weber: Wir weisen nach, dass über $\mathbb{Q}$ alle endlichen zyklischen Gruppen realisierbar sind. ⁜

Berechnung von Kreisteilungspolynomen

In der letzten Vorlesung haben wir die Beziehung $X^n - 1 = \prod_{d|n} \Phi_d$ bewiesen. Mit ihrer Hilfe kann man die Kreisteilungspolynome rekursiv berechnen:

Beispiel 31.1 (a) Es ist $X - 1 = X^1 - 1 = \prod_{d|1} \Phi_d = \Phi_1$.

(b) Für Primzahlen $p \in \mathbb{P}$ gilt $X^p - 1 = \prod_{d|p} \Phi_d = \Phi_1 \cdot \Phi_p$. Zusammen mit (a) und der geometrischen Summenformel $(X-1) \cdot \sum_{i=0}^{n-1} X^i = X^n - 1$ folgt

$$\Phi_p = \frac{X^p - 1}{X - 1} = \sum_{i=0}^{p-1} X^i = 1 + X + X^2 + \cdots + X^{p-1}.$$

Es folgt weiter, dass ein Polynom der Form $1 + X + X^2 + \cdots + X^n \in \mathbb{Z}[X]$ genau dann irreduzibel ist, wenn $n + 1 \in \mathbb{P}$ gilt. ⁉

(c) Eine ähnliche Schlussweise funktioniert für Primzahlpotenzen p^r mit $r \geq 1$. Hier nutzt man aus, dass die Teiler von p^r durch p^i mit $i \in \{0, 1, \ldots, r\}$ gegeben sind und sich die Faktoren, in die sich $X^{p^r} - 1$ zerlegt, schön zusammenfassen lassen:

$$X^{p^r} - 1 = \prod_{i=0}^{r} \Phi_{p^i} = \Phi_{p^r} \cdot \prod_{i=0}^{r-1} \Phi_{p^i} = \Phi_{p^r} \cdot \prod_{d|p^{r-1}} \Phi_d = \Phi_{p^r} \cdot (X^{p^{r-1}} - 1).$$

Setzen wir $Y := X^{p^{r-1}}$, so folgt aus obiger Zeile

$$\begin{aligned} \Phi_{p^r} &= \frac{X^{p \cdot p^{r-1}} - 1}{X^{p^{r-1}} - 1} = \frac{(X^{p^{r-1}})^p - 1}{X^{p^{r-1}} - 1} = \frac{Y^p - 1}{Y - 1} \overset{\text{vgl. (b)}}{=} \sum_{i=0}^{p-1} Y^i \\ &= \sum_{i=0}^{p-1} X^{i \cdot p^{r-1}} = 1 + X^{p^{r-1}} + X^{2 \cdot p^{r-1}} + X^{3 \cdot p^{r-1}} + \cdots + X^{(p-1) \cdot p^{r-1}}. \end{aligned}$$

(d) Wir wollen Φ_n für $n = 12$ berechnen. Es ist

$$\Phi_{12} = \frac{X^{12} - 1}{\prod_{d|12,\, d \neq 12} \Phi_d} = \frac{X^{12} - 1}{\Phi_1 \cdot \Phi_2 \cdot \Phi_3 \cdot \Phi_4 \cdot \Phi_6}.$$

Wir können verwenden, dass $\Phi_1 \cdot \Phi_2 \cdot \Phi_3 \cdot \Phi_6 = X^6 - 1$ ist. Damit erhalten wir

$$\Phi_{12} = \frac{X^{12}-1}{\Phi_4 \cdot (X^6-1)} \overset{\text{3. bin. Formel, (c)}}{=} \frac{X^6+1}{1+X^2} = X^4 - X^2 + 1. \qquad \text{※}$$

Bemerkung 31.2 (Koeffizientenvermutung für Φ_n) Wir haben im Beispiel unendlich viele Kreisteilungspolynome berechnet. Als Koeffizienten sind nur die Werte $1, 0, -1$ aufgetreten, so dass man vermuten könnte, dass stets nur diese Koeffizienten auftreten können.
Diese Vermutung ist falsch. Das kleinste n, für das ein anderer Koeffizient (nämlich -2) auftritt, ist $n = 105$. Zudem zeigte Issai Schur in den 1930er Jahren, dass die Koeffizienten der Φ_n für wachsende n betragsmäßig beliebig groß werden. ※

Galoistheorie der Kreisteilungserweiterungen

Nach 30.4 sind Kreisteilungserweiterungen galoissch. Da Φ_n nach 30.14 das Minimalpolynom *aller* primitiven n-ten Einheitswurzeln ist, können wir mit Hilfe von 28.3 die Galoisgruppe der Kreisteilungserweiterungen vollständig beschreiben:

Satz 31.3 *Sei $n \in \mathbb{N}$ gegeben. Sei $\xi := \exp(\frac{2\pi i}{n})$. Dann besteht die Galoisgruppe der n-ten Kreisteilungserweiterung $\mathbb{Q}(\xi)|\mathbb{Q}$ genau aus den Automorphismen*

$$\varphi_k : \mathbb{Q}(\xi) \to \mathbb{Q}(\xi) \text{ mit } \varphi_k(\xi) = \xi^k, \qquad \text{wobei } k \in \mathbb{Z} \text{ und } \operatorname{ggT}(k,n) = 1 \text{ gelten.}$$

Wieder kann die Auswahl für k eingeschränkt werden; so ist beispielsweise $k \in \{1, 2, \dots, n\}$ mit $\operatorname{ggT}(k,n) = 1$ möglich.
Die Galoisgruppe enthält daher genau $\varphi(n)$ Elemente. Es ist $[\mathbb{Q}(\xi) : \mathbb{Q}] = \varphi(n) = \deg \Phi_n$.

Die Struktur dieser Galoisgruppe wird durch die folgende Isomorphie klarer:

Korollar 31.4 *Wir benutzen die Bezeichnungen aus obigem Satz. Dann gilt: Die Abbildung*

$$f : \mathbb{Z}_n^\times \to \operatorname{Gal}(\mathbb{Q}(\xi)|\mathbb{Q}), \qquad \bar{k} \mapsto \varphi_k$$

ist ein Gruppenisomorphismus.
Die Galoisgruppe der n-ten Kreisteilungserweiterung ist also isomorph zur Einheitengruppe $\mathbb{Z}_n^\times$ von $\mathbb{Z}_n$ und daher insbesondere abelsch.

Beweis. Die Elemente aus $\mathbb{Z}_n$ sind Nebenklassen. Wir müssen f daher auf Wohldefiniertheit überprüfen: Seien $k, s \in \mathbb{Z}$ beliebig mit $\bar{k} = \bar{s} \in \mathbb{Z}_n^\times$. Dann ist $s = k + z \cdot n$ mit einem $z \in \mathbb{Z}$. Wir zeigen, dass $f(\bar{k}) = f(\bar{s})$ gilt. Damit ist nachgewiesen, dass f eine Abbildung ist. Es gilt ?

$$f(\bar{s})(\xi) = \varphi_s(\xi) = \xi^s = \xi^{k+zn} \overset{\xi^n=1}{=} \xi^k = \varphi_k(\xi) = f(\bar{k})(\xi).$$

f ist surjektiv; denn ist $\varphi \in \mathrm{Gal}(\mathbb{Q}(\zeta)|\mathbb{Q})$ beliebig, so existiert ein $k \in \{1, \dots, n\}$ mit $\mathrm{ggT}(k, n) = 1$, so dass $\varphi = \varphi_k$ ist. Es folgt $\overline{k} \in \mathbb{Z}_n^\times$ und $f(\overline{k}) = \varphi_k$. Weil Definitions- und Zielbereich von f gleichmächtig sind, ist damit die Bijektivität von f gezeigt.
Die Homomorphie von f zeigt man durch Nachrechnen der Verträglichkeitsbedingung $f(\overline{k} \cdot \overline{s}) = f(\overline{k}) \circ f(\overline{s})$. ■

Speziell für $n \in \mathbb{P}$ kennen wir den Isomorphietyp von $\mathbb{Z}_n^\times$: Dann gilt $\mathbb{Z}_n^\times \cong C_{\varphi(n)} = C_{n-1}$ nach 15.21. Dies liefert:

Korollar 31.5 *Seien n eine beliebige **Primzahl** und ζ eine primitive n-te Einheitswurzel. Dann ist*

$$\mathrm{Gal}(\mathbb{Q}(\zeta)|\mathbb{Q}) \cong C_{n-1}.$$

Für primes n ist die Galoisgruppe von $\mathbb{Q}(\zeta)|\mathbb{Q}$ also eine zyklische Gruppe.

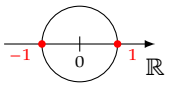
Beispiel 31.6 (Der Zwischenkörper $\mathbb{Q}(\zeta + \zeta^{-1})$) Sei ζ eine primitive n-te Einheitswurzel. Dann ist der Körper $\mathbb{Q}(\zeta + \zeta^{-1})$ offensichtlich ein Zwischenkörper der Galoiserweiterung $\mathbb{Q}(\zeta)|\mathbb{Q}$. Wir setzen $a := \zeta + \zeta^{-1}$ und untersuchen diesen Körper genauer.
Wir zeigen zunächst, dass $\mathbb{Q}(a)$ ein Unterkörper von $\mathbb{R}$ ist. Hierbei hilft die Beobachtung, dass ζ den Betrag Eins hat, dass also $|\zeta|^2 = \zeta \cdot \overline{\zeta} = 1$ gilt. Hieraus folgt $\overline{\zeta} = \zeta^{-1}$ und daher

$$a = \zeta + \zeta^{-1} = \zeta + \overline{\zeta} = 2 \cdot \mathrm{Re}(\zeta) \in \mathbb{R}.$$

Als nächstes beweisen wir, dass $[\mathbb{Q}(\zeta) : \mathbb{Q}(a)] \leq 2$ ist, indem wir ein Polynom f konstruieren, das über $\mathbb{Q}(a)$ definiert ist und ζ als Nullstelle besitzt. (Bevor Sie weiterlesen: Können Sie ein solches Polynom finden?) Nutzen wir die Beziehung

$$a \cdot \zeta = (\zeta + \zeta^{-1}) \cdot \zeta = \zeta^2 + 1,$$

so folgt, dass $f := X^2 - a \cdot X + 1 \in \mathbb{Q}(a)[X]$ das Gewünschte leistet.
Wir können daher feststellen: Ist ζ nicht reell, so hat die Erweiterung $\mathbb{Q}(\zeta)|\mathbb{Q}(a)$ den Grad Zwei und f ist das Minimalpolynom von ζ über $\mathbb{Q}(a)$.
Ist ζ hingegen reell, so gilt $\zeta = \pm 1$, denn ζ hat als Einheitswurzel den Betrag Eins, liegt aber zugleich auf der reellen Achse, vgl. die Skizze rechts. In diesem Fall gelten $n \in \{1, 2\}$ und $\mathbb{Q}(\zeta) = \mathbb{Q}(a) = \mathbb{Q}$.
Wir können also sagen: Genau für $n \geq 3$ ist $\mathbb{Q}(\zeta) \neq \mathbb{Q}(a)$. In diesem Fall ist $[\mathbb{Q}(\zeta) : \mathbb{Q}(a)] = 2$ und das oben definierte Polynom f ist ein Minimalpolynom für ζ über $\mathbb{Q}(a)$.⁂



Staatsexamensaufgabe (F2020T1A4) *Sei $\zeta \in \mathbb{C}$ eine primitive elfte Einheitswurzel und $K = \mathbb{Q}(\zeta)$.*

(a) *Zeigen Sie: K ist der Zerfällungskörper von $X^{11} - 1$ über $\mathbb{Q}$ und geben Sie den Isomorphietyp der Galois-Gruppe $\mathrm{Gal}(K|\mathbb{Q})$ an.*

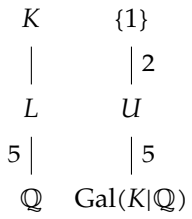
(b) *Zeigen Sie: Es gibt eine galoissche Körpererweiterung $\mathbb{Q} \subseteq L$ mit $[L : \mathbb{Q}] = 5$.*

zu (a) Wir setzen $f := X^{11} - 1 \in \mathbb{Q}[X]$. Da ξ eine Nullstelle von f ist, muss ξ im Zerfällungskörper von f enthalten sein. Dieser ist also ein Oberkörper von K. Umgekehrt enthält K alle Potenzen von ξ und damit alle elften Einheitswurzeln. Diese sind genau die Nullstellen von f. Also ist K bereits der Zerfällungskörper von f.

Nach 31.5 sind die Galoisgruppen von Kreisteilungserweiterungen mit primen Einheitswurzeln stets zyklisch. Damit ist $\mathrm{Gal}(K|\mathbb{Q}) \cong C_{\varphi(11)} \cong C_{10}$.

zu (b) Wir zeigen, dass L als Zwischenkörper der Galoiserweiterung $K|\mathbb{Q}$ gewählt werden kann.

Da die Galoisgruppe $G := \mathrm{Gal}(K|\mathbb{Q})$ zyklisch ist, besitzt sie zu jedem Teiler ihrer Ordnung (genau) eine Untergruppe. Sei $U \leq G$ eine Untergruppe vom **Index** fünf, also von **Ordnung** zwei. Da G abelsch ist, folgt sogar $U \trianglelefteq G$. Der Hauptsatz der Galoistheorie zeigt nun, dass $L := \mathrm{Fix}(U)$ ein Erweiterungskörper von $\mathbb{Q}$ vom Grad 5 ist und dass $L|\mathbb{Q}$ galoissch ist.



※

Realisierung zyklischer Galoisgruppen über $\mathbb{Q}$

Wir wollen in diesem Abschnitt zeigen, dass alle endlichen zyklischen Gruppen über $\mathbb{Q}$ realisierbar sind.
Tatsächlich gilt viel mehr: Über $\mathbb{Q}$ sind alle endlichen abelschen Gruppen realisierbar. Dies ist eine Folgerung aus dem (deutlich schwerer zu beweisenden) Satz von Kronecker-Weber, der die Zahlentheorie stark geprägt hat.

Satz 31.7 (Kronecker-Weber) *Zu jeder endlichen abelschen Gruppe G existiert ein $n \in \mathbb{N}$, so dass G isomorph zu einer Faktorgruppe von $\mathbb{Z}_n^\times$ ist.*
Dies zeigt: Jede endliche abelsche Gruppe ist über $\mathbb{Q}$ realisierbar.

Bemerkung 31.8 Die Realisierbarkeits-Aussage im Satz folgt analog zu Teil (b) in obiger Staatsexamensaufgabe:
Sei eine endliche abelsche Gruppe G gegeben und das nach Kronecker-Weber existierende n gewählt. Sei ξ eine primitive n-te Einheitswurzel. Es ist $\mathrm{Gal}(\mathbb{Q}(\xi) \mid \mathbb{Q}) \cong \mathbb{Z}_n^\times$. Nach Kronecker-Weber gibt es einen Normalteiler U von $\mathrm{Gal}(\mathbb{Q}(\xi) \mid \mathbb{Q})$, so dass $G \cong \mathrm{Gal}(\mathbb{Q}(\xi)|\mathbb{Q})/U$ ist. Setzen wir $K := \mathrm{Fix}(U)$, so folgt, dass $K|\mathbb{Q}$ galoissch ist mit

$$\mathrm{Gal}(K|\mathbb{Q}) \cong \mathrm{Gal}(\mathbb{Q}(\xi) \mid \mathbb{Q})/U \cong G.$$

Damit ist die Gruppe G als Galoisgruppe über $\mathbb{Q}$ realisiert. ※

Wir beweisen nun die nachstehende schwächere Version von Kronecker-Weber:

Satz 31.9 *Zu jedem $s \in \mathbb{N}$ existiert ein $n \in \mathbb{N}$, so dass C_s isomorph zu einer Faktorgruppe von $\mathbb{Z}_n^\times$ ist.*
Wie in 31.8 folgt dann: Alle endlichen zyklischen Gruppen sind über $\mathbb{Q}$ realisierbar.

Beispiel 31.10 (a) Wir betrachten zunächst den Fall, in dem $s = p - 1$ mit einer Primzahl $p \in \mathbb{P}$ ist.

In diesem Fall können wir $n := p$ setzen und erhalten $\mathbb{Z}_n^\times = \mathbb{Z}_p^\times \cong C_{p-1} = C_s$. Damit ist C_s isomorph zur Faktorgruppe $\mathbb{Z}_n^\times/\{1\}$.

(b) Nun betrachten wir den allgemeineren Fall, in dem s ein Teiler von $p - 1$ für eine Primzahl $p \in \mathbb{P}$ ist.

Setzen wir wieder $n := p$, so ist $\mathbb{Z}_n^\times \cong C_{p-1}$. Als zyklische Gruppe besitzt $\mathbb{Z}_n^\times$ eine Untergruppe U der Ordnung $|U| = \frac{p-1}{s}$. Der Quotient $\mathbb{Z}_n^\times/U$ ist dann nach 7.20 zyklisch und hat Ordnung

$$|\mathbb{Z}_n^\times/U| \overset{\text{Lagrange}}{=} \frac{|\mathbb{Z}_n^\times|}{\frac{p-1}{s}} = \frac{p-1}{\frac{p-1}{s}} = s.$$

Es ist also $\mathbb{Z}_n^\times/U \cong C_s$ und 31.9 gilt auch im Fall $s \mid p - 1$. ⋇

Man beweist 31.9 nun, indem man nachweist, dass Teil (b) des Beispiels für alle $s \in \mathbb{N}$ anwendbar ist. Hierzu ist zu zeigen, dass es zu jedem $s \in \mathbb{N}$ ein $p \in \mathbb{P}$ gibt, so dass $s \mid p - 1$ gilt. Dies folgt mit kreisteilungstheoretischen Mitteln.
Um die eigentliche Aussage zu zeigen, benötigen wir ein Hilfsresultat, das Aussagen über die Primteiler der Werte der Kreisteilungspolynome bereitstellt:

Lemma 31.11 *Seien $n \in \mathbb{N}$, $z \in \mathbb{Z}$ und $p \in \mathbb{P}$. Dann gilt: Ist p ein Teiler der ganzen Zahl $\Phi_n(z)$, so gilt $p \mid n$ oder $n \mid p - 1$.*

Beweis. Es gilt $\Phi_n \mid X^n - 1$. Einsetzen von z und die Voraussetzung $p \mid \Phi_n(z)$ liefern

$$p \mid \Phi_n(z) \mid z^n - 1, \qquad \text{also} \qquad p \mid z^n - 1.$$

Wir kennzeichnen im Folgenden die Koeffizientenreduktion modulo p mit einem Querstrich, vgl. den Beweis zu 30.14. Die Aussage $p \mid z^n - 1$ lässt sich dann in die Form $\bar{z}^n = \bar{1}$ umschreiben, was $\bar{z} \in \mathbb{Z}_p^\times$ zeigt. Definieren wir $t := \operatorname{ord}(\bar{z})$ als multiplikative Ordnung von $\bar{z}$, so erhalten wir zudem $t \mid n$. ⁉

Fall 1: Es gelte $t = n$.

Fermat 24.5 liefert $\bar{z}^p = \bar{z}$. Kürzen durch die Einheit $\bar{z}$ liefert $\bar{z}^{p-1} = \bar{1}$. Die Ordnung t von $\bar{z}$ ist daher ein Teiler von $p - 1$. Wegen $t = n$ folgt hieraus $n \mid p - 1$, was zu zeigen war.

Fall 2: Es gelte $t < n$.

Wir wissen, dass $\bar{z}$ eine Nullstelle des Polynoms $\overline{X^t - 1}$ ist. Über $\mathbb{Z}$ zerfällt $X^t - 1$ in der Form $X^t - 1 = \prod_{d \mid t} \Phi_d$. Über $\mathbb{Z}_p$ ist daher

$$\bar{0} = \overline{z^t - 1} = \prod_{d \mid t} \overline{\Phi_d(z)}.$$

Wegen der Nullteilerfreiheit des Körpers $\mathbb{Z}_p$ ist $\bar{z}$ daher Nullstelle des Polynoms $\overline{\Phi_d}$ für einen Teiler d von t.

Da d ein Teiler von n ist, kommt das Polynom Φ_d in der Zerlegung von $X^n - 1$ vor. Zudem gilt $d < n$ aufgrund unserer Voraussetzung $t < n$. Es gilt daher

$$\overline{X^n - 1} = \overline{\Phi_n} \cdot \overline{\Phi_d} \cdot \overline{\text{Produkt weiterer } \Phi_a \text{ mit gewissen Teilern } a \text{ von } n}.$$

Die Voraussetzung $p \mid \Phi_n(z)$ liefert $\overline{\Phi_n(z)} = \bar{0}$, die obigen Ausführungen $\overline{\Phi_d(z)} = \bar{0}$. Also ist $\bar{z}$ eine Mehrfachnullstelle von $\overline{X^n - 1}$. Aus 30.13 folgt dann, wie gewünscht, $p \mid n$. ■

Wir können nun die Existenz von Primzahlen p mit $s \mid p - 1$ zeigen und damit 31.9 beweisen.

Satz 31.12 *Zu jeder natürlichen Zahl $s \in \mathbb{N}$ existiert eine Primzahl $p \in \mathbb{P}$ mit $s \mid p - 1$.*

Beweis. Wir betrachten die Funktion

$$f : \mathbb{Z} \to \mathbb{Z}, \qquad z \mapsto \Phi_s(s \cdot z).$$

Da der Grad von Φ_s mindestens Eins beträgt, ist Φ_s unbeschränkt. Somit finden wir ein $z \in \mathbb{Z}$ mit $|f(z)| > 1$. Sei p eine Primzahl mit $p \mid f(z)$. Aus obigem Lemma folgt, dass

$$p \mid s \qquad \text{oder} \qquad s \mid p - 1.$$

Wir zeigen per Widerspruch, dass der Fall $p \mid s$ nicht eintritt. Dann muss $s \mid p - 1$ gelten, was den Satz beweist.
Angenommen, es sei $p \mid s$. Wegen $\Phi_s \mid X^s - 1$ folgt auch $f(z) = \Phi_s(sz) \mid (sz)^s - 1$. Zudem gilt $p \mid f(z)$ nach Wahl von p. Zusammen ergibt sich

$$p \mid (sz)^s - 1.$$

Zusammen mit der Annahme $p \mid s$ folgt nun der Widerspruch $p \mid -1$. ■

32. Der Satz von Vieta, symmetrische Polynome

Worum geht es? Wir untersuchen, wie sich die Koeffizienten eines Polynoms aus seinen Nullstellen berechnen lassen. Eine Abstraktion dieses Vorgehens liefert den Begriff des *symmetrischen Polynoms*. Im *Hauptsatz über symmetrische Polynome* zeigen wir, dass sich jedes symmetrische Polynom durch die elementarsymmetrischen Polynome darstellen lässt. ⋇

Der Satz von Vieta

Der Satz von Vieta gibt an, wie sich die Koeffizienten eines normierten Polynoms aus dessen Nullstellen zusammensetzen. Man beweist den Satz durch Ausmultiplizieren.

Seien K ein Körper und $f \in K[X]$ ein normiertes Polynom vom Grad n. Über seinem Zerfällungskörper Z zerlegt sich f in der Form

$$f = (X - z_1) \cdot (X - z_2) \cdots (X - z_n) \quad \text{mit den Nullstellen } z_1, \dots, z_n \in Z.$$

Um einfacher rechnen zu können, setzen wir $x_i := -z_i$ für $1 \leq i \leq n$. Auf diese Weise fallen in der Zerlegung von f die Minuszeichen weg; es ist also

$$f = (X + x_1)(X + x_2) \cdots (X + x_n).$$

Wir multiplizieren die rechte Seite aus: Hierzu wählen wir in jeder Klammer entweder den Summanden X oder einen Summanden der Form x_i. Diese n ausgewählten Objekte multiplizieren wir miteinander; entscheiden wir uns k Mal *nicht* für den Summanden X, also k Mal *für* die Summanden x_i, so entsteht ein Monom der Form

$$x_{i_1} x_{i_2} \cdots x_{i_k} \cdot X^{n-k}. \qquad (\star)$$

f ist die Summe dieser 2^n Monome. Wir fassen nun noch Monome mit gleichem Grad zusammen und erhalten eine Darstellung von f der Form

$$f = \prod_{i=1}^{n} (X + x_i) = s_0 X^n + s_1 X^{n-1} + s_2 X^{n-2} + \cdots + s_n X^0 = \sum_{i=0}^{n} s_i X^{n-i}.$$

s_k ist die Summe aller Koeffizienten von Monomen der Form $(\star)$, d. h. es gilt

$$\begin{aligned} s_k &= \text{Summe aller möglichen Produkte von } k \text{ Elementen aus } \{x_1, \dots, x_n\} \\ &= \sum_{1 \leq i_1 < i_2 < \dots < i_k \leq n} x_{i_1} x_{i_2} \cdots x_{i_k} = \sum_{\substack{S \subseteq \{1,\dots,n\} \\ |S| = k}} \prod_{i \in S} x_i. \end{aligned}$$

Beispiel 32.1 Mit den obigen Bezeichnungen gelten

$$\begin{aligned} s_0 &= \sum_{\substack{S\subseteq\{1,\dots,n\}\\|S|=0}} \prod_{i\in S} x_i = \prod_{i\in\emptyset} x_i = 1, \\ s_1 &= \sum_{\substack{S\subseteq\{1,\dots,n\}\\|S|=1}} \prod_{i\in S} x_i = \sum_{j=1}^{n} \prod_{i\in\{j\}} x_j = \sum_{j=1}^{n} x_j = x_1 + \cdots + x_n, \\ s_n &= \sum_{\substack{S\subseteq\{1,\dots,n\}\\|S|=n}} \prod_{i\in S} x_i = \prod_{i\in\{1,\dots,n\}} x_i = \prod_{i=1}^{n} x_i = x_1 \cdot x_2 \cdots x_n. \end{aligned}$$

Diese Überlegungen beweisen den Satz von Vieta:

Satz 32.2 (Vieta) *Seien K ein Körper und $f \in K[X]$ ein normiertes Polynom mit Zerfällungskörper Z und Nullstellen $z_1, \dots, z_n \in Z$. Wir setzen $x_i := -z_i$ für alle $i \in \{1, \dots, n\}$ sowie*

$$s_k := \sum_{\substack{S\subseteq\{1,\dots,n\}\\|S|=k}} \prod_{i\in S} x_i \qquad \text{für } 0 \le k \le n.$$

Dann gilt $f = \sum_{i=0}^{n} s_{n-i} X^i$ (oder nach Änderung der Summationsreihenfolge: $f = \sum_{i=0}^{n} s_i X^{n-i}$). Die Koeffizienten eines normierten Polynoms sind also Summen von Produkten des Negativen von dessen Nullstellen.

Bemerkung 32.3 In der Schule wird der Satz von Vieta typischerweise nur für quadratische Polynome gezeigt: Sind a, b die Nullstellen eines normierten quadratischen Polynoms f und setzen wir $x_1 := -a$ und $x_2 := -b$, so ist f nach Vieta gegeben durch

$$f = s_0 X^2 + s_1 X + s_2 \overset{32.1}{=} 1 \cdot X^2 + (x_1 + x_2)X + x_1 x_2 = x^2 - (a+b)X + ab.$$

Analoge Aussagen gelten nach Vieta für normierte Polynome beliebig hohen Grades. ⁜

Symmetrische Polynome

Im letzten Abschnitt waren die x_i konkrete „Zahlen", nämlich die Nullstellen eines gegebenen Polynoms f. Wir ersetzen die x_i nun durch abstrakte Polynomvariablen, arbeiten nun also in Ringen mit mehreren Polynomvariablen. Zur Verdeutlichung verändern wir die Notation und schreiben ab jetzt X_i.

Bemerkung 32.4 Polynomringe in mehreren Polynomvariablen sind uns bisher kaum begegnet. Wir gehen daher kurz auf ihre Definition und ihre grundlegenden Eigenschaften ein:
Seien R ein Ring und $X_1, X_2, \dots$ Polynomvariablen. Den Polynomring $R[X_1]$ in einer Unbestimmten kennen wir bereits. Man definiert rekursiv

$$R[X_1, \dots, X_{n+1}] := (R[X_1, \dots, X_n])[X_{n+1}] \qquad \text{für } n \in \mathbb{N}.$$

Ringe der Form $R[X_1, \dots, X_n]$ heißen **Polynomringe über R in den Polynomvariablen $X_1, \dots, X_n$**, ihre Elemente **Polynome in den Polynomvariablen $X_1, \dots, X_n$**.
Durch Ausmultiplizieren und Umsortieren sieht man, dass die Elemente aus $R[X_1, \dots, X_n]$ Summen von **Monomen** der Form

$$r_{i_1,\dots,i_n} X_1^{i_1} X_2^{i_2} \cdots X_n^{i_n} \qquad \text{mit } i_1, \dots, i_n \in \mathbb{N}_0 \text{ und } r_{i_1,\dots,i_n} \in R$$

sind. Es ist also

$$R[X_1, \dots, X_n] = \left\{ \sum_{i_1=0}^{s_1} \sum_{i_2=0}^{s_2} \cdots \sum_{i_n=0}^{s_n} r_{i_1,\dots,i_n} X_1^{i_1} X_2^{i_2} \cdots X_n^{i_n} : s_1, \dots, s_n \in \mathbb{N}_0, r_{i_1,\dots,i_n} \in R \right\}.$$

Sind S ein Oberring von R und $a_1, \dots, a_n \in S$, so definieren wir das **Einsetzen von $a_1, \dots, a_n$** als die Abbildung

$$R[X_1, \dots, X_n] \to S, \qquad f \mapsto f(a_1, \dots, a_n);$$

wir ersetzen hierbei die Variable X_i durch das Element a_i, und zwar für alle $i \in \{1, \dots, n\}$.
Das Einsetzen von $a_1, \dots, a_n$ entspricht einem n-malig nacheinander ausgeführten Einsetzen in die einzelnen Polynomvariablen: Zunächst setzen wir a_1 in X_1 ein, danach setzen wir a_2 in X_2 ein, etc.
Da das Einsetzen in eine einzige Variable nach 15.11 ein Homomorphismus ist, ist auch das Einsetzen von $a_1, \dots, a_n$ als n-malige Verkettung von Einsetzungen ein Homomorphismus. ⁂

Wir werden in den folgenden Vorlesungen den Ring $R[X_1, \dots, X_n]$ noch häufiger benötigen. Um die Lesbarkeit im Skript zu erhöhen, führen wir die folgende Notation ein:

Vereinbarung zur Schreibweise 32.5 Seien R ein Ring und $n \in \mathbb{N}$. Wir schreiben zukünftig R_n für den Polynomring $R[X_1, \dots, X_n]$ in den n Polynomvariablen $X_1, \dots, X_n$. ⁂

Wir lassen nun die symmetrische Gruppe S_n auf den Variablen $X_1, \dots, X_n$ durch Vertauschen von Indizes operieren:

σ
Sigma

Definition/Satz 32.6 *Seien R ein Ring, $f \in R_n$ und σ ein Element der symmetrischen Gruppe S_n. Dann setzen wir $\sigma \bullet f := f(X_{\sigma(1)}, X_{\sigma(2)}, \dots, X_{\sigma(n)})$.*
Hierdurch wird eine Operation von S_n auf R_n definiert, was man durch Überprüfen der Operations-Axiome schnell sieht.
Wir können diese Operation auch als Einsetzen von $X_{\sigma(1)}, \dots, X_{\sigma(n)}$ in f interpretieren. Dies zeigt, dass $\bullet$ für festes $\sigma \in S_n$ einen Ringhomomorphismus liefert: Für alle $f, g \in R_n$ ist daher

$$\sigma \bullet (f \cdot g) = (\sigma \bullet f) \cdot (\sigma \bullet g) \qquad \text{und} \qquad \sigma \bullet (f + g) = \sigma \bullet f + \sigma \bullet g.$$

Wir können nun definieren, was wir unter einem symmetrischen Polynom verstehen:

Definition 32.7 *Seien R ein Ring und $n \in \mathbb{N}$. Wir nennen $f \in R_n$ ein **symmetrisches Polynom**, wenn f ein Fixpunkt unter der Operation von S_n ist, also wenn gilt*

$$f = \sigma \bullet f \qquad \text{für alle } \sigma \in S_n.$$

Beispiel 32.8 (a) Für $f = X_1 + 2X_2 + 3X_3 \in \mathbb{R}_3$ und $\sigma = (1\,2\,3) \in S_3$ gelten

$$\sigma \bullet f = X_2 + 2X_3 + 3X_1 \quad \text{und} \quad \sigma^2 \bullet f = X_3 + 2X_1 + 3X_2.$$

f ist nicht symmetrisch.

τ Tau

(b) Ein Polynom $f \in R_n$ ist genau dann symmetrisch, wenn $\tau \bullet f = f$ für alle *Transpositionen* $\tau \in S_n$ gilt.

Dies folgt aus der Verträglichkeitsbedingung für Gruppenoperationen 10.2 und der Tatsache, dass nach 9.1 jedes Element aus S_n als Produkt von Transpositionen geschrieben werden kann.

(c) Das Polynom $X_1 + X_2$ ist symmetrisch in R_2, aber nicht in R_3.

(d) Für $k \in \mathbb{N}$ verstehen wir unter dem ***k*-ten Potenzsummenpolynom über R_n** das Polynom

$$\sum_{i=1}^{n} X_i^k = X_1^k + X_2^k + \cdots + X_n^k \in R_n.$$

Es ist symmetrisch für jedes $k \in \mathbb{N}$ und jeden Ring R.

(e) Sind $f, g \in R_n$ symmetrisch, so liefert die Homomorphie von $\bullet$, dass auch die Polynome $f + g, f \cdot g$ und $-f$ symmetrisch sind. Zudem sind das Null- und das Einspolynom symmetrisch.

Dies zeigt, dass die Menge der symmetrischen Polynome einen Unterring von R_n bilden, den **Ring der symmetrischen Polynome über R in n Variablen**. ⋇

Wir wollen eine besonders wichtige Klasse symmetrischer Polynome kennenlernen. Diese haben dasselbe Bildungsgesetz wie die Koeffizienten s_k aus dem Satz von Vieta:

Definition/Satz 32.9 *Seien R ein Ring und $n \in \mathbb{N}$. Für $k \in \mathbb{N}_0$ setzen wir*

$$E_k := \sum_{\substack{S \subseteq \{1,\ldots,n\} \\ |S|=k}} \prod_{i \in S} X_i \in R_n$$

*und nennen E_k das **k-te elementarsymmetrische Polynom über R in n Variablen**.*
Es gelten per Konvention $E_0 = 1$ und $E_k = 0$ für $k > n$.
Weiter ist E_k ein symmetrisches Polynom für jedes $k \in \mathbb{N}_0$.

Beweis. Wir zeigen die Symmetrie der elementarsymmetrischen Polynome. Sei hierzu $\sigma \in S_n$ eine beliebige Permutation. Da $\bullet$ ein Homomorphismus ist, können wir σ am Summen- und Produktzeichen vorbei direkt auf die Polynomvariablen anwenden:

$$\begin{aligned} \sigma \bullet E_k &= \sigma \bullet \sum_{\substack{S \subseteq \{1,\ldots,n\} \\ |S|=k}} \prod_{i \in S} X_i = \sum_{\substack{S \subseteq \{1,\ldots,n\} \\ |S|=k}} \prod_{i \in S} \sigma \bullet X_i = \sum_{\substack{S \subseteq \{1,\ldots,n\} \\ |S|=k}} \prod_{i \in S} X_{\sigma(i)} \\ &= \sum_{\substack{S \subseteq \{1,\ldots,n\} \\ |S|=k}} \prod_{i \in \sigma(S)} X_i. \end{aligned}$$

σ als Permutation der Zahlen $1, 2, \dots, n$ permutiert auch die k-elementigen Teilmengen von $\{1, \dots, n\}$. Dies bedeutet, dass die Anwendung von σ nur die Reihenfolge ändert, in der die Monome $\prod_{i \in S} X_i$ aufsummiert werden. Dies verändert das Polynom E_k aber nicht:

$$\sigma \bullet E_k = \sum_{\substack{S \subseteq \{1,\dots,n\} \\ |S|=k}} \prod_{i \in \sigma(S)} X_i \overset{\text{Summationsreihenfolge ändern}}{=} \sum_{\substack{S \subseteq \{1,\dots,n\} \\ |S|=k}} \prod_{i \in S} X_i = E_k.$$

Da σ beliebig war, folgt die zu zeigende Symmetrie. ■

Die Bedeutung der elementarsymmetrischen Polynome ist im folgenden Resultat begründet. Es sagt aus, dass sich jedes symmetrische Polynom eindeutig durch die elementarsymmetrischen Polynome darstellen lässt:

Satz 32.10 (Hauptsatz über symmetrische Polynome) *Seien R ein Ring, $n \in \mathbb{N}$, $f \in R_n$ ein symmetrisches Polynom und $E_k \in R_n$ die elementarsymmetrischen Polynome. Dann gibt es ein eindeutig bestimmtes Polynom $p \in R_n$ mit*

$$f = p(E_1, \dots, E_n).$$

Anders formuliert: Jedes symmetrische Polynom lässt sich in eindeutiger Weise als R-Linearkombination von Produkten der elementarsymmetrischen Polynome $E_1, \dots, E_n$ schreiben.

Beweisskizze. Der Beweis des Hauptsatzes ist technisch und findet sich beispielsweise in [Bos20, Satz 1 auf S. 219]. Wir skizzieren für die Existenz von p eine andere Beweisvariante, mit der man p explizit konstruieren kann. Sie beruht darauf, dass man die Monome aus R_n anordnet.

Anordnung der Monome Wir definieren auf den Monomen aus R_n eine *lexikographische Anordnung*: Für zwei Monome $r \cdot \prod_{i=1}^n X_i^{a_i}$ und $s \cdot \prod_{i=1}^n X_i^{b_i}$ aus R_n mit $r, s \neq 0$ scheiben wir

$$r \cdot \prod_{i=1}^n X_i^{a_i} < s \cdot \prod_{i=1}^n X_i^{b_i},$$

falls ein $i \in \{0, \dots, n-1\}$ existiert, so dass $a_j = b_j$ für alle $j \leq i$ und $a_{i+1} < b_{i+1}$ gilt. Wir setzen zudem fest, dass die Null aus R_n kleiner als jedes Nicht-Null-Monom ist.

Beachten Sie, dass der Koeffizient eines Monoms – sofern er ungleich Null ist – für die Anordnung keine Rolle spielt.

Es gelten beispielsweise $X_1X_2X_3 < X_1^2$ (mit $i = 0$) oder $100 \cdot X_1^2X_2^4X_5^3 < X_1^2X_2^4X_3^5$ (mit $i = 2$). Ferner ist $X_n < X_{n-1} < \cdots < X_3 < X_2 < X_1$.

Das Leitmonom Sei $f \in R_n$. Das bezüglich der eben definierten Anordnung größte Monom, das in der Darstellung von f auftritt, nennen wir das **Leitmonom von f** und schreiben $\mathrm{LM}(f)$ für es. Genau das Nullpolynom hat Leitmonom Null. Beispielsweise ist

$$\mathrm{LM}(19X_1^3X_2^9 - 23X_1^4X_2^7) = -23X_1^4X_2^7.$$

Direkt aus der Definition der elementarsymmetrischen Polynome folgt

$$\mathrm{LM}(E_k) = X_1 X_2 \cdots X_k \qquad \text{für alle } k \in \{1, 2, \ldots, n\}.$$

Man kann leicht nachweisen, dass das Leitmonom eines Produkts normierter Polynome dem Produkt der Leitmonome entspricht, dass dann also $\mathrm{LM}(f \cdot g) = \mathrm{LM}(f) \cdot \mathrm{LM}(g)$ gilt. Hieraus erhalten wir

$$\mathrm{LM}(E_k^r) = X_1^r \cdots X_k^r \qquad \text{für alle } k \in \{1, 2 \ldots, n\} \text{ und } r \in \mathbb{N}_0.$$

Leitmonome symmetrischer Polynome Sei $0 \neq f \in R_n$ ein *symmetrisches* Polynom mit Leitmonom $\mathrm{LM}(f) = r \cdot \prod_{i=1}^{n} X_i^{a_i}$. Dann ist $r \neq 0$, und es gilt

$$a_1 \geq a_2 \geq a_3 \geq \cdots \geq a_n.$$

Die Aussage $r \neq 0$ folgt wegen $f \neq 0$. Die Größenbeziehung der a_i zueinander folgt aus der Symmetrie von f: Wäre beispielsweise $a_1 < a_2$, so betrachten wir das Monom

$$(1\,2) \bullet \mathrm{LM}(f) = r \cdot X_1^{a_2} \cdot X_2^{a_1} \cdot \prod_{i=3}^{n} X_i^{a_i}.$$

Da f symmetrisch ist, taucht das Monom $(1\,2) \bullet \mathrm{LM}(f)$ in der Darstellung von f auf. Es ist aber größer als $\mathrm{LM}(f)$, was widersprüchlich ist. Ähnlich argumentiert man, wenn $a_i < a_j$ für beliebiges $i < j$ gilt.

Diese Feststellung hat eine wichtige Konsequenz: Leitmonome symmetrischer Polynome lassen sich durch die Leitmonome der elementarsymmetrischen Polynome darstellen. Genauer gilt: Ist $r \prod_{i=1}^{n} X_i^{a_i}$ das Leitmonom eines symmetrischen Polynoms f, so ist

$$\begin{aligned}
r \prod_{i=1}^{n} X_i^{a_i} &= r \cdot \prod_{i=1}^{n} X_i^{a_n} \cdot \prod_{i=1}^{n-1} X_i^{a_{n-1}-a_n} \cdot \prod_{i=1}^{n-2} X_i^{a_{n-2}-a_{n-1}} \cdots \prod_{i=1}^{1} X_i^{a_1-a_2} \\
&= r \cdot \prod_{i=1}^{n} X_i^{a_n} \cdot \prod_{j=1}^{n-1} \prod_{i=1}^{j} X_i^{a_j-a_{j+1}} \\
&= r \cdot \mathrm{LM}(E_n^{a_n}) \cdot \prod_{j=1}^{n-1} \mathrm{LM}(E_j^{a_j-a_{j+1}}) \\
&= \mathrm{LM}\Big(r \cdot E_n^{a_n} \cdot \prod_{j=1}^{n-1} E_j^{a_j-a_{j+1}}\Big).
\end{aligned}$$

Da nach Obigem stets $a_j \geq a_{j+1}$ ist, sind die in den Gleichungen auftretenden Exponenten nicht-negativ.

Setzen wir $p := r \cdot X_n \cdot \prod_{j=1}^{n-1} X_j^{a_j-a_{j+1}}$, so können wir die Gleichung auch in der Form

$$\mathrm{LM}(f) = \mathrm{LM}(p(E_1, \ldots, E_n))$$

schreiben.

Der eigentliche Beweis Sei f ein symmetrisches Polynom. Dann finden wir ein Polynom $p_0 \in R_n$ mit $\mathrm{LM}(f) = \mathrm{LM}(p_0(E_1, \dots, E_n))$. Wir setzen

$$f_1 := f - p_0(E_1, \dots, E_n) \in R_n.$$

Es ist $\mathrm{LM}(f_1) < \mathrm{LM}(f)$, denn das Leitmonom von f ist durch die Differenzbildung in f_1 weggefallen.

Nun gibt es ein Polynom $p_1 \in R_n$ mit $\mathrm{LM}(f_1) = \mathrm{LM}((p_1(E_1, \dots, E_n))$. Wir setzen

$$f_2 := f_1 - p_1(E_1, \dots, E_n).$$

Wieder fällt das Leitmonom von f_1 weg. f_2 ist also „kleiner“ als f_1.

Dies setzen wir immer weiter fort, ständig werden die Leitmonome kleiner. Nach endlich vielen Schritten erreichen wir dann die Gleichheit

$$f - p_1(E_1, \dots, E_n) - p_2(E_1, \dots, E_n) - \cdots - p_s(E_1, \dots, E_n) = 0.$$

Wir setzen $p := \sum_{i=1}^{s} p_i$ und haben das im Satz geforderte Polynom gefunden. ■

Beispiel 32.11 Wir stellen den Algorithmus aus dem Hauptsatz am zweiten Potenzsummenpolynom

$$f := X_1^2 + \cdots + X_n^2 \in R_n$$

vor. Es ist $\mathrm{LM}(f) = X_1^2 = \mathrm{LM}(E_1^2)$. Wir setzen $p_0 := X_1^2$ und erhalten

$$\begin{aligned} f_1 &:= f - p_0(E_1, \dots, E_n) = \sum_{i=1}^{n} X_i^2 - E_1^2 = \sum_{i=1}^{n} X_i^2 - \Big(\sum_{i=1}^{n} X_i\Big)^2 \\ &\overset{\text{binom. Formel}}{=} \sum_{i=1}^{n} X_i^2 - \Big(\sum_{i=1}^{n} X_i^2 + 2 \cdot \sum_{1 \le i < j \le n} X_i X_j\Big) \\ &= -2 \sum_{1 \le i < j \le n} X_i X_j = -2E_2. \end{aligned}$$

Wir setzen $p_1 := -2X_2$. Es folgt

$$f_2 := f_1 - p_1(E_1, \dots, E_n) = -2E_2 - (-2E_2) = -2E_2 + 2E_2 = 0.$$

Definieren wir $p := p_0 + p_1 = X_1^2 - 2X_2$, so erhalten wir

$$f = p(E_1, \dots, E_n) = E_1^2 - 2E_2$$

und haben somit eine Darstellung von f in den elementarsymmetrischen Polynomen gefunden.
Die Darstellung der Potenzsummenpolynome durch die elementarsymmetrischen Polynome wurde bereits von Newton untersucht. Die sich ergebenden Gleichungen nennt man auch die **Newton-Identitäten**.[4] ※

[4] Diese Identitäten wurden bereits 30 Jahre vor Newton von Albert Girard entdeckt. Dies scheint Newton aber nicht bekannt gewesen zu sein.

33. Das Diskriminantenkriterium

Worum geht es? Wir betrachten das Einsetzen von Nullstellen in symmetrische Polynome genauer. Als Hilfsmittel verwenden wir den Satz von Vieta sowie den Hauptsatz über symmetrische Polynome.
Danach leiten wir das Diskriminantenkriterium her. Dieses charakterisiert Polynome, deren Galoisgruppen ausschließlich gerade Permutationen enthalten. ⋇

In der letzten Vorlesung sind wir mit Nullstellen normierter Polynome gestartet, haben diese durch abstrakte Polynomvariablen ersetzt und sind schließlich beim Begriff des symmetrischen Polynoms angekommen.
Wir gehen diesen Weg nun rückwärts. Wir starten mit einem symmetrischen Polynom s und setzen in dessen Polynomvariablen Nullstellen normierter Polynome f ein. Wir erhalten auf diese Weise einen polynomialen Ausdruck in den Nullstellen von f:

Satz 33.1 *Seien K ein Körper, $n \in \mathbb{N}$ eine natürliche Zahl, $f = \sum_{i=0}^{n} a_i X^i \in K[X]$ ein normiertes Polynom mit Nullstellen $z_1, \dots, z_n$ (aus irgendeinem Zerfällungskörper von f) und $s \in K_n$ ein symmetrisches Polynom.*
Wir setzen $x_i := -z_i$ und bezeichnen mit $E_1, \dots, E_n \in K_n$ die elementarsymmetrischen Polynome und mit $p \in K_n$ das nach Hauptsatz existierende Polynom mit $s = p(E_1, \dots, E_n)$. Dann gelten die folgenden Aussagen:

(a) *Es ist $E_k(x_1, \dots, x_n) = a_{n-k}$ sowie $E_k(z_1, \dots, z_n) = (-1)^k \cdot a_{n-k}$.*

(b) *Es ist $s(x_1, \dots, x_n) = p(a_{n-1}, a_{n-2}, \dots, a_0) \in K$.*

(c) *Es ist $s(z_1, \dots, z_n) = p(-a_{n-1}, a_{n-2}, -a_{n-3}, \dots, (-1)^{n-1} a_1, (-1)^n a_0) \in K$.*

Beweis.

zu (a) Der erste Teil der Behauptung folgt direkt aus der Definition der E_k und dem Satz von Vieta. Der zweite Teil folgt nun durch konkretes Ausrechnen:

$$\begin{aligned} E_k(z_1, \dots, z_n) &= E_k(-x_1, \dots, -x_n) \overset{\text{Def. } E_k}{=} \sum_{\substack{S \subseteq \{1,\dots,n\} \\ |S|=k}} \prod_{i \in S} (-x_i) \\ &= (-1)^k \sum_{\substack{S \subseteq \{1,\dots,n\} \\ |S|=k}} \prod_{i \in S} x_i = (-1)^k E_k(x_1, \dots, x_n) = (-1)^k a_{n-k}. \end{aligned}$$

zu (b) Das Einsetzen der x_i in s führt letztlich auf das Einsetzen in die E_k. Es folgt

$$s(x_1, \dots, x_n) = p(E_1(x_1, \dots, x_n), \dots, E_n(x_1, \dots, x_n)) \overset{(a)}{=} p(a_{n-1}, \dots, a_0).$$

Der Ausdruck $p(a_{n-1}, \dots, a_0)$ ist eine K-Linearkombination von Produkten der a_i und somit ein Element aus K.

(c) folgt analog zu (b). ■

Beispiel 33.2 (Spuren von Matrixpotenzen) Sei $A \in K^{n\times n}$ eine Matrix mit charakteristischem Polynom $\chi_A := \sum_{i=0}^{n} a_i X^i \in K[X]$. Die Nullstellen $\lambda_1, \dots, \lambda_n$ von χ_A (in irgendeinem Zerfällungskörper von χ_A) sind genau die Eigenwerte von A. Für die Spur $\operatorname{tr}(A)$ gilt $\operatorname{tr}(A) = \sum_{i=1}^{n} \lambda_i$.
Wir sind an den Spuren der Potenzen von A interessiert, also an $\operatorname{tr}(A^k)$ mit $k \in \mathbb{N}$. Aus der Linearen Algebra ist bekannt, dass $\operatorname{tr}(A^k) = \sum_{i=1}^{n} \lambda_i^k$ gilt. Wir beschreiben nun, wie man diese Spuren ohne Kenntnis der λ_i berechnen kann.
Wir setzen $g_k := \sum_{i=1}^{n} X_i^k \in K_n$. Für alle $k \in \mathbb{N}$ ist g_k nach 32.8 (d) symmetrisch. Zudem gilt $\operatorname{tr}(A^k) = g_k(\lambda_1, \dots, \lambda_n)$ für alle $k \in \mathbb{N}$. Durch Ausnutzen der Newton-Identitäten 32.11 lassen sich mit Hilfe von 33.1 (c) alle Spuren als Polynome in den Koeffizienten a_i von χ_A ausdrücken. Beispielsweise gilt:

$k =$	Newton-Identität für g_k	Anwenden von 33.1 (c) liefert
1	$g_1 = E_1$	$\operatorname{tr}(A) = (-1)^1 a_{n-1} = -a_{n-1}$
2	$g_2 = E_1^2 - 2E_2$	$\operatorname{tr}(A^2) = ((-1)^1 a_{n-1})^2 - 2a_{n-2} = a_{n-1}^2 - 2a_{n-2}$
3	$g_3 = E_1^3 - 3E_1E_2 + 3E_3$	$\operatorname{tr}(A^3) = -a_{n-1}^3 + 3a_{n-1}a_{n-2} - 3a_{n-3}$

※

Die Diskriminante

Definition 33.3 (Diskriminante) *Seien K ein Körper und $n \in \mathbb{N}$. Dann bezeichnen wir den Ausdruck*

$$\begin{aligned} D_n &:= \prod_{1\le i<j\le n} (X_i - X_j)^2 \\ &= (X_1 - X_2)^2 \cdots (X_1 - X_n)^2 \cdot (X_2 - X_3)^2 \cdots (X_2 - X_n)^2 \cdots (X_{n-1} - X_n)^2 \in K_n \end{aligned}$$

*als **Diskriminante in n Variablen über K**.*
Ist $f \in K[X]$ ein normiertes Polynom vom Grad n mit Nullstellen $z_1, \dots, z_n$ (aus irgendeinem Zerfällungskörper von f), so nennen wir das Element

$$D_f := D_n(z_1, \dots, z_n) = \prod_{1\le i<j\le n} (z_i - z_j)^2$$

*die **Diskriminante von f**.*

Wir starten mit zwei einfachen Aussagen über die Diskriminante von f:

Lemma 33.4 *Wir verwenden die Bezeichnungen aus obiger Definition. Dann gelten:*

(a) *Genau dann gilt $D_f = 0$, wenn f in seinem Zerfällungskörper doppelte Nullstellen besitzt.*

(b) *Setzen wir $x_i := -z_i$ für alle $i \in \{1, \dots, n\}$, so gilt $D_f = D_n(x_1, \dots, x_n)$.*

Beweisskizze. Die Aussage in (a) folgt direkt aus der Definition von D_f.
Die Aussage in (b) gilt, weil sich die auftretenden Minuszeichen durch das Quadrieren in D_f wegheben. ■

Bemerkung 33.5 (a) Das Kriterium in (a) kann als Alternative zum ggT-Kriterium aus 23.22 benutzt werden. Für praktische Anwendungen ist das ggT-Kriterium allerdings meist deutlich besser geeignet.

(b) Die Aussage in (b) ist im Hinblick auf 33.1 interessant: Wir werden zeigen, dass D_n ein symmetrisches Polynom ist. Beim Übergang auf D_f können wir aber statt den z_i die x_i in D_n einsetzen und die einfachere Formel aus 33.1 (b) benutzen. ⋇

Wir zeigen nun, dass D_n ein symmetrisches Polynom ist. Im Beweis argumentieren wir nicht direkt mit D_n, sondern mit dem Polynom $\prod_{1\le i<j\le n}(X_i - X_j)$, das im Prinzip eine „Wurzel" aus D_n darstellt. Dieses Polynom wird uns im Diskriminantenkriterium wieder begegnen.

Satz 33.6 *Seien K ein Körper und $n \in \mathbb{N}$. Wir setzen*

$$d := \prod_{1\le i<j\le n} (X_i - X_j) \in K_n.$$

Dann gelten die folgenden Aussagen:

(a) *Es ist $d^2 = D_n$.*

(b) *Für jedes $\sigma \in S_n$ ist $\sigma \bullet d = \operatorname{sgn}(\sigma) \cdot d$.*

Beweis. Die Aussage in (a) ist klar.
Um (b) zu zeigen, untersuchen wir, wie eine beliebige Transposition $t := (a\,b) \in S_n$ mit $a < b$ das Polynom d verändert. Hierzu betrachten wir den Quotienten $q := \frac{t\bullet d}{d}$. Da das Anwenden von t ein Ringhomomorphismus ist, können wir t auf die einzelnen Faktoren von d anwenden. Wir können q also in der Form

$$q = \frac{t \bullet d}{d} = \frac{\prod_{1\le i<j\le n} t \bullet (X_i - X_j)}{\prod_{1\le i<j\le n}(X_i - X_j)}$$

darstellen. Wir diskutieren nun, wie sich die einzelnen Faktoren in q kürzen und betrachten hierzu einen beliebigen Faktor $p := X_i - X_j$ mit $i < j$ im Nenner von q.

Fall 1 Es gilt $|\{a,b\} \cap \{i,j\}| = 0$, d. h. weder i noch j stimmen mit a oder b überein.

Dann ist $t \bullet p = p$. Im Zähler und Nenner von q taucht p auf und kann gekürzt werden.

Fall 2 Es gilt $|\{a,b\} \cap \{i,j\}| = 2$, d. h. $a = i$ und $b = j$.

Dann gilt $t \bullet p = -p$. Im Zähler von q taucht $-p$ auf, im Nenner p. Nach dem Kürzen bleibt der Faktor -1 übrig.

Fall 3 Es gilt $|\{a,b\} \cap \{i,j\}| = 1$, d. h. genau eines der Elemente aus dem Träger von t stimmt mit genau einem Indizes i,j überein.

Angenommen, $t \bullet p$ taucht ebenfalls im Nenner von q auf. Dann finden sich im Nenner von q die Faktoren p und $t \bullet p$, im Zähler deren Bilder unter t, also die Faktoren $t \bullet p$ und

$$t \bullet (t \bullet p) = t^2 \bullet p = \mathrm{id} \bullet p = p.$$

Wir können dann in q durch p und $t \bullet p$ kürzen.

Angenommen, $t \bullet p$ taucht *nicht* im Nenner von q auf. Dann ist $(-1) \cdot t \bullet p$ ein Faktor im Nenner von q. Dann treten im Zähler von q die Bilder von p und $(-1) \cdot t \bullet p$ unter t auf, also die Faktoren $t \bullet p$ und

$$t \bullet ((-1) \cdot t \bullet p) = (-1) \cdot t^2 \bullet p = -p.$$

q hat also die Gestalt

$$q = \frac{(t \bullet p) \cdot (-p) \cdot \text{restliche Faktoren}}{p \cdot ((-1) \cdot t \bullet p) \cdot \text{restliche Faktoren}};$$

Kürzen durch $p \cdot (t \bullet p)$ liefert den Faktor $(-1)^2 = 1$.

Insgesamt folgt $q = -1$, denn in den Fällen 1 und 3 tritt der Faktor -1 nicht bzw. geradzahlig oft auf, im Fall 2, der genau einmal auftritt, entsteht der Faktor -1. Dies zeigt $t \bullet d = q \cdot d = -d$.
Sei nun $\sigma \in S_n$ eine beliebige Permutation. Nach 9.2 können wir $\sigma = t_1 \cdots t_k$ mit Transpositionen $t_i \in S_n$ schreiben. Dann gilt

$$\sigma \bullet d = t_1 \bullet t_2 \bullet \cdots \bullet t_k \bullet d \overset{\text{s.o.}}{=} (-1)^k \cdot d \overset{9.5}{=} \mathrm{sgn}(\sigma) \cdot d. \qquad \blacksquare$$

Wir erhalten die Symmetrie der Diskriminanten nun als einfache Folgerung:

Korollar 33.7 *Mit den Bezeichnungen aus 33.3 gilt: D_n ist ein symmetrisches Polynom.*

Beweis. Wir bezeichnen mit d das Polynom aus 33.6. Dann gilt für jedes beliebige $\sigma \in S_n$

$$\sigma \bullet D_n = \sigma \bullet d^2 = \sigma \bullet d \cdot \sigma \bullet d = \mathrm{sgn}(\sigma)^2 \cdot d^2 = \mathrm{sgn}(\sigma)^2 \cdot D_n.$$

Wegen $\mathrm{sgn}(\sigma) \in \{\pm 1\}$ folgt $\mathrm{sgn}(\sigma)^2 = 1$ und somit $\sigma \bullet D_n = D_n$ für alle $\sigma \in S_n$. $\blacksquare$

Bemerkung 33.8 (a) Das Korollar zeigt, dass die Diskriminante D_f eines Polynoms f wohldefiniert ist: Egal, auf welche Weise wir die Nullstellen von f durchnummerieren, der Wert von D_f ändert sich nicht.

(b) Eine analoge Aussage gilt jedoch nicht für das Polynom d aus 33.6: Setzen wir beispielsweise die Nullstellen $\pm\sqrt{2}$ des Polynoms $X^2 - 2 \in \mathbb{Q}[X]$ in d ein, so erhalten wir, je nach deren Nummerierung, die Werte $\pm 2\sqrt{2}$.

Allerdings folgt aus 33.6 (b), dass eine Umnummerierung der Nullstellen höchstens das Vorzeichen des Wertes von d ändern kann.

(c) Zusammen mit 33.1 folgt, dass wir die Diskriminante eines normierten Polynoms durch die Koeffizienten des Polynoms darstellen können. Man kann mit länglichen Rechnungen verifizieren, dass über jedem Körper K gilt:

- $X^2 + pX + q$ hat Diskriminante $p^2 - 4q$,
- $X^3 + aX^2 + bX + c$ hat Diskriminante $a^2b^2 - 4b^3 - 4a^3c + 18abc - 27c^2$.

Für Polynome größeren Grades werden die Diskriminantenformeln schnell sehr kompliziert und lang. Man nutzt dann andere Methoden zur Berechnung, siehe beispielsweise [Bos20, Korollar 10 auf S. 231]. ⁜

Das Diskriminantenkriterium

Mit diesen Vorarbeiten können wir nun das Diskriminantenkriterium formulieren und beweisen:

Satz 33.9 *Sei K ein Körper der Charakteristik ungleich Zwei. Sei $f \in K[X]$ ein normiertes Polynom vom Grad $n \in \mathbb{N}$, das in seinem Zerfällungskörper Z keine Mehrfachnullstellen besitze. Wir setzen $G := \mathrm{Gal}(f|K) \leq S_n$. Dann sind die beiden folgenden Aussagen äquivalent:*

(a) *G enthält nur gerade Permutationen, d.h. es gilt $G \leq A_n$.*

(b) *Die Diskriminante D_f von f ist ein Quadrat in K, d.h. es gibt ein Element $\delta \in K$ mit $\delta^2 = D_f$.*

Beweis. Wie in 33.6 setzen wir $d := \prod_{1 \leq i < j \leq n} (X_i - X_j) \in K_n$. Die Nullstellen von f bezeichnen wir mit $z_1, \ldots, z_n \in Z$ und setzen $\delta := d(z_1, \ldots, z_n)$. Als Produkt von Differenzen der z_i gilt $\delta \in Z$. Aus 33.6 folgen $\delta^2 = D_f$ und ⁉

$$g \bullet \delta = \mathrm{sgn}(g) \cdot \delta \qquad \text{für } g \in G. \tag{$\star$}$$

(a)$\Longrightarrow$(b) Wir zeigen, dass $\delta \in K$ ist. Wegen $\delta^2 = D_f$ ist die Aussage dann gezeigt.

Sei $g \in G$ beliebig. Da $g \in A_n$ eine gerade Permutation ist, folgt $g \bullet \delta = \delta$ nach $(\star)$. Das Element $\delta \in Z$ wird also von allen Galoisautomorphismen fixiert; daher ist $\delta \in \mathrm{Fix}(G) = K$.

(b)$\Longrightarrow$(a) Wir beweisen per Kontraposition. Sei $g \in G$ eine ungerade Permutation. Dann ist $g \bullet \delta = -\delta$ nach $(\star)$. Da $\delta \neq 0$ ist, folgt $\delta \neq -\delta$ aus der Charakteristik-Voraussetzung an K. Also ist $\delta \notin \mathrm{Fix}(G) = K$. ⁉

Da die Gleichung $X^2 = D_f$ genau die Lösungen $\pm\delta$ hat und keine der beiden in K liegt, ist gezeigt, dass D_f kein Quadrat in K ist. ■

Knobelfrage. Welcher Schluss würde im obigen Beweis nicht klappen, wenn f Mehrfachnullstellen hätte oder die Charakteristik von K gleich Zwei wäre? ⁉

Staatsexamensaufgabe (Teil (c) von H2018T3A2) *Sei $f = X^2 + pX + q$ ein Polynom mit rationalen Koeffizienten. Was können Sie über die Galoissche Gruppe G von f sagen, wenn die Diskriminante $\Delta_f := p^2 - 4q$ ein Quadrat in den rationalen Zahlen ist?*

Da f über $\mathbb{Q}$ definiert ist, ist die Charakteristik-Voraussetzung aus dem Diskriminantenkriterium erfüllt.
Falls zusätzlich $\Delta_f \neq 0$ ist, so liefert das Kriterium, dass G eine Untergruppe der A_2, also eine Untergruppe von $\{\mathrm{id}\}$ ist. Es folgt $G = \{\mathrm{id}\}$.
Falls $\Delta_f = 0$ ist, so besitzt f Mehrfachnullstellen. Daher haben f und $f' = 2X + p$ eine gemeinsame Nullstelle z, nämlich $z = -\frac{p}{2} \in \mathbb{Q}$. Diese ist eine doppelte Nullstelle von f, so dass $f = (X - z)^2$ gilt. Der Zerfällungskörper von f ist $\mathbb{Q}(z) = \mathbb{Q}$, was $G = \{\mathrm{id}\}$ zeigt. ⁉

Alternativ kann hier auch mit Hilfe der Mitternachtsformel argumentiert werden. Können Sie die Aufgabe auf diese Weise lösen? ⁂ ⁉

Staatsexamensaufgabe (H1979) *Bestimme die Galoissche Gruppe $G = \mathrm{Gal}(f|K)$ des Polynoms $f = X^3 - X + 1$ über den Körpern $K = \mathbb{F}_3, \mathbb{F}_7, \mathbb{Q}, \mathbb{Q}(\sqrt{-23})$.*

Wir benutzen die Formel aus 33.8 (c) und berechnen die Diskriminante von f zu

$$D_f = 4 - 27 = -23.$$

Die von uns benutzte Formel gilt körperunabhängig, so dass wir dieses Ergebnis in allen der folgenden Fälle benutzen können.

Fall $K = \mathbb{F}_3$ Hier ist $D_f = 1$ ein Quadrat. Die Voraussetzungen des Diskriminantenkriteriums sind erfüllt; es folgt $G \leq A_3 \cong C_3$, also $G \cong \{\mathrm{id}\}$ oder $G \cong C_3$.

Einsetzen der Elemente von K in f zeigt, dass f nullstellenfrei ist. Der Zerfällungskörper von f ist daher ein echter Oberkörper von K. Es gelten $|G| > 1$ und somit $G = A_3 \cong C_3$.

Fall $K = \mathbb{F}_7$ Hier ist $D_f = 5$. Testen aller Elemente aus K zeigt, dass D_f kein Quadrat in K ist. Die Voraussetzungen des Diskriminantenkriteriums sind erfüllt; es folgt, dass $G \leq S_3$ mindestens eine ungerade Permutation enthält.

f besitzt in K nur die Nullstelle $5 \in K$. Die Elemente aus G fixieren diese Nullstelle und operieren auf den anderen beiden transitiv. Damit folgt $G \cong S_2 \cong C_2$.

Fall $K = \mathbb{Q}$ Hier ist $D_f = -23$ kein Quadrat. Die Voraussetzungen des Diskriminantenkriteriums sind erfüllt; es folgt, dass $G \leq S_3$ mindestens eine ungerade Permutation enthält.

Mit 19.13 sehen wir, dass das Grad-3-Polynom f irreduzibel ist. Daher ist die Ordnung von G ein Vielfaches von Drei. Mit der Bedingung aus dem Diskriminantenkriterium folgt $G = S_3$. ⁉

Fall $K = \mathbb{Q}(\sqrt{-23})$ Hier ist D_f ein Quadrat. Die Voraussetzungen des Diskriminantenkriteriums sind erfüllt; es folgt $G \leq A_3$.

Wir zeigen, dass in K keine Nullstellen von f liegen: Sei z eine beliebige Nullstelle von f. Da f irreduzibel über $\mathbb{Q}$ ist, folgt $[\mathbb{Q}(z) : \mathbb{Q}] = 3$. Die Erweiterung $K|\mathbb{Q}$ hat aber Grad Zwei. Daher kann z nicht in K enthalten sein.

Als Grad-3-Polynom ohne Nullstelle ist f somit irreduzibel über K. Wie im vorherigen Fall sieht man, dass $|G|$ ein Vielfaches von Drei ist. Mit dem Diskriminantenkriterium ergibt sich $G = A_3 \cong C_3$. ⋇

34. Das Umkehrproblem der Galoistheorie

Worum geht es? Wir stellen zwei Varianten des Umkehrproblems vor: In der ersten Variante fragen wir, welche Gruppen überhaupt als Galoisgruppen realisierbar sind, in der zweiten Variante geben wir zusätzlich den Unterkörper der Galoiserweiterungen vor.
Die erste Variante des Umkehrproblems beantworten wir vollständig: Jede endliche Gruppe kommt als Galoisgruppe vor.
Wir realisieren die symmetrischen Gruppen S_p mit $p \in \mathbb{P}$ über $\mathbb{Q}$ und zeigen, dass jede endliche Gruppe als Galoisgruppe über einer endlichen Erweiterung von $\mathbb{Q}$ vorkommt.
Die Vorlesung beenden wir mit einer Vorstellung bekannter Resultate zum Umkehrproblem. ⋇

Wir haben das Umkehrproblem der Galoistheorie bereits auf Seite 208 angesprochen: Ist eine endliche Gruppe G gegeben, so fragt man, ob irgendeine Galoiserweiterung $L|K$ mit $G \cong \mathrm{Gal}(L|K)$ existiert. In diesem Fall sagt man auch, dass G **als Galoisgruppe realisierbar** ist.
In einer deutlich schwierigeren Variante des Umkehrproblems gibt man sich eine endliche Gruppe G *und* den Grundkörper K vor. Gefragt wird, ob ein Erweiterungskörper L von K existiert, so dass die Erweiterung $L|K$ galoissch mit $G \cong \mathrm{Gal}(L|K)$ ist. In diesem Fall sagt man auch, dass G **als Galoisgruppe über K realisierbar** ist. Diese Fragestellung ist offen und aktives Forschungsgebiet. Wir geben am Ende dieser Vorlesung einen knappen Überblick über bekannte Resultate.

Realisierung von S_n in beliebiger Charakteristik

Seien k ein beliebiger Körper, $n \in \mathbb{N}$ und $t_1, \dots, t_n$ paarweise verschiedene über k transzendente Elemente. Wir setzen $L := k(t_1, \dots, t_n)$.
Wir betrachten das Polynom $f := \prod_{i=1}^{n}(X - t_i)$. Nach Vieta gilt

$$f = \sum_{i=0}^{n} a_i X^i \qquad \text{mit} \qquad a_i = E_{n-i}(t_1, \dots, t_n),$$

wobei wir mit $E_i \in K_n$ die elementarsymmetrischen Polynome bezeichnen.
Wir setzen $K := k(a_0, a_1, \dots, a_n)$ und fassen f als Element von $K[X]$ auf. Dann gelten folgende Aussagen:

(a) L ist ein Oberkörper von K.

Die Koeffizienten a_i entstehen, indem man in die elementarsymmetrischen Polynome die Elemente t_i einsetzt. Die a_i sind also Summen von Produkten der t_i und damit in L enthalten. Dies zeigt $K \subseteq L$.

(b) L ist der Zerfällungskörper von f über K; die Erweiterung $L|K$ ist daher normal (und insbesondere algebraisch).

Die Nullstellen von f sind $t_1, \dots, t_n$. Daher ist

$$K(t_1, \dots, t_n) \underset{a_i \in k(t_1,\dots,t_n)}{=} k(a_0, \dots, a_n)(t_1, \dots, t_n) = k(a_0, \dots, a_n, t_1, \dots, t_n) = k(t_1, \dots, t_n) = L$$

der Zerfällungskörper von f über K.

(c) Die Erweiterung $L|K$ ist separabel, also zusammen mit (b) sogar galoissch.

Da $L|K$ nach (b) algebraisch ist, besitzt jedes der Elemente t_i ein Minimalpolynom $m_i \in K[X]$. Da $f(t_i) = 0$ ist, gilt $m_i \mid f$ für alle i. Nach Konstruktion besitzt f paarweise verschiedene Nullstellen. Damit haben auch die m_i paarweise verschiedene Nullstellen. Dies zeigt, dass alle t_i über K separabel sind. Mit 25.20 folgt die Separabilität der Erweiterung $L|K$.

(d) Es gilt $\mathrm{Gal}(L|K) \cong S_n$.

Die Gruppe S_n operiert auf $L = k(t_1, \dots, t_n)$ durch Vertauschen der Indizes der t_i. Jedes $\sigma \in S_n$ liefert auf diese Weise einen Körperautomorphismus $L \to L$, vgl. 32.6; verschiedene Elemente aus S_n liefern hierbei verschiedene Körperautomorphismen. ⁉

Die a_i als elementarsymmetrische Polynome in den t_i werden von diesen Automorphismen fixiert. Jedes Element aus S_n induziert daher einen K-Automorphismus von L.

Da L Zerfällungskörper des Grad-n-Polynoms f ist, gilt

$$\mathrm{Gal}(L|K) \cong \mathrm{Gal}(f|K) \leq S_n.$$

Obige Konstruktion liefert $n!$ viele Elemente aus $\mathrm{Gal}(L|K)$. Wegen $|S_n| = n!$ folgt hieraus

$$\mathrm{Gal}(L|K) \cong \mathrm{Gal}(f|K) = S_n.$$

Wir fassen unsere Ergebnisse als Satz zusammen:

Satz 34.1 *Seien k ein Körper, $n \in \mathbb{N}$ eine natürliche Zahl, $t_1, \dots, t_n$ paarweise verschiedene Transzendente über k und $E_1, \dots, E_n \in k_n$ die elementarsymmetrischen Polynome. Dann ist die Körpererweiterung*

$$k(t_1, \dots, t_n) | k(E_1(t_1, \dots, t_n), \dots, E_n(t_1, \dots, t_n))$$

galoissch. Ihre Galoisgruppe ist isomorph zur symmetrischen Gruppe S_n.

Beispiel 34.2 Seien k ein beliebiger Körper und a, b, c paarweise verschieden und transzendent über k. Dann ist die Erweiterung

$$k(a, b, c) | k(a + b + c, ab + ac + bc, abc)$$

galoissch. Ihre Galoisgruppe ist isomorph zu S_3. ⁂

Aus 34.1 folgt, dass jede endliche Gruppe als Galoisgruppe realisierbar ist:

Korollar 34.3 *Jede endliche Gruppe ist als Galoisgruppe realisierbar.*

Beweis. Sei G eine beliebige endliche Gruppe. Wir setzen $n := |G|$. Sei $L|K$ eine nach 34.1 existierende Galoiserweiterung mit $\mathrm{Gal}(L|K) \cong S_n$.
Nach Cayley 10.17 besitzt S_n eine Untergruppe, die isomorph zu G ist. Daher gibt es ein $U \leq \mathrm{Gal}(L|K)$ mit $U \cong G$. Setzen wir $Z := \mathrm{Fix}(U)$, so liefert der Hauptsatz der Galoistheorie

$$\mathrm{Gal}(L|Z) = U \cong G.$$

Damit ist die Aussage bewiesen. ■

Bemerkung 34.4 (a) Um die vorgegebene Gruppe G zu realisieren, sind wir mit einer passenden S_n-Erweiterung $L|K$ gestartet und haben den Unterkörper so lange vergrößert, bis die Galoisgruppe auf eine zu G isomorphe Gruppe geschrumpft ist.

Diese Technik steht uns in der zweiten Variante des Umkehrproblems nicht mehr zur Verfügung, da hier der Unterkörper der Erweiterung vorgegeben ist. Dies erklärt, warum das Umkehrproblem mit fixiertem Unterkörper so schwierig ist.

(b) An den Körper k, der in beiden obigen Resultaten vorkommt, werden keine Bedingungen gestellt. Insbesondere ist seine Charakteristik frei wählbar.

Dies zeigt, dass jede endliche Gruppe in jeder Charakteristik als Galoisgruppe realisierbar ist. ※

Realisierung von S_p mit $p \in \mathbb{P}$ über $\mathbb{Q}$

Um beliebige symmetrische Gruppen zu realisieren, haben wir im letzten Abschnitt komplizierte Körper mit vielen Transzendenten benötigt. In diesem Abschnitt realisieren wir symmetrische Gruppen mit einer anderen Technik. Hierdurch schaffen wir es, diese Gruppen über dem sehr einfachen Grundkörper $\mathbb{Q}$ zu realisieren. Ein Wermutstropfen ist, dass die Technik nur für die Gruppen S_p mit $p \in \mathbb{P}$ funktioniert.
Um die Technik anwenden zu können, benötigen wir zwei Hilfsaussagen:

Lemma 34.5 *Sei $n \geq 2$ eine natürliche Zahl. Dann gibt es ein normiertes irreduzibles Polynom $f \in \mathbb{Q}[X]$ vom Grad n, das genau zwei echt komplexe Nullstellen besitzt.*

Beweis. Wir betrachten das normierte Grad-n-Polynom

$$p := (X^2 + 4) \cdot \prod_{j=1}^{n-2} (X + 2^j) \in \mathbb{Q}[X].$$

Dieses besitzt die geforderte Nullstellenverteilung, ist aber für $n > 2$ reduzibel. Wir zeigen im Folgenden, dass eine leichte Abänderung des konstanten Koeffizienten von ⁉

p ein irreduzibles Polynom über $\mathbb{Q}$ mit passender Nullstellenverteilung liefert. Hierzu definieren wir für $s \in \mathbb{N}_0$ die Polynome

$$p_s := \frac{2}{3^s} + p = \frac{2}{3^s} + (X^2 + 4) \cdot \prod_{j=1}^{n-2} (X + 2^j) \in \mathbb{Q}[X].$$

Irreduzibilität aller p_s Für jedes $s \in \mathbb{N}_0$ ist das Polynom p_s irreduzibel über $\mathbb{Q}$. Wir zeigen dies mit Hilfe des Eisensteinkriteriums für die Primzahl $p = 2$.

Über $\mathbb{Q}$ ist die Irreduzibilität von p_s äquivalent zur Irreduzibilität von $P_s := 3^s \cdot p_s$, denn Multiplikation mit bzw. Division durch die Einheit $3^s \in \mathbb{Q}^\times$ verändert diese Eigenschaft nicht. P_s ist ein Element aus $\mathbb{Z}[X]$. Koeffizientenreduktion nach $\mathbb{Z}_2[X]$ liefert das Polynom $\overline{P_s}$ mit

$$\begin{aligned} \overline{P_s} &= \overline{2 + 3^s \cdot (X^2 + 4) \cdot \prod_{j=1}^{n-2} (X + 2^j)} = \overline{2} + \overline{3^s} \cdot (X^2 + \overline{4}) \cdot \prod_{j=1}^{n-2} (X + \overline{2^j}) \\ &= \overline{0} + \overline{1} \cdot X^2 \cdot \prod_{i=1}^{n-2} X = X^2 \cdot X^{n-2} = X^n. \end{aligned}$$

Dies zeigt, dass, bis auf den Leitkoeffizienten, alle Koeffizienten von P_s durch $p = 2$ teilbar sind.

Weiter ist p^2 kein Teiler des konstanten Koeffizienten $P_s(0)$, denn es gilt

$$P_s(0) = 2 + \underbrace{3^s \cdot 4 \cdot \prod_{j=1}^{n-2} 2^j}_{\text{Vielfaches von } p^2 = 4}.$$

P_s erfüllt also die Eisensteinbedingung bezüglich $p = 2$ und ist irreduzibel.

Nullstellenverteilung bleibt für große s erhalten Aus dem Satz über implizite Funktionen folgt, dass die Nullstellen der reellen Funktion

$$\mathbb{R} \to \mathbb{R}, \qquad x \mapsto \varepsilon + p(x)$$

stetig vom (hinreichend klein zu wählenden) Parameter $\varepsilon \in \mathbb{R}$ abhängen. Wählen wir daher ε klein genug, so unterscheiden sich die Nullstellen von $\varepsilon + p$ nur wenig von denen von p. Insbesondere besitzt dann $\varepsilon + p$ ebenfalls nur genau zwei echt komplexe Nullstellen.

Dieses Stetigkeitsargument greift auch beim normierten irreduziblen Polynom p_s, wenn wir $s \in \mathbb{N}_0$ hinreichend groß wählen. In diesem Fall haben wir lediglich den Parameter ε speziell in der Form $\frac{2}{3^s}$ gewählt und auf diese Weise zusätzlich Irreduzibilität erzwungen.

Insgesamt folgt, dass wir $f := p_s$ mit hinreichend großem $s \in \mathbb{N}_0$ setzen können. ■

Lemma 34.6 *Seien p eine Primzahl und U eine Untergruppe der symmetrischen Gruppe S_p. Weiter möge U eine Transposition und einen p-Zykel enthalten. Dann gilt $U = S_p$.*

Beweis. Wir zeigen, dass wir ohne Einschränkung davon ausgehen können, dass U die Transposition $(1\,2)$ und den p-Zykel $(1\,2\,\ldots\,p)$ enthält. Aus den Übungen wissen wir, dass diese beiden Elemente die volle S_p erzeugen. Es gilt daher → Übung

$$S_p = \langle (1\,2), (1\,2\,\ldots\,p) \rangle \leq U \leq S_p, \qquad \text{und somit} \qquad U = S_p.$$

Schritt 1: O. B. d. A. gilt $(1\,2) \in U$.

Nach Voraussetzung ist eine Transposition $(a\,b)$ in U enthalten. Wir benennen die Symbole $1, \ldots, p$ so um, dass a zu 1 und b zu 2 wird. Dann folgt $(1\,2) \in U$.

Schritt 2: U enthält einen p-Zykel der Form $(1\,2\,\ldots)$.

Nach Voraussetzung enthält U ein p-Zykel z. Sein Träger enthält alle Elemente aus $\{1, \ldots, p\}$. Wir können z daher so notieren, dass das Symbol 1 zu seinem „Startelement" wird, vgl. 8.8 (d). Dann hat z die Gestalt $z = (1\,a_2\,a_3\,\ldots a_p)$ mit paarweise verschiedenen $a_i \in \{2, 3, \ldots, p\}$.

Sei k dasjenige Element aus $\{2, \ldots, p\}$ mit $a_k = 2$. Dann gilt $z^{k-1} \bullet 1 = 2$. Weiter ist $\operatorname{ggT}(k-1, p) = 1$ und somit $\operatorname{ord}(z^{k-1}) = p$, vgl. 7.15 (c). Da p-Zykel die einzigen Elemente der Ordnung p in S_p sind, folgt, dass $z^{k-1} \in U$ ein p-Zykel der Form $(1\,2\,\ldots)$ ist.

Schritt 3: O. B. d. A. sind $(1\,2), (1\,2\,3\,\ldots\,p) \in U$.

Die beiden vorangegangenen Schritte zeigen $(1\,2), (1\,2\,b_3\,b_4\,\ldots\,b_p) \in U$; die paarweise verschiedenen b_i stammen hierbei aus der Menge $M := \{3, 4, \ldots, p\}$. Wie in Schritt 1 können wir die Elemente aus M so umbenennen, dass b_i zu i wird. Dann sind die beiden gesuchten Elemente in U enthalten, was den Beweis abschließt. ■

Knobelfrage. Wo wird in obigem Beweis benötigt, dass p eine Primzahl ist?

Wir können nun eine Bedingung angeben, unter der ein Polynom von Primzahlgrad die volle symmetrische Gruppe als Galoisgruppe besitzt:

Satz 34.7 *Seien K ein Unterkörper von $\mathbb{R}$ und $p \in \mathbb{P}$ eine Primzahl. Sei $f \in K[X]$ ein irreduzibles Polynom vom Grad p, das genau zwei echt komplexe Nullstellen besitzt. Dann ist durch f eine Galoiserweiterung gegeben, und es gilt $\operatorname{Gal}(f|K) = S_p$.*

Beweis. Aufgrund der Perfektheit des Charakteristik-Null-Körpers K liefert f eine Galoiserweiterung. Sei L der Zerfällungskörper von f. Die Irreduzibilität von f zeigt

$$p = \deg f \mid [L : K] = |\operatorname{Gal}(f|K)|.$$

Aus Sylow (oder Cauchy) folgt, dass $\operatorname{Gal}(f|K)$ ein Element der Ordnung p enthält. Weil $\operatorname{Gal}(f|K)$ eine Untergruppe der $S_{\deg f} = S_p$ ist, ist dieses Element ein p-Zykel.

Nach 28.8 ist die komplexe Konjugation ein Galoisautomorphismus der Erweiterung $L|K$. Dieser vertauscht die beiden echt-komplexen Nullstellen von f und fixiert die restlichen, entspricht also einer Transposition in der Gruppe $\mathrm{Gal}(f|K)$.
Damit ist gezeigt, dass die Gruppe $\mathrm{Gal}(f|K) \leq S_p$ eine Transposition und einen p-Zykel enthält. Mit 34.6 folgt $\mathrm{Gal}(f|K) = S_p$. ■

34.5 zeigt, dass über $\mathbb{Q}$ zu jedem $p \in \mathbb{P}$ Polynome existieren, die den Voraussetzungen des obigen Satzes genügen. Wir erhalten daher das folgende Realisierbarkeitsresultat:

Korollar 34.8 *Für jede Primzahl p ist die symmetrische Gruppe S_p über $\mathbb{Q}$ realisierbar.*

Ähnlich wie in 34.3 können wir aus diesem Korollar ein Realisierbarkeitsresultat für beliebige endliche Gruppen folgern:

Korollar 34.9 *Jede endliche Gruppe ist über einer endlichen Erweiterung von $\mathbb{Q}$ realisierbar.*

Beweis. Sei G eine beliebige endliche Gruppe. Wir setzen $n := |G|$. Sei $p \in \mathbb{P}$ eine Primzahl mit $p \geq n$. Dann besitzt S_p eine Untergruppe S mit $S \cong S_n$.
Mit Cayley finden wir eine Untergruppe $U \leq S$ mit $U \cong G$. Wir haben damit in S_p eine Untergruppe U gefunden, die isomorph zu G ist.
S_p ist nach 34.8 über $\mathbb{Q}$ realisierbar. Sei $L|\mathbb{Q}$ die zugehörige Galoiserweiterung. Wie in 34.3 konstruieren wir nun einen Zwischenkörper Z von $L|\mathbb{Q}$ mit $\mathrm{Gal}(L|Z) \cong G$.
Da $L|\mathbb{Q}$ als Galoiserweiterung endlich ist, ist der Zwischenkörper Z eine endliche Erweiterung von $\mathbb{Q}$. Wir haben die gegebene endliche Gruppe G damit über einer endlichen Erweiterung von $\mathbb{Q}$ realisiert. ■

Ein paar Anmerkungen zum Umkehrproblem

Die Frage, welche Gruppen G als Galoisgruppen über einem vorgegebenen Körper K auftreten, wird intensiv beforscht. Wir geben einen (unvollständigen) Überblick über bekannte Ergebnisse:

***K* ist algebraisch abgeschlossen** Dann existieren keine echten algebraischen Erweiterungen von K, vgl. 23.14. In diesem Fall gilt also zwingend $|G| = 1$.

$K = \mathbb{R}$ Die möglichen algebraischen Erweiterungen L von K sind $L = K$ oder $L = \mathbb{C}$. Im ersten Fall ist $G = \{\mathrm{id}\}$, im zweiten $G \cong C_2$.

$K = \mathbb{C}(t)$ mit über $\mathbb{C}$ transzendentem Element t Der *Riemannsche Existenzsatz* sagt aus, dass über K jede endliche Gruppe G realisierbar ist. Man beweist den Satz mit Hilfe von geometrischen Methoden, man kennt keinen rein algebraischen Beweis des Satzes.

$K = \mathbb{Q}$ Man vermutet, dass alle endlichen Gruppen über $\mathbb{Q}$ realisierbar sind. Man kann beweisen, dass die folgenden Gruppen G über $\mathbb{Q}$ realisierbar sind:

- G ist eine beliebige endliche abelsche Gruppe (Satz von Kronecker-Weber 31.7; wir haben den Beweis nur für endliche zyklische Gruppen geführt),
- $G \cong A_n$ oder $G \cong S_n$ für beliebige $n \in \mathbb{N}$; dieses Resultat geht auf Hilbert (1892) zurück (wir haben den Beweis nur für S_n und $n \in \mathbb{P}$ geführt),
- G ist eine beliebige p-Gruppe; dieses Resultat geht auf Schafarewitsch zurück,
- G ist eine beliebige endliche einfache sporadische Gruppe, allerdings nicht isomorph zur Mathieugruppe M_{23}.

Teil V.
Auflösbarkeit

Seit ungefähr 4 000 Jahren kann man die Nullstellen quadratischer Polynome explizit angeben: Für das Polynom $f = aX^2 + bX + c \in \mathbb{Q}[X]$ mit $a \neq 0$ sind sie in moderner Notation durch

$$z_{1,2} = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a} \qquad (\star)$$

gegeben. Eine naheliegende Frage ist, ob *ähnliche Nullstellen-Darstellungen* auch für Polynome höheren Grades möglich sind. In diesem Abschnitt werden wir die Frage mit galoistheoretischen Mitteln beantworten und mit dem *Satz von Abel-Ruffini* ein eher negatives Ergebnis geben.

Wir starten gruppentheoretisch und beschäftigen uns mit *auflösbaren Gruppen*. Diese stellen eine große und wichtige Gruppenklasse dar und können als Verallgemeinerung von abelschen und p-Gruppen aufgefasst werden. In auflösbaren Gruppen findet sich eine *Subnormalreihe*, die es ermöglicht, induktive Schlussweisen anzuwenden. Die *Faktoren* der Reihe sind abelsch. Mit Hilfe des *Korrespondenzsatzes* können viele „Zwischengruppen“ in der Subnormalreihe konstruiert werden, was für Beweise oft nützlich ist.

Danach gehen wir die Fragestellung körpertheoretisch an. Wir präzisieren, dass wir unter einer zu $(\star)$ ähnlichen Darstellung beliebig ineinander verschachtelte Wurzelausdrücke verstehen. Um diese algebraisch zu modellieren, führen wir *Radikale* und *Radikaltürme* ein. Ein wichtiges Hilfsmittel hierbei werden *reine Polynome* sein, die auch in vielen Aufgaben zur Galoistheorie vorkommen.

Für den Beweis des *Hauptsatzes über Auflösbarkeit durch Radikale* lernen wir einige fortgeschrittene Techniken der Galoistheorie kennen.
Hierzu gehören Resultate aus der *Kummer-Theorie*, mit denen man galoissche Erweiterungen mit zyklischer Galoisgruppe beschreiben kann.
Zudem beschäftigen wir uns mit dem *Transfer* von Körpererweiterungen. Wir zeigen, dass das *Translat* einer Galoiserweiterung galoissch bleibt und untersuchen seine Galoisgruppe im *Translationssatz*.

35. Kommutatorgruppen, auflösbare Gruppen

Worum geht es? Ausgehend vom *Kommutator* zweier Gruppenelemente konstruieren wir die (*höheren*) *Kommutatorgruppen*. Mit diesen Gruppen lässt sich die wichtige Klasse der *auflösbaren Gruppen* definieren. Wir beschäftigen uns weiter mit den sehr guten Vererbungseigenschaften dieser Gruppen. Dabei verwenden wir als Hilfsmittel den *Ersten Isomorphiesatz*. ⁜

Die Kommutatorgruppe

Sei G eine Gruppe. Für zwei Elemente $g, h \in G$ wird die Gleichung

$$gh = hg \cdot x$$

genau von $x = g^{-1}h^{-1}gh \in G$ gelöst. Man nennt dieses Element x den **Kommutator von g und h** und schreibt $[g,h]$ für ihn. Aus obiger Gleichung folgt, dass zwei Gruppenelemente g, h genau dann kommutieren, wenn ihr Kommutator $[g,h]$ mit dem Neutralen der Gruppe übereinstimmt.
Die im Folgenden definierte Untergruppe von G enthält alle Kommutatoren von G:

Definition 35.1 *Sei G eine Gruppe. Die von allen möglichen Kommutatoren von G erzeugte Untergruppe*

$$G' := \langle [g,h] : g,h \in G \rangle = \langle g^{-1}h^{-1}gh : g,h \in G \rangle$$

*nennen wir die **Kommutatorgruppe von G**.*
Sie ist die (per Mengeninklusion) kleinste Untergruppe von G, die alle Kommutatoren von G enthält. ⁉

Bemerkung 35.2 Das Produkt von Kommutatoren ist typischerweise kein Kommutator. Daher enthält die Kommutatorgruppe meist auch Elemente, die keine Kommutatoren sind: ⁉

Beispielsweise kann man zeigen, dass $\mathrm{SL}(2,\mathbb{R}) = \mathrm{SL}(2,\mathbb{R})'$ gilt, dass aber das Element $\left(\begin{smallmatrix} -1 & \\ & -1 \end{smallmatrix}\right) \in \mathrm{SL}(2,\mathbb{R})'$ kein Kommutator von Elementen aus $\mathrm{SL}(2,\mathbb{R})$ ist. ⁜ → Übung

Kommutatorgruppen sind Normalteiler:

Satz 35.3 *Sei G eine Gruppe. Dann ist $G' \trianglelefteq G$.*

Beweis. Wir bezeichnen mit $M := \{[x,y] : x,y \in G\}$ die Menge der Kommutatoren von G. Sei $g \in G$ beliebig gewählt. Konjugation mit g liefert dann den Automorphismus

$$k : G \to G, \qquad x \mapsto gxg^{-1}.$$

Schritt 1: Wir zeigen, dass M invariant unter k ist, dass also $k(M) \subseteq M$ ist.

Sei hierzu $m = [x,y] \in M$ ein beliebiges Element aus M Dann gilt

$$k(m) = k(x^{-1}y^{-1}xy) \overset{k \text{ ist Autom.}}{=} k(x)^{-1}k(y)^{-1}k(x)k(y) = [k(x),k(y)] \in M.$$

Schritt 2 Wir zeigen, dass G' invariant unter k ist, dass also $k(G') \subseteq G'$ ist.

Sei hierzu ein beliebiges Element $h \in G'$ gegeben. Da G' von den Elementen aus M erzeugt wird, gibt es $m_1, \dots, m_n \in M$ und $e_1, \dots, e_n \in \{\pm 1\}$ mit $h = \prod_{i=1}^{n} m_i^{e_i}$, vgl. 2.13. Mit der Automorphie von k ergibt sich

$$k(h) = \prod_{i=1}^{n} k(m_i)^{e_i}.$$

Wegen Schritt 1 ist $k(m_i) \in M$ für alle i. Hieraus folgt, dass $k(h) \in G'$ gilt.

Da obige Aussagen für beliebiges $g \in G$, also für alle möglichen Konjugationen gelten, folgt die Normalität von G' mit 5.3 (c). ■

Bemerkung 35.4 Die Schlussweise im obigen Beweis lässt sich wie folgt zusammenfassen:

$$\text{für alle } g \in G \text{ ist } gMg^{-1} \subseteq M \Longrightarrow \langle M \rangle \trianglelefteq G.$$

Sie kann in vielen Fällen zum Normalitätsnachweis benutzt werden. Beispielsweise folgt mit ihrer Hilfe sofort, dass die Gruppen $\langle g \mid \operatorname{ord}(g) = 2 \rangle$ bzw. $\langle g^2 \mid g \in G \rangle$ normal in G sind. ⁜

Die Kommutatorgruppe kann man als „Maß“ für die Nicht-Kommutativität einer Gruppe G auffassen: Kommutieren nur wenige Elemente von G miteinander, so enthält G viele Kommutatoren, die ungleich Eins sind. G' wird also von vielen Elementen erzeugt und ist ein „großer“ Normalteiler von G.
Diese heuristischen Überlegungen gießt der folgende Satz in eine mathematische Form:

Satz 35.5 *Seien G eine Gruppe und $N \trianglelefteq G$ ein Normalteiler von G. Dann sind äquivalent:*

(a) *Die Faktorgruppe G/N ist abelsch.*

(b) *N enthält alle Kommutatoren aus G, d. h. es ist $G' \leq N$.*

Dies zeigt insbesondere, dass G/G' eine abelsche Gruppe ist.
Die Kommutatorgruppe G' ist also der (per Mengeninklusion) kleinste Normalteiler, der eine abelsche Faktorgruppe von G liefert.

Beweis.

(b)$\Longrightarrow$(a) Sei $G' \leq N$. Dann gilt für alle $g, h \in G$

$$hN \cdot gN = hgN \overset{4.1\,(e)}{=} hg \cdot [g,h]N = ghN = gN \cdot hN.$$

Also ist G/N abelsch.

(a)$\Longrightarrow$(b) Sei nun G/N abelsch. Dann gilt für beliebige $g, h \in G$, dass $g^{-1}h^{-1}ghN = N$ ist, also dass $[g,h] \in N$ gilt. Somit enthält N alle Kommutatoren von G und damit auch ihr Erzeugnis, die Kommutatorgruppe G' von G. ■

Beispiel 35.6 (a) Ist G eine abelsche Gruppe, so ist $G' = \{1\}$.

Dies kann man direkt nachrechnen ($[g,h] = 1$ für beliebige $g, h \in G$, daher ist $G' = \langle 1 \rangle = \{1\}$) oder aus obigem Satz ableiten: Da Faktorgruppen abelscher Gruppen abelsch sind, ist $G/\{1\}$ abelsch. Also folgt $G' \leq \{1\}$ und somit $G' = \{1\}$.

(b) Sei G eine einfache, nicht-abelsche Gruppe. Dann gilt $G' = G$. Gruppen, die mit ihrer Kommutatorgruppe übereinstimmen, nennt man auch **perfekte Gruppen**. Einfache, nicht-abelsche Gruppen sind also perfekt.

Denn: Da G einfach und G' ein Normalteiler von G ist, folgt $G' \in \{\{1\}, G\}$. Da $G \cong G/\{1\}$ ist und G als nicht-abelsch vorausgesetzt wurde, ist $G' \neq \{1\}$. Somit muss $G' = G$ gelten.

Hieraus folgt beispielsweise, dass A_n für $n \geq 5$ perfekt ist.

(c) Wir bestimmen die Kommutatorgruppe von S_n für $n \geq 5$: Da S_n nicht abelsch ist, ist $S_n' \neq \{1\}$. Da $S_n/A_n \cong C_2$ ist, gilt $S_n' \leq A_n$. Zusammen mit der Klassifikation der Normalteiler der S_n aus 9.16 ergibt sich $S_n' = A_n$.

Mit ähnlichen Argumenten sieht man $S_4' = A_4$ und $A_4' = V_4$, wobei wir mit V_4 die Kleinsche Vierergruppe bezeichnen, vgl. 9.11. ⁉

(d) Seien p eine Primzahl und G eine Gruppe der Ordnung $p^r > 1$. Dann ist G' eine echte Untergruppe von G. Nicht-triviale p-Gruppen sind also nicht perfekt.

Denn: Nach 12.1 besitzt G einen Normalteiler N der Ordnung p^{r-1}. Die Faktorgruppe G/N hat Ordnung $p \in \mathbb{P}$, ist somit zyklisch und insbesondere abelsch. Daher ist $G' \leq N < G$. ⁂

Höhere Kommutatorgruppen, Auflösbarkeit

Die Grundidee hinter dem Begriff der Auflösbarkeit einer Gruppe besteht darin, die Kommutatorgruppen-Bildung zu iterieren, also Kommutatorgruppen von Kommutatorgruppen von Kommutatorgruppen usw. zu betrachten:

Definition 35.7 *Sei G eine Gruppe. Wir setzen $G^{(0)} := G$ und definieren rekursiv*

$$G^{(i+1)} := (G^{(i)})' \qquad \text{für } i \in \mathbb{N}_0.$$

*Man nennt die Gruppen $G^{(i)}$ für $i \geq 0$ die **höheren Kommutatorgruppen von G**.*
Es gelten $G^{(1)} = G'$ sowie $G^{(2)} = (G')'$, $G^{(3)} = \left((G')'\right)'$, etc.

Die Folge der Kommutatorgruppen bildet eine absteigende Kette, d. h. es gilt

$$G = G^{(0)} \geq G' = G^{(1)} \geq G^{(2)} \geq G^{(3)} \geq G^{(4)} \geq \cdots$$

Gruppentheoretisch ist vor allem der Fall interessant, bei dem diese Kette die triviale Gruppe $\{1\}$ erreicht. Man gibt ihm einen speziellen Namen:

Definition 35.8 *Wir nennen eine Gruppe G **auflösbar**, wenn sie endliche Ordnung besitzt und ein $k \in \mathbb{N}$ existiert, so dass $G^{(k)} = \{1\}$ ist.*
Beachten Sie, dass dann auch $G^{(n)} = \{1\}$ für alle $n \geq k$ gilt.

Beispiel 35.9 (a) Jede endliche abelsche Gruppe G ist auflösbar, denn es ist $G^{(1)} = \{1\}$.

(b) Jede p-Gruppe ist auflösbar, denn sind p eine Primzahl und G eine Gruppe der Ordnung p^n, so folgt aus 35.6 (d), dass $G^{(n)} = \{1\}$ ist. ⁉

(c) Aus 35.6 (c) folgt, dass die Gruppen S_n und A_n genau für $n \leq 4$ auflösbar sind.

(d) Endliche einfache Gruppen sind genau dann auflösbar, wenn sie abelsch sind, also wenn sie zyklisch von Primzahlordnung sind. Dies folgt aus 35.6 (b) und der Aussage in (a).

(e) Nach einem Satz von Burnside sind alle Gruppen der Ordnung $p^a q^b$ mit Primzahlen p, q und Exponenten $a, b \in \mathbb{N}_0$ auflösbar.

Hieraus folgt mit (d), dass die Ordnung einer nicht-abelschen einfachen Gruppe von mindestens drei verschiedenen Primzahlen geteilt werden muss.

Der Satz von Feit-Thompson sagt aus, dass alle endlichen Gruppen mit ungerader Ordnung auflösbar sind. Eine der obigen Primzahlen ist also Zwei, was zeigt, dass die Ordnung einer nicht-abelschen einfachen Gruppe stets gerade ist.

(f) Direkt aus 35.7 folgt, dass $(G^{(i)})^{(j)} = G^{(i+j)}$ für beliebige $i, j \in \mathbb{N}_0$ gilt. ⁂

Wir wollen ein Analogon zu 7.20 beweisen und zeigen, dass auflösbare Gruppen gute Vererbungseigenschaften besitzen. Hierzu benötigen wir einige Vorbereitungen:

Lemma 35.10

(a) *Seien G eine Gruppe und $U \leq G$ eine Untergruppe von G. Dann gilt $U^{(i)} \leq G^{(i)}$ für alle $i \geq 0$.*

(b) *Seien G, H Gruppen und $\varphi : G \to H$ ein Homomorphismus. Dann gilt $\varphi(G^{(i)}) = \varphi(G)^{(i)}$ für alle $i \geq 0$.*

Beweisskizze. Beide Aussagen lassen sich per Induktion zeigen. Wir stellen nur den Induktionsanfang vor. Der Induktionsschluss entspricht beinahe wörtlich dem Induktionsanfang.

zu (a) Wegen $U \leq G$ ist jeder Kommutator $[g,h] = g^{-1}h^{-1}gh$ mit $g, h \in U$ auch ein Element aus G. Dies zeigt $\langle [g,h] : g,h \in U \rangle \leq \langle [g,h] : g,h \in G \rangle$, also $U' \leq G'$.

zu (b) Wir schränken den Zielbereich von φ ein und fassen φ ab jetzt als Epimorphismus $\varphi : G \to \varphi(G)$ auf.
Man rechnet schnell nach, dass $\varphi([g,h]) = [\varphi(g), \varphi(h)]$ für beliebige $g, h \in G$ gilt.
Dies zeigt, dass Bilder von Kommutatoren aus G dann Kommutatoren in $\varphi(G)$

sind und dass sich, umgekehrt, jeder Kommutator von $\varphi(G)$ als Bild eines Kommutators aus G schreiben lässt. Daher ist

$$\varphi\big(\langle [g,h] : g,h \in G\rangle\big) = \big\langle [\varphi(g),\varphi(h)] : g,h \in G\big\rangle = \langle [x,y] : x,y \in \varphi(G)\rangle.$$

Dies liefert direkt die zu zeigende Aussage $\varphi(G)' = \varphi(G')$. ■

Satz 35.11 *Untergruppen, Faktorgruppen und homomorphe Bilder auflösbarer Gruppen sind auflösbar.*

Beweis. Sei G eine auflösbare Gruppe. Mit k bezeichnen wir die dann existierende natürliche Zahl mit $G^{(k)} = \{1\}$.

Untergruppen Sei $U \leq G$ eine Untergruppe von G. Dann folgt aus 35.10 (a), dass $U^{(k)} \leq G^{(k)} = \{1\}$ ist. Dies zeigt $U^{(k)} = \{1\}$ und somit die Auflösbarkeit von U.

homomorphe Bilder Sei $\varphi : G \to H$ ein Homomorphismus. Dann ist nach 35.10 (b)

$$\varphi(G)^{(k)} = \varphi(G^{(k)}) = \varphi(\{1\}) = \{1\}.$$

Also ist $\varphi(G)$ auflösbar.

Faktorgruppen Sei $N \trianglelefteq G$ ein Normalteiler von G. Wir bezeichnen mit

$$\varphi : G \to G/N, \qquad g \mapsto gN$$

den kanonischen Epimorphismus von G auf G/N. Dann gilt $G/N = \varphi(G)$. Also ist G/N ein homomorphes Bild von G und daher auflösbar. ■

Die Richtung „(b)$\Longrightarrow$(a)“ des folgenden Resultats wird in der Praxis häufig benutzt; sie ist das wohl wichtigste Kriterium zum Nachweis der Auflösbarkeit.

Satz 35.12 *Seien G eine Gruppe und N ein Normalteiler von G. Dann sind äquivalent:*

(a) *Die Gruppe G ist auflösbar.*

(b) *Die Gruppen N und G/N sind auflösbar.*

Beweis. Die Aussage „(a)$\Longrightarrow$(b)“ folgt direkt aus 35.11. Wir zeigen die Rückrichtung „(b)$\Longrightarrow$(a)“. Seien hierzu N und G/N auflösbar. Dann gibt es natürliche Zahlen $a, b \in \mathbb{N}$, so dass $N^{(a)} = \{1\}$ und $(G/N)^{(b)} = \{\overline{1}\} = \{N\}$ gelten. Wir zeigen, dass $G^{(a+b)} = \{1\}$ ist. Es sei

$$\varphi : G \to G/N, \qquad g \mapsto gN$$

der kanonische Epimorphismus von G auf G/N. Dann gilt

$$\{\overline{1}\} = \{N\} = (G/N)^{(b)} = \varphi(G)^{(b)} \overset{35.10\,(b)}{=} \varphi(G^{(b)}).$$

Dies zeigt, dass jedes Element der Gruppe $G^{(b)}$ im Kern von φ liegen muss, also dass $G^{(b)} \leq \ker\varphi = N$ gilt. Aus 35.10 (a) folgt $(G^{(b)})^{(a)} \leq N^{(a)} = \{1\}$. Insgesamt haben wir also

$$G^{(a+b)} \overset{35.9\,(f)}{=} (G^{(b)})^{(a)} = \{1\},$$

was die Auflösbarkeit von G zeigt. ■

Beispiel 35.13 (a) Jedes semidirekte Produkt $N \rtimes_\varphi H$ zweier auflösbarer Gruppen N, H ist auflösbar, denn es ist $(N \rtimes_\varphi H)/(N \rtimes_\varphi \{1\}) \cong H$.
Hieraus folgt, dass auch direkte Produkte auflösbarer Gruppen auflösbar sind.

(b) Ist G eine Gruppe der Ordnung $p^a q^b$ mit Primzahlen $p, q \in \mathbb{P}$ und $a, b \in \mathbb{N}_0$ und ist die q-Sylowgruppe Q von G normal, so ist G auflösbar.
Dies folgt, weil der Normalteiler Q als q-Gruppe und die Faktorgruppe G/Q als p-Gruppe nach 35.9 (b) auflösbar sind.
Diese Aussage ist ein (sehr einfach zu beweisender) Spezialfall des Satzes von Burnside aus 35.9 (e).

(c) Besitzt eine Gruppe G eine nicht-auflösbare Untergruppe, so ist G nicht auflösbar.
Dies ist die Kontraposition der Untergruppen-Aussage in 35.11. ⁜

Wir wollen Teil (a) des obigen Beispiels noch etwas verallgemeinern und zeigen, dass das Komplexprodukt eines auflösbaren Normalteilers und einer auflösbaren Untergruppe auflösbar ist (im Beispiel oben fordern wir zusätzlich noch, dass sich beide Gruppen trivial schneiden).
Hierzu benötigen wir ein wichtiges Resultat, das in der Literatur auch als *Erster Isomorphiesatz* bekannt ist und auf Emmy Noether zurückgeht:

Satz 35.14 (Erster Isomorphiesatz) *Seien G eine Gruppe, $N \trianglelefteq G$ ein Normalteiler von G und $U \leq G$ eine Untergruppe von G. Dann gelten die folgenden Aussagen:*

(a) *Die Abbildung*

$$\varphi : U \to G/N, \qquad u \mapsto uN$$

ist ein Homomorphismus. Es gelten $\ker\varphi = U \cap N$ *sowie* $U \cap N \trianglelefteq U$ *und* $\varphi(U) = UN/N$.

(b) *Per Homomorphiesatz liefert φ den Gruppenisomorphismus*

$$U/(U \cap N) \to UN/N, \qquad u(U \cap N) \mapsto uN.$$

Die Gruppen $U/(U \cap N)$ und UN/N sind also isomorph zueinander.

Beweis.

zu (a) Die Abbildung φ entsteht durch Einschränkung des kanonischen Epimorphismus $G \to G/N$ auf U. Dies zeigt die Homomorphie von G. Es ist

$$\ker\varphi = \{u \in U \mid uN = N\} \overset{4.1\,(e)}{=} \{u \in U \mid u \in N\} = U \cap N.$$

Da Kerne Normalteiler sind, folgt $U \cap N \trianglelefteq U$. Weiter erhalten wir

$$\varphi(U) = \{uN \mid u \in U\} \overset{4.1\,(e)}{=} \{unN \mid u \in U, n \in N\} = \{gN \mid g \in UN\} = UN/N.$$

(b) folgt, indem man den Zielbereich von φ auf UN/N verkleinert und dann den Homomorphiesatz anwendet. ■

Bemerkung 35.15 (a) Wenn man vom Ersten Isomorphiesatz spricht, meint man meist nur die Aussage

$$UN/N \cong U/(U \cap N)$$

aus Teil (b). Diese kann man sich merken, indem man die Ordnung von UN/N ausrechnet und dann die Betragsstriche weglässt:

$$|UN/N| \overset{\text{Lagrange}}{=} \frac{1}{|N|} \cdot |UN| \overset{13.3}{=} \frac{1}{|N|} \cdot \frac{|U| \cdot |N|}{|U \cap N|} = \frac{|U|}{|U \cap N|}.$$

(b) Wir wissen aus 13.6 (a), dass UN eine Untergruppe von G ist. Weiter ist klar, dass N ein Normalteiler von UN ist. Der Ausdruck UN/N bezeichnet die Faktorgruppe der Gruppe UN nach dem Normalteiler N, also die Menge der Nebenklassen von N in UN. Für $u, u' \in U$ und $n, n' \in N$ gilt $unN \cdot u'n'N = unu'n'N$. ⁉

(c) UN/N ist eine Untergruppe der Faktorgruppe G/N. ⁂ ⁉

Knobelfrage. Es gilt $UN/N = \{unN \mid u \in U, n \in N\} = \{uN \mid u \in U\}$. Das N im „Zähler“ wird ja scheinbar gar nicht gebraucht. Warum schreibt man also nicht nur U/N? ⁉

Korollar 35.16 *Seien G eine Gruppe, $N \trianglelefteq G$ und $U \leq G$.*
Sind N und U auflösbar, so ist das Komplexprodukt UN eine auflösbare Untergruppe von G.

Beweis. Wir zeigen die Auflösbarkeit von UN mit Hilfe von 35.12, indem wir nachweisen, dass N und UN/N auflösbar sind.
N ist nach Voraussetzung auflösbar. Nach dem Ersten Isomorphiesatz ist UN/N isomorph zu einer Faktorgruppe von U und daher nach 35.11 auflösbar. ■

36. Korrespondenzsatz, Auflösungen

Worum geht es? Wir lernen *Subnormalreihen* kennen und sehen, dass die höheren Kommutatorgruppen ein Beispiel für eine solche Reihe bilden. Wir charakterisieren anschließend Auflösbarkeit durch Subnormalreihen. An einigen Stellen benötigen wir hierzu den *Korrespondenzsatz*. Dieser übersetzt zwischen Aussagen über die Untergruppen einer Faktorgruppe und Aussagen über Untergruppen der Ausgangsgruppe hin und her. Er ist ein wichtiges Hilfsmittel in der Theorie auflösbarer Gruppen. ⁜

Korrespondenzsatz

Der Korrespondenzsatz ist ein wichtiges Hilfsmittel der Gruppentheorie. Er übersetzt Aussagen über gewisse Untergruppen einer Gruppe G in Aussagen über die Untergruppenstruktur von Faktorgruppen von G.
Ein großer Teil seiner Aussagen folgt direkt aus den grundlegenden Eigenschaften von Homomorphismen. Diese sind uns bereits in 6.4 begegnet.

Sei $\varphi : G \to H$ ein Gruppenepimorphismus mit Kern N. Ist U eine Untergruppe von G, so ist $\varphi(U)$ eine Untergruppe von H.
Umgekehrt folgt aus $V \leq H$, dass das Urbild $\varphi^{-1}(V) = \{g \in G \mid \varphi(g) \in V\}$ eine Untergruppe von G ist und dass $N \leq \varphi^{-1}(V)$ gilt. ⁉
φ „übersetzt“ also Untergruppen von G in Untergruppen von H und, umgekehrt, Untergruppen von H in Untergruppen von G, die N enthalten. Dies ist die wesentliche Idee hinter dem Korrespondenzsatz.

Satz 36.1 (Korrespondenzsatz für Epimorphismen) *Seien $\varphi : G \to H$ ein Gruppenepimorphismus mit Kern $N := \ker \varphi$. Wir bezeichnen mit $\mathcal{H}$ die Menge der Untergruppen von H und mit $\mathcal{G}$ die Menge der Untergruppen von G, die Obergruppen von N sind, d. h. es sei*

$$\mathcal{G} := \{U \mid N \leq U \leq G\} \qquad \text{sowie} \qquad \mathcal{H} := \{V \mid V \leq H\}.$$

Dann gelten die folgenden Aussagen:

(a) *Die durch φ induzierte Abbildung $f : \mathcal{G} \to \mathcal{H}, \quad U \mapsto \varphi(U)$ ist bijektiv.*
Ihre Umkehrabbildung ist $f^{-1} : \mathcal{H} \to \mathcal{G}, \quad U \mapsto \varphi^{-1}(U) = \{g \in G \mid \varphi(g) \in U\}$.

(b) *Seien $U, V \in \mathcal{G}$. Dann ist $V \leq U$ genau dann, wenn $f(V) \leq f(U)$ gilt. In diesem Fall gilt zudem $[U : V] = [f(U) : f(V)]$.*
Die Korrespondenz aus (a) überträgt also Untergruppenbeziehungen und erhält Indizes.

(c) *Seien $U, V \in \mathcal{G}$. Dann ist $V \trianglelefteq U$ genau dann, wenn $f(V) \trianglelefteq f(U)$ gilt.*
Die Korrespondenz aus (a) überträgt also Normalität.

Beweisskizze. Ein kompletter Beweis des Korrespondenzsatzes ist lang und benutzt an vielen Stellen recht einfache „Nachrechenargumente“. Wir stellen Beweis des Satzes hier daher nur skizzenhaft dar.

zu (a) Die Vorbemerkung zum Satz zeigt, dass f und f^{-1} Abbildungen sind. Die restlichen Behauptungen folgen durch Nachweis der Gleichungen

$$f^{-1} \circ f = \mathrm{id}_{\mathcal{G}} \qquad \text{und} \qquad f \circ f^{-1} = \mathrm{id}_{\mathcal{H}}\,.$$

Wir zeigen nur die linke Gleichheit. Sei $U \in \mathcal{G}$ beliebig vorgegeben. Es ist dann $f^{-1}(f(U)) = U$, also $\varphi^{-1}(\varphi(U)) = U$ zu zeigen.

Die „$\supseteq$"-Aussage lässt sich einfach nachrechnen.

Zum Nachweis von „$\subseteq$" betrachten wir ein beliebiges $x \in \varphi^{-1}(\varphi(U))$. Dann ist $\varphi(x) \in \varphi(U)$. Es gibt also $u \in U$ mit $\varphi(x) = \varphi(u)$. Mit der Homomorphie von φ folgt $\varphi(xu^{-1}) = 1$, also $xu^{-1} \in \ker\varphi = N$. Somit finden wir $n \in N$, so dass $x = nu$ gilt. Da $N \leq U$ ist, ist x als Produkt zweier Elemente aus U ein Element aus U.

zu (b) Die Aussage $V \leq U \iff f(V) \leq f(U)$ ist klar. ?

Seien nun $U, V \in \mathcal{G}$ mit $V \leq U$. Dann existieren eine Indexmenge I und Elemente $u_i \in U$ mit $i \in I$, so dass $U = \dot{\bigcup}_{i\in I} u_i V$ ist. Es gilt $[U : V] = |I| \in \mathbb{N} \cup \{\infty\}$. Wir zeigen nun, dass $f(U) = \dot{\bigcup}_{i\in I} \varphi(u_i)f(V)$ gilt. Dann erhalten wir $[f(U) : f(V)] = |I|$ und somit die Gleichheit beider Indizes.

Aussage über Vereinigungsmenge Die Aussage $f(U) = \bigcup_{i\in I} \varphi(u_i)f(V)$ lässt sich leicht nachrechnen. Hier geht praktisch nur die Homomorphie von φ ein.

paarweise Disjunktheit Seien $i, j \in I$ mit $i \neq j$. Wir zeigen, dass die Mengen $\varphi(u_i)f(V)$ und $\varphi(u_j)f(V)$ disjunkt sind.
Angenommen, es gäbe ein Element x im Schnitt. Dann gibt es $v, w \in V$, so dass

$$\varphi(u_i)\varphi(v) = x = \varphi(u_j)\varphi(w) \qquad \text{und daher} \qquad \varphi(w^{-1}u_j^{-1}u_i v) = 1$$

gelten. Wegen $\ker\varphi = N$ ist dann $w^{-1}u_j^{-1}u_i v \in N$. Wir erhalten hieraus

$$u_i \in u_j w N v^{-1} \overset{N\leq V}{\subseteq} u_j w V v^{-1} \overset{w,v\in V}{=} u_j V.$$

Dies ist ein Widerspruch, denn die Nebenklassen $u_i V$ und $u_j V$ sind disjunkt.

(c) beweist man durch Nachrechnen. Für die Richtung „$V \trianglelefteq U \Longrightarrow f(V) \trianglelefteq f(U)$" wird die Surjektivität von φ benötigt, vgl. die Knobelfrage auf Seite 6.5. ■

Bemerkung 36.2 (a) Beachten Sie die unterschiedlichen Definitionen der Mengen $\mathcal{G}$ und $\mathcal{H}$. Diese haben zur Folge, dass der Korrespondenzsatz Aussagen über *alle* Untergruppen der Gruppe H, aber nur über *gewisse* Untergruppen der Gruppe G liefert:
Der Korrespondenzsatz ist „blind" für alle Untergruppen von G, die keine Obergruppen von N sind.

(b) Wie Sie 36.1 beispielhaft entnehmen können, ist eine mathematisch präzise Formulierung des Korrespondenzsatzes länglich und schwerfällig. Die Aussage des Satzes wird klarer, wenn man zu Untergruppendiagrammen übergeht: 36.1 sagt dann aus, dass das Untergruppendiagramm von H und der Teil des Untergruppendiagramms von G, der über N liegt, gleich aussehen. Alle Indizes und alle Normalitäten übertragen sich.

(c) Mit praktisch wörtlich demselben Beweis lässt sich 36.1 auch für Ringe formulieren. Hier ist φ dann ein Ringepimorphismus, die Aussagen in den Teilen (a) und (b) sagen dann aus, dass Ideale mit Idealen bzw. Unterringe mit Unterringen korrespondieren.
Teil (c) ist im Ringkontext uninteressant, da die additive Gruppe von Ringen kommutativ und somit jedes Ideal bzw. jeder Unterring additiv gesehen automatisch ein Normalteiler im Ring ist. ⋇

Besonders häufig wählt man in 36.1 für φ den kanonischen Epimorphismus. Man hat also eine Gruppe G und einen Normalteiler $N \trianglelefteq G$ gegeben und betrachtet den Epimorphismus $\varphi : G \to G/N$ mit $g \mapsto gN$. Wenn man von *dem* Korrespondenzsatz spricht, ist meist dieser Spezialfall gemeint:

Korollar 36.3 (Korrespondenzsatz) *Seien G eine Gruppe und $N \trianglelefteq G$ ein Normalteiler von G. Wir betrachten den kanonischen Epimorphismus $\varphi : G \to G/N$ mit Kern N und setzen*

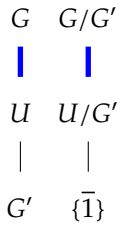
$$\mathcal{G} := \{U \mid N \leq U \leq G\} \qquad \textit{sowie} \qquad \mathcal{H} := \{V \mid V \leq H\}.$$

Dann sind die Abbildungen

$$f : \mathcal{G} \to \mathcal{H}, \quad U \mapsto U/N \qquad \textit{und} \qquad f^{-1} : \mathcal{H} \to \mathcal{G}, \quad V/N \mapsto V$$

bijektiv zueinander. Diese Korrespondenz überträgt Untergruppenbeziehungen und Normalität und erhält Indizes.

Beispiel 36.4 (a) Seien G eine Gruppe und U eine Untergruppe von G mit $G' \leq U$. Dann ist U sogar ein Normalteiler von G:



Wir betrachten den kanonischen Epimorphismus $G \to G/G'$ und wenden 36.3 an. Dann liefert die Existenz von U die Untergruppe U/G' in der Faktorgruppe G/G'. Da G/G' abelsch ist, ist U/G' normal in G/G'. Dies ist in der Skizze rechts durch den dicken blauen Strich markiert.
Diese Normalitäts-Eigenschaft übersetzt sich zurück nach G und zeigt $U \trianglelefteq G$.

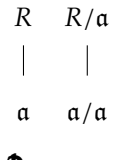
(b) Wir geben einen alternativen Beweis für die Aussage

$$R/\mathfrak{a} \text{ ist Körper} \iff \mathfrak{a} \text{ ist maximales Ideal von } R.$$

aus 17.18 (b). Seien R ein Ring und $\mathfrak{a} \lhd R$ ein Ideal von R. Wir betrachten den kanonischen Ringepimorphismus $R \to R/\mathfrak{a}$ und wenden den Korrespondenzsatz

an.
Dann folgt, dass der Faktorring $R/\mathfrak{a}$ genau dann nur die beiden Ideale $R/\mathfrak{a}$ und $\mathfrak{a}/\mathfrak{a} = \{\overline{0}\}$ besitzt, wenn $\mathfrak{a}$ ein maximales Ideal von R ist.

Ringe, die nur zwei Ideale besitzen, sind aber Körper. ⁂



Staatsexamensaufgabe (F2009T2A2) *Sei G eine Gruppe mit einer Untergruppe U vom Index 4. Zeigen Sie, dass G einen Normalteiler vom Index 2 oder 3 hat.*

Wir betrachten die Nebenklassenoperation von G auf den Nebenklassen von U, vgl. Seite 73. Sei

$$\varphi : G \to \mathrm{Sym}(G/U) \cong S_{[G:U]} = S_4$$

der zugehörige Operationshomomorphismus. Wir setzen $N := \ker \varphi$. Nach Homomorphiesatz ist die Gruppe G/N isomorph zu einer Untergruppe von S_4. Die Ordnung von $|G/N|$ ist nach Lagrange ein Teiler von $|S_4| = 24$, d. h. es gilt $|G/N| \in \{1, 2, 3, 4, 6, 8, 12, 24\}$. Wir diskutieren die einzelnen Ordnungen von $|G/N|$:

Fall $|G/N| = 1$: Dann ist $G = N = \ker \varphi$. Dies ist widersprüchlich, da G transitiv auf den vier Elementen von G/U operiert. Der Fall tritt also nicht auf.

Fälle $|G/N| \in \{2, 3, 4, 8\}$: Dann besitzt G/N nach 12.1 einen Normalteiler vom Index 2 oder 3. Mit dem Korrespondenzsatz folgt, dass auch G einen Normalteiler vom Index 2 oder 3 besitzt.

Fall $|G/N| = 6$: Dann ist die 3-Sylowgruppe von G/N ein Normalteiler vom Index 2. Der Korrespondenzsatz liefert dann die Existenz eines Normalteilers von G vom Index 2.

Fall $|G/N| = 12$: Da A_4 die einzige Untergruppe von S_4 von Ordnung 12 ist, ergibt sich $G/N \cong A_4$. Weil A_4 mit der Kleinschen Vierergruppe einen Normalteiler vom Index 3 besitzt, existiert auch in G/N und mit dem Korrespondenzsatz auch in G ein Normalteiler mit diesem Index.

Fall $|G/N| = 24$: Hier ist $G/N \cong S_4$. Der Index-2-Normalteiler A_4 von S_4 liefert dann analog zum vorherigen Fall einen Index-2-Normalteiler in G. ⁂

Subnormalreihen und Auflösungen

In auflösbaren Gruppen bilden die höheren Kommutatorgruppen eine Folge ineinander liegender Untergruppen, die nach endlich vielen Schritten die triviale Gruppe $\{1\}$ erreichen. Dies motiviert die folgende Definition:

Definition 36.5 *Sei G eine Gruppe. Für $n \in \mathbb{N}_0$ nennen wir ein $(n+1)$-Tupel $(U_0, U_1, \ldots, U_n)$ von Untergruppen von G eine **Subnormalreihe von G der Länge $n+1$**, wenn*

(a) *$U_0 = G$ und $U_n = \{1\}$ gelten und*

(b) $U_{i+1} \lhd U_i$ *für alle* $i \in \{0, 1, \dots, n-1\}$ *gilt.*

Eine solche Subnormalreihe kann man zusammenfassend auch in der Form

$$\{1\} = U_n \lhd U_{n-1} \lhd \cdots \lhd U_1 \lhd U_0 = G$$

notieren. Die Faktorgruppen U_i/U_{i+1} *mit* $i \in \{0, 1, \dots, n-1\}$ *bezeichnen wir als die* ***Faktoren der Subnormalreihe****.*
Um anzudeuten, dass der Faktor U_i/U_{i+1} *die Ordnung* k *hat, schreiben wir* $U_{i+1} \overset{k}{\lhd} U_i$ *in der Subnormalreihe.*

Bemerkung 36.6 Sei G eine Gruppe mit Subnormalreihe $\{1\} = G_n \lhd \cdots \lhd G_0 = G$.

(a) Da G_{i+1} eine *echte* Untergruppe von G_i für alle $i \in \{0, 1, \dots, n-1\}$ ist, sind die G_i paarweise verschieden.

(b) Im Allgemeinen sind die G_i keine Normalteiler von G, sondern nur normal im direkten Vorgänger G_{i-1}. ※

Beispiel 36.7 (a) Jede Gruppe G mit $|G| > 1$ besitzt eine Subnormalreihe der Länge Zwei, nämlich $\{1\} \lhd G$.

G ist genau dann einfach, wenn dies die einzige Subnormalreihe von G ist. ⁉

(b) Gruppen können verschiedene Subnormalreihen haben. Beispielsweise sind die Subnormalreihen von C_6 gegeben durch

$$C_1 \lhd C_6, \quad C_1 \lhd C_2 \lhd C_6, \quad C_1 \lhd C_3 \lhd C_6.$$

(c) Sei G eine auflösbare Gruppe. Dann besitzt G eine Subnormalreihe, deren Faktoren alle abelsch sind.

Die Aussage ist klar im Fall $|G| = 1$. Sei also $|G| > 1$. Da G auflösbar ist, existiert eine kleinste Zahl $n \in \mathbb{N}$ mit $G^{(n)} = \{1\}$. Wegen 35.3 gilt dann

$$\{1\} = G^{(n)} \trianglelefteq G^{(n-1)} \trianglelefteq \cdots \trianglelefteq G^{(1)} \trianglelefteq G^{(0)} = G.$$

Wir müssen noch zeigen, dass die einzelnen Kommutatorgruppen echt ineinander enthalten sind, dass also „$\lhd$“ statt „$\trianglelefteq$“ gilt.
Wenn dies nicht der Fall wäre, so gäbe es ein $i < n$ mit $G^{(i+1)} = G^{(i)}$. Aufgrund der Minimalität von n gilt zudem $\{1\} < G^{(i)}$. Es folgt

$$G^{(i+2)} = \left(G^{(i+1)}\right)' \overset{G^{(i+1)}=G^{(i)}}{=} \left(G^{(i)}\right)' = G^{(i+1)} \overset{G^{(i+1)}=G^{(i)}}{=} G^{(i)} > \{1\}.$$

Induktiv folgt, dass $G^{(i+k)} = G^{(i)} > \{1\}$ für alle $k \in \mathbb{N}_0$ gilt. Dies widerspricht aber der Auflösbarkeit von G. ※

Teil (c) des Beispiels ist die Grundlage für die folgende Charakterisierung auflösbarer Gruppen:

Satz 36.8 *Eine Gruppe G ist genau dann auflösbar, wenn sie endlich ist und eine Subnormalreihe mit lauter abelschen Faktoren besitzt.*

Beweis.

$\Longrightarrow$ Die Endlichkeit von G folgt aus der Auflösbarkeits-Definition 35.8, die Existenz der Subnormalreihe aus Teil (c) des obigen Beispiels.

$\Longleftarrow$ Seien nun G endlich und

$$\{1\} = G_n \lhd G_{n-1} \lhd \cdots \lhd G_1 \lhd G_0 = G$$

eine Subnormalreihe von G mit lauter abelschen Faktoren. Wir zeigen per absteigender Induktion, dass alle G_i auflösbar sind:

G_n ist abelsch, also auflösbar. Sei die Auflösbarkeit von G_i für ein $i \in \{n, n-1, \dots, 1\}$ bereits gezeigt. Dann ist G_{i-1} nach 35.12 auflösbar, denn sowohl G_i (Induktionsvoraussetzung) als auch G_{i-1}/G_i (nach Voraussetzung abelsch) sind auflösbar.

Dies zeigt, dass $G = G_0$ auflösbar ist. ■

Der folgende Satz verschärft 36.8:

Satz 36.9 *Für eine Gruppe G sind äquivalent:*

(a) *G ist auflösbar.*

(b) *G besitzt eine Subnormalreihe mit lauter zyklischen Faktoren von Primzahlordnung.*

*Jede solche Subnormalreihe nennt man auch eine **Auflösung von G**.*

Beweis.

(b)$\Longrightarrow$(a) Aufgrund der Indexmultiplikativität 7.6 entspricht das Produkt der Ordnungen der Faktoren der Subnormalreihe der Ordnung von G. Dies zeigt die Endlichkeit von G. Da zyklische Gruppen abelsch sind, folgt die Auflösbarkeit von G aus 36.8.

(a)$\Longrightarrow$(b) Wir beweisen die Behauptung per Induktion nach der Gruppenordnung:

Jede auflösbare Gruppe G mit $|G| = 1$ erfüllt das Kriterium in (b), denn Subnormalreihen von G besitzen keine Faktoren. ?

Sei nun „(a)$\Longrightarrow$(b)“ für alle Gruppen mit Ordnung höchstens $n \in \mathbb{N}$ gezeigt. Sei G eine auflösbare Gruppe der Ordnung $n+1$. Dann ist G' nach 36.7 (c) ein echter Normalteiler von G. Die Gruppe G/G' ist nicht-trivial, abelsch und endlich. Sie besitzt nach 8.5 einen Normalteiler von Primzahlindex. Der Korrespondenzsatz übersetzt diesen Normalteiler in einen Normalteiler G_1 von G mit $[G : G_1] \in \mathbb{P}$.

G_1 ist als echte Untergruppe von G auflösbar und hat kleinere Ordnung als G. Mit der Induktionsvoraussetzung besitzt G_1 daher eine Subnormalreihe $\{1\} = G_n \lhd \cdots \lhd G_1$ mit lauter zyklischen Faktoren von Primzahlordnung. Ergänzen wir diese Reihe auf der rechten Seite mit $G_0 := G$, so erhalten wir eine Subnormalreihe

$$\{1\} = G_n \lhd \cdots \lhd G_1 \lhd G_0 = G$$

von G mit lauter zyklischen Faktoren von Primzahlordnung. ■

Beispiel 36.10 (a) C_6 besitzt die beiden Auflösungen

$$C_1 \overset{2}{\lhd} C_2 \overset{3}{\lhd} C_6 \qquad \text{und} \qquad C_1 \overset{3}{\lhd} C_3 \overset{2}{\lhd} C_6.$$

Dies zeigt, dass eine Gruppe mehrere Auflösungen besitzen kann.

(b) Eine Auflösung von A_4 ist

$$\{\mathrm{id}\} \overset{2}{\lhd} \langle (1\,2)(3\,4) \rangle \overset{2}{\lhd} V_4 \overset{3}{\lhd} A_4;$$

hierbei bezeichnet V_4 die Kleinsche Vierergruppe. Gibt es weitere Auflösungen von A_4? ⁂

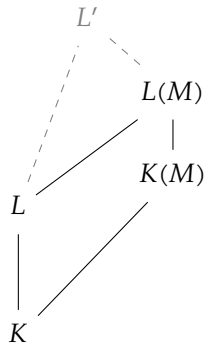
Bemerkung 36.11 Auflösbare Gruppen sind nach 36.8 genau die endlichen Gruppen G, die Subnormalreihen mit lauter abelschen Faktoren besitzen.
Auflösungen sind die längsten dieser Subnormalreihen. Hat die Ordnung von G die Primfaktorzerlegung $|G| = \prod_{i=1}^{s} p_i^{n_i}$, so hat jede Auflösung Länge $1 + \sum_{i=1}^{s} n_i$, denn die Gruppenordnungen in einer Auflösung werden in jedem Schritt stets um einen Primzahlfaktor kleiner. Dies zeigt, dass alle Auflösungen einer Gruppe dieselbe Länge besitzen.
Wir werden in den Übungen zeigen, dass eine auflösbare Gruppe G keine kürzere Subnormalreihe mit lauter abelschen Faktoren besitzen kann als ihre **Kommutatorreihe** → Übung

$$\{1\} = G^{(n)} \lhd G^{(n-1)} \lhd \cdots \lhd G^{(1)} \lhd G^{(0)} = G. \qquad ⁂$$

37. Translationssatz, Kummer-Theorie

Worum geht es? Wir lernen die für die Galoistheorie wichtige Konstruktion des *Transfers* kennen. Mit dem *Translationssatz* beschreiben wir seine Auswirkungen auf die Galoisgruppe.
Mit Hilfe von *Kummer-Theorie* finden wir „schöne“ primitive Elemente für (gewisse) Galoiserweiterungen mit zyklischen Galoisgruppen. ⋇

Der Translationssatz



In diesem Abschnitt untersuchen wir die Effekte, die durch „Heben“ einer Körpererweiterung auf einen größeren Unterkörper entstehen. Damit ist Folgendes gemeint:
Sei $L|K$ eine Körpererweiterung. Sei M irgendeine Teilmenge aus irgendeinem Oberkörper L' von L. Wir stellen an M keine weiteren Bedingungen; M kann beispielsweise überabzählbar sein oder ausschließlich transzendente Elemente enthalten.
Dann können wir M sowohl an K als auch an L adjungieren. Wir erhalten auf diese Weise die Körpererweiterung $L(M)|K(M)$, die man auch das **Translat von $L|K$ mit M** nennt.

Beispiel 37.1 (a) Das Translat von $L|K$ mit L liefert die Erweiterung $L|L$.

(b) Sei $L|K$ eine Körpererweiterung mit $L \subseteq \mathbb{C}$ und $K \subseteq \mathbb{R}$. Für das Translat $L(\mathbb{R})|K(\mathbb{R})$ gibt es genau zwei Möglichkeiten:

Falls sogar $L \subseteq \mathbb{R}$ ist, so gilt $L(\mathbb{R}) = K(\mathbb{R}) = \mathbb{R}$. Wir erhalten also die Grad-1-Erweiterung $\mathbb{R}|\mathbb{R}$.
Falls $L \not\subseteq \mathbb{R}$ ist, so gelten $[L : K] \geq 2$ sowie $L(\mathbb{R}) = \mathbb{C}$ und $K(\mathbb{R}) = \mathbb{R}$. Das Translat führt auf die Grad-2-Erweiterung $\mathbb{C}|\mathbb{R}$. ⋇

Im Beispiel oben reduziert der Transfer[5] den Grad der Erweiterung $L|K$. Dies ist kein Zufall und erklärt, warum der Abstand zwischen $K(M)$ und $L(M)$ im Bild oben kleiner ist als der von K zu L:

Lemma 37.2 *Seien $L|K$ eine Körpererweiterung und M eine Teilmenge eines Oberkörpers von L. Dann gilt*

$$[L(M) : K(M)] \leq [L : K].$$

Konvention: Für alle $n \in \mathbb{N} \cup \{\infty\}$ gilt $n \leq \infty$.

Beweis. L ist ein Oberkörper von K und lässt sich als K-Vektorraum auffassen. Sei B eine K-Basis von L. Dann gilt $L = K(B)$ und somit

$$L(M) = K(B)(M) = K(B, M) = K(M)(B).$$

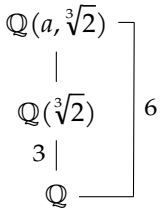
[5] Hier schlägt die lateinische Perfekt-Bildung *„ferre – tuli – latum“* zu. $L(M)|K(M)$ ist das *Translat* von $L|K$ mit M. Es entsteht als *Transfer* von $L|K$ mit M. Ein Translat ist also das Ergebnis eines Transfers.

Die Darstellung ganz rechts in obiger Zeile zeigt, dass B ein Erzeugendensystem für den $K(M)$-Vektorraum $L(M)$ ist. Da $K(M)$ eine Obermenge von K ist, muss B aber nicht linear unabhängig sein. Daher ist ⁉

$$[L(M) : K(M)] = \dim_{K(M)} L(M) = \dim_{K(M)} K(M)(B) \leq |B| = \dim_K L = [L : K]. \qquad \blacksquare$$

Die Aussage aus 37.2 lässt sich im Allgemeinen nicht zu einer Teilbarkeitsaussage verschärfen (was recht selten in der Algebra ist):

Beispiel 37.3 Wir betrachten das irreduzible Polynom $f := X^3 - 2 \in \mathbb{Q}[X]$ sowie eine nicht-reelle Nullstelle $a \in \mathbb{C}$ von f. Dann hat die Körpererweiterung $\mathbb{Q}(a)|\mathbb{Q}$ den Grad Drei.
Transfer mit dem Element $\sqrt[3]{2}$ liefert die Erweiterung $\mathbb{Q}(a, \sqrt[3]{2})|\mathbb{Q}(\sqrt[3]{2})$.
Der Körper $\mathbb{Q}(a, \sqrt[3]{2})$ ist der Zerfällungskörper von f und hat Grad Sechs über $\mathbb{Q}$. Der Unterkörper $\mathbb{Q}(\sqrt[3]{2})$ hat Grad Drei über $\mathbb{Q}$. Mit der Gradformel folgt, dass die obere Teilerweiterung im rechten Bild den Grad Zwei hat.
Durch den Transfer mit $\sqrt[3]{2}$ hat sich der Körpergrad von Drei auf den Nicht-Teiler Zwei verkleinert. ⁕



Wir untersuchen nun Translate von Galoiserweiterungen. Unser Hauptresultat wird der Translationssatz sein.

Lemma 37.4 *Seien $L|K$ eine Galoiserweiterung und M eine Teilmenge eines Oberkörpers von L. Dann ist auch das Translat $L(M)|K(M)$ galoissch.*

Beweis. Nach dem Satz vom primitiven Element existiert ein $a \in L$, so dass $L = K(a)$ gilt. Da $L|K$ galoissch und daher separabel ist, besitzt das Minimalpolynom $f \in K[X]$ von a keine Mehrfachnullstellen in seinem Zerfällungskörper L.
Wir fassen f nun als Polynom über $K(M)$ auf. Auch als Polynom über $K(M)$ besitzt f keine Mehrfachnullstellen in seinem Zerfällungskörper. Dieser ist gegeben durch ⁉

$$K(M)(a) = K(M, a) = K(a)(M) = L(M).$$

Nach 26.4 folgt, dass $L(M)|K(M)$ eine Galoiserweiterung ist. $\blacksquare$

Nach obigem Lemma ist mit $L|K$ auch $L(M)|K(M)$ galoissch. Der Translationssatz klärt, wie die Galoisgruppen beider Erweiterungen zueinander in Beziehung stehen:

Satz 37.5 (Translationssatz) *Seien $L|K$ eine Galoiserweiterung und M eine Teilmenge eines Oberkörpers von L. Dann gelten die folgenden Aussagen:*

(a) *Ist $\varphi : L(M) \to L(M)$ ein Galoisautomorphismus von $L(M)|K(M)$, so ist die Einschränkung*

$$\varphi|_L : L \to L, \qquad a \mapsto \varphi(a)$$

ein Galoisautomorphismus von $L|K$.

(b) *Die Abbildung*

$$f : \mathrm{Gal}(L(M)|K(M)) \to \mathrm{Gal}(L|K), \qquad \varphi \mapsto \varphi|_L$$

ist ein Gruppenmonomorphismus.

Insbesondere ist die Galoisgruppe von $L(M)|K(M)$ isomorph zu einer Untergruppe von $\mathrm{Gal}(L|K)$.

Beweis. Wir bezeichnen die Galoisgruppe von $L|K$ mit G. Aus 37.4 wissen wir, dass die Erweiterung $L(M)|K(M)$ galoissch ist. Ihre Galoisgruppe bezeichnen wir mit G_M. Sei a ein primitives Element von $L|K$. Im Beweis von 37.4 haben wir $L(M) = K(M)(a)$ gesehen. a ist also auch ein primitives Element von $L(M)|K(M)$.

zu (a) Wir bezeichnen das Minimalpolynom von a über K mit $f \in K[X]$ und über $K(M)$ mit $f_M \in K(M)[X]$. Da f als Polynom über $K(M)$ annullierend für a ist, folgt $f_M \mid f$ über $K(M)$ nach 20.21. Jede Nullstelle von f_M ist daher auch eine Nullstelle von f. ⁉

Nach 28.3 entstehen die Elemente φ aus G_M genau dadurch, dass man eine beliebige Nullstelle b von f_M wählt und dann $\varphi(a) := b$ fordert. Mit derselben Forderung kann man auch ein Element aus G konstruieren, denn b ist auch eine Nullstelle von f.

Zu jedem $\varphi \in G_M$ gibt es daher ein $\psi \in G$, das das primitive Element a auf dieselbe Weise abbildet. Wegen $L = K(a)$ bildet φ die Elemente aus L also in derselben Weise wie ψ ab. Daher ist $\varphi|_L = \psi \in G$.

zu (b) Einsetzen von Elementen aus L zeigt, dass $(\varphi \circ \psi)|_L = \varphi|_L \circ \psi|_L$ für alle $\varphi, \psi \in G_M$ gilt. Dies zeigt die Homomorphie von f.

Sei nun $\varphi \in \ker f$. Dann ist $f(\varphi) = \varphi|_L = \mathrm{id}_L$. Daher ist $\varphi|_L(a) = a$ und somit auch $\varphi(a) = a$. Dies zeigt, dass φ jedes Element des Grundkörpers $K(M)$ und das Element a fixiert. Also fixiert φ auch jedes Element des Körpers $K(M)(a) = L(M)$ und stimmt somit mit der Identität $\mathrm{id}|_{L(M)}$ überein.

Der Insbesondere-Aussage folgt aus dem Homomorphiesatz: Es gilt

$$G_M \cong G_M/\{1\} = G_M/\ker f \cong f(G_M) \leq G. \qquad \blacksquare$$

Bemerkung 37.6 (a) Der Beweis des Translationssatzes stützt sich darauf, dass man für die Erweiterungen $L|K$ und $L(M)|K(M)$ dasselbe primitive Element a benutzen kann. Allerdings ergeben sich unterschiedliche Minimalpolynome von a, da die Polynome einmal über K und einmal über dem größeren Körper $K(M)$ betrachtet werden.
Hieraus folgt eine Teilbarkeitsbeziehung zwischen den beiden Minimalpolynomen. 28.3 übersetzt diese dann in die Monomorphismus-Aussage.

(b) In der Praxis wird meist nur die Insbesondere-Aussage des Translationssatzes benötigt. Diese lautet knapp: Transfer liefert Untergruppen von Galoisgruppen. ⁂

Als Anwendungsbeispiel verschärfen wir 37.2 im Galois-Fall:

Korollar 37.7 *Seien $L|K$ eine Galoiserweiterung und M eine Teilmenge eines Oberkörpers von L. Dann ist $[L(M) : K(M)]$ ein Teiler von $[L : K]$.*
Der Grad eines Translats einer Galoiserweiterung teilt also den Grad der Galoiserweiterung.

Beweis. Wir setzen $G := \mathrm{Gal}(L|K)$ und $G_M := [L(M) : K(M)]$. Nach dem Translationssatz ist G_M isomorph zu einer Untergruppe von G. Mit Lagrange folgt, dass $|G_M| = [L(M) : K(M)]$ ein Teiler von $|G| = [L : K]$ ist. ■

Kummer-Theorie

Wir haben in 22.3 (d) gezeigt, dass man quadratische Erweiterungen von $\mathbb{Q}$ stets durch Adjunktion einer Wurzel darstellen kann: Ist $L|\mathbb{Q}$ eine quadratische Erweiterung, so gibt es ein $a \in \mathbb{Q}$ mit $L = \mathbb{Q}(\sqrt{a})$. Für solche Erweiterungen kann man also sehr einfache primitive Elemente finden.
Wir stellen nun eine Verallgemeinerung dieses Resultats vor, die in der Literatur auch als **Kummer-Theorie** bekannt ist.

Wir benötigen das folgende Lemma für den Beweis des Satzes von Kummer. Das Lemma selbst beweisen wir nicht, da sein Beweis eher der linearen Algebra zuzuordnen ist: Man nimmt an, dass es eine nicht-triviale Linearkombination zum Nullvektor gibt, konstruiert dann eine zweite, zieht beide voneinander ab und erhält einen Widerspruch. Details zum Beweis finden Sie beispielsweise in [Bos20, Satz 2 auf S. 250 f.].

Lemma 37.8 (Artin) *Sei $L|K$ eine Galoiserweiterung mit Galoisgruppe $G = \{\varphi_1, \dots, \varphi_n\}$. Dann sind die Elemente aus G linear unabhängig über L, d.h. für beliebige $a_i \in L$ stimmt die Linearkombination $\sum_{i=1}^{n} a_i\varphi_i$ genau dann mit der Nullfunktion überein, wenn $a_i = 0$ für alle i gilt.*

Wir können nun den Satz von Kummer beweisen:

Satz 37.9 (Kummer) *Sei $L|K$ eine Galoiserweiterung mit Galoisgruppe G. Es gelte $G \cong C_n$. Weiter existiere ein Element $\xi \in K^\times$ mit multiplikativer Ordnung n.*
Dann gibt es ein $b \in L$, so dass $L = K(b)$ und $b^n \in K$ gelten.

Beweis. Sei φ ein Erzeuger von G. Dann ist $G = \{\varphi^1, \varphi^2, \dots, \varphi^n\}$. Die Linearkombination

$$\xi \cdot \varphi + \xi^2 \cdot \varphi^2 + \cdots + \xi^n \cdot \varphi^n = \sum_{i=1}^{n} \xi^i \varphi^i$$

ist eine Funktion $L \to L$. Diese ist nach obigem Lemma nicht die Nullfunktion. Also gibt es ein Element $\beta \in L$, so dass

$$b := \Big(\sum_{i=1}^{n} \xi^i \varphi^i\Big)(\beta) = \sum_{i=1}^{n} \xi^i \varphi^i(\beta) \in L$$

von Null verschieden ist.

Vorbereitung: Funktionalgleichung für b Wir zeigen $\varphi^k(b) = \zeta^{-k} \cdot b$ für alle $k \in \mathbb{N}$.

Wir wenden φ auf b an und erhalten

$$\varphi(b) = \varphi\Big(\sum_{i=1}^{n} \zeta^i \varphi^i(\beta)\Big) \overset{\varphi \text{ ist Homom.}}{=} \sum_{i=1}^{n} \zeta^i \varphi^{i+1}(\beta) = \zeta^{-1} \cdot \sum_{i=1}^{n} \zeta^{i+1} \varphi^{i+1}(\beta)$$
$$\overset{\text{Indexverschiebung}}{=} \zeta^{-1} \cdot \sum_{i=2}^{n+1} \zeta^i \varphi^i(\beta) \overset{\substack{\text{ord}(\zeta)=n \Rightarrow \zeta^{n+1}=\zeta \\ \text{ord}(\varphi)=n \Rightarrow \varphi^{n+1}=\varphi}}{=} \zeta^{-1} \cdot \sum_{i=1}^{n} \zeta^i \varphi^i(\beta) = \zeta^{-1} \cdot b.$$

Induktiv folgt hieraus die behauptete Funktionalgleichung $\varphi^k(b) = \zeta^{-k} \cdot b$.

b ist primitives Element Wir zeigen, dass $L = K(b)$ ist.

Da $b \neq 0$ ist, liefert die Funktionalgleichung, dass b genau dann von φ^k fixiert wird, wenn $\zeta^{-k} = 1$ ist. Da ζ Ordnung n hat, ist dies genau dann der Fall, wenn $n \mid k$ ist. Dies zeigt, dass b ausschließlich vom Galoisautomorphismus $\varphi^n = \mathrm{id}_L$ fixiert wird. Nach dem Hauptsatz der Galoistheorie liegt b daher in $\mathrm{Fix}(\langle \mathrm{id}_L \rangle) = L$, jedoch in keinem echten Unterkörper von L.
Es gilt daher $K(b) = L$. Also ist b ein primitives Element von $L|K$.

b^n liegt in K Wir setzen $a := b^n$ und berechnen $\varphi(a)$.

Es gilt

$$\varphi(a) = \varphi(b^n) \overset{\varphi \text{ ist Homom.}}{=} (\varphi(b))^n$$
$$\overset{\text{Funktionalgl.}}{=} (\zeta^{-1} \cdot b)^n = \zeta^{-n} \cdot b^n \overset{\text{ord}(\zeta)=n}{=} 1 \cdot b^n = a.$$

a wird also von φ und damit auch von der gesamten Galoisgruppe $G = \langle \varphi \rangle$ fixiert. Analog zu oben folgt mit dem Hauptsatz der Galoistheorie, dass, wie gewünscht, $b^n = a \in \mathrm{Fix}(G) = K$ ist. ■

Bemerkung 37.10 (a) Im Satz von Kummer tritt ein Element ζ mit Ordnung n auf. Genau dann existiert ein solches Element in einem Erweiterungskörper von K, wenn die Charakteristik $p \in \mathbb{P} \cup \{0\}$ von K kein Teiler von n ist:

Sei $p \nmid n$. Nach 30.13 besitzt das Polynom $f := X^n - 1 \in K[X]$ in seinem Zerfällungskörper Z dann genau n paarweise verschiedene Nullstellen. Mit dem Untergruppenkriterium folgt, dass die Menge $N \subseteq Z^\times$ der Nullstellen von f eine Untergruppe von $Z^\times$ bildet. Nach 15.21 ist N eine zyklische Gruppe. Jeder Erzeuger von N ist dann ein Element mit multiplikativer Ordnung $\deg f = n$. ?

Gilt $p \mid n$, so ist $p \in \mathbb{P}$, und es gilt $n = p \cdot s$ mit einem $s \in \mathbb{N}$. Angenommen, wir hätten ein Element ζ mit multiplikativer Ordnung n in einem Erweiterungskörper von K gefunden. Dann wäre $\zeta^n = 1$ und somit ?

$$0 = \zeta^n - 1 = \zeta^{ps} - 1 = (\zeta^s)^p - 1^p \overset{\text{Frobenius}}{=} (\zeta^s - 1)^p.$$

Dies ist ein Widerspruch: Wir haben $\text{ord}(\zeta) = n$ vorausgesetzt, allerdings gilt bereits $\zeta^s = 1$.

(b) Wegen (a) ist der Satz von Kummer prinzipiell nicht in der Situation

$$\text{Charakteristik von } K \text{ ist } p \in \mathbb{P}, \quad \mathrm{Gal}(L|K) \cong C_n, \quad p \mid n$$

anwendbar. Hier muss man auf verwandte Resultate, die *Artin-Schreier-Theorie*, zurückgreifen.

(c) Erfüllt eine Körpererweiterung $L|K$ die Voraussetzungen des Satzes von Kummer, dann gibt es ein $a \in K$, so dass eine Nullstelle des Polynoms $X^n - a \in K[X]$ ein primitives Element für $L|K$ ist.
Interpretieren wir diese Nullstelle (mathematisch ungenau) als n-te Wurzel von a, so entsteht L also durch Adjunktion einer n-ten Wurzel an K.

(d) Ist K ein Erweiterungskörper von $\mathbb{Q}$, so ist das Element $\zeta \in K^\times$ aus dem Satz von Kummer nichts anderes als eine primitive n-te Einheitswurzel. ※

38. Radikale

Worum geht es? Wir lernen mit den *reinen Polynomen* eine Klasse von Polynomen kennen, deren Nullstellen, die *Radikale*, Verallgemeinerungen n-ter Wurzeln darstellen. Die Adjunktion von Radikalen beschreiben wir mit *Radikalerweiterungen*, die iterierte Adjunktion von Radikalen mit *Radikaltürmen*. ⋇

Reine Polynome und Radikale

Reine Polynome sind Polynome mit sehr einfacher Struktur. Ihre Nullstellen nennt man Radikale:

Definition 38.1 *Sei K ein Körper der Charakteristik $p \in \mathbb{P} \cup \{0\}$.*

(a) *Als **reines Polynom über K** bezeichnen wir jedes Polynom der Form $X^n - a \in K[X]$ mit $a \neq 0$, $n \geq 1$ und $p \nmid n$.*

(b) *Unter einem **Radikal über K** verstehen wir jede Nullstelle eines jeden reinen Polynoms über K.*

Bemerkung 38.2 (a) Reine Polynome besitzen nie die Nullstelle Null. Daher ist Null über keinem Körper ein Radikal.

(b) Die Bedingung $p \nmid n$ aus Teil (a) der obigen Definition heißt **Separabilitätsbedingung**. Zusammen mit der Forderung $a \neq 0$ stellt sie sicher, dass reine Polynome keine Mehrfachnullstellen in ihren jeweiligen Zerfällungskörpern besitzen. Den Beweis dieser Aussage haben wir im Spezialfall $a = 1$ in 30.13 geführt.

Die Separabilitätsbedingung ist in Charakteristik-Null-Körpern stets erfüllt. Über solchen Körpern sind also genau die Polynome $X^n - a$ mit $n \geq 1$ und $a \neq 0$ rein.

(c) Aus (b) folgt, dass jedes Radikal über K separabel über K ist. ⋇ ⁉

Beispiel 38.3 (a) Jede Einheitswurzel ist ein Radikal über $\mathbb{Q}$.

(b) Ist r ein Radikal über K, so existiert ein $n \in \mathbb{N}$, so dass $r^n \in K$ ist.
Aber nicht jedes Element r mit $r^n \in K$ ist ein Radikal. ⁉

(c) Ist r ein Radikal über K, so ist r auch ein Radikal über jedem Oberkörper von K. ⁉

(d) Sei $a \in \mathbb{Q}^+$. Dann ist $\sqrt[n]{a}$ für alle $n \in \mathbb{N}$ ein Radikal über $\mathbb{Q}$. ⋇

Bemerkung 38.4 (Wurzel vs. Radikal) Nach 38.3 (d) sind n-te Wurzeln stets Radikale. Umgekehrt gibt es Radikale, die man im strikten Sinne nicht als n-te Wurzeln interpretieren würde. Beispielsweise ist die imaginäre Einheit i eine Nullstelle des reinen Polynoms $X^4 - 1 \in \mathbb{Q}[X]$ und damit ein Radikal über $\mathbb{Q}$, man würde jedoch nicht $i = \sqrt[4]{1}$ schreiben.

Wir gehen in dieser und der nächsten Vorlesung mit dem Wurzelbegriff etwas großzügiger um[6] und benutzen die Begriffe *Radikal* und *n-te Wurzel* weitgehend synonym. Für Nullstellen reiner Polynome $X^n - a$ verwenden wir gelegentlich das Symbol $\sqrt[n]{a}$.
Diese Sprech- und Schreibregelungen sind bequem, aber mit Vorsicht zu genießen: In der Gleichung

$$i = \sqrt[4]{1} = 1$$

rechtfertigen sie beide Gleichheitszeichen, aber nicht die Gesamtgleichung.
Beachten Sie daher, dass die Notation $\sqrt[n]{a}$ meist nicht für ein konkret bestimmtes Element steht, sondern symbolisch als irgendeine Nullstelle von $X^n - a$ zu verstehen ist. ⁜

Adjungiert man ein Radikal an einen Körper, so entsteht eine Radikalerweiterung.

Definition 38.5 *Eine Körpererweiterung $L|K$ heißt **Radikalerweiterung**, wenn ein Radikal r über K existiert, so dass $L = K(r)$ gilt.*
Radikalerweiterungen sind also stets einfach, endlich und wegen der Separabilitätsbedingung auch separabel. ⁉

Der Satz von Kummer 37.9 lässt sich sehr elegant mit Hilfe von Radikalerweiterungen ausdrücken. Wir nutzen hierbei aus, dass die im Satz von Kummer geforderte Existenz eines Elements ξ mit $\operatorname{ord}(\xi) = n$ nach 37.10 (a) die Separabilitätsbedingung garantiert. ⁉

Korollar 38.6 (Kummer) *Sei $L|K$ eine Galoiserweiterung vom Grad $n \in \mathbb{N}$ mit zyklischer Galoisgruppe. In K existiere ein Element mit multiplikativer Ordnung n. Dann ist $L|K$ eine Radikalerweiterung.*

Bemerkung 38.7 Sei r ein Erzeuger der multiplikativen Gruppe des Körpers $\mathbb{F}_{16}$. Diese hat Ordnung 15 und ist nach 15.21 zyklisch. r hat also multiplikative Ordnung 15 und ist Nullstelle des reinen Polynoms $f := X^{15} - 1 \in \mathbb{F}_2[X]$. Somit ist r ein Radikal über $\mathbb{F}_2$.
Die Radikalerweiterung $\mathbb{F}_2(r)|\mathbb{F}_2$ hat den Grad

$$[\mathbb{F}_2(r) : \mathbb{F}_2] = [\mathbb{F}_{16} : \mathbb{F}_2] = [\mathbb{F}_{2^4} : \mathbb{F}_2] = 4.$$

Dies zeigt, dass der Grad des Polynoms f nicht den Grad der zugehörigen Radikalerweiterung festlegt.
Außerdem sehen wir, dass die Charakteristik des Grundkörpers die Grade von Radikalerweiterungen teilen kann. Die Separabilitätsbedingung schließt eine solche Teilbarkeit also nur auf Polynom-Ebene, nicht jedoch auf Körper-Ebene aus. ⁜

Wir klären das Aussehen der Nullstellen und des Zerfällungskörpers reiner Polynome.

Satz 38.8 *Seien K ein Körper und $f := X^n - a$ ein reines Polynom über K. Bezeichnen wir den algebraischen Abschluss von K mit $\overline{K}$, so gelten die folgenden Aussagen:*

[6] Das ist eine ziemlich beschönigende Formulierung; man könnte auch sagen: Wir arbeiten mathematisch sehr unsauber...

(a) *f besitzt n paarweise verschiedene Nullstellen in $\overline{K}$.*

(b) *In $\overline{K}$ existiert ein Element ξ mit multiplikativer Ordnung n. Ist α eine beliebige Nullstelle von f, so sind die Nullstellen von f gegeben durch $\alpha \cdot \xi^k$ mit $k \in \{0, 1, \dots, n-1\}$.*

(c) *Mit den Bezeichnungen aus (b) gilt: Der Zerfällungskörper von f ist $K(\alpha, \xi)$.*

Beweis.

(a) folgt, weil reine Polynome keine Mehrfachnullstellen besitzen.

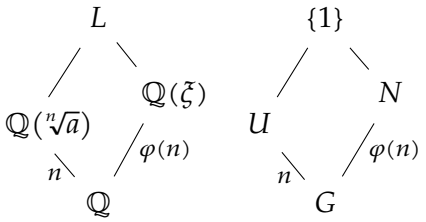
zu (b) Die Existenz von ξ folgt aus 37.10 (a).

Da $\operatorname{ord}(\xi) = n$ ist, sind die Potenzen $\xi^0, \xi^1, \dots, \xi^{n-1}$ paarweise verschieden. Weil α nach 38.2 (a) ungleich Null ist, sind die Produkte $\alpha \cdot \xi^k$ mit $k \in \{0, 1, \dots, n-1\}$ paarweise verschieden. Nachrechnen zeigt, dass jedes solche Produkt eine Nullstelle von f ist. Somit sind alle Nullstellen von f gefunden.

zu (c) Es ist klar, dass jedes Element der Form $\alpha \cdot \xi^k$ in $K(\alpha, \xi)$ enthalten ist.
Umgekehrt lassen sich α und ξ aus den Nullstellen $\alpha \cdot \xi^k$ gewinnen: Es ist $\alpha = \alpha \cdot \xi^0$ und, da $\alpha \neq 0$ ist, $\xi = \frac{\alpha \cdot \xi}{\alpha \cdot \xi^0}$.

Dies zeigt, dass der Zerfällungskörper von f mit $K(\alpha, \xi)$ übereinstimmt. ■

Bemerkung 38.9 Die Zerfällungskörper reiner Polynome besitzen auch für hohe Polynomgrade eine sehr einfache Darstellung. Dies ist der Grund, warum sie in vielen Staatsexamensaufgaben zur Galoistheorie auftauchen. Typischerweise werden in solchen Aufgaben reine Polynome über $\mathbb{Q}$ betrachtet.
Sei $f := X^n - a \in \mathbb{Q}[X]$ mit $n \geq 3$ und $a \in \mathbb{P}$ gegeben. f ist nach dem Eisenstein-Kriterium irreduzibel. Setzen wir $\xi := \exp(\frac{2\pi i}{n})$, so ist $L := \mathbb{Q}(\sqrt[n]{a}, \xi)$ der Zerfällungskörper von f. Die Erweiterung $L|\mathbb{Q}$ ist galoissch. Wir bezeichnen ihre Galoisgruppe mit G und stellen einige Aussagen zu den Zwischenkörpern $\mathbb{Q}(\xi)$ und $\mathbb{Q}(\sqrt[n]{a})$ zusammen, die in vielen Aufgabenstellungen eine Rolle spielen.



Die Erweiterung $\mathbb{Q}(\xi)|\mathbb{Q}$ ist galoissch, ihre Galoisgruppe ist nach 31.4 isomorph zu $\mathbb{Z}_n^\times$. Dies zeigt, dass G einen Normalteiler N vom Index $\varphi(n)$ besitzt, für den $G/N \cong \mathbb{Z}_n^\times$ gilt.
Da G/N abelsch ist, folgt $G' \leq N$ für die Kommutatorgruppe G' von G. Es ist also $[G : G'] \geq \varphi(n)$.

Aufgrund der Irreduzibilität von f gilt $[\mathbb{Q}(\sqrt[n]{a}) : \mathbb{Q}] = n$. Da $a > 0$ ist, ist der Körper $\mathbb{Q}(\sqrt[n]{a})$ ein Unterkörper der reellen Zahlen. Wegen $n \geq 3$ ist ξ echt komplex, vgl. das Schaubild auf Seite 217. Hieraus folgt, dass f über $\mathbb{Q}(\sqrt[n]{a})$ nicht vollständig zerfällt, also dass U kein Normalteiler von G ist. Also ist G insbesondere nicht abelsch. ※

Wir zeigen nun, dass reine Polynome auflösbare Galoisgruppen liefern.

Satz 38.10 *Seien K ein Körper und $f := X^n - a \in K[X]$ ein reines Polynom über K mit Zerfällungskörper L. Dann ist die Erweiterung $L|K$ galoissch. Ihre Galoisgruppe G ist auflösbar. Kurz: Reine Polynome haben auflösbare Galoisgruppen.*

Beweis. Die Erweiterung $L|K$ ist normal. Nach 38.2 (c) sind die Nullstellen von f separabel über K. Da L von diesen Nullstellen erzeugt wird, ist $L|K$ auch separabel. Insgesamt ist $L|K$ also eine Galoiserweiterung.
Sei $\xi \in L$ ein Element mit multiplikativer Ordnung n; dieses existiert nach 38.8 (c). Der Körper $K(\xi)$ ist ein Zwischenkörper von $L|K$. Die zugehörige Galoisgruppe $\mathrm{Gal}(L|K(\xi))$ bezeichnen wir mit N. Da $K(\xi)$ der Zerfällungskörper des Polynoms $X^n - 1 \in K[X]$ ist, gilt $N \trianglelefteq G$.

L	$\{1\}$
|	|
$K(\xi)$	N
|	|
K	G

Wir zeigen im Folgenden, dass N und G/N abelsch sind. 36.8 liefert dann die Auflösbarkeit von G. Damit ist der Satz bewiesen.

Kommutativität von G/N Nach dem Hauptsatz der Galoistheorie ist die Faktorgruppe G/N zur Galoisgruppe $H := \mathrm{Gal}(K(\xi)|K)$ isomorph. Es genügt also, zu zeigen, dass H abelsch ist.

Ist K ein Charakteristik-Null-Körper, so ist ξ eine Einheitswurzel. Die Galoisgruppe der Erweiterung $\mathbb{Q}(\xi)|\mathbb{Q}$ ist isomorph zu $\mathbb{Z}_n^\times$ und damit abelsch. Die Erweiterung $K(\xi)|K$ entsteht aus $\mathbb{Q}(\xi)|\mathbb{Q}$ durch Translation mit K. Nach Translationssatz ist H isomorph zu einer Untergruppe von $\mathbb{Z}_n^\times$ und somit abelsch.

Sei die Charakteristik von K nun eine Primzahl $p \in \mathbb{P}$. Da ξ algebraisch über $\mathbb{F}_p$ ist, ist die Erweiterung $\mathbb{F}_p(\xi)|\mathbb{F}_p$ endlich und $\mathbb{F}_p(\xi)$ daher ein endlicher Körper. ?
Nach 29.13 (b) ist die Galoisgruppe von $\mathbb{F}_p(\xi)|\mathbb{F}_p$ zyklisch.
Nun können wir wie im Charakteristik-Null-Fall argumentieren: Das Translat mit K liefert die Erweiterung $K(\xi)|K$. Mit Translationssatz ist H isomorph zu einer Untergruppe einer zyklischen Gruppe, also abelsch.

Kommutativität von N Sei $\alpha \in L$ eine beliebige Nullstelle von f. Nach 38.8 (c) ist dann $L = K(\alpha, \xi) = K(\xi)(\alpha)$. Wegen 28.3 ist ein Galoisautomorphismus φ von $L|K(\xi)$ durch Angabe des Bildes $\varphi(\alpha)$ eindeutig festgelegt. Als Werte für $\varphi(\alpha)$ kommen nur Nullstellen von f in Frage, also nach 38.8 (b) nur Elemente der Form $\alpha \cdot \xi^k$. ?

Seien nun $\varphi, \psi \in N$ zwei beliebige Galoisautomorphismen von $L|K(\xi)$. Dann existieren $k, s \in \mathbb{N}$ mit $\varphi(\alpha) = \alpha \cdot \xi^k$ und $\psi(\alpha) = \alpha \cdot \xi^s$. Es gilt

$$\begin{aligned}(\varphi \circ \psi)(\alpha) &= \varphi(\psi(\alpha)) = \varphi(\alpha \cdot \xi^s) \\ &\overset{\varphi \text{ fixiert } \xi}{=} \varphi(\alpha) \cdot \xi^s = \alpha \cdot \xi^k \cdot \xi^s = \alpha \cdot \xi^{k+s}.\end{aligned}$$

Analog sieht man $(\psi \circ \varphi)(\alpha) = \alpha \cdot \xi^{k+s}$. Also bilden $\psi \circ \varphi$ und $\varphi \circ \psi$ das Element α gleich ab; dies zeigt $\psi \circ \varphi = \varphi \circ \psi$ und somit die Kommutativität von N. ■

Radikaltürme

Setzt man endlich viele Radikalerweiterungen aufeinander, so erhält man einen Radikalturm:

Definition 38.11 *Sei K ein Körper. Unter einem **Radikalturm über K** verstehen wir endlich viele Oberkörper $K_0, K_1, \dots, K_n$ von K mit*

$$K = K_0 \subseteq K_1 \subseteq K_2 \subseteq \cdots \subseteq K_n,$$

so dass die Erweiterungen $K_{i+1}|K_i$ für alle $i \in \{0, 1, \dots, n-1\}$ Radikalerweiterungen sind. Wegen 25.20 sind die Erweiterung $K_n|K$ und daher auch alle ihre Teilerweiterungen separabel.

Vereinbarung zur Schreibweise 38.12 Um die Lesbarkeit zu erhöhen, schreiben wir Radikaltürme meist nicht aus, sondern ersetzen die Zwischenkörper durch das Symbol „⇛“. Der Radikalturm

$$K = K_0 \subseteq K_1 \subseteq K_2 \subseteq \cdots \subseteq K_n$$

würde beispielsweise in der Form $K = K_0 \Rrightarrow K_n$ notiert werden. ⋇

Wir stellen einige Eigenschaften von Radikaltürmen bereit, die wir in der nächsten Vorlesung benötigen werden.

Satz 38.13 *Seien $K_0 \Rrightarrow K_n$ ein Radikalturm und M eine Teilmenge eines Oberkörpers von K_n. Wir transferieren jeden der Körper K_i mit M. Dann ist der entstehende Körperturm*

$$K_0(M) \subseteq K_1(M) \subseteq \cdots \subseteq K_n(M)$$

wieder ein Radikalturm.

Beweis. Wir müssen zeigen, dass jede der Erweiterungen $K_{i+1}(M)|K_i(M)$ eine Radikalerweiterung ist. Sei hierzu $i \in \{0, 1, \dots, n-1\}$ beliebig vorgegeben. Nach Voraussetzung ist $K_{i+1}|K_i$ eine Radikalerweiterung, so dass ein Radikal r über K_i mit $K_{i+1} = K_i(r)$ existiert. Nach 38.3 (c) ist r auch ein Radikal über $K_i(M)$. Wegen

$$K_i(M)(r) = K_i(M, r) = K_i(r)(M) = K_{i+1}(M)$$

entsteht $K_{i+1}(M)$ durch Adjunktion eines Radikals an $K_i(M)$. Also ist $K_{i+1}(M)|K_i(M)$ eine Radikalerweiterung. ■

Das folgende Korollar ermöglicht es uns, Galoistheorie bei der Behandlung von Radikaltürmen einzusetzen. Im Beweis bilden wir geeignete Translate von Radikaltürmen und setzen diese aufeinander.

Korollar 38.14 *Sei $K = K_0 \Rrightarrow K_n$ ein Radikalturm über dem Körper K. Dann lässt sich dieser Turm zu einem Radikalturm $K = K_0 \Rrightarrow K_s$ mit $s \geq n$ fortsetzen, so dass die Erweiterung $K_s|K$ galoissch ist.*

Beweisskizze. Die Erweiterung $K_n|K$ ist endlich und separabel. Nach dem Satz vom primitiven Element gibt es daher ein $\alpha \in K_n$ mit $K_n = K(\alpha)$. Seien $m \in K[X]$ das Minimalpolynom von α und β eine beliebige Nullstelle von m. Nach Kronecker 22.11 existiert dann ein K-Isomorphismus $\varphi : K(\alpha) \to K(\beta)$ mit $\varphi(\alpha) = \beta$. Wir wenden φ auf den Radikalturm $K = K_0 \Rrightarrow K_n = K(\alpha)$ an. Da das Bild eines Radikals unter φ wieder ein Radikal ist, entsteht so der Radikalturm

$$K = \varphi(K) = \varphi(K_0) \Rrightarrow \varphi(K_n) = \varphi(K(\alpha)) = K(\varphi(\alpha)) = K(\beta).$$

Diese Konstruktion liefert zu jeder Nullstelle β von m einen Radikalturm $K \Rrightarrow K(\beta)$, also insgesamt $\deg m$ viele.

Wir skizzieren nun, wie sich diese Türme aufeinandersetzen lassen:
Seien α, β, γ drei verschiedene Nullstellen von m. Dann gibt es die drei Radikaltürme

$$T_1 : K \Rrightarrow K(\alpha), \qquad T_2 : K \Rrightarrow K(\beta) \qquad \text{und} \qquad T_3 : K \Rrightarrow K(\gamma).$$

Wir bilden das Translat von T_2 mit α und bezeichnen es mit T_2'. Dann startet T_2' mit $K(\alpha)$ und endet mit $K(\beta)(\alpha) = K(\alpha, \beta)$. Analog bilden wir T_3' als Translat von T_3 mit $\{\alpha, \beta\}$. Nach 38.13 entstehen so Radikaltürme, und zwar

$$T_1 : K \Rrightarrow K(\alpha), \qquad T_2' : K(\alpha) \Rrightarrow K(\alpha, \beta) \qquad \text{und} \qquad T_3' : K(\alpha, \beta) \Rrightarrow K(\alpha, \beta, \gamma).$$

Diese „kleben“ wir nun an den Körpern $K(\alpha)$ und $K(\alpha, \beta)$ aneinander und erhalten den Radikalturm $K \Rrightarrow K(\alpha, \beta, \gamma)$.

Obige Konstruktion lässt sich auf alle Nullstellen von m ausdehnen. Dann entsteht ein Radikalturm $K \Rrightarrow L$, wobei L den Zerfällungskörper von m bezeichnet. Die Erweiterung $L|K$ ist galoissch. Nach Konstruktion setzt $K \Rrightarrow L$ den gegebenen Turm $K \Rrightarrow K_n = K(\alpha)$ fort. ■

Wir wollen die Situation aus obigem Korollar sprachlich einfacher fassbar machen:

Definition 38.15 *Wir nennen einen Radikalturm $K \Rrightarrow L$* ***galoissch****, wenn die Körpererweiterung $L|K$ galoissch ist. Unter der* ***Galoisgruppe eines*** *solchen* ***Radikalturms*** *verstehen wir die Gruppe* $\mathrm{Gal}(L|K)$.
Obiges Korollar sagt also aus, dass jeder Radikalturm unterer Teilturm eines galoisschen Radikalturms ist.

Wir definieren galoissche Radikaltürme und deren Galoisgruppen nur über Start- und Endkörper der Türme. Aus dem Hauptsatz der Galoistheorie folgt daher direkt:

Korollar 38.16 *Sei $K_0 \Rrightarrow K_n$ ein galoisscher Radikalturm mit Galoisgruppe G. Dann gelten für jedes $i \in \{0, 1, \dots, n\}$:*

(a) *Auch $K_i \Rrightarrow K_n$ ist ein galoisscher Radikalturm. Seine Galoisgruppe ist eine Untergruppe von G.*

(b) *Sei $K_i|K_0$ normal. Dann ist $K_0 \Rrightarrow K_i$ ein galoisscher Radikalturm. Seine Galoisgruppe ist zu einer Faktorgruppe von G isomorph, nämlich zu $G/\mathrm{Gal}(K_n|K_i)$.*

39. Auflösbarkeit durch Radikale

Worum geht es? Wir zeigen, dass sich ineinander verschachtelte Wurzelausdrücke mit Hilfe von Radikaltürmen beschreiben lassen. Dies motiviert unsere Definition der *Auflösbarkeit durch Radikale*.
Danach führen wir unsere Resultate über auflösbare Gruppen und Radikaltürme zusammen und beweisen den *Hauptsatz über Auflösbarkeit durch Radikale*. Mit dem *Satz von Abel-Ruffini* leiten wir eine Schranke für die Existenz von Lösungsformeln rationaler Polynome her. ⁜

Der Auflösbarkeits-Begriff

Radikaltürme liefern eine rein algebraische Beschreibung ineinander verschachtelter Wurzelausdrücke:
Sei $K_0 \Rrightarrow K_n$ ein Radikalturm. Dann entstehen die Teilerweiterungen $K_{i+1}|K_i$ durch das Ziehen einer Wurzel aus einem Element aus K_i. Dieses Element kann aber selbst aus Wurzeln zusammengesetzt sein, die zuvor adjungiert wurden. K_{i+1} kann daher Wurzeln enthalten, deren Radikanten selbst Wurzelausdrücke sind. Mit wachsendem i können so immer kompliziertere ineinander verschachtelte Wurzelausdrücke dargestellt werden. ⁉

Beispiel 39.1 Gauß hat gezeigt, dass sich $\cos\left(\frac{2\pi}{17}\right)$ in der Form

$$\frac{1}{16}\left(-1+\sqrt{17}+\underbrace{\sqrt{2\left(17-\sqrt{17}\right)}}_{=:a}+2\underbrace{\sqrt{17+3\sqrt{17}}}_{=:b}-\sqrt{\underbrace{2\left(17-\sqrt{17}\right)-2\sqrt{2\left(17+\sqrt{17}\right)}}_{=:c}}\right)$$

darstellen lässt. Setzen wir

$$K_0 := \mathbb{Q}, \quad K_1 := K_0(\sqrt{17}), \quad K_2 := K_1\left(\sqrt{2(17+\sqrt{17})}\right), \quad K_3 := K_2(a), \quad K_4 := K_3(b)$$

und $K_5 := K_4(c)$, so erhalten wir den Radikalturm $\mathbb{Q} = K_0 \Rrightarrow K_5$. Im Körper K_5 ist das Element $\cos\left(\frac{2\pi}{17}\right)$ enthalten.
Dieser Radikalturm ist auch ein 2-Körperturm, vgl. 21.7. Dies zeigt, dass $\cos\left(\frac{2\pi}{17}\right)$ und somit auch das regelmäßige Siebzehneck mit Zirkel und Lineal konstruierbar sind. ⁉ ⁜

Diese Überlegungen motivieren die folgende Definition:

Definition 39.2 *Seien K ein Körper und a ein Element aus dem algebraischen Abschluss von K. Wir nennen a **über K durch Radikale darstellbar**, wenn ein Radikalturm $K \Rrightarrow L$ existiert, so dass $a \in L$ gilt.*

Bemerkung 39.3 Sei a über dem Körper K durch Radikale darstellbar. Dann ist a in einem Radikalturm über K enthalten und separabel über K. Dies ist mathematisch angenehm, schränkt die Menge der durch Radikale darstellbaren Elemente aber ein:
Für eine Primzahl $p \in \mathbb{P}$ und ein über $\mathbb{F}_p$ transzendentes Element t betrachten wir das Polynom $f := X^p - t \in \mathbb{F}_p(t)[X]$, vgl. 25.18. Beachten Sie, dass f *kein* reines Polynom ist. ⁉

Wir können zwar jede Nullstelle von f als p-te Wurzel aus t auffassen, $\sqrt[p]{t}$ ist jedoch *kein* Radikal über $\mathbb{F}_p(t)$. Da die Erweiterung $\mathbb{F}_p(\sqrt[p]{t})|\mathbb{F}_p(t)$ inseparabel ist, ist $\sqrt[p]{t}$ auch nicht durch Radikale über $\mathbb{F}_p(t)$ darstellbar. ⁜

Wir kommen zur zentralen Definition in der Theorie der durch Radikale auflösbaren Gleichungen. Sie besagt, dass wir ein Polynom durch Radikale auflösbar nennen, wenn sich alle seine Nullstellen durch Radikale darstellen lassen. Bei solchen Polynomen kann man also alle Nullstellen als ineinander verschachtelte Wurzelausdrücke schreiben.

Definition 39.4 *Seien K ein Körper und $f \in K[X]$ ein Polynom. Wir nennen f* ***durch Radikale auflösbar****, wenn jede Nullstelle von f über K durch Radikale darstellbar ist.*
Wegen 38.14 ist dies gleichbedeutend damit, dass ein galoisscher Radikalturm $K \Rrightarrow L$ existiert, so dass der Zerfällungskörper von f ein Unterkörper von L ist. ⁉

Beispiel 39.5 Sei K ein Körper, in dem $2 \neq 0$ gelte, der also nicht Charakteristik Zwei besitze. Mit Hilfe von quadratischer Ergänzung sieht man, dass jedes Polynom $f \in K[X]$ mit $\deg f = 2$ durch Radikale auflösbar ist. ⁜

Knobelfrage. Wo wird im Beispiel die Voraussetzung $2 \neq 0$ benötigt? ⁉

Der Hauptsatz über Auflösbarkeit durch Radikale, Teil 1

Wir beweisen nun den Hauptsatz der Theorie der Auflösbarkeit durch Radikale. Grob gesprochen sagt er, dass ein Polynom genau dann durch Radikale auflösbar ist, wenn seine Galoisgruppe auflösbar ist. Die wesentlichen Hilfsmittel für seinen Beweis sind der Satz von Kummer und die Auflösbarkeit der Galoisgruppen reiner Polynome.
Wir zerlegen den Hauptsatz in zwei Teilresultate, die wir getrennt beweisen.
Im Beweis des ersten Resultats spielt der Satz von Kummer in der Formulierung aus 38.6 eine zentrale Rolle. Dies erzwingt die Nicht-Teilbarkeitsvoraussetzung im Satz: Wir benötigen Elemente mit passender multiplikativer Ordnung. Für deren Existenz muss die Teilerfremdheit dieser Ordnung zur Charakteristik des Körpers sichergestellt werden.

Satz 39.6 (Hauptsatz über Auflösbarkeit durch Radikale, Hinrichtung) *Seien K ein Körper, $f \in K[X]$ und Z der Zerfällungskörper von f. Die Erweiterung $Z|K$ sei galoissch, die Charakteristik von K sei kein Teiler der Ordnung der Galoisgruppe $G := \mathrm{Gal}(Z|K)$. Dann gilt:*
Ist G auflösbar, so ist f durch Radikale auflösbar.

Beweis. Der Beweis der Aussage läuft in zwei Schritten ab. Als erstes adjungiert man ein Element ξ mit multiplikativer Ordnung n an K und ermöglicht so die Anwendung des Satzes von Kummer. Diesen benutzt man im Anschluss, um einen Radikalturm über K zu konstruieren, der den Zerfällungskörper von f enthält.

Schritt 1 Sei $n := |G|$ die Ordnung von G. Aufgrund der Charakteristik-Voraussetzung im Satz existiert ein Element ξ im algebraischen Abschluss von K mit multiplikativer Ordnung n, vgl. 37.10 (a). Wir setzen nun $K_0 := K$ und $K_1 := K(\xi)$. Da ξ eine Nullstelle des Polynoms $X^n - 1 \in K[X]$ ist, ist $K_1|K_0$ eine Radikalerweiterung.

Schritt 2 Um das Element ξ in der Erweiterung $Z|K$ zur Verfügung zu haben, bilden wir das Translat von $Z|K$ mit ξ. Wir erhalten die Erweiterung $Z(\xi)|K_1$. Mit Translationssatz ist diese galoissch, ihre Galoisgruppe $U := \mathrm{Gal}(Z(\xi)|K_1)$ ist isomorph zu einer Untergruppe von G, also nach 35.11 ebenfalls auflösbar. Sei

$$\{1\} = U_s \overset{p_{s-1}}{\lhd} U_{s-1} \overset{p_{s-2}}{\lhd} \cdots \overset{p_3}{\lhd} U_3 \overset{p_2}{\lhd} U_2 \overset{p_1}{\lhd} U_1 = U$$

eine Auflösung von U. Für $i \in \{1, 2, \dots, s\}$ setzen wir $K_i := \mathrm{Fix}(U_i)$. Dann gelten für alle i die folgenden Aussagen:

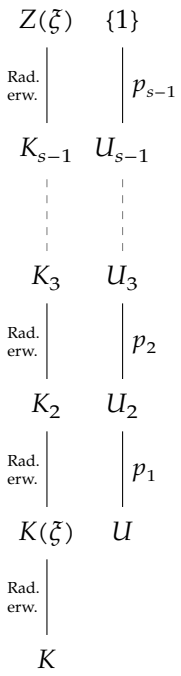
(a) Die Körpererweiterung $K_{i+1}|K_i$ hat Grad $[U_i : U_{i+1}] = p_i \in \mathbb{P}$.

(b) Da U_{i+1} ein Normalteiler von U_i ist, ist $K_{i+1}|K_i$ eine Galoiserweiterung. Zusammen mit (a) folgt, dass $\mathrm{Gal}(K_{i+1}|K_i)$ zyklisch von Ordnung p_i ist.

(c) K_i enthält ein Element der Ordnung p_i, beispielsweise ξ^{n/p_i}.

Aus (a)–(c) und Kummer 38.6 ergibt sich, dass die Erweiterungen $K_{i+1}|K_i$ für beliebiges $i \in \{1, 2 \dots, s-1\}$ Radikalerweiterungen sind. Daher ist $K = K_0 \Rrightarrow K_s = Z(\xi)$ ein Radikalturm.

Der Zerfällungskörper Z von f ist ein Unterkörper von $K_s = Z(\xi)$. Dies zeigt, dass f durch Radikale auflösbar ist. ■



Bemerkung 39.7 In der Literatur wird 39.6 oft nur für Charakteristik-Null-Körper formuliert. Wir formulieren den Satz allgemeiner, erkaufen uns dies aber mit zwei Einschränkungen:

(a) Um Galoistheorie anwenden zu können, müssen wir fordern, dass $Z|K$ galoissch ist. Dies ist in Charakteristik Null immer erfüllt, denn dort ist durch jedes Polynom eine Galoiserweiterung gegeben, vgl. 27.4.

(b) Um Kummer-Theorie anwenden zu können, müssen Elemente mit passender multiplikativer Ordnung existieren. Dies stellen wir sicher, indem wir fordern, dass die Ordnung von G, also der Grad von $Z|K$, kein Vielfaches der Charakteristik von K ist. In Charakteristik Null ist dies ebenfalls immer erfüllt. ※

Mit diesen Überlegungen formulieren wir 39.6 in Charakteristik Null:

Korollar 39.8 *Seien K ein Körper der Charakteristik Null und $f \in K[X]$. Dann gilt: Ist $\mathrm{Gal}(f|K)$ auflösbar, so ist f durch Radikale auflösbar.*

Der casus irreducibilis

Wir sehen in den Übungen, dass es ein irreduzibles Polynom $f \in \mathbb{Q}[X]$ von Grad 3 gibt, dessen Galoisgruppe G isomorph zu C_3 ist. → Übung
Sei Z der Zerfällungskörper von f. Dann ist Z ein Unterkörper von $\mathbb{R}$, denn ansonsten müsste die Ordnung von G nach 28.9 gerade sein. Also sind alle Nullstellen von f reell.

Da G auflösbar ist, ist f durch Radikale auflösbar. Allerdings ist $Z|\mathbb{Q}$ *keine* Radikalerweiterung:
Angenommen, wir könnten Z in der Form $Z = \mathbb{Q}(r)$ mit einer Nullstelle r eines reinen Polynoms $g := X^n - a \in \mathbb{Q}[X]$ schreiben. Wir bezeichnen das Minimalpolynom von r mit $m \in \mathbb{Q}[X]$. Da g das Element r annulliert, gilt $m \mid g$. Die Nullstellen von m sind daher auch Nullstellen von g und haben die Form aus 38.8 (b). Insbesondere kann m maximal zwei reelle Nullstellen besitzen. Allerdings ist ?

$$\deg m = [\mathbb{Q}(r) : \mathbb{Q}] = [Z : \mathbb{Q}] = 3.$$

m besitzt daher mindestens eine echt-komplexe Nullstelle. Dies widerspricht aber der Normalität der Erweiterung $Z|\mathbb{Q}$.

Dies zeigt: Die Nullstellen von f lassen sich durch Radikale über $\mathbb{Q}$ darstellen, jedoch enthält der Körper Z keine passenden Radikale, um diese Darstellungen zu erreichen. Analysieren wir den Beweis von 39.6, so stellen wir fest, dass wir den Radikalturm

$$\mathbb{Q} \subseteq \mathbb{Q}(\xi) \subseteq Z(\xi) \qquad \text{mit einer dritten primitiven Einheitswurzel } \xi$$

benötigen, um die Nullstellen von f durch Radikale über $\mathbb{Q}$ auszudrücken. Wir benötigen somit echt komplexe Zahlen aus $Z(\xi)$, um die *reellen* Nullstellen von f durch Radikale darstellen zu können.

Sind Radikaldarstellungen reeller Nullstellen eines Polynoms nur mit Hilfe von echt-komplexen Radikalen möglich, so spricht man vom **casus irreducibilis**, dem nicht (auf $\mathbb{R}$) zurückführbaren Fall. Historisch wurde er das erste mal bei Grad-3-Polynomen beobachtet und war lange Zeit unerklärlich. Er hat dazu beigetragen, dass komplexe Zahlen zum Allgemeingut in der Mathematik wurden, aber auch die anfängliche „Mystifizierung“ der komplexen Zahlen verstärkt.

Der Hauptsatz über Auflösbarkeit durch Radikale, Teil 2

Jetzt zeigen wir, dass durch Radikale auflösbare Polynome auch auflösbare Galoisgruppen besitzen. Dies kehrt die Aussage aus 39.6 (zumindest in Charakteristik Null) um.

Wir benötigen hierfür das nachstehende Lemma. Sein Beweis zehrt von der Tatsache, dass reine Polynome auflösbare Galoisgruppen besitzen.

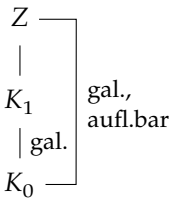
Lemma 39.9 *Sei $K_0 \Rrightarrow K_n$ ein galoisscher Radikalturm. Dann ist seine Galoisgruppe auflösbar.*

Beweis. Wir beweisen die Behauptung per Induktion nach n.

Ind.anf. Sei $n = 1$. Es ist zu zeigen, dass $\mathrm{Gal}(K_1|K_0)$ auflösbar ist.

K_1 entsteht durch Adjunktion eines Radikals an K_0. Es existieren also ein reines Polynom $f \in K_0[X]$ und eine Nullstelle r von f mit $K_1 = K_0(r)$.
Sei Z der Zerfällungskörper von f. Nach 38.10 ist die Erweiterung $Z|K_0$ galoissch mit auflösbarer Galoisgruppe G. Da r eine Nullstelle von f ist, gelten $r \in Z$ und

folglich $K_1 = K_0(r) \subseteq Z$.
Nach Voraussetzung ist $K_1|K_0$ galoissch. Daher ist $\mathrm{Gal}(K_1|K_0)$ zu einer Faktorgruppe der auflösbaren Gruppe G isomorph. Also ist $\mathrm{Gal}(K_1|K_0)$ auflösbar.



Ind.vor.: Für ein $n \in \mathbb{N}$ und beliebige galoissche Radikaltürme $K_1 \Rrightarrow K_{n+1}$ gelte nun: $\mathrm{Gal}(K_{n+1}|K_1)$ sei auflösbar.

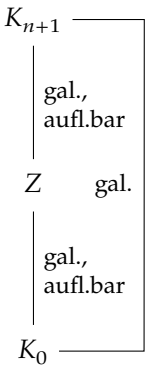
Machen Sie sich klar, dass wir hier die Nummerierung der Körper ändern. Warum klappt der Induktionsbeweis trotzdem?

Ind.schluss: Sei $K_0 \Rrightarrow K_{n+1}$ ein galoisscher Radikalturm. Zu zeigen ist, dass seine Galoisgruppe $\mathrm{Gal}(K_{n+1}|K_0)$ auflösbar ist. Hierzu konstruieren wir einen geeigneten Zwischenkörper der Erweiterung $K_{n+1}|K_0$:

Es ist $K_1 = K_0(r)$, wobei r Nullstelle eines reinen Polynoms $f \in K_0[X]$ ist. Sei $m \in K_0[X]$ das Minimalpolynom von r über K_0. Da die Erweiterung $K_{n+1}|K_0$ normal ist, zerfällt m vollständig über K_{n+1}. Der Zerfällungskörper Z von m ist somit ein Unterkörper der Erweiterung $K_{n+1}|K_0$.
Da Z auch Unterkörper des Zerfällungskörpers von f ist, ist $\mathrm{Gal}(Z|K_0)$ zu einer Faktorgruppe der nach 38.10 auflösbaren Gruppe $\mathrm{Gal}(f|K_0)$ isomorph. Also ist $\mathrm{Gal}(Z|K_0)$ auflösbar.

Wir bilden nun das Translat des galoisschen Radikalturms $K_1 \Rrightarrow K_{n+1}$ mit Z und erhalten den Körperturm

$$K_1(Z) \overset{K_1 \subseteq Z}{=} Z \subseteq K_2(Z) \subseteq \cdots \subseteq K_n(Z) \subseteq K_{n+1}(Z) \overset{Z \subseteq K_{n+1}}{=} K_{n+1}.$$



Dieser ist nach 38.13 ein Radikalturm, der nach Translationssatz sogar galoissch ist. Nach Induktionsvoraussetzung ist $\mathrm{Gal}(K_{n+1}|Z)$ auflösbar.

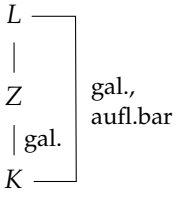
Insgesamt haben wir also in der Galoiserweiterung $K_{n+1}|K_0$ einen Zwischenkörper Z konstruiert, so dass die Erweiterungen $K_{n+1}|Z$ und $Z|K_0$ beide galoissch mit auflösbarer Galoisgruppe sind. Nach 35.12 ist dann auch $\mathrm{Gal}(K_{n+1}|K_0)$ auflösbar, was den Beweis abschließt.

■

Nachdem die ganzen technischen Details im Beweis des obigen Lemmas verpackt sind, können wir die Rückrichtung des Hauptsatzes sehr elegant beweisen:

Satz 39.10 (Hauptsatz über Auflösbarkeit durch Radikale, Rückrichtung) *Seien K ein Körper, $f \in K[X]$ ein durch Radikale auflösbares Polynom und Z der Zerfällungskörper von f. Dann gilt: Die Erweiterung $Z|K$ ist galoissch und besitzt eine auflösbare Galoisgruppe.*

Beweis. f ist durch Radikale auflösbar. Also existiert ein galoisscher Radikalturm $K \Rrightarrow L$ mit $Z \subseteq L$.
$Z|K$ ist galoissch und untere Teilerweiterung von $L|K$. Die Galoisgruppe $\mathrm{Gal}(Z|K)$ ist daher isomorph zu einer Faktorgruppe von $\mathrm{Gal}(L|K)$. Nach 39.9 ist $\mathrm{Gal}(L|K)$ auflösbar. 35.11 liefert die Auflösbarkeit von $\mathrm{Gal}(Z|K)$ und schließt den Beweis ab.



Für Charakteristik-Null-Körper haben wir damit folgende Charakterisierung erreicht:

Korollar 39.11 *Seien K ein Körper der Charakteristik Null und $f \in K[X]$. Dann gilt:*

$$f \text{ ist durch Radikale auflösbar} \iff \mathrm{Gal}(f|K) \text{ ist auflösbar}.$$

Der Satz von Abel-Ruffini

Sind K ein Charakteristik-Null-Körper und $f \in K[X]$ ein Polynom mit $\deg f \leq 4$, so ist $\mathrm{Gal}(f|K)$ isomorph zu einer Untergruppe der S_n mit $n \leq 4$. Alle diese Gruppen sind auflösbar. Wir können daher festhalten:

Satz 39.12 *In Charakteristik Null sind alle Polynome f mit $\deg f \leq 4$ durch Radikale auflösbar.*

Tatsächlich kann man explizite Formeln angeben, die die Nullstellen dieser Polynome durch Wurzelausdrücke darstellen. Aus der Schule ist Ihnen für $\deg f = 2$ die Mitternachtsformel bekannt. Im Jahr 1545 veröffentlichte Gerolamo Cardano sein Buch *Ars magna*. Dort finden sich vollständige Lösungsformeln für den Fall $\deg f \in \{3, 4\}$.

Wir haben in 34.8 gesehen, dass es ein Polynom $f \in \mathbb{Q}[X]$ mit $\deg f = 5$ und $\mathrm{Gal}(f|\mathbb{Q}) \cong S_5$ gibt. Da die einfache Gruppe A_5 eine Untergruppe von S_5 ist, ist $\mathrm{Gal}(f|\mathbb{Q})$ nicht auflösbar. Hieraus folgt:

Satz 39.13 (Abel-Ruffini) *Es gibt ein rationales Polynom mit Grad 5, das nicht durch Radikale auflösbar ist.*

Natürlich sind dann auch die Polynome $X^k \cdot f$ mit $k \in \mathbb{N}_0$ nicht durch Radikale auflösbar. Dies liefert:

Korollar 39.14 (Abel-Ruffini) *Zu jeder natürlichen Zahl $n \geq 5$ gibt es ein rationales Polynom f mit $\deg f = n$, das nicht durch Radikale auflösbar ist.*

Dieses Resultat zeigt, dass keine allgemeinen Lösungsformeln für rationale Polynome f mit $\deg f \geq 5$ geben kann. Mit den Formeln von Cardano hat die Suche nach allgemeinen Lösungsformeln rationaler Polynome also ihren Abschluss gefunden.

Knobelfrage. Das rationale Polynom $f := \prod_{i=1}^{1\,000} (X - i)$ hat einen hohen Grad, aber dennoch sehr einfach angebbare Nullstellen. Warum ist das kein Widerspruch zur Nichtexistenz allgemeiner Lösungsformeln?

Teil VI.
Zahlentheorie

In diesem Abschnitt untersuchen wir den Ring $\mathbb{Z}$ und seine Faktorringe $\mathbb{Z}_n$ genauer. Zunächst beschäftigen wir uns mit dem Lösen von *Kongruenzsystemen*. Als Anwendung stellen wir unter anderem das *RSA-Verfahren* zum Verschlüsseln von Nachrichten vor. Danach bestimmen wir die Isomorphietypen der Gruppen $\mathbb{Z}_n^\times$ und zeigen, dass sie für ungerade Primpotenzen n zyklisch sind. Dieses fundamentale Resultat der Zahlentheorie benötigen wir in vielen Beweisen, unter anderem auch, wenn wir den *Miller-Rabin-Test* zum Finden großer Primzahlen vorstellen und die Güte des Tests untersuchen.
Nachdem wir in den Übungen die Lösungstheorie linearer Kongruenzen hergeleitet haben, behandeln wir dieselbe Frage für quadratische Kongruenzen. Dies führt auf eine reichhaltige Theorie, die über verschiedene Reduktionsresultate und das *Legendre-Symbol* zum *quadratischen Reziprozitätsgesetz* führt. Dessen Verallgemeinerungen gehören zu den tiefsten Resultaten der Zahlentheorie.

→ Übung

Eine wichtige Technik, die uns in vielen Beweisen begegnen wird, ist das Übersetzen von ganzen Zahlen in Restklassen und, umgekehrt, das Auswählen von geeigneten ganzzahligen Vertretern aus Restklassen. Vom abstrakt-algebraischen Standpunkt aus lässt sich dies durch den kanonischen Epimorphismus $\mathbb{Z} \to \mathbb{Z}_n$ beschreiben. In der Zahlentheorie wird er jedoch selten explizit verwendet, sondern verbirgt sich in der häufig benutzten *Gaußschen Kongruenzschreibweise*.
Sie ist (wahrscheinlich) mit dafür verantwortlich, warum in der Zahlentheorie oft nicht strikt zwischen ganzer Zahl und Restklasse unterschieden wird. Dies kann befremdlich wirken, wenn man bisher vorwiegend Algebra betrieben hat und die dort herrschende Exaktheit gewöhnt ist.
Um den Einstieg in die Zahlentheorie zu erleichtern, achten wir auf eine strikte Trennung zwischen ganzen Zahlen und Restklassen. Hierzu stellen wir viele zahlentheoretische Begriffe in zwei inhaltlich äquivalenten Versionen bereit, einmal für Restklassen, einmal für ganze Zahlen. Die letztere Variante machen wir durch ein nachgestelltes *modulo n* kenntlich.
Beispielsweise bezeichnen wir manche Elemente von $\mathbb{Z}_n$ als *Einheiten* (und meinen diejenigen $\overline{a} \in \mathbb{Z}_n$ mit $\mathrm{ggT}(a,n) = 1$), sprechen aber auch von *Einheiten modulo n* (und meinen diejenigen ganzen Zahlen $a \in \mathbb{Z}$ mit $\mathrm{ggT}(a,n) = 1$). Es ist klar, dass $\overline{a} \in \mathbb{Z}_n$ genau dann eine Einheit ist, wenn $a \in \mathbb{Z}$ eine Einheit modulo n ist.

40. Kongruenzen

Worum geht es? Die Grundlagen der elementaren Zahlentheorie haben wir bereits in Vorlesung 3 und auf Seite 43 gelegt. Wir führen jetzt die *Gaußsche Kongruenzschreibweise* ein und beschäftigen uns mit Gleichungssystemen, die aus Kongruenzen aufgebaut sind. Als wichtiges Hilfsmittel lernen wir den *chinesischen Restsatz für Kongruenzen* kennen.⁕

Kongruenzschreibweise

Die auf Gauß zurückgehende Kongruenzschreibweise wird in der Zahlentheorie oft benutzt.

Definition 40.1 *Seien $n \in \mathbb{N}$ eine natürliche Zahl und $a, b \in \mathbb{Z}$ ganze Zahlen. Man schreibt*

$$a \equiv b \pmod{n}$$

*und sagt, dass **a und b kongruent modulo n** seien, wenn die Differenz $b - a$ von n geteilt wird. In diesem Kontext bezeichnet man n auch als den zugrunde liegenden **Modul**.*

Bemerkung 40.2 (a) Die Kongruenzschreibweise stellt eine weitere Schreibweise für das Faktum dar, dass a und b bezüglich n denselben Rest besitzen. Die folgenden Aussagen sind daher äquivalent:

- $a \equiv b \pmod{n}$.
- $a \bmod n = b \bmod n$, vgl. 3.3.
- In $\mathbb{Z}_n$ gilt $\overline{a} = \overline{b}$.
- Die Mengen $a + n\mathbb{Z}$ und $b + n\mathbb{Z}$ sind gleich.
- Es ist $n \mid b - a$.

(b) Die Rechenregeln für den Ring $\mathbb{Z}_n$ aus 4.10 übersetzen sich in die **Ersetzungsregeln der Kongruenzschreibweise**: Seien $a \equiv b \pmod{n}$ und $x \equiv y \pmod{n}$. Dann gilt in $\mathbb{Z}_n$

$$\overline{a} = \overline{b} \text{ und } \overline{x} = \overline{y} \qquad \text{und somit} \qquad \overline{ax} = \overline{a} \cdot \overline{x} = \overline{b} \cdot \overline{y} = \overline{by}.$$

Also ist $ax \equiv by \pmod{n}$. Analog sieht man $a + x \equiv b + y \pmod{n}$.

In der Kongruenzschreibweise können in Summen und Produkten also Elemente durch kongruente Elemente ersetzen werden. ⁉

(c) Der Vorteil der Kongruenzschreibweise besteht darin, dass in $\mathbb{Z}$ gearbeitet wird, jedoch trotzdem Methoden aus $\mathbb{Z}_n$ verwendet werden können, da die ganze Zahl a nach (b) jederzeit durch ein beliebiges Element $b \in \mathbb{Z}$ mit $a \equiv b \pmod{n}$ ersetzt werden kann. ⁕

Beispiel 40.3 Es ist

$$1002 + 102 \cdot 51 \cdot 49 \equiv 2 + 2 \cdot 1 \cdot (-1) = 2 - 2 \equiv 0 \pmod{50}.$$ ※

Der folgende Satz liefert eine weitere Rechenregel für die Kongruenzschreibweise und somit auch für die Ringe $\mathbb{Z}_n$. Seine Aussage und sein Beweis sind eng mit dem Satz von Fermat 24.5 verwandt.

Satz 40.4 (Euler-Fermat) *Sei $n \in \mathbb{N}$ eine natürliche Zahl. Die ganze Zahl $a \in \mathbb{Z}$ sei teilerfremd zu n. Bezeichnen wir mit φ die Eulersche φ-Funktion, so gilt*

$$a^{\varphi(n)} \equiv 1 \pmod{n} \qquad \text{bzw. in } \mathbb{Z}_n\text{:} \qquad \overline{a}^{\,\varphi(n)} = \overline{1}.$$

Beweisskizze. Aufgrund der Teilerfremdheit ist $\overline{a}$ ein Element der Gruppe $\mathbb{Z}_n^\times$. Diese hat Ordnung $\varphi(n)$. Nach Lagrange ist daher $a^{\varphi(n)} \equiv 1 \pmod{n}$. ■

Knobelfrage. Der Beweis von 24.5 benutzt die Gruppe $\mathbb{F}_q^\times$, obiger Beweis die Gruppe $\mathbb{Z}_n^\times$. Wann sind beide Gruppen (und daher auch die Beweise und letztlich die Aussagen der Sätze) identisch? ⁉

Staatsexamensaufgabe (Teil (a) von H2020T2A1) *Bestimmen Sie das $a \in \{0, 1, \dots, 5\}$ mit $3^{2020} \equiv a \pmod{7}$.*

Drei ist teilerfremd zum Modul Sieben. Wir können daher den Satz von Euler-Fermat anwenden und erhalten zusammen mit $\varphi(7) = 6$

$$3^{2020} = 3^{6 \cdot 336 + 4} = (3^6)^{336} \cdot 3^2 \cdot 3^2 \overset{3^6 \equiv 1}{\equiv} 1 \cdot 9 \cdot 9 \equiv 2 \cdot 2 = 4 \pmod{7}.$$

Da 3^{2020} nur zu genau einem Element aus $\{0, 1, \dots, 5\}$ kongruent sein kann, gilt daher eindeutig $a = 4$. ⁉ ※

Kongruenzsysteme

Eine Gleichung über den komplexen Zahlen kann man oft lösen, indem man sie in Real- und Imaginärteil zerlegt und so zu einem Gleichungssystem übergeht. Wendet man dieses Verfahren beispielsweise auf die Gleichung $z^2 = 3 - 4i$ an, schreibt also $z = a + bi$ und teilt dann in Real- und Imaginärteil auf, so folgt das Gleichungssystem

$$\left\{ \begin{array}{lcl} a^2 - b^2 & = & 3 \\ 2ab & = & -4 \end{array} \right\}.$$

Es ist über $\mathbb{R}$ definiert und lässt sich recht einfach lösen. ⁉

Wir stellen nun eine ähnliche Technik für Kongruenzen bereit. Sie bildet aus einer Kongruenz mit einem großen Modul ein äquivalentes Kongruenzsystem mit kleineren Moduln.

Satz 40.5 *Die natürliche Zahl n sei zerlegt in der Form $n = n_1 \cdots n_r$ mit paarweise teilerfremden $n_i \in \mathbb{N}$. Für beliebige $a, x \in \mathbb{Z}$ gilt dann: Die Kongruenz $x \equiv a \pmod{n}$ ist genau dann erfüllt, wenn die Kongruenzen $x \equiv a \pmod{n_i}$ für alle $i \in \{1, 2, \dots, r\}$ gelten.*
Es gilt also die Äquivalenz

$$x \equiv a \pmod{n} \iff \left\{ \begin{array}{lcll} x & \equiv & a & \pmod{n_1} \\ \vdots & \vdots & \vdots & \\ x & \equiv & a & \pmod{n_r} \end{array} \right\}$$

Beweis.

$\Longrightarrow$ Gilt $x \equiv a \pmod{n}$, so ist $n \mid a - x$. Da jedes der n_i ein Teiler von n ist, folgt $n_i \mid a - x$ für jedes i. Also ist $x \equiv a \pmod{n_i}$ für jedes i.

$\Longleftarrow$ Gilt $x \equiv a \pmod{n_i}$ für jedes i, so ist jedes der n_i ein Teiler von $a - x$. Da die n_i paarweise teilerfremd sind, ist auch das Produkt der n_i ein Teiler von $a - x$. Es gilt also $n_1 \cdots n_r = n \mid a - x$, d. h. es ist $x \equiv a \pmod{n}$. ■

Für den Beweis von „$\Longrightarrow$“ war die Teilerfremdheit der n_i gar nicht nötig. Diese Aussage gilt also für jede Zerlegung des Moduls n, was wir als eigenständiges (und ziemlich nützliches) Resultat formulieren:

Korollar 40.6 *$d \in \mathbb{N}$ teile $n \in \mathbb{N}$. Gilt dann $x \equiv a \pmod{n}$, so ist auch $x \equiv a \pmod{d}$.*

Ausgehend von einer Kongruenz $x \equiv a \pmod{n}$ liefert 40.5 ein System von Kongruenzen. Jede einzelne lässt sich unabhängig von den übrigen vereinfachen, so dass schließlich ein Kongruenzsystem der Form

$$\left\{ \begin{array}{lcll} x & \equiv & a_1 & \pmod{n_1} \\ \vdots & \vdots & \vdots & \\ x & \equiv & a_r & \pmod{n_r} \end{array} \right\} \qquad (\star)$$

mit irgendwelchen ganzen Zahlen $a_1, \dots, a_r \in \mathbb{Z}$ entsteht.
Der nächste Satz klärt, wann eine Lösung $x \in \mathbb{Z}$ für dieses System existiert und wie in diesem Fall die Lösungsmenge von $(\star)$ aussieht.

Satz 40.7 *Die natürliche Zahl n sei zerlegt in der Form $n = n_1 \cdots n_r$ mit paarweise teilerfremden $n_i \in \mathbb{N}$. Seien $a_1, \dots, a_r$ beliebige ganze Zahlen. Wir bezeichnen mit*

$$\varphi : \ \mathbb{Z} \to \mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_r}, \qquad z \mapsto (\overline{z}, \dots, \overline{z})$$

den Epimorphismus aus dem chinesischen Restsatz 6.19. Dann gelten die folgenden Aussagen:

(a) *Genau die $x \in \mathbb{Z}$ mit $\varphi(x) = (\overline{a_1}, \dots, \overline{a_r})$ lösen das System $(\star)$. Die Lösungsmenge des Systems ist also durch das Urbild $\varphi^{-1}(\overline{a_1}, \dots, \overline{a_r})$ gegeben.*

(b) *Das Urbild in (a) ist nicht-leer. Jedes System der Form $(\star)$ mit paarweise teilerfremden n_i besitzt also eine Lösung.*

(c) *Sei $x \in \mathbb{Z}$ eine Lösung von $(\star)$. Dann entspricht das Urbild aus (a) dem Element $\overline{x} \in \mathbb{Z}_n$. Die Lösungsmenge des Systems ist also durch die Menge*

$$\overline{x} = x + n\mathbb{Z} = \{x + nz \mid z \in \mathbb{Z}\} \qquad \textit{mit} \qquad x = \varphi^{-1}(\overline{a_1}, \dots, \overline{a_r})$$

gegeben.
Insbesondere gilt: $(\star)$ hat unendlich viele Lösungen, aber nur genau eine Lösung, die in der Menge $\{0, 1, \dots, n-1\}$ liegt.

Beweis.

zu (a) Die ganze Zahl x ist genau dann eine Lösung von $(\star)$, wenn $\overline{x} = \overline{a_i}$ in $\mathbb{Z}_{n_i}$ für alle i gilt. Diese ganzen Bedingungen können wir in Tupel-Schreibweise äquivalent zu

$$(\overline{x}, \dots, \overline{x}) = (\overline{a_1}, \dots, \overline{a_r}) \in \mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_r}$$

umformulieren. Da $\varphi(x) = (\overline{x}, \dots, \overline{x})$ ist, folgt hieraus die Behauptung.

zu (b) Da φ als Epimorphismus surjektiv ist, ist das Urbild $\varphi^{-1}(\overline{a_1}, \dots, \overline{a_r})$ nicht-leer. Mit (a) folgt die Lösbarkeit des Systems $(\star)$.

zu (c) Sei $x \in \mathbb{Z}$ eine Lösung von $(\star)$. Dann gilt für $y \in \mathbb{Z}$

$$y \text{ löst } (\star) \overset{\text{(b)}}{\iff} \varphi(x) = \varphi(y) \overset{\text{(K)}}{\iff} y - x \in n\mathbb{Z} \iff y \in x + n\mathbb{Z} \iff y \in \overline{x}.$$

Zu (K): Die Homomorphie von φ liefert $\varphi(x) = \varphi(y) \iff \varphi(y - x) = 0$. Nach 6.19 ist $\ker \varphi = n\mathbb{Z}$, was $y - x \in n\mathbb{Z}$ zeigt.

Da $\overline{x}$ unendlich viele Elemente enthält, existieren unendlich viele Lösungen für $(\star)$. Da die Nebenklassen $\overline{0}, \overline{1}, \dots, \overline{n-1}$ paarweise verschieden sind und ganz $\mathbb{Z}_n$ liefern, liegt genau eine der ganzen Zahlen $0, 1, \dots, n-1$ in $\overline{x}$. ■

Staatsexamensaufgabe (H2011T3A4) *Beweisen Sie, dass es vier aufeinanderfolgende natürliche Zahlen n, $n+1$, $n+2$, $n+3$ gibt, die jeweils durch eine Quadratzahl > 1 teilbar sind.*

Die Quadratzahlen sind nicht näher spezifiziert, wir wählen $2^2, 3^2, 5^2, 7^2$. Die zu zeigende Aussage modellieren wir durch das Kongruenzsystem

$$\left\{\begin{array}{lcll} n & \equiv & 0 & (\mathrm{mod}\ 2^2) \\ n+1 & \equiv & 0 & (\mathrm{mod}\ 3^2) \\ n+2 & \equiv & 0 & (\mathrm{mod}\ 5^2) \\ n+3 & \equiv & 0 & (\mathrm{mod}\ 7^2) \end{array}\right\} \quad \text{oder, äquivalent,} \quad \left\{\begin{array}{lcll} n & \equiv & 0 & (\mathrm{mod}\ 2^2) \\ n & \equiv & -1 & (\mathrm{mod}\ 3^2) \\ n & \equiv & -2 & (\mathrm{mod}\ 5^2) \\ n & \equiv & -3 & (\mathrm{mod}\ 7^2) \end{array}\right\}.$$

Da die auftretenden Moduln paarweise teilerfremd sind, besitzt das System nach 40.7 eine eindeutige Lösung $n \in \{0, 1, \dots, -1 + 2^2 \cdot 3^2 \cdot 5^2 \cdot 7^2\}$. Offenbar ist $n = 0$ keine Lösung, sodass n tatsächlich eine natürliche Zahl ist. ※

Bemerkung 40.8 (a) Der chinesische Restsatz 6.19 übersetzt zwischen dem Ring $\mathbb{Z}_n$ und den Ringen $\mathbb{Z}_{n_i}$, die Sätze 40.5 und 40.7 übersetzen zwischen einer Kongruenz modulo n und Kongruenzen modulo n_i.
Wegen dieser Ähnlichkeit bezeichnet man 40.5 und 40.7 oft gemeinsam als **chinesischen Restsatz für Kongruenzen**.

(b) Im chinesischen Restsatz tritt eine Zerlegung von n in paarweise disjunkte Faktoren n_i auf. In der Praxis handelt es sich hierbei fast immer um die Primfaktorzerlegung von n; die n_i sind dann Primpotenzen.
Hier endet die Nützlichkeit des chinesischen Restsatzes, da sich Primpotenzen nicht weiter teilerfremd zerlegen lassen. ⁉

(c) In der Zahlentheorie gibt es viele Sätze, die Aussagen über die Ringe $\mathbb{Z}_q$ mit einer Primpotenz q treffen. Die Nützlichkeit dieser Sätze ergibt sich aus (b): Mit dem chinesischen Restsatz kann man viele Probleme auf Fragestellungen in solchen Ringen herunterbrechen.
Beispiele hierfür haben wir bereits gesehen: Kennt man den Isomorphietyp von $\mathbb{Z}_q^\times$ für Primpotenzen q, so kann man den Isomorphietyp von $\mathbb{Z}_n^\times$ nach 6.20 für alle $n \in \mathbb{N}$ bestimmen.
Kennt man den Wert der Eulerschen φ-Funktion für Primpotenzen, so kann man $\varphi(n)$ nach 6.21 für alle $n \in \mathbb{N}$ berechnen. ⁂

Rechnerisches Lösen von Kongruenzsystemen

Um eine Lösung des Kongruenzsystems $(\star)$ zu berechnen, muss nach 40.7 das Urbild $\varphi^{-1}(\overline{a_1}, \dots, \overline{a_r})$ berechnet werden. Dies ist einfach, wenn alle der a_i übereinstimmen; die Definition von φ liefert dann direkt $\varphi^{-1}(\overline{a}, \dots, \overline{a}) = a + n\mathbb{Z}$. Andernfalls ist die Urbild-Bestimmung komplizierter.

Beispiel 40.9 Sei $\varphi : \mathbb{Z} \to \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_5$ der Epimorphismus aus dem chinesischen Restsatz. Wir betrachten die Systeme

$$\left\{\begin{array}{rcll} x & \equiv & 9 & (\mathrm{mod}\ 2) \\ x & \equiv & 9 & (\mathrm{mod}\ 3) \\ x & \equiv & 9 & (\mathrm{mod}\ 5) \end{array}\right\} \quad \text{bzw.} \quad \left\{\begin{array}{rcll} x & \equiv & 1 & (\mathrm{mod}\ 2) \\ x & \equiv & 0 & (\mathrm{mod}\ 3) \\ x & \equiv & 4 & (\mathrm{mod}\ 5) \end{array}\right\}.$$

Beide Systeme besitzen dieselbe Lösungsmenge, da die rechten Seiten bezüglich des jeweiligen Moduls kongruent zueinander sind. Die Lösungsmenge des linken Systems lässt sich sofort bestimmen; sie ist $\varphi^{-1}(\overline{9}, \overline{9}, \overline{9}) = 9 + 2 \cdot 3 \cdot 5\mathbb{Z} = 9 + 30\mathbb{Z}$. Die Lösungsmenge des rechten Systems lässt sich nicht unmittelbar ablesen. ⁉
Dies zeigt, dass die Schwierigkeit des Lösens von Kongruenzsystemen nicht von den Nebenklassen $\overline{a_i}$, sondern von den konkret auftauchenden Nebenklassenvertretern abhängt. ⁂

Wir beschreiben nun zwei Verfahren zum Lösen von Kongruenzsystemen.

Das erste Verfahren ist ein leicht optimierter Brute-Force-Ansatz: Es werden so lange ganze Zahlen für x eingesetzt, bis eine Lösung gefunden ist. Durch Einbeziehung der einzelnen Kongruenzen lässt sich die Menge der zu testenden Zahlen einschränken. Das Verfahren eignet sich für Kongruenzsysteme mit wenigen Gleichungen und kleinen Moduln, also insbesondere für Aufgabenstellungen in Klausuren. Wir stellen das Verfahren in folgendem Beispiel vor:

Beispiel 40.10 (Urbild-Berechnung per Brute-Force) Wir wollen die Lösungsmenge des Systems

$$\left\{\begin{array}{lcll} x & \equiv & 1 \pmod 3 & \text{(I)} \\ x & \equiv & 3 \pmod 4 & \text{(II)} \\ x & \equiv & 12 \pmod{13} & \text{(III)} \end{array}\right\}$$

bestimmen.
Setze $n := 3 \cdot 4 \cdot 13 = 156$. Da die Moduln paarweise teilerfremd sind, besitzt das System nach 40.7 (c) genau eine Lösung $x \in \mathbb{Z}$ mit $0 \leq x < n$. Aus Gleichung (III) folgt, dass x von der Form $12 + 13\mathbb{Z}$ ist, d. h. es ist

$$x \in \{12, 25, 38, 51, 64, 77, 90, 103, 116, 129, 142, 155\}.$$

Wir testen, welche dieser Elemente auch Gleichung (II) genügen; diese färben wir blau ein:

x	12	25	38	51	64	77	90	103	116	129	142	155
$x \bmod 4$	0	1	2	3	0	1	2	3	0	1	2	3

Also ist $x \in \{51, 103, 155\}$. Wir testen analog mit Gleichung (I):

x	51	103	155
$x \bmod 3$	0	1	2

Die einzige Lösung x des Systems mit $0 \leq x < n$ ist also $x = 103$. Alle Lösungen des Systems sind nach 40.7 (c) gegeben durch $103 + n\mathbb{Z} = 103 + 156\mathbb{Z}$. ⋇

Das zweite Verfahren bestimmt mit Hilfe des erweiterten Euklidischen Algorithmus zunächst Lösungen für besonders einfache rechte Seiten. Aus diesen Lösungen wird dann eine Lösung des gegebenen Systems konstruiert. Das Verfahren ist etwas komplizierter als das vorhergehende, skaliert aber gut und kann auch für umfangreiche Kongruenzsysteme mit hohen Moduln eingesetzt werden.

Beispiel 40.11 Wir betrachten dasselbe Kongruenzsystem wie in 40.10 und gehen in zwei Schritten vor:

Schritt 1: Rechte Seite als Standardeinheitsvektor annehmen und Lösungen finden

Wir ersetzen die rechte Seite $(1, 3, 12)^T$ des gegebenen Systems durch den Standardeinheitsvektor $(1, 0, 0)^T$ und bestimmen eine Lösung $x_1 \in \mathbb{Z}$ des abgeänderten Systems.

Die Gleichungen (II) und (III) lauten nun $x_1 \equiv 0 \pmod 4$ bzw. $x_1 \equiv 0 \pmod{13}$ und liefern $4 \cdot 13 = 52 \mid x_1$. Es ist also $x_1 = 52z$ mit einem $z \in \mathbb{Z}$. Aus Gleichung (I) folgt

$$52 \cdot z \equiv 1 \pmod 3.$$

z ist also modulo Drei multiplikativ invers zu 52. Mit dem erweiterten Euklidischen Algorithmus erhalten wir die Bézout-Gleichung

$$1 = 1 \cdot 52 - 17 \cdot 3$$

und hieraus $z = 1$. Es gilt also $x_1 = 52$.

Nun ersetzen wir die rechte Seite durch den Standardeinheitsvektor $(0,1,0)^T$ und suchen in analoger Weise eine Lösung $x_2 \in \mathbb{Z}$ des abgeänderten Systems:
Gleichungen (I) und (III) zeigen $3 \cdot 13 = 39 \mid x_2$ und somit $x_2 = 39z$. Aus Gleichung (II) folgt, dass 39 multiplikativ invers zu z in $\mathbb{Z}_4$ ist. Euklid liefert die Bézout-Gleichung

$$1 = (-1) \cdot 39 + 10 \cdot 4,$$

aus der $z = -1$ und daher $x_2 = -39$ folgen.

Analog ergibt sich $x_3 = -12$ für den Standardeinheitsvektor $(0,0,1)^T$.

Schritt 2: Lösung $x \in \mathbb{Z}$ des gegebenen Systems aus den x_i konstruieren

Wir benutzen die Einträge der rechte Seite des gegebenen Systems als Koeffizienten für eine Linearkombination der x_i, setzen also

$$x := 1 \cdot x_1 + 3 \cdot x_2 + 12 \cdot x_3 = 52 + 3 \cdot (-39) + 12 \cdot (-12) = -209.$$

Dann ist x eine Lösung des gegebenen Systems; Einsetzen in Gleichung (II) liefert beispielsweise

$$x = 1 \cdot x_1 + 3 \cdot x_2 + 12 \cdot x_3 \overset{x_1 \equiv x_3 \equiv 0}{\equiv} 3 \cdot x_2 \overset{x_2 \equiv 1}{\equiv} 3 \pmod 4.$$

Mit 40.7 (c) ergibt sich die Lösungsmenge des Systems nun zu

$$x + n\mathbb{Z} = -209 + 156\mathbb{Z} = 103 + 156\mathbb{Z}.$$

41. Anwendungen: Secret sharing, RSA

Worum geht es? Wir stellen eine Möglichkeit vor, wie man ein Geheimnis so auf verschiedene Personen verteilen kann, dass das Geheimnis nur zu lüften ist, wenn einige der Personen zusammenarbeiten.
Außerdem stellen wir einen weit verbreiteten Algorithmus zum asymmetrischen Verschlüsseln von Daten vor. ⁂

Secret sharing

Wir wollen ein Geheimnis G in r Teile $T_1, \dots, T_r$ zerlegen, so dass G nur dann mit Sicherheit[7] rekonstruiert werden kann, wenn mindestens k der T_i bekannt sind.
Wir nehmen dabei an, dass G ein Element aus $\mathbb{N}_0$ ist. Dies ist keine Einschränkung, da sich jede Information als Datei auf einem Computer und daher als Zahl abspeichern lässt. Weiterhin ermöglicht uns diese Festsetzung, zahlentheoretische Mittel zum Zerlegen von G einzusetzen. ⁉
In den T_i codieren wir Kongruenzgleichungen mit paarweise teilerfremden Moduln. Auf die T_i, die wir kennen, können wir dann den chinesischen Restsatz für Kongruenzen anwenden. Wir skizzieren nun eine Variante des *Asmuth-Bloom's threshold secret sharing scheme*:

Ausgangssituation Seien $k, r \in \mathbb{N}$ mit $2 \leq k \leq r$. Wir wollen ein Geheimnis $G \in \mathbb{N}_0$ so auf r Kongruenzgleichungen $T_1, \dots, T_r$ aufteilen, dass sich G bei Kenntnis von mindestens k der T_i berechnen lässt.

Erzeugung der T_i Wir wählen zufällige natürliche Zahlen $M, z, n_1, \dots, n_r$, die den folgenden Bedingungen genügen:

(B1) Die Zahlen $M, n_1, \dots, n_r$ sind paarweise teilerfremd.

(B2) Es gilt $G < M < n_1 < n_2 < \cdots < n_r$.

(B3) Es gilt $S := G + z \cdot M < n_1 \cdots n_k$.

Nun berechnen wir für alle $i \in \{1, 2, \dots, r\}$ die Zahlen $s_i := S \bmod n_i$ und definieren die Tripel $T_i := (s_i, n_i, M)$.

Wir zeigen nun, dass sich G berechnen lässt, sobald mindestens k der T_i bekannt sind.

Satz 41.1 *Die T_i seien entsprechend dem obigen Schema berechnet; bekannt seien k von ihnen, nämlich $T_{i_1}, \dots, T_{i_k}$. Dann lässt sich G durch folgenden Algorithmus berechnen:*

Schritt 1: *Bilde aus jedem der bekannten Tripel $T_{i_j} = (s_{i_j}, n_{i_j}, M)$ die Kongruenzgleichung $x \equiv s_{i_j} \pmod{n_{i_j}}$ und setze $N := \prod_{j=1}^{k} n_{i_j}$. Bestimme nun die kleinste nicht-negative Lösung x dieses Kongruenzsystems.*

[7] Die Formulierung *mit Sicherheit* bedeutet, dass sich G zufälligerweise auch einmal aus weniger als r Teilen gewinnen lassen kann; dann soll aber unklar bleiben, ob man wirklich das richtige G erhalten hat.

Schritt 2: *Berechne* $g := x \bmod M$.

Dann gilt $G = g$.

Beweis. Sei $T = (s, n, M)$ irgendeines der im *secret sharing scheme* erzeugten Tripel. Dann gilt nach Konstruktion $G + zM = S \equiv s \pmod{n}$. Jede aus einem der Tripel abgeleitete Kongruenzgleichung besitzt also die Zahl $S = G + zM \in \mathbb{N}$ als eine der unendlich vielen Lösungen.

Nun betrachten wir das aus den T_{i_j} gebildete Kongruenzsystem genauer.
Wegen der oben getroffenen Feststellung ist S eine Lösung des Systems. Weil die n_i nach (B1) paarweise teilerfremd sind, ist auf das System der chinesische Restsatz für Kongruenzen anwendbar. 40.7 (c) zeigt, dass es die Lösungsmenge $S + N\mathbb{Z}$ besitzt.
Wegen (B2) und (B3) gilt $S < n_1 \cdots n_k \leq N$, also $S \in \{0, 1, \ldots, N-1\}$. Wieder mit 40.7 erhalten wir, dass $S \in \mathbb{N}$ die kleinste nicht-negative Lösung Systems ist. Die Berechnung in Schritt 2 liefert nun

$$x \bmod M = S \bmod M = (G + zM) \bmod M \overset{G < M \text{ nach (B2)}}{=} G.$$

G ist also korrekt aus den vorliegenden Teilen $T_{i_1}, \ldots, T_{i_k}$ berechnet worden. ■

Bemerkung 41.2 (a) Im Satz schließen wir in Schritt 1 aus einem Kongruenzsystem auf eine ganze Zahl. Dies ist nicht eindeutig möglich, denn das System hat unendlich viele ganzzahlige Lösungen. Wir erzwingen Eindeutigkeit, indem wir uns für die kleinste nicht-negative Lösung entscheiden. Die Bedingungen (B1)–(B3) stellen sicher, dass diese willkürliche Festlegung das richtige Ergebnis für Schritt 2 liefert.

(b) Um möglichst wenig Informationen über G preiszugeben, verwenden wir zur Definition der s_i nicht G direkt, sondern benutzen die Hilfsvariable $S = G + zM$. Auf diese Weise hängen die T_i auch vom zufällig gewählten Parameter z ab.

(c) Beim Verteilen der T_i werden nur die Werte des Tupels übermittelt; der Index i wird nie mitgeteilt. Es ist daher nicht möglich, mit (B2) die restlichen Moduln abzuschätzen. ※

Wir illustrieren das Verfahren:

Beispiel 41.3 Jüngst hat das amerikanische Volk festgestellt, dass es eine dumme Idee ist, den Atomwaffen-Abschusscode G dem Präsidenten mitzuteilen und keinerlei sonstige Kontrollmechanismen einzurichten. Es entscheidet, dass G zukünftig so auf den Präsidenten (P), den Vorsitzenden des Senats (VS) und den Vorsitzenden des Repräsentantenhauses (VR) aufgeteilt werden soll, dass G aus zwei der drei Teile rekonstruiert werden kann.
Sei $G = 12$. Wir teilen G mit obigem Schema auf und setzen $r = 3, k = 2$ und

$$(M, n_1, n_2, n_3) = (53, 59, 61, 67).$$

Diese Zahlen sind alle prim, so dass (B1) erfüllt ist. Es ist klar, dass auch (B2) gilt. Um (B3) zu erfüllen, muss

$$z < \frac{n_1 \cdot n_2 - G}{M} \approx 67{,}7$$

gelten. Wir wählen $z = 36$ und erhalten $S = 1920$. Hieraus ergeben sich die Tripel

$$\begin{aligned} (\mathrm{P}): &\quad (1920 \bmod 59, 59, 53) = (32, 59, 53), \\ (\mathrm{VS}): &\quad (1920 \bmod 61, 61, 53) = (29, 61, 53), \\ (\mathrm{VR}): &\quad (1920 \bmod 67, 67, 53) = (44, 67, 53). \end{aligned}$$

(VS) und (VR) können gemeinsam G rekonstruieren: Die Lösungsmenge des ihnen bekannten Gleichungssystems

$$\left\{ \begin{array}{rcll} x & \equiv & 29 & (\mathrm{mod}\ 61) \\ x & \equiv & 44 & (\mathrm{mod}\ 67) \end{array} \right\}$$

ist $1920 + 4087\mathbb{Z}$ mit kleinster nicht-negativer Lösung $x = 1920$. Sie erhalten den korrekten Abschusscode $x \bmod 53 = 12$.
(P) alleine kann G nicht sicher rekonstruieren: Seine Gleichung $x \equiv 32 \pmod{59}$ hat die Lösungsmenge $L := 32 + 59\mathbb{Z}$. Um alle möglichen Abschusscode-Kandidaten zu erhalten, berechnet (P) für jedes $x \in L$ den Wert $x \bmod 53$. Dies führt auf die 53-elementige Menge $\{0, 1, \ldots, 52\}$. Also kann (P) aus seiner Gleichung allein keinerlei Information gewinnen. ⁕

Verschlüsselung mit RSA

Das RSA-Verfahren, eines der praktisch bedeutsamsten und am weitest verbreiteten Verschlüsselungsverfahren, basiert auf folgendem unscheinbaren Satz:

Satz 41.4 *Seien p, q zwei verschiedene Primzahlen. Dann gilt für alle $a \in \mathbb{Z}$ und $k \in \mathbb{N}_0$*

$$a^{1+k\cdot(p-1)(q-1)} \equiv a \pmod{pq}.$$

Beweis. Mit dem chinesischen Restsatz folgt

$$a^{1+k\cdot(p-1)(q-1)} \equiv a \pmod{pq} \iff \left\{ \begin{array}{rcll} a^{1+k\cdot(p-1)(q-1)} & \equiv & a \pmod{p} & \text{(I)} \\ a^{1+k\cdot(p-1)(q-1)} & \equiv & a \pmod{q} & \text{(II)} \end{array} \right\}.$$

Der Satz ist bewiesen, wenn wir die Richtigkeit der Gleichungen (I) und (II) zeigen. Wir tun dies nur für (I); der Nachweis funktioniert im anderen Fall analog.
Falls a nicht teilerfremd zur Primzahl p ist, so gilt $p \mid a$ und somit $a \equiv 0 \pmod{p}$. Gleichung (I) reduziert sich in diesem Fall auf die wahre Aussage $0 \equiv 0 \pmod{p}$.
Falls a teilerfremd zur Primzahl p ist, so können wir Euler-Fermat anwenden und erhalten

$$a^{1+k\cdot(p-1)(q-1)} = a \cdot (a^{p-1})^{k\cdot(q-1)} \overset{a^{p-1}\equiv 1}{\equiv} a \cdot 1^{k\cdot(q-1)} = a \pmod{p}.$$

Gleichung (I) ist daher für alle $a \in \mathbb{Z}$ erfüllt. ■

Wir beschreiben nun das RSA-Verfahren (benannt nach seinen Erfindern, den Mathematikern Rivest, Shamir und Adleman). Es erlaubt, eine Nachricht N zu ver- und entschlüsseln.
Wir gehen wie im Abschnitt davor davon aus, dass N ein Element aus $\mathbb{N}_0$ ist. Außerdem halten wir uns an die Gepflogenheiten der Kryptographie: Den Sender der Nachricht bezeichnen wir als Alice, den Empfänger Bob. Charlie belauscht die Kommunikation zwischen Alice und Bob und möchte die von Alice gesendete verschlüsselte Nachricht entschlüsseln.

Vorbereitungen von Bob

- Bob wählt zwei verschiedene Primzahlen p und q. Er berechnet $n := pq$ und $\varphi(n) = (p-1)(q-1)$.
- Bob wählt eine natürliche Zahl e mit $\operatorname{ggT}(e, \varphi(n)) = 1$. Dann ist $\bar{e}$ eine Einheit im Ring $\mathbb{Z}_{\varphi(n)}$. Daher existiert ein Element $d \in \{1, \dots, \varphi(n)-1\}$ mit

  $$ed \equiv 1 \pmod{\varphi(n)},$$

  das Bob mit Hilfe des erweiterten Euklidischen Algorithmus berechnen kann.
- Er veröffentlicht das Paar (e, n), hält das Paar (d, n) geheim und vergisst p, q und $\varphi(n)$.

Alice verschlüsselt Nachricht N

- Alice holt sich das Paar (e, n) und überprüft, ob $N < n$ gilt. Ansonsten schreibt sie ihre Nachricht so um, dass diese Bedingung erfüllt ist.
- Sie berechnet $V := N^e \bmod n$. Dies ist die verschlüsselte Nachricht.
- Sie veröffentlicht V.

Bob entschlüsselt V Bob holt sich V, erinnert sich an das Paar (d, n) und erhält die entschlüsselte Nachricht E, indem er $E := V^d \bmod n$ berechnet.

Wir beweisen, dass Ver- und Entschlüsselung invers zueinander sind:

Satz 41.5 *Mit den obigen Bezeichnungen gilt $E = N$.*

Beweis. Es sind $e, d \in \mathbb{N}$. Weiter erfüllen e und d die Kongruenz $ed \equiv 1 \pmod{\varphi(pq)}$. Somit ist $ed \geq 1$, und es gibt $k \in \mathbb{N}_0$ mit $ed = 1 + k(p-1)(q-1)$. Nun gilt

$$E \equiv V^d \equiv (N^e)^d = N^{ed} = N^{1+k(p-1)(q-1)} \overset{41.4}{\equiv} N \pmod{n}.$$

Es folgt daher bereits, dass E und N in derselben Restklasse von $\mathbb{Z}_n$ liegen.
Durch den in der Ver- und Entschlüsselung benutzten mod-Operator wird stets der eindeutig bestimmte Restklassenvertreter aus $\{0, 1, \dots, n-1\}$ gewählt. Da $N < n$ ist, folgt daher sogar $E = N$. ■

Bemerkung 41.6 (a) Die Berechnung von d mit Hilfe des erweiterten Euklidischen Algorithmus ist effizient durchführbar.
Zum Ver- und Entschlüsseln müssen Potenzen mit großen Exponenten berechnet werden. Auch hierfür existieren effiziente Algorithmen.

(b) Das Paar (e, n) muss nicht geheim gehalten werden. Man nennt es deshalb auch den **öffentlichen Schlüssel des RSA-Verfahrens**.
Bisher ist keine (effiziente) Möglichkeit veröffentlicht, um aus e und n das Element d zu berechnen. Dies liegt unter anderem daran, dass man keine (effizienten) Algorithmen kennt, um n zu faktorisieren. Der Wert des Produkts $(p-1)(q-1)$ ist daher nur Bob bekannt.

(c) Man kennt ebenfalls keine (effizienten) Algorithmen zum Berechnen von Wurzeln in Restklassenringen. Zwar gilt die Beziehung $N = \sqrt[e]{V}$, jedoch ist die konkrete Bestimmung der Wurzel in der Praxis nicht durchführbar. Dies ist der Grund, warum Alice ihre verschlüsselte Nachricht V veröffentlichen kann, ohne befürchten zu müssen, dass hierdurch auch N bekannt wird. Sollte Alice ihre Nachricht N vergessen, so ist auch sie selbst nicht mehr in der Lage, N aus V zu rekonstruieren.
Man spricht bei der Verschlüsselungs-Abbildung $\mathbb{Z}_n \to \mathbb{Z}_n$, $N \mapsto N^e$ auch von einer **Einweg-Funktion**: Funktionswerte lassen sich effizient berechnen, Urbilder jedoch nicht.

(d) Bob ersetzt das problematische Wurzelziehen durch das Potenzieren mit d. Er kann N effizient aus V zurückgewinnen, indem er $V^d \bmod n$ berechnet. Hierzu ist niemand sonst in der Lage, da d nur Bob bekannt ist. Aus diesem Grund nennt man das Paar (d, n) auch den **privaten Schlüssel des RSA-Verfahrens**.

(e) Damit sich das Fehlen von effizienten Algorithmen tatsächlich auswirkt und das Entschlüsseln ohne Kenntnis von d (nach momentanem Stand des Wissens und der Technik) wirksam verhindert wird, müssen die Primzahlen p und q hinreichend groß gewählt werden. Das Bundesamt für Sicherheit in der Informationstechnik fordert in seinen technischen Leitlinien beispielsweise

$$p, q > 2^{1500} \approx 10^{450} \qquad \text{(Stand: 24.03.2021)}.$$

Wir gehen in Vorlesung 43 darauf ein, wie man so große Primzahlen findet.

(f) Es gibt bisher keinen Beweis für die Nicht-Existenz von effizienten Algorithmen für die oben angesprochenen Probleme. Hieraus folgt, dass auch die Sicherheit von RSA bisher nicht beweisbar ist. Allerdings wird das Verfahren seit ca. 40 Jahren eingesetzt und intensiv beforscht. Es konnte in seiner allgemeinen Form bisher nicht gebrochen werden. Man sieht es deshalb bei hinreichend hoher Wahl von p und q (noch) als sicher an.

(g) Mit Quantencomputern kann auch man sehr große Zahlen effizient faktorisieren und somit RSA brechen. Da weltweit intensiv an dieser Technologie geforscht wird

und auch schon erste Durchbrüche erzielt wurden, zeichnet sich das Ende von RSA ab.
Im Fokus der modernen Kryptografie stehen daher das Finden und Untersuchen von Problemstellungen, die quantensicher sind. Man kennt bereits einige quantensichere Verschlüsselungsverfahren, allerdings sind diese nur bedingt praxistauglich (zu langsam, zu viele zu übertragenden Daten, etc.). ⋇

Wir schließen die Vorlesung mit einem Beispiel, das eine typische Anwendung des RSA-Verfahrens zeigt:

Beispiel 41.7 Alice, Besitzerin einer Coburger Klößerei, die für ihre außergewöhnlich wohlschmeckenden seidig-weichen Kartoffelklöße bekannt ist, möchte in den USA eine Filiale eröffnen. Hierzu muss sie ihr streng geheimes Rezept an Bob, der die Filiale leiten soll, schicken. Man einigt sich auf das folgende **hybride Verschlüsselungsverfahren**:

Alice benutzt das rechentechnisch aufwendige RSA-Verfahren, um ein Passwort P verschlüsselt an Bob zu versenden. Bob kann hierbei ausnutzen, dass er den öffentlichen Schlüssel des RSA-Verfahrens, den er zuvor erstellt hat, einfach per Postkarte an Alice schicken kann.
Danach verschlüsselt Alice das (sehr lange) Kloß-Rezept mit einem schnelleren, weniger rechenintensiven Verfahren, beispielsweise AES. Dieses Verfahren benötigt zum Ver- und Entschlüsseln *dasselbe* Passwort. Alice wählt hierfür P, denn P wurde ja bereits verschlüsselt übertragen und ist daher Alice und Bob (und nur diesen beiden) bekannt.

42. Einheitengruppen von Restklassenringen

Worum geht es? Wir bestimmen für beliebige $n \in \mathbb{N}$ den Isomorphietyp der Einheitengruppe $\mathbb{Z}_n^\times$. Wir zeigen, dass diese Gruppe für ungerade Primpotenzen n zyklisch ist, dass für diese n also *Primitivwurzeln modulo n* existieren. ⋇

Sei n eine beliebige natürliche Zahl mit Primfaktorzerlegung $n = p_1^{r_1} \cdots p_s^{r_s}$. Nach 6.20 gilt dann

$$\mathbb{Z}_n^\times \cong \mathbb{Z}_{p_1^{r_1}}^\times \times \mathbb{Z}_{p_2^{r_2}}^\times \times \cdots \times \mathbb{Z}_{p_s^{r_s}}^\times .$$

Die Isomorphietypen der Gruppen $\mathbb{Z}_n^\times$ können also bestimmt werden, sobald die Isomorphietypen von $\mathbb{Z}_{p^r}^\times$ für Primpotenzen p^r bekannt sind. Wir untersuchen daher die Struktur der Einheitengruppen $\mathbb{Z}_{p^r}^\times$ genauer.

Primitivwurzeln, Einheiten und Ordnungen modulo *n*

Um die folgenden Resultate besser formulieren zu können, führen wir den Begriff der Primitivwurzel ein. Um sauber zwischen ganzen Zahlen und Restklassen unterscheiden zu können, definieren wir den Begriff in zwei Varianten:

Definition 42.1 *Sei $n \in \mathbb{N}$. Unter einer **Primitivwurzel** verstehen wir jedes Element $\overline{g} \in \mathbb{Z}_n^\times$, das die multiplikative Ordnung $\varphi(n)$ besitzt.*
*Wir nennen eine ganze Zahl $g \in \mathbb{Z}$ eine **Primitivwurzel modulo n**, wenn die Restklasse $\overline{g} \in \mathbb{Z}_n^\times$ eine Primitivwurzel ist.*

Wir wollen auch den Einheiten-Begriff für die Ringe $\mathbb{Z}_n$ in den ganzen Zahlen zur Verfügung haben. Hierzu definieren wir analog zu oben:

Vereinbarung zur Schreibweise 42.2 Wir sagen, dass die ganze Zahl $a \in \mathbb{Z}$ eine **Einheit modulo *n*** sei, wenn das Element $\overline{a} \in \mathbb{Z}_n$ eine Einheit in $\mathbb{Z}_n$ ist.
4.20 zeigt, dass a genau dann eine Einheit modulo n ist, wenn a teilerfremd zu n ist. ⋇

Bemerkung 42.3 (a) Primitivwurzeln existieren in $\mathbb{Z}_n^\times$ genau dann, wenn $\mathbb{Z}_n^\times$ zyklisch ist. Sie sind dann genau die Erzeuger von $\mathbb{Z}_n^\times$.

(b) $\mathbb{Z}_n^\times$ hat Ordnung $\varphi(n)$. Falls $\mathbb{Z}_n^\times$ zyklisch ist, so existieren genau $\varphi(\varphi(n))$ Erzeuger von $\mathbb{Z}_n^\times$. Es gibt dann also genau $\varphi(\varphi(n))$ Primitivwurzeln.

(c) Ein Element $g \in \mathbb{Z}$ ist genau dann eine Primitivwurzel modulo n, wenn für alle $d \in \mathbb{N}$ mit $d \mid \varphi(n)$ gilt:

$$\text{Ist } d \neq \varphi(n), \text{ so ist } g^d \not\equiv 1 \pmod{n}.$$

Dies folgt direkt aus der Definition der Ordnung eines Gruppenelements in 7.7.

(d) Nach 15.21 existieren Primitivwurzeln modulo p für jede Primzahl $p \in \mathbb{P}$. ⋇

Bei Untersuchungen in Restklassenringen haben wir bisher stets den Modul n fixiert und dann verschiedene Elemente in $\mathbb{Z}_n$ betrachtet. In dieser Vorlesung untersuchen wir hingegen Eigenschaften ganzer Zahlen a bezüglich verschiedener Moduln. Die Nebenklassen-Schreibweise $\overline{a}$ ist hier eher hinderlich, da sie keine Information über den zugrunde liegenden Restklassenring liefert. Wir verzichten daher weitestgehend auf sie und führen geeignete Ersatznotationen ein.

Definition 42.4 *Seien n eine natürliche Zahl und $a \in \mathbb{Z}$ eine Einheit modulo n. Unter der **n-Ordnung von a** oder der **Ordnung von a modulo n** verstehen wir die multiplikative Ordnung des Elements $\overline{a} \in \mathbb{Z}_n^\times$ und schreiben $\operatorname{ord}_n(a)$ für sie.*
$\operatorname{ord}_n(a)$ ist also die kleinste natürliche Zahl s mit $a^s \equiv 1 \pmod{n}$.

Das nächste Resultat klärt die Einheiten-Eigenschaft modulo Primpotenzen:

Lemma 42.5 *Seien $p \in \mathbb{P}$ und $r \in \mathbb{N}$. Dann ist $a \in \mathbb{Z}$ genau dann eine Einheit modulo p, wenn a eine Einheit modulo p^r ist.*
Dies zeigt, dass die Menge der Einheiten modulo p^r unabhängig vom konkreten r ist und mit der Menge der Einheiten modulo p übereinstimmt.

Beweis. Genau dann ist a eine Einheit modulo p^r, wenn $\operatorname{ggT}(a, p^r) = 1$ ist. Dies ist genau dann der Fall, wenn $p \nmid a$ ist, wenn also $\operatorname{ggT}(a, p) = 1$ ist. Dies bedeutet, dass a eine Einheit modulo p ist. ■

Der Primitivwurzel-Nachweis wird oft über die Ordnung geführt, vgl. 42.3 (c). Wir stellen eine nützliche einschränkende Bedingung für Ordnungen bereit:

Satz 42.6 *Seien $p \in \mathbb{P}$ eine Primzahl, $r \in \mathbb{N}$ und $a \in \mathbb{Z}$ eine Einheit modulo p. Dann gilt $\operatorname{ord}_p(a) \mid \operatorname{ord}_{p^r}(a)$.*

Beweis. Da a eine Einheit modulo p ist, ist a nach 42.5 auch eine Einheit modulo p^r. Die jeweiligen Ordnungen $\operatorname{ord}_p(a)$ und $\operatorname{ord}_{p^r}(a)$ existieren also.
Per Definition ist $a^{\operatorname{ord}_{p^r}} \equiv 1 \pmod{p^r}$. Da $p \mid p^r$ ist, liefert 40.6, dass $a^{\operatorname{ord}_{p^r}} \equiv 1 \pmod{p}$ ist. Die Minimalität der Ordnung 7.15 (b) zeigt nun die Behauptung $\operatorname{ord}_p(a) \mid \operatorname{ord}_{p^r}(a)$. ■

Isomorphietyp von $\mathbb{Z}_{p^r}^\times$ mit ungeradem $p \in \mathbb{P}$

Die Struktur von $\mathbb{Z}_{p^r}$ für ungerades $p \in \mathbb{P}$ steckt bereits vollständig, aber sehr verklausuliert im folgenden technischen Lemma:

Lemma 42.7 *Sei p eine ungerade Primzahl. Dann existiert eine Primitivwurzel $g \in \mathbb{Z}$ modulo p, die $p^2 \nmid g^{p-1} - 1$ erfüllt. g hat die Eigenschaft:*
Zu jedem $s \in \mathbb{N}$ gibt es ein $z \in \mathbb{Z}$ mit

$$g^{(p-1)\cdot p^{s-1}} = 1 + z \cdot p^s \qquad \text{und} \qquad p \nmid z.$$

Beweis. Wir konstruieren zuerst eine geeignete Primitivwurzel g. Danach zeigen wir die behauptete Eigenschaft per Induktion nach s.

Konstruktion von g Nach 42.3 (d) existiert eine Primitivwurzel a modulo p. Für diese gilt $a^{p-1} \equiv 1 \pmod{p}$, was eine Darstellung der Form

$$a^{p-1} = 1 + z \cdot p \qquad \text{mit einem } z \in \mathbb{Z}$$

liefert. Falls p kein Teiler von z ist, gilt $p^2 \nmid a^{p-1} - 1$. Wir setzen $g := a$.

Ansonsten betrachten wir das Element $b := p + a$ und können b^{p-1} darstellen als

$$\begin{aligned} b^{p-1} &= (p+a)^{p-1} = \sum_{i=0}^{p-1} \binom{p-1}{i} p^i a^{p-1-i} \\ &= \binom{p-1}{0} a^{p-1} + \binom{p-1}{1} p \cdot a^{p-2} + \sum_{i=2}^{p-1} \binom{p-1}{i} p^i a^{p-1-i} \\ &\overset{a^{p-1}=1+zp}{=} 1 + z \cdot p + (p-1) \cdot p \cdot a^{p-2} + \sum_{i=2}^{p-1} \binom{p-1}{i} p^i a^{p-1-i}. \end{aligned}$$

Die beiden roten Summanden werden von p^2 geteilt (beim linken folgt dies, da nach Voraussetzung $p \mid z$ gilt). Der blaue Summand wird von p, nicht aber von p^2 geteilt. Wir können aus den eingefärbten Summanden also insgesamt den Faktor p, nicht aber den Faktor p^2 ausklammern und erhalten

$$b^{p-1} = 1 + z' \cdot p \qquad \text{mit } z' \in \mathbb{Z} \text{ und } p \nmid z';$$

es gilt also $p^2 \nmid b^{p-1} - 1$. Das Produkt $z' \cdot p$ entspricht dem farbig markierten Teil der Gleichung. Nun setzen wir $g := b = a + p$. Auch in diesem Fall ist g eine Primitivwurzel modulo p.

g besitzt für alle s die zu zeigende Eigenschaft Wir beweisen per Induktion nach s.

Wir haben im ersten Schritt g so konstruiert, dass $g^{p-1} = 1 + zp$ mit $p \nmid z$ gilt. Die zu zeigende Eigenschaft stimmt also für $s = 1$. Sie möge für ein beliebiges $s \in \mathbb{N}$ gelten. Dann ist

$$\begin{aligned} g^{(p-1)p^s} &= \left(g^{(p-1)p^{s-1}}\right)^p \overset{\text{Ind.vor.}}{=} \left(1 + zp^s\right)^p = \sum_{i=0}^{p} \binom{p}{i} z^i p^{si} \\ &= 1 + p \cdot z \cdot p^s + \sum_{i=2}^{p} \binom{p}{i} z^i p^{si}. \end{aligned}$$

Nun argumentieren wir wie im ersten Schritt: Der rote Summand wird von p^{s+1}, aber nicht von p^{s+2} geteilt, der blaue Summand wird von p^{s+2} geteilt. Daher lassen sich die eingefärbten Terme in der Form $z' \cdot p^{s+1}$ mit einem $z' \in \mathbb{Z}$ schreiben, wobei $p \nmid z'$ gilt. Dies schließt den Induktionsbeweis ab. ■

Wir können nun die Existenz von Primitivwurzeln modulo ungerader Primzahlpotenzen zeigen. Der Beweis sieht kompliziert aus, jedoch sind die Schlussweisen recht einfach: Man untersucht die p^r-Ordnung des Elements g aus 42.7 und stellt fest, dass sie $\varphi(p^r)$ beträgt.

Satz 42.8 (Gauß) *Seien p eine ungerade Primzahl und $r \in \mathbb{N}$. Dann ist die Gruppe $\mathbb{Z}_{p^r}^\times$ zyklisch. Da ihre Ordnung durch $\varphi(p^r) = (p-1)p^{r-1}$ gegeben ist, gilt also*

$$\mathbb{Z}_{p^r}^\times \cong C_{\varphi(p^r)} = C_{(p-1)p^{r-1}}.$$

Beweis. Die Aussage wurde für $r = 1$ bereits gezeigt, vgl. 42.3 (d). Sei nun $r \geq 2$. Wir bezeichnen mit g das Element aus 42.7 und zeigen, dass es eine Primitivwurzel modulo p^r ist.
Setzen wir $s := r$, so liefert die Gleichung aus 42.7

$$g^{(p-1)p^{r-1}} \equiv 1 \pmod{p^r}.$$

Also ist $\operatorname{ord}_{p^r}(g)$ ein Teiler von $(p-1)p^{r-1}$. Da g eine Primitivwurzel modulo p ist, gilt $\operatorname{ord}_p(g) = \varphi(p) = p - 1$und somit $p - 1 \mid \operatorname{ord}_{p^r}(g)$ nach 42.6. Zusammen folgt

$$\operatorname{ord}_{p^r}(g) = (p-1) \cdot p^k \qquad \text{mit einem } k \in \{0, 1, \dots, r-1\}.$$

Wäre $\operatorname{ord}_{p^r}(g) \neq (p-1)p^{r-1}$, so würde $\operatorname{ord}_{p^r}(g)$ ein Teiler von $(p-1)p^{r-2}$ sein. Es wäre dann

$$g^{(p-1)p^{r-2}} \equiv 1 \pmod{p^r}, \qquad \text{also} \qquad g^{(p-1)p^{r-2}} = 1 + z \cdot p^r$$

mit einem geeigneten $z \in \mathbb{Z}$. Dies widerspricht aber der Gleichung in 42.7.
Also gilt $\operatorname{ord}_{p^r}(g) = (p-1)p^{r-1} = \varphi(p^r)$ und g ist eine Primitivwurzel modulo p^r. ∎

Bemerkung 42.9 Aus dem Lemma und dem ersten Schritt des Beweises folgt, wie man Primitivwurzeln modulo ungerader Primzahlpotenzen konstruiert:
Man sucht eine Primitivwurzel a modulo p. Falls $p^2 \nmid a^{p-1} - 1$ ist, so ist a eine Primitivwurzel modulo aller Potenzen von p. Ansonsten ist $a + p$ eine Primitivwurzel modulo aller Potenzen von p.
Mit diesem Algorithmus folgt beispielsweise, dass 2 eine Primitivwurzel modulo 3^r für alle $r \in \mathbb{N}$ ist.
Nachrechnen zeigt, dass 14 eine Primitivwurzel modulo 29 ist und $29^2 \mid 14^{28} - 1$ gilt. Daher ist $14 + 29 = 43$ eine Primitivwurzel modulo aller Potenzen von 29. ⁜

Isomorphietyp von $\mathbb{Z}_{2^r}^\times$

Die Einheitengruppen $\mathbb{Z}_2^\times = \{\overline{1}\} \cong C_1$ und $\mathbb{Z}_{2^2}^\times = \langle\overline{3}\rangle = \{\overline{1}, \overline{3}\} \cong C_2$ sind zyklisch. Die Einheitengruppe von $\mathbb{Z}_{2^3}$ ist gegeben durch

$$\mathbb{Z}_{2^3}^\times = \{\overline{1}, \overline{3}, \overline{5}, \overline{7}\}.$$

Die 2^3-Ordnungen von 3, 5 und 7 sind jeweils Zwei. Also enthält $\mathbb{Z}_{2^3}^\times$ kein Element der Ordnung $\varphi(2^3) = 4$ enthält und ist nicht zyklisch. Dies liegt daran, dass sich die Darstellung aus 42.7 im Fall $p = 2$ nicht erreichen lässt. Wir stellen hierzu den Beweis von 42.7 nach und untersuchen, welche Schlussweisen fehlschlagen:
Für $s = 1$ existiert die Darstellung aus 42.7 noch. Beispielsweise können wir $g = 3$ und $z = 1$ setzen und erhalten

$$3^{2^{s-1}} = 3 = 1 + 1 \cdot 2 = 1 + z \cdot 2^s \qquad \text{mit } 2 \nmid z.$$

Nun führen wir den Induktionsschritt von $s = 1$ auf $s + 1 = 2$ durch:

$$\begin{aligned} g^{2^{(s+1)-1}} &= g^{2^s} = (g^{2^0})^2 \overset{\text{Ind.vor.}}{=} (1 + 2z)^2 \\ &= \binom{2}{0} \cdot 1 + \binom{2}{1} \cdot 2z + \binom{2}{2} \cdot 4z^2 = 1 + 4z + 4z^2 = 1 + 4 \cdot (z + z^2). \end{aligned}$$

Da z ungerade war, ist $z + z^2$ gerade. Eine Darstellung von g^{2^1} in der Form $1 + z' \cdot 2^2$ mit $2 \nmid z'$ ist daher nicht möglich, der Induktionsschritt nicht durchführbar.

Anders für ungerades p: Hier ist $p \geq 3$, und der oben blau markierte Binomialkoeffizient hat die Form $\binom{p}{2}$ und ist durch p teilbar. Der sich ergebende Term $\binom{p}{2}p^2z^2$ und alle weiteren Terme $\binom{p}{i}z^ip^i$ für $3 \leq i \leq p$ sind also durch p^3 teilbar. Wir können dann p^2 aus allen diesen Summanden ausklammern und erhalten eine Darstellung der Form $z \cdot p^2$ mit $p \nmid z$. Diese Argumentation haben wir am Ende des Beweises von 42.7 ausgenutzt. Die Induktion im Fall $p = 2$ scheitert also daran, dass die erste binomische Formel zu „kurz“ ist.

Für $p = 2$ kann man jedoch folgende Variante von 42.7 bereitstellen. Beachten Sie den Exponenten bei g im folgenden Lemma: Hier steht $2^{s-2} = \frac{1}{2}\varphi(2^s)$ und nicht $\varphi(p^s)$ wie in 42.7. Der Beweis des Lemmas erfolgt ebenfalls per Induktion nach s; wir führen ihn nicht.

Lemma 42.10 *Die ganze Zahl $g := 5$ ist eine Primitivwurzel modulo 2 mit der Eigenschaft: Zu jedem $s \geq 2$ gibt es ein $z \in \mathbb{Z}$ mit*

$$g^{2^{s-2}} = 1 + z \cdot 2^s \qquad \textit{und} \qquad 2 \nmid z.$$

Mit denselben Argumenten wie in 42.8 folgt dann:

Satz 42.11 *Für $r \geq 2$ hat das Element 5 Ordnung $\frac{1}{2}\varphi(2^r) = 2^{r-2}$ modulo 2^r.*

Der Satz sagt aus, dass das Erzeugnis von $\overline{5}$ eine Index-2-Untergruppe von $\mathbb{Z}_{2^r}^\times$ liefert. Es gibt also Elemente aus $\mathbb{Z}_{2^r}^\times$, die nicht in diesem Erzeugnis enthalten sind. $\overline{-1}$ ist ein solches:

Lemma 42.12 *Sei $r \geq 2$. Dann existiert kein $n \in \mathbb{N}$ mit $5^n \equiv -1 \pmod{2^r}$.*
Dies zeigt, dass die Gruppe $\langle\overline{5}\rangle \leq \mathbb{Z}_{2^r}^\times$ für $r \geq 2$ das Element $\overline{-1} \in \mathbb{Z}_{2^r}^\times$ nicht enthält.

Beweis. Die Aussage stimmt offenbar für $r = 2$, denn für alle $n \in \mathbb{N}$ ist

$$5^n \equiv 1^n = 1 \not\equiv -1 \pmod{2^2}.$$

Sei nun $r > 2$. Angenommen, es gäbe $n \in \mathbb{N}$ mit $5^n \equiv -1 \pmod{2^r}$. Dann wäre mit 40.6 auch $5^n \equiv -1 \pmod{2^2}$. Dies liefert einen Widerspruch, denn wir haben oben bereits gesehen, dass im Fall $r = 2$ ein solches n nicht existiert. ■

Nun können wir die Struktur der Gruppen $\mathbb{Z}_{2^r}^\times$ für $r \geq 3$ komplett klären:

Satz 42.13 (Gauß) *Für $r \geq 3$ wird die Gruppe $\mathbb{Z}_{2^r}^\times$ von den Elementen $\overline{-1}$ und $\overline{5}$ erzeugt. Es ist $\mathbb{Z}_{2^r}^\times \cong C_2 \times C_{2^{r-2}}$.*

Beweis. Wir definieren die beiden Untergruppen $A := \langle \overline{-1} \rangle$ und $B := \langle \overline{5} \rangle$ von $\mathbb{Z}_{2^r}^\times$. Es ist $A \cong C_2$. Aus 42.11 folgt $B \cong C_{2^{r-2}}$.
Da $\mathbb{Z}_{2^r}^\times$ abelsch ist, sind A und B sogar Normalteiler der Gruppe. Wegen 42.12 scheiden sie sich trivial. Es ist daher

$$|AB| \overset{13.3}{=} \frac{|A| \cdot |B|}{|A \cap B|} = 2 \cdot 2^{r-2} = 2^{r-1} = \varphi(2^r) = |\mathbb{Z}_{2^r}^\times|.$$

Aus Anzahlgründen folgt $AB = \mathbb{Z}_{2^r}^\times$. Der Satz vom internen direkten Produkt liefert

$$\mathbb{Z}_{2^r}^\times = AB \cong A \times B \cong C_2 \times C_{2^{r-2}}.$$ ■

Wir fassen die Ergebnisse zusammen:

Korollar 42.14 (Gauß) *Sei q eine beliebige Primpotenz. Dann ist die Gruppe $\mathbb{Z}_q^\times$ zyklisch von Ordnung $\varphi(q)$, außer im Fall $8 \mid q$. Hier gilt dann $q = 2^r$ mit $r \geq 3$, und es ist $\mathbb{Z}_q^\times \cong C_2 \times C_{q/4}$.*

Nun können wir den Isomorphietyp von $\mathbb{Z}_n^\times$ für alle $n \in \mathbb{N}$ bestimmen:

Beispiel 42.15 Sei $n = 2^5 \cdot 5^3 \cdot 11^7$. Dann gilt

$$\mathbb{Z}_n^\times \overset{6.20}{\cong} \mathbb{Z}_{2^5}^\times \times \mathbb{Z}_{5^3}^\times \times \mathbb{Z}_{11^7}^\times \overset{42.14}{\cong} C_2 \times C_{2^3} \times C_{4 \cdot 5^2} \times C_{10 \cdot 11^6}.$$ ⋇

43. Anwendung: Finden großer Primzahlen

Worum geht es? In vielen praktischen Anwendungen der Zahlentheorie werden große Primzahlen benötigt.
Man kennt keinen effizienten Algorithmus, der die Primeigenschaft großer Zahlen *beweisen* kann. Der *Miller-Rabin-Test* weist diese Eigenschaft aber mit *sehr hoher Wahrscheinlichkeit* nach. Er ist effizient implementierbar und einer der wichtigsten Algorithmen der angewandten Zahlentheorie. Wir stellen ihn vor. ⁜

In dieser Vorlesung bezeichnet P eine zufällig gewählte große natürliche Zahl. Das Adjektiv „groß“ meint hierbei $P \geq 2^{2048} \approx 10^{616}$, d. h. P besitzt mehr als 600 Stellen. Wir wollen eine Aussage darüber treffen, ob P prim ist.

Zunächst überprüfen wir, ob P von kleinen Primzahlen geteilt wird. Hierzu berechnen wir beispielsweise die ersten 10 000 Primzahlen[8] und testen, ob P von einer dieser Primzahlen geteilt wird. Der Test lässt sich schnell durchführen und zeigt für viele P[9], dass sie zusammengesetzt sind.
Wird P jedoch von keiner dieser Primzahlen geteilt, sind *exakte* Aussagen über die Primeigenschaft von P deutlich schwerer zu treffen. Hat P eine spezielle Struktur, ist P beispielsweise von der Form $2^n - 1$, so existieren noch (halbwegs) schnelle Primzahltests. Ansonsten ist es zum heutigen Zeitpunkt nicht möglich, die Primeigenschaft von P in vernünftiger Zeit algorithmisch zu beweisen.

Die Situation ändert sich radikal, wenn wir uns mit der Aussage „P ist mit festlegbar hoher Wahrscheinlichkeit prim“ zufrieden geben. Für diese Aussage existieren effiziente Testverfahren, die man **Pseudo-Primzahltests** nennt. Sie basieren auf dem Satz von Euler-Fermat 40.4, der für primes P die Form

$$P \text{ prim} \quad \Longrightarrow \quad \forall a \in \{1, 2, \dots, P-1\} : \; a^{P-1} \equiv 1 \pmod{P} \qquad \text{(EF)}$$

annimmt.
Wir stellen den einfachsten Pseudo-Primzahltest vor, den **Fermat-Test**: Wir arbeiten in mehreren **Runden** und legen vorher ein Rundenlimit fest. In jeder Runde

- wählen wir ein zufälliges a mit $1 \leq a \leq P-1$ und
- überprüfen die **Fermat-Bedingung** $a^{P-1} \equiv 1 \pmod{P}$.
- Ist diese *nicht* erfüllt, geben wir „*P ist sicher nicht prim*“ aus und beenden den Test; weitere Runden sind nicht mehr nötig.
  Ist diese erfüllt, geben wir „*P könnte prim sein*“ aus und starten mit der nächsten Runde, falls das Rundenlimit noch nicht erreicht ist.

Bricht der Test mit der Ausgabe „*P ist sicher nicht prim*“ ab, so ist mathematisch bewiesen, ⁉

[8] Dies kann mit mit Hilfe des Siebs des Eratosthenes geschehen und muss nur einmal durchgeführt werden; die fertige Liste kann fest in den Algorithmus eingebaut werden.
[9] In 50 % der Fälle ist P durch Zwei, in 33 % der Fälle durch Drei teilbar, etc.

dass P nicht prim ist. Erhalten wir ausschließlich die Ausgaben „*P könnte prim sein*“, so sehen wir P mit hoher Wahrscheinlichkeit als prim an. Es ist klar, dass der Test aussagekräftiger wird, wenn wir ein hohes Rundenlimit wählen.

Wir zeigen, dass der Fermat-Test prinzipiell in der Lage ist, sicher zwischen Prim- und Nichtprimzahlen zu unterscheiden:

Lemma 43.1 *Sei a mit $1 \leq a \leq P-1$ eine Nicht-Einheit modulo P. Dann verletzt a die Fermat-Bedingung, so dass P im Fermat-Test als nicht prim erkannt wird.*
Genau für Nicht-Primzahlen P existieren solche a.

Beweis. Sei a eine beliebige Nicht-Einheit modulo P. Würde a die Fermat-Bedingung erfüllen, so wäre $a \cdot a^{P-2} \equiv 1 \pmod{P}$. Aus dieser Kongruenz folgt aber, dass a eine Einheit modulo P ist, was einen Widerspruch liefert. ⁉
Nun zeigen wir das Existenzresultat: Nach 4.20 ist a genau dann eine Nicht-Einheit modulo P, wenn a und P nicht teilerfremd sind. Wegen $1 \leq a \leq P-1$ ist dies für ein a genau dann erfüllbar, wenn P nicht prim ist. ⁉ ■

Bemerkung 43.2 Das Lemma sieht nützlicher aus, als es tatsächlich ist:

(a) Man kann zeigen, dass es unendlich viele Nicht-Primzahlen P mit der Eigenschaft

$$a \text{ Einheit modulo } P \quad \Longrightarrow \quad a^{P-1} \equiv 1 \pmod{P}$$

gibt.[10] Man nennt diese Zahlen **Carmichael-Zahlen**. Wir gehen in den Übungen etwas näher auf diese Zahlen ein. → Übung
Für sie ist die Aussage im Lemma scharf: Genau dann verletzt a die Fermat-Bedingung, wenn a eine Nicht-Einheit modulo P ist.

(b) Die Existenz von Carmichael-Zahlen zeigt, dass der Fermat-Test nur dann sicher zwischen Prim- und Nichtprimzahlen unterscheiden kann, wenn in einer der Runden zufälligerweise eine Nicht-Einheit a ausgewählt wird. Dies kann, je nach Aussehen von P, *extrem* unwahrscheinlich sein:
Angenommen, es ist $P = pq$ mit verschiedenen Primzahlen $p, q \in \mathbb{P}$. Wir nehmen zudem an, dass p und q etwa gleich groß mit $p \approx 2^{1024} \approx q$ sind[11]. Die Anzahl der Nicht-Einheiten a in $\{1, 2, \ldots, P-1\}$ ist

$$\underbrace{P-1}_{\text{da } 1 \leq a \leq P-1} - \underbrace{\varphi(P)}_{\text{Anzahl Einheiten}} = pq - 1 - (p-1)(q-1) = p + q - 2 \approx 2 \cdot 2^{1024} = 2^{1025}.$$

Die Wahrscheinlichkeit, bei zufälliger Wahl von a eine Nicht-Einheit zu treffen, beträgt also rund $2^{1025}/P \approx 2^{1025-2048} = 2^{-1023} \approx 10^{-308}$.
Um diese Wahrscheinlichkeit zu illustrieren, betrachten wir ein Zufallsexperiment:

[10] Beachten Sie, dass dies nicht trivial ist! Euler-Fermat liefert für Einheiten a die Aussage $a^{\varphi(P)} \equiv 1 \pmod{P}$. Da P zusammengesetzt ist, ist $\varphi(P) \neq P-1$.
[11] Dies sind übliche Parameter für den Modul n im RSA-Verfahren.

Alice wählt irgendein Atom aus den ca. 10^{82} Atomen im Universum aus. Die Wahrscheinlichkeit, dass Bob durch zufälliges Raten das Atom von Alice wiederfindet, beträgt 10^{-82}. Dies ist 10^{226} Mal wahrscheinlicher als das Finden einer Nicht-Einheit modulo P. ⁜

Die Bemerkung zeigt, dass die Aussagekraft des Fermat-Tests stark von P abhängt: Es kann sein, dass der Test für Einheiten a systematisch zu oft „*P könnte prim sein*“ zurückliefert. Gesucht ist daher ein Pseudo-Primzahltest, der Einheiten besser bewertet. Genau dies leistet der Miller-Rabin-Test.

Der Miller-Rabin-Test

Der Miller-Rabin-Test kombiniert den Satz von Euler-Fermat mit der Nullteilerfreiheit von Polynomringen über Körpern:
Sei P eine ungerade Primzahl. Dann lässt sich $P-1$ in der Form $P-1 = 2^s \cdot u$ mit ungeradem $u \in \mathbb{N}$ und $s \geq 1$ schreiben. Sei $a \in \{1, 2, \dots, P-1\}$ beliebig. Nach Euler-Fermat ist dann

$$a^{2^s \cdot u} = a^{P-1} \equiv 1 \pmod{P}.$$

Das Element $a^{2^{s-1} \cdot u}$ ist dann eine Nullstelle des Polynoms $X^2 - 1 \in \mathbb{F}_P[X]$. Aus der Zerlegung $X^2 - 1 = (X+1) \cdot (X-1)$ folgt

$$a^{2^{s-1} \cdot u} \equiv \pm 1 \pmod{P}.$$

Falls $a^{2^{s-1} \cdot u} \equiv 1 \pmod{P}$ ist, können wir diese Argumentation nochmals anwenden und erhalten $a^{2^{s-2} \cdot u} \equiv \pm 1 \pmod{P}$. Falls $a^{2^{s-2} \cdot u} \equiv 1 \pmod{P}$, so folgt analog $a^{2^{s-3} \cdot u} \equiv \pm 1 \pmod{P}$, etc.
Dies können wir immer weiter fortsetzen, bis entweder $a^u \equiv 1 \pmod{P}$ oder

$$a^{2^k \cdot u} \equiv -1 \pmod{P} \qquad \text{für ein } k < s$$

gelten. Hier können wir nicht weiter argumentieren, weil unklar ist, wie sich die Polynome $X^u - 1$ bzw. $X^2 + 1$ über $\mathbb{F}_P$ zerlegen.

Der Miller-Rabin-Test prüft nun dieses Verhalten für Elemente a ab. Wir zerlegen $P-1$ wie oben in der Form $P-1 = 2^s \cdot u$ mit ungeradem u und $s \geq 1$. Der Test ist ebenfalls rundenbasiert. In jeder Runde

- wählen wir ein zufälliges a mit $1 \leq a \leq P-1$ und
- überprüfen die **Miller-Rabin-Bedingung**: Es gelten
  - $a^u \equiv 1 \pmod{P}$ oder
  - $a^{2^k \cdot u} \equiv -1 \pmod{P}$ für ein $k \in \{0, 1, \dots, s-1\}$.
- Ist die Bedingung *nicht* erfüllt, so geben wir „*P ist sicher nicht prim*“ aus und beenden den Test; weitere Runden sind nicht nötig.
  Ist diese erfüllt, geben wir „*P könnte prim sein*“ aus und starten mit der nächsten Runde, falls das Rundenlimit noch nicht erreicht ist.

Beispiel 43.3 Wir untersuchen, ob $P := 561$ prim ist. Es ist $P - 1 = 560 = 2^4 \cdot 35$. Wir testen die Miller-Rabin-Bedingung für die Elemente aus $\{103, 50, 4, 67, 375\}$, die zufällig gewählt wurden.
Wir berechnen die Potenzen pro Runde nur so weit, bis wir entscheiden können, ob a die Miller-Rabin-Bedingung erfüllt. Im Falle des Nichterfüllens färben wir das Rechenergebnis rot ein, das der Miller-Rabin-Bedingung widerspricht.

a	$a^{35} \bmod P$	$a^{2\cdot 35} \bmod P$	$a^{2^2\cdot 35} \bmod P$	$a^{2^3\cdot 35} \bmod P$
103	1			
50	$P - 1 \equiv -1$			
4	166	67	1	
67	67	1		
375	375	375	375	375

Jedes a, für das die Zeile in der obigen Tabelle einen roten Eintrag enthält, zeigt, dass P nicht prim ist. ⋇

Bemerkung 43.4 (a) Die Berechnung von a^u ist der aufwendige Teil bei der Überprüfung der Miller-Rabin-Bedingung. Die Potenzen $a^{2^k \cdot u}$ erhält man dann durch sukzessives Quadrieren. Dies ist sehr effizient machbar.

(b) Erfüllt a die Miller-Rabin-Bedingung, so erfüllt a auch die Fermat-Bedingung: Aufgrund der Voraussetzung gibt es ein $k \in \{0, 1, \ldots s-1\}$ mit $a^{2^k \cdot u} \equiv \pm 1 \pmod{P}$. Dann ist

$$a^{2^{k+1} \cdot u} = \left(a^{2^k \cdot u}\right)^2 \equiv (\pm 1)^2 = 1 \pmod{P}.$$

Hieraus folgt, dass $a^{P-1} = a^{2^s \cdot u} \equiv 1 \pmod{P}$ ist. ⋇ ؟

Ist P eine zusammengesetzte Zahl, so sagt Teil (b) der Bemerkung aus, dass die Miller-Rabin-Bedingung höchstens so oft die (falsche) Ausgabe „*P könnte prim sein*“ liefert wie die Fermat-Bedingung. Der Miller-Rabin-Test ist also mindestens so gut wie der Fermat-Test. Man kann aber mehr zeigen:

Satz 43.5 *Sei P eine ungerade zusammengesetzte Zahl. Dann ist die Anzahl der Elemente a mit $1 \le a \le P-1$, die (fälschlicherweise) die Miller-Rabin-Bedingung erfüllen, höchstens $\frac{1}{2}(P-1)$.*

Beweis. Es sei $M := \{a \in \{1, 2, \ldots, P-1\} \mid a \text{ erfüllt die Miller-Rabin-Bedingung}\}$. Wir müssen $|M| \le \frac{1}{2}(P-1)$ zeigen.
Zunächst folgt aus 43.4 (b), dass alle Elemente aus M die Fermat-Bedingung erfüllen und daher nach 43.1 Einheiten sind. Es ist also $M \subseteq \mathbb{Z}_P^\times$.
Wir benutzen nun einen gruppentheoretischen Trick und definieren eine Untergruppe $U \le \mathbb{Z}_P^\times$ mit $M \subseteq U$. Dann zeigen wir, dass $U \neq \mathbb{Z}_P^\times$ ist, es sich bei U also um eine *echte* Untergruppe handelt. Dann ist der Index $[\mathbb{Z}_P^\times : U] \ge 2$, was

$$|M| \le |U| < \frac{1}{2} \cdot |\mathbb{Z}_P^\times| = \frac{1}{2} \cdot \varphi(P)$$

zeigt. Da $\varphi(P) \leq P-1$ ist, folgt die zu zeigende Aussage.
Die Untergruppe U muss (leider) in Abhängigkeit von der Form von P definiert werden. Dies führt auf zwei Fälle:

***P* ist eine Primpotenz** Sei $P = p^r$ mit $p \in \mathbb{P}$. Da P als zusammengesetzt angenommen war, ist $r \geq 2$. Wir setzen

$$U := \{a \in \{1, 2, \dots, P-1\} \mid a^{\frac{1}{2}(P-1)} \equiv \pm 1 \pmod{P}\}.$$

Dann ist $M \subseteq U$. Weiter folgt mit dem Untergruppenkriterium $U \leq \mathbb{Z}_P^\times$. Wir konstruieren nun ein $a \in \mathbb{Z}_P^\times$ mit $a \notin U$. Dann ist der Satz in diesem Fall bewiesen.

Sei a eine Primitivwurzel modulo P. Die Existenz einer solchen folgt aus 42.14. Dann ist a eine Einheit, also ein Element von $\mathbb{Z}_P^\times$.
Läge a in U, so wäre

$$a^{\frac{1}{2}(P-1)} \equiv \pm 1 \pmod{P} \qquad \text{und somit} \qquad a^{P-1} \equiv 1 \pmod{P}.$$

Die rechte Kongruenz liefert dann $\operatorname{ord}_P(a) \mid P-1$. Dies ist ein Widerspruch, denn wegen $r \geq 2$ ist p ein Teiler von $\operatorname{ord}_P(a) = \varphi(P) = (p-1)p^{r-1}$, aber nicht von $P - 1 = p^r - 1$. Also ist $a \notin U$.

***P* ist keine Primpotenz** Nach Voraussetzung ist $P-1$ eine gerade Zahl und lässt sich in der Form $P - 1 = 2^s \cdot u$ mit ungeradem u und $s \geq 1$ schreiben. Für $i \in \{0, 1, \dots, s\}$ definieren wir die Mengen

$$M_i := \{a \in M \mid a^{2^i \cdot u} \equiv -1 \pmod{P}\} \subseteq M.$$

Man rechnet nach, dass $P-1 \in M_0$ ist. Weiter sieht man $M_s = \emptyset$, denn nach 43.4 (b) gilt

$$a^{2^s \cdot u} = a^{P-1} \equiv 1 \pmod{P} \qquad \text{für jedes } a \in M.$$

Daher existiert ein $k \in \{0, 1, \dots, s-1\}$ mit $M_k \neq \emptyset$ und $M_i = \emptyset$ für alle $i > k$.

Mit diesem k definieren wir

$$U := \{a \in \{1, 2, \dots, P-1\} \mid a^{2^k \cdot u} \equiv \pm 1 \pmod{P}\}.$$

Mit dem Untergruppenkriterium folgt, dass $U \leq \mathbb{Z}_P^\times$ ist. Weiter gilt aufgrund der Maximalität von k, dass $M \subseteq U$ ist. Wir konstruieren nun ein $a \in \mathbb{Z}_P^\times$ mit $a \notin U$. Dann ist der Satz auch in diesem Fall bewiesen.

Da P keine Primpotenz ist, wird P von mindestens zwei verschiedenen Primzahlen geteilt. Wir können P daher in der Form $P = p^r \cdot n$ mit einer Primpotenz p^r und zu p teilerfremdem $n > 2$ schreiben. Sei $m \in M_k$. Wir definieren $a \in \{1, 2, \dots, P-1\}$ als eindeutige Lösung des Kongruenzsystems

$$\left\{ \begin{array}{rcll} a & \equiv & m & \pmod{p^r} \\ a & \equiv & 1 & \pmod{n} \end{array} \right\};$$

die Existenz von a folgt aus dem chinesischen Restsatz. Für die Potenz $a^{2^k \cdot u}$ folgt dann

$$\left\{ \begin{array}{lcll} a^{2^k \cdot u} & \equiv & m^{2^k \cdot u} \overset{a \in M_k}{\equiv} -1 & (\text{mod } p^r) \\ a^{2^k \cdot u} & \equiv & 1^{2^k \cdot u} \equiv 1 & (\text{mod } n) \end{array} \right\}.$$

Dies zeigt, dass $a^{2^k \cdot u}$ kein Element aus U ist. ■

Bemerkung 43.6 (a) Im Beweis zu 43.5 unterscheiden wir, je nach der (unbekannten) Gestalt von P, zwei Fälle. Beide Male können wir jedoch dieselbe Abschätzung nachweisen. Die Aussage des Satzes gilt also unabhängig von der Gestalt von P.
Im Gegensatz zum Fermat-Test erhalten wir hier also eine für alle P garantierte Abschätzung für die Anzahl der a, die eine zusammengesetzte Zahl fälschlicherweise als prim erkennen.

(b) Man kann die Abschätzung in 43.5 mit einer etwas komplizierteren Beweisführung auf $\frac{1}{4}(P-1)$ verbessern. Dies wurde von Rabin im Jahr 1980 gezeigt. ※

Als Konsequenz aus 43.5 erhalten wir

Korollar 43.7 *Sei P eine ungerade zusammengesetzte Zahl. Dann beträgt die Wahrscheinlichkeit, dass P vom Miller-Rabin-Test nach n Runden fälschlicherweise als prim erkannt wird, höchstens $\frac{1}{2^n}$.*

Beweis. Damit P fälschlicherweise vom Test als prim erkannt wird, muss in jeder der n Runden ein Element $a \in \{1, 2, \ldots, P-1\}$ gewählt werden, das die Miller-Rabin-Bedingung erfüllt. Da die Auswahlen der Elemente a unabhängig und zufällig erfolgen, beträgt die Wahrscheinlichkeit hierfür nach 43.5 höchstens

$$\left(\frac{\frac{1}{2}(P-1)}{P-1} \right)^n = \frac{1}{2^n}.$$

■

Bemerkung 43.8 Die Schranke für die Wahrscheinlichkeit im obigen Korollar, fällt sehr schnell.
Ein Miller-Rabin-Test mit nur 20 Runden hat bereits eine Fehlerwahrscheinlichkeit von höchstens 10^{-6}. Das ist in etwa die Wahrscheinlichkeit, von einem Blitz getroffen zu werden.
Vergrößert man die Rundenanzahl auf 30, so gewinnt man im Schnitt sieben Mal den Jackpot im Lotto, bevor sich Miller-Rabin ein einziges Mal irrt. ※

44. Quadrate modulo n

Worum geht es? Die Lösbarkeitstheorie linearer Kongruenzen haben wir in den Übungen behandelt. Nun widmen wir uns dem nächst schwierigeren Fall: Seien $a \in \mathbb{Z}$ und $n \in \mathbb{N}$ gegeben. Wir sind an der Lösbarkeit der Kongruenz → Übung

$$x^2 \equiv a \pmod{n} \tag{Q}$$

interessiert, also an der Frage nach der Existenz eines passenden $x \in \mathbb{Z}$. Diese Frage ist intensiv studiert worden, hat ein großes Theoriegebäude hervorgebracht und bildet den Schwerpunkt der nächsten Vorlesungen.
In dieser Vorlesung wenden wir eine typische Strategie der Zahlentheorie an: Wir reduzieren die Fragestellung von allgemeinen Moduln auf Primpotenz-Moduln und diskutieren diesen Fall dann genauer. ⁜

Um Kongruenzen vom Typ (Q) sprachlich besser fassen zu können, führen wir den Begriff des *Quadrats* ein:

Definition 44.1 *Sei $n \in \mathbb{N}$ eine natürliche Zahl. Wir nennen ein Element $\overline{a} \in \mathbb{Z}_n$ ein **Quadrat**, wenn es ein $\overline{x} \in \mathbb{Z}_n$ mit $\overline{x}^2 = \overline{a}$ gibt. Andernfalls nennen wir $\overline{a}$ ein **Nichtquadrat**.*
*Analog nennen wir eine ganze Zahl $a \in \mathbb{Z}$ ein **Quadrat modulo n**, wenn es ein $x \in \mathbb{Z}$ mit $x^2 \equiv a \pmod{n}$ gibt. Andernfalls nennen wir a ein **Nichtquadrat modulo n**.*

Bemerkung 44.2 Wie auch in 42.1 und 42.2 stellen wir den Quadrat-Begriff in zwei Varianten bereit, einmal für Restklassen aus $\mathbb{Z}_n$, einmal für ganze Zahlen. Beide Begriffe beschreiben denselben Sachverhalt; genau dann ist a ein Quadrat modulo n, wenn $\overline{a} \in \mathbb{Z}_n$ ein Quadrat ist. ⁜

Der folgende Satz reduziert die Frage nach der Lösbarkeit von (Q) auf Primpotenz-Moduln. Das wesentliche Hilfsmittel für den Beweis ist die Mutter aller Reduktionsresultate, der chinesische Restsatz.

Satz 44.3 *Seien n eine natürliche Zahl mit Primfaktorzerlegung $n = p_1^{r_1} \cdots p_s^{r_s}$ und $a \in \mathbb{Z}$ eine ganze Zahl. Dann sind äquivalent:*

(a) *a ist ein Quadrat modulo n.*

(b) *Für jedes $i \in \{1, 2, \ldots, s\}$ ist a ein Quadrat modulo $p_i^{r_i}$.*

Beweis. Um die Lesbarkeit zu erhöhen, setzen wir $q_i := p_i^{r_i}$. Es ist also $n = q_1 \cdots q_s$.

(a)$\Longrightarrow$(b) Da a ein Quadrat modulo n ist, existiert ein $x \in \mathbb{Z}$ mit $x^2 \equiv a \pmod{n}$. Mit 40.6 folgt $x^2 \equiv a \pmod{q_i}$ für alle i. Somit ist a ein Quadrat modulo q_i für jedes i.

(b)$\Longrightarrow$(a) Da a ein Quadrat modulo aller der q_i ist, gibt es $x_1, \ldots, x_s \in \mathbb{Z}$ mit $x_i^2 \equiv a \pmod{q_i}$ für alle i. Da die q_i paarweise teilerfremd sind, existiert nach dem chinesischen Restsatz ein $x \in \mathbb{Z}$ mit $x \equiv x_i \pmod{q_i}$ für alle i.
Für alle i ist daher $x^2 \equiv x_i^2 \equiv a \pmod{q_i}$. Mit 40.5 ergibt sich $x^2 \equiv a \pmod{n}$, also die Aussage, dass a ein Quadrat modulo n ist. ■

Quadrate modulo Primzahlpotenzen

Wir beschränken uns im Folgenden auf Kongruenzen der Form (Q), bei denen n eine Primpotenz, also von der Form $n = p^r$ mit $p \in \mathbb{P}$ und $r \in \mathbb{N}$ ist.
In dieser Situation kann man bereits viele a als Quadrate modulo n ausschließen:

Satz 44.4 *Seien p eine Primzahl und $r \in \mathbb{N}$. Die ganze Zahl $a \neq 0$ sei zerlegt in der Form $a = m \cdot p^k$ mit $k \in \mathbb{N}_0$ und $p \nmid m$. Dann gilt: Genau dann ist a ein Quadrat modulo p^r, wenn einer der folgenden Fälle eintritt:*

(a) *Es gilt $k \geq r$, d.h. es ist $a \equiv 0 \pmod{p^r}$.*

(b) *Es ist $k < r$ und k ist gerade und m ist ein Quadrat modulo p^{r-k}.*

Beweis. Genau dann ist a ein Quadrat modulo p^r, wenn ein $x \in \mathbb{Z}$ mit $p^r \mid a - x^2$ existiert, also wenn

$$zp^r = mp^k - x^2 \qquad \text{für ein } z \in \mathbb{Z} \tag{$\star$}$$

gilt. Wir analysieren diese Bedingung genauer:

Fall $k \geq r$: Hier können wir $(\star)$ lösen, indem wir $x = 0$ und $z = m \cdot p^{k-r}$ setzen. Dies zeigt, dass a ein Quadrat modulo p^r ist.

Fall $k < r$ Wir formen $(\star)$ um und erhalten

$$(\star) \iff zp^r - mp^k = -x^2 \overset{k<r}{\iff} p^k \cdot (zp^{r-k} - m) = -x^2.$$

Die linke Seite der Gleichung rechts wird von p^k, nicht aber von p^{k+1} geteilt, da der Faktor $zp^{r-k} - m$ kein Vielfaches von p ist. Hieraus folgen

$$p^k \mid x^2 \qquad \text{und} \qquad p^{k+1} \nmid x^2.$$

Für ungerades k ist dies widersprüchlich, denn der Primfaktor p kommt in der Quadratzahl x^2 in gerader Häufigkeit vor.

k muss also gerade sein, so dass wir $k = 2s$ mit $s \in \mathbb{N}_0$ schreiben können. Dann folgt $p^{2s} \mid x^2$, also $p^s \mid x$. Wir können daher $x = p^s \cdot y$ mit $y \in \mathbb{Z}$ schreiben. Dies liefert

$$\begin{aligned}(\star) &\overset{\text{s.o.}}{\iff} p^{2s} \cdot (zp^{r-k} - m) = -p^{2s}y^2 \iff zp^{r-k} - m = -y^2 \iff zp^{r-k} = m - y^2 \\ &\iff m \text{ ist Quadrat modulo } p^{r-k}.\end{aligned}$$

Es folgt also, dass a im Fall $k < r$ genau dann ein Quadrat modulo p^r ist, wenn k gerade und m ein Quadrat modulo p^{r-k} ist. ∎

Bemerkung 44.5 Im obigen Satz wurde $a \neq 0$ gefordert. Dies hat einen rein technischen Hintergrund: Für $a = 0$ existiert die Zerlegung $a = m \cdot p^k$ mit $p \nmid m$ nicht.
Da Null ein Quadrat modulo jeder natürlichen Zahl ist, folgt zusammen mit 44.4: Genau dann ist $a \in \mathbb{Z}$ ein Quadrat modulo p^r, wenn $a = 0$ ist oder Fall (a) bzw. (b) des Satzes eintritt. ※

In Fall (b) des Satzes wird die Quadrat-Frage für a in eine Quadrat-Frage für m umformuliert. Beachten Sie, dass m teilerfremd zu p und daher eine Einheit modulo jeder Potenz von p ist. Da Einheiten viele angenehme Eigenschaften haben (man kann durch sie teilen, die Menge der Einheiten besitzt Gruppenstruktur), entsteht eine Fragestellung, die mehr „Struktur" besitzt und sich mathematisch besser behandeln lässt.
Um die Quadrat-Eigenschaft für zu p teilerfremde a besser fassen zu können, führen wir den Begriff des *Restes* ein:

Definition 44.6 *Sei $n \in \mathbb{N}$ eine natürliche Zahl. Wir nennen $\overline{a} \in \mathbb{Z}_n$ einen **quadratischen Rest**, wenn $\overline{a}$ Quadrat und Einheit ist. Ist $\overline{a}$ Nichtquadrat und Einheit, so nennen wir $\overline{a}$ einen **quadratischen Nichtrest**.*
*Analog nennen wir eine ganze Zahl $a \in \mathbb{Z}$ einen **quadratischen Rest modulo n**, wenn a ein Quadrat und Einheit modulo n ist. Falls a Nichtquadrat und Einheit modulo n ist, so sprechen wir bei a von einem **quadratischen Nichtrest modulo n**.*

Bemerkung 44.7 Der Begriff des quadratischen (Nicht-)Rests entspricht inhaltlich dem des (Nicht-)Quadrats, es wird aber zusätzlich gefordert, dass das entsprechende Element eine Einheit ist. Dies hat zur Folge, dass die Begriffe quadratischer (Nicht-)Rest auf Nicht-Einheiten nicht anwendbar sind.
Beispielsweise ist 22 ein Quadrat modulo 22, aber weder quadratischer Rest noch Nichtrest modulo 22. ⁉ ※

Quadratische Reste modulo Primzahlpotenzen

44.4 reduziert die Untersuchung von Quadraten modulo Primzahlpotenzen auf die Untersuchung von quadratischen Resten modulo Primzahlpotenzen.
Wir stellen zwei Resultate vor, mit denen sich die Fragestellung weiter vereinfachen lässt. Wir starten mit dem Fall ungerader Primzahlpotenzen. Beachten Sie, dass im Beweis des Satzes die Einheiten-Eigenschaft von a eine wichtige Rolle einnimmt.

Satz 44.8 *Seien p eine ungerade Primzahl, $r \in \mathbb{N}$ und $a \in \mathbb{Z}$. Dann sind äquivalent:*

(a) *a ist ein quadratischer Rest modulo p^r.*

(b) *a ist ein quadratischer Rest modulo p.*

Es reicht also aus, die quadratische Rest-Eigenschaft von a nur modulo ungerader Primzahlen zu untersuchen.

Beweis. Genau dann ist a eine Einheit modulo p^r, wenn a eine Einheit modulo p ist. Wir können uns im Folgenden also den Nachweis der Quadrat-Eigenschaft beschränken und die Rest-Eigenschaft vernachlässigen. ⁉

(a)$\Longrightarrow$(b) folgt aus 40.6.

(b)$\Longrightarrow$(a) Wir beweisen die Aussage in (a) per Induktion nach r. Im Fall $r = 1$ stimmt (a); dies ist gerade die gegebene Voraussetzung in (b).

Sei bereits nachgewiesen, dass a ein Quadrat modulo p^r ist, also dass eine Darstellung der Form

$$zp^r = a - x^2 \qquad \text{mit ganzen Zahlen } z, x \in \mathbb{Z} \tag{$\star$}$$

existiert.

Wegen $x^2 = a - zp^r$ und $p \nmid a$ ergibt sich $p \nmid x$. Also ist x eine Einheit modulo p und somit auch modulo p^r. Da p ungerade ist, ist auch 2 eine Einheit modulo p^r. Wir setzen nun $y := x + (2x)^{-1} \cdot zp^r \in \mathbb{Z}$, wobei wir mit $(2x)^{-1}$ eine ganze Zahl mit $(2x)^{-1} \cdot 2x \equiv 1 \pmod{p^r}$ meinen. Dann ist

$$\begin{aligned} a - y^2 &= a - \left(x + (2x)^{-1} \cdot zp^r\right)^2 = a - x^2 - 2x \cdot (2x)^{-1} \cdot zp^r + (2x)^{-2} \cdot z^2 p^{2r} \\ &\overset{(\star)}{=} zp^r - 2x \cdot (2x)^{-1} \cdot zp^r + (2x)^{-2} \cdot z^2 p^{2r} \\ &\equiv zp^r - zp^r + (2x)^{-2} \cdot z^2 p^{2r} = (2x)^{-2} \cdot z^2 p^{2r} \\ &\overset{2r \geq r+1}{\equiv} (2x)^{-2} \cdot z^2 \cdot 0 = 0 \pmod{p^{r+1}}. \end{aligned}$$

Dies zeigt, dass a ein Quadrat modulo p^{r+1} ist und beendet den Beweis. ■

Wir geben nun das Resultat für $p = 2$ an. Die Äquivalenz der Aussagen in (b) und (c) im Satz folgt, indem man die acht Elemente in $\mathbb{Z}_8$ untersucht und nachweist, dass $\overline{1} \in \mathbb{Z}_8$ der einzige quadratische Rest ist. Die Äquivalenz dieser Aussagen zu (a) zeigt man ähnlich wie im Beweis oben.

Satz 44.9 *Seien $r \in \mathbb{N}$ und $a \in \mathbb{Z}$. Dann sind äquivalent:*

(a) *a ist ein quadratischer Rest modulo 2^r mit $r \geq 3$.*

(b) *a ist ein quadratischer Rest modulo 2^3.*

(c) *Es ist $a \equiv 1 \pmod 8$.*

Bemerkung 44.10 Die Frage nach quadratischen Resten modulo 2^r wird durch den Satz für alle $r \geq 3$ geklärt. Wir diskutieren noch die Fälle $r = 1$ und $r = 2$ und klären so die Frage nach quadratischen Resten für alle 2-Potenzen:
Der einzige quadratische Rest in $\mathbb{Z}_2 = \{\overline{0}, \overline{1}\}$ ist $\overline{1} = 1 + 2\mathbb{Z}$. Daher sind genau die ungeraden Zahlen quadratische Reste modulo 2.
Die Einheitengruppe des Rings $\mathbb{Z}_4$ ist $\mathbb{Z}_4^\times = \{\overline{1}, \overline{3}\}$. Durch Einsetzen der vier Elemente von $\mathbb{Z}_4$ sieht man, dass $\overline{3}$ ein quadratischer Nichtrest ist. Also ist $\overline{1}$ der einzige quadratische Rest in $\mathbb{Z}_4$. Dies bedeutet, dass die Menge der quadratischen Reste modulo 4 durch $1 + 4\mathbb{Z}$ gegeben ist. ※

Beispiel 44.11 Wir wollen wissen, ob 180 ein Quadrat modulo $n := 2^4 \cdot 13^7 \cdot 19^2$ ist. Mit den Resultaten aus der Vorlesung können wir schließen

$$
\begin{aligned}
&\text{180 ist Quadrat modulo } n \\
&\overset{44.3}{\iff} \left\{ \begin{array}{l} 180 = 45 \cdot 2^2 \text{ ist Quadrat modulo } 2^4 \\ 180 \text{ ist Quadrat modulo } 13^7 \\ 180 \text{ ist Quadrat modulo } 19^2 \end{array} \right\} \\
&\overset{44.4}{\iff} \left\{ \begin{array}{l} 45 \text{ ist quadratischer Rest modulo } 2^2 \\ 180 \text{ ist quadratischer Rest modulo } 13^7 \\ 180 \text{ ist quadratischer Rest modulo } 19^2 \end{array} \right\} \\
&\overset{44.8}{\iff} \left\{ \begin{array}{l} 45 \equiv 1 \text{ ist quadratischer Rest modulo } 2^2 \\ 180 \equiv 11 \text{ ist quadratischer Rest modulo } 13 \\ 180 \equiv 9 \text{ ist quadratischer Rest modulo } 19 \end{array} \right\} \\
&\iff \left\{ \begin{array}{ll} 1 \text{ ist quadratischer Rest modulo } 2^2 & \text{(I)} \\ 11 \text{ ist quadratischer Rest modulo } 13 & \text{(II)} \\ 9 \text{ ist quadratischer Rest modulo } 19 & \text{(III)} \end{array} \right\}.
\end{aligned}
$$

Es ist klar, dass die Aussagen (I) und (III) stimmen.
Die Aussage in (II) können wir mit den jetzigen Mitteln noch nicht entscheiden. Die Frage, ob 180 ein Quadrat modulo n ist, bleibt also an dieser Stelle offen. Wir kommen aber in den nächsten Vorlesungen auf sie zurück. ※

45. Quadratische (Nicht-)Reste modulo ungerader Primzahlen

Worum geht es? Die Frage nach Quadraten modulo n lässt sich mit den Techniken aus der letzten Vorlesung auf die Frage nach quadratischen Resten modulo ungerader Primzahlen, also auf die Frage nach dem Wert des *Legendre-Symbols* reduzieren. Dieses lässt sich mit Hilfe des *Euler-Kriteriums* und, in Spezialfällen, auch mit Hilfe der *Ergänzungsgesetze* berechnen. ⁜

Seien p eine ungerade Primzahl und $\overline{a} \in \mathbb{Z}_p$ eine Einheit. Dann können wir ausnutzen, dass $\mathbb{Z}_p^\times$ zyklisch ist und $\overline{a}$ als Potenz einer Primitivwurzel schreiben. In dieser Darstellung lässt sich sehr leicht entscheiden, ob $\overline{a}$ ein quadratischer Rest oder Nichtrest ist:

Satz 45.1 *Seien $p \in \mathbb{P}$ ungerade und $\overline{g} \in \mathbb{Z}_p$ eine Primitivwurzel. Sei $\overline{a} = \overline{g}^n$ mit $n \in \mathbb{Z}$ ein beliebiges Element aus $\mathbb{Z}_p^\times$. Dann gelten die folgenden Aussagen:*

(a) *Genau dann ist $\overline{a}$ ein quadratischer Rest, wenn n eine gerade Zahl ist.*

(b) *Genau dann ist $\overline{a}$ ein quadratischer Nichtrest, wenn n eine ungerade Zahl ist.*

Beweis. Die Aussage in (b) ist die Kontraposition von (a). Wir zeigen daher nur (a):

$\Longleftarrow$ Sei n gerade, d. h. von der Form $n = 2z$ mit $z \in \mathbb{Z}$. Setzen wir $\overline{b} := \overline{g}^z$, so gilt $\overline{b}^2 = \overline{a}$. Somit ist $\overline{a}$ Einheit und Quadrat, also ein quadratischer Rest.

$\Longrightarrow$ Sei $\overline{a}$ ein quadratischer Rest. Dann existiert ein $\overline{b} \in \mathbb{Z}_p^\times$ mit $\overline{b}^2 = \overline{a}$. Da $\overline{b}$ eine Einheit ist, lässt sich $\overline{b}$ als Potenz von $\overline{g}$ schreiben. Es gibt also ein $m \in \mathbb{Z}$ mit $\overline{b} = \overline{g}^m$. Dann folgt $\overline{a} = \overline{b}^2 = \overline{g}^{2m}$.
Alle Darstellungen der Form $\overline{a} = \overline{g}^n$ mit $n \in \mathbb{Z}$ erfüllen nach 7.16 (b)

$$p - 1 = \operatorname{ord}(\overline{g}) \mid n - 2m \qquad \text{und daher} \qquad n \in 2m + (p-1)\mathbb{Z} \overset{p \text{ ungerade}}{\subseteq} 2\mathbb{Z}.$$

Dies zeigt, dass $n \in 2\mathbb{Z}$ gilt, also dass n gerade ist. ■

Wir können nun eine Aussage über die Anzahl der quadratischen (Nicht-)Reste in $\mathbb{Z}_p$ treffen:

Korollar 45.2 *Sei $p \in \mathbb{P}$ ungerade. Wir bezeichnen mit Q bzw. N die Menge der quadratischen Reste bzw. Nichtreste in $\mathbb{Z}_p$. Dann gilt $|N| = |Q| = \frac{p-1}{2}$.*
Es ist also

$$\mathbb{Z}_p^\times = N \cup Q \qquad \textit{und somit} \qquad \mathbb{Z}_p = N \cup \{\overline{0}\} \cup Q.$$

Beweis. Die disjunkten Zerlegungen von $\mathbb{Z}_p^\times$ und $\mathbb{Z}_p$ sind klar. Es sind nur noch die Mächtigkeiten der Mengen N und Q zu bestimmen.
Sei $\overline{g}$ eine Primitivwurzel von $\mathbb{Z}_p$. Wegen $\operatorname{ord}(\overline{g}) = p - 1$ folgt aus 45.1

$$|Q| = \left|\{\overline{g}^n \mid n \in \{2, 4, 6, \dots, p-3, p-1\}\}\right| = \left|\left\{\overline{g}^{2z} \mid z \in \left\{1, 2, 3, \dots, \frac{p-1}{2}\right\}\right\}\right| = \frac{p-1}{2}.$$

Hieraus folgt $|N| = |\mathbb{Z}_p^\times \setminus Q| = |\mathbb{Z}_p^\times| - |Q| = p - 1 - \frac{p-1}{2} = \frac{p-1}{2}$. ■

Wir ziehen eine weitere wichtige Folgerung aus 45.1:

Korollar 45.3 *Sei $p \in \mathbb{P}$ ungerade. Dann ist die Abbildung*

$$\varphi : \mathbb{Z}_p^\times \to C_2, \qquad \overline{a} \mapsto \begin{cases} 1 & \text{falls } \overline{a} \text{ ein quadratischer Rest ist,} \\ -1 & \text{falls } \overline{a} \text{ ein quadratischer Nichtrest ist} \end{cases}$$

ein Epimorphismus.

Beweisskizze. Es ist klar, dass φ eine Abbildung ist. Wir zeigen die Verträglichkeitsbedingung für Homomorphismen. Seien hierzu $\overline{g}$ eine Primitivwurzel von $\mathbb{Z}_p$ und $\overline{g}^x, \overline{g}^y$ mit $x, y \in \mathbb{Z}$ beliebige Elemente aus $\mathbb{Z}_p^\times$. Dann ist $\overline{g}^x \cdot \overline{g}^y = \overline{g}^{x+y}$.
Nun unterscheidet man, ob x bzw. y gerade bzw. ungerade sind und zeigt, dass in jedem der Fälle $\varphi(\overline{g}^x \cdot \overline{g}^y) = \varphi(\overline{g}^x) \cdot \varphi(\overline{g}^y)$ gilt. Beispielsweise ist für gerades x und gerades y auch $x + y$ gerade. Somit folgt

$$\varphi(\overline{g}^x \cdot \overline{g}^y) = \varphi(\overline{g}^{x+y}) \overset{\text{Def. } \varphi}{=} 1 = 1 \cdot 1 \overset{\text{Def. } \varphi}{=} \varphi(\overline{g}^x) \cdot \varphi(\overline{g}^y).$$

Ist $\overline{g} \in \mathbb{Z}_p^\times$ eine Primitivwurzel, so ist $\varphi(\overline{g}) = -1$. Dies zeigt, dass φ surjektiv ist. ■ ⁉

Knobelfrage. Hätten wir φ nicht auf Wohldefiniertheit prüfen müssen? ⁉

Bemerkung 45.4 (a) Der Homomorphismus aus dem Korollar beschreibt, wie sich quadratische (Nicht-)Reste bei Multiplikation verhalten. Kürzen wir quadratische Reste mit R und Nichtreste mit N ab, ergibt sich die Multiplikationstabelle

$\cdot$	R	N
R	R	N
N	N	R

(b) Aus (a) folgt, dass die Menge der quadratischen Reste unter Multiplikation abgeschlossen ist. Sie bildet daher eine Untergruppe der Einheitengruppe, die nach 45.2 Index Zwei besitzt.
Diese Aussage folgt mit dem Homomorphiesatz auch direkt aus 45.3. ⁂ ⁉

Bis jetzt haben wir vorwiegend im Ring $\mathbb{Z}_p$ gearbeitet. Wir stellen nun eine Notation vor, die über $\mathbb{Z}$ arbeitet:

Definition 45.5 (Legendre-Symbol) *Sei $p \in \mathbb{P}$ ungerade. Für Einheiten a modulo p setzen wir*

$$\left(\frac{a}{p}\right) := \begin{cases} 1 & \text{falls } a \text{ ein quadratischer Rest modulo } p \text{ ist,} \\ -1 & \text{falls } a \text{ ein quadratischer Nichtrest modulo } p \text{ ist} \end{cases}$$

*und nennen $\left(\frac{a}{p}\right)$ das **Legendre-Symbol von a über p**.*

Bemerkung 45.6 (a) Bezeichnen wir mit φ den Epimorphismus aus 45.3, so gilt $\left(\frac{a}{p}\right) = \varphi(\overline{a})$. Das Legendre-Symbol ist also nichts anderes als eine „ganzzahlige Variante" der Funktion φ mit seltsamer Notation.

(b) Manchmal definiert man das Legendre-Symbol auch im Fall $p \mid a$ und setzt dann $\left(\frac{a}{p}\right) := 0$. Dies hat den Vorteil, dass man die Zuordnung $a \mapsto \left(\frac{a}{p}\right)$ als Funktion mit Definitionsbereich $\mathbb{Z}$ auffassen kann und nicht, wie in unserer Definition, auf die komplizierter zu definierende Menge $\{a \in \mathbb{Z} \mid \mathrm{ggT}(a,p) = 1\}$ eingeschränkt ist. Welche der beiden Definitionen man vorzieht, ist Geschmackssache; die Elemente $a \in \mathbb{Z}$ mit $\left(\frac{a}{p}\right) = 0$ sind für die Theorie der quadratischen Reste uninteressant. ⋇

Wir stellen einige grundlegende Rechenregeln für das Legendre-Symbol zusammen:

Satz 45.7 *Sei $p \in \mathbb{P}$ ungerade. Dann gelten die folgenden Aussagen:*

(a) *Sind $a, k \in \mathbb{Z}$ und ist a teilerfremd zu p, so ist $\left(\frac{a}{p}\right) = \left(\frac{a+k\cdot p}{p}\right) = \left(\frac{a \bmod p}{p}\right)$.*

(b) *Für zu p teilerfremde Zahlen a, b gilt $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right) \cdot \left(\frac{b}{p}\right)$.*
Man sagt hierzu auch, dass das Legendre-Symbol ***multiplikativ im Zähler*** *ist.*

(c) *Es ist $\sum_{a=1}^{p-1} \left(\frac{a}{p}\right) = 0$.*

Beweisskizze.

(a) folgt, weil die Eigenschaft, quadratischer (Nicht-)Rest zu sein, nur von der Nebenklasse $\overline{a} \in \mathbb{Z}_p$, nicht aber von einzelnen Vertretern der Nebenklasse abhängt.

(b) folgt aus der Homomorphie der Funktion φ aus 45.3.

(c) folgt aus 45.2, denn in $\mathbb{Z}_p^\times$ stimmt die Anzahl der quadratischen Reste und Nichtreste überein. ■

Der folgende Satz erlaubt die Berechnung beliebiger Legendre-Symbole:

Satz 45.8 (Euler-Kriterium) *Seien p eine ungerade Primzahl und a eine zu p teilerfremde ganze Zahl. Dann ist*

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}.$$

Beweis. Wir setzen $A := a^{\frac{p-1}{2}}$ und führen den Beweis in zwei Schritten: Zunächst zeigen wir, dass $A \equiv \pm 1 \pmod{p}$ ist. Danach beweisen wir, dass $A \equiv 1 \pmod{p}$ genau dann gilt, wenn a ein quadratischer Rest modulo p ist. Dies beweist den Satz. ⁉

Schritt 1: Es gilt $A \equiv \pm 1 \pmod{p}$.

Für A^2 gilt

$$A^2 = a^{p-1} = a^{\varphi(p)} \overset{\text{Euler-Fermat } 40.4}{\equiv} 1 \pmod{p}.$$

Also ist A eine Nullstelle des Polynoms $X^2 - 1 = (X+1)(X-1) \in \mathbb{F}_p[X]$. Aufgrund der Nullteilerfreiheit des Rings $\mathbb{F}_p[X]$ folgt $\overline{A} = \pm\overline{1}$, also $A \equiv \pm 1 \pmod{p}$.

Schritt 2: Es gilt: $A \equiv 1 \pmod{p} \iff A$ ist quadratischer Rest modulo p.

Sei g eine Primitivwurzel modulo p. Da a eine Einheit modulo p ist, gibt es ein $n \in \mathbb{Z}$ mit $a \equiv g^n \pmod{p}$. Da $\overline{g}$ die multiplikative Ordnung $p-1$ hat, folgt

$$1 \equiv A \equiv a^{\frac{p-1}{2}} \equiv g^{n \cdot \frac{p-1}{2}} \pmod{p} \overset{\operatorname{ord}(\overline{g})=p-1}{\iff} p-1 \mid n \cdot \frac{p-1}{2}.$$

Die rechte Teilbarkeitsbedingung ist genau dann erfüllt, wenn n gerade ist. Nach 45.1 ist dies äquivalent dazu, dass a ein quadratischer Rest modulo p ist. ■

Knobelfrage. Können Sie die Frage aus 44.11 entscheiden? ?

Im Spezialfall $a = -1$ kann man im Euler-Kriterium die Kongruenz durch ein Gleichheitszeichen ersetzen, da dann Potenzen von a im Wertebereich des Legendre-Symbols liegen. Es folgt also

Korollar 45.9 (Erstes Ergänzungsgesetz) *Für ungerades $p \in \mathbb{P}$ ist* $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$.

Knobelfrage. Für welche $p \in \mathbb{P}$ gilt $\sqrt{-1} \in \mathbb{F}_p$? ?

Wir wollen nun das zweite Ergänzungsgesetz beweisen, mit dem man das Legendre-Symbol $\left(\frac{2}{p}\right)$ berechnen kann. Im Beweis arbeiten wir im Körper $\mathbb{F}_{p^2}$ und berechnen den Wert eines Ausdrucks auf zwei verschiedene Weisen.

Satz 45.10 (Zweites Ergänzungsgesetz) *Für ungerades $p \in \mathbb{P}$ gilt* $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$.

Beweis. Da p ungerade ist, ist p eine Einheit modulo Acht. Also lässt sich p in der Form $p = 8k + r$ mit $k \in \mathbb{N}_0$ und $r \in \{1, 3, 5, 7\}$ darstellen. Mit dieser Darstellung folgt, dass $8 \mid p^2 - 1$ ist, vgl. die zweite Tabelle am Ende des Beweises.

Dies zeigt, dass der Exponent $\frac{p^2-1}{8}$ im Satz ganzzahlig ist. Weiter folgt, dass der Körper $\mathbb{F}_{p^2}$ ein Element ξ mit multiplikativer Ordnung Acht besitzt, da dessen Einheitengruppe zyklisch ist. ?

Wir setzen nun $G := \xi + \xi^{-1}$ und berechnen die Potenz G^{p-1} auf zwei verschiedene Weisen. Beachten Sie, dass $G \in \mathbb{F}_{p^2}$ ist und die Berechnungen daher in $\mathbb{F}_{p^2}$ stattfinden.

Erste Berechnung Es gilt

$$\begin{aligned} G^2 &= (\xi + \xi^{-1})^2 = \xi^2 + \xi^{-2} + 2 \cdot \xi \cdot \xi^{-1} = \xi^2 + \xi^{-2} + 2 \\ &\overset{\xi^8=1}{=} \xi^2 + \xi^6 + 2 = \xi^2 + \xi^4 \cdot \xi^2 + 2 \\ &\overset{\xi^4=-1}{=} \xi^2 - \xi^2 + 2 = 2. \end{aligned}$$

Hieraus ergibt sich

$$G^{p-1} = (G^2)^{\frac{p-1}{2}} \overset{\text{s.o.}}{=} 2^{\frac{p-1}{2}} \overset{(\star)}{=} \left(\frac{2}{p}\right).$$

In $(\star)$ haben wir ausgenutzt, dass die Berechnung im Teilkörper $\mathbb{Z}_p$ von $\mathbb{F}_{p^2}$ stattfindet, und dann das Euler-Kriterium 45.8 benutzt.

Zweite Berechnung Im Charakteristik-p-Körper $\mathbb{F}_{p^2}$ steht uns der Frobenius-Endomorphismus zur Verfügung. Wir können daher wie folgt umformen:

$$\begin{aligned} G^{p-1} &\overset{G\neq 0}{=} G^{-1}\cdot G^p = G^{-1}\cdot(\xi+\xi^{-1})^p \\ &\overset{\text{Frobenius}}{=} G^{-1}\cdot(\xi^p+\xi^{-p}) = G^{-1}\cdot(\xi^{8k+r}+\xi^{-8k-r}) \\ &\overset{\xi^8=1}{=} a^{-1}\cdot(\xi^r+\xi^{-r}) = \frac{\xi^r+\xi^{-r}}{\xi+\xi^{-1}}. \end{aligned}$$

Insgesamt folgt also

$$\left(\frac{2}{p}\right) = \frac{\xi^r+\xi^{-r}}{\xi+\xi^{-1}}.$$

Die rechte Seite der Gleichung lässt sich für die in Frage kommenden r konkret berechnen. Wir stellen dies am Beispiel $r=3$ vor. Dann ist wegen $\operatorname{ord}(\xi)=8$

$$\frac{\xi^3+\xi^{-3}}{\xi+\xi^{-1}} = \frac{\xi^4\cdot\xi^4\cdot(\xi^3+\xi^{-3})}{\xi+\xi^7} = \frac{\xi^4\cdot(\xi^7+\xi^1)}{\xi+\xi^7} = \xi^4 = -1.$$

Für die restlichen r kann man den Ausdruck ähnlich berechnen und erhält

r	1	3	5	7
$\left(\frac{2}{p}\right)$	1	-1	-1	1

.

Nun ersetzt man p durch $8k+r$ und berechnet die Ausdrücke $\frac{p^2-1}{8}$ und $(-1)^{\frac{p^2-1}{8}}$. Es folgt

r	1	3	5	7
$\frac{p^2-1}{8}$	$8k^2+2k$	$8k^2+6k+1$	$8k^2+10k+3$	$8k^2+14k+6$
$(-1)^{\frac{p^2-1}{8}}$	1	-1	-1	1

.

Durch Vergleich der letzten Zeilen der beiden Tabellen folgt die Aussage im Satz. ■

Knobelfrage. Können Sie die Frage aus 44.11 auch mit Hilfe der Ergänzungsgesetze entscheiden? ?

46. Das quadratische Reziprozitätsgesetz

Worum geht es? Wir beschäftigen uns mit dem quadratischen Reziprozitätsgesetz und setzen es zum Berechnen von Legendre-Symbolen ein. ⋇

Seien p eine ungerade Primzahl und $a \in \mathbb{Z}$ mit $p \nmid a$. Wir wollen das dann definierte Legendre-Symbol $\left(\frac{a}{p}\right)$ berechnen, ohne auf das Euler-Kriterium zurückzugreifen.
Da wir im Zähler des Symbols nach 45.7 (a) modulo p rechnen dürfen, können wir $a \in \{1, 2, \dots, p-1\}$ annehmen. Sei die Primfaktorzerlegung von a durch

$$a = \prod_{i=1}^{r} q_i \qquad \text{mit } r \in \mathbb{N}_0 \text{ und } q_i \in \mathbb{P}$$

gegeben. Die Multiplikativität im Zähler des Symbols liefert

$$\left(\frac{a}{p}\right) = \prod_{i=1}^{r} \left(\frac{q_i}{p}\right).$$

Mit dem zweiten Ergänzungsgesetz können wir die Fälle behandeln, in denen $q_i = 2$ gilt. In den übrigen Fällen tauchen Legende-Symbole auf, die in Zähler und Nenner zwei verschiedene ungerade Primzahlen enthalten.
In dieser Situation greift das quadratische Reziprozitätsgesetz. Es erlaubt, das Symbol nach Einfügen eines Korrekturfaktors „herumzudrehen“:

Satz 46.1 (quadratisches Reziprozitätsgesetz (qRG)) *Seien p, q zwei verschiedene ungerade Primzahlen. Dann gilt*

$$\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}} \cdot \left(\frac{p}{q}\right).$$

Bemerkung 46.2 (a) Das qRG bringt die Frage nach quadratischen Resten modulo p mit der Frage nach quadratischen Resten modulo q in Verbindung. Dies ist mit Blick auf den chinesischen Restsatz recht überraschend:
40.7 sagt aus, dass das Kongruenzsystem $(\star)$ auf Seite 278 für beliebige rechte Seiten lösbar ist; für jeden der paarweise teilerfremden Moduln n_i darf man sich ein beliebiges Element a_i „wünschen“ und erhält dennoch eine Lösung x des Systems. Die Eigenschaften von x modulo der verschiedenen n_i sind also „unabhängig“ voneinander.

Das qRG sagt nun aus, dass bei quadratischen Kongruenzen Abhängigkeiten zwischen teilerfremden Moduln existieren.
Sind beispielsweise p und q zwei verschiedene Primzahlen mit $p, q \in 3 + 4\mathbb{Z}$, so gilt $(-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}} = -1$ und daher $\left(\frac{q}{p}\right) = -\left(\frac{p}{q}\right)$. Hieraus folgt, dass genau eine der Kongruenzen des Systems

$$\left\{ \begin{array}{rcll} x^2 & \equiv & p & (\mathrm{mod}\ q) \\ x^2 & \equiv & q & (\mathrm{mod}\ p) \end{array} \right\}$$

lösbar ist. Die Lösbarkeit der einen Kongruenz impliziert also die Unlösbarkeit der anderen, so dass die beiden Gleichungen des Systems trotz teilerfremder Moduln gekoppelt sind.

(b) Um das qRG in praktischen Rechnungen benutzen zu können, muss der Zähler a im Legendre-Symbol faktorisiert werden, was nur dann in akzeptabler Zeit möglich ist, wenn a klein ist. Das ist die typische Situation in Klausuren, weshalb das qRG gerade dort sehr wertvoll ist.

(c) Aus (a) und (b) folgt, dass das qRG weniger vom rechnerischen, vor allem aber vom mathematischen Standpunkt aus interessant ist. Tatsächlich gibt es keine leichte Erklärung für den in (a) beobachteten Effekt; der eigentliche Grund, warum das qRG gilt, liegt tief in der algebraischen Zahlentheorie verborgen.
Dies motiviert, warum es so viele elementare und gleichzeitig so wenig erhellende Beweise des Gesetzes gibt[12]: Viele Beweise rühren daher, dass man (im Wesentlichen vergeblich) mit einfachen Mitteln nach einem natürlichen Beweis suchte. Die so gefundenen Argumente zeigen das qRG zwar, jedoch liefern sie keine wirkliche Begründung für seine Gültigkeit.

(d) Mit Hilfe des Legendre-Symbols lässt sich das qRG sehr einprägsam formulieren. Dies ist der Grund, warum man die für heutige Standards unübliche Notation nach wie vor in der Mathematik verwendet. ⋇

Ein Beweis des quadratischen Reziprozitätsgesetzes

Man kann das qRG mit einer ähnlichen Technik wie das zweite Ergänzungsgesetz beweisen, indem man ein klug gewähltes Element G betrachtet und dann die Potenz G^{p-1} auf zwei verschiedene Weisen berechnet. Das Element G ist nun aber deutlich komplizierter.
Die Argumente, die wir nun skizzieren und die auf Gauß zurückgehen, lassen sich ausarbeiten und abstrahieren und dann als Beweis für viele Verallgemeinerungen des qRG benutzen.

Seien p und q zwei verschiedene ungerade Primzahlen, wobei ohne Einschränkung $q < p$ gelte. Da dann $q \nmid p$ gilt, gibt es nach 37.10 (a) in einem Erweiterungskörper K von $\mathbb{F}_p$ ein Element ξ mit multiplikativer Ordnung q. Wir setzen nun

$$G := \sum_{a=1}^{q-1} \left(\frac{a}{q}\right) \xi^a \in K.$$

Summen dieser Form nennt man auch **Gauß-Summen**.

Bemerkung 46.3 Beachten Sie, dass die Primzahlen p und q durch G miteinander gekoppelt werden: G ist ein Element eines Charakteristik-p-Körpers, das mit Hilfe eines Elements der Ordnung q definiert wird. ⋇

[12] Allein Gauß hat acht Beweise für das qRG gegeben; mittlerweile sind über 240 Beweise publiziert.

Wir berechnen nun G^p und nutzen hierbei den Frobenius des Körpers K aus.

Lemma 46.4 *Es gilt* $G^p = \left(\frac{p}{q}\right) \cdot G$.

Beweis. Es gilt

$$\begin{aligned}
G^p &= \left(\sum_{a=1}^{q-1} \left(\frac{a}{q}\right) \zeta^a\right)^p \overset{\text{Frobenius}}{=} \sum_{a=1}^{q-1} \left(\frac{a}{q}\right)^p \zeta^{ap} \\
&\overset{\text{(A)}}{=} \sum_{a=1}^{q-1} \left(\frac{a}{q}\right) \zeta^{ap} \overset{\text{(B)}}{=} \sum_{a=1}^{q-1} \left(\frac{a}{q}\right)\left(\frac{p}{q}\right)^2 \zeta^{ap} \\
&= \left(\frac{p}{q}\right) \cdot \sum_{a=1}^{q-1} \left(\frac{a}{q}\right)\left(\frac{p}{q}\right) \zeta^{ap} \overset{\text{Mult. im Zähler}}{=} \left(\frac{p}{q}\right) \cdot \sum_{a=1}^{q-1} \left(\frac{ap}{q}\right) \zeta^{ap} \\
&\overset{\text{(C)}}{=} \left(\frac{p}{q}\right) \cdot \sum_{a=1}^{q-1} \left(\frac{ap \bmod q}{q}\right) \zeta^{ap \bmod q} \overset{\text{(D)}}{=} \left(\frac{p}{q}\right) \cdot \sum_{a=1}^{q-1} \left(\frac{a}{q}\right) \zeta^a = \left(\frac{p}{q}\right) \cdot G.
\end{aligned}$$

Hier noch einige Anmerkungen zu den hervorgehobenen Umformungen:

zu (A) Legendre-Symbole nehmen nur die Werte ± 1 an. Da p ungerade ist, ergibt sich $\left(\frac{a}{q}\right)^p = \left(\frac{a}{q}\right)$.

zu (B) Wegen $q \nmid p$ ist das Symbol $\left(\frac{p}{q}\right)$ definiert. Es gilt $\left(\frac{p}{q}\right)^2 = (\pm 1)^2 = 1$.

zu (C) Die Umformung im Zähler des Legendre-Symbols folgt aus 45.7 (a), die im Exponenten von ζ aus 7.15 (a) und $\operatorname{ord}(\zeta) = q$.

zu (D) p ist teilerfremd zu q und daher eine Einheit modulo q. Somit ist die Abbildung

$$\mathbb{Z}_q^\times \to \mathbb{Z}_q^\times, \qquad \overline{a} \mapsto \overline{a} \cdot \overline{p}$$

eine Bijektion. Der Ausdruck $ap \bmod q$ nimmt für $a \in \{1, 2, \ldots, q-1\}$ also genau die Werte $1, 2, \ldots, q-1$ an. Durch Umsortieren der Summanden erhält man die Darstellung auf der rechten Seite des Gleichheitszeichens. ■

Mit ähnlichen Argumenten und geschicktem Rechnen mit Doppelsummen kann man den Wert von G^2 berechnen. Wir führen den recht technischen Beweis nicht, sondern verweisen auf [MüP11, S. 56 oben].

Lemma 46.5 *Es gilt* $G^2 = (-1)^{\frac{q-1}{2}} \cdot q \in K$.
Da K ein Körper der Charakteristik p ist und $p \nmid q$ gilt, folgt aus dieser Darstellung insbesondere, dass $G \neq 0$ ist.

Nach diesen Vorarbeiten können wir das quadratische Reziprozitätsgesetz beweisen.

Beweis. Da G nach 46.5 ungleich Null ist, können wir in der Darstellung aus 46.4 durch G teilen und erhalten

$$G^{p-1} = \left(\frac{p}{q}\right).$$

Hieraus folgt

$$\begin{aligned}
\left(\frac{p}{q}\right) &= G^{p-1} = (G^2)^{\frac{p-1}{2}} \\
&\overset{46.5}{=} \left((-1)^{\frac{q-1}{2}} \cdot q\right)^{\frac{p-1}{2}} = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}} \cdot q^{\frac{p-1}{2}} \\
&\overset{\text{Euler-Kriterium}}{=} (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}} \cdot \left(\frac{q}{p}\right).
\end{aligned}$$

Multiplikation mit dem Faktor $(-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}$ liefert dann die Darstellung aus 46.1. ■

Anwendungen

Wir stellen einige Aufgaben vor, in denen das qRG eingesetzt werden kann.

Staatsexamensaufgabe (H2012T1A2) *Gibt es ein $x \in \mathbb{Z}$ so, dass die Gleichung*

$$x^{101} - (x+1)^{101} + x^2 - 47 \equiv 0 \pmod{101}$$

erfüllt ist?

101 ist eine Primzahl. Die Kongruenz kann also als Gleichung im Körper $\mathbb{F}_{101}$ interpretiert werden. Hier steht uns der Frobenius zur Verfügung, der $(x+1)^{101} = x^{101} + 1$ liefert. Es folgt

$$\begin{aligned}
& x^{101} - (x+1)^{101} + x^2 - 47 \equiv 0 \pmod{101} \\
\iff\ & x^{101} - x^{101} - 1 + x^2 - 47 \equiv 0 \pmod{101} \\
\iff\ & x^2 - 48 \equiv 0 \pmod{101} \\
\iff\ & x^2 \equiv 48 \pmod{101}.
\end{aligned}$$

Die Lösbarkeit der letzten Gleichung ergibt sich aus dem Wert des Legendre-Symbols $\left(\frac{48}{101}\right)$. Es ist

$$\begin{aligned}
\left(\frac{48}{101}\right) &= \left(\frac{2^4\cdot 3}{101}\right) = \left(\frac{2}{101}\right)^4 \cdot \left(\frac{3}{101}\right) \overset{\left(\frac{a}{b}\right)^4=1}{=} \left(\frac{3}{101}\right) \\
&\overset{\text{qRG}}{=} (-1)^{\frac{3-1}{2}\cdot\frac{101-1}{2}} \cdot \left(\frac{101}{3}\right) \overset{101\equiv 2}{=} +1 \cdot \left(\frac{2}{3}\right) \\
&\overset{\text{2. Erg.gesetz}}{=} (-1)^{\frac{3^2-1}{8}} = -1.
\end{aligned}$$

Es gibt also kein $x \in \mathbb{Z}$, das die gegebene Gleichung löst. ⁜

Staatsexamensaufgabe (Teil (d) von F2014T3A2)
Ist die Kongruenz $y^2 + 97y \equiv 3 \pmod{101}$ *lösbar für* $y \in \mathbb{Z}$*?*

Wir benutzen quadratische Ergänzung, um die Frage nach Lösbarkeit der gegebenen Kongruenz in eine Frage über quadratische Reste umzuformulieren. Es gilt

$$\begin{aligned} & y^2 + 97y \equiv 3 \pmod{101} \\ \overset{97\equiv -4}{\iff} \quad & y^2 - 4y \equiv 3 \pmod{101} \\ \iff \quad & y^2 - 4y + 4 \equiv 3 + 4 \pmod{101} \\ \iff \quad & (y-2)^2 \equiv 7 \pmod{101}. \end{aligned}$$

Genau dann ist die gegebene Gleichung lösbar, wenn Sieben ein quadratischer Rest modulo 101 ist. Dies überprüfen wir mit Hilfe des Legendre-Symbols:

$$\begin{aligned} \left(\frac{7}{101}\right) & \overset{\text{qRG}}{=} (-1)^{\frac{7-1}{2}\cdot\frac{101-1}{2}} \cdot \left(\frac{101}{7}\right) \overset{101\equiv 3}{=} +1 \cdot \left(\frac{3}{7}\right) \\ & \overset{\text{qRG}}{=} (-1)^{1\cdot 3} \cdot \left(\frac{7}{3}\right) = -\left(\frac{1}{3}\right) \overset{\left(\frac{1}{\cdot\cdot}\right)=1}{=} -1. \end{aligned}$$

Die gegebene Kongruenz besitzt also keine Lösung in $\mathbb{Z}$. ⁜

Staatsexamensaufgabe (Teil (a) von F2013T1A1)
Sei $S = \{n \in \mathbb{Z} \mid$ *es gibt* $x, y \in \mathbb{Z}$ *mit* $n = x^2 - 23y^2\}$*. Zeigen Sie: Die Zahl* 97 *ist kein Element von* S*.*

Angenommen, die Zahl 97 sei ein Element von S. Dann existieren ganze Zahlen $x, y \in \mathbb{Z}$ mit $97 = x^2 - 23y^2$. Reduktion modulo 23 liefert die Kongruenz

$$x^2 \equiv 97 \equiv 5 \pmod{23}.$$

Wir zeigen, dass das Legendre-Symbol $\left(\frac{5}{23}\right)$ den Wert -1 hat:

$$\left(\frac{5}{23}\right) \overset{\text{qRG}}{=} (-1)^{2\cdot 11} \cdot \left(\frac{23}{5}\right) = \left(\frac{3}{5}\right) \overset{\text{qRG}}{=} (-1)^{1\cdot 2} \cdot \left(\frac{5}{3}\right) = \left(\frac{2}{3}\right) \overset{\text{s. o.}}{=} -1.$$

Dies zeigt, dass die obige Kongruenz keine Lösung besitzt. Hieraus folgt, wie gewünscht, dass $97 \notin S$ ist. ⁜