Algebra I

Sommersemester 2003

Christoph Schweigert
Universität Hamburg
Fachbereich Mathematik
Schwerpunkt Algebra und Zahlentheorie

(Stand: 24.08.2005)

Inhaltsverzeichnis

Literatur:

Literatur, die ich bei der Vorbereitung häufig herangezogen habe:

- Kurt Meyberg, Algebra, Teil 1, Hanser 1980.
- Falko Lorenz, Einführung in die Algebra, Teil I. Spektrum Akademischer Verlag, 1996.
- Wolfgang Soergel, Skript zur Vorlesung Algebra, erhältlich unter `http://home.mathematik.uni-freiburg.de/soergel/Skripten/Algebra.ps`

Die aktuelle Version dieses Skriptes finden Sie unter
`http://www.math.uni-hamburg.de/home/schweigert/ss03/skript.ps`
als postscript-Datei und unter
`http://www.math.uni-hamburg.de/home/schweigert/ss03/skript.pdf`
als pdf-Datei. Bitte schicken Sie Korrekturen und Bemerkungen an `schweigert@math.uni-hamburg.de`!

Bei Frau D. Glasenapp möchte ich mich für Ihre große Hilfe bei der Erstellung dieses Skriptes und bei den Hamburger Studenten, besonders bei Herrn Chr. Curilla, J. Hartmann, Frau A. Röser und Fraz G. Schlundt, für zahlreiche Hinweise bedanken.

1 Gruppen

1.1 Mengen mit Verknüpfung

Definition 1.1.1.

(i) Eine Verknüpfung $\top$ auf einer Menge A ist eine Abbildung

$$\begin{array}{rccc} \top: & A \times A & \to & A \\ & (a,b) & \mapsto & a \top b\,, \end{array}$$

die jedem geordneten Paar (a,b) von Elementen a,b der Menge A ein weiteres Element $(a \top b) \in A$ zuordnet.

(ii) Eine Verknüpfung $\top$ heißt assoziativ, wenn gilt $a \top (b \top c) = (a \top b) \top c \quad \forall a,b,c \in A$.

(iii) Die Verknüpfung heißt kommutativ oder abelsch genau dann, wenn gilt $a \top b = b \top a \quad \forall a,b \in A$.

Ist eine Verknüpfung assoziativ, so liefern Ausdrücke der Form $a_1 \top a_2 \ldots \top a_n$ wohlbestimmte Elemente von A, das Resultat ist unabhängig davon, wie man die Klammern setzt.

Definition 1.1.2.

(i) Sei $(A, \top)$ eine Menge mit Verknüpfung. Ein Element $e \in A$ heißt neutrales Element genau dann, wenn gilt

$$e \top a = a \top e = a \quad \forall a \in A\,.$$

(ii) Ein Monoid ist eine Menge mit einer assoziativen Verknüpfung, in der es ein neutrales Element gibt.

In einer Menge mit Verknüpfung kann es höchstens ein neutrales Element e geben, denn für jedes andere Element e' mit $e' \top a = a \top e' = a \quad \forall a \in A$ haben wir $e' = e' \top e = e$. Wir dürfen also in einer Menge mit Verknüpfung von *dem* neutralen Element reden. Manchmal bezeichnen wir es auch mit 1. Man beachte, dass hierfür weder Assoziativität noch die Existenz von Inversen gefordert werden muss.

1.2 Gruppen

Um eine reiche Theorie zu bekommen, reichen Monoide nicht aus.

Definition 1.2.1.
Eine Gruppe ist ein Monoid $(A, \top)$ derart, dass es für jedes $a \in A$ ein $\bar{a} \in A$ gibt mit $a \top \bar{a} = e$, für e das neutrale Element des Monoids A.

In einer Gruppe kann es für jedes $a \in A$ nicht mehr als ein $\bar{a} \in A$ geben mit $a \top \bar{a} = e$, es heißt das Inverse von a. Denn wählen wir zu einem $\bar{a}$ ein mögliches $\bar{\bar{a}}$ mit $\bar{a} \top \bar{\bar{a}} = e$, so folgt aus $a \top \bar{a} = e$ durch Anwenden von $\top \bar{\bar{a}}$ schon $a = \bar{\bar{a}}$, es gilt also auch in einer nicht notwendig kommutativen Gruppe $\bar{a} \top a = e$. Ist $b \in A$ irgendein anderes Element mit $a \top b = e$, so folgt durch Anwenden von $\bar{a} \top$ schon $b = \bar{a}$.

Das Inverse von $a \top b$ wird gegeben durch die Formel $\overline{(a \top b)} = \bar{b} \top \bar{a}$. In der Tat folgt aus der Assoziativität $(a \top b) \top (\bar{b} \top \bar{a}) = e$. Diese Formel ist auch aus dem täglichen Leben vertraut: Wenn man morgens zuerst die Strümpfe anzieht und dann die Schuhe, so muss man abends zuerst die Schuhe ausziehen und dann die Strümpfe.

Bemerkung 1.2.2.
Man findet manchmal als Teil der Definition einer Gruppe die Bedingung "abgeschlossen unter Verknüpfung". Es ist jedoch nicht sinnvoll, so etwas von einer Menge mit Verknüpfung zu fordern. Diese Bedingung wird vielmehr erst sinnvoll als Forderung an eine Teilmenge einer Menge mit Verknüpfung, und sie wird uns dementsprechend bei der Definition einer Untergruppe begegnen. In der Definition einer Gruppe hat diese Bedingung nichts zu suchen.

Beispiele 1.2.3.

(i) Beispiele von Gruppen sollten Sie aus der linearen Algebra kennen: die ganzen (rationalen, reellen, komplexen) Zahlen bezüglich der Addition, die nicht-verschwindenden ganzen (rationalen, reellen, komplexen) Zahlen bezüglich der Multiplikation. Die Elemente eines Vektorraums bilden unter Addition eine Gruppe mit dem Nullvektor als neutralem Element, die invertiblen Matrizen mit Einträgen in einem Körper unter Multiplikation von Matrizen bilden eine (nicht-kommutative) Gruppe.

(ii) Für jede Menge X ist die Menge $\mathcal{S}(X)$ aller Bijektionen von X auf sich selbst eine Gruppe, mit der Komposition von Abbildungen als Verknüpfung. Sie heißt die Gruppe der Permutationen von X. Die Gruppe der Permutationen der Menge $\{1, 2, \ldots, r\}$ heißt auch die r-te symmetrische Gruppe, Bezeichnung $\mathcal{S}_r$.

(iii) Gruppen als Symmetrien:
Stellen wir uns eine ebene Figur vor, d.h. eine beliebige Teilmenge der

Ebene $A \subset \mathbb{R}^2$. Unter einer "ursprungserhaltenden Symmetriebewegung" oder Symmetrie unserer Figur verstehen wir eine urspungserhaltende Bewegung $g \in \mathrm{O}(2)$ der Ebene, die unsere Figur in sich selber überführt, in Formeln $gA = A$. Alle Symmetrien einer Figur bilden unter der Hintereinanderausführung als Verknüpfung eine Gruppe, die Symmetriegruppe der Figur. Bei den meisten Figuren besteht die Symmetriegruppe nur aus dem neutralen Element, aber ein Herz hat schon zwei Symmetrien, die Identität und eine Spiegelung. Der Buchstabe H *hat sogar 4 Symmetrien. In gewissem Sinne können wir eine Gruppe interpretieren als einen "abstrakten Symmetrietyp". Gruppen treten daher in den verschiedensten Gebieten als Symmetriestrukturen auf. Interessanterweise wurden historisch Gruppen aus einem anderen Grund eingeführt, den wir in der Galoistheorie kennen lernen werden.*

Lemma 1.2.4 (Kürzen in einer Gruppe).
In einer Gruppe folgt aus $a \top x = a \top y$ schon $x = y$ und ebenso folgt aus $x \top b = y \top b$ schon $x = y$.

Beweis.
Wir multiplizieren (oder, allgemeiner, verknüpfen) unsere erste Gleichung von links mit dem Inversen von a, und die zweite von rechts mit dem Inversen von b. □

Gruppen werden meist additiv oder multiplikativ geschrieben. Bei additiv geschriebenen Gruppen nennt man das Inverse von a das Negative von a. Im folgenden werden wir abstrakte Gruppen stets multiplikativ schreiben, nur kommutative Gruppen manchmal auch additiv. In diesem Fall bezeichnen wir das neutrale Element auch mit 0.

Wir wollen nun die Frage untersuchen, welche Gruppen es überhaupt gibt. Um Gruppen überhaupt vergleichen zu können, brauchen wir die folgende

Definition 1.2.5.
Seien G, H Gruppen.

1. *Ein Gruppenhomomorphismus $\varphi : G \to H$ ist eine Abbildung, der die Multiplikation respektiert, d.h. es gilt $\varphi(ab) = \varphi(a)\varphi(b) \quad \forall a, b \in G$.*

2. *Ein injektiver Gruppenhomomorphismus heißt auch Monomorphismus. (Cf. griechisch μόνος einzig, z.B. der Mon-arch als Alleinherrscher.)*

3. *Ein surjektiver Gruppenhomomorphismus heißt auch Epimorphismus. (Cf. griechisch επί darauf, z.B. das Epizentrum eines Erdbebens, das auf der Erdoberfläche über dem Zentrum im Erdinneren liegt.)*

4. *Ein bijektiver Gruppenhomomorphismus heißt auch Isomorphismus. (Cf. griechisch ίσος derselbe, z.B. das Iso-top als Element am selben Platz im Periodensystem.)*

5. *Zwei Gruppen heißen isomorph genau dann, wenn es zwischen ihnen einen Isomorphismus gibt.*

6. *Ein Gruppenhomomorphismus einer Gruppe in sich selbst heißt auch Endomorphismus. (Cf. griechisch ενδο in hinein, z.B. die Endo-skopie, bei der man in den Körper hinein schaut.)*

Es gibt gute Gründe, Monomorphismus ein wenig anders zu definieren: ein Gruppenhomomorphismus $f : X \to Y$ heißt Monomorphismus, wenn für jede Gruppe Z und jedes Paar von Gruppenhomomorphismen $g_1, g_2 : Z \to X$ aus $f \circ g_1 = f \circ g_2$ folgt, dass $g_1 = g_2$. Analog heißt f Epimorphismus, wenn wenn für jede Gruppe Z und jedes Paar von Gruppenhomomorphismen $g_1, g_2 : Y \to Z$ aus $g_1 \circ f = g_2 \circ f$ folgt, dass $g_1 = g_2$. Isomorphismen sind dann Epimorphismen, die auch Monomorphismen sind.

Beispiel 1.2.6.
Die Exponentialfunktion ist ein Gruppenhomomorphismus von der additiven Gruppe der reellen Zahlen in die multiplikative Gruppe aller von Null verschiedenen reellen Zahlen $\exp : (\mathbb{R}, +) \to (\mathbb{R}^\times, \cdot)$.
(Ist dieser Homomorphismus injektiv? Surjektiv? Wie sieht diese Antwort für die Exponentialfunktion der komplexen Zahlen aus?)

Bemerkungen 1.2.7.

(i) Die Frage, welche Gruppen es überhaupt gibt, können wir nun konkret fassen als die folgende Frage:
Man gebe eine Liste von endlichen Gruppen an derart, dass jede beliebige endliche Gruppe isomorph ist zu genau einer Gruppe der Liste.

(ii) Man will also Isomorphieklassen *von Gruppen klassifizieren. Man soll immer streng zwischen einer Gruppe und ihrer Isomorphieklasse unterscheiden.*

(iii) Eine endliche Menge mit Verknüpfung beschreiben wir auch durch ihre Verknüpfungstabelle, die im Fall einer Gruppe auch Gruppentafel heißt. Zum Beispiel bilden die dritten Einheitswurzeln 1, $\zeta = \exp(2\pi\mathrm{i}/3)$, $\eta = \exp(4\pi\mathrm{i}/3)$ *in* $\mathbb{C}$ *unter der Multiplikation eine Gruppe mit der Gruppentafel*

	1	ζ	η
1	1	ζ	η
ζ	ζ	η	1
η	η	1	ζ

Haben wir eine Gruppentafel vor uns, so muss nach der Kürzungsregel in jeder Spalte und in jeder Zeile jedes Element genau einmal vorkommen.

1.3 Untergruppen

Definition 1.3.1.
Sei G Gruppe. Eine Teilmenge $H \subset G$ heißt eine Untergruppe von G genau dann, wenn sie abgeschlossen ist unter der Verknüpfung und der Inversenbildung und zusätzlich das neutrale Element enthält, in Formeln $a, b \in H \Rightarrow ab \in H$, $a \in H \Rightarrow a^{-1} \in H$ und $1 \in H$.

Bemerkungen 1.3.2.

(i) Sind diese Axiome für eine Untergruppe minimal?

(ii) Eine nicht-leere endliche *Teilmenge einer Gruppe ist genau dann Untergruppe, wenn sie unter der Multiplikation abgeschlossen ist. (Übung)*

(iii) Sei G eine Gruppe und $\{U_\alpha\}_{\alpha \in I}$ eine Familie von Untergruppen. Dann ist der Schnitt $\cap_{\alpha \in I} U_\alpha$ auch wieder eine Untergruppe. (Wie sieht das mit der Vereinigung aus?)

Lemma 1.3.3.
Sei $\varphi : G \to H$ ein Gruppenhomomorphismus.

1. *Der Kern (englisch kernel, französisch noyeau) $\ker \varphi = \varphi^{-1}(1)$ von φ ist eine Untergruppe von G.*
2. *Das Bild (engl. image) $\mathrm{Im}\varphi = \varphi(G)$ von φ ist eine Untergruppe von H.*
3. *Genau dann ist φ injektiv, wenn gilt $\ker \varphi = \{1\}$.*

Beweis.
1 und 2 sind klar. Wir zeigen 3 durch Widerspruch: Besteht $\ker \varphi$ aus mehr als einem Element, so kann φ natürlich nicht injektiv sein. Gibt es umgekehrt $x \neq y$ mit $\varphi(x) = \varphi(y)$, so liegt $x^{-1}y \neq 1$ in $\ker \varphi$. □

Beispiel 1.3.4.
Die Abbildung sgn*, die jeder Permutation $\tau \in \mathcal{S}_r$ ihr Signum zuordnet, ist ein Gruppenhomomorphismus* $\mathrm{sgn} : \mathcal{S}_r \to \{1, -1\}$*. Der Kern dieses Gruppenhomomorphismus, d.h. die Gruppe der geraden Permutationen, heißt auch die r-te alternierende Gruppe*

$$A_r = \ker(\mathrm{sgn} : \mathcal{S}_r \to \{1, -1\})$$

Satz 1.3.5 (Untergruppen von $\mathbb{Z}$).
Jede Untergruppe $H \subset \mathbb{Z}$ ist von der Form $H = m\mathbb{Z}$ für genau ein $m \in \mathbb{N} \cup \{0\}$.

Beweis.
Ist $H = \{0\}$, so ist $m = 0$ die einzige natürliche Zahl mit $H = m\mathbb{Z}$. Gilt $H \neq \{0\}$, so enthält H echt positive Elemente. Sei $m \in H$ das kleinste echt positive Element von H. Wir behaupten $H = m\mathbb{Z}$. Natürlich gilt $H \supset m\mathbb{Z}$. Aber gäbe es $n \in H \setminus m\mathbb{Z}$, so könnten wir n mit Rest teilen durch m und also schreiben $n = ms + r$ für geeignete $s, r \in \mathbb{Z}$ mit $0 < r < m$ und hätten $r = n - ms \in H$ im Widerspruch zur Minimalität von m. □

Widerspruchsbeweise, in denen Objekte mit Minimalitäts- oder Maximalitätseigenschaften benutzt werden, um einen Widerspruch zu konstruieren, werden uns noch oft begegnen.

Definition 1.3.6.
Seien $a, b \in \mathbb{Z}$. Wir sagen a teilt b und schreiben $a|b$ genau dann, wenn es $d \in \mathbb{Z}$ gibt mit $ad = b$. Gegeben zwei ganze Zahlen a, b, nicht beide Null, verstehen wir unter ihrem größten gemeinsamen Teiler die größte ganze Zahl c, die sie beide teilt, und bezeichnen diese Zahl mit

$$c = \mathrm{ggT}(a, b)\,.$$

Sind a und b nicht beide Null und ist 1 ihr größter gemeinsamer Teiler, so sagen wir auch, a und b seien teilerfremd.

Satz 1.3.7 (Über den größten gemeinsamen Teiler).
Seien $a, b \in \mathbb{Z}$ nicht beide Null und sei $c = \mathrm{ggT}(a, b)$ ihr größter gemeinsamer Teiler. So gilt:

(i) Es gibt $r, s \in \mathbb{Z}$ mit $c = ra + sb$. Für $c = 1$ heißt dieser Satz auch Satz von Bézout.

(ii) Teilt $d \in \mathbb{Z}$ sowohl a als auch b, so teilt d notwendig den größten gemeinsamen Teiler von a und b.

Beweis.
Man betrachte die Teilmenge $a\mathbb{Z}+b\mathbb{Z} \subset \mathbb{Z}$. Sie ist offensichtlich eine von Null verschiedene Untergruppe von $\mathbb{Z}$, also von der Form $a\mathbb{Z}+b\mathbb{Z} = c\mathbb{Z}$ für geeignetes $c > 0$, und es gilt

a. $c = ra + sb$ für geeignete $r, s \in \mathbb{Z}$.

b. (d teilt a und b) $\Rightarrow$ (d teilt c).

Daraus folgt sofort $c = \mathrm{ggT}(a, b)$ und damit dann der Satz. □

Gegeben $a_1, \ldots, a_n \in \mathbb{Z}$ kürzt man oft ab

$$a_1\mathbb{Z} + \ldots + a_n\mathbb{Z} = (a_1, \ldots, a_n)$$

Ein Ausdruck wie der auf der rechten Seite bezeichnet leider oft auch n-Tupel von ganzen Zahlen, also Elemente von $\mathbb{Z}^n$. Es gilt hier aus dem Kontext zu erschließen, was jeweils gemeint ist. Sind a und b nicht beide Null und ist c ihr größter gemeinsamer Teiler, so haben wir nach dem Vorhergehenden $(a, b) = (c)$. Wir benutzen später diese in der Mathematik übliche Notation und schreiben $(a, b) = (c)$ statt $\mathrm{ggT}(a, b) = c$.

Definition 1.3.8.
Eine Primzahl ist eine natürliche Zahl $p > 1$ derart, dass aus $p = ab$ mit $a, b \in \mathbb{N}$ schon folgt $a = 1$ oder $b = 1$.

Satz 1.3.9 (Primfaktorzerlegung).

(i) Jede von Null und Eins verschiedene natürliche Zahl $n \in \mathbb{N}$, $n \geq 2$ kann geschrieben werden als ein Produkt $n = p_1 p_2 \ldots p_r$ von Primzahlen p_i.

(ii) Diese Darstellung ist eindeutig bis auf die Reihenfolge der Faktoren.

Beweis.

(i) ist klar mit vollständiger Induktion.

(ii) folgt ebenso mit vollständiger Induktion aus dem anschließenden Lemma.

□

Lemma 1.3.10.
Teilt eine Primzahl ein Produkt von ganzen Zahlen, so teilt sie einen der Faktoren.

Beweis.

Sei p unsere Primzahl und seien $a, b \in \mathbb{Z}$ gegeben mit $p|ab$. Teilt p nicht a, so folgt $\mathrm{ggT}(p, a) = 1$, und nach 1.3.7 gibt es also $r, s \in \mathbb{Z}$ mit $1 = rp + sa$. Es folgt $b = rpb + sab$ und damit $p|b$. □

Der euklidischen Algorithmus erlaubt es, für zwei ganze Zahlen (a, b) ihren größten gemeinsamen Teiler $c = \mathrm{ggt}(a, b)$ und eine Darstellung $c = xa+yb$ mit $x, y \in \mathbb{Z}$ zu bestimmen. Erklärung am Beispiel $a = 160$, $b = 625$. In der linken Spalte der Gleichungen wird jeweils geteilt mit Rest, und will man nur den größten gemeinsamen Teiler kennen, so kann man die rechte Spalte ignorieren. Die oberste Zeile der rechten Tabelle ist eine Trivialität, die zweitoberste entsteht in offensichtlicher Weise aus der Zeile links daneben, und jede weitere Gleichung der rechten Spalte erhält man als eine Linearkombination der zwei darüberstehenden Gleichungen mit Koeffizienten, die sich aus der Gleichung links daneben ableiten lassen.

$$
\begin{array}{rcl@{\quad}rcl}
 & & & & 160 &=& 160 \\
625 = 3\cdot & 160 & + \; 145 & \Rightarrow & 625 - 3\cdot 160 &=& 145 \\
\swarrow & & \swarrow & & & & \\
160 = 1\cdot & 145 & + \; 15 & \Rightarrow & -1\cdot 625 + 4\cdot 160 &=& 15 \\
\swarrow & & \swarrow & & & & \\
145 = 9\cdot & 15 & + \; 10 & \Rightarrow & 10\cdot 625 - 39\cdot 160 &=& 10 \\
\swarrow & & \swarrow & & & & \\
15 = 1\cdot & 10 & + \; 5 & \Rightarrow & -11\cdot 625 + 43\cdot 160 &=& 5 \\
\swarrow & & \swarrow & & & & \\
10 = 2\cdot & 5 & + \; 0 & & & &
\end{array}
$$

Es folgt $(625, 160) = (160, 145) = (145, 15) = (15, 10) = (10, 5) = (5, 0) = 5$ und wir finden für den größten gemeinsamen Teiler die Darstellung $-11 \cdot 625 + 43 \cdot 160 = 5$.

Bemerkung 1.3.11.
Der euklidische Algorithmus liefert auch einen konstruktiven Beweis des Satzes 1.3.7 von Bézout.

1.4 Restklassen

Ist G eine Menge mit Verknüpfung und sind $A, B \subset G$ Teilmengen, so schreiben wir

$$AB = \{ab \,|\, a \in A,\ b \in B\} \subset G$$

und erhalten auf diese Weise eine Verknüpfung auf der Menge aller Teilmengen von G, der Potenzmenge $\mathcal{P}(G)$. Ist unsere ursprüngliche Verknüpfung assoziativ, so auch die induzierte Verknüpfung auf der Potenzmenge. (Gilt die Umkehrung?)

Wir kürzen in diesem Zusammenhang oft die einelementige Menge $\{a\}$ mit a ab, so dass also zum Beispiel aB als $\{a\}B$ zu verstehen ist.

Definition 1.4.1.

(i) Ist G eine Gruppe und $H \subset G$ eine Untergruppe, so betrachten wir in der Potenzmenge von G die beiden Teilmengen

$$\begin{aligned} G/H &= \{gH \,|\, g \in G\} \subset \mathcal{P}(G) \\ H\backslash G &= \{Hg \,|\, g \in G\} \subset \mathcal{P}(G) \end{aligned}$$

Die Elemente von G/H heißen die Linksnebenklassen von H in G, die Elemente von $H\backslash G$ heißen die Rechtsnebenklassen von H in G. Wir nennen gH auch die Linksnebenklasse von g unter H und Hg die Rechtsnebenklasse von g unter H.

(ii) Ein Element einer Restklasse nennt man auch oft einen Repräsentanten der besagten Restklasse.

Lemma 1.4.2.
Sei G eine Gruppe und $H \subset G$ eine Untergruppe. Jedes Element von G gehört zu genau einer H-Linksnebenklasse und zu genau einer H-Rechtsnebenklasse.

Beweis.
Nur für Linksnebenklassen. Aus $1 \in H$ folgt $g \in gH$, also gehört jedes Element von G zu mindestens einer Linksnebenklasse. Aus $g \in xH$ folgt $g = xh$ für geeignetes $h \in H$, also $gH = xhH = xH$, folglich ist gH die einzige Linksnebenklasse, die g enthält. □

Beispiel 1.4.3.
Im Fall $G = \mathbb{Z} \supset H = m\mathbb{Z}$ besteht die Nebenklasse aH oder additiv geschrieben $a + H = a + m\mathbb{Z}$ aus allen Elementen von $\mathbb{Z}$, die bei Teilung durch m denselben Rest lassen wie a. Wir nennen in diesem Fall $a + m\mathbb{Z} \subset \mathbb{Z}$ auch die Restklasse von a modulo m. Gehören a und b zur selben Restklasse, in Formeln $a + m\mathbb{Z} = b + m\mathbb{Z}$, so nennen wir sie kongruent modulo m und schreiben

$$a \equiv b \pmod{m}.$$

Offensichtlich gibt es für $m \in \mathbb{N}$, $m \geq 1$ genau m Restklassen modulo m, in Formeln $|\mathbb{Z}/m\mathbb{Z}| = m$, und mögliche Repräsentanten für diese m verschiedenen Restklassen sind die natürlichen Zahlen r mit $0 \leq r < m$.

Satz 1.4.4. *(Lagrange)*
Ist G eine endliche Gruppe und $H \subset G$ eine Untergruppe, so gilt

$$|G| = |H| \cdot |G/H| = |H| \cdot |H\backslash G|$$

Beweis.

Jedes Element von G gehört zu genau einer Links- bzw. Rechtsnebenklasse unter H, und jede dieser Nebenklassen hat genau $|H|$ Elemente. □

Definition 1.4.5.
Die Zahl der Restklassen $|G/H|$ nennt man auch den Index von H in G und schreibt $[G : H]$.

Korollar 1.4.6.
In einer endlichen Gruppe ist die Ordnung jeder Untergruppe ein Teiler der Gruppenordnung.

1.5 Normalteiler und Isomorphiesätze

Definition 1.5.1.

(i) Sei G eine Gruppe. Eine Untergruppe $H \subset G$ heißt ein Normalteiler von G genau dann, wenn gilt $gH = Hg \quad \forall g \in G$.

(ii) Sei G eine Gruppe. Eine Untergruppe $H \subset G$ heißt charakteristisch von G genau dann, wenn $\varphi(H) \subset H$ für alle Automorphismen $\varphi \in Aut\, G$.

Natürlich ist in einer kommutativen Gruppe jede Untergruppe ein Normalteiler. In der Gruppe $\mathcal{S}_3$ der Permutationen von 3 Elementen ist aber die Untergruppe $\mathcal{S}_2 \subset \mathcal{S}_3$ aller Permutationen, die die dritte Stelle festhalten, kein Normalteiler.

Bemerkungen 1.5.2.

(i) Der Kern eines Gruppenhomomorphismus ist stets ein Normalteiler.

(ii) Allgemeiner ist das Urbild eines Normalteilers unter einem Gruppenhomomorphismus stets ein Normalteiler, und das Bild eines Normalteilers unter einem surjektiven *Gruppenhomomorphismus ist wieder ein Normalteiler.*

(iii) Das Zentrum einer Gruppe, d.h. die Menge aller Gruppenelemente $g \in G$, die mit allen Gruppenelementen vertauschen, ist ein Normalteiler.

(iii) Charakteristische Untergruppen sind immer auch Normalteiler (Übung), die Umkehrung gilt aber nicht.

Satz 1.5.3 (Konstruktion der Restklassengruppe).
Ist $H \subset G$ ein Normalteiler, so ist G/H abgeschlossen unter der induzierten Verknüpfung auf $\mathcal{P}(G)$ und wird mit dieser Verknüpfung eine Gruppe, genannt die Restklassengruppe oder auch der Quotient von G nach H.

Beweis.

Es gilt $(gH)(g_1H) = gg_1HH = gg_1H$, also ist unsere Menge stabil unter der Verknüpfung. Das Assoziativgesetz gilt als Folge der Assoziativität in G, das neutrale Element ist H, und das Inverse zu gH ist $g^{-1}H$. □

Beispiel 1.5.4.
Zu $m \in \mathbb{Z}$ bilden wir die Restklassengruppe $\mathbb{Z}/m\mathbb{Z}$. Sie hat genau m Elemente. Man kürzt die Restklasse von a oft mit $\bar{a}$ ab. Man kann sich $\mathbb{Z}/12\mathbb{Z}$ als eine "Gruppe von Uhrzeiten" vorstellen. In dieser Gruppe gilt zum Beispiel $\bar{7} + \bar{7} = \bar{2}$ und $\bar{9} = -\bar{3}$.

Satz 1.5.5. *(Universelle Eigenschaft der Restklassengruppe*
Sei G eine Gruppe und $H \subset G$ ein Normalteiler.

(i) Die Abbildung can $: G \to G/H$, $g \mapsto gH$ *ist ein Gruppenhomomorphismus mit Kern H. Sie heißt kanonischer Epimorphismus, daher die Bezeichnung* can.

(ii) Ist $\varphi : G \to G'$ ein Gruppenhomomorphismus mit $\varphi(H) = \{1\}$, so gibt es genau einen Gruppenhomomorphismus $\tilde{\varphi} : G/H \to G'$ mit $\varphi = \tilde{\varphi} \circ$ can.

Beweis.

Die erste Aussage ist klar. Für die zweite Aussage beachten wir, dass unter der Annahme $\varphi(H) = \{1\}$ das Bild einer H-Nebenklasse $\varphi(gH) = \varphi(g)\varphi(H) = \{\varphi(g)\}$ nur aus einem einzigen Element besteht. Dies Element nennen wir $\tilde{\varphi}(gH)$, so dass also gilt $\tilde{\varphi}(gH) = \varphi(g)$ und $\varphi(gH) = \{\tilde{\varphi}(gH)\}$. Auf diese Weise erhalten wir das gesuchte $\tilde{\varphi}$. □

Satz 1.5.6 (Isomorphiesatz).
Sei $\varphi : G \to H$ ein Gruppenhomomorphismus. So induziert φ einen Isomorphismus $\tilde{\varphi} : G/\ker\varphi \xrightarrow{\sim} \mathrm{Im}\varphi$.

Beweis.

Natürlich ist unser $\tilde{\varphi}$ surjektiv. Es ist aber auch injektiv nach dem vorhergehenden Satz. □

Korollar 1.5.7 (Noetherscher Isomorphiesatz).
Sei G eine Gruppe und seien $K \subset H \subset G$ zwei Normalteiler von G. So ist H/K ein Normalteiler von G/K. Die Komposition von kanonischen Abbildungen $G \twoheadrightarrow (G/K) \twoheadrightarrow (G/K)/(H/K)$ induziert einen Isomorphismus

$$G/H \xrightarrow{\sim} (G/K)/(H/K)$$

Beweis.

Sicher ist unsere Komposition surjektiv. Unsere Aussage folgt also aus dem Isomorphiesatz 1.5.6, sobald wir zeigen, dass H der Kern unserer Komposition ist. Sicher ist H eine Teilmenge dieses Kerns. Liegt umgekehrt $g \in G$ im Kern unserer Komposition $G \twoheadrightarrow (G/K)/(H/K)$, so folgt $gK \subset HK$, also $gH \subset H$, also $g \in H$. □

Definition 1.5.8.
Eine Gruppe heißt einfach genau dann, wenn sie nicht nur aus dem neutralen Element besteht, aber außer dem neutralen Element und der ganzen Gruppe keine Normalteiler hat.

Beispiele 1.5.9.
Alle endlichen einfachen Gruppen sind seit etwa 1980 bekannt, ihre Klassifikation ist jedoch schwierig. Beispiele einfacher Gruppen sind die zyklischen Gruppen von Primzahlordnung und die alternierenden Gruppen

$$A_r = \ker(\operatorname{sgn} : \mathcal{S}_r \to \{\pm 1\})$$

aller geraden Permutationen von $r \geq 5$ Objekten, wie wir später zeigen werden. Die einfachen Gruppen kommen in 17 sogenannten Serien und 26 Einzelfällen, den sporadischen Gruppen. Die gröste darunter, das Monster mit

$$2^{46}.3^{20}.5^9.7^6.11^2.13^3.17.19.23.29.31.41.47.59.71$$

Elementen hat besonders interessante Eigenschaften. (Fields Medallie 1998 für Richard Borcherds.)

1.6 Zyklische Gruppen und Produkte

Definition 1.6.1.
Sei g ein Element einer Gruppe G. Die Ordnung $\operatorname{ord} g$ von g ist die kleinste echt positive natürliche Zahl $n \geq 1$ mit $g^n = 1_G$. Gibt es kein solches n, so setzen wir $\operatorname{ord} g = \infty$ und sagen, g habe unendliche Ordnung.

Der Schnitt über eine beliebige Familie von Untergruppen einer gegebenen Gruppe ist selbst wieder eine Untergruppe. Für eine Teilmenge T einer Gruppe G definieren wir die von T erzeugte Untergruppe $\langle T \rangle \subset G$ als die kleinste Untergruppe von G, die T enthält. Natürlich gibt es so eine kleinste Untergruppe, nämlich den Schnitt über alle Untergruppen von G, die T enthalten. Für $T \neq \emptyset$ können wir $\langle T \rangle$ konkret beschreiben als die Menge aller endlichen Produkte von Elementen aus T und deren Inversen, für $T = \emptyset$ besteht $\langle T \rangle$ eben nur aus dem neutralen Element.

Eine Gruppe, die von einem einzigen Element erzeugt wird, heißt zyklisch. Zum Beispiel ist eine Gruppe G, deren Kardinalität eine Primzahl ist, notwendig zyklisch, da sie nach Satz 1.4.4 außer $H = G$ und $H = 1$ keine weiteren Untergruppen haben kann. Für jede Gruppe G können wir die von einem Element $g \in G$ erzeugte Untergruppe beschreiben als

$$\langle g \rangle = \{g^n \mid n \in \mathbb{Z}\}$$

Lemma 1.6.2 (Struktur zyklischer Gruppen).
Sei G eine Gruppe und $g \in G$ ein Element. So stimmt die Ordnung von g überein mit der Kardinalität der von g erzeugten Untergruppe, in Formeln $\mathrm{ord} g = |\langle g \rangle|$. *Genauer gilt*

1. *Hat g unendliche Ordnung, so ist die Abbildung $n \mapsto g^n$ ein Isomorphismus $\mathbb{Z} \xrightarrow{\sim} \langle g \rangle$.*
2. *Hat g endliche Ordnung* $\mathrm{ord} g = m$, *so induziert $n \mapsto g^n$ einen Isomorphismus $\mathbb{Z}/m\mathbb{Z} \xrightarrow{\sim} \langle g \rangle$.*

Beweis.
Wir betrachten den Gruppenhomomorphismus $\varphi : \mathbb{Z} \to G$, $n \mapsto g^n$. Nach 1.5.6 haben wir einen Isomorphismus $\mathbb{Z}/\ker\varphi \xrightarrow{\sim} \mathrm{Im}\varphi = \langle g \rangle$. Nach 1.3.5 ist $\ker\varphi$ von der Form $\ker\varphi = m\mathbb{Z}$ für ein $m \in \mathbb{Z}$, $m \geq 0$, und dann gilt notwendig $m = \mathrm{ord} g$ für g von endlicher Ordnung bzw. $m = 0$ für g von unendlicher Ordnung. □

Motiviert durch dieses Lemma nennt man die Kardinalität einer Gruppe auch oft die Ordnung der Gruppe. Wir haben mit unserem Lemma im Übrigen auch bewiesen, dass jede Gruppe mit genau 5 Elementen isomorph ist zu $\mathbb{Z}/5\mathbb{Z}$.

Korollar 1.6.3 (Kleiner Fermatscher Satz).
Sei G eine endliche Gruppe und $g \in G$ ein Element. So teilt die Ordnung von g die Ordnung von G, in Formeln gilt also $g^{|G|} = 1$.

Beweis.
Man wende Satz 1.4.4 von Lagrange an auf die von g erzeugte Untergruppe $H = \langle g \rangle \subseteq G$. □

Korollar 1.6.4.
Jede Untergruppe einer zyklischen Gruppe ist zyklisch. Genauer haben wir für beliebiges $m \in \mathbb{N}$ eine Bijektion

$$\begin{array}{ccc} \{\text{Teiler } d \in \mathbb{N} \text{ von } m\} & \xrightarrow{\sim} & \{\text{Untergruppen von } \mathbb{Z}/m\mathbb{Z}\} \\ d & \mapsto & d\mathbb{Z}/m\mathbb{Z} \end{array}$$

Definition 1.6.5.

(i) Für $n \in \mathbb{N}$ bezeichnen wir mit $\mathbb{Z}_n^\times$ die Restklassen in $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$ der Zahlen $m \in \mathbb{Z}$, die mit n teilerfremd sind. Diese Restklassen sind gerade die Erzeugenden der zyklischen Gruppe $\mathbb{Z}_n$.

(ii) Die Restklassen in $\mathbb{Z}_n^\times$ bilden unter Multiplikation eine Gruppe. Die Ordnung dieser Gruppe wird mit $\varphi(n) := |\mathbb{Z}_n^\times|$ bezeichnet. φ heißt auch die Eulersche φ-Funktion.

Wir haben die Folgenden einfachen Konsequenzen aus dem Satz von Lagrange:

Korollar 1.6.6.

(i) Ist n eine natürliche Zahl und m eine zu n teilerfremde ganze Zahl, dann gilt $m^{\varphi(n)} = 1 \bmod n$ (Satz von Euler).

(ii) Ist $p \in \mathbb{N}$ eine Primzahl und $m \in \mathbb{Z}$, dann gilt $m^p = m \bmod p$.

(iii) Ist G eine Gruppe von Primzahlordnung, dann ist G zyklisch.

(iv) Sind U und V endliche Untergruppen einer Gruppe mit teilerfremden Ordnungen, dann ist $U \cap V = \{e\}$.

Beweis.

(i) folgt aus der Tatsache, dass die multiplikative Gruppe $\mathbb{Z}_n^\times$ Ordnung $\varphi(n)$ hat.

(ii) Für p prim ist $\varphi(p) = p - 1$. Also ist wegen (i) $m^{p-1} = 1 \bmod p$ für m teilerfremd mit p. Daraus folgt $m^p = m \bmod p$, was sogar für alle m gilt.

(iii) Sei $g \neq e$ ein Element in G. Die Ordnung der von g zyklisch erzeugten Untergruppe $\langle g \rangle$ von G muss $|G|$ teilen, ist also 1 oder p. Da die Gruppe $\langle g \rangle$ nicht trivial ist, erzeugt g schon die ganze Gruppe G.

(iv) Die Ordnung der Untergruppe $U \cap V$ muss sowohl die Ordnung von U als auch die Ordnung von V teilen. Aus der Teilerfremdheit folgt, dass $|U \cap V| = 1$.

□

Bemerkung 1.6.7.
Als Konsequenz aus dem Satz von Euler halten wir fest: sei $n \in \mathbb{N}$ und $r \in (\mathbb{Z}_n)^\times$. Dann ist $r^s \bmod n$ leicht zu berechnen, wenn man $s \bmod \varphi(n) =: s'$ kennt:

$$r^s = r^{q\varphi(n)+s'} = r^{s'}(r^{\varphi(n)})^{r'} = r^{s'} \bmod n\,.$$

Diese Beobachtung liegt dem sogenannten RSA-Verschlüsselungssystem (nach Ronald Rivest, *Adi* Shamir *und Leonard* Adlerman*) zugrunde. Dies ist ein System mit öffentlichem Schlüssel. Der Empfänger der Nachricht erzeugt dabei zwei große Primzahlen p und q, berechnet ihr Produkt $n := pq$ und erzeugt dann eine Zahl E koprim zu $\varphi(n) = (p-1)(q-1)$. Das ist leicht, und nur dann leicht, wenn man p und q kennt. Als Schlüssel macht er nur öffentlich das Produkt $n = pq$ und E. (n, E) ist der öffentliche Chiffrierschlüssel.*

Der Sender der Nachricht zerlegt diese in Zahlen P_i, die kleiner als n sind. Für jede dieser Zahlen berechnet er

$$C_i = P_i^E \bmod n$$

und schickt diese Zahl. Zum Entschlüsseln berechnet der Empfänger eine Zahl D mit $ED = 1 \bmod \varphi(n)$, was leicht ist, wenn p und q getrennt bekannt sind, aber rechnerisch schwer, wenn nur n bekannt ist. Darauf beruht die Sicherheit der Verschlüsselung. Der Dechiffrierschlüssel ist (D, n), und der Empfänger berechnet $C_i^E \bmod n$. Wegen

$$C_i^D = (P_i)^{ED} = P_i \bmod n$$

gibt dies die Nachricht im Klartext. Durch Vertauschen der Rollen von Chiffrier- und Dechiffrierschlüssel kann man sogar elektronische Unterschriften erzeugen.

Wir wollen jetzt zwei Produktbegriffe von Gruppen einführen.

Definition 1.6.8.
(i) Seien $G_1, \ldots G_n$ Gruppen. Die Produktmenge

$$G_1 \times G_2 \times \ldots G_n = \{(g_1, g_2, \ldots, g_n) | g_i \in G_i\}$$

mit komponentenweiser Multiplikation, neutralem Element $(e, e, \ldots, e)$ und komponentenweisem Inversen bildet eine Gruppe. Sie heißt das (äußere) direkte Produkt.

(ii) Sei G eine Gruppe und N_i eine Familie von Normalteilern von G. Dann heißt G das (innere) direkte Produkt von $N_1, \ldots N_m$, falls gilt:

$$\begin{aligned} &G = N_1 N_2 \ldots N_m \\ &N_i \cap (N_1 N_2 \ldots N_{i-1} N_{i+1} \ldots N_m) = \{e\}\ . \end{aligned}$$

Die folgenden Aussagen sind einfach zu beweisen.

Bemerkungen 1.6.9.

(i) Das Zentrum eines äußeren direkten Produkts ist gleich dem direkten Produkt der Zentren:

$$Z(\prod_{i=1}^{n} G_i) = \prod_{i=1}^{n} Z(G_i)\,.$$

(ii) Das äußere direkte Produkt ist eine abelsche Gruppe genau dann, wenn alle Gruppen G_i abelsch sind.

(iii) Ist G ein inneres direktes Produkt der Normalteiler $N_1, \dots N_n$, so gilt für $g_i \in N_i$ und $g_j \in N_j$ mit $i \neq j$, dass $g_i g_j = g_j g_i$. Denn wegen der Normalteilereigenschaft ist $g_i g_j g_i^{-1} \in N_j$ und $g_j g_i g_j^{-1} \in N_i$, also $g_i g_j g_i^{-1} g_j^{-1} \in N_i \cap N_j = \{e\}$.

(iv) Ist G ein inneres direktes Produkt der Normalteiler $N_1, \dots N_n$, so lässt jedes Element g von G sich bis auf die Reihenfolge der Faktoren eindeutig als Produkt $g = g_1 g_2 \dots g_n$ darstellen.
Die Existenz einer Darstellung als Produkt ist Teil der Definition. Es reicht aus, die Eindeutigkeit der Darstellung des neutralen Elements zu zeigen. Denn seien $g = g_1 \dots g_n$ und $g = h_1 \dots h_n$ zwei verschiedene Darstellungen eines Elements $g \in G$, so ist $(g_1 h_1^{-1}) \dots (g_n h_n^{-1})$ eine nicht-triviale Darstellung des neutralen Elements. Sei also $e = g_1 \dots g_n$, so $g_1^{-1} = g_2 \dots g_n$; aber die linke Seite ist in N_1, die rechte in $N_2 \cdot \dots N_n$, und der Schnitt dieser Gruppen ist per definitionem trivial, also $g_1 = e$. Man schließt induktiv weiter, dass alle $g_i = e$.

(v) Es gilt auch die Umkehrung: seien G_i Untergruppen von G, so dass für $i \neq j$ die Elemente von G_i und G_j vertauschen und sich jedes Element von G eindeutig *als Produkt von Elementen von G_i schreiben lässt. Dann sind die G_i Normalteiler und G ist das innere direkte Produkt der G_i.*

Denn aus der Vertauschbarkeit folgt sofort, dass alle G_i Normalteiler sind. Die Darstellbarkeit als Produkt war gefordert, und die Eindeutigkeit impliziert die zweite definierende Eigenschaft des inneren direkten Produkts.

Die entscheidende Beziehung zwischen äußerem und inneren direktem Produkt stellt der folgende Satz her:

Satz 1.6.10.
Ist $G = N_1 N_2 \dots N_k$ ein inneres direktes Produkt der Normalteiler N_i von G und ist N_i isomorph zur Gruppe G_i, $1 \leq i \leq k$, so ist G isomorph zum äusseren direkten Produkt $\prod_{i=1}^{k} G_i$.

Beweis.
Wegen der Eindeutigkeit der Zerlegung $G \ni g = g_1 g_2 \dots g_n$ definiert

$$\begin{array}{rccc} \varphi: & G & \to & \prod_{i=1}^{k} N_i \\ & g & \mapsto & (g_1, g_2, \dots, g_k) \end{array}$$

eine Bijektion, die wegen der Vertauschbarkeit von g_i und g_j für $i \neq j$ auch ein Homomorphismus von Gruppen ist. □

Satz 1.6.11. *(Verträglichkeit von direkten Produkten und Faktorgruppen)*

Das direkte Produkt ist in einfacher Weise verträglich mit dem Übergang zu Faktorgruppen. Für jedes $i \in \{1, \dots, k\}$ sei N_i ein Normalteiler von G_i. Dann ist

$$N := \prod_{i=1}^{k} N_i.$$

Normalteiler von $G := \prod_{i=1}^{k} G$ und es gilt

$$G/N \cong \prod_{i=1}^{k} G_i/N_i \tag{1}$$

Beweis.
Seien

$$\begin{array}{rccc} \pi_i: & G_i & \to & G_i/N_i \\ & g & \mapsto & gN_i \end{array}$$

die kanonischen Epimorphismen. Dann ist

$$\begin{array}{rccc} \pi: & \prod_{i=1}^{k} G_i & \to & \prod_{i=1}^{k} G_i/N_i \\ & (a_1, \dots, a_k) & \mapsto & (\pi(a_1), \dots, \pi_k(a_k)) \end{array}$$

ein Homomorphismus mit Kern $\prod_{i=1}^{k} N_i = N$. Als Kern des Homomorphismus π ist N normal in G. Der Isomorphiesatz 1.5.6 zeigt (1). □

Korollar 1.6.12.
Sei $G = G_1 \times G_2$, dann ist

$$G_1 \cong G/\{e\} \times G_2$$

Das direkte Produkt abelscher Gruppen ist wieder abelsch. Insofern ist die Eigenschaft "abelsch" mit dem direkten Produkt verträglich. Für die Eigenschaft "zyklisch" gilt das nicht: selbst wenn alle Gruppen G_i zyklisch sind, so muss ihr direktes Produkt nicht unbedingt zyklisch sein. Ein Gegenbeispiel hierzu ist die Kleinsche Vierergruppe $\mathbb{Z}_2 \times \mathbb{Z}_2$. Man hat aber immer noch:

Satz 1.6.13.

(i) Das direkte Produkt zweier zyklischer Gruppen teilerfremder Ordnung ist zyklisch.

(ii) Ist G zyklische Gruppe der Ordnung mn, wobei $ggT(m,n) = 1$, so gibt es zyklische Gruppen G_1 und G_2 der Ordnung m bzw. n mit

$$G \cong G_1 \times G_2.$$

Da jede zyklische Gruppe der Ordnung n isomorph ist zu $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$, zeigen wir den äquivalenten

Satz 1.6.14.

Für teilerfremde natürliche Zahlen $m, n \in \mathbb{N}$ gilt $\mathbb{Z}_{mn} = \mathbb{Z}_m \times \mathbb{Z}_n$.

Beweis.

- $\langle \overline{m} \rangle$ und $\langle \overline{n} \rangle$ sind zyklische Untergruppen der Ordnungen n bzw. m von $\mathbb{Z}_{mn}$ und als Untergruppen einer abelschen Gruppe offenbar normal.
- $\langle \overline{m} \rangle \cap \langle \overline{n} \rangle = \{\overline{0}\}$. Nach Lagrange ist der Schnitt eine Gruppe von einer Ordnung, die sowohl n als auch m teilt, also gleich eins. Der Schnitt ist also die triviale Gruppe.
- Nach dem Satz von Bézout 1.3.7 gibt es $h, k \in \mathbb{Z}$, so dass

  $$1 = hm + kn.$$

  Deshalb hat man für alle $l \in \mathbb{Z}$

  $$l = (lh)m + (lk)n$$

  Betrachtet man diese Gleichung modulo $n \cdot m$,

  $$\bar{l} = (lh)\overline{m} + (lk)\overline{n} \ ,$$

  so sieht man, dass die beiden Gruppen auch $\mathbb{Z}_{mn}$ erzeugen. Also

  $$\mathbb{Z}_{mn} = \langle \overline{m} \rangle \oplus \langle \overline{n} \rangle \cong \mathbb{Z}_n \oplus \mathbb{Z}_m$$

  Hier haben wir abelsche Gruppen additiv geschrieben, daher schreiben wir auch eine direkte Summe statt eines direkten Produkts.

□

Korollar 1.6.15. *(Chinesischer Restsatz)*

Sind m und n teilerfremde natürliche Zahlen und $a, b \in \mathbb{Z}$, so gibt es ein $x \in \mathbb{Z}$ mit

$$x = a \bmod m \quad \text{und} \quad x = b \bmod n.$$

Beweis.

Die Abbildung

$$\begin{array}{rcl} \varphi : \mathbb{Z} & \to & \mathbb{Z}_m \times \mathbb{Z}_n \\ z & \mapsto & (z \bmod m, z \bmod n) \end{array}$$

ist ein Gruppenhomomorphismus mit Kern $mn\mathbb{Z}$. Aus dem Isomorphiesatz folgt

$$\mathbb{Z}_{mn} \cong \text{ Im } \varphi \subseteq \mathbb{Z}_m \times \mathbb{Z}_n$$

Mit dem vorhergehende Satz sieht man, dass φ auch surjektiv ist, woraus der chinesische Restsatz folgt. □

Korollar 1.6.16.
Für die Eulersche φ-Funktion gilt

$$\varphi(mn) = \varphi(m)\varphi(n) \tag{2}$$

für alle teilerfremden natürlichen Zahlen m, n.

Beweis.

Die Eulersche φ-Funktion ist in Definition 1.6.5 eingeführt als die Zahl der erzeugenden Elemente der zyklischen Gruppe $\mathbb{Z}_n$. Nun ist (a, b) erzeugendes Element von $\mathbb{Z}_m \times \mathbb{Z}_n$ genau dann, wenn a ein erzeugendes Element von $\mathbb{Z}_m$ und b ein erzeugendes Element von $\mathbb{Z}_n$ ist. Daraus folgt aber für m und n teilerfremd die Produktformel (2). □

Wir werden später sehen, dass für eine Primzahlpotenz p^n gilt $\varphi(p^n) = (p-1)p^{n-1}$. Dies macht die Eulersche φ-Funktion explizit berechenbar.

1.7 Operationen von Gruppen auf Mengen

Wir beginnen mit dem folgenden Satz:

Satz 1.7.1 (Cayley).
Jede Gruppe G ist isomorph zu einer Gruppe von Permutationen von G.

Beweis.

Für $g \in G$ definieren wir eine Permutation $L(g) \in S(G)$ durch

$$L(g) : x \mapsto gx$$

Die Assoziativität der Gruppe impliziert, dass

$$(ab)x = a(bx) \iff L(ab) = L(a)L(b)\,.$$

Offensichtlich hat man $L(e) = \mathrm{id}$, und das Inverse ist $L(a)^{-1} = L(a^{-1})$. L ist also ein Gruppenhomomorphismus von G in die Permutationsgruppe $S(G)$. Er ist injektiv, denn $a \in \ker L$ heißt, dass $e = L(a)e = a$. Wegen des Isomorphiesatzes können wir G mit dem Bild unter L in $S(G)$ identifizieren. □

Als Verallgemeinerung dieser Untersuchung ergibt sich die folgende Fragestellung: sei X eine nicht-leere Menge, G eine Gruppe. Untersuche Gruppenhomomorphismen

$$\varphi : G \to S(X)$$

Definition 1.7.2.

(i) Sei G Gruppe , $X \neq \emptyset$. Wir sagen, G operiert auf X von links, wenn es eine Abbildung

$$\begin{array}{rcl} G \times X & \to & X \\ (g, x) & \mapsto & g \cdot x \end{array}$$

gibt mit

$$\begin{array}{lllll} (O1) & (gh)x & = & g(hx) & \forall g, h \in G \\ (O2) & ex & = & x & \forall x \in X \end{array}$$

(ii) Eine Menge mit einer Operation von G heißt auch G–Menge, und wir sagen, G wirkt auf X.

Bemerkung 1.7.3.
Es operiert G auf einer Menge X also genau dann, wenn es einen Gruppenhomomorphismus von G in die Permutationsgruppe $S(X)$ gibt.

Satz 1.7.4.
Es operiere G auf X. Dann ist

$$R(G) = \{(x, y) \in X \times X \mid \exists g \in G \text{ so dass } gx = y\}$$

eine Äquivalenzrelation auf X.

Beweis: Übung.

Bemerkung 1.7.5.

a) Die Äquivalenzklassen dieser Äquivalenzrelation heißen Bahnen oder Orbits. Wir bezeichnen die Bahn von x mit $[x]$:

$$[x] := \{y \in X \mid \exists g \in G \quad mit \quad gx = y\}\,.$$

Die Bahnen bilden eine Partition (d.h. eine Zerlegung) von X:

$$X = \bigcup_{x \in X} G \cdot x\,.$$

Die Menge $G\backslash X$ der Bahnen heißt auch Bahnenraum.

b) Beispiel: auf jeder nicht-leeren Menge kann man die triviale Operation für jede Gruppe definieren:

$$(g, x) \mapsto x\,.$$

c) Beispiel: jede Gruppe operiert auf sich selbst durch ihre Verknüpfung

$$\begin{array}{rcl} G \times G & \to & G \\ (x, y) & \mapsto & x \cdot y \end{array}$$

In Verallgemeinerung des Falles der additiven Gruppe eines Vektorraums sagt man auch, G operiert auf sich selbst durch Translation. Wir werden später noch eine andere Operation einer Gruppe auf sich selbst kennen lernen.

d) Beispiel: Sei V ein Vektorraum und bezeichne $GL(V)$ die Gruppe der linearen invertiblen Selbstabbildungen von V. "GL" steht für "general linear" und $GL(V)$ heißt auch die allgemeine lineare Gruppe von V. Die Anwendung eines Elements aus $GL(V)$ auf einen Vektor in V definiert eine Operation:

$$GL(V) \times V \to V$$

e) Sei H Untergruppe von G. Dann ist die Menge $X = G/H$ der Linksnebenklassen eine G–Menge.

f) Die komplexen Zahlen vom Betrag Eins wirken auf den komplexen Zahlen durch Multiplikation:

$$X = \mathbb{C} \quad G = \{z \in \mathbb{C} : |z| = 1\}.$$

Der Bahnenraum ist in diesem Fall die nicht-negative Halbachse $\mathbb{R}_{\geq 0}$.

Definition 1.7.6.
Sei X eine G–Menge.

(i) Die Standuntergruppe (oder Isotropiegruppe oder Stabilisator) von $x \in X$ ist die Menge

$$G_x = \{g \in G | gx = x\}.$$

Sie ist eine Untergruppe von G.

(ii) Für $A \subseteq X$ und $H \subseteq G$ schreiben wir HA für die Menge

$$HA = \{ha \,|\, h \in H, a \in A\}$$

Ist H Untergruppe, so ist HA eine H–Menge.

Lemma 1.7.7. *(Bahnen als Quotienten)*
Sei G Gruppe, X eine G–Menge und $x \in X$. Dann definiert die Operation von G auf X eine Bijektion zwischen den Nebenklassen des Stabilisators eines Elements $x \in X$ und dem Orbit von x:

$$G/G_x \cong Gx.$$

Beweis. Wir definieren eine Abbildung von Mengen

$$\begin{array}{rcl} G/G_x & \xrightarrow{\sim} & Gx \\ gG_x & \mapsto & g \cdot x \end{array}$$

Da die Abbildung auf Nebenklassen definiert ist, müssen wir zunächst zeigen, dass sie wohldefiniert ist. Sei also $h \in G_x$. Dann sind g und gh in derselben Nebenklasse. Das Axiom $(O1)$ für eine Operation liefert

$$(gh)x = g(h \cdot x) = gx\,,$$

also ist die Abbildung wohldefiniert. Sie ist auch surjektiv nach Definition des Orbits Gx. Injektivität folgt aus

$$\begin{array}{rl} & g_1 x = g_2 x \\ \iff & g_2^{-1} g_1 x = x \\ \iff & g_2^{-1} g_1 \in G_x \\ \iff & g_1 \text{ und } g_2 \text{ sind in der gleichen Nebenklasse.} \end{array}$$

□

Folgerungen 1.7.8.

(i) *Bahnformel*
Sei G endliche Gruppe. Dann hat man für die Kardinalitäten

$$|G| = |G_x| \; |Gx|$$

Insbesondere teilt die Kardinalität jeder Bahn $|Gx|$ die Kardinalität der Gruppe $|G|$.

(ii) *Ein Vertretersystem einer G–Menge X ist eine Untermenge $V \subset X$ mit den folgenden zwei Eigenschaften:*

a) $\forall x \in X \quad \exists v \in V,$ *so dass* $Gx = Gv$

b) $a, b \in V \; a \neq b \Rightarrow \qquad Ga \cap Gb = \emptyset$

Für eine gegebene Gruppenwirkung ist die Wahl eines Vertretersystems im Allgemeinen in hohem Maße nicht eindeutig, aber Elemente auf Orbits der Länge eins sind in jedem Vertretersystem enthalten. Solche Elemente x heißen Fixpunkte (der Wirkung) von G. Wir bezeichnen die Menge der Fixpunkte der Wirkung einer Gruppe G auf einer Menge X mit $Fix_G(X)$.

(iii) *Sei X eine endliche G–Menge und V ein Vertretersystem. Dann gilt*

$$|X| = \sum_{x \in V} [G : G_x] = |Fix_G(x)| + \sum_{\substack{x \in V \\ [G:G_x] > 1}} [G : G_x] \,. \tag{3}$$

(iv) *Wir leiten daraus den Fixpunktsatz ab: Sei G eine Gruppe der Ordnung p^r, p prim. Operiert G auf einer endlichen Menge X, so gilt*

$$|X| = |Fix_G(x)| \bmod p \,.$$

Insbesondere gibt es wenigstens einen Fixpunkt, wenn $|X|$ und p teilerfremd sind.

Beweis.

Aus (3) folgt

$$|X| - |Fix_G(x)| = \sum_{[G:G_x]>1} [G : G_r], \,.$$

Die rechte Seite besteht aus einer Summe von Zahlen der Form p^l mit $l \geq 1$. Also ist auch die linke Seite durch p teilbar:

$$|X| - |Fix_G(x)| = 0 \bmod \; p \,.$$

Ist $|X| \neq 0 \bmod p$, so muss auch $|Fix_G(X)| \bmod p$ ungleich null sein. Damit kann $|Fix_G(x)|$ aber nicht verschwinden. □

1.8 Konjugationsklassen

Definition 1.8.1.

(i) Ist G eine Gruppe und $x \in G$ ein Element, so ist

$$\begin{array}{rccc} int_x & : & G & \to & G \\ & & g & \mapsto & xgx^{-1} \end{array}$$

ein Gruppenautomorphismus, genannt die Konjugation mit x.

(ii) Die Automorphismen von G, die sich als Konjugation schreiben lassen, heißen innere Automorphismen, auf englisch interior automorphisms, daher die Notation int.

(iii) Wegen

$$int_x \circ int_y = int_{x \cdot y}$$

ist

$$\begin{array}{rccc} int & : & G & \to & Aut\ G \\ & & g & \mapsto & int_g \end{array}$$

ein Gruppenhomomorphismus. Was ist sein Kern?

(iv) G operiert auf sich selbst durch Konjugation.

$$\begin{array}{ccc} G \times G & \to & G \\ (x, y) & \mapsto & int_x(y) = xyx^{-1} \end{array}$$

Die Bahnen dieser Wirkung heißen Konjugationsklassen.

Bemerkungen 1.8.2.

(i) Die Theorie der Jordanschen Normalformen in der linearen Algebra kann man interpretieren als die Theorie der Konjugationsklassen der allgemeinen linearen Gruppe $GL(n, \mathbb{C})$.

(ii) Die Konjugationsklassen einer abelschen Gruppe bestehen aus je nur einem Element.

(iii) Die Standuntergruppe von $x \in G$ unter Konjugation heißt Zentralisator $Z_G(x)$ von x:

$$Z_G(x) = \{g \in G | gxg^{-1} = x\}$$

(iv) Als Spezialfall der Bahnengleichung leiten wir die Klassengleichung ab. Sei G endliche Gruppe und

$$G = C_1 \cup \cdots \cup C_r$$

eine disjunkte Zerlegung von G in Konjugationsklassen mit Vertretersystem $x_i \in C_i$. Dann ergibt die Bahnenformel

$$\begin{aligned} |G| &= |C_1| + \cdots + |C_r| \\ &= |G|/|Z_G(x_1)| + \cdots + |G|/|Z_G(x_r)| \\ &= |Z(G)| + \sum_{\substack{x_i \\ s.d.\,|G|/|Z_G(x_i)|>1}} |G|/|Z_G(x_i)| \end{aligned}$$

denn die Menge der Fixpunkte der Wirkung durch Konjugation ist

$$Fix_G(G) = \{x \in G | gxg^{-1} = x \ \forall g \in G\} = Z(G)$$

gleich dem Zentrum der Gruppe G.

Korollar 1.8.3.
Sei G eine Gruppe der Ordnung p^r und p prim. Dann hat G nicht–triviales Zentrum.

Beweis.

Als Untergruppe ist $|Z(G)|$ Teiler von $|G|$, also eine Potenz von p. Wir müssen ausschließen, dass $|G| = p^0 = 1$.

Andererseits folgt aus der Bahnengleichung

$$|Z(G)| = |G| - \sum_i |G|/|Z_G(x_r)|\,;$$

daher ist $|Z(G)|$ durch p teilbar, also ist $|Z(G)| = p^0 = 1$ ausgeschlossen. □

1.9 Endlich erzeugte abelsche Gruppen

Eine *Primzahlpotenz* ist eine natürliche Zahl der Form p^r mit p prim und $r \in \mathbb{N}$. Eine Gruppe, deren Ordnung eine Primzahlpotenz p^r ist, heißt auch p-Gruppe.

Ziel des Abschnitts sind die folgenden zwei Klassifikationenssätze für endlich–erzeugte *abelsche* Gruppen.

Satz 1.9.1.
Sei G eine endlich erzeugte abelsche Gruppe. So gibt es genau eine Folge von natürlichen Zahlen $d_1, d_2, \ldots, d_s \in \{0, 2, 3, 4, \ldots\}$ mit $d_i | d_{i+1}$ für $i = 1, \ldots, s-1$, derart, dass gilt

$$G \cong \mathbb{Z}_{d_1} \times \mathbb{Z}_{d_2} \times \cdots \times \mathbb{Z}_{d_s} \tag{4}$$

Hierbei beachte man, dass $\mathbb{Z}_0 = \mathbb{Z}/0\mathbb{Z} \cong \mathbb{Z}$ zugelassen ist.

Satz 1.9.2.
Sei G endlich erzeugte abelsche Gruppe.

(i) Es gibt Primzahlpotenzen $q_1, \ldots, q_t$ und eine natürliche Zahl $r \in \mathbb{N}$ mit

$$G \cong \mathbb{Z}_{q_1} \times \cdots \times \mathbb{Z}_{q_t} \times \mathbb{Z}^r \tag{5}$$

(ii) Die natürliche Zahl r wird durch G eindeutig festgelegt. Sie heißt auch der Rang von G. Die Primzahlpotenzen sind eindeutig bis auf die Reihenfolge.

Bemerkung 1.9.3.
Die Faktoren in den Zerlegungen (1.9.1) und (1.9.2) sind keinesfalls eindeutig als Untergruppen von G. Mit anderen Worten: die Isomorphien in (1.9.1) und (1.9.2) sind nicht kanonisch, d.h. in eindeutiger Weise ausgezeichnet.

Definition 1.9.4.
(i) Ein Element endlicher Ordnung in einer Gruppe heißt Torsionselement.

(ii) Eine Gruppe, in der alle vom neutralen Element verschiedenen Elemente unendliche Ordnung haben, heißt torsionsfrei .

Beispiele torsionsfreier Gruppen sind die abelschen Gruppen $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$.

(iii) Eine Gruppe heißt Torsionsgruppe, wenn alle ihre Elemente Torsionselemente sind.

Lemma 1.9.5.
Jede endlich erzeugte torsionsfreie abelsche Gruppe G ist isomorph zur sogenannten freien abelschen Gruppe $\mathbb{Z}^r = \mathbb{Z} \times \mathbb{Z} \times \ldots \times \mathbb{Z}$ für geeignetes $r \in \mathbb{N}$.

Beweis.
Wir führen den Beweis in additiver Notation. Offenbar reicht es, für G ein endliches Erzeugendensystem $x_1, \ldots x_r$ zu finden, das "linear unabhängig" ist in dem Sinne, dass es keine nicht–triviale Relation der Form

$$0 = a_1 x_1 + \cdots + a_r x_r \tag{6}$$

mit $a_i \in \mathbb{Z}$ gibt.

Dies zeigen wir durch einen Widerspruchsbeweis und nehmen an, alle Erzeugendensysteme wären linear abhängig. Wir wählen dann ein Erzeugendensystem minimaler Kardinalität r, in dem es dann mindestens

eine nicht–trivialer Relation gibt. Wir wählen in diesem Erzeugendensystem die Relation (6), in der

$$\sum_i |a_i| > 0$$

minimal ist.

In dieser minimalen Relation ist entweder nur ein Koeffizient ungleich 0. Dann hat man eine Relation $a_1 x_1 = 0$, was wegen der Torsionsfreiheit der Gruppe impliziert, dass $x_1 = 0$. Dann können wir aber x_1 als Erzeuger weglassen, im Widerspruch zur Annahme, dass das Erzeugendensystem von minimaler Kardinalität ist.

Also seien mindestens zwei Koeffizienten ungleich Null, wobei wir o.B.d.A. annehmen können, dass

$$0 < a_1 \leq a_2 \,.$$

Dann erhalten wir aber ein neues Erzeugendensystem, indem wir setzen

$$x_1' = x_1 + x_2 \quad x_i' = x_i \quad i = 2, \ldots r \,,$$

und in diesem Erzeugendensystem hat man die Relation

$$0 = a_1 x_1' + (a_2 - a_1) x_2' + \sum_{i=3}^{r} a_i x_i'$$

mit kleinerer Summe der Absolutbeträge der Koeffizienten, im Widerspruch zur zweiten Minimalitätsannahme. □

Lemma 1.9.6.
Sei G eine abelsche Gruppe.

(i) Die Menge $T = G_{\mathrm{tor}}$ aller Elemente endlicher Ordnung aus G ist eine Untergruppe von G. Sie heißt Torsionsbestandteil von G.

(ii) Der Quotient G/T ist torsionsfrei.

(iii) Ist G überdies endlich erzeugt, so ist der Torsionsbestandteil endlich,

$$|T| < \infty \,,$$

und wir haben

$$G/T \cong \mathbb{Z}^r$$

für geeignetes $r \in \mathbb{N}$. Ferner spaltet die Surjektion

$$\pi : G \twoheadrightarrow G/T, \quad \textit{d.h.}$$

es gibt einen Gruppenhomomorphismus $\varphi : G/T \to G$, so dass $\pi \circ \varphi = id_{G/T}$.

Beweis.

(i),(ii) Als Übung dem Leser überlassen.

(iii) In einer Übungsaufgabe werden wir sehen, dass Untergruppen einer endlich-erzeugten abelschen Gruppe selbst endlich erzeugt sind. T ist also endlich erzeugt. Da T abelsch ist und alle Elemente endliche Ordnung haben, ist T endlich.

Der Isomorphismus von G/T auf $\mathbb{Z}^r$ für geeignetes $r \in \mathbb{N}$ folgt aus Lemma 1.9.5. Die Surjektion $\pi : G \to G/T$ spaltet auf Grund des folgenden allgemeineren Lemmas. □

Lemma 1.9.7.
Jede Surjektion einer abelschen Gruppe G auf $\mathbb{Z}^r$

$$\pi : G \twoheadrightarrow \mathbb{Z}^r$$

spaltet.

Beweis.

Sei $\{a_i\}$ mit $i = 1 \dots r$ eine Basis von $\mathbb{Z}^r$, etwa die $a_i = (0, 0, \dots, 1, 0, \dots 0)$ mit 1 nur an der i-ten Stelle. Wähle Repräsentanten $x_i \in \pi^{-1}(a_i)$ und setze:

$$\begin{aligned} \varphi : \mathbb{Z}^r &\to G \\ a_i &\mapsto x_i \end{aligned}$$

Da G abelsch ist, ist φ Gruppenhomomorphismus und

$$\pi \circ \varphi(a_i) = \pi(x_i) = a_i.$$

Da $\{a_i\}_{i=1,\dots r}$ Basis ist, folgt $\pi \circ \varphi = \mathrm{id}_{\mathbb{Z}^r}$. Man beachte, dass der Gruppenhomomorphismus φ *nicht* kanonisch ist: die Wahl der Repräsentanten x_i der Urbilder ist willkürlich. □

Um weiter zu kommen, brauchen wir den folgenden allgemeinen

Satz 1.9.8.
Seien A, B, C (nicht notwendigerweise abelsche) Gruppen und ι, π Gruppenhomomorphismen

$$0 \to B \xrightarrow{\iota} A \xrightarrow{\pi} C \to 0\,, \tag{7}$$

so dass ι injektiv , π surjektiv ist und $\ker \pi = \text{Im } \iota$ gilt. Man nennt dann auch (7) eine kurze exakte Sequenz von Gruppen.

Es gilt dann: spaltet π, d.h. gibt es einen Gruppenhomomorphismus

$$\varphi : C \to A$$

so dass

$$\pi \circ \varphi = id_C\,,$$

so ist A ein direktes Produkt, $A = \text{Im } (\iota) \times \text{Im } \varphi$.

Beweis.

1) Wir müssen zunächst zeigen, dass die Untergruppen Im (i) und Im φ normal sind. $\text{Im}(\iota) = \ker \pi$ ist sicher normal als Kern von π. Um auch Im φ als Kern auffassen zu können, führen wir den Gruppenendomorphismus $p := \varphi \circ \pi : A \to A$ ein. Dies ist ein Idempotent oder Projektor:

$$p^2 = \varphi \circ \pi \circ \varphi \circ \pi = \varphi \circ \pi = p.$$

Ferner ist

$$\text{Im } p = \text{Im}\varphi.$$

Denn

$$\begin{aligned} x \in \text{ Im } p \quad &\Longleftrightarrow \quad x = py = \varphi \circ \pi(y) \Rightarrow x \in \text{ Im } \varphi. \\ x \in \text{ Im } \varphi \quad &\Longleftrightarrow \quad x = \varphi(y) \\ &\Rightarrow \quad px = \varphi \cdot \pi \circ \varphi(y) = \varphi(y) = x \end{aligned}$$

Aber Im φ = Im p = $\ker(\text{id} - p)$, also ist Im φ als Kern eines Gruppenhomomorphismus normal.

2) Wir zeigen als nächstes, dass

$$A = \text{Im } \varphi \cdot \text{Im}(\iota)\,.$$

Jedes $a \in A$ schreibt sich trivialerweise als

$$a = ap(a^{-1})p(a)$$

$p(a)$ ist offenbar in Im (φ). Wir müssen nur noch zeigen, dass $ap(a^{-1})$ in Im $(i) = \ker \pi$ ist. Dazu rechnen wir

$$\pi(ap(a^{-1})) = \pi(a)\pi\varphi\pi(a^{-1}) = \pi(a)\pi(a^{-1}) = e\,.$$

3) Schließlich müssen wir noch zeigen, dass Im $\varphi \cap$ Im $i = \{e\}$. Da $x \in$ Im $\iota = \ker \pi$ wissen wir, dass $\pi(x) = e$. Andererseits folgt aus $x \in$ Imφ, dass es ein y gibt so dass $x = \varphi(y)$. Die Kombination dieser beiden Gleichungen liefert

$$e = \pi(x) = \pi \circ \varphi(y) = y\,,$$

damit aber auch $x = \varphi(y) = \varphi(e) = e$.

□

Die Kombination der beiden vorhergehenden Sätze zeigt:

Korollar 1.9.9.
Sei G eine abelsche Gruppe. Dann ist G isomorph zum Produkt

$$G \cong T \times \mathbb{Z}^r\,.$$

Beachte: es gibt keine kanonische Wahl des freien Anteils $\mathbb{Z}^r$! Der Torsionsanteil T ist dagegen als Untergruppe eindeutig bestimmt.

Lemma 1.9.10.
(i) Sei T eine abelsche Gruppe und p eine Primzahl. Alle Elemente von T, deren Ordnung eine Potenz von p ist, bilden eine Untergruppe $T(p)$ von T.

(ii) Ist T eine endliche abelsche Gruppe und sind $p_1, \ldots, p_u$ die Primfaktoren der Gruppenordnung $|T|$, so hat man

$$T \cong T(p_1) \times \cdots \times T(p_u).$$

Beweis.
(i) In einer abelschen Gruppe teilt die Ordnung des Produkts zweier Elemente das Produkt ihrer Ordnungen.

$$(ab)^{\mathrm{ord}(a)\cdot\mathrm{ord}(b)} = a^{\mathrm{ord}(a)\mathrm{ord}(b)} b^{\mathrm{ord}(b)\mathrm{ord}(a)} = e.$$

(ii) Die Untergruppen $T(p_1)$ sind als Untergruppen einer abelschen Gruppe trivialerweise normal. Sei nun $x \in T(p_1) \cap T(p_2)$. Dann ist die Ordnung von x eine Potenz sowohl von p_1 als auch von p_2, also gleich eins. Folglich $x = e$. Die Surjektivität schließlich folgt aus dem chinesischen Restsatz, angewandt auf die zyklische Untergruppe $\langle x \rangle$ von T für jedes $x \in T$.

□

Die Hauptarbeit für den Beweis von 1.9.1 und 1.9.2 geht nun in das folgende vielleicht etwas technisch anmutende

Lemma 1.9.11.
Sei p prim und A eine abelsche p–Gruppe. Sei a ein Element maximaler Ordnung, $\langle a\rangle$ die von a erzeugte zyklische Untergruppe und $B \subset A$ maximal unter den Untergruppen von A, die $\langle a\rangle$ nur im neutralen Element treffen. Dann ist A inneres direktes Produkt,

$$A = B \cdot \langle a\rangle\,.$$

Beweis.

Als Untergruppen der abelschen Gruppe A sind B und $\langle a\rangle$ normal; $B \cap \langle a\rangle = \{e\}$ gilt nach Voraussetzung. Wir müssen also nur zeigen, dass A gleich dem Produkt von B und $\langle a\rangle$ ist. Dazu führen wir die Faktorgruppe

$$\overline{A} = A/B$$

mit der natürlichen Projektion

$$\pi : A \to \overline{A}$$

ein und zeigen, durch Widerspruchsbeweis, dass $\overline{A}$ vom Bild $\overline{a} = \pi(a)$ von a erzeugt wird. Dazu nehmen wir an, es gäbe $\overline{c} \in \overline{A}\backslash\langle\overline{a}\rangle$.

Wir nennen $\bar{Z}$ die von $\bar{a}$ zyklisch erzeugte Gruppe,

$$\bar{Z} := \langle\overline{a}\rangle\,.$$

Nun ist $\overline{A}$ als Quotient einer p-Gruppe eine p–Gruppe. Es gibt daher $s \in \mathbb{N}$, so dass

$$\overline{c}^{p^s} = \overline{e} \in \bar{Z}\,.$$

Eine p^l-te Potenz von $\bar{c}$ liegt also in $\bar{Z}$. Sei l die maximale natürliche Zahl, so dass $\overline{d} = \overline{c}^{p^l} \notin \overline{Z} = \langle\overline{a}\rangle$.

Wir haben also ein $\bar{d}$ gefunden mit der Eigenschaft

$$\overline{d} \notin \overline{Z}, \quad \text{aber} \quad \overline{d}^{p} \in \overline{Z}.$$

Nun ist die Ordnung von $\overline{a}$ in $\overline{Z}$ gleich der Ordnung von a in A, da B nach Voraussetzung die Untergruppe $\langle a\rangle$ nur im neutralen Element

trifft. Andererseits beachte man, dass für jedes $x \in A$ die Ordnung der Projektion $\pi(x)$ ein Teiler der Ordnung von x ist,

$$\operatorname{ord}(\pi(x)) \,|\, \operatorname{ord}(x).$$

Also ist die Ordnung von $\overline{a}$ auch maximal in $\overline{A}$.
Würde nun $\overline{d}^p$ die Gruppe $\overline{Z}$ erzeugen, so hätte $\overline{d}$ die Ordnung

$$\operatorname{ord}(\overline{d}) = p \operatorname{ord}(\overline{a})$$

im Widerspruch zur Maximalität der Ordnung von $\overline{a}$ in $\overline{A}$. Nach der Struktur zyklischer Gruppen gibt es daher $\overline{f} \in \overline{Z}$, so dass

$$\overline{d}^p = \overline{f}^p.$$

Daher ist die von $\overline{x} := \overline{d}(\overline{f})^{-1}$ erzeugte Untergruppe von $\overline{A}$ zyklisch von Primzahlordnung und deshalb ohne echte Untergruppen. Da

$$\overline{x} = \overline{d}(\overline{f})^{-1} \notin \overline{Z}\,,$$

ist der Schnitt mit $\overline{Z}$ trivial

$$\langle \overline{x} \rangle \cap \overline{Z} = \{\overline{e}\}.$$

$\pi^{-1}(\langle \overline{x} \rangle)$ ist nun eine Untergruppe von A, die

- B enthält, da $\overline{e} \in \langle \overline{x} \rangle$ und $\pi^{-1}(\overline{e}) = B$.
- B echt enthält, da $\langle \overline{x} \rangle$ nicht trivial ist.
- $\langle a \rangle$ nicht trifft: hätte man

  $$y \in \langle a \rangle \cap \pi^{-1}(\langle \overline{x} \rangle)\,,$$

  so $\pi(y) \in \overline{Z} \cap \langle \overline{x} \rangle = \{\overline{e}\}$. Also ist $\pi(y) = \overline{e}$, somit $y \in B$. Da auch $y \in \langle a \rangle$, folgt $y = e$.

Aber B war gewählt als maximale Untergruppe von A, die $\langle a \rangle$ nur im neutralen Element trifft. Wir haben also einen Widerspruch erreicht. □

Damit können wir nun 1.9.2 (i) zeigen:

$$G \cong G_{tor} \times \mathbb{Z}^r \cong T(p_1) \times \cdots \times T(p_u) \times \mathbb{Z}^r \cong \mathbb{Z}_{p_1^{s_1}} \times \cdots \times \mathbb{Z}_{p_{r_v}^{s_v}} \times \mathbb{Z}^r\,,$$

wobei wir die Sätze 1.9.9, 1.9.10 und 1.9.11 in dieser Reihenfolge angewandt haben. Wir müssen aber noch die Eindeutigkeit des Rangs und der Zerlegung des Torsionsanteils zeigen.

Lemma 1.9.12.
Der Rang einer abelschen Gruppe G ist

$$\operatorname{rank} G = \dim_{\mathbb{Q}} \operatorname{Hom}(G, \mathbb{Q})$$

Insbesondere hängt der Rang nicht von der Zerlegung ab.

Beweis.

Man beachte, dass der Raum der Gruppenhomomorphismen $\operatorname{Hom}(G, \mathbb{Q})$ von der Gruppe G in die additive Gruppe von $\mathbb{Q}$ natürlicherweise die Struktur eines $\mathbb{Q}$–Vektorraums trägt: die Addition ist definiert als Addition der Werte der Morphismen, und ähnlich die skalare Multiplikation.

Sei also $\varphi \in \operatorname{Hom}(G, \mathbb{Q})$ und g ein Torsionselement der Ordnung N. Dann gilt

$$N\varphi(g) = \varphi(g^N) = 0 \Rightarrow \varphi(g) = 0\,.$$

Also verschwinden alle Homomorphismen nach $\mathbb{Q}$ auf dem Torsionsanteil von G. Auf $\mathbb{Z}$ selbst rechnet man nach, dass

$$\begin{aligned} \operatorname{Hom}(\mathbb{Z}, \mathbb{Q}) &\xrightarrow{\cong} \mathbb{Q}\,, \\ \varphi &\mapsto \varphi(1)\,. \end{aligned}$$

Ferner hat man für jedes direkte Produkt von Gruppen einen Isomorphismus von $\mathbb{Q}$–Vektorräumen

$$\operatorname{Hom}\Big(\prod_{i=1}^{r} G_i, \mathbb{Q}\Big) \cong \operatorname{Hom}(G_1, \mathbb{Q}) \times \cdots \times \operatorname{Hom}(G_r, \mathbb{Q})$$

Hat also G die Zerlegung

$$G = G_{tor} \times \mathbb{Z}^r,$$

so ist $\dim_{\mathbb{Q}} \operatorname{Hom}(G, \mathbb{Q}) = r$. □

Bemerkung 1.9.13.
Insbesondere sind $\mathbb{Z}^m$ und $\mathbb{Z}^n$ nur für $m = n$ isomorph. Das könnte man natürlich auch anders sehen: ist

$$\varphi : \mathbb{Z}^m \xrightarrow{\sim} \mathbb{Z}^n$$

ein Isomorphismus und p prim, so ist die Einschränkung

$$\varphi : p\mathbb{Z}^m \to p\mathbb{Z}^n$$

auch ein Isomorphismus und man erhält einen Isomorphismus

$$\bar{\varphi} : \mathbb{Z}^m/p\mathbb{Z}^m \cong (\mathbb{Z}_p)^m \to (\mathbb{Z}_p)^n.$$

Der Vergleich der Anzahlen liefert $mp = np$, woraus $m = n$ folgt.

Lemma 1.9.14 (Eindeutigkeit der Zahl der zyklischen Faktoren).

Sei G eine abelsche p–Gruppe und p eine Primzahl. Wir bezeichnen mit

$$G_p = \{x \in G | x^p = e\}$$

die Untergruppe derjenigen Elemente, deren Ordnung p teilt. Dann gehorcht die Zahl der zyklischen Faktoren $z(G)$ der Gleichung

$$p^{z(G)} = |G_p|$$

und die Zerlegung in zyklische Faktoren ist eindeutig bis auf die Reihenfolge.

Beweis.

Wir bemerken, dass in der zyklischen Gruppe $\mathbb{Z}_{p^s}$ genau die p Elemente

$$\{0, p^{s-1}, 2p^{s-1}, \ldots (p-1)p^{s-1}\}$$

eine Ordnung haben, die p teilt. Man überzeugt sich, dass für Produkte gilt

$$\Big(\prod_{i=1}^{s} G_i\Big)_p = \prod_{i=1}^{s} (G_i)_p$$

Nach 1.9.2 (i) hat man eine Zerlegung

$$G \cong \mathbb{Z}_{p_1^{s_1}} \times \cdots \times \mathbb{Z}_{p_r^{s_r}},$$

also

$$\begin{aligned} G_p &= \prod_{i=1}^{r} (\mathbb{Z}_{p^{s_i}})_p \\ |G_p| &= p^r = p^{z(G)} \end{aligned}$$

Die Eindeutigkeit der Zerlegung von G beweist man induktiv aus der Eindeutigkeit der Zerlegung von G/G_p mit Hilfe der Relation

$$G/G_p = \prod_i G_i/(G_i)_p.$$

Damit ist auch 1.9.2 (ii) bewiesen. □

Beweis. von 1.9.1.

Zerlege für alle Teiler p von $|G_{tor}|$ die Gruppe $T(p)$ gemäß

$$T(p) = \prod_{j=1}^{m(p)} \mathbb{Z}_{p^{s(p,j)}} ,$$

mit $m(p) \in \{1, 2 \ldots\}$ und natürlichen Zahlen $s(p, j)$. Definiere

$$\begin{aligned} \tilde{d}_1 &= \text{Produkt der höchsten auftretenden Primzahlpotenzen} \\ \tilde{d}_2 &= \text{Produkt der zweithöchsten auftretenden Primzahlpotenzen} \end{aligned}$$

und so fort. Damit teilt $\tilde{d}_{i+1} | \tilde{d}_i$ und der chinesische Restsatz 1.6.15 erlaubt es, Produkte von zyklischen Gruppen zusammen zu fassen:

$$G_{tor} \cong \mathbb{Z}_{\tilde{d}_1} \times \mathbb{Z}_{\tilde{d}_2} \times \cdots \times \mathbb{Z}_{\tilde{d}_s}.$$

Anschließend benennt man die $\tilde{d}_i$ noch um. □

1.10 Symmetrische Gruppen

Definition 1.10.1.
Eine Partition einer natürlichen Zahl $n \in \mathbb{N}$ ist eine monoton fallende Folge natürlicher Zahlen $p_1 \geq \ldots \geq p_i \geq p_{i+1} \ldots$ derart, dass fast alle Folgenglieder verschwinden und sich die Folgenglieder zu n aufaddieren. Die Menge aller Partitionen von n nennen wir $\mathcal{P}_n$.

- Jede Permutation $\sigma \in S_n$ gibt eine Partition von n: die Längen der Bahnen der Operation der von σ zyklisch erzeugten Gruppe $\langle \sigma \rangle$ auf der Menge $\{1, \ldots, n\}$.
- Jede Partition tritt hierbei auf, wenn man alle Permutationen betrachtet. Permutationen mit gleicher Partition sind konjugiert (Übung).
- Hat $\langle \sigma \rangle$ außer einer p–elementigen Bahn nur Fixpunkte, so nennt man σ einen p–Zykel. 2–Zykel heißen auch Transpositionen.
- Hat $\langle \sigma \rangle$ genau zwei zweielementige Bahnen und sonst nur Fixpunkte, so heißt σ Doppeltransposition.
- Hat $\langle \sigma \rangle$ genau zwei dreielementige Bahnen und sonst nur Fixpunkte, so heißt σ Doppeldreizykel.

Satz 1.10.2.

(i) Die symmetrische Gruppe S_r wird von den Transpositionen erzeugt.

(ii) Die alternierende Gruppe A_r wird von den Dreizykeln erzeugt.

Beweis.
(i) sollte bekannt sein.
(ii) folgt aus der Tatsache, dass A_r durch Paare von Transpositionen erzeugt wird und für a, b, c, d paarweise verschieden gilt

$$\begin{aligned}(ab)(cd) &= (abc)(bcd)\,,\\ (ab)(ac) &= (acb)\,.\end{aligned}$$

□

Hauptziel dieses Abschnitts ist der Beweis des folgenden Satzes:

Satz 1.10.3.
Die alternierenden Gruppen A_r sind einfach für $r \geq 5$ und für $r = 3$.

Beweis.
Wir notieren zunächst die folgenden einfachen Beobachtungen:

- Die Gruppen A_1 und A_2 sind trivial.
- Wegen $|A_3| = \frac{3!}{2} = 3$ ist $A_3 \cong \mathbb{Z}_3$, also einfach.
- In der Gruppe A_4 gibt es drei Doppeltranspositionen. Sie bilden mit dem neutralen Element eine Untergruppe, die wegen

  $$(12)(34) \cdot (13)(24) = (14)(23)$$

  isomorph zur Kleinschen Vierergruppe $\mathbb{Z}_2 \times \mathbb{Z}_2$ ist.

  Diese Untergruppe ist auch normal. Denn die Gruppe A_4 hat zwölf Elemente: das neutrale Element, 3 Doppeltranspositionen der Ordnung 2 und 8 Dreizykeln der Ordnung 3. Die Konjugation mit einem Gruppenelement ändert aber die Ordnung eines Elements nicht. Daher werden alle Doppeltranspositionen von A_4 durch Konjugation auf Doppeltranspositionen abgebildet.

□

Um den allgemeinen Fall abhandeln zu können, brauchen wir erst ein

Lemma 1.10.4.
(i) Für $r \geq 5$ wird A_r erzeugt durch Doppeltranspositionen.

(ii) Für $r \geq 5$ sind je zwei Doppeltranspositionen schon konjugiert in A_r. Für $r \geq 5$ sind je zwei Dreizykel schon konjugiert in A_r.

Beweis: durch Nachrechnen.

Beweis. von 1.10.3.
Sei N ein nicht–trivialer Normalteiler von A_r.

- Enthält N einen Dreizykel, so enthält N als normale Untergruppe sogar alle Dreizykel, da die Dreizykel in A_r nach Lemma 1.10.4 in A_r konjugiert sind. Aber die Dreizykel erzeugen nach Satz 1.10.2 die Gruppe A_r, also ist $N = A_r$.

  Enthält N eine Doppeltransposition, so enthält N als normale Untergruppe sogar alle Doppeltranspositionen, da die Doppeltranspositionen nach 1.10.4 in A_r konjugiert sind. Das Produkt

  $$[(ab)(de)][(ac)(de)] = (acb)$$

  ist aber ein Dreizykel. Man kann nun das Argument des vorhergehenden Abschnitts anwenden und findet, dass $N = A_r$.
- Wir wollen also zeigen, dass jeder Normalteiler N von A_r entweder einen 3–Zykel oder eine Doppeltransposition enthält.

  Dazu betrachten wir einmal Elemente von A_r mit vielen Fixpunkten.

Zahl der Fixpunkte		Element
r	$\rightarrow$	Identität
$r-1$	$\rightarrow$	unmöglich
$r-2$	$\rightarrow$	Transposition, nicht in A_r
$r-3$	$\rightarrow$	3–Zykel
$r-4$	$\rightarrow$	4–Zykel, aber nicht in A_r oder Doppeltransposition.

  Um unsere Behauptung zu beweisen, wollen wir also zeigen, dass wir aus jedem $g \in N$, das weder Doppeltransposition noch Dreizykel ist ein *nicht–triviales* $\tilde{g} \in N$ mit mehr Fixpunkten konstruieren können. Durch wiederholte Anwendung dieser Konstruktion erhalten wir dann entweder einen Dreizykel oder eine Doppeltransposition in N und schliessen, dass $N = A_r$.

Sei also $g \in N$ weder Doppeltransposition noch Dreizykel. Durch Übergang zu einer Potenz von g dürfen wir annehmen, dass g von Primzahlordnung ist. Fallunterscheidung nach dieser Ordnung:

a) $\mathrm{ord}(g) \geq 5$ Sei $(a_1 \dots a_p)$ ein Zykel in g. Wir definieren den Dreizykel $h = (a_1, a_2, a_3)$ und betrachten das Element $\tilde{g} = h^{-1}g^{-1}hg$, das offenbar im Normalteiler N liegt. Alle Fixpunkte von g sind auch Fixpunkte von $\tilde{g}$; aber auch a_1 ist Fixpunkt von $\tilde{g}$. Somit hat $\tilde{g}$ mehr Fixpunkte als g.

b) $\mathrm{ord}(g) = 3$, aber g kein Dreizykel. Dann enthält g mindestens 2 disjunkte 3–Zykel. Dann gibt es aber eine "Dreifachtransposition" h_0, die die drei Elemente des ersten Dreizykels mit denen des zweiten Dreizykels vertauscht. Offenbar ist

$$h_0 g h_0^{-1} = g$$

und h_0 ist ungerade, d.h. $h_0 \in S_r \setminus A_r$. Damit bestehen aber die Konjugationsklassen von g in A_r und in S_r aus den gleichen Elementen.

In S_6 gibt es zwei Doppeldreizykel, deren Produkt nicht-trivial mit Fixpunkten ist. Betrachte etwa:

$$\begin{array}{lcll} g_1 & = & (123)(456) & \\ g_2 & = & (134)(265) & \\ g_2 g_1 & = & (16)(24) & \text{nicht–trivial mit 2 Fixpunkten} \end{array}$$

Wir betrachten daher die Einschränkung von g auf eine 6–elementige Menge, wo g als Doppeltransposition wirkt. Durch Konjugation können wir alle Doppeldreizykel auf dieser Menge erreichen, also auch ein geeignetes $\tilde{g}$ wie im Beispiel oben. Ausserdem ist $\tilde{g} \in N$, da N normal ist. Daher hat das Element $g\tilde{g} \in N$ mehr Fixpunkte als g.

c) $\mathrm{ord}(g) = 2$, aber g ist keine Doppeltransposition. Dann enthält g mindestens zwei disjunkte Doppeltranspositionen. Finde $\tilde{g} \in N$, so dass $\tilde{g}$ und g außerhalb einer 4–elementigen Teilmenge übereinstimmen, dort aber $\tilde{g}$ eine andere Doppeltransposition ist. Dies geht, da alle Doppeltranspositionen auf der 4–elementigen Teilmenge zu $\tilde{g}$ konjugiert sind, also in N liegen. Das Element $g\tilde{g}$ ist dann die dritte Doppeltransposition auf dieser Teilmenge, also enthält N eine Doppeltransposition.

□

1.11 Die Sätze von Sylow

Ziel dieses Abschnitts ist, es eine bessere Übersicht über die Untergruppen U einer endlichen Gruppe G zu bekommen. Der Satz 1.4.4 von Lagrange

sagt uns, dass die Ordnung einer Untergruppe $|U|$ die Gruppenordnung $|G|$ teilt. Im Fall von zyklischen Gruppen wissen wir schon, dass es eine Bijektion zwischen Teilern der Gruppenordnung und Untergruppen von G gibt. Allgemein kann aber eine solche Beziehung nicht gelten: zum Beispiel hat die alternierende Gruppe A_r keine Untergruppe der Ordnung $r!/4$. Denn diese wäre vom Index zwei in A_r und daher nach Übungsblatt 1 Normalteiler.

Alle Gruppen in Kapitel 1.11 sind endlich.

Satz 1.11.1. *(Struktur von p–Gruppen)*

Ist G eine p–Gruppe, so gibt es in G eine absteigende Kette

$$G = G_r \supseteq G_{r-1} \supseteq \cdots \supseteq G_0$$

von Normalteilern von G, so dass

$$G_i/G_{i-1} \cong \mathbb{Z}_p \quad \textit{für alle } i.$$

Beweis.

Wir schreiben die Gruppenordnung als $|G| = p^s$ und führen den Beweis mit Induktion nach s.

Die Gruppe G hat nach Korollar 1.8.3 nicht–triviales Zentrum. Nach Übergang zu einer geeigneten Potenz eines Elementes erhalten wir ein Element x von $Z(G)$ der Ordnung p. Wir setzen

$$G_1 = \langle x \rangle \cong \mathbb{Z}_p\,;$$

diese Untergruppe von G ist normal als Untergruppe des Zentrums.

Nach Induktionsannahme finden wir nun in $\overline{G} = G/G_1$ eine Kette

$$\overline{G} = \overline{G}_0 \supseteq \cdots \supseteq \overline{G}_1 \supset \overline{G}_0 = \{e\}$$

mit den gewünschten Eigenschaften. Sei nun

$$\pi : G \to G/G_1$$

die kanonische Surjektion. Die Urbilder

$$G_i = \pi^{-1}(\overline{G}_{i-1}).$$

sind als Urbilder normaler Untergruppen von $\overline{G}$ in G normal. Aus dem Isomorphiesatz lernen wir, dass

$$G_i/G_1 \xrightarrow{\sim} \overline{G}_{i-1}\,, \quad i \geq 1\,.$$

Der Noethersche Isomorphiesatz erlaubt uns dann, zu schließen

$$\begin{aligned} G_i/G_{i-1} &\cong (G_i/G_1) \,/\, (G_{i-1}/G_1) \\ &\cong \overline{G}_{i-1}/\overline{G}_{i-2} \cong \mathbb{Z}_p \quad \text{für} \quad i \geq 2. \end{aligned}$$

Damit hat aber die Kette der Urbilder die gewünschten Eigenschaften. □

Bemerkung 1.11.2. *(Doppelnebenklassen)*

(i) Für jede Untergruppe $H \leq G$ und jedes $g \in G$ ist die konjugierte Untergruppe

$$H^g = g^{-1}Hg$$

eine Untergruppe gleicher Kardinalität wie H. Die Menge

$$N_G(H) = \{g \in G | gHg^{-1} = H\}$$

heißt <u>Normalisator</u> von H in G. Sie ist eine Untergruppe. Der Normalisator enthält den Zentralisator; die Konjugation mit Elementen im Zentralisator bildet die Untergruppe H nicht nur auf sich ab, sondern wirkt auf H sogar als die Identität. Man hat folgende Inklusionen von Untergruppen:

$$H \leq N_G(H) \leq G\,.$$

Der Normalisator $N_G(H)$ ist die größte Untergruppe von G, in der H normal ist. Insbesondere gilt

$$N_G(H) = G \iff H \quad \textit{ist Normalteiler von } G\,.$$

Der Index des Normalisators $[G : N_G(H)]$ ist nach der Bahnengleichung die Zahl der zu H konjugierten Untergruppen von G.

(ii) Seien H und U Untergruppen von G. U operiert auf den Nebenklassen G/H vermöge

$$\begin{aligned} U \times G/H &\to G/H \\ (\sigma, \tau H) &\mapsto \sigma\tau H \end{aligned}$$

mit Stabilisator für τH

$$\tau H \tau^{-1} \cap U.$$

Die Untermenge

$$U\tau H$$

von G heißt <u>Doppelnebenklasse</u> von τ nach U, H.

(iii) Es gilt

(a) *G ist die disjunkte Vereinigung der verschiedenen Doppelnebenklassen nach U, H.*

(b) *Sei V ein Vertretersystem und G endliche Gruppe.*

$$|G| = \sum_{v \in V} \frac{|U|\ |H|}{|vHv^{-1} \cap U|} = \sum_{v \in V} \frac{|U|\ |H|}{|H \cap U^v|} \tag{8}$$

Beweis.

(i),(ii) Eigenschaften einer Operation.

(iii) Sei m die Länge der Bahn von τH unter der Operation von U auf G/H. Nach der Bahnengleichung gilt

$$m = \frac{|U|}{|\tau H \tau^{-1} \cap U|}\,.$$

Daher ist die Zahl der Elemente in der Doppelnebenklasse von τ nach U, H gleich

$$|U\tau H| = m|H| = \frac{|U|\ |H|}{|\tau H \tau^{-1} \cap U|}\,.$$

Ferner ist

$$\mathrm{int}_{\tau^{-1}} : \tau H \tau^{-1} \cap U \to H \cap U^{\tau}$$

eine Bijektion, was die Behauptung zeigt.

□

Definition 1.11.3.
Sei G endliche Gruppe. Sei p eine Primzahl und schreibe die Gruppenordnung in der Form $|G| = p^n a$ mit $(a, p) = 1$. Also ist p^n die maximale in $|G|$ aufgehende Potenz der Primzahl p. Eine Untergruppe $H \leq G$ der Ordnung $|H| = p^n$ heißt eine p–Sylowgruppe von G. Mit $Syl_p(G)$ bezeichnen wir die Menge der p–Sylowgruppen von G.

Bemerkung: $n = 0$ ist zulässig und beschreibt den Fall, wenn p die Gruppenordnung nicht teilt. In diesem Fall ist die triviale Untergruppe $\{e\}$ die einzige p-Sylowgruppe.

Beispiel 1.11.4.
Betrachte die endliche Gruppe

$$G = GL(n, p) = GL(n, \mathbb{F}_p)\,, \quad p \text{ prim}\,,$$

der invertierbaren Matrizen mit Koeffizienten im Körper $\mathbb{F}_p$ mit p Elementen. Wir rechnen

$$|G| = (p^n - 1)(p^n - p) \dots (p^n - p^{n-1}),$$

denn für das Bild des ersten Basisvektors hat man $p^n - 1$ Möglichkeiten, für den zweiten Basisvektor $p^n - p$ Möglichkeiten, etc.

Die maximale p–Potenz in $|G|$ ist daher

$$p^{1+2+\dots+(n-1)} = p^{n(n-1)/2}.$$

Die Untergruppe

$$P = \left\{ \begin{pmatrix} 1 & & & * \\ 0 & 1 & & \\ & & \ddots & \\ 0 & 0 & & 1 \end{pmatrix} \right\} \leq GL(n,p)$$

der oberen Dreicksmatrizen mit Einsen auf der Diagonale ist offensichtlich ein Beispiel für eine p–Sylowgruppe von G.

Das folgende Lemma wird zentral im Beweis der Sylowsätze sein:

Lemma 1.11.5.
Sei H Untergruppe von G und P eine p–Sylowgruppe von G. Dann gibt es ein Gruppenelement $\tau \in G$ so dass

$$H \cap P^\tau$$

eine p–Sylowgruppe von H ist.

Beweis.

Die Doppelnebenklassenzerlegung von G nach H und P liefert nach (8) die folgende Relation:

$$|G| = \sum_{\tau \in V} \frac{|H|\,|P|}{|H \cap P^\tau|}.$$

Teilt man diese Relation durch die maximale p-Potenz p^n in $|G|$ und beachtet, dass $p^n = |P|$, so findet man

$$\sum_{\tau \in V} \frac{|H|}{|H \cap P^\tau|} \neq 0 \bmod p.$$

Für wenigstens ein $\tau \in V$ ist daher

$$[H : H \cap P^\tau)] \neq 0 \bmod p.$$

Andererseits ist $H \cap P^\tau$ als Untergruppe von P^τ eine p–Gruppe. Damit muss aber $H \cap P^\tau$ eine p–Sylowgruppe von H sein. □

Theorem 1.11.6 (Sylowsätze).

(i) Jede endliche Gruppe G besitzt eine p–Sylowgruppe. Jede p–Untergruppe von G ist in einer geeigneten p–Sylowgruppe enthalten.

(ii) Je zwei p–Sylowgruppen von G sind konjugiert.

(iii) Sei n_p die Zahl der p-Sylowgruppen von G, $n_p := |Syl_p(G)|$. Dann gilt

(a) n_p teilt $[G : P]$ für $P \in Syl_p(G)$ und

(b) $n_p \equiv 1 \bmod p$.

Bemerkung 1.11.7.

(i) Wir verschärfen die Aussagen zu

(a') $n_p = [G : N_G(P)]$

(b') $n_p = 1 \bmod p^d$, wobei d folgendermassen definiert ist: durchlaufe P' alle von P verschiedenen p–Sylowgruppen von G. Dann ist der Index $[P : P \cap P']$ als Index einer Untergruppe einer p-Gruppe eine Potenz von p. Sei p^d die grösste p-Potenz, die in all diesen Indizes aufgeht.

Aus (b') folgt (b), weil die Untergruppe $P \cap P'$ eine echte Untergruppe von P ist, der Index $[P : P \cap P']$ also nicht gleich eins sein kann, so dass d stets größer gleich eins ist.

(ii) Ist $P \in \mathrm{Syl}_p(G)$ normal in G, so ist P die einzige p–Sylowgruppe. Hat G nur eine einzige p–Sylowgruppe, so ist diese normal, sogar charakteristisch.

Beweis.

(i) Sei G eine endliche Gruppe. Nach dem Satz 1.7.1 von Cayley können wir G in eine geeignete symmetrische Gruppe S_n einbetten. Diese wiederum betten wir in $GL(n, p)$ ein: die Permutation $\sigma \in S_n$ wird abgebildet auf den Endomorphismus φ_σ von $\mathbb{F}_p^n$, der auf den Vektoren e_i einer Basis von $\mathbb{F}_p^n$ folgendermaßen wirkt:

$$\varphi_\sigma(e_i) = e_{\sigma(i)}\,.$$

Wir fassen daher G als Untergruppe von $GL(n, p)$ auf. Die Gruppe $GL(n, p)$ hat aber, wie wir in Beispiel 1.11.4 gesehen haben, eine p–Sylowgruppe P. Nach Lemma 1.11.5 hat G eine p–Sylowgruppe der Form P^τ.

(ii) Sei P eine p–Sylowgruppe und $H \leq G$ eine beliebige p–Untergruppe von G. Nach Lemma 1.11.5 gibt es ein $\tau \in G$ so dass

$$H \cap P^\tau \in \mathrm{Syl}_p(H)\,.$$

Da H eine p–Gruppe ist, ist sie für sich selbst eine p–Sylowgruppe, also $H \cap P^\tau = H$, also $H \leq P^\tau$. Dies zeigt die Aussagen des ersten Sylowsatzes.

Ist $H \in \mathrm{Syl}_p(G)$, so ist $H = P^\tau$, da beide Gruppen gleiche Ordnung haben. Hieraus folgt die Aussage des zweiten Sylowsatzes.

(iii) Wegen (ii) ist für jede p–Sylowgruppe P

$$n_p = |\{P^\tau | \tau \in G\}| = [G : N_G(P)]\,.$$

Hieraus folgen (a') und daraus (a). Zum Beweis von (b') betrachten wir wieder Doppelnebenklassen von G, diesmal nach $P, N_G(P)$. Sei V ein Vertretersystem für die Doppelnebenklassen, das das neutrale Element enthält, $e \in V$.

Für alle vom neutralen Element verschiedenen Repräsentanten $\tau \neq e$ ist $\tau \notin N_G(P)$. Damit aber $P^\tau \neq P$. Der Schnitt

$$P^\tau \cap N_G(P)$$

– ist eine p–Gruppe, also in einer p–Sylowgruppe von $N_G(P)$ enthalten.
– aber andererseits liegt P normal in $N_G(P)$ und ist daher die einzige p–Sylowgruppe von $N_G(P)$. Also liegt

$$P^\tau \cap N_G(P) \subseteq P\,.$$

Daraus folgt $P^\tau \cap N_G(P) \subseteq P^\tau \cap P$; die umgekehrte Inklusion ist trivial, also gilt die Gleichheit $P^\tau \cap N_G(P) = P^\tau \cap P$.

Jetzt können wir die Bahnengleichung für Doppelnebenklassen anwenden:

$$|G| = \sum_{\tau \in V} \frac{|P|\ |N_G(P)|}{|N_G(P) \cap P^\tau|}.$$

Wir teilen sie durch $|N_G(P)|$ und erhalten

$$n_p = [G : N_G(P)] = \sum_{\tau \in V, \tau \neq e} [P : P^\tau \cap P] + 1\,.$$

Die Terme in der Summe sind als Indizes von echten Untergruppen einer p Gruppe durch p teilbar. Also ist $n_p = 1 \bmod p^d$.

□

Folgerungen 1.11.8.

(i) Zu jeder Primzahlpotenz p^k, die die Gruppenordnung $|G|$ teilt, gibt es eine Untergruppe H von G der Ordnung $|H| = p^k$. Dies folgt aus dem ersten Sylowsatz 1.11.6 (i) und dem Struktursatz 1.11.1 für p-Gruppen.

Wendet man diesen Satz für $k = 1$ an, so folgt: zu jedem Primzahlteiler p der Gruppenordnung $|G|$ gibt es in G ein Element der Ordnung p.

(ii) Jede Gruppe der Ordnung 6 ist entweder zyklisch oder isomorph zur symmetrischen Gruppe S_3.

Beweis.

Es gibt in G Elemente a, b der Ordnungen 2 und 3. Die Gruppe besteht aus den Elementen $\{e, a, b, b^2, ab, ab^2\}$, da man leicht nachrechnet, dass diese Elemente alle verschieden sein müssen. Nun muss ba gleich einem dieser Elemente sein, kann aber nicht gleich e, a, b oder b^2 sein. Also entweder $ba = ab$, dann ist G abelsch und isomorph zu $G \cong \mathbb{Z}_2 \times \mathbb{Z}_3 \cong \mathbb{Z}_6$. Anderenfalls gilt $ba = ab^2$, woraus folgt, dass $G \cong S_3$. □

(iii) Jede Gruppe der Ordnung 15 ist zyklisch.

Beweis.

Die Zahl n_3 der 3-Sylowgruppen teilt $\frac{15}{3} = 5$ und wir wissen, dass $n_3 = 1 \bmod 3$. Daher gilt $n_3 = 1$. Nur zwei Elemente der Gruppe haben also Ordnung 3.

Die Zahl n_5 der 5-Sylowgruppen teilt $\frac{15}{5} = 3$ und $n_5 = 1 \bmod 5$. Daher gilt $n_5 = 1$, nur 4 Elemente der Gruppe haben Ordnung 5. Damit müssen aber die restlichen 8 Elemente der Gruppe Ordnung 15 haben. Jedes von ihnen erzeugt die Gruppe, die somit zyklisch ist. □

1.12 Kompositionsreihen, Normalreihen, auflösbare Gruppen

Definition 1.12.1.

(i) Eine Normalreihe einer Gruppe G ist eine Folge von Untergruppen

$$G = G_r \supset G_{r-1} \supset \cdots \supset G_0 = \{e\}$$

derart, dass G_i Normalteiler von G_{i+1} ist.

Beachte: es ist für $i \leq r-2$ nicht gefordert, dass G_i sogar normal in ganz G ist, anders als in der Aussage des Struktursatzes 1.11.1 über p-Gruppen.

(ii) Eine Kompositionsreihe ist eine Normalreihe mit der zusätzlichen Eigenschaft, dass der Quotient

$$G_i/G_{i-1} \qquad \textit{einfach ist}\,.$$

Äquivalent dazu kann man fordern, dass G_{i-1} maximal ist in G_i in dem Sinne, dass $G_{i-1} \neq G_i$ und für jeden Normalteiler M von G_i mit

$$G_{i-1} \subset M \subset G_i$$

entweder gilt

$$M = G_{i-1} \quad \textit{oder} \quad M = G_i\,.$$

Die Gruppen G_i/G_{i-1} heißen Subquotienten der Kompositionsreihe.

Satz 1.12.2. *(Verfeinerungssatz von Schreier)*
Je zwei Normalreihen einer Gruppe haben äquivalente Verfeinerungen.
Ohne Beweis.

Satz 1.12.3. *(Jordan–Hölder)*
Je zwei Kompositionsreihen einer endlichen Gruppe G haben dieselbe Länge und bis auf Reihenfolge isomorphe Subquotienten. Wir nennen sie die Kompositionsfaktoren von G.
Sind genauer

$$G = G_r \supset \cdots \supset G_0 = \{e\}$$

und

$$G = G'_s \supset \cdots \supset G'_0 = \{e\}$$

zwei Kompositionsreihen, so haben wir $r = s$ und es gibt eine Permutation $\sigma \in S_r$ so dass

$$G'_i/G'_{i-1} \cong G_{\sigma(i)}/G_{\sigma(i)-1} \quad \textit{für alle} \quad i = 1, \ldots, r\,.$$

Beweis.
Induktion nach Gruppenordnung. Der Induktionsanfang ist trivial. Betrachte nun zwei Kompositionsreihen für die Gruppe G:

$$\begin{aligned} G &\supset M \supset \cdots \supset \{e\} \\ G &\supset N \supset \cdots \supset \{e\} \end{aligned}$$

Gilt $M = N$, so wendet man direkt die Induktionsvoraussetzung an. Andernfalls betrachte die kanonische Surjektion

$$\pi : G \to G/N\,.$$

Da π surjektiv ist und M normal in G ist, ist auch $\pi(M)$ normal in G/N. Aber G/N ist einfach, daher folgt $\pi(M) = G/N$. Also vermittelt π einen Isomorphismus

$$M/M \cap N \cong G/N\,. \tag{9}$$

Durch Vertauschen von M und N findet man analog

$$N/M \cap N \cong G/M\,. \tag{10}$$

Wir wählen jetzt eine Kompositionsreihe des Schnitts $M \cap N$ und vergleichen die vier Kompositionsreihen von G:

$$\begin{aligned} G &\supset M \supset \cdots \supset \{e\} \\ G &\supset M \supset (M \cap N) \supset \cdots \supset \{e\} \\ G &\supset N \supset (M \cap N) \supset \cdots \supset \{e\} \\ G &\supset N \supset \cdots \supset \{e\} \end{aligned}$$

Die erste und die zweite Kompositionsreihe sind äquivalent, nach Induktionsvoraussetzung, angewandt auf M. Analog sind auch die dritte und vierte Kompositionsreihe äquivalent. Die Äquivalenz der zweiten und der dritten Kompositionsreihe folgt aus den Isomorphismen (9) und (10). □

Definition 1.12.4.
Eine Gruppe G heißt auflösbar oder metazyklisch, wenn es eine Kompositionsreihe gibt, in der alle Kompositionsfaktoren zyklisch von Primzahlordnung sind.

Satz 1.12.5.
Sei G endliche Gruppe. Dann gilt:

(i) Mit G ist auch jede Untergruppe H von G auflösbar.

(ii) Mit G ist auch jede Faktorgruppe G/H von G auflösbar.

(iii) Sei N Normalteiler von G. Sind N und G/N auflösbar, so ist auch G auflösbar.

(iv) Abelsche Gruppen sind auflösbar.

(v) p–Gruppen sind auflösbar.

Viel tiefer liegen die folgenden beiden Sätze. Wir werden sie daher nicht beweisen.

(vi) p^aq^b–Satz von Burnside:
Alle Gruppen der Ordnung p^aq^b (mit p, q prim und $a, b \in \mathbb{N}$) sind auflösbar.

(vii) Feit–Thompson:
Alle endlichen Gruppen ungerader Ordnung sind auflösbar.

Beweis.

(i) Sei $H \subset G$, G auflösbar. Eine Kette für G

$$G = G_0 \supset G_1 \supset \cdots \supset G_r = \{e\} \tag{11}$$

gibt durch Schnitt mit H eine Kette für H:

$$H = (G_0 \cap H) \supset (G_1 \cap H) \supset \cdots \supset (G_r \cap H) = \{e\}.$$

Für jedes i betrachte die Einschränkung $\tilde{\pi}_i$ des Restklassenhomomorphismus

$$\tilde{\pi}_i \,:\, G_{i-1} \to G_{i-1}/G_i$$

auf die Untergruppe $G_{i-1} \cap H$ von G_{i-1}. Der Kern von $\tilde{\pi}_i$ ist $(G_{i-1} \cap H) \cap G_i = G_i \cap H$. Als Kern eines Gruppenhomomorphismus ist somit $G_i \cap H$ Normalteiler von $G_{i-1} \cap H$ und $\tilde{\pi}_i$ gibt eine Injektion

$$(G_{i-1} \cap H)/(G_i \cap H) \to G_{i-1}/G_i$$

Aber zyklische Gruppen von Primzahlordnung haben keine nichttrivialen Untergruppen. Also gilt entweder

$$G_{i-1} \cap H = G_i \cap H$$

oder es ist

$$G_{i-1} \cap H/G_i \cap H \cong G_{i-1}/G_i$$

zyklisch von Primzahlordnung. In jedem Fall folgt, dass H auflösbar ist.

(ii) Wir betrachten allgemeiner einen surjektiven Homomorphismus $\pi : G \to \overline{G}$. Die Anwendung von π auf eine Kette (11) von G gibt eine Kette

$$\overline{G} = \pi(G) \supseteq \pi(G_1) \supseteq \cdots \supseteq \pi(G_r) = \{e\}$$

in der jeweils $\pi(G_i)$ Normalteiler von $\pi(G_{i-1})$ ist. Ferner vermittelt π Surjektionen

$$\pi_i : G_{i-1}/G_i \to (\pi(G_{i-1}))/(\pi(G_i))\,.$$

Da $|G_i/G_{i-1}|$ prim ist, ist entweder $\pi(G_{i-1}) = \pi(G_i)$ oder π_i ist ein Isomorphismus. In jedem Fall ist $\overline{G}$ auflösbar.

(iii) Wir können ausgehen von zwei Ketten

$$\begin{array}{lllllll} G/N & = & Q_0 \supseteq Q_1 & \supseteq \cdots \supseteq & Q_m & = & \{e\} \\ N & = & N_m \supseteq N_{m+1} & \supseteq \cdots \supseteq & N_n & = & \{e\} \end{array}$$

Sei

$$\pi : G \to G/N$$

die kanonische Projektion. Wir setzen

$$N_i = \pi^{-1}(Q_i)\,,$$

was uns Untergruppen von G gibt, so dass N_{i+1} Normalteiler von N_i ist. (Wegen

$$\pi^{-1}(Q_m) = \pi^{-1}\{e\} = N = N_m$$

gibt es auch bei N_m keine Bezeichnungskollision.) Ferner vermittelt π einen Isomorphismus

$$N_{i-1}/N_i \cong Q_{i-1}/Q_i \quad i \leq m\,,$$

so dass G auflösbar ist.

(iv) Sei G abelsch. Induktion nach der Gruppenordnung $|G|$. Der Induktionsanfang für $|G| = 1$ ist trivial. Ist $|G| > 1$, dann enthält G ein Element σ von Primzahlordnung. Die von σ zyklisch erzeugte Gruppe $N = \langle\sigma\rangle$ ist als Untergruppe einer abelschen Gruppe normal und sicher auflösbar. G/N ist abelsch und nach Induktionsannahme auflösbar. Aussage (*iii*) impliziert nun, dass G auflösbar ist.

(v) Folgt aus der stärkeren Aussage 1.11.1.

□

Bemerkung 1.12.6.

(i) Aus Satz 1.12.5 (iii) und (iv) folgt per Induktion: Besitzt die endliche Gruppe G eine Kette von Untergruppen

$$G = G_0 \supseteq G_1 \supseteq G_2 \supseteq \ldots \supseteq G_r = \{e\}\,,$$

so dass G_{i+1} normal in G_i ist und alle Faktorgruppen abelsch sind, so ist G auflösbar. D.h. die auflösbaren Gruppen sind genau die Gruppen mit abelschen Normalreihen.

D.h. in der Definition 1.12.4 kann "zyklisch von Primzahlordnung" zu "abelsch" abgeschwächt werden.

(ii) Die symmetrische Gruppe S_n ist für $n \geq 5$ nicht auflösbar. Denn $S_r \supset A_r \supset \{e\}$ ist eine Kompositionsreihe mit Kompositionsfaktoren $S_n/A_n \cong \mathbb{Z}_2$ und A_n. A_n ist für $n \geq 5$ einfach und nicht abelsch.

Für $n \leq 4$ findet man Kompositionsreihen

$$\begin{array}{lllll} S_2 & = & \mathbb{Z}_2 & \supset & \{e\} \\ S_3 & \supseteq & A_3 & \cong & \mathbb{Z}_3 \supseteq \{e\} \\ S_4 & \supseteq & A_4 & \supseteq & \mathbb{Z}_2 \times \mathbb{Z}_2 \supseteq \mathbb{Z}_2 \supseteq \{e\}\,. \end{array}$$

Diese Gruppen sind also auflösbar.

Definition 1.12.7.

(i) Sei G eine Gruppe. Für $a, b \in G$ wird das Produkt

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

als <u>Kommutator</u> von a, b bezeichnet. Die von allen Kommutatoren erzeugte Untergruppe von G heißt <u>Kommutatorgruppe</u> von G.

$$K(G) = \langle [a, b], a \in G, b \in G \rangle$$

Warnung:
Ein Produkt von Kommutatoren ist im allgemeinen kein Kommutator.

(ii) Wir definieren rekursiv die <u>höheren Kommutatorgruppen:</u>

$$\begin{array}{rcl} K_0(G) & = & G\,, \\ K_{n+1}(G) & = & K(K_n(G))\,. \end{array}$$

Satz 1.12.8.

(i) Die Kommutatorgruppe $K(G)$ ist Normalteiler von G.

(ii) Für einen Normalteiler N von G ist die Faktorgruppe G/N genau dann abelsch, wenn $K(G)$ in N enthalten ist. Insbesondere ist $G/K(G)$ abelsch, und G ist genau dann abelsch, wenn $K(G) = \{e\}$.

Beweis.

(i) $K(G)$ ist sogar charakteristisch, denn für $\varphi \in \mathrm{Aut}(G)$ ist das Bild eines Kommutators

$$\varphi([a,b]) = \varphi(aba^{-1}b^{-1}) = [\varphi(a), \varphi(b)]$$

wieder ein Kommutator.

(ii) Wir rechnen:

$$\begin{aligned} G/N \text{ abelsch} &\iff aNbN = bNaN \qquad \forall a,b \in G \\ &\iff abN = baN \qquad \forall a,b \in G \\ &\iff b^{-1}a^{-1}baN = N \qquad \forall a,b \in G \\ &\iff [b^{-1},a^{-1}] \in N \quad \forall a,b \in G \end{aligned}$$

□

Lemma 1.12.9.

Seien G Gruppe, U Untergruppe von G, N Normalteiler von G und H eine weitere Gruppe. Dann gilt für alle $n \geq 0$:

(a) $K_n(U) \subseteq K_n(G)$

(b) $K_n(G/N) = K_n(G)N/N \cong K_n(G)/K_n(G) \cap N$

(c) $K_n(G \times H) = K_n(G) \times K_n(H)$.

Beweis.

Durch Induktion nach n. Für (a) und (c) ist der Beweis klar. Für (b) berechnet man:

$$\begin{aligned} K_{n+1}(G/N) &= K(K_n(G/N)) \\ &= K(K_n(G)N/N) \\ &= K(\{kN | k \in K_n(G)\}) \\ &= \langle [k_1,k_2]N \mid k_1,k_2 \in K_n(G) \rangle \\ &= K_{n+1}(G)N/N \\ &= K_{n+1}(G)/K_{n+1}(G) \cap N \end{aligned}$$

Hierbei wurde im ersten Schritt die Definition, im zweiten die Induktionsvoraussetzung und im letzten Schritt der Isomorphiesatz angewandt. □

Satz 1.12.10.
Eine Gruppe G ist genau dann auflösbar, wenn es ein $m \in \mathbb{N}$ gibt, so dass

$$K_m(G) = \{e\}.$$

Beweis.

- Wenn $K_m(G) = \{e\}$ gilt, so bildet die sogenannte abgeleitete Reihe
$$G \supseteq K_1(G) \supseteq \cdots \supseteq K_m(G) = \{e\}$$
eine abelsche Normalreihe.
- Die andere Richtung der Aussage beweist man mit Induktion nach der Länge einer abelschen Normalreihe. Im Falle $r = 1$ ist G abelsch und $K(G) = \{e\}$. Induktionsschritt: Sei
$$G \supset N \supset \cdots \supset \{e\}$$
eine abelsche Normalreihe. Dann ist G/N abelsch, $K(G/N) = \{e\}$, also $K(G)N \subset N$ nach Lemma 1.12.9(b). Damit ist aber $K(G) \subset N$. Nach Induktionsannahme gibt es $r \in \mathbb{N}$, so dass $K_r(N) = \{e\}$. Wir finden mit 1.12.9(a)
$$K_{r+1}(G) \subseteq K_r(N) = \{e\}\,.$$

□

1.13 Etwas homologische Algebra

Definition 1.13.1.
(i) Eine Sequenz von Gruppen mit Gruppenhomomorphismen f, g

$$A' \xrightarrow{f} A \xrightarrow{g} A''$$

heißt exakt bei A genau dann, wenn $\operatorname{Im} f = \ker g$.

(ii) Eine Sequenz von Gruppen

$$\cdots \to A_{i+1} \to A_i \to A_{i-1} \to \ldots$$

heißt exakt genau dann, wenn sie exakt ist an jeder Stelle A_i.

(iii) Eine Sequenz von Gruppen

$$A' \xrightarrow{f} A \xrightarrow{g} A''$$

heißt kurze exakte Sequenz genau dann, wenn sie exakt ist in der Mitte, f injektiv ist und g surjektiv. Als Notation verwenden wir auch

$$A' \hookrightarrow A \twoheadrightarrow A''$$

oder

$$0 \to A' \to A \to A'' \to 0\,.$$

Lemma 1.13.2 (Neunerlemma).
Gegeben sei ein Diagramm von Gruppen mit kurzen exakten Zeilen:

$$\begin{array}{ccccc} A' & \overset{\hookrightarrow}{i_1} & A & \overset{\twoheadrightarrow}{\pi_1} & A'' \\ \downarrow \varphi_1 & & \downarrow \varphi_2 & & \downarrow \varphi_3 \\ B' & \overset{\hookrightarrow}{i_2} & B & \overset{\twoheadrightarrow}{\pi_2} & B'' \\ \downarrow \psi_1 & & \downarrow \psi_2 & & \downarrow \psi_3 \\ C' & \overset{\hookrightarrow}{i_3} & C & \overset{\twoheadrightarrow}{\pi_3} & C'' \end{array}$$

und seien die senkrechten Kompositionen null:

$$\psi_i \circ \varphi_i = e.$$

Das Diagramm sei kommutativ in dem Sinne, dass alle 4 Quadrate kommutieren. Dann gilt: Sind zwei der Spalten kurze exakte Sequenzen, so ist auch die dritte Spalte eine kurze exakte Sequenz.

Beweis.

Wir behandeln das Beispiel, in dem die beiden linken Spalten exakt sind.

- Die Surjektivität von ψ_3 folgt aus der Kommutativität des rechten unteren Quadrats, $\psi_3 \circ \pi_2 = \pi_3 \circ \psi_2$. Daher

  $$\mathrm{Im}(\psi_3) \supseteq \mathrm{Im}(\psi_3 \circ \pi_2) = \mathrm{Im}(\pi_3 \circ \psi_2) = C''\,,$$

  da π_3 und ψ_2 surjektiv sind.
- Um die Injektivität von φ_3 zu zeigen, wählen wir $a'' \in A''$, so dass $\varphi_3(a'') = e$. Wegen der Surjektivität von π_1 finden wir ein Urbild unter π_1:

  $$\pi_1(a) = a''\,.$$

Definiere $b := \varphi_2(a) \in B$. Dieses Element hat zwei Eigenschaften:

$$\begin{aligned}\psi_2(b) &= \psi_2 \circ \varphi_2(a) = e \\ \pi_2(b) &= \pi_2\varphi_2(a) = \varphi_3\pi_1(a) = \varphi_3(a'') = e\end{aligned}$$

Die letzte Eigenschaft erlaubt es, $b' \in B'$ zu finden, so dass

$$b = i_2(b')$$

und die erste Eigenschaft impliziert dann

$$\psi_2 \circ i_2(b') = \psi_2(b) = e = i_3 \circ \psi_1(b')\,.$$

Da i_3 injektiv ist, folgt $\psi_1(b') = e$. Jetzt können wir die Exaktheit der ersten Spalte ausnützen und finden

$$b' = \varphi_1(a') \quad \text{mit} \quad a' \in A'.$$

Wir rechnen $\varphi_2 \circ i_1(a') = i_2\varphi_1(a') = i_2(b') = b = \varphi_2(a)$. Nun war aber φ_2 injektiv vorausgesetzt, also gilt $i_1(a') = a$. Das erlaubt uns die Rechnung $a'' = \pi(a) = \pi i_1(a') = e$, was zeigt, dass φ_3 injektiv ist.

- $\mathrm{Im}\varphi_3 \subset \ker\ \psi_3$ war schon vorausgesetzt. Sei also $b'' \in \ker \psi_3$. Da π_2 surjektiv ist, finden wir $b \in B$, so dass $\pi_2(b) = b''$. Wir rechnen

$$e = \psi_3(b'') = \psi_3 \circ \pi_2(b) = \pi_3 \circ \psi_2(b)\,,$$

was aber impliziert, dass $c := \psi_2(b)$ sich schreiben lässt als $i_3(c') = c$. Da ψ_1 surjektiv ist, finden wir ein Urbild $b' \in B'$ in B', $\psi_1(b') = c'$. Wir betrachten nun $x_b := i_2(b')^{-1}b \in B$:

$$\begin{aligned}\pi_2(x_b) &= \pi_2 \circ i_2(b')^{-1}b_2(b) = \pi_2(b) = b'' \\ \psi_2(x_b) &= \psi_2 i_2(b')^{-1}\psi_2(b) = i_3\psi_1(b')^{-1}c \\ &= i_3(c')^{-1}c = c^{-1}c = e.\end{aligned}$$

Wegen der letzten Gleichung gibt es $a \in A$, so dass $\varphi_2(a) = x_b$. Setze $a'' = \pi_1(a)$ und rechne

$$\varphi_3(a'') = \varphi_3 \circ \pi_1(a) = \pi_2 \circ \varphi_2(a) = \pi_2(x_b) = b''\,.$$

Daher $b'' \in \mathrm{Im}\varphi_3$, auch die rechte Spalte ist exakt.

□

Beispiel 1.13.3. *(Noetherscher Isomorphiesatz)*
Betrachte das folgende kommutierende Diagramm:

$$\begin{array}{lllll} K & \to & H & \to & H/K \quad \text{(ex)} \\ \mathrm{id}\downarrow & \# & \downarrow & \# & \downarrow \\ K & \to & G & \to & G/K \quad \text{(ex)} \\ \downarrow & \# & \downarrow & \# & \downarrow \\ \{e\} & \to & G/H & \overset{\to}{\mathrm{id}} & G/H \quad \text{(ex)} \\ \text{(ex)} & & \text{(ex)} & & \end{array}$$

Als Morphismen treten die natürlichen Inklusionen von Untergruppen und die kanonischen Projektionen auf Faktorgruppen auf, soweit nicht anders beschriftet. Damit sind aber die mit (ex) markierten Zeilen und Spalten exakt. Wir können somit das Neunerlemma anwenden und lernen, dass auch die Sequenz

$$H/K \to G/K \to G/H$$

exakt ist, woraus die Aussage des Noetherschen Isomorphiesatzes folgt:

$$(G/K)/(H/K) \cong G/H\,.$$

2 Körpererweiterungen

Historisch haben neben anderen die beiden folgenden Fragestellungen die Entwicklung der mathematischen Disziplin Algebra motiviert.

— Die Frage nach der Auflösbarkeit von Gleichungen höherer Ordnung.

— Konstruktionsprobleme mit Zirkel und Lineal.

Letztere sollen uns nun als Orientierung dienen. Zwischendurch werden wir immer wieder auch etwas über Ringe lernen.

2.1 Konstruierbarkeit

Wir untersuchen nun die folgende

Aufgabe : in der Ebene $\mathbb{R}^2$ sollen aus einer Menge M mit Zirkel und Lineal ein weiterer Punkt konstruiert werden.

Es gelten hierfür die folgenden Regeln:

A 1 : Es ist eine Teilmenge $M \subset \mathbb{R}^2$ mit mindestens zwei Punkten vorgegeben, $|M| \geq 2$

A 2 : Durch je zwei konstruierte oder vorgegebene Punkte kann man eine Gerade legen.

A 3 : Um jeden konstruierten oder vorgegebenen Punkt kann man einen Kreis schlagen mit einem Radius, den man als Verbindungsstrecke abgreift.

A 4 : Schnittpunkte von Kreisen mit Kreisen, von Kreisen und Geraden und von Geraden mit Geraden sind konstruierte Punkte.

Wir setzen:

$$\mathcal{A}\, M := \{ P \in \mathbb{R}^2 \mid P \quad \text{ist aus } M \text{ mit Zirkel und Lineal konstruierbar.} \}$$

Wir betrachten nun die folgenden klassischen Probleme, die schon seit der Antike bekannt sind:

Beispiele 2.1.1.

1. *Winkeldrittelung:*
   Gegeben sei ein Winkel φ durch seine Spitze O und zwei Punkte P, Q auf seinen Schenkeln mit gleichem Abstand zu O. Sei X ein Punkt auf dem Kreis um O durch P, der einem Drittel des Winkels φ entspricht. Die Frage der Konstruierbarkeit der Winkeldrittelung ist dann die Frage: ist $X \in \mathcal{A}\, \{O, P, Q\}$?

2. *Konstruktion des regulären n–Ecks:*
   Hierzu identifizieren wir die reelle Ebene $\mathbb{R}^2$ *mit den komplexen Zahlen* $\mathbb{C}$. *Einen Vertex des n-Ecks legen wir auf* $1 \in \mathbb{C}$, *den Schwerpunkt des n-Ecks auf* 0. *Die Frage nach der Konstruierbarkeit des n-Ecks ist dann die Frage: Ist* $e^{2\pi \mathrm{i}/n} \in \mathcal{A}\ \{0,1\}$?

3. *Quadratur des Kreises:*
   Finde ein Quadrat mit gleicher Fläche wie die eines vorgegebenen Kreises. Zu lösen ist $x^2 = \pi r^2$ *für gegebenes* r. *Finde Punkte* P, Q *so dass* $\overline{PQ} = r$ *und konstruiere* X *so dass* $\overline{PX} = r\sqrt{\pi}$. *Hier ist also die Frage: ist* $X \in \mathcal{A}\ \{P, Q\}$?

4. *Delisches Problem:*
   Konstruiere einen Würfel mit doppeltem Volumen.

Bemerkung 2.1.2.
Die algebraischen Grundoperationen sind konstruktiv beschreibbar. Sei $M \subset \mathbb{C}$ *beliebige Teilmenge mit* $0, 1 \in M$. *Dann gilt*

1) $\mathrm{i} \in \mathcal{A}\ M$

2) $z \in \mathcal{A}M \Rightarrow \overline{z}, \mathrm{Re}\ (z), \mathrm{Im}\ (z) \in \mathcal{A}\ M$.

3) $z_1, z_2 \in \mathcal{A}\ M \Rightarrow z_1 + z_2, -z_1 \in \mathcal{A}\ M$

4) $z_1, z_2 \in \mathcal{A}\ M \Rightarrow z_1 z_2 \in \mathcal{A}\ M; \quad z \in \mathcal{A}\ M, z \neq 0 \Rightarrow z^{-1} \in \mathcal{A}\ M$.

Beweis.

1) Mittelsenkrechte auf $[-1, 1]$.
2) Lot von z auf die Koordinatenachsen.
3) Ziehe einen Kreis um z_1 mit Radius $r_2 = |z_2|$ und einen Kreis um z_2 mit Radius $r_1 = |z_1|$. Ein Schnittpunkt ist die Summe $z_1 + z_2$. Das negative erhält man durch Punktspiegelung.
4) Wegen $z_1 z_2 = (a_1 a_2 - b_1 b_2) + \mathrm{i}(a_1 b_2 + b_1 a_2)$ und der Konstruierbarkeit der Real- und Imaginärteile a_i, b_i reicht es aus, die Behauptung nur für reelle Zahlen zu zeigen. Dort folgt sie aus dem Strahlensatz. Beim Inversen beachtet man, dass $z^{-1} = (z\overline{z})^{-1}\overline{z}$, so dass es auch wieder ausreicht, die Behauptung für reelle Zahlen zu zeigen. Wiederum folgt sie aus dem Strahlensatz.

Insbesondere sehen wir, dass $\mathcal{A}\ M \subset \mathbb{C}$ ein Teilkörper der komplexen Zahlen ist, der $\mathbb{Q}$ enthält. □

Lemma 2.1.3.
Der Körper $\mathcal{A}$ M ist quadratisch abgeschlossen, d.h. für $z \in \mathbb{C}$ gilt: mit $z \in \mathcal{A}$ M ist auch $\pm\sqrt{z} \in \mathcal{A}$ M.

Beweis.
Da man Winkel mit Zirkel und Lineal halbieren kann, reicht es wiederum aus, die Behauptung für $r = |z|$ zu zeigen. Fixiere die Punkte -1 und $+r$ auf der reellen Achse und schlage den Thaleskreis über dem Interval $[-1, r]$. Dessen Schnittpunkt ix mit der rein imaginären Achse defininiert nach Thales ein rechtwinkliges Dreieck $(-1, r, \mathrm{i}x)$. Der Höhensatz, angewandt auf dieses Dreieck liefert $x^2 = 1 \cdot r$. Also ist die Quadratwurzel von r mit Zirkel und Lineal konstruierbar. □

Zur Algebraisierung des Problems führen wir die folgenden Begriffe ein:

Definition 2.1.4.
(i) Sei E ein Körper, $k \subseteq E$ Teilkörper. E heißt Erweiterungskörper von k.

(ii) Sei $A \subseteq E$ eine beliebige Teilmenge. Wir setzen

$$k(A) = \bigcap F$$

wobei der Schnitt über alle Teilkörper F von E geht, die k und A enthalten. $k(A)$ heißt der von A über k erzeugte Teilkörper von E. Man sagt auch, dass $k(A)$ durch Adjunktion der Elemente von A zu k entsteht.

Ist $A = \{\alpha_1 \dots \alpha_m\} \subset E$ endlich, so schreiben wir auch

$$k(A) = k(\alpha_1, \dots, \alpha_m)$$

Offenbar ist $k(A)$ der kleinste Teilkörper von E, der k und A enthält. Beispiel: Sei $E = \mathbb{C}$, dann ist $\mathbb{Q}(i) = \{a + bi, |a, b \in \mathbb{Q}\}$.

Definition 2.1.5.
Sei E ein Erweiterungskörper eines Körpers k.

(i) Man sagt, E entsteht aus k durch Adjunktion einer Quadratwurzel, wenn es ein $\omega \in E$ gibt mit

$$\omega^2 \in K \quad \textit{und} \quad E = k(\omega)$$

ω heißt Quadratwurzel des Elements $v \in k$, wenn

$$v = \omega^2 \quad \textit{gilt.}$$

(ii) E entsteht aus k durch sukzessive Adjunktion von Quadratwurzeln, wenn es eine endliche Kette

$$k = k_0 \subset k_1 \subset \ldots \subset k_m = E$$

von Teilkörpern gibt, so dass k_i durch Adjunktion einer Quadratwurzel aus k_{i-1} entsteht.

Satz 2.1.6.
Sei $M \subset \mathbb{C}$ eine Menge mit $0, 1 \in M$. Setze $K := \mathbb{Q}(M \cup \overline{M})$, wobei $\overline{M} = \{\overline{z} \in \mathbb{C} | z \in M\}$ die zu M komplex konjugierten Elemente enthält. Dann sind für $z \in \mathbb{C}$ folgende Aussagen äquivalent:

(i) $z \in \mathcal{A}\ M$, d.h. z ist konstruierbar aus M.

(ii) z liegt in einem Teilkörper von E von $\mathbb{C}$ der K enthält und aus K durch sukzessive Adjunktion von Quadratwurzeln entstanden ist.

Beweis.
(ii) $\Rightarrow$ (i). Nach Voraussetzung gibt es eine Kette

$$K = K_0 \subset \cdots \subset K_m = E$$

so dass

$$K_i = K_{i-1}(\omega_i) \quad \omega_1^2 \in K_{i-1}$$

wobei der Körper E die komplexe Zahl z enthält.

Wegen Bemerkung 2.1.2 ist $K \subset \mathcal{A}\ M$. Da $\omega_0^2 \in K_0$, ist wegen der quadratischen Abgeschlossenheit 2.1.3 auch $\omega_0 \in \mathcal{A}\ M$. Da $\mathcal{A}\ M$ ein Körper ist, folgt $K_1 = K_0(\omega_0) \subset \mathcal{A}\ M$. Per Induktion folgt nun $z \in E \subset \mathcal{A}\ M$.

(i) $\Rightarrow$ (ii). Ohne Beschränkung der Allgemeinheit können wir annehmen, dass z aus M durch Anwendung *eines* Konstruktionsschritts entstanden ist. Dann wenden wir vollständige Induktion auf die Zahl der Konstruktionsschritte an. Zunächst beachten wir, dass aus $M \subset K \subset \mathcal{A}\ M$ folgt, dass $\mathcal{A}\ K = \mathcal{A}\ M$. Wir betrachten jetzt die folgenden drei Fälle getrennt

(a) z ist Schnittpunkt von zwei Geraden $\Rightarrow$ $z \in K$, denn Geradenschnitte führen zu linearen Gleichungssystemen über K, das in K lösbar ist.

(b) z ist Schnittpunkt von Gerade und Kreis $\Rightarrow$

$$\exists\, \omega \in \mathbb{C} \quad \text{mit} \quad \omega^2 \in K \quad z \in K(\omega)$$

Denn der Schnitt von Gerade und Kreis führt auf quadratische Gleichungen über K. Die Lösungen liegen also in einem quadratischen Erweiterungskörper.

(c) Auch der Schnitt zweier Kreise führt auf quadratische Gleichungen über K und daher zur gleichen Körpererweiterung wie bei (b). Also liegt in jedem Fall z in einem Teilkörper K_1 von $\mathbb{C}$, der aus K durch die Adjunktion von Quadratwurzeln hervorgegangen ist.

□

Daher sind die vier klassischen Probleme äquivalent zu folgenden algebraischen Problemen:

(a) Für die Winkeldrittelung betrachte $\varphi \in \mathbb{R}$ und $K = \mathbb{Q}(e^{\mathrm{i}\varphi})$. Das algebraische Problem ist dann: ist $e^{\mathrm{i}\varphi/3}$ in einem Teilkörper von $\mathbb{C}$ enthalten, der durch sukzessive Adjunktion von Quadratwurzeln aus K entstanden ist?

(b) Delisches Problem: dieselbe Frage für $\sqrt[3]{2}$ über $\mathbb{Q}$.

(c) Reguläres n–Eck: dieselbe Frage für $e^{2\pi\mathrm{i}/n}$ über $\mathbb{Q}$.

(d) Quadratur des Kreises: dieselbe Frage für π über $\mathbb{Q}$.

Definition 2.1.7.
Sei K Körper, E Erweiterungskörper von K. Durch Einschränkung der Multiplikation $E \times E \to E$ im Körper E auf $K \times E \to E$ kann man E als Vektorraum über K auffassen (tatsächlich sogar als Algebra über K). Die natürliche Zahl

$$[E : K] = \dim_K E$$

heißt (Körper-)Grad von E über K.

Beispiel 2.1.8.
Der Körpergrad der komplexen Zahlen über den rationalen Zahlen ist offenbar zwei, $[\mathbb{C} : \mathbb{R}] = 2$, ähnlich $[\mathbb{Q}(i) : \mathbb{Q}] = 2$. Dagegen ist $[\mathbb{R} : \mathbb{Q}] = \infty$, da die reellen Zahlen überabzählbar sind.

Lemma 2.1.9.
Sei E ein Erweiterungskörper von K und in K gelte $1+1 \neq 0$. Dann gilt

$$[E:K]=2 \iff E \text{ entsteht aus } K \text{ durch Adjunktion einer Quadratwurzel, d.h. es gibt } \omega \in E \backslash K \quad E=K(\omega) \quad \omega^2 \in K\,.$$

Beweis.
"$\Rightarrow$" Sei $\alpha \in E\backslash K$. Dann ist $\{1,\alpha\}$ eine K–Basis von E. Es gibt also eine nicht-triviale Relation

$$\alpha^2 + p\alpha + q = 0 \qquad \text{mit} \quad p,q \in K\,, \tag{12}$$

wobei wir ohne Beschränkung der Allgemeinheit annehmen dürfen, dass der Koeffizient von α^2 gleich eins ist. Da in K gilt, dass $2 \neq 0$, definieren wir $\omega = \alpha + \frac{p}{2}$. Dann ist wegen (12)

$$\omega^2 = \frac{p^2}{4} - q \in K$$

und $E = K(\alpha) = K(\omega)$. Also entsteht E durch Adjunktion der Quadratwurzel ω.
"$\Leftarrow$" Sei $E = K(\omega)$ mit $\omega^2 = d \in K$, $\omega \in E$. Offenbar ist

$$E' = \{a + b\omega | a,b \in K\}$$

ein Teilkörper von E, der ω und K enthält, also $E' \supseteq E = K(\omega)$, da $K(\omega)$ der kleinste solche Körper ist. Umgekehrt ist aber auch $E' \subset E$, also $E = E'$, und der Grad ist $[E:K] = [E':K] = 2$. □

Satz 2.1.10. *(Gradformel)*
Man betrachte einen Körperturm, d.h.

$$\begin{array}{c} E \\ | \\ F \\ | \\ K \end{array}$$

, was heißt, dass F Unterkörper von E und K seinerseits Unterkörper von F ist. In dieser Situation gilt für die Körpergrade: $[E:K] = [E:F] \cdot [F:K]$

Beweis.
Für unendlichen Körpergrad ist die Aussage trivial. Sei also

$$[E:F] = n \quad \text{und} \quad [F:K] = m\,.$$

Dann gibt es Vektorraumisomorphismen von F- bzw. K-Vektorräumen

$$E \cong F^n \quad \text{und} \quad F \cong K^m$$

und damit den folgenden Isomorphismus von K-Vektorräumen:

$$E \cong F^n \cong (K^m)^n = K^{m \cdot n}\,.$$

Wir bemerken außerdem: Ist

$$\begin{array}{ll} \{\alpha_j | j = 1 \ldots n\} & \text{Basis von} \quad E \text{ über } F \\ \{\beta_i | i = 1 \ldots m\} & \text{Basis von} \quad F \text{ über } K \end{array}$$

so ist $\{\alpha_j \beta_i\}$ Basis von E über K. □

Korollar 2.1.11.

(i) Entsteht E aus K durch sukzessive Adjunktion von Quadratwurzeln, so gilt

$$[E : K] = 2^m \qquad m \in \mathbb{N}$$

(ii) Sei $K = \overline{K} \subseteq \mathbb{C}$ ein Teilkörper von $\mathbb{C}$. Damit $z \in \mathbb{C}$ aus K konstruierbar ist, muss notwendigerweise gelten

$$[K(z) : K] = 2^r \qquad r \in \mathbb{N}$$

Beweis.

(i) Lemma 2.1.9 und die Gradformel.

(ii) Nach Satz 2.1.6 ist $z \in \mathcal{A}K$ in einem Erweiterungskörper E von K enthalten, der durch sukzessive Adjunktion von Quadratwurzeln entstanden ist. Mit Hilfe der Gadformel und des Resultats aus (i) finden wir:

$$2^m = [E : K] = [E : K(z)][K(z) : K]$$

woraus folgt

$$[K(z) : K] = 2^r \qquad 0 \leq r \leq m\,.$$

□

2.2 Algebraische Körpererweiterungen

Wesentlich in den Konstruktionsproblemen war, Lösungen von quadratischen Gleichungen zu finden. Wir wollen dies auf allgemeine polynomiale Gleichungen verallgemeinern.

Definition 2.2.1.
Sei E/K eine Körpererweiterung.

Ein Element $\alpha \in E$ heißt algebraisch über K, falls es ein Polynom $f(X) \neq 0$ gibt in dem Polynomring

$$K[X] = \left\{ \sum_{i=0}^{n} a_i X^i \mid a_i \in K, n \in \mathbb{N} \right\}$$

mit $f(\alpha) = 0$.
Ist α nicht algebraisch über K, so heißt α transzendent über K.

Bemerkung 2.2.2.

1) *Im Spezialfall $K = \mathbb{Q}$ und $E = \mathbb{C}$ nennt man algebraische bzw. transzendente Elemente algebraische bzw. transzendente Zahlen. Die Menge der algebraischen Zahlen ist abzählbar, die Menge der transzendenten Zahlen ist überabzählbar.*

2) *Wir werden später sehen: ist $M \subset \mathbb{C}$, $0, 1 \in M$, $z \in \mathcal{A}M$, so ist z algebraisch über $K = \mathbb{Q}(M \cup \overline{M})$.*

3) *Es gilt (Lindemann 1882): π ist transzendent über $\mathbb{Q}$. Also ist die Quadratur des Kreises unmöglich.*

Satz 2.2.3.
Sei E/K Körpererweiterung, $\alpha \in E$ algebraisch über K. Dann ist der Körpergrad von $K(\alpha)$ endlich, $[K(\alpha) : K] < \infty$.

Beweis.

Da α algebraisch ist, ist es Nullstelle eines nicht–trivialen Polynoms

$$f(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_0 \in K[X]\,.$$

Indem wir zu einem Vielfachen des Polynoms übergehen, können wir annehmen, dass der höchste Koeffizient auf Eins normiert ist, $a_n = 1$. Betrachte den K–Algebrenhomomorphismus, den sogenannten Einsetzungshomomorphismus

$$\varphi_\alpha : \begin{array}{ccc} K[X] & \to & E \\ X & \mapsto & \alpha \\ \sum_{i=0}^{m} b_i x^i & \mapsto & \sum_{i=0}^{m} b_i \alpha^i \end{array} .$$

(Der Einsetzungshomomorphismus tritt in folgendem wichtigen Sachverhalt der linearen Algebra auf: ein Endomorphismus A eines endlichdimensionalen Vektorräums ist Nullstelle seines charakterstischen Polynoms. Hier wird der Einsetzungshomomorphismus sogar auf den nichtkommutativen Ring der Endomorphismen eines Vektorraeums angewandt.)

Wir wollen das Bild

$$K[\alpha] = \mathrm{Im}\varphi_\alpha = \Big\{ \sum_{i=1}^{m} b_i \alpha^i | b_i \in K, m \geq 0 \Big\}$$

des Einsetzungshomomorphismus untersuchen. Es trägt die algebraische Struktur eines Rings mit Eins. Daher brauchen wir die folgende
□

Definition 2.2.4.

(i) Ein Ring ist eine Menge mit zwei assoziativen Verknüpfungen $(R, +, \cdot)$ derart, dass

- *$(R, +)$ ist abelsche Gruppe, $(R, \cdot)$ ist eine assoziative Verknüpfung.*
- *Es gelten zwei Distributivgesetze*

$$\begin{aligned} a(b+c) &= ab + ac \\ (a+b)c &= ac + bc \end{aligned}$$

Man beachte, dass wir nicht gefordert haben, dass die Multiplikation kommutativ ist. Ist dies der Fall, so heißt der Ring kommutativ. Wir werden überwiegend mit kommutativen Ringen zu tun haben.

(ii) Ein Ring mit Eins oder unitaler Ring ist ein Ring mit einem Element $1 \in R$, so dass $1 \cdot a = a \cdot 1 = a$ für alle $a \in R$.

Ein wichtiges Beispiel für einen unitalen Ring ist der Ring der Polynome $k[X]$ mit Koeffizienten in einem Körper k. Tatsächlich können wir auch den Ring $R[X]$ der Polynome mit Koeffzienten in einem Ring R betrachten.

(iii) Ein Ringhomomorphismus $\varphi : R \to S$ ist eine Abbildung, für die gilt

$$\begin{aligned} \varphi(a+b) &= \varphi(a) + \varphi(b) \\ \varphi(ab) &= \varphi(a)\varphi(b)\,. \end{aligned}$$

Für einen unitalen Ringhomomorphismus fordert man zusätzlich

$$\varphi(1) = 1\,.$$

(iv) *Ein kommutativer, nullteilerfreier Ring R (d.h. ein Ring, in dem $ab = 0$ impliziert, dass $a = 0$ oder $b = 0$) mit Eins ($1 \neq 0$) heißt* Integritätsring. *R heißt auch* integer.

(v) *Eine* Algebra $(A, +, \cdot)$ *über einem Körper K ist ein K-Vektorraum, der auch ein Ring ist und für den die Ringmultiplikation K-bilinear ist:*

$$(\lambda a)b = a(\lambda b) = \lambda(ab) \qquad a, b \in A, \lambda \in K\,.$$

Eine Algebra mit Eins hat zusätzlich ein neutrales Element für die Multplikation.

(vi) *Alle Algebren und Ringe in der Vorlesung Algebra I werden kommutativ sein und ein Einselement haben. Gelegentlich werden wir daher nicht immer explizit "mit Eins" dazusagen.*

Lemma 2.2.5.
Ist ein Integritätsring R eine endlich-dimensionale K–Algebra, so ist R ein Körper.

Beweis.
Sei $a \in R, a \neq 0$. Betrachte

$$\begin{array}{rccc} h_a: & R & \to & R \\ & x & \mapsto & ax \end{array}$$

Die Abbildung h_a ist ein Endomorphismus des K-Vektorraums R; sie ist injektiv, da R nullteilerfrei ist:

$$ax = ay \;\Rightarrow\; a(x - y) = 0 \;\Rightarrow\; x = y\,.$$

Da $\dim_K R < \infty$, ist h_a als injektive Selbstabbildung von R auch surjektiv. Insbesondere gibt es eine $b \in R$ mit $ab = 1$. □

Weiter im Beweis von 2.2.3:

$$K[\alpha] = \Big\{ \sum_{i=1}^{m} b_i \alpha^i | b_i \in K, m \geq 0 \Big\}$$

ist als Teilring des Körpers E sicher integer und auch eine K-Algebra. Wegen

$$\alpha^n = -a_{n-1}\alpha^{n-1} - a_{n-2}\alpha^{n-2} - \cdots - a_0$$

können wir Potenzen von α höher als n ersetzen und finden $K[\alpha] = \{g(\alpha) | g(X) \in K[X] \text{ mit } \operatorname{grad} g \leq n-1\}$. Somit ist $\dim_K K[\alpha] \leq n$.

Wegen Lemma 2.2.5 ist $K[\alpha]$ sogar ein Körper, also $K[\alpha] = K(\alpha)$. Somit finden wir

$$[K(\alpha) : K] \leq n < \infty\,.$$

Definition 2.2.6.

(i) Ein Polynom heißt normiert, wenn der höchste Koeffizient Eins ist.

(ii) Erinnerung an die lineare Algebra (siehe z.B. Kowalsky, Lineare Algebra, p.78): Sei A ein Endomorphismus eines endlich–dimensionalen Vektorraums V. Das Minimalpolynom von A ist das eindeutig bestimmte normierte Polynom kleinsten Grades, welches A als Nullstelle besitzt.

(iii) Sei nun α ein algebraisches Element über K. Die Multiplikation mit α definiert einen Endomorphismus h_α von $K(\alpha)$:

$$\begin{array}{rccc} h_\alpha: & K(\alpha) & \to & K(\alpha) \\ & x & \mapsto & \alpha x \end{array}$$

Das Minimalpolynom $f = \min_K(\alpha)$ von h_α heißt Minimalpolynom von α über K. Es ist das eindeutige normierte Polynom kleinsten Grades, das α als Nullstelle besitzt.

Satz 2.2.7.

Sei E/K eine Körpererweiterung und $\alpha \in E$ algebraisch über K mit

$$\operatorname{grad} \min_K(\alpha) = n\,.$$

Dann ist

$$\{1, \alpha, \alpha^2, \ldots \alpha^{n-1}\}$$

eine Basis von $K(\alpha)$ über K. Insbesondere ist

$$[K(\alpha) : K] = \operatorname{grad} \min_K(\alpha)\,.$$

D.h. der Körpergrad des durch Adjunktion von α erhaltenen Körpers ist gleich dem Grad des Minimalpolynoms.

Beweis.

Sei $\min_K(\alpha) = f(X) = X^n + \cdots + a_0$. Aus dem Beweis von 2.2.3 folgt schon, dass $[K(\alpha) : K] \leq n$. Es reicht also aus zu zeigen, dass $\{1, \alpha, \alpha^2, \ldots \alpha^{n-1}\}$ linear unabhängig über K ist. Sei also

$$\sum_{i=0}^{n-1} c_i \alpha^i = 0 \text{ mit } c_i \in K, \text{ mindestens ein } c_i \neq 0$$

eine nicht-triviale Relation. Dann besitzt das nicht-verschwindende Polynom

$$g(X) := \sum_{i=0}^{n-1} c_i X^i$$

α als Nullstelle und hat grad $g < n$, also kleineren Grad als das Minimalpolynom. Dies ist ein Widerspruch. Damit ist aber

$$[K(\alpha) : K] = n\,.$$

□

Definition 2.2.8.
(i) Eine Körpererweiterung E/K heißt algebraisch, wenn jedes $\alpha \in E$ algebraisch über K ist.

(ii) Eine Körpererweiterung heißt endlich, falls $[E : K] < \infty$ ist.
Beispiele: $\mathbb{C}/\mathbb{R}$ *ist endlich*
$\mathbb{R}/\mathbb{Q}$ *ist nicht algebraisch (ohne Beweis).*

Satz 2.2.9.
Ist E/K endlich, so ist E/K algebraisch und für jedes $\alpha \in E$ gilt:

$$\text{grad } \min_K(\alpha) \text{ teilt } [E : K]\,.$$

Bemerkung: Die Umkehrung ist falsch: nicht jede algebraische Körpererweiterung ist unbedingt endlich.

Beweis.
Sei $[E : K] = n < \infty$ und $\alpha \in E \backslash K$. Dann ist die Menge

$$\{1, \alpha, \alpha^2, \ldots \alpha^n\}$$

als Menge von $n + 1$ Vektoren im n-dimensionalen K-Vektorraum E linear abhängig über K. Es gibt also $a_i \in K$, die nicht alle 0 sind, mit

$$\sum_{i=0}^{n} a_i \alpha^i = 0\,.$$

Also ist α algebraisch. Ferner gilt mit 2.2.7

$$\text{grad } \min_K(\alpha) = [K(\alpha) : K] \mid [E : K]$$

wegen der Gradformel. □

Korollar 2.2.10.
(i) Sei E/K Körpererweiterung und $\alpha \in E$ algebraisch über K. Dann ist $K(\alpha)/K$ algebraisch.

(ii) Sei $0, 1 \in M \subset \mathbb{C}$ und $K = \mathbb{Q}(M \cup \overline{M})$. Dann ist $\mathcal{A}M/K$ algebraisch.

(iii) E/K ist endlich $\Longleftrightarrow$ Es gibt endlich viele über K algebraische Elemente $\alpha_1 \dots \alpha_m$ aus E, so dass $E = K(\alpha_1, \dots, \alpha_m)$.

Beweis.

(i) Nach Satz 2.2.3 ist die Körpererweiterung $K(\alpha)/K$ endlich und damit nach Satz 2.2.9 auch algebraisch.

(ii) $z \in \mathcal{A}M \Rightarrow [K(z) : K] < \infty$. Mit 2.2.9 folgt, dass z algebraisch über K ist.

(iii) "$\Rightarrow$" Sei $\{\alpha_1 \dots \alpha_m\}$ eine K–Basis von E. Dann ist $E = K(\alpha_1, \dots \alpha_m)$ und nach Satz 2.2.9 ist E algebraisch.

"$\Leftarrow$" durch Induktion nach m. Der Induktionsanfang ist durch 2.2.7 gegeben. Sei also $K' = K(\alpha_1 \dots \alpha_{m-1})$, dann ist nach Induktionsannahme K'/K endlich. Wir haben $E = K'(\alpha_m)$ mit α_m algebraisch über K. Dann ist aber α_m erst recht algebraisch über K'. Damit ist auch $[E : K'] < \infty$. Aus der Gradformel schließen wir, dass $[E : K] < \infty$.

□

Definition 2.2.11.

(i) Sei E/K eine Körpererweiterung. Ein Körper L mit $L \subseteq E, K \subseteq L$ heißt Zwischenkörper.

(ii) Sei eine Körpererweiterung E/K vorgegeben. Betrachte

$$F := \{\alpha \in E : \alpha \text{ algebraisch über } K\}.$$

Dann ist F ein Zwischenkörper von E/K und heißt algebraischer Abschluss. Insbesondere ist die Menge $\overline{\mathbb{Q}}$ aller algebraischen Zahlen in $\mathbb{C}$ ein Teilkörper von $\mathbb{C}$.

Beweis.

Wir müssen noch zeigen, dass F ein Körper ist. Das ist schwer nur mit der definierenden Eigenschaft algebraischer Elemente zu machen: weiss man, dass α Nullstelle eines Polynoms f und β Nullstelle eines Polynoms g ist, so hat man noch kein Polynom, für das $\alpha + \beta$ oder $\alpha\beta$ Nullstellen sind. Deshalb ist es wesentlich, dass Algebraizität eine *Endlichkeitseigenschaft* ist.

Seien $\alpha, \beta \in F$, also algebraisch über K. Nach 2.2.10 (iii) ist $K(\alpha, \beta)$ endlich über K. Jedes $\gamma \in K(\alpha, \beta)$ ist dann algebraisch nach 2.2.9, also

$$K(\alpha, \beta) \quad \subset \quad F\,.$$

Insbesondere liegen mit α und β auch $\alpha+\beta, \alpha-\beta, \alpha\beta$ und für $\alpha \neq 0$ auch α^{-1} im algebraischen Abschluss F. Dieser ist also ein Teilkörper von E, der K enthält. □

Satz 2.2.12. *(Transitivität algebraischer Erweiterungen)*

Sei L ein Zwischenkörper einer Körpererweiterung E/K. Dann gilt

$$E/K \text{ algebraisch} \iff E/L \text{ und } L/K \text{ algebraisch}.$$

Beweis.

"$\Rightarrow$" klar: Dass L algebraisch über K ist, heißt, dass jedes $\alpha \in L$ Nullstelle eines Polynoms mit Koeffizienten in K ist. Aber das gilt sogar für alle $\alpha \in E$. Dass E algebraisch über L ist, heißt, dass jedes $\alpha \in E$ Nullstelle eines Polynoms mit Koeffizienten in L ist. Aber wir finden sogar schon ein Polynom mit Koeffizienten in K.

"$\Leftarrow$": Sei umgekehrt $\beta \in E$ algebraisch über L. Betrachte das Minimalpolynom von β über L:

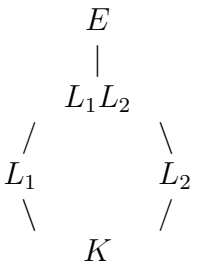
$$\min_L(\beta) = \sum_{i=0}^{n} \alpha_i X^i \quad \alpha_i \in L \quad \alpha_n = 1\,.$$

Offenbar ist dann β bereits algebraisch über dem kleineren Körper $F = K(\alpha_1, \ldots \alpha_{n-1}) \subset L$, wobei nach dem zweiten Teil der Voraussetzung alle α_i algebraisch über K sind. Mit Hilfe von 2.2.10(iii) folgt, dass $[F : K] < \infty$, mit Hilfe der Gradformel daraus wiederum $[F(\beta) : K] < \infty$. Damit ist der Körper $F(\beta)$ endlich über K, also algebraisch über K, also ist β als Element von $F(\beta)$ algebraisch. □

Definition 2.2.13.
Sei E/K eine Körpererweiterung. Der Zwischenkörper

$$L_1L_2 := L_1(L_2) = L_2(L_1)$$

heißt das <u>Kompositum</u> von L_1 und L_2 in E.



Satz 2.2.14.
In dieser Situation gilt:

(a) Ist die Körpererweiterung L_1/K algebraisch, so ist auch L_1L_2 über L_2 algebraisch.

(b) Ist die Körpererweiterung L_1/K endlich, $[L_1 : K] < \infty$, so ist auch L_1L_2 über L_2 endlich und $[L_1L_2 : L_2] \leq [L_1 : K]$.

(c) Sind sowohl L_1/K als auch L_2/K algebraisch, so ist das Kompositum L_1L_2 über K algebraisch.

(d) Sind sowohl L_1/K als auch L_2/K endlich, so ist das Kompositium L_1L_2 über K endlich.
Sind die Körpergrade $[L_1 : K]$ und $[L_2 : K]$ überdies teilerfremd, so gilt

$$[L_1L_2 : K] = [L_1 : K][L_2 : K] \text{ und } L_1 \cap L_2 = K\,.$$

Beweis.

(a) Ist L_1/K algebraisch, so sind die Elemente von L_1 erst recht über L_2 algebraisch. Das Kompositum geht also durch Adjunktion algebraischer Elemente aus L_2 hervor und ist daher über L_2 algebraisch.

(b) Offenbar ist

$$R := \Big\{ \sum_{\text{endlich}} a_i b_i | a_i \in L_1, b_i \in L_2 \Big\}$$

ein Teilring von E, der L_1 und L_2 enthält. Sei $\{\gamma_\lambda\}$ eine Basis von L_1/K. Dann ist $\{\gamma_\lambda\}$ auch ein Erzeugendensystem (aber nicht unbedingt eine Basis!) des L_2–Vektorraums R. Somit ist

$$[R : L_2] \leq [L_1; K]\,.$$

Ist also $[L_1 : K]$ endlich, so ist auch $\dim_{L_2} R < \infty$. Nach Lemma 2.2.5 ist daher R ein Körper. Also ist $R = L_1L_2$ und wir haben die gewünschte Abschätzung für den Körpergrad des Kompositums L_1L_2.

(c) Folgt aus Satz 2.2.12 und der Beobachtung, dass im Körperturm $L_1L_2 - L_2 - K$ die erste Erweiterung algebraisch ist nach Teil (a) dieser Bemerkung und L_2 über K nach Voraussetzung algebraisch ist.

(d) Nach der Gradformel und Abschätzung (b) gilt

$$[L_1L_2 : K] = [L_1L_2 : L_2][L_2 : K] \leq [L_1 : K][L_2 : K]\,.$$

Ferner teilen die Grade der Zwischenkörper $[L_i : K]$ nach der Gradformel $[L_1L_2 : K]$. Sind also diese Grade teilerfremd, so teilt auch ihr Produkt $[L_1 : K][L_2 : K]$ den Körpergrad $[L_1L_2 : K]$, woraus die behauptete Gleichheit folgt. Die Aussage, dass $L_1 \cap L_2 = K$ kommt als Übungsaufgabe.

□

2.3 Einfache Erweiterungen

Definition 2.3.1.
(i) Eine Körpererweiterung E/K heißt einfach, oder primitiv, falls es ein Element $\alpha \in E$ gibt, so dass $E = K(\alpha)$.

(ii) $\alpha \in E$ heißt dann primitives Element von E/K.

Bemerkung 2.3.2.
Sei E/K eine Körpererweiterung, $\alpha \in E$. Dann sind äquivalent

(i) α ist algebraisch

(ii) $K(\alpha) = K[\alpha]$

(iii) $K[\alpha]$ ist ein Körper.

Beweis: (i) $\Rightarrow$ (ii) folgt aus dem Beweis von 2.2.3.
(ii) $\Rightarrow$ (iii) ist klar, da $K(\alpha)$ ein Körper ist.
(iii) $\Rightarrow$ (i) folgt daher, dass dann α^{-1} in $K[\alpha]$ liegt, also sich als Polynom in α schreiben lässt: $\alpha^{-1} = p(\alpha)$. Damit ist aber α Nullstelle des Polynoms $Xp(X) - 1$, also algebraisch.

Wir werden einfache Erweiterungen durch Minimalpolynome primitiver Elemente studieren. Da Polynome einen Ring bilden, brauchen wir einige Information über Ringe. Ebenso wie die normalen Untergruppen besonders wichtige Untergruppen sind, [1] brauchen wir eine ausgezeichnete Klasse von Unterringen.

Definition 2.3.3.
Sei R ein beliebiger Ring mit 1. Eine nicht–leere Teilmenge I von R heißt (zweiseitiges) Ideal von R, wenn

[1] Auf französisch heißen Normalteiler sogar sogar "sousgroupes distingués".

(i) $a, b \in I \Rightarrow a + b \in I$

(ii) $a \in I, x \in R \Rightarrow ax, xa \in I$.

Somit sind Ideale insbesondere Unterringe und additive Untergruppen.

Bemerkung 2.3.4.
(i) Ist $\varphi : R \to R'$ *ein Ringhomomorphismus von Ringen mit Eins, dann ist*

$$\ker \varphi = \{x \in R | \varphi(x) = 0\}$$

ein Ideal.

(ii) Ist $I \subset R$ *ein Ideal in einem Ring* R *mit Eins, so ist* I *der Kern eines Ringhomomorphismus von* R *in einen Ring* R'. *Dazu brauchen wir die folgende*

Definition 2.3.5.
Sei R *Ring mit Eins und* I *ein Ideal in* R. *Betrachte die Äquivalenzrelation*

$$a \sim b \iff a - b \in I$$

Schreibweise für $a \sim b : a \equiv b \bmod I$.
Die Menge der Äquivalenzklassen

$$R/I = \{\overline{a} = \{a' \in R : a' \sim a\}\}$$

ist ein Ring durch $\begin{aligned} \overline{a} + \overline{b} &:= \overline{a + b} \\ \overline{a}\overline{b} &:= \overline{ab}. \end{aligned}$
R/I *heißt der* Restklassenring *modulo dem Ideal* I. *Die Abbildung*

$$\begin{array}{rccc} \pi : & R & \to & R/I \\ & a & \mapsto & \overline{a} \end{array}$$

heißt Restklassenabbildung *oder kanonische Abbildung von* R *auf* R/I. *Es ist* $\ker \pi = I$.

Bemerkung 2.3.6.
(i) Es gibt einen Isomorphiesatz auch für Ringe: ein Ringhomomorphismus

$$\varphi : R \to R'$$

induziert einen Isomorphismus von Ringen

$$\tilde{\varphi} : R/\ker \varphi \xrightarrow{\sim} \text{Im } \varphi\,.$$

(ii) Beispiel: sei E/K eine Körpererweiterung und $\alpha \in E$. Dann ist

$$\begin{array}{rcl} \varphi_\alpha : \ K[X] & \to & K[\alpha] \subset E \\ X & \mapsto & \alpha \end{array}$$

ein Ringhomomorphismus, der Einsetzungshomomorphismus. Sein Kern

$$I_\alpha = \ker \varphi_\alpha = \{g \in K[X] \,|\, g(\alpha) = 0\}$$

ist ein (zweiseitiges) Ideal, das Verschwindensideal in α.

$$\begin{array}{rcl} K[X]/I_\alpha & \to & K[\alpha] \\ X \bmod I_\alpha & \mapsto & \alpha \end{array}$$

ist dann ein Isomorphismus von K–Algebren.

(iii) Sei E/K eine Körpererweiterung und $\alpha \in E$. Dann sind äquivalent

- *(a) α genügt keiner algebraischen Relation über K, d.h. aus $f(\alpha) = 0$ für ein Polynom $f \in K[X]$ folgt $f = 0$.*
- *(b) α ist transzendent*
- *(c) $K[X] \cong K[\alpha]$*
- *(d) $K[\alpha]$ ist kein Körper.*

Definition 2.3.7.

(i) Sei R ein kommutativer Ring mit Eins. Dann heißt

$$R^\times = \{x \in R | \exists \ y \in R : xy = 1\}$$

die Einheitengruppe des Rings R. Die Verknüpfung ist hierbei die Multiplikation. Ist der Ring $R = K$ sogar ein Körper, so gilt $R^\times = K \backslash \{0\}$.

(ii) Sei R kommutativer Ring mit Eins. Setze für jedes $a \in R$

$$(a) = Ra = \{ca | c \in R\}\,.$$

(a) ist ein Ideal in R, das von a in R erzeugte Hauptideal. Zur Vereinfachung der Bezeichung schreiben wir auch $x = y \mod a$ für $x = y \bmod (a)$ sowie R/a anstelle von $R/(a)$.

Satz 2.3.8.
Sei E/K eine einfache algebraische Körpererweiterung und $\alpha \in E$ ein primitives Element. Sei $f = \min_K(\alpha)$ das Minimalpolynom von α. Dann liefert der Einsetzungshomomorphismus

$$\begin{array}{rcl} K[X] & \to & K[\alpha] = K(\alpha) = E \\ X & \mapsto & \alpha \end{array}$$

einen Algebrenisomorphismus: $K[X]/f \cong K(\alpha)$. Insbesondere wird jedes $g \in K[X]$, das α als Nullstelle hat, $g(\alpha) = 0$, durch das Minimalpolynom geteilt, $f|g$.

Beweis.

Sei $g \in K[X]$ ein Polynom mit Nullstelle α, $g(\alpha) = 0$. Division mit Rest von Polynomen erlaubt, g in der Form zu schreiben

$$g = qf + r \qquad q, r \in K[X] \quad \text{grad } r < \text{ grad } f\,.$$

Setzt man in diese Gleichung α ein, so sieht man, dass $r(\alpha) = 0$ gelten muss. Wegen der Minimalität von des Minimalpolynoms folgt dann aber $r = 0$. Also ist das Verschwindensideal

$$I_\alpha = \{g \in K[X] \mid g(\alpha) = 0\} = K[X]f$$

gleich dem vom Minimalpolynom f erzeugten Hauptideal. □

Wir wollen nun Algebren und Körper aus Idealen in Polynomringen konstruieren. Dafür führen wir die folgende Betrachtung durch: sei $f \in K[X]$ ein beliebiges Polynom, grad $f = n \geq 1$. Dann ist die Restklassenalgebra $K_f := K[X]/f$ eine Algebra über K. Wir haben das folgende Diagramm

$$\begin{array}{rccl} \pi: & g & \mapsto & g \bmod f \\ \pi: & K[X] & \twoheadrightarrow & K_f \\ & \uparrow & \nearrow & \text{injektiv, da grad } f \geq 1 \\ & K & & . \end{array}$$

denn für $a \in K$, aufgefasst als das konstante Polynom in $K[X]$, hat man $\overline{a} = 0$ dann und nur dann, wenn $a \in K[X]f$, was aus Gradgründen nur erfüllt ist, wenn $a = 0$. Also kann der Körper K sogar als Teilkörper der Algebra K_f aufgefasst werden.

Sei betrachten wir nun das Element $\alpha := \pi(X)$ im Restklassenring K_f. Wir haben

$$\pi(g) = g(\alpha) \qquad \forall\ g \in K[X]$$

und π ist der einzige Algebrenhomomorphismus mit dieser Eigenschaft. Insbesondere haben wir

$$0 = \pi(f) = f(\alpha)\,,$$

also ist α eine Nullstelle von f in K_f. Wir haben also eine Algebra konstruiert, nämlich K_f, in der f Nullstellen hat! Es ist aber nicht klar, wann die Algebra K_f auch ein Körper ist. Wir wollen dafür Lemma 2.2.5 anwenden, weshalb wir zunächst die Dimension von der Algebra K_f als K-Vektorraum berechnen wollen und dann sehen, für welche Polynome f die Algebra K_f nullteilerfrei ist.

Lemma 2.3.9.
$\{1, \alpha, \ldots, \alpha^{n-1}\}$ ist eine Basis des K–Vektorraumes K_f. Insbesondere ist $\dim_K K_f = n$.

Beweis.

Sei $g \in K[X]$ ein Polynom, dann ist $\pi(g) = g(\alpha) \in K_f$. Auf diese Weise bekommen wir auch alle Elemente von K_f. Division von Polynomen mit Rest gibt $g = qf + r$ mit grad $r \leq n-1$. Einsetzen von α zeigt, dass $g(\alpha) = r(\alpha)$, also reichen die Polynome vom Grade kleiner als n aus, um alle Elemente in K_f zu beschreiben. Es bleibt zu zeigen, dass $\{1, \alpha, \ldots \alpha^{n-1}\}$ linear unabhängig ist. Sei eine Relation gegeben

$$\sum_{i=0}^{n-1} c_i \alpha^i = 0 \qquad \text{mit} \;\; c_i \in K\,. \tag{13}$$

Betrachte das Polynom $h(X) := \sum_{i=0}^{n-1} c_i X^i \in K[X]$, das offenbar α als Nullstelle hat, $h(\alpha) = 0$. Daraus folgt aber nach Satz 2.3.8, dass h durch das Minimalpolynom f von α geteilt wird. Da aber grad $h <$ grad f, folgt $h = 0$, also müssen alle c_i verschwinden, also ist die Relation (13) trivial. □

Definition 2.3.10.
Ein Polynom $f \in K[X]$ heißt irreduzibel oder Primpolynom, falls grad $f \geq 1$ *und $f = f_1 f_2$ mit $f_1 \in K[X]$ und $f_2 \in K[X]$ impliziert, dass $f_1 \in K$ oder $f_2 \in K$.*

Beispiele 2.3.11.

- *In $\mathbb{C}[X]$ sind nach dem Fundamentalsatz der Algebra die linearen Polynome die irreduziblen Elemente.*

- *In $\mathbb{R}[X]$ sind irreduzibel die linearen Polynome und die Polynome der Form*
$$f(X) = ax^2 + bx + x \quad mit \quad b^2 - 4ac < 0\,,$$
denn diese haben nur komplexe Nullstellen.

Diese Definition für Polynome, also Elemente des Polynomrings, wird in Kapitel 3 in einen allgemeinen ringtheoretischen Rahmen gestellt werden. Das folgende Lemma rechtfertigt dann den Namen *Prim*polynom:

Lemma 2.3.12.
Sei $f \in K[X]$ irreduzibel. Dann gilt

$$f|gh \quad mit \quad g, h \in K[X] \Rightarrow f|g \quad oder \quad f|h.$$

Beweis.

- Wir zeigen zunächst, dass wir annehmen können, dass grad $g <$ grad f. Denn Division von Polynomen mit Rest erlaubt uns zu schreiben
$$g = qf + r \quad \text{mit} \ \ \text{grad}\ r < \text{grad}\ f\,.$$
Teilt nun f das Polynom gh, so teilt f auch $rh = gh - qh \cdot f$. Wenn wir die Aussage für den Fall eines Polynoms vom Grad strikt kleiner als dem von f bewiesen haben, können wir sie nun auf r, h anwenden. Also teilt f das Polynom r oder h. Damit gilt aber $f|g$ oder $f|h$.
- Angenommen, es gibt ein $g \in K[X]$ mit $\text{grad}\, g \ <\ \text{grad}\ f$, so dass die Aussage nicht gilt. Sei g ein Gegenbeispiel minimalen Grades: $f|gh$, aber f teilt weder g noch h. Division mit Rest erlaubt uns zu schreiben $f = sg+t$ mit $\text{grad}\, t <\ \text{grad}\, g$. Dies heißt $th = fh - sgh$, also teilt f auch th.
Da aber grad $t <$ grad g und g ein Gegenbeispiel *minimalen* Grades war, folgt
$$f \quad \text{teilt} \quad t \quad \text{oder} \quad f \quad \text{teilt} \quad h\,.$$
Aber $\text{grad}\, t <\ \text{grad}\, g <\ \text{grad}\, f$, also muss f das Polynom h teilen. Dies aber wiederum ist im Widerspruch zur Annahme, dass g ein Gegenbeispiel war.

□

Satz 2.3.13.
K_f ist ein Körper genau dann, wenn $f \in K[X]$ irreduzibel ist.

Beweis.

- Sei $f \in K[X]$ und K_f ein Körper. Sei $f = f_1 f_2$; daraus folgt

$$f(\alpha) = f_1(\alpha) f_2(\alpha) = 0\,.$$

  K_f ist aber als Körper nullteilerfrei, so dass entweder $f_1(\alpha) = 0$ oder $f_2(\alpha) = 0$ gilt. Damit gilt aber auch entweder $f | f_1$ oder $f | f_2$, also ist f irreduzibel.

- Sei f irreduzibel. Wegen Lemma 2.3.9 und Lemma 2.2.5 reicht es aus zu zeigen, dass K_f nullteilerfrei ist. Sei also $\overline{g}\overline{h} = 0$, was aber gerade heißt, dass f das Polynom gh teilt. Nach Lemma 2.3.12 folgt daraus $f | g$ oder $f | h$. Damit gilt aber

$$\overline{g} = 0 \quad \text{oder} \quad \overline{h} = 0\,,$$

  so dass K_f tatsächlich nullteilerfrei ist.

□

Satz 2.3.14.
Sei E/K eine Körpererweiterung, $\alpha \in E$ ein algebraisches Element über K.

(i) Dann ist $f = \min_K(\alpha)$ ein Primpolynom in $K[X]$.

(ii) Ist umgekehrt $g \in K[X]$ irreduzibel und normiert mit $g(\alpha) = 0$, so ist $g = \min_K(\alpha)$.

Beweis.

(i) Nach 2.3.8 gilt $K_f = K[X]/f \cong K(\alpha)$, also ist K_f ein Körper. Nach 2.3.13 folgt, dass f irreduzibel ist.

(ii) Aus $g(\alpha) = 0$ folgt, dass $\min_K(\alpha)$ das Polynom g teilt, $g = \min_K(\alpha) \cdot h$. Aber g ist irreduzibel und normiert, also $g = \min_K(\alpha)$.

□

Satz 2.3.15. *(Kronecker)*
Jedes nicht–konstante Polynom $f \in K[X]$ besitzt in einem geeigneten Erweiterungskörper von K eine Nullstelle.

Beweis.

Wegen grad $f \geq 1$ gibt es einen irreduziblen Faktor g von f, d.h. $g | f$ und g ist irreduzibel. Wir lösen die Aufgabe für g, d.h. wir können annehmen, dass f irreduzibel ist. Dann aber ist K_f ein Erweiterungskörper von K und $\alpha = \pi(X)$ wegen $f(\alpha) = \pi(f) = 0$ Nullstelle von f. □

Satz 2.3.16.
$\sqrt[3]{2}$ ist mit Zirkel und Lineal aus $\{0,1\}$ nicht konstruierbar. Das delische Problem der Würfelverdoppelung ist also nicht lösbar.

Beweis.

Betrachte das normierte Polynom $g(X) = X^3 - 2 \in \mathbb{Q}[X]$. Wir wollen zeigen, dass es das Minimalpolynom von $\sqrt[3]{2}$ ist, $g = \min_{\mathbb{Q}}\left(\sqrt[3]{2}\right)$. Da $g\left(\sqrt[3]{2}\right) = 0$, ist nach 2.3.12 (ii) nur noch zu zeigen, dass g irreduzibel ist.

Sei also $g = g_1 g_2$, notwendigerweise mit grad $g_1 = 1$ und grad $g_2 = 2$. Also

$$g_1(X) = X - \beta \in \mathbb{Q}[X]\,.$$

Dann gäbe es aber $\beta \in \mathbb{Q}$ mit $\beta^3 = 2$, Widerspruch. (Später werden wir viel bessere Hilfsmittel haben, um die Irreduzibilität von Polynomen nachzuweisen!)

Damit haben wir aber

$$\left[\mathbb{Q}\left(\sqrt[3]{2}\right) : \mathbb{Q}\right] = \operatorname{grad} \min_{\mathbb{Q}}\left(\sqrt[3]{2}\right) = 3,$$

was keine Potenz von 2 ist. Mit Hilfe von Korollar 2.1.11 (ii) schliessen wir, dass $\sqrt[3]{2} \notin \mathcal{A}\{0,1\}$. □

Zum Abschluss dieses Abschnitts wollen wir eine Charakterisierung der einfachen Körpererweiterungen vorstellen. Hierfür brauchen wir das folgende

Lemma 2.3.17.
Sei E/K eine einfache Körpererweiterung, $\alpha \in E$ ein primitives Element von E/K und L ein Zwischenkörper von E.

$$g(X) = X^m + \beta_{m-1}X^{m-1} + \cdot + \beta_0 \in L[X]$$

bezeichne das Minimalpolynom von α über L. (Achtung, nicht über K!) Dann gilt

$$L = K(\beta_0, \beta_1, \ldots, \beta_{m-1})\,.$$

Beweis.

Setze $F = K(\beta_0, \beta_1, \ldots, \beta_{m-1})$. Die Inklusion $F \subset L$ ist offensichtlich. Da $g \in F[X]$, $g(\alpha) = 0$ und g in $F[X]$ irreduzibel ist (g ist ja als Minimalpolynom sogar in $L[X]$ irreduzibel), ist

$$g = \min_F(\alpha)\,.$$

Nach Satz 2.2.7 ist

$$[F(\alpha) : F] = [L(\alpha) : L] = \operatorname{grad} g = m\,. \tag{14}$$

Aus $E = K(\alpha)$ folgt, dass erst recht $F(\alpha) = L(\alpha) = E$. Aus (14) folgt daher $[E : F] = [E : L]$. Nach der Gradformel gilt andererseits $[E : F] = [E : L][L : F]$, insgesamt also $[L : F] = 1$ und somit $L = F$. □

Satz 2.3.18.
Sei E/K eine algebraische Körpererweiterung. Dann gilt

$$E/K \quad \textit{ist einfach} \quad \Longleftrightarrow \quad E/K \quad \textit{besitzt nur endlich viele Zwischenkörper}\,.$$

Beweis.
Mit $\mathcal{Z}$ bezeichnen wir die Menge aller Zwischenkörper von E/K.

"⇒" Sei E einfach, $E = K(\alpha)$ und f das Minimalpolynom von α, $f = \min_K(\alpha)$. Bezeichne mit $\mathcal{T}$ die normierten Teiler von f in $E[X]$,

$$\mathcal{T} = \{g \in E[X] \,|\, g \quad \text{normiert}, \quad g|f \quad \text{in} \quad E[X]\}\,.$$

Da f in $E[X]$ nur endlich viele Teiler besitzt, ist $\#\mathcal{T} < \infty$.
Betrachte nun die Abbildung

$$\begin{array}{rcl} & \mathcal{T} & \to \quad \mathcal{Z} \\ g(X) = \sum X^m + \beta_{m-1}X^{m-1} + \ldots + \beta_0 & \mapsto & K(\beta_{m-1}, \ldots, \beta_0) \end{array}$$

Wir behaupten, dass sie surjektiv ist: denn sei $L \in \mathcal{Z}$, dann teilt: $g = \min_L(\alpha)$ das Polynom f in $L[X]$, also erst recht in $E[X]$. Nach Lemma 2.3.17 ist aber $L = K(\beta_{m-1}, \ldots \beta_0)$. Also ist die Abbildung surjektiv und damit $\mathcal{Z}$ als Bild der endlichen Menge $\mathcal{T}$ unter einer surjektiven Abbildung auch endlich.

"⇐" Wird hier nur unter der Voraussetzung gezeigt, dass der Körper K unendlich viele Elemente besitzt. (Endliche Körper werden in der Vorlesung Algebra II noch genauer untersucht werden.)
Wenn $\#\mathcal{Z} < \infty$, dann wird E von endlich vielen Elementen erzeugt, $E = K(\alpha_1, \ldots, \alpha_m)$. Denn andernfalls erhielte man durch sukzessives Adjungieren der erzeugenden Elemente eine Kette von unendlich vielen Zwischenkörpern. Wir führen den Beweis durch

Induktion nach m, der Induktionsanfang $m = 1$ ist trivial. Die Darstellung des Induktionsschritts erleichtern erleichtern wir uns durch die Annahme, dass $m = 2$, also $E = K(\alpha, \beta)$.

Da es nur endlich viele Zwischenkörper gibt, gibt es unter den unendlich vielen Elementen von K sicher zwei solche $\lambda_1, \lambda_2 \in K$, die den gleichen Zwischenkörper erzeugen:

$$K(\lambda_1\alpha + \beta) = K(\lambda_2\alpha + \beta) =: L\,.$$

Damit liegt aber auch die Differenz

$$(\lambda_1\alpha + \beta) - (\lambda_2\alpha + \beta) = (\lambda_1 - \lambda_2)\alpha \in L$$

und somit auch $\alpha \in L$ und schließlich auch $\beta \in L$. Damit ist aber $K(\lambda_1\alpha + \beta) = L = K(\alpha, \beta) = E$. Das heißt aber, dass E über K durch die Adjunktion des einzigen Elements $\lambda_1\alpha + \beta$ erzeugt wird, also einfach ist.

Man beachte, dass dieser Beweis nicht konstruktiv ist, d.h. das primitive Element $\lambda_1\alpha + \beta$ nicht explizit konstruiert wird!

□

3 Ringe

3.1 Lokalisierung von Ringen, maximale Ideale, Primideale

Sei R in diesem Abschnitt ein kommutativer Ring mit Eins.

Definition 3.1.1.

(i) Eine Teilmenge $S \subseteq R$ heißt multiplikativ, falls

$$1 \in S \quad \textit{und} \quad x, y \in S \Rightarrow xy \in S\,.$$

(ii) Definition des Quotientenrings $S^{-1}(R)$ von R bezüglich S.

Betrachte auf $R \times S$ die Äquivalenzrelation

$$(r, s) \sim (r', s') \iff \exists s_1 \in S, \quad \textit{so dass} \quad s_1(rs' - sr') = 0\,.$$

Wir definieren die Lokalisierung von R nach S als die Menge der Äquivalenzklassen und schreiben

$$S^{-1}R := (R \times S) \,/\, \sim$$

und schreiben für die Elemente von $S^{-1}R$ Brüche, d.h. $\frac{r}{s}$ mit $r \in R$ und $s \in S$ steht für die Äquivalenzklasse von (r, s).

Die üblichen Regeln der Bruchrechnung geben der Lokalisierung $S^{-1}R$ die Struktur eines Rings mit Eins. Zum Beispiel wird die Multiplikation definiert durch $\frac{r}{s}\,\frac{r'}{s'} := \frac{rr'}{ss'}$. Sie ist wohldefiniert: sei $(\overline{r}, \overline{s}) \in \frac{r}{s}$ ein anderer Repräsentant. Dann gibt es $s_1 \in S$, so dass

$$s_1(s\overline{r} - r\overline{s}) = 0\,.$$

Daraus folgt aber auch durch Multiplikation mit $s'r'$

$$s_1(ss'\overline{r}r' - \overline{s}s'rr') = s_1 s'r'(s\overline{r} - r\overline{s}) = 0\,,$$

woraus wir schließen, dass $\frac{\overline{r}r'}{\overline{s}s'} = \frac{rr'}{ss'}$.

Das Einselement ist die Äquivalenzklasse $\frac{1}{1}$, eine Addition wird durch $\frac{r}{s} + \frac{r'}{s'} = \frac{rs'+r's}{ss'}$ definiert. Als Übung zeige der Leser, dass dies wohldefiniert ist. Man überzeugt sich, dass durch diese Definitionen eine Ringstruktur auf $S^{-1}R$ definiert wird. Die Abbildung

$$\begin{array}{rccc} \varphi_s : & R & \to & S^{-1}R \\ & r & \mapsto & \dfrac{r}{1} \end{array}$$

ist ein (nicht notwendigerweise injektiver!) Ringhomomorphismus. Außerdem sieht man leicht, dass die Elemente von $\varphi_s(S)$ in $S^{-1}R$ invertierbar sind: $(\frac{s}{1})^{-1} = \frac{1}{s}$ für $s \in S$.

Bemerkung 3.1.2.

(i) Seien A, B kommutative Ringe mit Eins, $S \subset A$ multiplikative Teilmenge von A und

$$f : A \to B$$

ein Ringhomomorphismus derart, dass alle Element des Bilds $f(S)$ in B invertierbar sind. Dann gibt es genau einen Ringhomomorphismus h, so dass das folgende Diagramm kommutiert:

$$\begin{array}{ccc} A & \xrightarrow{f} & B \\ & \searrow & \uparrow \quad \exists! h \\ \varphi_s & & S^{-1}A \end{array}$$

(ii) $S^{-1}A$ ist bis auf Isomorphie der einzige Ring, der in A und S diese Eigenschaft besitzt.
Beweis von (i) und (ii) wird als Übungsaufgabe gestellt. Dies ist die universelle Eigenschaft der Lokalisierung.

(iii) Sei R integer und $S \subseteq R$ multiplikativ mit $0 \notin S$. Dann ist die kanonische Abbildung

$$\begin{array}{rccc} \varphi_s : & R & \to & S^{-1}R \\ & r & \mapsto & \dfrac{r}{1} \end{array}$$

injektiv. Denn $\frac{r}{1} = \frac{0}{1}$ dann und nur dann, wenn es $s \in S$ gibt, so dass $sr = 0$. Da R integer und $s \neq 0$, folgt $r = 0$.

(iv) Sei R integer und $S = R\backslash\{0\}$. S ist multiplikativ abgeschlossen, da R integer ist. In dieser Situation ist $S^{-1}R$ sogar ein Körper, der Quotientenkörper von R. Wir bezeichnen ihn mit $\mathrm{Quot}(R) = S^{-1}R$. R wird bezüglich der Injektion $\varphi_s : R \to S^{-1}R$ als Teilring aufgefasst.

Beispiele
- $\mathrm{Quot}(\mathbb{Z}) = \mathbb{Q}$.
- *Sei K ein Körper und $R = K[X]$ der Polynomring über K.*

$$K(X) = \text{ Quot } K[X] = \left\{ \frac{f(x)}{g(x)} \Big| f, g \in K[X], g \neq 0 \right\}$$

heißt rationaler Funktionenkörper in einer Variablen über K.

Satz 3.1.3.
Sei E/K Körpererweiterung, $\alpha \in E$. α ist transzendent über K genau dann, wenn es eine natürliche Isomorphie von Körpern $K(\alpha) \cong K(X)$ gibt.
Zu K gibt es also bis auf Isomorphie nur einen Typ einer einfachen transzendenten Erweiterung, nämlich $K(X)/K$.

Beweis.

"$\Leftarrow$" Weil schon der Unterring $K[X]$ unendliche Dimension hat, $\dim_K K[X] = \infty$, ist erst recht $\dim_K K(X) = \infty$. Aus der Isomorphie folgt

$$\dim_K K(\alpha) = \infty\,.$$

Nach Satz 2.2.3 ist dann aber α nicht algebraisch über K, also transzendent.

"$\Rightarrow$" Nach 2.3.6 (iii) liefert für transzendentes α der Einsetzungshomomorphismus einen Isomorphismus von Ringen:

$$\begin{array}{rccc} \varphi_\alpha & : & K[X] & \to & K[\alpha] \\ & & X & \mapsto & \alpha \end{array}\,.$$

Daraus folgt auch, dass die beiden Quotientenkörper isomorph sind, $K(X) \cong K(\alpha)$.

□

Definition 3.1.4.
Sei R ein kommutativer Ring mit Eins.

(i) Ein Ideal $\mathfrak{p}$ in R heißt <u>Primideal</u>, falls $\mathfrak{p} \neq R$ und $R/\mathfrak{p}$ Integritätsring ist. Das ist äquivalent zu der Aussage:

$$xy \in \mathfrak{p} \;\Rightarrow\; x \in \mathfrak{p} \quad \textit{oder} \quad y \in \mathfrak{p}\,.$$

Zum Beispiel ist $3\mathbb{Z}$ ein Primideal des Rings $\mathbb{Z}$, aber $4\mathbb{Z}$ nicht: 4 liegt in $4\mathbb{Z}$, und $4 = 2 \cdot 2$, aber $2 \notin 4\mathbb{Z}$.

(ii) Ein Ideal $\mathfrak{m}$ von R heißt <u>maximales Ideal</u>, wenn $\mathfrak{m} \neq R$ und $R/\mathfrak{m}$ ein Körper ist. Wir bemerken, dass dies äquivalent zu der folgenden Aussage ist:
Ist $\mathfrak{a} \subset R$ ein Ideal mit $\mathfrak{m} \subset \mathfrak{a}$, so gilt $\mathfrak{a} = \mathfrak{m}$ oder $\mathfrak{a} = R$.

Beweis der Bemerkung:

"⇒" Sei $m \subseteq \mathfrak{a} \subset R$. Betrachte

$$\begin{array}{rccc} \varphi & : & R/\mathfrak{m} & \to & R/\mathfrak{a} \\ & & r \bmod \mathfrak{m} & \mapsto & r \bmod \mathfrak{a} \end{array}$$

Dies ist offenbar wohldefiniert. Der Kern $\ker\varphi = \mathfrak{a}/\mathfrak{m}$ ist ein Ideal im Körper $R/\mathfrak{m}$, also entweder der Körper selbst oder trivial. Im ersten Fall ist $\mathfrak{a} = R$, im zweiten Fall $\mathfrak{a} = \mathfrak{m}$. Man beachte, dass ein maximales Ideal $\mathfrak{m}$ nie gleich dem ganzen Ring R sein kann: der Quotient $R/\mathfrak{m}$ hat als Körper wenigstens zwei Elemente, somit muss es wenigstens zwei Restklassen geben.

"⇐" Da $\mathfrak{m} \neq R$ gilt, ist die Restklasse der Eins $\bar{1} \in R/\mathfrak{m}$ von Null verschieden, $\bar{1} \neq 0$.

Sei nun $\bar{x} = x \bmod \mathfrak{m} \in R/\mathfrak{m}$ eine nicht-verschwindende Restklasse, $\bar{x} \neq 0$, also $x \notin \mathfrak{m}$. Da $\mathfrak{m} + Rx \subseteq R$ ein Ideal von R ist, das das maximale Ideal $\mathfrak{m}$ echt enthält, folgt $\mathfrak{m} + Rx = R$. Das heißt aber, dass es $m_0 \in \mathfrak{m}$ und $y \in R$ gibt, so dass

$$m_0 + yx = 1\,.$$

Modulo dem Ideal $\mathfrak{m}$ betrachtet, gibt dies $\overline{y}\ \overline{x} = \overline{1}$, also hat $\overline{x}$ ein Inverses. Somit ist $R/\mathfrak{m}$ ein Körper.

Bemerkung 3.1.5.

(i) Jedes maximale Ideal ist Primideal, denn Körper sind nullteilerfrei.

(ii) Die Umkehrung gilt nicht. Ist R integer, aber kein Körper, so ist das Ideal (0) prim, aber nicht maximal.

Bemerkung 3.1.6. *Sei S eine Menge. Wir erinnern an die folgenden Begriffe und Resultate der Mengenlehre:*

(i) Eine partielle Ordnung auf S ist eine Relation $x \leq y$ mit den folgenden Eigenschaften:

$$\begin{array}{lll} x \leq x & & \textit{Reflexivität} \\ x \leq y \ \wedge\ y \leq z & \Rightarrow\ x \leq z & \textit{Transitivität} \\ x \leq y \ \wedge\ y \leq x & \Rightarrow\ x = y & \textit{Antisymmetrie}\,. \end{array}$$

(ii) Eine Totalordnung auf S ist eine partielle Ordnung, für die je zwei Elemente vergleichbar sind:

$$x, y \in S \quad \Rightarrow \quad x \leq y \quad \textit{oder} \quad y \leq x\,.$$

(iii) *Sei S partiell geordnet, $T \subset S$ Teilmenge.*

Ein Element $b \in S$ heißt obere Schranke von T, falls

$$x \leq b \quad \text{für alle} \quad x \in T\,.$$

(iv) *Sei S partiell geordnet. Ein Element $m \in S$ heißt maximales Element, falls*

$$m \leq x \quad \Rightarrow \quad m = x\,.$$

Das maximale Element muss nicht eindeutig sein.

(v) *Eine partiell geordnete Menge S heißt induktiv geordnet, falls jede nicht–leere, total geordnete Teilmenge von S eine obere Schranke besitzt.*

(vi) *Zornsches Lemma*

Sei S eine nicht–leere, induktiv geordnete Menge. Dann besitzt S maximale Elemente.

Satz 3.1.7.
Sei R ein kommutativer Ring mit Eins, und $\mathfrak{a}$ ein von R verschiedenes Ideal. Dann ist $\mathfrak{a}$ in einem maximalen Ideal enthalten.

Beweis.

Wir setzen $\mathfrak{M} = \{\mathfrak{b} \subset R | \mathfrak{b} \text{ Ideal}, \mathfrak{a} \subseteq \mathfrak{b}, \mathfrak{b} \neq R\}$. Offenbar ist $\mathfrak{a} \in \mathfrak{M}$, also ist $\mathfrak{M} \neq \emptyset$. Außerdem ist $\mathfrak{M}$ induktiv geordnet durch Inklusion: sei $\{\mathfrak{b}_i\}_{i\in I}$ eine total geordnete Teilmenge von $\mathfrak{M}$. Dann ist $\mathfrak{b} := \bigcup_{i\in I} \mathfrak{b}_i$ ein Ideal in R, das $\mathfrak{a}$ enthält. Es ist auch eine obere Schranke der $\{\mathfrak{b}_i\}_{i\in I}$. Wir können nun das Zornsche Lemma anwenden und schließen, dass $\mathfrak{M}$ maximale Elemente besitzt. Ein solches maximales Element $\mathfrak{m} \in \mathfrak{M}$ ist sicher ein Ideal und enthält $\mathfrak{a}$. Es ist auch ein maximales Ideal: ist $\mathfrak{d}$ ein weiteres von R verschiedenes Ideal, das $\mathfrak{m}$ enthält, $\mathfrak{m} \subseteq \mathfrak{d}$, so liegt $\mathfrak{d}$ offensichtlich in $\mathfrak{M}$. Aber in $\mathfrak{M}$ war $\mathfrak{m}$ doch maximal bezüglich der Inklusion, also $\mathfrak{d} = \mathfrak{m}$. □

Definition 3.1.8.
Ein kommutativer Ring mit 1 heißt lokaler Ring, falls R genau ein maximales Ideal besitzt.
Beispiel: Körper sind lokale Ringe, $\mathbb{Z}$ aber nicht, denn jedes Primideal (p) mit $p \neq 0$ ist maximal.

Bemerkung 3.1.9.
Ein Ring mit Eins ist lokal genau dann, wenn es ein Ideal $\mathfrak{m} \subseteq R$ gibt mit $R\backslash\mathfrak{m} = R^\times$. Hierbei ist $R^\times$ die Gruppe der Einheiten von R.

Beweis.

"$\Rightarrow$" Sei $x \in R\backslash\mathfrak{m}$. Wäre x keine Einheit, so wäre das Hauptideal Rx ein echtes Ideal in R. Satz 3.1.7 sagt, dass dieses Ideal in einem maximalen Ideal enthalten ist. Aber es gibt nur ein maximales Ideal, nämlich $\mathfrak{m}$. Also $Rx \subset \mathfrak{m}$, und somit liegt x in $\mathfrak{m}$, was ein Widerspruch ist. Also ist $R\backslash\mathfrak{m} \subset R^\times$. Ferner enthält $\mathfrak{m}$ keine Einheiten, da sonst auch $1 \in \mathfrak{m}$, womit man $\mathfrak{m} = R$ hätte. Damit haben wir auch die umgekehrte Inklusion gezeigt: $R^\times \subset R\backslash\mathfrak{m}$.

"$\Leftarrow$" Sei $\mathfrak{m}$ ein Ideal mit der Eigenschaft, dass $R\backslash\mathfrak{m} = R^\times$. Die Ringeins ist eine Einheit, $1 \in R^\times$, also ist das Ideal $\mathfrak{m}$ nicht ganz R. Ferner ist $R/\mathfrak{m}$ ein Körper: jedes nicht-verschwindende $\overline{a} \in R/\mathfrak{m}$ hat einen Repräsentanten $a \in R\backslash\mathfrak{m} = R^\times$ und kann daher in R invertiert werden. Damit ist klar, dass $\mathfrak{m}$ ein maximales Ideal ist. Wir müssen zeigen, dass dies das einzige maximale Ideal ist. Sei $\mathfrak{m}'$ ein weiteres maximales Ideal von R. Damit $\mathfrak{m}' \neq R$ gilt, darf $\mathfrak{m}'$ keine Einheiten enthalten. Also

$$R\backslash\mathfrak{m}' \supset R^\times = R\backslash\mathfrak{m}$$

Damit ist aber $\mathfrak{m}'$ in $\mathfrak{m}$ enthalten; da $\mathfrak{m}'$ maximal sein soll, müssen die beiden Ideale übereinstimmen.

□

Beispiele 3.1.10.

- *Sei R ein kommutativer Ring mit 1 und $\mathfrak{p} \subset R$ ein Primideal von R. Dann ist*

$$S_\mathfrak{p} := R\backslash\mathfrak{p}$$

eine multiplikative Teilmenge von R, denn $1 \notin \mathfrak{p}$, also ist $1 \in S$. Die Negation der Definition 3.1.4 (i) eines Primideals zeigt, dass aus $x, y \notin \mathfrak{p}$ folgt, dass $xy \notin \mathfrak{p}$. Sei nun $R_\mathfrak{p} = S_\mathfrak{p}^{-1}R$ die Lokalisierung von R nach $S_\mathfrak{p}$. Dies ist ein lokaler Ring mit maximalem Ideal

$$\mathfrak{m} := \left\{ \frac{r}{s} \middle| s \notin \mathfrak{p}, r \in \mathfrak{p} \right\}$$

denn alle Element von $R\backslash\mathfrak{m} = \left\{ \frac{r}{s} \middle| s \notin \mathfrak{p}, r \notin \mathfrak{p} \right\}$ können invertiert werden.

- *Der Name* lokal *kommt von folgendem Beispiel: Sei X eine differenzierbare Mannigfaltigkeit, x ein Punkt von X und $\mathcal{O}_x$ der Ring der Keime differenzierbarer Funktionen in x. Das sind alle Funktionen, die auf einer offenen Menge $U \ni x$ definiert werden können, wobei Funktionen, die auf dem Durchschnitt ihrer Definitionsgebiete übereinstimmen, identifiziert werden. Der Ring $\mathcal{O}_x$ ist offenbar im Wortsinn ein lokales Objekt, und er ist auch ein lokaler Ring, dessen einziges maximale Ideal $\mathfrak{m}_x$ aus den (Klassen von) Funktionen besteht, die in x verschwinden. Denn für alle anderen Funktionen f kann man lokal f^{-1} definieren, sie sind also Einheiten im Ring $\mathcal{O}_x$.*

Bemerkung 3.1.11.
Sei K ein Körper, betrachte den Ringhomomorphismus

$$\begin{array}{rccc} \varphi: & \mathbb{Z} & \to & K \\ & z & \mapsto & z \cdot 1_K \end{array}$$

Hierbei steht $z \cdot 1_K$ im Falle natürlicher z für die z-fache Summe der Körpereins 1_K mit sich selbst. Für negative z verwendet man Inverse.

1. Fall: $\ker \varphi \neq 0$. *Da der Kern ein Ideal ist und da der Ring $\mathbb{Z}$ ein Hauptidealring ist, ist* $\ker \varphi = n\mathbb{Z}$. *Wir bekommen also eine Injektion $\mathbb{Z}/n\mathbb{Z} \hookrightarrow K$. Da K als Körper nullteilerfrei ist, muss n prim sein: wäre $n = n_1 n_2$, so wäre $(n_1 1_K)(n_2 1_K) = n1_K = 0$.*

Also ist für eine geeignete Primzahl p der Körper $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$ Teilkörper von K, da $p\mathbb{Z}$ im Ring $\mathbb{Z}$ ein maximales Ideal ist.

2. Fall $\ker \varphi = 0$. *Dann haben wir eine Injektion φ von $\mathbb{Z}$ in K. Alle Elemente von $\varphi(\mathbb{Z}\backslash\{0\})$ sind in K invertierbar. Nach Bemerkung 3.1.2 (i) bekommen wir eine eindeutig bestimme Abbildung ψ, so dass das folgende Diagram kommutiert:*

$$\begin{array}{ccccc} \mathbb{Z} & \overset{\varphi}{\hookrightarrow} & & K & \\ & \searrow & & \uparrow & \exists! \psi \\ & & \text{Quot } (\mathbb{Z}) = \mathbb{Q} & & \end{array}$$

Die Abbildung ψ ist injektiv, denn $\ker \psi$ *ist ein Ideal im Körper $\mathbb{Q}$ und daher entweder 0 oder ganz $\mathbb{Q}$. Letzteres ist ausgeschlossen, weil das Bild von $\mathbb{Z}$ unter φ in K liegt. Also sind die rationalen Zahlen $\mathbb{Q}$ ein Teilkörper von K.*

Definition 3.1.12.

(i) *Ein Körper K heißt Primkörper, wenn er keinen echten Teilkörper enthält. Es gilt $K \cong \mathbb{Q}$ oder $K \cong \mathbb{F}_p$ für eine Primzahl p.*

(ii) *Der Primkörper eines beliebigen Körpers K ist der eindeutig bestimmte Primkörper, der Teilkörper von K ist. Er ist gleich dem Durchschnitt aller Teilkörper.*
Ist dieser isomorph zu $\mathbb{Q}$ oder $\mathbb{F}_p$, $p > 0$, so sagt man K hat die Charakteristik 0 oder p und schreibt $\operatorname{char} K = 0$ *oder* $\operatorname{char} K = p$.
Beispiel: $\operatorname{char} \mathbb{F}_p(X) = p$.

3.2 Teilbarkeitslehre

Auch in diesem Abschnitt ist R ein kommutativer Ring mit Eins.

Definition 3.2.1.
(i) *Seien $a, b \in R$. Wir sagen a teilt b, in Zeichen $a|b$, wenn es $c \in R$ gibt, so dass $b = ac$.*

(ii) *a und $b \in R$ heißen assoziiert, in Zeichen $a \overset{\wedge}{=} b$, falls*

$$a|b \quad \textit{und} \quad b|a\,.$$

Bemerkungen 3.2.2.
(i) *Teilbarkeit ist reflexiv und transitiv, aber wegen der Existenz assoziierter Elemente im allgemeinen keine partielle Ordnung! Ferner gilt:* 1 *teilt jedes $a \in R$, und jedes $a \in R$ teilt 0. Außerdem*

$$\begin{aligned} a|b \wedge c|d &\Rightarrow ac|bd \\ a|b \wedge a|c &\Rightarrow a|b+c \end{aligned}$$

In integren Ringen gilt $ac|bc$ mit $c \neq 0 \Rightarrow a|b$.

(ii) *Ist R integer, so gilt: $a \overset{\wedge}{=} b \iff \exists \epsilon \in R^\times \; b = \epsilon a$ (Übung).*

(iii) *In den Übungsaufgaben werden Sie zeigen: ist R integer, so ist auch der Polynomring $R[X]$ integer. Für die Einheitengruppe gilt, wenn R integer ist: $R[X]^\times = R^\times$. Beispiele für Einheitengruppen: $R = \mathbb{Z}[i]^\times = \{\pm 1, \pm i\}$, $R = \mathbb{Z}[\sqrt{2}]^\times = \{\pm(1+\sqrt{2})^j, j \in \mathbb{Z}\}$.*

(iv) *Man führt das ggT und kgV ein wie bei ganzen Zahlen:*

$$ggT(a_1, \ldots a_n)|a_i \quad bzw. \quad a_i|kgV(a_1 \ldots a_2) \quad \forall i = 1, \ldots, n$$

und gilt

$$t|a_i \; \forall i \quad bzw. \quad a_i|t \; \forall i\;,$$

so folgt

$$t|ggT(a_1 \dots a_n) \quad bzw. \quad kgV(a_1 \dots a_n)|t.$$

ggT und kgV sind bis auf Assoziiertheit eindeutig, sofern sie überhaupt existieren. (Wir werden später eine Klasse von Ringen kennen lernen, die faktoriellen Ringe, in denen ggT und kgV immer existieren.)

(v) Wir halten fest, dass Teilbarkeit auch idealtheoretisch formuliert werden kann, nämlich als Aussagen über die entsprechenden Hauptideale.

$$\begin{array}{lcl} a|b & \Longleftrightarrow & (b) \subset (a) \\ a \overset{\wedge}{=} b & \Longleftrightarrow & (b) = (a) \end{array}$$

Gleiches gilt für die Relation "Vielfaches oder Teiler von einander sein":
$v \in R$ ist Vielfaches von a und b, dann und nur dann, wenn das von v erzeugte Hauptideal im Schnitt der Hauptideale von a und b liegt: $(v) \subseteq (a) \cap (b)$.
Insbesondere gilt für das vom kgV erzeugte Hauptideal $(kgV(a,b)) = (a) \cap (b)$.

(vi) Mit $\mathfrak{a}_1$ und $\mathfrak{a}_2$ Idealen in R sind auch $\mathfrak{a}_1 \cap \mathfrak{a}_2$ und $\mathfrak{a}_1 + \mathfrak{a}_2 = \{a_1 + a_2 | a_i \in \mathfrak{a}_i\}$ Ideale in R. Als Notation vereinbaren wir:

$$(a_1) + (a_2) + \dots + (a_n) = (a_1, \dots, a_n)\,.$$

$d \in R$ ist Teiler von a und b, dann und nur dann wenn $(a) + (b) \subseteq (d)$.

Definition 3.2.3.

(i) Ein Integritätsring heißt Hauptidealring, wenn jedes Ideal Hauptideal ist. Ein Hauptidealring heißt auch prinzipal.

(ii) Ein Integritätsring heißt euklidischer Ring, wenn es eine "Division mit Rest" gibt. Da ein Rest in einem geeigneten Sinn klein sein soll, fordert man für einen euklidischen Ring die Existenz einer sogenannten euklidischen Normfunktion ν auf R,

$$\nu : \quad R \to \mathbb{N}_0 = \mathbb{N} \cup \{0\}$$

mit $\nu(0) = 0$. Die Division mit Rest wird durch die Forderung verallgemeinert, dass es zu je zwei $a, b \in R$ mit $a \neq 0$ Elemente $q, r \in R$ gibt, so dass

$$b = qa + r \quad und \quad \nu(r) < \nu(a)\,.$$

Man beachte, dass hieraus und aus dem Wertebereich der Normfunktion ν folgt, dass nur für das Nullelement die Norm verschwinden kann.

Bemerkung 3.2.4.

(i) Sei R ein Hauptidealring. Dann existiert zu beliebig vorgegebenen $a_1, \ldots, a_n \in R$ ein größter gemeinsamer Teiler $d \in R$ mit Darstellung

$$d = x_1 a_1 + \cdots + x_n a_n \quad \textit{mit} \quad x_i \in R\,.$$

Beweis.
Da R Hauptidealring ist, existiert ein $d \in R$ so dass

$$(a_1) + \cdots + (a_n) = (d)\,.$$

Da jedes a_i im Ideal auf der linken Seite liegt, ist klar, dass d jedes a_i teilt, also gemeinsamer Teiler ist. Da d im Ideal auf der rechten Seite ist, ist klar, dass es eine Darstellung gibt $d = x_1 a_1 + \cdots + x_n a_n$.

Um zu sehen, dass d auch größter *gemeinsamer Teiler ist, wählen wir einen weiteren gemeinsamen Teiler $t \in R$ aller a_i, also $(a_i) \subseteq (t)$. Damit aber auch $(d) = (a_1) + \ldots + (a_n) \subseteq (t)$, was impliziert, dass t auch d teilt. Also ist d wirklich das $ggT(a_1, \ldots, a_n)$.*

(ii) Ein euklidischer Ring ist Hauptidealring.

Beweis

Sei $\mathfrak{a} \subset R$ Ideal, $\mathfrak{a} \neq (0)$. Sei $a \in \mathfrak{a}$ mit $\nu(a)$ minimal unter den von Null verschiedenen Werten von ν. Dann gilt $(a) = \mathfrak{a}$: die Inklusion $(a) \subset \mathfrak{a}$ ist für jedes Element $a \in \mathfrak{a}$ ohnehin klar, da $\mathfrak{a}$ ein Ideal ist.

Sei nun b ein beliebiges Element in $\mathfrak{a}$. Da R euklidisch ist, können wir schreiben $b = qa + r$ mit $\nu(r) < \nu(a)$ und $q, r \in \mathfrak{a}$. Da aber $\nu(a)$ minimal sein sollte, muss $\nu(r) = 0$ gelten. Also gilt $r = 0$, und somit $b \in (a)$.

(iii) Beispiele für Euklidische Ringe sind $R = \mathbb{Z}$ mit $\nu(a) = |a|$ und $K[X]$ mit K Körper, wobei die Normfunktion für nicht-verschwindende Polynome der Polynomgrad (plus Eins) ist. Diese Ringe sind also insbesondere Hauptidealringe.

(iv) In Euklidischen Ringen kann der euklidische Algorithmus aus Kapitel 1.3 angewandt werden, um einen größten gemeinsamen Teiler zu finden.

Definition 3.2.5.
Ein Element $\pi \in R$ heißt irreduzibel (oder unzerlegbar), wenn $\pi \notin R^\times$ und $\pi = ab$ impliziert, dass entweder $a \in R^\times$ oder $b \in R^\times$.
Beispiele für irreduzible Elemente:

- *In $\mathbb{Z}$ sind irreduzibel $\pm p, p$ mit p prim.*
- *Die irreduziblen Elemente im Ring $K[X]$ der Polynome über einem Körper K wurden schon in Beispiel 2.3.11 eingeführt.*

Definition 3.2.6.

(a) Ein Element $a \in R$ besitzt eine Zerlegung in irreduzible Elemente, wenn a eine Darstellung

$$a = \epsilon\pi_1 \dots \pi_r \qquad \epsilon \in R^\times,\ \pi_i \in R \quad \textit{irreduzibel}$$

hat. $r = 0$ ist hierbei erlaubt.

(b) Ein Integritätsring R heißt faktoriell (oder ZPE Ring), falls jedes $a \in R$, $a \neq 0$ eine eindeutige *Zerlegung in irreduzible Faktoren besitzt. Das heißt ausführlicher: ist $a = \epsilon\pi_1 \dots \pi_r = \epsilon'\pi'_1 \dots \pi'_s$, so folgt $r = s$ und nach geeigneter Umnummerierung ist*

$$\pi_i \overset{\wedge}{=} \pi'_i \quad \textit{für} \quad i = 1 \dots r\,.$$

(c) Ein Element $\pi \in R$ heißt Primelement, falls $\pi \neq 0$ und $\pi | ab$ impliziert, dass $\pi | a$ oder $\pi | b$.

Bemerkung: $\pi \in R$ ist genau dann Primelement, wenn das Hauptideal (π) Primideal ist.

Die Klasse der faktoriellen Ringe wird uns in der Folge interessieren. Um sie besser in den Griff zu bekommen, müssen wir die Eigenschaft "faktoriell" durch äquivalente Eigenschaften ausdrücken können.

Satz 3.2.7.
Sei R integer. Dann sind äquivalent:

(i) R ist faktoriell

(ii) Jedes $a \in R \setminus \{0\}$ besitzt eine Zerlegung in irreduzible Faktoren und jedes irreduzible Element ist Primelement.

Beweis.

(i)⇒ (ii) Die Existenz einer Zerlegung ist klar, da sogar eine eindeutige Zerlegung gefordert wird. Sei nun $\pi \in R$ irreduzibel und teile $\pi | ab$, mit $a, b \in R$. Da R faktoriell ist, können wir eindeutig schreiben

$$a = \epsilon\pi_1 \dots \pi_r \qquad b = \tilde{\epsilon}\tilde{\pi}_1 \dots \tilde{\pi}_s\,.$$

Also

$$ab = \epsilon\tilde{\epsilon}\pi_1 \dots \pi_r \tilde{\pi}_1 \dots \tilde{\pi}_s \,.$$

Aus der Eindeutigkeit der Zerlegung folgt, dass π assoziiert sein muss zu einem der π_i oder $\tilde{\pi}_i$. Damit teilt aber π entweder a oder im anderen Falle b. Damit ist π aber auch Primelement.

(ii)⇒ (i) Da die Existenz einer Zerlegung in irreduzible Elemente gefordert wird, ist nur die Eindeutigkeit nachzuweisen. Sei $a = \epsilon\pi_1 \dots \pi_r = \epsilon'\pi'_1 \dots \pi'_s$ und wir können uns auf $r \geq 1$ beschränken. Offenbar haben wir

$$\pi_1 \,|\, \epsilon'\pi'_1 \dots \pi'_s \,.$$

Da π_1 prim, folgt $\pi_1 | \pi'_j$ für ein j, durch Umnumerierung dürfen wir annehmen, dass $j = 1$. Da π_1 auch irreduzibel ist, folgt $\pi_1 \overset{\wedge}{=} \tilde{\pi}_1$. Per Induktion nach r folgt nun die Aussage.

□

Bemerkung 3.2.8.

(i) In einem Integritätsring ist jedes Primelement irreduzibel. Denn sei π Primelement und $\pi = ab$. Da π prim ist, teilt dann $\pi|a$ oder $\pi|b$. Wir können $\pi c = a$ annehmen, woraus folgt $\pi cb = ab = \pi$. Damit aber $\pi(cb - 1) = 0$; da R integer vorausgesetzt wurde, folgt $b \in R^\times$.

(ii) Die Umkehrung ist in allgemeinen Ringen falsch! Gegenbeispiel: Im Ring $R = \mathbb{Z}[\sqrt{-5}]$ ist 2 irreduzibel, aber nicht prim. In der Tat ist auch die Eindeutigkeit der Zerlegung in irreduzible Elemente nicht gegeben: das Element 6 hat zwei verschiedene Zerlegungen in ein Produkt irreduzibler Elemente:

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

Der Ring $\mathbb{Z}[\sqrt{-5}]$ ist also nicht faktoriell.

(iii) Wir werden in Satz 3.3.1 sehen, dass Polynomringe über Körpern faktoriell sind. In diesem Fall wurde schon in Lemma 2.3.12 gezeigt, dass alle irreduziblen Polynome auch prim sind.

Lemma 3.2.9.

Sei R integer. Dann ist R faktoriell dann und nur dann, wenn

1. *jede Kette von Hauptidealen $(a_1) \subseteq (a_2) \subseteq \dots$ stationär wird: das heißt, wenn es ein n gibt, so dass $(a_m) = (a_n)$ für alle $m \geq n$.*
   und

2. jedes irreduzible Element Primelement ist.

Beweis.

"$\Leftarrow$" Sei $\mathfrak{M} = \{(a) | a \in R, a \neq 0, a \text{ besitzt keine Zerlegung in irreduzible Elemente }\}$. Unser Ziel ist zu zeigen, dass $\mathfrak{M} = \emptyset$.

Angenommen, es wäre $\mathfrak{M} \neq \emptyset$. Wegen (i) ist $\mathfrak{M}$ durch Inklusion induktiv geordnet. Nach dem Zornschen Lemma besitzt $\mathfrak{M}$ maximale Elemente, etwa (a). Nun kann a keine Einheit sein und auch nicht irreduzibel, da es sonst in irreduzible Element zerlegbar wäre, was aber wegen $(a) \in \mathfrak{M}$ unmöglich ist. Damit schreibt sich

$$a = bc\,,$$

also

$$(a) \subset (b) \quad \text{und} \quad (a) \subset (c)$$

mit echten Inklusionen. Aber (a) ist überdies maximal, also können $(b), (c)$ nicht in $\mathfrak{M}$ liegen. Damit besitzen aber b und c und somit auch $a = bc$ Zerlegungen in irreduzible Faktoren. Dies ist ein Widerspruch zu $(a) \in \mathfrak{M}$. Damit muss $\mathfrak{M} = \emptyset$ gelten. Nach Satz 3.2.7 ist dann aber R faktoriell.

"$\Rightarrow$" Satz 3.2.7 impliziert (ii). Betrachte $a_1, a_2 \in R$ mit $(0) \neq (a_1) \subset (a_2) \neq R$ und Zerlegungen

$$\begin{aligned} a_1 &= \epsilon\pi_1 \dots \pi_r \\ a_2 &= \tilde{\epsilon}\tilde{\pi}_1 \dots \tilde{\pi}_s \end{aligned}$$

Wegen $a_2 | a_1$ und wegen der eindeutigen Zerlegung in irreduzible Elemente ist im Falle echter Inklusion $(a_1) \subset (a_2)$ das Element a_2 ein echter Teiler von a_1. Damit muss aber $s < r$ gelten. Da r endlich ist, wird also auch jede Kette stationär.

□

Satz 3.2.10.
Jeder Hauptidealring ist faktoriell.

Beweis.

Sei $(a_1) \subseteq (a_2) \subseteq \dots$ eine Kette von Hauptidealen. Betrachte die Vereinigung

$$I := \bigcup_i (a_i)\,.$$

Da I ein Ideal ist, folgt $I = (a)$ mit $a \in R$. Da $a \in I$, gibt es ein n, so dass $a \in (a_n)$. Für alle $m \geq n$ gilt:

$$(a_m) \subseteq I = (a) \subseteq (a_n) \subseteq (a_m)\,.$$

Somit $(a_m) = (a_n)$ $\forall m \geq n$, jede Kette von Hauptidealen wird also stationär.

Sei weiter $\pi \in R$ ein irreduzibles Element. Um zu zeigen, dass es auch Primelement ist, betrachten wir $a, b \in R$ mit der Eigenschaft, dass $\pi | ab$. Wir nehmen an, dass π nicht a teilt und wollen zeigen, dass $\pi | b$.

Da π irreduzibel ist, ist $ggT(\pi, a) = 1$. (Das ggT existiert für den Hauptidealring R nach Bemerkung 3.2.4 (i).) Damit existieren aber $x, y \in R$, so dass

$$x\pi + ya = 1\,.$$

Wir multiplizieren mit b:

$$b = bx\pi + yab\,.$$

Da π nach Voraussetzung ab teilt, teilt dann π auch b. Also ist π Primelement. Die Behauptung folgt jetzt aus Lemma 3.2.9. □

Bemerkung 3.2.11.

(i) Die Umkehrung ist falsch: der Ring $\mathbb{Z}[X]$ ist faktoriell (Beweis später mittels des Satzes von Gauß!), aber nicht prinzipal: das Ideal $(n) + (X)$ mit $n \in \mathbb{Z}$ ist kein Hauptideal (Gradgründe).

(ii) Wir haben die folgenden Inklusionen für Ringe:

$$\underset{}{\textit{euklidisch}} \overset{\textit{3.2.4(ii)}}{\Rightarrow} \textit{prinzipal} \overset{\textit{3.2.10}}{\Rightarrow} \textit{faktoriell}$$

Definition 3.2.12.

Sei R ein faktorieller Ring und $\pi \in R$ irreduzibel. Wir betrachten die Abbildung

$$\omega_\pi : R \to \mathbb{Z}_{\geq 0} \cup \{\infty\}\,,$$

die definiert ist durch $\omega_\pi(0) = \infty$ und für $a \neq 0$ der Form $a = \pi^e a'$ mit $\pi \nmid a'$ durch $\omega_\pi(a) = e$. Wir setzen sie auf $K = \mathrm{Quot}(R)$ fort durch

$$\begin{array}{rccl} \omega_\pi : & K & \to & \mathbb{Z} \cup \{\infty\} \\ & \frac{a}{b} & \mapsto & \omega_\pi(a) - \omega_\pi(b)\,. \end{array}$$

Die Abbildung ω_π heißt die zum Primelement π gehörige Exponentialbewertung von K. Es gilt

$$\begin{array}{rcl} \omega_\pi(xy) & = & \omega_\pi(x) + \omega_\pi(y) \\ \omega_\pi(x+y) & \geq & \min\big(\omega_\pi(x), \omega_\pi(y)\big) \end{array}$$

Satz 3.2.13.
Sei R faktoriell, $K = \text{Quot}\,(R)$ und $\mathfrak{P}$ ein Repräsentantensystem für die Klassen assoziierter Primelemente. Dann gilt:

(i) Jedes $a \in K, a \neq 0$ besitzt eine eindeutige Darstellung

$$a = \epsilon \prod_{\pi \in \mathfrak{P}} \pi^{\omega_\pi(a)} \qquad \text{mit } \epsilon \in R^\times$$

wobei $\omega_\pi(a) = 0$ für fast alle $\pi \in \mathfrak{P}$.

(ii) Sei $x \in K$. Dann $x \in R \iff \omega_\pi(x) \geq 0 \quad \forall \pi \in \mathfrak{P}$.

(iii) $a, b \in R$. Dann $a|b \iff \omega_\pi(a) \leq \omega_\pi(b) \quad \forall \pi \in \mathfrak{P}$.

(iv) Zu $a_1 \ldots a_n \in R$ existiert

$$\begin{aligned} ggT(a_1, \ldots, a_n) &= \prod_{\pi \in \mathfrak{P}} \pi^{\min_i(\omega_\pi(a_i))} \\ kgV(a_1, \ldots, a_n) &= \prod_{\pi \in \mathfrak{P}} \pi^{\max_i(\omega_\pi(a_i))} \end{aligned} .$$

Hierbei setzen wir $\pi^\infty = 0$. Der Beweis dieser Behauptungen folgt unmittelbar aus der Eindeutigkeit der Zerlegung bis auf assoziierte Elemente.

Definition 3.2.14.
Seien $\mathfrak{a}, \mathfrak{b}$ Ideale in einem Ring R mit Eins.

(i) $\mathfrak{a}$ und $\mathfrak{b}$ heißen teilerfremd, falls $\mathfrak{a} + \mathfrak{b} = R$ ist.

(ii) Die Menge

$$\mathfrak{ab} = \left\{ \sum_{endl} a_i b_i | a_i \in \mathfrak{a} \quad \text{und} \quad b_i \in \mathfrak{b} \right\}$$

heißt Produkt der Ideale $\mathfrak{a}$ und $\mathfrak{b}$. Sie ist ein Ideal von R mit

$$\mathfrak{ab} \subset \mathfrak{a} \cap \mathfrak{b} .$$

Lemma 3.2.15.
(i) Seien $\mathfrak{a}$ und $\mathfrak{b}$ teilerfremde Ideale von R. Dann ist

$$\mathfrak{ab} = \mathfrak{a} \cap \mathfrak{b} .$$

(ii) Ist $\mathfrak{b}$ teilerfremd zu $\mathfrak{a}_i$, $i = 1 \ldots n$, so ist $\mathfrak{b}$ auch teilerfremd zum Produkt $\mathfrak{a}_1 \ldots \mathfrak{a}_n$.

Beweis.

(i) Da $\mathfrak{a}$ und $\mathfrak{b}$ teilerfremd sind, gibt es eine Darstellung $1 = a + b$ mit $a \in \mathfrak{a}, b \in \mathfrak{b}$. Sei $c \in \mathfrak{a} \cap \mathfrak{b}$, dann gilt $c = ac + cb \in \mathfrak{ab}$. Damit ist auch die umgekehrte Inklusion $\mathfrak{a} \cap \mathfrak{b} \subset \mathfrak{ab}$ gezeigt.

(ii) Da $\mathfrak{a}_i$ und $\mathfrak{b}$ teilerfremd sind, finden wir Darstellungen $1 = b_i + a_i$ mit $a_i \in \mathfrak{a}_i$ und $b_i \in \mathfrak{b}$. Multiplikation dieser Gleichungen liefert

$$1 = \prod_{i=1}^{n}(b_i + a_i) = \underbrace{b_1 b_2 \dots b_n + \dots}_{\in \mathfrak{b}} + a_1 a_2 \dots a_n \in \mathfrak{b} + \mathfrak{a}_1\mathfrak{a}_2 \dots \mathfrak{a}_n$$

Damit ist aber $R = \mathfrak{b} + \mathfrak{a}_1 \dots \mathfrak{a}_n$, also sind auch $\mathfrak{a}_1\mathfrak{a}_2 \dots \mathfrak{a}_n$ und $\mathfrak{b}$ teilerfremd.

□

Satz 3.2.16. *(Chinesischer Restsatz, abstrakte Form)*
Seien $\mathfrak{a}_1 \dots \mathfrak{a}_n$ paarweise teilerfremde Ideale von R. Dann ist der natürliche Homomorphismus

$$\begin{array}{rcl} R/\mathfrak{a}_1 \dots \mathfrak{a}_n & \to & R/\mathfrak{a}_1 \times \dots \times R/\mathfrak{a}_n \\ x \bmod \mathfrak{a}_1, \dots \mathfrak{a}_n & \mapsto & (x \bmod \mathfrak{a}_1, \dots, x \bmod \mathfrak{a}_n) \end{array}$$

ein Isomorphismus. Dies heißt insbesondere: gegeben $x_1, \dots, x_n \in R$, gibt es ein $x \in R$ mit $x = x_i \mod \mathfrak{a}_i$. x ist modulo dem Ideal $\mathfrak{a}_1 \dots \mathfrak{a}_n$ eindeutig bestimmt.

Beweis.

Wegen Lemma 3.2.15 reicht es aus, den Fall $n = 2$ zu betrachten und dann vollständige Induktion anzuwenden.

Wir zeigen zunächst die Surjektivität von

$$\begin{array}{rcl} R & \to & R/\mathfrak{a}_1 \times R/\mathfrak{a}_2 \\ x & \mapsto & (x \mod \mathfrak{a}_1, x \mod \mathfrak{a}_2) \end{array} \tag{15}$$

Da $\mathfrak{a}_1, \mathfrak{a}_2$ teilerfremde Ideale sind, können wir $a_i \in \mathfrak{a}_i$ finden, so dass $1 = a_1 + a_2$. Für beliebige vorgegebene $x_1, x_2 \in R$ ist

$$x = x_2 a_1 + x_1 a_2$$

wegen

$$\begin{array}{rcccl} x & = & x_2 a_1 + x_1(1 - a_1) & = & x_1 \bmod \mathfrak{a}_1 \\ x & = & x_2(1 - a_2) + x_1 a_2 & = & x_2 \bmod \mathfrak{a}_2 \end{array}$$

eine Lösung der gesuchten Kongruenzen. Der Kern der Surjektion (15) ist $\mathfrak{a}_1 \cap \mathfrak{a}_2 = \mathfrak{a}_1\mathfrak{a}_2$ nach Lemma 3.2.15 (i). □

3.3 Primfaktorzerlegung in Polynomringen, Satz von Gauß

Offensichtlich wäre es eine grosse Hilfe bei der Untersuchung von Polynomen, zu wissen, dass gewisse Polynomringe faktoriell sind. Hauptresultat ist der Satz von Gauß, der aussagt, dass $R[X]$ faktoriell ist dann und nur dann, wenn R faktoriell ist. Im Beweis werden Quotientenkörper eine Rolle spielen. Daher wenden wir uns zunächst Polynomringen über Körpern zu.

Sei R in diesem Kapitel immer ein Integritätsring.

Satz 3.3.1.
$R[X]$ ist Hauptidealring genau dann, wenn R ein Körper ist. (Insbesondere sind Polynomringe über Körpern faktoriell.)

Beweis.

Sei R ein Körper, dann ist $R[X]$ euklidisch und nach 3.2.4 (ii) prinzipal.

Sei umgekehrt $R[X]$ Hauptidealring und I der Kern des Einsetzungeshomomorphismus:

$$\begin{array}{rccc} \varphi: & R[X] & \to & R \\ & X & \to & 0 \end{array}$$

Es ist offenbar $I = (X)$ und $R[X]/(X) \cong R$ ist integer. Also ist $X \in R[X]$ ein Primelement. Nach 3.2.8(i) ist im integren Ring $R[X]$ das Primelement X auch irreduzibel. Die Behauptung folgt daher aus $\square$

Lemma 3.3.2.
Sei A ein Hauptidealring und $\pi \in A$ irreduzibel. Dann ist A/π ein Körper.

Beweis.

Nach Satz 3.1.7 gibt es ein maximales Ideal $\mathfrak{m} \subset A$, das das Hauptideal (π) enthält. Da im Hauptidealring A das maximale Ideal von der Form $\mathfrak{m} = (a)$ mit $a \in A$ sein muss, folgt $a|\pi$. Da π irreduzibel ist, folgt $(a) = (\pi)$, also ist $A/\pi = A/\mathfrak{m}$ Körper.
Bemerkung: Für den Beweis ist ganz wesentlich, dass A ein Hauptidealring ist. $\square$

Lemma 3.3.3.
Sei $a \in R$, wobei R ein Ring mit Eins ist.

(i) Die kanonische Surjektion $R \twoheadrightarrow R/a$ setzen wir durch Anwendung auf die Koeffizienten fort auf die Polynomringe: $R[X] \twoheadrightarrow (R/a)[X]$. Sie gibt einen natürlichen Isomorphismus von R–Algebren

$$R[X]/a \xrightarrow{\sim} (R/a)[X]$$

(ii) $a \in R$ *ist prim in* R *dann und nur dann, wenn* a *ist prim in* $R[X]$ *ist.*

Beweis.

(i) Im Kern der Surjektion $R[X] \twoheadrightarrow (R/a)[X]$ liegen die Polynome, deren Koeffizienten alle Vielfache von a sind. Sie bilden aber gerade das von a erzeugte Hauptideal in $R[X]$.

(ii) $a \in R$ ist in R prim, dann und nur dann, wenn R/a integer ist, nach Definition von Primidealen. Genau dann ist aber auch der Ring $(R/a)[X]$ integer, der nach (i) isomorph zu $R[X]/a$ ist. Also ist genau in diesem Fall $R[X]/a$ integer, was aber wiederum heisst, dass a prim in $R[X]$ ist.

□

Satz 3.3.4.
Ist $R[X]$ *faktoriell, so auch* R*.*

Beweis.

Sei $a \in R, a \neq 0$. Als Element im faktoriellen Ring $R[X]$ hat a eine eindeutige Zerlegung

$$a = \epsilon p_1(X) \dots p_r(X)$$

mit $\epsilon \in R[X]^\times = R^\times$ und $p_i \in R[X]$ irreduziblen Polynomen, die im faktoriellen Ring $R[X]$ auch prim sind. Aus Gradgründen sind diese Polynome alle vom Grade Null, also $p_i(X) = \pi_i \in R$.

Nach Lemma 3.3.3 (ii) sind die π_i auch prim in R. Somit besitzt jedes $a \neq 0$ $a \in R$ eine Darstellung

$$a = \epsilon \pi_1 \dots \pi_r$$

mit $\epsilon \in R^\times$ und Primelementen $\pi_i \in R$. Für irreduzibles a ist diese Zerlegung nach Definition von Irreduzibilität von der Form $a = \epsilon\pi_1$. Mit π_1 ist dann aber auch a prim. Nach Satz 3.2.7 ist dann aber R faktoriell. □

Um die Umkehrung zu zeigen, brauchen wir einige Vorbereitungen.

Sei R im Folgenden faktoriell und $K = \mathrm{Quot}(R)$. Für ein Primelement $\pi \in R$, $\pi \neq 0$, bezeichne

$$\omega_\pi : K \to \mathbb{Z} \cup \{\infty\}$$

die zugehörige Exponentialbewertung. Die wird fortgesetzt auf den Polynomring durch:

$$\begin{aligned} \omega_\pi : \ K[X] &\to \mathbb{Z} \cup \{\infty\} \\ \omega_\pi\Big(\sum_i a_i X^i\Big) &= \min_i\{\omega_\pi(a_i)\} \end{aligned}$$

Es gilt

$$\omega_\pi(cf) = \omega_\pi(c) + \omega_\pi(f) \qquad \forall c \in K, f \in K[X]\,. \tag{16}$$

Lemma 3.3.5.
Sei R faktoriell und $0 \neq \pi \in R$ prim. Betrachte zwei Polynome $f, g \in K[X]$. Dann gilt

$$\omega_\pi(gf) = \omega_\pi(g) + \omega_\pi(f)\,.$$

Beweis.

Indem wir einen Hauptnenner für die Koeffizienten des Polynoms finden, finden wir für jedes $f \in K[X]$ ein $c \in R$, so dass $cf \in R[X]$. Wegen (16) reicht es daher aus, die Behauptung für $f, g \in R[X]$ zu zeigen. Zur Abkürzung lassen wir den Index π fort und schreiben $\omega(f) = \omega_\pi(f)$.

Sei nun $g = \pi^{\omega(g)} g_1 \quad f = \pi^{\omega(f)} f_1$ mit $\omega(g_1) = \omega(f_1) = 0$. Damit ist auch

$$gf = \pi^{\omega(g)}\pi^{\omega(f)} g_1 f_1 = \pi^{\omega(g)+\omega(f)} g_1 f_1$$

und wegen $(*)$

$$\omega(gf) = \omega(g) + \omega(f) + \omega(g_1 f_1)\,.$$

Es bleibt somit zu zeigen, dass

$$\omega(g_1 f_1) = 0\,.$$

Aber wäre $\omega(g_1 f_1) > 0$, so teilte $\pi | g_1 f_1$. Nach Lemma 3.3.3 (ii) ist π auch prim im Polynomring, also müsste π entweder f_1 oder g_1 teilen, so dass entweder $\omega(g_1) > 0$ oder $\omega(f_1) > 0$ gelten müsste, Widerspruch. □

Definition 3.3.6.

(i) Sei f ein Polynom in $R[X]$, $f(X) = \sum_{i=0}^n a_i X^i$, $\operatorname{grad}(f) \geq 1$. f heißt primitiv, falls $ggT(a_0, \ldots, a_n) = 1$.

(ii) Sei R faktoriell, $f \in R[X]$, grad $f \geq 1$. Dann gibt es eine Darstellung von f

$$f = ag \quad a \in R\backslash\{0\} \quad g \in R[X] \quad \textit{primitiv}$$

a ist das ggT der Koeffizienten und bis auf Assoziiertheit eindeutig. Das Hauptideal (a) heißt Inhalt von f.

Aus Lemma 3.3.5 folgt

$$\textit{Inhalt}\,(gf) \;=\; \textit{Inhalt}\,(g) \;\cdot \textit{Inhalt}\,(f)\,.$$

Lemma 3.3.7.
Sei R faktoriell, $K :=$ Quot (R) und $g \in R[X]$ mit grad $f \geq 1$. *Ist g primitiv, so gilt*

$$g \textit{ irreduzibel in } K[X] \;\Rightarrow\; g \textit{ irreduzibel in } R[X]\,.$$

Beweis.

Sei $g \in R[X]$ irreduzibel in $K[X]$. Wir nehmen an, dass wir g als Produkt schreiben können,

$$g = ab \quad \text{mit} \quad a, b \in R[X] \hookrightarrow K[X]\,.$$

Da g irreduzibel in $K[X]$ ist, ist einer der Faktoren, etwa $a \in K[X]^\times = K^\times$. Also liegt a in $K^\times \cap R[X] = R \setminus \{0\}$. g ist also genau dann in $R[X]$ irreduzibel, wenn man aus den Koeffizienten keinen gemeinsamen Faktor in R herausziehen kann, also wenn g primitiv ist.

Ein Beispiel: Das Polynom $g(X) = 2X + 4$ ist irreduzibel in $\mathbb{Q}[X]$, nicht in $\mathbb{Z}[X]$, da $g = 2(X + 2)$ und 2 zwar eine Einheit in $\mathbb{Q}$, aber nicht in $\mathbb{Z}$ ist. □

Satz 3.3.8. *(Gauß)*
Ist R faktoriell, so auch $R[X]$. Genauer gilt:
Sei R faktoriell mit Quot$(R) = K$ *und $\mathfrak{P}_1$ (bzw. $\mathfrak{P}_2$) ein Repräsentantensystem für die Klassen assoziierter Primelemente von R (bzw. von $K[X]$ bestehend aus primitiven Polynomen von $R[X]$).*

Dann ist $R[X]$ faktoriell und $\mathfrak{P}_1 \cup \mathfrak{P}_2$ ist ein Repräsentantensystem der Klassen assoziierter Primelemente von $R[X]$.

Beweis.

Die Idee des Beweises ist, erst mit dem Polynomring über dem Quotientenkörper zu arbeiten und dann Bewertungen einzusetzen.

$K[X]$ ist nach Satz 3.3.1 Hauptidealring und daher nach Satz 3.2.10 faktoriell. Jedes Primelement in $K[X]$ ist assoziiert zu einem primitiven

Polynom in $R[X]$. Daher existieren die geforderten Repräsentantensysteme.

Wir wollen zeigen, dass ein beliebiges Element $g \in R[X]$ eindeutig als Produkt von Element in $\mathfrak{P}_1 \cup \mathfrak{P}_2$ und einer Einheit geschrieben werden kann. Dazu fassen wir g zunächst als Element des faktoriellen Rings $K[X]$ auf. Dort finden wir eine Zerlegung

$$g = a \prod_{f \in \mathfrak{P}_2} f^{e_f}$$

mit $a \in K^\times$ und $e_f \geq 0$, aber fast alle e_f gleich Null. Diese Zerlegung ist eindeutig in $K[X]$, da dieser Ring faktoriell ist.

Für jedes $\pi \in \mathfrak{P}_1$ gilt nach Lemma 3.3.5

$$0 \leq \omega_\pi(g) = \omega_\pi(a) + \sum_{f \in \mathfrak{P}_2} e_f \omega_\pi(f) = \omega_\pi(a)$$

da alle f primitive Polynome in $R[X]$ sind.

Da somit $\omega_\pi(a) \geq 0$ für alle $\pi \in \mathfrak{P}_1$ ist, ist $a \in R$. Sei also

$$a = \epsilon \prod_{\pi \in \mathfrak{P}_1} \pi^{e_\pi} \quad \text{mit} \quad \epsilon \in R^\times, e_\pi \geq 0, \quad \text{fast alle Null}$$

die Primfaktorzerlegung im faktoriellen Ring R. Auch diese Zerlegung ist eindeutig. Insgesamt erhalten wir eine Zerlegung in irreduzible Elemente

$$g = \epsilon \prod_{\pi \in \mathfrak{P}_1} \pi^{e_\pi} \prod_{f \in \mathfrak{P}_2} f^{e_f}$$

in $R[X]$, da nach 3.3.3 (ii) π auch in $R[X]$ prim ist und nach Lemma 3.3.7 f auch in $R[X]$ irreduzibel ist. Diese Zerlegung ist überdies eindeutig, also ist $R[X]$ faktoriell. □

Korollar 3.3.9.
Sei R faktoriell, $K :=$ Quot (R) und $g \in R[X]$ mit grad $f \geq 1$. *Dann gilt:*

$$g \text{ irreduzibel in } R[X] \;\Rightarrow\; g \text{ irreduzibel in } K[X]$$

Beweis.
Sei g irreduzibel in $R[X]$. Nach Satz dem Satz 3.3.8 von Gauß schreibt sich $g = \epsilon f$ mit $\epsilon \in R^\times$ und $f \in \mathfrak{P}_2$. Damit ist aber g auch irreduzibel in $K[X]$. □

Satz 3.3.10. *(Lemma von Gauß)*
Sei R faktoriell, $K = \text{Quot}\,(R)$ und $f \in R[X]$. Lässt sich f als Produkt von normierten Polynomen $g, h \in K[X]$ schreiben, $f = gh$, so liegen sind deren Koeffizienten schon in R: es gilt $g, h \in R[X]$.

Beweis.

Der Beweis benutzt Bewertungen im faktoriellen Ring $R[X]$. Sei $\pi \in R$ prim. Da $f \in R[X]$ liegt, ist $\omega_\pi(f) \geq 0$. Da g, h normierte Polynome sind, ist

$$\begin{aligned} \omega_\pi(g) &\leq \omega_\pi(1) = 0 \\ \omega_\pi(h) &\leq \omega_\pi(1) = 0 \end{aligned}$$

Aus Lemma 3.3.5 folgt $\omega_\pi(f) = \omega_\pi(g) + \omega_\pi(h)$. Damit ist aber $\omega_\pi(g) = \omega_\pi(h) = 0$, somit liegen $g, h \in R[X]$. □

Korollar 3.3.11.
Sei R faktoriell und $K = \text{Quot}\,(R)$. Sei $f \in R[X]$ ein normiertes Polynom und sei $\alpha \in K$ eine Nullstelle von f. Dann liegt $\alpha \in R$ und α teilt den Absolutkoeffizienten $a_0 = f(0)$ von f.

Beweis.

Nach den Annahmen gilt in $K[X]$ die Zerlegung $f(X) = (X - \alpha)g(X)$ mit $g(X) \in K[X]$ einem normierten Polynom. Nach dem Lemma 3.3.10 von Gauß ist dann $X - \alpha \in R[X]$ und $g \in R[X]$. Damit liegt aber $\alpha \in R$. Ferner gilt $a_0 = f(0) = -\alpha g(0)$, also teilt α den Absolutkoeffizienten a_0. □

Dieser Satz ist bemerkenswert: er sagt insbesondere aus, dass die Nullstellen normierter Polynome mit ganzen Koeffizienten entweder ganze Zahlen sind oder irrational. Sind sie ganz, so kommen auch nur die Teiler des Absolutkoeffizienten in Frage. Betrachtet man z.B. das Polynom $f(X) = X^n - 2$ mit $n \geq 2$, so sieht man, dass alle Wurzeln aus 2 irrational sein müssen.

Wir wollen nun noch ein wichtiges Kriterium herleiten, mit dem wir irreduzible Polynome erkennen können. Dies wird es uns insbesondere ermöglichen, Minimalpolynome zu identifizieren. Zur Vorbereitung beweisen wir den folgenden Satz:

Satz 3.3.12.
Sei R integer, $I \subseteq R$ Primideal. Die kanonische Surjektion

$$\begin{aligned} R &\twoheadrightarrow R/I =: \overline{R} \\ a &\mapsto \overline{a} = \text{mod}\, I \end{aligned}$$

setzen wir fort zu einer Surjektion

$$R[X] \twoheadrightarrow \overline{R}[X]\,.$$

Sei $f(X) = a_nX^n + \cdots + a_0 \in R[X]$ *primitiv mit* $\overline{a}_n \neq 0$. *Ist dann* $\overline{f}$ *irreduzibel in* $\bar{R}[X]$, *so ist auch* f *irreduzibel in* $R[X]$.
Achtung, die Umkehrung gilt nicht! Aus Bemerkung 3.3.14 wird folgen, dass $f(X) = X^2 - p \in \mathbb{Z}[X]$ *irreduzibel ist, aber* $\overline{f}(X) = X^2 = X \cdot X$ *ist in* $\mathbb{Z}/p[X]$ *natürlich reduzibel.*

Beweis.

Angenommen, wir finden eine Darstellung $f = gh$ mit $g, h \in R[X]$. Da f primitiv ist, kann man keinen Faktor in R aus f ziehen. Also haben g und h Grad größer gleich Eins.

Aus der Darstellung $\overline{f} = \overline{g}\overline{h}$ und der Tatsache, dass $\overline{a}_n \neq 0$, folgt auch, dass

$$\text{grad } \overline{g} = \text{grad } g \geq 1 \quad \text{ und grad } \overline{h} = \text{grad } h \geq 1\,.$$

Da I prim ist, ist $\overline{R}$ integer, also sind alle Einheiten Polynome vom Grad Null, $\overline{R}[X]^\times = \overline{R}^\times$. Man hat somit einen Widerspruch zur Irreduzibilität von $\overline{f}$ in $\bar{R}[X]$. □

Satz 3.3.13. *(Irreduzibilitätskriterium von Eisenstein)*

Sei R *integer und* $f(X) = a_nX^n + \cdots + a_1X^1 + a_0 \in R[X]$ *primitiv. Sei* $\pi \in R$ *prim und gelte*

$$\begin{array}{lll} \text{(i)} & \pi \nmid a_n & \\ \text{(ii)} & \pi \mid a_i & i = 0, 1, \ldots, n-1\,. \\ \text{(iii)} & \pi^2 \nmid a_0 & \end{array}$$

Dann ist f *irreduzibel in* $R[X]$. *Ist* R *faktoriell, so ist* f *nach 3.3.9* (i) *auch irreduzibel in* Quot $(R)[X]$.

Ein primitives Polynom mit den Eigenschaften (i)–(iii) heißt auch Eisensteinpolynom bezüglich $\pi \in R$.

Beweis.

Da π prim ist, ist $\overline{R} = R/\pi$ integer. Wäre f reduzibel, so hätte man, da f primitiv ist,

$$f = gh$$

mit $r = \text{grad } g \geq 1$ und $s = \text{grad } h \geq 1$. Dies ergäbe eine entsprechende Zerlegung in $\bar{R}[X]$ der Form

$$\bar{f} = \bar{g}\bar{h}$$

Aus Bedingung (i) folgt grad $\overline{g} = r$ und grad $\overline{h} = s$.
Aus Bedingung (ii) können wir $\bar{f}$ berechnen: $\overline{f}(X) = \overline{a}_n X^n$.

Da $\overline{R}$ integer ist, existiert der Quotientenkörper $k = \text{Quot}\,(\overline{R})$. Wir fassen $\overline{f}$ als Element des Rings $k[X]$ auf, der als Hauptidealring faktoriell ist. In diesem Ring sind die einzig möglichen Zerlegungen von $\bar{f}$

$$\overline{g} = \beta X^r \quad \overline{h} = \gamma X^s \quad \beta, \gamma \in k \quad \text{so dass} \quad \beta\gamma = \overline{a}_n\,.$$

Da $r, s \geq 1$, ist $\overline{g}(0) = \overline{h}(0) = 0$.

Also teilt π sowohl $g(0)$ also auch $h(0)$, so dass das π^2 in $g(0)h(0) = a_0$ aufgeht, im Widerspruch zur Bedingung (iii). □

Bemerkungen 3.3.14.

(i) Sei $a \in \mathbb{Z}\backslash\{\pm 1\}$ quadratfrei, d.h. für alle $p \in \mathbb{Z}$ prim gelte $p^2 \not| a$. Dann ist $X^n - a \in \mathbb{Z}[X]$ nach Satz 3.3.13 irreduzibel.

(ii) Wir werden das Eisensteinkriterium vor allem auf normierte Polynome anwenden, da Minimalpolynome normiert sind. Normierte Polynome sind immer primitiv, und auch Kriterium (i) in Satz 2.3.13 ist dann automatisch erfüllt.

Korollar 3.3.15.
Sei $p \in \mathbb{Z}$ eine Primzahl. Dann ist das Polynom

$$F_p(X) = X^{p-1} + X^{p-2} + \cdots + x + 1$$

irreduzibel in $\mathbb{Q}[X]$.

Beweis.

Offenbar ist $F_p(X)(X-1) = X^p - 1$. Betrachte

$$f(X) := F_p(x+1)\,.$$

Es gilt

$$f(X)X = (x+1)^p - 1 = \sum_{k=0}^{p} \binom{p}{k} X^k - 1$$

mithin

$$f(X) = \sum_{k=1}^{p} \binom{p}{k} X^{k-1} = X^{p-1} + \binom{p}{p-1} X^{p-2} + \cdots + \binom{p}{2} X + p\,.$$

Dies ist ein Eisensteinpolynom bezüglich p, also irreduzibel. Lediglich Bedingung (ii) ist nicht ganz offensichtlich, aber

$$p \left| \binom{p}{k} = \frac{p(p-1)\dots(p-k+1)}{1 \cdot 2 \cdot \ldots \cdot k} \quad \text{für } k = 2, \dots p-1 \ , \right.$$

denn die Primzahl p teilt den Zähler genau einmal, den Nenner aber nicht.

Nun induziert aber die Abbildung $X \mapsto X+1$ einen Ringautomorphismus von $\mathbb{Q}[X]$ mit Umkehrabbildung. $X \mapsto X-1$. Damit folgt aus der Irreduzibilität von f die von $F_p(X)$.

□

Mit Hilfe des Eisensteinkriteriums können wir zwei Konstruktionsprobleme näher untersuchen.

Satz 3.3.16.
Sei $n = p$ eine Primzahl. Ist $p-1$ keine Potenz von 2, so ist die Konstruktion des regulären p–Ecks mit Zirkel und Lineal nicht *möglich.*

Man kann also z.B. das reguläre $p = 7, 11, 13$ und 19-Eck nicht mit Zirkel und Lineal konstruieren. Gauß hat als 18-jähriger das reguläre 17–Eck konstruiert. In der Vorlesung Algebra II werden wir sehen, dass die Konstruktion für Primzahlen der Form $p = 2^m + 1$ tatsächlich möglich ist; siehe auch Satz 4.3.11.

Beweis.
Sei $\xi = e^{2\pi \mathrm{i}/p}$. Da ξ eine algebraische Gleichung erfüllt, $\xi^p - 1 = 0$, ist ξ algebraisch. Ist $\xi \in \mathcal{A}\mathbb{Q}$, so muss wegen 2.1.11 (ii) der Körpergrad $[\mathbb{Q}(\xi) : \mathbb{Q}]$ eine Potenz von 2 sein. Wir berechnen den Körpergrad als Grad des Minimalpolynoms und behaupten:

$$\min_{\mathbb{Q}}(\xi) = F_p(X) \, ,$$

denn $F_p(X)$ ist normiert, irreduzibel nach 3.3.15, also wegen $F_p(\xi) = 0$ nach 2.3.14 (ii) das Minimalpolynom von ξ. Damit finden wir $[\mathbb{Q}(\xi) : \mathbb{Q}] = \operatorname{grad} F_p(X) = p - 1$. □

Satz 3.3.17.
Sei φ mit $0 \leq \varphi < 2\pi$ derart, dass $e^{\mathrm{i}\varphi}$ transzendent ist. Dann ist die Winkeldrittelung von φ mit Zirkel und Lineal nicht möglich.

(Bemerkung: da $\varphi \mapsto e^{\mathrm{i}\varphi}$ eine Bijektion zwischen $[0, 2\pi)$ und dem Einheitskreis ist, ist die Voraussetzung für überabzählbar viele Winkel φ erfüllt.)

Beweis.

Sei $t := e^{\mathrm{i}\varphi}$ transzendent über $\mathbb{Q}$. Wir betrachten den Körper $K := \mathbb{Q}(t)$ und wollen zeigen, dass $z := e^{\mathrm{i}\varphi/3} \notin \mathcal{A}K$. Wegen 2.1.11 (ii) reicht es zu zeigen, dass

$$[K(z) : K] = 3\,.$$

Da z eine Nullstelle des normierten Polynoms $X^3 - t \in K[X]$ ist, ist die Behauptung gezeigt, wenn wir wissen, dass $X^3 - t$ in $K[X]$ irreduzibel ist.

Nach Satz 3.1.3 ist K isomorph zum rationalen Funktionenkörper über $\mathbb{Q}$. Unter der Isomorphie geht die Variable X des Funktionenkörpers auf t. Daher ist K der Quotientenkörper des Rings $\mathbb{Q}[t]$, der isomorph zum Polynomring über dem Körper $\mathbb{Q}$ ist. Daher ist $R = \mathbb{Q}[t]$ euklidisch, also insbesondere faktoriell. Das Element t ist im Ring $R = \mathbb{Q}[t]$ prim, denn $\mathbb{Q}[t]/t \cong \mathbb{Q}$ ist integer.

$X^3 - t$ ist dann aber Eisensteinpolynom in $R[X]$ bezüglich des Primelements t und somit irreduzibel. Damit ist die Behauptung gezeigt. □

4 Galoistheorie

Wir haben jetzt alle Hilfsmittel bereitgestellt, um uns der Galoistheorie zuwenden zu können. Diese stellt eine tiefe Beziehung zwischen einer Klasse von Körpererweiterungen und Gruppen her. Um zu verstehen, welche Klasse von Körpererweiterungen uns interessiert, erinnern wir daran, dass eine der grundlegenden Motivationen der Algebra die Frage der Auflösbarkeit von (polynomialen) Gleichungen war. Wir wenden uns daher in Kapitel 4.1 Zerfällungskörpern von Polynomen zu, was uns auf den Begriff der normalen Körpererweiterung führen wird. Eine weitere wichtige Bedingung wird sein, dass Minimalpolynome keine mehrfachen Nullstellen haben. Dadurch werden wir in Kapitel 4.2 auf den Begriff einer separablen Körpererweiterung geführt. In Kapitel 4.3 geben wir dann einen Ausblick auf die Galoistheorie, die im Rahmen der Vorlesung Algebra II vertieft behandelt werden wird.

4.1 Zerfällungskörper und normale Körpererweiterungen

Definition 4.1.1.
Sei K ein Körper und $f \in K[X]$ ein Polynom. Unter einem Zerfällungskörper von f verstehen wir eine Körpererweiterung L/K, so dass

(i) f in $L[X]$ vollständig in Linearfaktoren zerfällt.

(ii) L über K von den Nullstellen von f erzeugt wird.

Wir wollen auf den folgenden Satz hinaus:

Satz 4.1.2.
Sei K ein Körper und $f \in K[X]$. Sind L/K und L'/K zwei Zerfällungskörper von f, so gibt es einen Isomorphismus

$$\sigma : L \to L'$$

mit der Eigenschaft, dass $\sigma_{|K} = id_K$.

Warnung: man spricht zwar von *dem* Zerfällungskörper, aber die Isomorphismen zwischen verschiedenen Zerfällungskörpern sind i.a. nicht eindeutig.

Definition 4.1.3.

(i) Seien $i : K \hookrightarrow L$ und $j : K \hookrightarrow L'$ zwei Körpererweiterungen desselben Grundkörpers K. Ein Körperhomomorphismus $\varphi : L \to L'$ mit $\varphi \circ i = j$ heißt auch Homomorphismus von Körpererweiterungen.
$Alg_K(L, L')$ bezeichne die Menge aller solchen Homomorphismen.

(ii) Wir schreiben auch $\tilde{j} = \varphi$ und nennen $\tilde{j}$ die Ausdehnung von j auf L. Diese Bezeichnung wird aus dem folgenden kommutierenden Diagram deutlich:

$$\begin{array}{ccccc} & & L & \overset{\tilde{j}}{\searrow} & \\ i & \uparrow & & & L' \\ & K & \overset{j}{\nearrow} & & \end{array}$$

Satz 4.1.4.
Sei $K(\alpha)$ eine primitive algebraische Erweiterung eines Körpers K und sei $j : K \hookrightarrow M$ eine beliebige Körpererweiterung. Dann werden die Ausdehnungen von j zu einer Einbettung

$$\tilde{j} : K(\alpha) \hookrightarrow M$$

parametrisiert durch die Nullstellen des Minimalpolynoms $\min_K(\alpha)$ in M:

$$\begin{array}{ccc} Alg_K(K(\alpha), M) & \xrightarrow{\sim} & \{\beta \in M | \min_K(\alpha)(\beta) = 0\} \\ \varphi & \mapsto & \varphi(\alpha) \end{array}$$

Beweis.
Sicher ist dies eine injektive Abbildung zwischen den angegebenen Mengen und nur die Surjektivität ist zu zeigen. Sei also $\beta \in M$ eine Nullstelle des Minimalpolynoms. Wir wissen, dass der Körper $K[X]/\min_K(\alpha)$ sowohl isomorph zu $K(\alpha)$ ist, wobei die Klasse von X auf α abgebildet wird, also auch zum Unterkörper $K(\beta) \subseteq M$, wobei die Klasse von X auf β abgebildet wird. Es gibt also einen Körperisomorphismus, der $K(\alpha)$ und $K(\beta) \hookrightarrow M$ identifiziert und α auf β abbildet. □

Satz 4.1.5. *(Ausdehnbarkeitskriterium)*
Sei $K(\alpha_1, \ldots, \alpha_n)$ eine endliche Erweiterung eines Körpers K und sei $j : K \hookrightarrow M$ eine Körpererweiterung mit der Eigenschaft, dass alle Minimalpolynome

$$\min_K(\alpha_i) \qquad i = 1 \ldots n$$

in $M[X]$ vollständig in Linearfaktoren zerfallen. Dann lässt sich j ausdehnen zu

$$\begin{array}{ccc} K & \hookrightarrow & K(\alpha_1, \ldots, \alpha_n) \\ & \overset{j}{\searrow} & \downarrow \tilde{j} \\ & & M \ . \end{array}$$

Beweis.

Nach Satz 4.1.4 liefert die Einschränkung Surjektionen

$$\begin{aligned}&\mathrm{Alg}_K(K(\alpha_1,\dots\alpha_n),M) \twoheadrightarrow \mathrm{Alg}_K(K(\alpha_1,\dots\alpha_{n-1}),M)\\ &\twoheadrightarrow\cdots\twoheadrightarrow \mathrm{Alg}_K(K,M)\end{aligned}$$

□

Wir zeigen nun Satz 4.1.2:

Beweis.

Nach Satz 4.1.5 haben wir Injektionen $L' \hookrightarrow L$ und $L \hookrightarrow L'$. Da L und L' endlich–dimensionale K–Vektorräume sind, sind dies sogar Isomorphismen. □

Satz 4.1.6.

Sei L/K endliche Körpererweiterung und $j : K \hookrightarrow M$ eine Einbettung in einen Körper M. Dann gibt es höchstens $[L : K]$ Fortsetzungen von j zu $\tilde{j} : L \hookrightarrow M$:

$$\Big|\ Alg_K(L,M)\Big| \leq [L:K]\,.$$

Beweis.

Besitzt L/K einen echten Zwischenkörper $K \subset L' \subset L$, so folgt der Satz mittels vollständiger Induktion nach dem Körpergrad $[L : K]$:

$$\Big|\,\mathrm{Alg}_K(L,M)\Big| = \Big|\,\mathrm{Alg}_K(L',M)\Big|\Big|\mathrm{Alg}_{L'}(L,M)\Big| \leq [L':K][L:L'] = [L:K]\,.$$

Hierbei ging in der Ungleichung die Induktionsannahme und in der letzten Gleichung die Gradformel ein.

Gibt es keine Zwischenkörper, so ist nach Satz 2.3.18 L/K einfache Körpererweiterung, $L = K(\alpha)$. Wir finden

$$\Big|\mathrm{Alg}_K(L,M)\Big| = \#\{\text{Nst.von}\min_K(\alpha)\text{ in }M\} \leq \operatorname{grad}\min_K(\alpha) = [K(\alpha):K]\,.$$

wobei erst Satz 4.1.4 benutzt wird und dann die Tatsache, dass die Zahl der Nullstellen eines Polynoms durch seinen Grad beschränkt ist. □

Definition 4.1.7.

Eine Körpererweiterung L/K heißt <u>normal</u>, wenn sie algebraisch ist und wenn jedes irreduzible *Polynom aus $K[X]$, das in L eine Nullstelle hat, in $L[X]$ schon vollständig in Linearfaktoren zerfällt.*

Beispiel 4.1.8.
$\mathbb{Q}\left(\sqrt[3]{2}\right)$ ist nicht normal über $\mathbb{Q}$, denn wir können $\mathbb{Q}\left(\sqrt[3]{2}\right)$ in $\mathbb{R}$ einbetten. Die beiden anderen Wurzeln des in $\mathbb{Q}[X]$ irreduziblen Polynoms X^3-2 sind nicht reell und können nicht in $\mathbb{Q}\left(\sqrt[3]{2}\right)$ liegen.

Satz 4.1.9.
Für eine endliche Körpererweiterung L/K sind äquivalent:

(i) L/K ist normal

(ii) L ist Zerfällungskörper eines Polynoms $f \in K[X]$.

Beweis.

(i)⇒ (ii) Ist L/K normal, $L = K(\alpha_1, \ldots, \alpha_r)$, so ist L der Zerfällungskörper des Produkts

$$f = \prod_{i=1}^{r} \min_K(\alpha_i)$$

Für die umgekehrte Richtung zeigen wir (ii) ⇒ (iii) ⇒ (i) mit

(iii) Gegeben eine beliebige Körpererweiterung $j : K \hookrightarrow M$, dann haben alle Fortsetzungen von j zu Einbettungen $\psi, \varphi : L \hookrightarrow M$ dasselbe Bild:

$$\varphi(L) = \psi(L) \quad \text{für alle } \varphi, \psi \in \operatorname{Alg}_K(L, M)\,.$$

(ii) ⇒ (iii) Sowohl φ als ψ identifizieren die Nullstellen von f in L mit den Nullstellen von f in M, aber vielleicht in verschiedener Weise. Da L als Zerfällungskörper von diesen Nullstellen erzeugt wird, folgt die Gleichheit der Bilder, $\psi(L) = \varphi(L)$.

(iii) ⇒ (i) Sei $f \in K[X]$ irreduzibel mit Nullstelle $\alpha \in L$. Wir wollen zeigen, dass f in L vollständig in Linearfaktoren zerfällt. Dazu ergänzen wir α zu einem endlichen Erzeugendensystem von L über K:

$$L = K(\alpha, \beta_1, \ldots, \beta_n)\,.$$

Wähle für M eine Körpererweiterung von L, in der alle Polynome

$$\min_K(\alpha) \quad \text{und} \quad \min_K(\beta_i)$$

vollständig in Linearfaktoren zerfallen.

Sei α' eine Nullstelle von f. Nach Satz 4.1.4 können wir $K \hookrightarrow M$ fortsetzen zu

$$\begin{array}{ccc} K(\alpha) & \hookrightarrow & M \\ \alpha & \mapsto & \alpha' \end{array}$$

und dies nach 4.1.5 und der Konstruktion von M zu einer Einbettung

$$\varphi : L \hookrightarrow M\,.$$

Jede Nullstelle von f liegt also in $\varphi(L)$ für ein geeignetes φ, also in $\varphi(L) = \mathrm{id}(L) = L$ wegen (iii), da ja L in M liegt und die Identität eine andere Einbettung liefert. Also ist L/K normal.

□

Satz 4.1.10.
Jede endliche Körpererweiterung L/K lässt sich zu einer endlichen normalen Körpererweiterung N/K vergrößern, d.h. es gibt einen Körperturm $N \supset L \supset K$, so dass N/K normal ist.

Beweis.
Seien $\alpha_1, \ldots \alpha_r$ Erzeuger von L über K. Konstruiere N als Zerfällungskörper über L von

$$f = \prod_{i=1}^{r} \min_K(\alpha_i)$$

N ist auch Zerfällungskörper von f über K und damit nach Satz 4.1.9 normal. □

Man kann zeigen, dass die kleinste solche Erweiterung bis auf Isomorphie von Körpererweiterungen eindeutig ist. Sie heißt *normale Hülle*. Zum Beispiel ist die Körperweiterung $\mathbb{Q}(\sqrt[3]{2}, \mathrm{i})$ über $\mathbb{Q}$ die normale Hülle von $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$.

4.2 Vielfachheit von Nullstellen, separable Körpererweiterungen

Ziel ist der Beweis des folgenden Satzes:

Satz 4.2.1.
Seien $K \subset L$ Körper und $f \in K[X]$ irreduzibel. Ist $\mathrm{char}(K) = 0$*, so hat f keine mehrfachen Nullstellen in L.*

Lemma 4.2.2.
Seien $K \subset L$ Körper, $f, g \in K[X]$ und $g \neq 0$.

(i) Teilen mit Rest führt auf das gleiche Resultat in $K[X]$ und $L[X]$.

(ii) g teilt f in $L[X]$ dann und nur dann, wenn g das Polynom f in $K[X]$ teilt.

(iii) Der normierte größte gemeinsame Teiler d_K von f und g in $K[X]$ ist gleich dem normierten größten gemeinsamen Teiler d_L in $L[X]$.

Beweis.

(i) Der euklidische Algorithmus erlaubt es, in eindeutiger Weise $f = qg + r$ zu schreiben mit $q, r \in K[X]$ und grad $r <$ grad g.

(ii) Ist ein Spezialfall von (i) mit $r = 0$.

(iii) Offenbar ist d_K auch gemeinsamer Teiler von f und g in $L[X]$, also $d_K | d_L$. Andererseits liefert der euklidische Algorithmus $p, q \in K[X]$ so dass

$$d_K = qf + pg\,.$$

Da diese Gleichung erst recht in $L[X]$ gilt, folgt $d_L | d_K$. Da die beiden Polynome d_L und d_K normiert sind, folgt $d_K = d_L$.

□

Definition 4.2.3.
Sei R ein Ring, $f \in R[X]$. Die formale Ableitung $f' \in R[X]$ ist das Polynom

$$\begin{aligned} f &= \sum_{i=0}^{n} a_i X^i \\ f' &= \sum_{i=0}^{n} i a_i X^{i-1}\,. \end{aligned}$$

Lemma 4.2.4.
(i) Ist $f \in R \subseteq R[X]$ konstant, so gilt $f' = 0$. (Vorsicht, die Umkehrung gilt für allgemeine Ringe nicht!)

(ii) $(f + g)' = f' + g'$

(iii) Leibnizregel: $(fg)' = f'g + fg'$

(iv) Sei K ein Körper, $g \in K[X]$ ungleich Null und $\alpha \in K$ eine Nullstelle von g.

$$\alpha \quad \textit{ist mehrfache Nullstelle von } G \quad \iff g'(\alpha) = 0$$

Beweis.

(i) – (iii) sollte aus der Schule bekannt sein.

(iv) Ist α mehrfache Nullstelle, so gilt $g = (X-\alpha)^2 f$ für ein $f \in K[X]$. Damit ist $g' = 2(X-\alpha)f + (X-\alpha)^2 f'$; Einsetzen zeigt $g'(\alpha) = 0$. Gilt umgekehrt $g(\alpha) = g'(\alpha) = 0$, so schreibe $g = (X-\alpha)h(X)$. Ableiten und Einsetzen von α zeigt $0 = g'(\alpha) = h(\alpha)$, also $g(X) = (X-\alpha)^2\tilde{h}(X)$.

□

Satz 4.2.5.
Sei K Körper und $f \in K[X]$. Dann sind äquivalent:

(i) f hat in seinem Zerfällungskörper mehrfache Nullstellen.

(ii) f und f' sind nicht teilerfremd, $(f) + (f') \neq L[X]$.

Beweis.

(i) ⇒ (ii) Ist α mehrfache Nullstelle, so ist $(X-\alpha)$ gemeinsamer Teiler von f und f' in $L[X]$.

(ii) ⇒ (i) Im Zerfällungskörper des Produkts ff' gibt es ein Element α, so dass $X-\alpha$ sowohl f als auch f' teilt. Also hat f eine mehrfache Nullstelle.

□

Bemerkung 4.2.6.
In einem Körper K der Charakteristik p hat jedes Element $a \in K$ höchstens eine p–te Wurzel. Denn gilt $b^p = a$, so ist $X^p - a = (X-b)^p$, so dass b die einzige Nullstelle des Polynoms $X^p - a$ ist.

Korollar 4.2.7.
Sei K ein Körper und $f \in K[X]$ irreduzibel. *Dann sind äquivalent:*

(i) f hat mehrfache Nullstellen in seinem Zerfällungskörper

(ii) Die Ableitung f' von f ist das Nullpolynom.

(iii) Es gilt char $K > 0$, *also* char $K = p$ *mit* p *prim und es gibt* $g \in K[X]$ *mit* $f(X) = g(X^p)$.

Beweis.

(i) $\Rightarrow$ (ii) Nach Satz 4.2.5 sind dann f und f' nicht teilerfremd. Da f irreduzibel sein soll, teilt f seine Ableitung f'. Diese hat aber kleineren Grad als f, daher ist nur $f' = 0$ möglich.

(ii) $\Rightarrow$ (iii) Offenbar ist $f' = 0$ äquivalent zu $ia_i = 0$ für alle i. Dies ist nur in endlicher Charakteristik möglich, und es können nur die a_i mit $i = 0 \bmod p$ nicht verschwinden.

(iii) $\Rightarrow$ (i) In diesem Falle ist offenbar $f' = 0$, so dass f und f' zumindest f als gemeinsamen Teiler haben. Nach Satz 4.2.5 hat dann f eine mehrfache Nullstelle.

□

Definition 4.2.8.

(i) Sei K ein Körper. Ein Polynom $f \in K[X]$ vom Grad $n \geq 1$ heißt separabel, wenn f in einem Zerfällungskörper von f über K genau n verschiedene Nullstellen hat.

(ii) Sei L/K Körpererweiterung. Ein Element $\alpha \in L$ heißt separabel über K, wenn es algebraisch ist über K und sein Minimalpolynom separabel ist.

(iii) Die Körpererweiterung L/K heißt separabel, wenn jedes Element von L über K separabel ist.

(iv) Ein Körper heißt perfekt, wenn er entweder Charakteristik Null hat oder aber für $p = char\ K$ die Abbildung $K \to K$ mit $x \mapsto x^p$ surjektiv ist. (Insbesondere ist jeder endliche Körper perfekt, nicht aber der rationale Funktionenkörper $\mathbb{F}_p(t)$.)

Satz 4.2.9.

Ist K perfekt, so ist jede algebraische Erweiterung von K separabel.

Beweis.

Sei zunächst char $K = 0$. Ein Polynom $f \in K[X]$ hat nach Korollar 4.2.7 nur dann mehrfache Nullstellen in seinem Zerfällungskörper, wenn seine Ableitung verschwindet, was in Charakteristik Null nur für konstante Polynome geschehen kann. Solche treten aber nicht als Minimalpolynome auf. Damit sind alle Minimalpolynome separabel, also ist die Körpererweiterung separabel.

Sei nun char $K = p$, L/K algebraisch, $\alpha \in L$ und $f = \min_K(\alpha)$. Nach Korollar 4.2.7 (iii) wäre das Minimalpolynom von der Form

$$f = b_n(X^p)^n + \cdots + b_1 X^p + b_0 \,,$$

wenn α mehrfache Nullstelle wäre. Da K perfekt vorausgesetzt ist, können wir a_i finden, so dass $b_i = (a_i)^p$. Sei

$$g = \sum_i a_i X^i \in K[X] \,.$$

Dann gilt $f = g^p$, im Widerspruch zur Irreduzibilität von f. □

Satz 4.2.10.
Für eine Körpererweiterung L/K sind äquivalent:

(i) L/K ist separabel.

(ii) L wird über K erzeugt von Elementen, die über K separabel sind.

Ist L/K überdies endlich, so gilt auch äquivalent

(iii) Ist N/L eine Erweiterung von L zu einer normalen Erweiterung von K, so gibt es genau $[L : K]$ Ausdehnungen von $K \hookrightarrow N$ zu $L \hookrightarrow N$,

$$Alg_K\ (L, N) = [L : K] \,.$$

Beweis.

(i) ⇒ (ii) ist klar.

(ii) ⇒ (iii) Mit Induktion über $[L : K]$ dürfen wir wieder annehmen, dass $L = K(\alpha)$. Da α separabel ist, sind die $[L : K]$ Nullstellen seines Minimalpolynoms $\min_K(\alpha)$ in N paarweise verschieden und liefern verschiedene Erweiterungen von $K \hookrightarrow N$ zu $K(\alpha) = L \hookrightarrow N$.

(iii) ⇒ (i) für L/K endlich. Wäre $\alpha \in L$ nicht separabel, so gäbe es weniger als $[K(\alpha) : K]$ Ausdehnungen von $K \hookrightarrow N$ zu einer Einbettung $K(\alpha) \hookrightarrow N$ und damit auch weniger als $[L : K]$ Ausdehnungen von $K \hookrightarrow N$ zu einer Einbettung $L \hookrightarrow N$.

Ist L/K nicht endlich, wähle $\alpha \in L$ und arbeite mit $K(\alpha)$. (Übung)

□

4.3 Galoiserweiterungen

Definition 4.3.1.
Sei L/K Körpererweiterung. Die Gruppe aller Körperautomorphismen von L, die K punktweise festlassen, heißt die Galoisgruppe $\mathrm{Gal}\,(L/K)$ *der Körpererweiterung L/K.*

Bemerkung 4.3.2.

(i) Offenbar hat man die Inklusion $\mathrm{Gal}(L/K) \subseteq \ Alg_K(L,L)$. *Gleichheit für endliche Körpererweiterungen folgt, da jeder Monomorphismus des endlich-dimensionalen K-Vektorraums L auch surjektiv ist. Gleichheit gilt aber sogar für alle algebraischen Erweiterungen (ohne Beweis).*

(ii) $\mathrm{Gal}(\mathbb{C},\mathbb{R}) = \{Id,\ Konjugation\}$

(iii) $\mathrm{Gal}\left(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}\right) = \{Id\}$.

Satz 4.3.3.
Für jede endliche Körpererweiterung gilt

$$|\ \mathrm{Gal}\ (L/K)|\ \leq [L:K]$$

Beweis. Folgt aus Satz 4.1.6, wegen 4.3.2 (i). □

Definition 4.3.4.
Eine Körpererweiterung L/K heißt Galoiserweiterung oder galoisch, wenn sie normal und separabel ist.

Wir brauchen einige Begriffe, um Gruppenwirkungen zu beschreiben:

Definition 4.3.5.

(i) Operiert eine Gruppe G auf einer Menge X, so schreiben wir X^G für die Menge der Fixpunkte:

$$X^G = \{x \in X \mid gx = x \quad \forall g \in G\}\,.$$

Ist $X = L$ ein Körper und ist G eine Gruppe von Körperautomorphismen, so ist $L^G \subseteq L$ ein Unterkörper von L, der Fixkörper von G. Er enthält K, also $K \subseteq L^G \subseteq L$.

(ii) Eine Operation einer Gruppe G auf einer Menge X heißt treu, wenn

$$gx = x \quad \forall x \in X \quad \Rightarrow \quad g = e \in G\,.$$

(iii) Eine Operation mit nur einer Bahn heißt transitiv.

Satz 4.3.6.
Sei L/K endliche *Körpererweiterung und $G = \mathrm{Gal}(L/K)$. Dann sind äquivalent:*

(i) L/K ist galoisch.

(ii) $|\ \mathrm{Gal}(L/K)\ | = [L : K]$

(iii) $K = L^G$

(iv) Für alle $\alpha \in L$ gilt

$$\min_K(\alpha) = \prod_{\beta \in G\alpha} (X - \beta)\,.$$

Beweis.

(i)⇒(ii) Da L/K separabel und normal ist, können wir in 4.2.10 (iii) $N = L$ setzen. Also $|\ \mathrm{Alg}_K(L_1 L)| = [L : K]$. Da L/K endlich ist, gilt außerdem nach Bemerkung 4.3.2 (i) $\mathrm{Alg}_K(L, L) = \mathrm{Gal}(L/K)$.

(ii)⇒(iii) Wir betrachten die Abschätzung

$$|G| = [L : K] \geq [L : L^G] \geq |G|\,,$$

wobei wir zunächst die Gradformel und dann Satz 4.3.3 benutzt haben. In allen Ungleichungen muss dann aber Gleichheit gelten, also $K = L^G$.

(iii)⇒ (iv) Sei $f \in K[X]$ und $\alpha \in L$ eine Nullstelle von f. Dann ist auch $\sigma(\alpha)$ für alle $\sigma \in G$ eine Nullstelle von f. Also teilt das Produkt der Linearfaktoren

$$\prod_{\beta \in G\alpha} (X - \beta) \in L^G[X] = K[X]$$

auch f. Ist $f = \min_K(\alpha)$, so ist f prim und beide Polynome sind normiert. Somit folgt die Gleichheit beider Polynome.

(iv)⇒ (i) Offenbar sind für jedes $\alpha \in L$ die Nullstellen des Minimalpolynoms über K verschieden. Damit ist jedes $\alpha \in L$ über K separabel und so ist die Körpererweiterung L/K separabel.
Da L/K endlich ist, ist $L = K(\alpha_1, \ldots, \alpha_r)$ und L ist als Zerfällungskörper von

$$f = \prod_{i=1}^{r} \min_K(\alpha_i) \in K[X]$$

normal.

□

Wir wollen nun einen Einblick über die Galoistheorie unter Verzicht auf Beweise geben. Diese werden in der Vorlesung Algebra II nachgeholt werden.

Satz 4.3.7. *(Operation der Galoisgruppe auf Nullstellen)*
Sei $f \in K[X]$ ein irreduzibles Polynom und L sein Zerfällungskörper. Dann operiert $\mathrm{Gal}(L/K)$ transitiv und treu auf der Menge

$$\{\alpha \in L \mid f(\alpha) = 0\}$$

der Nullstellen von f in L.

Beispiel 4.3.8.
Sei L der Zerfällungskörper des Polynoms $f = X^3 - 2 \in \mathbb{Q}[X]$. Wir behaupten, dass $\mathrm{Gal}(L/\mathbb{Q}) \cong S_3$. Wir fassen dazu zunächst L als Teilkörper von $\mathbb{C}$ auf:

$$L = \mathbb{Q}\Big(\sqrt[3]{2}, \xi\sqrt[3]{2}, \xi^2\sqrt[3]{2}\Big) \subseteq \mathbb{C}$$

mit $\xi = e^{2\pi \mathrm{i}/3}$. Da $\mathbb{Q}\Big(\sqrt[3]{2}\Big) \subseteq \mathbb{R}$, ist sicher $\mathbb{Q}\Big(\sqrt[3]{2}\Big) \neq L$. In $\mathbb{Q}\Big(\sqrt[3]{2}\Big)[X]$ zerfällt das über $\mathbb{Q}$ irreduzible Polynom f in einen Linearfaktor und ein quadratisches Polynom. Somit ist

$$\Big[L : \mathbb{Q}\big(\sqrt[3]{2}\big)\Big] = 2\,,$$

und nach der Gradformel $[L : \mathbb{Q}] = 6$. Die Operation von $\mathrm{Gal}(L/\mathbb{Q})$ auf der Menge $\Big\{\sqrt[3]{2}, \xi\sqrt[3]{2}, \xi^2\sqrt[3]{2}\Big\}$ liefert nach Satz 4.3.7 eine Einbettung der Galoisgruppe in die symmetrische Gruppe S_3. Wegen

$$6 = [L : \mathbb{Q}] = |\ \mathrm{Gal}(L/\mathbb{Q})| \leq |S_3| = 6$$

folgt, dass die Galoisgruppe gleich S_3 sein muss.

Theorem 4.3.9. *(Hauptsatz der Galoistheorie)*
Sei L/K eine endliche Galoiserweiterung mit Galoisgruppe $G = \mathrm{Gal}(L/K)$. Dann gilt:

(i) Es gibt eine Bijektion

$$\left\{ \begin{array}{c} \text{Zwischenkörper } M \\ K \subset M \subset L \end{array} \right\} \overset{\sim}{\leftrightarrow} \left\{ \begin{array}{c} \text{Untergruppe } H \\ H \subset G \end{array} \right\}$$

$$\begin{array}{rcl} M & \leftrightarrow & \{g \in G \,|\, g_{|_M} = \mathrm{id}\} \\ L^H & \leftrightarrow & H \end{array}$$

(ii) Unter dieser Bijektion entsprechen normalen Untergruppen H von G Zwischenkörper M, die normal über K sind. Ihre Galoisgruppe über K ist die Quotientengruppe:

$$\text{Gal}\,(M/K) \cong G/H\,.$$

Wir wollen nun noch eine Anwendung von Galoisgruppen skizzieren.

Satz 4.3.10.
Der n–te Kreisteilungskörper $\mathbb{Q}\big(e^{2\pi \mathrm{i}/n}\big)$ ist eine Galoiserweiterung von $\mathbb{Q}$ und

$$\text{Gal}\,\big(\mathbb{Q}(e^{2\pi \mathrm{i}/n})/\mathbb{Q}\big) = (\mathbb{Z}/n\mathbb{Z})^\times\,.$$

Beweis.
Wir werden den Satz in der Vorlesung Algebra II beweisen und hier nur die Idee angeben. Offenbar ist $\zeta_n := e^{2\pi \mathrm{i}/n}$ ein primitives Element für die Körpererweiterung. Es reicht daher aus, die Wirkung eines Elements der Galoisgruppe auf ζ_n anzugeben. Für $(k,n) = 1$ betrachten wir

$$\sigma_k \,:\, \zeta_n \mapsto (\zeta_n)^k\,.$$

Die Bedingung $(k,n) = 1$ ist sicher notwendig, damit $\tilde{\zeta} := (\zeta_n)^k$ eine sogenannte primitive n–te Einheitswurzel ist, d.h. damit n die kleinste positive Zahl r ist, so dass $(\tilde{\zeta})^r = 1$ gilt. □

Wir können jetzt den folgenden Satz zeigen:

Satz 4.3.11.
Das reguläre n–Eck ist genau dann konstruierbar mit Zirkel und Lineal, wenn $\varphi(n)$ eine Zweierpotenz ist.

Beweis.
Ist $\varphi(n) = |(\mathbb{Z}/n\mathbb{Z})^\times| = [\mathbb{Q}(\zeta_n) : \mathbb{Q}]$ keine Zweierpotenz, so kann nach 2.1.11 (ii) die Einheitswurzel ζ_n nicht konstruierbar sein.

Ist dagegen $\varphi(n)$ eine Zweierpotenz, so ist $(\mathbb{Z}/n\mathbb{Z})^\times$ eine Zwei–Gruppe. Nach dem Struktursatz 1.11.1 für p-Gruppen gibt eine Kette von Normalteilen von $\text{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) =: G$,

$$G = G_r \supseteq G_{r-1} \supseteq \cdots \supseteq G_0 = \{e\}\,,$$

mit $G_i/G_{i-1} \cong \mathbb{Z}_2$. Nach dem Hauptsatz 4.3.9 der Galoistheorie bilden die Fixkörper

$$K_i = \mathbb{Q}(\zeta_n)^{G_i}$$

eine Kette von Zwischenkörpern

$$\mathbb{Q} = K_r \subseteq K_{r-1} \subseteq \ldots \subseteq K_0 = \mathbb{Q}(\zeta)$$

mit $[K_{i-1} : K_i] = 2$. Nach Satz 2.1.6 ist ζ_n dann konstruierbar. □

Wir können die natürlichen Zahlen n, für die das reguläre n-Eck konstruierbar ist, explizit berechnen:

Bemerkung 4.3.12.
Besitzt die natürliche Zahl n die Primzahlzerlegung $n = \prod_i p_i^{s_i}$, so ist der Wert der Eulerschen φ-Funktion .

$$\varphi(n) = \prod_i p_i^{s_i - 1}(p_i - 1)\,.$$

Damit $\varphi(n)$ Zweierpotenz ist, darf also jede Primzahl ungleich zwei maximal einmal auftreten. Außerdem müssen die auftretenden Primzahlen p_i von der Form $p_i = 2^{r_i} + 1$ sein, genauer sogar von der Form $p_i = 2^{2^{\tilde{r}_i}} + 1$.

Weitere Anwendungen der Galoistheorie werden in der Vorlesung Algebra II vorgestellt werden. Sie betreffen etwa die Auflösbarkeit polynomialer Gleichungen $f(X) = 0$, für $f \in K[X]$, die Galoistheorie für endliche Körper und Kreisteilungskörper und die unendliche Galoistheorie.

Index