Algebra (Bachelor)

Wintersemester 2016/17

Christoph Schweigert
Universität Hamburg
Fachbereich Mathematik
Bereich Algebra und Zahlentheorie

(Stand: 20.10.2022)

Inhaltsverzeichnis

Literatur:

Literatur, die ich bei der Vorbereitung häufig herangezogen habe:

- Falko Lorenz, Einführung in die Algebra, Teil I. Spektrum Akademischer Verlag, 1996.
- Jens Carsten Jantzen, Joachim Schwermer, Algebra, Springer 2006

Dieses Skript basiert auf einer Vorlesung, die ich im Wintersemester 2016/17, an der Universität Hamburg gehalten habe.

Die aktuelle Version dieses Skriptes finden Sie unter
`http://www.math.uni-hamburg.de/home/schweigert/skripten/a1skript.pdf`
als pdf-Datei. Bitte schicken Sie Korrekturen und Bemerkungen an `christoph.schweigert@uni-hamburg.de`!

Den Studierenden der Vorlesung, insbesondere Jan Hottenrott und Dennis Sommer, danke ich für hilfreiche Hinweise zum Skript.

1 Einleitung

Ein Ziel der Algebra ist es, Strukturen wie Gruppen, Ringe, Körper, Moduln über Ringen als Verallgemeinerung von Vektorräumen über Körpern besser zu verstehen. Hier werden wir Methoden lernen, die weit über die der linearen Algebra hinaus gehen und die für (fast) alle Gebiete der Mathematik sehr nützlich sind. Wir wollen aber als Einstieg zwei Fragestellungen vorstellen, die die Entwicklung der mathematischen Disziplin Algebra motiviert haben.

— Die Frage nach der Auflösbarkeit von Gleichungen höherer Ordnung durch Formeln, wie wir sie für die quadratische Gleichung $X^2+pX+q=0$ in der Form $-\frac{p}{2}\pm\sqrt{\frac{p^2}{4}-q}$ kennen, also durch (eine Schachtelung) von Polynomen und Wurzeln.

— Konstruktionsprobleme mit Zirkel und Lineal.

Für beide Fragestellungen brauchen wir Wissen über Gruppen und Ringe.

1.1 Konstruierbarkeit mit Zirkel und Lineal

Wir gehen auf das Problem der Konstruierbarkeit ein. Dabei werden wir sehen, wie weit wir mit Begriffen aus der linearen Algebra kommen. Es geht um die folgende Aufgabe:

> In der Ebene $\mathbb{R}^2$ soll aus einer Teilmenge $M\subset\mathbb{R}^2$ mit Zirkel und Lineal ein weiterer Punkt konstruiert werden.

Es gelten hierfür die folgenden Regeln:

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

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

R 3 : Um jeden konstruierten oder vorgegebenen Punkt kann man einen Kreis schlagen mit einem Radius, den man als Verbindungsstrecke zweier Punkte in M abgreift.

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

Wir setzen:

$$\lhd M := \left\{ P\in\mathbb{R}^2 \mid P \quad \text{ist aus } M \text{ mit Zirkel und Lineal konstruierbar.} \right\}\subset\mathbb{R}^2$$

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

Beispiele 1.1.1.

1. Winkeldrittelung:
   Gegeben sei ein beliebieger 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: gilt $X\in\lhd\{O,P,Q\}$ für beliebige Wahl der drei Punkte O,P und 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 $e^{2\pi \mathrm{i}/n} \in \lhd \{0, 1\}$?

3. Quadratur des Kreises:
   Finde ein Quadrat mit gleicher Fläche wie die eines vorgegebenen Kreises. Zu lösen ist die Gleichung $x^2 = \pi r^2$ 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 $X \in \lhd \{P, Q\}$?

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

Bemerkung 1.1.2.
Die algebraischen Grundoperationen sind konstruktiv beschreibbar. Sei $M \subset \mathbb{C}$ beliebige Teilmenge mit $0, 1 \in M$. Dann gilt

1) $\mathrm{i} \in \lhd M$

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

3) $z_1, z_2 \in \lhd M \Rightarrow z_1 + z_2, -z_1 \in \lhd M$

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

Insbesondere ist $\lhd M \subset \mathbb{C}$ ein Teilkörper der komplexen Zahlen, der $\mathbb{Q}$ enthält.

Beweis.

1) Konstruiere die Mittelsenkrechte auf $[-1, 1]$.

2) Fälle das 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.

□

Lemma 1.1.3.
Der Körper $\lhd M$ ist quadratisch abgeschlossen, d.h. für $z \in \mathbb{C}$ gilt: mit $z \in \lhd M$ ist auch $\pm\sqrt{z} \in \lhd M$.

Beweis.
Da man Winkel mit Zirkel und Lineal halbieren kann, reicht es wiederum aus, die Behauptung für die reelle Zahl $r = |z|$ 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 1.1.4

1. *Sei E ein Körper, $K \subseteq E$ Teilkörper. E heißt Erweiterungskörper von K.*

2. *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. Dies ist ein Körper. $K(A)$ 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 die Menge $A = \{\alpha_1 \dots \alpha_m\} \subset E$ 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 1.1.5
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 $\omega^2 \in K$ und $E = K(\omega)$. Das Element $\omega \in E$ heißt Quadratwurzel des Elements $v \in K$, wenn $v = \omega^2$ 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 1.1.6.
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) $z \in \lhd M$, d.h. z ist aus M konstruierbar.

(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

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

von Teilkörpern, so dass

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

wobei der Körper E die komplexe Zahl z enthält, $z \in E$.

Wegen Bemerkung 1.1.2 ist $K \subset \lhd M$. Da $\omega_1^2 \in K_0$, ist wegen der quadratischen Abgeschlossenheit 1.1.3 auch $\omega_1 \in \lhd M$. Da $\lhd M$ ein Körper ist, folgt $K_1 = K_0(\omega_1) \subset \lhd M$. Per Induktion folgt nun $z \in \lhd M$.

(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.

Wir behaupten, dass $\lhd K = \lhd M$ gilt. Aus $M \subset K$ folgt sofort die Inklusion $\lhd M \subset \lhd K$. Wir wissen andererseits, dass die Elemente von K aus M konstruierbar sind, also $K \subset \lhd M$. Daraus folgt $\lhd K \subset \lhd\lhd M = \lhd M$.

Wir können also ohne Einschränkung der Allgemeinheit die Menge M durch den Körper $K = \mathbb{Q}(M \cup \overline{M})$ ersetzen. Man beachte, dass dann $\overline{K} = K$ gilt. Induktiv erreicht man dan auch $\overline{K_i} = K_i$, indem man immer Paare von Quadratwurzeln adjungiert. Wir betrachten jetzt die folgenden drei Fälle getrennt:

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

(b) z ist Schnittpunkt von Gerade und Kreis gegeben durch Punkte in $K \Rightarrow$

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

Denn der Schnitt von Gerade und Kreis führt auf quadratische Gleichungen über K. Die Lösungen liegen also in einem quadratischen Erweiterungskörper von K. (Hier geht die Bedingung $\overline{K} = K$ ein: der Kreis ist beschrieben als Menge der Punkte $\{z \,|\, (z-a)\overline{(z-a)} = r^2\}$. Wenn er aus K konstruierbar ist, so ist $a \in K$ und es gibt ein $b \in K$ auf dem Kreis. Wegen $\overline{K} = K$ ist dann auch $r^2 = (b-a)(\overline{b} - \overline{a}) \in K$. Die Schnittgleichung mit der Gerade $\{z_0 + tz_1 \,|\, t \in \mathbb{R}\}$ mit $z_0, z_1 \in K$

$$(z_0 + z_1 t - a)(\overline{z}_0 + \overline{z}_1 t - \overline{a}) = r^2$$

führt dann auf eine quadratische Gleichung mit Koeffizienten in K.)

(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 ein beliebiges $\varphi \in \mathbb{R}$ und den Erweiterungskörper $K := \mathbb{Q}(e^{\mathrm{i}\varphi})$ von $\mathbb{Q}$. Man beachte, dass für $z := e^{\mathrm{i}\varphi}$ gilt $\overline{z} = e^{-\mathrm{i}\varphi} = \frac{1}{z} \in K$, so dass $\overline{K} = K$ gilt.

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 $\mathbb{Q}$.

Damit ist klar, dass es für diese Probleme wichtig ist, die Unterkörper eines Erweiterungskörpers zu verstehen. Dieses Problem ist auch wichtig, um Auflösungsformeln für polynomiale Formeln durch sukzessive Wurzeln zu finden.

Die folgende Beobachtung erlaubt es uns, Methoden der linearen Algebra anzuwenden:

Definition 1.1.7
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 1.1.8.
Der Körpergrad der komplexen Zahlen über den reellen 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, die rationalen Zahlen aber abzählbar sind.

Lemma 1.1.9.
Sei E ein Erweiterungskörper von K, und in K gelte $1 + 1 \neq 0$. Dann gilt

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

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

$$\alpha^2 + p\alpha + q = 0 \qquad \text{mit} \quad p, q \in K\,, \qquad (*)$$

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 $(*)$

$$\omega^2 = \alpha^2 + p\alpha + \frac{p^2}{4} \overset{(*)}{=} \frac{p^2}{4} - q \in K\ .$$

Also ist ω eine Quadratwurzel. Es gilt $E = K(\alpha) = K(\omega)$. Also entsteht E durch Adjunktion der Quadratwurzel ω aus K.
"$\Leftarrow$" Sei $E = K(\omega)$ für $\omega \in E \setminus K$ mit $\omega^2 = d \in K$. Offenbar ist

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

ein Teilkörper von E, der ω und K enthält. Da $K(\omega)$ der kleinste solche Körper ist, folgt $E' \supseteq E = K(\omega)$. Also ist $E = E'$, und der Grad ist $[E : K] = [E' : K] = 2$. $\square$

Satz 1.1.10. (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: ist

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

so bilden die Produkte $\{\alpha_j \cdot \beta_i\}$ eine Basis von E über K.

Korollar 1.1.11.

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

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

(ii) Sei $K = \overline{K} \subseteq \mathbb{C}$ ein Teilkörper von $\mathbb{C}$. Damit $z \in \mathbb{C}$ aus K konstruierbar ist, muss $[K(z) : K] = 2^r$ für ein $r \in \mathbb{N}$ gelten.

Beweis.

(i) Lemma 1.1.9 und die Gradformel 1.1.10.

(ii) Nach Satz 1.1.6 ist $z \in \lhd K$ in einem Erweiterungskörper E von K enthalten, der durch sukzessive Adjunktion von Quadratwurzeln entstanden ist. Mit Hilfe der Gradformel und des Resultats aus (i) finden wir:

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

woraus folgt

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

□

Hier haben wir nur Methoden der linearen Algebra benutzt. Wir brauchen feinere Methoden:

- Wir müssen Körpererweiterungen konstruieren. Dazu brauchen wir ein gutes Verständnis von Quotienten von Polynomringen. Wir werden in den nächsten Unterkapiteln sehen, wie weit wir dabei mit Methoden aus der linearen Algebra kommen werden.
- Wir müssen Körpererweiterungen E/K verstehen. Dafür sind Symmetrien der Körpererweiterungen wichtig. Zum Bespiel wirkt auf $\mathbb{Q}[\mathrm{i}]/\mathbb{Q}$ die Gruppe $\mathbb{Z}_2$ durch $(a+b\mathrm{i}) \mapsto (a-b\mathrm{i})$. Dafür werden wir dann erst unsere Kenntnisse über Gruppen vervollständigen müssen.

1.2 Algebraische Körpererweiterungen

Wesentlich in den Konstruktionsproblemen waren Lösungen von quadratischen Gleichungen mit rationalen Koeffizienten. Wir betrachten Lösungen polynomialer Gleichungen beliebigen Grades.

Definition 1.2.1
Sei E/K eine Körpererweiterung. Ein Element $\alpha \in E$ heißt algebraisch über K, falls es ein von Null verschiedenes Polynom $f \in K[X]$, $f \neq 0$ gibt mit $f(\alpha) = 0$.
Ist α nicht algebraisch über K, so heißt α transzendent über K.

Bemerkung 1.2.2.

1. Indem wir zu einem Vielfachen des Polynoms übergehen, können wir annehmen, dass das Polynom f normiert ist, also höchsten Koeffizienten $a_n = 1$ hat:

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

2. 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 offensichtlich abzählbar, die Menge der transzendenten Zahlen ist überabzählbar.

3. Wir werden später sehen: sei $M \subset \mathbb{C}$ mit $0, 1 \in M$. Ist $z \in \lhd M$, so ist z algebraisch über dem Körper $K = \mathbb{Q}(M \cup \overline{M})$.

4. Es gilt (Lindemann 1882): die Kreiszahl π ist transzendent über $\mathbb{Q}$. [1] Also ist die Quadratur des Kreises unmöglich.

Da der Polynomring nun eine wichtige Rolle spielt, müssen wir an einige Aussagen über Ringe erinnern.

Definition 1.2.3

1. *Ein Ring ist eine Menge mit zwei assoziativen Verknüpfungen $(R, +, \cdot)$ so dass eine abelsche Gruppe ist und die beiden Distributivgesetze*

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

   gelten.

2. *Ist die Multiplikation kommutativ, so heißt der Ring kommutativ. 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 $a \in R$ gilt.*

3. *Seien R und S Ringe. Ein Ringhomomorphismus $\varphi : R \to S$ ist eine Abbildung, für die gilt*

$$\varphi(a + b) = \varphi(a) + \varphi(b) \quad \text{und} \quad \varphi(ab) = \varphi(a)\varphi(b)$$

   für alle $a, b \in R$. Für einen unitalen Ringhomomorphismus fordert man zusätzlich $\varphi(1) = 1$.

[1] Für einen elementaren Beiweis, siehe: I. Niven, *The Transcendence of π*, The American Mathematical Monthly, 46 (1939) 469-471. Für einen elementaren Beweis der Transzendenz der Eulerschen Zahl e auf einer Seite siehe A. Hurwitz, *Beweis der Transzendenz der Zahl* e, Mathematische Annalen 43 (1893) 220-221.

4. *Ein kommutativer Ring mit Eins heißt nullteilerfrei oder integer oder Integritätsring, wenn $ab = 0$ impliziert, dass $a = 0$ oder $b = 0$ gilt.*

5. *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:*

$$(\lambda a)b = a(\lambda b) = \lambda(ab) \qquad \text{für alle } \ a, b \in A, \lambda \in K\,.$$

Körper sind natürlich insbesondere unitale kommutative Ringe. Alle Algebren und Ringe in dieser Vorlesung werden kommutativ sein und ein Einselement haben. Gelegentlich werden wir daher nicht immer explizit "mit Eins" dazusagen. Der Polynomring $K[X]$ über einem Körper ist ein wichtiges Beispiel einer K-Algebra.

Bemerkung 1.2.4.
Ein wichtiges Beispiel für einen Morphismus von Algebren ist der Einsetzungshomomorphismus. Sei K ein Körper, $K[X]$ der Polynomring über K und E eine beliebige K-Algebra. Für ein gegebenes Element $\alpha \in E$ betrachte den eindeutigen Ringhomomorphismus

$$\varphi_\alpha : \quad K[X] \to E$$

mit $X \mapsto \alpha$. Für diesen Ringhomomorphismus gilt $\sum_{i=0}^m b_i X^i \mapsto \sum_{i=0}^m b_i \alpha^i$. Er wird in linearen Algebra sogar auf nicht-kommutative Ringe angewandt: setzt man einen Endomorphismus A eines endlich-dimensionalen Vektorraums in sein charakteristisches Polynom $P_A(X) = \det(X\mathrm{id} - A)$ ein, so erhält man nach dem Satz von Cayley-Hamilton Null.

Lemma 1.2.5.
Eine endlich-dimensionale kommutative K-Algebra R, die integer ist, ist ein Körper.

Beweis.
Sei $a \in R \setminus \{0\}$. Die K-lineare Abbildung

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

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 lineare Selbstabbildung von R auch surjektiv. Insbesondere gibt es ein Element $b \in R$ mit $ab = 1$. □

Wir können nun Algebraizität als Endlichkeitseigenschaft beschreiben:

Satz 1.2.6.
Sei E/K Körpererweiterung und $\alpha \in E$ algebraisch über K. Dann ist der Körpergrad des Erweiterungskörpers $K(\alpha)$ von K endlich, $[K(\alpha) : K] < \infty$.

Beweis.
Das Element α ist als algebraisches Element Nullstelle eines nicht-trivialen normierten Polynoms

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

Das Bild des Einsetzungshomomorphismus

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

ist eine K-Algebra und als Teilring des Körpers E integer. 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 $K[\alpha] = \{g(\alpha) | g(X) \in K[X]$ mit $\mathrm{grad}\, g \leq n-1\}$. Somit ist $\dim_K K[\alpha] \leq n$.

Wegen Lemma 1.2.5 ist $K[\alpha]$ ein Körper. Da dieser Körper K und α enthält, ist er in $K(\alpha)$ als kleinstem solchen Körper enthalten. Umgekehrt enthält jeder Körper, der K und α enthält, auch $K[\alpha]$. Also gilt $K[\alpha] = K(\alpha)$. Somit finden wir $[K(\alpha) : K] \leq n < \infty$. □

Bemerkung 1.2.7.
Wir erinnern an die lineare Algebra: 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. Alle Polynome, die A als Nullstelle haben, sind Vielfache des Minimalpolynoms.

Zum Beispiel hat der Endomorphismus $\lambda \mathrm{id}_V$ das charakteristische Polynom $(X-\lambda)^{\dim V}$, aber das Minimalpolynom $(X-\lambda)$. Eine Matrix ist genau dann diagonalisierbar, wenn das Minimalpolynom in paarweise verschiedene Linearfaktoren zerfällt.

Definition 1.2.8
Sei E/K eine Körpererweiterung und $\alpha \in E$ ein algebraisches Element über K. Die Multiplikation mit α definiert einen K-linearen Endomorphismus h_α von des K-Vektorraums $K(\alpha)$, der nach Satz 1.2.6 endlich-dimensional ist:

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

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

Nun können wir mit Methoden der linearen Algebra Körpergrade berechnen:

Satz 1.2.9.
Sei E/K eine Körpererweiterung und $\alpha \in E$ algebraisch über K mit $\mathrm{grad}\, \min_K(\alpha) = n$. Dann ist $\{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$ eine K-Basis von $K(\alpha)$. Insbesondere ist

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

Der Körpergrad des durch Adjunktion von α erhaltenen Körpers ist also gleich dem Grad des Minimalpolynoms.

Beweis.
Sei $\min_K(\alpha) = f(X) = X^n + \cdots + a_0$. Aus dem Beweis von Satz 1.2.6 folgt schon, dass

$[K(\alpha) : K] \leq n$. Es reicht also aus zu zeigen, dass die Teilmenge $\{1, \alpha, \alpha^2, \ldots \alpha^{n-1}\} \subset K(\alpha)$ 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. □

Definition 1.2.10

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

(ii) Eine Körpererweiterung heißt endlich, falls $[E : K] < \infty$ ist.

Zum Beispiel ist die Körpererweiterung $\mathbb{C}/\mathbb{R}$ endlich, denn jede komplexe Zahl ist Nullstelle eines Polynoms der Ordnung höchstens 2. Die Körperweiterung $\mathbb{R}/\mathbb{Q}$ ist nicht algebraisch, zum Beispiel weil die reellen Zahlen π und e nicht algebraisch sind.

Satz 1.2.11.
Ist E/K eine endliche Körpererweiterung, so ist die Körpererweiterung E/K algebraisch und für jedes $\alpha \in E$ teilt grad $\min_K(\alpha)$ den Körpergrad $[E : K]$.

Vorsicht: nicht jede algebraische Körpererweiterung ist endlich.

Beweis.
Sei $[E : K] = n < \infty$ und $\alpha \in E$ beliebig. 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. 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 als Nullstelle eine Polynoms in $K[X]$ algebraisch. Ferner gilt mit 1.2.9

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

wegen der Gradformel 1.1.10 □

Korollar 1.2.12.

1. Sei E/K eine Körpererweiterung und $\alpha \in E$ algebraisch über K. Dann ist die Körpererweiterung $K(\alpha)/K$ algebraisch.

2. Sei $0, 1 \in M \subset \mathbb{C}$ und $K = \mathbb{Q}(M \cup \overline{M})$. Dann ist die Körpererweiterung $\lhd M/K$ algebraisch.

3. E/K ist endlich $\iff$ Es gibt endlich viele über K algebraische Elemente $\alpha_1 \dots \alpha_m$ aus E, so dass $E = K(\alpha_1, \dots, \alpha_m)$.

Aus dem zweiten Punkt folgt, da π transzendent ist, die Unmöglichkeit der Quadratur des Kreises mit Zirkel und Lineal.

Beweis.

1. Nach Satz 1.2.6 ist die Körpererweiterung $K(\alpha)/K$ endlich und damit nach Satz 1.2.11 auch algebraisch.

2. Aus $z \in \lhd M$ folgt $[K(z) : K] < \infty$ wegen Korollar 1.1.11. Mit Satz 1.2.11 folgt, dass z algebraisch über K ist.

3. "$\Rightarrow$" Sei $\{\alpha_1, \dots, \alpha_m\}$ eine K–Basis von E. Dann ist $E = K(\alpha_1, \dots, \alpha_m)$ und nach Satz 1.2.11 ist E algebraisch und somit sind alle α_i algebraisch.

   "$\Leftarrow$" durch Induktion nach m. Der Induktionsanfang ist durch Satz 1.2.9 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 dem Körper K'. Damit ist nach Satz 1.2.9 auch $[E : K'] < \infty$. Aus der Gradformel schließen wir, dass $[E : K] < \infty$.

□

Korollar 1.2.13.
Sei E/K eine Körpererweiterung und $M \subset E$ eine beliebige Menge von Elementen, die über K algebraisch sind. Dann ist die Körpererweiterung $K(M)/K$ algebraisch.

Beweis.
Wir überlegen uns zunächst: der Körper $K(M)$ ist die Vereinigung über alle Unterkörper der Form $K(M_0)$ mit $M_0 \subset M$ endlich. Die Inklusion $F := \cup_{M_0} K(M_0) \subset K(M)$ ist folgt aus $M_0 \subset M$. Andererseits ist F ein Körper: mit $\alpha \in K(M_0)$ und $\beta \in K(M_0')$ liegen Summen und Produkte in $K(M_0 \cup M_0')$, und $M_0 \cup M_0$ ist endlich.

Wegen Satz 1.2.12 ist aber $K(M_0)/K$ endlich und daher algebraisch. Also enthält $K(M)$ nur Elemente, die algebraisch über K sind. □

Definition 1.2.14
Sei E/K eine Körpererweiterung. Ein Körper L mit $K \subset L \subseteq E$ heißt Zwischenkörper.

Satz 1.2.15.
Sei eine Körpererweiterung E/K vorgegeben. Betrachte

$$F := \{\alpha \in E \mid \alpha \text{ algebraisch über } K\}.$$

Dann ist F ein Zwischenkörper von E/K.

Der Zwischenkörper F heißt algebraischer Abschluss von K in E. Insbesondere ist die Menge $\overline{\mathbb{Q}}$ aller algebraischen Zahlen in $\mathbb{C}$ ein Teilkörper von $\mathbb{C}$.

Beweis.
Wir müssen zeigen, dass F ein Körper ist. Seien $\alpha, \beta \in F$, also algebraisch über K. Nach Korollar 1.2.12.3 ist $K(\alpha, \beta)$ endlich über K. Jedes $\gamma \in K(\alpha, \beta)$ ist dann algebraisch nach 1.2.11, also

$$K(\alpha, \beta) \quad \subset \; F\,.$$

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 1.2.16. (Transitivität algebraischer Erweiterungen)
Sei L ein Zwischenkörper einer Körpererweiterung E/K. Dann ist die Körpererweiterung E/K genau dann algebraisch, wenn die beiden Körpererweiterungen E/L und L/K algebraisch sind.

Beweis.
"⇒" ist 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.
"⇐": Nach der ersten Annahme ist jedes $\beta \in E$ algebraisch über L. Betrachte das Minimalpolynom von β über L:

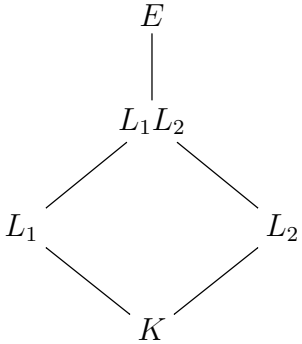
$$\min_L(\beta) = \sum_{i=0}^{n} \alpha_i X^i \quad \alpha_i \in L \quad \alpha_n = 1\,.$$

Offenbar ist dann β bereits algebraisch über dem kleineren Körper $F := K(\alpha_0, \ldots \alpha_{n-1}) \subset L$, wobei nach dem zweiten Teil der Voraussetzung alle α_i algebraisch über K sind. Mit Hilfe von 1.2.12.3 folgt, dass $[F : K] < \infty$, mit Hilfe der Gradformel daraus wiederum $[F(\beta) : K] = [F(\beta) : F] \cdot [F : K] < \infty$. Damit ist der Körper $F(\beta)$ endlich über K, also nach Satz 1.2.11 algebraisch über K, also ist β als Element von $F(\beta)$ algebraisch. □

Definition 1.2.17
Sei E/K eine Körpererweiterung und L_1, L_2 Zwischenkörper. Der Zwischenkörper

$$L_1L_2 := L_1(L_2) = L_2(L_1)$$

heißt das Kompositum von L_1 und L_2 in E.



Satz 1.2.18.
In dieser Situation gilt:

(a) Ist die Körpererweiterung L_1/K algebraisch, so ist auch die Körpererweiterung L_1L_2 über L_2 algebraisch.

(b) Ist die Körpererweiterung L_1/K endlich, $[L_1 : K] < \infty$, so ist auch die Körpererweiterung L_1L_2 über L_2 endlich. Es gilt für die Körpergrade $[L_1L_2 : L_2] \leq [L_1 : K]$.

(c) Sind die beiden Körpererweiterungen L_1/K und 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 L_1L_2 geht also durch Adjunktion algebraischer Elemente aus L_2 hervor. und ist nach Korollar 1.2.13 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 des Körpers E, der L_1 und L_2 enthält. Sei $\{\gamma_\lambda\}$ eine K-Basis von L_1. 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 $\dim_{L_2} R < \infty$. Als Unterring eines Körpers ist R integer; nach Lemma 1.2.5 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 1.2.16 und der Beobachtung, dass im Körperturm $L_1L_2 - L_2 - K$ die erste Erweiterung algebraisch ist nach Teil (a) dieses Satzes 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 $L_1 \cap L_2 = K$ gilt, kommt als Übungsaufgabe.

□

1.3 Einfache Körpererweiterungen

Wir untersuchen nun eine Klasse von Körpererweiterungen:

Definition 1.3.1
Eine Körpererweiterung E/K heißt einfach oder primitiv, falls es ein Element $\alpha \in E$ gibt, so dass $E = K(\alpha)$. Das Element $\alpha \in E$ heißt dann ein primitives Element von E/K.

Bemerkung 1.3.2.
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 1.2.6.
(ii) $\Rightarrow$ (iii) ist klar, da $K(\alpha)$ per Definition ein Körper ist.
(iii) $\Rightarrow$ (i) folgt daher, dass dann α^{-1} in $K[\alpha]$ liegt, also sich als Polynom in α schreiben lässt: $\alpha^{-1} = p(\alpha)$ mit $p \in K[X]$. Damit ist aber α Nullstelle des Polynoms $Xp(X) - 1 \in K[X]$, also algebraisch. □

Um Körper aus Polynomringen zu konstruieren, brauchen wir einige Begriffe:

Definition 1.3.3
Sei R ein beliebiger Ring mit 1. Eine nicht–leere Teilmenge I von R heißt (beidseitiges) Ideal von R, wenn gilt:

(i) $a, b \in I \Rightarrow a + b \in I$

(ii) $a \in I, x \in R \Rightarrow ax, xa \in I$.

Bemerkung 1.3.4.

1. Somit sind Ideale insbesondere Unterringe und additive Untergruppen.
2. Ist $\varphi : R \to R'$ ein Ringhomomorphismus von Ringen mit Eins, dann ist
$$\ker \varphi := \{x \in R | \varphi(x) = 0\}$$
ein Ideal.
3. Ein Körper K hat als Ideale nur das Nullideal und K selbst. Denn ist $x \neq 0$ in einem Ideal $I \subset K$, so folgt für beliebiges $y \in K$, dass $y = (yx^{-1})x \in I$ gilt, also $I = K$.

Definition 1.3.5
Sei R Ring mit Eins und I ein Ideal in R. Betrachte die Äquivalenzrelation
$$a \sim b \iff a - b \in I \ .$$

Wir schreiben auch $a \equiv b \bmod I$ für $a \sim b$. Die Menge der Äquivalenzklassen

$$R/I = \{\overline{a} = \{a' \in R : a' \sim a\}\}$$

ist ein Ring durch $\overline{a} + \overline{b} := \overline{a+b}$ und $\overline{a}\overline{b} := \overline{ab}$, der Restklassenring modulo dem Ideal I.
Die surjektive 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 $\ker \pi = I$.

Bemerkungen 1.3.6.

1. Jedes Ideal ist also auch der Kern eines Ringhomomorphismus, nämlich der Restklassenabbildung.

2. Es gilt der folgende Isomorphiesatz für Ringe: ein Ringhomomorphismus

   $$\varphi : R \to R'$$

   induziert einen Isomorphismus von Ringen

   $$\tilde{\varphi} : R/\ker \varphi \xrightarrow{\sim} \text{ Im } \varphi\,.$$

3. Als Beispiel betrachte eine Körpererweiterung E/K und wähle $\alpha \in E$. Dann ist

   $$\begin{array}{rccc} \varphi_\alpha : & K[X] & \to & K[\alpha] \subset E \\ & X & \mapsto & \alpha \end{array}$$

   ein Ringhomomorphismus, der Einsetzungshomomorphismus. Sein Kern

   $$I_\alpha = \ker \varphi_\alpha = \{g \in K[X] \,|\, g(\alpha) = 0\}$$

   ist ein Ideal, das Verschwindensideal in α. Der induzierte Ringhomomorphismus

   $$\begin{array}{rcl} K[X]/I_\alpha & \to & K[\alpha] \\ X \bmod I_\alpha & \mapsto & \alpha \end{array}$$

   ist dann ein Isomorphismus von K–Algebren.

4. 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 1.3.7

1. *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.

2. *Sei R kommutativer Ring mit Eins. Setze für $a \in R$*

$$(a) = Ra = \{ca | c \in R\}\,.$$

Dann ist (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 $R/(a)$.

Zum Beispiel ist die Einheitengruppe des Rings $\mathbb{Z}$ der ganzen Zahlen gleich $\{\pm 1\}$, die Einheitengruppe eines Körpers K gleich $K^\times = K\backslash\{0\}$ und die Einheitengruppe des Polynomrings $K[X]$ über einem Körper K gleich $K^\times$, den konstanten Polynomen ungleich Null.

Satz 1.3.8.
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.
Die Surjektivität des Einsetzungsmorphismus folgt aus der Tatsache, dass α primitiv ist. Wir bestimmen das Verschwindensideal in α. Sei $g \in K[X]$ ein Polynom mit Nullstelle α, also $g(\alpha) = 0$. Division mit Rest von Polynomen erlaubt es, g in der Form $g = qf + r$, mit $q, r \in K[X]$ und grad $r <$ grad f. Setzt man in diese Gleichung α ein, so sieht man, dass $r(\alpha) = 0$ gelten muss. Wegen der Minimalität des Grades 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. □

Betrachtung 1.3.9.

- Zur Konstruktion von Algebren aus Idealen in Polynomringen betrachte ein beliebiges Polynom $f \in K[X]$ vom Grad grad $f = n \geq 1$. Die Restklassenalgebra $K_f := K[X]/(f)$ ist eine K-Algebra. Den Körper identifizieren wir mit der Unteralgebra von $K[X]$, die aus den konstanten Polynome besteht. Durch die kanonische Surjektion ist sein Bild eine Unteralgebra von K_f. Die Abbildung $K \to K[X] \to K_f$ ist injektiv, da ein Körper keine nicht-trivialen Ideale hat. Also kann der Körper K als Teilkörper der Algebra K_f aufgefasst werden.

- Betrachten wir nun das Element $\alpha := \pi(X) \in K_f$. Da π ein Morphismus von Algebren ist, gilt

  $$\pi(g) = g(\alpha) \qquad \text{für alle} \quad g \in K[X]\,.$$

  Insbesondere gilt

  $$0 = \pi(f) = f(\alpha)\,,$$

  also ist α eine Nullstelle von f in der K-Algebra K_f. Wir haben also eine Algebra konstruiert, nämlich K_f, in der ein beliebig vorgegebenes Polynom f Nullstellen hat!

- Es ist aber nicht klar, wann die Algebra K_f auch ein Körper ist. Wir wollen dafür Lemma 1.2.5 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 1.3.10.
Sei K ein Körper und $f \in K[X]$ ein Polynom vom Grad $n \geq 1$. Betrachte die Surjektion $\pi : K[X] \to K_f := K[X]/(f)$ und setze $\alpha := \pi(X)$. Dann ist die Menge $\{1, \alpha, \ldots, \alpha^{n-1}\}$ eine Basis des K–Vektorraumes K_f. Insbesondere ist $\dim_K K_f = n$.

Beweis.
Sei $g \in K[X]$ ein Polynom, dann gilt $\pi(g) = g(\alpha) \in K_f$. Alle Elemente der Algebra K_f sind von dieser Form. Division von Polynomen mit Rest gibt $g = qf + r$ mit grad $r \leq n-1$. Einsetzen von α zeigt wegen $f(\alpha) = 0$, dass $g(\alpha) = r(\alpha)$ gilt. Also reichen die Polynome vom Grade kleiner als n aus, um alle Elemente in K_f zu beschreiben. Also ist K_f endlich-dimensional.

Wir können also das Minimalpolynom von $\alpha \in K_f$ betrachten. Nun gilt $0 = g(\alpha) = \pi(g)$ genau dann, wenn $g \in (f)$, also wenn $f|g$. Setzt man f als normiert voraus, so ist f das Minimalpolynom von α.

Es bleibt zu zeigen, dass die erzeugende Familie $\{1, \alpha, \ldots \alpha^{n-1}\}$ linear unabhängig ist. Sei eine Relation gegeben

$$\sum_{i=0}^{n-1} c_i \alpha^i = 0 \qquad \text{mit} \quad c_i \in K\,. \qquad (*)$$

Betrachte das Polynom $h(X) := \sum_{i=0}^{n-1} c_i X^i \in K[X]$, das offenbar $\alpha \in K_f$ als Nullstelle hat, $h(\alpha) = 0$. Daraus folgt aber nach Satz 1.3.8, 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 $(*)$ trivial. □

Wir müssen nun herausfinden, für welche Polynome $f \in K[X]$ die Quotientenalgebra $K_f = K[X]/(f)$ integer ist.

Definition 1.3.11
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 $f_1 \in K^\times$ oder $f_2 \in K^\times$ gilt.*

Beispiele 1.3.12.

- Im Polynomring $\mathbb{C}[X]$ sind nach dem Fundamentalsatz der Algebra genau die linearen Polynome die irreduziblen Elemente.

- Im Polynomring $\mathbb{R}[X]$ sind genau die linearen Polynome und die Polynome der Form

$$f(X) = aX^2 + bX + c \quad \text{mit} \quad b^2 - 4ac < 0$$

  irreduzibel, 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 1.3.13.
Sei $f \in K[X]$ ein von Null verschiedenes Polynom. Dann ist f genau dann irreduzibel, wenn aus $f|gh$ mit $g, h \in K[X]$ folgt, dass $f|g$ oder $g|h$.

Beweis.

- Gelte die im Satz formulierte Eigenschaft. Um zu zeigen, dass f dann irreduzibel ist, sei $f = f_1 f_2$. Dann gilt insbesondere $f|f_1 f_2$, und aus der Annahme folgt ohne Beschränkung der Allgemeinheit $f|f_1$, also $f_1 = fg$ mit einem $g \in K[X]$. Damit ist $f = f_1 f_2 = gff_2$ und somit $f(gf_2 - 1) = 0$. Da Polynomringe über Körpern integer sind und da f nicht null ist, folgt $gf_2 = 1$ und f_2 ist eine Einheit in $K[X]$. Also ist f irreduzibel. (Man beachte, dass bei dieser Richtung nur eingeht, dass der Polynomring $K[X]$ integer ist.)

- Sei f irreduzibel und gelte $f|gh$. Wir zeigen zunächst, dass wir annehmen können, dass grad $g <$ grad f gilt. Denn Division von Polynomen mit Rest erlaubt uns, g in der Form

  $$g = qf + r \quad \text{mit } q, r \in K[X] \text{ und grad } r < \text{grad } f$$

  zu schreiben. Teilt nun f das Polynom gh, so teilt f auch $rh = gh - qh \cdot f$. Angenommen, die Aussage ist bewiesen für den Fall, dass grad $g <$ grad f gilt. Wir wenden sie dann für die Polynome r, h an und finden, dass f entweder r oder h teilen muss. Dann gilt aber auch $f|g$ oder $f|h$.

- Angenommen, es gibt ein $g \in K[X]$ mit grad $g <$ 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 grad $t <$ grad g. Dies heißt $th = fh - sgh$, also teilt f auch das Produkt th.

  Da aber grad $t <$ grad g und g ein Gegenbeispiel *minimalen* Grades war, folgt daraus f teilt t oder f teilt h. Aber grad $t <$ grad $g <$ grad f, also muss f das Polynom h teilen. Dies aber wiederum ist im Widerspruch zur Annahme, dass g ein Gegenbeispiel liefert.

□

Wir erinnern an die Bezeichnungen: $f \in K[X]$ ist ein nicht-konstantes Polynom, $K_f := K[X]/f$ der Restklassenring mit kanonischer Surjektion $\pi : K[X] \to K_f$ und $\alpha := \pi(X) \in K_f$. Es gilt für $g \in K[X]$, dass $g(\alpha) = 0$ genau dann, wenn $f|g$.

Satz 1.3.14.
Der Restklassenring $K_f = K[X]/(f)$ ist ein Körper genau dann, wenn das Polynom $f \in K[X]$ irreduzibel ist.

Beweis.

- Angenommen, K_f ist ein Körper. Gelte $f \mid f_1 f_2$; daraus folgt

  $$f_1(\alpha) f_2(\alpha) = 0\,.$$

  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 nach Lemma 1.3.13 irreduzibel.

- Sei f irreduzibel. Wegen Lemma 1.3.10 ist K_f endlich-dimensional. Daher reicht es wegen Lemma 1.2.5 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 1.3.13 folgt aus der Tatsache, dass f irreduzibel ist, dass $f|g$ oder $f|h$. Damit gilt aber

  $$\overline{g} = 0 \quad \text{oder} \quad \overline{h} = 0\,,$$

  so dass die endlich-dimensionale K-Algebra K_f nullteilerfrei ist.

□

Satz 1.3.15.
Sei E/K eine Körpererweiterung, $\alpha \in E$ ein algebraisches Element über K.

1. Dann ist $f := \min_K(\alpha)$ ein Primpolynom in $K[X]$.
2. Ist umgekehrt $g \in K[X]$ ein normiertes und irreduzibles Polynom, für das $g(\alpha) = 0$ gilt, so ist g das Minimalpolynom von α, also $g = \min_K(\alpha)$.

Beweis.
1. Nach Satz 1.3.8 gilt $K_f = K[X]/f \cong K(\alpha)$, also ist K_f ein Körper. Nach Satz 1.3.14 folgt, dass f irreduzibel ist.
2. 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 1.3.16. (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. Es reicht, einen Erweiterungskörper mit einer Nullstelle des Faktors g zu finden. Daher können wir annehmen, dass es sich bei f um ein irreduzibles Polynom handelt. Nach Satz 1.3.14 ist dann K_f ein Erweiterungskörper von K und $\alpha = \pi(X)$ wegen $f(\alpha) = \pi(f) = 0$ eine Nullstelle von f. □

Wir können nun ein weiteres klassisches Konstruktionsproblem lösen:

Satz 1.3.17.
$\sqrt[3]{2}$ 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 1.3.15.2 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 ein $\beta \in \mathbb{Q}$ mit $\beta^3 = 2$. Dies wäre eine rationale Zahl β, deren dritte Potenz gleich 2 ist, Widerspruch. (Später werden wir viel bessere Hilfsmittel haben, um die Irreduzibilität von Polynomen nachzuweisen!)

Damit haben wir aber nach Satz 1.3.8 $\mathbb{Q}(\sqrt[3]{2}) = \mathbb{Q}[X]/(g)$

$$\left[\mathbb{Q}\left(\sqrt[3]{2}\right) : \mathbb{Q}\right] \overset{1.3.10}{=} \operatorname{grad} \min_{\mathbb{Q}}\left(\sqrt[3]{2}\right) = 3,$$

was keine Potenz von 2 ist. Mit Hilfe von Korollar 1.1.11 (ii) schliessen wir, dass $\sqrt[3]{2} \notin \lhd\{0,1\}$. □

Zum Abschluss dieses Abschnitts wollen wir eine Charakterisierung der einfachen Körpererweiterungen vorstellen. Hierfür brauchen wir das folgende

Lemma 1.3.18.
Sei E/K eine einfache algebraische Körpererweiterung und $\alpha \in E$ ein primitives Element von E/K. Sei L ein Zwischenkörper von E und

$$\min_L(\alpha) = g(X) = X^m + \beta_{m-1}X^{m-1} + \cdot + \beta_0 \in L[X]$$

das Minimalpolynom von α über dem Zwischenkörper L. 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 $F \subset L$ folgt aus $\beta_i \in L$. Da $g \in F[X]$, $g(\alpha) = 0$ gilt und g in $F[X]$ irreduzibel ist (denn g ist ja als Minimalpolynom sogar in $L[X]$ irreduzibel), ist g auch das Minimalpolynom über F, also $g = \min_F(\alpha)$. Nach Satz 1.2.9 ist

$$[F(\alpha) : F] = [L(\alpha) : L] = \operatorname{grad} g = m\,. \qquad (*)$$

Aus $E = K(\alpha)$ folgt $F(\alpha) = L(\alpha) = E$. Die Gleichung $(*)$ wird daher zu $[E : F] = [E : L]$. Nach der Gradformel gilt andererseits $[E : F] = [E : L][L : F]$, insgesamt also $[L : F] = 1$ und somit $L = F$. □

Der folgende Satz beschreibt einfache algebraische Körpererweiterungen durch Aussagen über Zwischenkörper.

Satz 1.3.19.
Sei E/K eine algebraische Körpererweiterung. Dann ist E/K genau dann einfach, wenn E/K endlich viele Zwischenkörper besitzt.

Beweis.
Mit $\mathcal{Z}$ bezeichnen wir die Menge aller Zwischenkörper der Körpererweiterung E/K.

"⇒" Sei E einfach, $E = K(\alpha)$ mit einem primitiven Element $\alpha \in E$. Bezeichne mit f das Minimalpolynom von α, $f := \min_K(\alpha)$. Bezeichne mit $\mathcal{T}$ die Menge der normierten Teiler des Polynoms f im Polynomring $E[X]$,

$$\mathcal{T} = \{g \in E[X] \mid g \quad \text{normiert}, \quad g|f \quad \text{in} \quad E[X]\}\,.$$

Da das Polynom f in $E[X]$ wie jedes Polynom nur endlich viele normierte Teiler besitzt, ist die Menge $\mathcal{T}$ endlich.

Die Abbildung

$$\begin{array}{rcl} \mathcal{T} & \to & \mathcal{Z} \\ g(X) = X^m + \beta_{m-1}X^{m-1} + \ldots + \beta_0 & \mapsto & K(\beta_{m-1}, \ldots, \beta_0) \end{array}$$

ist surjektiv: denn sei $L \in \mathcal{Z}$ ein Zwischenkörper. Dann teilt $g = \min_L(\alpha)$ das Polynom f in $L[X]$, also erst recht in $E[X]$. Nach Lemma 1.3.18 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.

"$\Leftarrow$" Wird hier nur unter der Voraussetzung gezeigt, dass der Körper K unendlich viele Elemente besitzt. 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, also

$$K(\lambda_1\alpha + \beta) = K(\lambda_2\alpha + \beta) =: L\,.$$

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!

□

Wir fassen den Stand unserer Überlegungen zusammen: von den klassischen Konstruktionsproblemen konnten wir das Problem der Quadratur des Kreises und das delische Problem lösen. Für die Probleme der Winkeldrittelung und der Konstruktion des regulären n-Ecks sowie Untersuchungen zur Auflösbarkeit von polynomialen Gleichungen brauchen wir zusätzliches Wissen über Körpererweiterungen E/K und ihre Zwischenkörper. Hier werden Symmetrien von Körpererweiterungen wesentlich sein, die durch Gruppen beschrieben werden. Diesen wenden wir uns nun zu.

2 Gruppen

Wir müssen nun einige algebraische Grundbegriffe durchgehen.

2.1 Mengen mit Verknüpfung, Gruppen

Wir fangen dabei an mit dem Begriff der Gruppe und ergänzen elementare Definitionen um einige neue Sätze.

Definition 2.1.1

(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. (Dies ist eigentlich ein Satz über Bäume und kein Satz der Algebra!)

Definition 2.1.2

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

$$e \top a = a \top e = a \qquad \text{für alle } a \in A\,.$$

2. *Ein Monoid ist eine Menge mit einer assoziativen Verknüpfung, in der es ein neutrales Element gibt.*

3. *Ein Monoid heißt abelsch oder kommutativ, wenn für alle $a,b \in A$ gilt $a \top b = b \top a$.*

Bemerkung 2.1.3.
In einer Menge mit Verknüpfung kann es höchstens ein neutrales Element e geben, denn für jedes andere Element e' mit $e' \top a = a \top e' = a$ für alle $a \in A$ 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.

Gruppen sind spezielle Monoide:

Definition 2.1.4
Eine Gruppe ist ein Monoid $(A, \top)$ derart, dass es für jedes $a \in A$ ein $\bar{a} \in A$ gibt mit $a \top \bar{a} = e$, wobei e das neutrale Element des Monoids A ist.

Bemerkung 2.1.5.

1. In einem Monoid 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 immer auch $\bar{a} \top a = e$. Das Rechtsinverse ist also immer auch ein Linksinverses.

   Ist $b \in A$ irgendein anderes Element mit $a \top b = e$, so folgt durch Anwenden von $\bar{a} \top$ schon $b = \bar{a}$.

2. 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 2.1.6.
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.

Beispiele 2.1.7.

1. Die Elemente eines Vektorraums bilden unter der Addition eine (abelsche) Gruppe mit dem Nullvektor als neutralem Element. Insbesondere bilden die Elemente eines Körpers unter der Addition eine (abelsche) Gruppe. Man findet unter diesen Beispielen schon endliche und unendliche Gruppen.

2. Die von Null verschiedenen Elemente eines Körpers K bilden unter der Multiplikation die (abelsche) Gruppe $K^\times$. Die invertiblen Matrizen mit Einträgen in einem Körper unter Multiplikation von Matrizen bilden eine (nicht-kommutative) Gruppe.

3. 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 $\mathcal{S}_r$ mit $r!$ Elementen.

4. Gruppen als Symmetrien:
   Stellen wir uns eine ebene Figur vor, d.h. eine beliebige Teilmenge der euklidischen 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.

5. Die Symmetrien einer Körpererweiterung E/K sind die Körperhomomorphismen $E \to E$, die den Unterkörper K punktweise festlassen. Zum Beispiel ist die Symmetrie der Körpererweiterung $\mathbb{C}/\mathbb{R}$ die Gruppe $\mathbb{Z}_2$.

6. In gewissem Sinne können wir eine Gruppe interpretieren als einen "abstrakten Symmetrietyp".

Lemma 2.1.8 (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 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.

Definition 2.1.9
Seien G, H Gruppen.

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

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.)*

Bemerkung 2.1.10.
Es gibt gute Gründe, die Definitionen etwas anders zu fassen:

1. 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 $g_1 = g_2$.

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 $g_1 = g_2$.

3. Isomorphismen sind Morphismen, die ein beidseitiges Inverses haben.

Beispiel 2.1.11.
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 2.1.12.

1. Man will also *Isomorphieklassen* von Gruppen klassifizieren. Man soll immer zwischen einer Gruppe und ihrer Isomorphieklasse unterscheiden.

2. 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.

2.2 Untergruppen

Definition 2.2.1
Eine nicht-leere Teilmenge H einer Gruppe G heißt Untergruppe, wenn sie mit zwei Elementen a, b auch deren Produkt ab und mit jedem Element $a \in H$ auch das Inverse a^{-1} enthält.

Bemerkungen 2.2.2.
1. Eine nicht-leere *endliche* Teilmenge einer Gruppe ist genau dann eine Untergruppe, wenn sie unter der Multiplikation abgeschlossen ist. (Übung)

2. 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 2.2.3.
Sei $\varphi : G \to H$ ein Gruppenhomomorphismus.

1. Der Kern $\ker\varphi = \varphi^{-1}(1)$ 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 der Kern trivial ist, $\ker\varphi = \{1\}$.

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 $x^{-1}y \neq 1$ wegen $\varphi(x^{-1}y) = \varphi(x)^{-1}\varphi(y) = 1$ in $\ker\varphi$. □

Beispiel 2.2.4.
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

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

Sie hat Ordnung $|A_r| = \frac{r!}{2}$.

Satz 2.2.5 (Untergruppen von $\mathbb{Z}$)**.**
Jede Untergruppe H der Gruppe $(\mathbb{Z}, +)$ 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 die Untergruppe H echt positive ganze Zahlen. Sei $m \in H$ die kleinste echt positive Zahl in 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 durch m teilen. Wir schreiben also $n = ms + r$ für geeignete $s, r \in \mathbb{Z}$ mit $0 < r < m$ und hätten $r = n - ms \in H$, im Widerspruch zur Minimalität von m. □

Definition 2.2.6
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 $ad = b$,also genau dann, wenn $b \in a\mathbb{Z}$. 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 2.2.7 (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:

1. Es gibt $r, s \in \mathbb{Z}$ mit $c = ra + sb$. Für $c = 1$ heißt diese Aussage auch Satz von Bézout.
2. Teilt $d \in \mathbb{Z}$ sowohl a als auch b, so teilt d auch den größten gemeinsamen Teiler von a und b.

Beweis.
Die Teilmenge $a\mathbb{Z} + b\mathbb{Z} \subset \mathbb{Z}$ ist eine von Null verschiedene Untergruppe von $\mathbb{Z}$, also nach Satz 2.2.5 von der Form $a\mathbb{Z} + b\mathbb{Z} = c\mathbb{Z}$ für ein eindeutiges $c > 0$. Es gilt

a. Wegen $a \in c\mathbb{Z}$ gilt $c|a$. Ebenso gilt wegen $b \in c\mathbb{Z}$, dass $c|a$. Also ist c ein gemeinsamer Teiler von a und b.

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

c. Teilt eine Zahl d sowohl a und b, so teilt d auch $c = ra + sb$.

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

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

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

Dies soll nicht mit einem n-Tupel ganzer Zahlen verwechselt werden. Sind a und b nicht beide Null und ist c ihr größter gemeinsamer Teiler, so haben wir nach dem Vorhergehenden $(a, b) = (c)$. Wir schreiben daher auch $\mathrm{ggT}(a, b) = (a, b)$.

Definition 2.2.8

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

Man vergleiche diese Definition mit Definition 1.3.11.

Satz 2.2.9 (Primfaktorzerlegung)**.**

1. Jede von Null und Eins verschiedene natürliche Zahl $n \in \mathbb{N}$, $n \geq 2$ kann geschrieben werden als ein Produkt $n = p_1 p_2 \dots p_r$ von Primzahlen p_i.
2. Diese Darstellung ist eindeutig bis auf die Reihenfolge der Faktoren.

Beweis.

1. folgt mit vollständiger Induktion. Die Behauptung ist klar für $n = 2$. Angenommen, die Behauptung ist für alle Zahlen $\leq n$ gezeigt. Entweder ist $N + 1$ prim; dann gilt die Behauptung. Andernfalls schreibe $n+1 = ab$ mit $a, b \leq n$ und wende die Induktionsannahme an.
2. folgt ebenso mit vollständiger Induktion aus dem anschließenden Lemma.

□

Lemma 2.2.10.
Teilt eine Primzahl ein Produkt von ganzen Zahlen, so teilt sie einen der Faktoren.

Beweis.
Sei p eine Primzahl und seien $a, b \in \mathbb{Z}$ gegeben mit $p|ab$. Der ggT kann als Teiler von p nur p oder 1 sein. Teilt p nicht a, so folgt $\mathrm{ggT}(p, a) = 1$, und nach Satz 2.2.7 gibt es also $r, s \in \mathbb{Z}$ mit $1 = rp + sa$. Es folgt $b = rpb + sab$ und damit $p|b$. □

Betrachtung 2.2.11.

- 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.
- Wir erklären ihn am Beispiel $a = 160$, $b = 625$.
  In der linken Spalte der Gleichungen wird jeweils geteilt mit Rest. Will man nur den größten gemeinsamen Teiler kennen, so kann man die rechte Spalte ignorieren.

  Aus der Gleichung $625 = 3 \cdot 160 + 145$ schließen wir: jeder Teiler d von 625 und 160 ist auch ein Teiler von 160 und $145 = 625 - 3 \cdot 160$. Umgekehrt ist auch jeder Teiler von 160 und 145 ein Teiler von 625 und 160. Also gilt für den ggT

  $$(625, 160) = (160, 145) = (145, 15) = (15, 10) = (10, 5) = (5, 0) = 5 \ .$$

- Die oberste Zeile der rechten Tabelle ist eine Trivialität, die zweitoberste entsteht in offensichtlicher Weise aus der Zeile links daneben.

  Die dritte Zeile erhält man folgendermaßen: aus der linken Spalte der dritten Zeile folgt $15 = 160 - 1 \cdot 145$. Für 160 und 145 setzen wir die Ausdrücke aus den beiden darüberliegenden Zeilen ein:

  $$15 = 160 - 1 \cdot 145 = 160 - 1 \cdot (625 - 3 \cdot 160) = -625 + 4 \cdot 160$$

und haben 15 als ganzzahlige Kombination von 625 und 160 geschrieben. So fährt man fort und erhält so jede weitere Gleichung der rechten Spalte als eine Linearkombination der zwei darüberstehenden Gleichungen mit Koeffizienten, die sich aus der Gleichung links daneben ableiten lassen.

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

Wir finden für den größten gemeinsamen Teiler die Darstellung $-11 \cdot 625 + 43 \cdot 160 = 5$. Diese Darstellung ist nicht eindeutig, es gilt $(-11 + 32n) \cdot 625 + (43 - 125n) \cdot 160 = 5$ für alle $n \in \mathbb{Z}$.

Bemerkung 2.2.12.
Der euklidische Algorithmus liefert auch einen konstruktiven Beweis des Satzes 2.2.7 von Bézout.

2.3 Restklassen

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

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

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 die einelementige Menge $\{a\}$ mit a ab, so dass also zum Beispiel aB als $\{a\}B$ zu verstehen ist.

Definition 2.3.1

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

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

der Potenzmenge von G. 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 heißt auch ein Repräsentanten der Restklasse.

Lemma 2.3.2.
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 die Teilmenge $gH \subset G$ die einzige Linksnebenklasse, die g enthält. □

Beispiel 2.3.3.
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 $|\mathbb{Z}/m\mathbb{Z}| = m$. Mögliche Repräsentanten für diese m verschiedenen Restklassen sind die natürlichen Zahlen r mit $0 \leq r < m$.

Satz 2.3.4. (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 wegen Lemma 2.3.2 zu genau einer Links- bzw. Rechtsnebenklasse unter H. Für jedes $g \in G$ ist die Abbildung

$$\begin{array}{ccc} H & \to & gH \\ h & \mapsto & gh \end{array}$$

surjektiv und wegen der Kürzungsregel in Lemma 2.1.8 in Gruppen injektiv. Also hat jede dieser Nebenklassen genau $|H|$ Elemente. □

Weil die Linksnebenklassen die Menge G in paarweise disjunkte Teilmengen zerlegen, definieren sie eine Äquivalenzrelation auf G, mit $g_1 \sim g_2$, genau dann, wenn $g_2^{-1}g_1 \in H$.

Definition 2.3.5
Die Zahl der Restklassen $|G/H|$ nennt man auch den Index der Untergruppe H in G und schreibt $[G : H]$.

Korollar 2.3.6.
In einer endlichen Gruppe ist die Ordnung jeder Untergruppe ein Teiler der Gruppenordnung.

2.4 Normalteiler und Isomorphiesätze

Definition 2.4.1

1. *Sei G eine Gruppe. Eine Untergruppe H von G heißt ein Normalteiler von G genau dann, wenn für jedes $g \in G$ gilt $gH = Hg$.*

2. *Sei G eine Gruppe. Eine Untergruppe H von G heißt charakteristisch von G genau dann, wenn $\varphi(H) \subset H$ für alle Automorphismen $\varphi \in \operatorname{Aut} G$ gilt.*

Bemerkungen 2.4.2.

1. Für eine normale Untergruppe $N \subset G$ gilt $gNg^{-1} = N$ für alle $g \in G$. Um zu zeigen, dass eine Untergruppe normal ist, reicht es aus zu zeigen, dass für alle $g \in G$ gilt $gNg^{-1} \subseteq N$. Denn hieraus folgt $N = g^{-1}gNg^{-1}g \subset g^{-1}Ng$ für alle $g \in G$, also auch die umgekehrte Inklusion.

2. In einer kommutativen Gruppe ist jede Untergruppe ein Normalteiler, aber nicht jede Untergruppe ist charakteristisch.

3. 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.

4. Der Kern eines Gruppenhomomorphismus ϕ ist ein Normalteiler. Denn ist $g \in \ker \phi$, also $\phi(g) = e$, so folgt für jedes $h \in G$, dass $\phi(hgh^{-1}) = \phi(g)\phi(h)\phi(g)^{-1} = \phi(g)\phi(g)^{-1} = e$, also $hgh^{-1} \in \ker \phi$.

5. 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.

6. Das Zentrum einer Gruppe

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

   d.h. die Menge aller Gruppenelemente $g \in G$, die mit allen Gruppenelementen vertauschen, ist ein Normalteiler.

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

Wir hatten zu Beginn des Kapitels eine Verknüpfung von Teilmengen einer Gruppe G definiert. Die Elemente von G/H sind gerade Teilmengen vo G.

Satz 2.4.3 (Konstruktion der Restklassengruppe)**.**
Ist $H \subset G$ ein Normalteiler, so ist G/H abgeschlossen unter der induzierten Verknüpfung auf $\mathcal{P}(G)$: das Produkt von zwei Nebenklassen ist wieder eine Nebenklasse. Die Menge G/H der Nebenklassen wird mit dieser Verknüpfung eine Gruppe, genannt die Restklassengruppe oder auch der Quotient von G nach H.

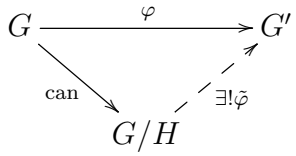
Beweis.
Es gilt $(gH)(g_1H) = gg_1HH = gg_1H$, also ist auf der Menge der Restklassen eine Verknüpfung definiert. Das Assoziativgesetz gilt als Folge der Assoziativität in G, das neutrale Element ist die Restklasse H. Das Inverse der Restklasse gH ist die Restklasse $g^{-1}H$. □

Beispiel 2.4.4.
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 2.4.5 (Universelle Eigenschaft der Restklassengruppe)**.**
Sei G eine Gruppe und $H \subset G$ ein Normalteiler.

1. Die Abbildung $\mathrm{can} : G \to G/H$, $g \mapsto gH$ ist ein Gruppenhomomorphismus mit Kern H. Sie heißt kanonischer Epimorphismus.

2. Sei $\varphi : G \to G'$ ein Gruppenhomomorphismus mit $\varphi(H) = \{1\}$, d.h. $H \subset \ker \varphi$. Dann gibt es genau einen Gruppenhomomorphismus $\tilde{\varphi} : G/H \to G'$ mit $\varphi = \tilde{\varphi} \circ \mathrm{can}$,



Beweis.
Die erste Aussage ist klar: es gibt immer eine Surjektion auf die Menge der Restklassen. Nach Definition der Verknüpfung der Restklassengruppe ist sie ein Gruppenhomomorphismus:

$$\mathrm{can}(g)\mathrm{can}(g_1) = gH\ g_1H = gg_1H = \mathrm{can}(gg_1)\ .$$

Um die zweite Aussage zu zeigen, überlegen wir uns, dass alle Elemente einer Restklasse gH das gleiche Element von G' als Bild haben. Ist nämlich $g' \in gH$, also $g' = gh$ mit $h \in H$, so ist $\varphi(g') = \varphi(gh) = \varphi(g)\varphi(h) = \varphi(g)$, da $h \in H \subset \ker \varphi$ gilt.

Dieses Element muss das Bild von gH unter $\tilde{\varphi}$ sein, $\tilde{\varphi}(gH)$. Damit ist $\tilde{\varphi}$ eindeutig festgelegt, und es gilt $\tilde{\varphi}(gH) = \varphi(g)$. Diese Abbildung ist ein Gruppenhomomorphismus: $\tilde{\varphi}(g_1Hg_2H) = \tilde{\varphi}(g_1g_2H) = \varphi(g_1g_2) = \varphi(g_1)\varphi(g_2) = \tilde{\varphi}(g_1H)\tilde{\varphi}(g_2H)$. □

Wir wenden das nun auf den Fall an, dass $H = \ker \varphi$ gilt:

Satz 2.4.6 (Isomorphiesatz)**.**
Sei $\varphi : G \to H$ ein Gruppenhomomorphismus. So induziert φ einen Isomorphismus $\tilde{\varphi} : G/\ker\varphi \xrightarrow{\sim} \mathrm{Im}\,\varphi$.

Beweis.
Nach dem vorhergehenden Satz 2.4.5 gibt es einen induzierten Morphismus $\tilde{\varphi}$ mit Definitionsbereich $G/\ker\varphi$. Durch die Einschränkung auf $\mathrm{Im}\,\varphi \subset H$ wird er surjektiv. Die Nebenklasse $g\ker\varphi$ ist im Kern $\ker\tilde{\varphi}$ genau dann, wenn $e = \tilde{\varphi}(g\ker\varphi) = \varphi(g)$ gilt, also genau für $g \in \ker\varphi$. Damit ist aber der Kern trivial und $\tilde{\varphi}$ injektiv. □

Korollar 2.4.7 (Noetherscher Isomorphiesatz)**.**
Sei G eine Gruppe und seien $K \subset H \subset G$ zwei Normalteiler von G. Dann 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.
Als Komposition surjektiver Abbildungen ist $G \to (G/K)/(H/K)$ surjektiv. Unsere Aussage folgt also aus dem Isomorphiesatz 2.4.6, sobald wir zeigen, dass H der Kern der 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 $gK \subset HK$. Da $1 \in K$ folgt $g \in HK \subset H$, also $g \in H$. □

Definition 2.4.8
Eine Gruppe heißt einfach, wenn sie nicht nur aus dem neutralen Element besteht, aber außer dem neutralen Element und der ganzen Gruppe keine Normalteiler hat.

Beispiel 2.4.9.
Alle endlichen einfachen Gruppen sind seit etwa 1980 bekannt, ihre Klassifikation ist jedoch schwierig. Beispiele von Serien einfacher Gruppen sind die zyklischen Gruppen von Primzahlordnung und die alternierenden Gruppen

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

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 größte darunter, das Monster mit

$$2^{46}.3^{20}.5^9.7^6.11^2.13^3.17.19.23.29.31.41.47.59.71 \sim 8 \cdot 10^{53}$$

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

2.5 Zyklische Gruppen

Definition 2.5.1
Sei g ein Element einer Gruppe G. Die Ordnung 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* 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.

Definition 2.5.2

1. *Für eine Teilmenge T einer Gruppe G definieren wir die von T erzeugte Untergruppe $\langle T \rangle \subset G$ als den Schnitt aller Untergruppen von G, die die Teilmenge T enthalten.*
2. *Eine Gruppe, die von einem einzigen Element erzeugt wird, heißt zyklisch.*

Bemerkungen 2.5.3.

1. Die von T erzeugte Untergruppe $\langle T \rangle$ ist bezüglich der durch Inklusion gegebenen Halbordnung die kleinste Untergruppe von G, die T enthält.

2. 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 $\langle T \rangle$ nur aus dem neutralen Element.

3. Insbesondere können wir für jede Gruppe G die von einem Element $g \in G$ erzeugte Untergruppe beschreiben als die Teilmenge

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

4. Eine Gruppe G, deren Kardinalität eine Primzahl ist, notwendig zyklisch. Nach Satz 2.3.4 kann sie außer $H = G$ und $H = 1$ keine weiteren Untergruppen haben. Insbesondere ist die Gruppe einfach, vgl. Beispiel 2.4.9. Also ist jedes vom neutralen Element verschiedene Element von G ein Erzeuger.

   Vorsicht: es gibt im Allgemeinen in zyklischen Gruppen Elemente, die keine Erzeuger sind.

Lemma 2.5.4 (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 der Gruppenhomomorphismus $n \mapsto g^n$ ein Isomorphismus $\mathbb{Z} \xrightarrow{\sim} \langle g \rangle$.

2. Hat g endliche Ordnung $\mathrm{ord} g = m$, so induziert der Gruppenhomomorphismus $n \mapsto g^n$ einen Isomorphismus $\mathbb{Z}/m\mathbb{Z} \xrightarrow{\sim} \langle g \rangle$.

Beweis.
Wir wenden den Isomorphiesatz 2.4.6 auf den Gruppenhomomorphismus $\varphi : \mathbb{Z} \to G$, $n \mapsto g^n$ an. Sein Bild ist die von g erzeugte Untergruppe $\langle g \rangle \subset G$.

Hat g unendliche Ordnung, so gibt es nach Definition 2.5.1 kein $n \in \mathbb{Z}$, so dass $g^n = 1$ gilt. Also ist der Gruppenhomomorphismus φ injektiv.

Nach Satz 2.2.6 ist $\ker \varphi$ von der Form $\ker \varphi = m\mathbb{Z}$ für ein $m \in \mathbb{Z}$, $m \geq 0$. Ist $m > 0$, so ist m ist die kleinste natürliche Zahl, für die $g^m = e$ gilt und somit nach Definition 2.5.1 die Ordnung von g. □

Motiviert durch dieses Lemma nennt man die Kardinalität einer Gruppe auch die Ordnung der Gruppe.

Korollar 2.5.5 (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 2.4.4 von Lagrange auf die von g erzeugte Untergruppe $H = \langle g \rangle \subseteq G$ an. □

Korollar 2.5.6.
Jede Untergruppe einer zyklischen Gruppe ist zyklisch. Genauer haben wir für beliebiges $m \in \mathbb{N}$ eine Bijektion

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

Beweis.
Für den Fall einer unendlichen zyklischen Gruppe ist die Aussage genau die von Satz 2.2.5. Wenn G zyklisch ist, können wir einen Erzeuger von G wählen. Jede Wahl eines Erzeugers $g \in G$ liefert einen Gruppenhomorphismus

$$\begin{array}{rccc} \varphi : \mathbb{Z} & \to & G \\ n & \mapsto & g^n \end{array},$$

der surjektiv ist, weil g ein Erzeuger ist. Der Kern von φ ist eine Untergruppe $K \subset \mathbb{Z}$, also nach Satz 2.2.5 von der Form $K = m\mathbb{Z}$. Sei $U \subset G$ eine Untergruppe. Dann ist das Urbild $H := \varphi^{-1}(U) \subset \mathbb{Z}$ eine Untergruppe, also von der Form $d\mathbb{Z}$. Das Bild $\varphi(d) \in U$ ist ein Erzeuger von U, also ist U zyklisch.

Es gilt $m\mathbb{Z} \subset d\mathbb{Z}$, also $m \in d\mathbb{Z}$, also $d|m$. Der Isomorphiesatz 2.4.6 liefert dann $U \cong d\mathbb{Z}/m\mathbb{Z}$. □

Definition 2.5.7
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.

Lemma 2.5.8.
Diese Restklassen in $\mathbb{Z}_n^\times$ sind gerade die Erzeugenden der zyklischen Gruppe $\mathbb{Z}_n$. Sie 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.

Beweis.
Nach dem Satz von Bézout 2.2.7 sind die Zahlen m und n genau dann teilerfremd, wenn es ganze Zahlen α, β gibt, so dass $1 = \alpha m + \beta n$ gilt. Genau dann gilt aber $\overline{1} = \overline{\alpha m} \bmod n$, d.h. die Restklassen in $\mathbb{Z}_n^\times$ sind genau diejenigen, ein multiplikatives Inverses haben. Damit ist klar, dass sie bezüglich der Multiplikation eine Gruppe bilden.

Die von einem teilerfremden $m \in \mathbb{Z}$ erzeugte Untergruppe enthält $\overline{1} = \alpha\overline{m} \in \mathbb{Z}_n$, also einen Erzeuger von $\mathbb{Z}_n$. Somit ist $\overline{m}$ selbst ein Erzeuger. Ist d ein nicht-trivialer gemeinsamer Teiler von m und n, so ist die Untergruppe $\langle\overline{m}\rangle \subset \mathbb{Z}_n$ in der nicht-trivialen Untergruppe $d\mathbb{Z}/m\mathbb{Z}$ enthalten; also kann $\overline{m}$ kein Erzeuger von $\mathbb{Z}_n$ sein. □

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

Korollar 2.5.9.

1. Ist n eine natürliche Zahl und m eine zu n teilerfremde ganze Zahl, dann gilt $m^{\varphi(n)} = 1 \bmod n$ (Satz von Euler).
2. Ist $p \in \mathbb{N}$ eine Primzahl und $m \in \mathbb{Z}$, dann gilt $m^p = m \bmod p$.
3. Sind U und V endliche Untergruppen einer Gruppe mit teilerfremden Ordnungen, dann ist $U \cap V = \{e\}$.

Beweis.

1. Die multiplikative Gruppe $\mathbb{Z}_n^\times$ hat Ordnung $\varphi(n)$; aus dem kleinen Fermatschen Satz 2.5.5 folgt, dass die Ordnung von $\overline{m} \in \mathbb{Z}_n^\times$ ein Teiler der Gruppenordnung $\varphi(n)$ ist.

2. Für p prim ist nach Bemerkung 2.5.3.4 jede von Null verschiedene Restklasse ein Erzeuger von $\mathbb{Z}_p$, also $\varphi(p) = p - 1$. Also ist wegen (i) $m^{p-1} = 1 \bmod p$ für m teilerfremd mit p. Daraus folgt $m^p = m \bmod p$, was auch noch für $m = 0$ gilt.

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

□

Bemerkung 2.5.10 (RSA-Verschlüsselung)**.**

- Als Konsequenz aus dem Satz von Euler halten wir zunächst fest:
  seien $n \in \mathbb{N}$ und $r \in (\mathbb{Z}_n)^\times$ gegeben. Dann ist für jedes $s \in \mathbb{Z}$ die Restklasse $r^s \bmod n$ leicht zu berechnen, wenn man $s \bmod \varphi(n)$ kennt. Denn sei $0 \leq s' < \varphi(n) - 1$ ein Repräsentant modulo $\varphi(n)$, also $s = q\varphi(n) + s'$. Dann gilt

$$r^s = r^{q\varphi(n)+s'} = r^{s'}(r^{\varphi(n)})^{r'} \overset{2.5.9.1}{=} r^{s'} \bmod n\,.$$

- Diese Beobachtung liegt dem sogenannten RSA-Verschlüsselungssystem (nach Ronald *R*ivest, Adi *S*hamir und Leonard *A*dlerman) zugrunde. Dies ist ein System mit öffentlichem Schlüssel.

  Derjenige, der eine Nachricht empfangen will, erzeugt zunächst zwei große Primzahlen p und q. Dann berechnet er ihr Produkt $n := pq$ und erzeugt dann eine Zahl E koprim zu $\varphi(n)$.

  Man wählt hierfür oft die Primzahl $E = 2^{16} + 1 = 65537$. Als Schlüssel macht er nur öffentlich das Paar (n, E), den öffentlichen Chiffrierschlüssel. Er hält aber die beiden Primzahlen p und q geheim.

- Der Sender der Nachricht zerlegt diese in Zahlen P_i, die kleiner als die Zahl n sind, die er aus dem öffentlichen Schlüssel kennt. Für jede der Zahlen P_i berechnet er mit Hilfe des öffentlichen Schlüssels (n, E)

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

  und schickt die Folge dieser Zahlen an den Empfänger.

- Zum Entschlüsseln berechnet der Empfänger eine Zahl D mit $ED = 1 \bmod \varphi(n) = (p-1)(q-1)$, zum Beispiel mit dem erweiterten euklidischen Algorithmus. Dazu muss man $\varphi(n)$ kennen, was wegen $\varphi(n) = (p-1)(q-1)$ leicht ist, wenn p und q getrennt bekannt sind, aber rechnerisch schwer, wenn nur n bekannt ist. (Diese Gleichheit werden wir im nächsten Unterkapitel zeigen.) Darauf beruht die Sicherheit der Verschlüsselung. Der Dechiffrierschlüssel ist (D, n).

  Der Empfänger benutzt ihn und berechnet $C_i^D \bmod n$. Wegen

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

  gibt dies die Nachricht im Klartext. Das geht wegen der Eingangsbemerkung schon, wenn man $ED \bmod \varphi(n)$ kennt.

- Durch Vertauschen der Rollen von Chiffrier- und Dechiffrierschlüssel kann man sogar elektronische Unterschriften erzeugen.

  Um eine Nachricht m zu signieren, wird vom Sender auf die Nachricht der eigene private Schlüssel D angewendet. Zum Prüfen wendet der Empfänger auf die Signatur $m^D \bmod N$ mit Hilfe des öffentlichen Schlüssels des Senders die Umkehrfunktion an und vergleicht diese mit der zusätzlich übermittelten unverschlüsselten Nachricht m. Wenn beide übereinstimmen, ist die Signatur gültig. Der Empfänger kann sicher sein, dass derjenige, der das Dokument signiert hat, auch den privaten Schlüssel besitzt.

2.6 Produkte und Erweiterungen

Definition 2.6.1

1. *Seien $G_1, \dots G_n$ Gruppen. Die Produktmenge*

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

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

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

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

Die folgenden Aussagen sind einfach zu beweisen.

Bemerkungen 2.6.2.

1. Das Zentrum eines äußeren direkten Produkts ist gleich dem direkten Produkt der Zentren:

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

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

3. 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 gilt sowohl $g_i g_j g_i^{-1} \in N_j$ als auch $g_j g_i g_j^{-1} \in N_i$, also $g_i g_j g_i^{-1} g_j^{-1} \in N_i \cap N_j = \{e\}$.

4. 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 $g_i = e$.

5. 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 in G 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 2.6.3.
Ist eine Gruppe $G = N_1 N_2 \dots N_k$ 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 2.6.4. (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 $N := \prod_{i=1}^{k} N_i$ ein Normalteiler von $G := \prod_{i=1}^{k} G$ und es gilt $G/N \cong \prod_{i=1}^{k} G_i/N_i$.

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

$$\begin{array}{rccc} \pi: & \prod_{i=1}^{k} G_i & \to & \prod_{i=1}^{k} G_i/N_i \\ & (a_1, \dots, a_k) & \mapsto & (\pi_1(a_1), \dots, \pi_k(a_k)) \end{array}$$

ein Homomorphismus mit Kern $\prod_{i=1}^{k} N_i = N$. Als Kern des Homomorphismus π ist N normal in G. Der Isomorphiesatz 2.4.6 zeigt die Behauptung. □

Korollar 2.6.5.
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 2.6.6.

1. Das direkte Produkt zweier zyklischer Gruppen *teilerfremder* Ordnung ist zyklisch.
2. Ist G zyklische Gruppe der Ordnung mn, wobei $\mathrm{ggT}(m,n) = 1$, 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 wegen Lemma 2.5.4 isomorph ist zu $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$, zeigen wir den äquivalenten

Satz 2.6.7.
Für teilerfremde natürliche Zahlen $m, n \in \mathbb{N}$ gilt $\mathbb{Z}_{mn} \cong \mathbb{Z}_m \times \mathbb{Z}_n$.

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 dem Satz von 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 2.2.7 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 $n \cdot m$,

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

so sieht man, dass die beiden Untergruppen $\langle \overline{n} \rangle$ und $\langle \overline{m} \rangle$ auch die Gruppe $\mathbb{Z}_{mn}$ 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 2.6.8. (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 2.6.7 sieht man, dass φ auch surjektiv ist, woraus der chinesische Restsatz folgt. □

Korollar 2.6.9.
Für die Eulersche φ-Funktion gilt

$$\varphi(mn) = \varphi(m)\varphi(n)$$

für alle teilerfremden natürlichen Zahlen m, n.

Beweis.
Die Eulersche φ-Funktion ist in Definition 2.5.7 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. □

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.

Definition 2.6.10

1. *Eine Sequenz von Gruppen mit Gruppenhomomorphismen*

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

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

2. *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 an jeder Stelle A_i ist.

3. *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

   $$1 \to A' \to A \to A'' \to 1\,.$$

   Wir sagen dann auch, A sei eine Gruppenerweiterung von A' durch A''.

Bemerkung 2.6.11.
Dann können wir A' mit einem Normalteiler von A identifizieren, und A'' mit der Faktorgruppe $A'' \cong A/A'$.

Definition 2.6.12
Sei N eine normale Untergruppe einer Gruppe G und H eine Untergruppe, so dass $G = HN$ und $H \cap N = \{e_G\}$ gelten. Dann heißt G das semidirekte Produkt von N und H.

Bemerkungen 2.6.13.

1. Der Vergleich mit Definition 2.6.1.2 zeigt, dass (innere) direkte Produkte spezielle semidirekte Produkte sind.

2. Wie in Bemerkung 2.6.2.4 zeigt man: jedes Element $g \in G$ kann *eindeutig* in der Form $g = nh$ mit $n \in N$ und $h \in H$ geschrieben werden. Denn $n_1h_1 = n_2h_2$ impliziert $n_2^{-1}n_1 = h_2h_1^{-1}$, und wegen $H \cap N = \{e_G\}$ auch $h_1 = h_2$ und $n_1 = n_2$.

3. Für jedes $h \in H$ ist $\gamma_h : n \mapsto hnh^{-1}$ ein Gruppenautomorphismus von N. Die Abbildung
$$\begin{array}{rcl} H & \to & \mathrm{Aut}(N) \\ h & \mapsto & \gamma_h \end{array}$$
ist ein Gruppenhomomorphismus. Es gilt in G
$$n_1h_1n_2h_2 = n_1\gamma_{h_1}(n_2)h_1h_2 \ ,$$
so dass G durch H, N und $\gamma : H \to \mathrm{Aut}(N)$ bestimmt ist. Das direkte Produkt liegt genau dann vor, wenn $\gamma_h = \mathrm{id}_N$ für alle $h \in H$. (Es ist allerdings schwieriger feststellen, ob das semidirekte Produkt zum direkten Produkt als Gruppe *isomorph* ist.)

4. Umgekehrt kann man, gegeben zwei Gruppen N und H mit Hilfe eines Gruppenhomomorphismus $\gamma : H \to \mathrm{Aut}(N)$ auf der Menge $N \times H$ eine Gruppenstruktur durch
$$(n_1, h_1)(n_2, h_2) = (n_1\gamma_{h_1}(n_2), h_1h_2)$$
definieren. Wir bezeichnen diese Gruppe mit $N \rtimes_\gamma H$. Man rechnet nach, dass dann N eine normale Untergruppe ist, H Untergruppe ist und die Sequenz
$$1 \to N \to N \rtimes_\gamma H \to H \ \to 1$$
die durch Injektionen und Projektionen gegeben ist, exakt ist. (Merkregel: die Spitze des Dreiecks $\rtimes$ zeigt auf den Normalteiler.)

5. Man beachte, dass es auch einen Gruppenhomomorphismus $H \to N \rtimes_\gamma H$ mit $h \mapsto (e_N, h)$ gibt.

Satz 2.6.14.
Sei $1 \to A' \xrightarrow{\iota} A \xrightarrow{\pi} A'' \to 1$ eine Gruppenerweiterung, für die ein Schnitt $s : A'' \to A$ existiert, d.h. ein Gruppenhomomorphismus mit $\pi \circ s = \mathrm{id}_{A''}$. Man sagt dann, die exakte Sequenz spaltet mit einem Schnitt $s : A'' \to A$. Dann ist A zu dem semidirekten Produkt $A' \rtimes_\gamma A''$ isomorph, das durch den Gruppenhomomorphismus
$$\begin{array}{rcl} \gamma : \quad A'' & \to & \mathrm{Aut}(A') \\ h & \mapsto & \gamma_h \end{array}$$
mit $\gamma_h(a') := \iota^{-1}\left(s(h)\iota(a')s(h)^{-1}\right)$ für $a' \in A'$ und $h \in A''$ gegeben ist. Hierzu beachte man, dass $\iota(A') = \ker\pi$ als Kern eine normale Untergruppe von A ist, so dass $s(h)\iota(a')s(h)^{-1} \in \iota(A')$ gilt.

Beweis.
Betrachte die Abbildung

$$\begin{array}{rccc} \phi: & A' \times A'' & \to & A \\ & (a', a'') & \mapsto & \iota(a')s(a'') \end{array}$$

1. Dies ist ein Gruppenhomomorphismus $A' \rtimes_\gamma A'' \to A$, denn es gilt:

$$\begin{array}{rcl} \phi((a_1'a_1'')(a_2', a_2'')) & = & \phi((a_1's(a_1'')a_2's(a_1'')^{-1}, a_1''a_2'') \\ & = & a_1's(a_1'')a_2's(a_1'')^{-1}s(a_1'')s(a_2'') = a_1's(a_1'')a_2s(a_2'') \\ & = & \phi(a_1', a_1'') \cdot \phi(a_2', a_2'') \ . \end{array}$$

2. Der Gruppenhomomorphismus ist injektiv: gilt $\iota(a')s(a'') = e_A$, so ist

$$e_{A''} = \pi(e_A) = \pi(a') \cdot \pi \circ s(a'') = \ a'' \ ,$$

da $\pi \circ s = \mathrm{id}_{A''}$ und $\pi|_{A'}$ trivial ist. Wegen der Injektivität von ι ist $a' = e_{A'}$ und der Gruppenhomomorphismus ϕ injektiv.

3. Die Abbildung ist surjektiv. Für jedes $a \in A$ gilt für $d := a \cdot s\pi(a)^{-1}$, dass $\pi(d) = \pi(a) \cdot \pi \circ s \circ \pi(a)^{-1} = \pi(a)\pi(a)^{-1} = e_{A''}$. Also gilt $d \in \ker \pi = \mathrm{im}\iota$, und es gibt $a' \in A'$ mit $\iota(a') = d = a \cdot s\pi(a)^{-1}$. Damit ist $a = \iota(a')s\pi(a)$ im Bild der Abbildung ϕ.

□

Beispiele 2.6.15.

1. Die Signums-Abbildung liefert die kurze exakte Sequenz

$$1 \to A_n \to \mathcal{S}_n \to \mathbb{Z}_2 \cong \{\pm 1\} \to 1 \ .$$

Sei $\tau \in \mathcal{S}_n$ eine beliebige Transposition. Dann ist $s(1) = 1$ und $s(-1) = \tau$ ein Schnitt der Signums-Abbildung. Es folgt $\mathcal{S}_n = A_n \rtimes \mathbb{Z}_2$. Es liegt kein direktes Produkt vor, weil die Permutation τ nicht mit allen Elementen von A_n vertauscht.

2. Für die die allgemeine lineare Gruppe $\mathrm{GL}_n(K)$ über einem Körper K liefert die Determinante die kurze exakte Sequenz

$$1 \to \mathrm{SL}_n(K) \to \mathrm{GL}_n(K) \xrightarrow{\det} K^\times \to 1 \, .$$

Indem man $a \in K^\times$ auf die Diagonalmatrix mit Einträgen $(a, 1, \ldots, 1)$ abbildet, wird ein Schnitt für die Determinante definiert. Wiederum liegt kein direktes Produkt vor.

3. Sei $G \cong \langle g \rangle$ zyklisch der Ordnung 4. Die Untergruppe $N := \langle g^2 \rangle$ ist ein Normalteiler und zyklisch der Ordnung 2. Der Quotient G/N ist auch zyklisch der Ordnung 2 mit Erzuger $\overline{g} \in G/N$. Die exakte Sequenz

$$1 \to N \to G \ \to G/N \to 1$$

spaltet nicht. Denn ein Schnitt $s : G/N \to G$ müsste die Nebenklasse gN auf g oder g^3 abbilden, aber diese Elemente haben Ordnung 4.

2.7 Operationen von Gruppen auf Mengen

Wir beginnen mit dem folgenden Satz:

Satz 2.7.1 (Cayley)**.**
Jede Gruppe G ist zu einer Gruppe von Permutationen der Menge G isomorph.

Beweis.
Für $g \in G$ definieren wir eine Permutation $L(g) \in \mathcal{S}(G)$ durch

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

Aus der Assoziativität der Gruppe folgt $L(ab)x = (ab)x = a(bx) = L(a)(L(b)(x)$. Es gilt $L(e) = \mathrm{id}$, und das Inverse ist $L(a)^{-1} = L(a^{-1})$. Also ist L ein Gruppenhomomorphismus von G in die Permutationsgruppe $\mathcal{S}(G)$. Er ist injektiv, denn $a \in \ker L$ heißt, dass $e = L(a)e = a$. Wegen des Isomorphiesatzes 2.4.6 können wir G mit dem Bild unter L in $\mathcal{S}(G)$ 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 2.7.2

1. *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

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

2. *Eine Menge mit einer Operation von G heißt auch G–Menge, und wir sagen, G wirkt auf X.*

Bemerkung 2.7.3.
Es operiert G auf einer Menge X also genau dann, wenn es einen Gruppenhomomorphismus von G in die Permutationsgruppe $\mathcal{S}(X)$ gibt.

Satz 2.7.4.
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.

Bemerkungen 2.7.5.

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

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

Wie bei jeder Äquivalenzrelation bilden die Äquivalenzklassen, also hier die Bahnen 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.

2. Auf jeder nicht-leeren Menge kann man für jede Gruppe die triviale Operation definieren:

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

3. 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 von links durch Translation. Wir werden später noch eine andere Operation einer Gruppe auf sich selbst kennen lernen.

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

$$\mathrm{GL}(V) \times V \to V\,.$$

Beschreiben Sie hier den Bahnenraum!

5. Sei H eine Untergruppe von G. Dann ist die Menge $X = G/H$ der Linksnebenklassen durch Linksmultiplikation eine G–Menge.

6. 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 2.7.6
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 eine Untergruppe, so ist HA eine H–Menge.

Lemma 2.7.7. (Bahnen als Quotienten)
Sei G Gruppe, X eine G–Menge und $x \in X$. Dann definiert die Operation von G auf X eine Bijektion von Mengen 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 sein soll, 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

$$g_1 x = g_2 x \iff g_2^{-1} g_1 x = x \iff g_2^{-1} g_1 \in G_x\ ,$$

was genau dann der Fall ist, wenn g_1 und g_2 in der gleichen Nebenklasse bezüglich G_x sind. □

Korollar 2.7.8.

1. Bahnformel
   Sei G *endliche* Gruppe. Dann hat man für die Kardinalitäten

   $$|G| = |G_x|\ |Gx| \qquad (*)$$

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

2. Ein Vertretersystem einer G–Menge X ist eine Teilmenge $V \subset X$ mit den folgenden zwei Eigenschaften:

   a) Für jedes $x \in X$ existiert ein $v \in V$, so dass, $Gx = Gv$ gilt.

   b) Für je zwei verschiedene $a, b \in V$ sind die Bahnen disjunkt, $Ga \cap Gb = \emptyset$.

   Für eine gegebene Gruppenwirkung ist die Wahl eines Vertretersystems im Allgemeinen 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 $\mathrm{Fix}_G(X)$.

3. Sei X eine endliche G–Menge und V ein Vertretersystem. Dann gilt als Folge von $(*)$

$$|X| \overset{(*)}{=} \sum_{x \in V} [G : G_x] = |\mathrm{Fix}_G(x)| + \sum_{\substack{x \in V \\ [G:G_x]>1}} [G : G_x]\,. \tag{1}$$

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

$$|X| = |\mathrm{Fix}_G(x)| \bmod p\,.$$

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

Beweis.
Aus (1) folgt

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

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

$$|X| - |\mathrm{Fix}_G(x)| = 0 \bmod \ p\,.$$

Ist $|X| \neq 0 \bmod p$, so muss auch $|\mathrm{Fix}_G(X)| \bmod p$ ungleich null sein. Damit kann $|\mathrm{Fix}_G(x)|$ aber gleich Null sein. □

2.8 Konjugationsklassen

Definition 2.8.1

1. *Ist G eine Gruppe und $x \in G$ ein Element, so ist*

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

ein Gruppenautomorphismus von G, genannt die Konjugation mit g.

2. *Die Automorphismen von G, die sich als Konjugation schreiben lassen, heißen innere Automorphismen.*

3. *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. Sein Kern ist das Zentrum von G.

4. *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 2.8.2.

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

2. Die Konjugationsklassen einer abelschen Gruppe bestehen aus je nur einem Element.

3. Die Standuntergruppe eines Elements $x \in G$ unter der Wirkung durch Konjugation heißt der Zentralisator $Z_G(x)$ von x:

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

4. Als Spezialfall der Bahnengleichung aus Korollar 2.7.8 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

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

denn die Menge der Fixpunkte der Wirkung durch Konjugation ist

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

gleich dem Zentrum der Gruppe G.

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.

Korollar 2.8.3.
Eine p-Gruppe G hat 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. □

2.9 Endlich erzeugte abelsche Gruppen

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

Satz 2.9.1.
Sei G eine endlich erzeugte abelsche Gruppe. Dann 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

$$G \cong \mathbb{Z}_{d_1} \times \mathbb{Z}_{d_2} \times \cdots \times \mathbb{Z}_{d_s} \tag{2}$$

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

Satz 2.9.2.
Sei G eine endlich erzeugte abelsche Gruppe.

1. Dann gibt es Primzahlpotenzen $q_1, \ldots, q_t$ und eine natürliche Zahl $r \in \mathbb{N}$ mit

$$G \cong \mathbb{Z}_{q_1} \times \cdots \times \mathbb{Z}_{q_t} \times \mathbb{Z}^r \tag{3}$$

2. 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 2.9.3.
Die Faktoren in den Zerlegungen in den Sätzen 2.9.1 und 2.9.2 sind nicht eindeutig als Untergruppen von G. Mit anderen Worten: die Isomorphien in 2.9.1 und 2.9.2 sind *nicht* kanonisch, d.h. in eindeutiger Weise ausgezeichnet.

Definition 2.9.4

1. *Ein Element endlicher Ordnung in einer Gruppe heißt Torsionselement.*
2. *Eine Gruppe, in der alle vom neutralen Element verschiedenen Elemente unendliche Ordnung haben, heißt torsionsfrei .*
3. *Eine Gruppe heißt Torsionsgruppe, wenn alle ihre Elemente Torsionselemente sind.*

Beispiele torsionsfreier Gruppen sind die abelschen Gruppen $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$. Endliche Gruppen sind wegen des kleinen Fermatschen Satzes 2.5.5 Beispiele für Torsionsgruppen.

Lemma 2.9.5.
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

$$0 = a_1 x_1 + \cdots + a_r x_r \qquad (*)$$

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–triviale Relation gibt. Wir wählen in diesem Erzeugendensystem die Relation $(*)$, in der die natürliche Zahl

$$\sum_i |a_i| > 0$$

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 2.9.6.
Sei G eine abelsche Gruppe.

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

2. Der Quotient G/T ist torsionsfrei.

3. 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 in der exakten Sequenz

   $$1 \to T \to G \to G/T \to 1 \ ,$$

   d.h. es gibt einen Gruppenhomomorphismus $s : G/T \to G$, so dass $\pi \circ s = \mathrm{id}_{G/T}$.

Beweis.

1.,2. Als Übung dem Leser überlassen.

3. 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.

Die Gruppe G/T ist als Quotient einer endlich-erzeugten Gruppe endlich erzeugt. Der Isomorphismus von G/T auf $\mathbb{Z}^r$ für geeignetes $r \in \mathbb{N}$ folgt aus Lemma 2.9.5. Die Surjektion $\pi : G \to G/T$ spaltet auf Grund des folgenden allgemeineren Lemmas. □

Lemma 2.9.7.
Jede Surjektion $\pi : G \to \mathbb{Z}^r$ einer *abelschen* Gruppe G auf die freie abelsche Gruppe $\mathbb{Z}^r$ spaltet.

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

$$\begin{array}{rcl} s : \mathbb{Z}^r & \to & G \\ e_i & \mapsto & x_i \end{array}$$

Da G abelsch ist, ist s ein Gruppenhomomorphismus und es gilt

$$\pi \circ s(e_i) = \pi(x_i) = e_i.$$

Da $\{e_i\}_{i=1,\dots r}$ Basis ist, folgt $\pi \circ s = \mathrm{id}_{\mathbb{Z}^r}$, so dass s ein Schnitt ist. Man beachte, dass der Schnitt s nicht kanonisch ist: die Wahl der Repräsentanten x_i der Urbilder ist nicht eindeutig. □

Die Kombination dieses Resultats mit Satz 2.6.14 zeigt:

Korollar 2.9.8.
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 nach Lemma 2.9.6.1 als Untergruppe eindeutig bestimmt.

Beweis.
Da G abelsch ist, ist für jede Wahl eines Schnitts $s : \mathbb{Z}^r \to G$ der Homomorphismus $\mathbb{Z}^r \to \mathrm{Aut}(T)$ mit $a'' \mapsto \gamma_{a''}$ mit $\gamma_{a''}(a') = s(a'')a's(a'')^{-1}$ aus Satz 2.6.14 die Identität. □

Lemma 2.9.9.

1. 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, den p-Torsionsanteil.

2. Ist T eine endliche abelsche Gruppe und sind $p_1, \dots, p_u$ die Primfaktoren der Gruppenordnung $|T|$, so hat man
$$T \cong T(p_1) \times \cdots \times T(p_u).$$

Beweis.

1. In einer abelschen Gruppe teilt die Ordnung des Produkts zweier Elemente das Produkt ihrer Ordnungen, denn es gilt:
$$(ab)^{\mathrm{ord}(a)\cdot\mathrm{ord}(b)} = a^{\mathrm{ord}(a)\mathrm{ord}(b)} b^{\mathrm{ord}(b)\mathrm{ord}(a)} = e.$$

2. Die Untergruppen $T(p_1)$ sind als Untergruppen einer abelschen Gruppe trivialerweise normal. Sei nun $x \in T(p_1) \cap T(p_2)T(p_3)\dots T(p_u)$. Dann ist einerseits die Ordnung von x wegen $x \in T(p_1)$ eine Potenz von p_1. Andererseits teilt die Ordnung von x auch die Gruppenordnung von $T(p_2)T(p_3)\dots T(p_u)$, die zu p_1 koprim ist. Folglich ist die Ordnung von x gleich eins, also $x = e$. Dass das Produkt aller Untergruppen $T(p)$ gleich T ist, folgt schließlich aus dem chinesischen Restsatz 2.6.7, angewandt auf die zyklische Untergruppe $\langle x\rangle$ von T für jedes $x \in T$.

□

Die Hauptarbeit für den Beweis von 2.9.1 und 2.9.2 geht nun in das folgende vielleicht etwas technisch anmutende

Lemma 2.9.10.
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 die zyklische Untergruppe $\langle a\rangle$ nur im neutralen Element treffen. Dann ist A ein 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 betrachten wir die kanonische Projektion

  $$\pi : A \to \overline{A} := A/B$$

  auf die Faktorgruppe ein und zeigen durch einen Widerspruchsbeweis, dass $\overline{A}$ vom Bild $\overline{a} = \pi(a)$ von a erzeugt wird. Sei $\bar{Z} := \langle\overline{a}\rangle$ die von $\bar{a}$ erzeugte Untergruppe vder Faktorgruppe $\overline{A}$.

- Wir nehmen also an, es gäbe ein Element $\overline{c} \in \overline{A} \setminus \overline{Z}$. Als Quotient einer p-Gruppe ist $\overline{A}$ eine p-Gruppe. Es gibt daher eine natürliche Zahl $s \in \mathbb{N}$, 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

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

  mit dem wir weiter arbeiten werden.

- Die Ordnung von $\overline{a}$ in $\overline{Z}$ ist gleich der Ordnung von a in A, da B nach Voraussetzung die Untergruppe $\langle a\rangle$ nur im neutralen Element trifft. Andererseits ist allgemein für jedes $x \in A$ die Ordnung der Projektion $\pi(x)$ ein Teiler der Ordnung von x,

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

  Die Ordnung des Bilds $\pi(x)$ im Quotienten $\overline{A}$ ist also kleiner oder gleich der Ordnung von x. Also ist die Ordnung von $\overline{a}$ auch die maximale Ordnung unter allen Elementen der Faktorgruppe $\overline{A}$.

- Würde nun die Potenz $\overline{d}^p \in \overline{Z}$ die Gruppe $\overline{Z}$ erzeugen, so hätte $\overline{d}$ selbst die Ordnung

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

im Widerspruch zur Maximalität der Ordnung von $\overline{a}$ in $\overline{A}$. Also kann $\overline{d}^p$ kein Erzeuger von $\overline{Z}$ sein.

Aus der Struktur zyklischer Gruppen folgt, dass es ein Element $\overline{f} \in \overline{Z}$ gibt mit

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

Aus dieser Gleichung folgt, dass die von $\overline{x} := \overline{d}(\overline{f})^{-1}$ erzeugte Untergruppe von $\overline{A}$ zyklisch von Primzahlordnung ist. Diese Gruppe hat daher keine echten Untergruppen. Da $\overline{x} \notin \overline{Z}$, ist der Schnitt dieser Untergruppe mit $\overline{Z}$ trivial:

$$\langle \overline{x} \rangle \cap \overline{Z} = \{\overline{e}\}\ . \qquad (*)$$

- Die Untergruppe $\pi^{-1}(\langle \overline{x} \rangle) \subset A$
  - enthält B, da $\overline{e} \in \langle \overline{x} \rangle$ und $\pi^{-1}(\overline{e}) = B$.
  - enthält B echt, da $\langle \overline{x} \rangle$ nicht trivial ist.
  - trifft $\langle a \rangle$ nur im neutralen Element: denn für

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

folgt $\pi(y) \in \overline{Z} \cap \langle \overline{x} \rangle \overset{(*)}{=} \{\overline{e}\}$. Also ist $\pi(y) = \overline{e}$, somit $y \in B$. Da auch $y \in \langle a \rangle$ und B die Gruppe $\langle a \rangle$ nur im neutralen Element trifft, 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 Satz 2.9.2.1 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 2.9.8, 2.9.9 und 2.9.10 in dieser Reihenfolge angewandt haben. Wir müssen aber noch die Eindeutigkeit des Rangs r der freien Gruppe und der Zerlegung des Torsionsanteils zeigen. Dazu schreiben wir den Rang in einer Weise, die offensichtlich nicht von der Zerlegung abhängt.

Wir beobachten zunächst, dass der Raum der Gruppenhomomorphismen $\mathrm{Hom}(G, \mathbb{Q})$ 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.

Lemma 2.9.11.
In jeder Zerlegung $G = G_{tor} \times \mathbb{Z}^r$ einer endlich erzeugten abelschen Gruppe, wobei G_{tor} eine Torsionsgruppe ist, gilt

$$r = \dim_{\mathbb{Q}}\ \mathrm{Hom}\ (G, \mathbb{Q})\ .$$

Wir nennen r den Rang von G; er hängt nicht von der Zerlegung ab.

Beweis.

- Sei $\varphi \in \mathrm{Hom}(G, \mathbb{Q})$ und g ein Torsionselement der Ordnung N. Dann gilt $N\varphi(g) = \varphi(g^N) = 0$. In $\mathbb{Q}$ folgt daraus $\varphi(g) = 0$. Also verschwinden alle Homomorphismen nach $\mathbb{Q}$ auf dem Torsionsanteil von G.

- Für jede Gruppe G liefert

$$\begin{aligned} \mathrm{Hom}(\mathbb{Z}, G) &\overset{\cong}{\to} G\,, \\ \varphi &\mapsto \varphi(1) \end{aligned}$$

  einen Isomorphismus mit der Umkehrabbildung, die $g \in G$ den Gruppenhomomorphismus $\varphi_g : \mathbb{Z} \to G$ mit $\varphi_g(n) = g^n$ zuordnet.

- Für das endliche direkte Produkt von Gruppen hat man einen Isomorphismus von $\mathbb{Q}$–Vektorräumen

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

  unter dem die Familie $(\varphi_1, \ldots, \varphi_r)$ auf den Gruppenhomomorphismus $\varphi(g_1, \ldots, \varphi_r) = \sum_{i=1}^{r} \varphi_i(g_i)$ abgebildet wird.

- Hat also G die Zerlegung $G = G_{tor} \times \mathbb{Z}^r$, so ist $\dim_{\mathbb{Q}} \mathrm{Hom}(G, \mathbb{Q}) = r$.

□

Bemerkung 2.9.12.
Insbesondere sind die endlich-erzeugten freien abelschen Gruppen $\mathbb{Z}^m$ und $\mathbb{Z}^n$ genau 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 auf die Untergruppen

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

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 2.9.13 (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 die Primzahl p teilt. Dann gehorcht die Zahl der zyklischen Faktoren $z(G)$ von G der Gleichung

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

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

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

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

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

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

Nach Satz 2.9.2.1 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 des Isomorphismus

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

□

Damit ist auch die Aussage von Satz 2.9.2.2 bewiesen. Es bleibt Satz 2.9.1 zu zeigen.

Beweis.
Zerlege für alle Teiler p von $|G_{tor}|$ den p-Torsionanteil $T(p)$ gemäß

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

mit $m(p) \in \{1, 2 \dots\}$ 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 $\tilde{d}_{i+1} | \tilde{d}_i$. Da alle Faktoren in $\tilde{d}_1$ koprim sind, erlaubt es der chinesische Restsatz 2.6.8, Produkte von zyklischen Gruppen zusammen zu fassen:

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

□

2.10 Symmetrische Gruppen

Definition 2.10.1
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 $\sigma \in \mathcal{S}_n$ gibt eine Partition von n: die Längen der Bahnen der Operation der von σ zyklisch erzeugten Gruppe $\langle\sigma\rangle$ auf der n-elementigen Menge $\{1, \ldots, n\}$.
- Die Teilmenge derjenigen Punkte, die σ nicht festlässt, heißen der Träger der Permutation.
- Hat $\langle\sigma\rangle$ außer einer p–elementigen Bahn nur Fixpunkte, so nennt man σ einen p–Zykel. Wir schreiben dann auch $(m_1, m_2, \ldots, m_p)$ für den p-Zykel mit $m_1 \mapsto m_2 \mapsto \ldots \mapsto m_p \mapsto m_1$. 2–Zykel (m_1, m_2) heißen auch Transpositionen.
- Hat $\langle\sigma\rangle$ genau zwei zweielementige Bahnen und sonst nur Fixpunkte, so heißt σ Doppeltransposition.
- Zykel mit disjunkten Trägern kommutieren in $\mathcal{S}_n$. Aus dem ersten Punkt folgt, dass man jede Permutation als Produkt von Zykeln mit disjunkten Trägern schreiben kann. Diese Zerlegung ist eindeutig bis auf Reihenfolge.
- Wenn man alle Permutationen in $\mathcal{S}_n$ betrachtet, tritt jede Partition von n auf.

  Es gilt für jeden Zyklus $\sigma := (m_1, m_2, \ldots, m_k) \in \mathcal{S}_n$ und jede Permutation $\pi \in \mathcal{S}_n$, dass

  $$\pi(m_1, m_2, \ldots, m_k)\pi^{-1} = (\pi(m_1), \pi(m_2), \ldots, \pi(m_k)) \qquad (*)$$

  gilt, denn man rechnet nach

  $$\pi\sigma\pi^{-1}(\pi(m_i)) = \pi\sigma(m_i) = \pi(m_{i+1}) \quad \text{für } i = 1, \ldots k-1$$

  und $\pi\sigma\pi^{-1}(\pi(m_k)) = \pi\sigma(m_k) = \pi(m_1)$.
- Aus der Relation $(*)$ folgt leicht mit Hilfe einer Zykelzerlegung $\pi' = \sigma_1 \ldots \sigma_r$ und $\pi\pi'\pi^{-1} = \pi\sigma_1\pi^{-1} \ldots \pi\sigma_r\pi^{-1}$, dass zwei Permutationen genau dann konjugiert sind, wenn sie die gleiche Partition haben.

Satz 2.10.2.

1. Die symmetrische Gruppe $\mathcal{S}_r$ wird von den Transpositionen erzeugt.
2. Die alternierende Gruppe A_r wird von den Dreizykeln erzeugt.

Beweis.

1. Jede Permutation kann als kommutierendes Produkt von Zykeln geschrieben werden. Für jeden Zykel finden wir

   $$(m_1, m_2, \ldots, m_k)^{-1} = (m_1, m_2)(m_2, m_3) \ldots (m_{k-1}, m_k)$$

   Unsere Konvention ist dabei so, dass Permutationen von links nach rechts multipliziert werden.

2. folgt aus der Tatsache, dass A_r durch Paare von Transpositionen erzeugt wird und für a, b, c, d paarweise verschiedene Elemente gilt

$$(ab)(cd) = (bcd)(abc) \quad \text{und} \quad (ab)(bc) = (cab)\,.$$

□

Hauptziel dieses Abschnitts ist der Beweis des folgenden Satzes:

Satz 2.10.3.
Die alternierenden Gruppen A_r sind einfach für $r \geq 5$ und für $r = 3$.

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 nach Bemerkung 2.5.3.4 einfach.
- In der Gruppe A_4 gibt es drei Doppeltranspositionen. Sie bilden mit dem neutralen Element eine vierelementige 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, die 3 Doppeltranspositionen der Ordnung 2 und 8 Dreizykel, die alle Ordnung 3 haben. Die Konjugation mit einem Gruppenelement ist ein Gruppenautomorphismus und ändert daher die Ordnung eines Elements nicht. Daher werden alle Doppeltranspositionen von A_4 durch Konjugation auf Doppeltranspositionen abgebildet. Die Untergruppe, die aus den Doppeltranspositionen und dem neutralen Element besteht, ist also eine normale Untergruppe von A_4. Somit ist A_4 keine einfache Gruppe.

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

Lemma 2.10.4.
1. Für $r \geq 5$ sind je zwei Doppeltranspositionen schon konjugiert in A_r.
2. Für $r \geq 5$ sind je zwei Dreizykel schon konjugiert in A_r.

Beweis.
1. Wir zeigen, dass jede Doppeltransposition zu $(1,2)(3,4)$ konjugiert ist. Dazu beachte, dass aus $(*)$ folgt, dass die Doppeltransposition $(i,j)(k,l)$ durch Konjugation mit jeder der beiden Permutationen

   $$\begin{pmatrix} 1 & 2 & 3 & 4 & \dots n \\ i & j & k & l & \dots \end{pmatrix} \quad \begin{pmatrix} 1 & 2 & 3 & 4 & \dots n \\ i & j & l & k & \dots \end{pmatrix}$$

   in die Doppeltransposition $(1,2)(3,4)$ überführt werden kann. Eine der beiden Permutationen hat aber signum $+1$ und liegt in A_r.

2. Wir zeigen, dass jeder Dreizykel zum 3-Zykel $(1,2,3)$ konjugiert ist. Dazu beachte, dass aus $(*)$ folgt, dass der Dreizykel (i,j,k) durch Konjugation mit jeder der beiden Permutationen

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & \dots n \\ i & j & k & l & m & \dots \end{pmatrix} \quad \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & \dots n \\ i & j & k & m & l & \dots \end{pmatrix}$$

mit l, m von i, j, k verschiedenen Werten inden 3-Zykel $(1,2,3)$ überführt werden kann. Eine der beiden Permutationen hat aber signum $+1$ und liegt in A_r.

□

Wir können nun Satz 2.10.3 beweisen:

Beweis.
Sei N ein Normalteiler von A_r. Sei $\sigma \in N$ eine Permutation mit einer maximalen Zahl von Fixpunkten, die vom neutralen Element von A_r verschieden ist. Wir wollen zeigen, dass σ ein 3-Zykel ist. Dann folgt aus Lemma 2.10.4.2, dass N als Normalteiler von A_r alle 3-Zykel enhält. Nach Satz 2.10.2.2 erzeugen aber die 3-Zykel ganz A_r, also folgt $N = A_r$.

Wir betrachten die Bahnen von σ.

- Hat jede Bahn von σ höchstens 2 Elemente, so gibt es mindestens 2 Bahnen (ab) und (cd), da σ als Element von A_r gerade ist. Wähle ein weiteres Element $e \neq a, b, c, d$ und setze $\tau := (cde)$. Wir betrachten $\sigma' := \tau\sigma\tau^{-1}\sigma^{-1}$, was wieder im Normalteiler N liegt. Fixpunkte außerhalb von $a, b, c, d, e, \sigma(e)$ sind auch Fixpunkte von σ'. Außerdem sind a, b nun Fixpunkte von σ'. Vielleicht ist e ein Fixpunkt von σ gewesen, aber ist keiner von σ'; auch in diesem Fall hat σ' mehr Fixpunkte. Man rechnet nach, dass $\sigma'(c) = \sigma(e) \neq c$. Also ist σ' nicht die Identität. Dies ist im Widerspruch zur Wahl von σ als Element mit maximal vielen Fixpunkten.

- Also hat σ eine Bahn mit mindestens 3 Elementen. Wir nehmen an, dass $\sigma(a) = b$ und $\sigma(b) = c$ mit paarweise verschiedenen a, b, c gilt. Wenn σ ein 3-Zykel ist, sind wir fertig. Ist σ kein 3-Zykel, so muss σ mindestens ein weiteres Element bewegen. Nur ein Element geht nicht, da dann ein 4-Zykel vorliegt, der ungerade ist. Also gibt es zwei weitere Elemente d, e, die keine Fixpunkte von σ sind. Setze $\tau := (cde)$ und betrachte wieder $\sigma' := \sigma^{-1}\tau^{-1}\sigma\tau \in N$. Jeder Fixpunkt von σ ist auch Fixpunkt von σ'. Zusätzlich gilt $\sigma'(b) = b$. Also hat σ' mehr Fixpunkte als σ. Da $\sigma'(c) = d$, liegt auch nicht die Identität vor. Also haben wir auch hier einen Widerspruch, wenn σ kein 3-Zykel ist.

□

2.11 Die Sylowsätze

Ziel dieses Abschnitts ist, es eine gewisse Übersicht über die Untergruppen U einer endlichen Gruppe G zu bekommen. Der Satz 2.3.4 von Lagrange sagt uns, dass die Ordnung einer Untergruppe $|U|$ die Gruppenordnung $|G|$ teilt. Im Fall von zyklischen Gruppen wissen wir schon aus Satz 2.5.6, 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 als einfache Gruppe keine Untergruppe der Ordnung $r!/4$. Denn diese wäre vom Index zwei in A_r und daher nach einem Übungsblatt Normalteiler.

Alle Gruppen in diesem Kapitel 2.11 sind endlich.

Satz 2.11.1. (Struktur von p–Gruppen)
Ist G eine p–Gruppe, so gibt es in G eine absteigende Kette

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

von Normalteilern von G, so dass

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

Beweis.
Wir schreiben die Gruppenordnung als $|G| = p^s$ und führen den Beweis mit Induktion nach s. Der Induktionsanfang ist wegen Bemerkung 2.5.3.4 klar.

Die Gruppe G hat nach Korollar 2.8.3 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 der p-Gruppe $\overline{G} = G/G_1$ eine Kette

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

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 $\overline{G}$ nach Bemerkung 2.4.2.5 in G normal. Aus dem Isomorphiesatz folgt

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

Der Noethersche Isomorphiesatz 2.4.7 liefert dann die Isomorphien

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

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

Bemerkungen 2.11.2. (Doppelnebenklassen)

1. Für jede Untergruppe $H \subset G$ 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 Normalisator von H in G. Sie ist eine Untergruppe von G. Man hat folgende Inklusionen von Untergruppen:

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

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

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

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

2. Seien H und U Untergruppen einer Gruppe G. U operiert auf den Nebenklassen G/H vermöge

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

Ist $\sigma \in U$ im Stabilisator der Nebenklasse $\tau\ H$, so gilt $\sigma\tau H = \tau H$, also $\tau^{-1}\sigma\tau \in H$. Dazu ist $\sigma \in \tau H\tau^{-1}$ äquivalent, der Stabilisator der Nebenkalsse τH ist also die Untergruppe

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

Die Untermenge $U\tau H \subset G$ heißt Doppelnebenklasse von τ nach den Untergruppen U, H.

3. Es gilt

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

   (b) Sei V ein Vertretersystem der Doppelnebenklassen und G endliche Gruppe. Dann gilt

$$|G| = \sum_{v \in V} \frac{|U|\ |H|}{|vHv^{-1} \cap U|} = \sum_{v \in V} \frac{|U|\ |H|}{|H \cap U^v|} \tag{4}$$

Beweis.
Sei m die Länge der Bahn der Nebenklasse τH unter der Operation von U auf G/H. Nach der Bahnengleichung gilt mit dem unter 1. berechneten Stabilisator $\tau H\tau^{-1} \cap U$

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

Daher ist die Zahl der Elemente von G 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 2.11.3
Sei G endliche Gruppe und p eine Primzahl. Wir schreiben die Gruppenordnung in der Form $|G| = p^n a$ mit $(a, p) = 1$, so dass p^n die maximale in $|G|$ aufgehende Potenz der Primzahl p ist.

Eine Untergruppe $H \subset G$ der Ordnung $|H| = p^n$ heißt eine p–Sylowgruppe von G. Mit $Syl_p(G)$ bezeichnen wir die Menge der p–Sylowgruppen von G.

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

Beispiel 2.11.4.
Betrachte die endliche Gruppe

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

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

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

Die Untergruppe

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

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 2.11.6 sein:

Lemma 2.11.5.
Sei H eine 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 Gleichung (4) in Bemerkung 2.11.2.3 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 $p^n = |P|$ gilt, so findet man

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

Für wenigstens einen Vertreter $\tau \in V$ ist daher der Index

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

Andererseits ist $H \cap P^\tau$ als Untergruppe der p-Gruppe P^τ eine p–Gruppe. Beide Aussagen zusammen zeigen, dass $H \cap P^\tau$ eine p–Sylowgruppe von H ist. □

Theorem 2.11.6 (Sylowsätze)**.**

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

2. Je zwei p–Sylowgruppen von G sind konjugiert.

3. Sei n_p die Zahl der p-Sylowgruppen von G, $n_p := |\mathrm{Syl}_p(G)|$. Dann gilt

   (a) n_p teilt $[G : P]$ für $P \in \mathrm{Syl}_p(G)$ und

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

Bemerkungen 2.11.7.

1. Wir verschärfen die Aussagen des dritten Sylow-Satzes zu

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

   (b') $n_p = 1 \bmod p^d$, wobei d folgendermassen definiert ist: gibt es mehrere p-Sylowgruppen, so durchlaufe P' alle von P verschiedenen p–Sylowgruppen von G. Dann ist der Index $[P : P \cap P']$ als Index einer echten Untergruppe einer p-Gruppe eine Potenz von p. Sei p^d die größte p-Potenz, die in all diesen Indizes aufgeht. Gibt es nur eine p-Sylowgruppe, so gilt die Aussage natürlich für jedes d wahr.

   Aus (a') folgt (a) wegen $P \subset N_G(P) \subset G$. 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.

2. Ist $P \in \mathrm{Syl}_p(G)$ normal in G, so ist P die einzige p-Sylowgruppe. Hat G umgekehrt nur eine einzige p–Sylowgruppe, so muss diese sogar eine charakteristische Untergruppe sein und somit normal sein.

Beweis.

- Sei G eine endliche Gruppe. Nach dem Satz 2.7.1 von Cayley können wir G in eine geeignete symmetrische Gruppe $\mathcal{S}_n$ einbetten. Diese wiederum betten wir folgendermaßen in $\mathrm{GL}(n, p)$ ein:
  die Permutation $\sigma \in \mathcal{S}_n$ wird abgebildet auf den Endomorphismus φ_σ des Vektorraums $\mathbb{F}_p^n$, der auf den Vektoren e_i einer Basis von $\mathbb{F}_p^n$ folgendermaßen wirkt:

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

  Wir können daher jede endliche Gruppe als Untergruppe von $\mathrm{GL}(n, p)$ für geeignetes n auffassen. In Beispiel 2.11.4 haben wir gesehen, dass die Gruppe $\mathrm{GL}(n, p)$ die oberen Dreiecksmatrizen als p-Sylowgruppe P besitzt. Nach Lemma 2.11.5 hat dann aber G eine p–Sylowgruppe der Form $P^\tau \cap G$. Damit ist die Existenz von p-Sylowgruppen gezeigt.

- Sei P eine p–Sylowgruppe und $H \subset G$ eine beliebige p–Untergruppe von G. Nach Lemma 2.11.5 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 $H \subset P^\tau$. Dies zeigt die übrigen Aussagen des ersten Sylowsatzes.

- Ist H nicht nur eine p-Gruppe, sondern sogar eine p-Sylowgruppe, also $H \in \mathrm{Syl}_p(G)$, so folgt sogar Gleichheit $H = P^\tau$, da die beiden Gruppen H und P^τ die gleiche Ordnung haben. Hieraus folgt die Aussage des zweiten Sylowsatzes.

- Weil je zwei Sylowgruppen konjugiert sind, ist für jede p–Sylowgruppe P

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

Hieraus folgt (a') und daraus (a).

- Zum Beweis von (b') betrachten wir wieder Doppelnebenklassen von G, diesmal nach P und $N_G(P)$. 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 ist aber auch $P^\tau \neq P$. Hat das Vertretersystem hat also Elemente $\tau \neq e$, so gibt es mehr als eine p-Sylowgruppe. 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 wegen des weiten Sylowsatzes 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 $P^\tau \cap N_G(P) = P^\tau \cap P$ für alle $\tau \in V \setminus \{e\}$.

Jetzt können wir die Bahnengleichung für Doppelnebenklassen aus Bemerkung 2.12.3.3 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 für die Zahl n_p der p-Sylowgruppen

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

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

□

Korollar 2.11.8.

1. 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 2.11.6.1 und dem Struktursatz 2.11.1 für p-Gruppen.

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

2. Jede Gruppe der Ordnung 6 ist entweder zyklisch oder isomorph zur symmetrischen Gruppe S_3.

   Begründung:
   Nach dem ersten Punkt gibt es in G Elemente a, b der Ordnungen 2 bzw. 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 gilt 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 $G \cong S_3$.

3. Jede Gruppe der Ordnung 15 ist zyklisch.

   Begründung:
   Die Zahl n_3 der 3-Sylowgruppen ist ein Teiler von $\frac{15}{3} = 5$. Wir wissen ferner, dass $n_3 = 1 \bmod 3$ gilt. Daher gilt $n_3 = 1$. Es gibt also nur eine 3-Sylowgruppe und genau 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 $n_5 = 1$, genau 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.

2.12 Kompositionsreihen, Normalreihen, auflösbare Gruppen

Definition 2.12.1

1. *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.

2. *Eine Kompositionsreihe ist eine Normalreihe mit der zusätzlichen Eigenschaft, dass der Quotient G_i/G_{i-1} 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

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

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

Man beachte, dass in der Definition einer Normalreihe für $i \leq r-2$ *nicht* gefordert wird, dass G_i sogar normal in ganz G ist, anders als in der Aussage des Struktursatzes 2.11.1 über p-Gruppen.

Satz 2.12.2. (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

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

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 auf M 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

$$M/M \cap N \cong G/N\,. \qquad (*)$$

Durch Vertauschen der Rollen von M und N findet man analog einen Isomorphismus

$$N/M \cap N \cong G/M\,. \qquad (**)$$

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$(*)$ und $(**)$ und der Induktionsvoraussetzung, angewandt auf $M \cap N$. □

Hieraus folgt sofort:

Satz 2.12.3. (Verfeinerungssatz von Schreier)
Je zwei Normalreihen einer Gruppe haben äquivalente Verfeinerungen.

Definition 2.12.4
Eine Gruppe G heißt auflösbar oder metazyklisch, wenn es eine Kompositionsreihe gibt, in der alle Kompositionsfaktoren zyklisch von Primzahlordnung sind.

Satz 2.12.5.
Sei G endliche Gruppe. Dann gilt:

1. Mit G ist auch jede Untergruppe H von G auflösbar.
2. Mit G ist auch jede Faktorgruppe G/H von G auflösbar.
3. Sei N Normalteiler von G. Sind N und G/N auflösbar, so ist auch G auflösbar.
4. Abelsche Gruppen sind auflösbar.

5. p–Gruppen sind auflösbar.

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

6. 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.

7. Feit–Thompson:
   Alle endlichen Gruppen ungerader Ordnung sind auflösbar.

Beweis.

1. Sei $H \subset G$ und G auflösbar. Eine Kette von Untergruppen für G

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

   ergibt durch Schnitt mit H eine Kette von Untergruppen 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

$$\pi_i \; : \; G_{i-1} \to G_{i-1}/G_i$$

   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 des Gruppenhomomorphismus $\tilde{\pi}_i$ ist $G_i \cap H$ ein 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 nicht-trivialen 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.

2. Wir betrachten allgemeiner einen surjektiven Homomorphismus $\pi : G \to \overline{G}$. Die Anwendung von π auf eine Kette 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.

3. Wir können ausgehen von zwei Ketten

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

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.

4. 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 auflösbar. G/N ist abelsch und nach Induktionsannahme auflösbar. Aussage 3. impliziert nun, dass G auflösbar ist.

5. Folgt aus dem stärkeren Struktursatz 2.11.1 über p-Gruppen.

□

Bemerkung 2.12.6.

1. Aus Satz 2.12.5.3 und 4 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. Die auflösbaren Gruppen sind also genau die Gruppen mit abelschen Normalreihen. In der Definition 2.12.4 kann "zyklisch von Primzahlordnung" zu "abelsch" abgeschwächt werden.

2. Die symmetrische Gruppe $\mathcal{S}_n$ ist für $n \geq 5$ nicht auflösbar. Denn $\mathcal{S}_r \supset A_r \supset \{e\}$ ist eine Kompositionsreihe, deren Kompositionsfaktoren die einfachen Gruppen $\mathcal{S}_n/A_n \cong \mathbb{Z}_2$ und A_n sind. Die alternierende Gruppe A_n ist nach Satz 2.10.3 für $n \geq 5$ einfach und nicht abelsch.

   Für $n \leq 4$ findet man Kompositionsreihen

$$\begin{array}{lllll} \mathcal{S}_2 & = & \mathbb{Z}_2 & \supset & \{e\} \\ \mathcal{S}_3 & \supseteq & A_3 & \cong & \mathbb{Z}_3 \supseteq \{e\} \\ \mathcal{S}_4 & \supseteq & A_4 & \supseteq & \mathbb{Z}_2 \times \mathbb{Z}_2 \supseteq \mathbb{Z}_2 \supseteq \{e\}\,. \end{array}$$

   Diese symmetrischen Gruppen sind also auflösbar.

Definition 2.12.7

1. *Sei G eine Gruppe. Für zwei Elemente $a, b \in G$ wird das Gruppenelement*

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

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

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

2. *Wir definieren rekursiv die höheren Kommutatorgruppen:*

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

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

Satz 2.12.8.

1. Die Kommutatorgruppe $K(G)$ ist ein Normalteiler von G.
2. 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.

1. Die Kommutatorgruppe $K(G)$ ist sogar eine charakteristische Untergruppe, 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.

2. 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 2.12.9.
Seien G eine Gruppe, U eine Untergruppe von G und N ein Normalteiler von G. Sei 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.
Für (a) und (c) ist der Beweis klar. Den Beweis für (b) führen wir mit vollständiger Induktion nach n. Wir rechnen:

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

Hierbei wurde im letzten Schritt der folgende Isomorphiesatz angewandt: sei $A \subset G$ eine Untergruppe und $B \subset G$ ein Normalteiler. Dann ist $AB \subset G$ eine Untergruppe. Der surjektive Gruppenhomomorphismus

$$\begin{array}{rcl} A & \to & AB/\ B \\ a & \mapsto & a \bmod B \end{array}$$

hat den Kern $A \cap B$, so dass $AB/B \cong A/A \cap B$ aus dem Isomorphiesatz 2.4.6 folgt. Insbesondere ist $A \cap B \subset A$ eine normale Untergruppe. □

Satz 2.12.10.
Eine Gruppe G ist genau dann auflösbar, wenn es ein $m \in \mathbb{N}$ gibt, so dass $K_m(G) = \{e\}$ gilt.

Beweis.

- Wenn es ein $m \in \mathbb{N}$ gibt, so dass $K_m(G) = \{e\}$ gilt, so bildet die sogenannte abgeleitete Reihe
$$G \supseteq K_1(G) \supseteq \cdots \supseteq K_m(G) = \{e\}$$
wegen Bemerkung 2.12.6.2 eine abelsche Normalreihe. Dann ist G nach Bemerkung 2.12.6.1 auflösbar.

- 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 2.12.9(b). Damit ist aber $K(G) \subset N$. Als Untergruppe einer auflösbaren Gruppe ist N nach Satz 2.12.5.1 auflösbar und hat eine kürzere Normalreihe. Nach Induktionsannahme gibt es $r \in \mathbb{N}$, so dass $K_r(N) = \{e\}$. Wir finden mit 2.12.9 (a) aus $K(G) \subset N$
$$K_{r+1}(G) = K_r(K(G)) \subseteq K_r(N) = \{e\}\,.$$

□

2.13 Freie Gruppen, freie abelsche Gruppen

Wir haben schon im Beweis von Lemma 2.9.7 benutzt, dass man Gruppenhomomorphismen aus einer freien abelschen Gruppe $\mathbb{Z}^r$ heraus in irgend eine abelsche Gruppe konstruieren kann, indem man beliebige Bilder für eine Basis von $\mathbb{Z}^r$ vorschreibt. Diese Vorgehensweise ist natürlich auch von der Konstruktion von linearen Abbildungen bekannt. Bei Gruppen funktioniert dies aber nicht für beliebige Gruppen: zum Beispiel gibt es überhaupt keinen Gruppenhomomorphismus $\mathbb{Z}_2 \to \mathbb{Z}$. (Die Gruppe $\mathbb{Z}_2$ hat in der Tat keine Teilmenge, die man Basis nennen dürfte.)

Wir formalisieren dies wie folgt:

Definition 2.13.1

1. *Sei X eine Teilmenge einer abelschen Gruppe F. Dann heißt F freie abelsche Gruppe mit Basis X, falls $\langle X\rangle = F$ gilt, also X ein Erzeugendensystem ist, und es zu jeder abelschen Gruppe A und jeder Abbildung $f : X \to A$ von Mengen einen Gruppenhomomorphismus $\varphi : F \to A$ gibt, der f fortsetzt, $\varphi|_X = f$.*

2. *Sei X eine Teilmenge einer Gruppe F. Dann heißt F freie Gruppe mit Basis X, falls $\langle X\rangle = F$ gilt und es zu jeder Gruppe G und jeder Abbildung $f : X \to G$ von Mengen einen Gruppenhomomorphismus $\varphi : F \to G$ gibt, der f fortsetzt, $\varphi|_X = f$.*

Auf Grund der Definition ist nicht klar, ob freie Gruppen und freie abelsche Gruppen für beliebige Mengen existieren. Wir können aber zeigen:

Satz 2.13.2.
Sei X eine Menge, F eine freie Gruppe mit Basis X und $K(F)$ die Kommutatoruntergruppe, vgl. Definition 2.12.7. Die kanonischen Surjektion $\pi : F \to F^{ab} := F/K(F)$ auf die abelsche Gruppe F^{ab}, die Abelisierung von F, ist injektiv auf der Teilmenge X. Fassen wir X als Teilmenge von F^{ab} auf, so ist F^{ab} eine freie abelsche Gruppe mit Basis X.

Beweis.
Sei A eine beliebige abelsche Gruppe und $f : X \to A$ eine Abbildung von Mengen. Dann gibt es nach Definition 2.13.1.2 einen eindeutig bestimmten Gruppenhomomorphismus $f : F \to A$. Weil abelsch ist, liegt $K(F) \subset \ker f$. Nach Satz 2.4.5.2 gibt es daher einen eindeutig bestimmten Gruppenhomomorphismus $\tilde{f} : F^{ab} \to A$, für den $\tilde{f} \circ \pi = f$ gilt.

Setze $\tilde{X} := \pi(X) \subset F^{ab}$. Betrachte eine injektive Abbildung $f : X \to A$ in eine geeignete abelsche Gruppe A. Da aus $\pi(x_1) = \pi(x_2)$ auch $f(x_1) = \tilde{f}\pi(x_1) = \tilde{f}\pi(x_2) = f(x_2)$ folgen würde, muss π auf X injektiv sein. Damit ist aber F^{ab} eine freie abelsche Gruppe mit Basis $\tilde{X}$. □

Satz 2.13.3.

1. Seien A_1 und A_2 freie abelsche Gruppen mit Basen X_1 bzw. X_2. Dann sind A_1 und A_2 isomorph genau dann, wenn es eine Bijektion $X_1 \to X_2$ gibt, im Falle endlicher Basen also wenn $|X_1| = |X_2|$ gilt.

2. Seien F_1 und F_2 freie Gruppen mit Basen X_1 bzw. X_2. Dann sind F_1 und F_2 isomorph genau dann, wenn es eine Bijektion $X_1 \to X_2$ gibt, im Falle endlicher Basen also wenn $|X_1| = |X_2|$ gilt.

Beweis.

- Wir betrachten freie Gruppen. Gegeben eine Bijektion $f : X_1 \to X_2$, so finden wir Gruppenhomomorphismen $\varphi : F_1 \to F_2$ und $\psi : F_2 \to F_1$ mit $\varphi|_{X_1} = f$ und $\psi|_{X_2} = f^{-1}$. Für den Gruppenhomomorphismus $\psi \circ \varphi : F_1 \to F_1$ gilt $\psi \circ \varphi(x) = x$ für alle $x \in X_1$. Da $\langle X_1 \rangle = F_1$, folgt $\psi \circ \varphi = \mathrm{id}_{F_1}$ und analog $\varphi \circ \psi = \mathrm{id}_{F_2}$. Also sind die freien Gruppen F_1 und F_2 isomorph. Das Argument für freie abelsche Gruppen ist genau gleich.

- Sind F_1 und F_2 isomorphe freie Gruppen, so sind nach Satz 2.13.2 als Faktorgruppen auch die freien abelschen Gruppen A_1 und A_2 mit Basen X_1 bzw. X_2 isomorph. In einer abelschen Gruppe A_i ist die Menge $2A_i := \{g + g \,|\, g \in A\}$ eine Untergruppe und die Faktorgruppe $A_i/2A_i$ ein Vektorraum über dem Körper mit zwei Elementen, mit Basis X_i. Nun folgt der Satz aus einem bekannten Satz über Vektorräume.

□

Wir weisen die Existenz freier Gruppen nach:

Betrachtung 2.13.4.

- Sei X eine Menge. Für jedes $x \in X$ führen wir die Symbole w_x, w_x^{-1} ein. Diese Elemente heißen Buchstaben. Wir kürzen ab und schreiben x statt w_x. Ein Wort ist eine endliche Folge von Buchstaben, $w = x_1^{\epsilon_1} \dots x_n^{\epsilon_n}$ mit $\epsilon_i \in \{\pm 1\}$ und $x_i \in X$.

- Man verknüpft Wörter durch Nebeneinanderstellen. Das sogenannte leere Wort e hat die Verknüpfungen $ew = we$ für alle Wörter. Dadurch erhalten wir ein assoziatives Monoid mit Eins.

- Eine elementare Transformation von Wörtern besteht nun darin, einen Ausdruck der Form $x^{-1}x$ oder xx^{-1} wegzulassen. Dies definiert eine Äquivalenzrelation auf dem Monoid aller Wörter.

- Die Menge der Äquivalenzklassen mit der vererbten Verknpfung ist eine Gruppe, die von X erzeugt wird.

Satz 2.13.5.
Die Gruppe F ist eine freie Gruppe mit Basis X. Insbesondere existiert für jede Menge X eine freie Gruppe mit Basis X.

Beweis.
Es gilt offensichtlich $\langle X \rangle = F$. Sei $f : X \to G$ eine Abbildung in einer Gruppe. Dann definiert

$$x_1^{\epsilon_1} \dots x_n^{\epsilon_n} \mapsto f(x_1)^{\epsilon_1} \dots f(x_n)^{\epsilon_n}$$

eine Abbildung auf dem Monoid, die mit der Äquivalenzrelation verträglich ist und einen Gruppenhomomorphismus liefert, der f fortsetzt. □

Korollar 2.13.6.
Für jede Menge X existiert eine freie abelsche Gruppe mit Basis X,

Beweis.
Wende Satz 2.13.2 an. Alternativ betrachte die Menge $A(X)$ aller Abbildungen $X \to \mathbb{Z}$, die nur auf endlich vielen Elementen $x \in X$ einen Wert ungleich Null annimmt. Sie wird durch Addition

der Werte zu einer abelschen Gruppe. Identifiziert man $x \in X$ mit der Funktion $\delta_x : X \to \mathbb{Z}$, die überall Wert Null hat, außer $\delta_x(x) = 1$, so kann man X als Teilmenge von $A(X)$ auffassen. Jedes Element in $A(X)$ ist dann eine endliche Linearkombination $\sum_{x\in X} \lambda_x \delta_x$ mit $\lambda_x \in \mathbb{Z}$. Also gilt $\langle X\rangle = A(X)$, d.h. X ist ein Erzeugendensystem.

Eine Abbildung $f : X \to A$ in eine abelsche Gruppe A kann zu der Funktion $A(X) \to A$ durch $\sum_{x\in X} \lambda_x \delta_x \mapsto \sum_{x\in X} \lambda_x f(x)$ fortgesetzt werden. □

Satz 2.13.7.

1. Ist A eine abelsche Gruppe, so existiert eine freie abelsche Gruppe F mit einem surjektiven Gruppenhomomorphismus $\alpha : F \to A$. Jede abelsche Gruppe ist also Faktorgruppe einer freien abelschen Gruppe.

2. Ist G eine Gruppe, so existiert eine freie Gruppe F mit einem surjektiven Gruppenhomomorphismus $\alpha : F \to G$. Jede Gruppe ist also Faktorgruppe einer freien Gruppe.

Beweis.
Betrachte die freie Gruppe F, deren Basis die G zu Grunde liegende Menge ist. Zu der Abbildung von Mengen $\mathrm{id}_G : G \to G$ existiert dann ein Gruppenhomomorphismus $\varphi : F \to G$. Da dieser auf der Teilmenge $G \subset F$ mit der Identität übereinstimmt, ist er surjektiv. Der Beweis für die freie abelsche Gruppe ist identisch. □

Definition 2.13.8

1. *Sei G eine Gruppe und $X \subset G$ eine Teilmenge. Der Durchschnitt aller Normalteiler von G, die die Teilmenge X enthalten, heißt der von X erzeugte Normalteiler oder die normale Hülle von X.*

2. *Ist $G = F/N$, wobei F frei mit einer Basis X ist und $N \subset F$ eine normale Untergruppe von F ist, die normale Hülle einer Menge $R \subset F$. Dann nennt man das Paar (X, R) eine Präsentation der Gruppe G und schreibt $G = \langle X|R\rangle$.*

3. *Eine Präsentation heißt endlich, falls die Mengen X und R endlich sind. Existieren solche Mengen, so heißt die Gruppe endlich präsentierbar.*

Bemerkung 2.13.9.

1. Ist $\pi : F \to F/N = G$ die kanonische Projektion und $\overline{X} := \pi(X)$, so erzeugt die Teilmenge $\overline{X} \subset G$ die Gruppe X, vgl. Definition 2.5.2. Die Elemente von X heißen daher auch Erzeugende von X.

2. Ein Wort $\tilde{r}$ in den Erzeugern von F definiere ein Element $r \in R \subset F$. Dann gilt in $G = \langle X|R\rangle$ die Identität $\pi(r) = 1$. Man nennt daher sowohl das Wort $\tilde{r}$ in den Erzeugern als auch das Element $r \in F$ eine Relation.

Beispiele 2.13.10.

1. Die zyklische Gruppe $\mathbb{Z}_n$ hat die endliche Präsentation $\mathbb{Z}_n = \langle x, x^n = 1\rangle$.

2. Die symmetrische Gruppe $\mathcal{S}_n$ mit $n \geq 2$ wird wegen Satz 2.10.2 von den Transpositionen $w_i := (i, i+1)$ mit $i = 1, \ldots n-1$ erzeugt. Man kann zeigen, dass die folgenden Relationen dann die symmetrische Gruppe $\mathcal{S}_n$ beschreiben (siehe etwa [Jantzen-Schwermer, Kapitel IIA]):

$$\begin{aligned} w_i^2 &= 1 \quad \text{für} \quad 1 \leq i \leq n-1 \\ (w_i w_{i+1})^3 &= 1 \quad \text{für} \quad 1 \leq i \leq n-2 \\ (w_i w_{j+1})^2 &= 1 \quad \text{für} \quad 1 \leq i < j \leq n-2 \end{aligned}$$

3 Ringe

3.1 Lokalisierung von Ringen, maximale Ideale, Primideale

Sei R in diesem Abschnitt ein kommutativer Ring mit Eins.

Definition 3.1.1

1. *Eine Teilmenge $S \subseteq R$ heißt multiplikativ, falls sie die Eins enthält und unter Multiplikation abgeschlossen ist,*

$$1 \in S \quad \textit{und} \quad x, y \in S \Rightarrow xy \in S\,.$$

2. *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 des Rings R nach der multiplikativen Teilmenge S als die Menge der Äquivalenzklassen und schreiben

$$S^{-1}R := (R \times S) \,/\, \sim \ .$$

Die Elemente von $S^{-1}R$ schreiben wir als Brüche, d.h. $\frac{r}{s}$ mit $r \in R$ und $s \in S$ steht für die Äquivalenzklasse von (r, s).

Bemerkung 3.1.2.

- Die üblichen Regeln der Bruchrechnung geben der Lokalisierung $S^{-1}R$ die Struktur eines Rings mit Eins. Er heißt der Quotientenring $S^{-1}(R)$ von R bezüglich S.

- 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 ein Element $s_1 \in S$, so dass $s_1(s\overline{r} - r\overline{s}) = 0$ gilt. Daraus folgt aber auch durch Multiplikation mit $s'r'$

$$s_1(ss'\overline{r}r' - \overline{s}s'rr') = s_1s'r'(s\overline{r} - r\overline{s}) = 0\,,$$

  woraus wir schließen, dass $\frac{\overline{r}r'}{\overline{s}s'} = \frac{rr'}{ss'}$ gilt.

- 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

$$\begin{array}{rccc} \varphi_s: & R & \to & S^{-1}R \\ & r & \mapsto & \dfrac{r}{1} \end{array}$$

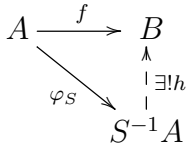
  ist ein (nicht notwendigerweise injektiver!) Ringhomomorphismus. Außerdem sieht man leicht, dass die Elemente in $\varphi_s(S)$ in $S^{-1}R$ invertierbar sind: $(\frac{s}{1})^{-1} = \frac{1}{s}$ für $s \in S$.

Bemerkung 3.1.3.

1. Seien A, B kommutative Ringe mit Eins, $S \subset A$ multiplikative Teilmenge von A und

$$f : A \to B$$

ein Ringhomomorphismus derart, dass alle Elemente des Bilds $f(S)$ in B invertierbar sind. Dann gibt es genau einen Ringhomomorphismus h, so dass das folgende Diagramm kommutiert:



2. $S^{-1}A$ ist bis auf Isomorphie der einzige kommutative Ring, der für gegebenes A und S diese Eigenschaft für alle kommutativen Ringe B besitzt. Dies ist die universelle Eigenschaft der Lokalisierung.
(Der Beweis von 1. und 2. wird als Übungsaufgabe gestellt.)

3. 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 $\frac{r}{1} = \frac{0}{1}$ gilt dann und nur dann, wenn es ein $s \in S$ gibt, so dass $sr = 0$. Da R integer und $s \neq 0$, folgt $r = 0$.

4. Sei R integrer Ring und $S := R\backslash\{0\}$. Die Teilmenge S ist multiplikativ abgeschlossen, da R integer ist. In dieser Situation ist der Ring $S^{-1}R$ sogar ein Körper, der Quotientenkörper von R. Wir bezeichnen ihn mit $\mathrm{Quot}(R) = S^{-1}R$. Der Ring 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 3.1.4.
Sei E/K Körpererweiterung. Ein Element $\alpha \in E$ ist genau dann transzendent über K, 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 die durch den rationalen Funktionenkörper gegebene Erweiterung $K(X)/K$.

Beweis.
"$\Leftarrow$" Weil schon der Unterring $K[X] \subset K(X)$ unendliche Dimension hat, $\dim_K K[X] = \infty$, ist erst recht $\dim_K K(X) = \infty$. Aus der Isomorphie $K(\alpha) \cong K(X)$ folgt

$$\dim_K K(\alpha) = \infty .$$

Nach Satz 1.2.6 ist dann aber α nicht algebraisch über K, also transzendent.

"⇒" Nach Bemerkung 1.3.6.3 (c) liefert für ein transzendentes Element 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, also $K(X) \cong K(\alpha)$.

□

Definition 3.1.5
Sei R ein kommutativer Ring mit Eins.

1. *Ein Ideal $\mathfrak{p}$ in R heißt Primideal, falls $\mathfrak{p} \neq R$ und der Quotientenring $R/\mathfrak{p}$ ein Integritätsring ist. Das ist äquivalent zu der Aussage:*

$$xy \in \mathfrak{p} \;\Rightarrow\; x \in \mathfrak{p} \quad \textit{oder} \quad y \in \mathfrak{p}\,.$$

2. *Ein Ideal $\mathfrak{m}$ von R heißt maximales Ideal, wenn $\mathfrak{m} \neq R$ und der Quotientenring $R/\mathfrak{m}$ ein Körper ist.*

Bemerkungen 3.1.6.

1. Zum Beispiel ist $3\mathbb{Z}$ ein Primideal des Rings $\mathbb{Z}$, denn der Quotientenring $\mathbb{Z}/3\mathbb{Z}$ ist integer. Aber das Ideal $4\mathbb{Z} \subset \mathbb{Z}$ ist kein Primideal: 4 liegt in $4\mathbb{Z}$, und $4 = 2 \cdot 2$, aber $2 \notin 4\mathbb{Z}$.

2. Jedes maximale Ideal ist Primideal, denn Körper sind nullteilerfrei.

3. Die Umkehrung gilt nicht. Ist R integer, aber kein Körper, so ist das Ideal (0) prim, aber nicht maximal.

4. Die Definition eines maximalen Ideals ist äquivalent zu der folgenden Aussage über $\mathfrak{m}$, die den Namen "'maximales Ideal" rechtfertigt:
   Ist $\mathfrak{a} \subset R$ ein Ideal mit $\mathfrak{m} \subset \mathfrak{a}$, so gilt $\mathfrak{a} = \mathfrak{m}$ oder $\mathfrak{a} = R$. Diese Äquivalenz sieht man folgendermaßen:

   "⇒" Sei $\mathfrak{m} \subseteq \mathfrak{a} \subset R$ und $\mathfrak{m}$ maximal im Sinne von Definition 3.1.5.2. Betrachte die Surjektion

$$\begin{array}{rccc} \varphi: & R/\mathfrak{m} & \to & R/\mathfrak{a} \\ & r \bmod \mathfrak{m} & \mapsto & r \bmod \mathfrak{a} \end{array}$$

   Dies ist wegen $\mathfrak{a} \subset \mathfrak{m}$ 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 modulo $\mathfrak{m}$ geben.

   "⇐" Sei $\mathfrak{m}$ ein Ideal mit der oben genannten Maximalitätseigenschaft. 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 die Restklasse $\overline{x}$ ein Inverses. Somit ist der Restklassenring $R/\mathfrak{m}$ ein Körper.

Bemerkung 3.1.7.
Sei S eine Menge. Wir erinnern an die folgenden Begriffe und Resultate der Mengenlehre:

1. Eine partielle Ordnung auf S ist eine Relation $x \leq y$ mit den folgenden Eigenschaften:

$$x \leq x \qquad \text{Reflexivität}$$
$$x \leq y \ \wedge \ y \leq z \ \Rightarrow \ x \leq z \qquad \text{Transitivität}$$
$$x \leq y \ \wedge \ y \leq x \ \Rightarrow \ x = y \qquad \text{Antisymmetrie}\,.$$

2. Eine Totalordnung auf S ist eine partielle Ordnung, für die je zwei Elemente vergleichbar sind: für je zwei $x, y \in S$ gilt entweder $x \leq y$ oder $y \leq x$.

3. Sei S partiell geordnet, $T \subset S$ eine Teilmenge. Ein Element $b \in S$ heißt obere Schranke von T, falls $x \leq b$ für alle $\in T$ gilt.

4. Sei S partiell geordnet. Ein Element $m \in S$ heißt maximales Element, falls für alle $x \in S$ azs $m \leq x$ folgt $m = x$. Das maximale Element muss nicht eindeutig sein.

5. Eine partiell geordnete Menge S heißt induktiv geordnet, falls jede nicht–leere, total geordnete Teilmenge von S eine obere Schranke besitzt.

6. Zornsches Lemma

   Sei S eine nicht–leere, induktiv geordnete Menge. Dann gibt es zu jedem $a \in S$ ein maximales Element m mit $a \leq m$. Insbesondere besitzt S maximale Elemente.

Satz 3.1.8.
Sei R ein kommutativer Ring mit Eins, und $\mathfrak{a}$ ein von R verschiedenes Ideal. Dann ist $\mathfrak{a}$ in einem maximalen Ideal enthalten. Insbesondere hat jeder Ring maximale Ideale.

Beweis.
Die Menge $\mathfrak{M} := \{\mathfrak{b} \subset R | \mathfrak{b} \text{ Ideal}, \mathfrak{a} \subseteq \mathfrak{b}, \mathfrak{b} \neq R\}$ enthält $\mathfrak{a}$, ist also nicht leer. Außerdem ist $\mathfrak{M}$ induktiv geordnet durch Inklusion: sei $\{\mathfrak{b}_i\}_{i \in I}$ eine total geordnete Teilmenge von $\mathfrak{M}$. Dann ist die Vereinigung $\mathfrak{b} := \bigcup_{i \in I} \mathfrak{b}_i$ ein Ideal in R, das $\mathfrak{a}$ enthält. Keines der Ideale $\mathfrak{b}_i$ enthält die Eins $1 \in R$, denn ein Ideal, das 1 enthält, ist gleich R. Also enthält auch die Vereinigung $\mathfrak{b}$ nicht die Eins.

Das Ideal $\mathfrak{b}$ 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 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 $\mathfrak{m}$ maximal bezüglich der Inklusion, also $\mathfrak{d} = \mathfrak{m}$. □

Definition 3.1.9
Ein kommutativer Ring mit 1 *heißt lokaler Ring, falls R genau ein maximales Ideal besitzt.*

Zum Beispiel sind Körper lokale Ringe. Der Ring der ganzen Zahlen $\mathbb{Z}$ ist nicht lokal, denn jedes Primideal (p) mit $p \neq 0$ ist maximal.

Bemerkung 3.1.10.
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, vgl. Definition 1.3.7

Beweis.

"⇒" Sei $x \in R\backslash\mathfrak{m}$. Wäre x keine Einheit, so wäre das Hauptideal Rx ein echtes Ideal in R. Nach Satz 3.1.8 ist dieses Ideal in in einem maximalen Ideal enthalten. 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 $1 \in \mathfrak{m}$ gelten würde, womit $\mathfrak{m} = R$ gelten würde. Damit haben wir auch die umgekehrte Inklusion gezeigt: $R^\times \subset R\backslash\mathfrak{m}$.

"⇐" 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, also erst recht in $R/$ mod $\mathfrak{m}$. Damit ist klar, dass $\mathfrak{m}$ ein maximales Ideal ist.

Wir müssen zeigen, dass $\mathfrak{m}$ 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 $\mathfrak{m}'$ überdies maximal sein soll, müssen die beiden Ideale übereinstimmen.

□

Beispiele 3.1.11.

- 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 3.1.5.1 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 Elemente des Komplements $R\backslash\mathfrak{m} = \left\{ \frac{r}{s} \middle| s \notin \mathfrak{p}, r \notin \mathfrak{p} \right\}$ können invertiert werden, sind also Einheiten.

- 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 3.1.12.

Sei K ein Körper, betrachte den Ringhomomorphismus

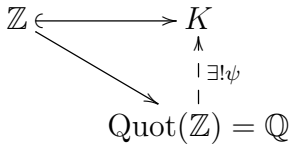
$$\begin{array}{rccc} \varphi: & \mathbb{Z} & \to & K \\ & z & \mapsto & z \cdot 1_K \end{array}$$

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 additive 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 das Hauptideal $p\mathbb{Z}$ 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. Mit Hilfe der universellen Eigenschaft aus Bemerkung 3.1.3.1 bekommen wir eine eindeutig bestimme Abbildung ψ, so dass das folgende Diagram kommutiert:



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 3.1.13

1. *Ein Körper K heißt Primkörper, wenn er keinen echten Teilkörper enthält.*
2. *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 habe die Charakteristik 0 oder p, und schreibt $\mathrm{char}\ K = 0$ *oder* $\mathrm{char}\ K = p$.

Die möglichen Primkörper sind also $\cong \mathbb{Q}$ oder $\mathbb{F}_p$ für eine Primzahl p. Zum Beispiel ist $\mathrm{char}\,\mathbb{F}_p(X) = p$.

3.2 Teilbarkeitslehre

Auch in diesem Abschnitt ist R ein kommutativer Ring mit Eins.

Definition 3.2.1

1. *Seien $a, b \in R$. Wir sagen a teilt b, in Zeichen $a|b$, wenn es ein $c \in R$ gibt, so dass $b = ac$ gilt.*
2. *Zwei Elemente a und $b \in R$ heißen assoziiert, in Zeichen $a \overset{\wedge}{=} b$, falls $a|b$ und $b|a$ gilt.*

Bemerkungen 3.2.2.

1. Teilbarkeit ist reflexiv und transitiv, aber wegen der Existenz verschiedener 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 $c \neq 0 \Rightarrow a|b$.

2. Ist R integer, so gilt: $a \overset{\wedge}{=} b$ genau dann, wenn es eine Einheit $\epsilon \in R^\times$ gibt mit $b = \epsilon a$ (Übung).

3. 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: $R = \mathbb{Z}[i]^\times = \{\pm 1, \pm i\}$, $R = \mathbb{Z}[\sqrt{2}]^\times = \{\pm(1+\sqrt{2})^j, j \in \mathbb{Z}\}$.

4. Wie im Ring der ganzen Zahlen führt man das ggT und kgV ein. Das ggT ist ein gemeinsamer Teiler (bzw. das kgV ein gemeinsames Vielfaches), d.h.

$$\text{ggT}(a_1, \ldots a_n)|a_i \quad \text{bzw.} \quad a_i|\text{kgV}(a_1 \ldots a_2) \quad \text{für alle } i = 1, \ldots, n$$

mit der folgenden zusätzlichen Eigenschaft: gilt für ein weitere Element $t \in R$

$$t|a_i \quad \text{bzw.} \quad a_i|t \quad \text{für alle } i \ ,$$

so folgt

$$t|\text{ggT}(a_1 \ldots a_n) \quad \text{bzw.} \quad \text{kgV}(a_1 \ldots a_n)|t.$$

ggT und kgV sind bis auf Assoziiertheit eindeutig, sofern sie existieren. (Wir werden später eine Klasse von Ringen kennen lernen, die faktoriellen Ringe, in denen ggT und kgV immer existieren.)

5. Teilbarkeit kann auch idealtheoretisch als Aussage über die entsprechenden Hauptideale formuliert werden:

$$\begin{array}{lcccc} a|b & \Longleftrightarrow & (b) & \subset & (a) \\ a \overset{\wedge}{=} b & \Longleftrightarrow & (b) & = & (a) \end{array}$$

6. Insbesondere gilt: $v \in R$ ist gemeinsames Vielfaches von a und b dann und nur dann, wenn das von v erzeugte Hauptideal im Schnitt der Hauptideale von a und b liegt: $(v) \subseteq (a) \cap (b)$. Gibt es ein kgV, so gilt für das vom kgV erzeugte Hauptideal $(\text{kgV}(a, b)) = (a) \cap (b)$.

7. Sind $\mathfrak{a}_1$ und $\mathfrak{a}_2$ Ideale in R, so 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:

$$(a_1) + (a_2) + \cdots + (a_n) = (a_1, \ldots, a_n)\,.$$

$d \in R$ ist gemeinsamer Teiler von a und b, dann und nur dann wenn $(a) \subset (d)$ und $(b) \subset (d)$ gilt, also genau dann, wenn $(a) + (b) \subseteq (d)$ gilt.

Definition 3.2.3

1. *Ein Integritätsring heißt Hauptidealring, wenn jedes Ideal ein Hauptideal ist. Ein Hauptidealring heißt auch prinzipal.*

2. *Ein Integritätsring heißt euklidischer Ring, wenn es eine Abbildung*

$$\nu : \quad R \setminus \{0\} \to \mathbb{N}$$

gibt, so dass es zu je zwei $a, b \in R$ mit $a \neq 0$ Elemente $q, r \in R$ gibt, so dass $b = qa + r$ gilt und $r = 0$ oder $\nu(r) < \nu(a)$ gilt. Die Funktion ν heißt Gradabbildung oder euklidische Normfunktion. Es gibt also in euklidischen Ringen eine Division mit Rest.

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.

1. 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

$$d = x_1 a_1 + \cdots + x_n a_n \quad \text{mit} \quad x_i \in R\,.$$

   Begründung.
   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 $(a_i) \subset (d)$ gilt, also d jedes a_i teilt. Somit ist d gemeinsamer Teiler ist. Da d im Ideal auf der rechten Seite liegt, 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 Elemente a_i, also $(a_i) \subseteq (t)$. Damit gilt aber auch $(d) = (a_1) + \ldots + (a_n) \subseteq (t)$, was impliziert, dass t auch d teilt. Also ist d wirklich das $\mathrm{ggT}(a_1, \ldots, a_n)$.

2. Jeder euklidischer Ring ist ein Hauptidealring.

   Begründung:
   Sei $\mathfrak{a} \subset R$ Ideal, $\mathfrak{a} \neq (0)$. Sei $a \in \mathfrak{a}$ mit $\nu(a)$ minimal und $a \neq 0$. 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 $b = qa + r$ schreiben mit $q, r \in R$. Es folgt $r = b - qa \in \mathfrak{a}$. Nun gilt entweder $r = 0$, dann ist aber $b \in (a)$. Oder es ist $\nu(r) < \nu(a)$; dies kann aber wegen der Minimalität von a und weil $r \in \mathfrak{a}$ gilt, nicht sein.

3. Beispiele für Euklidische Ringe sind der Ring der ganzen Zahlen $R = \mathbb{Z}$ mit Normfunktion $\nu(a) = |a|$ und der Polynomring $K[X]$ über einem K Körper, wobei die Normfunktion für nicht-verschwindende Polynome der Polynomgrad (plus Eins) ist. Diese Ringe sind also insbesondere Hauptidealringe.

4. In Euklidischen Ringen kann der euklidische Algorithmus aus Betrachtung 2.2.11 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 $b \in R^\times$ gilt.

Beispiele für irreduzible Elemente:

- Im Ring $\mathbb{Z}$ der ganzen Zahlen sind die Zahlen $\pm p, p$ mit p prim irreduzibel.
- Die irreduziblen Elemente im Ring $K[X]$ der Polynome über einem Körper K wurden schon in Beispiel 1.3.12 eingeführt.

Definition 3.2.6

1. *Ein Element $a \in R$ besitzt eine Zerlegung in irreduzible Elemente, wenn a eine Darstellung*

$$a = \epsilon\pi_1 \dots \pi_r \quad \text{mit } \epsilon \in R^\times \text{ und } \pi_i \in R \quad \text{irreduzibel}$$

hat. $r = 0$ ist hierbei zugelassen.

2. *Ein Integritätsring R heißt faktoriell (oder ZPE Ring[2]), 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*

$$\pi_i \overset{\wedge}{=} \pi'_i \quad \text{für} \quad i = 1 \dots r\,.$$

3. *Ein Element $\pi \in R$ heißt Primelement, falls $\pi \neq 0$ keine Einheit ist und $\pi | ab$ impliziert, dass $\pi | a$ oder $\pi | b$.*

Man vergleiche die Definition eines Primelements mit der Aussage von Lemma 1.3.13. Man zeige, dass ein Element $\pi \in R$ genau dann Primelement ist, wenn das Hauptideal (π) ein Primideal ist.

Die Klasse der faktoriellen Ringe wird uns in der Folge interessieren; sie enthält so wichtige Ringe wie den Polynomring $\mathbb{Z}[X]$. Um sie besser zu beschreiben, müssen wir die Eigenschaft "faktoriell" durch äquivalente Eigenschaften ausdrücken können.

Satz 3.2.7.
Sei R integer. Dann sind äquivalent:

1. R ist faktoriell
2. Jedes $a \in R \setminus \{0\}$ besitzt eine Zerlegung in irreduzible Faktoren und jedes irreduzible Element ist Primelement.

Beweis.

1.$\Rightarrow$ 2. Die Existenz einer Zerlegung ist klar, da in Definition 3.3.6 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 a und b eindeutig in irreduzible Faktoren zerlegen:

$$a = \epsilon\pi_1 \dots \pi_r \qquad \text{und} \qquad b = \tilde{\epsilon}\tilde{\pi}_1 \dots \tilde{\pi}_s\ .$$

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 auch ein Primelement.

2.$\Rightarrow$ 1. 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 ist, folgt $\pi_1 | \pi'_j$ für ein j. Durch Umnumerierung dürfen wir annehmen, dass $j = 1$ gilt. Da π_1 auch irreduzibel ist, folgt $\pi_1 \overset{\wedge}{=} \tilde{\pi}_1$. Per Induktion nach r folgt nun die Aussage.

[2]ZPE steht für Zerlegung in Primelemente.

□

Bemerkung 3.2.8.

1. 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 $b \in R^\times$.

2. Die Umkehrung ist in allgemeinen Integritätsringen 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.

3. Wir werden in Bemerkung 3.2.11 sehen, dass Polynomringe über Körpern faktoriell sind. Für Polynomringe über Körpern wurde schon in Lemma 1.3.13 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 $(a_1) \subseteq (a_2) \subseteq \ldots$ 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 $\mathfrak{M} = \{(a) | a \in R,\ a \neq 0,\ a$ besitzt keine Zerlegung in irreduzible Elemente$\}$. Unser Ziel ist zu zeigen, dass $\mathfrak{M} = \emptyset$.

Angenommen, es wäre $\mathfrak{M} \neq \emptyset$. Wegen 1. 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 2. Betrachte $a_1, a_2 \in R$ mit $(0) \neq (a_1) \subset (a_2) \neq R$ und Zerlegungen

$$\begin{aligned} a_1 &= \epsilon\pi_1 \ldots \pi_r \\ a_2 &= \tilde{\epsilon}\tilde{\pi}_1 \ldots \tilde{\pi}_s \end{aligned}$$

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 jede Kette von Hauptidealen 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, ist I im Hauptidealring von der Form $I = (a)$ mit einem $a \in R$. 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 $\mathrm{ggT}(\pi, a) = 1$. (Das ggT existiert für den Hauptidealring R nach Bemerkung 3.2.4.1.) 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.

1. Die Umkehrung ist falsch: aus dem Satz von Gauß 3.3.8 folgt, dass der der Ring $\mathbb{Z}[X]$ faktoriell ist. Das Ideal $(n) + (X)$ mit $n \in \mathbb{Z}$ ist kein Hauptideal. Denn wäre $(f) = (n) + (X)$, so wäre f nach Bemerkung 3.2.4.1 ein gemeinsamer Teiler von n und X. Ein solcher Teiler müsste aber als Teiler von n ein konstantes Polynom sein. Einen solchen Teiler hat das Monom X aber nicht.

2. Wir haben die folgenden Inklusionen für Ringe:
   euklidisch $\overset{3.2.4.2}{\Longrightarrow}$ prinzipal $\overset{3.2.10}{\Longrightarrow}$ faktoriell
   Insbesondere sind Polynomringe über Körpern und der Ring $\mathbb{Z}$ der ganzen Zahlen als euklidische Ringe prinzipal und 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 $\pi \not| a'$ durch $\omega_\pi(a) = e$. Wir setzen sie auf den Quotientenkörper $K = \mathrm{Quot}(R)$ fort durch

$$\begin{array}{rccl} \omega_\pi : & K & \to & \mathbb{Z} \cup \{\infty\} \\ & \frac{a}{b} & \mapsto & \omega_\pi(a) - \omega_\pi(b)\,. \end{array}$$

(Man überlege sich, dass dies auf dem Quotientenkörper wohldefiniert ist.) 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, $K = \mathrm{Quot}\ (R)$ und $\mathfrak{P}$ ein Repräsentantensystem für die Klassen assoziierter Primelemente. Dann gilt:

1. Jedes $a \in K, a \neq 0$ besitzt eine eindeutige Darstellung

$$a = \epsilon \prod_{\pi \in \mathfrak{P}} \pi^{\omega_\pi(a)} \text{ mit } \epsilon \in R^\times$$

   wobei $\omega_\pi(a) = 0$ für fast alle $\pi \in \mathfrak{P}$.

2. Sei $x \in K$. Dann $x \in R \iff \omega_\pi(x) \geq 0$ für alle $\pi \in \mathfrak{P}$.

3. $a, b \in R$. Dann $a|b \iff \omega_\pi(a) \leq \omega_\pi(b)$ für alle $\pi \in \mathfrak{P}$.

4. Zu $a_1 \ldots a_n \in R$ existiert

$$\begin{array}{rcl} \mathrm{ggT}(a_1, \ldots, a_n) & = & \prod\limits_{\pi \in \mathfrak{P}} \pi^{\min_i(\omega_\pi(a_i))} \\ \mathrm{kgV}(a_1, \ldots, a_n) & = & \prod\limits_{\pi \in \mathfrak{P}} \pi^{\max_i(\omega_\pi(a_i))} \end{array} .$$

   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.

1. *Zwei Ideale $\mathfrak{a}$ und $\mathfrak{b}$ heißen teilerfremd, falls $\mathfrak{a} + \mathfrak{b} = R$ gilt.*

2. *Das Ideal*

$$\mathfrak{ab} := \left\{ \sum_{endl} a_i b_i | a_i \in \mathfrak{a} \quad und \quad b_i \in \mathfrak{b} \right\}$$

   heißt das Produkt der Ideale $\mathfrak{a}$ und $\mathfrak{b}$.

Es gilt offensichtlich stets $\mathfrak{ab} \subset \mathfrak{a} \cap \mathfrak{b}$.

Lemma 3.2.15.

1. Seien $\mathfrak{a}$ und $\mathfrak{b}$ teilerfremde Ideale von R. Dann ist

$$\mathfrak{ab} = \mathfrak{a} \cap \mathfrak{b}\,.$$

2. 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.

1. 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 für teilerfremde Ideale auch die umgekehrte Inklusion $\mathfrak{a} \cap \mathfrak{b} \subset \mathfrak{ab}$ gezeigt.

2. 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

$$1 = \prod_{i=1}^{n}(b_i + a_i) = \underbrace{b_1 b_2 \ldots b_n + \ldots}_{\in \mathfrak{b}} + a_1 a_2 \ldots a_n \in \mathfrak{b} + \mathfrak{a}_1\mathfrak{a}_2 \ldots \mathfrak{a}_n$$

   Damit ist aber $R = \mathfrak{b} + \mathfrak{a}_1 \ldots \mathfrak{a}_n$, also sind auch die beiden Ideale $\mathfrak{a}_1\mathfrak{a}_2 \ldots \mathfrak{a}_n$ und $\mathfrak{b}$ teilerfremd.

□

Satz 3.2.16. (Chinesischer Restsatz, abstrakte Form)
Seien $\mathfrak{a}_1 \ldots \mathfrak{a}_n$ paarweise teilerfremde Ideale von R. Dann ist der natürliche Homomorphismus

$$\begin{array}{rcl} R/\mathfrak{a}_1 \ldots \mathfrak{a}_n & \to & R/\mathfrak{a}_1 \times \cdots \times R/\mathfrak{a}_n \\ x \bmod \mathfrak{a}_1, \ldots \mathfrak{a}_n & \mapsto & (x \bmod \mathfrak{a}_1, \ldots, x \bmod \mathfrak{a}_n) \end{array}$$

ein Isomorphismus.

Dies heißt insbesondere: gegeben $x_1, \ldots, x_n \in R$, gibt es eine Lösung $x \in R$ der Gleichungen $x = x_i \mod \mathfrak{a}_i$. Die Lösung x ist modulo dem Ideal $\mathfrak{a}_1 \ldots \mathfrak{a}_n$ 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

$$\begin{array}{rcll} R & \to & R/\mathfrak{a}_1 \times R/\mathfrak{a}_2 & (*) \\ x & \mapsto & (x \bmod \mathfrak{a}_1, x \bmod \mathfrak{a}_2) & \end{array}$$

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 $x = x_2a_1 + x_1a_2$ wegen

$$\begin{array}{rcccl} x & = & x_2a_1 + x_1(1-a_1) & = & x_1 \bmod \mathfrak{a}_1 \\ x & = & x_2(1-a_2) + x_1a_2 & = & x_2 \bmod \mathfrak{a}_2 \end{array}$$

eine Lösung der gesuchten Kongruenzen. Der Kern der Surjektion $(*)$ ist $\mathfrak{a}_1 \cap \mathfrak{a}_2 = \mathfrak{a}_1\mathfrak{a}_2$ nach Lemma 3.2.15.1. □

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 3.3.8, der aussagt, dass der Polynomring $R[X]$ dann und nur dann faktoriell ist, 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 3.2.4.2 prinzipal.

Sei umgekehrt $R[X]$ ein Hauptidealring und I der Kern des Einsetzungshomomorphismus:

$$\begin{array}{rccc} \varphi: & R[X] & \to & R \\ & X & \to & 0 \end{array}$$

Es ist offenbar $I = (X)$ und $R[X]/(X) \cong R$ ist integer. Also ist das Element $X \in R[X]$ ein Primelement. Nach Bemerkung 3.2.8.1 ist im integren Ring $R[X]$ das Primelement X auch irreduzibel. Die Behauptung folgt daher aus dem folgenden Lemma. □

Lemma 3.3.2.
Sei A ein Hauptidealring und $\pi \in A$ irreduzibel. Dann ist A/π ein Körper.

Beweis.
Nach Satz 3.1.8 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. □
Für den Beweis ist wesentlich, dass A ein Hauptidealring ist.

Lemma 3.3.3.
Sei $a \in R$, wobei R ein Ring mit Eins ist.

1. 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
$$R[X]/a \xrightarrow{\sim} (R/a)[X]$$
2. $a \in R$ ist prim in R dann und nur dann, wenn a ist prim in $R[X]$ ist.

Beweis.
1. 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 $R[X]$.
2. Das Element $a \in R$ ist im Ring R prim, wenn R/a integer ist. Genau dann ist aber auch der Ring $(R/a)[X]$ integer, der nach 1. isomorph zu $R[X]/a$ ist. Also ist genau in diesem Fall $R[X]/a$ integer, was aber wiederum heisst, dass a prim im Polynomring $R[X]$ ist.

□

Satz 3.3.4.
Ist der Polynomring $R[X]$ faktoriell, so auch der Ring R.

Beweis.
Sei $a \in R, a \neq 0$. Als Element im faktoriellen Ring $R[X]$ hat a eine eindeutige Zerlegung

$$a = \epsilon p_1(X) \dots p_r(X) \qquad (*)$$

mit $\epsilon \in R[X]^\times = R^\times$ und $p_i \in R[X]$ irreduziblen Polynomen, die im faktoriellen Ring $R[X]$ nach Satz 3.2.7 auch prim sind. Aus Gradgründen sind die in $(*)$ auftretenden Polynome alle vom Grade Null, also $p_i(X) = \pi_i \in R$.

Nach Lemma 3.3.3.2 sind die Elemente 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 der Aussage von Satz 3.3.4 zu zeigen, brauchen wir einige Vorbereitungen. Sei R im Folgenden faktoriell und $K := \mathrm{Quot}(R)$ der Quotientnkörper. Für ein Primelement $\pi \in R$, $\pi \neq 0$, bezeichne wie in Definition 3.2.12

$$\omega_\pi : K \to \mathbb{Z} \cup \{\infty\}$$

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

$$\omega_\pi(cf) = \omega_\pi(c) + \omega_\pi(f) \qquad \text{für alle } c \in K \text{ und alle } f \in K[X]\,. \qquad (*)$$

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 $(*)$ reicht es daher aus, die Behauptung für Polynome $f, g \in R[X]$ 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 3.3.3.2 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

1. *Ein Polynom* $f(X) = \sum_{i=0}^{n} a_i X^i \in R[X]$ *vom Grad* $\operatorname{grad}(f) \geq 1$ *heißt* <u>primitiv</u>, *falls* $\operatorname{ggT}(a_0, \ldots, a_n) = 1$.

2. *Sei* R *faktoriell,* $f \in R[X]$, $\operatorname{grad} f \geq 1$. *Der größte gemeinsame Teiler* a *der Koeffizienten von* f *ist bis auf Assoziiertheit eindeutig. Das von ihm erzeugte Hauptideal* (a) *von* R *ist eindeutig und heißt* <u>Inhalt</u> *des Polynoms* f.

Bemerkungen 3.3.7.

1. Es gibt eine Darstellung von $f = ag$ mit $a \in R \setminus \{0\}$ einem Erzeuger des Inhalts und $g \in R[X]$ einem primitiven Polynom.

2. Aus Lemma 3.3.5 folgt

$$\text{Inhalt } (gf) \;=\; \text{Inhalt } (g) \;\cdot \text{Inhalt } (f)\,.$$

Lemma 3.3.8.
Sei R faktoriell, $K := \text{Quot } (R)$ und $g \in R[X]$ mit $\operatorname{grad} g \geq 1$. Ist g primitiv, so gilt

$$g \text{ irreduzibel in } K[X] \;\Rightarrow\; g \text{ irreduzibel in } R[X]\,.$$

Beweis.
Sei $g \in R[X]$ irreduzibel in $K[X]$. Wir nehmen an, dass wir g als Produkt im Polynomring $R[X]$ schreiben können, also $g = ab$ mit $a, b \in R[X]$.

Da nach Annahme g irreduzibel in $K[X]$ ist, ist einer der Faktoren eine Einheit, 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. □

Zum Beispiel ist das Polynom $g(X) = 2X + 4$ irreduzibel in $\mathbb{Q}[X]$, aber nicht in $\mathbb{Z}[X]$, da $g = 2(X+2)$ und 2 zwar eine Einheit in $\mathbb{Q}$, aber nicht in $\mathbb{Z}$ ist. Daher kann auf die Voraussetzung, dass g primitiv ist, nicht verzichtet werden.

Satz 3.3.9. (Gauß)
Ist ein Ring R faktoriell, so auch der Polynomring $R[X]$ über diesem Ring. Genauer gilt:
Sei R faktoriell mit Quotientenkörper $\mathrm{Quot}(R) = K$. Sei $\mathfrak{P}_1$ ein Repräsentantensystem für die Klassen assoziierter Primelemente des Rings R und $\mathfrak{P}_2$ ein Repräsentantensystem für die Klassen assoziierter Primelemente des Polynomrings $K[X]$.

Das Repräsentantensystem $\mathfrak{P}_2$ kann so gewählt werden, dass es aus primitiven Polynomen von $R[X]$ besteht. Dann ist $R[X]$ faktoriell und $\mathfrak{P}_1 \cup \mathfrak{P}_2$ ist ein Repräsentantensystem der Klassen assoziierter Primelemente des Polynomrings $R[X]$.

Beweis.
Die Idee des Beweises ist, erst mit dem Polynomring über dem Quotientenkörper zu arbeiten und dann Bewertungen einzusetzen.

- Der Polynomring $K[X]$ ist nach Satz 3.3.1 ein Hauptidealring und daher nach Satz 3.2.10 faktoriell. Jedes Primelement in $K[X]$ ist assoziiert zu einem primitiven Polynom in $R[X]$, denn man kann Hauptnenner und gemeinsame Faktoren herausziehen. 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 $\omega_\pi(a) \geq 0$ für alle $\pi \in \mathfrak{P}_1$ ist, ist nach Satz 3.2.13.2 $a \in R$. 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

  $$g = \epsilon \prod_{\pi \in \mathfrak{P}_1} \pi^{e_\pi} \prod_{f \in \mathfrak{P}_2} f^{e_f} \qquad (*)$$

  in $R[X]$, da nach 3.3.3.2 π auch in $R[X]$ prim ist und nach Lemma 3.3.8 f auch in $R[X]$ irreduzibel ist. Diese Zerlegung ist überdies eindeutig.

- Nun gilt allgemein: ist ein Ring $\tilde{R}$ integer und $\mathcal{P} \subset \tilde{R} \setminus \{0\}$, so dass jedes $a \in \tilde{R} \setminus \{0\}$ *eindeutig* in der Form $(*)$ geschrieben werden kann, dann ist $\tilde{R}$ faktoriell und $\mathcal{P}$ ein Repräsentantensystem der Primelemente.

  Denn nach Annahme ist jedes $\pi \in \mathcal{P}$ irreduzibel. Ein beliebiges irreduzibles Element $\pi \in \tilde{R}$ können wir nach Annahme eindeutig in der Form $\pi = \epsilon\tilde{\pi}$ mit $\tilde{\pi} \in \mathcal{P}$ schreiben. Also ist π zu genau einem Element aus $\mathcal{P}$ assoziiert. Damit hat jedes Element eine eindeutige Zerlegung in irreduzible Elemente, also ist $\tilde{R}$ faktoriell.

□

Korollar 3.3.10.
Sei R faktoriell, $K := \text{Quot}(R)$ und $g \in R[X]$ mit grad $g \geq 1$. Dann gilt:

$$g \text{ irreduzibel in } R[X] \;\Rightarrow\; g \text{ irreduzibel in } K[X]$$

Beweis.
Sei g irreduzibel in $R[X]$. Nach dem Satz 3.3.9 von Gauß ist der Ring $R[X]$ faktoriell. Wir können schreiben $g = \epsilon f$ mit einer Einheit $\epsilon \in R^\times$ und $f \in \mathfrak{P}_2$. Damit ist aber g auch irreduzibel in $K[X]$. □

Satz 3.3.11. (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 deren Koeffizienten schon in R: es gilt $g, h \in R[X]$.

Beweis.
Der Beweis benutzt Bewertungen im faktoriellen Ring $R[X]$. Sei $\pi \in R$ ein beliebiges Primelement. 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 3.3.12.
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 3.3.11 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 $f(X) = X^n - 2 \in \mathbb{Z}[X]$ 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 3.3.13.
Sei R integer, $I \subseteq R$ Primideal. Die kanonische Surjektion

$$\begin{array}{ccc} R & \twoheadrightarrow & R/I =: \overline{R} \\ a & \mapsto & \overline{a} = \mathrm{mod} I \end{array}$$

setzen wir fort zu einer Surjektion des Polynomrings

$$R[X] \twoheadrightarrow \overline{R}[X]\,.$$

Sei $f(X) = a_n X^n + \cdots + a_0 \in R[X]$ primitiv mit $\overline{a}_n \neq 0$. Ist $\overline{f}$ irreduzibel in $\bar{R}[X]$, so ist auch f irreduzibel in $R[X]$.

Achtung, die Umkehrung gilt nicht! Aus Korollar 3.3.12 folgt, dass $f(X) = X^2 - p \in \mathbb{Z}[X]$ mit p prim 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 den Koeffizienten von f ziehen. Also haben die beiden Polynome 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 der Quotientenring $\overline{R}$ integer, also sind alle Einheiten Polynome vom Grad Null, $\overline{R}[X]^\times = \overline{R}^\times$. Also sind $\overline{g}$ und $\overline{h}$ keine Einheiten in $\overline{R}[X]$. Man hat somit einen Widerspruch zur vorausgesetzten Irreduzibilität von $\overline{f}$ in $\bar{R}[X]$. □

Satz 3.3.14. (Irreduzibilitätskriterium von Eisenstein)
Sei R integer und $f(X) = a_n X^n + \cdots + a_1 X^1 + a_0 \in R[X]$ primitiv. Sei $\pi \in R$ prim und gelte

$$\begin{array}{lll} \text{(i)} & \pi \nmid a_n & \\ \text{(ii)} & \pi \mid a_i & \text{für } i = 0, 1, \ldots, n-1\,. \\ \text{(iii)} & \pi^2 \nmid a_0 & \end{array}$$

Dann ist f irreduzibel im Polynomring $R[X]$.

Bemerkungen 3.3.15.

1. Ist R faktoriell, so ist f nach Korollar 3.3.10 auch irreduzibel in Quot $(R)[X]$.
2. Ein primitives Polynom mit den Eigenschaften (i)–(iii) heißt Eisensteinpolynom bezüglich $\pi \in R$.

Beweis.

- Da π prim ist, ist der Ring $\overline{R} = R/\pi$ 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 $\bar{f} = \bar{g}\bar{h}$ im Polynomring $\bar{R}[X]$. Aus Bedingung (i) folgt grad $\overline{g} = r$ und grad $\overline{h} = s$.

- Aus Bedingung (ii) folgt $\overline{f}(X) = \overline{a}_n X^n$.

  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 $g(0)$ als auch $h(0)$, so dass das Element π^2 in $g(0)h(0) = a_0$ aufgeht, im Widerspruch zur Bedingung (iii).

□

Bemerkungen 3.3.16.

1. 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 das Polynom $X^n - a \in \mathbb{Z}[X]$ für jede Primzahl p, die a teilt, ein Eisensteinpolynom und nach Satz 3.3.14 irreduzibel. Es ist als normiertes irreduzibles Polynom nach Satz 1.3.15.1 Minimalpolynom von $\sqrt[n]{a}$.

   Das Polynom hat keine ganzen Nullstellen und nach Korollar 3.3.12 keine rationalen Nullstellen. Die Wurzeln quadratfreier Zahlen sind also nie rational.

2. 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 1.3.14 ist dann automatisch erfüllt.

Korollar 3.3.17.
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 das Polynom $f(X) := F_p(X+1) \in \mathbb{Q}[X]$. 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 der Primzahl p, also irreduzibel. Lediglich Bedingung (ii) ist nicht ganz offensichtlich, aber

$$p \,\Big|\, \binom{p}{k} = \frac{p(p-1)\ldots(p-k+1)}{1 \cdot 2 \cdot \ldots \cdot k} \quad \text{für } k = 2, \ldots p-1\ ,$$

denn die Primzahl p teilt den Zähler genau einmal, den Nenner aber nicht.

Die Abbildung $X \mapsto X+1$ induziert einen Ringautomorphismus des Polynomrings $\mathbb{Q}[X]$ mit Umkehrabbildung. $X \mapsto X-1$. Damit folgt aus der Irreduzibilität des Polynoms $f(X)$ die

Irreduzibiltät des Polynoms $F_p(X)$. $\square$

Mit Hilfe des Eisensteinkriteriums können wir zwei Konstruktionsprobleme näher untersuchen.

Satz 3.3.18.
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. Später, in Satz 4.5.10, werden wir sehen, dass die Konstruktion für Primzahlen der Form $p = 2^m + 1$ tatsächlich möglich ist.

Beweis.
Da $\zeta := \mathrm{e}^{2\pi \mathrm{i}/p} \in \mathbb{C}$ die polynomiale Gleichung $\zeta^p - 1 = 0$ erfüllt, ist ζ algebraisch. Ist $\zeta \in \lhd\mathbb{Q}$, so muss wegen Korollar 1.1.11.2 der Körpergrad $[\mathbb{Q}(\zeta) : \mathbb{Q}]$ eine Potenz von 2 sein. Wir berechnen den Körpergrad als Grad des Minimalpolynoms. Es gilt $\min_{\mathbb{Q}}(\zeta) = F_p(X)$. Denn $F_p(X)$ ist normiert, irreduzibel nach Lemma 3.3.17, also wegen $F_p(\zeta) = 0$ nach Satz 1.3.15.2 das Minimalpolynom von ζ. Damit finden wir $[\mathbb{Q}(\zeta) : \mathbb{Q}] = \operatorname{grad} F_p(X) = p - 1$. $\square$

Satz 3.3.19.
Sei φ mit $0 \leq \varphi < 2\pi$ derart, dass die komplexe Zahl $\mathrm{e}^{\mathrm{i}\varphi}$ transzendent über $\mathbb{Q}$ ist. Dann ist die Winkeldrittelung von φ mit Zirkel und Lineal nicht möglich.

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 $z := \mathrm{e}^{\mathrm{i}\varphi/3} \notin \lhd K$. Wegen Satz 1.1.11.2 reicht es zu zeigen, dass $[K(z) : K] = 3$ gilt. Da z eine Nullstelle des normierten Polynoms $X^3 - t \in K[X]$ ist, ist die Behauptung gezeigt, wenn wir wissen, dass $X^3 - t$ im Polynomring $K[X]$ irreduzibel ist.

Nach Satz 3.1.4 ist $K = \mathbb{Q}(t)$ isomorph zum rationalen Funktionenkörper über $\mathbb{Q}$. Daher ist K der Quotientenkörper des Rings $R = \mathbb{Q}[t]$, der isomorph zum Polynomring über dem Körper $\mathbb{Q}$ ist. Dieser Ring ist euklidisch, also insbesondere faktoriell. Das Element t ist im Ring $R = \mathbb{Q}[t]$ prim, denn der Quotient $\mathbb{Q}[t]/t \cong \mathbb{Q}$ ist integer.

$X^3 - t$ ist dann aber ein Eisensteinpolynom in $R[X]$ bezüglich des Primelements t und somit nach dem Eisensteinkriterium 3.3.13 irreduzibel in $R[X]$ und wegen Korollar 3.3.10 auch in $K[X]$ irreduzibel. Damit ist die Behauptung gezeigt. $\square$

4 Galoistheorie

Die Galoistheorie stellt eine tiefe Beziehung zwischen einer Klasse von Körpererweiterungen und Gruppen her.

4.1 Zerfällungskörper und normale Körpererweiterungen

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 Zerfällungskörpern von Polynomen zu.

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

1. *das Polynom f im Polynomring $L[X]$ vollständig in Linearfaktoren zerfällt.*
2. *der Körper L über K von den Nullstellen von f erzeugt wird.*

Nach dem Satz von Kronecker 1.2.16 gibt es für jedes Polynom $f \in K[X]$ einen Erweiterungskörper L' eine Nullstelle. Indem wir Linearfaktoren abspalten und dann diesen Satz wiederholt anwenden, finden wir für jedes Polynom einen Zerfällungskörper. Wir wollen den folgenden Satz beweisen:

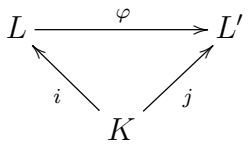
Satz 4.1.2.
Sei K ein Körper und $f \in K[X]$. Sind L/K und L'/K zwei Zerfällungskörper von f, so gibt es einen Isomorphismus

$$\sigma : L \to L'$$

mit der Eigenschaft, dass $\sigma_{|K} = \mathrm{id}_K$.

Warnung: man spricht zwar von *dem* Zerfällungskörper, aber die Isomorphismen zwischen verschiedenen Zerfällungskörpern sind i.a. nicht eindeutig.

Definition 4.1.3
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. Als Diagramm:



$\mathrm{Alg}_K(L, L')$ *bezeichne die Menge aller solchen Homomorphismen.*

Wir nennen auch φ eine Ausdehnung von j auf L.

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:

$$\begin{array}{rcl} \mathrm{Alg}_K(K(\alpha), M) & \tilde{\to} & \{\beta \in M | \min_K(\alpha)(\beta) = 0\} \\ \varphi & \mapsto & \varphi(\alpha) \end{array}$$

Beweis.
Sei $f := \min_K(\alpha)$; dann folgt aus $f(\alpha) = 0$ auch $0 = \varphi(f(\alpha)) = f(\varphi(\alpha))$. Daher ist $\varphi(\alpha)$ eine Nullstelle in M. Da φ durch seinem Wert auf dem primitiven Element α festliegt, ist die Abbildung injektiv. Um die Surjektivität zu zeigen, sei $\beta \in M$ eine Nullstelle des Minimalpolynoms von α. Wir haben nach Satz 1.2.9 einen Körperisomorphismus

$$\begin{array}{rcl} K[X]/\min_K(\alpha) & \to & K(\alpha) \\ \overline{X} & \mapsto & \alpha \end{array}$$

und auch einen Isomorphismus auf den Unterkörper $K(\beta) \subseteq M$,

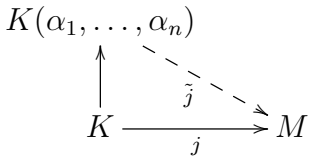
$$\begin{array}{rcl} K[X]/\min_K(\alpha) & \to & K(\beta) \\ \overline{X} & \mapsto & \beta \end{array}$$

Es gibt also einen Körperisomorphismus, der $K(\alpha)$ und den Unterkörper $K(\beta)$ von 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

$$\min_K(\alpha_i) \qquad i = 1 \ldots n$$

im Polynomring $M[X]$ vollständig in Linearfaktoren zerfallen. Dann gibt es eine Ausdehnung von j



Beweis.
Nach Satz 4.1.4 liefern die Einschränkungen Surjektionen

$$\begin{array}{l} \mathrm{Alg}_K(K(\alpha_1, \ldots \alpha_n), M) \twoheadrightarrow \mathrm{Alg}_K(K(\alpha_1, \ldots \alpha_{n-1}), M) \\ \twoheadrightarrow \cdots \twoheadrightarrow \mathrm{Alg}_K(K, M) \end{array}$$

□

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 eine endliche Körpererweiterung und $j : K \hookrightarrow M$ eine Einbettung in einen Körper M. Dann gibt es höchstens $[L : K]$ Fortsetzungen von j zu $\tilde{\jmath} : L \hookrightarrow M$:

$$\Big| \operatorname{Alg}_K(L, M)\Big| \leq [L : K] \,.$$

Beweis.
Besitzt die Körpererweiterung L/K einen echten Zwischenkörper $K \subset L' \subset L$, so folgt der Satz mittels vollständiger Induktion nach dem Körpergrad $[L : K]$:

$$\Big| \operatorname{Alg}_K(L, M)\Big| = \Big| \operatorname{Alg}_K(L', M)\Big|\Big|\operatorname{Alg}_{L'}(L, M)\Big| \leq [L' : K][L : L'] = [L : K] \,.$$

Hierbei ging in der Ungleichung die Induktionsannahme und in der letzten Gleichung die Gradformel 1.1.10 ein.

Gibt es keine Zwischenkörper, so ist nach Satz 1.3.19 die Körpererweiterung L/K eine einfache Körpererweiterung, $L = K(\alpha)$. Wir finden

$$\Big|\operatorname{Alg}_K(L, M)\Big| \overset{4.1.4}{=} \#\{\text{Nst. von } \min_K(\alpha) \text{ in } M\} \leq \operatorname{grad} \min_K(\alpha) \overset{1.2.9}{=} [K(\alpha) : K] \,.$$

wobei die Tatsache benutzt wird, dass die Zahl der Nullstellen eines Polynoms durch seinen Grad nach oben beschränkt ist. □

Wir geben noch einen zweiten Beweis, der auf dem folgenden Überlegungen beruht:

Definition 4.1.7
Sei K ein Körper und M ein Monoid. Ein Charakter von M mit Werten in K ist ein Homomorphismus von Monoiden

$$\chi : M \to K^\times \,.$$

Ein Charakter heißt trivial, wenn $\chi(m) = 1$ für alle $m \in M$ gilt.

Satz 4.1.8 (E. Artin)**.**
Seien $\chi_1, \ldots \chi_n$ paarweise verschiedene Charaktere eines Monoids M mit Werten in einem Körper K. Dann sind diese Charaktere im Vektorraum der K-wertigen Funktionen auf M linear unabhängig.

Beweis.
Der Fall $n = 1$ behandeln wir direkt: wegen $\chi(M) \subseteq K^\times$ ist ein einzelner Charakter linear unabhängig. Sei $n > 1$ und

$$a_1\chi_1 + \cdots + a_m\chi_m = 0 \qquad (*)$$

eine Relation minimaler Länge $2 \leq m \leq n$, in der alle Koeffizienten $a_m \neq 0$ sind.

Da $\chi_1 \neq \chi_2$ sein soll, gibt es wenigstens ein $z \in M$, für das $\chi_1(z) \neq \chi_2(z)$ gilt. Es gilt für alle $x \in M$

$$0 = a_1\chi_1(zx) + \cdots + a_m\chi_m(zx) = a_1\chi_1(z)\chi_1(x) + \cdots + a_m\chi_m(z)\chi_m(x) \,.$$

Wir teilen diese Gleichung durch $\chi_1(z)$ und subtrahieren sie von $(*)$ und erhalten die verschwindende Linearkombination

$$a_2\Bigg(\underbrace{\frac{\chi_2(z)}{\chi_1(z)}-1}_{\neq 0}\Bigg)\chi_2+\cdots+a_m\left(\frac{\chi_m(z)}{\chi_1(z)}-1\right)\chi_m=0\,.$$

Sie ist nicht trivial und hat eine kürzere Länge als die Relation $(*)$, die aber als minimal angenommen war. □

Wir geben nun den zweiten Beweis von Satz 4.1.6.

Beweis.
Sind $\sigma_1,\sigma_2,\ldots,\sigma_r$ paarweise verschiedene K-lineare Körperhomomorphismen $L\to M$, so müssen sie nach Satz 4.1.8 bereits linear unabhängig sein im M-Vektorraum $\mathrm{Map}(L^\times,M)$. Sei nun $\lambda_1,\lambda_2,\ldots,\lambda_s$ eine Basis von L über K mit s Elementen, so betrachte das lineare Gleichungssystem $\sum_{i=1}^r a_i\sigma_i(\lambda_j)=0$ aus s Gleichungen mit Koeffizienten in M für die r Variablen a_i. Wäre nun $r>s$, so finden wir eine nicht-triviale Lösung, also gäbe es $a_1,\ldots,a_s\in M$, nicht alle Null, mit $\sum_i a_i\sigma_i(\lambda_j)=0$ für alle j. Ein beliebiges Element $l\in L$ schreibt sich als $l=\sum_{j=1}^s\kappa_j\lambda_j$ mit $\kappa_s\in K$. Es folgt mit Hilfe der K-Linearität der Abbildungen σ_j

$$\sum_{i=1}^r a_i\sigma_i(l)=\sum_{i=1}^r\sum_{j=1}^s\kappa_j a_i\sigma_i(\lambda_s)=0\qquad\text{für alle } l\in L\ .$$

Somit wäre $\sum_i a_i\sigma_i$ die Nullabbildung, im Widerspruch zu Satz 4.1.8 über die lineare Unabhängigkeit von Charakteren. □

Definition 4.1.9
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 4.1.10.
Der Körper $\mathbb{Q}\left(\sqrt[3]{2}\right)$ ist nicht normal über $\mathbb{Q}$, denn wir können den Erweiterungskörper $\mathbb{Q}\left(\sqrt[3]{2}\right)$ von $\mathbb{Q}$ nach Satz 4.1.4 in den Körper $\mathbb{R}$ 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.

Wir charakterisieren nun normale Körpererweiterungen als Zerfällungskörper:

Satz 4.1.11.
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 und $L = K(\alpha_1, \ldots, \alpha_r)$, so ist L der Zerfällungskörper des Produkts

$$f = \prod_{i=1}^{r} \min_K(\alpha_i) \in K[X] \; .$$

Denn L enthält als normale Körpererweiterung alle Nullstellen von f, weil L von jedem irreduziblen Faktor eine Nullstelle enthält. Nun wird aber $L = K(\alpha_1, \ldots, \alpha_r)$ von den Nullstellen der Minimalpolynome über K erzeugt.

Für die umgekehrte Richtung zeigen wir (ii) ⇒ (iii) ⇒ (i), wobei wir die weitere Behauptung einführen:

(iii) Gegeben eine beliebige Körpererweiterung $j : K \hookrightarrow M$, dann haben alle Fortsetzungen von j zu Einbettungen $\psi, \varphi : L \hookrightarrow M$ dasselbe Bild:

$$\varphi(L) = \psi(L) \quad \text{für alle } \; \varphi, \psi \in \; \mathrm{Alg}_K(L, M) \, .$$

(ii) ⇒ (iii) Sowohl φ als ψ identifizieren die Nullstellen von f im Zerfällungskörper L mit den Nullstellen von f in M, aber vielleicht in verschiedener Weise. Da das Urbild L als Zerfällungskörper von diesen Nullstellen erzeugt wird, folgt die Gleichheit der Bilder, $\psi(L) = \varphi(L)$.

(iii) ⇒ (i) Sei $f \in K[X]$ ein beliebiges irreduzibes Polynom 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 mit Satz 1.3.16 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 $\alpha' \in M$ eine Nullstelle von f. Nach Satz 4.1.4 können wir $K \hookrightarrow M$ fortsetzen zu einem Körperhomomorphismus

$$\begin{array}{ccc} K(\alpha) & \hookrightarrow & M \\ \alpha & \mapsto & \alpha' \end{array}$$

und dies nach Satz 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 $L \hookrightarrow M$ liefert. Also ist L/K normal.

□

Satz 4.1.12.
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 die Körpererweiterung N/K normal ist.

Beweis.
Seien $\alpha_1, \dots \alpha_r$ 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 4.1.11 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 $\mathbb{Q}(\sqrt[3]{2}, \mathrm{e}^{2\pi \mathrm{i}/3})$ über $\mathbb{Q}$ die normale Hülle der Körpererweiterung $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ aus Beispiel 4.1.10.

4.2 Endliche Körper

Wir brauchen einige Hilfsmittel für den späteren Gebrauch.

Satz 4.2.1.
Jede endliche Untergruppe G der multiplikativen Gruppe eines Körpers K ist zyklisch.

- Die Elemente ζ endlicher Ordnung der multiplikativen Gruppe eines Körpers sind genau diejenigen Elemente, die eine Gleichung der Gestalt $\zeta^n = 1$ für ein geeignetes $n \in \mathbb{N}$ erfüllen. Sie heißen auch die Einheitswurzeln des Körpers.
- Insbesondere folgt aus Satz 4.2.1, dass die multiplikative Gruppe $K^\times$ eines endlichen Körpers K zyklisch ist, da sie endlich ist. Ein erzeugendes Element von $K^\times$ heißt Primitivwurzel.

Beweis.
In jeder endlichen abelschen Gruppe wird nach dem Klassifikationssatz 2.9.1 die maximale von einem Gruppenelement erreichte Ordnung n geteilt durch die Ordnungen aller Gruppenelemente. Wäre die Gruppe G nicht zyklisch, so gibt es kein Element der Ordnung $|G|$, also wäre $n < |G|$. Für dieses n wäre $\zeta^n = 1$ für alle $\zeta \in G$. Nun kann das Polynom $X^n - 1$ aber im Körper K höchstens n Nullstellen haben kann, im Widerspruch zur Annahme $n < |G|$. □

Dies liefert uns den Schlüssel zur Strukturtheorie endlicher Körper:

Satz 4.2.2.
Die Kardinalität eines endlichen Körpers $\mathbb{F}$ ist eine Primzahlpotenz. Zu jeder Primzahlpotenz q gibt es bis auf Isomorphie genau einen endlichen Körper $\mathbb{F}_q$ dieser Kardinalität.

Es ist schon nachBemerkung 3.1.12 klar, dass die Charakteristik eines endlichen Körpers $\mathbb{F}$ eine Primzahl ist und $\mathbb{F}$ den Körper $\mathbb{F}_p$ als Primkörper enthält. Dadurch ist $\mathbb{F}$ ein endlichdimensionaler $\mathbb{F}_p$-Vektorraum. Mit $r := \dim_{\mathbb{F}_p} \mathbb{F}$ gilt $\mathbb{F} \cong \mathbb{F}_p^r$ und somit $|\mathbb{F}| = p^r$. Dies zeigt die erste Aussage des Satzes.

Um Satz 4.2.2 vollständig zu zeigen, zeigen wir zunächst:

Lemma 4.2.3.
Sei p eine Primzahl, $q = p^r$ mit $r \geq 1$ eine echte Primzahlpotenz und L ein Körper der Charakteristik p. Zerfällt das Polynom $X^q - X$ über L vollständig in Linearfaktoren, so bilden die Nullstellen einen Unterkörper der Kardinalität q.

Beweis.
Die Abbildung

$$\begin{array}{ccc} L & \to & L \\ a & \mapsto & a^q \end{array}$$

ist wegen $\text{char}(L) = p$ ein Körperhomomorphismus. Die Nullstellen von $X^q - X$ sind genau die Fixpunkte des Körperhomomorphismus und bilden daher einen Unterkörper $\mathbb{F}$ von L.

Um zu zeigen, dass dieser genau q Elemente hat, müssen wir zeigen, dass alle Nullstellen von $X^q - X$ einfach sind. Die Nullstelle $X = 0$ ist einfach. Es gilt $(X-a)^q - (X-a) = X^q - a^q - X + a = X^q - X$ für jede Nullstelle a von $X^q - X$. Also ist auch jede weitere Nullstelle a einfach. □

Wir beweisen nun Satz 4.2.2:

Beweis.

- Es gibt nach Satz 1.3.16 eine Körpererweiterung L von $\mathbb{F}_p$, in der das Polynom $X^q - X$ vollständig in Linearfaktoren zerfällt. Nach Lemma 4.2.3 bilden die Nullstellen dieses Polynoms einen Unterkörper von L der Kardinalität q. Damit ist die Existenz eines solchen endlichen Körpers gezeigt.

- Wir müssen nur noch zeigen, dass je zwei solche Körper isomorph sind. Sei K ein Körper mit $q = p^r$ Elementen. Dann gilt für jedes $a \in K^\times$ nach Satz 4.2.1, dass $a^{q-1} = 1$, also $a^q - a = 0$ für alle $a \in K$. Damit ist K ein Zerfällungskörper des Polynoms $X^q - X$, und nach Satz 4.1.2 sind je zwei Zerfällungskörper isomorph.

□

4.3 Vielfachheit von Nullstellen, separable Körpererweiterungen

Ziel ist der Beweis des folgenden Satzes:

Satz 4.3.1.
Seien $K \subset L$ Körper und $f \in K[X]$ irreduzibel. Ist $\text{char}(K) = 0$, so hat f keine mehrfachen Nullstellen in L.

Lemma 4.3.2.
Seien $K \subset L$ Körper, $f, g \in K[X]$ und $g \neq 0$.

1. Teilen mit Rest führt auf das gleiche Resultat in $K[X]$ und $L[X]$.

2. g teilt f in $L[X]$ dann und nur dann, wenn g das Polynom f in $K[X]$ teilt.

3. 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.

1. Der euklidische Algorithmus erlaubt es, in eindeutiger Weise $f = qg + r$ zu schreiben mit $q, r \in K[X]$ und grad $r <$ grad g.

2. Ist ein Spezialfall von 1. mit $r = 0$.

3. Offenbar ist d_K auch gemeinsamer Teiler von f und g in $L[X]$, also $d_K | d_L$. Andererseits liefert der euklidische Algorithmus im Polynomring $K[X]$ Polynome $p, q \in K[X]$, so dass

$$d_K = qf + pg\,.$$

Da diese Gleichung auch im Polynomring $L[X]$ gilt, folgt $d_L | d_K$. Da die beiden Polynome d_L und d_K normiert sind, folgt $d_K = d_L$.

□

Definition 4.3.3
Sei R ein Ring und $f = \sum_{i=0}^{n} a_i X^i \in R[X]$. Die formale Ableitung $f' \in R[X]$ ist das Polynom $f' = \sum_{i=0}^{n} i a_i X^{i-1} \in R[X]$.

Lemma 4.3.4.

1. Ist $f \in R \subseteq R[X]$ konstant, so gilt $f' = 0$. (Vorsicht, die Umkehrung gilt für allgemeine Ringe nicht, siehe Korollar 4.3.7!)
2. $(f+g)' = f' + g'$
3. Leibnizregel: $(fg)' = f'g + fg'$
4. Sei K ein Körper, $g \in K[X]$ ungleich Null und $\alpha \in K$ eine Nullstelle von g. Dann ist α genau dann mehrfache Nullstelle von g, wenn $g'(\alpha) = 0$ gilt.

Beweis.

1. – 3. sollte aus der Schule bekannt sein.
4. Ist α mehrfache Nullstelle von g, so gilt $g = (X-\alpha)^2 f$ für ein $f \in K[X]$. Nach der Leibnizregel 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 $g(X) = (X-\alpha)^2 \tilde{h}(X)$ für ein $\tilde{h} \in K[X]$.

□

Satz 4.3.5.
Sei K Körper und $f \in K[X]$. Dann sind äquivalent:

1. f hat in seinem Zerfällungskörper mehrfache Nullstellen.
2. f und f' sind nicht teilerfremd, $(f) + (f') \neq L[X]$.

Beweis.

1. $\Rightarrow$ 2. Ist α mehrfache Nullstelle, so ist nach Lemma 4.3.4.4 α Nullstelle von f und f', also der Linearfaktor $(X-\alpha)$ gemeinsamer Teiler von f und f' in $L[X]$.
2. $\Rightarrow$ 1. Im Zerfällungskörper des Produkts ff' gibt es ein Element α, so dass $X-\alpha$ sowohl f als auch f' teilt. Also hat f nach Lemma 4.3.4.4 eine mehrfache Nullstelle.

□

Bemerkung 4.3.6.
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 4.3.7.
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 4.3.5 sind dann f und f' nicht teilerfremd. Da f irreduzibel sein soll, muss f seine Ableitung f' teilen. 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 Koeffizienten a_i mit $i = 0 \bmod p$ nicht verschwinden.

(iii) $\Rightarrow$ (i) In diesem Falle ist offenbar $f' = 0$, so dass f und f' das Polynom f als gemeinsamen Teiler haben. Nach Satz 4.3.5 hat dann f eine mehrfache Nullstelle.

□

Definition 4.3.8

1. *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.*

2. *Sei L/K Körpererweiterung. Ein Element $\alpha \in L$ heißt separabel über K, wenn es algebraisch über K ist und sein Minimalpolynom separabel ist.*

3. *Die Körpererweiterung L/K heißt separabel, wenn jedes Element von L über K separabel ist.*

4. *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.*

Da die Abbildung $x \mapsto x^p$ als Körperhomomorphismus injektiv ist, ist jeder endliche Körper perfekt. Der rationale Funktionenkörper $\mathbb{F}_p(t)$ ist nicht perfekt.

Satz 4.3.9.
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 4.3.7 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 in Charakteristik 0 jede algebraische Körpererweiterung separabel.

- Sei nun char $K = p$. Betrachte eine algebraische Körpererweiterung L/K und $\alpha \in L$. Angenommen α wäre eine mehrfache Nullstelle seines Minimalpolynoms $f = \min_K(\alpha)$. Nach Korollar 4.3.7(iii) ist f dann von der Form

  $$f = b_n(X^p)^n + \cdots + b_1 X^p + b_0 \,,$$

  Da der Körper K als perfekt vorausgesetzt ist, können wir $a_i \in K$ finden mit $b_i = (a_i)^p$. Dann gilt

  $$f = g^p \quad \text{mit dem Polynom} \quad g = \sum_i a_i X^i \in K[X] \,,$$

  im Widerspruch zur Irreduzibilität des Minimalpolynoms f.

□

Satz 4.3.10.
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 die Körpererweiterung L/K überdies endlich, so ist 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 $L \hookrightarrow N$,

$$|\mathrm{Alg}_K\ (L, N)| = [L : K] \,.$$

Die Körpererweiterung L/K ist also genau dann separabel, wenn in der Ungleichung in Satz 4.1.6 Gleichheit herrscht.

Beweis.

(i) $\Rightarrow$ (ii) ist klar, weil dann jedes Element von L per Definition über K separabel ist.

(ii) $\Rightarrow$ (iii) Mit Induktion über $[L : K]$ dürfen wir wieder annehmen, dass $L = K(\alpha)$. Da α separabel ist, sind die $[L : K]$ Nullstellen des Minimalpolynoms $\min_K(\alpha)$ in N paarweise verschieden und liefern nach Satz 4.1.4 verschiedene Erweiterungen von $K \hookrightarrow N$ zu $K(\alpha) = L \hookrightarrow N$.

(iii) $\Rightarrow$ (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)

□

Wir brauchen später noch den folgenden Satz:

Satz 4.3.11 (Satz vom primitiven Element)**.**
Ist L/K eine endliche separable Körpererweiterung, so gibt es ein Element $\alpha \in L$ mit $L = K(\alpha)$.

Beweis.
Da die multiplikative Gruppe jedes endlichen Körpers nach Satz 4.2.1 zyklisch ist, finden wir Erzeuger der multiplikativen Gruppe von L, die natürlich primitive Elemente sind.

Daher dürfen wir ohne Beschränkung der Allgemeinheit K als unendlich annehmen. Nach Satz 4.1.12 können wir L vergrößern zu einer normalen Erweiterung N von K. Wegen der Separabilität von L/K gibt es dann nach Satz 4.3.10 genau $[L : K]$ Körperhomomorphismen über K von L in die normale Hülle N, also $|\mathrm{Alg}_K(L, N)| = [L : K]$.

Diejenigen Elemente von L, auf denen zwei feste, aber verschiedene derartige Körperhomomorphismen übereinstimmen, bilden einen echten K-Untervektorraum von L. Falls der Körper K unendlich ist, kann ein K-Vektorraum jedoch nicht durch endlich viele echte Untervektorräume überdeckt werden. Es gibt folglich Elemente $\alpha \in L$ derart, dass die Elemente $\sigma(\alpha)$ für verschiedene $\alpha \in \mathrm{Alg}_K(L, N)$ paarweise verschieden sind.

Für ein solches α ist der von der Restriktion erzeugte Morphismus $\mathrm{Alg}_K(L, N) \to \mathrm{Alg}_K(K(\alpha), N)$ aber eine Injektion. Nun folgt

$$[L : K] = |\mathrm{Alg}_K(L, N)| \leq |\mathrm{Alg}_K(K(\alpha), N)| = [K(\alpha) : K] \ ,$$

woraus $L = K(\alpha)$ folgt. □

4.4 Galoiserweiterungen und Galoiskorrespondenz

Definition 4.4.1
Sei L/K eine Körpererweiterung. Die Gruppe aller Körperautomorphismen von L, die K punktweise festlassen, heißt die Galoisgruppe $\mathrm{Gal}\,(L/K)$ *der Körpererweiterung L/K.*

Es handelt sich also bei den Elementen der Galoisgruppe um die Symmetrien der Körpererweiterung.

Bemerkung 4.4.2.

1. Offenbar hat man die Inklusion $\mathrm{Gal}(L/K) \subseteq \mathrm{Alg}_K(L, L)$. Für endliche Körpererweiterungen folgt Gleichheit, da jeder injektive Endomorphismus des endlich-dimensionalen K-Vektorraums L auch surjektiv ist. Aus Satz 4.1.6 folgt somit für endliche Körpererweiterungen die Abschätzung $|\mathrm{Gal}\,(L/K)| \leq [L : K]$.

2. Die Gleichheit $\mathrm{Gal}(L/K) = \mathrm{Alg}_K(L, L)$ gilt sogar für alle algebraischen Erweiterungen (ohne Beweis).

3. Es gilt $\mathrm{Gal}(\mathbb{C}, \mathbb{R}) = \{\mathrm{id},\ \text{Konjugation}\}$ und $\mathrm{Gal}\left(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}\right) = \{\mathrm{id}\}$.

4. Ist q eine Primzahlpotenz und $r \geq 1$, so ist $\mathrm{Gal}(\mathbb{F}_{q^r}/\mathbb{F}_q)$ eine zyklische Gruppe der Ordnung r, erzeugt vom Frobenius-Homomorphismus

$$\begin{array}{rccc} F: & \mathbb{F}_{q^r} & \to & \mathbb{F}_{q^r} \\ & a & \mapsto & a^q \end{array}$$

   Denn F erzeugt in der Galoisgruppe eine zyklische Untergruppe der Ordung r. Nach der vorhergehenden Bemerkung 4.4.2.1 hat die Galoisgruppe jedoch höchstens $[\mathbb{F}_{q^r} : \mathbb{F}_q] = \dim_{\mathbb{F}_q} \mathbb{F}_{q^r} = r$ Elemente.

Definition 4.4.3
Eine Körpererweiterung L/K heißt Galoiserweiterung oder galoisch, wenn sie normal und separabel ist.

Wir brauchen einige Begriffe, um Gruppenwirkungen zu beschreiben:

Bemerkungen 4.4.4.

1. Operiert eine Gruppe G auf einer Menge X, so schreiben wir in diesem Kapitel auch X^G für die Menge der Fixpunkte:
$$X^G = \{x \in X \mid gx = x \quad \text{für alle } g \in G\}\,.$$
2. Eine Operation einer Gruppe G auf einer Menge X heißt treu, wenn
$$gx = x \quad \forall x \in X \quad \Rightarrow \quad g = e \in G\,.$$
3. Eine Operation mit nur einer Bahn heißt transitiv.
4. 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.
5. Ist U eine Untergruppe von $\mathrm{Gal}(L/K)$, so gilt $K \subseteq L^U \subseteq L$.

Satz 4.4.5.
Sei L/K eine *endliche* Körpererweiterung und $G := \mathrm{Gal}(L/K)$. Dann sind äquivalent:

(i) L/K ist galoisch, d.h. nach Definition 4.4.3 normal und separabel.

(ii) Es gilt $|\mathrm{Gal}(L/K) \mid = [L : K]$, d.h. inder Ungleichung $|\mathrm{Gal}(L/K)| \leq [L : K]$ herrscht Gleichheit.

(iii) Es gilt $K = L^G$, d.h. die Inklusion $K \subset L^G$ aus Bemerkung 4.4.4.4 ist keine echte Inklusion.

(iv) Für alle $\alpha \in L$ gilt
$$\min_K(\alpha) = \prod_{\beta \in G\alpha} (X - \beta)\,.$$

Beweis.

(i)⇒(ii) Da die Körpererweiterung L/K nach Voraussetzung separabel und normal ist, können wir in Satz 4.3.10 (iii) $N = L$ setzen und erhalten $\mid \mathrm{Alg}_K(L, L)| = [L : K]$. Da L/K endlich ist, gilt außerdem nach Bemerkung 4.4.2.1 $\mathrm{Alg}_K(L, L) = \mathrm{Gal}(L/K)$.

(ii)⇒(iii) Wir betrachten die Abschätzung
$$|G| \overset{\text{(ii)}}{=} [L : K] \geq [L : L^G] \geq |G|\,,$$
wobei wir zunächst die Gradformel 1.1.10 und dann Bemerkung 4.4.2.1 benutzt haben. In allen Ungleichungen muss dann aber Gleichheit gelten, also folgt aus $K \subset L^G$ sogar $K = L^G$.

(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

$$\prod_{\beta \in G\alpha} (X - \beta) \in L^G[X] \overset{\text{(iii)}}{=} K[X]$$

das Polynom f. Ist speziell $f = \min_K(\alpha)$, so ist f als Minimalpolynom prim nach Satz 1.3.15.1 und beide Polynome sind normiert. Somit folgt die Gleichheit beider Polynome.

(iv)⇒ (i) Nach Voraussetzung 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 Zerfällungskörper des Polynoms

$$f = \prod_{i=1}^{r} \min_K(\alpha_i) \in K[X]$$

und als Zerfällungskörper nach Satz 4.1.11 normal.

□

Der folgende Satz folgt leicht aus den Sätzen 4.1.4 und 4.1.5:

Satz 4.4.6. (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.

Bemerkung 4.4.7.
Ist L/K eine endliche Galois-Erweiterung, so ist $\alpha \in L$ ein primitives Element genau dann, wenn es von keinem nicht-trivialen Element der Galoisgruppe festgehalten wird. Wir können sogar stets ein $\alpha \in L$ so wählen, dass es mit seinen Galois-Konjugierten eine K-Basis von L bildet (Satz von der Normalbasis). Diese Aussage stimmt keineswegs für jedes primitive Element, wie das Beispiel $L = \mathbb{C}$, $K = \mathbb{R}$ und $\alpha = \mathrm{i}$ zeigt.

Wir konstruieren Galoiserweiterungen durch Gruppenwirkungen:

Satz 4.4.8.
Ist L ein Körper und G eine Gruppe von Körperautomorphismen von L, so gilt $|G| = [L : L^G]$.

Aus Satz 4.4.5 folgt dann, dass für eine endliche Gruppe G die Körpererweiterung L/L^G eine endliche Galoiserweiterung mit Galoisgruppe G ist.

Wir bringen zwei Beweise. Der erste Beweis benutzt die lineare Unabhängigkeit von Charakteren aus Satz 4.1.8.

Beweis.
Wir wissen schon aus Bemerkung 4.4.2.1, dass $|G| \leq [L : L^G]$ gilt. Es reicht also aus, im Falle einer endlichen Gruppe die strikte Ungleichung $|G| < [L : L^G]$ zum Widerspruch zu führen. Dazu sei $G = \{\sigma_1, \ldots, \sigma_r\}$; wir finden mit der Widerspruchsannahme eine über L^G linear unabhängige Familie $x_0, x_1, \ldots, x_r \in L$.

In der Matrix $(\sigma_i(x_j))$ sind dann die $r+1$ Spalten aus Spaltenvektoren in L^r über L linear abhängig, d.h. wir finden eine nicht-triviale Linearkombination

$$\sum_{j=1}^{r} y_j \sigma_i(x_j) = 0 \quad \text{für alle } i = 0, 1, \dots r \qquad (*)$$

mit Koeffizienten $y_0, \dots, y_r$ in L. Durch Anwenden von σ_i^{-1} finden wir

$$\sum_{j=1}^{r} \sigma_i^{-1}(y_j) x_j = 0 \quad \text{für alle } i = 0, 1, \dots r$$

Die Summation dieser Gleichungen ergibt

$$\sum_{j=1}^{r} \lambda_j x_j = 0$$

mit Koeffizienten $\lambda_j := \sum_i \sigma_i^{-1}(y_j) \in L^G$ für alle j.

Wegen der linearen Unabhängigkeit der Charaktere 4.1.8 finden wir ein $z \in L$ mit $\sum_i \sigma_i^{-1}(z) \neq 0$. Indem wir notfalls die Koeffizienten $y_0, \dots, y_r$ in $(*)$ durch Durchmultiplizieren ersetzen durch $yy_0, \dots, yy_r$, können wir erreichen, dass einer der Koeffizienten λ_j nicht verschwindet, im Widerspruch zur Annahme, dass die Familie $x_0, x_1, \dots, x_r$ über L^G linear unabhängig ist. □

Wir geben einen zweiten Beweis von Satz 4.4.8 mit dem Satz 4.3.11 vom primitiven Element:

Beweis.

- Wir zeigen zunächst:
  Für jedes $\alpha \in L$ ist $g_\alpha := \prod_{\beta \in G\alpha}(X - \beta)$ das Minimalpolynom von α über L^G.

  Denn es gilt $g_\alpha \in L^G[X]$. Damit ist α als Nullstelle von g_α algebraisch über L^G. Da mit α auch alle $\sigma\alpha$ mit $\sigma \in G$ Nullstellen des Minimalpolynoms sein müssen, teilt g_α das Minimalpolynom von α. Da g_α normiert ist und das Minimalpolynom irreduzibel und normiert ist, folgt Gleichheit.

- Als nächstes zeigen wir, dass die Körpererweiterung L/L^G endlich ist. Aus der Implikation $(iv) \Rightarrow (i)$ von Satz 4.4.5 folgt ann, dass sie auch normal und separabel und somit galoisch ist.

  Sei $L^G \subset M \subset L$ ein Zwischenkörper, der endlich über L^G ist. Dann besitzt M nach Satz 4.3.11 ein primitives Element $\alpha \in M$, es gilt also $M = L^G(\alpha)$. Da das Minimalpolynom von α nach dem vorhergehenden Punkt höchstens Grad $|G|$ hat, folgt $[M : L^G] \leq |G|$.

  Gilt nun $|G| < [L : L^G] \leq \infty$, so gibt es eine endliche Teilmenge $S \subset L$, so dass für den Zwischenkörper $M = L^G(S)$ gilt $|G| < [M : L^G] < \infty$, im Widerspruch zu dem, was gerade gezeigt wurde. Daraus folgt aber, dass L/L^G endlich ist. Dann können wir aber $M = L$ setzen und finden die Abschätzung $[L : L^G] \leq |G|$.

- Es ist klar, dass $G \subset \mathrm{Gal}(L/L^G)$ gilt. Die Gleichheit $G = \mathrm{Gal}(L/L^G)$ ergibt sich dann aus der Ungleichungskette

  $$|G| \leq |\mathrm{Gal}(L/L^G)| \leq [L : L^G] \leq |G| \ .$$

  Hierbei folgt die erste Ungleichung aus $G \subset \mathrm{Gal}(L/L^G)$, die zweite aus Bemerkung 4.4.2.1 und die letzte Ungleichung wurde gerade gezeigt.

□

Korollar 4.4.9 (Hauptsatz der Galoistheorie für endliche galoische Erweiterungen)**.**
Sei L/K eine endliche galoische Körpererweiterung mit Galoisgruppe G.

1. Dann ist die Abbildung von Zwischenkörpern auf Untergruppen der Galoisgruppe G

$$\begin{aligned} \mathcal{Z}(L/K) &\to \mathcal{U}(G) \\ F &\mapsto \mathrm{Gal}(L/F) \end{aligned}$$

   eine Bijektion. Die Umkehrabbildung ist durch Bilden des Fixkörpers gegeben:

$$\begin{aligned} \mathcal{U}(G) &\to \mathcal{Z}(L/K) \\ U &\mapsto L^U\,. \end{aligned}$$

2. Die Abbildung ist inklusionsumkehrend: für je zwei Zwischenkörper F_1 und $F_2 \in \mathcal{Z}(E/K)$ gilt

$$F_1 \subseteq F_2 \iff \mathrm{Gal}(E/F_2) \subseteq \mathrm{Gal}(E/F_1)$$

3. Unter dieser Bijektion entsprechen die Normalteiler H von G genau denjenigen Zwischenkörpern F, die normal über K sind. In diesen Fällen definiert das Einschränken von Elementen der Galoisgruppe einen Isomomorphismus von Gruppen $G/H \cong \mathrm{Gal}(L^H/K)$, also eine kurze exakte Sequenz

$$1 \to \mathrm{Gal}(L/F) \to \mathrm{Gal}(L/K) \to \mathrm{Gal}(F/K) \to 1\ .$$

Beweis.

1. Offensichtlich ist für jeden Zwischenkörper F auch die Körpererweiterung L/F galoisch.

   - Sie ist normal: weil die Körpererweiterung L/K normal ist, können wir L nach Satz 4.1.11 als Zerfällungskörper eines Polynoms in $K[X]$ auffassen und somit erst recht als Zerfällungskörper eines Polynoms in $F[X]$.
   - Sie ist separabel. Für jedes $a \in L$ hat $\min_K(a)$ nur einfache Nullstellen in L. Nun teilt aber $\min_F(a)$ das Minimalpolynom $\min_K(a)$ und hat daher auch nur einfache Nullstellen.

   Damit folgt $L^{\mathrm{Gal}(L/F)} = F$ aus (iii) in Satz 4.4.5. Umgekehrt gilt $\mathrm{Gal}(L/L^H) = H$ nach der Folgerung aus Satz 4.4.8. Das zeigt die erste Behauptung. Die zweite Behauptung ist offensichtlich.

2. Man sieht leicht, dass gilt $g(L^H) = L^{gHg^{-1}}$. Insbesondere ist L^H genau dann invariant unter der Galoisgruppe G, wenn H ein Normalteiler in G ist.

   Andererseits ist L^H genau dann invariant unter G, wenn die Körpererweiterung L^H/K normal ist. Denn weil L/K galoisch ist, ist nach Satz 4.4.5 $\min_K(\alpha) = \prod_{\beta \in G\alpha}(X - \beta)$ für alle $\alpha \in L$. Ist L^H/K normal, so zerfällt das Minimalpolynom eines beliebigen Elements $\alpha \in L^H$ schon in L^H, somit gilt $g\alpha \in L^H$ für alle $g \in G$. Also ist L^H invariant unter G.

   Ist umgekehrt L^H invariant unter G, so enthält L^H alle Nullstellen des Minimalpolynoms eines beliebigen Elements $\alpha \in L^H$, also ist L^H/K normal.

3. Sei nun $H \subset G$ normale Untergruppe. Dann faktorisiert dann die offensichtliche Abbildung $G \to \mathrm{Gal}(L^H/K)$ über G/H durch Einschränkung $\sigma \mapsto \sigma|_{L^H}$ und liefert eine Injektion $G/H \to \mathrm{Gal}(L^H/K)$. Es gilt nun

$$|\mathrm{Gal}(L^H/K)| = [L^H : K] = \frac{[L:K]}{[L:L^H]} = \frac{|G|}{|H|} = |G/H| \ ,$$

wobei die erste Gleichheit aus Satz 4.4.5 (ii) folgt, weil L^H/K galoisch ist, dann die Gradformel verwendet wird, und dann wieder Satz 4.4.5 (ii), so dass die Injektion eine Bijektion sein muss.

□

Definition 4.4.10
Sei $\mathrm{char}\, K \neq 2$. *Eine Körpererweiterung* L/K *heißt biquadratisch, wenn sie Grad* $[L:K] = 4$ *hat und von zwei Elementen* $L = K(\alpha, \beta)$ *erzeugt ist, mit* $\alpha^2, \beta^2 \in K$.

Beispiel 4.4.11.
Der Körper $\mathbb{Q}(\sqrt{3}, \sqrt{5})$ ist biquadratisch über $\mathbb{Q}$, denn $(a + b\sqrt{5})^2 = a^2 + 2b\sqrt{5} + 5b^2$ ist nie gleich 3.

Betrachtung 4.4.12.

1. Jede biquadratische Erweiterung E/K ist galoisch. Ihre Galois-Gruppe ist die Klein'sche Vierergruppe $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

   Um dies zu sehen, konstruieren wir nicht-triviale Elemente in $\mathrm{Gal}(E/K)$. Da β nicht im Zwischenkörper $K(\alpha)$ liegt, ist sein Minimalpolynom auch über $K(\alpha)$ gleich $\min_{\mathbb{Q}(\alpha)}(\beta) = X^2 - \beta^2$. Ein Körperautomorphismus von E, der $K(\alpha)$ festlässt, kann nach Satz 4.1.4 konstruiert werden, indem wir β auf die andere Nullstelle $-\beta$ abbilden. Er erhalten so Körperautomorphismen

   $$\sigma : \begin{cases} \alpha & \mapsto & \alpha \\ \beta & \mapsto & -\beta \end{cases} \qquad \text{und} \qquad \tau : \begin{cases} \alpha & \mapsto & -\alpha \\ \beta & \mapsto & \beta \end{cases}$$

   so dass in der Galoisgruppe die Teilmenge $\{\mathrm{id}, \sigma, \tau, \sigma\tau\}$ liegt. Wegen $[L:K] = 4$ muss das die ganze Galoisgruppe sein.

2. Die Kleinsche Vierergruppe hat 5 Untergruppen: die triviale, die ganze Gruppe und drei zyklische Gruppen der Ordnung 2. Sie entsprechen den Unterkörpern

   $$K \subset K(\alpha), K(\beta), K(\alpha\beta) \subset L$$

   Eine K-Basis von L besteht aus $1, \alpha, \beta, \alpha\beta$. Das Element $\alpha + \beta$ ist primitiv.

Wir können nun die Struktur der Unterkörper eines endlichen Körpers verstehen:

Korollar 4.4.13.
Gegeben zwei endliche Körper, so lässt sich der eine in den anderen einbetten genau dann, wenn die Kardinalität des einen eine Potenz der Kardinalität des anderen ist.

Beweis.
Ein endlicher Körper ist nach Satz 4.2.2 von der Form $\mathbb{F}_q$ mit einer Primzahlpotenz $q = p^r$. Sein Primkörper ist $\mathbb{F}_p$. Nach Bemerkung 4.4.2.4 ist die Galoisgruppe $\mathrm{Gal}(\mathbb{F}_q/\mathbb{F}_p)$ zyklisch von Ordnung von Ordnung r, mit dem Frobenius-Automorphismus als Erzeuger. Die Untergruppen der zyklischen Gruppen sind nach Korollar 2.5.6 in Bijektion zu Teilern $d|r$ und durch ihre Mächtigkeit d eindeutig bestimmt. Damit ist $[\mathbb{F}_q : \mathbb{F}_q^U] = |U| = d$. Es folgt $\dim_{\mathbb{F}_q^U} \mathbb{F}_q = d$ und somit für die Kardinalitäten $|\mathbb{F}_q| = |\mathbb{F}_q^U|^d$. □

Satz 4.4.14.
Der Körper der komplexen Zahlen ist algebraisch abgeschlossen, d.h. jedes nicht-konstante Polynom mit komplexen Koeffizienten hat in $\mathbb{C}$ eine Nullstelle. Daher zerfallen komplexe Polynome in Linearfaktoren.

Beweis.
Sei $L/\mathbb{R}$ eine endliche normale Erweiterung des Körpers der reellen Zahlen $\mathbb{R}$ und $G := \mathrm{Gal}(L/\mathbb{R})$ ihre Galoisgruppe. Sei $S \subset G$ eine 2-Sylowgruppe. Dann ist $[L : \mathbb{R}] = |G|$ und $[L : L^S] = |S|$. Folglich ist der Körpergrad $[L^S : \mathbb{R}]$ ungerade.

Sei $\alpha \in L^S$. Das Minimalpolynom $\min_{\mathbb{R}}(\alpha)$ muss wegen $\mathrm{gradmin}_{\mathbb{R}}(\alpha) = [\mathbb{R}(\alpha) : \mathbb{R}] \,|\, [L^S : \mathbb{R}]$ ungeraden Grad haben. Aber jedes Polynom aus $\mathbb{R}[X]$ von ungeradem Grad hat, wie aus der Analysis bekannt, wenigstens eine reelle Nullstelle, im Widerspruch zur Irreduzibilität von Minimalpolynomen. Es folgt $L^S = \mathbb{R}$. Mithin haben wir $S = G$ und die Galoisgruppe G von $L/\mathbb{R}$ ist eine 2-Gruppe.

Nach dem Struktursatz 2.11.1 über 2-Gruppen gibt es in G eine absteigende Kette

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

von Normalteilern von G, so dass

$$G_i/G_{i-1} \cong \mathbb{Z}_2 \quad \text{für alle } i.$$

Also entsteht notwendig L aus $\mathbb{R}$ durch sukzessive Adjunktion von Quadratwurzeln. Adjungiert man aber eine echte Quadratwurzel zu $\mathbb{R}$, so erhält man $\mathbb{C}$, und in $\mathbb{C}$ hat jedes Element schon eine Quadratwurzel. Daraus folgt $L = \mathbb{R}$ oder $L = \mathbb{C}$. Somit zerfällt jedes reelle Polynom in $\mathbb{R}$ oder in $\mathbb{C}$. Sei nun $L/\mathbb{C}$ Zerfällungskörper eines Polynoms in $\mathbb{C}[X|$; für die normale Hülle $N/\mathbb{R}$ folgt $N = \mathbb{C}$. □

Aus dem Satz vom primitiven Element 4.3.11 folgt sofort:

Satz 4.4.15.
1. Ist E/K endliche, galoische Erweiterung, so ist E Zerfällungskörper eines separablen irreduziblen Polynoms $f \in K[X]$.
2. Umgekehrt gilt: der Zerfällungskörper eines separablen Polynoms $f \in K[X]$ ist eine endliche galoische Erweiterung von K.

Beweis.
1. Nach dem Satz vom primitiven Element gibt es für die endliche separable Erweiterung E/K ein primitives Element $\alpha \in E$, so dass $E = K(\alpha)$. Das Minimalpolynom $\min_K(\alpha)$ ist irreduzibel, separabel und zerfällt in E, weil E normal ist. Also ist E der Zerfällungskörper des Minimalpolynoms.

2. Als Zerfällungskörper eines Polynoms ist E/K endlich und nach Satz 4.1.11 normal. Da E von den Nullstellen des separablen Polynoms f erzeugt wird, ist f nach Satz 4.3.10 separabel.

□

Definition 4.4.16
Sei $f \in K[X]$ ein separables Polynom. (Es würde ausreichen, zu fordern, dass alle Primteiler von f separabel sind.) Sei E der Zerfällungskörper von f über K. Dann nennen wir auch $\mathrm{Gal}(f, K) := \mathrm{Gal}(E/K)$ *die Galoisgruppe des Polynoms f über K.*

Beispiel 4.4.17.
Sei E Zerfällungskörper des Polynoms $f(X) = X^4 - 2$ über $\mathbb{Q}$.

1. Dann ist
$$E = \mathbb{Q}\left(\sqrt[4]{2}, \mathrm{i}\right),$$
denn sei $a := \sqrt[4]{2}$, dann sind $a, \mathrm{i}a, -a, -\mathrm{i}a$ die vier Nullstellen von f. Das Polynom f ist normiert und nach Eisenstein für $p = 2$ irreduzibel, also Minimalpolynom von a. Daher gilt:
$$[E : \mathbb{Q}] = [E : \mathbb{Q}(a)][\mathbb{Q}(a) : \mathbb{Q}] = 2 \cdot 4 = 8\,.$$
Aus der Gradformel folgt für $E = \mathbb{Q}(a, \mathrm{i})$
$$[\mathbb{Q}(a, \mathrm{i}) : \mathbb{Q}(\mathrm{i})] = 4\,,$$
also ist f auch das Minimalpolynom von a über $\mathbb{Q}(\mathrm{i})$.
Sei wie in Betrachtung 4.4.12 $\sigma \in G(E/\mathbb{Q})$ die Fortsetzung von $\mathrm{id}_{\mathbb{Q}(i)}$ auf E durch
$$\sigma(\mathrm{i}) = \mathrm{i} \qquad \sigma(a) = \mathrm{i}a\,.$$
Offensichtlich gilt $\sigma^4 = \mathrm{id}$. Sei ferner $\tau \in G(E/\mathbb{Q})$ die Fortsetzung von $\mathrm{id}_{\mathbb{Q}(a)}$ auf E durch
$$\tau(a) = a \qquad\qquad \tau(\mathrm{i}) = -\mathrm{i}\,.$$
Es ist klar, dass $\tau \notin \{1, \sigma, \sigma^2, \sigma^3\}$.
Da $|G(E/\mathbb{Q})| = [E : \mathbb{Q}] = 8$, haben wir die vollständige Galoisgruppe gefunden:
$$G(E/\mathbb{Q}) = \{1, \sigma, \sigma^2, \sigma^3, \tau, \tau\sigma, \tau\sigma^2, \tau\sigma^3\}$$
Da außerdem gilt
$$\begin{array}{rclcrcl} \tau\sigma a & = & \tau(\mathrm{i}a) & = & -\mathrm{i}a & \qquad \sigma^3\tau(a) & = & \sigma^3(a) & = & -\mathrm{i}a \\ \tau\sigma\mathrm{i} & = & \tau\mathrm{i} & = & -\mathrm{i} & \qquad \sigma^3\tau(\mathrm{i}) & = & \sigma^3(-\mathrm{i}) & = & -\mathrm{i} \end{array},$$
finden wir die folgende Relation:
$$\tau\sigma = \sigma^3\tau = \sigma^{-1}\tau\,.$$
Die Galoisgruppe $G(f, \mathbb{Q})$ ist also isomorph zur Diedergruppe D_4.

2. Wir zählen die Untergruppen von D_4 auf:

$$\begin{aligned} U_0 = \{1\} \qquad & U_1 = \{1, \sigma^2\} \\ & U_2 = \{1, \tau\},\ U_3 = \{1, \sigma\tau\},\ U_4 = \{1, \sigma^2\tau\},\ U_5 = \{1, \sigma^3\tau\} \\ & U_6 = \langle\sigma\rangle \\ & U_7 = \{1, \sigma^2, \tau, \sigma^2\tau\} \\ & U_8 = \{1, \sigma^2, \sigma\tau, \sigma^3\tau\} \\ & U_9 = D_4\,. \end{aligned}$$

Die Untergruppe U_0 ist die triviale Gruppe, die Untergruppen U_1 bis U_5 sind zyklisch der Ordnung zwei, U_6 ist zyklisch der Ordnung vier, und U_7 und U_8 sind isomorph zur Kleinschen Vierergruppe. Die Inklusionsbeziehungen von Untergruppen sind nun offensichtlich. Sie entsprechen im Unterkörperverband

$$U_i \subseteq U_j \iff F_i \supseteq F_j\,.$$

3. Wir wollen noch erklären, wie man die zugehörigen Zwischenkörper bestimmt: Sei für eine Untergruppe $U \subset G(E/K)$ die Spur über U definiert durch

$$\mathrm{Sp}_U(x) = \sum_{g\in U} gx \quad \text{für } x \in E\,.$$

Die Spur ist linear nimmt ihre Werte im Fixkörper E^U an, denn es gilt für alle $h \in U$

$$h(\mathrm{Sp}_U(x)) = \sum_{g\in U} hgx = \sum_{g\in U} gx = \mathrm{Sp}_U(x)\,.$$

Die Abbildung

$$\mathrm{Sp}_U : E \to E^U$$

ist in Charakteristik 0 surjektiv, denn sei $y \in E^U$, so ist

$$\mathrm{Sp}\left(\frac{1}{|U|}y\right) = y\,.$$

Wir können also die Unterkörper durch das Ausrechnen von Spuren bestimmen. Wir zeigen dies am Beispiel der zyklischen Untergruppe $U_5 = \{1, \sigma^3\tau\}$ der Ordnung 2:

$$\begin{aligned} \mathrm{Sp}_{U_5}(1) &= 2 \\ \mathrm{Sp}_{U_5}(\mathrm{i}) &= \mathrm{i} + \sigma^3\tau(\mathrm{i}) = \mathrm{i} - \mathrm{i} = 0 \\ \mathrm{Sp}_{U_5}(a) &= a + \sigma^3\tau(a) = a - \mathrm{i}a = \sqrt[4]{2}(1 - \mathrm{i}) \\ \mathrm{Sp}_{U_5}(\mathrm{i}a) &= \mathrm{i}a + \sigma^3\tau(\mathrm{i})\sigma^3\tau(a) = \mathrm{i}a + (-\mathrm{i})(-\mathrm{i}a) \\ &= -a(1 - \mathrm{i}) = -\sqrt[4]{2}(1 - \mathrm{i}) \end{aligned}$$

Ähnlich rechnet man weiter für die anderen Elemente der K-Basis $\{1, \mathrm{i}, a, a\mathrm{i}, a^2, a^2\mathrm{i}, a^3, a^3\mathrm{i}\}$. Damit folgt $F_5 = \mathbb{Q}\left(\sqrt[4]{2}(1 - \mathrm{i})\right)$.

Beispiel 4.4.18.
Wir wollen $\mathrm{Gal}(X^3 - 2, \mathbb{Q})$ ausrechnen. Seien $\alpha_1, \alpha_2, \alpha_3$ die Nullstellen von $X^3 - 2$ in $\mathbb{C}$. Dann ist

$$E = \mathbb{Q}\left(\sqrt[3]{2}, \zeta_3\right)$$

der Zerfällungskörper von f über $\mathbb{Q}$. Wir erhalten eine Injektion

$$\begin{aligned} \mathrm{Gal}(E/\mathbb{Q}) &\hookrightarrow \mathcal{S}_3 \\ \sigma &\mapsto \sigma(\alpha_1, \alpha_2, \alpha_3) = (\sigma\alpha_1, \sigma\alpha_2, \sigma\alpha_3) \end{aligned}$$

da σ durch seine Wirkung auf den Nullstellen α_1, α_2 und α_3 eindeutig bestimmt ist. Ferner gilt $|\mathcal{S}_3| = 3! = 6$ und

$$|\mathrm{Gal}(E/\mathbb{Q})| = [E : \mathbb{Q}] = [\mathbb{Q}\left(\sqrt[3]{2}\right) : \mathbb{Q}][E : \mathbb{Q}\left(\sqrt[3]{2}\right)] = 3 \cdot 2 = 6$$

Also ist die Injektion auch surjektiv und die Galoisgruppe ist $\mathrm{Gal}(X^3 - 2, \mathbb{Q}) \cong \mathcal{S}_3$.

Bemerkung 4.4.19.
Ist $f \in K[X]$ ein separables Polynom vom Grade n, so hat man allgemein nach Satz 4.4.6 eine Injektion

$$\mathrm{Gal}(f, K) \hookrightarrow \mathcal{S}_n$$

d.h. die Galoisgruppe $\mathrm{Gal}(f, K)$ ist isomorph zu einer Untergruppe der Permutationsgruppe $\mathcal{S}_n$. Es folgt $G(f, K) \leq (\mathrm{grad}\ f)!$.

Die Injektion muss nicht surjektiv sein: in Beispiel 4.4.17 war für das Polynom $f = X^4 - 2$ die Galoisgruppe $\mathrm{Gal}(f/\mathbb{Q}) \cong D_4$; aber es gilt $|D_4| = 8$, während $|\mathcal{S}_4| = 24$.

4.5 Einheitswurzeln und Kreisteilungskörper

Wir beginnen mit einem Nachtrag zur Eulerschen φ-Funktion:

Bemerkung 4.5.1.
Für die Eulersche φ-Funktion gilt

$$\varphi(n) = |(\mathbb{Z}/n)^\times| = |\{k \in \mathbb{N} | 1 \leq k \leq n, (k, n) = 1\}|$$

$$= \#\text{ Erzeugende Elemente von } \mathbb{Z}/n\,,$$

Die φ-Funktion ist nach Korollar 2.6.9 für teilerfremde ganze Zahlen m, n multiplikativ, $\varphi(mn) = \varphi(m)\varphi(n)$. Ferner gilt $\varphi(p^m) = p^{m-1}(p-1)$ für p prim.

Denn es gibt genau p^{m-1} Vielfache np von p mit $0 \leq n \leq p^m - 1$, also ist die Zahl von zu p^m koprimen Restklassen gleich $\varphi(p^m) = p^m - p^{m-1} = p^{m-1}(p-1)$.

Definition 4.5.2
Sei K ein Körper. Dann bezeichnet $W(K) \subset K^\times$ die Gruppe aller Elemente endlicher Ordnung in $K^\times$ und

$$W_n(K) := \{\zeta \in K \,|\, \zeta^n = 1\}$$

die Gruppe aller Elemente aus $K^\times$, deren Ordnung n teilt. Die Elemente aus $W_n(K)$ heißen n-te Einheitswurzeln von K. Ein Element $\zeta \in W_n(K)$ heißt primitive Einheitswurzel, falls ord $\zeta = n$.

Bemerkung 4.5.3.

1. Die Gruppe $W_n(K)$ ist endlich, da alle ihre Elemente Nullstellen des Polynoms $X^n - 1$ sind. Als endliche Untergruppe der Einheitengruppe $K^\times$ eines Körpers ist $W_n(K)$ nach Satz 4.2.1 zyklisch. Sei ζ ein Erzeuger von $W_n(K)$; seine Ordnung ord $(\zeta) = |W_n(K)|$ teilt dann n. Daher ist $W_n(K)$ eine endliche zyklische Gruppe, deren Ordnung n teilt.

2. Die Gruppe der komplexen Einheitswurzeln $W_n(\mathbb{C}) = \{e^{2\pi ik/n} \mid k = 0, 1, \ldots n-1\}$ hat n Elemente.

3. Ist $p = \text{char } (K) > 1$, so so folgt aus

$$\zeta^{np} = (\zeta^n)^p = 1$$

schon $\zeta^n = 1$, denn der Frobeniushomomorphismus $\sigma_p : x \mapsto x^p$ ist als Körperhomomorphismus injektiv. Es gilt also

$$W_{np}(K) = W_n(K)\,.$$

In einem Körper der Charakteristik p kann es also keine primitiven n-ten Einheitswurzeln geben, wenn n durch die Charakteristik des Körpers geteilt wird.

4. Sei C ein algebraisch abgeschlossener Körper und $n \in \mathbb{N}$. Ist char $K = p > 0$, so sei $(n, p) = 1$. Dann ist das Polynom $f(X) = X^n - 1$ in $C[X]$ separabel, da seine Ableitung $f'(X) = nX^{n-1}$ ungleich Null ist. Nach Korollar 4.3.7 hat es keine mehrfachen Nullstellen. Es folgt

$$|W_n(C)| = n\,.$$

Da die Gruppe $W_n(C)$ zyklisch ist, gibt es insbesondere eine primitive n-te Einheitswurzel in C.

Satz 4.5.4. und **Definition**
Sei K ein Körper, $n \in \mathbb{N}$. Der Zerfällungskörper E des Polynoms $X^n - 1$ über K heißt Körper der n-ten Einheitswurzeln über K. Es gilt:

1. $E = K(\zeta)$, wobei ζ eine primitive m-te Einheitswurzel ist mit

$$\begin{array}{rcll} m & = & \frac{n}{p^{w_p(n)}} & , \text{ falls } \ p = \text{char } (K) > 0 \\ m & = & n & , \text{ falls } \ \text{char } (K) = 0 \end{array}$$

2. E/K ist galoisch und es gibt eine Injektion

$$\text{Gal}(E/K) \hookrightarrow (\mathbb{Z}/m)^\times$$

Insbesondere ist die Galoisgruppe $\text{Gal}(E/K)$ abelsch.

Beweis.

- Die Behauptung in 1. ist nach Bemerkung 4.5.3 offensichtlich.

- Wegen Bemerkung 4.5.3.2 können wir annehmen, dass $(n, p) = 1$ gilt, mit $p = \text{char } K > 0$. Daraus folgt, dass das Polynom $X^n - 1$ separabel über K ist; nach Satz 4.5.7 ist die Körpererweiterung E/K galoisch ist.

- Sei $\zeta_n \in E$ eine primitive n-te Einheitswurzel, ord $(\zeta_n) = n$. Für jedes Element $\sigma \in \text{Gal}(E/K)$ hat $\sigma(\zeta_n)$ ebenfalls die Ordnung n, also gilt $\sigma\zeta_n = \zeta_n^k$ mit $(k, n) = 1$, denn nur dann ist ζ_n^k wieder primitiv. Um k eindeutig festzulegen, schreiben wir vor, dass $1 \leq k \leq n$ gilt.

  Sei $\zeta \in W_n(E)$, so ist $\zeta = \zeta_n^j$ für ein geeignetes $j \in \mathbb{Z}$. Es gilt dann

$$\sigma(\zeta) = \sigma(\zeta_n^j) = \sigma(\zeta_n)^j = (\zeta_n^k)^j = \zeta^k$$

Daher bekommen wir eine Abbildung

$$\begin{array}{ccc} \mathrm{Gal}(E/K) & \hookrightarrow & (\mathbb{Z}/n)^\times \\ \sigma & \mapsto & k \text{ mit } \sigma\zeta = \zeta^k \,. \end{array}$$

Die ist ein Gruppenhomomorphismus. Er ist injektiv, denn wegen $E = K(\zeta_n)$ ist σ schon durch die Angabe des Bildes $\sigma(\zeta_n)$ festgelegt.

□

Man beachte, dass im Falle $K = \mathbb{R}$ oder $K = \mathbb{C}$ und $n > 2$

$$\mathbb{R}(\zeta_n) = \mathbb{C} = \mathbb{C}(\zeta_n)$$

ist, also für die Galoisgruppe gilt $|\mathrm{Gal}(K(\zeta_n)/K)| = 2$ oder 1. Die obige Abbildung ist in diesem Fall also nicht surjektiv. Anders verhält sich dies für Einheitswurzeln über den rationalen Zahlen:

Satz 4.5.5 (Gauß)**.**
Sei $E = \mathbb{Q}(\zeta_n)$ mit $\zeta = \zeta_n$ einer primitiven n-ten Einheitswurzel. Dann ist die Injektion in Satz 4.5.4.2 ein Isomorphismus,

$$\mathrm{Gal}(E/\mathbb{Q}) \xrightarrow{\sim} (\mathbb{Z}/n)^\times \,.$$

Insbesondere gilt $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \varphi(n)$.

Beweis.
Zu zeigen ist, dass es zu jedem $k \in \mathbb{Z}$, das koprim zu n ist, $(k, n) = 1$, ein $\sigma \in \mathrm{Gal}(E/\mathbb{Q})$ gibt, so dass $\sigma\zeta = \zeta^k$ gilt.

- Sei $f := \min_{\mathbb{Q}}(\zeta)$ das Minimalpolynom von ζ. Es reicht aus, zu zeigen, dass auch ζ^k eine Nullstelle von f ist. Denn f ist als Minimalpoynom irreduzibel, und in char $\mathbb{Q} = 0$ separabel, so dass nach Satz 4.4.6 die Galoisgruppe transitiv auf den Nullstellen von f operiert.

- Wir reduzieren nun die Behauptung auf den Fall, dass $k = p$ eine Primzahl ist, die n nicht teilt.

  Denn ist $k = p_1^{r_1} \dots p_s^{r_s}$ ein Produkt solcher Primzahlen, so finden wir zunächst Automorphismen σ_i von $E/\mathbb{Q}$ mit

  $$\sigma_i(\zeta) = \zeta^{p_i} \,,$$

  für die dann natürlich auch

  $$\sigma_i^{r_i}(\zeta) = \zeta^{p_i^{r_i}}$$

  gilt. Wir rechnen dann nach, dass

  $$\sigma_1^{r_1} \dots \sigma_s^{r_s}(\zeta) = \zeta^{p_1^{s_1} \dots p_s^{r_s}} = \zeta^k$$

  gilt, also haben wir den gewünschten Automorphismus gefunden.

- Da ζ eine Nullstelle von $X^n - 1 \in \mathbb{Q}[X]$ ist, finden wir in $\mathbb{Q}[X]$ eine Zerlegung

  $$f(X)g(X) = X^n - 1$$

  mit $f = \min_{\mathbb{Q}}(\zeta)$ und einem normierten Polynom $g \in \mathbb{Q}[X]$. Nach dem Lemma von Gauß 3.3.11 sind $f, g \in \mathbb{Z}[X]$.

- Sei also p eine Primzahl, die n nicht teilt. Widerspruchsbeweis: Angenommen, es würde $f(\zeta^p) \neq 0$ gelten. Dann muss $g(\zeta^p) = 0$ gelten, also ist ζ Nullstelle des Polynoms $g(X^p) \in \mathbb{Z}[X]$. Dieses wird daher vom Minimalpolynom f von ζ geteilt und wir finden ein normiertes Polynom $h \in \mathbb{Q}[X]$ mit

  $$f(X)h(X) = g(X^p)\,. \qquad (*)$$

  Wiederum nach dem Lemma von Gauß 3.3.11 gilt $h \in \mathbb{Z}[X]$.

  Die Idee ist nun, modulo der Primzahl p zurechnen und die Surjektion

  $$\mathbb{Z}[X] \twoheadrightarrow \mathbb{F}_p[X]$$

  von Polynomringen durch Reduktion der Koeffizienzen modulo p auszunutzen, denn alle Polynome haben ganzzahlige Koeffizienten.

  Für

  $$\bar{g} = \sum_i \alpha_i X^i \in \mathbb{F}_p[X]$$

  gilt

  $$(\bar{g}(X))^p = \sum_i \alpha_i^p X^{ip} = \sum_i \alpha_i X^{ip} = \bar{g}(X^p)\,.$$

  Aus Gleichung $(*)$ folgt daher

  $$\bar{f}(X)\bar{h}(X) = \overline{g(X^p)} = (\bar{g}(X))^p\,.$$

  Aus ihr folgt, dass die Polynome $\bar{f}$ und $\bar{g}$ eine gemeinsame Nullstelle in einem gemeinsamen Zerfällungskörper haben. Dann hat aber das Polynom

  $$\bar{f}\bar{g} = X^n - 1 \in \mathbb{F}_p[X]$$

  in diesem Körper eine doppelte Nullstelle. Aber das Polynom $X^n - 1$ ist auch im Polynomring $\mathbb{F}_p[X]$ separabel: für seine Ableitung gilt $nX^{n-1} \neq 0$, da $(n, p) = 1$, so dass die Annahme $f(\zeta^p) \neq 0$ zum Widerspruch geführt ist.

□

Sei C eine algebraisch abgeschlossene Erweiterung von $\mathbb{Q}$, etwa $\mathbb{C}$ oder der algebraische Abschluß $\overline{\mathbb{Q}}$. Setze $W_n = W_n(C)$. Dann gilt die Zerlegung

$$X^n - 1 = \prod_{\zeta \in W_n} (X - \zeta)\,. \qquad (\clubsuit)$$

Es liegt nahe, die Linearfaktoren zu Wurzeln gleicher Ordnung zusammenzufassen. Dies motiviert die folgende

Definition 4.5.6
Das Polynom

$$F_n(X) := \prod_{\text{ord } \zeta = n} (X - \zeta)$$

heißt n-tes Kreisteilungspolynom.

Lemma 4.5.7.
Es gilt:

(i) F_n ist normiert.

(ii) grad $F_n = \varphi(n)$

(iii) $X^n - 1 = \prod_{d|n} F_d(X)$

(iv) $F_n(X) \in \mathbb{Z}[X]$.

Beweis.

(i), (ii) sind offensichtlich.

(iii) Sei $\zeta \in W_n$, dann ist $d := \text{ord } \zeta$ ein Teiler von n. Dann benutze die Zerlegung $X^n - 1 = \prod_{\zeta \in W_n}(X - \zeta)$ aus (♣).

(iv) Sei ζ_n eine primitive n-te Einheitswurzel und $\sigma \in \text{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$. Es gilt

$$F_n^\sigma(X) = \prod_{\text{ord } \zeta = n} (X - \sigma(\zeta)) = F_n(X)\,.$$

Da die Erweiterung $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ nach Satz 4.5.5 galoisch ist, heißt dies, dass alle Koeffizienten von F_n im Fixkörper $\mathbb{Q}$ liegen, $F_n^G \in \mathbb{Q}[X]$. Da außerdem $F_n(X)$ das Polynom $X^n - 1$ teilt, gibt es ein Polynom $g \in \mathbb{Q}[X]$ mit $F_n(X)g(X) = X^n - 1$. Weil die Polynome normiert sind, folgt nach dem Lemma von Gauß 3.3.11, dass $F_n(X) \in \mathbb{Z}[X]$.

□

Satz 4.5.8.
Das Kreisteilungspolynom $F_n(X)$ ist irreduzibel im Polynomring $\mathbb{Q}[X]$ über den rationalen Zahlen.

Beweis.
Sei ζ_n eine primitive n-te Einheitswurzel. Das Minimalpolynom $\min_{\mathbb{Q}}(\zeta_n)$ teilt dann das Kreisteilungspolynom F_n. Es gilt nun

$$\text{grad } \min_{\mathbb{Q}}(\zeta) \overset{1.3.10}{=} [\mathbb{Q}(\zeta) : \mathbb{Q}] \overset{4.5.5}{=} \varphi(n) \overset{4.5.7(\text{iii})}{=} \text{grad } F_n(X)\,.$$

Also gilt $\min_{\mathbb{Q}}(\zeta) = F_n$, da auch das Kreisteilungspolynom F_n normiert ist. F_n ist dann als Minimalpolynom nach Satz 1.3.15.1 irreduzibel. □

Beispiel 4.5.9.
Sei p eine Primzahl. Dann ist, wie schon in Korollar 3.3.17 gesehen, das Polynom

$$F_p(X) = \frac{X^p - 1}{X - 1} = 1 + X + \cdots + X^{p-1}$$

irreduzibel und somit nach Satz 1.3.15.2 das Minimalpolynom von ζ_p. Allgemeiner gilt für Primzahlpotenzen

$$F_{p^m}(X) = \frac{X^{p^m}-1}{X^{p^{m-1}}-1} = 1 + X^{p^{m-1}} + X^{2p^{m-1}} + \ldots + X^{(p-1)p^{m-1}},$$

denn $F_{p^m}(X)$ teilt $1+X^{p^{m-1}}+\cdots+X^{(p-1)p^{m-1}}$: jede Einheitswurzel der Ordnung p^m ist Nullstelle des Zählers, aber nicht des Nenners. Außerdem stimmen die Grade der Polynome überein:

$$\text{grad } F_{p^m} = \varphi(p^m) = p^{m-1}(p-1)\,.$$

Wir können jetzt die Konstruierbarkeit des regelmäßigen n-Ecks untersuchen: für welche natürliche Zahlen n ist $\zeta := \mathrm{e}^{2\pi\mathrm{i}/n} \in \lhd\mathbb{Q}$?

Satz 4.5.10 (Gauß)**.**
Das regelmäßige n-Eck ist genau dann mit Zirkel und Lineal konstruierbar, wenn n von der Form

$$n = 2^e p_1 \ldots p_s$$

ist, mit $e \geq 0$, p_i paarweise verschiedene Primzahlen der Gestalt

$$p_i = 1 + 2^{2^{k_i}} \quad k_i \geq 0\,.$$

Beweis.
Sei $\zeta := \mathrm{e}^{2\pi\mathrm{i}/n}$ eine n-te Einheitswurzel.

- Nach Korollar 1.1.11 muss $[\mathbb{Q}(\zeta) : \mathbb{Q}] \overset{4.5.5}{=} \varphi(n)$ eine Zweierpotenz sein, damit das regelmäßige n-Eck konstruierbar ist.
- Ist $[\mathbb{Q}(\zeta) : \mathbb{Q}]$ eine Zweierpotenz, so ist die Galoisgruppe der Galoiserweiterung $\mathbb{Q}(\zeta)/\mathbb{Q}$ eine 2-Gruppe. Nach Satz 2.11.1 gibt es eine Kette von Untergruppen

  $$\mathrm{Gal}(E/K) = H_0 \supset H_1 \supset \ldots \supset H_n = \{1\}\,,$$

  so dass H_i ein Normalteiler von $\mathrm{Gal}(E/K)$ ist und $[H_{i-1} : H_i] = 2$ ist. Nach dem Hauptsatz der Galoistheorie 4.4.15 gibt es eine Kette von Zwischenkörpern

  $$K = K_0 \subset K_1 \subset K_2 \subset \ldots \subset K_m = E\,,$$

  mit Körpergraden

  $$[K_i : K_{i-1}] = [H_{i-1} : H_i] = 2$$

  Es liegen also sukzessive quadratische Körpererweiterungen vor. Nach Satz 1.1.6 ist daher z aus $\mathbb{Q}$ konstruierbar, $z \in \lhd\mathbb{Q}$.
- Sei $n = 2^e p_1^{e_1} \ldots p_s^{e_s}$ die Primzahlzerlegung von n, wobei die p_i paarweise verschiedene ungerade Primzahlen sind. Dann ist

  $$\varphi(n) = 2^{e-1}(p_1-1)p_1^{e_1-1} \ldots (p_s-1)p_s^{e_s-1}\,.$$

  Daher ist $\varphi(n)$ genau dann Zweierpotenz, wenn n von der Form $n = 2^e p_1 \ldots p_s$ ist und für alle p_i die Zahl $p_i - 1$ eine Zweierpotenz ist.

□

Der Beweis dieses Satzes wird vervollständigt durch das folgende

Lemma 4.5.11.
Für $m \in \mathbb{N}$ ist $1 + 2^m$ höchstens dann eine Primzahl, wenn der Exponent m von der Form $m = 2^k$ für ein $k \geq 0$ ist.

Beweis.
Sei m ein Produkt $m = m_1 m_2$ mit $m_2 > 1$ einer ungeraden Zahl. Im Polynomring $\mathbb{Z}[X]$ gilt die Identität

$$(1 - X^t) = (1 - X)(1 + X + \ldots + X^{t-1}) \; .$$

Setzen wir $X := -2^{m_1}$, so finden wir mit $t = m_2$ ungerade

$$p = 1 - (-2^{m_1})^{m_2} = (1 + 2^{m_1})(1 - 2^{m_1} + 2^{2m_1} - \ldots + 2^{m_1(m_2-1)}) \, ,$$

also ist $p = 1 + 2^{m_1 m_2}$ das Produkt zweier natürlicher Zahlen größer als Eins und keine Primzahl. □

Bemerkung 4.5.12.
Für $k \in \mathbb{N} \cup \{0\}$ heißt die Zahl

$$F_k = 2^{2^k} + 1$$

k-te Fermatzahl. Die Zahlen

$$F_0 = 3 \quad F_1 = 5 \quad F_2 = 17 \quad F_3 = 257 \quad F_4 = 65537$$

sind alle Primzahlen. Fermat selbst hat behauptet, alle Fermatzahlen F_k seien prim, aber es ist heute bekannt, dass die Fermatzahlen

$$F_k \quad \text{mit} \quad 5 \leq k \leq 21$$

keine Primzahlen sind. Es ist zur Zeit keine weitere Fermat-Primzahl F_k mit $k > 4$ bekannt.

4.6 Das quadratische Reziprozitätsgesetz

Als Motivation schildern wir die folgende Fragestellung: sei $p \neq 2$ eine Primzahl und $E = \mathbb{Q}(\zeta_p)$ der p-te Kreisteilungskörper. Da die Galoisgruppe nach Satz 4.5.5 gleich

$$\mathrm{Gal}(E/\mathbb{Q}) = (\mathbb{Z}/p)^\times \; ,$$

also wegen Satz 4.2.1 zyklisch von der Ordnung $p - 1$ ist, gibt es genau eine Untergruppe vom Index 2 und somit wegen der Galois-Korrespondenz genau eine quadratische Erweiterung F der rationalen Zahlen $\mathbb{Q}$, die in diesem Kreisteilungskörper enthalten ist, $F \subseteq \mathbb{Q}(\zeta_p)$. Mit anderen Worten: es gibt genau eine quadratfreie Zahl $d \neq 1$ mit

$$\sqrt{d} \in \mathbb{Q}(\zeta_p) \, .$$

Welche Zahl ist das? – Wir werden in Antwort in Satz 4.6.4.2 geben.

Wir beginnen mit der folgenden Überlegung: betrachte den Körper $\mathbb{F}_{p^r}$ mit p^r Elementen. Seine Einheitengruppe $\mathbb{F}_{p^r}^\times$ ist nach Satz 4.2.1 zyklisch von der Ordnung $p^r - 1$, also hat die Untergruppe $\mathbb{F}_{p^r}^{\times 2}$ der Elemente von $\mathbb{F}_{p^r}^\times$, die sich als Quadrat schreiben lassen, Index zwei:

$$[\mathbb{F}_{p^r}^\times : \mathbb{F}_{p^r}^{\times 2}] = 2 \quad \text{für} \quad p^r \neq 2\,. \qquad (*)$$

Definition 4.6.1
Sei $\nu \in \mathbb{Z}$, $\nu \neq 0$. Dann setze

$$\left(\frac{\nu}{p}\right) := \begin{cases} +1 & \textit{falls} \quad \nu = x^2 \bmod p \quad \textit{für ein} \quad x \in \mathbb{Z} \\ -1 & \textit{falls} \quad \nu \neq x^2 \bmod p \quad \textit{für alle} \quad x \in \mathbb{Z} \end{cases}$$

In Worten: $\left(\frac{\nu}{p}\right) = 1$ genau dann, wenn $\nu \bmod p$ ein Quadrat in $\mathbb{F}_p^\times$ ist. $\left(\frac{\nu}{p}\right)$ heißt das Legendre-Symbol.

Das Legendre-Symbol hängt nur von der Restklasse von ν modulo p ab. Für $p \neq 2$ zeigt (*), dass die Faktorgruppe $\mathbb{F}_{p^r}^\times / \mathbb{F}_{p^r}^{\times 2}$ isomorph zu $\mathbb{Z}_2$ ist. Daraus folgt sofort

$$\left(\frac{\nu}{p}\right)\left(\frac{\mu}{p}\right) = \left(\frac{\nu\mu}{p}\right),$$

d.h.

$$\left(\frac{\cdot}{p}\right) : \left(\mathbb{Z}/p\right)^\times \to \{\pm 1\}$$

ist ein Gruppenhomomorphismus, der für $p \neq 2$ surjektiv ist.

Lemma 4.6.2.
Nach Satz 4.5.5 ist die Abbildung

$$\mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q}) \to (\mathbb{Z}/p)^\times,$$

die $\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$ das Elemente $a \in (\mathbb{Z}/p)^\times$ zuordnet, für das $\sigma(\zeta_p) = (\zeta_p)^a$ gilt, ein Isomorphismus von Gruppen. Daher ist auch die Abbildung

$$\begin{array}{rccc} \chi : & \mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q}) & \to & \{\pm 1\} \\ & \sigma & \mapsto & \left(\frac{a}{p}\right) \end{array}$$

ein Gruppenhomomorphismus.

Sei $p \neq 2$ und setze $\ker \chi =: H$. Dann ist der eindeutig bestimmte quadratische Teilkörper von $\mathbb{Q}(\zeta_p)$ gleich dem Fixkörper E^H.

Das folgende Lemma fasst elementare Eigenschaften des Legendre-Symbols zusammen:

Lemma 4.6.3 (Eulersches Kriterium)**.**
Sei $p \neq 2$ eine Primzahl. Dann gilt:

(i) $\left(\frac{\nu}{p}\right) = 1 \iff \nu^{\frac{p-1}{2}} = 1 \bmod p$

(ii) $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$

(iii) $\left(\frac{1}{p}\right) = 1$

Beweis.
Aussage (iii) folgt wegen $1^2 = 1$ aus der Multiplikativität des Legendre-Symbols. (ii) folgt als Spezialfall unmittelbar aus (i). Zum Beweis von (i) bemerken wir, dass $\left(\frac{\nu}{p}\right) = 1$ genau dann gilt, wenn $\nu \in H$ liegt. Die Untergruppe H der zyklischen Gruppe $(\mathbb{Z}/p)^\times$ von $p-1$ Elementen enthält aber genau diejenigen Elemente, deren Ordnung die ganze Zahl $\frac{p-1}{2}$ teilt. □

Satz 4.6.4.

1. Sei $\zeta = \zeta_p$ eine primitive p-te Einheitswurzel. Betrachte

$$S := \sum_{\nu \in \mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})} \chi(\sigma)\sigma(\zeta) = \sum_{\nu \in (\mathbb{Z}/p)^\times} \Big(\frac{\nu}{p}\Big)\zeta^\nu \in \mathbb{Q}(\zeta_p)\,.$$

   Dann gilt

$$S^2 = \Big(\frac{-1}{p}\Big)p = (-1)^{\frac{p-1}{2}}p =: p^* \quad \text{für} \quad p \neq 2\,.$$

2. Für $p \neq 2$ ist $\mathbb{Q}(\sqrt{p^*})$ der eindeutig bestimmte quadratische Erweiterungskörper von $\mathbb{Q}$ in $\mathbb{Q}(\zeta_p)$.

Beweis.

2. folgt unmittelbar aus 1.: da $S \in \mathbb{Q}(\zeta_p)$ liegt und $S^2 = p^*$ gilt, ist $\pm\sqrt{p^*} \in \mathbb{Q}(\zeta_p)$. Andererseits liegt $\sqrt{p^*} \notin \mathbb{Q}$, also ist $\mathbb{Q}(\sqrt{p^*})$ der gesuchte quadratische Erweiterungskörper von $\mathbb{Q}$.

1. folgt aus der folgenden Rechnung:

$$S^2 = \sum_{\nu,\mu} \Big(\frac{\nu}{p}\Big)\,\Big(\frac{\mu}{p}\Big)\zeta^{\nu+\mu} = \sum_{\nu,\mu} \Big(\frac{\nu\mu}{p}\Big)\zeta^{\nu+\mu}$$

   Ersetze nun die Summationsvariable ν durch $\mu\nu$. Läuft ν über die multiplikative Gruppe $(\mathbb{Z}/p)^\times$, so auch $\nu\mu$:

$$S^2 = \sum_{\nu,\mu} \Big(\frac{\nu\mu^2}{p}\Big)\zeta^{\nu\mu+\mu} = \sum_{\nu,\mu} \Big(\frac{\nu}{p}\Big)\zeta^{\mu(\nu+1)}\,.$$

   Wir spalten nun die Summe über ν auf, um die Identität

$$1 + \zeta + \zeta^2 + \ldots \zeta^{p-1} = 0 \qquad (*)$$

   benutzen zu können:

$$\begin{aligned} S^2 &= \sum_{\mu=1}^{p-1} \Big(\frac{-1}{p}\Big)\zeta^0 + \sum_{\nu \neq -1} \Big(\frac{\nu}{p}\Big) \sum_{\mu=1}^{p-1} \zeta^{\mu(\nu+1)} \\ &\overset{(*)}{=} \Big(\frac{-1}{p}\Big)(p-1) + \sum_{\nu \neq -1} \Big(\frac{\nu}{p}\Big)(-1) \\ &= \Big(\frac{-1}{p}\Big)p - \sum_{\nu \in (\mathbb{Z}/p)^\times} \Big(\frac{\nu}{p}\Big) = \Big(\frac{-1}{p}\Big)p\,. \end{aligned}$$

   Die letzte Gleichheit folgt, da das Legendre-Symbol genauso oft den Wert $+1$ wie den Wert -1 annimmt.

□

Bemerkung 4.6.5.
Für $p \neq 2$ gilt

$$\sigma\Big(\sqrt{p^*}\Big) = \chi(\sigma)\sqrt{p^*}$$

für alle $\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$.

Beweis.
Sei $\sigma = \sigma_a$ mit a koprim zu p, so gilt:

$$\sigma(S) = \sigma_a(S) = \sum_\nu \Big(\frac{\nu}{p}\Big)\zeta^{a\nu} = \sum_\nu \Big(\frac{\nu a^{-1}}{p}\Big)\zeta^\nu = \Big(\frac{a}{p}\Big)\sum_\nu \Big(\frac{\nu}{p}\Big)\zeta^\nu = \chi(\sigma)S\,.$$

□

Theorem 4.6.6 (quadratisches Reziprozitätsgesetz von Gauß)**.**

(i) Seien p, q zwei verschiedene Primzahlen ungleich zwei, $p, q \neq 2$ und $p \neq q$. Dann gilt

$$\Big(\frac{q}{p}\Big) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}\Big(\frac{p}{q}\Big)$$

In Worten:
Gilt $p = 1 \bmod 4$ oder $q = 1 \bmod 4$, so ist q ein quadratischer Rest modulo p genau dann, wenn p ein quadratischer Rest modulo q ist.
Gilt $p = q = 3 \bmod 4$, so ist q quadratischer Rest modulo p genau dann, wenn p *nicht* quadratischer Rest q ist.

(ii) Für $p \neq 2$ gelten die folgenden Ergänzungssätze :

$$\Big(\frac{-1}{p}\Big) = (-1)^{\frac{p-1}{2}} = \begin{cases} +1 & \text{für} \quad p = 1 \bmod 4 \\ -1 & \text{für} \quad p = 3 \bmod 4 \end{cases}$$

$$\Big(\frac{2}{p}\Big) = (-1)^{\frac{p^2-1}{8}} = \begin{cases} 1 & p = 1, -1 \bmod 8 \\ -1 & p = 3, -3 \bmod 8 \end{cases}$$

Anwendungsbeispiel: Ist 29 ein Quadrat modulo 43? Wir rechnen

$$\Big(\frac{29}{43}\Big) = \Big(\frac{43}{29}\Big) = \Big(\frac{14}{29}\Big) = \Big(\frac{2}{29}\Big)\Big(\frac{7}{29}\Big) = -\Big(\frac{7}{29}\Big) = -\Big(\frac{29}{7}\Big) = -\Big(\frac{1}{7}\Big) = -1\,,$$

also ist 29 kein Quadrat modulo 43.

Beweis.

(i) Wir rechnen im Ring $R = \mathbb{Z}[\zeta]$ mit einer p-ten Einheitswurzel $\zeta = \zeta_p$. Ein allgemeines Element dieses Ring R ist von der Form

$$\alpha = \sum_{\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})} a_\sigma \sigma(\zeta) \quad \text{mit} \quad a_\sigma \in \mathbb{Z}\,.$$

Wir rechnen nun modulo dem Hauptideal qR:

$$\sigma_q(\alpha) = \sum a_\sigma \sigma(\zeta)^q = \sum a_\sigma^q \sigma(\zeta)^q \bmod qR = \Big(\sum a_\sigma \sigma(\zeta)\Big)^q \bmod qR$$

Also gilt $\sigma_q(\alpha) = \alpha^q \bmod qR$. Setzen wir speziell $\alpha = \sqrt{p^*}$, so liefert Bemerkung 4.6.5

$$\sigma_q\Big(\sqrt{p^*}\Big) \overset{4.6.5}{=} \Big(\frac{q}{p}\Big)\sqrt{p^*} = \Big(\sqrt{p^*}\Big)^q \bmod qR\,.$$

Diese Gleichung multiplizieren wir mit $\sqrt{p^*} \in R$ und erhalten

$$\Big(\frac{q}{p}\Big)p^* = (p^*)^{\frac{q+1}{2}} \bmod qR\,.$$

Nach unseren Voraussetzungen gilt $(p^*, q) = 1$, also ist $p^* \bmod q$ invertierbar in $\mathbb{Z}/q \subseteq R/q$. Es folgt

$$\Big(\frac{q}{p}\Big) = (p^*)^{\frac{q-1}{2}} \bmod qR\,,$$

also $\Big(\frac{q}{p}\Big) - (p^*)^{\frac{q-1}{2}} \in qR \cap \mathbb{Z}$, da q ungerade sein sollte.

Ein Koeffizientenvergleich bezüglich der $\mathbb{Q}$-Basis $(1, \zeta, \zeta^2, \ldots, \zeta^{p-2})$ von $\mathbb{Q}(\zeta)/\mathbb{Q}$ zeigt, dass $q\mathbb{Z}[\zeta] \cap \mathbb{Z} = q\mathbb{Z}$ gilt. Daher folgt

$$\Big(\frac{q}{p}\Big) = (p^*)^{\frac{q-1}{2}} \bmod q\mathbb{Z} = \Big(\frac{p^*}{q}\Big) \bmod q\mathbb{Z}\ ,$$

wobei in der letzten Gleichung Lemma 4.6.3 (i) verwendet wurde. Wir finden

$$\Big(\frac{q}{p}\Big) = \Big(\frac{p^*}{q}\Big) = \Big(\frac{-1}{q}\Big)^{\frac{p-1}{2}}\Big(\frac{p}{q}\Big) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}\Big(\frac{p}{q}\Big)\,,$$

wobei in der letzten Gleichheit noch einmal $q \neq 2$ benutzt wurde.

(ii) Um die Gleichung $\Big(\frac{2}{p}\Big) = (-1)^{\frac{p^2-1}{8}}$ zu zeigen, betrachten wir den Körper $\mathbb{Q}(\zeta)$ mit $\zeta = \zeta_8 = \mathrm{e}^{2\pi\mathrm{i}/8}$ und rechnen im Ring $\mathbb{Q}(\zeta_8)$. Wegen

$$(\zeta + \zeta^{-1})^2 = \zeta^2 + 2 + \zeta^{-2} = 2 + \mathrm{i} - \mathrm{i} = 2$$

ist

$$y = \zeta + \zeta^{-1} = \sqrt{2}$$

Ferner gilt

$$y^p = \zeta^p + \zeta^{-p} \bmod p\,.$$

Ist $p = \pm 1 \bmod 8$, so gilt

$$y^p = \zeta + \zeta^{-1} = y \bmod p\,,$$

also ist $y^{p-1} = 1 \bmod p$, d.h. $2^{\frac{p-1}{2}} = 1 \bmod p$. Nach Eulers Kriterium 4.6.3 (i) folgt $\Big(\frac{2}{p}\Big) = 1$ Ist $p = \pm 5 \bmod 8$, so gilt

$$y^p = -\zeta - \zeta^{-1} = -y \bmod p\,,$$

d.h. es ist $2^{\frac{p-1}{2}} = -1 \bmod p$. Wiederum mit 4.6.3 (i) folgt $\Big(\frac{2}{p}\Big) = -1$.

□

4.7 Wurzeln und auflösbare Körpererweiterungen

Zur Vereinfachung nehmen wir in diesem Kapitel an, dass alle auftretenden Körper Charakteristik Null haben.

Definition 4.7.1

1. *Eine Galoiserweiterung mit zyklischer Galoisgruppe nennt man eine zyklische Erweiterung. Eine Galoiserweiterung mit abelscher Galoisgruppe nennt man eine abelsche Erweiterung.*

2. *Sei K ein Körper. Dann heißt das separable Polynom*

$$f(X) = X^n - \gamma \quad \in K[X]$$

für $\gamma \neq 0$ ein reines Polynom über K. Seine Nullstellen in einem Zerfällungskörper von f über K heißen n-te Wurzeln von γ.

Satz 4.7.2.
Sei K ein Körper, der eine primitive n-te Einheitswurzel enthält.

1. Sei $\gamma \in K^\times$. Dann ist die Galoisgruppe G des reinen Polynoms $X^n - \gamma$ zyklisch von einer Ordnung, die n teilt.

2. Alle zyklischen Erweiterungen von K vom Grad n entstehen durch die Adjunktion einer n-ten Wurzel.

Man beachte den Unterschied zwischen der Erweiterung eines Körpers durch n-te Einheitswurzeln und der Erweiterung eines Körpers mit n-ten Einheitswurzeln durch n-te Wurzeln aus von 1 verschiedenen Elementen: für einen Körper der Charakteristik Null ist im ersten Fall nach Satz 4.5.4 die Ordnung der Galois-Gruppe ein Teiler von $\varphi(n) = |(\mathbb{Z}/n\mathbb{Z})^\times|$, im zweiten Fall hingegen ein Teiler von n.

Beweis.

- Sei α eine feste Nullstelle von $X^n - \gamma$. Dann erhält man alle Nullstellen von $X^n - \gamma$ in der Form $\alpha\zeta$, wenn ζ alle n-ten Einheitswurzeln durchläuft. Die Einheitswurzeln liegen aber nach Annahme bereits in K. Also gilt für den Zerfällungskörper von $X^n - \gamma$, dass $E = K(\alpha)$. Diese Körpererweiterung ist als Zerfällungskörper nach Satz 4.1.11 normal und in Charakteristik Null nach Satz 4.3.1 separabel.

- Sei $\sigma \in G := \mathrm{Gal}(X^n - \gamma, K)$. Dann ist auch $\sigma\alpha$ eine Nullstelle von $X^n - \gamma$, also gilt $\sigma(\alpha) = \alpha\zeta$ mit $\zeta = \zeta(\sigma)$ einer n-ten Einheitswurzel. Wir bekommen so eine Injektion in die Gruppe $W_n(K)$ der n-ten Einheitswurzeln:

$$\begin{array}{rcl} G & \to & W_n(K) \\ \sigma & \mapsto & \frac{\sigma(\alpha)}{\alpha} =: \zeta(\sigma)\,, \end{array}$$

  denn $\zeta(\sigma) = 1$ impliziert $\sigma(\alpha) = \alpha$, also auch $\sigma = \mathrm{id}$. Dies ist ein Gruppenhomomorphismus, denn es gilt

$$\rho\sigma(\alpha) = \rho(\zeta(\sigma)\alpha) = \zeta(\sigma)\rho(\alpha) = \zeta(\sigma)\zeta(\rho)\alpha = \zeta(\rho\sigma)\alpha\,.$$

  G ist also Untergruppe der zyklischen Gruppe $W_n(K)$ der Ordnung n und daher zyklisch. Die Ordnung $|G|$ teilt n. Dies zeigt die erste Behauptung.

- Sei umgekehrt L/K eine zyklische Erweiterung vom Grad n und σ ein Erzeuger der Galoisgruppe. Dann ist $\sigma \neq \mathrm{id}_L$, es gilt $\sigma^n = \mathrm{id}_L$. Fassen wir $\sigma : L \to L$ als K-linearen Endomorphismus auf, so sind die Eigenwerte n-te Einheitswurzeln, die ja nach Annahme im Körper K liegen. Haben wir einen Eigenvektor $\alpha \in L$ zum Eigenwert ζ, also $\sigma(\alpha) = \zeta\alpha$ und einen Eigenvektor $\sigma(\beta) = \eta\beta$, so gilt $\sigma(\alpha\beta) = \zeta\eta\alpha\beta$, so dass das Produkt $\alpha\beta$ ein Eigenvektor zum Eigenwert $\zeta\eta$ ist. Die Eigenwerte bilden also eine Untergruppe $U \subset W_n(K)$.

  Wir zeigen, dass diese Untergruppe alle n-ten Einheitswurzeln enthält. Denn sonst gäbe es d, so dass σ^d nur den Eigenwert 1 hat, also von der Form wäre $\sigma^d = \mathrm{id}_L + N$ mit $N \neq 0$ nilpotent. Daraus folgt $\sigma^n = \mathrm{id} + \frac{n}{d}N \ + N^2Q(N)$ mit einem geeigneten Polynom $Q \in \mathbb{Z}[X]$. Wegen $\sigma^n = \mathrm{id}_L$ folgt daraus

  $$\frac{n}{d}N = -N^2Q(N) \ .$$

  Bilden wir Potenzen beider Seiten, so verschwindet die rechte Seite bei einer kleineren Potenz als die linke Seite.

  Es gibt also zu jeder n-ten Einheitswurzel einen Eigenvektor. Insbesondere gibt es für eine primitive n-te Einheitswurzel ζ ein Element $\alpha \in L^\times$ mit $\sigma(\alpha) = \zeta\alpha$. Es folgt, $\sigma(\alpha^i) = \sigma(\alpha)^i = \zeta^i\alpha^i$, und die Potenzen α^i sind linear unabhängig als Eigenvektoren zu paarweise verschiedenen Eigenwerten von σ. Es folgt $[K(\alpha) : K] = n$ und aus $[L : K] = n$, dass $L = K(\alpha)$.

□

Korollar 4.7.3 (Adjunktion primer Wurzeln)**.**
Sei p eine Primzahl und K ein Körper der Charakteristik Null, der alle p-ten Einheitswurzeln enthält. Genau dann ist eine echte Erweiterung von K galoisch vom Grad p, wenn sie durch Adjunktion einer p-ten Wurzel entsteht.

Beweis.
Eine Galoiserweiterung von Primzahlordnung ist nach Bemerkung 2.5.3.4 zyklisch. Das Korollar folgt nun aus Satz 4.7.2. □

Satz 4.7.4 (Translationssatz der Galoistheorie)**.**
Seien in einem Körper E zwei Teilkörper K, L gegeben und KL das Kompositum von K und L, vgl. Definition 1.2.7. Ist nun $K \cap L \subset K$ eine Galoiserweiterung, so ist KL/L eine Galoiserweiterung und die Restriktion definiert einen Isomorphismus der Galoisgruppen

$$\mathrm{Gal}(KL/L) \xrightarrow{\sim} \mathrm{Gal}(K/K \cap L) \ .$$

(Insbesondere gilt $[K : K \cap L] = [KL : L]$.)

Beweis.
Wir zeigen die Aussage nur für endliche Erweiterungen und verzichten hier auf die Annahme, dass die Körper Charakteristik Null haben.

- K wird über $K \cap L$ von separablen Elementen $\alpha_1, \alpha_2, \ldots \alpha_r$ erzeugt. Also hat $\min_{K\cap L}(\alpha_i)$ nur einfache Nullstellen. Da $\min_L(\alpha_i)$ das Polynom $\min_{K\cap L}(\alpha_i)$ teilt, kann es auch nur einfache Nullstellen haben, also sind die Elemente $\alpha_1, \alpha_2, \ldots \alpha_r$ auch über L separabel. Diese Elemente erzeugen auch das Kompositum LK über L. Da $K/K \cap L$ normal ist, ist es Zerfällungskörper eines Polynoms $f \in (K \cap L)[X]$. Dann ist aber das Kompositum KL Zerfällungskörper des gleichen Polynoms, aufgefasst als Element im Polynomring $L[X]$.

- Im Körperturm $LK \supset K \supset K \cap L$ ist die untere Erweiterung $K/K \cap L$ nach Annahme normal. Im Beweis des Hauptsatzes 4.4.9.3 haben wir gesehen, dass dann alle Körperautomorphismen von KL den Unterkörper K stabilisieren und dass die Restriktion

$$\begin{array}{ccc} \mathrm{Gal}(KL/K \cap L) & \to & \mathrm{Gal}(K/K \cap L) \\ \sigma & \mapsto & \sigma|_K \end{array}$$

  surjektiv ist. Schränkt man diese Abbildung auf die Untergruppe $\mathrm{Gal}(KL/L) \subset \mathrm{Gal}(KL/K \cap L)$ ein, so ist der Fixkörper des Bildes genau $K \cap L$, was die Bijektivität im Fall endlicher Erweiterungen zeigt.

□

Definition 4.7.5

1. *Sei F/K eine Körpererweiterung. Man sagt, F entstehe aus K durch sukzessive Adjunktion von Radikalen der Exponenten $n_1, \ldots n_r$, wenn es eine Kette*

$$K = K_0 \subseteq K_1 \subseteq \cdots \subseteq K_r = F$$

   von Zwischenkörpern K_i von F/K gibt, so dass K_i aus K_{i-1} durch Adjunktion einer n_i-ten Wurzel (auch ein Radikal vom Exponenten n_i genannt) entsteht. F/K heißt dann Radikalerweiterung.

2. *Eine Körpererweiterung E/K heißt durch Radikale (der sukzessiven Exponenten n_i) auflösbar, wenn es eine Radikalerweiterung F/K (der sukzessiven Exponenten n_i) gibt mit $E \subseteq F$.*

3. *Ein Polynom $f \in K[X]$ bzw. die polynomiale Gleichung $f(X) = 0$ heißt durch Radikale auflösbar, wenn es eine Körpererweiterung E/K gibt, die durch Radikale auflösbar ist, und f über E in Linearfaktoren zerfällt.*

Satz 4.7.6.
Sei weiterhin K ein Körper der Charakteristik 0. Sei $f \in K[X]$. Dann sind äquivalent:

1. Die Gleichung $f(X) = 0$ lässt sich durch Radikale auflösen.

2. Die Galoisgruppe des Zerfällungskörpers E von f über K ist eine auflösbare Gruppe.

Dies folgt sofort aus dem folgenden Satz:

Satz 4.7.7.
Sei K ein Körper der Charakteristik 0 und L/K eine Körpererweiterung von K. Dann sind äquivalent:

1. Die Erweiterung L lässt sich in eine Radikalerweiterung von K einbetten.

2. Die Erweiterung L lässt sich einbetten in eine endliche Galoiserweiterung von K mit auflösbarer Galoisgruppe.

Beweis.

2.⇒ 1. Sei ohne Beschränkung der Allgemeinheit L/K eine endliche Galoiserweiterung mit auflösbarer Galoisgruppe $G = \mathrm{Gal}(L/K)$. Nach Definition gibt es eine Folge von Untergruppen

$$G = G_0 \supset G_1 \supset G_2 \ldots \supset G_r = 1$$

mit G_i normal in G_{i-1} und G_{i-1}/G_i zyklisch von Primzahlordnung für alle $1 \leq i \leq r$. Die zugehörige Kette von Fixkörpern ist eine Kette von zyklischen Erweiterungen von Primzahlordnung

$$K = K_0 \subset K_1 \subset \ldots \subset K_r = L \ .$$

Adjungieren wir eine primitive $|G|$-te Einheitswurzel ζ, so erhalten wir nach dem Translationssatz 4.7.4 wieder eine Kette

$$K = K_0 \subset K(\zeta) \subset K_1(\zeta) \subset \ldots \subset K_r(\zeta) = L(\zeta)$$

von zyklischer Galoiserweiterungen von Primzahlordnung. Nach dem Satz über die Adjunktion primer Wurzeln 4.7.3 entsteht jede Stufe durch Adjunktion eine geeigneten Wurzel aus der vorherigen Stufe. Also lässt sich L in eine Radikalerweiterung von K einbetten, nämlich in die Radikalerweiterung $L(\zeta)$.

1.⇒ 2. Sei ohne Beschränkung der Allgemeinheit L/K eine Radikalerweiterung. Offensichtlich können wir L auch erhalten, indem wir sukzessive Wurzeln $\sqrt[p]{a_i}$ von Primzahlordnung für geeignete Primzahlen p adjungieren. Es gibt also eine Körperkette

$$K = K_0 \subset K_1 \subset \ldots \subset K_r = L$$

sowie geeignete $\alpha_i \in K_i$ und Primzahlen p_i derart, dass für alle $i \geq 1$ gilt $K_i = K_{i-1}(\alpha_i)$ und $\alpha_i^{p_1} \in K_{i-1}$. Ist n das Produkt dieser p_i und adjungieren wir zu L eine n-te Einheitswurzel ζ, so ist im Körperturm

$$K = K_0 \subset K(\zeta) \subset K_1(\zeta) \subset \ldots \subset K_r(\zeta) = L(\zeta)$$

jeder Schritt eine abelsche Erweiterung. Vergrößern wir nun $L(\zeta)$ zu einer normalen Erweiterung N/K und betrachten das Kompositum $\tilde{L} \subset N$ aller $\varphi(K(\zeta))$ mit $\varphi \in \mathrm{Alg}_K(L(\zeta), N)$, so ist $\tilde{L}$ eine Galoiserweiterung von K und es gibt einen Körperturm

$$K = \tilde{L}_0 \subset \tilde{L}_1 \subset \tilde{L}_2 \subset \ldots \subset \tilde{L}_t = \tilde{L} \ ,$$

in dem jede Stufe eine abelsche Erweiterung ist. Die Galoiskorrespondenz zeigt dann, dass die Galoisgruppe $\mathrm{Gal}(\tilde{L}/K)$ auflösbar ist.

□

Diese Sätze geben eine befriedigende Antwort auf die Frage, für welche Polynome $f \in K[X]$ die Nullstellen durch sukzessives Wurzelziehen ausgedrückt werden können.

Wir wenden uns zwei weiteren Fragen zu:

- Gibt es allgemeine Auflösungsformeln für *alle* Polynome eines gegebenen Grades? Wir denken hierbei an Verallgemeinerungen der aus der Schule bekannten Formeln für die Nullstellen des quadratischen Polynoms $X^2 + pX + q$, dessen Koeffizienten die Variable p, q sind.
- Welche endlichen Gruppen können als Galoisgruppen von galoischen Erweiterungen auftreten?

Unser Leitgedanke ist, die Koeffizienten des zu untersuchenden Polynoms variabel zu lassen. Wir untersuchen daher den Fall,dass die Koeffizienten des Polynoms im Körper

$$k(X_1, \ldots, X_n) = \text{Quot } (k[X_1, \ldots, X_n]) = \left\{ \frac{g_1}{g_2} \;\middle|\; g_1, g_2 \in k[X_1, \ldots, X_n], g_2 \neq 0 \right\}$$

der rationalen Funktionen in n Variablen $X_1 \ldots, X_n$ über k, vgl. Bemerkung 3.1.3.4, liegen.

Definition 4.7.8
Die Polynome $s_i = s_i(X_1, \ldots, X_n) \in k[X_1, \ldots X_n]$

$$\begin{aligned} s_1 &= X_1 + \ldots + X_n \\ s_2 &= X_1X_2 + X_1X_3 + \ldots + X_1X_n + X_2X_3 + \ldots + X_{n-1}X_n \\ s_3 &= X_1X_2X_3 + \ldots \\ s_n &= X_1X_2X_3 \ldots X_n \end{aligned}$$

heißen i-te elementarsymmetrische Funktion in den Variablen $X_1, \ldots, X_n$.

Es gilt im Polynomring $k(X_1, \ldots X_n)[X]$ über dem Körper $k(X_1, \ldots X_n)$

$$f(X) = \prod_{i=1}^{n}(X - X_i) = X^n - s_1X^{n-1} + s_2X^{n-2} - \ldots (-1)^n s_n \,. \qquad (\heartsuit)$$

Satz 4.7.9.
Die Körpererweiterung $k(X_1, \ldots, X_n)/k(s_1 \ldots, s_n)$ ist galoisch mit Galoisgruppe $\mathcal{S}_n$.

Die Permutationsgruppe $\mathcal{S}_n$ kommt also als Galoisgruppe einer Körpererweiterung vor. Nach dem Satz von Cayley 2.7.1 ist jede Gruppe isomorph zu einer Gruppe von Permutationen und tritt somit als Galoisgruppe auf. Unbekannt ist, ob jede Gruppe als Galoisgruppe mit vorgegebenen Grundkörper auftritt. (Umkehrproblem der Galoistheorie). Es ist aber bekannt (Safarevič), dass jede endliche auflösbare Gruppe Galoisgruppe einer Erweiterung von $\mathbb{Q}$ ist.

Beweis.

- Für eine Permutation $\sigma \in \mathcal{S}_n$ setze $\sigma h(X_1, \ldots, X_n) := h(X_{\sigma(1)}, \ldots, X_{\sigma(n)})$. Dann ist

$$\begin{array}{ccc} k[X_1, \ldots, X_n] & \to & k[X_1, \ldots, X_n] \\ h & \mapsto & \sigma h \end{array}$$

ist ein Isomorphismus von k-Algebren, der sich eindeutig auf den Quotientenkörper $k(X_1, \ldots, X_n)$ fortsetzen lässt. Dies definiert eine Operation von $\mathcal{S}_n$ auf dem Polynomring $k[X_1, \ldots, X_n]$ und seinem Quotientenkörper $F := k(X_1, \ldots, X_n)$.

- Wir fassen die symmetrische Gruppe $\mathcal{S}_n$ als Untergruppe der Galoisgruppe $\mathrm{Gal}(F/k)$ auf. Nun operiert $\mathcal{S}_n$ durch Operation auf den Koeffizienten auf dem Polynomring $F[X]$. Wir finden für $\sigma \in \mathcal{S}_n$ und das Polynom f aus (♡)

$$\sigma f = \prod_{i=1}^{n}(X - X_{\sigma i}) = \prod_{i=1}^{n}(X - X_i) = f\,.$$

  Also liegen die Koeffizienten von f im Fixkörper

$$F^{\mathcal{S}_n} = k(X_1, \ldots, X_n)^{\mathcal{S}_n}\,.$$

- Andererseits können wir f auch als Polynom mit Koeffizienten im Körper $k(s_1, \ldots, s_n)$ auffassen. Der rationale Funktionenkörper $k(X_1, \ldots, X_n)$ ist der Zerfällungskörper des separablen Polynoms f über $k(s_1, \ldots, s_n)$. Also ist die Körpererweiterung $k(X_1, \ldots, X_n)/k(s_1, \ldots, s_n)$ galoisch.

- Es gilt

$$\mathrm{Gal}(k(X_1, \ldots, X_n)/k(s_1 \ldots, s_n)) \cong \mathcal{S}_n\,.$$

  Denn jedes Element σ der Galoisgruppe bewirkt nach Satz 4.4.6 eine Permutation der Nullstellen von f und jede Permutation aus $\mathcal{S}_n$ ist umgekehrt ein Element der Galoisgruppe. Also kommt die Permutationsgruppe $\mathcal{S}_n$ als Galoisgruppe einer Körpererweiterung vor.

□

Korollar 4.7.10.

1. Eine rationale Funktion $r \in k(X_1, \ldots, X_n)$ ist genau dann symmetrisch, d.h. es gilt $\sigma r = r$ für alle $\sigma \in \mathcal{S}_n$, wenn r eine rationale Funktion in den elementarsymmetrischen Funktionen s_i aus Definition 4.7.8 ist, also wenn $r \in k(s_1, \ldots, s_n)$.

2. Das Polynom $f = \prod_{i=1}^{n}(X - X_i)$ aus (♡) ist irreduzibel über $k(s_1 \ldots, s_n)$.

Beweis.

1. Eine rationale Funktion $r \in k(X_1, \ldots, X_n)$ ist genau dann symmetrisch, wenn $r \in k(X_1, \ldots, X_n)^{\mathcal{S}_n} = k(s_1, \ldots, s_n)$. Die letzte Gleichheit gilt, weil nach Satz 4.7.9 die Körpererweiterung $k(X_1, \ldots, X_n)/k(s_1, \ldots, s_n)$ galoisch ist.

2. Da die Permutationsgruppe $\mathcal{S}_n$ transitiv auf den Nullstellen des separablen Polynoms f operiert, können wir Satz 4.4.6 anwenden, um f als Minimalpolynom zu erkennen.

□

Jetzt haben wir die Hilfsmittel bereit, um Variablen in den Koeffizienten eines Polynoms in X zu behandeln.

Definition 4.7.11

Sei k ein Körper und $K = k(u_1, \ldots, u_n)$ der rationale Funktionenkörper über k in n Variablen. Das Polynom

$$g(X) = X^n - u_1 X^{n-1} + u_2 X^{n-2} - \ldots (-1)^n u_n \in K[X]$$

heißt das allgemeine Polynom n-ten Grades über k.

Satz 4.7.12.
Das allgemeine Polynom n-ten Grades über k ist separabel. Es ist irreduzibel über dem Körper $K = k(u_1, \ldots, u_n)$ seiner Koeffizienten. Seine Galoisgruppe heißt Galoisgruppe der allgemeinen Gleichung n-ten Grades über k und ist isomorph zur Permutationsgruppe $\mathcal{S}_n$.

Beweis.

- Sei E der Zerfällungskörper des allgemeinen Polynoms g aus Definition 4.7.11 über $K = k(u_1, \ldots, u_n)$:
$$g(X) = \prod_{i=1}^{n}(X - x_i) \in E[X] \quad \text{mit} \quad x_i \in E\,.$$
Dann ist
$$E = K(x_1, \ldots, x_n) = k(x_1, \ldots, x_n)$$
da $u_i := s_i(x_1, \ldots, x_n)$ schon im Körper $k(x_1, \ldots, x_n)$ liegt.

- Kern des Beweises ist es, zu zeigen, dass der Zerfällungskörper E isomorph ist zum rationalen Funktionenkörper über k in n Variablen. Dazu betrachten wir den Polynomring $k[X_1, \ldots, X_n]$. Sei
$$\varphi: \quad k[X_1, \ldots, X_n] \to k[x_1, \ldots, x_n]$$
der durch Einsetzen $\varphi(X_i) = x_i$ eindeutig bestimmte k-Algebrenhomomorphismus. Für diesen Homomorphismus gilt
$$s_i = s_i(X_1, \ldots, X_n) \mapsto s_i(x_1, \ldots, x_n) = u_i\,.$$
Durch Restriktion erhalten wir einen k-Algebrenhomomorphismus
$$\tilde{\varphi}: \qquad k[s_1, \ldots, s_n] \xrightarrow{\sim} k[u_1, \ldots, u_n]\,,$$
der die Umkehrabbildung $u_i \mapsto s_i$ hat, also ein Isomorphismus ist. Er induziert einen Isomorphismus der Quotientenkörper:
$$\tilde{\varphi} : K' := k(s_1, \ldots, s_n) \xrightarrow{\sim} K = k(u_1, \ldots, u_n)\,.$$

- Wir behaupten, dass auch $\varphi : k[X_1, \ldots, X_n] \to k[x_1, \ldots, x_n]$ ein Ringisomorphismus ist. Surjektivität ist klar, sei also $h \in k[X_1, \ldots, X_n]$ mit der Eigenschaft, dass Einsetzen der $x_i \in E$ in h Null ergibt, $h(x_1, \ldots, x_n) = 0$. Betrachte das Polynom
$$N(h) := \prod_{\sigma \in \mathcal{S}_n} \sigma h = h \prod_{\sigma \neq e} \sigma h \;\in\; k[X_1, \ldots, X_n]$$
Sicher ist $N(h)^\sigma = N(h)$ für alle $\sigma \in \mathcal{S}_n$, also ist $N(h) \in k(s_1, \ldots, s_n)$. Da $h \in \ker\varphi$, ist auch $N(h) \in \ker\varphi$. Da aber $\tilde{\varphi} = \varphi|_{K'}$ ein Isomorphismus ist, folgt $N(h) = 0$ und daraus $h = 0$. Also haben wir die Injektivität von φ gezeigt. Insbesondere sind die Nullstellen $x_i \in E$ von g paarweise verschieden und das Polynom g ist separabel.

- Setze nun φ zu einem eindeutigen Isomorphismus $\tilde{\varphi}$ der Quotientenkörper fort:
$$\begin{array}{ccc} k(X_1, \ldots, X_n) & \xrightarrow{\quad\varphi\quad} & k(x_1, \ldots, x_n) = E \\ \uparrow & & \uparrow \\ K' = k(s_1, \ldots, s_n) & \xrightarrow{\quad\tilde{\varphi}\quad} & k(u_1, \ldots, u_n) = K \end{array}$$

Unter φ geht das Polynom $f = \prod_{i=1}^{n}(X - X_i)$ aus ($\heartsuit$) über dem Körper $k(X_1, \ldots X_n)$ auf das allgemeine Polynom g, i.e. $\varphi(f) = g$. Wegen Korollar 4.7.10 ist dann das Polynom g irreduzibel und wegen Satz 4.7.9 ist die Galoisgruppe

$$\text{Gal}\,(g, k(u_1, \ldots, u_n)) \cong \mathcal{S}_n\,.$$

□

Satz 4.7.13 (Abel)**.**
Das allgemeine Polynom n-ten Grades ist für $n \geq 5$ nicht durch Radikale auflösbar.

Beweis.
Nach Satz 4.7.12 ist die Galoisgruppe des Polynoms die symmetrische Gruppe $\mathcal{S}_n$, die nach Bemerkung 2.12.6.2 für $n \geq 5$ nicht auflösbar ist. Die Behauptung folgt nun aus Satz 4.7.7. □

Satz 4.7.14.
Sei k ein Körper der Charakteristik Null. Dann ist jedes Polynom $f \in K[X]$ vom Grad $n \leq 4$ durch Radikale auflösbar.

Beweis.
Die Galoisgruppe ist als Untergruppe der auflösbaren Gruppe $\mathcal{S}_4$ auflösbar. □

Literatur

[Jantzen-Schwermer] J.C. Jantzen, J. Schwermer, *Algebra*, Springer 2006

Index