# V2A1 – Einführung in die Algebra

## Galoistheorie

Dozent:
Prof. Dr. Daniel Huybrechts

Mitschriften von:
Tien Nguyen Thanh

Wintersemester 2023/2024
Stand: 21. März 2024

*Haftungsausschluss:* Das sind meine persönlichen Mitschriften aus der Vorlesung und hängen in keiner Weise mit der Dozent*in als Person oder der Universität zusammen. Die Mitschriften basieren zwar auf der Vorlesung der Dozent*in, wurden aber mehrfach von mir und mithilfe anderer Quellen (Personen, Bücher, Internet, Tutorien) überarbeitet, sodass sie nur in ferner bis keiner Weise die Vorlesung widerspiegeln. Trotz großer Sorgfalt bei der Erstellung der Mitschriften sind alle Angaben ohne Gewähr und Anspruch auf Vollständigkeit.

*Anmerkung:* Die mit einem Stern markierten Inhalte (wie z. B. *Bemerkung**) und Fußnoten sind von mir hinzugefügt worden und stammen nicht aus der Vorlesung.

## Inhaltsverzeichnis

**Updates** Da ich jeden Montag nicht zur Vorlesung kann, werden die Mitschriften womöglich nicht immer vollständig sein. Zudem werde ich sie nach Lust und Laune aktualisieren.

22.01.2024: Sorry für die lange Update-Pause. Ich war mit Topologie lernen beschäftigt, werde aber nun das Skript so bald wie möglich aktualisieren.

**Feedback** Für Anmerkungen und Fehler aller Art bin ich offen. Ihr könnt mich persönlich ansprechen, mir per Signal/WhatsApp schreiben (falls ihr meine Nummer habt), und mir an tien.nguyen@uni-bonn.de eine E-Mail schreiben.

**Nutzung** Die Vorlesungsinhalte werden (bis auf ein Epsilon) ziemlich getreu wiedergegeben. Die einzigen Inhalte, die ich selbst hinzugefügt habe, sind die Unterabschnitte *Notizen**, die meines Erachtens nach nennenswerte Fakten aus meinem Tutorium enthalten, und die Fußnoten, welche als Kommentare und Ergänzung der Vorlesungsinhalte dienen.

Die PDF ist mit internen Hyperlinks ausgestattet, auf die ihr klicken könnt. Ihr erkennt das daran, dass der Text farbig ist. Zudem gibt es ein automatisch generiertes Stichwortverzeichnis am Ende des Dokuments. Die Qualität der Stichwörter ist dementsprechend nicht sehr gut, hilft aber bereits beim Nachschlagen.

**Literatur** Folgende Literatur kann hilfreich sein:

[ArM] Artin, Michael: *Algebra.* Birkhäuser, Babel 1998.

[Bos] Bosch, Siegfried: *Algebra.* Springer, Berlin 2023, 10. Auflg.[1]

[Sch] Schröer, Jan: *Einführung in die Algebra.* Vorlesungsskript, Bonn, Wintersemester 2022/23. Zu finden auf eCampus.

[St1] Stix, Jacob: *Grundlagen der Algebra.* Vorlesungsskript, Frankfurt, Sommersemester 2019. Online auf https://www.uni-frankfurt.de/115671781/stix-grundlagenalgebra-skript2019.pdf.

[St2] Stix, Jacob: *Algebra.* Vorlesungsskript, Frankfurt, Wintersemester 2019/2020. Online auf https://www.uni-frankfurt.de/115677802/stix-algebra-skriptws2020.pdf.

[1] Mein Lieblingsbuch zur Galoistheorie und grundlegenden Algebra. Sehr umfassend und gut lesbar.

Hier weitere Nachschlagewerke, primär auf Englisch.

[Tig] Tignol, Jean-Pierre: *Galois' Theory of Algebraic Equations.* World Scientific, New Jersey 2016, 2. Auflg. Auf Englisch.

[Lan] Lang, Serge: *Algebra.* Springer, New York 2002. Auf Englisch.

[Kun] Kunz, Ernst: *Algebra.* Vieweg, Wiesbaden 1991.

[Kna] Knapp, Anthony W.: *Basic algebra.* Birkhäuser, Boston 2006, 1. Auflg. Auf Englisch. 2. Auflg. online auf https://www.math.stonybrook.edu/~aknapp/download/b2-alg-coverandinside.pdf.

[ArE] Artin, Emil: *Galois theory.* Dover, New York 1998, 2. Auflg. Auf Englisch.

Hier weitere Quellen von mir.

[MSE] Long: *Counter example of Zorn's lemma when we only take countable chains.* Math Stack Exchange Post, online auf https://math.stackexchange.com/questions/539052.

[Gil] Gilmer, Robert: *A Note on the Algebraic Closure of a Field.* In: The American Mathematical Monthly **75**(10), 1968, 1101–1102.

**Danksagung** Vielen Dank an Laurens Peter und Alexander Fuhs für ihre Mitschriften jeden Montag. Danke auch an Yang Zhang für die Inhalte aus unserem Tutorium. Zuletzt bedanke ich mich für Korrekturvorschläge (in chronologischer Reihenfolge) bei Juri Kaganskiy, Alexander Fuhs, Leon Karlson und Can Matthias Bieber.

# 1 Gruppentheorie

VL 1
09.10.23

## 1.1 Gruppen, Homomorphismen, Untergruppen

Die folgenden Begriffen sollten aus der linearen Algebra bekannt sein.

def:group

**Definition 1.1.1.** Eine **Gruppe** besteht aus einer Menge $G$ und einer Abbildung

$$G \times G \longrightarrow G, \qquad (a, b) \longmapsto ab \coloneqq a \cdot b,$$

sodass:

(i) **Assoziativität**: $a(bc) = (ab)c$ für alle $a, b, c \in G$.

def:group:2 (ii) **Einheit** oder **Einselement**: Es existiert ein $e \in G$, sodass $ea = ae = a$ für alle $a \in G$. Insbesondere ist $G \neq \varnothing$.

def:group:3 (iii) **Inverse**: Für alle $a \in G$ gibt es ein $a^{-1} \in G$, sodass $aa^{-1} = a^{-1}a = e$.

$G$ heißt **albelsch** oder **kommutativ**, falls $ab = ba$ für alle $a, b \in G$.

Nils Hendrich Abel (1802-1829) ist neben Galois ein Mitbegründer der Galois-und Gruppentheorie. Diese Theorie zeigt, dass alle Polynome vom Grad mindestens fünf nicht auflösbar sind. Seit 2003 gibt es den *Abel Prize* (dotiert mit ca. 750 000 €). Gewinner sind unter anderem Serre, Atiyah, Deligne, usw.

**Notation 1.1.2.** Manchmal schreiben wir die Gruppenstruktur auch additiv, also eine Abbildung $G \times G \to G$, $(a,b) \mapsto a+b$.[2] Ferner schreiben wir

$$a^n := \begin{cases} \underbrace{a \cdots a}_{n \text{ mal}}, & \text{falls } n > 0, \\ (\underbrace{a \cdots a}_{-n \text{ mal}})^{-1}, & \text{falls } n < 0, \end{cases}$$

und $a^0 := e$. Statt $e$ schreiben wir auch 1.

**Fakt 1.1.3.** *Sei $G$ eine Gruppe, und seien $a,b,c \in G$. Dann gelten folgende Aussagen:*

(i) *$a^{-1}$ ist eindeutig.*

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

(iii) $(a^{-1})^{-1} = a$.

(iv) *Aus $ab = ac$ folgt $b = c$. Insbesondere impliziert $aa = a$ dann $a = e$.*

*Beweis.*

(i) Falls $ab = e$, dann $b = eb = (a^{-1}a)b = a^{-1}(ab) = a^{-1}e = a^{-1}$.

(ii) Wir müssen zeigen, dass $(ab)(b^{-1}a^{-1}) = e$. Die linke Seite ist $a(bb^{-1})a = aea^{-1} = aa^{-1} = e$.

(iii) Das folgt aus der Eindeutigkeit von Inversen.

(iv) Multiplikation von links mit $a^{-1}$ ergibt

$$b = eb = (a^{-1}a)b = a^{-1}(ab) = a^{-1}(ac) = (a^{-1}a)c = ec = c. \qquad \square$$

**Aufgabe 1.1.4.** Statt die Bedingungen (ii) und (iii) in Definition 1.1.1 zu fordern, genügt es, die folgenden schwächeren Bedingungen zu fordern:

itm:group:alt:2 (ii') Es gibt ein $e \in G$, sodass $ea = e$ für alle $a \in G$.

itm:group:alt:3 (iii') Für alle $a \in G$ gibt es ein $a^{-1} \in G$, sodass $a^{-1}a = e$.

*Lösung.* Dass (ii) und (iii) die Bedingungen (ii') und (iii') implizieren, ist klar. Für die Rückrichtung haben wir

$$\begin{aligned} aa^{-1} &= eaa^{-1} = ((a^{-1})^{-1}a^{-1})(aa^{-1}) = (a^{-1})^{-1}(a^{-1}a)a^{-1} \\ &= (a^{-1})^{-1}ea^{-1} = (a^{-1})^{-1}a^{-1} = e \end{aligned}$$

[2] Das vor allem für abelsche Gruppen $G$. In diesem Fall sind Inverse $-a$ und die Einheit ist 0.

und $ae = a(a^{-1}a) = (aa^{-1})a = ea = a$ für alle $a \in G$. Somit implizieren (ii') und (iii') die Bedingungen (ii) und (iii).

**Definition 1.1.5.** Eine Teilmenge $H \subset G$ einer Gruppe $G$ heißt **Untergruppe**, falls $e \in H$ und $ab, a^{-1} \in H$ für alle $a, b \in H$. Mit der Einschränkung von $\cdot\colon G \times G \to G$ auf $H \times H$ wird $H$ selbst zur Gruppe.

**Definition 1.1.6.** Eine Abbildung $\varphi\colon G_1 \to G_2$ zwischen zwei Gruppen $G_1$ und $G_2$ heißt **Gruppenhomomorphismus**, falls

$$\varphi(ab) = \varphi(a)\varphi(b)$$

für alle $a, b \in G_1$.

**Fakt 1.1.7.** *Sei $\varphi\colon G_1 \to G_2$ ein Gruppenhomomorphismus. Dann gilt $\varphi(e_1) = e_2$, wobei $e_i \in G_i$ die jeweiligen Einheiten sind.*

*Beweis.* $\varphi(e_1)\varphi(e_1) = \varphi(e_1e_1) = \varphi(e_1) = \varphi(e_1)e_2$, woraus $\varphi(e_1) = e_2$ folgt. □

**Aufgabe 1.1.8.** Sei $\varphi\colon G_1 \to G_2$ ein Gruppenhomomorphismus. Dann gilt $\varphi(a^{-1}) = \varphi(a)^{-1}$ für alle $a \in G_1$.

*Lösung.* $\varphi(a)\varphi(a^{-1}) = \varphi(aa^{-1}) = \varphi(e_1) = e_2 = \varphi(a)\varphi(a)^{-1}$, woraus $\varphi(a^{-1}) = \varphi(a)^{-1}$ folgt.

**Definition 1.1.9.** Ein Gruppenhomomorphismus $\varphi\colon G_1 \to G_2$ ist ein **Gruppenisomorphismus**, falls $\varphi$ bijektiv ist. In diesem Fall ist auch $\varphi^{-1}\colon G_2 \to G_1$ ein Gruppenisomorphismus. $G_1$ und $G_2$ heißen dann **isomorph**.

*Beispiel* 1.1.10.

(i) Die **triviale Gruppe** $G = \{e\}$ ist eine Gruppe. Bis auf Isomorphie gibt es auch nur eine triviale Gruppe. So sind z. B. $\mathbb{Z}/\mathbb{Z}$, $\{0\} \subset \mathbb{Z}$, etc. alle trivial.

(ii) $(\mathbb{Z}, +)$ ist eine Gruppe. $(\mathbb{Q}, +)$ und allgemeiner $(K, +)$ für Körper $K$ sind Gruppen. Für $K$-Vektorräume $V$ ist $(V, +)$ eine Gruppe.

(iii) $(\mathbb{N}, +)$ ist keine Gruppe (für $a \in \mathbb{N}$ ist im Allgemeinen $a^{-1} \notin \mathbb{N}$).

(iv) $(\mathbb{Q}^*, \cdot)$, $(\mathbb{R}^*, \cdot)$ und allgemeiner $(K^*, \cdot)$ mit $K^* \coloneqq K \setminus \{0\}$ sind alles Gruppen.

(v) $(\mathbb{Z} \setminus \{0\}, \cdot)$ ist keine Gruppe. $(\mathbb{Z}/2\mathbb{Z}, +) \simeq (\{\pm 1\}, \cdot)$ ist eine Untergruppe von $(\mathbb{Q}^*, \cdot)$.

Die obigen Gruppen sind alle abelsch.

(vi) Sei $M$ eine beliebige Menge. Dann ist

$$G = \mathrm{Bij}(M) \coloneqq \{\varphi\colon M \longrightarrow M \text{ bijektiv}\}$$

mit der Komposition eine Gruppe. Für $|M| > 2$ ist $G$ nicht abelsch.

(vii) Als Spezialfall gibt es die **symmetrische Gruppe**

$$S_n \coloneqq \mathfrak{S}_n \coloneqq \mathrm{Bij}(\{1,\dots,n\})$$

(vgl. Definition 1.6.1). Die Abbildung $\mathrm{sgn}\colon S_n \to \{\pm 1\}$, die das Vorzeichen angibt, ist ein Gruppenhomomorphismus. Die **alternierende Gruppe** ist

$$A_n \coloneqq \mathfrak{A}_n \coloneqq \mathrm{Ker}(\mathrm{sgn}) = \{\sigma \in S_n \mid \mathrm{sgn}(\sigma) = 1\}.$$

(viii) Lineare Gruppen wie $\mathrm{GL}(n,K)$, $\mathrm{SL}(n,K)$, $\mathrm{O}(n,K)$, $\mathrm{SO}(n,K)$, $\mathrm{U}(n,K)$, etc. sind Gruppen. Für $n > 2$ sind sie alle nicht abelsch.

(ix) Das wichtigste Beispiel von Gruppen ist die **Automorphismengruppe**

$$\mathrm{Aut}(K) \coloneqq \{\varphi\colon K \longrightarrow K \text{ Körperautomorphismen}\}$$

für Körper $K$ (z. B. $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{Q}(\sqrt{-1})$, $\mathbb{C}$, etc.). $\varphi\colon K \to K$ ist ein **Körperautomorphismus**, falls $\varphi$ bijektiv ist und falls

$$\varphi(a+b) = \varphi(a) + \varphi(b) \qquad \text{sowie} \qquad \varphi(ab) = \varphi(a)\varphi(b)$$

für alle $a, b \in K$.

(x) Die $n$-strängige **Zopfgruppe** $B_n$ ist eine Gruppe: Jedes Element (*Zopf*) besteht aus zwei parallelen Reihen von $n$ nummerierten Punkten, die durch $n$ viele Fäden gepaart werden. Hierbei ist ausschlaggebend, ob ein Faden über- oder unter einem anderen verläuft; jede Möglichkeit liefert einen anderen Zopf. Hingegen sind zwei Zöpfe gleich, wenn sie durch Verschieben und Dehnen der Fäden ineinander überführt werden können.[3] Die Gruppenoperation ist gegeben durch die Verkettung von Zöpfen. Das Einselement ist der Zopf ohne Überkreuzungen. Das Inverse eines Zopfes erhalten wir, indem wir ihn „rückwärts“ durchlaufen.

Es gibt zwei Zugänge, Gruppen zu beschreiben.

(i) Gruppen als Symmetriegruppen.

*Beispiel:* $\mathcal{B}_2$ ist die Gruppe der Bewegungsabbildungen auf $\mathbb{R}^2$. $D_{2n} \subset \mathcal{B}_2$ ist die Gruppe aller Bewegungen von $\mathbb{R}^2$, die ein reguläres $n$-Eck in sich selbst überführt. Also ist $D_{2n}$ die Symmetriegruppe des regulären $n$-Ecks.

(ii) Beschreibung durch Erzeuger und Relationen.

*Beispiel:* $D_{2n}$ ist die Gruppe mit Erzeuger $d_\theta$ (die Rotation um $\theta = \frac{2\pi}{n}$) und $s$ (die Spiegelung an der $x$-Achse) sowie Relationen $d_\theta^n = \mathrm{id}$, $s^2 = \mathrm{id}$ und $d_\theta \circ s = s \circ d_{-\theta}$.

**Definition 1.1.11.** Eine Teilmenge $A$ einer Gruppe $G$ **erzeugt** die Gruppe $G$, falls für jedes $a \in G$ es $a_1,\dots,a_k \in A$ und $n_1,\dots,n_k \in \mathbb{Z}$ gibt, sodass $a = a_1^{n_1} \cdots a_k^{n_k}$.
*Achtung:* Wir schließen $a_i = a_j$ nicht unbedingt aus.

[3] Anders gesagt, Zöpfe bestehen aus zwei Mengen von $n$ nummerierten Punkten, die durch stetige monotone injektive Kurven im $\mathbb{R}^3$ gepaart werden. Dabei betrachten wir Zöpfe bis auf Homotopieäquivalenz.

**Notation 1.1.12.** Im Allgemeinen können wir $G$ schreiben als

$$G = \langle \text{Erzeuger} \mid \text{Relationen} \rangle,$$

wobei die Relationen dadurch bestimmt werden, welche erzeugten Elemente gleich sind.

*Beispiel* 1.1.13. Die Zopfgruppe $B_n$ lässt sich alternativ wie folgt beschreiben:

(i) Sei $\sigma_i$ der Zopf, der einen Faden $(i, i+1)$ über dem Faden $(i+1, i)$ hat. Alle anderen Fäden sind $(j, j)$ für $j \notin \{i, i+1\}$. Dann sind die Erzeuger $\sigma_1, \ldots, \sigma_{n-1}$.

(ii) Als Relationen wählen wir

- $\sigma_i \sigma_j = \sigma_j \sigma_i$, falls $|i - j| \geq 2$, und
- $\sigma_i \sigma_{i+1} \sigma_i = \sigma_{i+1} \sigma_i \sigma_{i+1}$ für alle $i$.

Dass diese Relationen nicht der Definition der Zopfgruppe widersprechen, lässt sich grafisch veranschaulichen (Abb. 1.1).

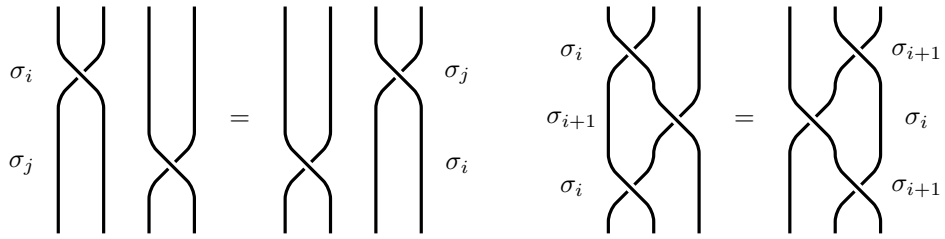



fig:braid

Abbildung 1.1: Relationen der Zopfgruppe.

*Beispiel* 1.1.14. Die **freie Gruppe** in $n$ Variablen ist

$$F_n \coloneqq \langle \alpha_1, \ldots, \alpha_n \mid \text{keine Relationen} \rangle,$$

bestehend aus $n$ Erzeugern und keinen Relationen. Die Elemente in $F_n$ sind alle von der Form $\alpha_{i_1}^{n_1} \cdots \alpha_{i_k}^{n_k}$ mit $n_i \in \mathbb{Z}$. Diese Darstellung ist **reduziert**, falls $\alpha_{i_j} \neq \alpha_{i_{j+1}}$. Die reduzierte Darstellung ist eindeutig, welche wir **Wort** nennen. Die Gruppenoperation ist gegeben durch Hintereinanderschreiben von Wörtern (und ggf. Reduzieren).

Konkret haben wir $F_1 \simeq \mathbb{Z} = \langle 1 \mid \text{keine Relationen} \rangle$. Des Weiteren ist

$$F_2 = \{e, \alpha_1, \alpha_2, \alpha_1^{-1}, \alpha_2^{-1}, \alpha_1\alpha_2, \alpha_2\alpha_1, \alpha_1\alpha_2^2\alpha_1\alpha_2^3\alpha_1, \ldots\}.$$

Beobachte, dass $F_n$ für $n \geq 2$ nicht abelsch ist.

Falls $A = \{a_1, \ldots, a_n\} \subset G$ die Gruppe $G$ erzeugt, so definiert

$$F_n \twoheadrightarrow G, \qquad \alpha_1^{n_1} \cdots \alpha_k^{n_k} \longmapsto a_1^{n_1} \cdots a_k^{n_k}$$

einen surjektiven Gruppenhomomorphismus.

*Beispiel* 1.1.15. Die **freie abelsche Gruppe** in $n$ Variablen ist

$$\langle \beta_1, \dots, \beta_n \mid \beta_i \beta_j = \beta_j \beta_i \rangle.$$

Diese ist isomorph zu $\mathbb{Z}^n := \mathbb{Z} \times \cdots \times \mathbb{Z}$ ($n$ mal) mit komponentenweiser Addition. Der Isomorphismus ist gegeben durch $e_i \mapsto \beta_i$.

Analog zu eben: Falls $A = \{a_1, \dots, a_n\} \subset G$ eine abelsche Gruppe $G$ erzeugt, so definiert

$$\mathbb{Z}^n \longrightarrow\!\!\!\!\!\rightarrow G, \qquad (m_1, \dots, m_n) \longmapsto a_1^{m_1} \cdots a_n^{m_n}$$

einen surjektiven Gruppenhomomorphismus.

*Beispiel* 1.1.16. Die **zyklischen Gruppen** definieren wir wie folgt: Es sei VL 2 13.10.23

$$C_\infty := \langle a \mid \text{keine Relationen} \rangle,$$

d. h. für jedes $g \in C_\infty$ gibt es ein eindeutiges $n \in \mathbb{Z}$, sodass $g = a^n$. Für jedes $m \in \mathbb{Z}_{>0}$ sei

$$C_m := \langle a \mid a^m = e \rangle,$$

d. h. für jedes $g \in C_n$ gibt es genau ein $n \in \{0, \dots, m-1\}$, sodass $g = a^n$. Im letzten Fall gilt $a^{-1} = a^{m-1}$.

**Bemerkung 1.1.17.** Seien $G$ eine beliebige Gruppe und $a \in G$. Dann definiert $\varphi\colon \mathbb{Z} \to G$, $n \mapsto a^n$ einen Gruppenhomomorphismus. Im Beispiel der zyklischen Gruppen liefert die Abbildung einen surjektiven Gruppenhomomorphismus $\mathbb{Z} \twoheadrightarrow C_m$, $n \mapsto a^n$. Dieser Gruppenhomomorphismus induziert für $m \in \mathbb{Z}_{>0}$ Gruppenisomorphismen $\mathbb{Z}/m\mathbb{Z} \xrightarrow{\sim} C_m$, falls $m \in \mathbb{Z}_{>0}$, und $\mathbb{Z} \xrightarrow{\sim} C_\infty$, falls $m = \infty$.[4]

**Definition 1.1.18.** Seien $G$ eine Gruppe und $a \in G$. Dann ist die **Ordnung** von $a$ die Zahl

$$\operatorname{ord}(a) := |a| := \min\{n \in \mathbb{N}_{>0} : a^n = e\}.$$

Die **Ordnung** von $G$ ist die Kardinalität von $|G|$.

**Bemerkung 1.1.19.**

(i) Es gilt $|a| = 1$ genau dann, wenn $a = e$.

(ii) Wir schreiben

$$H = \langle a \rangle := \{a^n \mid n \in \mathbb{Z}\} \subset G$$

für die von $a$ erzeugte Untergruppe (es gilt dann $(a^n)^{-1} = a^{-n}$). Dann gilt $|H| = |a|$.

(iii) Offenbar ist $|a| \leq |G|$ für alle $a \in G$. (Später zeigen wir, dass $|a|$ die Ordnung $|G|$ teilt, was aus dem Satz von Lagrange 1.2.15 folgt.)

*Achtung:* Für $a \in G$ gilt $\langle a \rangle \simeq \langle \alpha \mid \alpha^{|a|} = e \rangle$.

[4] Tatsächlich kann man zeigen, dass $\mathbb{Z}$ und $\mathbb{Z}/m\mathbb{Z}$ für $m \in \mathbb{Z}_{>0}$ bis auf Isomorphie die einzigen zyklischen Gruppen sind.

(iv) Eine Gruppe $G$ wird genau dann durch ein Element $a \in G$ erzeugt, wenn $|a| = |G|$. Das folgt aus der Beobachtung, dass $a, a^2, \ldots, a^{|a|} = 1$ aufgrund der Minimalität von $|a|$ paarweise verschieden sind.

(v) Für alle $a \in G$ gilt

$$\langle a \rangle \simeq \begin{cases} C_m, & \text{falls } m = |a|, \\ C_\infty, & \text{falls } |a| = \infty. \end{cases}$$

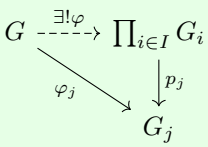
(vi) Zyklische Gruppen sind abelsch.

(vii) Alle Untergruppen von $\mathbb{Z}$ sind zyklisch (Aufgabe 9).

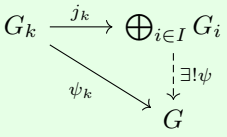
def:productsum

**Definition 1.1.20.** Sei $I$ eine geordnete (Index-)menge[5] (z. B. $I = \{1, 2\}$ oder $I = \mathbb{N}$) und für jedes $i \in I$ sei eine Gruppe $G_i$ gegeben. Dann konstruieren wir das **direkte Produkt** $\prod_{i \in I} G_i$ und die **direkte Summe** $\bigoplus_{i \in I} G_i$ mit folgenden **Universaleigenschaften**:

(i) **Universelle Eigenschaft des Produkts**: Es gibt für jedes $j \in I$ einen Gruppenhomomorphismus $p_j \colon \prod_{i \in I} G_i \to G_j$ (**Projektionen**), sodass für alle Familien von Gruppenhomomorphismen $\varphi_j \colon G \to G_j$ mit $j \in I$ ein *eindeutiger* Gruppenhomomorphismus $\varphi \colon G \to \prod_{i \in I} G_i$ existiert, sodass $p_j \circ \varphi = \varphi_j$ für alle $j \in I$. Anders gesagt, folgendes Diagramm kommutiert für alle $j \in I$:




(ii) **Universelle Eigenschaft des Koprodukts**: Es gibt für jedes $k \in I$ einen Gruppenhomomorphismus $j_k \colon G_k \to \bigoplus_{i \in I} G_i$ (**Inklusionen**), sodass für alle Familien von Gruppenhomomorphismen $\psi_k \colon G_k \to G$ mit $k \in I$ ein eindeutiger Gruppenhomomorphismus $\psi \colon \bigoplus_{i \in I} G_i \to G$ existiert, sodass $\psi_k = \psi \circ j_k$ für alle $k \in I$. Anders gesagt, folgendes Diagramm kommutiert für alle $k \in I$:




**Beobachtung 1.1.21** (Konstruktion von Produkt und direkte Summe (Koprodukt) von Gruppen)**.** Für die Existenz müssen wir Produkt und direkte Summe explizit konstruieren.

Die zugrundeliegende Menge von $\prod_{i \in I} G_i$ sei das (kartesische) Produkt der Mengen $G_i$, ausgestattet mit der Gruppenstruktur $(a_i) \cdot (b_i) \coloneqq (a_i b_i)$. Für $I = \{1, 2\}$ ist $\prod_{i \in I} G_i = G_1 \times G_2$ mit der Gruppenstruktur $(a_1, a_2) \cdot (b_1, b_2) = (a_1 b_1, a_2 b_2)$, Inversen $(a_1, a_2)^{-1} =$

[5] Ich bin mir ziemlich sicher, dass die Indexmenge nicht geordnet sein muss. Mengentheoretisch muss für das kartesische Produkt die Indexmenge nicht geordnet sein.

$(a_1^{-1}, a_2^{-1})$ und der Einheit $e = (e_1, e_2)$. Die Projektionen $p_i \colon \prod_{i\in I} G_i \twoheadrightarrow G_j$ sind gegeben durch $(a_i) \mapsto a_j$.

Wir wollen hier die direkte Summe von Gruppen nur für abelsche Gruppen konstruieren.[6] Die zugrundeliegende Menge von $\bigoplus_{i\in I} G_i$ ist die Menge aller Elemente $(a_i) \in \prod_{i\in I} G_i$, sodass $a_i \neq e_i$ nur für endlich viele $i$. Dann erhält $\bigoplus_{i\in I} G_i$ die Untergruppenstruktur von $\prod_{i\in I} G_i$. Die Inklusionen $j_k \colon G_k \hookrightarrow \bigoplus_{i\in I} G_i$ sind gegeben durch $j_k(a) = (a_i)$, wobei

$$a_i = \begin{cases} e_i, & \text{falls } i \neq k, \\ a, & \text{falls } i = k. \end{cases}$$

Man muss noch zeigen, dass beide Konstruktionen die universelle Eigenschaft erfüllen.

**Warnung 1.1.22.** Wenn $|I| < \infty$, dann ist $\prod_{i\in I} G_i \simeq \bigoplus_{i\in I} G_i$ für abelsche Gruppen $G_i$.

## 1.2 Normalteiler und Nebenklassen

**Definition 1.2.1.** Seien $G$ eine Gruppe und $H \subset G$ eine Untergruppe. Dann heißt $H$ **Normalteiler** (oder **normale** Untergruppe) von $G$, falls

$$aHa^{-1} \subset H$$

für alle $a \in G$. Wir schreiben $H \lhd G$.

**Bemerkung 1.2.2.** Seien $H \subset G$ und $a \in G$. Dann ist $aH \coloneqq \{ab \mid b \in H\} \subset G$ eine Teilmenge von $G$ (die im Allgemeinen keine Untergruppe ist), eine sog. **Linksnebenklasse** von $H$. Analog ist $Ha \coloneqq \{ba \mid b \in H\} \subset G$ eine sog. **Rechtsnebenklasse** von $H$.

Dann ist $aHa^{-1} \coloneqq \{aba^{-1} \mid b \in H\} \subset G$ eine Untergruppe, denn

$$(ab_1a^{-1})(ab_2a^{-1}) = a(b_1b_2)a^{-1}, \qquad (aba^{-1})^{-1} = (a^{-1})^{-1}b^{-1}a^{-1} = ab^{-1}a^{-1}$$

für alle $b \in H$. Wir sagen, dass $aba^{-1}$ **konjugiert** zu $b$ ist. (In der linearen Algebra entspricht die Konjugation $AMA^{-1}$ einem Basiswechsel der Matrix $M$.)[7]

fac:normal:coset

**Fakt 1.2.3.** *Es gilt $H \lhd G$ genau dann, wenn $aH = Ha$ für alle $a \in G$.*

*Beweis.* Angenommen $H \lhd G$. Seien $a \in G$ und $b \in H$. Wegen $H \lhd G$ gilt $aHa^{-1} \subset H$. Also existiert ein $b' \in H$ mit $aba^{-1} = b'$ bzw. $ab = b'a$. Folglich ist $ab \in Ha$, d. h. $aH \subset Ha$. Analog zeigen wir $ba \in aH$: Wegen $H \lhd G$ gilt $a^{-1}Ha \subset H$. Damit existiert ein $b' \in H$ mit $ba = ab' \in aH$, d. h. $Ha \subset aH$.

Die Rückrichtung ist eine einfache Übung. □

[6] Für beliebige Gruppen $G_i$ mit $i \in I$ ist das Koprodukt das *freie Produkt* $*_{i\in I} G_i$; für zwei Gruppen schreiben wir $G_1 * G_2$. Sind Gruppen $G_i = \langle A_i \mid R_i \rangle$ durch Wörter und Relationen gegeben, so gilt $*_{i\in I} G_i = \langle \bigcup_{i\in I} A_i \mid \bigcup_{i\in I} R_i \rangle$.

[7] Beachte aber, dass $AMA^{-1}$ keine Konjugation im Sinne der Gruppentheorie ist, denn im Allgemeinen sind $A$ und $M$ nicht aus derselben (Matrix-)gruppe.

**Fakt 1.2.4.** *Wenn $H \lhd G$, dann gilt $aHa^{-1} = H$ für alle $a \in G$.*

*Beweis.* Sei $a \in G$. Nach Voraussetzung gilt $a^{-1}Ha \subset H$. Also gibt es für jedes $b \in H$ ein $b' \in H$, sodass $a^{-1}ba = b'$. Umstellen liefert $b = ab'a^{-1} \in aHa^{-1} \subset H$. Somit gilt $aHa^{-1} = H$. □

**Fakt 1.2.5.** *Wenn $G$ abelsch ist, so ist jede Untergruppe $H$ ein Normalteiler.*

*Beweis.* Für alle $b \in H$ und $a \in G$ gilt $aba^{-1} = aa^{-1}b = b$, also $aHa^{-1} = H$. □

**Bemerkung 1.2.6.** Für $a \in G$ ist die Untergruppe $aHa^{-1} \subset G$ eine zu $H$ **konjugierte** Untergruppe. Es gilt $aHa^{-1} \cap H \neq \varnothing$, z. B. $e \in aHa^{-1} \cap H$.

fac:coset:subgroup

**Fakt 1.2.7.** *Seien $H \subset G$ eine Untergruppe und $a \in G$. Dann ist $aH \subset G$ genau dann eine Untergruppe, wenn $a \in H$.*

*Beweis.* Falls $aH \subset G$ eine Untergruppe ist, so ist $e \in aH$. Daher gibt es ein $b \in H$ mit $e = ab$ und schließlich $a = b^{-1} \in H$. Gilt umgekehrt $a \in H$, so haben wir $b = a(a^{-1}b) \in aH$ für alle $b \in H$, also $H \subset aH$. Offenbar ist auch $aH \subset H$ nach Annahme, d. h. $aH = H$ ist eine Untergruppe. □

obs:cosets:disjoint

**Beobachtung 1.2.8.** Wie verhalten sich Nebenklassen zueinander?

*Behauptung:* Allgemein sind zwei Linksnebenklassen $a_1H$ und $a_2H$ entweder gleich oder disjunkt.

*Beweis:* Wir müssen zeigen, dass $a_1H = a_2H$ falls ein $a \in a_1H \cap a_2H$ existiert. Schreibe dazu $a = a_1b_1 = a_2b_2$ mit $b_1, b_2 \in H$. Dann folgt $a_1 = a_2(b_2b_1^{-1}) \in a_2H$, also $a_1b \in a_2H$ für alle $b \in H$. Es folgt $a_1H \subset a_2H$ und komplett analog folgt auch $a_2H \subset a_1H$.

*Folgerung:* Sei $H \subset G$ eine Untergruppe. Dann ist $G$ die disjunkte Vereinigung aller Linksnebenklassen

$$G = \bigsqcup_{i \in I} a_iH$$

(analog für Rechtsnebenklassen). Hierbei ist die Menge der Repräsentanten $\{a_i \mid i \in I\} \subset G$ so gewählt, dass $a_iH \neq a_jH$ für alle $i \neq j$.

**Bemerkung 1.2.9.** Falls $H \lhd G$, dann ist die Menge aller Linksnebenklassen gleich der Menge aller Rechtsnebenklassen nach Fakt 1.2.3 (welche beide Teilmengen der Potenzmenge $\mathcal{P}(G)$ sind).

**Notation 1.2.10.** Seien $G$ eine Gruppe und $H \subset G$ eine Untergruppe. Bezeichne mit $G/H \subset \mathcal{P}(G)$ die Menge der Linksnebenklassen und mit $H\backslash G \subset \mathcal{P}(G)$ die Menge der Rechtsnebenklassen.

*Alternativ:* Für eine gegebene Untergruppe $H$ definieren wir zwei Äquivalenzrelationen. Für Links- bzw. Rechtsnebenklassen sei[8]

$$a_1 \sim_L a_2 :\iff a_1H = a_2H \iff a_2^{-1}a_1 \in H,$$
$$a_1 \sim_R a_2 :\iff Ha_1 = Ha_2 \iff a_1a_2^{-1} \in H.$$

Dann existieren natürliche Bijektionen

$$G/\!\sim_L \xrightarrow{\sim} G/H, \quad [a] \longmapsto aH \qquad \text{und} \qquad G/\!\sim_R \xrightarrow{\sim} H\backslash G, \quad [a] \longmapsto Ha,$$

wobei $G/\!\sim$ die Menge der Äquivalenzklassen bedeutet.

lem:normal:group

**Lemma 1.2.11.** *Seien $G$ eine Gruppe und $H \lhd G$. Dann definiert*

$$(a_1H)(a_2H) \coloneqq (a_1a_2)H$$

*eine Gruppenstruktur auf $G/H$. Ferner ist die Abbildung*

$$G \longrightarrow\!\!\!\!\!\rightarrow G/H, \qquad a \longmapsto aH$$

*ein surjektiver Gruppenhomomorphismus.*

*Beweis.* Der zentraler Punkt ist, warum die Gruppenoperation überhaupt wohldefiniert ist.

Angenommen $a_1H = a_1'H$ (d. h. $a_1^{-1}a_1' \in H$). Wir müssen zeigen, dass $(a_1'a_2)H = (a_1a_2)H$. Sei also $a_1'a_2b \in (a_1'a_2)H$ mit $b \in H$. Da $H \lhd G$, gibt es ein $b' \in H$ mit $a_2b = b'a_2$. Wir erhalten $a_1'a_2b = a_1'b'a_2$. Da $a_1'b' \in a_1'H = a_1H$, gibt es ein $b'' \in H$ mit $a_1'b' = a_1b''$ und wir erhalten $a_1'b'a_2 = a_1b''a_2$. Wegen $H \lhd G$ gibt es ein $b''' \in H$ mit $b''a_2 = a_2b'''$. Wir erhalten $a_1b''a_2 = a_1a_2b'''$. Insgesamt ergibt sich $a_1'a_2b = a_1a_2b''' \in (a_1a_2)H$ und somit $(a_1'a_2)H \subset (a_1a_2)H$. Komplett analog zeigt man $(a_1a_2)H \subset (a_1'a_2)H$, woraus wir $(a_1a_2)H = (a_1'a_2)H$ schließen.

Wir sehen leicht, dass $G/H$ eine Gruppe mit Inversen $(aH)^{-1} = a^{-1}H$ und Einheit $eH$ bildet.

Für die Surjektion betrachten wir die Abbildung $G \twoheadrightarrow G/\!\sim_L \;\simeq G/H$, $a \mapsto [a] \mapsto aH$, welche offenbar surjektiv ist und offenbar ein Gruppenhomomorphismus ist. □

**Bemerkung 1.2.12.** Vgl. den surjektiven Gruppenhomomorphismus $G \twoheadrightarrow G/H$ mit dem Fall von Vektorräumen. Seien $V$ ein Vektorraum und $U \subset V$ ein Unterraum. Dann ist $V \twoheadrightarrow V/U \simeq V/\!\sim_U$ eine surjektive lineare Abbildung, wobei $v_1 \sim_U v_2$ genau dann, wenn $v_1 - v_2 \in U$ für alle $v_1, v_2 \in V$.

Für Vektorräume haben wir das Konzept von Normalteilern nicht gebraucht, da die additive Gruppenstruktur auf Vektorräumen abelsch ist und somit jeder Unterraum ein Normalteiler ist.

[8] Falls $a_1H = a_2H$, so gibt es ein $b \in H$ mit $a_1e = a_2b$, d. h. $a_2^{-1}a_1 = b \in H$. Falls umgekehrt $a_2^{-1}a_1 \in H$, so gilt $a_2(a_2^{-1}a_1) \in a_2H$, aber auch $(a_2a_2^{-1})a_1 = a_1e \in a_1H$, d. h. $a_1H \cap a_2H \neq \varnothing$ und daher $a_1H = a_2H$ nach Beobachtung 1.2.8.

**Satz 1.2.13.** *Seien $G$ eine Gruppe und $H \subset G$ eine Untergruppe. Dann ist $H \lhd G$ genau dann, wenn es einen Gruppenhomomorphismus $\varphi\colon G \to G'$ gibt, sodass $H = \mathrm{Ker}(\varphi)$.*

*Beweis.* Zur Rückrichtung: Sei $\varphi\colon G \to G'$ ein Gruppenhomomorphismus. Wir behaupten, dass $\mathrm{Ker}(\varphi) \lhd G$, d. h. für alle $a \in G$ und $b \in \mathrm{Ker}(\varphi)$ gelte $aba^{-1} \in \mathrm{Ker}(\varphi)$. Es gilt aber

$$\varphi(aba^{-1}) = \varphi(a)\varphi(b)\varphi(a^{-1}) = \varphi(a)e_{G'}\varphi(a)^{-1} = \varphi(a)\varphi(a)^{-1} = e_{G'},$$

d. h. tatsächlich $aba^{-1} \in \mathrm{Ker}(\varphi)$.

Zur Hinrichtung: Sei $H \lhd G$ und sei $\pi\colon G \twoheadrightarrow G/H$ der kanonische Gruppenhomomorphismus aus Lemma 1.2.11. Wir behaupten, dass $\mathrm{Ker}(\pi) = H$ gilt. Das stimmt aber, denn für alle $a \in G$ gilt $\pi(a) = e_{G/H}$ genau dann, wenn $aH = eH = H$. Das ist nach Fakt 1.2.7 äquivalent zu $a \in H$. □

**Bemerkung 1.2.14.** Für Gruppenhomomorphismen $\varphi\colon G \to G'$ ist $\mathrm{Im}(\varphi) \subset G'$ eine Untergruppe, aber im Allgemeinen nicht normal.

thm:lagrange

**Satz 1.2.15 (Satz von Lagrange).** *Seien $G$ eine endliche Gruppe und $H \subset G$ eine Untergruppe. Setze $(G : H) := |G/H|$. Dann gilt*

$$(G : H) \cdot |H| = |G|.$$

*Insbesondere ist $|H|$ ein Teiler von $|G|$.*

*Beweis.* Wir wissen, dass $G = \bigsqcup_{a \in R} aH$, wobei $R \subset G$ eine Teilmenge von Repräsentanten von Linksnebenklassen ist (d. h. wir wählen für jede Linksnebenklasse $M \subset G$ ein $a \in G$ mit $aH = M$). Nun ist $H \xrightarrow{\sim} aH$, $b \mapsto ab$ für alle $a \in G$ eine Bijektion mit Inversem $aH \to H$, $b \mapsto a^{-1}b$. Es folgt

$$|G| = \sum_{a \in R} |aH| = \sum_{a \in R} |H| = |R| \cdot |H| = |G/H| \cdot |H| = (G : H) \cdot |H|. \qquad \square$$

Wir werden später sehen, dass das ein Spezialfall von Aussagen über Gruppenbahnen ist.

**Beobachtung 1.2.16.** Sei $H \subset G$ eine Untergruppe. Was haben $G/H$ und $H\backslash G$ miteinander zu tun? VL 3 16.10.23

Wir wissen bereits, dass es surjektive Abbildungen von Mengen $G \twoheadrightarrow G/H$, $a \mapsto aH$ sowie $G \twoheadrightarrow H\backslash G$, $a \mapsto Ha$ gibt. Die Idee ist, eine Abbildung

$$\varphi\colon G/H \longrightarrow H\backslash G, \qquad aH \longmapsto Ha$$

zu konstruieren.

Ist $\varphi$ wohldefiniert, d. h. wenn $a_1H = a_2H$, dann auch $Ha_1 = Ha_2$? Wir wissen, dass $a_1H = a_2H$ genau dann, wenn $a_1^{-1}a_2 \in H$. Ähnlich ist $Ha_1 = Ha_2$ genau dann, wenn $a_2a_1^{-1} \in H$. Nun gilt im Allgemeinen aber nicht, dass $a_1^{-1}a_2 \in H$ genau dann, wenn $a_2a_1^{-1} \in H$. Mit anderen Worten, die Abbildung ist nicht wohldefiniert.

Wir beobachten hingegen, dass falls $H \lhd G$, dann $a_1H = Ha_1$ und $a_2H = Ha_2$ gelten. Vielmehr sind $G/H$ und $H\backslash G$ beides Gruppen. In diesem Fall folgt aus $a_1H = a_2H$ dann $Ha_1 = Ha_2$. Damit definiert $\varphi$ eine Bijektion, falls $H \lhd G$.

Ist das aber ein Gruppenhomomorphismus? Es gilt

$$\varphi((a_1H)(a_2H)) = \varphi(a_1a_2H) = Ha_1a_2 = (Ha_1)(Ha_2) = \varphi(a_1H)\varphi(a_2H) = (Ha_1)(Ha_2).$$

Somit ist $\varphi\colon G/H \xrightarrow{\sim} H\backslash G$ ein Gruppenisomorphismus, falls $H \lhd G$.[9] Tatsächlich beschreibt $\varphi$ nichts anderes die Gleichheit $G/H = H\backslash G$, welche natürlich die Gruppenstruktur erhält. Im Fall von Normalteilern müssen wir also nicht zwischen Links-und Rechtsnebenklassen unterscheiden. Konventionell benutzt man stets die Notation linker Nebenklassen.

Der Satz von Lagrange 1.2.15 impliziert folgende Aussage, die nach Pierre de Fermat (1602–1665) benannt wurde.

cor:fermat:small

**Korollar 1.2.17** (**kleiner Satz von Fermat**)**.** *Seien $G$ eine endliche Gruppe und $a \in G$. Dann ist $|a|$ ein Teiler von $|G|$ (bisher hatten wir $|a| \leq |G|$); insbesondere gilt $a^{|G|} = e$.*

*Beweis.* Sei $H \coloneqq \langle a \rangle$ die von $a$ erzeugte Untergruppe. Dann gilt $|H| = |a|$, und nach dem Satz von Lagrange 1.2.15 ist $|a|$ ein Teiler von $|G|$.

Für die zweite Aussage schreibe $|G| = |a|n$ für ein $n \in \mathbb{N}$. Dann gilt

$$a^{|G|} = \underbrace{a \cdots a}_{|G| \text{ mal}} = \underbrace{a^{|a|} \cdots a^{|a|}}_{n \text{ mal}} = \underbrace{e \cdots e}_{n \text{ mal}} = e. \qquad \square$$

**Bemerkung 1.2.18** ((historische) *kleine Satz von Fermat*)**.** Folgender Spezialfall stammt aus der Zahlentheorie. Sei $p$ eine Primzahl. Wir erinnern uns an $\mathbb{F}_p \coloneqq \mathbb{Z}/p\mathbb{Z}$ mit $|\mathbb{F}_p| = p$. Für $a \in \mathbb{Z}$ bezeichne $\bar{a} \in \mathbb{F}_p$ die Restklasse von $a$ modulo $p$.

Betrachte die Gruppe $G = \mathbb{F}_p^* \coloneqq \mathbb{F}_p \setminus \{0\}$ der Ordnung $|G| = p - 1$. Falls $a \in \mathbb{Z}$ nicht durch $p$ teilbar ist, so gilt $\bar{a} \in \mathbb{F}_p^* = G$ und damit $a^{p-1} \equiv 1 \mod p$ nach dem kleinen Satz von Fermat 1.2.17. Ferner folgt $a^p \equiv a \mod p$, d. h. für alle Primzahlen $p$ und alle $a \in \mathbb{Z}$ mit $p \nmid a$ gilt $p \mid a^p - a$.

**Bemerkung 1.2.19** (Euler)**.** Falls $p \neq 2$ eine Primzahl ist und $a \in \mathbb{Z}$ mit $p \nmid a$, so gilt $a^{(p-1)/2} \equiv \pm 1 \mod p$.

*Beweis:* Wir haben

$$(a^{(p-1)/2} - 1)(a^{(p-1)/2} + 1) = a^{p-1} - 1 \equiv 0 \mod p,$$

d. h. $p$ teilt einen der Faktoren. Wir erhalten $a^{(p-1)/2} \equiv 1 \mod p$ oder $a^{(p-1)/2} \equiv -1 \mod p$.

**Korollar 1.2.20.** *Sei $G$ eine endliche Gruppe, deren Ordnung eine Primzahl $p \coloneqq |G|$ ist. Dann ist $G$ zyklisch. (Insbesondere gilt $G \simeq \mathbb{Z}/p\mathbb{Z}$.)*

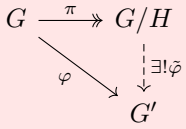
[9] An der Stelle brach der Dozent die Ausführung ab, da irgendetwas nicht so funktionierte, wie er es wollte.

*Beweis.* Nehme ein beliebiges $a \in G \setminus \{e\}$. Betrachte die zyklische Untergruppe $\langle a \rangle \subset G$. Da $|a|$ ein Teiler von $p$ ist (kleiner Satz von Fermat 1.2.17) und $|a| \neq 1$, folgt notwendigerweise $|a| = p$ und damit $\langle a \rangle = G$, d. h. $G$ ist zyklisch. □

thm:homomorphism

**Satz 1.2.21** (**Homomorphiesatz**). *Sei $H \lhd G$. Dann hat die Quotientengruppe $G/H$ zusammen mit der kanonischen Projektion $\pi\colon G \twoheadrightarrow G/H$ die folgende **Universaleigenschaft des Quotienten**: Für alle Gruppenhomomorphismen $\varphi\colon G \to G'$ sind folgende Aussagen äquivalent:*

(i) *Es gibt genau einen Gruppenhomomorphismus $\tilde{\varphi}\colon G/H \to G'$, sodass $\tilde{\varphi} \circ \pi = \varphi$, oder äquivalent dazu, sodass folgendes Diagramm kommutiert:*




(ii) *Es gilt $H \subset \mathrm{Ker}(\varphi)$.*

*Beweis.* Angenommen ein $\tilde{\varphi}$ mit $\varphi = \tilde{\varphi} \circ \pi$ existiert. Für alle $a \in H$ gilt dann

$$\varphi(a) = \tilde{\varphi}(\pi(a)) = \tilde{\varphi}(aH) = \tilde{\varphi}(H) = \tilde{\varphi}(e_{G/H}) = e_{G'}.$$

Somit $a \in \mathrm{Ker}(\varphi)$.

Für die Umkehrung sei $H \subset \mathrm{Ker}(\varphi)$. Definiere $\tilde{\varphi}(aH) := \varphi(a)$ für alle $a \in G$, was die einzige Möglichkeit ist, damit $\tilde{\varphi} \circ \pi = \varphi$. Für die Wohldefiniertheit nehmen wir $a_1 H = a_2 H$ an, was äquivalent zu $a_1^{-1} a_2 \in H \subset \mathrm{Ker}(\varphi)$ ist. Es folgt $e = \varphi(a_1^{-1} a_2) = \varphi(a_1)^{-1} \varphi(a_2)$, also $\varphi(a_1) = \varphi(a_2)$. Somit ist $\tilde{\varphi}$ wohldefiniert. Ferner ist $\tilde{\varphi}$ ein Gruppenhomomorphismus, denn

$$\tilde{\varphi}((aH)(bH)) = \tilde{\varphi}(abH) = \varphi(ab) = \varphi(a)\varphi(b) = \tilde{\varphi}(aH)\tilde{\varphi}(bH).$$ □

**Bemerkung 1.2.22.**

(i) Weil $\pi$ surjektiv ist, haben wir $\mathrm{Im}(\varphi) = \mathrm{Im}(\tilde{\varphi})$ sowie $\mathrm{Ker}(\tilde{\varphi}) = \pi(\mathrm{Ker}(\varphi))$ bzw. $\mathrm{Ker}(\varphi) = \pi^{-1}(\mathrm{Ker}(\tilde{\varphi}))$.

(ii) $\tilde{\varphi}$ ist genau dann injektiv, wenn $H = \mathrm{Ker}(\varphi)$. In diesem Fall ist nämlich $\mathrm{Ker}(\tilde{\varphi}) = \{e_{G/H}\}$.

cor:homomorphism

**Korollar 1.2.23.** *Jeder surjektive Gruppenhomomorphismus $\varphi\colon G \twoheadrightarrow G'$ induziert einen natürlichen Isomorphismus*[10]

$$G/\mathrm{Ker}(\varphi) \xrightarrow{\sim} G', \qquad a\,\mathrm{Ker}(\varphi) \longmapsto \varphi(a).$$

Beachte, dass $\mathrm{Ker}(\varphi) \lhd G$.

[10] Hier ist kein natürlicher Isomorphismus im Sinne der Kategorientheorie gemeint! Ich finde, dass diese Verwendung irreführend ist. Besser ist der Begriff *kanonischer Isomorphismus*.

cor:isomorphism:1

**Korollar 1.2.24 (erster Isomorphiesatz).** *Seien $H \subset G$ eine Untergruppe und $N \lhd G$. Dann sind $HN := \{ab \mid a \in H, b \in N\} \subset G$ eine Untergruppe, $N \lhd HN$ und $H \cap N \lhd H$. Ferner existiert ein natürlicher Isomorphismus*

$$H/(H \cap N) \simeq HN/N.$$

*Beispiel* 1.2.25. Aus der linearen Algebra I kennen wir eine ähnliche Aussage. Sei $V$ ein Vektorraum und seien $U_1, U_2 \subset V$ Unterräume. Dann können wir all diese Räume als additive abelsche Gruppen auffassen, d. h. wir interpretieren $V$ als $G$, $U_1$ als $H$ und $U_2$ als $N$. Ferner erhalten wir die Entsprechungen $HN \leftrightarrow U_1 + U_2$ und $H \cap N \leftrightarrow U_1 \cap U_2$. Die bekannte Aussage ist dann

$$U_1/(U_1 \cap U_2) \simeq (U_1 + U_2)/U_2.$$

*Beweis des Isomorphiesatzes 1.2.24.* $HN \subset G$ ist eine Untergruppe: Nehme dazu $a_1b_1, a_2b_2 \in HN$ mit $a_1, a_2 \in H$ und $b_1, b_2 \in N$. Da $N \lhd G$ gibt es ein $b_1' \in N$ mit $b_1a_2 = a_2b_1'$. Es folgt $(a_1b_1)(a_2b_2) = a_1(b_1a_2)b_1 = (a_1a_2)(b_1'b_1) \in HN$. Also ist $HN$ unter der Gruppenoperation abgeschlossen. Die Einheit ist offensichtlich $ee \in HN$. Für alle $ab \in HN$ gilt $b^{-1}a^{-1} \in HN$ (Aufgabe). Also ist $HN$ eine Untergruppe.

$N \lhd HN$: Das ist wegen $N \lhd G$ klar.

$H \cap N \lhd H$: Dazu betrachten wir $a \in H$ und $b \in H \cap N$. Wegen $N \lhd G$ ist $ab = b'a$ für ein gewisses $b' \in N$. Es folgt $b' = aba^{-1} \in H$, also $ab = b'a \in (H \cap N)a$, weshalb $a(H \cap N) \subseteq (H \cap N)a$. Die umgekehrte Richtung $(H \cap N)a \subseteq a(H \cap N)$ folgt analog. Wir erhalten $a(H \cap N) = (H \cap N)a$ für alle $a \in H$ und somit $H \cap N \lhd H$.

Für den Isomorphismus betrachten wir die Komposition $\varphi\colon H \hookrightarrow HN \twoheadrightarrow HN/N$. Wenn wir zeigen, dass $\varphi$ surjektiv ist und $\operatorname{Ker}(\varphi) = H \cap N$, dann folgt mit Korollar 1.2.23 die Behauptung.

Zuerst zum Kern: Sei $a \in H$ mit $\varphi(a) = e_{HN/N} = eN = N$. Wegen $\varphi(a) = aN$ folgt $a \in N$, also $a \in H \cap N$, d. h. $\operatorname{Ker}(\varphi) \subseteq H \cap N$. Umgekehrt gilt für alle $a \in H \cap N$ offenbar $\varphi(a) = aN = N = e_{HN/N}$ und somit $H \cap N \subseteq \operatorname{Ker}(\varphi)$. Für die Surjektivität betrachten wir $ab \in HN$ mit $a \in H$ und $b \in N$. Dann gilt

$$(ab)N = \{abc \mid c \in N\} = \{ad \mid d \in N\} = aN = \varphi(a). \qquad \square$$

cor:isomorphism:2

**Korollar 1.2.26 (zweiter Isomorphiesatz).** *Seien $G$ eine Gruppe und $H \lhd G$, $N \lhd G$ zwei Normalteiler, sodass $N \subset H$. Dann gilt $H/N \lhd G/N$ und es existiert ein natürlicher Isomorphismus*

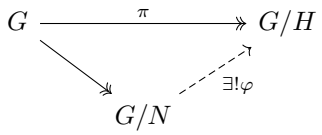
$$(G/N)/(H/N) \simeq G/H.$$

*Beispiel* 1.2.27. Auch diese Aussage ist aus der linearen Algebra I bekannt. Seien $U_1 \subset U_2 \subset V$ Unterräume eines Vektorraums $V$. Dann gilt

$$(V/U_1)/(U_2/U_1) \simeq V/U_2.$$

*Beweis des Isomorphiesatzes 1.2.26.* Nach Definition wissen wir $H/N \subset G/N$. Nach Definition der Gruppenstruktur ist $H/N$ eine Untergruppe; für beide ist das Produkt definiert als $(a_1N)(a_2N) := (a_1a_2)N$. Seien $aN \in G/N$ und $bN \in H/N$, wobei $a \in G$ und $b \in H$. Dann folgt $(aN)(bN)(a^{-1}N) = (aba^{-1})N \in H/N$, da $H \lhd G$ und daher $aba^{-1} \in H$. Somit ist $H/N \lhd G/N$.

Für den Isomorphismus betrachten wir die folgenden Surjektionen:




Dann ist $\operatorname{Ker}(\pi) = H$ und nach Voraussetzung gilt $N \subset \operatorname{Ker}(\pi)$. Nach dem Homomorphiesatz 1.2.21 erhalten wir den surjektiven Gruppenhomomorphismus $\varphi\colon G/N \twoheadrightarrow G/H$. Gemäß Korollar 1.2.23 genügt es zu zeigen, dass $\operatorname{Ker}(\varphi) = H/N$. Wir stellen fest, dass $aN \in \operatorname{Ker}(\varphi)$ genau dann, wenn $\varphi(aN) = aH = e_{G/H} = H$. Ist $aH = H$, so folgt $a \in H$ und daher $aN \in H/N$. Umgekehrt funktioniert das genauso. □

## 1.3 Gruppenwirkungen

**Definition 1.3.1.** Seien $G$ eine Gruppe und $X$ eine Menge. Eine **Wirkung** (auch **Aktion** oder **Operation**) von $G$ auf $X$ ist eine Abbildung

$$G \times X \longrightarrow X, \qquad (a, x) \longmapsto ax \in X,$$

sodass folgende Eigenschaften erfüllt sind:

(i) $ex = x$ für alle $x \in X$.

(ii) $(ab)x = a(bx)$ für alle $x \in X$ und $a, b \in G$.

Für $x \in X$ heißen

$$Gx \coloneqq \{ax \mid a \in G\} \subset X$$

die **Bahn** oder der **Orbit** von $x$ und

$$G_x \coloneqq \operatorname{Stab}(x) \coloneqq \{a \in G \mid ax = x\} \subset G$$

der **Stabilisator** von $x$.

In der Definition $(ab)x = a(bx)$ ist auf der linken Seite $ab$ das Produkt in $G$, während $(ab) \cdot x$ die Wirkung ist. Auf der rechten Seite sind $a \cdot (b \cdot x)$ beides die Wirkung von $G$.

*Beispiel* 1.3.2. Betrachte $G = \mathrm{SO}(2) \simeq S^1$ und $X = \mathbb{R}^2$. Dann ist die Rotation der Ebene

$$G \times X = \mathrm{SO}(2) \times \mathbb{R}^2 \longrightarrow X = \mathbb{R}^2, \qquad (A, v) \longmapsto Av$$

eine Wirkung (die Identität ist $\mathrm{id} \in \mathrm{SO}(2)$, und Kompatibilität folgt aus der Assoziativität der Matrixmultiplikation). Für $x \in X$ sind die Bahnen

$$Gx = \begin{cases} \text{Kreis um 0 durch } x, & \text{falls } x \neq 0, \\ \{0\}, & \text{falls } x = 0. \end{cases}$$

und die Stabilisatoren

$$\operatorname{Stab}(x) = \begin{cases} \{\mathrm{id}\}, & \text{falls } x \neq 0, \\ \mathrm{SO}(2), & \text{falls } x = 0. \end{cases}$$

fact:action

**Fakt 1.3.3.** *Sei $G \times X \to X$ eine Wirkung.*

(i) *Für alle $x \in X$ ist dann $G_x = \operatorname{Stab}(x) \subset G$ eine Untergruppe.*

itm:action:2

(ii) *Jedes $x \in X$ induziert die Abbildung $G \to Gx$, $a \mapsto ax$ eine Bijektion*

$$G/\operatorname{Stab}(x) \xrightarrow{\sim} Gx, \qquad a \operatorname{Stab}(x) \longmapsto ax$$

*von Mengen.*[11]

(iii) *Für endliche Gruppen $G$ gilt $|Gx| = (G : \operatorname{Stab}(x))$ für beliebige $x \in X$.*

(iv) *$X$ ist die disjunkte Vereinigung aller Bahnen. Anders ausgedrückt: Für $x, y \in X$ gilt $Gx \cap Gy \neq \varnothing$ genau dann, wenn $Gx = Gy$.*

*Beweis.*

(i) Seien $a, b \in \operatorname{Stab}(x)$, d. h. $ax = x = bx$. Dann folgt $(ab)x = a(bx) = ax = x$, d. h. $ab \in \operatorname{Stab}(x)$. Ferner gilt $a^{-1}x = a^{-1}(ax) = (a^{-1}a)x = ex = x$, d. h. $a^{-1} \in \operatorname{Stab}(x)$.

(ii) Die Abbildung ist wohldefiniert: Falls $a_1 \operatorname{Stab}(x) = a_2 \operatorname{Stab}(x)$, dann gilt $a \coloneqq a_2^{-1}a_1 \in \operatorname{Stab}(x)$. Es folgt $a_1 = a_2 a$ und daher $a_1 x = (a_2 a)x = a_2(ax) = a_2 x$.

Die Abbildung ist offensichtlich surjektiv. Für die Injektivität sei $a_1 x = a_2 x$ mit $a_1, a_2 \in G$. Wir müssen $a_1 \operatorname{Stab}(x) = a_2 \operatorname{Stab}(x)$ zeigen. Nach Annahme ist

$$(a_2^{-1}a_1)x = a_2^{-1}(a_1 x) = a_2^{-1}(a_2 x) = (a_2^{-1}a_2)x = ex = x.$$

Also gilt $a_2^{-1}a_1 \in \operatorname{Stab}(x)$ und somit $a_1 \operatorname{Stab}(x) = a_2 \operatorname{Stab}(x)$.

(iii) Das folgt direkt aus (ii), da $(G : \operatorname{Stab}(x)) = |G/\operatorname{Stab}(x)|$ nach Definition.

(iv) Angenommen $z \in Gx \cap Gy$ existiert. Schreibe $z = ax = by$ für gewisse $a, b \in G$. Für alle $c \in G$ gilt dann

$$cx = (ca^{-1})(ax) = (ca^{-1})(by) = (ca^{-1}b)y \in G(y),$$

d. h. $Gx \subset Gy$. Analog zeigt man $Gx \supset Gy$. □

Fakt 1.3.3 impliziert folgende Aussage.

thm:orbit

**Satz 1.3.4 (Bahnengleichung).** *Seien $X$ eine endliche Menge und $G \times X \to X$ eine Wirkung. Dann gilt*

$$|X| = \sum_{i=1}^{n} |Gx_i| = \sum_{i=1}^{n} (G : \operatorname{Stab}(x_i)),$$

*wobei $x_1, \ldots, x_n \in X$ ein Repräsentantensystem für Bahnen durchlaufen.*

[11] Im englischsprachigen Raum als *orbit-stabiliser theorem* bekannt.

VL 4
20.10.23

**Notation 1.3.5.** Sei
$$G\backslash X \coloneqq \{Gx \mid x \in X\} \subset \mathcal{P}(X)$$
die Menge der Bahnen. Es gilt $X = \bigsqcup_{Y \in G\backslash X} Y$.

ex:action:left

*Beispiel* 1.3.6. Seien $X = G$ und $G \times G \to G$, $(a, b) \mapsto ab$. Dies ist eine Wirkung (Identität folgt aus der Einheit, und Kompatibilität der Gruppenwirkung folgt aus der Assoziativität der Gruppenoperation). Es gibt nur eine Bahn, denn $Gb = G$ für alle $b \in G$ und $\mathrm{Stab}(b) = \{e\}$.

**Fakt 1.3.7.** *Sei $G \times X \to X$ eine Wirkung. Angenommen $Gx = Gy$. Dann sind die Stabilisatoren* $\mathrm{Stab}(x)$ *und* $\mathrm{Stab}(y)$ *konjugiert, d. h. es gibt ein $a \in G$, sodass* $\mathrm{Stab}(x) = a\,\mathrm{Stab}(y)a^{-1}$. *Unter dieser Annahme sind* $\mathrm{Stab}(x), \mathrm{Stab}(y) \subset G$ *häufig verschieden, aber konjugiert zueinander und als Gruppen gilt* $\mathrm{Stab}(x) \simeq \mathrm{Stab}(y)$.

*Beweis.* Es gilt $Gx = Gy$ genau dann, wenn es ein $a \in G$ mit $y = ax$ gibt. Falls $by = y$, d. h. falls $b \in \mathrm{Stab}(y)$, dann gilt $bax = ax$ und daher $(a^{-1}ba)x = x$. Also ist $a^{-1}ba \in \mathrm{Stab}(x)$ und damit $a^{-1}\,\mathrm{Stab}(y)a \subseteq \mathrm{Stab}(x)$. Die umgekehrte Inklusionen geht analog. □

ex:action:right

*Beispiel* 1.3.8. Seien $X = G$ und $G \times G \to G$, $(a, b) \mapsto ba^{-1}$. Das ist eine Gruppenwirkung. Die einzige Bahn ist $G$ und $\mathrm{Stab}(b) = \{e\}$ für alle $b \in G$.

*Achtung:* $\varphi\colon (b, a) \mapsto ba$ definiert im Allgemeinen keine Wirkung. Es gilt $\varphi(a_1a_2, b) = b(a_1a_2)$, aber $\varphi(a_1, \varphi(a_2b)) = (ba_2)a_1 = b(a_2a_1)$, d. h. $\varphi$ ist nicht kompatibel.

ex:centralisor

*Beispiel* 1.3.9. Seien $X = G$ und $G \times G \to G$, $(a, b) \mapsto aba^{-1}$. Das ist eine Gruppenwirkung, und es gilt
$$\mathrm{Stab}(b) = \{a \in G \mid aba^{-1} = b\} =: Z(b)$$
für alle $b \in G$, der sog. **Zentralisator** von $b$. Es gibt eventuell viele Bahnen.

*Beispiel* 1.3.10. Wir können Beispiele 1.3.6 und 1.3.8 modifizieren: Seien $X = G$ und $H \subset G$ eine Untergruppe. Betrachte die Wirkung $H \times G \to G$, $(a, b) \mapsto ab$. Dann sind die Bahnen die Rechtsnebenklassen von $H$, d. h. $H\backslash G = \{Hb \mid b \in G\}$, und $\mathrm{Stab}(b) = \{e\}$ für alle $b \in G$, denn $\mathrm{Stab}(b)$ ist Teilmenge des Stabilisators bzgl. der Wirkung $G \times G \to G$, $(a, b) \mapsto ab$.

Betrachte Analog die Wirkung $H \times G \to G$, $(a, b) \mapsto ba^{-1}$. Dann sind die Bahnen die Linksnebenklassen und wir haben $G/H = H\backslash G$. (Notationskonflikt: $H\backslash G$ sind hier nicht Rechtsnebenklassen, sondern Bahnen!)

ex:action:gl

*Beispiel* 1.3.11. Sei $X = K^n$ ein $K$-Vektorraum und betrachte $G = \mathrm{GL}(n, K)$ mit der Wirkung
$$\mathrm{GL}(n, K) \times K^n \longrightarrow K^n, \qquad (A, v) \longmapsto Av.$$
Die Bahnen sind $K^n \setminus \{0\}$ und $\{0\}$ (für zwei nichttriviale Vektoren finden wir immer eine Matrix, die den einen in den anderen überführt), d. h. $|\mathrm{GL}(n, K)\backslash K^n| = 2$. Ferner gilt
$$\mathrm{Stab}(e_1) = \left\{ \begin{pmatrix} 1 & * & \cdots & * \\ 0 & & & \\ \vdots & & A & \\ 0 & & & \end{pmatrix} \;\middle|\; A \in \mathrm{GL}(n-1, K) \right\}.$$
Diese Matrizen sind wirklich invertierbar, denn entwickeln wir die Determinante nach der ersten Spalte, so ist das genau dann invertierbar, wenn $\det(A) \neq 0$.

*Beispiel* 1.3.12. Seien $X = K^{n+1} \setminus \{0\}$ und $G = K^* \coloneqq K \setminus \{0\}$. Betrachte die Wirkung

$$K^* \times (K^{n+1} \setminus \{0\}) \longrightarrow K^{n+1} \setminus \{0\}, \qquad (\lambda, v) \longmapsto \lambda v.$$

Die Bahnen sind dann $K^*v \subset K^{n+1} \setminus \{0\}$, d. h. Geraden durch 0 ohne den Punkt 0. Die Stabilisatoren sind $\mathrm{Stab}(v) = \{e\}$, denn für $v \in K^{n+1} \setminus \{0\}$ ist $\lambda v = v$ genau dann, wenn $\lambda = 1$. Die Menge der Bahnen nennt man den **projektiven Raum**

$$\mathbb{P}^n_K \coloneqq K^* \backslash (K^{n+1} \setminus \{0\}) = \{L \setminus \{0\} \mid L \subset K^{n+1} \text{ Gerade}\}.$$

*Beispiel* 1.3.13. Einige Anwendungen.

(i) Betrachte $S_n$ mit der üblichen Wirkung $S_n \times \{1, \dots, n\} \to \{1, \dots, n\}$. Für $i \in \{1, \dots, n\}$ gilt

$$\mathrm{Stab}(x) = \{\sigma \in S_n \mid \sigma(i) = i\} = \mathrm{Bij}\{1, \dots, i-1, i+1, \dots, n\} \simeq S_{n-1}.$$

Diese Wirkung ist **transitv**, d. h. für alle $i, j \in \{1, \dots, n\}$ gibt es eine Permutation $\sigma$ mit $\sigma(i) = j$; insbesondere gibt es nur eine Bahn. Aus der Bahnengleichung 1.3.4 folgt $n = |\{1, \dots, n\}| = (S_n : S_{n-1})$, wobei $S_{n-1} = \mathrm{Stab}(n)$.

*Anmerkung:* Das beweist über Induktion den bekannten Fakt $|S_n| = n!$. Die Gruppenwirkung $S_{n-1} \times S_n \to S_n$, $(\sigma_1, \sigma_2) \mapsto \sigma_1\sigma_2$ liefert $S_n = \bigsqcup_{i=1}^{(S_n : S_{n-1})} S_{n-1}\sigma_i$ für geeignete Repräsentanten $\sigma_i$, also $n = (S_n : S_{n-1}) = |S_n|/|S_{n-1}|$ nach Satz von Lagrange 1.2.15.

(ii) Sei $D_n$ die Diedergruppe, welche die Symmetriegruppe des regulären $n$-Ecks ist. Seien $d_\theta$ die Rotation um $\theta = \frac{2\pi}{n}$ und $s$ die Spiegelung an der $x$-Achse. Betrachte die Wirkung auf der Menge der Ecken $D_n \times \{E_1, \dots, E_n\} \to \{E_1, \dots, E_n\}$.

Die Wirkung ist transitiv, d. h. es gibt nur eine Bahn. Tatsächlich ist schon die Wirkung der Untergruppe $\langle d_\theta \rangle \subset D_n$ transitiv. Aus der Bahnengleichung 1.3.4 und dem Satz von Lagrange 1.2.15 folgt

$$n = |\{E_1, \dots, E_n\}| = (D_n : \mathrm{Stab}(E_1)) = \frac{|D_n|}{|\mathrm{Stab}(E_1)|},$$

aber $|\mathrm{Stab}(E_1)| = |\langle s \rangle| = 2$. Folglich ist $|D_n| = 2n$.

(iii) Sei $\mathbb{F}$ ein endlicher Körper, also z. B. $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$, und sei $q \coloneqq |\mathbb{F}|$ (wir zeigen später, dass $q$ eine Primzahlpotenz ist). Dann ist $|\mathbb{F}^n| = q^n$.

Betrachte die Wirkung $\mathrm{GL}(n, \mathbb{F}) \times \mathbb{F}^n \to \mathbb{F}^n$. Dann gilt mit Beispiel 1.3.11:

$$\begin{aligned}
|\mathrm{GL}(n, \mathbb{F})| &= (\mathrm{GL}(n, \mathbb{F}) : \mathrm{Stab}(e_1)) \cdot |\mathrm{Stab}(e_1)| \\
&= |\mathrm{GL}(n, \mathbb{F})e_1| \cdot |\mathrm{Stab}(e_1)| \\
&= |\mathbb{F}^n \setminus \{0\}| \cdot |\mathrm{Stab}(e_1)| \\
&= (q^n - 1) \left| \left\{ \begin{pmatrix} 1 & * & \cdots & * \\ 0 & & & \\ \vdots & & A & \\ 0 & & & \end{pmatrix} \;\middle|\; A \in \mathrm{GL}(n-1, K) \right\} \right|.
\end{aligned}$$

*Behauptung:* Es gilt $|\mathrm{GL}(n,\mathbb{F})| = \prod_{r=0}^{n-1}(q^n - q^r)$.

*Beweis:* Wir zeigen das über Induktion. Es gilt $|\mathrm{GL}(1,\mathbb{F})| = q-1$. Für $n \geq 2$ ist

$$|\mathrm{Stab}(e_1)| = |\mathrm{GL}(n-1,\mathbb{F})|q^{n-1} = \prod_{r=0}^{n-2}(q^{n-1} - q^r)q^{n-1}$$

(es gibt $|\mathrm{GL}(n-1,\mathbb{F})|$ Möglichkeiten für $A$ und $q^{n-1}$ Möglichkeiten für die Einträge $*$), woraus die Behauptung folgt.

**Aufgabe 1.3.14.** Aus $|D_n| = 2n$ lässt sich (erneut, vgl. lineare Algebra) schließen, dass $D_n = \langle d_\theta, s\rangle$.

*Lösung.* $d_\theta$ erzeugt insgesamt $n$ unterschiedliche Symmetrien $\langle d_\theta\rangle = \{d_\theta^k \mid 0 \leq k < n\}$, denn $d_\theta^k(E_1) = E_k$. Rechtsmultiplikation mit $s$ liefert $n$ weitere Symmetrien $\langle d_\theta\rangle s = \{d_\theta^k s \mid 0 \leq k < n\}$. Diese unterscheiden sich von denen in $\langle d_\theta\rangle$ dadurch, dass die Reihenfolge der Ecken entgegengesetzt ist. Folglich ist $12 \leq |\langle d_\theta, s\rangle| \leq |D_n| = 12$, also $D_n = \langle d_\theta, s\rangle$.

**Beobachtung 1.3.15.** Wie viele Wirkungen einer Gruppe $G$ auf einer Menge $X$ gibt es?

Es gibt eine Bijektion zwischen Gruppenwirkungen $G \times X \to X$ und Gruppenhomomorphismen $G \to \mathrm{Bij}(X)$. Diese ist gegeben durch

$$[G \times X \longrightarrow X] \longmapsto [a \longmapsto [x \longmapsto ax]].$$

Hier müsste man noch prüfen, dass die Abbildung wohldefiniert ist, d. h. dass die Axiome der Gruppenwirkung genau den Axiomen eines Gruppenhomomorphismus entsprechen.

*Beispiel* 1.3.16. Sei $X = \{1,\dots,n\}$. In diesem Fall ist $\mathrm{Bij}(X) = S_n$. Damit entsprechen Wirkungen von $G$ auf $\{1,\dots,n\}$ den Gruppenhomomorphismen $G \to S_n$.

**Korollar 1.3.17 (Klassengleichung).** *Seien $G$ eine endliche Gruppe und*

$$Z(G) \coloneqq \{a \in G \mid ab = ba \text{ für alle } b \in G\}$$

*das **Zentrum**. Dann gilt*

$$|G| = |Z(G)| + \sum_{i=1}^{n}(G : Z(a_i)),$$

*wobei $Z(a) \coloneqq \{b \in G \mid ab = ba\}$ der Zentralisator von $a$ ist und die $a_i$ so gewählt sind, dass $G \setminus Z(G) = \bigsqcup_{i=1}^{n}\{aa_ia^{-1} \mid a \in G\}$.*

*Beweis.* Wir betrachten die Wirkung $G \times G \to G$, $(a,b) \mapsto aba^{-1}$, welche durch Konjugation gegeben ist.

Beobachte, dass $b \in Z(G)$ genau dann, wenn $Gb = \{b\}$. Falls $b \in Z(G)$, so gilt nämlich $|Gb| = (G : \mathrm{Stab}(b)) = 1$. Da $G$ die disjunkte Vereinigung der Bahnen ist, ist $G = Z(G) \sqcup (G \setminus Z(G)) = Z(G) \sqcup \bigsqcup_{i=1}^{n} Ga_i$. Die Behauptung folgt aus Fakt 1.3.3 und Beispiel 1.3.9. □

**Bemerkung 1.3.18.** Diese Formel ist sehr nützlich. Es folgt direkt

$$|G| = |Z(G)| + \sum_{i=1}^{n} \frac{|G|}{|\mathrm{Stab}(a_i)|}.$$

Die Summanden $|G|/|\mathrm{Stab}(a_i)|$ sind insbesondere ungleich 1 und $|\mathrm{Stab}(a_i)|$ teilt $|G|$. Ist z. B. $|G| = p^n$, so ist $p$ ein Teiler von $|Z(G)|$, d. h. $Z(G) \neq \{e\}$.

*Beispiel* 1.3.19. Sei $S_n \times \{1, \dots, n\} \to \{1, \dots, n\}$ die Standardwirkung. Jedes $\sigma \in S_n$ induziert die Wirkung $\langle\sigma\rangle \times \{1, \dots, n\} \to \{1, \dots, n\}$. Dann ist $\{1, \dots, n\}$ die disjunkte Vereinigung der Bahnen der Wirkung von $\langle\sigma\rangle$, sagen wir $M_1 \sqcup \dots \sqcup M_k$. Genauer sind

$$\begin{aligned} M_1 &\coloneqq \{i_{11}, i_{12} \coloneqq \sigma(i_{11}), i_{13} \coloneqq \sigma^2(i_{11}), \dots, i_{1n_1}\}, \\ &\vdots \\ M_k &\coloneqq \{i_{k1}, i_{k2} = \sigma(i_{k1}), \dots, i_{k,n_k}\}. \end{aligned}$$

Also ist $\sigma = (i_{11}, \dots, i_{1n_1}) \circ \dots \circ (i_{k1}, \dots, i_{kn_k})$, d. h. $\sigma$ ist die Komposition disjunkter Zyklen. Diese Darstellung ist eindeutig bis auf Permutation der Zyklen.[12]

## 1.4 Endlich erzeugte abelsche Gruppen

Das Ziel ist folgendes Theorem zur Klassifikation endlich erzeugter abelscher Gruppen bis auf Isomorphie. Damit haben wir ein komplettes Bild dieser Gruppen.[13]

abelian:fundamental

**Satz 1.4.1 (Fundamentalsatz für endlich erzeugte abelsche Gruppen).** *Sei $G$ eine endlich erzeugte abelsche Gruppe. Dann ist*

$$G \simeq \mathbb{Z}^{\oplus r} \times \prod_{i=1}^{N} \mathbb{Z}/p_i^{n_i}\mathbb{Z},$$

*wobei $\mathbb{Z}^{\oplus r} \coloneqq \mathbb{Z} \oplus \dots \oplus \mathbb{Z}$ und die $p_i$ (nicht notwendigerweise verschiedene) Primzahlen sind. Diese Zerlegung ist eindeutig bis auf Permutation. Hierbei heißt $r$ der **Rang** der Gruppe $G$.*

**Notation 1.4.2.** Da hier alle Gruppen abelsch sind, benutzen wir die additive Schreibweise.

not:pgroup

**Notation 1.4.3.** Seien $G$ eine abelsche Gruppe und $p$ eine Primzahl. Dann sei

$$G(p) \coloneqq \{a \in G \mid |a| = p^n \text{ für ein } n\}.$$

$G(p) \subset G$ ist eine Untergruppe, denn für $a, b \in G(p)$ folgt aus $p^n a = 0 = p^m b$ dann $p^{m+n}(a + b) = 0$, d. h. $a + b \in G(p)$.

[12] Vgl. Satz 1.6.3.

[13] Eine Verallgemeinerung ist der *Strukturssatz für endlich erzeugte Moduln über Hauptidealringen.*

**Satz 1.4.4.** *Sei $G$ eine endlich erzeugte abelsche Gruppe, sodass $|a| < \infty$ für alle $a \in G$ (in diesem Fall ist $G$ eine **Torsionsgruppe**). Dann induzieren die natürlichen Injektionen $G(p) \hookrightarrow G$ einen Isomorphismus*

$$\bigoplus_{p \text{ prim}} G(p) \xrightarrow{\sim} G.$$

*Beweis.* Zur Surjektivität: Setze

$$G_n \coloneqq \operatorname{Ker}(G \longrightarrow G, a \longmapsto na) = \{a \in G \mid na = 0\}.$$

Seien $n = n_1 n_2$ mit $n_1$ und $n_2$ teilerfremd. Wir behaupten, dass $G_n = G_{n_1} + G_{n_2}$, d. h. jedes Element $a$ mit $na = 0$ lässt sich schreiben als $a = a_1 + a_2$ mit $n_i a_i = 0$. Um das zu zeigen, schreiben wir $1 = k_1 n_1 + k_2 n_2$, was wegen der Teilerfremdheit von $n_1$ und $n_2$ möglich ist. Für alle $a \in G_n$ gilt also $a = k_1 n_1 a + k_2 n_2 a$ mit $a_1 \coloneqq k_2 n_2 a \in G_{n_1}$ und $a_2 \coloneqq k_1 n_1 a \in G_{n_2}$. Das zeigt die Behauptung.

Sei nun allgemeiner $a \in G$ mit $na = 0$, wobei $n = \prod_{i=1}^{N} p_i^{m_i}$ mit paarweise verschiedenen Primzahlen $p_i$. Nach Induktion ist $a = \sum_{i=1}^{N} a_i$ mit $a_i \in G(p_i)$ (wir können induktiv Primpotenzen von $n$ abspalten). Damit ist $\bigoplus_p G(p) \to G$ surjektiv.

Zur Injektivität: Betrachte endlich viele $a_i \in G(p_i)$ mit $\sum_{i=1}^{k} a_i = 0$, d. h. $(a_i)_{i=1}^{k}$ ist ein Element im Kern der Abbildung. Es gibt $m_i$ mit $|a_i| = p_i^{m_i}$ und es folgt

$$\prod_{i=1}^{k-1} p_i^{m_i} \sum_{i=1}^{k} a_i = \prod_{i=1}^{k-1} p_i^{m_i} a_k = 0.$$

Da $p_k$ und $\prod_{i=1}^{k-1} p_i^{m_i}$ teilerfremd sind, muss $a_k = 0$ sein. Per Induktion gilt $a_i = 0$ für alle $i$. Somit ist der Kern trivial und $\bigoplus_p G(p) \to G$ injektiv. □

**Definition 1.4.5.** Eine Gruppe $G$ heißt **$p$-Gruppe** mit $p$ prim, falls für jedes $a \in G$ ein gewisses $n$ existiert, sodass $|a| = p^n$.

VL 5
27.10.23

**Bemerkung 1.4.6.** Man kann zeigen, dass eine endliche Gruppe genau dann eine $p$-Gruppe ist, wenn $|G| = p^N$ für ein $N$.

*Beispiel* 1.4.7. $G(p)$ in Notation 1.4.3 ist eine $p$-Gruppe.

thm:abelian:pgroup

**Satz 1.4.8.** *Sei $G$ eine endliche abelsche $p$-Gruppe. Dann existiert ein Isomorphismus*

$$G \simeq \mathbb{Z}/p^{n_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p^{n_k}\mathbb{Z}$$

*Beweis.* Für alle $a \in G$ gibt es ein $n$, sodass $|a| = p^n$. Daher existiert ein $n_1$, sodass $|a| \leq p^{n_1}$ für alle $a \in G$ und $|a_1| = p^{n_1}$ für ein $a_1 \in G$ (da $G$ endlich ist, gibt es ein Element $a_1$ maximaler Ordnung). Definiere $G_1 \coloneqq \langle a_1 \rangle \subset G$, wobei $G_1 \simeq \mathbb{Z}/p^{n_1}\mathbb{Z}$. Nach Induktionsvoraussetzung ist $G/G_1 \simeq \mathbb{Z}/p^{n_2}\mathbb{Z} \times \cdots \times \mathbb{Z}/p^{n_k}\mathbb{Z}$ (dabei existiert $G/G_1$, da $G$ abelsch ist). Wir erhalten die

**kurze exakte Sequenz**[14]

$$G_1 \simeq \mathbb{Z}/p^{n_1}\mathbb{Z} \overset{\lhd}{\hookrightarrow} G \twoheadrightarrow G' \coloneqq G/G_1 \simeq \mathbb{Z}/p^{n_2}\mathbb{Z} \times \cdots \times \mathbb{Z}/p^{n_k}\mathbb{Z}.$$

Unser Ziel ist $G \simeq \mathbb{Z}/p^{n_1}\mathbb{Z} \times \mathbb{Z}/p^{n_2}\mathbb{Z} \times \cdots \times \mathbb{Z}/p^{n_k}\mathbb{Z}$. Dazu müssen wir Elemente aus $G'$ geeignet nach $G$ liften, sodass der Lift dieselbe Ordnung wie das Element hat.

*Behauptung:* Definiere $G_{p^i} \coloneqq \{a \in G \mid |a| = p^i\}$ und analog $G'_{p^i} \coloneqq \{a \in G' \mid |a| = p^i\}$ für jedes $i \in \mathbb{N}$. Dann induziert die Projektion $G \twoheadrightarrow G'$ eine Surjektion $G_{p^i} \twoheadrightarrow G'_{p^i}$.

*Beweis:* Bezeichne $\pi\colon G \twoheadrightarrow G'$. Sei $b \in G$, sodass $\bar{b} \coloneqq \pi(b) \in G'_{p^i}$, d. h. $b$ ist ein Lift von $\bar{b}$ nach $G$. Wir ändern nun $b$ ab, sodass im Endeffekt $|b| = p^i$ gilt, d. h. $b \in G_{p^i}$. Da $\pi(p^i b) = p^i \pi(b) = p^i \bar{b} = 0$ in $G'$, gilt $p^i b \in \operatorname{Ker}(\pi) = G_1 = \langle a_1 \rangle$. Also gilt $p^i b = k a_1$ für ein $k$. Schreibe $k = p^m k'$ mit $p \nmid k'$, woraus $|a_1| = |k' a_1| = p^{n_1}$ folgt (Aufgabe 9).

Falls $m \geq n_1$, so folgt $p^i b = k a_1 = p^m k' a_1 = 0$ und daher $b \in G_{p^i}$. Andernfalls ist $m < n_1$. Es folgt $|k a_1| = p^{n_1 - m}$ und daher $|b| = p^{n_1 - m + i}$. Wegen der Maximalität von $n_1$ muss $n_1 - m + i \leq n_1$ sein und damit $i \leq m$. Dann können wir $p^i b = k a_1 = p^m k' a_1 = p^i (p^{m-i} k' a_1)$ schreiben. Ändere $b$ nun zu $b' \coloneqq b - p^{m-i} k' a_1$ ab. Dann gilt $\pi(b') = \pi(b) - \pi(p^{m-i} k' a_1) = \bar{b}$, da $\operatorname{Ker}(\pi) = \langle a_1 \rangle$, und es gilt $p^i b' = 0$. Daraus folgt die Behauptung.

Mit der Behauptung folgt aus der Induktionsvoraussetzung, dass wir Elemente $\bar{a}_i \in G'$ zu Elementen $a_i \in G$ mit $|\bar{a}_i| = |a_i| = p^{n_i}$ für $i = 1, \ldots, k$ liften können. Wir müssen nun zeigen, dass die induzierte Abbildung

$$\varphi\colon \mathbb{Z}/p^{n_1}\mathbb{Z} \times \mathbb{Z}/p^{n_2}\mathbb{Z} \times \cdots \times \mathbb{Z}/p^{n_k}\mathbb{Z} \longrightarrow G, \qquad (\bar{m}_1, \ldots, \bar{m}_k) \longmapsto m_1 a_1 + \cdots + m_k a_k$$

ein Isomorphismus ist.

Beobachte für die Surjektivität, dass $G_1 \subset \operatorname{Im}(\varphi)$, da $G_1 = \varphi(\mathbb{Z}/p^{n_1}\mathbb{Z})$. Weil $\pi \circ \varphi$ nach Induktionsvoraussetzung surjektiv ist, existieren für beliebige $a \in G$ Zahlen $m_2, \ldots, m_k \in \mathbb{N}$, sodass $a - \sum_{i=2}^{k} m_i a_i = l a_1 \in \operatorname{Ker}(\pi) = \langle a_1 \rangle$ für ein $l \in \mathbb{N}$. Also gilt $a = \varphi(\bar{l}, \bar{m}_2, \ldots, \bar{m}_k)$.

Beobachte für die Injektivität, dass wenn $\varphi(\bar{m}_1, \ldots, \bar{m}_k) = 0$, dann $\pi \circ \varphi(\bar{m}_1, \ldots, \bar{m}_k) = m_2 \bar{a}_2 + \cdots + m_k \bar{a}_k = 0$ in $G'$ gilt. Da $G' = G/G_1 \simeq \mathbb{Z}/p^{n_2}\mathbb{Z} \times \cdots \times \mathbb{Z}/p^{n_k}\mathbb{Z}$, folgt sodann $\bar{m}_i = 0 \in \mathbb{Z}/p^{n_i}$ für $i \geq 2$. Also ist $\varphi(\bar{m}_1, \ldots, \bar{m}_k) = \varphi(\bar{m}_1, 0, \ldots, 0) = m_1 a_1$. Wenn das verschwindet, so ist $\bar{m}_1 = 0$ in $\mathbb{Z}/p^{n_1}\mathbb{Z}$. □

cor:abelian:finite

**Korollar 1.4.9.** *Falls $G$ eine endliche abelsche Gruppe ist, was auch eine endlich erzeugte abelsche Torsionsgruppe ist, dann gilt*

$$G \simeq \prod_{i=1}^{k} \mathbb{Z}/p_i^{n_i}\mathbb{Z}$$

*für gewisse Primzahlen $p_i$ (wobei $p_i = p_j$ erlaubt ist) und $n_i \in \mathbb{N}$.*

[14] Eine Sequenz

$$\cdots \xrightarrow{\varphi_{i-2}} G_{i-1} \xrightarrow{\varphi_{i-1}} G_i \xrightarrow{\varphi_i} G_{i+1} \xrightarrow{\varphi_{i+1}} \cdots$$

von Gruppenhomomorphismen $\varphi_i\colon G_i \to G_{i+1}$ ist **exakt**, falls $\operatorname{Im}(\varphi_i) = \operatorname{Ker}(\varphi_{i+1})$ für alle $i$. Eine exakte Sequenz ist **kurz** falls sie von der Form $0 \to G_1 \to G_2 \to G_3 \to 0$ ist (mit unendlich vielen Nullen auf beiden Seiten). In diesem Fall sind $G_1 \hookrightarrow G_2$ injektiv und $G_2 \twoheadrightarrow G_3$ surjektiv. Ein sehr häufiges Beispiel ist folgendes: Sei $H \lhd G$. Dann ist $0 \to H \to G \to G/H \to 0$ eine kurze exakte Sequenz.

thm:abelian:free

**Satz 1.4.10.** *Jede endlich erzeugte torsionsfreie Gruppe ist isomorph zu $\mathbb{Z}^{\oplus r}$ für ein $r$.*

*Beweis.* Schreibe die endlich erzeugte Gruppe als $G = \langle a_1, \dots, a_N \rangle$. O. B. d. A. sei $a_i \neq 0$ für alle $i$. Nach Voraussetzung gilt $|a_i| = \infty$ für alle $i$. Wir können annehmen, dass $a_1, \dots, a_k$ mit $1 \leq k \leq N$ linear unabhängig sind, d. h. $\sum_{i=1}^{k} m_i a_i = 0$ mit $m_i \in \mathbb{Z}$ impliziert $m_1 = \cdots = m_k = 0$. Damit ist die Abbildung

$$\mathbb{Z}^{\oplus k} \xrightarrow{\sim} H \coloneqq \langle a_1, \dots, a_k \rangle \subset G, \qquad (m_1, \dots, m_k) \longmapsto m_1 a_1 + \cdots + m_k a_k$$

ein Isomorphismus.

Ist $H = G$, so sind wir fertig. Andernfalls gibt es ein $a \in \{a_1, \dots, a_N\} \setminus H$. Wenn $a_1, \dots, a_k, a$ linear unabhängig sind, so gilt $\mathbb{Z}^{\oplus k+1} \xrightarrow{\sim} H' \coloneqq \langle a_1, \dots, a_k, a \rangle \subset G$ und wir können $H$ durch $H'$ ersetzen. Dieses Prozedere können wir wiederholen und bricht irgendwann ab. Reduziere nun auf den Fall, dass $a_1, \dots, a_k$ linear unabhängig sind, und dass für jedes $a_i$ Zahlen $m, m_1, \dots, m_k \in \mathbb{Z}$ existieren, sodass $ma_i + \sum_{i=1}^{k} m_i a_i = 0$ in $G$ gilt, d. h. $ma_i \in H = \langle a_1, \dots, a_k \rangle$. Da $G$ endlich erzeugt ist, existiert ein $m \in \mathbb{Z}$, sodass $ma \in \langle a_1, \dots, a_k \rangle$ für alle $a \in G$; setze nämlich $m$ als das Produkt aller Koeffizienten vor den $a_i$. Also ist $mG \subset H$. Betrachte $G \to mG \subset H$, $a \mapsto ma$. Da $G$ torsionsfrei ist, ist $G \xrightarrow{\sim} mG \subset H$ Isomorphismus, wobei $H \simeq \mathbb{Z}^{\oplus k}$ frei abelsch ist.

Wir müssen nun zeigen, dass jede Untergruppe eine freien abelschen Gruppe wieder frei abelsch ist. Der Beweis erfolgt per Induktion. Für den Induktionsanfang stellen wir fest, dass jede Untergruppe von $\mathbb{Z}$ von der Form $n\mathbb{Z} \simeq \mathbb{Z}$ und damit frei abelsch ist. Für den Induktionsschritt betrachten wir das kommutative Diagramm

$$\begin{array}{ccccc} & & G & \twoheadrightarrow & G' \coloneqq \pi(G) \\ & & \downarrow & & \downarrow \\ \mathbb{Z} \simeq \operatorname{Ker}(\pi) & \hookrightarrow & \mathbb{Z}^{\oplus k} & \xrightarrow{\pi} & \mathbb{Z}^{\oplus k-1} \end{array}$$

wobei $\pi \colon \mathbb{Z}^{\oplus k} \to \mathbb{Z}^{\oplus k-1}$, $(a_1, \dots, a_k) \mapsto (a_1, \dots, a_{k-1})$.[15] Nach Induktionsvoraussetzung ist $G'$ frei abelsch, d. h. $G' \simeq \mathbb{Z}^{\oplus n}$. Ferner ist $G \cap \operatorname{Ker}(\pi) \subset \mathbb{Z}$ eine Untergruppe und damit auch frei abelsch. Wir erhalten die kurze exakte Sequenz

$$\operatorname{Ker}(\pi) \cap G \overset{\lhd}{\hookrightarrow} G \twoheadrightarrow G' \coloneqq \pi(G) \simeq \mathbb{Z}^{\oplus n} \simeq G/(\operatorname{Ker}(\pi) \cap G).$$

(der letzte Isomorphismus ist Korollar 1.2.23). Falls $\operatorname{Ker}(\pi) \cap G = 0$, dann ist $G \simeq G' \simeq \mathbb{Z}^{\oplus n}$ frei abelsch. Falls $\operatorname{Ker}(\pi) \cap G \neq 0$, dann induziert die Inklusion $\operatorname{Ker}(\pi) \cap G \hookrightarrow G$ eine Abbildung $(\operatorname{Ker}(\pi) \cap G) \times G' \to G$, indem wir Urbilder von den freien Erzeugern $e_1, \dots, e_n \in G' \simeq \mathbb{Z}^{\oplus n}$ wählen. Analog zum Beweis von Satz 1.4.8 zeigen wir, dass die Abbildung ein Isomorphismus ist, d. h. $G \simeq \mathbb{Z}^{\oplus n+1}$. □

*Beweis des Fundamentalsatzes Satz 1.4.1.* Sei $G_{\text{tors}} \coloneqq \{a \in G \mid |a| < \infty\}$, was eine Untergruppe ist, da $G$ abelsch ist. Wir müssen zeigen, dass auch $G_{\text{tors}}$ wieder endlich erzeugt ist. Dazu zeigen wir folgende allgemeinere Aussage:

[15] Hier passiert *abuse of notation*: Wir fassen $G \hookrightarrow \mathbb{Z}^{\oplus k}$ nicht nur als injektiven Gruppenhomomorphismus, sondern als *Inklusion* auf, d. h. $G$ ist eine Untergruppe von $\mathbb{Z}^{\oplus k}$. Das können wir realisieren, indem wir $G$ durch die zu $G$ isomorphe Untergruppe von $\mathbb{Z}^{\oplus k}$ ersetzen.

*Behauptung:* Für endlich erzeugte *abelsche* Gruppen $G$ und Untergruppen $H \subset G$ ist $H$ wieder endlich erzeugt.

*Beweis:* Da $G$ endlich erzeugt ist, existiert eine Surjektion $\pi\colon \mathbb{Z}^{\oplus k} \twoheadrightarrow G$; falls $G = \langle a_1, \dots, a_k\rangle$, so ist die Surjektion explizit gegeben durch $e_i \mapsto a_i$. Es genügt zu zeigen, dass $\tilde{H} \coloneqq \pi^{-1}(H) \subset \mathbb{Z}^{\oplus k}$ endlich erzeugt ist.

Wir beweisen das über Induktion. Falls $k = 1$, so sind alle Untergruppen von $\mathbb{Z}$ endlich erzeugt, denn diese sind von der Form $n\mathbb{Z}$. Für den Induktionsschritt betrachten wir

$$\psi\colon \mathbb{Z}^{\oplus k} \longrightarrow\!\!\!\!\!\rightarrow \mathbb{Z}^{\oplus k-1}, \qquad (a_1, \dots, a_k) \longmapsto (a_1, \dots, a_{k-1})$$

mit $\operatorname{Ker}(\psi) = \{(0, \dots, 0, a) \mid a \in \mathbb{Z}\} \simeq \mathbb{Z}$. Dann ist $\psi(\tilde{H}) \subset \mathbb{Z}^{\oplus k-1}$ eine Untergruppe, welche nach Induktionsvoraussetzung endlich erzeugt ist. Wähle nun $\alpha_1, \dots, \alpha_N \in \tilde{H}$, sodass $\psi(\tilde{H}) = \langle \psi(\alpha_1), \dots, \psi(\alpha_N)\rangle$. Ferner ist $\tilde{H} \cap \operatorname{Ker}(\psi) \subset \mathbb{Z}$ eine Untergruppe und damit wird $\tilde{H} \cap \operatorname{Ker}(\psi)$ durch ein Element $\alpha$ erzeugt. Somit gilt $\tilde{H} = \langle \alpha_1, \dots, \alpha_N, \alpha\rangle$ (d. h. es gibt eine Surjektion $\mathbb{Z}^{\oplus N+1} \twoheadrightarrow \tilde{H}$).[16] Damit ist die Behauptung bewiesen.

Also ist $G_{\text{tors}}$ endlich erzeugt, und nach Definition hat jeder Erzeuger endliche Ordnung. Folglich ist $G_{\text{tors}}$ endlich und nach Korollar 1.4.9 gilt $G_{\text{tors}} \simeq \prod_{i=1}^{k} \mathbb{Z}/p_i^{n_i}\mathbb{Z}$. Andererseits ist $G/G_{\text{tors}}$ torsionsfrei und endlich erzeugt, weshalb nach Satz 1.4.10 dann $G/G_{\text{tors}} \simeq \mathbb{Z}^{\oplus r}$. Der letzte Schritt ist die folgende kurze exakte Sequenz:

$$G_{\text{tors}} \simeq \textstyle\prod_{i=1}^{k} \mathbb{Z}/p_i^{n_i}\mathbb{Z} \hookrightarrow G \longrightarrow\!\!\!\!\!\rightarrow G/G_{\text{tors}} \simeq \mathbb{Z}^{\oplus r}$$

Analog zum Beweis von Satz 1.4.8 erhalten wir den Isomorphismus $G_{\text{tors}} \times G/G_{\text{tors}} \xrightarrow{\sim} G$. □

*Beweis der Eindeutigkeit*.* Eindeutigkeit wurde in der Vorlesung nicht gezeigt. Das folgt so: Angenommen

$$\mathbb{Z}^{\oplus r} \times \prod_{i=1}^{N} \mathbb{Z}/p_i^{n_i}\mathbb{Z} \simeq \mathbb{Z}^{\oplus s} \times \prod_{j=1}^{M} \mathbb{Z}/q_j^{m_j}.$$

Betrachten wir die Ordnung der Elemente, so erhalten wir Isomorphismen $\mathbb{Z}^{\oplus r} \simeq \mathbb{Z}^{\oplus s}$ (Elemente unendlicher Ordnung) und

$$G \coloneqq \prod_{i=1}^{N} \mathbb{Z}/p_i^{n_i}\mathbb{Z} \simeq G' \coloneqq \prod_{j=1}^{M} \mathbb{Z}/q_j^{m_j}\mathbb{Z}$$

(Elemente endlicher Ordnung). Nun gilt $\prod_{i=1}^{N} p_i^{n_i} = |G| = |G'| = \prod_{j=1}^{M} q_j^{m_j}$, d. h. aus der Eindeutigkeit der Primfaktorzerlegung folgt, dass auf beiden Seiten dieselben Primzahlen vorkommen. Ist $a \in G$ von Ordnung $p^k$, so sind die $n_i$-ten Einträge von $a$ mit $p_i \neq p$ null. Folglich erhalten wir einen Isomorphismus von $p$-Gruppen $G(p) \simeq G'(p)$.

Wir reduzieren also auf den Fall

$$G(p) \coloneqq \prod_{i=1}^{N} \mathbb{Z}/p^{n_i}\mathbb{Z} \simeq \prod_{j=1}^{M} \mathbb{Z}/p^{m_j}\mathbb{Z} =: G'(p),$$

[16] Hier stand irgendeine Nebenbemerkung in Klammern. Wenn das jemand weiß, wäre ich sehr dankbar, wenn sie oder er mir das schreiben kann.

wobei o. B. d. A. $n_1 \leq \cdots \leq n_N$ sowie $m_1 \leq \cdots \leq m_M$. Weil alles abelsch ist, sind $p^{k+1}G(p) \subset p^kG(p)$ beides Untergruppen von $G(p)$ für $1 \leq k < n_N$, wobei $p^kG(p) = \prod_{i=1}^N p^k\mathbb{Z}/p^{n_i}\mathbb{Z}$. Insbesondere ist

$$(p^k\mathbb{Z}/p^{n_i}\mathbb{Z})/(p^{k+1}\mathbb{Z}/p^{n_i}\mathbb{Z}) \simeq \begin{cases} \{0\}, & \text{falls } k \geq n_i, \\ p^k\mathbb{Z}/p^{k+1}\mathbb{Z} \simeq \mathbb{Z}/p\mathbb{Z}, & \text{falls } k < n_i \end{cases}$$

(für $k < n_i$ folgt das aus dem zweiten Isomorphiesatz 1.2.26). Wir brauchen folgenden Fakt.

*Fakt:* Für abelsche Gruppen ist die direkte Summe von Quotientengruppen isomorph zum Quotient der direkten Summen, d. h. für eine Familie $\{(G_i, H_i) \mid i \in I\}$ von abelschen Gruppen $G_i$ und Untergruppen $H_i \subset G_i$ gilt

$$\bigoplus_{i\in I} G_i/H_i \simeq \left(\bigoplus_{i\in I} G_i\right) / \left(\bigoplus_{i\in I} H_i\right).$$

*Beweisidee:* Das zeigt man am besten über die universelle Eigenschaft des Quotienten (Homomorphiesatz 1.2.21) und der direkten Summe (Definition 1.1.20). Genauer: Man zeige mit Definition 1.1.20, dass jeder Gruppenhomomorphismus $\varphi\colon \bigoplus_{i\in I} G_i \to G'$ von abelschen Gruppen mit $\bigoplus_{i\in I} H_i \subset \operatorname{Ker}(\varphi)$ durch $\bigoplus_{i\in I} G_i/H_i$ faktorisiert. Aus der Universalität folgt bereits, dass $\bigoplus_{i\in I} G_i/H_i$ isomorph zur kanonischen Quotientengruppe ist. Alternativ weiß man vielleicht aus der Kategorientheorie, dass Kolimiten stets kommutieren!

O. B. d. A. sei $n_N = \max\{n_N, m_M\}$. Kommt $n_N$ genau $K$ mal unter den Zahlen $n_1, \ldots, n_N$ vor, so gilt

$$\begin{aligned} p^{n_N-1}G(p)/p^{n_N}G(p) &= \left(\prod_{i=1}^N p^{n_N-1}\mathbb{Z}/p^{n_i}\mathbb{Z}\right) / \left(\prod_{i=1}^N p^{n_N}\mathbb{Z}/p^{n_i}\mathbb{Z}\right) \\ &\simeq (\mathbb{Z}/p\mathbb{Z})^{\oplus K} \simeq p^{n_N-1}G'(p)/p^{n_N}G'(p) \end{aligned}$$

Da $n_N \geq m_M$, folgt $n_N = m_M$ und $m_M$ kommt genau $K$ mal unter den Exponenten $m_1, \ldots, m_M$ vor. Somit können wir $\prod_{i=N-K+1}^N \mathbb{Z}/p^{n_N}\mathbb{Z}$ aus $G(p) \simeq G'(p)$ herausteilen und erhalten den Isomorphismus

$$\prod_{i=1}^{N-K} \mathbb{Z}/p^{n_i}\mathbb{Z} \simeq \prod_{j=1}^{M-K} \mathbb{Z}/p^{m_j}\mathbb{Z}.$$

Fahre nun induktiv fort, bis wir $\{0\}$ erreichen, woraus wir $N = M$ schließen.

Bleibt noch $\mathbb{Z}^{\oplus r} \simeq \mathbb{Z}^{\oplus s}$. Analog zu eben ist $2\mathbb{Z}^{\oplus r} \simeq (2\mathbb{Z})^{\oplus r}$ eine Untergruppe von $\mathbb{Z}^{\oplus r}$. Wir erhalten

$$(\mathbb{Z}/2\mathbb{Z})^{\oplus r} \simeq \mathbb{Z}^{\oplus r}/2\mathbb{Z}^{\oplus r} \simeq \mathbb{Z}^{\oplus s}/2\mathbb{Z}^{\oplus s} \simeq (\mathbb{Z}/2\mathbb{Z})^{\oplus s}.$$

Beobachte, dass $(\mathbb{Z}/2\mathbb{Z})^{\oplus r}$ auf natürliche Weise ein Vektorraum über den Körper $\mathbb{Z}/2\mathbb{Z} = \mathbb{F}_2$ ist. Aus der linearen Algebra wissen wir, dass dann $r = s$ ist. □

## 1.5 Auflösbare Gruppen

*Auflösbare Gruppen* spielen eine entscheidende Rolle in der Galoistheorie. Demnach hat eine polynomielle Gleichung über einem Körper der Charakteristik null genau dann eine „Lösungsformel“, wenn ihre Galoisgruppe auflösbar ist.

**Definition 1.5.1.** Eine Gruppe $G$ heißt **einfach**, falls es außer trivialen Untergruppen $\{e\}$ und $G$ keine Normalteiler gibt.

**Bemerkung 1.5.2.** Die Idee ist also, eine Gruppe in gewisser Weise in einfache Gruppen zu zerlegen: Ist $H \lhd G$ ein Normalteiler, so ist $G/H$ eine Gruppe. Dann können wir $G$ durch die kurze exakte Sequenz

$$0 \longrightarrow H \longrightarrow G \longrightarrow G/H \longrightarrow 0$$

in „kleinere“ Gruppen $H$ und $G/H$ zerlegen.

*Achtung:* Die kleineren Gruppen $H$ und $G/H$ bestimmen $G$ eventuell nicht eindeutig.

**Warnung 1.5.3.** Eine einfache Gruppe kann nichttriviale Untergruppen enthalten.

**Definition 1.5.4.** Eine **Normalreihe** einer Gruppe $G$ ist eine Folge

$$\{e\} = G_n \lhd G_{n-1} \lhd \cdots \lhd G_0 = G.$$

*Beispiel* 1.5.5. Für $n = 1$ ist $\{e\} = G_1 \lhd G_0 = G$ stets eine Normalreihe.

**Definition 1.5.6.** Eine Gruppe $G$ heißt **auflösbar**, falls $G$ eine Normalreihe $\{e\} = G_n \lhd \cdots \lhd G_0 = G$ mit *abelschen* **Faktoren** oder **Quotienten** $G_i/G_{i+1}$ besitzt.

*Problem* 1.5.7. Wie können wir Normalteiler systematisch produzieren?

VL 6
30.10.23

**Definition 1.5.8.** Für jede Gruppe $G$ sei $[G, G] \subset G$ die **Kommutatorgruppe**. Sie ist definiert als die Untergruppe von $G$, die durch alle **Kommutatoren** erzeugt wird:

$$[G, G] \coloneqq \langle [a, b] \coloneqq aba^{-1}b^{-1} \mid a, b \in G \rangle.$$

**Bemerkung 1.5.9.** Es gelten $[a, b]^{-1} = (aba^{-1}b^{-1})^{-1} = bab^{-1}a^{-1} = [b, a]$ und $e = [a, a^{-1}]$ für alle $a, b \in G$.

**Warnung 1.5.10.** Im Allgemeinen ist $[a, b][a', b']$ kein Kommutator für $a, b, a', b' \in G$, d. h. $[G, G]$ muss durch Erzeuger definiert werden. Es gilt nämlich $[a, b][a', b'] = aba^{-1}b^{-1}a'b'a'^{-1}b'^{-1}$, was im Allgemeinen nicht von der Form $[c, d] = cdc^{-1}d^{-1}$ für $c, d \in G$ ist.

**Bemerkung 1.5.11.** Alle Elemente von $[G, G]$ sind von der Form $[a_1, b_1] \cdots [a_n, b_n]$.

lem:commutator

**Lemma 1.5.12.** *Für alle Gruppen $G$ gelten folgende Aussagen.*

(i) $[G, G] \lhd G$.

(ii) $G/[G, G]$ *ist abelsch.*

(iii) *Falls $H \lhd G$, sodass $G/H$ abelsch ist, dann ist $[G,G] \subset H$.*

In diesem Sinne ist die Kommutatorgruppe die kleinste Gruppe, um eine Gruppe zu *abelisieren*, d. h. ein $H \lhd G$ zu finden, sodass $G/H$ abelsch ist.

*Beweis.*

(i) Sei $\alpha \in [G,G]$, d. h. $\alpha = [a_1,b_1]\cdots[a_n,b_n]$. Zu zeigen ist, dass $\beta a \beta^{-1} \in [G,G]$ für alle $\beta \in G$. Wegen $\beta\alpha\beta^{-1} = (\beta[a_1,b_1]\beta^{-1})\cdots(\beta[a_n,b_n]\beta^{-1})$ genügt es zu zeigen, dass $\beta[a,b]\beta^{-1}$ ein Kommutator und daher in $[G,G]$ liegt für alle $a,b,\beta \in G$. Tatsächlich ist

$$\beta[a,b]\beta^{-1} = (\beta\alpha\beta^{-1})(\beta b\beta^{-1})(\beta a^{-1}\beta^{-1})(\beta b^{-1}\beta^{-1}) = [\beta\alpha\beta^{-1}, \beta b\beta] \in [G,G].$$

(ii) Betrachte die kanonische Projektion $G \twoheadrightarrow G/[G,G]$, $a \mapsto \bar{a}$. Damit ist $G/[G,G]$ genau dann abelsch, wenn $\bar{a}\bar{b} = \bar{b}\bar{a}$ bzw. $\overline{aba^{-1}b^{-1}} = \bar{a}\bar{b}\bar{a}^{-1}\bar{b}^{-1} = \bar{e}$ für alle $a,b \in G$. Das ist aber gleichbedeutend mit $[a,b] = aba^{-1}b^{-1} \in \mathrm{Ker}(G \twoheadrightarrow G/[G,G]) = [G,G]$ für alle $a,b \in G$. Diese Bedingung ist aber erfüllt, weshalb $G/[G,G]$ abelsch ist.

(iii) Sei $H \lhd G$, sodass $G/H$ abelsch ist. Betrachte wieder $G \twoheadrightarrow G/H$, $a \mapsto \bar{a}$. Wie eben ist $G/H$ genau dann abelsch, wenn $[a,b] = aba^{-1}b^{-1} \in \mathrm{Ker}(G \twoheadrightarrow G/H) = H$ für alle $a,b \in G$. Folglich ist $[G,G] \subset H$. □

**Definition 1.5.13.** Die $i$-te **abgeleitete Gruppe** $D^iG$ einer Gruppe $G$ definieren wir rekursiv durch

$$D^0G := G, \qquad D^{i+1}G := [D^iG, D^iG].$$

Insbesondere ist $D^1G = [G,G]$. Damit erhalten wir eine absteigende Reihe $\cdots \lhd D^2G \lhd D^1G \lhd D^0G = G$ von Normalteilern.

hm:solvable:derived

**Satz 1.5.14.** *Eine Gruppe $G$ ist genau dann auflösbar, wenn es ein $n$ mit $D^nG = \{e\}$ gibt. (Sodann ist $D^mG = \{e\}$ für alle $m \geq n$.)*

*Beweis.* Angenommen $D^nG = \{e\}$ für ein $n$. Dann ist $\{e\} = D^nG \lhd \cdots \lhd D^0G$ eine Normalreihe mit Quotienten $D^iG/D^{i+1}G = D^i/[D^iG, D^iG]$, welche nach Lemma 1.5.12 abelsch sind.

Nehme umgekehrt an, dass $G$ auflösbar ist. Dann existiert eine endliche Normalreihe $\{e\} = G_n \lhd \cdots \lhd G_0 = G$ mit abelschen Quotienten $G_i/G_{i+1}$.

*Behauptung:* $D^iG \subset G_i$, woraus $D^nG = \{e\}$ folgt.

*Beweis:* Wir beweisen das induktiv. Für den Induktionsanfang gilt $D^0G = G = G_0$. Alternativ können wir als Induktionsanfang $D^1G = [G,G]$ betrachten. Da $G/G^1$ abelsch ist, folgt $D^1G = [G,G] \subset G_1$ nach Lemma 1.5.12. Für den Induktionsschritt gilt: Wenn $D^iG \subset G_i$, dann $D^{i+1}G = [D^iG, D^iG] \subset [G_i, G_i]$, und nach Lemma 1.5.12 gilt $[G_i,G_i] \subset G_{i+1}$, also $D^{i+1}G \subset G_{i+1}$. □

Wir wollen nun die Auflösbarkeit der symmetrischen Gruppen untersuchen. Dazu brauchen wir folgende Aussage.

n:alternating:cycle3

**Lemma 1.5.15.** *Sei $A_n$ die alternierende Gruppe. Jedes Element $\sigma \in A_n$ lässt sich schreiben als $\prod_{i=1}^{k} \sigma_i$, wobei $\sigma_i$ Zykel der Länge 3 sind.*

*Beweis.* Schreibe $\sigma = \tau_1 \cdots \tau_N \in S_n$ mit Transpositionen $\tau_i$. Dann ist $\sigma \in A_n$ genau dann, wenn $N$ gerade ist. Es genügt also zu zeigen, dass $\tau_1\tau_2$ ein Produkt von Zykel der Länge 3 für alle Transpositionen $\tau_1$ und $\tau_2$ ist. Wir unterscheiden drei Fälle.

(i) Fall $\tau_1 = \tau_2$: In diesem Fall gilt $\tau_1\tau_2 = e$.

(ii) Fall $\tau_1 = (ij)$ und $\tau_2 = (jk)$ (also nicht disjunkt): Dann gilt $(ij)(jk) = (ijk)$.

(iii) Fall, dass $\tau_1 = (ij)$ und $\tau_2 = (kl)$ disjunkt sind: Dann gilt $(ij)(kl) = (ikj)(ikl)$. □

**Satz 1.5.16.** *Seien $S_n$ die symmetrische Gruppe und $A_n \subset S_n$ die alternierende Gruppe. Dann gilt $D^1S_n = [S_n, S_n] = A_n$ für alle $n \geq 1$ und*

$$D^2S_n = [A_n, A_n] = \begin{cases} \{e\}, & \text{falls } n = 2, 3, \\ \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}, & \text{falls } n = 4, \\ A_n, & \text{falls } n \geq 5. \end{cases}$$

.

*Beweis.* Per Definition ist $A_n \coloneqq \operatorname{Ker}(\operatorname{sgn})$ mit $\operatorname{sgn}\colon S_n \twoheadrightarrow \{\pm 1\} \simeq \mathbb{Z}/2\mathbb{Z}$, also $A_n \lhd S_n$ und $S_n/A_n \simeq \mathbb{Z}/2\mathbb{Z}$ ist abelsch (letzteres folgt aus dem Satz von Lagrange 1.2.15). Somit ist $[S_n, S_n] \subset A$ nach Lemma 1.5.12.

Für die Inklusion $A_n \subset [S_n, S_n]$ schreiben wir $(ijk) = [(ik), (jk)]$ (das kann man nachrechnen). Damit sind nach Lemma 1.5.15 alle Elemente in $A_n$ Produkte von Kommutatoren, also $A_n \subset [S_n, S_n]$.

Wir wenden uns nun $D^2S_n$ zu. Für $n = 2$ gilt $A_2 = \{e\}$, also offenbar $[A_2, A_2] = \{e\}$. Für $n = 3$ gilt $|A_3| = 3$. Also ist $A_3$ zyklisch und damit abelsch. Folglich muss $[A_3, A_3] = \{e\}$ sein.

Sei nun $n \geq 5$. Da nach Definition $[A_n, A_n] \subset A_n$, brauchen wir nur noch $A_n \subset [A_n, A_n]$. Es genügt zu zeigen, dass jeder Zykel der Länge 3 in $[A_n, A_n]$ liegt. Sei $(ijk) \in A_n$ ein Zykel. Da $n \geq 5$, existieren $a, b \in \{1, \ldots, n\} \setminus \{i, j, k\}$ mit $a \neq b$. Dann prüft man $(ijk) = [(ija), (ikb)] \in [A_n, A_n]$ und wir sind in diesem Fall fertig.

Sei nun $n = 4$. Betrachte

$$\varphi_1\colon \mathbb{Z}/2\mathbb{Z} \hookrightarrow S_4, \quad \bar{1} \longmapsto (12)(34) \qquad \text{und} \qquad \varphi_2\colon \mathbb{Z}/2\mathbb{Z} \hookrightarrow S_4, \quad \bar{1} \longmapsto (13)(24).$$

Da $(12)(34)$ und $(13)(24)$ Ordnung 2 haben, sind $\varphi_1$ und $\varphi_2$ wohldefinierte Gruppenhomomorphismen. Ferner ist $\varphi_1(\bar{1})\varphi_2(\bar{1}) = \varphi_2(\bar{1})\varphi_1(\bar{1})$, d. h. $(12)(34)(13)(24) = (13)(24)(12)(34)$. Damit ist

$$\varphi\colon \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \longrightarrow S_4, \qquad (\bar{1}, 0) \longmapsto \varphi_1(\bar{1}), \quad (0, \bar{1}) \longmapsto \varphi_2(\bar{1}), \quad (\bar{1}, \bar{1}) \longmapsto \varphi_1(\bar{1})\varphi_2(\bar{1})$$

ein Gruppenhomomorphismus, der tatsächlich injektiv ist. Auf diese Weise wird die **kleinsche Vierergruppe** $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ zur Untergruppe von $S_4$. Es gilt aber $\varphi(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}) \subset A_4$, weshalb $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ eine Untergruppe von $A_4$ ist. Nun sind $|\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}| = 4$ und $|A_4| = 12$. Also ist der Index der Gruppen 3. Tatsächlich gilt $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \lhd A_4$

(Übung), sodass $A_4/\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ zyklisch der Ordnung 3 und damit abelsch ist. Somit ist $[A_4, A_4] \subset \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ nach Lemma 1.5.12. Für $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \subset [A_4, A_4]$ schreiben wir $\varphi_1(\bar{1}) = (12)(34) = [(123), (124)]$ und $\varphi_2(\bar{1}) = (13)(24) = [(132), (134)]$. □

**Korollar 1.5.17.** *Für $n \geq 5$ ist $S_n$ nicht auflösbar.*

Später sehen wir, dass im Allgemeinen Polynome vom Grad $n \geq 5$ nicht aufgelöst werden können.

**Bemerkung 1.5.18.** Für $n \leq 4$ ist $S_n$ auflösbar.

**Bemerkung 1.5.19.** Für $n \geq 5$ ist $A_n$ tatsächlich einfach, d. h. es besitzt keine nichttrivialen Normalteiler. Aber $A_n$ besitzt viele Untergruppen.

ble:subgroupquotient

**Satz 1.5.20.** *Sei $H \subset G$ eine Untergruppe.*

(i) *Falls $G$ auflösbar ist, so ist auch $H$ auflösbar.*

(ii) *Angenommen $H \lhd G$. Dann ist $G$ genau dann auflösbar, wenn $H$ und $G/H$ beide auflösbar sind.*

*Beweis.*

(i) Mit einer analogen Induktion wie in Satz 1.5.14 gilt $D^i H \subset D^i G$ für alle $i$. Wenn $G$ auflösbar ist, dann gilt nach Satz 1.5.14, dass $D^n G = \{e\}$ für hinreichend große $n$. Damit ist $D^n H = \{e\}$ und somit $H$ auflösbar.

(ii) Betrachte das folgende Diagramm:

$$\begin{array}{ccc} G & \xrightarrow{\pi} & G/H \\ \uparrow & & \uparrow \\ D^1 G = [G, G] & \twoheadrightarrow & \pi(D^1 G) \end{array}$$

Wir können leicht prüfen, dass das Diagramm kommutiert, woraus $\pi(D^1 G) = D^1(G/H)$ folgt. Allgemein gilt rekursiv $D^n(G/H) = \pi(D^n G)$.

Ist $G$ auflösbar, so gilt $D^n G = \{e\}$ für hinreichend große $n$ und damit $D^n(G/H) = \{e\}$, d. h. $G/H$ ist wieder auflösbar. Aus dem obigen Punkt wissen wir bereits, dass $H$ auflösbar ist.

Umgekehrt nehmen wir an, dass $H$ und $G/H$ beide auflösbar sind. Dann gilt $\pi(D^n G) = D^n(G/H) = \{e\}$ für ein hinreichend großes $n$. Folglich ist $D^n G \subset \mathrm{Ker}(\pi) = H$ und mit einer Induktion wie in Satz 1.5.14 gilt $D^{n+m} G \subset D^m H = \{e\}$ für hinreichend großes $m$. Somit ist $G$ auflösbar. □

**Satz 1.5.21.** *Sei $G$ eine endliche auflösbare Gruppe. Dann existiert eine Normalreihe $\{e\} = G_n \lhd \cdots \lhd G_0 = G$, sodass die Faktoren $G_i/G_{i+1}$ zyklisch von Primzahlordnung ist, d. h. $G_i/G_{i+1} \simeq \mathbb{Z}/p_i\mathbb{Z}$ für eine gewisse Primzahl $p_i$.*

*Beweis.* Da $G$ auflösbar ist, existiert eine Normalreihe $\{e\} = G_n \lhd \cdots \lhd G_0 = G$ mit abelschen Faktoren $G_i/G_{i+1}$. Wir verfeinern die Reihe (bleibt aber eine Normalreihe), sodass nach endlich vielen Schritten die Faktoren von der Gestalt $\mathbb{Z}/p\mathbb{Z}$ mit $p$ prim sind.

Angenommen $G_i/G_{i+1} \not\simeq \mathbb{Z}/p\mathbb{Z}$ für alle Primzahlen $p$. Wähle ein $a \in G_1$, und betrachte das Bild $\bar{a} \in G_i/G_{i+1}$. Sei $|\bar{a}| = \prod_{i=1}^{k} p_i^{n_i}$ die Primfaktorzerlegung. Setze $m \coloneqq p_1^{n_1-1} \prod_{i=2}^{k} p_i^{n_i}$, sodass $|\bar{a}^m| = p_1$. Ersetzen wir nun $a$ durch $a^m$, so können wir o. B. d. A. annehmen, dass es ein $a \in G_i$ gibt, sodass $\bar{a} \in G_i/G_{i+1}$ Primzahlordnung hat.

Wir verfeinern nun $G_{i+1} \subset G_i$ zu $G_{i+1} \subset \tilde{G}_{i+1} \subset G_i$, wobei $\tilde{G}_{i+1} \coloneqq \langle G_{i+1}, a\rangle$ durch $G_{i+1}$ und $a$ erzeugt wird. Wegen $G_{i+1} \lhd G_i$ ist auch $G_{i+1} \lhd \tilde{G}_{i+1}$. Können wir zeigen, dass $\tilde{G}_{i+1} \lhd G_i$, so sind wir fertig. Dann ist nämlich $\{e\} = G^n \lhd \cdots \lhd G_{i+1} \lhd \tilde{G}_{i+1} \lhd G_i \lhd \cdots \lhd G_0 = G$ wieder eine Normalreihe mit abelschen Faktoren: Als Untergruppe ist $\tilde{G}_{i+1}/G_{i+1} \subset G_i/G_{i+1}$ wieder abelsch, und nach dem zweiten Isomorphiesatz 1.2.26 ist $G_i/\tilde{G}_{i+1}$ eine Quotientengruppe von $G_i/G_{i+1}$ und damit auch abelsch. Beobachte, dass $\tilde{G}_{i+1}/G_{i+1} = \langle \bar{a}\rangle \simeq \mathbb{Z}/p\mathbb{Z}$. Nun fahren wir mit $G_i/\tilde{G}_{i+1}$ fort, und analog auch alle anderen Faktoren. Da $G$ endlich ist, bricht dieser Prozess irgendwann ab.

Wir zeigen nun $\tilde{G}_{i+1} = \langle G_{i+1}, a\rangle \lhd G_i$. Wegen $G_{i+1} \lhd G_i$ genügt es zu zeigen, dass $bab^{-1} \in \tilde{G_{i+1}}$ für alle $b \in G_i$. Aber das Bild von $bab^{-1} \in G_i$ unter der Surjektion $G_i \twoheadrightarrow G_i/G_{i+1}$ ist $\bar{b}\bar{a}\bar{b}^{-1} = \bar{a}$, da $G_i/G_{i+1}$ abelsch ist. Somit ist $bab^{-1} \in \tilde{G}_{i+1}$. □

Hier noch einige historische Bemerkungen. Die vollständige Klassifikation endlicher einfacher Gruppen war eines der größten Projekte der Mathematik. Höhepunkt dieses Projekts war der Zeitraum von 1955 bis 2004 und umfasst mehrere hundert Arbeiten von bis zu 100 Autoren, die zusammengenommen zehntausende Seiten umfassen. An einer Vereinheitlichung und Vereinfachung der Beweise wird gearbeitet. Die Klassifikation liefert folgendes: Es gibt drei Serien von endlichen einfachen Gruppen.

(i) *Zyklische Gruppen* $G \simeq \mathbb{Z}/p\mathbb{Z}$ für Primzahlen $p$.

(ii) *Alternierende Gruppen* $A_n \coloneqq \operatorname{Ker}(\operatorname{sgn}\colon S_n \to \{\pm 1\})$ für $n \geq 5$. Hier ist $n \geq 5$ kein Zufall. Bereits Galois entdeckte diesen Umstand, weshalb es auch keine Lösungsformel für Polynome fünften Grades gibt.

(iii) *Gruppen vom Lie-Typ*, wie z. B. $\mathrm{SL}(2, \mathbb{F}_p)/\{\pm I_2\}$.

Zuletzt gibt es 26 *sporadische Gruppen*, die endlich einfach sind und in keine der obigen Serien passen. Diese können wie folgt eingeteilt werden:

(i) Die *1st generation of happy family*: die fünf *Mathieugruppen* $M_{11}, M_{12}, M_{22}, M_{23}, M_{24}$. Diese wurden von Émile Léonard Mathieu zwischen 1861 und 1873 beschrieben und sind Untergruppen von symmetrischen Gruppen. Die größte ist $M_{24}$ mit $|M_{24}| = 244\,823\,040$.

(ii) Die *2nd generation of happy family* besteht aus den drei *Conwaygruppen* $Co_1, Co_2, Co_3$ sowie vier weitere Gruppen. Diese sind eng mit der Symmetriegruppe des 24-dimensionalen *Leech lattice* verwandt. Die verallgemeinerte *Monstrous Moonshine* Vermutung stellt einen Zusammenhang zwischen bestimmten sporadischen Gruppen und gewissen Reihen der Form $q^{-1} + r_0 + r_1 q + r_2 q^2 + \cdots$ aus der komplexen Analysis her, wie z. B. für $Co_3$.

(iii) Die *3rd generation of happy family*, welche aus allen anderen sporadischen Gruppen besteht, die Untergruppen von Quotienten der *Monstergruppe* $M$ sind. Darunter zählen insgesamt acht Gruppen, u. a. die *Thompsongruppe* $Th$, das *Baby Monster* $B$ oder die Monstergruppe $M$ (auch *friendly giant* genannt) selbst. Dabei ist $M$ die größte aller endlich einfachen Gruppen mit Ordnung

$$|M| = 2^{46} \cdot 3^{20} \cdot 5^9 \cdot 7^6 \cdot 11^2 \cdot 13^3 \cdot 17 \cdot 19 \cdot 23 \cdot 29 \cdot 31 \cdot 41 \cdot 47 \cdot 59 \cdot 71.$$

(iv) Es verbleiben noch die restlichen sechs Gruppen, die manchmal auch *pariah groups* genannt werden.

## 1.6 Notizen*

def:symmetricgroup

**Definition 1.6.1.** Sei $M_n \coloneqq \{1, \dots, n\}$. Die **Symmetriegruppe** ist $S_n \coloneqq \mathrm{Bij}(M_n)$, deren Elemente wir **Permutationen** nennen. Eine Permutation $\sigma \in S_n$, die $k \mapsto \sigma(k)$ für alle $k \in M_n$ abbildet, schreiben wir als

$$\sigma = \begin{pmatrix} 1 & 2 & \cdots & n \\ \sigma(1) & \sigma(2) & \cdots & \sigma(n) \end{pmatrix}.$$

Die Komposition zweier Permutationen ist dabei (wie bei der Komposition von Abbildungen) von rechts nach links zu lesen. Sind also $\sigma, \tau \in S_n$, so ist deren Komposition durch $k \mapsto \sigma(\tau(k))$ für alle $k \in M_n$ gegeben. Z. B. ist

$$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}.$$

**Definition 1.6.2.** Eine Permutation $\sigma \in S_n$ heißt **Zyklus**, falls es eine Folge $(p_1, \dots, p_k)$ in $M_n$ gibt, sodass $\sigma(p_1) = p_2$, $\sigma(p_2) = p_3$, $\dots$, $\sigma(p_k) = p_1$ sowie $\sigma(i) = i$ für alle $i \in M_n \setminus \{p_1, \dots, p_k\}$. Zwei Zyklen $(p_1, \dots, p_k)$ und $(q_1, \dots, q_l)$ sind **disjunkt**, falls $\{p_1, \dots, p_k\}$ und $\{q_1, \dots, q_l\}$ disjunkt sind.

p:permutation:cycle

**Proposition 1.6.3.** *Jede Permutation lässt sich in disjunkte Zyklen zerlegen, d. h. für jedes $\sigma \in S_n$ gibt es Zyklen $z_1, \dots, z_k \in S_n$, sodass $\sigma = z_k \circ \cdots \circ z_1$.*

*Beweis.* Der Beweis basiert auf folgender Idee: Wir fangen bei einem Element an und verfolgen, wie dieses Element durch wiederholte Anwendung von $\sigma$ abgebildet, bis wir wieder beim Startelement angekommen sind. Diese *Bahn* von $\sigma$ beschreibt einen Zyklus $z_1$. Dann ist $z_1^{-1} \circ \sigma$ wieder eine Permutation. Fahren wir mit dieser neuen Permutation induktiv fort, so erhalten wir die gewünschte Zerlegung. Man überzeugt sich leicht, dass die Zyklen disjunkt sind (denn $\sigma$ ist bijektiv). □

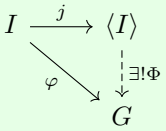
Formal definiert man die freie Gruppe wie folgt.

**Definition 1.6.4.** Sei $I$ eine (endliche) Menge. Sei $J$ (beliebige) Menge mit $|I| = |J|$, d. h. es gibt eine Bijektion $\varphi\colon I \to J$. Setze $a^{-1} \coloneqq \varphi(a)$ für alle $a \in I$, sprich $J$ ist die Menge der Inversen von $I$. Definiere die Äquivalenzrelation $\sim$ auf $I \cup J$, die Teilwörter

$aa^{-1}$ und $a^{-1}a$ mit $\varnothing$ identifiziert. Dann ist die **freie Gruppe**

$$G = \langle I \rangle \coloneqq \{\text{endliche Wörter in } I \cup J\}/\sim.$$

Noch abstrakter sind freie Gruppen durch eine universelle Eigenschaft gegeben: Sei $I$ eine (endliche) Menge. Dann erfüllt die **freie Gruppe** $\langle I \rangle$ folgende universelle Eigenschaft: Es gibt eine Abbildung $j\colon I \to \langle I \rangle$ von Mengen, sodass für jede Abbildung $\varphi\colon I \to G$ von Mengen, wobei $G$ eine Gruppe ist, es genau einen Gruppenhomomorphismus $\Phi\colon \langle I \rangle \to G$ gibt, sodass folgendes Diagramm kommutiert:




Äquivalent dazu lässt sich die universelle Eigenschaft auch durch den natürlichen Isomorphismus $\mathrm{Hom}_{\mathsf{Set}}(I, G) \cong \mathrm{Hom}_{\mathsf{Grp}}(\langle I \rangle, G)$ für alle Gruppen $G$ ausdrücken. Die universelle Eigenschaft bestimmt die freie Gruppe bis auf eindeutige Isomorphie.

Diese Definitionen sind aber für unsere Zwecke komplett nutzlos.

*Beispiel* 1.6.5. Es gilt $\varphi\colon \mathbb{Z} \xrightarrow{\sim} \langle a \rangle$, $n \mapsto a \cdots a$.

**Proposition 1.6.6.** *Seien $G$ eine Gruppe und $I \subset G$ eine (endliche) Teilmenge. Dann ist $G$ genau dann von $I$ erzeugt, wenn es einen eindeutigen surjektiven Gruppenhomomorphismus $\varphi\colon \langle I \rangle \to G$ gibt mit $\varphi(a) = a$ für alle $a \in \langle I \rangle$.*

*Beweis.* Definiere $\varphi(a) \coloneqq a$ für alle $a \in I$. Das können wir auf $\langle I \rangle$ rekursiv fortsetzen durch $\varphi(ab) \coloneqq \varphi(a)\varphi(b)$. Das ist auch die einzige Möglichkeit, falls $\varphi$ ein Gruppenhomomorphismus sein soll. Dann ist $\varphi$ genau dann surjektiv, wenn $G$ von $I$ erzeugt wird. □

**Bemerkung 1.6.7.** Freie Gruppen sind nützlich, da wir jede Gruppe als Quotientengruppe schreiben können. Ist $I \subset G$ ein Erzeuger einer Gruppe $G$, so gibt es einen surjektiven Gruppenhomomorphismus $\varphi\colon I \twoheadrightarrow G$. Nach dem Homomorphiesatz gilt $G \cong \langle I \rangle / \operatorname{Ker} \varphi$. Man nennt $\varphi$ eine **Präsentation** von $G$.

*Beispiel* 1.6.8.

(i) Wir wollen $S_3$, die Symmetriegruppe des Dreiecks, als Präsentation schreiben. Man kann zeigen, dass die Drehung $d$ um 60° gegen den Uhrzeigersinn und die Spiegelung $s$ an der $y$-Achse gesamt $S_3$ erzeugen. Mit anderen Worten, es gibt einen surjektiven Gruppenhomomorphismus $\varphi\colon \langle d, s \rangle \twoheadrightarrow S_3$ (das kann man elementweise in einer Multiplikationstabelle nachrechnen). Der Kern wird erzeugt durch $\operatorname{Ker} \varphi = \langle d^3, s^2, dsds \rangle$ (was auch nicht so trivial zu zeigen ist).

(ii) Es gilt $\mathbb{Z}/6\mathbb{Z} \simeq \langle a \mid a^6 \rangle$.

**Proposition 1.6.9.** *Die Abbildungen $l\colon G \to \mathrm{Bij}(G)$, $a \mapsto (b \mapsto ab)$ sowie $r\colon G \to \mathrm{Bij}(G)$, $a \mapsto (b \mapsto ba^{-1})$ sind Gruppenhomomorphismen.*

*Beweis.* Tatsächlich sind $l(a)$ und $r(a)$ Bijektionen für alle $a \in G$; z. B. ist das Inverse von $l(a)$ gegeben durch $b \mapsto a^{-1}b$. Ferner ist $l$ ein Gruppenhomomorphismus, denn $l(a_1a_2) = (b \mapsto a_1a_2b) = (b \mapsto a_1b) \circ (b \mapsto a_2b) = l(a_1)l(a_2)$. Analog für $r$. □

**Bemerkung 1.6.10.**

(i) $r\colon a \mapsto (b \mapsto ba)$ ist genau dann ein Gruppenhomomorphismus, wenn $G$ abelsch ist. Das hängt mit $(ab)^{-1} = b^{-1}a^{-1}$ zusammen.

(ii) Es gilt $l(a) \in \mathrm{Aut}(G)$ genau dann, wenn $a = e$, denn im Allgemeinen erhält $l$ die Einheit nicht: $l(a)$ bildet $e \mapsto a$ ab.

(iii) Die Konjugation ist gegeben durch $a \mapsto bab^{-1}$. Sie ist genau dann trivial, wenn $G$ abelsch ist.

**Bemerkung 1.6.11.** Für jede Gruppe $G$ gilt $Z(G) = \bigcap_{a \in G} Z(a)$.

*Beispiel* 1.6.12. Es lohnt sich, alle Gruppen kleiner Ordnung zu kennen. Hier bis Ordnung 8.

(i) $\{e\} \simeq \mathbb{Z}/1\mathbb{Z} \simeq S_1 \simeq A_2$.

(ii) $\mathbb{Z}/2\mathbb{Z} \simeq S_2 \simeq D_1$.

(iii) $\mathbb{Z}/3\mathbb{Z} \simeq A_3$.

(iv) $\mathbb{Z}/4\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \simeq D_2$ (die **kleinsche Vierergruppe**).

(v) $\mathbb{Z}/5\mathbb{Z}$.

(vi) $\mathbb{Z}/6\mathbb{Z} \simeq \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, $S_3 \simeq D_3$.

(vii) $\mathbb{Z}/7\mathbb{Z}$.

(viii) $\mathbb{Z}/8\mathbb{Z}$, $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, $(\mathbb{Z}/2\mathbb{Z})^3$, $D_4$, $Q_8$ (die **Quaternionengruppe**).

Wir werden die drei *Sätze von Sylow* nicht beweisen. Dennoch bilden sie einen Grundpfeiler in der Theorie endlicher Gruppen und in der Klassifikation endlicher einfacher Gruppen. Deren Beweise verwenden u. a. den *Satz von Cauchy* sowie Gruppenwirkungen auf äußerst kreative Weise. Wir listen sie im Folgenden nur auf.

**Satz 1.6.13 (erster Satz von Sylow).** *Sei $G$ eine endliche Gruppe mit $|G| = p^n m$, wobei $p$ eine Primzahl ist und $p \nmid m$. Dann existiert eine Untergruppe $H \subset G$ der Ordnung $p^i$ für alle $i = 1, \dots, n$.*

**Satz 1.6.14 (zweiter Satz von Sylow).** *Eine Untergruppe $H =: S_p \subset G$ der maximalen Primpotenzordnung $|H| = p^n$ heißt **$p$-Sylowgruppe**. Zwei $p$-Sylowgruppen sind stets*

*zueinander konjugiert, d. h. für p-Sylowgruppen $S_p, S_p' \subset G$ gibt es ein $a \in G$, sodass $S_p' = aS_pa^{-1}$.*

**Satz 1.6.15 (dritter Satz von Sylow).** *Bezeichne $s_p$ die Anzahl der verschiedenen p-Sylowgruppen $S_p \subset G$. Dann gelten $s_p \mid |G|$ und $s_p \equiv 1 \mod p$.*

Hier eine Motivation für direkte Produkte.

**Definition 1.6.16.** Eine kurze exakte Sequenz

$$1 \longrightarrow A \xrightarrow{f} B \underset{h}{\overset{g}{\rightleftarrows}} C \longrightarrow 1$$

von Gruppen **spaltet**, falls es einen Gruppenhomomorphismus $h\colon C \to B$ gibt, sodass $g \circ h = \mathrm{id}_C$.

**Proposition 1.6.17.** *Eine kurze exakte Sequenz*

$$1 \longrightarrow A \xrightarrow{f} B \underset{h}{\overset{g}{\rightleftarrows}} C \longrightarrow 1$$

*von Gruppen spaltet genau dann, wenn es einen Isomorphismus $B \xrightarrow{\sim} A \rtimes C$ gibt, sodass folgendes Diagramm kommutiert:*

$$\begin{array}{ccccccccc} 1 & \longrightarrow & A & \xrightarrow{f} & B & \xrightarrow{g} & C & \longrightarrow & 1 \\ & & \| & & \downarrow\wr & & \| & & \\ 1 & \longrightarrow & A & \longrightarrow & A \rtimes C & \longrightarrow & C & \longrightarrow & 1 \end{array}$$

*Beweisskizze.* Zur Hinrichtung: Wir konstruieren

$$\varphi\colon B \longrightarrow A \rtimes C, \qquad b \longmapsto (f^{-1}(b \cdot (h \circ g)(b)^{-1}), g(b)).$$

Für die Wohldefiniertheit müssen wir zeigen, dass $b \cdot (h \circ g)(b)^{-1} \in \mathrm{Im}(f) = \mathrm{Ker}(g)$ (das Urbild ist eindeutig, da $f$ injektiv ist). Mit $g \circ h = \mathrm{id}_C$ gilt tatsächlich

$$g(b \cdot (h \circ g)(b)^{-1}) = g(b) \cdot (g \circ h \circ g)(b)^{-1} = g(b)g(b)^{-1} = e_C.$$

Statten wir $A \rtimes C$ mit der Gruppenaktion $C \to \mathrm{Aut}(A)$, $c \mapsto (a \mapsto h(c)ah(c)^{-1})$ aus, so folgt für alle $b_1, b_2 \in B$

$$\begin{aligned} \varphi(b_1)\varphi(b_2) &= (b_1 \cdot (h \circ g)(b_1)^{-1}, g(b_1)) \cdot (b_2 \cdot (h \circ g)(b_2)^{-1}, g(b_2)) \\ &= (b_1 \cdot (h \circ g)(b_1)^{-1} \cdot (h \circ g)(b_1) \cdot b_2 \cdot (h \circ g)(b_2)^{-1} \cdot (h \circ g)(b_1)^{-1}, g(b_1b_2)) \\ &= (b_1b_2 \cdot (h \circ g)(b_2^{-1}b_1^{-1}), g(b_1b_2)) \\ &= \varphi(b_1b_2), \end{aligned}$$

d. h. $\varphi$ ist ein Gruppenhomomorphismus. Die Gruppenhomomorphismen $A \to A \rtimes C$ und $A \rtimes C$ sind durch die kanonische Inklusion und Projektion gegeben, d. h. $a \mapsto (a, e_C)$ und $(a, c) \mapsto c$. Man kann nun nachrechnen, dass das Diagramm kommutiert und in $A \rtimes C$ exakt ist. Dass $\varphi$ ein Isomorphismus ist, kann man auch nachrechnen. anwenden, was in jeder abelschen Kategorie gilt.

Für die Umkehrung definieren wir $h\colon C \to A \rtimes C$, $c \mapsto (e_A, c)$. □

**Bemerkung 1.6.18.** Betrachte die gewöhnliche Wirkung $\mathrm{GL}_{n+1}(K) \times \mathbb{P}^n(K) \to \mathbb{P}^n(K)$. Dann ist

$$\mathrm{Stab}(\mathbb{P}^n(K)) = \{\lambda \mathrm{id}_{\mathbb{P}^n(K)} \mid \lambda \in K^*\} \simeq K^*,$$

nämlich alle skalierenden Matrizen. Wir erhalten einen injektiven Gruppenhomomorphismus $K^* \hookrightarrow \mathrm{GL}_{n+1}(K)$. Wir definieren $\mathrm{PGL}_{n+1}(K) := \mathrm{GL}_{n+1}(K)/K^*$.

# 2 Ringtheorie

VL 7
04.11.23

## 2.1 Ringe, Homomorphismen, Ideale

def:ring

**Definition 2.1.1.** Ein **Ring** besteht aus einer Menge $R$ und zwei Verknüpfungen

$$R \times R \longrightarrow R,\ (a, b) \longmapsto a + b, \qquad R \times R \longrightarrow R,\ (a, b) \longmapsto a \cdot b =: ab$$

(**Addition** und **Multiplikation**), sodass folgende Eigenschaften gelten:

(i) $(R, +)$ ist eine abelsche Gruppe.

(ii) **Einselement**: Es existiert $1 \in R$, sodass $1a = a1 = a$ für alle $a \in R$.

(iii) **Assoziativität**: $a(bc) = (ab)c$ für alle $a, b, c \in R$.

(iv) **Distributivität**: $a(b + c) = ab + ac$ für alle $a, b, c \in R$.[17]

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

**Notation 2.1.2.** In dieser Vorlesung werde alle (wichtigen) Ringe kommutativ und nicht der **Nullring** $\{0\}$ sein,[18] d. h. $1 \neq 0$, wobei 0 das neutrale Element bzgl. Addition ist.

**Bemerkung 2.1.3.**

(i) Definition 2.1.1 ist ähnlich zur Definition eines Körpers. Ein Ring ist genau dann ein Körper, falls $(R \setminus \{0\}, \cdot)$ eine Gruppe ist. Mit anderen Worten, nur die Existenz des Inversen (bzgl. Multiplikation) fehlt.[19]

(ii) Es gilt $0a = a0 = 0$ für alle $a \in R$.

[17] Wir übernehmen stillschweigend die Konvention *Punkt- vor Strichrechnung*. Das ist nicht Teil der Definition.

[18] Den Nullring auszuschließen ist meiner Meinung nach unüblich. Es fehlt dann nämlich ein *Finalobjekt* in der Kategorie der Ringe, was die Kategorie hässlicher macht.

*Beweis:* $0a = (0+0)a = 0a + 0a$, also $0a = 0$. Analog $a0 = 0$.

(iii) Für $a \in R$ schreiben wir $-a \in R$ für das Inverse bzgl. Addition, d. h. $a + (-a) = 0$. Es gilt $(-a)b = -(ab)$ für alle $a, b \in R$.

*Beweis:* $(-a)b + ab = ((-a) + a)b = 0b = 0$.

*Beispiel* 2.1.4.

(i) Jeder Körper ist ein Ring. Z. B. sind $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ und $\mathbb{F}_p$ alles Ringe.

(ii) $\mathbb{Z}$ ist ein Ring. $\mathbb{Z}/n\mathbb{Z}$ ist ein Ring für alle $n \in \mathbb{N}_0$; das ist aber genau dann ein Körper, wenn $n = p$ eine Primzahl ist.

(iii) Die **ganzen gaußschen Zahlen** $\mathbb{Z}[\mathrm{i}] \coloneqq \{a + b\mathrm{i} \mid a, b \in \mathbb{Z}\} \subset \mathbb{C}$ bilden einen Ring.

(iv) $\mathbb{Z}[\sqrt{5}] \coloneqq \{a + b\sqrt{5} \mid a, b \in \mathbb{Z}\}$ ist ein Ring.

(v) $\mathbb{Z}[\sqrt{-5}] \coloneqq \{a + b\sqrt{-5} \mid a, b \in \mathbb{Z}\}$ ist ein Ring, ein wichtiges Beispiel aus der Zahlentheorie.

**Definition 2.1.5.** Eine Abbildung $\varphi\colon R_1 \to R_2$ zwischen zwei Ringen heißt **Ringhomomorphismus**, falls $\varphi\colon (R_1, +) \to (R_2, +)$ ein Gruppenhomomorphismus ist und falls

$$\varphi(ab) = \varphi(a)\varphi(b) \qquad \text{und} \qquad \varphi(1_{R_1}) = 1_{R_2}$$

für alle $a, b \in R_1$ gilt.

**Bemerkung 2.1.6.** $\varphi(0) = 0$ folgt bereits, $\varphi(1) = 1$ muss extra gefordert werden.

*Beispiel* 2.1.7.

(i) Die kanonische Abbildung $\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ ist ein Ringhomomorphismus.

(ii) $\mathbb{Z}[\sqrt{5}] \to \mathbb{Z}$, $a + b\sqrt{5} \mapsto a$ ist *kein* Ringhomomorphismus, da es nicht mit der Multiplikation verträglich ist (z. B. ist $\varphi(\sqrt{5})^2 = 0 \neq 5 = \varphi(\sqrt{5}^2)$).

(iii) Die üblichen Inklusionen $\mathbb{Z} \hookrightarrow \mathbb{R}$, $\mathbb{Q} \hookrightarrow \mathbb{C}$, $\mathbb{Z} \hookrightarrow \mathbb{Z}[\sqrt{5}]$ sind Ringhomomorphismen.

*Beispiel* 2.1.8. Für einen beliebigen Ring $R$ definiert $\mathbb{Z} \to R$, $n \mapsto n1_R$ einen Ringhomomorphismus.[20]

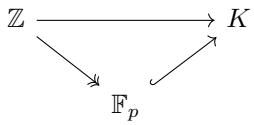
. Wiederholung Aus der linearen Algebra wissen wir, dass es für einen Körper $R = K$ zwei Fälle für die *Charakteristik* $\mathrm{char}(K)$ gibt.

(i) $\mathbb{Z} \hookrightarrow K$ ist genau dann injektiv, wenn $\mathrm{char}(K) = 0$.

[19] Ein weiterer Unterschied ist, dass in Körper $0 \neq 1$ gilt, d. h. 0 ist nicht invertierbar. Mit anderen Worten, ein Körper mit nur einem Element existiert per Definition nicht, aber der Nullring existiert. An sinnvollen Theorien, in der ein Körper mit einem Element realisiert werden können, wird noch geforscht.

[20] Dieser ist auch der einzig mögliche Ringhomomorphismus $\mathbb{Z} \to R$. Damit ist $\mathbb{Z}$ das *Initialobjekt* in der Kategorie der Ringe.

(ii) $\mathbb{Z} \to K$ faktorisiert durch $\mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$ genau dann, wenn $\operatorname{char}(K) = p$ eine Primzahl ist.




**Definition 2.1.9.** Sei $R$ ein Ring. Eine Teilmenge $\mathfrak{a} \subset R$ heißt **Ideal** von $R$, falls $(\mathfrak{a}, +) \subset (R, +)$ eine Untergruppe ist und $ab \in \mathfrak{a}$ für alle $a \in R$ und $b \in \mathfrak{a}$ gilt.[21,22]

*Beispiel* 2.1.10. Betrachte $R = \mathbb{Z}$. Wir wissen, dass $n\mathbb{Z} \coloneqq \{na \mid a \in \mathbb{Z}\}$ alle Untergruppen von $\mathbb{Z}$ sind. Diese sind aber auch Ideale. Also sind alle Ideale von $\mathbb{Z}$ die Teilmengen $n\mathbb{Z}$ für alle $n \in \mathbb{Z}$ (bzw. für alle $n \in \mathbb{N}_0$).

**Lemma 2.1.11.** *Sei $\varphi\colon R_1 \to R_2$ ein Ringhomomorphismus. Dann ist*

$$\operatorname{Ker}(\varphi) \coloneqq \{a \in R_1 \mid \varphi(a) = 0_{R_2}\}$$

*ein Ideal.*

*Beweis.* $\operatorname{Ker}(\varphi)$ ist der Kern eines Gruppenhomomorphismus, und insbesondere eine Untergruppe. Falls $b \in \operatorname{Ker}(\varphi)$, dann gilt $\varphi(ab) = \varphi(a)\varphi(b) = \varphi(a)0 = 0$ für alle $a \in R_1$, also $ab \in \operatorname{Ker}(\varphi)$. □

**Lemma 2.1.12.** *Sei $\mathfrak{a} \subset R$ ein Ideal. Dann wird*

$$R/\mathfrak{a} \coloneqq (R, +)/(\mathfrak{a}, +) \qquad \text{durch} \qquad \bar{a}\bar{b} \coloneqq \overline{ab}$$

*zu einem Ring und die kanonische Abbildung $\pi\colon R \twoheadrightarrow R/\mathfrak{a}$, $a \mapsto \bar{a}$ ist ein Ringhomomorphismus mit $\operatorname{Ker}(\pi) = \mathfrak{a}$. Wir nennen $R/\mathfrak{a}$ den **Quotient** (oder der **Quotientenring**) von $R$ nach $\mathfrak{a}$.*

*Beweis.* Wir müssen zeigen, dass die Multiplikation wohldefiniert ist. Nehme dafür $a_1, a_2 \in R$ mit $\bar{a}_1 = \bar{a}_2$. Dann ist $\bar{a}_1 = \bar{a}_2$ äquivalent zu $a_1 - a_2 \in \mathfrak{a}$. Für alle $b \in R$ gilt dann $a_1 b - a_2 b = (a_1 - a_2)b \in \mathfrak{a}$, da $\mathfrak{a}$ ein Ideal ist. Also ist $\overline{a_1 b} = \overline{a_2 b}$.

Nun zur Abbildung $\pi\colon R \twoheadrightarrow R/\mathfrak{a}$. $\operatorname{Ker}(\pi) = \mathfrak{a}$ ist klar, da $\pi$ ein Gruppenhomomorphismus ist. Für alle $a, b \in R$ gilt $\pi(ab) = \pi(a)\pi(b)$, was aus der Definition der Multiplikation in $R/\mathfrak{a}$ folgt. Ferner ist $1_{R/\mathfrak{a}} = \pi(1)$, denn $\pi(a) = \pi(1a) = \pi(a)$ für alle $a \in R$. Also ist $\pi$ ein Ringhomomorphismus. □

**Warnung 2.1.13.** Es gibt ein kleines Problem. $\mathfrak{a} = R$ ist nach Definition ein Ideal. Dann ist $R/\mathfrak{a} = \{0\}$ der Nullring, d. h. $1_{R/\mathfrak{a}} = 0$. Das widerspricht aber unserer Konvention. Daher schließen wir im allgemeinen $\mathfrak{a} = R$ als Ideal aus.

*Beispiel* 2.1.14. Sei $R$ ein beliebiger Ring. Dann ist $\mathfrak{a} = \{0\}$ das **Nullideal**, was ein Ideal ist.

[21] Ideale werden meist in Fraktur geschrieben. Handschriftlich (wie der Dozent an der Tafel) meistens in Sütterlin.

[22] Streng genommen ist das ein *Linksideal*. Analog definiert man *Rechtsideale* mit der Eigenschaft $ba \in \mathfrak{a}$ für alle $a \in R$ und $b \in \mathfrak{a}$. Falls $R$ kommutativ ist, so sind Links-und Rechtsideale dasselbe, weshalb wir dann von *Idealen* sprechen.

**Notation 2.1.15.** Für eine beliebige Teilmenge $M \subset R$ eines Rings sei

$$(M) \coloneqq \left\{ \sum_{i=1}^{n} a_i b_i \;\middle|\; a_i \in R, b_i \in M, n \in \mathbb{N}_0 \right\}$$

Beachte, dass alle Elemente endliche Summen sind. Für $M = \{a\}$ schreiben wir $(a) \coloneqq (\{a\}) = \{ca \mid c \in R\}$. Dann ist $(M)$ ein Ideal, das **von** $M$ **erzeugte Ideal**.

**Definition 2.1.16.** Ein Ideal $\mathfrak{a} \subset R$ von der Gestalt $\mathfrak{a} = (a)$ für ein $a \in R$ heißt **Hauptideal**.

*Beispiel* 2.1.17. Alle Ideale in $\mathbb{Z}$ sind Hauptideale, denn $n\mathbb{Z} = (n)$.

**Definition 2.1.18.** Ein Element $a \in R$ heißt **Nullteiler**, falls es ein $0 \neq b \in R$ mit $ab = 0$ gibt.

**Warnung 2.1.19.** Insbesondere ist 0 ein Nullteiler.

**Definition 2.1.20.** Ein Element $a \in R$ heißt **Einheit** (oder **invertierbar**), falls es ein $b \in R$ mit $ab = 1$ gibt. Dann ist $R^* \coloneqq \{a \in R \mid a \text{ Einheit}\}$ und $(R^*, \cdot)$ ist eine Gruppe.

*Beispiel* 2.1.21.

(i) Für Körper $R = K$ ist $R^* = K^* = K \setminus \{0\}$.

(ii) $\mathbb{Z}^* = \{\pm 1\}$.

(iii) $(\mathbb{Z}/n\mathbb{Z})^* = \{\bar{m} \mid m, n \text{ teilerfremd}\}$.

*Beispiel* 2.1.22. Was sind die Einheiten von $\mathbb{Z}[\mathrm{i}]$? Die Antwort ist $(\mathbb{Z}[\mathrm{i}])^* = \{\pm 1, \pm \mathrm{i}\}$.

*Beweis:* Angenommen $(a+b\mathrm{i})(c+d\mathrm{i}) = 1$ für $a, b, c, d \in \mathbb{Z}$. Das ergibt das Gleichungssystem

$$\begin{cases} ac - bd = 1, \\ bc + ad = 0. \end{cases}$$

(i) Fall $a \neq 0$: Sei $p$ eine Primzahl mit $p \mid a$. Dann folgt $p \mid bc$, also $p \mid b$ oder $p \mid c$. Aus $p \mid b$ folgt aber $p \mid 1$, ein Widerspruch. Darum ist $p \mid c$. Induktiv gilt das auch für alle Primpotenzen, d. h. $p^k \mid c$, falls $p^k \mid a$.

Mit demselben Argument schließen wir von $p^k \mid c$ auf $p^k \mid a$. Also gilt $a = \pm c$ und damit $b = \mp d$. Falls $a = c$, dann $b = -d$. Aus $ac - bd = 1$ folgt $a^2 + b^2 = 1$ und somit $a + b\mathrm{i} \in \{\pm 1, \pm \mathrm{i}\}$. Der Fall $a = -c$ funktioniert ähnlich.

(ii) Fall $a = 0$: Dann ist $-bd = 1$, also $b = \pm 1$, also $a + b\mathrm{i} \in \{\pm \mathrm{i}\}$.

*Alternativ:* Angenommen $1 = (a + b\mathrm{i})(c + d\mathrm{i})$. Dann gilt

$$1^2 = |a + b\mathrm{i}| \cdot |c + d\mathrm{i}| = (a^2 + b^2)(c^2 + d^2)$$

wegen $|z|^2 = z\bar{z}$ für alle $z \in \mathbb{C}$. Eine Fallunterscheidung liefert dann die Einheiten.

Deutlich schwieriger sind die Einheiten von $\mathbb{Z}[\sqrt{5}]$ und $\mathbb{Z}[\sqrt{-5}]$. Das wird in der algebraischen Zahlentheorie beantwortet.

**Definition 2.1.23.** Sei $R$ ein Ring. Dann ist $R$ ein **Integritätsbereich**, falls außer 0 keine weiteren Nullteiler existieren.

*Beispiel* 2.1.24.

(i) Körper $R = K$ sind Integritätsbereiche.

(ii) $R = \mathbb{Z}$ ist ein Integritätsbereich.

(iii) $R = \mathbb{Z}/n\mathbb{Z}$ ist kein Integritätsbereich, falls $n \in \mathbb{N} \setminus \{0, 1\}$ nicht prim ist.

**Definition 2.1.25.** Sei $R$ ein Integritätsbereich. Dann definieren wir

$$Q(R) \coloneqq \{(a, b) \mid a \in R, b \in R \setminus \{0\}\}/\sim$$

als eine Menge von Äquivalenzklassen bzgl. der Äquivalenzrelation

$$(a, b) \sim (a', b') \iff ab' = a'b.$$

Wir schreiben $\frac{a}{b} \in Q(R)$ für die Äquivalenzklasse von $(a, b) \in Q(R)$. Mit den Operationen

$$\frac{a}{b} + \frac{a'}{b'} \coloneqq \frac{ab' + a'b}{bb'}, \qquad \frac{a}{b} \cdot \frac{a'}{b'} \coloneqq \frac{aa'}{bb'}$$

für alle $\frac{a}{b}, \frac{a'}{b'} \in Q(R)$ wird $Q(R)$ zu einem Körper (das muss man nachrechnen). Wir nennen $Q(R)$ den **Quotientenkörper** des Integritätsbereichs $R$.[23]

**Bemerkung 2.1.26.** $R \hookrightarrow Q(R)$, $a \mapsto \frac{a}{1}$ ist ein injektiver Ringhomomorphismus, was das Analogon zu $\mathbb{Z} \hookrightarrow \mathbb{Q} = Q(\mathbb{Z})$ ist.

**Definition 2.1.27.** Seien $R$ ein Integritätsbereich und $0 \neq a \in R \setminus R^*$. Dann heißt $a$ **irreduzibel**, wenn aus $a = bc$ schon $b \in R^*$ oder $c \in R^*$ folgt.

**Definition 2.1.28.** Sei $R$ ein Integritätsbereich. Für $a, b \in R$ sagen wir $a$ **teilt** $b$ und schreiben wir $a \mid b$, falls $b \in (a)$, d. h. $b = ac$ für ein $c \in R$.

**Definition 2.1.29.** Seien $R$ ein Integritätsbereich und $0 \neq a \in R \setminus R^*$. Dann ist $a$ ein **Primelement**, falls aus $a \mid bc$ schon $a \mid b$ oder $a \mid c$ folgt.

**Bemerkung 2.1.30.** Falls $R = \mathbb{Z}$, so ist $a \in \mathbb{Z}$ eine Primzahl genau dann, wenn $a$ irreduzibel ist genau dann, wenn $a$ ein Primelement ist.

[23] Quotientenkörper werden in der Literatur mit $\mathrm{Quot}(R)$ oder $\mathrm{Frac}(R)$ abgekürzt. Das lässt sich zum Konzept von *Lokalisierungen* verallgemeinern, bei dem nicht alle Elemente in $R \setminus \{0\}$, sondern nur eine (multiplikative) Teilmenge dessen invertierbar gemacht werden.

n:prime:irreducible

**Lemma 2.1.31.** *Sei $R$ ein Integritätsbereich. Wenn $a \in R$ ein Primelement ist, dann ist $a$ auch irreduzibel.*

*Beweis.* Angenommen $a = bc$ mit $b, c \in R$. Dann ist $a \mid bc$. Weil $a$ ein Primelement ist, ist $a \mid b$ oder $a \mid c$. O. B. d. A. sei $a \mid b$. Schreibe $b = b'a$ für ein $b' \in R$. Dann ist $a = b'ac$ bzw. $a(1 - b'c) = 0$. Da $R$ ein Integritätsbereich ist und $a \neq 0$, folgt $1 - b'c = 0$, also $c \in R^*$. □

*Beispiel* 2.1.32. Sei $R = \mathbb{Z}[\mathrm{i}]$ (was ein Integritätsbereich ist) und sei $p \in \mathbb{Z}$ eine Primzahl. Dann ist $p \in \mathbb{Z}[\mathrm{i}]$ genau dann reduzibel, wenn es $a, b \in \mathbb{Z}$ mit $a^2 + b^2 = p$ gibt. Bspw. ist $5 \in \mathbb{Z}$ eine Primzahl, aber kein Primelement in $\mathbb{Z}[\mathrm{i}]$.

*Beweis:* Falls $a^2 + b^2 = p$, dann $p = (a + b\mathrm{i})(a - b\mathrm{i})$. Dabei sind die Faktoren keine Einheiten, denn $\mathbb{Z}[\mathrm{i}]^* = \{\pm 1, \pm \mathrm{i}\}$. Die Umkehrung ist eine Aufgabe.

**Bemerkung 2.1.33.** Falls $R = \mathbb{Z}$, so ist ein Element genau dann irreduzibel, wenn es prim ist. In $\mathbb{Z}[\sqrt{-5}]$ gilt das hingegen nicht. Z. B. gilt $2 \cdot 3 = 6 = (1 + \sqrt{-5})(1 - \sqrt{-5})$. Dann sind 2 und 3 irreduzibel,[24] Aber nicht prim, da $2 \nmid 1 \pm \sqrt{-5}$ und $3 \nmid 1 \pm \sqrt{-5}$.

VL 8
06.11.23

**Definition 2.1.34.** Ein Ideal $\mathfrak{a} \subsetneq R$ ist ein **Primideal**, falls aus $ab \in \mathfrak{a}$ schon $a \in \mathfrak{a}$ oder $b \in \mathfrak{a}$ folgt. Wir schreiben üblicherweise $\mathfrak{p} \subset R$ statt $\mathfrak{a} \subset R$.

**Lemma 2.1.35.** *Seien $R$ ein Integritätsbereich und $0 \neq a \in R \setminus R^*$. Dann ist $(a) \subset R$ genau dann ein Primideal, wenn $a$ ein Primelement ist.*

*Beweis.* Sei $a \in R$ ein Primelement. Angenommen $bc \in (a)$. Zu zeigen ist $b \in (a)$ oder $c \in (a)$. $bc \in (a)$ heißt, dass es ein $\alpha \in R$ gibt mit $bc = a\alpha$, d. h. $a \mid bc$. Weil $a$ ein Primelement ist, folgt $a \mid b$ oder $a \mid c$. Daher gilt $b \in (a)$ oder $c \in (a)$.

Umgekehrt sei $(a) \neq \{0\}$ ein Primideal; insbesondere ist $a \neq 0$. Angenommen $a \mid bc$, d. h. $bc \in (a)$. Weil $(a)$ ein Primideal ist, folgt $b \in (a)$ oder $c \in (a)$. Das bedeutet aber $a \mid b$ oder $a \mid c$, weshalb $a$ ein Primelement ist. □

thm:prime

**Satz 2.1.36.** *Sei $\mathfrak{a} \subset R$ ein Ideal. Dann ist $\mathfrak{a}$ genau dann ein Primideal, wenn $R/\mathfrak{a}$ ein Integritätsbereich ist.*

*Beweis.* Sei $\mathfrak{a}$ ist ein Primideal. Nehme $\alpha, \beta \in R/\mathfrak{a}$ mit $\alpha\beta = 0$. Wir müssen zeigen, dass $\alpha = 0$ oder $\beta = 0$. Da die kanonische Projektion $R \twoheadrightarrow R/\mathfrak{a}$, $a \mapsto \bar{a}$ surjektiv ist, können wir $\alpha = \bar{a}$ und $\beta = \bar{b}$ für $a, b \in R$ schreiben. Damit ist $\alpha\beta = 0$ äquivalent zu $\alpha\beta = \bar{a}\bar{b} = \overline{ab} = 0$ bzw. $ab \in \mathfrak{a} = \mathrm{Ker}(R \twoheadrightarrow R/\mathfrak{a})$. Da $\mathfrak{a}$ ein Primideal ist, folgt $a \in \mathfrak{a}$ oder $b \in \mathfrak{a}$, d. h. $\alpha = 0$ oder $\beta = 0$.

Die Umkehrung erfolgt mit analogen Argumenten. □

**Definition 2.1.37.** Ein Ideal $\mathfrak{a} \subsetneq R$ heißt **Maximalideal**,[25] falls kein Ideal $\mathfrak{a} \subsetneq \mathfrak{b} \subsetneq R$ existiert.

[24] Das kann man leicht durch z. B. $2 = (a + b\sqrt{-5})(c + d\sqrt{-5})$ mit $a, b, c, d \in \mathbb{Z}$ nachrechnen. Es gilt nämlich nach komplexer Konjugation auch $2 = (a - b\sqrt{-5})(c - d\sqrt{-5})$. Dann kann man unter Ausnutzung von $(x + y\mathrm{i})(x - y\mathrm{i}) = x^2 + y^2$ fortfahren.

[25] In der Literatur häufiger *maximales Ideal*.

**Satz 2.1.38.** *Sei $\mathfrak{a} \subset R$ ein Ideal.*

(i) *Falls $\mathfrak{a}$ ein Maximalideal ist, dann ist $\mathfrak{a}$ auch ein Primideal.*

itm:maximal:1

(ii) *$\mathfrak{a}$ ist genau dann ein Maximalideal, wenn $R/\mathfrak{a}$ ein Körper ist.*

*Beweis.*

(i) Das folgt aus (ii): Wenn $\mathfrak{a} \subset R$ ein Maximalideal ist, so ist nach (ii) $R/\mathfrak{a}$ ein Körper und insbesondere ein Integritätsbereich. Nach Satz 2.1.36 ist ein Primideal.

(ii) Sei $\mathfrak{a} \subset R$ ein Maximalideal. Zu zeigen ist, dass $R/\mathfrak{a}$ ein Körper ist, d. h., dass jedes Element $0 \neq \alpha \in R/\mathfrak{a}$ ein multiplikatives Inverses besitzt. Schreibe dazu $\alpha = \bar{a}$ für ein gewisses $a \in R$. Da $\alpha \neq 0$ gilt $a \notin \mathfrak{a}$.

Wir bilden $\alpha' \coloneqq \alpha + (a) = \{b + ca \mid b \in \mathfrak{a}, c \in R\} \subset R$. Beobachte, dass $\alpha' \subset R$ ein Ideal ist:[26] Für alle $b, b' \in \mathfrak{a}$ und $c, c' \in R$ gilt $(b + ca) + (b' + c'a) = (b + b') + (c + c')a \in \mathfrak{a}'$ da $b + b' \in \mathfrak{a}$, und für alle $d \in R$ gilt $d(b + ca) = (db) + (dc)a \in \mathfrak{a}'$ da $db \in \mathfrak{a}$.

Wegen $a \notin \mathfrak{a}$ ist $\mathfrak{a} \subsetneq \mathfrak{a}'$. Weil $\mathfrak{a} \subset R$ ein Maximalideal ist, folgt $\mathfrak{a}' = R$,[27] also $1 \in \mathfrak{a}'$. Daher existiert ein $b \in \mathfrak{a}$ und ein $c \in R$ mit $1 = b + ca$. Wir erhalten $1_{R/\mathfrak{a}} = \bar{1} = \bar{b} + \bar{c}\bar{a}$. Beachte, dass $\bar{b} = 0$, da $b \in \mathfrak{a}$. Folglich ist $1_{R/\mathfrak{a}} = \bar{c}\alpha$ und $\alpha$ besitzt ein multiplikatives Inverse.

Die Rückrichtung erfolgt mit ähnlichen Argumenten. □

**Bemerkung 2.1.39.** Wenn $R = K$ ein Körper ist, dann ist $(0) \subsetneq R$ das einzige echte Ideal und damit auch das einzige Maximalideal und $R \xrightarrow{\sim} R/(0)$.

**Fakt 2.1.40.** *$R$ ist genau dann ein Körper, wenn $(0) \subset R$ ein Maximalideal ist.*

## 2.2 Polynomringe

**Definition 2.2.1.** Sei $R$ ein beliebiger Ring. Dann ist der **Polynomring** in einer Variablen mit Koeffizienten in $R$ der Ring

$$R[X] \coloneqq \left\{ \sum_{i=0}^{n} a_i X^i \;\middle|\; a_i \in R \right\}.$$

Beachte, dass die Summen immer endliche Summen sind.

*Anmerkung:* Es ist überhaupt nicht klar, was das Symbol $X$ sein soll. Die formal richtige Definition ist folgende:

$$R[X] \coloneqq \{f \colon \mathbb{N} \longrightarrow R \mid |\mathrm{Supp}(f)| < \infty\} \subset \mathrm{Abb}(\mathbb{N}, R).$$

Hierbei ist $\mathrm{Supp}(f) \coloneqq \{a \in \mathbb{N} \mid f(i) \neq 0\}$ der *Träger*. Mit anderen Worten,

$$R[X] \coloneqq \{f \colon \mathbb{N} \longrightarrow \mathbb{R} \mid f(i) = 0 \text{ für alle } i \gg 0\}.$$

[26] Allgemeiner ist die Summe zweier Ideale immer ein Ideal.

[27] Widerspricht das nicht unserer Konvention, dass $R$ kein Ideal ist? Ich fand die Konvention schon immer komisch, und man macht das auch nicht.

Hierbei bedeutet „$f(i) = 0$ für alle $i \gg 0$“, dass „es ein $i_0 \geq 0$ gibt, sodass $f(i) = 0$ für alle $i \geq i_0$“.

*Bemerkung:* Eine Abbildung $f \in R[X]$ ist eindeutig bestimmt durch die Koeffizienten $(f(i))_{i\in\mathbb{N}} = (a_i)_{i\in\mathbb{N}}$. Diese haben die Eigenschaft, dass $a_i = 0$ für alle $i \gg 0$.

Seien also $f \mathrel{\hat{=}} (a_i)_{i\in\mathbb{N}}$ und $g \mathrel{\hat{=}} (b_i)_{i\in\mathbb{N}}$ Polynome in $R[X]$. Dann definieren wir $f + g \in R[X]$ als die Abbildung, die durch

$$(c_i \coloneqq a_i + b_i)_{i\in\mathbb{N}}$$

gegeben ist. Mit anderen Worten,

$$\sum_{i=0}^{n} a_i X^i + \sum_{i=0}^{m} b_i X^i \coloneqq \sum_{i=0}^{\max(m,n)} (a_i + b_i) X^i$$

mit $a_i \coloneqq b_i \coloneqq 0$ für alle $i > \max(m, n)$, was die übliche Addition von Polynomen ist. Ferner definieren wir $f \cdot g \in R[X]$ als die Abbildung, die durch

$$\left( d_i \coloneqq \sum_{j=0}^{i} a_j b_{i-j} \right)_{i\in\mathbb{N}}$$

gegeben ist, was die übliche Multiplikation von Polynomen ist.

**Bemerkung 2.2.2.**

(i) Mit $+$ und $\cdot$ wie oben definiert wird $R[X]$ zu einem Ring.

(ii) Die Abbildung $R \hookrightarrow R[X]$, $a \mapsto aX^0$ ist ein Ringhomomorphismus. Alternativ können wir ihn durch

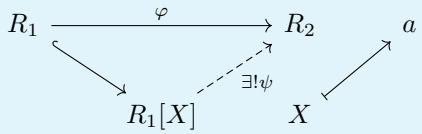
$$a \longmapsto (a_i) \qquad \text{mit} \qquad a_i \coloneqq \begin{cases} a, & \text{falls } i = 0, \\ 0, & \text{falls } i > 0, \end{cases}$$

definieren.

(iii) Falls $R$ ein Integritätsbereich, dann ist die kanonische Abbildung $R \hookrightarrow Q(R)$, $a \mapsto \frac{a}{1}$ in den Quotientenkörper ein Ringhomomorphismus, der einen injektiven Ringhomomorphismus $R[X] \hookrightarrow K[X]$ induziert.

**Beobachtung 2.2.3.** Der Polynomring erfüllt folgende Universaleigenschaft. Seien $\varphi\colon R_1 \to R_2$ ein Ringhomomorphismus und $a \in R_2$ ein beliebiges Element. Dann existiert genau ein Ringhomomorphismus $\psi\colon R_1[X] \to R_2$, sodass $\psi(X) = a$ und sodass folgendes

Diagramm kommutiert:



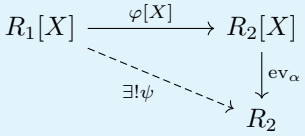

Das lässt sich ausbauen zu einer „universellen Beschreibung“ von $R_1[X]$.

Wenden wir diese Universaleigenschaft auf $\varphi = \mathrm{id}\colon R \to R$ und ein $\alpha \in R$ an, so erhalten wir einen eindeutigen Ringhomomorphismus

$$\mathrm{ev}_\alpha\colon R[X] \longrightarrow R, \qquad X \longmapsto \alpha.$$

Für beliebige Polynome $f = \sum_{i=0}^n a_i X^i$ gilt $\mathrm{ev}_\alpha(f) = \sum_{i=0}^n a_i \alpha^i$, was nicht anderes als $X = \alpha$ einzusetzen ist (engl. *evaluation*).

Umgekehrt können wir auch aus der Existenz von $\mathrm{ev}_\alpha$ die universelle Eigenschaft folgern. Seien $\varphi\colon R_1 \to R_2$ ein Ringhomomorphismus und $\alpha \in R_2$ ein beliebiges Element. Dann gibt es einen Ringhomomorphismus $\psi\colon R_1[X] \to R_2$, sodass folgendes Diagramm kommutiert:




wobei $\varphi[X]\colon \sum_{i=0}^n a_i X^i \mapsto \sum_{i=0}^n \varphi(a_i) X^i$.

Wenn $f \in \mathrm{Ker}(\mathrm{ev}_\alpha\colon R[X] \to R)$, dann ist $\alpha$ eine **Nullstelle** von $f$. Offenbar ist $\alpha$ eine Nullstelle von $f = X - \alpha$. Dann ist $(X - \alpha) \subset \mathrm{Ker}(\mathrm{ev}_\alpha)$.

**Bemerkung 2.2.4.** Die Abbildung

$$R[X] \longrightarrow \mathrm{Abb}(R, R), \qquad f = \sum_{i=0}^n a_i X^i \longmapsto \left(\alpha \longmapsto \mathrm{ev}_\alpha(f) = \sum_{i=0}^n a_i \alpha^i\right)$$

ist ein Ringhomomorphismus. Hierbei wird $\mathrm{Abb}(R, R)$ durch punktweise Addition und Multiplikation, d. h. durch Addition und Multiplikation im Zielring, zu einem Ring.

*Beispiel* 2.2.5. Sei $K = \mathbb{R}, \mathbb{C}$. Dann erhalten wir $K[X] \hookrightarrow \mathrm{Abb}(K, K)$. Damit könnte man $K[X]$ auch als Ring von polynomiellen Funktionen $K \to K$ auffassen.

**Warnung 2.2.6.** Im Allgemeinen ist $K[X] \to \mathrm{Abb}(K, K)$, $f \mapsto (\alpha \mapsto \mathrm{ev}_\alpha(f))$ nicht injektiv. Nehmen wir $K = \mathbb{F}_2 = \mathbb{Z}/2\mathbb{Z}$, so ist $f = X + X^2 \in \mathbb{F}_2[X]$ nicht null, induziert aber die Abbildung $\mathbb{F}_2 \to \mathbb{F}_2$, $a \mapsto a + a^2 = 0$.

**Bemerkung 2.2.7.** Ist $R$ ein Integritätsbereich, so ist $(R[X])^* = R^*$. Das muss aber für Ringe, die keine Integritätsbereiche sind, nicht mehr gelten. Betrachte z. B. $R = \mathbb{Z}/4\mathbb{Z}$. Dann ist $(-2X + 1)(2X + 1) = -4X^2 + 1 = 1$, d. h. $2X + 1$ ist eine Einheit in $R[X]$.

**Definition 2.2.8.** Für beliebige Ringe $R$ definieren wir

$$\deg\colon R[X]\setminus\{0\}\longrightarrow\mathbb{N},\qquad \deg\left(\sum_{i=0}^{n}a_iX^i\right)=\max\{i\mid a_i\neq 0\}.$$

Für $0\neq f\in R[X]$ nennen wir $\deg(f)$ den **Grad** von $f$.

In der Literatur findet man auch häufig noch die Definition $\deg(0)=-\infty$ für das Nullpolynom $0\in R[X]$. Diese ist kompatibel mit den folgenden Eigenschaften.

**Fakt 2.2.9.** *Für $0\neq f,g\in R[X]$ gelten folgende Eigenschaften:*

(i) $\deg(fg)\leq\deg(f)+\deg(g)$ *mit Gleichheit, falls $R$ ein Integritätsbereich ist.*

(ii) $\deg(f+g)\leq\max\{\deg(f),\deg(g)\}$.

:polynomialdivision

**Satz 2.2.10 (Polynomdivision).** *Seien $R$ ein Integritätsbereich und $f=\sum_{i=0}^{n}a_iX^i\in R[X]$ mit $a_n\in R^*$, d. h. $\deg(f)=n$. Dann existieren für jedes Polynom $g\in R[X]$ eindeutige $q,r\in R[X]$, sodass $g=fq+r$ und sodass $r=0$ oder $\deg(r)<\deg(f)=n$.*

*Beweis.* Zuerst die Eindeutigkeit: Falls $g=fq+r=fq'+r'$, dann $(q-q')f=r'-r$, wobei $\deg(r'-r)<\deg(f)=n$ oder $r'=r$. Ferner ist entweder $q=q'$ oder $\deg((q-q')f)\geq n$, da $a_n\in R^*$. Damit erhalten wir stets $q=q'$ und $r'=r$.

Nun zur Existenz: Ist $\deg(g)<\deg(f)$ so können wir $q=0$ und $r=g$ wählen. Andernfalls ist $\deg(g)\geq\deg(f)=n$. Setze $g':=g-b_ma_n^{-1}X^{m-n}f$, wobei wir $g=\sum_{i=0}^{m}b_iX^i$ mit $m=\deg(g)$ schreiben. Dann ist $\deg(g')<\deg(g)=m$. Nach Induktion gibt es $q',r\in R[X]$ mit $g'=fq'+r$ und mit $r=0$ oder $\deg(r)<\deg(f)$. Sodann können wir $q:=g'+b_ma_n^{-1}X^{m-n}$ setzen und erhalten $g=fq+r$. □

**Beobachtung 2.2.11.** Wir betrachten wieder

$$\mathrm{ev}_\alpha\colon R[X]\longrightarrow R,\qquad \sum_{i=1}^{n}a_iX^i\longmapsto\sum_{i=1}^{n}a_i\alpha^i.$$

Wir haben bereits gesehen, dass $f:=X-\alpha\in\mathrm{Ker}(\mathrm{ev}_\alpha)\subset R[X]$ gilt.

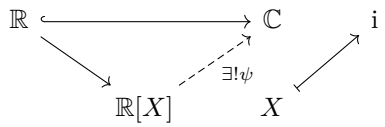
*Behauptung:* $\mathrm{Ker}(\mathrm{ev}_\alpha)=(X-\alpha)$.

*Beweis:* Da $\mathrm{Ker}(\mathrm{ev}_\alpha)$ ein Ideal ist, gilt $(f)\subseteq\mathrm{Ker}(\mathrm{ev}_\alpha)$. Für die umgekehrte Inklusion betrachten wir $g\in\mathrm{Ker}(\mathrm{ev}_\alpha)$. Nach Polynomdivision 2.2.10 gilt $g=fq+r$. Ist $r=0$, so ist $g\in(f)$ und wir sind fertig. Andernfalls ist $r\neq 0$ und $\deg(r)=0$, d. h. $r=a_0X^0$ mit $a_0\neq 0$. Es gilt aber $\mathrm{ev}_\alpha(g)=\mathrm{ev}_\alpha(f)\mathrm{ev}_\alpha(q)+\mathrm{ev}_\alpha(r)$. Wegen $g\in\mathrm{Ker}(\mathrm{ev}_\alpha)$ ist $\mathrm{ev}_\alpha(g)=0$, und es gilt $\mathrm{ev}_\alpha(f)=0$. Wir erhalten $a_0=\mathrm{ev}_\alpha(r)=0$, ein Widerspruch.

*Folgerung:* Da $\mathrm{ev}_\alpha$ surjektiv ist, folgt $R[X]/(X-\alpha)\simeq R$ aus dem Homomorphiesatz (Aufgabe 18).

*Beispiel* 2.2.12. Seien $\mathbb{R}\hookrightarrow\mathbb{C}$ die kanonische Inklusion und $\mathrm{i}\in\mathbb{C}$ die imaginäre Einheit. Nach der universellen Eigenschaft von Polynomringen gibt es genau einen Ringhomomorphismus

$\psi\colon \mathbb{R}[X] \to \mathbb{C}$ mit $\psi(X) = \mathrm{i}$, sodass folgendes Diagramm kommutiert:




(Konkret haben wir $\psi(\sum_{j=0}^{n} a_j X^j) = \sum_{j=0}^{n} a_j \mathrm{i}^j$ mit $a_i \in \mathbb{R}$.) Die Abbildung $\psi$ ist surjektiv, da $a+b\mathrm{i} = \psi(a+bX)$ für alle $a, b \in \mathbb{R}$. Also erhalten wir den Isomorphismus $\mathbb{R}[X]/\operatorname{Ker}(\psi) \simeq \mathbb{C}$. Wie sieht $\operatorname{Ker}(\psi)$ aus?

*Behauptung:* $\operatorname{Ker}(\psi) = (X^2+1)$.

*Beweis:* Offenbar ist $f \coloneqq X^2 + 1 \in \operatorname{Ker}(\psi)$ wegen $\psi(X^2+1) = \mathrm{i}^2 + 1 = 0$. Also ist $(f) \subseteq \operatorname{Ker}(\psi)$. Umgekehrt sei $g \in \operatorname{Ker}(\psi)$. Dann gilt $g = fq + r$ nach Polynomdivision 2.2.10. Ist $r = 0$, so ist $g \in (f)$. Andererseits sind $r \neq 0$ und $\deg(r) < \deg(f) = 2$, also $r = a_0 + a_1 X$. Wegen $\psi(f) = 0$ ist

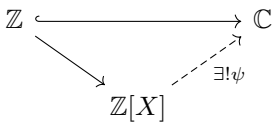
$$0 = \psi(g) = \psi(f)\psi(q) + \psi(r) = \psi(r) = a_0 + a_1\mathrm{i}$$

mit $a_0, a_2 \in \mathbb{R}$. Wir erhalten $a_0 + a_1\mathrm{i} = 0$ und daher $a_0 = a_1 = 0$, ein Widerspruch. Das beweist die Behauptung.

Wir erhalten $\mathbb{R}[X]/(X^2+1) \simeq \mathbb{C}$. Weil $\mathbb{C}$ ein Körper ist, muss $(X^2+1)$ ein Maximalideal sein.

*Beispiel* 2.2.13. Sei $R = \mathbb{Z}$ und betrachte $\mathbb{Z}[\sqrt{n}]$ für $n \in \mathbb{Z}$. Wie definieren wir das formal richtig? Bspw. ist für $n = \pm 5$ dann $\mathbb{Z}[\sqrt{\pm 5}] = \{a + b\sqrt{\pm 5} \mid a, b \in \mathbb{Z}\} \subset \mathbb{C}$.

Wähle $\alpha \in \mathbb{C}$ mit $\alpha^2 = n$, wobei $\alpha$ bis auf Vorzeichen eindeutig ist. Wenden wir die universelle Eigenschaft auf $\alpha$ an, erhalten wir einen eindeutigen Ringhomomorphismus $\psi$ mit $\psi(X) = \alpha$, sodass folgendes Diagramm kommutiert:




Wegen $\alpha^2 = n$ gilt dann $(X^2 - n) \subseteq \operatorname{Ker}(\psi)$.

*Frage:* Ist $\operatorname{Ker}(\psi) = (X^2 - n)$?

*Antwort:* Nicht falls $n = m^2$ mit $m \in \mathbb{Z}$. In diesem Fall ist $\alpha = \pm m$ und daher $X - m \in \operatorname{Ker}(\psi)$ oder $X + m \in \operatorname{Ker}(\psi)$, wobei $X \pm m \notin (X^2 - n)$. Falls $n$ keine Quadratzahl ist, dann gilt $\operatorname{Ker}(\psi) = (X^2 - n)$ und wir erhalten $\operatorname{Im}(\psi) \simeq \mathbb{Z}[X]/(X^2 - n)$.

Damit erklären wir formal den Ring $\mathbb{Z}[\sqrt{n}]$ als $\mathbb{Z}[X]/(X^2 - n)$, falls $n$ eine Quadratzahl ist.

## 2.3 Euklidische Ringe, Hauptidealringe, faktorielle Ringe

VL 9
10.11.23

*Problem* 2.3.1. Wir wollen zeigen, dass euklidische Ringe Hauptidealringe sind, die wiederum faktorielle Ringe sind.

def:euclidean

**Definition 2.3.2.** Ein **euklidischer Ring** besteht aus einem Integritätsbereich $R$ und einer Abbildung $\delta\colon R\setminus\{0\}\to\mathbb{N}$, sodass für alle $f,g\in R$ mit $f\neq 0$ Elemente $q,r\in R$ existieren, sodass $g=fq+r$ und sodass $r=0$ oder $\delta(r)<\delta(f)$.

Solche Ringe erlauben den *euklidischen Algorithmus*. Eine alternative Definition setzt auch $\delta(0)=0$ fest.

*Beispiel* 2.3.3.

(i) $R=\mathbb{Z}$ mit $\delta(n):=|n|$ ist ein euklidischer Ring. Das ist nichts anderes als Division mit Rest.

(ii) $R=K[X]$ mit $K$ einen Körper und $\delta(f)=\deg(f)$ ist ein euklidischer Ring. Das ist Polynomdivision 2.2.10 mit Rest.

(iii) $R=\mathbb{Z}[\mathrm{i}]\subset\mathbb{C}$ mit $\delta(a+b\mathrm{i})=|a+b\mathrm{i}|=a^2+b^2$ ist ein euklidischer Ring.

*Beweis:* Wir müssen zeigen, dass Division mit Rest existiert. Sei $0\neq f=a+b\mathrm{i}\in\mathbb{Z}[\mathrm{i}]$ mit $a,b\in\mathbb{Z}$. Dann gibt es $f^{-1}\in\mathbb{C}$. Damit existiert für beliebiges $g\in\mathbb{C}$ die Zahl $gf^{-1}\in\mathbb{C}$. Diese landet in einer der Zellen in Abb. 2.1. Folglich gibt es eine Zahl $c+d\mathrm{i}\in\mathbb{Z}[\mathrm{i}]$ mit $c,d\in\mathbb{Z}$, sodass $|gf^{-1}-(c+d\mathrm{i})|\leq\frac{1}{2}\sqrt{2}=1/\sqrt{2}$ (das ist die nächste Ecke dieser Zelle). Folglich ist $|g-(c+d\mathrm{i})f|\leq|f|/\sqrt{2}<|f|$. Setze $q:=c+d\mathrm{i}$ und $r:=g-(c+d\mathrm{i})f$.

(iv) $R=\mathbb{Z}[\sqrt{-5}]$ ist kein euklidischer Ring, d. h. es existiert kein $\delta$ wie in Definition 2.3.2. (Wir werden das zeigen, indem wir zeigen, dass das kein faktorieller Ring, s. Beispiel 2.3.14.)

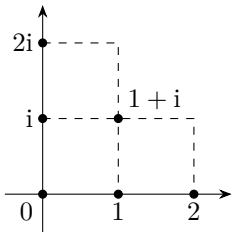



fig:Zi

Abbildung 2.1: Das von $\mathbb{Z}[\mathrm{i}]$ aufgespannte Gitter.

**Definition 2.3.4.** Ein Integritätsbereich $R$ heißt **Hauptidealring** (HIR), falls alle Ideale Hauptideale sind, d. h. für alle Ideale $\mathfrak{a}\subset R$ existiert ein $a\in R$, sodass $\mathfrak{a}=(a)=aR$.

thm:euclidean:pid

**Satz 2.3.5.** *Ein euklidischer Ring ist immer ein Hauptidealring.*

*Beweis.* Seien $(R,\delta)$ ein euklidischer Ring und $\mathfrak{a}\subset R$ ein Ideal. Für alle $0\neq f\in R$ ist $\delta(f)\in\mathbb{N}$. Falls $\mathfrak{a}\neq(0)$, dann existiert ein $a\in\mathfrak{a}$ mit $\delta(a)$ minimal (d. h. für alle $b\in\mathfrak{a}$ gilt $\delta(a)\leq\delta(b)$).

*Behauptung:* $\mathfrak{a}=(a)$.

*Beweis:* Dazu sei $b \in \mathfrak{a}$. Division mit Rest liefert $b = aq + r$ mit $r = 0$ oder $\delta(r) < \delta(a)$. Wegen $b \in \mathfrak{a}$ und $aq \in \mathfrak{a}$ muss $r \in \mathfrak{a}$ sein. Nun kann $\delta(r) < \delta(a)$ aufgrund der Minimalität von $a$ nicht eintreten, weshalb $r = 0$ ist. Also gilt $b \in (a)$ und daher $\mathfrak{a} = (a)$. □

**Bemerkung 2.3.6.** Ähnlich zur Polynomdivision 2.2.10 ist die Division mit Rest für euklidische Ringe auch eindeutig.

*Beispiel* 2.3.7.

(i) $\mathbb{Z}$, $K[X]$ und $\mathbb{Z}[\mathrm{i}]$ sind alles Hauptidealringe.

(ii) $\mathbb{Z}[\sqrt{-5}]$ ist kein Hauptidealring (sehen wir später in Beispiel 2.3.14).

**Warnung 2.3.8.** Es gibt Hauptidealringe, die nicht euklidisch sind. Ein Beispiel ist $R = \mathbb{Z}[\frac{1}{2}(1 + \sqrt{-19})]$.

**Satz 2.3.9.** *Seien $R$ ein Hauptidealring und $a \in R$. Dann sind die folgenden Bedingungen äquivalent:*

itm:pid:element:1 (i) *$a$ ist irreduzibel.*

itm:pid:element:2 (ii) *$a$ ist ein Primelement.*

itm:pid:element:3 (iii) *$(a)$ ist ein Maximalideal.*

*Beweis.*

- (ii) $\Longrightarrow$ (i): Das haben wir bereits in Lemma 2.1.31 gesehen.
- (iii) $\Longrightarrow$ (ii): Angenommen $(a)$ ist ein Maximalideal. Insbesondere ist $(a)$ ein Primideal, weshalb $a$ ein Primelement ist.
- (i) $\Longrightarrow$ (iii): Seien $a \in R$ irreduzibel und $(a) \subset \mathfrak{a} \subset R$ ein Ideal. Nach Voraussetzung ist $\mathfrak{a}$ ein Hauptideal, d. h. es gibt ein $b \in \mathfrak{a}$ mit $\mathfrak{a} = (b)$. Also ist $a \in (b)$, d. h. es gibt ein $c \in R$ mit $a = bc$. Da $a$ irreduzibel ist, gilt $b \in R^*$ oder $c \in R^*$. Falls $b \in R^*$, so ist $\mathfrak{a} = R$. Falls $c \in R^*$, so ist $(a) = \mathfrak{a}$. Das zeigt, dass $(a)$ ein Maximalideal ist. □

def:ufd **Definition 2.3.10.** Ein Integritätsbereich $R$ heißt **faktoriell**, falls folgende Bedingungen gelten.

itm:ufd:1 (i) Sei $0 \neq a \in R \setminus R^*$. Dann existieren irreduzible Elemente $a_1, \ldots, a_n \in R$ mit $a = a_1 \cdots a_n$.

itm:ufd:2 (ii) Die Zerlegung $a = a_1 \cdots a_n$ ist eindeutig bis auf Permutation und Einheiten.

Die Eindeutigkeit meint, dass z. B. $a_1 \cdots a_n = (\varepsilon a_1)(\varepsilon^{-1} a_2) a_4 a_3 \cdots a_n$ mit $\varepsilon \in R^*$ dieselbe Zerlegung sind.

Folgende Aussage vereinfacht den Hauptsatz.

**Satz 2.3.11.** *Seien $R$ ein Integritätsbereich und es gelte (i) in Definition 2.3.10. Dann sind (ii), (ii') und (ii'') alle äquivalent, wobei:*

itm:ufd:2a (ii') *Jedes irreduzible Element ist ein Primelement (d. h. irreduzibel und prim sind äquivalent).*

itm:ufd:2b (ii'') *Alle $0 \neq a \in R \setminus R^*$ besitzen eine Produktdarstellung $a = a_1 \cdots a_n$ mit $a_1, \ldots, a_n$ Primelementen.*

*Beweis.*

- (ii') $\implies$ (ii''): Nach (i) gibt es für jedes $0 \neq a \in R \setminus R^*$ irreduzible $a_1, \ldots, a_n$, sodass $a = a_1 \cdots a_n$. Nach (ii') sind die $a_i$ Primelemente.
- (ii'') $\implies$ (ii'): Sei $a \in R$ irreduzibel. Nach (ii'') gilt $a = a_1 \cdots a_n$ mit Primelementen $a_i$. Da $a$ irreduzibel ist, folgen $n = 1$ und, dass $a$ ein Primelement ist.
- (ii) $\implies$ (ii'): Seien $a \in R$ irreduzibel und $a \mid bc$, d. h. es git ein $a' \in R$ mit $aa' = bc$. Nach (i) existieren Zerlegungen $a' = a'_1 \cdots a'_n$, $b = b_1 \cdots b_m$ und $c = c_1 \cdots c_k$ mit $a'_i, b_i, c_i$ irreduzibel. Wir erhalten $aa'_1 \cdots a'_n = b_1 \cdots b_m c_1 \cdots c_k$. Alle Elemente sind irreduzibel. Nach (ii) (Eindeutigkeit der Zerlegung), folgt $a = \varepsilon b_i$ oder $a = \delta c_j$ für gewisse $i$ und $j$ und $\varepsilon, \delta \in R^*$. Wir erhalten $a \mid b$ bzw. $a \mid c$. Also ist $a$ ein Primelement.
- ((ii') $\iff$ (ii'')) $\implies$ (ii): Seien $0 \neq a \in R \setminus R^*$ und $a = a_1 \cdots a_n = b_1 \cdots b_m$ mit $a_i, b_j \in R$ irreduzibel. Nach Annahme sind $a_i, b_j$ alle Primelemente. Aus $b_1 \mid (a_1, \ldots, a_n)$ folgt, dass $b_1$ eines der Faktoren teilt, sagen wir o. B. d. A. $b_1 \mid a_1$. Dann gibt es ein $\varepsilon \in R$ mit $a_1 = b_1 \varepsilon$. Weil $a_1$ irreduzibel ist, ist $b_1 \in R^*$ oder $\varepsilon \in R^*$. Aber $b_1 \in R^*$ ist unmöglich, also $\varepsilon \in R^*$. Dann können wir durch $b_1$ teilen[28] und erhalten $(\varepsilon a_2) a_3 \cdots a_n = b_2 \cdots b_m$. Fahre nun induktiv über $n$ und $m$ fort. □

**Satz 2.3.12.** *Sei $R$ ein Ring. Dann gelten folgende Implikationen:*

$$R \text{ ist euklidischer Ring} \implies R \text{ ist Hauptidealring} \implies R \text{ ist faktoriell.}$$

*Beweis.* Wegen Satz 2.3.5 müssen wir nur noch zeigen, dass wenn $R$ ein Hauptidealring ist, es dann auch faktoriell ist.

Wir zeigen (i): Sei $0 \neq a \in R \setminus R^*$. Unser Ziel ist es, $a = a'b$ mit $a'$ irreduzibel zu schreiben.

Falls $a$ irreduzibel ist, so sind wir fertig. Falls nicht, so existiert eine Zerlegung $a = a_1 b$ mit $a_1, b \notin R^*$. Falls $a_1$ irreduzibel ist, so sind wir fertig. Falls nicht, so existiert eine weitere Zerlegung $a_1 = a_2 a'_2$ mit $a_2, a'_2 \notin R^*$; insbesondere ist $(a_1) \subset (a_2)$. Wenn $a_2$ irreduzibel ist, so gilt $a = a_2(a'_2 b)$ und wir sind fertig. Ansonsten können wir $a_2$ weiter zu $a_2 = a_3 a'_3$ zerlegen, d. h. $a = a_3(a'_3 a'_2 b)$ mit $(a_2) \subset (a_3)$.

Induktiv erhalten wir die aufsteigen Sequenz $(a_1) \subset (a_2) \subset (a_3) \subset \cdots$ von Idealen. Wenn der Prozess abbricht, dann gilt $a = a'b$ mit $a'$ irreduzibel, d. h. wir sind fertig. Falls nicht, setzen wir $\mathfrak{a} := \bigcup_{i=1}^{\infty} (a_i) \subset R$, was wieder ein Ideal ist (für alle $x, y \in \mathfrak{a}$ gibt es ein gemeinsames $(a_i)$, in der sie drin liegen). Da $R$ ein Hauptidealring ist, gibt es ein $\alpha \in \mathfrak{a}$ mit $\mathfrak{a} = (\alpha)$. Folglich gibt es ein $i_0$, sodass $\alpha \in (a_{i_0}) \subset (a_{i_0+1}) \subset \cdots$, also $\mathfrak{a} = (a_{i_0}) = (a_{i_0+1}) = \cdots$.

[28] Das erfordert, dass $R$ ein Integritätsbereich ist. Stelle nämlich $b_1(\varepsilon a_2 \cdots a_n - b_2 \cdots b_m) = 0$ um, wobei $b_1 \neq 0$.

Also ist $a_{i_0}$ irreduzibel und dieser Prozess bricht immer ab. Schließlich erhalten wir $a = b_1 b$ mit $b_1$ irreduzibel.

Wenden wir dieselbe Idee induktiv auf $b$ an, so gilt $a = b_1 b = b_1 b_2 b' = \cdots = b_1 \cdots b_n \hat{b}$ mit $b_1, \ldots, b_n$ irreduzibel. Wir erhalten wieder eine aufsteigende Sequenz von Idealen, die wieder abbrechen muss, da $R$ ein Hauptidealring ist. Somit folgt, dass $a$ ein Produkt von irreduziblen Elementen ist.

Wir zeigen (ii) bzw. äquivalent dazu (ii'): Zu zeigen ist, dass jedes irreduzible Element $a \in R$ ein Primelement ist. Wir wissen, dass $a$ genau dann ein Primelement ist, wenn $(a)$ ein Primideal ist. Ferner ist jedes Maximalideal ein Primideal. Sodann genügt es zu zeigen, dass $(a) \subset R$ ein Maximalideal ist.

Dazu sei $(a) \subset \mathfrak{a} \subset R$ ein Ideal. Da $R$ ein Hauptidealring ist, existiert ein $b \in R$ mit $\mathfrak{a} = (b)$, d. h. es gibt ein $a' \in R$ mit $a = a'b$. Da $a$ irreduzibel ist, folgt $a' \in R^*$ oder $b \in R^*$. Wenn $a' \in R^*$, dann $(a) = (b) = \mathfrak{a}$. Wenn $b \in R^*$, dann $\mathfrak{a} = (b) = R$. □

Der Beweis ergibt direkt folgende Aussage.

**Korollar 2.3.13.** *Für Hauptidealringe $R$ gelten:*

(i) *Jedes Primideal $0 \neq \mathfrak{p} \subset R$ ist ein Maximalideal.*

(ii) *Für beliebige Ideale $\mathfrak{a} \subset R$ ist $\mathfrak{a}$ genau dann ein Primideal, wenn $R/\mathfrak{a}$ ein Körper ist.*

(iii) *Ein Ideal $\mathfrak{a} \subset R$ ist genau dann ein Maximalideal, wenn $\mathfrak{a} = (a)$ für ein Primelement $a \in \mathfrak{a}$ gilt.*

ex:zsqrtm5

*Beispiel* 2.3.14. $\mathbb{Z}[\sqrt{-5}]$ ist nicht faktoriell und somit weder euklidisch noch ein Hauptidealring. Es gilt nämlich $2 \cdot 3 = 6 = (1 + \sqrt{-5})(1 - \sqrt{-5})$, wobei $2, 3, 1 \pm \sqrt{-5}$ alles irreduzibel sind.

**Bemerkung 2.3.15.** Faktorielle Ringe sind im Allgemeinen keine Hauptidealringe. Z. B. ist $K[X_1, X_2]$ ist faktoriell, aber kein Hauptidealring, da z. B. $(X_1) \subset K[X_1, X_2]$ ein Primideal, aber kein Maximalideal ist.

**Bemerkung 2.3.16.** Eine Frage aus der Zahlentheorie: Wann sind Ringe der Form $\mathbb{Z}[\sqrt{-n}]$ mit quadratfreien $n \in \mathbb{N}$ faktoriell? Z. B. ist $n = 1$ faktoriell, aber $n = 5$ nicht faktoriell.

Tatsächlich gilt der **Satz von Stark-Heegner**: Nur für die folgenden Zahlen $n$ ist $\mathbb{Z}[\sqrt{-n}]$ faktoriell (das ist nicht ganz korrekt, tatsächlich muss das $\mathcal{O}_{\mathbb{Q}(\sqrt{-n})}$ statt $\mathbb{Z}[\sqrt{-n}]$ sein, was in der Natur aber wie $\mathbb{Z}[\sqrt{-n}]$ funktioniert):

$$n = 1, 2, 3, 7, 11, 19, 43, 67, 163.$$

Für Ringe der Form $\mathbb{Z}[\sqrt{n}]$ ist das noch ein ungelöstes Problem, ob es nur endlich viele solche $n$ gibt.

*Problem* 2.3.17. Als nächstes Ziel wollen wir Kriterien für die Irreduzibilität von Polynomen $f \in K[X]$ finden. Einige Beispiele:

VL 10
15.11.23

(i) Betrachte $f \in K[X]$ mit $\deg(f) \geq 2$. Gibt es eine Nullstelle $a \in K$ von $f$, so ist $f$ nicht irreduzibel, denn dann ist $(X - a) \mid f$ und $f$ zerfällt in zwei nichtinvertierbare Faktoren vom Grad mindestens 1.

(ii) Betrachte $f \in K[X]$ von Grad 2 oder 3. Dann ist $f$ genau dann irreduzibel, wenn $f$ keine Nullstelle in $K$ besitzt.

Wir wollen das in zwei Schritten lösen. Seien hierzu $R$ ein Integritätsbereich (z. B. $R = \mathbb{Z}$) und $K = Q(R)$ der Quotientenkörper (also $K = \mathbb{Q}$).

(i) Wir betrachten $R[X]$ als Unterring von $K[X]$. Was ist die Beziehung zwischen irreduziblen $f \in R[X]$ und irreduziblen $f \in K[X]$.

*Antwort:* Das läuft auf das *gaußsche Lemma* hinaus.

(ii) Wir betrachten ein Primideal $\mathfrak{p} \subset R$ und die zugehörige Projektion $R[X] \twoheadrightarrow R/\mathfrak{p}[X]$, $f \mapsto \bar{f}$. Was ist die Beziehung zwischen irreduziblen $\bar{f} \in R/\mathfrak{p}[X]$ und irreduziblen $f \in R[X]$?

*Antwort:* Das läuft auf das *Eisensteinkriterium* hinaus. Das liefert auch ein einfaches Kriterium für die Irreduzibilität sog. *Kreisteilungspolynome.*

*Beispiel:* Das fünfte Kreisteilungspolynom $\Phi_5 = X^4 + X^3 + X^2 + X + 1 \in \mathbb{Q}[X]$ ist irreduzibel über $\mathbb{Q}$. Wegen $\Phi_5(X + 1) = X^5 - 1$ ist sehen wir, dass die Nullstellen von $\Phi_5$ genau die fünften Einheitswurzeln ungleich 1 sind.

*Beispiel* 2.3.18. Wir zeigen, dass $\Phi_5$ zumindest in $\mathbb{Z}[X]$ irreduzibel ist.

*Beweis:* Es gilt $\Phi_5(a) \neq 0$ für all $a \in \mathbb{Q}$, denn die Nullstellen von $\Phi_5$ sind

$$\{e^{2\pi i n/5} \mid n = 1, 2, 3, 4\} \subseteq \mathbb{C} \setminus \mathbb{R}$$

(s. Abb. 2.2). Falls $\Phi_5$ nicht irreduzibel ist, so zerfällt $\Phi_5 = g_1 g_2$ mit $g_1 = b_2X^2 + b_1X + b_0$ und $g_2 = c_2X^2 + c_1 + c_0$ mit $b_i, c_i \in \mathbb{Z}$. Koeffizientenvergleich liefert $b_2c_2 = 1$, also $b_2 = c_2 = \pm 1$. O. B. d. A. sei $b_2 = c_2 = 1$. Analog erhalten wir durch Vergleich von Koeffizienten vor $X^3, X^2, X^1, X^0$ in der Gleichung

$$(X^4 + X^3 + X^2 + X + 1) = (X^2 + b_1X + b_0)(X^2 + c_1X + c_0)$$

die Relationen

$$1 = b_1 + c_1, \qquad 1 = b_0 + b_1c_1 + c_0, \qquad 1 = b_0c_0.$$

Aus $1 = b_0c_0$ folgt $b_0 = c_0 = \pm 1$.

(i) Fall $b_0 = c_0 = 1$: Dann folgt $b_1c_1 = -1$ also $b_1 = -c_1 = \pm 1$. Das widerspricht aber $1 = b_1 + c_1$.

(ii) Fall $b_0 = c_0 = -1$: Dann folgt $b_1c_1 = 3$. Aufgrund Symmetrie seien o. B. d. A. $b_1 = \pm 1$ und $c_1 = \pm 3$. Das widerspricht aber $1 = b_1 + c_1$.

Somit ist $\Phi_5 \in \mathbb{Z}[X]$ irreduzibel.

*Bemerkung:* Diese Methode ist nicht zufriedenstellend. Wir wissen immer noch nicht, ober $\Phi_5$ auch als Element in $\mathbb{Q}[X]$ irreduzibel ist. Ferner wissen wir auch nicht, ob andere Polynome wie $\Phi_{17} = X^{16} + \cdots + X + 1 \in \mathbb{Z}[X]$ irreduzibel sind.

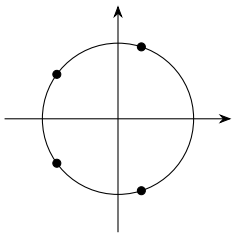


fig:cyclotomic5

Abbildung 2.2: Nullstellen von $\Phi_5$ in $\mathbb{C}$.

## 2.4 Gaußsches Lemma

*Problem* 2.4.1. Ziel ist folgende Aussage: *Ist $R$ ein faktorieller Ring, so ist auch $R[X]$ faktoriell.* Z. B. ist $K[X_1, X_2] = K[X_1][X_2]$ faktoriell, obwohl es weder ein euklidischer Ring noch ein Hauptidealring ist.

**Definition 2.4.2.** Sei $R$ ein faktorieller Ring. Dann heißt $\alpha$ der **größte gemeinsame Teiler** von $a, b \in R$, falls $\alpha \mid a$ und $\alpha \mid b$, und falls aus $c \mid a$ und $c \mid b$ auch $\alpha \mid c$ folgt. Wir schreiben $\alpha =: \mathrm{ggT}(a, b)$.

Das können wir auch auf mehrere Elemente $a_i \in R$ verallgemeinern; der größte gemeinsame Teiler ist dann $\mathrm{ggT}(a_1, \dots, a_n)$.

*Beweis.* Wir zeigen die Existenz. Schreibe $a = \prod_{i=1}^{k} a_i^{n_i}$ und $b = \varepsilon \prod_{i=1}^{l} a_i^{m_i}$ mit paarweise verschiedenen irreduziblen Elementen $a_i$ (welche Primelemente sind) und $\varepsilon \in R^*$, wobei eventuell $n_i = 0$ oder $m_i = 0$ für gewisse $i$.[29] Dann gilt $\mathrm{ggT}(a, b) = \prod_{i=1}^{\max(k,l)} a_i^{\min(m_i, n_i)}$. □

**Warnung 2.4.3.** Der größte gemeinsame Teiler ist nur eindeutig bis auf Multiplikation mit Einheiten.

**Definition 2.4.4.** Seien $R$ ein faktorieller Ring und $f = \sum_{i=0}^{n} a_i X^i \in R[X]$.

(i) Dann heißt $c(f) \coloneqq \mathrm{ggT}(a_0, \dots, a_n)$ der **Inhalt** von $f$.

(ii) $f$ heißt **primitiv**, falls $c(f) \in R^*$.

Einige einfache Beobachtungen.

fact:primitive

**Fakt 2.4.5.**

(i) *Falls $f \in R[X]$ mit $\deg(f) > 0$ irreduzibel ist, dann ist $f$ primitiv.*[30]

itm:content:2

(ii) *Jedes $f \in R[X]$ lässt sich als Produkt $f = c(f) f_0$ mit $f_0 \in R[X]$ primitiv schreiben.*

(iii) *Seien $R$ ist ein Integritätsbereich und $K \coloneqq Q(R)$. Für jedes $f \in K[X]$ existieren $c(f) \in K$ und $f_0 \in R[X]$ primitiv mit $f = c(f) f_0$. Dieses Produkt ist eindeutig bis auf Multiplikation mit Einheiten in $R$, d. h. alle anderen Zerlegungen sind von der Form $f = (c(f)\varepsilon)(\varepsilon^{-1} f_0)$ mit $\varepsilon \in R^*$.*

[29] Das funktioniert natürlich nicht, wenn $a = 0$ oder $b = 0$. In diesem Fall ist $\mathrm{ggT}(a, 0) = a$ für alle $a \in R$.

Achtung: *$c(f)$ ist hier ein (nur) Element in $K$. Da der Inhalt bis auf Einheiten eindeutig ist, ist $c(f)$ auch der Inhalt von $f$.*

[30] In der Vorlesung behauptete der Dozent, dass diese Aussage für alle $f \in R[X]$ gilt, was falsch ist. Für $f \in R$ ist nämlich $c(f) = f$.

*Beweis.*

(i) Seien $f = \sum_{i=1}^{n} a_i X^i$ und $c \coloneqq c(f)$. Dann gilt $f = cf_0$ mit $f_0 \coloneqq \sum_{i=1}^{n} (a_i/c) X^i$, wobei $c, a_i/c \in R$. Wäre $f$ nicht primitiv, so ist $c \notin R^*$ und damit auch $c \notin R[X]^*$. Ferner ist $f_0 \notin R[X]^*$ da $\deg(f_0) \geq 1$. Folglich ist $f$ nicht irreduzibel.

(ii) Trivial per Definition.

(iii) Schreibe $f = \sum_{i=1}^{n} a_i X^i$ mit $a_i \in K$, d. h. $a_i = b_i/c_i$ für $b_i, c_i \in R$. Definiere

$$g \coloneqq f \prod_{i=1}^{n} c_i = \sum_{i=1}^{n} b_i X^i \in R[X].$$

Nach (ii) gilt $g = c(g) f_0$ mit $f_0 \in R[X]$ primitiv. Wir erhalten $f = (c(g)/\prod_{i=1}^{n} c_i) f_0$. Das zeigt die Existenz der Zerlegung.

Für die Eindeutigkeit nehmen wir $f = c_1 f_1 = c_2 f_2$ mit $c_1, c_2 \in K$ und $f_1, f_2 \in R[X]$ primitiv an. Dann gibt es einen Hauptnenner $0 \neq d \in R$, sodass $dc_1, dc_2 \in R$. Wir erhalten $df = (dc_1) \cdot f_1 = (dc_2) \cdot f_2$ in $R$, also

$$(dc_1) \cdot c(f_1) = c((dc_1) \cdot f_1) = c((dc_2) \cdot f_2) = (dc_2) \cdot c(f_2).$$

Aufgrund Primitivität sind $c(f_1), c(f_2) \in R^*$, woraus $c_1 = \varepsilon c_2$ für ein $\varepsilon \in R^*$ folgt. □

lem:gauss

**Lemma 2.4.6 (Lemma von Gauß).** *Seien $R$ ein faktorieller Ring und $f_1, \ldots, f_2 \in R[X]$ primitive Polynome. Dann ist auch $f_1 \cdots f_n \in R[X]$ primitiv.*

*Beweis.* O. B. d. A. zeigen wir das für $n = 2$; der Rest ist Induktion. Seien $f_1 = \sum_{i=1}^{n} a_i X^i$, $f_2 = \sum_{i=1}^{m} b_i X^i$ und $f_1 f_2 = \sum_{i=1}^{n+m} c_i X^i$ mit $c_j = \sum_{i=0}^{j} a_{j-i} b_i$.

Um zu zeigen, dass $f_1 f_2$ primitiv ist, müssen wir $c(f_1 f_2) \in R^*$ nachweisen. Angenommen $c(f_1 f_2) \notin R^*$. Dann existiert ein Primelement $a \in R$ mit $a \mid c_i$ für alle $i = 0, \ldots, n+m$. Nach Voraussetzung sind $f_1$ und $f_2$ beide primitiv. Wähle also $k \leq n$ und $l \leq m$ maximal, sodass $a \nmid a_k$ und $a \nmid b_l$. Untersuchen wir

$$c_{k+l} = \underbrace{(a_{k+l} b_0 + a_{k+l-1} b_1 + \cdots + a_{k+1} b_{l-1})}_{=:A} + a_k b_k + \underbrace{(a_{k-1} b_{l+1} + \cdots + a_0 b_{l+k})}_{=:B}.$$

Aufgrund Maximalität von $k$ gelten $a \mid a_{k+1}$ bis $a \mid a_{k+l}$, also $a \mid A$. Analog gelten $a \mid b_{l+1}$ bis $a \mid b_{l+k}$, also $a \mid B$. Aber $a \nmid (a_k b_l)$, d. h. $a \nmid c_{k+l}$, ein Widerspruch. □

**Definition 2.4.7.** Ein Polynom $f \in R[X]$ heißt **normiert**, falls der **Leitkoeffizient** eins ist, d. h. $f = X^n + a_{n-1} X^{n-1} + \cdots + a_1 X + a_0$.

Einige einfache Folgerungen.

cor:gauss

**Korollar 2.4.8.** *Seien $R$ ein faktorieller Ring und $K \coloneqq Q(R)$.*

itm:gauss:1

(i) *Wenn $f, g \in R[X]$ mit $g$ primitiv und $h \in K[X]$, sodass $f = gh$, dann gilt bereits $h \in R[X]$.*

itm:gauss:2 (ii) *Sei $f \in R[X]$ mit $\deg(f) > 0$. Wenn $f \in R[X]$ irreduzibel ist, dann ist auch $f \in K[X]$ irreduzibel.*

itm:gauss:3 (iii) *Sei $f \in R[X]$ primitiv. Wenn $f \in K[X]$ irreduzibel ist, dann ist auch $f \in R[X]$ irreduzibel.*

(iv) *Sei $f \in R[X]$ mit $\deg(f) > 0$. Dann ist $f \in R[X]$ genau dann irreduzibel, wenn $f \in K[X]$ irreduzibel und $f$ primitiv ist.*

(v) *Seien $f \in R[X]$ und $g, h \in K[X]$ mit $f = gh$. Falls $f$ und $g$ beide normiert sind, so gilt $g, h \in R[X]$.*

itm:gauss:6 (vi) *Umkehrung des Lemmas von Gauß 2.4.6: Seien $f_1, f_2 \in R[X]$. Ist $f_1 f_2 \in R[X]$ primitiv, so sind auch $f_1, f_2 \in R[X]$ beide primitiv.*

*Beweis.*

(i) Schreibe $f = c(f)f_0$ mit $f_0 \in R[X]$ primitiv und $c(f) \in R$, und schreibe $h = c(h)h_0$ mit $h_0 \in R[X]$ primitiv und $c(h) \in K$ (Fakt 2.4.5). Dann ist $c(f)f_0 = f = gh = c(h)(gh_0)$. Weil $g$ und $h_0$ beide primitiv sind, ist nach dem Lemma von Gauß 2.4.6 $gh_0 \in R[X]$ primitiv. Aus der Eindeutigkeit dieser Zerlegung folgt, dass es ein $\alpha \in R^*$ gibt, sodass $c(f)\alpha = c(h)$. Insbesondere ist $c(h) \in R$ und damit $h = c(h)h_0 \in R[X]$.

(ii) Angenommen $f = gh$ mit $g, h \in K[X]$ und $\deg(g), \deg(h) > 0$. Schreibe $g = c(g)g_0$ mit $g_0 \in R[X]$ primitiv und $c(g) \in K$. Dann gilt $f = gh = c(g)g_0h = g_0(c(g)h)$. Nach (i) ist $c(g)h \in R[X]$. Also ist $f = g_0(c(g)h)$ ein Produkt in $R[X]$ mit $\deg(g_0) > 0$ und $\deg(c(g)h) > 0$, was aber der Irreduzibilität von $f$ widerspricht.

(iii) Angenommen $f = gh$ in $R[X]$ mit $g, h \in R[X] \setminus R[X]^* = R[X] \setminus R^*$. Da $f \in K[X]$ irreduzibel ist, impliziert die Annahme, dass $g \in K$ oder $h \in K$. O. B. d. A. sei $g \in K \cap R[X] = R$. Damit teilt $g$ alle Koeffizienten von $f$. Da $f$ primitiv ist, folgt daraus $g \in R^*$, ein Widerspruch.

(iv) Das folgt aus (ii) und (iii) und Fakt 2.4.5.

(v) Schreibe $g = c(g)g_0$ mit $g_0 \in R[X]$ primitiv und $c(g) \in K$. Es folgt $f = gh = g_0(c(g)h)$ und mit (i) daher $c(g)h \in R[X]$. Bezeichne mit $\mathrm{LK}(p)$ den Leitkoeffizienten eines Polynoms $p$. Weil $f$ normiert ist, gilt $1 = \mathrm{LK}(f) = \mathrm{LK}(g_0)\mathrm{LK}(c(g)h)$, d. h. $\mathrm{LK}(g_0) \in R^*$. Weil $g$ normiert ist, gilt $1 = \mathrm{LK}(g) = c(g)\mathrm{LK}(g_0)$, woraus $c(g) \in R^*$ folgt. Somit sind $g = c(g)g_0 \in R[X]$ und $h = c(g)^{-1}(c(g)h) \in R[X]$.

(vi) Schreibe $f_i = c(f_i)\tilde{f}_i$ mit $\tilde{f}_i \in R[X]$ primitiv. Dann gilt $f_1 f_2 = c(f_1)c(f_2)\tilde{f}_1\tilde{f}_2$. Nach dem Lemma von Gauß 2.4.6 ist $\tilde{f}_1\tilde{f}_2$ primitiv. Mit der Voraussetzung folgt also $c(f_1)c(f_2) = c(f_1 f_2) \in R^*$ und daher $c(f_1), c(f_2) \in R^*$. □

Kommen wir nun zum Hauptsatz dieses Unterabschnitts.

**Satz 2.4.9.** *Sei $R$ ein faktorieller Ring. Dann ist auch $R[X]$ faktoriell.*

*Beispiel* 2.4.10. $\mathbb{Z}$ und $K[X]$ sind faktoriell. Deshalb sind auch $\mathbb{Z}[X]$ und $K[X_1, X_2]$ faktoriell, welche beide weder euklidisch noch Hauptidealringe sind. ($\mathbb{Z}[X]$ ist kein Hauptidealring, da z. B. $(2, X) \subset \mathbb{Z}[X]$ kein Hauptideal ist. Ein anderes Argument ist, dass $(2) \subset \mathbb{Z}[X]$ zwar ein Primideal, aber kein Maximalideal ist.)

*Beweis.* Wir müssen zwei Eigenschaften nachweisen.

(i) Jedes Element $0 \neq f \in R[X] \setminus R[X]^*$ lässt sich als Produkt irreduzibler Elemente (oder Primelemente) schreiben.

itm:ufd:2a
(ii′) Jedes irreduzible Element ist ein Primelement.

Ans Werk.

(i) Wir wollen $f$ in ein Produkt von irreduziblen Elementen zerlegen. Dazu induzieren über $\deg(f)$. Falls $\deg(f) = 0$, d. h. $f \in R$, so existiert eine Produktzerlegung $f = a_1 \cdots a_n$ in $R$ mit $a_i \in R$ irreduzibel. Dann sind auch alle $a_i \in R[X]$ irreduzibel,[31] womit wir fertig wären.

Sei also $\deg(f) > 0$. Schreibe $f = c(f)f_0$ mit $f_0 \in R[X]$ primitiv und $c(f) \in R$. Wie eben ist $c(f)$ ein Produkt irreduzibler Elemente in $R[X]$. Ist $f_0$ irreduzibel, so sind wir fertig. Ansonsten gilt $f_0 = gh$ mit $g, h \in R[X] \setminus R[X]^* = R[X] \setminus R^*$. Aus Korollar 2.4.8 (vi) folgt, dass $g, h \in R[X]$ primitiv sind. Falls $\deg(g) = 0$, d. h. $g \in R$, so ist $g \in R^*$, ein Widerspruch; analog für $h$. Also ist $\deg(g), \deg(h) > 0$ und damit $\deg(g), \deg(h) < \deg(f_0)$. Nach Induktionsvoraussetzung sind $g$ und $h$ jeweils ein Produkt von irreduziblen Elementen in $R[X]$ und damit auch $f_0$.[32]

itm:ufd:2a
(ii′) Sei $f \in R[X]$ irreduzibel. Angenommen $\deg(f) > 0$. Aufgrund Korollar 2.4.8 (ii) ist $f \in K[X]$ irreduzibel. Weil $K[X]$ euklidisch und damit faktoriell ist, ist $f \in K[X]$ ein Primelement. Falls also $f \mid gh$ mit $g, h \in R[X]$, so gilt auch $f \mid gh$ in $K[X]$ und damit $f \mid g$ oder $f \mid h$ in $K[X]$. O. B. d. A. sei $f \mid g$ in $K[X]$, sagen wir $g = fg_1$ mit $g_1 \in K[X]$. Weil $f$ irreduzibel ist, ist es auch primitiv. Wegen Korollar 2.4.8 (i) ist $g_1 \in R[X]$, d. h. $f \mid g$ in $R[X]$. Somit ist $f$ ein Primelement in $R[X]$. □

**Aufgabe 2.4.11.** Wie behebt man den zweiten Teil des Beweises, wenn $\deg(f) = 0$?

*Lösung.* Sei $f \in R[X]$ irreduzibel mit $\deg(f) = 0$, d. h. $f \in R$. Dann ist auch $f$ irreduzibel in $R$, denn falls $f = gh$ mit $g, h \in R$, dann auch $f = gh$ in $R[X]$. Es folgt $g \in R[X]^* = R^*$ oder $h \in R[X]^* = R^*$.

Weil $R$ faktoriell ist, ist $f$ insbesondere ein Primelement in $R$. Angenommen $f \mid gh$ mit $g, h \in R[X]$. Schreibe $g = c(g)g_0$ und $h = c(h)h_0$ mit $g_0, h_0 \in R[X]$ primitiv und $c(g), c(h) \in R$. Weil $g_0$ und $h_0$ primitiv sind und $f \in R \setminus R^*$, muss $f \mid c(g)c(h)$ in $R$ sein.

[31] Sei $f \in R$ irreduzibel. Angenommen $f = gh \in R[X]$ mit $g, h \in R[X]$. Wegen $\deg(f) = 0$ gilt $\deg(g) = 0 = \deg(h)$, d. h. $g, h \in R$ und damit $g \in R^*$ oder $h \in R^*$. Wegen $R^* = R[X]^*$ ist $f \in R[X]$ irreduzibel.

[32] In diesem Teil des Beweises war der Dozent sehr grob, und mir war seine Beweisidee auch nicht sofort klar (vielen Dank an Laurens). Hier ein anderer Beweis, den ich aus p15: sch [Sch, 5.50] kenne: Beim Übergang zu $K := Q(R)$ finden wir für $0 \neq f \in R[X] \setminus R[X]^*$ eine Zerlegung $f = f_1 \cdots f_n$ in $K[X]$ mit $f_i \in K[X]$ irreduzibel. Schreibe $f_i = c(f_i)\tilde{f}_i$ mit $\tilde{f}_i \in R[X]$ primitiv und $c(f_i) \in K^*$. Beobachte, dass auch $\tilde{f}_i \in K[X]$ irreduzibel ist, weshalb $\tilde{f}_i \in R[X]$ irreduzibel ist nach Korollar 2.4.8 (iii). Ferner impliziert Korollar 2.4.8 (vi), dass $\tilde{f}_1 \cdots \tilde{f}_n \in R[X]$ primitiv, d. h. nach Korollar 2.4.8 (i) ist $c' := c(f)c(f_1) \cdots c(f_n) \in R$. Wir finden also eine Primfaktorzerlegung $c' = \varepsilon a_1 \cdots a_m$ in $R$ mit $a_i \in R$ irreduzibel und $\varepsilon \in R^*$. Somit ist $f = \varepsilon a_1 \cdots a_m \tilde{f}_1 \cdots \tilde{f}_n$ eine Zerlegung in irreduzible Elemente in $R[X]$.

Weil $f$ ein Primelement ist, folgt $f \mid c(g)$ oder $f \mid c(h)$, d. h. $f \mid g$ oder $f \mid h$. Also ist $f$ auch prim in $R[X]$.

## 2.5 Irreduzibilitätskriterien

VL 11
17.11.23

*Problem* 2.5.1. Wir werden beantworten, wann $\Phi_p(X) = X^{p-1} + \cdots + X + 1$ irreduzibel ist.

. Erinnerung Seien $R$ ein faktorieller Ring (also z. B. $\mathbb{Z}$, $K[X]$, $K[X_1, X_2]$) und $\mathfrak{p} \subset R$ ein Primideal. Dann gibt es den surjektiven Ringhomomorphismus $R \twoheadrightarrow R/\mathfrak{p}$, $a \mapsto \bar{a}$, wobei $R/\mathfrak{p}$ ein Integritätsbereich ist. Dieser induziert die Reduktion

$$R[X] \longrightarrow\!\!\!\!\!\rightarrow R/\mathfrak{p}[X], \qquad f = \sum_{i=1}^{n} a_i X^i \longmapsto \bar{f} = \sum_{i=1}^{n} \bar{a}_i X^i.$$

thm:reduction

**Satz 2.5.2.** *Seien $R$ ein faktorieller Ring und $\mathfrak{p} \subset R$ ein Primideal. Sei $f = a_n X^n + \cdots + a_0 \in R[X]$ mit $a_n \notin \mathfrak{p}$, wobei $\bar{f} \in R/\mathfrak{p}[X]$ irreduzibel sei. Dann gelten folgende Aussagen:*

itm:reduction:1

(i) *Falls $\deg(f) > 0$, so ist $f \in Q(R)[X]$ irreduzibel.*[33]

itm:reduction:2

(ii) *Falls $f \in R[X]$ primitiv ist, so ist $f \in R[X]$ irreduzibel.*

*Beweis.* Tatsächlich sind beide Aussagen äquivalent.

- (i) $\Longrightarrow$ (ii): Sei $f$ primitiv. Dann ist $\deg(f) > 0$; andernfalls wäre $f = c(f) \in R^*$ und daher $\bar{f} \in (R/\mathfrak{p})^*$, was der Irreduzibilität von $\bar{f}$ widerspricht.

  Falls $f = gh$ in $R[X]$, dann folgt aus (i), dass $g$ oder $h$ eine Einheit in $Q(R)[X]$ ist, d. h. in $Q(R)[X]^* = Q(R)$ liegen. Mit anderen Worten, $g$ oder $h$ liegen in $R \cap Q(R) = R$. Da $f$ primitiv ist, folgt $g \in R^*$ oder $h \in R^*$. Insbesondere ist $g \in R[X]^*$ oder $h \in R[X]^*$, d. h. $f \in R[X]$ ist irreduzibel.

- (ii) $\Longrightarrow$ (i): Sei $\deg(f) > 0$. Für $f$ primitiv folgt (i) aus Korollar 2.4.8 (ii).

  Allgemeiner können wir $f = c(f) f_0$ mit $f_0 \in R[X]$ primitiv schreiben. Dann gilt $\bar{f} = \overline{c(f)} \bar{f}_0$ mit $\overline{c(f)} \in R/\mathfrak{p}$ und $\bar{f}_0 \in R/\mathfrak{p}[X]$. Wegen der Irreduzibilität von $\bar{f}$ und $\deg(\bar{f}_0) > 0$ muss $\bar{f}_0 \in R/\mathfrak{p}[X]$ irreduzibel sein. Wenden wir den obigen Fall auf das primitive Element $f_0$ an, so ist $f_0 \in Q(R)[X]$ irreduzibel. Weil $c(f) \in R \subset Q(R)$ eine Einheit ist, ist auch $f \in Q(R)[X]$ irreduzibel.

Wir beweisen nun (ii): Seien $f$ primitiv und $f = gh$ in $R[X]$ mit $g, h \notin R[X]^*$. Aus der Primitivität von $f$ folgt $g, h \notin R$, d. h. $\deg(g), \deg(h) > 0$. Schreibe also $g = \sum_{i=0}^{k} b_i X^i$ und $h = \sum_{i=0}^{l} c_i X^i$, wobei $b_k, c_l \neq 0$. Durch Ausmultiplizieren erhalten $a_n = b_k c_l$. Wegen $a_n \notin \mathfrak{p}$ gilt $0 \neq \bar{a}_n = \overline{b_k c_l} = \bar{b}_k \bar{c}_l$ und daher $\bar{b}_k, \bar{c}_l \neq 0$ in $R/\mathfrak{p}$. Folglich ist $\deg(\bar{g}), \deg(\bar{h}) > 0$ und insbesondere $\bar{g}, \bar{h} \notin R[X]^*$. Das widerspricht der Irreduzibilität von $\bar{f} \in R/\mathfrak{p}[X]$. □

*Beispiel* 2.5.3. Betrachte $R = \mathbb{Z}$ und $\mathfrak{p} = (p)$ für eine Primzahl $p \in \mathbb{Z}$. Dann ist $R/\mathfrak{p} = \mathbb{Z}/(p) = \mathbb{F}_p$.

[33] In der Vorlesung fehlte die Bedingung $\deg(f) > 0$; ohne diese ist die Aussage falsch. *Gegenbeispiel:* Betrachte $R = \mathbb{Z}[Y]$, $\mathfrak{p} = (Y)$ und $f = 2 \in \mathbb{Z}[Y]$. Dann ist $2 \notin (Y)$ und $\bar{2} \in \mathbb{Z}[Y]/(Y) \simeq \mathbb{Z}$ ist irreduzibel. Aber $2 \in Q(R) = \mathbb{Z}(Y)$ ist nicht irreduzibel, da es eine Einheit ist. Konsequenterweise habe ich den Beweis gefixt.

(i) $f = \Phi_3(X) = X^2 + X + 1$ ist normiert und damit automatisch primitiv. Probieren wir $p = 2$. Der Leitkoeffizient ist $1 \notin \mathfrak{p}$. Nach Reduktion ist $\bar{f} = X^2 + X + 1 \in \mathbb{F}_2[X]$ irreduzibel, da $\bar{f}$ keine Nullstelle in $\mathbb{F}_2 = \{\bar{0}, \bar{1}\}$ besitzt. Somit ist $f$ in $\mathbb{Z}[X]$ und $\mathbb{Q}[X]$ irreduzibel aufgrund Satz 2.5.2.

*Frage:* Wir haben $p = 2$ betrachtet. Was passiert mit $p = 3$?

Nach Reduktion ist $\bar{f} = X^2 + X + 1 \in \mathbb{F}_3[X]$. Wir wissen, dass $\bar{f}$ genau dann irreduzibel ist, wenn $\bar{f}$ keine Nullstelle in $\mathbb{F}_3 = \{\bar{0}, \bar{1}, \bar{2}\}$ hat. $\bar{f}$ hat aber $\bar{1}$ als Nullstelle, weshalb wir Satz 2.5.2 nicht anwenden können. Es ist also eine Kunst, eine richtige Primzahl $p$ zu finden.

(ii) Betrachte $f = X^4 + 6X^3 + 7X^2 - 5X + 4 \in \mathbb{Z}[X]$. Da $f$ normiert ist, ist es primitiv.

Für $p = 2$ gilt

$$\bar{f} = X^4 + X^2 + X = X(X^3 + X + 1) \in \mathbb{F}_2[X],$$

was nicht irreduzibel ist. Also können wir Satz 2.5.2 nicht anwenden.

Für $p = 3$ gilt $\bar{f} = X^4 + X^2 + X + 1 \in \mathbb{F}_3[X]$. Da das ein Polynom vierten Grads ist, ist es nicht so klar, ob das irreduzibel ist.

(a) Wir prüfen, dass $\bar{f}$ keine Nullstelle in $\mathbb{F}_3$ hat. Es gelten

$$\bar{f}(0) = \bar{1} \neq 0, \qquad \bar{f}(1) = \bar{4} \neq 0, \qquad \bar{f}(2) = \bar{f}(-1) = 1 + 1 - 1 + 1 \neq 0.$$

(b) Falls $\bar{f} \in \mathbb{F}_3[X]$ nicht irreduzibel ist, so gibt es $g, h \in \mathbb{F}_3[X]$ mit $\deg(g), \deg(h) > 0$, sodass $\bar{f} = gh$. Da $\bar{f}$ keine Nullstellen hat, dürfen $g$ und $h$ nicht linear sein. Also gilt $\deg(g) = \deg(h) = 2$. Ferner dürfen auch $g$ und $h$ keine Nullstellen haben, weshalb $g$ und $h$ irreduzible Polynome in $\mathbb{F}_3[X]$ von Grad 2 sind. Diese irreduziblen Polynome sind genau

$$g, h \in \{F_1 := X^2 + 1, F_2 := X^2 + X - 1, F_3 := X^2 - X - 1\}.$$

Wir finden sie durch Probieren: Liste alle neun möglichen Polynome auf und prüfe, dass sie keine Nullstellen haben. Zuletzt rechnen wir nach, dass $\bar{f} \neq F_i F_j$ für alle $i$ and $j$.

Somit ist $\bar{f}$ irreduzibel und nach Satz 2.5.2 ist $f \in \mathbb{Z}[X]$ irreduzibel.

*Problem* 2.5.4. Zurück zur Frage, wann $\Phi_p$ irreduzibel ist. $\Phi_p$ ist ein normiertes Polynom und damit primitiv. Ferner ist $1 \notin \mathfrak{p} = (p')$ für jede beliebige Primzahl $p' \in \mathbb{Z}$. Wie können wir aber nachweisen, dass $\bar{\Phi}_p \in \mathbb{F}_{p'}[X]$ für eine Primzahl $p'$ irreduzibel ist?

thm:eisenstein

**Satz 2.5.5 (Eisensteinkriterium).** *Sei $R$ ein faktorieller Ring. Sei $f \in R[X]$ primitiv mit $\deg(f) > 0$, und sei $p \in R$ ein Primelement. Schreibe $f = a_n X^n + a_{n-1} X^{n-1} + \cdots + a_0$. Angenommen $p \mid a_{n-1}$, $p \mid a_{n-2}$, usw., $p \mid a_0$, aber $p^2 \nmid a_0$. (Es gilt $p \nmid a_n$, da $f$ primitiv ist). Dann ist $f$ als Element von $R[X]$ (oder auch von $Q(R)[X]$) irreduzibel.*

*Beweis.* Wegen $\deg(f) > 0$ ist $f \notin R[X]^*$. Angenommen $f = gh$ mit $g, h \notin R[X]^* = R^*$. Da $f$ primitiv ist, sind $g, h \notin R$, d. h. $\deg(g), \deg(h) > 0$. Schreibe $f = \sum_{i=0}^{n} a_i X^i$, $g = \sum_{i=0}^{k} b_i X^i$ und $h = \sum_{i=0}^{l} c_i X^i$ mit $n = \deg(f)$, $k = \deg(g)$, $l = \deg(h)$ und $a_n, b_k, c_l \neq 0$. Dann gilt

$a_0 = b_0c_0$. Da $p \mid a_0$ muss $p \mid b_0$ oder $p \mid c_0$; o. B. d. A. sei $p \mid b_0$. Wegen $p^2 \nmid a_0$ folgt $p \nmid c_0$. Ferner ist $a_n = b_kc_l$. Da $f$ primitiv ist, gilt $p \nmid a_n$, weshalb $p \nmid b_k$ und $p \nmid c_l$. Also können wir $i$ minimal wählen, sodass $p \mid b_0$, usw., $p \mid b_{i-1}$, aber $p \nmid b_i$. Betrachte $a_i = b_ic_0 + b_{i-1}c_1 + \cdots + b_0c_i$. Nach Wahl von $i$ ist $p \nmid b_ic_0$, aber $p \mid b_{i-1}c_1 + \cdots + b_0c_i$. Also ist $p \nmid a_i$, was der Voraussetzung widerspricht, falls $i < n$. Wir wissen, dass $i \leq k = \deg(g) < \deg(f) = n$, da $\deg(h) > 0$. Also haben wir tatsächlich einen Widerspruch und $f$ ist in $R[X]$ irreduzibel. Die Irreduzibilität in $Q(R)[X]$ folgt aus Korollar 2.4.8 (ii). □

Gotthold Eisenstein (1823-1852), gebürtiger Berliner, stammte aus ärmlichen Verhältnissen. In jungen Jahren fing er an, sich für Mathematik zu interessieren und wurde von seinem Gymnasiallehrer gefördert. Als sein Vater für höhere Berufschancen nach England übersiedelte, traf Eisenstein auf Hamilton, wo er mit der Arbeit von Abel in Berührung kam. Später studierte er an der Universität Berlin und erhielt mithilfe von Alexander von Humboldt großzügige finanzielle Zuwendungen. Gauss, der sonst mit Lob nur sparsam umgeht, bezeichnete Eisensteins Begabung in einem Brief an Humboldt als eine, welche „die Natur in jedem Jahrhundert nur Wenigen erteilt“.

Eisenstein war zu Lebzeiten unglaublich produktiv (allein in 1844 schrieb er insgesamt 25 Arbeiten). Die meisten Arbeiten veröffentlichte er im Journal von Leopold Crelle. Eine seiner Arbeit bestand aus nur einer Seite: Damals war bekannt, dass jede natürliche Zahl eine Summe von fünf Quadraten ist. Eisenstein schrieb (ohne Beweis) auf diese eine Seite eine Formel, auf *wie viele Arten* man eine Zahl so schreiben kann. In der Hinsicht ist er sehr ähnlich zum indischen Genie Ramanujan (von dem es einen guten Film gibt).

*Beispiel* 2.5.6. Einige Anwendungen.

(i) Sei $X^n - p \in \mathbb{Z}[X]$ mit $n > 0$. Nach dem Eisensteinkriterium 2.5.5 ist $X^n - p$ in $\mathbb{Z}[X]$ und $\mathbb{Q}[X]$ irreduzibel.

(ii) Sei $f = X^n + Y^n - 1 \in \mathbb{Z}[X, Y]$, die sog. *Fermatgleichung*. Setzen wir $R \coloneqq \mathbb{Z}[Y]$, so gilt $\mathbb{Z}[X, Y] = \mathbb{Z}[Y][X] = R[X]$. Wir erhalten

$$f = X^n + (Y - 1)(Y^{n-1} + \cdots + 1).$$

Da $p = Y - 1 \in R = \mathbb{Z}[Y]$ ein Primelement ist und $Y - 1 \nmid Y^{n-1} + \cdots + 1$, denn 1 ist keine Nullstelle von $Y^{n-1} + \cdots + 1$, gilt $p^2 \nmid Y^n - 1$. Somit folgt aus dem Eisensteinkriterium 2.5.5, dass $f$ irreduzibel in $\mathbb{Z}[X]$ (und in $\mathbb{Q}[X]$) ist.

(iii) Für Kreisteilungpolynome $\Phi_p(X) = X^{p-1} + \cdots + X + 1$ können wir das Eisensteinkriterium 2.5.5 nicht direkt anwenden. Wir können aber die Variablentransformation

$$\varphi \colon \mathbb{Z}[X] \xrightarrow{\sim} \mathbb{Z}[Y], \qquad X \longmapsto Y + 1$$

anwenden. Insbesondere gelten $\varphi(X-1) = Y$ und $\varphi(X^p-1) = (Y+1)^p-1$. Bezeichnen wir $F \coloneqq \varphi(\Phi_P)$, so ist $\Phi_p \in \mathbb{Z}[X]$ genau dann irreduzibel, wenn $F \in \mathbb{Z}[Y]$ irreduzibel ist (Isomorphismen erhalten Irreduzibilität).

Wir wissen, dass

$$(X - 1)\Phi_p = (X - 1)(X^{p-1} + \cdots + 1) = X^p - 1.$$

Wenden wir $\varphi$ an, so folgt

$$\begin{aligned} YF = (Y+1)^p - 1 &= \sum_{i=0}^{p} \binom{p}{i} Y^i - 1 = Y^p + pY^{p-1} + \binom{p}{2} Y^{p-2} + \cdots + pY \\ &= Y\left(Y^{p-1} + pY^{p-2} + \binom{p}{2} Y^{p-3} + \cdots + p\right) \\ \implies F &= Y^{p-1} + pY^{p-2} + \binom{p}{2} Y^{p-3} + \cdots + p. \end{aligned}$$

Weil $F$ normiert ist, ist $F$ primitiv. Ferner sind alle Koeffizienten von $F$ außer dem Leitkoeffizienten durch $p$ teilbar und der konstante Koeffizient ist nicht durch $p^2$ teilbar. Somit folgt aus dem Eisensteinkriterium 2.5.5, dass $F \in \mathbb{Z}[Y]$ irreduzibel ist. Also ist $\Phi_p$ irreduzibel.

(iv) Betrachte

$$f = 2X^7 - 15X^6 + 60X^4 - 18X^4 - 9X^3 + 45X^2 - 3X + 5 \in \mathbb{Z}[X],$$

was nicht normiert, aber dennoch primitiv ist. Mit $p = 3$ erfüllt es alle Voraussetzungen des Eisensteinkriteriums 2.5.5, weshalb $f \in \mathbb{Z}[X]$ irreduzibel ist.

*Eisensteinpolynome*, d. h. Polynome, die das Eisensteinkriterium erfüllen, spielen eine herausragende Rolle in der Zahlentheorie.[34]

Es gibt einen direkteren Beweis für folgenden einfacheren Sachverhalt.

**Satz 2.5.7.** *Seien $R = \mathbb{Z}$ und $f = X^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0 \in \mathbb{Z}[X]$. Für eine Primzahl $p \in \mathbb{Z}$ gelte $p \mid a_{n-1}, \ldots, p \mid a_1, p \mid a_0$, aber $p^2 \nmid a_0$. Dann ist $f$ irreduzibel. Das lässt sich leicht auf beliebige Hauptidealringe $R$ verallgemeinern.*

*Beweis.* Betrachte

$$\mathbb{Z}[X] \twoheadrightarrow \mathbb{Z}/(p)[X] = \mathbb{F}_p[X], \qquad f \longmapsto \bar{f} = X^n.$$

Angenommen $f = gh$ mit $g, h \notin \mathbb{Z}[X]^*$. Wegen der Eindeutigkeit der Primfaktorzerlegung von $\bar{f} = \bar{g}\bar{h}$ in $\mathbb{F}_p[X]$ sind $\bar{g} = X^k$ und $\bar{h} = X^l$ mit $k, l > 0$. Alle Koeffizienten von $g$ und $h$ sind also bis auf Leitkoeffizienten durch $p$ teilbar. Schreibe $g = \sum_{i=0}^{k} b_i X^i$ und $h = \sum_{i=0}^{l} c_i X^i$ mit $p \mid b_i$ und $p \mid c_i$ sowie $b_k = c_l = 1$. Insbesondere gelten $p \mid b_0$ und $p \mid c_0$, also $p^2 \mid b_0c_0 = a_0$, ein Widerspruch. □

## 2.6 Notizen*

**Bemerkung 2.6.1.** Der Quotient von Ringen ist nicht wohldefiniert, wenn wir durch einen Unterring statt einem Ideal teilen. Sei $S \subset R$ ein Unterring. Dann ist $R/S$ als abelsche Gruppe wohldefiniert, aber die Multiplikation nicht. Angenommen $\bar{a} = \bar{a}'$. Dann

[34] Eisensteinpolynome klassifizieren total verzweigte Körpererweiterungen über lokale Körper der Charakteristik null.

folgt $\overline{ab} = \bar{a}\bar{b} = \bar{a}'\bar{b} = \overline{a'b}$, also $(a - a')b \in S$. Es ist zwar $a - a' \in S$, aber nicht unbedingt $b \in S$, Widerspruch! Dieses Problem lösen Ideale.

Weitere wichtige Aussagen, die in der Vorlesung nicht behandelt wurden.

**Proposition 2.6.2.** *Seien $R$ ein Ring und $\mathfrak{a} \subset R$ ein Ideal. Sei $\pi\colon R \twoheadrightarrow R/\mathfrak{a}$ die kanonische Projektion. Dann gibt es eine Bijektion*

$$\{\textit{Ideale in } R, \textit{ die } \mathfrak{a} \textit{ enthalten}\} \xrightarrow{\sim} \{\textit{Ideale in } R/\mathfrak{a}\},$$
$$\mathfrak{b} \longmapsto \mathfrak{b}/\mathfrak{a} = \pi(\mathfrak{b}), \qquad \pi^{-1}(\bar{\mathfrak{b}}) \longmapsfrom \bar{\mathfrak{b}}.$$

*Beweis.* Man überprüft leicht, dass $\mathfrak{b}/\mathfrak{a}$ ein Ideal in $R/\mathfrak{a}$ ist. Auch $\pi^{-1}(\bar{\mathfrak{b}})$ ist ein Ideal: Für alle $a, b \in \pi^{-1}(\bar{\mathfrak{b}})$ gilt $\bar{a}, \bar{b} \in \bar{\mathfrak{b}}$ und damit $\bar{a} + \bar{b} = \overline{a+b} \in \bar{\mathfrak{b}}$, also $a + b \in \pi^{-1}(\bar{\mathfrak{b}})$. Für alle $r \in R$ gilt $\bar{r}\bar{a} = \overline{ra} \in \bar{\mathfrak{b}}$, also $ra \in \pi^{-1}(\bar{\mathfrak{b}})$.

Weil $\pi$ surjektiv ist, gilt mengentheoretisch stets $\pi(\pi^{-1}(\bar{\mathfrak{b}})) = \bar{\mathfrak{b}}$. Ferner gilt mengentheoretisch stets $\mathfrak{b} \subseteq \pi^{-1}(\pi(\mathfrak{b})) = \pi^{-1}(\mathfrak{b}/\mathfrak{a})$. Umgekehrt gilt für alle $\bar{b} \in \mathfrak{b}/\mathfrak{a}$ nämlich $\pi^{-1}(\bar{b}) = \{a + b \mid a \in \mathfrak{a}\}$. Wegen $\mathfrak{a} \subseteq \mathfrak{b}$ folgt $\pi^{-1}(\bar{b}) \subseteq \mathfrak{b}$. □

*Beispiel* 2.6.3. Das ist besonders hilfreich in folgenden Situationen. Wir wollen zeigen, dass $2 \in \mathbb{Z}[\mathrm{i}]$ nicht prim ist. Angenommen $2 \in \mathbb{Z}[\mathrm{i}]$ ist prim. Dann ist $(2) \subset \mathbb{Z}[\mathrm{i}]$ ein Primideal. Wir wissen $\mathbb{Z}[\mathrm{i}] \simeq \mathbb{Z}[X]/(X^2 + 1)$, d. h. $(2)$ entspricht dem Ideal

$$(2, X^2 + 1)/(X^2 + 1) \subseteq \mathbb{Z}[X]/(X^2 + 1).$$

Nach dem zweiten Isomorphiesatz für Ringe ist

$$\begin{aligned}\mathbb{Z}[\mathrm{i}]/(2) &\simeq (\mathbb{Z}[X]/(X^2+1))/((2, X^2+1)/(X^2+1)) \\ &\simeq \mathbb{Z}[X]/(2, X^2+1) \\ &\simeq (\mathbb{Z}[X]/(2))/((2, X^2+1)/(2)) \\ &= \mathbb{F}_2[X]/(X^2+1)\end{aligned}$$

ein Integritätsbereich. Es gilt aber $(\overline{X+1})^2 = \overline{X^2+1} = 0$ in $\mathbb{F}_2[X]/(X^2+1)$ mit $\overline{X+1} \neq 0$, ein Widerspruch.

**Definition 2.6.4.** Eine **Halbordnung** $\leq$ auf $M$ ist eine Relation, die folgende Eigenschaften hat:

(i) **Reflexivität**: $x \leq x$ für alle $x \in M$,

(ii) **Antisymmetrie**: $x \leq y$ und $y \leq x$ impliziert $x = y$,

(iii) **Transitivität**: $x \leq y$ und $y \leq z$ impliziert $x \leq z$.

Eine **Kette** in $M$ ist eine Teilmenge $K \subseteq M$, sodass $x \leq y$ oder $y \leq x$ für alle $x, y \in S$ (d. h. man kann alles vergleichen). Eine **obere Schranke** einer Kette $K$ ist ein Element $s \in M$, sodass $x \leq s$ für alle $x \in K$.

lem:zorn

**Lemma 2.6.5 (Lemma von Zorn).** *Sei $M$ eine Menge mit einer Halbordnung $\leq$. Falls jede Kette in $M$ eine obere Schranke besitzt, so besitzt $M$ ein maximales Element, d. h. ein $m \in M$ mit $x \leq m$ für alle $x \in M$, falls $x \leq m$ definiert ist.*

**Bemerkung 2.6.6.** Da auch $K = \varnothing$ eine Kette in $M$ ist, impliziert die Voraussetzung insbesondere, dass $M \neq \varnothing$.

**Bemerkung 2.6.7.** Das Lemma von Zorn 2.6.5 sollte aus der linearen Algebra bekannt sein (Beweis der Existenz unendlicher Basen). Ferner ist diese Aussage äquivalent zum Auswahlaxiom, welche alle weitreichenden Konsequenzen nach sich zieht.

Damit beweisen wir folgende wichtige Aussage aus der kommutativen Algebra.

thm:krull

**Satz 2.6.8.** *Jeder Ring $R \neq 0$ besitzt ein maximales Ideal. Oder noch stärker: Sei $\mathfrak{a} \subsetneq R$ ein echtes Ideal. Dann gibt es ein Maximalideal $\mathfrak{m} \subset R$ mit $\mathfrak{a} \subseteq \mathfrak{m}$.*

*Beweis.* Betrachte die Menge $M \coloneqq \{\text{Ideale } \mathfrak{b} \subsetneq R\}$, die mit der Inklusion von Mengen eine halbgeordnete Menge definiert.

Sei $K \subseteq M$ eine Kette.[35] Dann ist $\mathfrak{c} \coloneqq \bigcup_{\mathfrak{b} \in K} \mathfrak{b}$ wieder ein Ideal: Für $a, b \in \mathfrak{c}$ gibt es Ideale $\mathfrak{b}_a, \mathfrak{b}_b \in K$ mit $a \in \mathfrak{b}_a$ und $b \in \mathfrak{b}_b$. Weil $K$ eine Kette ist, gilt o. B. d. A. $\mathfrak{b}_a \subset \mathfrak{b}_b$. Somit gilt $a + b \in \mathfrak{b}_b \subset \mathfrak{c}$. Für $a \in \mathfrak{c}$ und $r \in R$ gilt $ra \in \mathfrak{b}_a \subset \mathfrak{c}$. Ferner ist $\mathfrak{c} \neq R$ da kein $\mathfrak{b} \in K$ eine Einheit enthält. Folglich ist $\mathfrak{c} \in M$ eine obere Schranke von $K$.

Nach dem Lemma von Zorn 2.6.5 existiert ein maximales Element $\mathfrak{m} \in M$, was damit auch ein Maximalideal von $R$ ist. Für die allgemeinere Aussage funktioniert der Beweis analog. Wähle hierzu $M \coloneqq \{\text{Ideale } \mathfrak{b} \subsetneq R \mid \mathfrak{a} \subset \mathfrak{b}\}$. □

# 3 Körpererweiterungen

## 3.1 Definition

**Definition 3.1.1.** Sei $K$ ein Körper. Dann besteht eine **Körpererweiterung** von $K$ aus einem Körper $L$ und einer Inklusion $K \subset L$, die mit der Körperstruktur verträglich ist. Hierbei heißen $K$ **Unterkörper** und $L$ **Erweiterungskörper**. Wir schreiben $L/K$.[36]

**Bemerkung 3.1.2.**

(i) Für eine Körpererweiterung $K \subset L$ gilt $1_K = 1_L$ und $0_K = 0_L$.

(ii) Falls $K$ ein Körper und $\varphi\colon K \to R$ ein Ringhomomorphismus ist, so ist $\varphi$ injektiv (Aufgabe 19). Damit entsprechen Körpererweiterungen Ringhomomorphismen zwischen Körpern.

*Beispiel* 3.1.3. Körpererweiterungen sind $\mathbb{C}/\mathbb{R}$, $\mathbb{R}/\mathbb{Q}$, $\mathbb{C}/\mathbb{Q}$, $\mathbb{Q}(\mathrm{i})/\mathbb{Q}$, $\mathbb{Q}(\sqrt{-5})/\mathbb{Q}$.

[35] Yang meinte hier, dass abzählbare Ketten ausreichen. Da bin ich mir nicht so sicher, da das Lemma von Zorn 2.6.5 nur mit abzählbaren Ketten im Allgemeinen falsch ist.

[36] Das hat überhaupt nichts mit Quotienten zu tun! Ist leider historisch gewachsen.

VL 12
20.11.23

**Notation 3.1.4.** Seien $L/K$ eine Körpererweiterung und $A \subset L$ eine Teilmenge. Definieren $K(A)$ als den kleinsten Unterkörper von $L$, der $K$ und alle Elemente von $A$ enthält. Genauer,

$$K(A) \coloneqq \bigcap_{\substack{K \subset K' \subset L \\ A \subset K'}} K',$$

wobei $K'$ alle Körper, sodass $K'/K$ und $L/K'$ Körpererweiterungen sind. Man überprüft leicht, dass $K \subset K(A) \subset L$ und $K(A)$ wieder ein Körper ist. Wir bezeichnen $K(A)$ mit $K$ **adjungiert** $A$.

Analog definieren wir $K[A] \subset L$ als den kleinsten Unterring von $L$, der $K$ und alle Elemente von $A$ enthält, d. h.

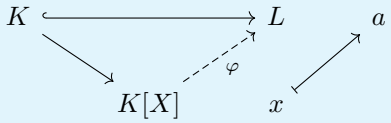
$$K[A] \coloneqq \bigcap_{\substack{K \subset R \subset L \\ A \subset R}} R$$

wobei $R$ alles Unterringe von $L$ sind. Dann gilt $K \subset K[A] \subset K(A) \subset L$ und alle Inklusionen respektieren Addition und Multiplikation.

*Spezialfall:* Falls $A = \{a\}$ für ein gewisses $a \in L$, so schreiben wir $K(a) \coloneqq K(\{a\})$ sowie $K[a] \coloneqq K[\{a\}]$.

**Beobachtung 3.1.5.** Sei $L/K$ eine Körpererweiterung. Wir können einfache Körpererweiterungen $K(a)/K$ mit $a \in L$ explizit beschreiben.

Im Allgemeinen gibt es genau einen Ringhomomorphismus $\varphi$, sodass folgendes Diagramm kommutiert:




Dann ist $K[a] = \mathrm{Im}(\varphi)$ ein Unterring mit $K \subset \mathrm{Im}(\varphi) \subset L$. Wir erhalten

$$K[a] = \mathrm{Im}(\varphi) = \left\{ \sum_{i=0}^{n} a_i a^i \;\middle|\; a_i \in K \right\}.$$

Mit dem Homomorphiesatz erhalten wir

$$K[a] \simeq \mathrm{Im}(\varphi) \simeq K[x]/\operatorname{Ker}(\varphi).$$

Da $L$ ein Körper ist und damit $\mathrm{Im}(\varphi)$ ein Integritätsbereich, muss $\operatorname{Ker}(\varphi) \subset K[X]$ ein Primideal sein. Da $K[X]$ ein Hauptidealring ist, gibt es ein irreduzibles Polynom $f \in K[X]$, sodass $\operatorname{Ker}(\varphi) = (f)$.

Analog erhalten wir

$$K(a) = \left\{ \frac{\sum_{i=1}^{n} a_i a^i}{\sum_{j=1}^{m} b_j a^j} \;\middle|\; a_i, b_j \in K, \sum_{j=1}^{m} b_j a^j \neq 0 \text{ in } L \right\} \subset L.$$

*Beispiel* 3.1.6. Betrachte die Körpererweiterung $\mathbb{Q} \subset \mathbb{C}$. Für $a = \pi, \sqrt{2}, \sqrt{-5}, \mathrm{e}, \dots \subset \mathbb{C}$ sind $\mathbb{Q} \subset \mathbb{Q}(a)$ und $\mathbb{Q}(a) \subset \mathbb{C}$ Körpererweiterungen.

## 3.2 Quadratische Polynome

*Problem* 3.2.1. Warum interessieren wir uns für Körpererweiterungen? Eine Antwort ist, um Nullstellen von Polynomen zu produzieren.

Wir wollen nun die Lösbarkeit quadratischer Polynome verstehen.

obs:quadratic

**Beobachtung 3.2.2.** Sei $K$ ein Körper mit $\mathrm{char}(K) \neq 2$ und sei $f = X^2 + a_1 X + a_0 \in K[X]$ ein normiertes quadratisches Polynom. Wir schreiben der Einfachheit halber $f = X^2 + pX + q$.

Die **Tschirnhausreduktion** ist der Ringisomorphismus

$$\varphi\colon K[X] \xrightarrow{\sim} K[Y], \quad X \longmapsto Y - \frac{p}{2}, \qquad \text{d. h.} \qquad \sum_{i=0}^{n} a_i X^i \longmapsto \sum_{i=0}^{n} a_i \Big(Y - \frac{p}{2}\Big)^i.$$

Hier haben wir verwendet, dass $2 \coloneqq 1_K + 1_K \neq 0$ in $K$. Insbesondere folgt

$$\varphi(f) = \Big(Y - \frac{p}{2}\Big)^2 + p\Big(Y - \frac{p}{2}\Big) + q = Y^2 + \frac{p^2}{4} - \frac{p^2}{2} + q = Y^2 + \left(q - \frac{p^2}{4}\right) =: g(Y).$$

Beobachte, dass kein linearer Term vorkommt. Ferner induziert $\varphi$ auch eine Bijektion zwischen den Nullstellenmengen von $f$ und $g$:

$$\left\{\alpha \in K \;\middle|\; \alpha = -\frac{p}{2} \pm \sqrt{\frac{p^2}{4} - q}\right\} \longleftrightarrow \left\{\beta \in K \;\middle|\; \beta^2 = \frac{p^2}{4} - q\right\}$$
$$\alpha \longmapsto \alpha + \frac{p}{2},$$

wobei

$$\beta \coloneqq \pm\sqrt{\frac{p^2}{4} - q}.$$

Damit haben wir die Lösbarkeit von $f$ in $K$ auf die Lösbarkeit von $g$ in $K$ reduziert.

*Fazit:* Die Nullstellen von $f$ existieren in $K$ und sind explizit beschreibbar, falls

(i) $\mathrm{char}(K) \neq 2$ und

(ii) es gibt $\sqrt{p^2/4 - q} \in K$, d. h. es gibt ein $\beta \in K$, sodass $\beta^2 = p^2/4 - q$.

Falls die obigen Punkte erfüllt sind, so hat $f$ zwei Nullstellen

$$x_\pm = -\frac{p}{2} \pm \beta.$$

Für diese gelten $x_+ + x_- = -p$ und $x_+ x_- = q$, denn

$$f = X^2 + pX + q = (X - x_+)(X - x_-) = X^2 - (x_+ + x_-)X + x_+ x_-.$$

**Definition 3.2.3.** Für quadratische Polynome $f = X^2 + pX + q \in K[X]$ sei die **Diskriminante** von $f$ definiert als

$$D(f) \coloneqq (x_+ - x_-)^2 = p^2 - 4q.$$

fact:discriminant

itm:discriminant:1

**Fakt 3.2.4.** *Angenommen* $\mathrm{char}(K) \neq 2$. *Dann gelten folgende Aussagen:*

(i) *$f$ besitzt genau dann eine Nullstelle in $K$, falls $\sqrt{D(f)} \in K$ existiert.*

(ii) *Angenommen $\sqrt{D(f)} \in K$. Dann gilt $x_+ = x_-$ genau dann, wenn $D(f) = 0$.*

(iii) *Selbst wenn $f$ keine Nullstelle in $K$ besitzt, so existieren $x_+ + x_-, x_+x_- \in K$.*

**Beobachtung 3.2.5.** Für $K = \mathbb{R}$ existiert $\sqrt{D(f)} \in \mathbb{R}$ genau dann, wenn $D(f) \geq 0$. Wir unterscheiden drei Fälle.

(i) $D(f) > 0$ genau dann, wenn $f$ zwei verschiedene Nullstellen in $\mathbb{R}$ hat.

(ii) $D(f) = 0$ genau dann, wenn $f$ genau eine Nullstelle in $\mathbb{R}$.

(iii) $D(f) < 0$ genau dann, wenn $f$ keine Nullstelle in $\mathbb{R}$ hat.

Was ist aber mit Charakteristik 2?

**Beobachtung 3.2.6** (*Artin-Schreier-Theorie*)**.** Sei $K$ ein Körper mit $\mathrm{char}(K) = 2$. Betrachte wieder $f = X^2 + pX + q \in K[X]$.

(i) Angenommen $p = 0$. Es gilt $D(f) = p^2 - 4q = 0 - 0$, da $\mathrm{char}(K) = 2$. Würden wir Fakt 3.2.4 (i) glauben, so würde $f$ immer eine Nullstelle in $K$ besitzen. Das ist aber im Allgemeinen falsch. Tatsächlich hat $f$ genau dann eine Nullstelle in $K$, wenn es $\sqrt{q} \in K$ gibt.

(ii) Angenommen $p = 1$. Dann ist $f = X^2 + X + q = X^2 - X + q$, da $\mathrm{char}(K) = 2$.

*Behauptung:* Wenn $r(q) \in K$ eine Nullstelle von $f$ ist, dann ist auch $r(q) + 1$ eine Nullstelle.

*Beweis:* Wir rechnen

$$(r(q) + 1)^2 + (r(q) + 1) + q = (r(q)^2 + r(q) + 1) + (2r(q) + 1 + 1) = 0 + 0.$$

Also sind $\{r(q), r(q)+1\}$ die Nullstellen von $f$ und $f$ hat zwei verschiedene Nullstellen.

(iii) Angenommen $p \neq 0$.

*Behauptung:* $f$ hat genau dann eine Nullstelle in $K$, wenn $r(q/p^2) \in K$, d. h. das Polynom $X^2 + X + q/p^2$ hat eine Nullstelle in $K$.

*Beweis:* Falls $\alpha$ eine Nullstelle von $f$ ist, so gilt $\alpha^2 + p\alpha + q = 0$. Division durch $p^2$ liefert

$$\left(\frac{\alpha}{p}\right)^2 + \frac{\alpha}{p} + \frac{q}{p^2} = 0.$$

Setze $r(q/p^2) \coloneqq \frac{\alpha}{p}$. Die Umkehrung ist klar.

*Beispiel* 3.2.7. Wir untersuchen die Nullstellen von $X^2+X+q$ über verschiedenen Körpern $K$ mit $\mathrm{char}(K)=2$.

(i) Für $K=\mathbb{F}_2=\mathbb{Z}/2\mathbb{Z}=\{0,1\}$ gilt $q=0$ oder $q=1$. Falls $q=0$, so hat $X^2+X\in\mathbb{F}_2[X]$ genau zwei Nullstellen 0 und 1. Falls $q=1$, so hat $X^2+X+1\in\mathbb{F}_2[X]$ keine Nullstellen in $\mathbb{F}_2$.

(ii) Für $K=\mathbb{F}_4=\{0,1,\alpha,\alpha+1\}$, wobei $\alpha$ eine Variable ist, gilt $\mathrm{char}(K)=2$. Dann erfüllt $\alpha$ die Relation $\alpha^2=\alpha+1$, d. h. wir haben $K\simeq\mathbb{F}_2[X]/(X^2-(X+1))$. Der Grund ist, dass $X^2-(X+1)=X^2+X+1$ irreduzibel ist, da $X^2+X+1$ keine Nullstellen in $\mathbb{F}_2$ hat. Also ist $(X^2+X+1)$ ein Maximalideal in $\mathbb{F}_2[X]$ und $\mathbb{F}_2[X]/(X^2+X+1)$ ist ein Körper mit Charakteristik 2. Es gilt auch $|\mathbb{F}_2[X]/(X^2+X+1)|=4$. Setze $\alpha:=\bar{X}$.

Es ist klar, dass $\mathbb{F}_2\hookrightarrow\mathbb{F}_4$ eine Körpererweiterung ist. Damit haben wir eine Körpererweiterung von $\mathbb{F}_2$ gefunden, sodass $f=X^2+X+1\in\mathbb{F}_4[X]$ Nullstellen hat, nämlich die zwei verschiedenen Lösungen $\alpha$ und $\alpha+1$, d. h. $r(1)\in\mathbb{F}_4$ existiert.

*Frage:* Hat $X^2+r(1)X+1\in\mathbb{F}_4[X]$ eine Nullstelle in $\mathbb{F}_4$? Das ist genau dann der Fall, wenn $r(r(1)^{-2})\in\mathbb{F}_4$, d. h. wenn $X^2+X+r(1)^{-2}\in\mathbb{F}_4[X]$ eine Nullstelle in $\mathbb{F}_4$ hat.

*Antwort:* Dieses Polynom hat tatsächlich keine Nullstellen in $\mathbb{F}_4$. Wegen $r(1)=\alpha$ können wir von $X^2+X+\alpha^{-2}\in\mathbb{F}_4[X]$ alle Nullstellen durchprobieren. Mit $\alpha^2=\alpha+1$ gelten

$$0^2+0+\frac{1}{\alpha^2}\neq 0,\quad 1^2+1+\frac{1}{\alpha^2}\neq 0,\quad \alpha^2+\alpha+\frac{1}{\alpha^2}\neq 0,\quad (\alpha+1)^2+(\alpha+1)+\frac{1}{\alpha^2}\neq 0.$$

(iii) Um für dieses Polynom Nullstellen zu finden, brauchen wir immer größere Körper. Das ergibt den Turm von Körpererweiterungen $\mathbb{F}_2\subset\mathbb{F}_4\subset\mathbb{F}_8\subset\mathbb{F}_{16}\subset\cdots$.

## 3.3 Primkörper

. Wiederholung Sei $K$ ein Körper. Dann ist die *Charakteristik* von $K$

$$\mathrm{char}(K)=\begin{cases}0, & \text{falls } n:=n\cdot 1_K\neq 0 \text{ für alle } n\in\mathbb{N}_{>0},\\ p, & \text{falls } p:=\min\{n\in\mathbb{N}_{>0}\mid n\cdot 1_K=0\}.\end{cases}$$

$\mathrm{char}(K)$ ist dann entweder 0 oder eine Primzahl.

**Definition 3.3.1.** Sei $K$ ein Körper. Dann ist der **Primkörper** $K_0$ von $K$ der kleinste Unterkörper von $K$, d. h.

$$K_0:=\bigcap_{K'\subset K}K',$$

wobei $K'\subset K$ Unterkörper sind. $K_0$ ist ein Unterkörper von $K$.

**Satz 3.3.2.** *Sei $K$ ein Körper. Für seinen Primkörper gilt dann*

$$K_0\simeq\begin{cases}\mathbb{Q}, & \textit{falls } \mathrm{char}(K)=0,\\ \mathbb{F}_p, & \textit{falls } \mathrm{char}(K)=p.\end{cases}$$

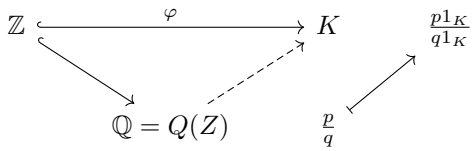
*Beweis.* Betrachte den Ringhomomorphismus

$$\varphi\colon \mathbb{Z} \longrightarrow K, \qquad n \longmapsto n \cdot 1_K.$$

Dann ist $\mathrm{Im}(\varphi) \subset K$ ein Unterring von $K$ und damit ein Integritätsbereich. Folglich ist $\mathrm{Ker}(\varphi) \subset \mathbb{Z}$ ein Primideal. Genauer ist

$$\mathrm{Ker}(\varphi) = \begin{cases} (0), & \text{falls } \mathrm{char}(K) = 0, \\ (p), & \text{falls } \mathrm{char}(K) = p \text{ Primzahl.} \end{cases}$$

Falls $\mathrm{char}(K) = 0$, so gibt es (genau) einen Ringhomomorphismus, sodass folgendes Diagramm kommutiert:




Dabei ist stets $q1_K \neq 0$, da $\mathrm{char}(K) = 0$. Somit ist $\mathbb{Q} \subset K$ ein Unterkörper. Also muss $\mathbb{Z} \subset K_0 \subset \mathbb{Q}$ sein, wobei $\mathbb{Z} \hookrightarrow K_0$ durch $\frac{p}{q} \mapsto p1_{K_0}/(q1_{K_0})$ gegeben ist. Weil $\mathbb{Q} = Q(\mathbb{Z})$ und $K_0$ ein Körper ist, muss $K_0 = \mathbb{Q}$ (der Quotientenkörper ist der kleinste Körper, der einen Ring enthält).

Falls $\mathrm{char}(K) = p$, dann ist $\mathbb{F}_p \simeq \mathbb{Z}/(p) \simeq \mathrm{Im}(\varphi) \subset K$ ein Unterkörper. Also ist $K_0 \subset \mathrm{Im}(\varphi)$. Insbesondere ist $1_{K_0} \in \mathrm{Im}(\varphi)$. Da $1_{K_0}$ durch Addition $\mathrm{Im}(\varphi)$ erzeugt, erhalten wir $\mathrm{Im}(\varphi) \subset K_0$. Somit gilt $K_0 = \mathrm{Im}(\varphi) \simeq \mathbb{F}_p$. □

## 3.4 Einheitengruppe

*Problem* 3.4.1. Sei $K$ ein Körper und setze $K^* \coloneqq K \setminus \{0\}$. Das ist bzgl. Multiplikation eine abelsche Gruppe. Wie sieht diese aus?

. Erinnerung Wir wissen aus Satz 1.4.1, dass falls $K^*$ endlich erzeugt ist, dann

$$K^* \simeq \mathbb{Z}^{\oplus n} \oplus \bigoplus_{i=1}^{N} \mathbb{Z}/p_i^{n_i}.$$

Insbesondere ist $K^*$ eine direkte Summe von zyklischen Untergruppen.

thm:unitgroup

**Satz 3.4.2.** *Seien $K$ ein Körper und $H \subset K^*$ eine endliche Untergruppe. Dann ist $H$ eine zyklische Gruppe.*

*Beweis.*

itm:unitgroup:1

(i) *Fakt:* Sei $H$ eine beliebige abelsche Gruppe. Seien $a, b \in H$ sowie $n \coloneqq |a|$ und $m \coloneqq |b|$; sei $k = \mathrm{kgV}(m, n)$. Dann existiert ein $c \in H$ mit $|c| = k$, nämlich $c = ab$.

(ii) Sei $H \subset K^*$ eine endliche Untergruppe. Sei $n \coloneqq \max\{|b| \mid b \in H\}$ und sei $a \in H$ mit $|a| = n$. Betrachte

$$H_n \coloneqq \{b \mid |b| \text{ teilt } n\} \subset H.$$

Dann ist $\langle a\rangle \subset H_n$ eine Untergruppe der Ordnung $n$. Ferner wissen wir, dass $b^n = 1$ für alle $b \in H_n$, denn $|b|$ teilt $n$ und $b^{|b|} = 1$. Daher sind alle Elemente in $H_n$ Nullstellen des Polynoms $X^n - 1 \in K[X]$. Weil $X^n - 1$ ein Polynom von Grad $n$ ist, hat es maximal $n$ Nullstellen. Somit ist $|H_n| \leq n$, und wegen $\langle a\rangle \subset H_n$ folgt $|H_n| = \langle a\rangle$.

(iii) Angenommen es gibt ein $b \in H \setminus \langle a\rangle = H \setminus H_n$. Nach Definition von $H_n$ ist $\langle b\rangle \nmid n$, d. h. $\mathrm{kgV}(\langle b\rangle, n) > n$. Dann impliziert (i), dass es ein $c \in H$ mit $|c| = \mathrm{kgV}(|b|, n)$ gibt, was aber der Maximalität von $n$ widerspricht. Somit ist $H = H_n = \langle a\rangle$ zyklisch. □

*Alternativer Beweis.* Sei $H \subset K^*$ eine endliche Untergruppe der Ordnung $n$. Betrachte

$$f\colon \mathbb{N} \longrightarrow \mathbb{N}, \qquad f(m) = |\{a \in H \mid |a| = m\}|.$$

Für jedes $a \in H$ ist $|a|$ ein Teiler von $|H|$, weshalb

$$n = \sum_{m|n} f(m)$$

gilt. Betrachte andererseits die **eulersche $\varphi$-Funktion**

$$\varphi(m) \coloneqq |\{d \in \mathbb{N} \mid d \leq m, \mathrm{ggT}(d, m) = 1\}|.$$

*Behauptung:* Wenn $f(m) \neq 0$, dann $f(m) = \varphi(m)$.

*Beweis:* Wenn $f(m) \neq 0$, so gibt es ein $a \in H$ mit $|a| = m$. Bemerke, dass $\langle a\rangle$ mit $|\langle a\rangle| = m$ genau die Nullstellen des Polynoms $X^m - 1$ in $K$ sein müssen. Nun gilt $|a^d| = m$ genau dann, wenn $\mathrm{ggT}(d, m) = 1$. Daher ist die Anzahl der Elemente in $\langle a\rangle$ der Ordnung $m$ genau $\varphi(m)$. Bemerke weiterhin, dass alle Elemente in $H$ der Ordnung $m$ Nullstellen von $X^m - 1$ sind. Folglich ist die Anzahl der Elemente in $\langle a\rangle$ der Ordnung $m$ auch $f(m)$, weshalb $f(m) = \varphi(m)$. Das beweist die Behauptung.

*Behauptung:* Es gilt

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

*Beweis:* Definiere

$$A_n(d) \coloneqq \{k \in \{1, \dots, n\} \mid \mathrm{ggT}(k, n) = d\}.$$

Dann gilt $\{1, \dots, n\} = \bigsqcup_{d|n} A_n(d)$, also $n = \sum_{d|n} |A_n(d)|$. Des Weiteren haben wir die Bijektion $A_n(d) \xrightarrow{\sim} A_{n/d}(1)$, $k \mapsto \frac{k}{d}$. Mit $|A_n(1)| = \varphi(n)$ folgt $\sum_{d|n} |A_n(d)| = \sum_{d|n} \varphi(d)$. Das beweist die Behauptung.

Nach der ersten Behauptung erhalten wir $f(m) \leq \varphi(m)$ für alle $m \mid n$. Hingegen impliziert die zweite Behauptung $\sum_{m|n} f(m) = \sum_{m|n} \varphi(m)$, weshalb $f(m) = \varphi(m)$ für alle $m \mid n$ gelten muss. Insbesondere ist $f(n) = \varphi(n) \neq 0$, d. h. es gibt ein $a \in H$ mit $|a| = n = |H|$ und $H$ ist zyklisch. □

## 3.5 Endliche Körpererweiterungen

VL 13
24.11.23

**Definition 3.5.1.** Eine Körpererweiterung $L/K$ heißt **endlich erzeugt**, falls eine endliche Teilmenge $A \subset L$ existiert, sodass $L = K(A)$. Konkret bedeutet das: Es gibt endlich viele $a_1, \dots, a_n \in L$, sodass jedes $a \in L$ von der Form $a = \frac{f}{g}$ mit endlichen Summen $f = \sum_i \alpha_i a_1^{i_1} \cdots a_n^{i_n}$ und $g = \sum_j \beta_j a_1^{j_1} \cdots a_n^{j_n}$, wobei $i, j \in \mathbb{N}^n$ Tupel sind und $\alpha_i, \beta_j \in K$.

Endliche erzeugte Objekte kommen in der Algebra oft vor, da viele Ausdrücke endlich sind (endliche Produkte, endliche Summen, etc.).

rationalpolynomial

*Beispiel* 3.5.2. Der Körper $L = Q(K[X]) =: K(X)$ der rationalen Funktionen in einer Variablem mit Koeffizienten in $K$, d. h. $L = \{\sum_{i=0}^n a_i X^i / \sum_{i=0}^m b_i X^i\}$, ist endlich erzeugt.

**Beobachtung 3.5.3.** Wenn $L/K$ eine Körpererweiterung ist, dann ist $L$ auf natürlicher Weise ein $K$-Vektorraum. Daher können wir von $\dim_K(L)$ reden. Wir schreiben

$$[L : K] \coloneqq \dim_K(L)$$

und nennen es den **Grad** der Körpererweiterung.

**Definition 3.5.4.** Eine Körpererweiterung heißt **endlich**, falls $[L : K] < \infty$. Sonst ist sie **unendlich**.

**Fakt 3.5.5.** *Sei $L$ ein endlicher Körper. Dann existiert eine Primzahl $p$ und ein $n \in \mathbb{Z}_{>0}$, sodass $|L| = p^n$.*

*Beweis.* Wir wissen, dass der Primkörper von $L$ isomorph zu $\mathbb{F}_p$ für ein gewisses $p$ ist, denn notwendigerweise $\mathrm{char}(L) > 0$. Damit ist $L/\mathbb{F}_p$ eine Körpererweiterung. Wegen $|L| < \infty$ gilt $n \coloneqq [L : \mathbb{F}_p] < \infty$. Mittels linearer Algebra folgt also $L \simeq \mathbb{F}_p^{\oplus n}$ als $\mathbb{F}_p$-Vektorraum. Wir schließen $|L| = p^n$. □

*Beispiel* 3.5.6.

(i) $\mathbb{C}/\mathbb{R}$ ist endlich vom Grad $[\mathbb{C} : \mathbb{R}] = 2$, da $\mathbb{C} \simeq \mathbb{R} \oplus \mathrm{i}\mathbb{R}$.

(ii) $\mathbb{C}/\mathbb{Q}$ ist weder eine endliche Erweiterung noch endlich erzeugt. Der Grund ist, dass $\mathbb{Q}$ abzählbar, aber $\mathbb{C}$ überabzählbar ist.

(iii) $K(X)/K$ ist endlich erzeugt (Beispiel 3.5.2), aber nicht endlich. Es gilt nämlich $K \subset K[X] \subset K(X)$, wobei $K[X]$ ein unendlichdimensionaler Vektorraum mit Basis $X^i$ für $i = 0, 1, \dots$ ist. Es folgt $[K(X) : K] = \infty$.

**Bemerkung 3.5.7.** Wenn $L/K$ endlich ist, dann ist es auch endlich erzeugt. Denn es gibt $a_1, \dots, a_n \in L$ die ein Erzeugendensystem (oder sogar eine Basis) von $L$ als $K$-Vektorraum bilden. Somit gibt es für jedes $a \in L$ die Darstellung $a = \alpha_1 a_1 + \cdots + \alpha_n a_n$ mit $\alpha_i \in K$. Schließlich ist $L = K(\{a_1, \dots, a_n\})$ endlich erzeugt.

thm:tower

**Satz 3.5.8 (Produktformel).** *Seien $K \subset L$ und $L \subset L'$ Körpererweiterungen (ein sog. **Turm** von Körpererweiterungen $K \subset L \subset L'$ oder $L'/L/K$). Dann gilt*

$$[L' : K] = [L' : L] \cdot [L : K].$$

*Beweis.* Wir brauchen einige Beobachtungen.

itm:tower:1 (i) Falls eine Teilmenge $\{y_i\} \subset L$ linear unabhängig über $K$ ist, so ist sie auch linear unabhängig als Elemente des $K$-Vektorraums $L'$ (per Definition).

itm:tower:2 (ii) Falls eine Teilmenge $\{x_i\} \subset L'$ linear unabhängig über $L$ ist, so ist sie auch linear unabhängig über $K$ (denn $K \subset L$).

Wir führen eine Fallunterscheidung durch.

(i) Angenommen $[L : K] = \infty$. Dann existieren unendlich viele Elemente $y_i \in L$, die über $K$ linear unabhängig sind. Nach (i) sind diese auch linear unabhängig im $K$-Vektorraum $L'$, d. h. $[L' : K] = \infty$. Damit steht $\infty$ auf beiden Seiten der behaupteten Gleichung.

(ii) Angenommen $[L : L'] = \infty$. Dann existieren unendlich viele Elemente $x_i \in L'$, die linear unabhängig über $L$ sind. Nach (ii) sind diese auch linear unabhängig in $L'$ als $K$-Vektorraum, d. h. $[L' : K] = \infty$. Damit steht $\infty$ auf beiden Seiten der behaupteten Gleichung.

(iii) Angenommen $[L' : L] < \infty$ und $[L : K] < \infty$. Wähle eine Basis $y_1, \dots, y_n$ von $L'$ als $L$-Vektorraum und eine Basis $x_1, \dots, x_m$ von $L$ als $K$-Vektorraum.

*Behauptung:* $x_j y_i \in L'$ für $i = 1, \dots, n$, $j = 1, \dots, m$ bilden eine Basis von $L'$ als $K$-Vektorraum. Dann folgt bereits $[L' : K] = mn = [L' : L][L : K]$.

*Beweis:* Wir zeigen zunächst, dass das ein Erzeugendensystem ist. Sei $a \in L'$. Dann ist $a = \sum_{i=1}^{n} a_i y_i$ mit $a_i \in L$, und für jedes $a_i$ gilt $a_i = \sum_{j=1}^{m} b_{ij} x_j$ mit gewissen $b_{ij} \in K$. Nach Einsetzen erhalten wir $a = \sum_{i,j} b_{ij}(x_j y_i)$, d. h. $(x_j y_i)$ bildet ein Erzeugendensystem.

Nun zeigen wir, dass das Erzeugendensystem linear unabhängig ist. Angenommen es gilt $\sum_{i,j} b_{ij}(x_j y_i) = \sum_{i=1}^{n}(\sum_{j=1}^{m} b_{ij} x_j) y_i = 0$ mit $b_{ij} \in K$. Aufgrund der linearen Unabhängigkeit der $y_i$ folgt $\sum_{j=1}^{m} b_{ij} x_j = 0$ für alle $i$. Aufgrund der linearen Unabhängigkeit der $x_j$ folgt $b_{ij} = 0$ für alle $i, j$. Somit sind die $x_j y_i$ linear unabhängig. □

*Beispiel* 3.5.9. Einige Anwendungen.

(i) Sei $\mathbb{C}/L/\mathbb{R}$ ein Turm von Körpererweiterungen, d. h. $\mathbb{R} \subset L \subset \mathbb{C}$. Dann gilt $L = \mathbb{C}$ oder $L = \mathbb{R}$.

*Beweis:* Nach der Produktformel 3.5.8 gilt $2 = [\mathbb{C} : \mathbb{R}] = [\mathbb{C} : L][L : \mathbb{R}]$. Damit ist $[\mathbb{C} : L] = 1$ oder $[L : \mathbb{R}] = 1$ und daher $\mathbb{C} = L$ bzw. $L = \mathbb{R}$.

(ii) Das lässt sich verallgemeinern. Seien $L'/L/K$ ein Turm von Körpererweiterungen und $[L' : K]$ eine Primzahl. Dann gilt $L' = L$ oder $L = K$.

In der Galoistheorie werden wir später alle Zwischenerweiterungen einer gegeben Körpererweiterung (die bestimmte Bedingungen erfüllen muss) bis auf Isomorphie klassifizieren.

## 3.6 Algebraische Körpererweiterungen

**Definition 3.6.1.** Sei $L/K$ eine Körpererweiterung. Dann heißt ein Element $a \in L$ **algebraisch** (über $K$), falls ein Polynom $0 \neq p \in K[X]$ existiert, sodas $p(a) = 0$ in $L$. Konkret bedeutet das, dass ein $p = \sum_{i=0}^{n} a_i X^i \neq 0$ mit $a_i \in K$ gibt, sodass $\sum_{i=1}^{n} a_i a^i = 0$ in $L$. Andernfalls heißt $a$ **transzendent**.

**Definition 3.6.2.** Eine Zahl $z \in \mathbb{C}$ heißt **algebraisch**, falls $z$ über $\mathbb{Q}$ algebraisch ist. (Hier betrachten wir $\mathbb{C}/\mathbb{Q}$). Andernfalls heißt $z$ **transzendent**.

*Beispiel* 3.6.3. $\sqrt{2} \in \mathbb{C}$ ist algebraisch: Nehme $p = X^2 - 2$ mit $p(\sqrt{2}) = 0$. Hingegen sind $\mathrm{e}, \pi \in \mathbb{C}$ transzendent (zuerst von Hermite bzw. Lindemann;[37] die Beweise hiervon sind nicht so einfach und verwenden Analysis.)

**Notation 3.6.4.** Schreibe $\bar{\mathbb{Q}} \coloneqq \{\text{algebraische } z \in \mathbb{C}\}$. Wir werden sehen, dass $\bar{\mathbb{Q}}/\mathbb{Q}$ eine Körpererweiterung ist, d. h. $\bar{\mathbb{Q}} \subset \mathbb{C}$ ist ein Unterkörper. Dieser ist nicht endlich erzeugt.

Viele Themen der modernen Algebra handeln von $\bar{\mathbb{Q}}/\mathbb{Q}$ und dessen Struktur, die sehr kompliziert ist.

Ein noch offenes Problem ist, ob e und $\pi$ linear unabhängig über $\mathbb{Q}$ sind, d. h. ob es $a, b \in \mathbb{Q}$ mit $a\mathrm{e} + b\pi = 0$ gibt. Oder, ob es ein Polynom in zwei Variablen gibt, sodass $(\mathrm{e}, \pi)$ eine Nullstelle ist. Die Vermutung besagt, dass das nur passiert, wenn es einen „guten Grund“ dafür gibt.

**Bemerkung 3.6.5.** Wenn $L/K$ eine Körpererweiterung ist, dann sind alle $a \in K$ algebraisch über $K$, da sie Nullstellen des Polynoms $p = X - a \in K[X]$ sind.

**Definition 3.6.6.** Eine Körpererweiterung $L/K$ heißt **algebraisch**, falls alle Elemente in $L$ algebraisch über $K$ sind.

*Beispiel* 3.6.7.

(i) $L = K/K$ ist algebraisch.

(ii) $\mathbb{C}/\mathbb{R}$ ist algebraisch.

*Beweis:* Z. B. ist i eine Nullstelle von $X^2+1 \in \mathbb{R}[X]$. Für allgemeine $a+b\mathrm{i} \in \mathbb{C}$ können wir leicht nachrechnen, dass $z = a + b\mathrm{i}$ eine Nullstelle von $p = X^2 - 2aX + (a^2 + b^2) \in \mathbb{R}[X]$ ist. Also ist $\mathbb{C}$ algebraisch über $\mathbb{R}$.

*Anmerkung:* Es genügt tatsächlich, nur Polynome $p$ vom Grad 2 für die algebraische Abhängigkeit zu betrachten. Im Allgemeinen gibt es aber auch Körpererweiterungen, bei der man den Grad des Polynoms $p$ nicht beschränken kann (z. B. in $\bar{\mathbb{Q}}/\mathbb{Q}$ gibt es irreduzible Polynome über $\mathbb{Q}$ beliebigen Grades).

[37] Ich glaube der Dozent hat Lindelöf geschrieben.

lem:simple

**Lemma 3.6.8.** *Seien $L/K$ eine Körpererweiterung und $a \in L$. Dann ist $a$ genau dann algebraisch über $K$, wenn $\dim_K K[a] < \infty$ (wir erinnern uns, dass $K[a] \subset L$ ein Unterring und ein $K$-Vektorraum ist).*

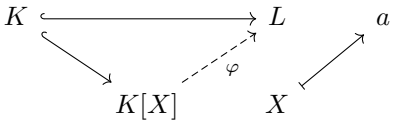
*Beweis.* Nach Definition ist $K[a] = \{\sum_{i=0}^{n} a_i a^i \mid a_i \in K\}$. Angenommen $a$ ist algebraisch. Dann gibt es ein Polynom $0 \neq p \in K[X]$ mit $p(a) = 0$. O. B. d. A. sei $p$ normiert, d. h. $p = X^n + a_{n-1}X^{n-1} + \cdots + a_0$. Folglich gilt $a^n \in \langle 1, a, a^2, \ldots, a^{n-1}\rangle_K$. Rekursiv gilt dann $a^m \in \langle 1, a, a^2, \ldots, a^{n-1}\rangle_K$ für alle $m \geq n$. Bspw. ist

$$a^{n+1} = a(a^n) = a\left(-\sum_{i=0}^{n-1} a_i a^i\right) = -\sum_{i=0}^{n-2} a_i a^{i+1} - a_{n-1}a^n = -\sum_{i=1}^{n-1} a_i a^{i+1} - a_{n-1}\left(-\sum_{i=0}^{n-1} a_i a^i\right)$$

ein Element in $\langle 1, a, \ldots, a^{n-1}\rangle_K$. Somit ist $K[a] \subset \langle 1, a, \ldots, a^{n-1}\rangle_K$, wobei die rechte Seite ein endlichdimensionaler Vektorraum ist. Daher ist $\dim_K K[a] < \infty$.

Umgekehrt sei $\dim_K K[a] < \infty$. Dann sind die unendlich vielen Elemente $a^0 = 1, a, a^2, \ldots$ linear abhängig. D. h. es existiert eine endliche Linearkombination $\sum_{i=0}^{n} a_i a^i = 0$ mit mindestens einem Koeffizienten $a_i \neq 0$. Sodann ist $p \coloneqq \sum_{i=0}^{n} a_i X^i$ ein Polynom mit $a$ als Nullstelle. □

. Erinnerung Seien $L/K$ eine Körpererweiterung und $a \in L$. Dann existiert ein Ringhomomorphismus, sodass folgendes Diagramm kommutiert.




Konkret ist

$$\varphi\colon K[X] \longrightarrow L, \qquad \sum_{i=0}^{n} a_i X^i \longmapsto \sum_{i=0}^{n} a_i a^i.$$

Da $L$ ein Körper ist, so ist $K[a] = \mathrm{Im}(\varphi) \subset L$ ein Integritätsbereich. Also ist $\mathrm{Ker}(\varphi) \subset K[X]$ ein Primideal. Da $K[X]$ ein ein Hauptidealring ist, ist $\mathrm{Ker}(\varphi) = (0)$ oder $\mathrm{Ker}(\varphi) = (p)$ für ein irreduzibles $p \in K[X]$.

**Bemerkung 3.6.9.**

(i) Falls $\mathrm{Ker}(\varphi) = (0)$, dann ist $\varphi\colon K[X] \simeq K[a] \subset L$. Wegen $\dim_K K[X] = \infty$ ist $\dim_K K[a] = \infty$. Also ist $a$ nicht algebraisch über $K$.

(ii) Falls $\mathrm{Ker}(\varphi) \neq (0)$, dann ist $\mathrm{Ker}(\varphi) = (p)$ für ein irreduzibles Polynom $p$. In diesem Fall ist $\mathrm{Ker}(\varphi)$ ein Maximalideal und $K[X]/\mathrm{Ker}(\varphi) \simeq K[a]$ ist ein Körper. Also gilt $K[a] = K(a)$.

*Folgerung:* $a$ ist genau dann algebraisch über $K$, wenn $\mathrm{Ker}(\varphi) \neq 0$ genau dann, wenn $K[a] = K(a)$.

**Definition 3.6.10.** Seien $L/K$ eine Körpererweiterung und $a \in L$ algebraisch über $K$. Dann ist das **Minimalpolynom** $p_a \in K[X]$ von $a$ genau das normierte Polynom mit $(p_a) = \operatorname{Ker}(\varphi\colon K[X] \twoheadrightarrow K[a])$.[38] Wir nennen $\deg(a) := \deg(p_a)$ auch den **Grad** des Elements $a$. Dann gilt[39]

$$\deg(a) = \deg(p_a) = \dim_K K[a] = \dim_K K(a) = [K(a) : K].$$

*Bemerkung:* $p_a$ ist eindeutig.

**Bemerkung 3.6.11.**

(i) Sei $f \in K[X]$ mit $f(a) = 0$ in $L$. Dann ist $p_a \mid f$, d. h. es gibt ein $g \in K[X]$ mit $f = p_a g$.

(ii) Seien $a \in L$ algebraisch über $K$ und $b \in K(a) = K[a]$. Dann ist auch $b$ algebraisch über $K$.

*Beweis:* Für $b \in K(a)$ gilt $K \subset K[b] \subset K(a)$, wobei $[K(a) : K] < \infty$. Dann ist $\dim_K K[b] < \infty$ und daher $b$ algebraisch über $K$.

*Frage:* Schreibe $b = \sum_{i=0}^{n} a_i a^i$. Wir wissen, dass es ein Polynom $p \neq 0$ mit $p(a) = 0$ gibt. Aber wie konstruiert man danach $q \in K[X]$ mit $q(b) = 0$? Das ist deutlich schwerer.

(iii) Sei $L'/L/K$ ein Turm von Körpererweiterungen. Sei $a \in L$ algebraisch über $K$. Ist $p_a \in K[X]$ das Minimalpolynom von $a \in L$ über $K$, so ist $a$, aufgefasst als Element von $L'$, algebraisch über $K$ und dieses Minimalpolynom stimmt mit $p_a$ überein.

**Lemma 3.6.12.** *Falls $L/K$ eine endliche Körpererweiterung ist, so ist sie auch algebraisch.*

*Beweis.* Für jedes $a \in L$ gilt $K \subset K[a] \subset L$ von $K$-Vektorräumen, wobei $\dim_K L < \infty$ nach Voraussetzung. Also ist $\dim_K K[a] < \infty$ und $a$ ist algebraisch über $K$. □

**Bemerkung 3.6.13.** Da $\deg(p_a) = [K(a) : K]$ und $[L : K] = [L : K(a)][K(a) : K] < \infty$ nach der Produktformel 3.5.8, folgt $\deg(p_a) \leq [L : K]$ für alle $a \in L$.

**Bemerkung 3.6.14.** Sei $L/K$ eine Körpererweiterung. Jedes $a \in L$ induziert eine $K$-lineare Abbildung $\varphi_a\colon L \to L$, $b \mapsto ab$. Wenn $\dim_K L = [L : K] < \infty$, so ist das Minimalpolynom $p_a$ von $a$ auch das Minimalpolynom von $\varphi_a$ (im Sinne der linearen Algebra).

VL 14
27.11.23

[38] Eine äquivalente Charakterisierung ist, dass $p_a$ das normierte Polynom in $\operatorname{Ker}(\varphi)$ von minimalem Grad ist.

[39] Die zweite Gleichheit folgt aus dem Homomorphiesatz. Konkret: $\dim_K K[a] = \dim_K K[X]/(p_a) = \deg(p_a)$ mit Basis $\bar{1}, \bar{X}, \bar{X}^2, \ldots, \bar{X}^{\deg(p_a)-1}$.

**Lemma 3.6.15.** *Eine Körpererweiterung $L/K$ ist genau dann endlich, wenn sie endlich erzeugt und algebraisch ist.*

*Beweis.* Angenommen $[L : K] < \infty$. Dann gibt es $a_1, \ldots, a_n \in L$, die ein Erzeugendensystem (oder sogar eine Basis) von $L/K$ bilden. Daher ist $L = K(a_1, \ldots, a_n)$ und somit ist $L/K$ endlich erzeugt. $L/K$ ist auch algebraisch, weil es endlich ist.

Sei umgekehrt $L/K$ endlich erzeugt und algebraisch, sagen wir $L = K(a_1, \ldots, a_n)$ für gewisse $a_1, \ldots, a_n$. Da $L/K$ algebraisch ist, sind alle $a_i$ algebraisch über $K$. Insbesondere ist $a_n$ algebraisch über $K(a_1, \ldots, a_{n-1})$, d. h.

$$[L = K(a_1, \ldots, a_n) : K(a_1, \ldots, a_{n-1})] < \infty$$

wegen Lemma 3.6.8. Nach der Produktformel 3.5.8 gilt

$$[L : K] = [L : K(a_1, \ldots, a_{n-1})] \cdot [K(a_1, \ldots, a_{n-1}) : K] < \infty,$$

da der zweite Faktor nach Induktionsvoraussetzung endlich ist. Der Induktionsanfang ist Lemma 3.6.8. □

**Fakt 3.6.16.** *Sei $L'/L/K$ ein Turm von Körpererweiterungen. Angenommen $L/K$ ist algebraisch und $a \in L'$ ist algebraisch über $L$. Dann ist auch $a$ algebraisch über $K$.*

*Beweis.* Weil $a \in L'$ algebraisch über $L$ ist, existiert ein Polynom $0 \neq f \in L[X]$, sodass $f(a) = 0$. Schreibe $f(X) = \sum_{i=0}^{n} a_i X^i$ mit $a_i \in L$. Da $L/K$ algebraisch ist, sind auch alle Koeffizienten $a_i$ algebraisch über $K$. Wir erhalten einen Turm von endlichen Körpererweiterungen

$$K \subset K(a_0) \subset K(a_0, a_1) \subset \cdots \subset K(a_0, \ldots, a_n),$$

weshalb $K(a_0, \ldots, a_n)/K$ nach Produktformel 3.5.8 endlich und insbesondere endlich ist. Ferner ist $f(X) \in K(a_0, \ldots, a_n)[X]$, d. h. $a$ ist algebraisch über $K(a_0, \ldots, a_n)$. Daher ist

$$[K(a_0, \ldots, a_n, a) : K(a_0, \ldots, a_n)] < \infty.$$

Nach Produktformel 3.5.8 gilt dann

$$\underbrace{[K(a_0, \ldots, a_n, a) : K(a_0, \ldots, a_n)]}_{<\infty} \cdot \underbrace{[K(a_0, \ldots, a_n) : K]}_{<\infty} = [K(a_0, \ldots, a_n, a) : K]$$
$$= [K(a) : K] \cdot \underbrace{[K(a_0, \ldots, a_n) : K(a)]}_{<\infty}.$$

Somit ist $[K(a) : K] < \infty$, d. h. $a$ ist algebraisch über $K$. □

**Korollar 3.6.17.** *Ist $L'/L/K$ ein Turm von Körpererweiterungen, sodass $L'/L$ und $L/K$ jeweils algebraisch sind, so ist auch $L'/K$ algebraisch.*[40]

[40] Die Umkehrung gilt trivialerweise auch.

**Satz 3.6.18** (**Kroneckerverfahren**). *Seien $K$ ein Körper und $f \in K[X]$ mit $\deg(f) > 0$. Dann existiert eine Körpererweiterung $L/K$, sodass $f$ als Polynom in $L[X]$ eine Nullstelle hat. Konkreter: Es gibt ein $a \in L$ mit $f(a) = 0$.*

*Beweis.* Betrachte die Primfaktorzerlegung $f = f_1 \cdots f_n$ mit $f_i$ irreduzibel. Falls eine Körpererweiterung $L/K$ existiert, sodass ein $a \in L$ eine Nullstelle von $f_1$ ist, so ist $a$ auch eine Nullstelle von $f$ und wir sind fertig.

O. B. d. A. sei also $f$ irreduzibel. Dann ist $(f) \subset K[X]$ ein Maximalideal und $L \coloneqq K[X]/(f)$ ein Körper, die mittels

$$K \xhookrightarrow{a \mapsto aX^0} K[X] \xrightarrow{\pi} K[X]/(f)$$

eine Körpererweiterung von $K$ ist (wegen $\deg(f) > 0$ ist die Komposition injektiv). Setze $a \coloneqq \pi(X) \in L$. Dann gilt $f(a) = \pi(f) = 0$,[41] d. h. $a$ ist eine Nullstelle von $f$. □

cor:kronecker

**Korollar 3.6.19.** *Jedes Polynom $f \in K[X]$ mit $\deg(f) = n > 0$ besitzt eine Körpererweiterung $L/K$, sodass $f$, aufgefasst als Polynom in $L[X]$, sich schreiben lässt als*

$$f = c \prod_{i=1}^{n} (X - \alpha_i)$$

*mit $c \in K$ und $\alpha_1, \ldots, \alpha_n \in L$.*

## 3.7 Algebraischer Abschluss und Zerfällungskörper

**Definition 3.7.1.** Ein Körper $K$ heißt **algebraisch abgeschlossen** falls jedes Polynom $f \in K[X]$ mit $\deg(f) > 0$ eine Nullstelle in $K$ besitzt. Anders ausgedrückt, jedes Polynom $f \in K[X]$ mit $\deg(f) > 0$ zerfällt in Linearfaktoren, d. h.

$$f = c \prod_{i=1}^{n} (X - \alpha_i)$$

mit $c, \alpha_1, \ldots, \alpha_n \in K$.

Kommen wir zu einer der historisch gesehen wichtigsten Aussage der Algebra. Für noch mehr geschichtliche Hintergründe sei [Tig, Kap. 9] nahe gelegt (was auch ein prima Weihnachtsgeschenk ist).

bib:tig

**Satz 3.7.2** (**Fundamentalsatz der Algebra**). *Der Körper der komplexen Zahlen $\mathbb{C}$ ist algebraisch abgeschlossen.*

*Beweis.*

itm:fundamental:1

(i) Der Beweis braucht etwas Analysis; wir brauchen folgenden Fakt. Sei $f \in \mathbb{R}[X]$ ein Polynom von ungeradem Grad. Nach dem *Zwischenwertsatz* besitzt $f$ eine Nullstelle.

[41] Wieder *abuse of notation*. Mit $f(a)$ meinen wir, dass wir $f$ als Polynom in $L[X]$ unter der Inklusion $K \hookrightarrow L$ auffassen.

itm:fundamental:2

(ii) Wir wollen zeigen, dass $\sqrt{\alpha} \in \mathbb{C}$ für alle $\alpha \in \mathbb{C}$, d. h. dass es eine Zahl $\beta \in \mathbb{C}$ gibt mit $\beta^2 = \alpha$. Dazu sei $\alpha = x + \mathrm{i}y$ mit $x, y \in \mathbb{R}$. Wir suchen $\beta = a + \mathrm{i}b$ mit $\alpha = \beta^2$, d. h. $a, b \in \mathbb{R}$ mit $a^2 - b^2 = x$ und $2ab = y$.

Falls $b \neq 0$, so folgt aus der zweiten Gleichung $a = \frac{y}{2b}$. Einsetzen in die erste Gleichung liefert

$$\left(\frac{y}{2}\right)^2 \frac{1}{b^2} - b^2 = x.$$

Substituieren wir $c \coloneqq b^2$, so gilt

$$c^2 - cx - \left(\frac{y}{2}\right)^2 = 0$$

mit Lösungen

$$c = -\frac{x}{2} + \sqrt{\left(\frac{x}{2}\right)^2 + \left(\frac{y}{2}\right)^2} \in \mathbb{R}.$$

$c$ existiert, weil der Radikand positiv ist. Ferner ist $c \geq 0$, weshalb $b = \sqrt{c} \in \mathbb{R}$ existiert. Letztendlich können wir

$$b \coloneqq \sqrt{-\frac{x}{2} + \sqrt{\left(\frac{x}{2}\right)^2 + \left(\frac{y}{2}\right)^2}}, \qquad a \coloneqq \frac{y}{2b}$$

setzen.

Für den Fall $b = 0$ gilt $y = 0$. Dann können wir $a \coloneqq \sqrt{x}$, falls $x \geq 0$, und $a \coloneqq \mathrm{i}\sqrt{-x}$, falls $x < 0$, setzen.

(iii) Jetzt geht es richtig los. Sei $f = \sum_{i=0}^{n} a_i X^i \in \mathbb{C}[X]$ mit $n = \deg(f) > 0$ und setze $F \coloneqq f\bar{f}$. Hierbei ist $\bar{f} \coloneqq \sum_{i=0}^{n} \bar{a}_i X^i \in \mathbb{C}[X]$ (allgemeiner ist

$$\overline{(-)} \colon \mathbb{C}[X] \longrightarrow \mathbb{C}[X], \qquad \sum_{i=0}^{n} b_i X^i \longmapsto \sum_{i=0}^{n} \bar{b}_i X^i$$

ein Ringhomomorphismus). Dann gilt

$$\bar{F} = \overline{f\bar{f}} = \bar{f}\bar{\bar{f}} = \bar{f}f = F,$$

d. h. $F \in \mathbb{R}[X]$.

Angenommen $a \in \mathbb{C}$ ist eine Nullstelle von $F$. Dann gilt $0 = F(a) = f(a)\bar{f}(a)$. In diesem Fall ist $f(a) = 0$ oder $\bar{f}(a) = 0$, d. h. $f(a) = 0$ oder $f(\bar{a}) = 0$. Damit ist $a$ oder $\bar{a}$ eine Nullstelle von $f$ und wir sind fertig.

*Problem:* Wir wollen gerne (i) auf $F$ anwenden. Jedoch ist $\deg(F) = 2\deg(f)$ gerade.

Von nun an sei $F \in \mathbb{R}[X]$ ein beliebiges Polynom mit $\deg(F) > 0$. Wir wollen zeigen, dass $F$ eine Nullstelle in $\mathbb{C}$ hat. Schreibe dafür $\deg(F) = 2^l m$ mit $2 \nmid m$. Nach Induktionsvoraussetzung können wir annehmen, dass jedes $G \in \mathbb{R}[X]$ vom Grad $2^{l'} m' > 0$ mit $l' < l$ eine Nullstelle in $\mathbb{C}$ besitzt. O. B. d. A. sei $F$ normiert.

Nach dem Kroneckerverfahren (Korollar 3.6.19) gibt es eine Körpererweiterung $L/\mathbb{C}$, sodass $F$ in $L[X]$ in Linearfaktoren zerfällt, d. h. $F = \prod_{i=1}^{\deg(F)}(X - \alpha_i)$ mit $\alpha_i \in L$. Für jede reelle Zahl $c \in \mathbb{R}$ können wir ein Polynom

$$G_c(X) \coloneqq \prod_{i<j}(X - y_{ij}(c)) \in L[X], \qquad \text{wobei} \quad y_{ij}(c) \coloneqq \alpha_i + \alpha_j + c(\alpha_i\alpha_j) \in L,$$

definieren.

*Behauptung:* $G_c(X) \in \mathbb{R}[X]$.

Wenn diese Behauptung stimmt, dann ist $G_c \in \mathbb{R}[X]$ vom Grad

$$\deg(G_c) = \frac{\deg(F)(\deg(F)-1)}{2} = \frac{2^l m(2^l m - 1)}{2} = 2^{l'} m'$$

mit $l' \coloneqq l - 1 < l$ und $2 \nmid m' \coloneqq (2^l m - 1)m$. Nach Induktionsannahme hat $G_c$ eine Nullstelle in $\mathbb{C}$. Wir wissen aber, dass die Nullstellen von $G_c$ in $L$ genau $y_{ij}(c) = \alpha_i + \alpha_j + c(\alpha_i\alpha_j)$ sind. Somit gibt es für jedes $c \in \mathbb{R}$ ein Paar $i < j$ mit $y_{ij}(c) \in \mathbb{C}$. Weil es nur endlich viele solche Paare gibt, finden wir verschiedene $c_1, c_2 \in \mathbb{R}$ mit $y_{ij}(c_1), y_{ij}(c_2) \in \mathbb{C}$. Damit gilt

$$y_{ij}(c_1) - y_{ij}(c_2) = (c_1 - c_2)(\alpha_i\alpha_j) \in \mathbb{C}.$$

Falls $\alpha_i = 0$ oder $\alpha_j = 0$, so hat $F$ die Nullstelle $0 \in \mathbb{C}$. Andernfalls $\alpha_i\alpha_j \neq 0$, d. h. $\alpha_i\alpha_j \in \mathbb{C}$. Dann folgt $\alpha_i + \alpha_j \in \mathbb{C}$, da $y_{ij}(c_1) \in \mathbb{C}$. Wir beobachten, dass $X^2 - (\alpha_i + \alpha_j)X + \alpha_i\alpha_j$ die Nullstellen $\alpha_i, \alpha_j \in L$ hat. Nach (ii) gilt aber $\alpha_i, \alpha_j \in \mathbb{C}$ (wenn wir uns die quadratische Lösungsformel hinschreiben, sind alle Ausdrücke in $\mathbb{C}$). Wir setzen den Beweis bald fort, brauchen aber folgenden Einschub. ♡

**Definition 3.7.3.** Die **elementarsymmetrischen Polynome** in $n$ Variablen $X_1, \dots, X_n$ sind

$$\begin{aligned} e_1(X_1, \dots, X_n) &= \sum_i X_i, \\ e_2(X_1, \dots, X_n) &= \sum_{i<j} X_i X_j, \\ &\vdots \\ e_k(X_1, \dots, X_n) &= \sum_{i_1<\dots<i_k} X_{i_1} \cdots X_{i_k}. \end{aligned}$$

*Beobachtung:* $e_k(X_{\sigma(1)}, \dots, X_{\sigma(n)}) = e_k(X_1, \dots, X_n)$ für alle $\sigma \in \mathfrak{S}_n$.

Allgemein heißen Polynome $g \in K[X_1, \dots, X_n]$ **symmetrisch**, falls

$$g(X_{\sigma(1)}, \dots, X_{\sigma(n)}) = g(X_1, \dots, X_n)$$

für alle $\sigma \in \mathfrak{S}_n$. Mit $K[X_1, \dots, X_n]^{\mathfrak{S}_n} \subset K[X_1, \dots, X_n]$ bezeichnen wir den **Ring der symmetrischen Polynome** (oder auch **$\mathfrak{S}_n$-invariante Polynome**).

symmetricpolynomial

**Satz 3.7.4 (Hauptsatz über symmetrische Polynome).**

$$K[X_1, \dots, X_n]^{\mathfrak{S}_n} = K[e_1, \dots, e_n] \simeq K[Y_1, \dots, Y_n].$$

Die obige Aussage beweisen wir nicht und verweisen stattdessen auf Aufgabe 41.

*Fortsetzung des Beweises.*

(v) *Beobachtung:* Für $\prod_{i=1}^{n}(T - X_i) \in K[X_1, \dots, X_n, T]$ gilt

$$\begin{aligned}\prod_{i=1}^{n}(T - X_i) &= T^n - \left(\sum_{i=1}^{n} X_i\right)T^{n-1} + \left(\sum_{i<j} X_iX_j\right)T^{n-2} - \cdots \\ &= \sum_{k=0}^{n}(-1)^k T^{n-k} e_k(X_1, \dots, X_n).\end{aligned}$$

Zurück zu $G_c$. Schreibe

$$G_c = \prod_{i<j}(X - y_{ij}(c)) = \sum_{l=0}^{N} \beta_l X^l.$$

Nach der obigen Beobachtung ist $\beta_l$ symmetrisch in $y_{ij}(c)$ und damit symmetrisch in den $\alpha_i$. Andererseits ist

$$F = \prod_{i=1}^{\deg(F)} (X - \alpha_i) = \sum_{i=1}^{\deg(F)} (-1)^k X^{n-k} e_k(\alpha_1, \dots, \alpha_n) \in \mathbb{R}[X],$$

d. h. $e_k(\alpha_1, \dots, \alpha_n) \in \mathbb{R}$. Aus dem Hauptsatz über symmetrische Polynome 3.7.4 folgt, dass $\beta_l$ Polynome in den $e_k(\alpha_1, \dots, \alpha_n)$ über $\mathbb{R}$ sein. Folglich ist $\beta_l \in \mathbb{R}$ und damit $G_c \in \mathbb{R}$. □

*Problem* 3.7.5. Als nächstes Ziel wollen wir den algebraischen Abschluss eines beliebigen Körpers konstruieren.

**Warnung 3.7.6.** Es gibt viele algebraisch abgeschlossene Körper; $\mathbb{C}$ ist nicht der einzige von $\mathbb{Q}$.

**Definition 3.7.7.** Sei $L/K$ eine Körpererweiterung. Dann heißt

$$L_0 \coloneqq \{a \in L \mid a \text{ algebraisch über } K\}$$

der **algebraische Abschluss von $K$ in $L$.**

**Lemma 3.7.8.** *Sei $L/K$ eine Körpererweiterung. Dann ist der algebraische Abschluss $L_0$ von $K$ in $L$ ein Körper.*

*Beweis.* Offenbar ist $K \subset L_0$, weshalb $0, 1 \in L_0$. Zu zeigen ist, dass $ab, a+b, a^{-1} \in L_0$ für alle $a, b \in L_0$ mit $a \neq 0$.

Da $b \in L_0$ algebraisch über $K$ ist, ist $b$ algebraisch über $K(a)$. Daher ist $K(a,b) = K(a)(b) = K(a)[b]$. Zudem ist $a$ algebraisch über $K$, d. h. $K(a) = K[a]$. Wir erhalten $K(a,b) = K[a,b]$. Nach der Produktformel 3.5.8 gilt

$$[K(a,b) : K] = [K(a,b) : K(a)][K(a) : K] < \infty,$$

weshalb $K(a,b)/K$ algebraisch ist. Es gilt aber $a+b, ab, a^{-1} \in K(a,b)$, d. h. diese Elemente sind algebraisch über $K$ und damit in $L_0$ enthalten. □

*Beispiel* 3.7.9. Mit $\mathbb{Q} \subset \bar{\mathbb{Q}} \subset \mathbb{C}$ bezeichnen wir den algebraischen Abschluss von $\mathbb{Q}$ in $\mathbb{C}$. Das ist wieder ein Körper, der Körper aller algebraischer Zahlen.

**Lemma 3.7.10.** *Seien $L/K$ eine Körpererweiterung, wobei $L$ algebraisch abgeschlossen ist, und $L_0$ der algebraische Abschluss von $K$ in $L$. Dann ist $L_0$ algebraisch abgeschlossen.*

*Beweis.* Sei $f \in L_0[X] \subset L[X]$ mit $\deg(f) > 0$. Da $L$ algebraisch abgeschlossen ist, gibt es ein $a \in L$ mit $f(a) = 0$. Schreibe $f = \sum_{i=0}^{n} a_i X^i$ mit $a_i \in L_0$ und betrachte die Körpererweiterungen

$$K \subset K(a_0, \ldots, a_n) \subset K(a_0, \ldots, a_n, a).$$

Die erste Körpererweiterung ist endlich, da sie endlich erzeugt und algebraisch ist. Die zweite ist endlich, da $a$ algebraisch über $K(a_0, \ldots, a_n)$ ist. Damit ist auch

$$K \subset K(a) \subset K(a_0, \ldots, a_n, a)$$

endlich. Nach Produktformel 3.5.8 ist $K \subset K(a)$ endlich, d. h. $a$ ist algebraisch über $K$ und $a \in L_0$. □

*Beispiel* 3.7.11. $\bar{\mathbb{Q}}$ ist ein algebraisch abgeschlossener Körper. (Wie wir gleich zeigen, ist es „der“ algebraische Abschluss von $\mathbb{Q}$, bis auf Isomorphie.)

**Definition 3.7.12.** Sei $K$ ein Körper. Dann ist *der* **algebraische Abschluss von** $K$ eine Körpererweiterung $\bar{K}/K$, sodass:

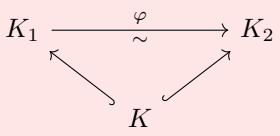
(i) $\bar{K}$ ist algebraisch abgeschlossen.

(ii) $\bar{K}/K$ ist eine algebraische Körpererweiterung.

Der folgende ist eines der Hauptsätze der Körpertheorie.

thm:extension

**Satz 3.7.13.** *Jeder Körper $K$ besitzt einen algebraischen Abschluss. Dieser ist eindeutig bis auf nicht-eindeutigen Isomorphismus. Genauer: Sind $K_1$ und $K_2$ zwei algebraische Abschlüsse von $K$ wie im Diagramm*



*so existiert ein Isomorphismus $\varphi\colon K_1 \xrightarrow{\sim} K_2$ mit $\varphi|_K = \mathrm{id}_K$. Aber $\varphi$ ist nicht eindeutig (nicht kanonisch).*

VL 15 01.12.23

*Beweis der Existenz*.* Die Existenz wurde übersprungen, da die verwendeten Techniken für die Körpertheorie unwichtig sind. Stattdessen verwies der Dozent auf das Übungsblatt, wo folgender Beweis vorzufinden war.

Sei $I \coloneqq \{f \in K[X] \mid \deg(f) \geq 1\}$ eine Indexmenge. Betrachte die Menge von Variablen $\mathcal{X} \coloneqq \{X_f\}_{f\in I}$ und den Polynomring $K[\mathcal{X}] = K[X_f \mid f \in I]$. Jedes $f \in I$ definiert eine Einbettung $K[X] \hookrightarrow K[\mathcal{X}]$, $g(X) \mapsto g(X_f)$. Sei $\mathfrak{a} \subset K[\mathcal{X}]$ das Ideal, welches durch $f(X_f)$ für alle $f \in I$ erzeugt wird (z. B. $f(X_f) = X_f^2 + 1$, falls $f = X^2 + 1$).

Wäre $\mathfrak{a} = (1)$, so gäbe es $f_1, \dots, f_n \in K[X]$ und $g_1, \dots, g_n \in K[\mathcal{X}]$ mit $\sum_{i=1}^n g_i f_i(X_{f_i}) = 1$. Nach dem Kronekerverfahren (Korollar 3.6.19) gibt es eine Körpererweiterung $L/K$, sodass $\alpha_1, \dots, \alpha_n \in L$ mit $f_i(\alpha_i) = 0$ existieren. Betrachte den Ringhomomorphismus

$$\varphi\colon K[\mathcal{X}] \longrightarrow L[\mathcal{X} \setminus \{X_{f_1}, \dots, X_{f_n}\}],$$

welcher durch $K \hookrightarrow L$, $X_{f_i} \mapsto \alpha_i$ und $X_f \mapsto X_f$ für alle $f \notin \{f_1, \dots, f_n\}$ gegeben ist. Dann gilt $\varphi(1) = \sum_{i=1}^n \varphi(g_i) f_i(\alpha_i) = 0$, Widerspruch. Also ist $\mathfrak{a} \neq K[\mathcal{X}]$ und nach Satz 2.6.8 existiert ein Maximalideal $\mathfrak{a} \subset \mathfrak{m} \subset K[\mathcal{X}]$. Betrachte die Körpererweiterung $K_1/K$ mit $K_1 \coloneqq K[\mathcal{X}]/\mathfrak{m}$.

*Behauptung:* $K_1/K$ ist algebraisch.

*Beweis:* Sei $\bar{X}_f$ das Bild von $X_f$ unter der Projektion $K[\mathcal{X}] \twoheadrightarrow K_1$. Per Definition ist $f(X_f) \in \mathfrak{a} \subset \mathfrak{m}$, d. h. $f(\bar{X}_f) = 0$ für alle Polynome $f \in K[X]$ mit $\deg(f) \geq 1$. Also hat jedes nichtkonstante Polynom eine Nullstelle in $K_1$; das beweist die Behauptung.

Wenden wir die Konstruktion rekursiv auf $K_1$ an, so erhalten wir $K \subset K_1 \subset K_2 \subset \cdots$. Setze

$$\bar{K} \coloneqq \bigcup_{i=1}^{\infty} K_i.$$

Nach der Behauptung sind alle $K_i/K_{i-1}$ algebraisch, weshalb per Induktion auch $K_i/K$ für alle $i$ algebraisch ist. Tatsächlich ist auch $\bar{K}/K$ algebraisch. Dazu sei $f \in \bar{K}[X]$ beliebig mit $\deg(f) \geq 1$. Da $f$ nur endlich viele Koeffizienten hat, gibt es ein $i$, sodass $f \in K_i$. Per Konstruktion besitzt aber $f$ eine Nullstelle in $K_{i+1} \subset \bar{K}$. □

Wir zeigen die Eindeutigkeit. Zuerst aber eine Vorbemerkung.

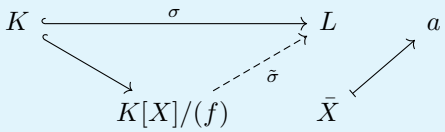
obs:extension

**Beobachtung 3.7.14.** Seien $K$ ein Körper und $f \in K[X]$ irreduzibel. Dann ist $K[X]/(f)$ eine Körpererweiterung von $K$. Sei $\bar{X}$ das Bild von $X$ unter $K[X] \twoheadrightarrow K[X]/(f)$. Dann ist $\bar{X}$ eine Nullstelle des Polynoms $f \in K[X]$. Wenn eine Körpererweiterung $L/K$ gegeben ist, sodass $f \in K[X]$ eine Nullstelle $a \in L$ besitzt, dann ist $K(a)$ als Zwischenkörper von $L/K$ isomorph zu $K[X]/(f) \xrightarrow{\sim} K(a)$, was durch $\bar{a} \mapsto a$ gegeben ist.

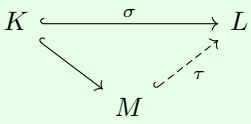
Etwas allgemeiner betrachten wir den Körperhomomorphismus $\sigma\colon K \hookrightarrow L$. Diese induziert die bekannte Abbildung

$$K[X] \longrightarrow L[X], \qquad g = \sum_{i=0}^{n} a_i X^i \longmapsto g^\sigma \coloneqq \sum_{i=0}^{n} \sigma(a_i) X^i \in \sigma(K)[X].$$

Falls für ein irreduzibles Polynom $f \in K[X]$ eine Nullstelle $a \in L$ von $f^\sigma \in L[X]$ existiert, dann können wir $\sigma\colon K \hookrightarrow L$ fortsetzen zu $\tilde{\sigma}\colon K[X]/(f) \simeq K(a) \to L$, sodass folgendes Diagramm kommutiert:



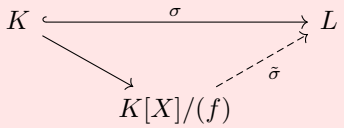

**Definition 3.7.15.** Sei $\sigma\colon K \hookrightarrow L$ ein Körperhomomorphismus. Wir nennen einen Körperhomomorphismus $\tau\colon M \hookrightarrow L$ mit $K \subset M$ eine **Fortsetzung** von $\sigma$ auf $M$, falls folgendes Diagramm kommutiert:




Mit anderen Worten, $\tau|_K = \sigma$.

tension:irreducible

**Korollar 3.7.16.** *Seien $f \in K[X]$ ein irreduzibles Polynom und $\sigma\colon K \hookrightarrow L$ ein Körperhomomorphismus. Dann ist die Anzahl der Fortsetzungen*

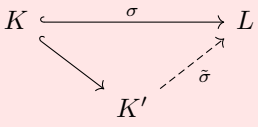



*gleich der Anzahl der Nullstellen von $f^\sigma$ (ohne Vielfachheiten).*

*Beweis.* Jede Nullstelle $a \in L$ von $f^\sigma$ definiert eine Fortsetzung wie in Beobachtung 3.7.14. Umgekehrt bildet jede Fortsetzung $\tilde{\sigma}$ das Element $\bar{X} \in K[X]/(f)$ auf eine Nullstelle von $f^\sigma$ in $L$ ab. □

extension:algebraic

**Korollar 3.7.17.** *Seien $K'/K$ eine algebraische Körpererweiterung und $\sigma\colon K \hookrightarrow L$ ein Körperhomomorphismus in einen algebraisch abgeschlossenen Körper $L$. Dann existiert eine Fortsetzung*

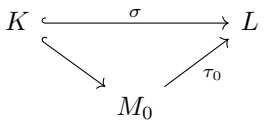



. Widerholung (Lemma von Zorn 2.6.5) Sei $\mathcal{P}$ eine Menge, ausgestattet mit einer Halbordnung, sodass jede aufsteigende Kette eine obere Schranke in $\mathcal{P}$ besitzt. Dann existiert ein maximales Element.

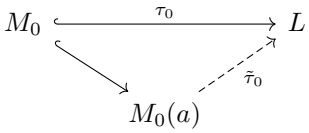
*Beweis.* Wir wollen das Lemma von Zorn verwenden. Betrachte die Menge $\mathcal{P}$ aller Paare $(M, \tau)$, wobei $K \subset M \subset K'$ ein Zwischenkörper und $\tau\colon M \to L$ eine Fortsetzung von $\sigma$ sind.

Definiere die Halbordnung $(M,\tau) \leq (M',\tau')$, falls $M \subset M' \subset K'$ und $\tau'|_M = \tau$, d. h., falls $\tau'$ eine Fortsetzung von $\tau$ auf $M$ ist.

Das Lemma von Zorn 2.6.5 greift in unserem Fall wie folgt: Falls $(M_1,\tau_1) \leq (M_2,\tau_2) \leq \cdots$ eine Kette ist,[42] dann ist $(M,\tau)$ eine obere Schranke, wobei $M \coloneqq \bigcup_{i=1}^{\infty} M_i$ und $\tau|_{M_i} \coloneqq \tau_i$ sind. Sei also $(M_0,\tau_0) \in \mathcal{P}$ maximal, wobei folgendes Diagramm kommutiert:

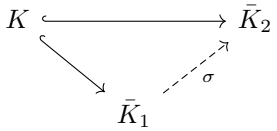



Da $K'/K$ algebraisch ist, ist auch $K'/M_0$ algebraisch. Nach Korollar 3.7.16 existiert damit für alle $a \in K'$ eine Fortsetzung




Aufgrund der Maximalität von $(M_0,\tau_0)$ folgt $M_0 = M_0(a)$, also $M_0 = K'$. □

*Beweis der Eindeutigkeit in Satz 3.7.13.* Angenommen es existieren zwei algebraische Abschlüsse $\bar{K}_1/K$ und $\bar{K}_2/K$ eines Körpers $K$. Dann betrachten wir folgende Fortsetzung, die nach Korollar 3.7.17 existiert:




Es folgt $K \subset \bar{K}_1 \simeq \sigma(\bar{K}_1) \subset \bar{K}_2$. Da $\bar{K}_2/K$ algebraisch ist, ist auch $\bar{K}_2/\sigma(\bar{K}_1)$ algebraisch. Jedes $a \in \bar{K}_2$ besitzt ein Minimalpolynom über $\sigma(\bar{K}_1)$. Weil $\sigma(\bar{K}_1)$ algebraisch abgeschlossen ist, muss das Minimalpolynom linear sein, d. h. $a \in \sigma(\bar{K}_1)$. Somit ist $\sigma(\bar{K}_1) = \bar{K}_2$. □

**Warnung 3.7.18.** Den algebraischen Abschluss eines Körpers $K$ erhalten wir nicht einfach dadurch, dass wir alle Nullstellen aller Polynome in $K[X]$ adjungieren und so $K'$ erhalten, denn es fehlen alle Nullstellen von Polynomen in $K'[X]$ usw. Vgl. auch den Beweis für die Existenz eines algebraischen Abschlusses.

**Definition 3.7.19.** Seien $K$ ein Körper und $\mathcal{F} = \{f_i\}_{i\in I}$ mit Polynomen $f_i \in K[X]$ vom Grad $\deg(f_i) \geq 1$. Dann heißt $L/K$ **Zerfällungskörper** von $\mathcal{F}$, falls alle $f_i \in K[X] \subset L[X]$ in $L[X]$ in Linearfaktoren zerfallen. Anders gesagt, $f_i = c_i \prod_{j=0}^{\deg(f_i)} (X - \alpha_{ij})$ mit $\alpha_{ij} \in L$ und $L$ minimal, d. h. $L$ wird erzeugt durch die Nullstellen der Polynome $f_i \in L[X]$.

[42] Auch wenn auf Nachfrage der Dozent anderer Meinung ist, bin ich immer noch der festen Überzeugung, dass es nicht ausreicht, das Lemma von Zorn nicht nur auf abzählbare Ketten anzuwenden. Für Gegenbeispiele s. [MSE].

*Beispiel* 3.7.20. Sei $\mathcal{F} = \{f_1, \dots, f_n\}$ eine endliche Menge. Dann ist der Zerfällungskörper von $\mathcal{F}$ der Zerfällungskörper von $f_1 \cdots f_n$.

*Problem* 3.7.21. Oft wollen wir den Zerfällungskörper eines Polynoms $f \in K[X]$ bestimmen. In der Galoistheorie studieren wir dann die Galoisgruppe $\mathrm{Gal}(f)$, um Aussagen über die Nullstellen von $f$ zu beweisen.

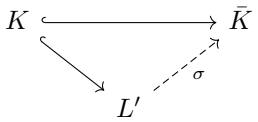
**Satz 3.7.22.** *Jede Menge $\mathcal{F} \subset K[X]$ besitzt einen (bis auf nicht-eindeutige Isomorphie) eindeutigen Zerfällungskörper $L/K$.*

*Beweis.* Es existiert ein algebraischer Abschluss $\bar{K}/K$. Definiere die Menge der Nullstellen

$$A \coloneqq \{a \in \bar{K} \mid f_i(a) = 0 \text{ für ein } f_i \in \mathcal{F}\}.$$

Setze dann $L \coloneqq K(A)$. Da $\bar{K}$ algebraisch abgeschlossen ist, zerfallen alle $f_i \in \mathcal{F}$ in $\bar{K}$ in Linearfaktoren, weshalb sie auch in $L[X]$ in Linearfaktoren zerfallen. Also existiert der Zerfällungskörper.

Für die Eindeutigkeit sei $L'/K$ ein weiterer Zerfällungskörper von $\mathcal{F}$. Nach Korollar 3.7.17 existiert folgende Fortsetzung:




Für alle $a \in L'$ mit $f_i(a) = 0$ gilt auch $f_i(\sigma(a)) = 0$, also $\sigma(a) \in L$. Da $L'/K$ durch die Nullstellen der Polynome $f_i \in \mathcal{F}$ in $L'$ erzeugt wird, gilt $\sigma(L') \subset L$. Wegen der Minimalität des Zerfällungskörpers $L/K$ folgt $\sigma(L') = L$ und daher $L' \simeq L$. □

**Beobachtung 3.7.23** (Konstruktion des Zerfällungskörpers eines Polynoms)**.** Sei $\mathcal{F} = \{f\}$ mit $f \in K[X]$. Zerlege $f$ in irreduzible Polynome $f = g_1 \cdots g_n$. Wir erhalten $K \subset L \coloneqq K[X]/(g_1)$, wobei $a \coloneqq \bar{X}$ eine Nullstelle von $g_1$ ist. Wir erhalten $f = (X - a)g_1' g_2 \cdots g_n$ in $L[X]$. Dann ist $g_1' g_2 \cdots g_n$ ein Polynom kleineren Grads, und nach Induktion gibt es einen Zerfällungskörper $\tilde{L}/L$ von diesem Polynom. Damit ist $\tilde{L}(a)/K$ ein Zerfällungskörper von $f$.

**Lemma 3.7.24.** *Sei $L/K$ der Zerfällungskörper eines Polynoms $f \in K[X]$. Dann gelten:*

(i) $[L : K] \mid \deg(f)!$.

(ii) *Falls $[L : K] = \deg(f)!$, dann ist $f \in K[X]$ irreduzibel.*
Achtung: *Die Umkehrung gilt nicht.*

*Beweis.*

(i) Wir induzieren über $\deg(f)$. Sei $a \in L$ eine Nullstelle von $f$. Betrachte $K \subset K(a) \subset L$. Falls $f$ irreduzibel ist, dann ist $K(a) \simeq K[X]/(f)$ und damit $[K(a) : K] = \deg(f)$. Dann ist $L/K(a)$ der Zerfällungskörper von $f/(X - a) \in K(a)[X]$. Nach

Induktionsvoraussetzung ist $[L : K(a)] \mid (\deg(f) - 1)!$. Sodann folgt $[L : K] = [L : K(a)][K(a) : K]$ aus der Produktformel 3.5.8, also $[L : K] \mid \deg(f)!$.

Falls $f$ nicht irreduzibel ist, schreibe $f = g_1 g_2$ mit $g_1$ irreduzibel. Weil $L/K$ der Zerfällungskörper von $f$ ist, zerfällt $g_1$ in $L$ in Linearfaktoren. Betrachte $K \subset K_1 \subset L$, wobei $K_1$ der Zerfällungskörper von $g_1$ ist. Damit ist $L/K_1$ der Zerfällungskörper von $g_2$, und nach Induktionsvoraussetzung gilt $[L : K_1] \mid \deg(g_2)!$. Nach Produktformel 3.5.8 gilt $[L : K] = [L : K_1][K_1 : K]$ mit $[L : K_1] \mid \deg(g_2)!$ und $[K_1 : K] \mid \deg(g_1)!$. Wegen $\deg(f) = \deg(g_1) + \deg(g_2) \in \mathbb{Z}$ und $\deg(g_1) \in \mathbb{Z}$ gilt $\binom{\deg(f)}{\deg(g_1)} \in \mathbb{Z}$, weshalb wir $\deg(g_1)!\deg(g_2)! \mid \deg(f)!$ folgern können. Also ist $[L : K] \mid \deg(f)!$.

(ii) Sei $[L : K] = \deg(f)!$. Angenommen $f$ wäre nicht irreduzibel, sagen wir $f = f_1 f_2$ mit $\deg(f_1), \deg(f_2) \geq 1$. Seien $K_1/K$ der Zerfällungskörper von $f_1$ und $L/K_1$ der Zerfällungskörper von $f_2 \in K_1[X]$. Dann gilt $\deg(f)! = [L : K] = [K_1 : K][L : K_1]$ mit $[K_1 : K] \mid \deg(f_1)!$ und $[L : K_1] \mid \deg(f_2)!$. Da $\binom{n}{k} = 1$ genau dann, wenn $k = 0$ oder $k = n$, folgt $\deg(f_1) = \deg(f)$ oder $\deg(f_2) = \deg(f)$. □

*Beispiel* 3.7.25. Sei $f = X^3 + 3X + 1 \in \mathbb{Q}[X]$. Wir wollen den Zerfällungskörper $L/\mathbb{Q}$ von $f$ verstehen und insbesondere die Zahl $[L : \mathbb{Q}]$. Wir wissen, dass $[L : \mathbb{Q}] \mid \deg(f)! = 6$. Dann ist $[L : \mathbb{Q}] \in \{1, 2, 3, 6\}$.

Da $\deg(f) = 3$ ungerade ist, besitzt $f$ eine Nullstelle in $\mathbb{R}$. Wegen $f' = 3X^2 + 3 > 0$ für alle $X \in \mathbb{R}$ ist $f$ monoton wachsend und besitzt daher genau eine Nullstelle $\alpha \in \mathbb{R}$ sowie zwei weitere $\beta, \bar{\beta} \in \mathbb{C}$. Es gilt also $f = (X - \alpha)(X - \beta)(X - \bar{\beta}) \in \mathbb{C}[X]$ und daher $L \simeq \mathbb{Q}(\alpha, \beta, \bar{\beta}) \subset \mathbb{C}$. Es folgen $\mathbb{Q} \subset \mathbb{Q}(\alpha) \subset \mathbb{Q}(\alpha, \beta, \bar{\beta}) \simeq L$ und

$$[L : \mathbb{Q}] = [\mathbb{Q}(\alpha) : \mathbb{Q}] \cdot [\mathbb{Q}(\alpha, \beta, \bar{\beta}) : \mathbb{Q}(\alpha)].$$

Was ist $[\mathbb{Q}(\alpha) : \mathbb{Q}]$? Falls $f$ irreduzibel ist, gilt $[\mathbb{Q}(\alpha) : \mathbb{Q}] = \deg(f) = 3$. Es gilt aber mit der Transformation $X = Y - 1$

$$X^3 + 3X + 1 = (Y - 1)^3 + 3(Y - 1) + 1 = Y^3 + 3Y^2 - 1 - 3 + 1 = Y^3 + 3Y^2 - 3$$

und nach dem Eisensteinkriterium 2.5.5 ist $f$ tatsächlich irreduzibel. Beobachte ferner, dass $[\mathbb{Q}(\alpha, \beta, \bar{\beta}) : \mathbb{Q}(\alpha)] \neq 1$, da $\beta \notin \mathbb{Q}(\alpha) \subset \mathbb{R}$. Folglich muss $[L : \mathbb{Q}] = 6$. (Später sehen wir, dass $\mathrm{Gal}(f) = \mathfrak{S}_3$.)

*Problem* 3.7.26. Als nächstes wollen wir den Zerfällungskörper $L/\mathbb{Q}$ von $g = X^3 - 3X + 1$ betrachten (was ein Minus hat). Wir werden zeigen, dass $[L : \mathbb{Q}] = 3$.

**Definition 3.7.27.** Die Diskriminante eines kubischen Polynoms der Gestalt $f = X^3 + pX + q \in K[X]$ (der quadratische Term verschwindet mit einer Tschirnhaustransformation) ist $D(f) := -4p^3 - 27q^2$.

n:discriminant:cubic

**Bemerkung 3.7.28.** Betrachte den Zerfällungskörper $L/K$ von $f$ (oder gleich $\bar{K}/K$). Dann gilt $f = (X - \alpha_1)(X - \alpha_2)(X - \alpha_3) \in L[X]$ mit $\alpha_1, \alpha_2, \alpha_3 \in L$. Mit etwas Rechnung gilt

$$D(f) = [(\alpha_1 - \alpha_2)(\alpha_1 - \alpha_3)(\alpha_2 - \alpha_3)]^2.$$

Koeffizientenvergleich liefert

$$q = -\alpha_1\alpha_2\alpha_3, \qquad 0 = -(\alpha_1+\alpha_2+\alpha_3), \qquad p = \alpha_1\alpha_2+\alpha_1\alpha_3+\alpha_2\alpha_3.$$

Insbesondere ist $D(f) \in K$.

**Satz 3.7.29.** *Sei $f = X^3 + pX + q \in K[X]$ ein irreduzibles Polynom und sei $L$ sein Zerfällungskörper. Dann gilt*

$$[L:K] = \begin{cases} 6, & \text{falls } \sqrt{D(f)} \notin K, \text{ d. h. es gibt kein } \alpha \in K \text{ mit } \alpha^2 = D(f), \\ 3, & \text{falls } \sqrt{D(f)} \in K, \text{ d. h. es gibt ein } \alpha \in K \text{ mit } \alpha^2 = D(f), \end{cases}$$

*Beweis.* Wir wissen bereits, dass $[L:K] \mid \deg(f)! = 6$. Da $f$ irreduzibel ist, ist $[L:K] \neq 1$. Ferner ist $3 \mid [L:K]$, denn für eine Nullstelle $\alpha \in L$ von $f$ ist $K \subset K(\alpha) \simeq K[X]/(f) \subset L$; nach Produktformel 3.5.8 gilt $3 = [K(\alpha):K] \mid [L:K]$. Wir erhalten $[L:K] = 3$ oder $[L:K] = 6$.

(i) Fall $\sqrt{D(f)} \notin K$: Wir kürzen $D \coloneqq D(f)$ ab. Betrachte den Turm von Körpererweiterungen $K \subset K(\sqrt{D}) \subset L$. $\sqrt{D}$ ist eine Nullstelle von $X^2 - D$, d. h. $[K(\sqrt{D}):K] = 2$. Daher ist $2 \mid [L:K]$ und somit $[L:K] = 6$.

(ii) Fall $\sqrt{D(f)} \in K$ existiert: Betrachte $q = -\alpha_1\alpha_2\alpha_3$ und $\alpha_1+\alpha_2+\alpha_3 = 0$. Dann gilt $q = \alpha_1\alpha_2(\alpha_1+\alpha_2)$ bzw. $\alpha_1\alpha_2^2 + \alpha_1^2\alpha_2 - q = 0$. Dann ist $\alpha_2$ eine Nullstelle von

$$g_1(X) \coloneqq \alpha_1 X^2 + \alpha_1^2 X - q \in K(\alpha_1)[X].$$

Nach Voraussetzung ist

$$\sqrt{D} = (\alpha_1-\alpha_2)(\alpha_1-\alpha_3)(\alpha_2-\alpha_3) = (\alpha_1-\alpha_2)(2\alpha_1+\alpha_2)(2\alpha_2+\alpha_1) \in K.$$

Deshalb ist $\alpha_2$ auch eine Nullstelle von

$$g_2(X) \coloneqq (\alpha_1 - X)(2\alpha_1 + X)(2X + \alpha_1) - \sqrt{D} \in K(\alpha_1)[X].$$

Zusammenfassend ist $\alpha_2$ eine Nullstelle von $g_1(X), g_2(X) \in K(\alpha_1)[X]$ mit $\deg(g_1) = 2$ und $\deg(g_2) = 3$. Man kann nachrechnen, dass

$$\alpha_1 g_2(X) + 2X g_1(X) + \alpha_1 g(X) = (4\alpha_1^3 - 2q)X + 2\alpha_1^4 - \alpha_1 q - \alpha_1\sqrt{D} \in K(\alpha_1)[X], \quad (3.7.30)$$

{eqn:cubic:split}

was ein Polynom ersten Grads ist. (Beobachte, dass dieses Polynom den kubischen Summanden von $g_2(X)$ eliminiert.) Insbesondere ist $\alpha_2$ eine Nullstelle davon, d. h. $\alpha_2 \in K(\alpha_1)$. Es folgt $[K(\alpha_1):K] = 3$ und $K(\alpha_1) = K(\alpha_1,\alpha_2) = K(\alpha_1,\alpha_2,\alpha_3) = L$. Somit ist $[L:K] = 3$.

*Warnung:* Wir müssten noch zeigen, dass (3.7.30) nicht das Nullpolynom ist, was eine lange Rechnung ist. Hierbei muss besonders auf Charakteristik 2 acht gegeben werden. □

*Beispiel* 3.7.31. Die Diskriminanten von

$$f = X^3 + 3X + 1 \in \mathbb{Q}[X] \qquad \text{und} \qquad g = X^3 - 3X + 1 \in \mathbb{Q}[X]$$

sind

$$D(f) = -4 \cdot 27 - 27 = -5 \cdot 27 \qquad \text{und} \qquad D(g) = 4 \cdot 27 - 27 = +3 \cdot 27 = 9^2.$$

Ist $L$ der Zerfällungskörper von $g$, so ist $[L : \mathbb{Q}] = 3$ da $\sqrt{D(g)} = 9 \in \mathbb{Q}$.

*Beispiel* 3.7.32. Betrachte das Polynom $f = X^3 - 2 \in \mathbb{Q}[X]$, was irreduzibel gemäß dem Eisensteinkriterium 2.5.5 modulo 2 ist. Nun ist $D(f) = -27 \cdot 4$, d. h. $\sqrt{D(f)} \notin \mathbb{Q}$ und für den Zerfällungskörper $L$ von $f$ gilt $[L : \mathbb{Q}] = 6$.

*Beispiel* 3.7.33. Betrachte das Polynom $f = X^4 + 2X^2 - 2 \in \mathbb{Q}[X]$ und sei $L$ der Zerfällungskörper von $f$. Was ist $[L : \mathbb{Q}]$?

Setze $Y \coloneqq X^2$ und

$$g(Y) \coloneqq Y^2 + 2Y - 2 = (Y + 1)^2 - 3.$$

Die Nullstellen von $g$ sind $\pm\sqrt{3} - 1$, und somit hat $f$ vier Nullstellen $\pm\sqrt{\pm\sqrt{3} - 1} \in \mathbb{C}$. Betrachte den Körper

$$L_1 \coloneqq \mathbb{Q}(\sqrt{3} - 1) = \mathbb{Q}(\sqrt{3}) \subset L.$$

Dann ist $L_1/\mathbb{Q}$ der Zerfällungskörper von $g$ und daher $[L_1 : \mathbb{Q}] = 2$, weil $L_1 \neq \mathbb{Q}$.

Sei nun $L_2 \subset L$ der Zerfällungskörper von $X^2 - (\sqrt{3} - 1)$, d. h.

$$L_2 = \mathbb{Q}\left(\sqrt{3} - 1, \sqrt{\sqrt{3} - 1}\right) \subset \mathbb{R}.$$

Weil $\sqrt{-\sqrt{3} - 1} \in L$ nicht reell ist, ist $L_2 \neq L$. Beobachte, dass

$$L = \mathbb{Q}\left(\sqrt{\sqrt{3} - 1}, \sqrt{-\sqrt{3} - 1}\right)$$

der Zerfällungskörper von $X^2 - (-\sqrt{3} - 1) \in L_2[X]$ ist, weshalb $[L : L_2] = 2$ gilt.

Weil $L_2$ der Zerfällungskörper von $X^2 - (\sqrt{3} - 1) \in L_1[X]$ ist, ist entweder $[L_2 : L_1] = 1$ oder $[L_2 : L_1] = 2$. Angenommen $[L_2 : L_1] = 1$. Dann ist $\sqrt{\sqrt{3} - 1} \in \mathbb{Q}(\sqrt{3})$, d. h. es gibt $a, b \in \mathbb{Q}$ mit $\sqrt{\sqrt{3} - 1} = a + b\sqrt{3}$. Quadrieren liefert $\sqrt{3} - 1 = a^2 + 3b^2 + 2ab\sqrt{3}$, und weiteres Umformen führt zu einem Widerspruch. Folglich ist $[L_2 : L_1] = 2$.

Rückblickend haben wir einen Turm $\mathbb{Q} \subset L_1 \subset L_2 \subset L$ konstruiert, wobei jede Körpererweiterung von aufeinanderfolgenden Körpern Grad 2 hat, d. h. $[L : \mathbb{Q}] = 8$.

*Beispiel* 3.7.34. Weitere Beispiele.[43]

(i) Betrachte den Zerfällungskörper $L$ des Polynoms $f = X^4 + 1 \in \mathbb{Q}[X]$ über $\mathbb{Q}$. Wir wollen $[L : \mathbb{Q}]$ bestimmen.

Dazu sei $\zeta = \mathrm{e}^{2\pi\mathrm{i}/8}$ eine achte primitive Einheitswurzel. Dann gilt $\zeta^4 = -1$. Also ist $\zeta$ eine Nullstelle von $f$, genauso $\zeta^3$, $\zeta^5$ und $\zeta^7$. Folglich ist $L = \mathbb{Q}(\zeta)$ und wir erhalten $[L : \mathbb{Q}] = \deg(p_\zeta)$, wobei $p_\zeta$ das Minimalpolynom von $\zeta$ über $\mathbb{Q}$ ist.

[43] Folgende Beispiele wurden am 08.12.23 gezeigt.

Betrachte

$$f(Y+1) = Y^4 + 4Y^3 + 6Y^2 + 4Y + 1 + 1.$$

Nach Eisenstein mit $p = 2$ folgt, dass $f = p_\zeta$ irreduzibel ist. Also ist $[L : \mathbb{Q}] = 4$.

(ii) Sei $L$ der Zerfällungskörper des Polynoms $f = X^5 + 2 \in \mathbb{Q}[X]$. Wir wollen $[L : \mathbb{Q}]$ bestimmen.

Sei $\mu = \mathrm{e}^{2\pi \mathrm{i}/10}$ eine zehnte primitive Einheitswurzel. Dann sind die Nullstellen von $f$ $\eta_i = \sqrt[5]{2}\mu^i \in \mathbb{C}$ für $i = 1, 3, 5, 7, 9$. Also ist $L = \mathbb{Q}(\eta_1, \eta_3, \eta_5, \eta_7, \eta_9)$. Wir können das reduzieren. Betrachte den Turm von Körpererweiterungen $\mathbb{Q} \subset \mathbb{Q}(\eta_1) \subset \mathbb{Q}(\eta_1, \eta_3)$. Da $\eta_3/\eta_1 = \mu^2$ ist, gelten $\eta_5 = \eta_1\mu^4$, $\eta_7 = \eta_1\mu^6$ und $\eta_9 = \eta_1\mu^8$. Deshalb gilt $L = \mathbb{Q}(\eta_1, \eta_3)$.

Nach Produktformel 3.5.8 gilt

$$[L : \mathbb{Q}] = [\mathbb{Q}(\eta_1) : \mathbb{Q}][\mathbb{Q}(\eta_1, \eta_3) : \mathbb{Q}(\eta_1)].$$

Wir wissen, dass $[\mathbb{Q}(\eta_1) : \mathbb{Q}] = \deg(p_{\eta_1})$, wobei $p_{\eta_1}$ das Minimalpolynom von $\eta_1$ über $\mathbb{Q}$ ist. Da $f \in \mathbb{Q}[X]$ nach dem Eisensteinkriterium mit $p = 2$ irreduzibel ist und da $f(\eta_1) = 0$, gilt $f = p_{\eta_1}$. Wir erhalten $[\mathbb{Q}(\eta_1) : \mathbb{Q}] = 5$.

Es verbleibt $[\mathbb{Q}(\eta_1, \eta_3) : \mathbb{Q}(\eta_1)]$. Wegen $\eta_3 = \eta_1\mu^2$ gilt $\mathbb{Q}(\eta_1, \eta_3) = \mathbb{Q}(\eta_1, \mu^2)$. Es folgt

$$[\mathbb{Q}(\eta_1, \eta_3) : \mathbb{Q}(\eta_1)] = [\mathbb{Q}(\eta_1, \mu^2) : \mathbb{Q}(\eta_1)] = \det(p_{\mu^2}),$$

wobei $p_{\mu^2}$ das Minimalpolynom von $\mu^2$ über $\mathbb{Q}(\eta_1)$ ist. Wir wissen, dass $(\mu^2)^5 = 1$, d. h. $\mu^2$ ist eine Nullstelle vom Kreisteilungspolynom $\Phi_5 = X^4 + X^3 + X^2 + X + 1$. Wir wissen ferner, dass $\Phi_5 \in \mathbb{Q}[X]$ irreduzibel ist.

*Frage:* Ist $\Phi_5 \in \mathbb{Q}(\eta_1)[X]$ irreduzibel? Wenn ja, so gilt $[\mathbb{Q}(\eta_1, \eta_3) : \mathbb{Q}(\eta_1)] = 4$.

Wir wissen definitiv, dass $p_{\mu^2} \mid \Phi_5$ in $\mathbb{Q}(\eta_1)[X]$. Also ist $\deg(p_{\mu^2}) \leq 4$. Andererseits können wir den Turm von Körpererweiterungen $\mathbb{Q} \subset \mathbb{Q}(\mu^2) \subset L$ betrachten. Wegen der Irreduzibilität von $\Phi_5 \in \mathbb{Q}[X]$ ist $[\mathbb{Q}(\mu^2) : \mathbb{Q}] = 4$. Nach Produktformel 3.5.8 muss $4 \mid [L : \mathbb{Q}]$ sein, d. h. $4 \mid [\mathbb{Q}(\eta_1, \eta_3) : \mathbb{Q}(\eta_1)]$ und damit $[\mathbb{Q}(\eta_1, \eta_3) : \mathbb{Q}(\eta_1)] = 4$. Schließlich ist $[L : \mathbb{Q}] = 20$.

## 3.8 Endliche Körper

**Definition 3.8.1.** Sei $\mathbb{F}$ ein Körper der Charakteristik $p$. Dann ist der **Frobenius**

$$F \colon \mathbb{F} \longrightarrow \mathbb{F}, \qquad a \longmapsto a^p,$$

was nach Aufgabe 34 ein Körperhomomorphismus und insbesondere injektiv ist.

Frobenius Georg Frobenius (1849–1917) ist der Nachfolger von Kronecker.

**Bemerkung 3.8.2.** Wenn $\mathbb{F}$ endlich ist, dann ist $F \colon \mathbb{F} \xrightarrow{\sim} \mathbb{F}$ ein Isomorphismus, d. h. $F$ ist auch surjektiv.

**Bemerkung 3.8.3.** Da $\operatorname{char}(\mathbb{F}) = p$ ist, ist $\mathbb{F}_p \hookrightarrow \mathbb{F}$ der Primkörper; insbesondere ist $\mathbb{F}/\mathbb{F}_p$ eine Körpererweiterung. Falls $\mathbb{F}/\mathbb{F}_p$ endlich ist (was äquivalent zu $|\mathbb{F}| < \infty$ ist), ist $\mathbb{F} \simeq \mathbb{F}_p^{\oplus n}$ als $\mathbb{F}_p$-Vektorraum für $[\mathbb{F} : \mathbb{F}_p] = n$. Damit ist $|\mathbb{F}| = q := p^n$.

**Lemma 3.8.4.** *Sei $\mathbb{F}$ ein endlicher Körper mit $q := |\mathbb{F}|$. Dann ist $\mathbb{F}$ der Zerfällungskörper von $X^q - X$ über $\mathbb{F}_p$.*

*Beweis.* Offenbar ist $\mathbb{F}^*$ eine endliche Gruppe. Gemäß Satz 3.4.2 ist $\mathbb{F}^* \simeq \mathbb{Z}/(q-1)$ eine zyklische Gruppe der Ordnung $q-1$. Für alle $a \in \mathbb{F}^*$ gilt dann $a^{q-1} - 1 = 0$ nach dem kleinen Satz von Fermat 1.2.17. Also gilt $a^q - a = 0$ für alle $a \in \mathbb{F}$ und alle $a \in \mathbb{F}$ sind Nullstellen von $X^q - X \in \mathbb{F}_p[X]$. Also ist $\mathbb{F} \subset \{\text{Nullstellen von } X^q - X\} \subset \bar{\mathbb{F}}$. Da $q = \bar{\mathbb{F}}$, muss bereits $\mathbb{F}$ die Menge der Nullstellen von $X^q - X$ sein, d. h. $\mathbb{F}$ ist der Zerfällungskörper von $X^q - X$. □

**Korollar 3.8.5.** *Wenn $\mathbb{F}$ endlich ist, dann ist $\mathbb{F}$ bis auf Isomorphie eindeutig durch dessen Kardinalität bestimmt.*

obs:field:finite

**Beobachtung 3.8.6.** Gibt es für jede Primzahlpotenz $q = p^n$ einen Körper $\mathbb{F}$ mit $|\mathbb{F}| = q$?

Die naive Idee ist einfach, $\mathbb{F}$ als den Zerfällungskörper von $X^q - X \in \mathbb{F}_p[X]$ zu setzen. Warum gilt aber mit dieser Definition $|\mathbb{F}| = q$?

*Behauptung:* $|\mathbb{F}| = q$.

*Beweis:* Sei $K$ die Menge der Nullstellen von $f$. Weil $\mathbb{F}$ der Zerfällungskörper von $f$ ist, gilt $K \subset \mathbb{F}$. Aber $K$ ist automatisch ein Körper (für $a^p - a = 0$ und $b^p - b = 0$ folgt mit Frobenius $(a+b)^p - (a+b) = 0$), weshalb $K = \mathbb{F}$ gilt.

Daher genügt es zu zeigen, dass $f$ genau $q$ verschiedene Nullstellen hat. Schreibe $f = X^q - X = \prod_{i=1}^{q}(X - \alpha_i)$. Wir müssen $\alpha_i \neq \alpha_j$ für alle $i \neq j$ zeigen. Es gilt

$$f'(X)w = \sum_{i=1}^{q} \prod_{j=1, j\neq i}^{q} (X - \alpha_j).$$

Falls $\alpha_i = \alpha_j$ für $i \neq j$, so gilt $f'(\alpha_i) = 0$. Andererseits ist

$$f'(X) = (X^q - X)' = qX^{q-1} - 1 = -1$$

wegen $\operatorname{char}(\mathbb{F}) = p \mid q$, was keine Nullstelle hat; Widerspruch!

**Korollar 3.8.7.** *Für jede Primzahlpotenz $q = p^n$ gibt es einen Körper $\mathbb{F}$ mit $|\mathbb{F}| = q$. Dieser ist eindeutig bis auf (nichteindeutige, d. h. nichtkanonische) Isomorphie.*

**Bemerkung 3.8.8.** Sei $\bar{\mathbb{F}}_p$ ein algebraischer Abschluss von $\mathbb{F}_p$. Für alle $n$ gilt dann $\mathbb{F}_{p^n} \subset \bar{\mathbb{F}}_p$ und

$$\bar{\mathbb{F}}_p = \bigcup_{n=1}^{\infty} \mathbb{F}_{p^n},$$

was man leicht prüfen kann.[44] was man leicht prüfen kann.

Ferner ist der Frobenius $F\colon \bar{\mathbb{F}}_p \hookrightarrow \bar{\mathbb{F}}_p$ auch surjektiv. Da jedes $a \in \bar{\mathbb{F}}_p$ algebraisch über $\mathbb{F}_p$ ist, gilt nach obiger Charakterisierung von endlichen Körpern $\mathbb{F}_p(a) = \mathbb{F}_{p^n}$ für ein gewisses $n$. Zudem wissen wir, dass die Einschränkung $F\colon \mathbb{F}_{p^n} \xrightarrow{\simeq} \mathbb{F}_{p^n}$ auf endlichen Körpern bijektiv ist.

Das Argument im Beweis von Beobachtung 3.8.6 zeigt folgende Aussage.

**Fakt 3.8.9.** *$f \in K[X]$ hat genau dann eine gemeinsame Nullstelle mit $f'$, wenn $f$ eine mehrfache Nullstelle in $\bar{K}$ besitzt.*

**Bemerkung 3.8.10.** Sei $\mathbb{F}'/\mathbb{F}$ eine eine Körpererweiterung eines endlichen Körpers. Dann gibt es $n, m$, sodass $\mathbb{F} = \mathbb{F}_{p^n}$ und $\mathbb{F}' = \mathbb{F}_{p^m}$. Es folgt $\mathbb{F}' \simeq \mathbb{F}^{\oplus[\mathbb{F}':\mathbb{F}]}$, d. h. $p^m = |\mathbb{F}'| = |\mathbb{F}|^{[\mathbb{F}':\mathbb{F}]} = p^{n[\mathbb{F}':\mathbb{F}]}$ und somit $m = n[\mathbb{F}' : \mathbb{F}]$. Da alle Elemente in $\mathbb{F}'$ Nullstellen von $X^{p^m} - X$ und alle Elemente in $\mathbb{F}$ Nullstellen von $X^{p^n} - X$ sind, gilt $X^{p^n} - X \mid X^{p^m} - X$.

Betrachten wir $\mathbb{F}_{p^n} \subset \bar{\mathbb{F}}$ und $\mathbb{F}_{p^m} \subset \bar{\mathbb{F}}$, so folgern wir: $\mathbb{F}_{p^n} \subset \mathbb{F}_{p^m}$ genau dann, wenn $n \mid m$. Vgl. mit Aufgabe 47: Für irreduzible $f \in \mathbb{F}_p[X]$ ist $\deg(f) \mid n$ genau dann, wenn $f$ ein irreduzibler Faktor von $X^{p^n} - X$ ist.

## 3.9 Normale Körpererweiterungen

**Definition 3.9.1.** Eine algebraische Körpererweiterung $L/K$ heißt **normal**, falls jedes irreduzible Polynom $f \in K[X]$ mit mindestens einer Nullstelle in $L$ komplett in Linearfaktoren in $L[X]$ zerfällt.

thm:normal

**Satz 3.9.2.** *Sei $L/K$ eine Körpererweiterung. Dann sind die folgenden Bedingungen äquivalent:*

itm:normal:1 (i) *$L/K$ ist normal.*

itm:normal:2 (ii) *Es gibt eine Menge $\mathcal{F} \subset K[X]$, sodass $L$ der Zerfällungskörper von $\mathcal{F}$ ist.*

itm:normal:3 (iii) *Für alle Körperhomomorphismen $\varphi\colon L \to \bar{L}$ mit $\varphi|_K = \mathrm{id}_K$ gilt $\varphi(L) \subset L$.*

*Beweis.*

- (i) $\implies$ (ii): Schreibe $L = K(A)$ für eine gewisse Teilmenge $A \subset L$. Da $L/K$ algebraisch ist, sind alle $a \in A$ algebraisch über $K$ und das Minimalpolynom $p_a \in K[X]$ besitzt eine Nullstelle in $L$. Da $L/K$ normal ist, folgt daraus, dass $p_a$ in $L[X]$ komplett in Linearfaktoren zerfällt. Setze nun $\mathcal{F} := \{p_a \mid a \in A\}$. Sei $L'$ der Zerfällungskörper von $\mathcal{F}$. Dann gilt $K, A \subset L' \subset L$ und damit $K(A) = L \subset L' \subset L$.
- (ii) $\implies$ (iii): Angenommen $L \subset \bar{L}$ ist der Zerfällungskörper einer gewissen Teilmenge $\mathcal{F} \subset K[X]$. Sei $\varphi\colon L \hookrightarrow \bar{L}$ mit $\varphi|_K = \mathrm{id}_K$ ein Körperhomomorphismus. Dann ist $\varphi(L)$

[44] Diese Konstruktion kommt in Algebra und Topologie häufiger vor und heißt *filtrierter Kolimes*. In diesem Fall ist $\bar{\mathbb{F}}_p$ der Kolimes des Diagramms $\mathbb{F}_p \hookrightarrow \mathbb{F}_{p^2} \hookrightarrow \mathbb{F}_{p^3} \hookrightarrow \cdots$, auch mit $\bar{\mathbb{F}}_p = \varinjlim_n \mathbb{F}_{p^n}$ notiert.

ein Zerfällungskörper von $\mathcal{F} = \mathcal{F}^\varphi$: Es gilt nämlich

$$\left(\sum_{i=0}^{n} a_i X^i\right)^\varphi = \sum_{i=0}^{n} \varphi(a_i) X^i = \sum_{i=0}^{n} a_i X^i \in K[X].$$

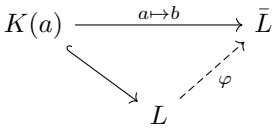
Damit sind $L, \varphi(L) \subset \bar{L}$ beides Zerfällungskörper derselben Menge $\mathcal{F}$ und damit $L = \varphi(L)$.

- (iii) $\implies$ (i): Sei $f \in K[X]$ irreduzibel $f(a) = 0$ für ein gewisses $a \in L$, d. h. $f$ hat eine Nullstelle in $L$. Zu zeigen ist, dass weitere Nullstelle $b \in \bar{L}$ von $f$ schon in $L$ liegt.

  Betrachte $K \hookrightarrow L \hookrightarrow \bar{L}$. Weil $f$ das Minimalpolynom von $a$ über $K$ ist, ist es auch das Minimalpolynom von $b$ über $K$. Damit erhalten wir eine Abbildung

$$K(a) \xrightarrow{\sim} K[X]/(f) \xrightarrow{\sim} K(b) \hookrightarrow \bar{L}, \qquad a \longmapsto b,$$

  welche nach Korollar 3.7.17 fortgesetzt werden kann:




  Nach Voraussetzung (iii) ist aber $\varphi(L) \subset L$, d. h. $b = \varphi(a) \in L$. □

*Problem* 3.9.3. Als kurzfristiges Ziel wollen wir *normale* und *separable* Körpererweiterungen behandeln. Das führt dann in den nächsten Abschnitt 4, *Galoistheorie*. VL 16 08.12.23

*Beispiel* 3.9.4. Typischerweise betrachten wir Zerfällungskörper von $f \in K[X]$ über $K$, was eine normale Körpererweiterung ist.

cor:normal:finite

**Korollar 3.9.5.** *Sei $L/K$ eine endliche Körpererweiterung (die damit auch algebraisch ist). Dann ist $L/K$ genau dann normal, wenn es ein $f \in K[X]$ gibt, sodass $L$ der Zerfällungskörper von $f$ ist.*

*Beweis.* Nehme einfach das Produkt aller Minimalpolynome aller endlich vielen Erzeuger. □

**Korollar 3.9.6.** *Sei $L/K$ der Zerfällungskörper eines Polynoms $f \in K[X]$. Dann zerfällt jedes Polynom $g \in K[X]$ mit mindestens einer Nullstelle in $L$ komplett in Linearfaktoren in $L[X]$.*

*Beweis.* Das ist eine direkte Konsequenz aus Korollar 3.9.5. □

**Korollar 3.9.7.** *Sei $M/L/K$ ein Turm von Körpererweiterungen, wobei $M/K$ normal ist. Dann ist auch $M/L$ normal.*

*Beweis.* Nach Satz 3.9.2 ist $M/K$ genau dann normal, wenn $M$ ein Zerfällungskörper einer Menge $\mathcal{F} \subset K[X] \subset L[X]$ ist. Also ist $M$ der Zerfällungskörper von $\mathcal{F} \subset L[X]$ und damit ist $M/L$ normal. □

**Warnung 3.9.8.** Im Allgemeinen ist aber $L/K$ nicht normal. Dafür kann man eine Nullstelle $\alpha \in \bar{K}$ von $f \in K[X]$ betrachten. Sei dann $L := K(\alpha)$ und $M$ der Zerfällungskörper von $f$. Dann sind $M/K$ und $M/L$ normal, aber $L/K$ in den meisten Fällen natürlich nicht normal.

**Warnung 3.9.9.** Falls $M/L$ und $L/K$ normal sind, muss noch nicht $M/K$ normal sein (Aufgabe 45).

*Beispiel* 3.9.10.

(i) Sei $L/K$ eine Körpererweiterung vom Grad $[L : K] = 2$. Dann ist $L/K$ normal.

*Beweis:* Da $L = K(a)$ für eine Nullstelle $a$ von $X^2 + pX + q \in K[X]$, ist die zweite Nullstelle dieses Polynoms $-p - a \in L$. Folglich ist $L$ bereits der Zerfällungskörper von $X^2 + pX + q$, d. h. $L/K$ ist normal.

(ii) Seien $\mathbb{F}$ ein endlicher Körper, d. h. isomorph zu $\mathbb{F}_{p^n}$ für ein $n$, und $K/\mathbb{F}$ eine algebraische Körpererweiterung. Dann ist $K/\mathbb{F}$ normal.

*Beweis:* Da $\mathbb{F}(a)/\mathbb{F}$ für $a \in K$ eine endliche Körpererweiterung ist, ist $\mathbb{F}(a) \simeq \mathbb{F}_{p^{nm}}$ ein Zerfällungskörper eines Polynoms in $\mathbb{F}_p[X]$ (mit $\mathbb{F} = \mathbb{F}_{p^n}$). Also ist $\mathbb{F}(a)/\mathbb{F}_p$ normal und damit $\mathbb{F}(a)/\mathbb{F}$ normal. Falls $a$ eine Nullstelle eines irreduziblen Polynoms $f \in \mathbb{F}[X]$ ist, dann liegen auch alle anderen Nullstellen von $f$ in $\mathbb{F}(a)$ und damit natürlich in $K$. Die Aussage folgt nun mit Satz 3.9.2, wenn wir die Menge aller Minimalpolynome von Elementen in $K$ über $\mathbb{F}$ betrachten.

*Anmerkung:* Körpererweiterungen endlicher Körper sind in der Galoistheorie nicht das Problem. Das Problem ist eher die positive Charakteristik, was im Allgemeinen nicht mehr die *Separabilität* garantiert, wie wir später sehen werden.

**Definition 3.9.11.** Sei $L/K$ eine algebraische Körpererweiterung. Eine Körpererweiterung $L'/L$ heißt **normale Hülle** von $L/K$, falls $L'/K$ normal und $L'/K$ minimal mit dieser Eigenschaft ist (d. h. falls $L'/L''/L$ mit $L''/K$ normal ist, dann folgt bereits $L'' = L'$).

**Satz 3.9.12.** *Sei $L/K$ eine algebraische Körpererweiterung. Dann existiert eine normale Hülle $L'/L/K$ von $L/K$ und diese ist eindeutig bis auf Isomorphie.*

*Beweis.* Wir zeigen nur die Existenz; Eindeutigkeit ist eine Aufgabe.

Wähle $A \subset L$, sodass $L = K(A)$. Für jedes $a \in A$ sei $p_a \in K[X]$ das Minimalpolynom von $a$. Sei $L'$ der Zerfällungskörper von $\{p_a \mid a \in A\}$. Dabei realisieren wir $L'$ im algebraischen Abschluss $\bar{K}/K$, welcher $K(A) = L$ enthält.[45]

*Behauptung:* $L'/L/K$ ist die normale Hülle von $L/K$.

*Beweis:* Es ist klar, dass $L'/K$ normal ist, denn es ist ein Zerfällungskörper. Auch ist klar, dass $L \subset L' \subset \bar{K}$, da $p_a(a) = 0$. Für die Minimalität betrachten wir $L \subset L'' \subset L'$ mit $L''/L$ normal. Für jedes $a \in A$ zerfällt dann $p_a \in K[X]$ in $L''[X]$ komplett in Linearfaktoren. Somit sind alle Nullstellen aller $p_a$ in $L''$ enthalten, also $L'' = L'$. □

[45] Das passiert sehr häufig in der Körpertheorie und ist wieder ein Fall von *abuse of notation*. Was wir meinen ist, dass wir statt $L$ als einen isomorphen Unterkörper von $\bar{K}$ betrachten.

**Bemerkung 3.9.13.**

(i) Seien $L/K$ eine endliche Körpererweiterung und $L'/L/K$ die normale Hülle. Dann ist auch $L'/K$ endlich.

Wir können nämlich im obigen Beweis $A$ endlich wählen, da $L/K$ endlich ist. Also ist $L'/K$ der Zerfällungskörper endlich vieler Polynome, d. h. insbesondere Zerfällungskörper eines Polynoms $f \in K[X]$ und damit endlich.[46]

(ii) Sei $M/L/K$ ein Turm von Körpererweiterungen, wobei $M/K$ normal ist. Dann existiert eine normale Hülle $L'/L/K$ von $L/K$, die in $M$ enthalten ist.

Wir können nämlich im Beweis $K \subset L \subset M \subset \bar{K}$ wählen, wobei $M/K$ normal ist. Wegen der Minimalität von $L'$ ist $L' \subset M$.

(iii) Sei $M/L/K$ ein Turm von Körpererweiterungen, wobei $M/K$ normal ist. Sei $S := \{\sigma\colon L \to M \mid \sigma|_K = \mathrm{id}_K\}$. Dann ist $L' = L(\{\sigma(L) \mid \sigma \in S\})$ eine normale Hülle von $L/K$ (Aufgabe 49).

## 3.10 Separable Körpererweiterungen

**Beobachtung 3.10.1.** *Wiederholung:* Sei $f \in K[X]$ ein normiertes Polynom und schreibe $f = \prod_{i=1}^{n}(X - \alpha_i) \in \bar{K}[X]$. Dann ist $f' = \sum_{i=1}^{n}\prod_{j=1,j\neq i}^{n}(X - \alpha_j)$. Wir sahen, dass $f'(\alpha_i) = \prod_{j=1,j\neq i}^{n}(\alpha_i - \alpha_j)$. Also ist $\alpha$ genau dann eine mehrfache Nullstelle von $f$, wenn $f(\alpha) = 0$ und $f'(\alpha) = 0$ (vgl. Beobachtung 3.8.6).

*Fazit:* $f$ hat genau dann eine mehrfache Nullstelle in $\bar{K}$, wenn $f$ und $f'$ eine gemeinsame Nullstelle in $\bar{K}$ besitzen.

**Korollar 3.10.2.** *Sei $f \in K[X]$ irreduzibel. Dann besitzt $f$ genau dann eine mehrfache Nullstelle in $\bar{K}$, wenn $f' = 0$ in $K[X]$.*

*Beweis.* Falls $f' = 0$ gilt, dann ist jede Nullstelle von $f$ bereits eine Nullstelle von $f'$ und damit eine mehrfache Nullstelle.

Falls umgekehrt $\alpha \in \bar{K}$ eine mehrfache Nullstelle von $f$ ist, ist $f'(\alpha) = 0$. Da $f$ irreduzibel ist, ist $f = p_\alpha \in K[X]$ das Minimalpolynom von $\alpha$, also $p_\alpha \mid f'$ in $K[X]$. Das ist aber ein Widerspruch, falls $f' \neq 0$, denn $\deg(f') < \deg(f)$. Also ist $f' = 0$. □

rem:multipleroot

itm:multipleroot:1

**Bemerkung 3.10.3.**

(i) Die Rückrichtung „$f' = 0$ *impliziert* $f$ *hat eine mehrfache Nullstelle*“ gilt auch ohne Irreduzibilität.

(ii) Falls ein irreduzibles Polynom $f \in K[X]$ eine mehrfache Nullstelle in $\bar{K}$ besitzt (also $f' = 0$), so sind *alle* Nullstellen von $f$ mehrfach (das folgt aus dem obigen Beweis).

[46] Ein paar Details: Da $L'$ Zerfällungskörper von $f$ ist, müssen wir nur endlich viele Nullstellen von $f$ adjungieren, die offenbar alle algebraisch über $K$ sind. Also ist $L'/K$ auch algebraisch und endlich erzeugt, also endlich.

(iii) Falls $\mathrm{char}(K) = 0$, dann folgt aus $f' = 0$ bereits $f \in K$, weshalb $f$ nicht irreduzibel sein kann. Also hat ein Polynom $f \in K[X]$ mit $\mathrm{char}(K) = 0$ nur einfache Nullstellen in $\bar{K}$.

**Definition 3.10.4.**

(i) Ein nichtkonstantes Polynom $f \in K[X]$ ist **separabel**, falls alle Nullstellen von $f$ in $\bar{K}$ einfach sind.

(ii) Seien $L/K$ eine Körpererweiterung und $a \in L$ algebraisch über $K$. Dann heißt $a$ separabel über $K$, falls sein Minimalpolynom $p_a \in K[X]$ **separabel** ist (oder äquivalent dazu $p_a' \neq 0$).

*Beispiel* 3.10.5. In Charakteristik null sind irreduzible Polynome bereits separabel. In positiver Charakteristik gilt das im Allgemeinen nicht. Betrachte $f = X^p + a \in \mathbb{F}_{p^n}[X]$. Das ist nicht separabel, da $f' = pX^{p-1} = 0$.

*Achtung:* Wir werden sehen, dass $f$ nicht irreduzibel ist, aber wegen Bemerkung 3.10.3 (i) hat $f$ trotzdem eine mehrfache Nullstelle in $\bar{\mathbb{F}}_p$.

thm:separable

**Satz 3.10.6.** *Sei $f \in K[X]$ irreduzibel.*

(i) *Falls $\mathrm{char}(K) = 0$, so ist $f$ separabel.*

(ii) *Angenommen. $\mathrm{char}(K) = p > 0$ Wähle $r$ maximal, sodass $f(X) = g(X^{p^r})$ für ein gewisses Polynom $g \in K[X]$. Für diese $g$ und $r$ gelten dann folgende Eigenschaften:*

(a) *Jede Nullstelle von $f$ in $\bar{K}$ hat Vielfachheit $p^r$.*

(b) *$g$ ist irreduzibel und separabel.*

(c) *Die Nullstellen von $f(X)$ in $\bar{K}$ sind dieselben wie die von $g(X^{p^r})$ in $\bar{K}$.*

*Beweis.*

(i) Das kennen wir schon.

(ii) (c) Das ist klar.

(b) Da $f$ irreduzibel ist, ist auch $g$ irreduzibel. Denn wäre $g = g_1 g_2$ mit nichtkonstanten $g_1, g_2 \in K[X]$, so ist $f(X) = g(X^{p^r}) = g_1(X^{p^r}) g_2(X^{p^r})$, d. h. $f$ ist nicht irreduzibel, ein Widerspruch.
Für die Separabilität nehmen wir $g' = 0$ an. Schreibe $g(X) = \sum_{i=0}^{n} a_i X^i$. Dann ist $g'(X) = \sum_{i=0}^{n} i a_i X^{i-1} = 0$, was genau dann der Fall ist, wenn $i a_i = 0$ für alle $i$ bzw. $a_i = 0$ für alle $i \not\equiv 0 \mod (p)$. Dann gilt $g(X) = h(X^p)$ mit $h(X) = \sum_{p|i} a_i X^{i/p}$.
Wir erhalten $f(X) = g(X^{p^r}) = h(X^{p^{r+1}})$, was der Maximalität von $r$ widerspricht. Also ist $g$ separabel.

(a) Schreibe $g(X) = \prod_{i=1}^{n} (X - \beta_i) \in \bar{K}[X]$. Da $g$ separabel ist, ist $\beta_i \neq \beta_j$ für alle $i \neq j$. Wähle $\alpha_i \in \bar{K}$ mit $\alpha_i^{p^r} = \beta_i$ für jedes $i$. In Charakteristik $p$ gilt dann mit dem Frobenius

$$f(X) = g(X^{p^r}) = \prod_{i=1}^{n} (X^{p^r} - \beta_i) = \prod_{i=1}^{n} (X^{p^r} - \alpha_i^{p^r}) = \prod_{i=1}^{n} (X - \alpha_i)^{p^r}$$

mit $\alpha_i \neq \alpha_j$ für alle $i \neq j$. Also haben alle Nullstellen $\alpha_i$ von $f$ Vielfachheit $p^r$. □

**Korollar 3.10.7.** *Seien $\mathbb{F}$ ein endlicher Körper und $f \in \mathbb{F}[X]$ irreduzibel. Dann ist $f$ separabel.*

VL 17
11.12.23

*Beweis.* Wir benutzen, dass der Frobenius $F\colon \mathbb{F} \to \mathbb{F}$, $a \mapsto a^p$ surjektiv ist. Wäre $f$ nicht separabel, so gilt $f = \sum_{i=0}^{n} a_i X^i = \sum_{p|i} a_i (X^{i/p})^p$. Da $F$ surjektiv ist, existieren $b_i \in \mathbb{F}$ mit $a_i = b_i^p$. Es folgt $f = \sum_{p|i} b_i^p (X^{i/p})^p = (\sum_{p|i} b_i X^{i/p})^p$, was der Irreduzibilität von $f$ widerspricht. □

*Beispiel* 3.10.8. Die Aussage gilt nicht mehr für unendliche Körper mit positiver Charakteristik. Betrachte den Körper $K = \mathbb{F}_p(t)$ der rationalen Funktionen in der Variablen $t$ mit Koeffizienten in $\mathbb{F}_p$. Bemerke, dass $\mathrm{char}(K) = p > 0$ und $K$ unendlich ist. Dann ist $f = X^p - t$ *inseparabel*, da $f' = pX^{p-1} = 0$. Wir sehen auch, dass $f$ keine Nullstelle in $K$ hat, und man kann zeigen, dass $f$ sogar irreduzibel ist.

**Definition 3.10.9.** Eine algebraische Körpererweiterung $L/K$ heißt **separabel** falls alle $a \in L$ separabel über $K$ sind.

**Bemerkung 3.10.10.**

(i) Falls $\mathrm{char}(K) = 0$, dann ist jede algebraische Körpererweiterung $L/K$ separabel.

(ii) Falls $|K| < \infty$, dann ist auch jede algebraische Körpererweiterung $L/K$ separabel.

Das wissen wir bereits, aber können das auch anders argumentieren. Sei $a \in L$ und betrachte die Körpererweiterung $K(a)/K$. Weil $K$ endlich ist und $K(a)/K$ endlich ist, gelten $K = \mathbb{F}_{p^n}$ und $K(a) = \mathbb{F}_{p^{mn}}$. Dann ist $a$ eine Nullstelle von $X^{p^{mn}} - X =: f$ mit $f' \neq 0$. Also ist $a$ separabel.

. Ausblick Folgende Definition ist für die Galoistheorie namensgebend: Eine algebraische Körpererweiterung $L/K$ heißt *galoissch*, falls sie normal und separabel ist.

*Beispiel* 3.10.11. $\bar{\mathbb{Q}}/\mathbb{Q}$ und $\mathbb{Q}(\mathrm{i})/\mathbb{Q}$ sind galoissch.

Nun zurück zu separablen Körpererweiterungen.

separable:extension

**Lemma 3.10.12.** *Sei $L/K$ eine Körpererweiterung, wobei $\mathrm{char}(K) = p > 0$. Dann ist ein Element $a \in L$ genau dann separabel über $K$, wenn $K(a) = K(a^p)$.*

*Beweis.* Wir machen einige Vorbemerkungen. Es gilt stets $K \subset K(a^p) \subset K(a)$. Seien $p_a \in K[X]$ das Minimalpolynom von $a$ über $K$ und $q_a \in K(a^p)[X]$ das Minimalpolynom von $a$ über $K(a^p)$. Dann ist $p_a(a) = q_a(a) = 0$, d. h. $q_a \mid p_a$ in $K(a^p)[X]$, sagen wir $p_a = q_a h$ für ein $h \in K(a^p)[X]$. Beobachte, dass $a$ eine Nullstelle von $X^p - a^p \in K(a^p)[X]$ ist und $X^p - a^p = (X-a)^p$ gilt. Da $q_a$ das Minimalpolynom ist, gilt $q_a \mid (X-a)^p$, woraus $q_a = (X-a)^k$ für ein $k \leq p$ folgt.

Nun zur Hinrichtung: Sei $a$ separabel über $K$. Dann ist $a$ eine einfache Nullstelle von $p_a$ und damit auch eine einfache Nullstelle von $q_a$. Also ist $k = 01$ und $a \in K(a^p)$.

Umgekehrt nehmen wir $K(a) = K(a^p)$ an. Wäre $a$ nicht separabel, dann ist $p_a$ nicht separabel. Im Sinne von Satz 3.10.6 können wir $p_a = \sum_{i=0}^{n} a_i X^i$ als $\sum_{p|i} a_i (X^p)^{i/p}$ schreiben.

Definiere $f \coloneqq \sum_{j=1}^{n/p} a_{jp} X^j \in K[X]$, sodass $f(a^p) = p_a(a) = 0$. Also gilt $p_{a^p} \mid f$ für das Minimalpolynom $p_{a^p}$ von $a^p$ über $K$. Wir erhalten

$$[K(a^p) : K] = \deg(p_{a^p}) \leq \deg(f) < \deg(p_a) = [K(a) : K].$$

Wegen $K(a) = K(a^p)$ gilt aber $[K(a^p) : K] = [K(a) : K]$, ein Widerspruch. Also war $a$ doch separabel. □

**Definition 3.10.13.** Ein Körper $K$ heißt **perfekt**, falls alle algebraische Körpererweiterungen $L/K$ separabel sind.

*Beispiel* 3.10.14. Jeder Körper $K$ mit Charakteristik null ist perfekt und jeder endliche Körper ist perfekt.

**Korollar 3.10.15.** *Ein Körper $K$ ist genau dann perfekt, wenn entweder $\operatorname{char}(K) = 0$, oder wenn $\operatorname{char}(K) = p > 0$ und der Frobenius $F\colon K \to K$, $a \mapsto a^p$ bijektiv ist.*

*Beweis.* Der Beweis funktioniert mit ähnlichen Argumenten zu vorhin. Da Körper der Charakteristik null bereits perfekt sind, können wir o. B. d. A. $\operatorname{char}(K) = p > 0$ annehmen.

Angenommen $K$ ist perfekt. Wir müssen zeigen, dass $F\colon K \xrightarrow{\sim} K$ bijektiv ist, d. h. $F$ surjektiv ist. Dazu sei $\alpha \in K$ und wir müssen $\alpha \in \operatorname{Im}(F)$ zeigen. Betrachte $K = K(\alpha) \subset K(\sqrt[p]{\alpha}) \subset \bar{K}$, wobei wir einen algebraischen Abschluss $\bar{K}$ fixieren. Definiere $a \coloneqq \sqrt[p]{\alpha}$, sodass $\alpha = a^p$. Weil $K$ perfekt ist, ist $a \in \bar{K}$ über $K$ separabel, und aus Lemma 3.10.12 folgt dann $K(a^p) = K(a)$, also $a \in K$. Somit gibt es ein $a \in K$ mit $a^p = F(a) = \alpha$.

Sei umgekehrt $L/K$ eine algebraische Körpererweiterung und sei $a \in L$. Angenommen $a$ ist nicht separable über $K$. Dann gilt für sein Minimalpolynom $p_a \in K[X]$ aufgrund der Surjektivität von $F$

$$p_a(X) = \sum_{p \mid i} a_i X^i = \sum_{p \mid i} b_i^p (X^{i/p})^p = \left( \sum_{p \mid i} b_i X^{i/p} \right)^p,$$

ein Widerspruch zur Irreduzibilität von $p_a$. □

. Wiederholung (Satz 3.9.2) Sei $L/K$ eine algebraische Körpererweiterung. Dann sind folgende Aussagen äquivalent:

(i) $L/K$ ist normal.

(ii) $L$ ist der Zerfällungskörper für eine Familie von Polynomen $\mathcal{F} \subset K[X]$.

(iii) Für alle Körperhomomorphismen $\varphi\colon L \to \bar{L}$ mit $\varphi|_K = \mathrm{id}$ gilt $\varphi(L) \subset L$.

Wir wollen gleich folgende Aussage zeigen.

hm:separable:degree

**Satz 3.10.16.** *Sei $L/K$ eine endliche Körpererweiterung. Dann sind folgende Aussagen äquivalent:*

:separable:degree:1

(i) *$L/K$ ist separabel.*

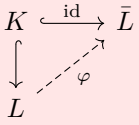
n:separable:degree:2

(ii) *$L/K$ ist **separabel erzeugt**, d. h. es gilt $L = K(A)$, wobei alle Elemente aus $A$ separabel über $K$ sind.*

n:separable:degree:3

(iii) *Für den Separabilitätsgrad gilt $[L : K]_s = [L : K]$.*

*Grob gesagt gibt es „genau richtig viele“ Fortsetzungen $\varphi$ von $\mathrm{id}\colon K \hookrightarrow L$:*




**Bemerkung 3.10.17.** Die Äquivalenz (i) $\iff$ (ii) gilt für alle algebraischen Körpererweiterungen $L/K$.

**Definition 3.10.18.** Sei $L/K$ eine algebraische Körpererweiterung. Dann ist der **Separabilitätsgrad** definiert als

$$[L : K]_S := |\{\varphi\colon L \longrightarrow \bar{K} \text{ Körperhomomorphismen} \mid \varphi|_K = \mathrm{id}\}|.$$

Wir bezeichnen die obige Menge mit $\mathrm{Hom}_K(L, \bar{K})$ und deren Elemente als **$K$-Homomorphismen** von $L$ nach $\bar{K}$.

bs:separable:degree

**Beobachtung 3.10.19.** Sei $L/K$ eine algebraische Körpererweiterung und fixiere ein $a \in L$.

(i) Sei $\varphi\colon L \to \bar{K}$ ein $K$-Homomorphismus und sei $p_a \in K[X]$ das Minimalpolynom von $a$. Dann ist $\varphi(a) \in \bar{K}$ wieder eine Nullstelle von $p_a$. Beschränken wir uns nun auf $\varphi\colon L = K(a) \to \bar{K}$, so ist die Abbildung eindeutig durch die Vorgabe einer Nullstelle von $p_a$ bestimmt. Damit ist $[K(a) : K]_S$ die Anzahl der Nullstellen von $p_a$ in $\bar{K}$ ohne Vielfachheiten und wir erhalten im Allgemeinen

$$[K(a) : K]_s \leq \deg(p_a) = [K(a) : K]$$

Allgemein gilt sogar $[L : K]_S \leq [L : K]$ (Aufgabe 50).

(ii) Wie in Satz 3.10.6 schreiben wir $p_a(X) = g(X^{p^r})$ mit $r$ maximal unter der Annahme, dass $\mathrm{char}(K) = p > 0$. Dann ist $g$ separabel und alle Nullstellen von $p_a$ haben Vielfachheit $p^r$. Also ist die Anzahl der Nullstellen von $p_a$ ohne Vielfachheiten die Anzahl der Nullstellen von $g$. In Formeln:

$$[K(a) : K]_S = \deg(g) = \deg(p_a)/p^r \implies [K(a) : K] = p^r [K(a) : K]_S.$$

(iii) Betrachte den Turm von Körpererweiterungen $K \subset K(a^{p^r}) \subset K(a)$. Dann ist $a^{p^r}$ eine Nullstelle von $g$ und $g$ ist das Minimalpolynom von $a^{p^r}$ über $K$. Weil $g$ separabel ist, gilt

$$\deg(g) = [K(a^{p^r}) : K] = [K(a^{p^r}) : K]_S.$$

Andererseits gilt $[K(a) : K(a^{p^r})] = 1$, da $a$ die einzige Nullstelle von $X^{p^r} - a^{p^r} = (X-a)^{p^r}$ ist. Wir erhalten

$$[K(a) : K]_S = [K(a^{p^r}) : K]_S [K(a) : K(a^{p^r})]_S,$$

was ein Spezialfall der allgemeinen Produktformel ist.

thm:tower:separable

**Satz 3.10.20.** *Sei $M/L/K$ ein Turm von algebraischen Körpererweiterungen. Dann gilt*

$$[M : K]_S = [M : L]_S \cdot [L : K]_S.$$

*Beweis.* Wähle einen gemeinsamen algebraisch Abschluss, sodass $K \subset L \subset M \subset \bar{K} = \bar{L} = \bar{M}$, und betrachte die Abbildung

$$f\colon \operatorname{Hom}_K(L, \bar{K}) \times \operatorname{Hom}_L(M, \bar{K}) \longrightarrow \operatorname{Hom}_K(M, \bar{K}), \quad (\sigma, \tau) \longmapsto [M \xrightarrow{\tau} \bar{K} \xrightarrow{\tilde{\sigma}} \bar{K}],$$

wobei wir für jeden $K$-Homomorphismus $\sigma\colon L \to \bar{K}$ eine Fortsetzung $\tilde{\sigma}\colon \bar{K} \to \bar{K}$ mit $\tilde{\sigma}|_L = \sigma$ fixieren. Dann ist $(\tilde{\sigma} \circ \tau)|_K = \tilde{\sigma}|_K \circ \tau|_K = \mathrm{id}_K \circ \mathrm{id}_K = \mathrm{id}_K$. Falls $f$ bijektiv ist, dann gilt die Produktformel

$$[L : K]_S [M : L]_S = |\operatorname{Hom}_K(L, \bar{K})| \cdot |\operatorname{Hom}_L(M, \bar{K})| = |\operatorname{Hom}_K(M, \bar{K})| = [M : K]_S.$$

Wir zeigen die Injektivität. Angenommen $(\sigma, \tau)$ und $(\sigma', \tau')$ liefern dieselbe Komposition $\tilde{\sigma} \circ \tau = \tilde{\sigma}' \circ \tau'$. Insbesondere gilt $(\tilde{\sigma} \circ \tau)|_L = (\tilde{\sigma}' \circ \tilde{\tau})|_L$. Wegen $\tau|_L = \tau'|_L = \mathrm{id}$ folgt $\sigma = \tilde{\sigma}|_L = \tilde{\sigma}'|_L = \sigma'$. Somit ist auch $\tau = \tau'$ und die Injektivität schließlich gezeigt. □

**Aufgabe 3.10.21.** Zeige die Surjektivität von $f$.

*Lösung.* Bemerke, dass alle $\tilde{\sigma}$ Isomorphismen sind, da, wie im Eindeutigkeitsbeweis von Korollar 3.7.17, $\tilde{\sigma}(\bar{K}) \simeq \bar{K}$ algebraisch abgeschlossen ist. Sei $\alpha \in \operatorname{Hom}_K(M, \bar{K})$. Dann ist $\sigma \coloneqq \alpha|_L \in \operatorname{Hom}_K(L, \bar{K})$. Ferner ist $\tau \coloneqq \tilde{\sigma}^{-1} \circ \alpha \in \operatorname{Hom}_L(M, \bar{K})$ und wir erhalten wie gewünscht $\tilde{\sigma} \circ \tau = \alpha$.

**Korollar 3.10.22.** *Sei $L/K$ eine endliche Körpererweiterung.*

(i) *Falls $\mathrm{char}(K) = 0$, dann gilt $[L : K] = [L : K]_S$.*

(ii) *Falls $\mathrm{char}(K) = p > 0$, dann gilt $[L : K] = [L : K]_S \cdot p^r$ für ein gewisses $r$.*

*Beweis.* Schreibe $L/K$ als $K \subset K(a_1) \subset K(a_1, a_2) \subset \cdots \subset L = K(a_1, \ldots, a_n)$. Mithilfe der Produktformeln 3.10.20 und 3.5.8 und Beobachtung 3.10.19 folgt die Aussage per Induktion. □

Folgende Folgerung benutzt auch Satz 3.10.16.

cor:separable:tower

**Korollar 3.10.23.** *Sei $M/L/K$ ein Turm von endlichen Körpererweiterungen. Dann ist $M/K$ genau dann separabel, wenn $M/L$ und $L/K$ beide separabel sind.*

. Erinnerung Für Normalität haben wir nur: Ist $M/K$ normal, so ist $M/L$ normal.

*Beweis von Korollar 3.10.23.* Mithilfe der Produktformeln 3.5.8 und 3.10.20 haben wir

$$[M : K] = [M : L][L : K], \qquad [M : K]_S = [M : L]_S[L : K]_S.$$

Nach Aufgabe 50 ist für jede Körpererweiterung der Separabiltitäsgrad höchstens dessen Grad. Gilt dabei Gleichheit von Separabilitätsgrad und Grad auf einer Seite der Gleichungen, so muss sie auch auf der anderen Seite gelten. □

*Beweis von Satz 3.10.16.*

- (i) $\implies$ (ii): Wähle $A = L$.
- (ii) $\implies$ (iii): Sei $L = K(A)$, wobei $A$ aus Elementen besteht, die separabel über $K$ sind. Da $L/K$ endlich ist, sei o. B. d. A. $|A| < \infty$, sagen wir $A = \{a_1, \dots, a_n\}$. Wir erhalten den Turm

  $$K \subset K(a_1) \subset K(a_1, a_2) \subset \cdots \subset K(a_1, a_2, \dots, a_n) = L.$$

  Jedes $a_i$ ist separabel über $K$ und damit separabel über $K(a_1, \dots, a_{i-1})$. Wir erhalten also

  $$[K(a_1, \dots, a_i) : K(a_1, \dots, a_{i-1})] = [K(a_1, \dots, a_i) : K(a_1, \dots, a_{i-1})]_S.$$

  Die Produktformeln 3.5.8 und 3.10.20 beweist $[L : K] = [L : K]_S$.
- (iii) $\implies$ (i): Sei $a \in L$. Zu zeigen ist, dass $a$ separabel über $K$ ist. Wir wissen, dass $a$ genau dann separabel über $K$ ist, wenn $[K(a) : K] = [K(a) : K]_S$. Mit den Produktformeln 3.5.8 und 3.10.20 für $K \subset K(a) \subset L$ folgt

  $$[L : K(a)][K(a) : K] = [L : K] = [L : K]_S = [L : K(a)]_S[K(a) : K]_S.$$

  Wegen $[L : K(a)]_S \leq [L : K(a)]$ und $[K(a) : K]_S \leq [K(a) : K]$ folgt sodann die Gleichheit dieser Ungleichungen. Also ist $a$ separabel über $K$. □

**Korollar 3.10.24.** *Sei $f \in K[X]$ irreduzibel und sei $L$ der Zerfällungskörper von $f$. Dann ist $L/K$ genau dann separabel, wenn $f$ separabel ist.*

*Beweis.* Wenn $f$ separabel über $K$ ist, so sind alle Nullstellen von $f$ separabel über $K$. Da $L$ durch die Adjunktion von Nullstellen von $f$ entsteht, ist $L/K$ separabel erzeugt und nach Satz 3.10.16 ist $L/K$ separabel. Die Umkehrung ist trivial. □

hm:primitiveelement

**Satz 3.10.25 (Satz über das primitive Element).** *Sei $L/K$ eine endliche separable Körpererweiterung. Dann existiert ein $a \in L$, sodass $L = K(a)$. Das Element $a$ heißt dann **primitives Element**.*

VL 18
15.12.23

*Beweis.* Angenommen $K$ ist ein endlicher Körper. Dann ist auch $L$ ein endlicher Körper und $L^*$ ist eine endliche zyklische Gruppe, sagen wir $L^* = \langle a \rangle$ für ein $a \in L$. Dann gilt bereits $L = K(a)$ und wir sind fertig.

Sei andererseits $K$ unendlich. Da $L/K$ endlich ist, existieren $a_1, \dots, a_n \in L$, sodass

$$K \subset K(a_1) \subset K(a_1, a_2) \subset \cdots \subset K(a_1, \dots, a_n) = L.$$

Da $L/K$ separabel ist, sind auch $K(a_1,\dots,a_i)/K(a_1,\dots,a_{i-1})$ für alle $i$ separabel. Aufgrund Induktion genügt es zu zeigen, dass wenn $L = K(a_1,a_2)/K$ separabel ist, es dann ein $a \in L$ mit $L = K(a)$ gibt.

Da $L/K$ separabel ist, gilt $[L:K]_S = [L:K] =: d$. Also existieren $d$ viele paarweise verschiedene Einbettungen $\sigma_1,\dots,\sigma_d\colon L \hookrightarrow \bar{K}$. Setze

$$F(X) \coloneqq \prod_{i\neq j}(\sigma_i(a_1)-\sigma_j(a_1)+(\sigma_i(a_2)-\sigma_j(a_2))X) \in K[X].$$

*Behauptung:* $F(X) \neq 0$.
*Beweis:* Wäre $F(X)=0$, so gibt es $i \neq j$ mit

$$\sigma_i(a_1)-\sigma_j(a_1)+(\sigma_i(a_2)-\sigma_j(a_2))X = 0.$$

Von diesem linearen Polynom müssen die Koeffizienten null sein, d. h. $\sigma_i(a_1)=\sigma_j(a_1)$ sowie $\sigma_i(a_2)=\sigma_j(a_2)$. Da $L = K(a_1,a_2)$, folgt daraus $\sigma_i = \sigma_j$, ein Widerspruch. Das zeigt die Behauptung.

Jedes Polynom ungleich null hat höchstens endlich viele Nullstellen. Da $K$ unendlich ist, existiert ein $\alpha \in K$ mit $F(\alpha) \neq 0$.

*Behauptung:* $a \coloneqq a_1 + \alpha a_2$ ist ein primitives Element von $L/K$.
*Beweis:* Es gilt $\sigma_i(a) \neq \sigma_j(a)$ für alle $i \neq j$, denn

$$\begin{aligned}
F(\alpha) &= \prod_{i\neq j}(\sigma_i(a_1)-\sigma_j(a_1)+(\sigma_i(a_2)-\sigma_j(a_2))\alpha) \\
&= \prod_{i\neq j}(\sigma_i(a_1)-\sigma_i(a_2)\alpha-(\sigma_j(a_1)+\sigma_j(a_2)\alpha)) \\
&= \prod_{i\neq j}(\sigma_1(a_1+a_2\alpha)-\sigma_j(a_1+\alpha a_2)) \\
&= \prod_{i\neq j}(\sigma_i(a)-\sigma_j(a)) \neq 0.
\end{aligned}$$

Sei $p_a \in K[X]$ das Minimalpolynom von $a$ über $K$. Wir wissen, dass $p_a(a)=0$, und wegen $\sigma_i|_K = \mathrm{id}$ ist $p_a(\sigma_i(a))=0$. Aufgrund Separabilität hat $p_a$ also mindestens $d$ verschiedene Nullstellen in $\bar{K}$. Es folgt $[K(a):K] = \deg(p_a) \geq d = [L:K]$. Da aber $K \subset K(a) \subset L$ ist, erhalten wir $L = K(a)$. □

**Bemerkung 3.10.26.** Der Beweis zeigt, dass falls $K$ endlich ist, es dann nur endlich viele primitive Elemente gibt.

**Fakt 3.10.27** (Aufgabe 55)**.** *Sei $L/K$ eine algebraische Körpererweiterung. Dann ist $L/K$ genau dann **einfach** (d. h. es gibt ein $a \in L$ mit $L = K(a)$), falls es endlich viele Zwischenkörper gibt.*

**Satz 3.10.28.** *Sei $L/K$ eine algebraische Körpererweiterung, sodass jedes $f \in K[X]$ mit $\deg(f) > 0$ eine Nullstelle von $f$ in $L$ hat. Dann ist $L$ algebraisch abgeschlossen (und weil $L/K$ algebraisch ist, folgt $L = \bar{K}$).*

*Teilbeweis. Behauptung:* Sei $L/K$ eine beliebige Körpererweiterung, sodass jedes $f \in K[X]$ mit $\deg(f) > 0$ eine Nullstelle in $L$ existiert. Dann zerfällt jedes $f \in K[X]$ in Linearfaktoren in $L[X]$.

Wenn diese Behauptung gilt, dann können wir den Beweis wie folgt beenden. Sei $\bar{K}/L/K$ ein Turm von Körpererweiterungen mit $L/K$ algebraisch. Sei $a \in \bar{K}$ und sei $p_a \in K[X]$ das Minimalpolynom von $a$. Nach Voraussetzung hat $p_a$ eine (ggf. andere) Nullstelle in $L$ und nach der Behauptung liegen alle Nullstellen (also insbesondere $a$) auch in $L$. Wir schließen $L = \bar{K}$ und wir sind fertig.

*Beweis der Behauptung:* Wir zeigen die Aussage nur, falls $L/K$ separabel ist. Sei $f \in K[X]$ mit $\deg(f) > 0$; o. B. d. A. sei $f$ irreduzibel. Sei $K'$ der Zerfällungskörper von $f$. Da nach Voraussetzung $f$ eine Nullstelle in $L$ besitzt und $L/K$ separabel ist, sind $f$ und $K'/K$ separabel. Nach dem Satz über das primitive Element 3.10.25 existiert ein $a \in K'$, sodass $K' = K(a)$. Auch das Minimalpolynom $p_a \in K[X]$ von $a$ besitzt nach Voraussetzung eine Nullstelle $b \in L$. Wir erhalten $K' = K(a) \simeq K[X]/(p_a) = K[X]/(p_b) \simeq K(b)$ (hier verwenden wir $p_a = p_b$). Weil $K'/K$ als Zerfällungskörper normal ist, ist auch $K(b)/K$ normal, weshalb auch $a \in K(b) \subset L$. Also gilt $K' = K(a) \subset K(b) \subset L$ und alle Nullstellen von $f$ liegen in $L$.

*Hinweis:* Die Behauptung gilt auch für inseparable Körpererweiterungen, was wir nicht zeigen werden.[47] □

# 4 Galoistheorie

sec:galois

## 4.1 Galoiserweiterungen

**Definition 4.1.1.** Eine algebraische Körpererweiterung $L/K$ heißt **galoissch**,[48] falls $L/K$ separabel und normal ist. Für uns sind die Galoiserweiterungen $L/K$ fast immer endlich.

*Beispiel* 4.1.2.

(i) Für $\mathrm{char}(K) = 0$ ist $\bar{K}/K$ galoissch, z. B. $\bar{\mathbb{Q}}/\mathbb{Q}$ oder $\mathbb{C}/\mathbb{R}$.

(ii) Für $\mathrm{char}(K) > 0$ ist der *separable Abschluss* $K_S/K$ galoissch (Aufgabe 53).

(iii) Ist $K$ perfekt, so ist $\bar{K}/K$ galoissch.

(iv) Ist $L$ der Zerfällungskörper eines separablen Polynoms $f \in K[X]$, so ist $L/K$ galoissch.

(v) Ist $K = \mathbb{F}_{p^n}$ endlich, so ist jede Körpererweiterung $L/K$ galoissch.

[47] Der Satz ist als Übungsaufgabe in [Bos, 3.7/Aufg. 10] gelistet. Die Behauptung im Speziellem ist meinen Recherchen nach zum ersten Mal in [Gil] bewiesen worden. Nach dem separablen Fall darf man o. B. d. A. $\mathrm{char}(K) = p > 0$ annehmen. Dann wird $K$ um einen etwas größeren Körper $K_0$ erweitert, sodass $K_0/K$ *rein inseparabel* ist. Dann lässt sich zeigen, dass $K_0$ perfekt ist, und die Behauptung gilt somit auch in diesem Fall.

bib:bos
bib:gil

[48] Der Dozent verwendet den Begriff *Galois*, aber ich bleibe der deutschen Rechtschreibung treu und adjektiviere Galois zu *galoissch*, vlg. Abel und *abelsch*, Descartes und *kartesisch*, usw.

(vi) $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}$ ist separabel, aber nicht normal und damit nicht galoissch. Betrachte insbesondere den Turm $\mathbb{Q} \subset \mathbb{Q}(\sqrt{2}) \subset \mathbb{Q}(\sqrt[4]{2})$. Die Teilkörpererweiterungen $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ und $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}(\sqrt{2})$ sind galoissch, aber $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}$ ist nicht normal, denn $X^4 - 2$ besitzt eine Nullstelle $\mathrm{i}\sqrt[4]{2} \notin \mathbb{Q}(\sqrt[4]{2})$.

(vii) $\mathbb{F}_p(t)/\mathbb{F}_p(t^p)$ ist nicht separabel und damit nicht galoissch.

**Definition 4.1.3.**

(i) Sei $L$ ein Körper. Dann bezeichnet $\mathrm{Aut}(L)$ die *Gruppe* aller Körperhomomorphismen $\varphi\colon L \xrightarrow{\sim} L$.

(ii) Sei eine Körpererweiterung $L/K$ gegeben. Dann ist $\mathrm{Aut}_K(L) \subset \mathrm{Aut}(L)$ die Untergruppe aller $\varphi\colon L \xrightarrow{\sim} L$ mit $\varphi|_K = \mathrm{id}_K$.

Falls $L/K$ galoissch ist, heißt diese Gruppe **Galoisgruppe** und wir schreiben $\mathrm{Gal}(L/K) \coloneqq \mathrm{Aut}_K(L)$.

(iii) Ist $L$ der Zerfällungskörper eines separablen Polynoms $f \in K[X]$, so ist $L/K$ galoissch. Wir schreiben $\mathrm{Gal}(f) \coloneqq \mathrm{Gal}(L/K)$ für die Galoisgruppe.

Die Idee der Galoistheorie ist es, Körpererweiterungen $L/K$ mittels $\mathrm{Gal}(L/K)$ durch Gruppentheorie zu studieren. Historisch gesehen ist $L$ meist ein Zerfällungskörper. Die Frage lautet dann: Lassen sich alle Nullstellen von $f$ durch *Radikale* beschreiben?

**Definition 4.1.4.** Seien $L/K$ eine Körpererweiterung und $G \subset \mathrm{Aut}_K(L)$ eine Untergruppe (oder Teilmenge). Setze

$$L^G \coloneqq \{a \in L \mid \sigma(a) = a \text{ für alle } \sigma \in G\}.$$

Offenbar ist $K \subset L^G \subset L$ ein Zwischenkörper. (Z. B. falls $\sigma(a_i) = a_i$, dann

$$\sigma(a_1 + a_2) = \sigma(a_1) + \sigma(a_2) \qquad \text{und} \qquad \sigma(a_1 a_2) = \sigma(a_1)\sigma(a_2)$$

für alle $\sigma \in \mathrm{Aut}_K(L)$.) Wir nennen $L^G$ den **Fixkörper** von $L$ unter $G$.

obs:galois

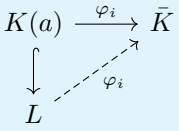
**Beobachtung 4.1.5.** *Wiederholung:* Seien $L/K$ eine Körpererweiterung und $a \in L$ algebraisch über $K$. Für das Minimalpolynom $p_a$ von $a$ über $K$ gelten dann $K(a) \simeq K[X]/(p_a)$ und $[K(a) : K] = \deg(p_a)$.

itm:galois:1 (i) Sei $\varphi\colon L \hookrightarrow \bar{K}$ ein $K$-Körperhomomorphismus mit $\varphi|_K = \mathrm{id}_K$. Dann ist auch $\varphi(a)$ eine Nullstelle von $p_a$. Ist $L/K$ normal, so folgt $\varphi(a) \in L$.

itm:galois:2 (ii) Falls $L/K$ separabel ist, so ist auch $K(a)/K$ separabel. Dann existieren $n \coloneqq \deg(p_a)$ paarweise verschiedene $K$-Homomorphismen $\varphi_1, \ldots, \varphi_n\colon K(a) \hookrightarrow \bar{K}$ (d. h. $\varphi_i(a) \neq \varphi_j(a)$ für $i \neq j$) mit $\varphi_i|_K = \mathrm{id}_K$.

itm:galois:3 (iii) Sei nun $L/K$ (endlich) galoissch. Dann existieren $n$ paarweise verschiedene Fortsetzungen $\varphi_1, \ldots, \varphi_n \in \mathrm{Gal}(L/K)$ mit $\varphi_i(a) \neq \varphi_j(a)$ für alle $i \neq j$. Nach (ii) können

wir nämlich $\varphi_i\colon K(a) \to \bar{K}$ fortsetzen:




Nach (i) ist $\varphi_i(L) = L$.

lem:galois:normal

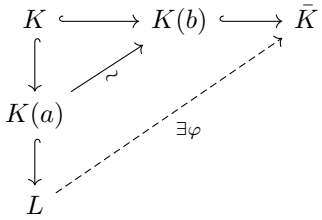
**Lemma 4.1.6.** *Sei $L/K$ eine algebraische Körpererweiterung. Dann ist $L/K$ genau dann normal, wenn $\mathrm{Aut}_K(L) = \mathrm{Hom}_K(L, \bar{K} = \bar{L})$.*

*Beweis.* Angenommen $L/K$ ist normal. Offenbar ist $\mathrm{Aut}_K(L) \subset \mathrm{Hom}_K(L, \bar{K} = \bar{L})$, denn für jedes $\varphi \in \mathrm{Aut}_K(L)$ ist $\varphi\colon L \xrightarrow{\sim} L \subset \bar{L}$ und $\varphi|_K = \mathrm{id}_K$.

Für die umgekehrte Inklusion sei $\varphi\colon L \hookrightarrow \bar{L}$ mit $\varphi|_K = \mathrm{id}_K$ gegeben. Wegen der Normalität von $L/K$ gilt $\varphi(L) \subset L$. (Falls $L/K$ endlich ist, gilt $\varphi(L) = L$.) Sei $a \in L$ mit Minimalpolynom $p_a \in K[X]$. Da $L/K$ normal ist, ist der Zerfällungskörper $Z$ von $p_a$ in $L$ enthalten. Also gilt $\varphi(Z) \subset Z$. Weil $Z/K$ eine endliche normale Körpererweiterung ist, folgt $\varphi(Z) = Z$. Daher ist $a \in \varphi(Z) \subset \mathrm{Im}(\varphi)$ und $\varphi$ ist surjektiv auf $L$.

Für die Rückrichtung sei $\mathrm{Aut}_K(L) = \mathrm{Hom}_K(L, \bar{L})$. Sei $a \in L$ mit Minimalpolynom $p_a \in K[X]$. Zu zeigen ist, dass der Zerfällungskörper $Z$ von $p_a$ in $L$ liegt (d. h. $L/K$ ist normal). Sei $b \in \bar{K}$ eine Nullstelle von $p_a$. Wir müssen also $b \in L$ zeigen.

Wir wissen, dass $K(a) \simeq K[X]/(p_a) = K[X]/(p_b) \simeq K(b)$ wegen $p_a = p_b$. Da $L/K$ algebraisch und $\bar{K}$ algebraisch abgeschlossen ist, existiert eine Fortsetzung $\varphi\colon L \to \bar{K}$ mit $\varphi(a) = b$, sodass folgendes Diagramm kommutiert:




Damit ist $\varphi \in \mathrm{Hom}_K(L, \bar{K}) = \mathrm{Aut}_K(L)$, weshalb $b = \varphi(a) \in L$. □

**Bemerkung 4.1.7.** Die Hinrichtung im obigen Beweis zeigt, dass wir in Beobachtung 4.1.5 (iii) die Voraussetzung der Endlichkeit von $L/K$ streichen können.

**Lemma 4.1.8.** *Seien $L/K$ eine normale Körpererweiterung und $G \coloneqq \mathrm{Aut}_K(L)$. Dann ist $L/L^G$ eine normale und separabel Körpererweiterung.*

*Beweis.* Wir wissen bereits, dass $L/L^G$ normal ist. (Nach Voraussetzung ist $L$ der Zerfällungskörper einer gewissen Teilmenge $\mathcal{F} \subset K[X] \subset L^G[X]$. Somit ist auch $L/L^G$ normal.)

Zu zeigen ist, dass $L/L^G$ separabel ist. Dazu sei $a \in L$ mit Minimalpolynom $p_a \in L^G[X]$. Schreibe $p_a = \prod_{i=1}^{n}(X - \alpha_i)^{n_i} \in L[X]$, wobei $\alpha_i \neq \alpha_j$ für alle $i \neq j$. Dann ist $a$ genau

dann separabel über $L^G$, wenn $n_i = 1$ für alle $i$. Sei $\varphi \in \mathrm{Aut}_{L^G}(L) = \mathrm{Aut}_K(L)$, wobei die Gleichheit aus der Definition von $L^G$ folgt. Klar ist $\varphi(\{\alpha_i\}) = \{\alpha_i\}$, d. h. $\varphi|_{\{\alpha_i\}} \in \mathrm{Bij}(\{\alpha_i\})$. Dann sind die Koeffizienten des Polynoms $g(X) \coloneqq \prod_{i=1}^n (X - \alpha_i)$ (bis auf Vorzeichen) die symmetrischen Polynome in den $\alpha_i$. Z. B. ist $\pm\prod_{i=1}^n \alpha_i$ der konstante Koeffizient und $\pm\sum_{i=1}^n \alpha_i$ der Koeffizient von $X^{n-1}$. Die Koeffizienten von $g$ sind invariant unter allen $\varphi \in G$, d. h. sie sind in $L^G$. Also ist $g(X) \in L^G[X]$ und $g(\alpha_i) = 0$ für alle $\alpha_i$. Es folgt $g(a) = 0$ und daher $p_a \mid g$. Somit ist $p_a = g$, d. h. $n_i = 1$ für alle $i$. □

Hier einfache Fakten, die später Teil des Hauptsatzes der Galoistheorie werden. VL 19 18.12.23

fact:galoisgroup

itm:galoisgroup:1

**Fakt 4.1.9.**

(i) *Seien $L/K$ eine Galoiserweiterung und $G \coloneqq \mathrm{Gal}(L/K)$. Dann ist $K = L^G$.*

(ii) *Sei $L/K$ eine endliche Galoiserweiterung. Dann gilt*

$$|\mathrm{Gal}(L/K)| = [L : K]_S = [L : K].$$

(iii) *Sei $L/L'/K$ ein Turm von Körpererweiterungen mit $L/K$ galoissch. Dann ist $L/L'$ galoissch und $\mathrm{Gal}(L/L') \subset \mathrm{Gal}(L/K)$ ist eine Untergruppe.*

(iv) *Seien $L/K$ eine Galoiserweiterung und $G \coloneqq \mathrm{Gal}(L/K)$. Dann ist*

$$\{\text{Türme } L/L'/K\} \hookrightarrow \{\text{Untergruppen } H \subset G\}, \qquad L' \longmapsto \mathrm{Gal}(L/L')$$

*eine Injektion.*

*Beweis.*

(i) Per Definition ist $K \subset L^G$. Um $L^G \subset K$ zu zeigen, sei $a \in L$ mit $n \coloneqq \deg(a) \coloneqq \deg(p_a)$. Nach Beobachtung 4.1.5 gibt es $K$-Automorphismen $\varphi_1, \dots, \varphi_n \in G$ mit $\varphi_i(a) \neq \varphi_j(a)$ für $i \neq j$. Wenn jetzt $a \in L^G$, dann $\varphi_i(a) = \varphi_j(a)$ für alle $i \neq j$. Folglich ist $n = 1$ und $a \in K$.

(ii) Das folgt durch

$$[L : K] = [L : K]_S \coloneqq |\{\varphi \colon L \longrightarrow \bar{K} \mid \varphi|_K = \mathrm{id}\}| = |\mathrm{Hom}_K(L, \bar{K})| = |\mathrm{Gal}(L/K)|.$$

Dabei gilt die erste Gleichheit, da $L/K$ endlich separabel ist, und die letzte Gleichheit, weil $L/K$ normal ist (Lemma 4.1.6).

(iii) Weil $L/K$ galoissch ist, ist es normal und separabel. Das bedeutet, dass $L/K$ normal erzeugt (d. h. durch Adjunktion on Nullstellen von Polynomen entsteht) und separabel erzeugt (d. h. durch Adjunktion von separablen Elementen) ist. Insbesondere ist auch $L/L'$ normal und separabel erzeugt, und damit ist $L/L'$ Galois.

Der Gruppenhomomorphismus $\mathrm{Gal}(L/L') \hookrightarrow \mathrm{Gal}(L/K)$ ist gegeben durch $\varphi \mapsto \varphi$, die einen $L'$-Automorphismus $\varphi \colon L \xrightarrow{\sim} L$ (also $\varphi|_{L'} = \mathrm{id}$) als $K$-Automorphismus (also $\varphi|_K = \mathrm{id}$) interpretiert, da $K \subset L'$.

(iv) Sei $L/L'/K$ ein Zwischenkörper und sei $H \coloneqq \mathrm{Gal}(L/L')$. Dann gilt $L' = L^H$ nach (i) und $L/L'/K$ ist bereits eindeutig durch $H$ bestimmt. □

**Warnung 4.1.10.** Sei $f \in K[X]$ separabel und sei $L/K$ der Zerfällungskörper von $f$. Dann gibt es nach dem Satz über das primitive Element 3.10.25 ein primitives Element $a \in L$, sodass $L = K(a)/K$. Im Allgemeinen wird $a$ aber keine Nullstelle von $f$ sein. Tatsächlich ist im Allgemeinen keine Nullstelle von $f$ primitives Element von $L/K$.

**Beobachtung 4.1.11.** Sei $f \in K[X]$ separabel und sei $L/K$ der Zerfällungskörper von $f$. Sei $a \in L$ ein primitives Element mit Minimalpolynom $p_a \in K[X]$. Wir wissen dann

$$[K(a) : K] = \deg(a) = \deg(p_a) = [L : K] = |\mathrm{Gal}(f)|,$$

wobei die letzte Gleichheit aus Fakt 4.1.9 folgt.

*Frage:* Wie verhalten sich $|\mathrm{Gal}(f)|$ und $\deg(f)$ zueinander? Im Allgemeinen haben wir keine Gleichheit.

*Konstruktion:* Sei $f \in K[X]$ ein separables Polynom vom Grad $\deg(f) = n$ und seien $a_1, \dots, a_n \in \bar{K}$ die Nullstellen von $f$ in einem gewählten algebraischen Abschluss. Sei $L \coloneqq K(a_1, \dots, a_n)$ der Zerfällungskörper von $f$. Dann gibt es einen Gruppenhomomorphismus

$$\mathrm{Gal}(f) = \mathrm{Gal}(L/K) = \mathrm{Gal}(K(a_1, \dots, a_n)/K) \hookrightarrow \mathrm{Bij}\{a_1, \dots, a_n\}, \quad \varphi \longmapsto \varphi|_{\{a_1,\dots,a_n\}}.$$

Diese Abbildung ist injektiv, aber im Allgemeinen kein Isomorphismus. Man erinnere sich, dass $\mathrm{Bij}\{a_1, \dots, a_n\} \simeq S_n$ die symmetrische Gruppe ist.

**Korollar 4.1.12.** *Sei $f \in K[X]$ ein separables Polynom vom Grad $n$. Dann gelten:*

(i) $|\mathrm{Gal}(f)| \mid n!$.

(ii) *Falls $f$ irreduzibel ist,*[49] *dann operiert* $\mathrm{Gal}(f)$ *transitiv auf der Menge der Nullstellen $\{a_1, \dots, a_n\}$ von $f$, d. h. für alle $i$ und $j$ gibt es ein $\sigma \in \mathrm{Gal}(f)$ mit $\sigma(a_i) = a_j$.*

(iii) *Es gilt $|\mathrm{Gal}(f)| = n!$ genau dann, wenn $\mathrm{Gal}(f) \simeq S_n$.*

(iv) *Falls $f$ irreduzibel ist,*[50] *gilt $\deg(f) \leq |\mathrm{Gal}(f)|$ mit Gleichheit genau dann, wenn $a_2, \dots, a_n \in K(a_1)$.*

*Beweis.*

(i) Das folgt mit dem Satz von Lagrange 1.2.15.

(ii) Sei $L = K(a_1, \dots, a_n)$ der Zerfällungskörper von $f$. Es gilt $K(a_i) \simeq K[x]/(f) \simeq K(a_j)$. Wir können diesen Isomorphismus aufgrund Normalität von $L/K$ zu einem $K$-Automorphismus $\sigma\colon L \xrightarrow{\sim} L$ fortsetzen mit $\sigma(a_i) = a_j$.

(iii) Trivial.

(iv) Wir haben
$$\deg(f) = [K(a_1) : K] \leq [K(a_1, \dots, a_n) : K] = |\mathrm{Gal}(f)|.$$
Der Gleichheitsfall ist klar. □

[49] Das hat der Dozent vergessen!
[50] Das hat der Dozent auch vergessen!

*Problem* 4.1.13. Für irreduzible und separable $f \in K[X]$ wissen wir, dass $\mathrm{Gal}(f) \subset S_n$ eine Untergruppe ist. Welche Elemente von $S_n$ liegen aber in $\mathrm{Gal}(f)$?

oisgroup:quadratic

*Beispiel* 4.1.14. Sei $f \in K[X]$ mit $\deg(f) = 2$; o. B. d. A. sei $f = X^2 + a_1X + a_0$. Dann sind $\{\alpha_1, \alpha_2\} \subset \bar{K}$ die Nullstellen von $f$. Wir erhalten $X^2 + a_1X + a_0 = (X - \alpha_1)(X - \alpha_2)$ mit $a_0 = \alpha_1\alpha_2$ und $a_1 = -(\alpha_1 + \alpha_2)$.

Nun ist $f$ genau dann separabel, wenn $\alpha_1 \neq \alpha_2$. Ferner ist $f$ genau dann irreduzibel, wenn $\alpha_1 \notin K$ bzw. $\alpha_2 \notin K$. Der Zerfällungskörper von $f$ ist $K(\alpha_1) = K(\alpha_2)$. Falls also $\alpha_1 \neq \alpha_2$ gilt, d. h. falls $f$ separabel ist, erhalten wir

$$\mathrm{Gal}(f) \simeq \begin{cases} \{1\}, & \text{falls } f \text{ nicht irreduzibel ist,} \\ \mathbb{Z}/2\mathbb{Z}, & \text{falls } f \text{ irreduzibel ist.} \end{cases}$$

Das stimmt mit unserem Wissen $\mathrm{Gal}(f) \subset S_2 \simeq \mathbb{Z}/2\mathbb{Z}$ überein.

*Beispiel* 4.1.15. Sei $f \in K[X]$ mit $\deg(f) = 3$; o. B. d. A. sei

$$f = X^3 + a_2X^2 + a_1X + a_0.$$

Seien $\{\alpha_1, \alpha_2, \alpha_3\} \subset \bar{K}$ die Nullstellen von $f$ in einem fixierten algebraischen Abschluss. Dann gilt

$$f = (X - \alpha_1)(X - \alpha_2)(X - \alpha_3) \in \bar{K}[X].$$

Angenommen $f$ ist separabel, d. h. $\alpha_i \neq \alpha_j$ für alle $i \neq j$. Wir betrachten zwei Fälle.

(i) $f$ ist nicht irreduzibel. Dann gibt es ein $i$, sodass $\alpha_i \in K$; o. B. d. A. sei $i = 1$. Dann ist $K = K(\alpha_1) \subset K(\alpha_1, \alpha_2, \alpha_3)$, wobei $K(\alpha_1, \alpha_2, \alpha_3)$ der Zerfällungskörper von $f$, aber auch von $f/(X - \alpha_1) \in K[X]$ ist. Da $f/(X - \alpha_1)$ quadratisch ist, können wir diesen Fall auf Beispiel 4.1.14 zurückführen. Es gilt

$$\mathrm{Gal}(f) \simeq \begin{cases} \{1\}, & \text{falls } \alpha_1, \alpha_2 \in K, \\ \mathbb{Z}/2\mathbb{Z}, & \text{falls } \alpha_1 \in K \text{ und } \alpha_2 \notin K. \end{cases}$$

(ii) $f$ ist irreduzibel. Betrachte den Turm $K \subset K(\alpha_1) \subset K(\alpha_1, \alpha_2, \alpha_3)$, wobei $K(\alpha_1)/K$ Grad 3 hat. Beobachte wieder, dass $K(\alpha_1, \alpha_2, \alpha_3)$ Zerfällungskörper des quadratischen Polynoms $f/(X - \alpha_1) \in K(\alpha_1)[X]$ ist. Folglich ist nach Beispiel 4.1.14

$$[K(\alpha_1, \alpha_2, \alpha_3) : K(\alpha_1)] = \begin{cases} 1, & \text{falls } \alpha_2, \alpha_3 \in K(\alpha_1), \\ 2, & \text{falls } \alpha_2 \notin K(\alpha_1). \end{cases}$$

Wir erhalten

$$|\mathrm{Gal}(f)| = [K(\alpha_1, \alpha_2, \alpha_3) : K] = \begin{cases} 3, & \text{falls } \alpha_2 \in K(\alpha_1), \\ 6, & \text{falls } \alpha_2 \notin K(\alpha_1), \end{cases}$$

Weil $\mathrm{Gal}(f) \subset S_3$ eine Untergruppe ist, sind die einzigen Untergruppen dieser Ordnung

$$\mathrm{Gal}(f) \simeq \begin{cases} A_3 \simeq \mathbb{Z}/3\mathbb{Z}, & \text{falls } \alpha_2 \in K(\alpha_1), \\ S_3, & \text{falls } \alpha_2 \notin K(\alpha_1). \end{cases}$$

Wir wollen eine Methode angeben, mit der man entscheiden kann, ob $\mathrm{Gal}(f)$ isomorph zu $A_3$ oder $S_3$ ist.

**Definition 4.1.16.** Sei $f \in K[X]$ mit $f = \prod_{i=1}^{n}(X - \alpha_i)$ in $\bar{K}$. Dann ist die **Diskriminante** von $f$

$$D(f) \coloneqq \prod_{i<j}(\alpha_i - \alpha_j)^2.$$

**Fakt 4.1.17.** *$D(f) \in K$ (das haben wir bereits für kubische Polynome nachrechnet, Bemerkung 3.7.28).*

*Beweis.* Wir haben $D(f) \neq 0$ genau dann, wenn $f$ separabel ist. Sei also $f$ separabel. Der Zerfällungskörper von $f$ sei $K(\alpha_1, \ldots, \alpha_n)$ und wir haben $K = K(\alpha_1, \ldots, \alpha_n)^{\mathrm{Gal}(f)}$. Da $\mathrm{Gal}(f) \subset \mathrm{Bij}\{\alpha_1, \ldots, \alpha_n\}$ und da $D(f)$ offensichtlich invariant unter Permutation der $\alpha_i$ bleibt, folgt $D(f) \in K$. □

iminant:galoisgroup

**Beobachtung 4.1.18.** Sei $f \in K[X]$ irreduzibel und separabel mit $\deg(f) = n$. Sei $L$ der Zerfällungskörper von $f$ und sei $G \coloneqq \mathrm{Gal}(f)$. Die Wurzel der Diskriminante ist

$$\delta(f) \coloneqq \prod_{i<j}(\alpha_i - \alpha_j) \in L.$$

Für $\sigma \in G \subset S_n = \mathrm{Bij}\{\alpha_1, \ldots, \alpha_n\}$ gilt dann $\sigma(\delta(f)) = \mathrm{sgn}(\sigma)\delta(f)$, d. h. $\delta(f) \in K = L^G$ genau dann, wenn $G \subset A_n = \mathrm{Ker}(\mathrm{sgn}) \subset S_n$.

Für irreduzible und separable $f$ vom Grad $n = 3$ gilt also

$$\mathrm{Gal}(f) \simeq \begin{cases} A_3, & \text{falls } \delta(f) \in K, \\ S_3, & \text{falls } \delta(f) \notin K. \end{cases}$$

*Beispiel* 4.1.19. Hier einige konkrete Beispiele für Beobachtung 4.1.18. Wir schreiben $f = X^3 + pX + q \in \mathbb{Q}[X]$ (vgl. Bemerkung 3.7.28).

(i) Für $f = X^3 - 2 \in \mathbb{Q}[X]$ ist

$$D(f) = -4p^3 - 27q^2 = -27 \cdot 4.$$

Nun ist $\sqrt{D(f)} = \delta(f) \notin \mathbb{Q}$ und daher $\mathrm{Gal}(f) \simeq S_3$.

(ii) Für $f = X^3 - 3X + 1$ ist

$$D(f) = -4p^3 - 27 = 4 \cdot 27 - 27 = 3 \cdot 27 = 9^2.$$

Nun ist $\delta(f) \in \mathbb{Q}$, d. h. $\mathrm{Gal}(f) \simeq A_3$.

## 4.2 Hauptsatz der Galoistheorie

Folgende Aussage erlaubt uns, die Körper innerhalb einer endlichen Galoiserweiterung vollständig zu klassifizieren.

thm:correspondence

**Satz 4.2.1** (**Hauptsatz der Galoistheorie**[51]). *Sei $L/K$ eine endliche Galoiserweiterung.*

(i) *Dann existiert eine Bijektion*

$$\begin{aligned}\{\text{Türme } L/L'/K\} &\longleftrightarrow \{\text{Untergruppen } H \subset \mathrm{Gal}(L/K)\},\\ L' &\longmapsto \mathrm{Gal}(L/L'),\\ L^H &\longleftarrow\!\shortmid H.\end{aligned}$$

(ii) *Für einen Turm $L/L'/K$ ist $L'/K$ genau dann galoissch, wenn $\mathrm{Gal}(L/L') \lhd \mathrm{Gal}(L/K)$ ein Normalteiler ist. In diesem Fall gilt*

$$\mathrm{Gal}(L'/K) \simeq \mathrm{Gal}(L/K)/\mathrm{Gal}(L/L').$$

*Beweis.*

(i) Wir haben bereits gesehen, dass $L/L'$ galoissch ist und $\mathrm{Gal}(L/L') \subset \mathrm{Gal}(L/K)$ eine Untergruppe ist (Fakt 4.1.9), d. h. die Abbildungen sind wohldefiniert. Ferner haben wir gesehen, dass $\mathrm{Gal}(L/K)$ endlich ist und die Abbildung injektiv ist. Tatsächlich haben wir gezeigt, dass die Komposition

$$L' \longmapsto \mathrm{Gal}(L/L') \longmapsto L^{\mathrm{Gal}(L/L')}$$

die Identität ist.

Für die Surjektivität genügt es zu zeigen, dass die Komposition

$$H \longmapsto L^H \longmapsto \mathrm{Gal}(L/L^H)$$

die Identität ist, d. h. $\mathrm{Gal}(L/L^H) = H$. Bezeichne $H' \coloneqq \mathrm{Gal}(L/L^H)$. Dann ist $H \subset H'$ nach Definition. Es genügt also $|H'| \leq |H|$ zu zeigen.

Wähle ein primitives Element $\alpha \in L$, d. h. $L = K(\alpha)$. Wegen $K \subset L^H$ gilt auch $L = L^H(\alpha)$. Sei $p_\alpha \in L^H[X]$ das Minimalpolynom von $\alpha$ über $L^H$, sodass $[L : L^H] = \deg(p_\alpha)$. Schreibe $H = \{\varphi_1, \ldots, \varphi_n\}$ mit $n \coloneqq |H|$ und betrachte

$$F_\alpha(X) \coloneqq \prod_{i=1}^{n} (X - \varphi_i(\alpha)) \in L[X].$$

Tatsächlich ist $F_\alpha(X) \in L^H[X]$, da die Koeffizienten des Polynoms bis auf Vorzeichen symmetrische Polynome in den $\varphi_i(\alpha)$ sind und damit unter Permutation der $\varphi_i(\alpha)$ durch $\varphi_j \in H$ unverändert bleiben. Sei o. B. d. A. $\varphi_1 = \mathrm{id}_L$ mit $\varphi_1(\alpha) = \alpha$. Dann gilt $F_\alpha(\alpha) = 0$, d. h. $p_\alpha \mid F_\alpha$. Mit Fakt 4.1.9 folgt

$$|H'| = |\mathrm{Gal}(L/L^H)| = [L : L^H] = \deg(p_\alpha) \leq \deg(F_\alpha) = n = |H|.$$

[51] Erstaunlicherweise gibt es solche *Galoiskorrespondenzen*, d. h. eine inklusionsumkehrende Bijektionen zwischen mathematischen (Unter-)strukturen, nicht nur in der Galoistheorie, sondern auch in vielen anderen Bereichen der Mathematik. Hier sei die Galoiskorrespondenz in der Überlagerungstheorie (Topologie) und Hilbert's Nullstellensatz über Varietäten (algebraische Geometrie, kommutative Algebra) genannt.

(ii) Angenommen $L'/K$ ist galoissch. Setze $H \coloneqq \mathrm{Gal}(L/L')$ und $G \coloneqq \mathrm{Gal}(L/K)$, d. h. $L' = L^H$. Zu zeigen ist $H \lhd G$.

Aufgrund Normalität von $L^H/K$ gilt $\varphi(L^H) = L^H$ für alle $\varphi \in G$. (Falls nämlich $p_a \in K[X]$ das Minimalpolynom eines beliebigen $a \in L^H$ ist, so liegen auch alle Nullstellen von $p_a$ in $L^H$. Jedes $\varphi \in G$ permutiert nur diese Nullstellen.) Also erhalten wir einen Gruppenhomomorphismus

$$\pi\colon \mathrm{Gal}(L/K) \longrightarrow \mathrm{Gal}(L^H/K), \qquad \varphi \longmapsto \varphi|_{L^H}.$$

Mithilfe von Korollar 3.7.17 lässt sich jeder $K$-Automorphismus $L^H \xrightarrow{\sim} L^H$ zu einem $K$-Homomorphismus $L \to L$ fortsetzen, welcher aufgrund Lemma 4.1.6 ein Automorphismus ist. Folglich ist $\pi$ surjektiv mit $\mathrm{Ker}(\pi) \lhd \mathrm{Gal}(L/K) = G$. Sodann genügt es $H = \mathrm{Ker}(\pi)$ zu zeigen; der induzierte Gruppenisomorphismus ist Korollar 1.2.23.

Wir haben

$$[L : L^H] \cdot [L^H : K] = [L : K] = |G| = |\mathrm{Ker}(\pi)| \cdot |\mathrm{Gal}(L^H/K)|.$$

Da aber nach Annahme $[L^H : K] = |\mathrm{Gal}(L^H/K)|$, erhalten wir $|H| = [L : L^H] = |\mathrm{Ker}(\pi)|$. Dann folgt aus $H \subset \mathrm{Ker}(\pi)$ schon die Gleichheit $H = \mathrm{Ker}(\pi)$.

Sei umgekehrt $H \lhd \mathrm{Gal}(L/K)$. Wir müssen zeigen, dass $L^H/K$ normal ist, d. h. für alle $K$-Homomorphismen $\varphi\colon L^H \to \bar{L}$ gilt $\varphi(L^H) = L^H$ (Separabilität gilt bereits).

Wähle eine Fortsetzung $\tilde{\varphi}\colon L \to \bar{L}$ von $\varphi$. Dann gilt $\tilde{\varphi}(L) = L$ aufgrund Normalität von $L/K$ und daher $\tilde{\varphi} \in \mathrm{Gal}(L/K)$. Seien $a \in L^H$ und $b \coloneqq \tilde{\varphi}(a) = \varphi(a) \in L$. Dann gilt $b \in L^H$ genau dann, wenn $\tau(b) = b$ für alle $\tau \in H$. Wegen $H \lhd G$ gibt es ein gewisses $\tau' \in H$, sodass

$$\tau(b) = \tau(\tilde{\varphi}(a)) = (\tau \circ \tilde{\varphi})(a) = (\tilde{\varphi} \circ \tau')(a) = \tilde{\varphi}(\tau'(a)) = \tilde{\varphi}(a) = b. \qquad \square$$

espondence:inclusion

**Korollar 4.2.2.** *Sei $L/K$ eine endliche Galoiserweiterung. Seien $K \subset L_1, L_2 \subset L$ Körper und $H_i \coloneqq \mathrm{Gal}(L/L_i)$. Dann gelten folgende Aussagen:*

(i) *$H_1 = H_2$ genau dann, wenn $L_1 = L_2$.*

(ii) *$L_1 \subset L_2$ genau dann, wenn $H_1 \supset H_2$.*

VL 20
08.01.24

*Beweis.* Aus dem Hauptsatz der Galoistheorie 4.2.1 wissen wir $L_i = L^{H_i}$. Nun folgt die Aussage aus der folgender Beobachtung: $L^{H_1} \subset L^{H_2}$ genau dann, wenn $H_1 \supset H_2$. $\square$

**Korollar 4.2.3.** *Sei $L/K$ eine endliche Galoiserweiterung. Seien $K \subset L_1, L_2 \subset L$ Körper und $H_i \coloneqq \mathrm{Gal}(L/L_i)$. Dann gelten folgende Aussagen:*

(i) *$L_1 \cap L_2 = L^{\langle H_1, H_2\rangle}$. Hierbei ist $\langle H_1, H_2\rangle = \langle H_1 \cup H_2\rangle$ die kleinste Untergruppe von $G$, die $H_1$ und $H_2$ enthält.*

(ii) *$L_1L_2 = L^{H_1 \cap H_2}$. Hierbei ist $L_1L_2 \coloneqq L_1 \cdot L_2 \coloneqq \{\sum_i a_i b_i \mid a_i \in L_1, b_i \in L_2\}$ der kleinste Unterkörper von $L$, der $L_1$ und $L_2$ enthält.*[52]

[52] Auch *Kompositum* von $L_1$ und $L_2$ genannt.

*Beweis.*

(i) $a \in L_1 \cap L_2 = L^{H_1} \cap L^{H_2}$ genau dann, wenn $\sigma(a) = a$ für alle $\sigma \in H_1 \cup H_2$ genau dann, wenn $a \in L^{H_1 \cup H_2} = L^{\langle H_1, H_2 \rangle}$ (die Gleichheit folgt aus Aufgabe 59).

(ii) Wegen $H_1 \cap H_2 \subset H_1, H_2$ gelten $L_1 = L^{H_1} \subset L^{H_1 \cap H_2}$ und $L_2 = L^{H_2} \subset L^{H_1 \cap H_2}$. Für die umgekehrte Inklusion betrachten wir

$$H_1 \cap H_2 = \mathrm{Gal}(L/L^{H_1 \cap H_2}) \subset \mathrm{Gal}(L/L_1 L_2) \subset H_1 \cap H_2,$$

d. h. es gilt überall Gleichheit. Mit Korollar 4.2.2 folgt $L^{H_1 \cap H_2} = L_1 L_2$. □

espondence:composite

pondence:composite:1

**Korollar 4.2.4.** *Seien $L/K$ eine Körpererweiterung und $K \subset L_1, L_2 \subset L$ Körper. Angenommen $L_i/K$ sind endlich galoissch. Dann gelten folgende Aussagen:*

(i) *$L_1 L_2/K$ ist eine endliche Galoiserweiterung und*

$$\mathrm{Gal}(L_1 L_2/L_1) \xrightarrow{\sim} \mathrm{Gal}(L_2/L_1 \cap L_2), \qquad \sigma \longmapsto \sigma|_{L_2}$$

*ist ein Gruppenisomorphismus.*

(ii) *Es gibt einen injektiven Gruppenhomomorphismus*

$$\mathrm{Gal}(L_1 L_2/K) \hookrightarrow \mathrm{Gal}(L_1/K) \times \mathrm{Gal}(L_2/K), \qquad \sigma \longmapsto (\sigma|_{L_1}, \sigma|_{L_2})$$

*und dieser ist surjektiv (d. h. ein Gruppenisomorphismus), falls $K = L_1 \cap L_2$.*

*Beweis.*

(i) Da $L_i/K$ normal und separabel sind, sind sie normal erzeugt und separabel erzeugt. Folglich ist $L_1 L_2/K$ normal erzeugt und separabel erzeugt, d. h. $L_1 L_2/K$ ist normal und separabel, d. h. galoissch. Endlichkeit ist klar.

Aus $L_1 L_2/K$ galoissch folgt $L_1 L_2/L_1$ galoissch, und aus $L_2/K$ galoissch folgt $L_2/L_1 \cap L_2$ galoissch. Also sind die Galoisgruppen und die Abbildung zwischen ihnen wohldefiniert.

Für die Injektivität sei $\sigma|_{L_2} = \mathrm{id}_{L_2}$. Da auch $\sigma|_{L_1} = \mathrm{id}_{L_1}$, folgt daraus $\sigma = \mathrm{id}_{L_1 L_2}$. Für die Surjektivität beobachten wir

$$L_1 \cap L_2 = L_2^{\mathrm{Gal}(L_2/L_1 \cap L_2)} \subset L_2^H$$

wobei

$$H \coloneqq \mathrm{Gal}(L_1 L_2/L_1) \subset \mathrm{Gal}(L_1/L_1 \cap L_2).$$

Weiterhin gilt

$$L_2^H \subset (L_1 L_2)^H \cap L_2 = L_1 \cap L_2.$$

Zusammengenommen erhalten wir $L_2^H = L_1 \cap L_2$, was aufgrund von Korollar 4.2.2 dann $H = \mathrm{Gal}(L_2/L_1 \cap L_2)$ impliziert.

(ii) Die Abbildung $\sigma \mapsto (\sigma|_{L_1}, \sigma|_{L_2})$ ist ein wohldefinierter Gruppenhomomorphismus und da aus $\sigma|_{L_1} = \mathrm{id}$ und $\sigma|_{L_2} = \mathrm{id}$ schon $\sigma|_{L_1 L_2} = \mathrm{id}$ folgt, ist dieser injektiv. Es bleibt also zu zeigen, dass die Abbildung surjektiv ist, falls $K = L_1 \cap L_2$.

Dazu seien $\sigma_i \in \mathrm{Gal}(L_i/K)$ für $i = 1, 2$. Wir verwenden vom Hauptsatz der Galoistheorie 4.2.1, dass

$$\mathrm{Gal}(L_i/K) \simeq \mathrm{Gal}(L_1L_2/K)/\mathrm{Gal}(L_1L_2/L_i).$$

Somit gibt es $\tilde{\sigma}_i \in \mathrm{Gal}(L_1L_2/K)$, sodass $\tilde{\sigma}_i|_{L_i} = \sigma_i$ für $i = 1, 2$. Setzen wir $\sigma \coloneqq \tilde{\sigma}_1 \circ \tilde{\sigma}_2 \in \mathrm{Gal}(L_1L_2/K)$, so kann man prüfen, dass $\sigma|_{L_i} = \sigma_i$.[53] □

*Beispiel* 4.2.5. Wir wollen das auf kubische Polynome anwenden. Sei $f \in K[X]$ separabel und irreduzibel mit $\deg(f) = 3$. Sei $L/K$ der Zerfällungskörper von $f$, welcher galoissch ist. Nun wollen wir alle Zwischenkörper $L/L'/K$ klassifizieren.

Es gilt $\mathrm{Gal}(f) \simeq \mathbb{Z}/3\mathbb{Z} \simeq A_3$ genau dann, wenn $\delta(f) = \sqrt{D(f)} \in K$; andernfalls ist $\mathrm{Gal}(f) \simeq S_3$. Wir haben also zwei Fälle zu unterscheiden.

Angenommen $\mathrm{Gal}(f) \simeq A_3$. Dann besitzt $A_3$ nur die Untergruppen $\{1\} \subset A_3$ und $A_3 \subset A_3$. Diese korrespondieren zu Zwischenkörpern $L' = L$ bzw. $L' = K$.

Falls hingegen $\mathrm{Gal}(f) \simeq S_3$ ist, so ergibt sich Tabelle 4.1. Wir beweisen, dass $L^{A_3} = K(\delta(f))$. Betrachte den Turm $K \subset K(\delta(f)) \subset L$. Es gelten $[L : K] = |S_3| = 6$ und $[K(\delta(f)) : K] = 2$ (denn $\delta(f)$ ist eine Quadratwurzel). Also gilt $[L : K(\delta(f))] = 3 = |A_3|$, und da es nur eine Untergruppe der Ordnung 3 von $S_3$ gibt, ist notwendigerweise $L^{A_3} = K(\delta(f))$.

| Untergruppen von $S_3$ | Zwischenkörper $L'$ |
|---|---|
| $\{1\} \subset S_3$ | $L' = L$ |
| $A_3 \subset S_3$ | $L' = K(\delta(f))$ |
| $\mathbb{Z}/2\mathbb{Z} \simeq \langle(12)\rangle \subset S_3$ | $L' = K(\alpha_3)$ |
| $\mathbb{Z}/2\mathbb{Z} \simeq \langle(13)\rangle \subset S_3$ | $L' = K(\alpha_2)$ |
| $\mathbb{Z}/2\mathbb{Z} \simeq \langle(23)\rangle \subset S_3$ | $L' = K(\alpha_1)$ |

Tabelle 4.1: Zwischenkörper $L'$ des Zerfällungskörpers $L$ eines separablen irreduziblen kubischen Polynoms $f \in K[X]$. Dabei sind $\alpha_1, \alpha_2, \alpha_3 \in \bar{K}$ die Nullstellen von $f$.

tab:correspondence

*Beispiel* 4.2.6. Wir wollen das auf endliche Körper anwenden. Sei $L/K$ eine Erweiterung endlicher Körper, d. h. $K \simeq \mathbb{F}_{p^n}$ und $L \simeq \mathbb{F}_{p^k}$. Als $K$-Vektorräume gilt $L \simeq (\mathbb{F}_{p^n})^{\oplus m}$, weshalb $k = mn$. Wir betrachten also $\mathbb{F}_{p^{mn}}/\mathbb{F}_{p^n}$, was galoissch ist.

Sei

$$\varphi \coloneqq F^n \colon \mathbb{F}_{p^{mn}} \xrightarrow{\sim} \mathbb{F}_{p^{mn}}, \qquad a \longmapsto a^{p^n}$$

die $n$-te Potenz des Frobenius. Sie erfüllt $\varphi|_{\mathbb{F}_{p^n}} = \mathrm{id}$, da $a^{p^n} = a$ für alle $a \in \mathbb{F}_{p^n}$. Also ist $\varphi \in \mathrm{Gal}(\mathbb{F}_{p^{mn}}/\mathbb{F}_{p^n})$. Definiere den Gruppenhomomorphismus

$$\mathbb{Z} \longrightarrow \mathrm{Gal}(\mathbb{F}_{p^{mn}}/\mathbb{F}_{p^n}), \qquad k \longmapsto \varphi^k.$$

*Behauptung:* Obige Abbildung induziert den Isomorphismus $\mathbb{Z}/m\mathbb{Z} \xrightarrow{\sim} \mathrm{Gal}(\mathbb{F}_{p^{mn}}/\mathbb{F}_{p^n})$.

*Beweis:* Offenbar ist $\varphi^m(a) = a^{p^{mn}} = a$ für alle $a \in \mathbb{F}_{p^{mn}}$, d. h. die Abbildung ist wohldefiniert. Für die Injektivität sei $\varphi^k = \mathrm{id}$. Dann gilt $a^{p^{nk}} = a$ für alle $a \in \mathbb{F}_{p^{mn}}$. Also ist

[53] Wegen $K = L_1 \cap L_2$ können wir den Isomorphismus aus (i) benutzen. Wir können also $\tilde{\sigma}_1 \in \mathrm{Gal}(L_1L_2/K)$ so wählen, dass $\tilde{\sigma}_1|_{L_1} = \sigma_1$, aber auch $\tilde{\sigma}_1|_{L_2} = \mathrm{id}_{L_2}$. Analog für $\sigma_2$.

$\mathbb{F}_{p^{nk}} \supset \mathbb{F}_{p^{mn}}$, was $|\mathbb{F}_{p^{nk}}| \geq |\mathbb{F}_{p^{mn}}|$ impliziert, d. h. $k \geq m$. Für die Surjektivität beobachten wir

$$|\mathbb{Z}/m\mathbb{Z}| = m = [\mathbb{F}_{p^{mn}} : \mathbb{F}_{p^n}] = |\mathrm{Gal}(\mathbb{F}_{p^{mn}}/\mathbb{F}_{p^n})|.$$

Also ist die Inklusion $\mathbb{Z}/m\mathbb{Z} \hookrightarrow \mathrm{Gal}(\mathbb{F}_{p^{mn}}/\mathbb{F}_{p^n})$ bijektiv.

Für einen Turm von endlichen Körpern $\mathbb{F}_{p^{m'n}}/\mathbb{F}_{p^{mn}}/\mathbb{F}_{p^n}$ mit $m \mid m'$ erhalten wir folgende kurze exakte Sequenz:

$$\begin{array}{ccccc} \mathrm{Gal}(\mathbb{F}_{p^{m'n}}/\mathbb{F}_{p^{mn}}) & \hookrightarrow & \mathrm{Gal}(\mathbb{F}_{p^{m'n}}/\mathbb{F}_{p^n}) & \twoheadrightarrow & \mathrm{Gal}(\mathbb{F}_{p^{mn}}/\mathbb{F}_{p^n}) \\ \downarrow\wr & & \downarrow\wr & & \downarrow\wr \\ \mathbb{Z}/(m'/m)\mathbb{Z} & \hookrightarrow & \mathbb{Z}/m'\mathbb{Z} & \twoheadrightarrow & \mathbb{Z}/m\mathbb{Z} \end{array}$$

## 4.3 Auflösbarkeit durch Radikale I

*Problem* 4.3.1. Wir wollen nun beschreiben, was eine „Lösungsformel“ für eine polynomielle Gleichung bedeutet.

*Wiederholung (Beobachtung 3.2.2):* Die Nullstellen einer quadratischen Gleichung $X^2 + pX + q \in K[X]$ (mit $\mathrm{char}(K) \neq 2$) sind

$$-\frac{p}{2} \pm \sqrt{\left(\frac{p}{2}\right)^2 - q} \in \bar{K}.$$

Auch für kubische Gleichungen $X^3 + pX + q \in K[X]$ (für diese Form nach Tschirnhaus mit $\mathrm{char}(K) \neq 2, 3$) lassen sich die Nullstellen explizit angeben:

$$\sqrt[3]{-\frac{q}{2} \pm \sqrt{\left(\frac{p}{3}\right)^3 + \left(\frac{q}{2}\right)^2}} - \sqrt[3]{\frac{q}{2} \pm \sqrt{\left(\frac{p}{3}\right)^3 + \left(\frac{q}{2}\right)^2}}.$$

Auch für quartische Gleichungen $X^4 + \cdots \in K[X]$ gibt es eine explizite Formel, s. dazu [Tig]. bib:tig

**Definition 4.3.2.** Wir setzen $\mathrm{char}(K) = 0$ voraus.

(i) Dann heißt $a \in \bar{K}$ **durch Radikale ausdrückbar**, falls es einen Turm

$$K = K_1 \subset K_2 \subset \cdots \subset K_n \subset \bar{K}$$

gibt, sodass $a \in K_n$ und $K_i = K_{i-1}(a_i)$ mit $b_i \coloneqq a_i^{n_i} \in K_{i-1}$ für gewisse $n_i$. Das bedeutet, dass $K_i$ durch Adjunktion einer Wurzel $a_i = \sqrt[n_i]{b_i}$ zu $K_{i-1}$ entsteht.

(ii) Ein $f \in K[X]$ heißt **durch Radikale lösbar**, falls alle Nullstelen von $f$ in $\bar{K}$ durch Radikale ausdrückbar sind.

(iii) Eine Körpererweiterung $L/K$ heißt **durch Radikale auflösbar**, falls es einen Turm $K = K_0 \subset K_1 \subset \cdots \subset K_n$ gibt, sodass mit $L \subset K_n$ und $K_i = K_{i-1}(a_i)$ mit $a_i^{n_i} \in K_{i-1}$ für gewisse $n_i$.

Ziel ist folgende Aussage. Die Rückrichtung war die historisch ausschlaggebende Aussage.

hm:radical:solvable

**Satz 4.3.3** (Galois). *Sei $L/K$ eine endliche Körpererweiterung. Dann ist $L/K$ genau dann durch Radikale auflösbar, wenn $L/K$ auflösbar ist.*

Dabei bedeutet „$L/K$ auflösbar“ Folgendes.

**Definition 4.3.4.**

(i) Eine Galoiserweiterung $L/K$ heißt **abelsch**, **zyklisch**, **auflösbar**, etc. falls $\mathrm{Gal}(L/K)$ abelsch, zyklisch, auflösbar, etc. ist.

(ii) Eine endliche Körpererweiterung $L/K$ heißt **auflösbar**, wenn es einen Erweiterungskörper $L'/L/K$ gibt, sodass $L'/K$ endlich galoissch und auflösbar ist.

. Wiederholung Eine Gruppe $G$ heißt *auflösbar*, falls es ein $n$ mit $D^nG = \{e\}$ gibt (hierbei sind $D^iG = [D^{i-1}G, D^{i-1}G]$ und $D^0G = G$). Das ist gleichbedeutend mit der Existenz einer Normalreihe $\{1\} = G_n \lhd \cdots \lhd G_0 = G$ mit abelschen Faktoren $G_i/G_{i+1}$. Das ist wiederum gleichbedeutend mit der Existenz einer Normalreihe $\{1\} = G_n \lhd \cdots \lhd G_0 = G$ mit zyklischen Faktoren $G_i/G_{i+1} \simeq \mathbb{Z}/p_i\mathbb{Z}$ von Primzahlordnung $p_i$.

. Motivation Wir erinnern uns, dass $S_n$ genau dann auflösbar ist, wenn $n \leq 4$. Später werden wir sehen, dass ein „allgemeines“ Polynom $f$ vom Grad 5 Galoisgruppe $\mathrm{Gal}(f) = S_5$ hat. Damit ist $\mathrm{Gal}(f)$ nicht auflösbar und somit die Nullstellen eines „allgemeinen“ Polynoms $f$ vom Grad 5 sich nicht Radikale ausdrücken lassen.

Um Satz 4.3.3 zu zeigen, bedarf es einiger Vorbereitungen.

em:radical:solvable

n:radical:solvable:1

**Lemma 4.3.5.**

(i) *Seien $L/K$ und $M/K$ endliche Körpererweiterungen. Wir wählen einen gemeinsamen algebraischen Abschluss $L, M \subset \bar{K}$. Ist $L/K$ auflösbar, so ist $ML/M$ auflösbar.*

(ii) *Sei $M/L/K$ ein Turm von endlichen Körpererweiterungen. Dann ist $M/K$ genau dann auflösbar, wenn $M/L$ und $L/K$ beide auflösbar sind.*

*Beweis.*

(i) Wenn $L/K$ auflösbar ist, so gibt es einen Erweiterungskörper $L'/L/K$, sodass $L'/K$ endlich galoissch und $\mathrm{Gal}(L'/K)$ auflösbar ist. Insbesondere ist $ML'/M$ endlich. Da $L'/K$ normal und separabel ist, ist $L'/K$ normal erzeugt und separabel erzeugt. Also ist auch $ML'/M$ normal erzeugt und separabel erzeugt, d. h. es ist endlich galoissch. Damit erhalten wir den Turm $ML'/ML/M$. Es bleibt zu zeigen, dass $\mathrm{Gal}(ML')$ auflösbar ist, woraus die Behauptung folgt.

Nach Korollar 4.2.4 haben wir

$$\mathrm{Gal}(ML'/M) \simeq \mathrm{Gal}(L'/L' \cap M) \subset \mathrm{Gal}(L'/K).$$

Nun ist die rechte Seite auflösbar, und wegen Satz 1.5.20 ist auch die linke Seite auflösbar. Folglich ist $ML'/M$ eine endliche auflösbare Galoiserweiterung.

(ii) Zur Hinrichtung: Angenommen $M/K$ ist auflösbar. Dann gibt es eine Körpererweiterung $M'/M$, sodass $M'/K$ endlich galoissch und $\mathrm{Gal}(M'/K)$ auflösbar ist. Es gilt $\mathrm{Gal}(M'/L) \subset \mathrm{Gal}(M'/K)$, wobei die rechte Gruppe auflösbar ist. Also ist auch $\mathrm{Gal}(M'/L)$ auflösbar und daher $M/L$ auflösbar. Aus der Auflösbarkeit von $M'/K$ folgt sofort, dass $L/K$ auflösbar ist.

Für die Rückrichtung seien $M/L$ und $L/K$ beide auflösbar. VL 21 12.01.24

*Behauptung:* Wir können auf den Fall reduzieren, dass $M/L$ und $L/K$ endlich galoissch und auflösbar sind.

*Beweis:* Da $L/K$ auflösbar ist, gibt es eine Körpererweiterung $L'/L/K$, sodass $L'/K$ endlich galoissch und auflösbar ist. Ferner ist $ML'/L'$ nach (i) auflösbar, da $M/L$ auflösbar ist. Also gibt es einen Erweiterungskörper $M'/ML'/L'$, sodass $M'/L'$ endlich galoissch und auflösbar ist. Ersetze nun $M/L/K$ durch $M'/L'/K$; das zeigt die Behauptung.

Wir können also annehmen, dass $M/L$ und $L/K$ beide endlich galoissch und auflösbar sind. Dann ist $M/K$ schonmal separabel. (Wir wiederholen hier das Argument: Es gilt

$$[M : K] = [M : L][L : K] = [M : L]_S[L : K]_S = [M : K]_S,$$

da die Körpererweiterungen galoissch sind. Wir erhalten $[M : K] = [M : K]_S$, d. h. $M/K$ ist separabel.) Eventuell ist aber $M/K$ nicht normal. Wähle hierzu die normale Hülle $\tilde{M}/M/K$, d. h. wir adjungieren alle Nullstellen von irreduziblen Polynomen $f \in K[X]$ mit einer Nullstelle in $M$; diese $f$ sind automatisch separabel. Damit ist $\tilde{M}/K$ endlich galoissch.

Ist $\mathrm{Gal}(\tilde{M}/L)$ auflösbar, so erhalten wir mithilfe des Hauptsatz der Galoistheorie 4.2.1 die kurze exakte Sequenz

$$\mathrm{Gal}(\tilde{M}/L) \hookrightarrow \mathrm{Gal}(\tilde{M}/K) \twoheadrightarrow \mathrm{Gal}(L/K),$$

wobei die linke und rechte Gruppen beide auflösbar sind. Nach Satz 1.5.20 ist $\tilde{M}/K$ auflösbar und wir wären fertig.

Es gibt noch eine andere Konstruktion der normalen Hülle, nämlich[54]

$$\tilde{M} = \prod_{\sigma \in \mathrm{Hom}_K(M, \bar{K})} \sigma(M).$$

Da $L/K$ normal ist, gilt $\sigma(L) = L$ für alle $\sigma \colon M \to \bar{K}$. Also ist

$$\mathrm{Gal}(M/L) \simeq \mathrm{Gal}(\sigma(M)/\sigma(L)) \simeq \mathrm{Gal}(\sigma(M)/L)$$

für alle $\sigma$ auflösbar. Gemäß Korollar 4.2.4 existiert eine Inklusion

$$\mathrm{Gal}(\tilde{M}/L) = \mathrm{Gal}\left(\prod_\sigma \sigma(M)/L\right) \hookrightarrow \prod_\sigma \mathrm{Gal}(\sigma(M)/L).$$

Per Induktion mit einer exakten Sequenz[55] folgt, dass das Produkt rechts auflösbar ist und wegen Satz 1.5.20 auch links die Untergruppe auflösbar ist. □

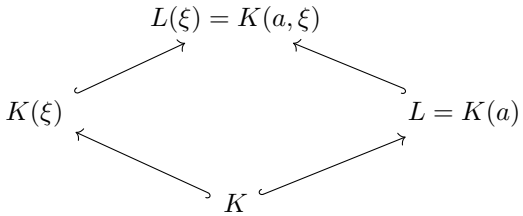
[54] Beachte, dass das ein endliches Produkt ist, da $M/K$ separabel ist und daher $[M : K]_S = [M : K] < \infty$. Das ist notwendig, um Korollar 4.2.4 induktiv anwenden zu können.

[55] Gemeint ist $\mathrm{Gal}(\sigma(M)/L) \hookrightarrow \mathrm{Gal}(\sigma(M)/L) \times \mathrm{Gal}(\sigma'(M)/L) \twoheadrightarrow \mathrm{Gal}(\sigma'(M)/L)$ für $\sigma, \sigma' \in \mathrm{Hom}_K(M, \bar{K})$.

*Beweis von Satz 4.3.3. Warnung:* Es gibt zwei Lücken, die wir später stopfen werden.

Angenommen $L/K$ ist durch Radikale auflösbar, d. h. es gibt einen Turm $K = K_0 \subset K_1 \subset \cdots \subset K_n$, sodass $L \subset K_n$ und $K_i = K_{i-1}(a_i)$ mit $a_i^{n_i} = b_i \in K_{i-1}$. Nach Induktion und Lemma 4.3.5 genügt es zu zeigen, dass $K_i/K_{i-1}$ auflösbar ist. O. B. d. A. sei also $L = K(a)/K$ mit $a^n = b \in K$. Wähle $L \subset \bar{K}$ und $\xi \in \bar{K}$ mit $\xi^n = 1$ und $\xi^{n'} \neq 1$ für alle $1 \leq n' \leq n$ (eine sog. *primitive n-te Einheitswurzel*).

Betrachte




Gelingt es uns zu zeigen, dass $K(\xi)/K$ und $K(\xi, a)/K(\xi)$ auflösbar sind, so folgt aus Lemma 4.3.5, dass $L(\xi)/K$ und daher $L/K$ auflösbar sind; dann sind wir fertig. Hier die erste Lücke.

*Fakt:* $K(\xi)/K$ ist galoissch und es gibt die Einbettung $\mathrm{Gal}(K(\xi)/K) \hookrightarrow (\mathbb{Z}/n\mathbb{Z})^*$ (der Ring der Einheiten von $\mathbb{Z}/n\mathbb{Z}$).

*Beweisidee:* $\xi$ ist Nullstelle von $X^n - 1$. Alle anderen Nullstellen sind dann von der Form $\xi^i$ mit $0 \leq i < n$, weshalb $K(\xi)/K$ normal ist. Betrachte nun den Gruppenhomomorphismus $\mathrm{Gal}(K(\xi)/K) \hookrightarrow \mathbb{Z}/n\mathbb{Z}$, die $\sigma \in \mathrm{Gal}(K(\xi)/K)$ mit $\sigma(\xi) = \xi^i$ das Element $\bar{i} \in \mathbb{Z}/n\mathbb{Z}$ zuordnet. Ende der Beweisidee.

Da $(\mathbb{Z}/n\mathbb{Z})^*$ abelsch ist, ist $\mathrm{Gal}(K(\xi)/K)$ nach dem Fakt auflösbar. Es bleibt zu zeigen, dass $K(\xi, a)/K(\xi)$ auflösbar ist. Beobachte, dass $a$ eine Nullstelle von $X^n - b$ ist. Alle anderen Nullstellen sind von der Form $\xi^i a$ mit $0 \leq i < n$. Diese sind auch paarweise verschieden: Aus $a^n = b = (a')^n$ folgt $(a'/a)^n = 1$, also $a'/a = \xi^i$ für ein $i$. Somit ist $K(\xi, a)/K(\xi)$ galoissch.

Mit dem injektiven Gruppenhomomorphismus $\mathrm{Gal}(K(\xi, a)/K(\xi)) \hookrightarrow \mathbb{Z}/n\mathbb{Z}$ in eine abelsche Gruppe, welche $\sigma \in \mathrm{Gal}(K(\xi, a)/K(\xi))$ mit $\sigma(a) = \xi^i a$ das Element $\bar{i} \in \mathbb{Z}/n\mathbb{Z}$ zuordnet, ist $\mathrm{Gal}(K(\xi, a)/K(\xi))$ abelsch und letztlich auflösbar.

Für die Rückrichtung sei $L/K$ auflösbar und o. B. d. A. auch galoissch. Sei

$$\{e\} = G_n \lhd G_{n-1} \lhd \cdots \lhd G_0 = G \coloneqq \mathrm{Gal}(L/K)$$

eine Normalreihe mit zyklischen Faktoren $G_i/G_{i+1} \simeq \mathbb{Z}/p_i\mathbb{Z}$ für eine Primzahl $p_i$. Nach dem Hauptsatz der Galoistheorie 4.2.1 bekommen wir den Turm von Fixkörpern

$$L = K_n \supset K_{n-1} \supset \cdots \supset K = K_0,$$

wobei $K_i = L^{G_i}$. Da $G_{i+1} \lhd G_i$, ist $K_{i+1}/K_i$ Galois. Zudem ist

$$\mathrm{Gal}(K_{i+1}/K_i) \simeq G_i/G_{i+1} \simeq \mathbb{Z}/p_i\mathbb{Z}.$$

Hier die zweite Lücke.

*Fakt:* Es gibt ein $a \in K_i$, sodass $K_i = K_{i+1}(a)$ mit $a^{p_i} \in K_i$.

Mit dem Fakt folgt, dass $L/K$ durch Radikale auflösbar ist. □

*Problem* 4.3.6. Nach Galois und auch Abel gibt es Polynome (vom Grad mindestens 5), deren Nullstellen nicht durch Radikale auflösbar sind, d. h. es gibt *keine* „Lösungsformel“ für die Nullstelle. Um die Existenz wirklich zu beweisen, benötigen wir ein konkretes Polynom $f$ vom Grad $n \geq 5$ mit $\mathrm{Gal}(f) \simeq S_n$.

**Beobachtung 4.3.7.** Wir konstruieren nun ein explizites Polynom $f$, sodass $\mathrm{Gal}(f) \simeq S_n$.

Sei $k$ ein beliebiger Körper und sei

$$L \coloneqq k(X_1, \ldots, X_n) = \left\{ \frac{g}{h} \;\middle|\; g, h \in k[X_1, \ldots, X_n]; h \neq 0 \right\}$$

der Körper der rationalen Funktionen in $n$ Variablen. $L$ kommt mit der Wirkung $S_n \hookrightarrow \mathrm{Aut}(L)$, die die Variablen permutiert. Sei $K \coloneqq L^{S_n}$. Betrachte den Turm

$$k \subset K_0 \coloneqq k(e_1, \ldots, e_n) \subset K = L^{S_n} \subset L = k(X_1, \ldots, X_n),$$

wobei $e_i$ die $i$-ten elementarsymmetrischen Polynomen in $X_1, \ldots, X_n$ sind (vgl. Aufgabe 41). Bspw. gilt $e_1 = \sum_{i=1}^{n} X_i$.

Betrachte das Polynom

$$F \coloneqq \prod_{i=1}^{n} (T - X_i) = T^n - e_1 T^{n-1} + \cdots \pm e_n \in k[e_1, \ldots, e_n][T].$$

Dieses hat $n$ verschiedene Nullstellen in $L$, d. h. die Körpererweiterung $L/K_0$ ist separabel, und da $L$ Zerfällungskörper von $F \in K_0[T]$ ist, ist $L/K_0$ galoissch. Wir erhalten

$$\mathrm{Gal}(F) = \mathrm{Gal}(L/K_0) \hookrightarrow \mathrm{Bij}\{X_1, \ldots, X_n\} \simeq S_n.$$

*Behauptung:* $\mathrm{Gal}(L/K_0) = S_n$.

*Beweis:* Wir wissen, dass $L/K$ eine Galoiserweiterung mit $\mathrm{Gal}(L/K) = S_n$ ist. Also gilt $K = L^{S_n} \subset L^{\mathrm{Gal}(L/K_0)} = K_0$ nach dem Hauptsatz der Galoistheorie 4.2.1. Da schon $K_0 \subset K$ gilt, folgt $K_0 = K$ und daher $\mathrm{Gal}(L/K_0) = S_n$ nach Korollar 4.2.2.

Das liefert ein Beispiel eines Polynoms $F$ mit $\mathrm{Gal}(F) \simeq S^n$. Insbesondere ist $F$ nicht durch Radikale auflösbar, falls $n \geq 5$.

**Bemerkung 4.3.8.** Der Hauptsatz über symmetrische Polynome 3.7.4 besagt, dass $k[X_1, \ldots, X_n]^{S_n} = k[e_1, \ldots, e_n]$. Wir haben den zwar nicht gezeigt, aber die obige Beobachtung zeigt diese Gleichung zumindest, wenn man zu Körpern rationaler Funktionen übergeht: $k(X_1, \ldots, X_n)^{S_n} = k(e_1, \ldots, e_n)$.

*Beispiel* 4.3.9. Seien $b_1, \ldots, b_n \in \mathbb{R}$ *allgemeine* Elemente, d. h. $b_1, \ldots, b_n$ sind transzendent und es gibt kein Polynom $0 \neq g \in \mathbb{Q}[X_1, \ldots, X_n]$ mit $g(b_1, \ldots, b_n) = 0$. Betrachte z. B. Elemente von der Natur $b_1 = \mathrm{e}$, $b_2 = \pi$, etc. Wir erhalten einen Isomorphismus

$$\mathbb{Q}(X_1, \ldots, X_n) \xrightarrow{\sim} \mathbb{Q}(b_1, \ldots, b_n), \qquad X_i \longmapsto b_i.$$

Unter diesem Isomorphismus wird

$$\mathbb{Q}(e_1, \ldots, e_n)[T] \ni F \longmapsto \bar{F} \in \mathbb{Q}(e_1(b_1, \ldots, b_n), \ldots, e_n(b_1, \ldots, b_n))[T]$$

abgebildet. Es folgt

$$S_n \simeq \mathrm{Gal}(\bar{F}) = \mathrm{Gal}(\mathbb{Q}(b_1,\dots,b_n)/\mathbb{Q}(e_1(b_1,\dots,b_n),\dots,e_n(b_1,\dots,b_n))).$$

*Beispiel* 4.3.10. Betrachte nun ganz explizit $f = X^5 - 16X + 2 \in \mathbb{Q}[X]$. Nach dem Eisensteinkriterium 2.5.5 ist dieses Polynom irreduzibel. Dann operiert $\mathrm{Gal}(f) \subset S_5 \simeq \mathrm{Bij}\{\alpha_1,\dots,\alpha_5\}$ transitiv auf den Nullstellen $\{\alpha_1,\dots,\alpha_5\}$ von $f$.

Betrachte $g := X^5 - 16X = X(X^2-4)(X^2+4)$. Diese hat reelle Nullstellen $0, \pm 2 \in \mathbb{R}$ (Abb. 4.2). Nun unterscheiden sich $f$ und $g$ nur um eine Konstante, d. h. $f$ hat genau reelle Nullstellen $\alpha_1, \alpha_2, \alpha_3 \in \mathbb{R}$ (Abb. 4.2); das benutzt, dass $g$ genau zwei Extrempunkte hat, was man durch Ableitung nachrechnen kann.

Betrachte $\sigma\colon \mathbb{C} \xrightarrow{\sim} \mathbb{C}$, $z \mapsto \bar{z}$. Damit gilt $\sigma(\alpha_i) = \alpha_i$ für $i = 1,2,3$ und notwendigerweise $\sigma(\alpha_4) = \alpha_5$, denn $\sigma \neq \mathrm{id}$. Folglich können wir (nach Einschränkung auf den Zerfällungskörper von $f$) $\sigma \in \mathrm{Gal}(f)$, was $(45) \in \mathrm{Gal}(f)$ entspricht. Nach Aufgabe 63 folgt aus der Transitivität von $\mathrm{Gal}(f) \subset S_5$ und $(45) \in \mathrm{Gal}(f)$, dass $\mathrm{Gal}(f) = S_5$.

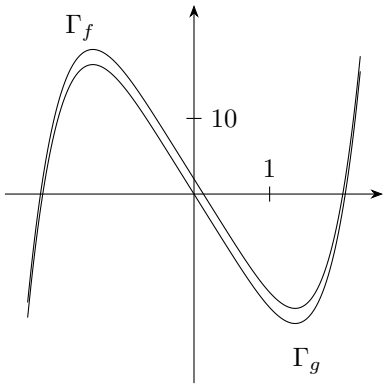



fig:radical

Abbildung 4.2: Graphen $\Gamma_g$ (unten) und $\Gamma_f$ (oben).

## 4.4 Einheitswurzeln

**Beobachtung 4.4.1.** Seien $K$ ein beliebiger Körper und $\bar{K}$ ein algebraischer Abschluss von $K$. Sei

$$U_n \coloneqq \{\zeta \in \bar{K} \mid \zeta^n = 1\}$$

die Menge der $n$-ten Einheitswurzeln, d. h. die Nullstellenmenge von $X^n - 1$. Tatsächlich ist $U_n \subset \bar{K}^*$ eine endliche Untergruppe und daher ist $U_n$ zyklisch.

Um $U_n$ genau zu bestimmen, betrachten wir zwei Fälle.

itm:units:1

(i) Fall $\operatorname{char}(K) \nmid n$, z. B. $\operatorname{char}(K) = 0$. Für $f = X^n - 1$ gilt $f' n X^{n-1}$, was nur Nullstelle 0 hat. Damit haben $f$ und $f'$ keine gemeinsamen Nullstellen und $f$ ist daher separabel. In diesem Fall gilt also $|U_n| = n$, d. h. $U_n \simeq \mathbb{Z}/n\mathbb{Z}$.

(ii) Fall $\operatorname{char}(K) =: p \mid n$. Schreibe $n = p^k n'$ mit $p \nmid n'$. Wir erhalten

$$X^n - 1 = X^{p^k n'} - 1 = (X^{n'})^{p^k} - 1 = (X^{n'} - 1)^{p^k}.$$

Damit sind die Nullstellen von $X^n - 1$ dieselben wie von $X^{n'} - 1$. In diesem Fall ist also $U_n = U_{n'} \simeq \mathbb{Z}/n'\mathbb{Z}$ nach (i).

**Definition 4.4.2.** Ein Element $\zeta \in U_n$ heißt **primitive $n$-te Einheitswurzel**, falls $U_n = \langle \zeta \rangle$, d. h. alle Einheitswurzeln sind von der Form $\zeta^i$ für $0 \leq i < n$.

**Beobachtung 4.4.3.** Nach Wahl einer primitiven Einheitswurzel $\zeta \in U_n$ erhalten wir einen Isomorphismus $U_n \simeq \mathbb{Z}/n'\mathbb{Z}$, wobei

VL 22
15.01.24

$$n' = \begin{cases} n, & \text{falls } \operatorname{char}(K) \nmid n, \\ m, & \text{falls } n = \operatorname{char}(K)^k m \text{ mit } \operatorname{char}(K) \nmid m. \end{cases}$$

Wie sehen die primitiven Einheitswurzeln aus?

Sei $U_n^{\mathrm{pr}} \subset U_n$ die Teilmenge der primitiven $n$-ten Einheitswurzeln. Mit dem Isomorphismus $U_n \simeq \mathbb{Z}/n'\mathbb{Z}$ können wir $U_n^{\mathrm{pr}}$ mit der Menge der Einheiten des Rings $\mathbb{Z}/n'\mathbb{Z}$ identifizieren. Es gilt $\bar{m} \in (\mathbb{Z}/n\mathbb{Z})^*$ genau dann, wenn es ein $k \in \mathbb{Z}$ mit $\bar{k}\bar{m} = 1$ gibt, was genau dann möglich ist, wenn $m$ und $n$ teilerfremd sind. Damit entspricht $U_n^{\mathrm{pr}}$ der Teilmenge

$$(\mathbb{Z}/n\mathbb{Z})^* = \{\bar{m} \in \mathbb{Z}/n\mathbb{Z} \mid \operatorname{ggT}(m, n) = 1\}.$$

Konkret für z. B. $n = 8$ ist $(\mathbb{Z}/8\mathbb{Z})^* = \{\bar{1}, \bar{3}, \bar{5}, \bar{7}\}$.

Wir erinnern uns, dass die *eulersche $\varphi$-Funktion*

$$\varphi(n) \coloneqq |(\mathbb{Z}/n\mathbb{Z})^*| = |\{1 \leq m < n \mid \operatorname{ggT}(m, n) = 1\}|$$

ist. Um $\varphi(n)$ zu berechnen, betrachten wir folgende Fälle:

(i) Für $n = p$ ist $\varphi(p) = p - 1$.

(ii) Seien $n_1$ und $n_2$ teilerfremd. Dann ist $\mathbb{Z}/n_1 n_2\mathbb{Z} \simeq \mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z}$ als Ringe.[56] Das ergibt $(\mathbb{Z}/n_1 n_2\mathbb{Z})^* \simeq (\mathbb{Z}/n_1\mathbb{Z})^* \times (\mathbb{Z}/n_2\mathbb{Z})^*$, woraus $\varphi(n_1 n_2) = \varphi(n_1)\varphi(n_2)$ folgt.

(iii) Für Primzahlen $p$ ist

$$\varphi(p^k) = |\{1 \le m < p^k \mid p \nmid m\}| = p^k - 1 - (p^{k-1} - 1) = p^{k-1}(p-1).$$

Damit gilt für die Primfaktorzerlegung $n = \prod_{i=1}^m p_i^{k_i}$:

$$\varphi(n) = \prod_{i=1}^m p_i^{k_i - 1}(p_i - 1).$$

Wir fassen zusammen.

**Fakt 4.4.4.** *Seien $K$ ein Körper und $n \ge 1$. Schreibe $n = n'$, falls $\mathrm{char}(K) \nmid n$, oder sonst $n = p^k n'$ mit $\mathrm{char}(K) = p \nmid n'$. Dann gilt $U_n \simeq \mathbb{Z}/n'\mathbb{Z}$ und mit der Primfaktorzerlegung $n' = \prod_i p_i^{k_i}$ gilt*

$$|U_n^{\mathrm{pr}}| = \varphi(n') = \prod_i p_i^{k_i - 1}(p_i - 1).$$

**Lemma 4.4.5.** *Sei $\zeta \in U_n^{\mathrm{pr}}$. Dann ist $K(\zeta)/K$ eine endliche Galoiserweiterung.*

*Beweis.* $K(\zeta)/K$ ist der Zerfällungskörper von $X^n - 1$ da alle Nullstellen von $X^n - 1$ von der Gestalt $\zeta^k$ sind. Daher ist die Körpererweiterung normal. Schreibe $n = p^q n'$ mit $\mathrm{char}(K) = p \nmid n'$ bzw. $n = n'$, falls $\mathrm{char}(K) = 0$. Dann ist $K(\zeta)/K$ Zerfällungskörper von $X^{n'} - 1$ (für den ersten Fall gilt $X^n - 1 = (X^{n'} - 1)^{p^k}$). Aber $X^{n'} - 1$ ist separabel, d. h. $K(\zeta)/K$ ist galoissch. □

*Problem* 4.4.6. Was ist $[K(\zeta) : K]$? Beachte, dass $[K(\zeta) : K] = 1$, falls $\zeta \in K$, und sonst $[K(\zeta) : K] > 1$.

**Definition 4.4.7.** Wir betrachten jetzt $K = \mathbb{Q}$ und eine $n$-te primitive Einheitswurzel $\zeta \in \bar{\mathbb{Q}}$. (Konkret bedeutet das $\zeta = \mathrm{e}^{2\pi \mathrm{i}/n}$ oder allgemeiner $\zeta = \mathrm{e}^{2\pi \mathrm{i} m/n}$ mit $\mathrm{ggT}(m, n) = 1$ nach Einbettung $\bar{Q} \subset \mathbb{C}$.) Dann heißt $\mathbb{Q}(\zeta)/\mathbb{Q}$ der $n$-te **Kreisteilungskörper**. Bis auf Isomorphie ist $\mathbb{Q}(\zeta)$ unabhängig von der Wahl von $\zeta$.

thm:cyclic

**Satz 4.4.8.** *Sei $\mathbb{Q}(\zeta)/\mathbb{Q}$ der $n$-te Kreisteilungskörper. Dann ist $\mathbb{Q}(\zeta)/\mathbb{Q}$ eine Galoiserweiterung von Grad $[\mathbb{Q}(\zeta) : \mathbb{Q}] = \varphi(n)$ mit Galoisgruppe $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q}) \simeq (\mathbb{Z}/n\mathbb{Z})^*$.*

**Bemerkung 4.4.9** (*Satz von Kronecker-Weber*)**.** Sei $K/\mathbb{Q}$ eine endliche abelsche Galoiserweiterung, d. h. mit abelscher Galoisgruppe $\mathrm{Gal}(K/\mathbb{Q})$. Dann existiert ein $n$, sodass $K \subset \mathbb{Q}(\zeta)$, wobei $\zeta$ eine $n$-te primitive Einheitswurzel ist. In diesem Fall gibt es eine Projektion $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q}) \twoheadrightarrow \mathrm{Gal}(K/\mathbb{Q})$ nach dem Hauptsatz der Galoistheorie 4.2.1.

*Beweis von Satz 4.4.8.* Wir fangen erst mit einem beliebigen Körper $K$ statt $\mathbb{Q}$ an. Sei $n = p^k n'$ mit $\mathrm{char}(K) = p \nmid n'$, oder $n = n'$ für $\mathrm{char}(K) = 0$. Dann haben wir $U_n \simeq (\mathbb{Z}/n'\mathbb{Z}, +)$

[56] Das ist der *chinesische Restsatz*.

und $U_n^{\mathrm{pr}} \simeq (\mathbb{Z}/n'\mathbb{Z})^*$. Weil jeder $K$-Automorphismus auf $K(\zeta)$ die Elemente in $U_n$ permutiert, erhalten wir einen wohldefinierten Gruppenhomomorphismus

$$\mathrm{Gal}(K(\zeta)/K) \hookrightarrow \mathrm{Bij}(U_n) \xrightarrow{\sim} U_n^{\mathrm{pr}} \xrightarrow{\sim} (\mathbb{Z}/n'\mathbb{Z})^*, \qquad \sigma \longmapsto \sigma|_{U_n} \longmapsto \sigma(\zeta) = \zeta^i \longmapsto i.$$

Dieser ist offenbar injektiv und impliziert

$$[K(\zeta) : K] = |\mathrm{Gal}(K(\zeta)/K)| \leq |(\mathbb{Z}/n'\mathbb{Z})^*| = \varphi(n').$$

Als nächstes spezialisieren wir auf $K = \mathbb{Q}$ und zeigen, dass der obige Gruppenhomomorphismus bijektiv ist. (Ab jetzt ist $n = n'$.) Dazu sei $f \in \mathbb{Q}[X]$ das Minimalpolynom von $\zeta \in \mathbb{Q}(\zeta)$. Sodann ist $[\mathbb{Q}(\zeta) : \mathbb{Q}] = \deg(f)$ und es genügt zu zeigen, dass $\deg(f) \geq \varphi(n)$. Wir zerlegen $X^n - 1 \in \mathbb{Z}[X]$ in irreduzible Faktoren $X^n - 1 = f_1 \cdots f_k$. Dann sind die Leitkoeffizienten der $f_i$ dann $\pm 1$ und wir können o. B. d. A. annehmen, dass die $f_i$ normiert und damit primitiv sind. Nach Korollar 2.4.8 sind $f_i \in \mathbb{Q}[X]$ irreduzibel. Also ist $f \mid X^n - 1$; sagen wir o. B. d. A. $f = f_1$. Setze $g \coloneqq f_2 \cdots f_k$.

Definiere für eine beliebige Primzahl $p$ die Reduktion modulo $p$:

$$\mathbb{Z}[X] \twoheadrightarrow \mathbb{Z}/p[X] = \mathbb{F}_p[X], \qquad h \longmapsto \bar{h}. \tag{4.4.10}$$

{eqn:cyclic:2}

Um $\deg(f) \geq \varphi(n)$ zu zeigen, müssen wir nur $\varphi(n)$ viele Nullstellen von $f$ finden. Es ist hinreichend, wenn alle $n$-ten primitiven Einheitswurzeln Nullstellen von $f$ sind. Angenommen es gibt eine $n$-te primitive Einheitswurzel $\zeta'$ mit $f(\zeta') \neq 0$.

itm:cyclic

(i) Wir betrachten zunächst $\zeta' = \zeta^p$ für eine Primzahl $p$. Betrachte (4.4.10). Da $\zeta'$ Nullstelle von $X^n - 1 = fg$ ist, folgt $g(\zeta') = g(\zeta^p) = 0$, d. h. $\zeta$ ist eine Nullstelle von $g(X^p)$. Da $f$ das Minimalpolynom von $\zeta$ ist, gilt dann $f(X) \mid g(X^p)$. Schreibe $g(X^p) = f(X)h(X)$. Unter (4.4.10) erhalten wir $(\bar{g}(X))^p = \bar{g}(X^p) = \bar{f}(X)\bar{h}(X)$. Also sind $\bar{g}(X)$ und $\bar{f}(X)$ nicht teilerfremd in $\mathbb{F}_p[X]$.[57] Folglich haben sie eine gemeinsame Nullstelle in $\bar{\mathbb{F}}_p$. Es gilt aber $X^n - 1 = \bar{f}(X)\bar{g}(X)$, d. h. $X^n - 1$ hat eine mehrfache Nullstelle in $\bar{\mathbb{F}}_p$. Daraus folgt $(X^n - 1)' = nX^{n-1} = 0$, was aber $p \nmid n$ widerspricht ($\zeta' = \zeta^p$ war primitiv).

(ii) Sei nun allgemeiner $\zeta' = \zeta^k$. Schreibe die Primfaktorzerlegung $k = \prod_{i=1}^{l} p_i^{n_i}$, und schreibe $k = k'p_1$. Weil $\zeta'$ primitiv ist, gilt $\mathrm{ggT}(k, n) = 1$, d. h. $p_i \nmid n$ für alle $i$. Insbesondere ist $\zeta^{k'}$ eine $n$-te primitive Einheitswurzel. Nach Induktionsvoraussetzung ist $f(\zeta^{k'}) = 0$ und mit demselben Beweis wie in (i) folgt $f((\zeta^{k'})^{p_1}) = f(\zeta^k) = 0$, was $f(\zeta') = f(\zeta^k) \neq 0$ widerspricht. □

**Korollar 4.4.11.** *Seien $\zeta_m, \zeta_n \in \bar{\mathbb{Q}}$ eine $m$-te bzw. ein $n$-te primitive Einheitswurzel mit $\mathrm{ggT}(m, n) = 1$. Dann gelten:*

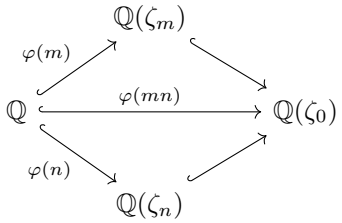
(i) $\mathbb{Q}(\zeta_m) \cap \mathbb{Q}(\zeta_n) = \mathbb{Q}$.

(ii) $\mathrm{Gal}(\mathbb{Q}(\zeta_m, \zeta_n)/\mathbb{Q}) \simeq \mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q}) \times \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$.

*Beweis.*

[57] Es gilt $\deg(\bar{f}(X)) > 0$ da $\deg(f) > 0$ und $f$ normiert ist.

(i) Es gilt $\mathbb{Q}(\zeta_m, \zeta_n) = \mathbb{Q}(\zeta_0)$ mit $\zeta_0 \coloneqq \zeta_m\zeta_n$, wobei $\zeta_0$ wegen $\mathrm{ggT}(m,n) = 1$ eine primitive $mn$-te Einheitswurzel ist (Aufgabe 67). ($\zeta_m$ und $\zeta_n$ sind als Nullstellen von $X^{mn} - 1$ auch im Zerfällungskörper $\mathbb{Q}(\zeta_0)$.) Betrachte nun folgendes kommutative Diagramm:




Da $\mathrm{ggT}(m,n) = 1$, gilt $\varphi(mn) = \varphi(m)\varphi(n)$. Somit folgt aus der Produktformel 3.5.8

$$[\mathbb{Q}(\zeta_0) : \mathbb{Q}(\zeta_m)] = \varphi(n), \qquad [\mathbb{Q}(\zeta_0) : \mathbb{Q}(\zeta_n)] = \varphi(m). \tag{4.4.12}$$

{eqn:cyclic:mixed}

Andererseits haben wir den Turm $\mathbb{Q} \subset \mathbb{Q}(\zeta_m) \cap \mathbb{Q}(\zeta_n) \subset \mathbb{Q}(\zeta_n)$ und mit der Produktformel 3.5.8 folgt

$$\varphi(n) = [\mathbb{Q}(\zeta_n) : \mathbb{Q}] = [\mathbb{Q}(\zeta_n) : \mathbb{Q}(\zeta_m) \cap \mathbb{Q}(\zeta_n)][\mathbb{Q}(\zeta_m) \cap \mathbb{Q}(\zeta_n) : \mathbb{Q}].$$

Unser Ziel ist es zu zeigen, dass der rechte Faktor 1 ist. Also genügt es nachzuweisen, dass der linke Faktor $\varphi(n)$ ist. Wegen $\mathbb{Q}(\zeta_n) = (\mathbb{Q}(\zeta_m) \cap \mathbb{Q}(\zeta_n))(\zeta_n)$ ist der linke Faktor $\deg(\zeta_n)$ über $\mathbb{Q}(\zeta_m) \cap \mathbb{Q}(\zeta_n)$. Aber $\mathbb{Q}(\zeta_m) \cap \mathbb{Q}(\zeta_n) \subset \mathbb{Q}(\zeta_m)$, d. h. der obige Grad $\deg(\zeta_n)$ ist mindestens der Grad $\deg(\zeta_n)$ über $\mathbb{Q}(\zeta_m)$; dieser ist aber mindestens $\varphi(n)$ nach (4.4.12). Folglich haben wir $[\mathbb{Q}(\zeta_n) : \mathbb{Q}(\zeta_m) \cap \mathbb{Q}(\zeta_n)] = \varphi(n)$ wie gewünscht.

(ii) Das folgt aus Korollar 4.2.4. □

*Problem* 4.4.13. Wie sieht das Minimalpolynom einer $n$-ten Einheitswurzel aus?

**Definition 4.4.14.** Sei $K$ ein beliebiger Körper mit $U_n^{\mathrm{pr}} = \{\zeta_1, \dots, \zeta_{\varphi(n')}\} \subset \bar{K}$, wobei $n' = n$, falls $\mathrm{char}(K) = 0$, und $n = p^k n'$ mit $p = \mathrm{char}(K) \nmid n'$, sonst. Definiere das $n$-te **Kreisteilungspolynom** als

$$\Phi_n \coloneqq \prod_{i=1}^{\varphi(n')} (X - \zeta_i) \in \bar{K}[X].$$

fact:cyclotomic

**Fakt 4.4.15.**

(i) $\Phi_n$ *ist normiert und separabel.*

(ii) $\Phi_n \in K[X]$.

(iii) $X^{n'} - 1 = \prod_{d \mid n'} \Phi_d(X)$ *mit* $n = n'$, *falls* $\mathrm{char}(K) = 0$, *und* $n = p^k n'$ *mit* $p = \mathrm{char}(K) \mid n'$, *sonst.*

*Beweis.*

(i) Normiertheit ist offensichtlich und Separabilität gilt wegen $\zeta_i \neq \zeta_j$ für alle $i \neq j$.

(ii) Wir erinnern uns, dass $K(\zeta_1)/K$ galoissch ist und alle $\zeta_i$ enthält. Zudem gibt es die Einbettung $\mathrm{Gal}(K(\zeta_1)/K) \hookrightarrow \mathrm{Bij}(U_n^{\mathrm{pr}})$, d. h. jedes $\sigma \in \mathrm{Gal}(K(\zeta_1)/K)$ permutiert die $\zeta_i$ und lässt damit $\Phi_n$ fix. Also gilt $\Phi_n \in K(\zeta_1)^{\mathrm{Gal}(K(\zeta_1)/K)}[X] = K[X]$.

(iii) A priori gilt $X^{n'} - 1 = \prod_{i=1}^{N}(X - \mu_i)$ mit $U_{n'} = U_n = \{\mu_1, \ldots, \mu_N\}$. Wähle für jedes $\mu \in U_n$ das minimale $d$ mit $\mu^d = 1$. Dann ist $\mu$ eine primitive $d$-te Einheitswurzel. Wir erhalten

$$X^{n'} - 1 = \prod_{i=1}^{N}(X - \mu_i) = \prod_{d|n'} \prod_{\{\text{prim. } d\text{-te EW}\}} (X - \mu) = \prod_{d|n'} \Phi_d(X). \qquad \square$$

**Satz 4.4.16.** *Sei $K = \mathbb{Q}$. Dann ist $\Phi_n \in \mathbb{Z}[X]$ und in $\mathbb{Q}[X]$ irreduzibel. Insbesondere ist $\Phi_n$ das Minimalpolynom jeder primitiven $n$-ten Einheitswurzel.*

*Beweis.* Wir wissen, dass $[\mathbb{Q}(\zeta) : \mathbb{Q}] = \varphi(n)$ für jede primitive $n$-te Einheitswurzel $\zeta$. Ferner wissen wir, dass wenn $f$ das Minimalpolynom von $\zeta$ ist, dann $f \mid \Phi_n$ wegen $\Phi_n(\zeta) = 0$ folgt. Also ist $\deg(f) \leq \deg(\Phi_n) = \varphi(n)$. Andererseits ist $\varphi(n) = [\mathbb{Q}(\zeta) : \mathbb{Q}] = \deg(f)$, d. h. $\deg(f) = \deg(\Phi_n)$. Weil $f$ und $\Phi_n$ beide normiert sind, gilt $f = \Phi_n$ und $\Phi_n \in \mathbb{Q}[X]$ ist irreduzibel. Ferner wissen wir, dass $\Phi_n \mid X^n - 1$. Weil $\Phi_n$ und $X^n - 1 \in \mathbb{Z}[X]$ beide normiert sind, folgt aus Korollar 2.4.8, dass $\Phi_n \in \mathbb{Z}[X]$ irreduzibel ist. $\square$

*Beispiel* 4.4.17.

(i) Per Definition $\Phi_1 = X - 1$.

(ii) Sei $n = p$ eine Primzahl. Dann ist $\deg(\Phi_p) = \varphi(p) = p - 1$. Aus Fakt 4.4.15 folgt $X^p - 1 = \Phi_1\Phi_p = (X - 1)\Phi_p$, was die Primfaktorzerlegung ist. Für $p = 2$ gilt also $\Phi_2 = X + 1$ wegen $X^2 - 1 = (X - 1)(X + 1)$. Für $p = 3$ gilt dann $\Phi_3 = X^2 + X + 1$ wegen $X^3 - 1 = (X - 1)(X^2 + X + 1)$. Für $p = 5$ gilt $\Phi_5 = X^4 + X^3 + X^2 + X + 1$. Allgemein gilt
$$\Phi_p = X^{p-1} + \cdots + X + 1.$$

(iii) Was ist $\Phi_4$? Es gilt
$$X^4 - 1 = \Phi_1\Phi_2\Phi_4 = (X - 1)(X + 1)\Phi_4.$$
Also ist $\Phi_4 = X^2 + 1$.

(iv) Was ist $\Phi_6$? Es gilt
$$X^6 - 1 = \Phi_1\Phi_2\Phi_3\Phi_6 = (X - 1)(X + 1)(X^2 + X + 1)\Phi_6.$$
Mit Polynomdivision 2.2.10 folgt $\Phi_6 = X^2 - X - 1$.

**Bemerkung 4.4.18.** Man könnte meinen, dass die Koeffizienten der Kreisteilungspolynome stets aus $0, \pm 1$ stammen. Das ist aber nicht der Fall: Das kleinste $n$, für dass die

Koeffizienten von $\Phi_n$ nicht alle $0, \pm 1$ sind, ist $n = 105$. Es gilt

$$\Phi_{105} = X^{48} + \cdots - 2X^{41} - \cdots - 2X^2 + 1.$$

Tatsächlich können die Koeffizienten beliebig groß werden und an dem Wachstumsverhalten der Koeffizienten in Abhängigkeit von $n$ wird noch geforscht.

VL 23
19.01.24

## 4.5 Konstruktion mit Zirkel und Lineal

VL 24
22.01.24

Nun wollen wir eine Anwendung der Galoistheorie sehen: Wir wollen die Unmöglichkeit einiger klassischer geometrischer Konstruktionsprobleme zeigen.

**Definition 4.5.1.** Sei $M \subset \mathbb{C}$ eine Teilmenge mit $|M| \geq 2$. Ein Punkt $z \in \mathbb{C}$ heißt **elementar mit Zirkel und Lineal aus $M$ konstruierbar**, falls eine er drei folgenden Aussagen gilt:

(i) Es gibt Geraden $L_1, L_2 \subset \mathbb{C}$ und $z_1, \ldots, z_4 \in M$, wobei $z_1 \neq z_2$ in $L_1$ sowie $z_3 \neq z_4$ in $L_2$ liegen, sodass $L_1 \cap L_2 = \{z\}$ (s. Abb. 4.3, insbesondere sind $z_1, \ldots, z_4$ nicht kollinear).

(ii) Es gibt eine Gerade $L \subset \mathbb{C}$, einen Kreis $K \subset \mathbb{C}$ und $z_1, \ldots, z_5 \in M$, wobei $z_4 \neq z_5$ in $L$ liegen und $K$ ein Kreis mit Mittelpunkt $z_1$ und Radius $|z_3 - z_2|$ ist, sodass $z \in L \cap K$ (s. Abb. 4.4).

(iii) Es gibt Kreise $K_1, K_2 \subset \mathbb{C}$ und $z_1, \ldots, z_6 \in M$, wobei $K_1$ und $K_2$ Mittelpunkte $z_1 \neq z_2$ und Radien $|z_3 - z_2|$ bzw. $|z_6 - z_5|$ sind, sodass $z \in K_1 \cap K_2$ (s. Abb. 4.5).

**Definition 4.5.2.** Sei $M \subset \mathbb{C}$ eine Teilmenge mit $|M| \geq 2$. Wir definieren rekursiv $M_0 \coloneqq M$ und $M_{i+1} \subset \mathbb{C}$ als die Menge aller Punkte $z \in \mathbb{C}$, die elementar durch Zirkel und Lineal aus $M_i$ konstruierbar sind. Wir erhalten eine Kette $M_0 \coloneqq M \subset M_1 \subset M_2 \subset \cdots \subset \mathbb{C}$. Definiere

$$L_M \coloneqq \bigcup_{i=0}^{\infty} M_i.$$

Ein Punkt $z \in \mathbb{C}$ lässt sich mit **Zirkel und Lineal aus $M$ konstruieren**, falls $z \in L_M$. Ein Punkt $z \in \mathbb{C}$ lässt sich mit **Zirkel und Lineal konstruieren**, falls $z \in L_{\{0,1\}}$.

**Aufgabe 4.5.3.** Es gilt $M_i \subset M_{i+1}$, d. h. wenn $z_1, z_2 \in M_i$, dann $z_1, z_2 \in M_{i+1}$.

*Lösung.* Da $|M_i| \geq 2$, können wir o. B. d. A. $z_1 \neq z_2$ wählen. Nun ist $z_2$ ein Schnittpunkt der Gerade durch $z_1 \neq z_2$ und des Kreises mit Mittelpunkt $z_1$ und Radius $|z_2 - z_1|$. Analog für $z_1$.

**Fakt 4.5.4.** *Falls $0, 1 \in M$, so folgt aus $z \in L_M$ schon $\bar{z} \in L_M$.*

*Beweisidee.* Das muss man mit Kreisgleichungen in $\mathbb{C}$ nachrechnen, aber die suggerierte Konstruktion in Abb. 4.6 liefert tatsächlich $\bar{z}$. □

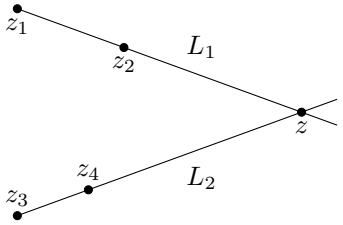



fig:geometry:1

Abbildung 4.3: Geraden $L_1$ durch $z_1, z_2 \in M$ und $L_2$ durch $z_3, z_4 \in M$ schneiden sich in $z$.

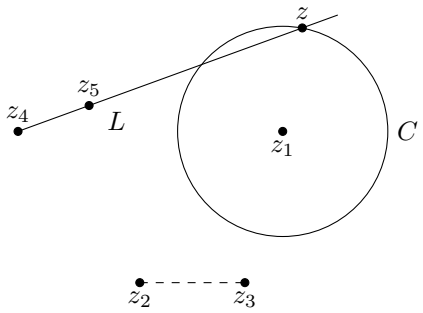



fig:geometry:2

Abbildung 4.4: Gerade $L$ durch $z_4, z_5 \in M$ und Kreis $C$ mit Mittelpunkt $z_1 \in M$ und Radius $|z_3 - z_2|$ (mit $z_2, z_3 \in M$) schneiden sich in $z$.

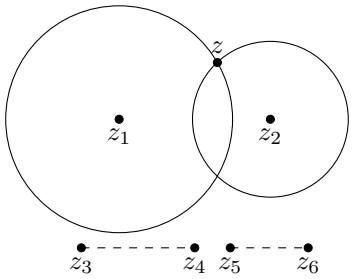
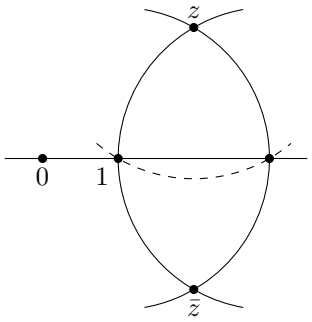



fig:geometry:3

Abbildung 4.5: Kreise $C_1$ mit Mittelpunkt $z_1 \in M$ und Radius $|z_3 - z_2|$ sowie $C_2$ mit Mittelpunkt $z_2 \in M$ und Radius $|z_6 - z_5|$ (mit $z_3, z_4, z_5, z_6 \in M$) schneiden sich in $z$.




geometry:conjugate

Abbildung 4.6: Konstruktion der komplex Konjugierten.

thm:geometry

**Satz 4.5.5.** *Seien $0, 1 \in M \subset \mathbb{C}$ und $z \in \mathbb{C}$. Dann sind folgende Aussagen äquivalent:*

itm:geometry:1

(i) *$z \in L_M$, d. h. $z$ ist aus $M$ mit Zirkel und Lineal konstruierbar.*

itm:geometry:2

(ii) *Es gibt einen Turm*

$$K_M \coloneqq \mathbb{Q}(M \cup \bar{M}) \subset K_1 \subset \cdots \subset K_n \subset \mathbb{C}$$

*mit $z \in K_n$ und $[K_{i+1} : K_i] = 2$. Hier ist $\bar{M} \coloneqq \{\bar{z} \in \mathbb{C} \mid z \in M\}$.*

itm:geometry:3

(iii) *Es gibt eine normale Körpererweiterung $L/K_M$ mit $z \in L$ und $[L : K_M] = 2^k$.*

Bevor wir diese wichtige Aussage zeigen, werden wir sie anwenden.

ometry:constructible

**Korollar 4.5.6.** *Sei $0, 1 \in M \subset \mathbb{C}$. Dann gelten folgende Aussagen:*

(i) *$L_M$ ist ein Körper.*

(ii) *$L_M/K_M \coloneqq \mathbb{Q}(M \cup \bar{M})$ ist algebraisch.*

(iii) *Für alle $a \in L_M$ mit Minimalpolynom $p_a \in K_M[X]$ hat Grad $\deg(p_a) = 2^r$.*

*Beweis.*

(i) Seien $z_1, z_2 \in L_M$. Wir benutzen Satz 4.5.5, (i) $\implies$ (ii): Es gibt Türme

$$K_0 = K_M \subset K_1 \subset \cdots \subset K_n \ni z_1, \qquad K_0 = K_M \subset K_1' \subset \cdots \subset K_m' \ni z_2$$

mit $[K_{i+1} : K_i] = 2$ und $[K'_{j+1} : K'_j] = 2$. Wegen $[K_{i+1} : K_i] = 2$ gilt $K_{i+1} = K_i(a_i)$ mit $\deg_{K_i}(a_i) = 2$ (tatsächlich funktioniert jedes $a_i \in K_{i+1} \setminus K_i$). Wir setzen nun den zweiten Turm fort zu

$$K_M \subset K_1' \subset \cdots \subset K_m' \subset K'_{m+1} \coloneqq K_m'(a_0) \subset \cdots \subset K'_{m+n} \coloneqq K'_{m+n-1}(a_{n-1}).$$

Das sind alles Körpererweiterungen von Grad 2 mit $z_1, z_2 \in K_m' \cup K_n \subset K'_{m+n}$. Somit sind $z_1 + z_2, z_1 z_2, z_1^{-1}, \cdots \in K'_{m+n}$. Nach Satz 4.5.5, (ii) $\implies$ (i) sind alle diese Elemente mit Zirkel und Lineal aus $M$ konstruierbar, d. h. sie sind tatsächlich in $L_M$ und $L_M$ ist ein Körper.

(ii) Offenbar sind (wegen Satz 4.5.5, (i) $\implies$ (ii)) alle Elemente in $L_M$ algebraisch über $K_M$, d. h. $L_M/K_M$ ist algebraisch.

(iii) Sei $a \in L_M$. Dann gibt es einen Turm $K_M \subset K_1 \subset \cdots \subset K_n \ni a$ mit $[K_{i+1} : K_i] = 2$ und $K_M(a) \subset K_n$. Folglich ist $\deg(p_a) = [K(a) : K_M] \mid [K_n : K_M] = 2^n$, d. h. $\deg(p_a) = 2^r$. □

try:inconstructible

**Korollar 4.5.7.** *Sei $z \in \mathbb{C}$, sodass*

(i) *$z$ nicht algebraisch ist (d. h. $z \in \bar{\mathbb{Q}}$) oder*

(ii) *wenn $z$ doch algebraisch ist, dann für das Minimalpolynom $\deg(p_a) \neq 2^r$.*

*Dann ist $z$ nicht mit Zirkel und Lineal konstruierbar.*

*Beweis.* Wende Korollar 4.5.6 auf den Fall $M = \{0, 1\}$ an. □

**Beobachtung 4.5.8** (Quadratur des Kreises)**.** *Frage:* Kann man ein Quadrat mit Zirkel und Lineal von Flächeninhalt eines Einheitskreises konstruieren?

Der Einheitskreis mit Mittelpunkt 0 und Radius 1 hat Flächeninhalt $\pi$. Wäre die Konstruktion möglich, so können wir ein achsenparalleles Quadrat mit Mittelpunkt 0 und Seitenlänge $2z$ konstruieren, sodass $(2z)^2 = \pi$ (s. Abb. 4.7). Falls also $z$ mit Zirkel und Lineal konstruierbar ist, so gilt $\sqrt{\pi} \in \bar{\mathbb{Q}}$ bzw. $\pi \in \bar{\mathbb{Q}}$.

Die Transzendenz von Zahlen zu zeigen, ist sehr schwierig. Euler (1744) zeigte, dass $e \notin \mathbb{Q}$, und Hermite (1873) zeigte, dass $e \notin \bar{\mathbb{Q}}$. Tatsächlich konnte Lindemann (1882) zeigen, dass $\pi \notin \bar{\mathbb{Q}}$, was eine Menge Analysis benutzt. Damit ist nach Korollar 4.5.7 die Quadratur des Kreises unmöglich.

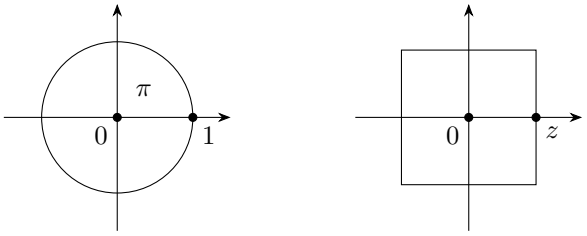



fig:square

Abbildung 4.7: Quadratur des Kreises.

**Beobachtung 4.5.9** (Würfeldopplung)**.** Folgendes Resultat wurde zuerst von Pierre Wantzel (1814–1848) bewiesen.

*Frage:* Gegeben sei ein Würfel mit Kantenlänge 1. Kann man mit Zirkel und Lineal einen Würfel doppelten Volumens konstruieren?

Ein Würfel mit Kantenlänge 1 hat Volumen 1. Wäre ein Würfel mit Volumen 2 konstruierbar, so gelte für seine Kantenlänge $\sqrt[3]{2} \in \bar{\mathbb{Q}}$.

Das Minimalpolynom von $\sqrt[3]{2}$ ist $p_{\sqrt[3]{2}} = X^3 - 2 \in \mathbb{Q}[X]$, was irreduzibel von Grad 3 ist. Also folgt aus Korollar 4.5.7, dass $\sqrt[3]{3}$ nicht mit Zirkel und Lineal konstruierbar ist. Insbesondere ist die Würfeldopplung unmöglich.

**Beobachtung 4.5.10** (Winkeldreiteilung)**.** Auch folgendes Resultat geht auf Wantzel zurück.

*Frage:* Lässt sich allgemein jeder gegebene Winkel mit Zirkel und Lineal dreiteilen?

Winkel zu halbieren ist tatsächlich möglich (s. Abb. 4.8). Wir werden zeigen, dass für $\theta = 60°$ die Dreiteilung nicht möglich ist, d. h. $\frac{\theta}{3} = 20°$ nicht mit Zirkel und Lineal konstruierbar ist.

Ein Winkel $\theta$ lässt sich nach Definition genau dann mit Zirkel und Lineal konstruieren, wenn $z$ wie in Abb. 4.9 konstruierbar ist. Das ist aber genau dann möglich, wenn $\cos(\theta) = \frac{1}{2}(z + \bar{z})$ mit Zirkel und Lineal konstruierbar ist.

Mit der eulerschen Identität gilt

$$(\cos(\alpha) + \mathrm{i}\sin(\alpha))^3 = \mathrm{e}^{\mathrm{i}\alpha 3} = \cos(3\alpha) + \mathrm{i}\sin(3\alpha)$$

Für den Realteil folgt dann mit dem trigonometrischen Pythagoras

$$\begin{aligned}\cos(3\alpha) &= \cos^3(\alpha) - 3\cos(\alpha)\sin^2(\alpha)\\ &= \cos^3(\alpha) - 3\cos(\alpha)(1 - \cos^2(\alpha))\\ &= 4\cos^3(\alpha) - 3\cos(\alpha).\end{aligned}$$

Für $3\alpha = \theta = 60°$ gilt dann $\cos(3\alpha) = \frac{1}{2}$. Also ist $\cos(\alpha) = \cos(\frac{\theta}{3})$ Nullstelle des Polynoms $8X^3 - 6X - 1 \in \mathbb{Q}[X]$. Dieses Polynom ist irreduzibel (das folgt per Widerspruch, wenn man annimmt, dass es eine Nullstelle $\frac{p}{q} \in \mathbb{Q}$ mit $\mathrm{ggT}(p, q) = 1$ gibt).[58] Somit hat $\cos(20°)$ Grad 3 über $\mathbb{Q}$, was keine Zweierpotenz ist. Nach Korollar 4.5.7 ist also $\cos(20°)$ nicht mit Zirkel und Lineal konstruierbar.

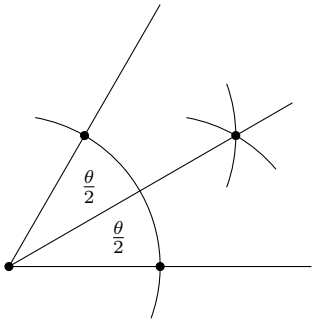



fig:anglebisect

Abbildung 4.8: Halbierung eines Winkels $\theta$.

[58] Die Idee ist der *Satz über rationale Nullstellen*: Ist $p/q \in \mathbb{Q}$ mit $\mathrm{ggT}(p, q) = 1$ eine Nullstelle des Polynoms $a_n X^n + a_{n-1} X^{n-1} + \cdots + a_0 \in \mathbb{Z}[X]$, so gilt $p \mid a_0$ und $q \mid a_n$.

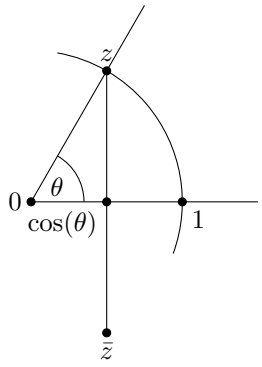



fig:angle

Abbildung 4.9: Konstruktion eines Winkels $\theta$.

**Beobachtung 4.5.11** (regelmäßige $n$-Ecke)**.** *Frage:* Welche regelmäßigen $n$-Ecke lassen sich mit Zirkel und Lineal konstruieren (Abb. 4.10)?

Wir betrachten zunächst den Fall, dass $n = p$ eine Primzahl ist. Dann wissen wir, dass das Minimalpolynom $p_{\zeta_p} = \Phi_p = X^{p-1} + \cdots + X + 1$ irreduzibel ist, wobei $\deg(\zeta_p) = p - 1$. Falls $\zeta_p$ mit Zirkel und Lineal konstruierbar ist, dann gilt $p - 1 = 2^r$ bzw. $p = 2^r + 1$. Das ist nur möglich, wenn $r = 2^k$ eine Zweierpotenz ist, d. h. $p = 2^{2^k} + 1$. Dies sind die sog. **Fermatzahlen** $F_k = 2^{2^k} + 1$. Die ersten Fermatzahlen sind

$$F_0 = 3, \qquad F_1 = 5, \qquad F_2 = 17, \qquad F_3 = 257, \qquad F_4 = 65\,537,$$

was alles Primzahlen sind.

*Frage:* Sind alle Fermatzahlen Primzahlen? Nein! $F_5 = 641 \cdot 6\,700\,417$ ist bereits keine Primzahl. Ein noch offenes Problem ist, ob es weitere fermatsche Primzahlen gibt. Wir wissen bereits, dass $F_n$ für $5 \leq n \leq 32$ keine Primzahl ist, und die Vermutung ist, dass es wahrscheinlich wirklich keine weiteren gibt.

Aus Korollar 4.5.7 folgt somit, dass regelmäßige 7-, 11- oder 13-Ecke nicht mit Zirkel und Lineal konstruierbar sind.

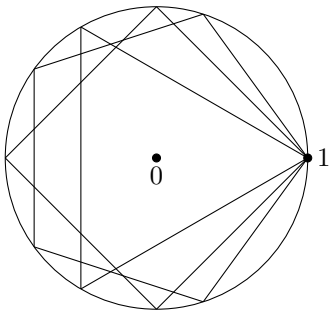



fig:ngon

Abbildung 4.10: Eingeschriebene $n$-Ecke für $n = 3, 4, 5$.

**Aufgabe 4.5.12.** Zeige, dass wenn $p = 2^r + 1$ eine Primzahl ist, dann $r = 2^k$.

*Lösung.* Schreibe $r = l2^k$ mit $2 \nmid l$. Dann gilt

$$2^r + 1 = 1 - (-2^{2^k})^l = \underbrace{(1 + 2^{2^k})}_{>1}\underbrace{(1 - 2^{2^k} + (2^{2^k})^2 - \cdots + (2^{2^k})^{l-1})}_{\geq 1}.$$

Falls das eine Primzahl ist, so muss eines der Faktoren auf der rechten Seite 1 sein. Nun ist der zweite Faktor genau dann 1, wenn $l = 1$.

Folgende Aussage geht auf Carl Friedrich Gauss (1771–1855) zurück.

**Satz 4.5.13** (Gauss, 30. März 1796, Tagebuch 365)**.** *Das regelmäßige 17-Eck ist mit Zirkel und Lineal konstruierbar: Es gilt*

$$\cos\left(\frac{2\pi}{17}\right) = \frac{1}{16}\Bigg(-1 + \sqrt{17} + \sqrt{2(17 - \sqrt{17})} + 2\sqrt{17 + 3\sqrt{17} - \sqrt{2(17 - \sqrt{17})} - 2\sqrt{2(17 + \sqrt{17})}}\Bigg) \in L.$$

*Diese Zahl liegt in einer geeigneten Galoiserweiterung $L/\mathbb{Q}$ mit $[L : \mathbb{Q}] = 16$.*

Aus Sätze 4.5.5 und 4.4.8 folgt allgemein:

**Satz 4.5.14.** *Ein regelmäßiges $n$-Eck ist genau dann konstruierbar, wenn $p_{\zeta_n} = \Phi_n$ mit Grad $\deg(\Phi_n) = \varphi(n) = 2^r$. Das ist genau dann der Fall, wenn $n = 2^m \prod_i p_i$ mit paarweise verschiedenen fermatschen Primzahlen $p_i$.*

*Beweis von Satz 4.5.5.*

- (i) $\implies$ (ii): Per Induktion genügt es zu zeigen, dass wenn $z \in \mathbb{C}$ *elementar* mit Zirkel und Lineal aus $M$ konstruierbar ist, dann es einen Turm

  $$K_M = K_0 \subset K_1 \subset \cdots \subset K_n \ni z$$

  mit $[K_{i+1} : K_i] = 2$ und $K_n = \{\bar{z} \mid z \in K_n\}$ gibt.[59]

  Wir unterscheiden drei Fälle.

  (a) *$z$ ist der Schnittpunkt zweier Geraden.* Seien $z_1, \ldots, z_4 \in M$ wie in Abb. 4.3. Dann gilt für $z$

  $$z = z_1 + t(z_2 - z_1) = z_3 + s(z_4 - z_3)$$

  mit $s, t \in \mathbb{R}$. Wir erhalten ein Gleichungssystem

  $$\begin{cases} \mathrm{Re}(z_1) + t\,\mathrm{Re}(z_2 - z_1) = \mathrm{Re}(z_3) + s\,\mathrm{Re}(z_4 - z_3), \\ \mathrm{Im}(z_1) + t\,\mathrm{Im}(z_2 - z_1) = \mathrm{Im}(z_3) + s\,\mathrm{Im}(z_4 - z_3). \end{cases}$$

[59] Die zweite Bedingung hatter der Dozent vergessen. Ansonsten funktioniert die Induktion nicht.

Also ist $(t, s) \in \mathbb{R}^2$ die Lösung des folgenden inhomogenen[60] linearen Gleichungssystems

$$\begin{cases} \mathrm{Re}(z_2 - z_1)x_1 - \mathrm{Re}(z_4 - z_3)x_2 = \mathrm{Re}(z_3 - z_1), \\ \mathrm{Im}(z_2 - z_1)x_1 - \mathrm{Im}(z_4 - z_3)x_2 = \mathrm{Im}(z_3 - z_1). \end{cases} \tag{4.5.15}$$

{eqn:geometry}

mit Koeffizienten in $\mathbb{R}$. Beachte, dass (4.5.15) eine Lösung hat! Wegen $z_1, \dots, z_4 \in M \subset K_M = \mathbb{Q}(M \cup \bar{M})$ sind auch $\bar{z}_1, \dots, \bar{z}_4 \in K_M$. Also sind $\mathrm{Re}(z_i), \mathrm{Im}(Z_i) \in K_M$ und (4.5.15) ist ein lineares Gleichungssystem mit Koeffizienten in $K_M$. Falls es eine Lösung hat, so muss sie in $K_M$ liegen. Es gibt aber eine Lösung $(s, t)$, d. h. $s, t \in K_M$. In diesem Fall können wir $n = 0$ wählen und erhalten den trivialen Turm $K_M \ni z$.

iitm:geometry:2

(b) *$z$ ist der Schnittpunkt einer Gerade und eines Kreises.* Seien $z_1, \dots, z_5 \in M$ wie in Abb. 4.4. Dann erfüllt $z$ die Gleichungen

$$\begin{cases} z = z_4 + t(z_4 - z_5), \\ |z_1 - z|^2 = |z_2 - z_3|^2 \end{cases}$$

mit $t \in \mathbb{R}$. Eingesetzt liefert das eine quadratische Gleichung für die Lösung $t \in \bar{\mathbb{Q}}$. Also ist $z \in K_M(t)$. Setze nun $K_1 \coloneqq K_m(t)$ mit $[K_1 : K_M] \leq 2$ und $K_2 \coloneqq K_1(\bar{z})$ mit $[K_2 : K_1] \leq 2$. Damit erhalten wir einen Turm $K_M \subset K_1 \subset K_2 \ni z$ mit $K_2 = \{\bar{x} \mid x \in K_2\}$, denn $K_M = \mathbb{Q}(M \cup \bar{M})$.

(c*) *$z$ ist der Schnittpunkt zweier Kreise.* Seien $z_1, \dots, z_6 \in M$ wie in Abb. 4.5. Dann erfüllt $z$ die Gleichungen

$$\begin{cases} |z_1 - z|^2 = |z_3 - z_4|^2, \\ |z_2 - z|^2 = |z_5 - z_6|^2. \end{cases}$$

Subtraktion dieser beiden Gleichungen und Umformen liefert eine Geradengleichung der Form $rx + ty = s$ mit $z = x + \mathrm{i}y$ sowie $r, t, s \in \mathbb{R}$. Also ist $z$ ein Schnittpunkt einer Geraden und eines Kreises und wir haben diesen Fall auf (b) zurückgeführt.

- * (ii) $\Longrightarrow$ (i): Sei ein Turm $K_m \subset K_1 \subset \cdots \subset K_n \ni z$ mit $[K_{i+1} : K_i] = 2$ gegeben. Dann ist $K_{i+1} = K_i(a_i)$ mit $\deg_{K_i}(a_i) = 2$. Aus der Lösungsformel für quadratische Polynome folgt, dass o. B. d. A. $a_i$ ein Radikal ist, d. h. $a_i^2 \in K_i$. Wegen $K_M \subset L_M$ genügt es aufgrund Induktion zu zeigen, dass wenn $K_i \subset L_M$, dann auch $K_{i+1} \subset L_M$, d. h., dass wir mit Zirkel und Lineal aus $a_i^2 \in K_i \subset L_M$ die Quadratwurzel ziehen können.

  Wir haben schon gesehen, dass sich jeder Winkel mit Zirkel und Lineal halbieren lässt (Abb. 4.8). Ferner können wir aus jedem $r \in \mathbb{R}_{>0}$ mit Zirkel und Lineal die Quadratwurzel ziehen, indem man z. B. Euklids Höhensatz aus der Satzgruppe des Pythagoras benutzt (betrachte ein rechtwinklige Dreieck mit Hypotenusenabschnitten $r$ und 1; dann ist die Höhe $\sqrt{r}$). Ist also $z = re^{2\pi\mathrm{i}\theta} \in L_M$, so gilt auch $\sqrt{z} \in L_M$.

[60] Dafür braucht man die ganzen Nebenbedingungen, dass $z_1 \neq z_2$ und $z_3 \neq z_4$ sowie, dass $\{z_1, z_2, z_3, z_4\}$ nicht kollinear sind.

- * (ii) $\Longrightarrow$ (iii): Wie wir bereits sahen, ist $K_n$ wie in (ii) aus $K_M$ durch Quadratwurzeln darstellbar, d. h.

$$K_M \subset K_M(a_0) \subset K_M(a_0, a_1) \subset \cdots \subset K_M(a_0, \ldots, a_{n-1}) = K_n$$

mit $a_i^2 \in K_M(a_0, \ldots, a_{i-1})$. Sei

$$L \coloneqq \prod_{j=1}^{r} \sigma_i(K_n)$$

die normale Hülle von $K_n/K_M$ mit $\mathrm{Hom}_{K_M}(K_n, \mathbb{C}) = \{\sigma_1, \ldots, \sigma_r\}$. Genauso wie $K_n$ ist jedes $\sigma_j(K_n)$ aus $\sigma_j(K_M) = K_M$ durch Quadratwurzeln darstellbar ($\sigma_j(a_i)$ ist Nullstelle von $X^2 - \sigma_j(a_i^2) \in \sigma_j(K_i)[X]$). Somit ist auch $L$ aus $K_M$ durch Quadratwurzeln darstellbar, denn es gibt den Turm

$$K_M \subset \sigma_1(K_M) = \sigma_1(K_M)K_M \subset \sigma_1(K_M)\sigma_2(K_M) \subset \cdots \subset \prod_{j=1}^{r} \sigma_j(K_M) = L,$$

wobei die Körpererweiterungen den Grad einer Zweierpotenz haben. Daraus folgt die Aussage.

- (iii) $\Longrightarrow$ (ii): Sei $L/K_M$ eine normale Körpererweiterung mit $[L : K_M] = 2^r$ und $z \in L$. Da $\mathrm{char}(L) = 0$, ist auch $L/K_M$ separabel und damit galoissch. Also ist $\mathrm{Gal}(L/K_M)$ eine Gruppe der Ordnung $2^r$. Mittels Gruppentheorie lässt sich zeigen, dass $\mathrm{Gal}(L/K_M)$ auflösbar ist mit zyklischen Faktoren der Ordnung 2 (Aufgabe 60). Nach dem Hauptsatz der Galoistheorie 4.2.1 korrespondiert diese zu einem Turm wie in (ii). □

## 4.6 Überblick: Gal($f$)

VL 25
26.01.24

Wir haben $f \in K[X]$ mit $K = \mathbb{Q}, \mathbb{R}, \mathbb{C}, \bar{\mathbb{Q}}, \mathbb{F}_p, \mathbb{F}_{p^n}, \bar{\mathbb{F}}_p, \mathbb{Q}(t), \ldots$ betrachtet. Dabei haben wir (je nach Körper) verschiedene Techniken verwendet, um Gal($f$) zu bestimmen.

**Irreduzibilität** Wir haben Polynomdivision mit Rest: Seien $f \in K[X]$ und $g \in K[X]$. Dann können wir $g = fq + r$ mit $\deg(r) < \deg(f)$ schreiben.

*Bemerkung:* Das ist auch für $f \in R[X]$ mit $R$ ein Ring möglich. Für uns war das aber nur ein Hilfsmittel.

Für Integritätsbereiche $R$ haben wir dessen Quotientenkörper $Q(R)$ eingeführt. Es gibt eine Einbettung $R \hookrightarrow Q(R)$, die sich zu $R[X] \hookrightarrow Q(R)[X]$ fortsetzen lässt.

Eigenschaften von Ringen:

$$\text{euklidisch} \Longrightarrow \text{Hauptidealring} \Longrightarrow \text{faktoriell}.$$

Eigenschaften für Elemente:

$$\text{prim} \Longrightarrow \text{irreduzibel}.$$

Die Rückrichtung gilt, falls $R$ faktoriell ist.

*Lemma von Gauß:* Ist $R$ faktoriell, so ist auch $R[X]$ faktoriell.

*Folgerung:*

(i) Falls $f = gh \in Q(R)[X]$ mit $f, g \in R[X]$ und $g$ primitiv, dann $h \in R[X]$.

(ii) Falls $f \in R[X]$ irreduzible, dann $f \in Q(R)[X]$ irreduzibel.

(iii) Falls $f = gh \in Q(R[X])$ mit $f \in R[X]$ und $f$ und $g$ normiert, dann $g, h \in R[X]$.

*Irreduzibilitätskriterien:* Sei $R$ faktoriell, z. B. $R = \mathbb{Z}$. Sei $f = X^n + \cdots \in R[X]$ und sei $p \in R$ prim. Ist $\bar{f} \in R/(p)[X]$ irreduzible, dann ist auch $f \in Q(R)[X]$ irreduzibel. Es ist auch $f \in R[X]$ irreduzibel, da $f$ primitiv ist.

*Eisensteinkriterium:* Seien $R$ faktoriell und $f = a_n X^n + \cdots + a_0 \in R[X]$ primitiv. Falls $p \mid a_0, \ldots, a_{n-1}$ und $p^2 \nmid a_0$, dann ist $f \in R[X]$ irreduzibel.

*Beispiel:*

(i) $X^n - p \in \mathbb{Z}[X]$ ist irreduzibel.

(ii) $\Phi_p = X^{p-1} + X^{p-2} + \cdots + 1$ ist irreduzibel.

*Tricks:*

(i) Sei $f \in K[X]$ mit $\deg(f) = 2, 3$. Dann ist $f$ genau dann reduzibel, wenn $f$ eine Nullstelle in $K$ besitzt.

(ii) Für $K = \mathbb{R}$ und $\deg(f) = 2$ ist $f$ genau dann irreduzibel, wenn $(\frac{p}{2})^2 < q$ genau dann, wenn $D(f) = p^2 - 4q < 0$.

(iii) Für $K = \mathbb{R}$ und $\deg(f) = 3$ ist $f$ nie irreduzibel. Alle drei Nullstellen in $\mathbb{C}$ sind genau dann in $\mathbb{R}$, wenn $D(f) \geq 0$. Hierbei ist $D(f) = -4p^3 - 27q^2$ für $f = X^3 + pX + q$.

(iv) Für $K = \mathbb{Q}$ und $\deg(f) = 2$ ist $f$ genau dann irreduzibel, wenn $\sqrt{D(f)} \notin \mathbb{Q}$. Für $\deg(f) = 3$ haben wir kein konkretes Kriterium.

*Fakt:* Falls $f \in K[X]$ irreduzibel ist und eine Nullstelle $\alpha \in \bar{K}$ hat, und falls $g \in K[X]$ mit $g(\alpha) = 0$, dann $f \mid g$.

Damit haben wir für $\alpha \in \bar{K}$ das Minimalpolynom $p_\alpha = X^n + \cdots$ definiert, was das eindeutige normierte irreduzible Polynom mit $p_\alpha(\alpha) = 0$ ist.

**Separabilität** Sei $f \in K[X]$ normiert. Dann lässt sich $f = \prod_{i=1}^{n}(X - \alpha_i) \in \bar{K}[X]$ schreiben, wobei $\alpha_1, \ldots, \alpha_n$ die Nullstellen von $f$ sind. Dann ist $f$ genau dann separabel, wenn alle Nullstellen paarweise verschieden sind. Äquivalent dazu ist, dass $f$ und $f'$ keine gemeinsamen Nullstellen haben.

Falls $f \in K[X]$ irreduzibel ist, dann ist $f$ genau dann separabel, wenn $f' \neq 0$.

*Folgerung:* Inseparable irreduzible Polynome existieren nur in positiver Charakteristik.

Falls $f \in K[X]$ irreduzibel ist mit $\mathrm{char}(K) = p > 0$, dann können wir $f(X) = g(X^{p^r})$ mit $g$ separabel schreiben. Dann ist $f$ genau dann separabel, wenn $r = 0$ bzw. $f = g$.

Für $f \in K[X]$ ist $L/K$ der Zerfällungskörper von $f$, falls $L = K(\alpha_1, \ldots, \alpha_n)$ mit Nullstellen $\alpha_1, \ldots, \alpha_n \in \bar{K}$ von $f$. $L/K$ ist stets eine endliche Körpererweiterung (und damit algebraisch).

Ist $L$ der Zerfällungskörper von $f$, so gilt für alle $K$-Homomorphismen $\varphi\colon L \hookrightarrow \bar{K}$, d. h. $\varphi|_K = \mathrm{id}$, dann $\varphi(L) = L$. Insbesondere ist $\varphi|_{\{\alpha_1,\ldots,\alpha_n\}}$ eine Permutation.

Der Separabilitätsgrad einer Körpererweiterung $L/K$ ist

$$[L : K]_S \coloneqq |\{\varphi\colon L \hookrightarrow \bar{K} \ K\text{-Homomorphismen}\}| \leq [L : K] = \dim_K(L).$$

Es gilt genau dann Gleichheit, wenn $f$ separabel ist.

## 4.6 Überblick: Gal($f$)

**Galois** Sei $L/K$ eine endliche Körpererweiterung. Dann ist $L/K$ genau dann galoissch, wenn es normal und separabel ist. Das ist genau dann der Fall, wenn $L$ der Zerfällungskörper eines separablen Polynoms $f \in K[X]$ ist. Dann ist

$$\mathrm{Gal}(f) \coloneqq \mathrm{Gal}(L/K) = \mathrm{Aut}_K(L) = \{\varphi\colon L \xrightarrow{\sim} L \mid \varphi|_K = \mathrm{id}\}.$$

Es gelten

$$|\mathrm{Gal}(f)| = [L:K]_S = [L:K]$$

und $K = L^{\mathrm{Gal}(f)}$.

*Ziel:* Wir wollen Gal($f$) beschreiben. Dazu betrachten wir Gruppenwirkungen von Gal($f$), wie z. B. $\mathrm{Gal}(f) \times L \to L$ oder $\mathrm{Gal}(f) \times L^* \to L^*$ (s. Hilbert 90). Insbesondere haben wir

$$\mathrm{Gal}(f) \times \{\alpha_1, \ldots, \alpha_n\} \longrightarrow \{\alpha_1, \ldots, \alpha_n\}$$

für die Nullstellen von $f$, was einen injektiven Gruppenhomomorphismus

$$\mathrm{Gal}(f) \hookrightarrow \mathrm{Bij}\{\alpha_1, \ldots, \alpha_n\} \simeq S_n$$

induziert. Daraus folgt $|\mathrm{Gal}(f)| \mid |S_n| = n!$.

Allgemein gelten:

(i) $|H| \mid |G|$ für Untergruppen $H \subset G$.

(ii) Für $g \in G$ gilt $|g| = |\langle g\rangle| \mid |G|$.

Auch nützlich:

(i) $g^{|G|} = e$ für alle $g \in G$.

(ii) Ist $|G| = p$ eine Primzahl, so ist $G \simeq \mathbb{Z}/p\mathbb{Z}$ zyklisch.

(iii) Ist $|G| = p^n$ mit $p$ Primzahl, so gilt für das Zentrum $Z(G) \neq \{e\}$,

(iv) Ist $|G| = p^2$ mit $p$ Primzahl, dann ist $G$ abelsch. Nach der Klassifikation endlich erzeugter abelscher Gruppen ist dann $G \simeq \mathbb{Z}/p^2\mathbb{Z}$ oder $G \simeq \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$.

Elemente in der symmetrischen Gruppe $S_n$ sind z. B. Transpositionen $(ij)$ und Zyklen $(i_1 \ldots i_k)$. Es gilt

$$S_n = \langle (ij)\rangle = \langle (i, i+1)\rangle = \langle (12), (1, \ldots, n)\rangle.$$

Jedes Element in $S_n$ ist das Produkt von disjunkten Zyklen.

(i) Die alternierende Gruppe ist $A_n \coloneqq \mathrm{Ker}(\mathrm{sgn}\colon S_n \to \{\pm 1\})$.

(ii) Es gilt $[S_n, S_n] = A_n$.

(iii) $[A_n, A_n] = A_n$, falls $n \geq 5$. Daraus folgt, dass $S_n$ nicht auflösbar ist. Also gibt es Polynome, deren Nullstellen nicht durch Radikale darstellbar sind.

## 4.6 Überblick: Gal($f$)

Falls $f$ irreduzibel ist, so wirkt $\mathrm{Gal}(f) \subset S_n$ transitiv auf $\{1,\dots,n\} = \{\alpha_1,\dots,\alpha_n\}$, d. h. für alle $i,j$ gibt es ein $\sigma \in \mathrm{Gal}(f)$, sodass $\sigma(\alpha_i) = \alpha_j$. Insbesondere gilt $K(\alpha_i) \simeq K[X]/(f) \simeq K(\alpha_j)$ für irreduzible $f$, was sich zu einem Automorphismus $\sigma\colon L \xrightarrow{\sim} L$ auf den Zerfällungskörper $L$ von $f$ fortsetzen lässt. Also gilt $n \leq |\mathrm{Gal}(f)|$. Betrachten wir den Turm $K \subset K(\alpha_1) \subset L$, so gilt

$$|\mathrm{Gal}(f)| = [L:K] = [K(\alpha_1):K][L:K(\alpha_1)].$$

Wegen $[K(\alpha_1):K] = n$ gilt $n \mid \mathrm{Gal}(f)$.

Die Galoisresolvente entspricht dem Satz über das primitive Element. Ist $f \in K[X]$ separabel, so ist der Zerfällungskörper $L/K$ von $f$ eine separable endliche Körpererweiterung. Damit gibt es ein $a \in L$, sodass $L = K(a)$. Für das Minimalpolynom $p_a \in K[X]$ von $a$ gilt dann

$$|\mathrm{Gal}(f)| = [L:K] = [K(a):K] = \deg(p_a).$$

Weil $L/K$ normal ist, ist $L = K(a)$ der Zerfällungskörper von $p_a$. Also ist $\mathrm{Gal}(f) \simeq \mathrm{Gal}(p_a)$. Wir erhalten

$$\deg(f) \mid |\mathrm{Gal}(f)| = |\mathrm{Gal}(p_a)| = [K(a):K] = \deg(p_a).$$

**Mehr Tricks (Diskriminante)** Sei $f \in K[X] \subset \bar{K}[X]$ normiert. Schreibe $f = \prod_{i=1}^{n}(X - \alpha_i)$ mit $n = \deg(f)$. Dann ist

$$D(f) \coloneqq \left(\prod_{i<j}(\alpha_i - \alpha_j)\right)^2.$$

Dann ist $f$ genau dann separabel, wenn $D(f) \neq 0$.

Hier einige Diskriminanten:

| $f$ | $D(f)$ |
|---|---|
| $X^2 + pX + q$ | $p^2 - 4q$ |
| $X^3 + pX + q$ | $-4p^3 - 27q^2$ |
| $X^4 + pX + q$ | $-27p^4 + 256q^3$ |
| $X^4 + pX^2 + q$ | $169(p^2 - 4q)^2$ |

Für Grad 3 folgt die Form durch Tschirnhausreduktion. Für Grad 4 haben natürlich auch allgemeinere quartische Gleichungen eine explizite Diskriminante; diese werden aber sehr kompliziert.

Offenbar ist $\mathrm{Gal}(f) \hookrightarrow S_n = \mathrm{Bij}\{\alpha_1,\dots,\alpha_n\}$ eine Untergruppe. Dann ist $\mathrm{Gal}(f) \subset A_n$ genau dann, wenn es ein $\sqrt{D(f)} \in K$ gibt.

Für Grad 2 ist $f$ genau dann irreduzibel, wenn $\mathrm{Gal}(f) \simeq \mathbb{Z}/2\mathbb{Z}$.

Für Grad 3 ist $f$ genau dann reduzibel, wenn $|\mathrm{Gal}(f)| \leq 2$. Falls $f$ irreduzibel ist, so gilt für $\mathrm{Gal}(f) \subset S_3$ mit $|S_3| = 6$

$$\mathrm{Gal}(f) \simeq \begin{cases} A_3 \simeq \mathbb{Z}/3\mathbb{Z}, & \text{falls } \sqrt{D(f)} \in K, \\ S_3, & \text{falls } \sqrt{D(f)} \notin K, \end{cases}$$

Alternativ können wir $\sqrt{D(f)} = \prod_{i<j}(\alpha_i - \alpha_j)$ einfach hinzuadjungieren. Dann erhalten wir den Turm $K \subset K(\sqrt{D(f)}) \subset K(\alpha_1, \alpha_2, \alpha_3)$, wobei $K(\alpha_1, \alpha_2, \alpha_3)$ der Zerfällungskörper von $f$ ist. Insbesondere ist $K \subset K(\sqrt{D(f)})$ ist von Grad 1 oder 2. Falls $\sqrt{D(f)} \notin K$, so ist $2 \mid |\mathrm{Gal}(f)|$, d. h. $\mathrm{Gal}(f) \simeq S_3$.

Für Grad 4 sei $f$ irreduzibel und separabel. Dann ist $\mathrm{Gal}(f) \subset S_4$ mit $|S_4| = 24$. Aufgrund Irreduzibilität ist $\mathrm{Gal}(f)$ eine transitive Untergruppe. Die transitiven Untergruppen von $S_4$ sind

$$\begin{aligned} S_4, \\ A_4, \\ \mathbb{Z}/4\mathbb{Z} &= \langle (1234) \rangle, \\ \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} &= \langle (12)(34), (13)(24) \rangle, \\ D_4 &= \langle s = (12)(34), d = (1234) \rangle. \end{aligned}$$

Diese haben Ordnung $|S_4| = 24$, $|A_4| = 12$, $|\mathbb{Z}/4\mathbb{Z}| = 4$, $|\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}| = 4$, $|D_8| = 8$.

*Achtung:* $\langle (12), (34) \rangle \subset S_4$ ist zwar isomorph zur kleinschen Vierergruppe $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, aber nicht transitiv.

*Folgerung:* $|\mathrm{Gal}(f)|$ bestimmt den Isomorphietyp der Galoisgruppe eindeutig, außer für $|\mathrm{Gal}(f)| = 4$. In diesem Fall kommen $\mathbb{Z}/4\mathbb{Z}$ und $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ in Frage.

Wie unterscheidet man $\mathrm{Gal}(f) \simeq \mathbb{Z}/4\mathbb{Z}$ bzw. $\mathrm{Gal}(f) \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$? Wir haben $\mathbb{Z}/4\mathbb{Z} \not\subset A_4$ genau dann, wenn $\sqrt{D(f)} \in K$, und $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \subset A_4$ genau dann, wenn $\sqrt{D(f)} \in K$.

*Beispiel:* Für $f = X^4 + 2X^2 + 5 \in \mathbb{Q}[X]$ sind die Nullstellen $\{\alpha, -\alpha, \beta, -\beta\}$. Dann ist $(1234) \notin \mathrm{Gal}(f)$ (wir können nicht $\alpha$ auf $\pm\beta$ abbilden). Also ist $\mathrm{Gal}(f) \simeq A_4$ oder $\mathrm{Gal}(f) \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Für Grad 5 sei $f \in K[X]$ irreduzibel. Falls $5 \mid |\mathrm{Gal}(f)|$ und es eine Transposition in $\mathrm{Gal}(f)$ gibt, so ist $\mathrm{Gal}(f) \simeq S_5$.

# Index