Vorlesung Algebra

(Sommersemester 2013)

Dirk Kussin

Fakultät für Mathematik, Technische Universität Chemnitz
E-mail address: dirk.kussin@mathematik.tu-chemnitz.de

Hinweis. Für Druckfehler wird keine Haftung übernommen.

Copyright © 2013 by Dirk Kussin

Version vom 19. Juli 2013

Inhaltsverzeichnis

Kapitel I. Elementare Gruppentheorie 5
1. Motivation und Einordung 5
2. Untergrupppen, Nebenklassenzerlegung 5
3. Der Satz von Cayley 8
4. Konjugation 9

Kapitel II. Faktorstrukturen 11
1. Faktorgruppen 11
2. Der Homomorphiesatz 12
3. Der Satz von Cauchy 13
4. Gruppen kleiner Ordnung 13
5. Ringe und Körper 16
6. Ideale und Faktorringe 18
7. Der Faktorring $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$ 19

Kapitel III. Gruppenaktionen 21
1. Grundlegende Eigenschaften und Beispiele 21
2. Die Sylowsätze 22
3. Eine Anwendung: Gruppen der Ordnung 15 sind zyklisch 24
4. Die Anzahl der Bahnen 24
5. Einfache Gruppen 25
6. Einfachheit der alternierenden Gruppe A_5 27
7. Auflösbare Gruppen 28

Kapitel IV. Einführung in die Ringtheorie 31
1. Euklidische Ringe 31
2. Teilbarkeit und Faktorisierung 31
3. Polynomringe 33
4. Quotientenkörper 34
5. Faktorisierung von Polynomen: Der Satz von Gauss 35
6. Ein Irreduzibilitätskriterium 37

Kapitel V. Algebraische Körpererweiterungen 39
1. Algebraische und transzendente Elemente 39
2. Konstruktion einfacher algebraischer Körpererweiterungen 42
3. Der Gradsatz 43
4. Berechnung des Minimalpolynoms 44
5. Arithmetische Eigenschaften des Körpers $\mathbb{Q}$ 45
6. Konstruktionen mit Zirkel und Lineal 46
7. Isomorphie einfacher algebraischer Erweiterungen 49
8. Algebraischer Abschluss 50

Kapitel VI. Galoistheorie 53
1. Die Galoisgruppe einer Körpererweiterung 53
2. Der Hauptsatz der Galoistheorie (Formulierung) 55

3. Zerfällungskörper 56
4. Endliche Körper 57
5. Separabilität 58
6. Normalität 60
7. Der Satz von Artin 61
8. Charakterisierung von Galoiserweiterungen 62
9. Der Hauptsatz der Galoistheorie (Beweis) 63
10. Ein Beispiel 63

Kapitel VII. Auflösung algebraischer Gleichungen 67
1. Die Polynome $T^n - a$ 67
2. Auflösbarkeit von Gleichungen 69
3. Nichtauflösbare Gleichungen 71

Literaturverzeichnis 73

KAPITEL I

Elementare Gruppentheorie

Lernziele:

- Das Konzept einer Gruppe und Untergruppe, sowie einer (Links-/Rechts-) Nebenklasse verstehen. Zyklische Gruppen.
- Das Konzept eines Homomorphismus verstehen.
- Kern eines Homomorphismus, Normalteiler und das Injektivitätskriterium.
- Den ubiquitären Satz von Lagrange und seine Varianten verstehen, samt der Beweisidee.
- Die abelsche Gruppe $(\mathbb{Z}, +)$ und seine (zyklischen) Untergruppen. Division-mit-Rest-Argument verstehen.
- Den Satz von Cayley samt Beweis kennen.
- Die Klassengleichung kennen und eine Vorstellung vom Beweis haben.

1. Motivation und Einordung

Der Gruppenbegriff ist zentral für die ganze Mathematik, nicht etwa nur von Bedeutung in der Algebra. Jedem mathematischen Objekt M (einer Menge, einem Vektorraum, einem topologischen Raum, einer Gruppe, einer geordneten Menge, etc.) kann man nämlich seine Symmetriegruppe $S(M)$ zuordnen, gebildet aus allen die gegebene Struktur von M bewahrenden Isomorphismen $f\colon M \to M$. [...]

2. Untergrupppen, Nebenklassenzerlegung

DEFINITION 2.1. Eine Teilmenge U einer Gruppe G heisst Untergruppe von G (Schreibweise: $U < G$), falls gilt

(U1) $e_G \in U$
(U2) $U \cdot U \subseteq U$
(U3) $U^{-1} \subseteq U$.

Dabei ist $U \cdot U \stackrel{def}{=} \{u_1 u_2 \mid u_1,\, u_2 \in U\}$ und $U^{-1} \stackrel{def}{=} \{u^{-1} \mid u \in U\}$. Mit der von G induzierten Multiplikation

$$\cdot_U\colon U \times U \to U,\ (x, y) \mapsto x \cdot_G y$$

ist eine Untergruppe selbst eine Gruppe.

BEISPIELE 2.2. (a) Sei G eine Gruppe. Dann sind $\{e\}$ und G Untergruppen.
(b) Sei G eine Gruppe und $g \in G$ Dann ist

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

eine Untergruppe von G. Sie heisst due von g erzeugte (zyklische) Untergruppe.
(c) A_n ist Untergruppe von S_n.
(d) $\mathrm{SL}_n(K) < \mathrm{GL}_n(K)$.

DEFINITION 2.3. Eine Gruppe G heisst zyklisch, falls es ein $g \in G$ gibt mit $G = \langle g \rangle$.

Jede zyklische Gruppe ist abelsch. Die Umkehrung gilt nicht.

BEISPIELE 2.4. (a) Die Permutation

$$\sigma = \begin{pmatrix} 1 & 2 & \dots & n-1 & n \\ 2 & 3 & \dots & n & 1 \end{pmatrix}$$

erzeugt eine zyklische Gruppe $\langle\sigma\rangle$, bestehend aus $1, \sigma, \sigma^2, \dots, \sigma^{n-1}$, der Ordnung n.

(b) Sei $z_n = e^{2\pi i/n}$ betrachtet als Element von $(\mathbb{C}^\times, \cdot)$, wobei $\mathbb{C}^\times = \mathbb{C} \setminus \{0\}$. Dann besteht $U_n = \langle z_n\rangle$ aus den Elementen $1, z_n, z_n^2, \dots, z_n^{n-1}$. Also $|U_n| = n$.

(c)* Jede endliche Untergruppe von $(\mathbb{C}^\times, \cdot)$ der Ordnung n stimmt mit U_n überein, ist also zyklisch.

(d)* Jede endliche Untergruppe der multiplikativen Gruppe $K^\times = K \setminus \{0\}$ eines Körpers K ist zyklisch.

(e) $(\mathbb{Z}, +)$ ist zyklisch (und unendlich).

DEFINITION 2.5. Sei G eine Gruppe und U eine Untergruppe von G. Für $g \in G$ heisst

$$Ug = \{ug \mid u \in U\}$$

die Linksnebenklasse von G nach U. Mit G/U bezeichnen wir die Menge aller Linksnebenklassen von G nach U.

LEMMA 2.6. *Äquivalent sind:*

(a) $Ug = Uh$
(b) $Ug \cap Uh \neq \emptyset$
(c) $hg^{-1} \in U$

BEWEIS. (Siehe Vorlesung.) □

SATZ 2.7. *Sei U eine Untergruppe von G Dann ist*

$$G = \coprod_{N \in G/U} N$$

eine disjunkte Zerlegung von G in Linksnebenklassen N, die alle zu U gleichmächtig sind.

Hierbei bezeichne $\coprod$ die disjunkte Vereinigung. Zwei Menge M und N heissen gleichmächtig, wenn es eine bijektive Abbildung $f\colon M \to N$ gibt. Im Fall endlicher Mengen bedeutet dies, dass die Anzahlen von Elementen von M und von N übereinstimmen.

BEWEIS. Jedes $g \in G$ liegt in einer Nebenklasse, z. B. in Ug. Verschiedene Nebenklassen sind nach Lemma 2.6 disjunkt. Dies zeigt den ersten Teil der Aussage. Für $g \in G$ ist die Abbildung

$$h\colon U \to Ug,\ u \mapsto ug$$

bijektiv mit Umkehrabbildung $Ug \to U$, $y \mapsto yg^{-1}$; daher sind U und Ug gleichmächtig. □

FOLGERUNG 2.8 (Satz von Lagrange). *Sei G eine endliche Gruppe und U eine Untergruppe. Dann gilt*

$$|G| = |U| \cdot |G/U|.$$

Insbesondere sind daher die Ordnung $|U|$ von U und der Index $[G : U] \stackrel{def}{=} |G/U|$ *von G nach U Teiler der Ordnung $|G|$ von G.*

FOLGERUNG 2.9. *Jede Gruppe G von Primzahlordnung p ist zyklisch und hat $\{e\}$ und G als einzige Untergruppen.*

BEWEIS. Ist U eine Untergruppe von G, so ist $|U|$ ein Teiler von p, also $|U| = 1$ oder $|U| = p$. Dies zeigt $U = \{e\}$ oder $U = G$. Wähle nun $e \neq g \in G$. Es folgt $\langle g\rangle \neq \{e\}$, also $\langle g\rangle = G$. □

FOLGERUNG 2.10 ("Kleiner Fermat"). *Ist G eine Gruppe der Ordnung n und $g \in G$, so gilt $g^n = e$.*

BEWEIS. Die von g erzeugte zyklische Untergruppe $U = \langle g \rangle$ hat als Ordnung einen Teiler m von n. Es reicht also folgende Aussage zu zeigen:

In einer zyklischen Gruppe $U = \langle g \rangle$ der Ordnung m gilt $g^m = e$; ferner ist m die kleinste natürliche Zahl ≥ 1 mit $g^m = e$.

Beweis hierfür: Sei r die kleinste natürliche Zahl ≥ 1 mit $g^r = e$. (Diese heisst auch die Ordnung von g.) Dann sind die Elemente

$$e,\ g,\ g^2, \ldots,\ g^{r-1}$$

paarweise verschieden: sonst gilt für $0 \leq j < k \leq r-1$ $g^j = g^k$, also $g^{k-j} = e$, im Widerspruch zur Wahl von r. Ferner ist $\{e,\ g, \ldots,\ g^{r-1}\}$ gegen Multiplikation abgeschlossen (beachte $g^r = e$), also (Übung) eine Untergruppe von G. Es folgt $|\langle g \rangle| = r$. □

SATZ UND DEFINITION 2.11. *Sind G und H Gruppen, so ist $G \times H$ vermöge*

$$(g, h) \cdot (g', h') = (gg', hh')$$

wieder eine Gruppe. $G \times H$ heisst direktes Produkt von G und H.

BEMERKUNG 2.12. Sei G eine endliche Gruppe der Ordnung ≥ 2 oder unendlich. Dann ist $G \times G$ nie zyklisch.

BEWEIS. Vgl. Übungen. □

DEFINITION 2.13. Seien G und H Gruppen. Eine Abbildung $f\colon G \to H$ heisst Homomorphismus, wenn

$$f(x \cdot_G y) = f(x) \cdot_H f(y)$$

für alle $x,\ y \in G$ gilt. Ist F zusätzlich bijektiv, so nennen wir f Isomorphismus. Zwei Gruppen G und H heissen isomorph (Schreibweise: $G \simeq H$), falls es einen Isomorphismus $f\colon G \to H$ gibt.

EIGENSCHAFTEN 2.14. *$f\colon G \to H$ sei ein Gruppenhomomorphismus. Dann gilt*

(a) $f(e_G) = e_H$
(b) $f(x^{-1}) = f(x)^{-1}$
(c) $U < G \Rightarrow f(U) < H$
(d) $V < H \Rightarrow f^{-1}(V) < G$.

BEWEIS. (Siehe Vorlesung.) □

DEFINITION 2.15 (Normalteiler). Eine Untergruppe N von G heisst Normalteiler, wenn für jedes $g \in G$

$$gNg^{-1} \subseteq N$$

gilt. Notation: $N \lhd G$.

Äquivalent sind:

- $gNg^{-1} \subseteq N$ für jedes $g \in G$.
- $gNg^{-1} = N$ für jedes $g \in G$.
- $gN \subseteq Ng$ für jedes $g \in G$.
- $gN = Ng$ für jedes $g \in G$.

SATZ 2.16. *Sei $f\colon G \to H$ ein Gruppenhomomorphismus. Dann ist*

$$N = \mathrm{Kern}(f) = \{x \in G \mid f(x) = e_H\} = f^{-1}(\{e_H\})$$

ein Normalteiler in G.

BEISPIELE 2.17. (1) $\det\colon \mathrm{GL}_n(K) \to K^\times$ hat Kern $\mathrm{SL}_n(K)$.
(2) $\mathrm{sgn}\colon S_n \to \{\pm 1\}$ hat Kern A_n.
(3) $\exp\colon (\mathbb{R}, +) \longrightarrow (\mathbb{R}^\times, \cdot)$ ist injektiver Gruppenhomomorphismus, also $\mathrm{Kern}(\exp) = \{0\}$.

SATZ 2.18 (Injektivitätskriterium). *Ein Gruppenhomomorphismus $h\colon G \to H$ ist genau dann injektiv, wenn* $\mathrm{Kern}(H) = \{e_G\}$ *gilt.*

BEWEIS. (Siehe Vorlesung.) □

3. Der Satz von Cayley

SATZ 3.1 (Cayley). *Sei G eine endliche Gruppe der Ordnung n. Dann ist G isomorph zu einer Untergruppe der symmetrischen Gruppe S_n.*

BEWEIS. Für jedes $g \in G$ ist die Abbildung

$$\varphi_g\colon G \to G,\ x \mapsto gx$$

eine bijektive Abbildung, somit ein Mitglied der symmetrischen Gruppe $S(G) = \{f\colon G \to G \mid f \text{ bijektiv}\}$. Wir zeigen, dass

$$\varphi\colon G \to S(G),\ g \mapsto \varphi_g$$

ein injektiver Gruppenhomomorphismus ist:

(a) φ ist Homomorphismus:

$$\varphi_{gh}(x) = (gh)x = g(hx) = \varphi_g(\varphi_h(x)) = \varphi_g \circ \varphi_h(x).$$

(b) φ ist injektiv: Ist $\varphi_g = 1_G$, so folgt

$$x = 1_G(x) = \varphi_g(x) = gx$$

für alle $x \in G$; insbesondere für $x = e$, und $g = e$ folgt.

Wegen $|G| = n$ gilt $S(G) \simeq S_n$, und die Behauptung folgt. □

SATZ 3.2. *Jede Untergruppe einer zyklischen Gruppe ist zyklisch.*

BEWEIS. Wesentliches Hilfsmittel ist die Division mit Rest in $\mathbb{Z}$: Seien m, n ganze Zahlen mit $n \neq 0$. Dann gibt es eindeutig bestimmte ganze Zahlen q, r mit

$$m = qn + r$$

und mit $0 \leq r < |n|$. (Beweis siehe Vorlesung.) Sei nun $(G, \cdot)$ ein zyklische Gruppe, etwa $G = \langle g \rangle$. Sei U eine Untergruppe von G, wobei wir $U \neq \{e\}$ annehmen. Sei $e \neq u \in U$. Es gibt dann ein $n \neq 0$ mit $u = g^n$. Da mit u auch u^{-1} in U ist, können wir $n > 0$ annehmen, und außerdem, dass $n > 0$ minimal ist mit $g^n \in U$. Wir zeigen $U = \langle u \rangle = \langle g^n \rangle$: Da $g^n = u \in U$ gilt, ist $\langle u \rangle \subseteq U$ klar. Sei $v \in U$ beliebig. Es gibt ein $m \in \mathbb{Z}$ mit $v = g^m$. Division mit Rest ergibt q, r mit $m = qn + r$ mit $0 \leq r < n$. Wegen g^m, $g^n \in U$ gilt auch $g^r = g^{m-qn} = g^m \cdot g^{-qn} \in U$. Wegen $r < n$ und der Minimalität von n folgt $r = 0$, also $v = g^m = g^{qn} = u^n \in \langle u \rangle$. □

Dies Argument mit der Division mit Rest wird uns später auch in anderen Situationen wieder begegnen.

FOLGERUNG 3.3. *Jede Untergruppe von $(\mathbb{Z}, +)$ ist zyklisch.*

LEMMA 3.4. *Sei $G = \langle g \rangle$ eine zyklische Gruppe der Ordnung $n < \infty$. Sei d ein Teiler von n ($d > 0$). Dann ist $U = \langle g^{n/d} \rangle$ eine Untergruppe der Ordnung d.*

BEWEIS. Ersichtlich ist d der kleinste Exponent mit

$$(g^{n/d})^d = e.$$

□

Für zyklische Gruppen lässt sich der Satz von Lagrange ($|U| \mid |G|$) gewissermaßen "umkehren". Allerdings ist dies generell nicht der Fall:

BEISPIEL 3.5. Die alternierende Gruppe A_4 hat die Ordnung 12, aber keine Untergruppe der Ordnung 6. (Werden wir später sehen.)

4. Konjugation

Für jedes $g \in G$ ist $h_g \colon G \to G$, $x \mapsto gxg^{-1}$ ein Automorphismus von G.

DEFINITION 4.1. Elemente x, $y \in G$ heißen konjugiert, falls es ein $g \in G$ gibt mit $y = gxg^{-1}$. Wir bezeichnen mit $C(x) = \{gxg^{-1} \mid g \in G\}$ die Menge aller zu x konjugierten Elemente. Diese heisst die Konjugationsklasse von x.

Ist U eine Untergruppe von G, so ist $h_g(U) = gUg^{-1}$ eine Untergruppe von G, die zu U konjugiert heisst. Genau die Normalteiler von G stimmen mit ihren konjugierten Untergruppen überein.

DEFINITION 4.2. $Z(G) = \{x \in G \mid gx = xg \text{ für alle } g \in G\}$ heisst das Zentrum von G.

SATZ 4.3. *Z(G) ist Normalteiler in G.*

BEWEIS. (Siehe Vorlesung.) □

SATZ 4.4. (a) $x \in C(x)$.
(b) $C(x) \cap C(y) \neq \emptyset \;\Rightarrow\; C(x) = C(y)$.
(c) $|C(x)| = 1 \;\Leftrightarrow\; C(x) = \{x\} \;\Leftrightarrow\; x \in Z(G)$.

BEWEIS. (Siehe Vorlesung.) □

SATZ 4.5 (Klassengleichung). *Ist G eine endliche Gruppe, so gilt*

$$|G| = |Z(G)| + \sum_{|C(x)|>1} |C(x)|.$$

BEWEIS. (Siehe Vorlesung.) □

Sei $Z(x) = \{g \in G \mid gxg^{-1} = x\}$ (der Zentralisator von x).

LEMMA 4.6. $|C(x)| = |G|/|Z(x)|$.

BEWEIS. Durch $G/Z(x) \to C(x)$, $gZ(x) \mapsto gxg^{-1}$ ist eine Bijektion gegeben. □

LEMMA 4.7. *Sei G eine Gruppe der Ordnung p^n (p prim, $n \geq 1$). Dann ist das Zentrum $Z(G) = \{g \in G \mid gx = xg$ für alle $x \in G\} \neq \{e\}$.*

BEWEIS. Nach dem Lemma ist $|C(x)| = |G|/|Z(x)|$ ein Teiler von $|G| = p^n$. Ist $|C(x)| > 1$, so wird $|C(x)|$ also von p geteilt. Es folgt, dass auch $|Z(G)|$ von p geteilt wird. Also ist $Z(G)$ nicht trivial. □

FOLGERUNG 4.8. *Jede Gruppe der Ordnung p^2 (p prim) ist abelsch.*

BEWEIS. Nach Lemma 4.7 sind nur

$$|Z(G)| = \begin{cases} p \\ p^2 \end{cases}$$

möglich. Falls $|Z(G)| = p^2$, so sind wir fertig. Nehme also $|Z(G)| = p$ an. Dann ist G nicht abelsch. Es gibt dann ein $x \in G$, dessen Zentralisator $Z(x)$ echt in G enthalten ist. Es folgt

$$Z(G) \subseteq Z(x) \subsetneq G$$

und damit (Lagrange) $Z(G) = Z(x)$. Aber $x \in Z(x)$ und $x \notin Z(G)$, Widerspruch. □

KAPITEL II

Faktorstrukturen

Lernziele:

- Das Konzept einer Faktorgruppe verstehen, und warum hier Normalteiler wichtig sind.
- Homomorphiesatz.
- Satz von Cauchy.
- Beispiele von Gruppen kleiner Ordnung kennen.
- Ringtheoretische Analoga verstehen.
- Der Restklassenring $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$. Nullteilerfreiheit und Körpereigenschaften in Abhängigkeit von n verstehen.

1. Faktorgruppen

Ist N ein Normalteiler in einer Gruppe G, so gilt $gN = Ng$ für jedes $g \in G$; wir schreiben im folgenden $[g] := Ng$.

Satz und Definition 1.1. *Sei G eine Gruppe und N ein Normalteiler in G. Dann bildet*

$$G/N = \{[g] \mid g \in G\}$$

bezüglich der Verknüpfung

$$[x] \cdot [y] \stackrel{def}{=} [xy]$$

eine Gruppe. Dabei ist $[e_G]$ das neutrale Element und $[x^{-1}]$ zu $[x]$ invers.

G/N heißt die Faktorgruppe *von G* nach *N (oder auch* Quotient *von G* nach *N.)*

Beweis. (Siehe Vorlesung.) Hauptaugenmerk liegt hier darauf zu zeigen, dass die angegebene Verknüpfung wohldefiniert ist; dazu muss man die Normalteilereigenschaft verwenden. □

Zusatz 1.2. *Die Abbildung*

$$\nu\colon G \to G/N,\ x \mapsto [x]$$

ist ein surjektiver Gruppenhomomorphismus mit $\mathrm{Kern}(\nu) = N$.

$\nu\colon G \to G/N$ heißt der *natürliche Homomorphismus.*

Bemerkung 1.3. (a) Jeder Kern eines Gruppenhomomorphismus $h\colon G \to H$ ist Normalteiler in G. Umgekehrt ist nach dem vorherigen jeder Normalteiler N in G Kern des natürlichen Homomorphismus

$$\nu_N\colon G \to G/N,\ x \mapsto [x]_N.$$

(b) Für $N = G$ ist $G/N = \{[e]\}$ die einelementige, triviale Gruppe.

(c) Für $N = \{e\}$ ist der natürliche Homomorphismus $\nu\colon G \to G/\{e\}$ surjektiv mit $\mathrm{Kern}(\nu) = \{e\}$, also ein Isomorphismus.

(d) Die allgemeine Situation liegt zwischen den beiden Extremfällen (b) und (c). Durch die Faktorkontruktion wird beim Übergang von G nach G/N durch ν eine "Verkleinerung"von G erreicht, bei der N auf das neutrale Element $[e]$ von G/N und allgemein eine Nebenklasse $Nx \subseteq G$ auf das Element $[x]$ zusammenschrumpft.

HINWEIS 1.4.
- Wenn G eine abelsche Gruppe und U in G eine Untergruppe ist, können wir somit stets die Faktorgruppe G/U bilden.
- Man mache sich klar, wo es mit der Faktorbildung im nicht-abelschen Fall schiefgeht, wenn U nur eine Untergruppe, aber kein Normalteiler von G ist!

SATZ 1.5. *Für jedes natürliche $n \geq 1$ ist*

$$\mathbb{Z}_n := \mathbb{Z}/\mathbb{Z} \cdot n$$

eine zyklische Untergruppe von $(\mathbb{Z}, +)$ der Ordnung n, die gerade aus den Nebenklassen

$$[0],\ [1],\ [2], \ldots,\ [n-1]$$

besteht.

BEWEIS. Per Division mit Rest. (Vgl. Vorlesung.) □

Wie sieht *konkret* die Addition auf $\mathbb{Z}_n$ aus? Seien $0 \leq x,\ y < n$ und

$$[x] + [y] = [x + y] = \begin{cases} [x+y] & \text{falls } x + y < n, \\ [x+y-n] & \text{sonst.} \end{cases}$$

Wir können daher auf $\{0,\ 1, \ldots,\ n-1\}$ eine Addition $+_n$ erklären durch

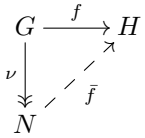
$$x +_n y = \begin{cases} x + y & \text{falls } x + y < n, \\ x + y - n & \text{sonst.} \end{cases}$$

Nimmt man dies als Startpunkt, müßte zunächst die Assoziativität der Verknüpfung gezeigt werden, was relativ aufwändig ist. Die Bildung der Faktorgruppe erledigt dies wesentlich eleganter.

2. Der Homomorphiesatz

Das Konzept der Faktorgruppe entfaltet seine volle Wirksamkeit erst im Zusammenwirken mit dem Homomorphiesatz, der besagt, dass – bis auf eine nachfolgende Einbettung – jeder Homomorphismus so aussieht, wie ein natürlicher Homomorphismus $\nu\colon G \to G/N$.

SATZ 2.1 (Homomorphiesatz). *Sei $f\colon G \to H$ ein Gruppenhomomorphismus und $N = \mathrm{Kern}(f)$. Dann ist N ein Normalteiler in G und es gibt genau einen Homomorphismus $\bar{f}\colon G/N \to H$ mit $\bar{f} \circ \nu = f$; es gilt also $\bar{f}([x]) = f(x)$ für alle $x \in G$, d. h. das folgende Diagramm kommutiert:*



Ferner ist $\bar{f}$ injektiv.

BEWEIS. Man definiert $\bar{f}([x]) = f(x)$ für alle $x \in G$. (Dies ist die einzige Möglichkeit, wenn die Aussage im Satz richtig sein soll.) Man muss zeigen, dass dies wohldefiniert ist. Seien also $x,\ y \in G$ mit $[x] = [y]$. Dies bedeutet $xy^{-1} \in N = \mathrm{Kern}(f)$, also $f(x)f(y)^{-1} = f(xy^{-1}) = e_H$, was gleichbedeutend zu $f(x) = f(y)$ ist. — Man rechnet nun leicht nach, dass $\bar{f}$ ein Gruppenhomomorphismus ist, der, wegen $\mathrm{Kern}(f) \subseteq N$, trivialen Kern hat, also injektiv ist. Die Eigenschaft $\bar{f}([x]) = f(x)$ gilt unmittelbar nach Definition von $\bar{f}$. □

FOLGERUNG 2.2. *Ist f surjektiv, so ist $\bar{f}$ ein Isomorphismus.*

SATZ 2.3.
(a) *Jede unendliche zyklische Gruppe G ist isomorph zu $(\mathbb{Z}, +)$.*
(b) *Jede endliche zyklische Gruppe der Ordnung n ist isomorph zu $\mathbb{Z}_n$.*

BEWEIS. (Siehe Vorlesung.) □

SATZ 2.4 (über induzierte Homomorphismen). *Sei $f\colon G \to H$ ein Gruppenhomomorphismus, und sei N ein Normalteiler in G, und P ein Normalteiler in H. Falls $f(N) \subseteq P$ gilt, so gibt es genau einen Homomorphismus $\bar{f}\colon G/N \to H/P$, für den $\bar{f} \circ \nu_N = \nu_P \circ f$ gilt.*

BEWEIS. Man definiert $\bar{f}\colon G/N \to H/P$ durch

$$\bar{f}([x]_N) = [f(x)]_P.$$

Man zeigt dann:

(a) $\bar{f}$ ist wohldefiniert (wenn $f(N) \subseteq P$);
(b) $\bar{f}$ ist Homomorphismus;
(c) Für $\bar{f}$ gilt die Formel.

(Siehe Vorlesung.) □

HINWEIS 2.5. In dieser generellen Situation ist $\bar{f}$ i. a. nicht injektiv.

3. Der Satz von Cauchy

Die behandelten Faktorgruppen sind außerordentlich nützlich. Sie ermöglichen z. B. für endliche Gruppen intelligente Induktionsargumente. Wir diskutieren hier als einen solchen Anwendungsfall den Satz von Cauchy.

LEMMA 3.1. *Sei G eine Gruppe der Ordnung p^n (p prim, $n \geq 1$). Dann enthält das Zentrum $Z(G)$ ein Element g der Ordnung p, und $N = \langle g \rangle$ ist ein Normalteiler in G.*

BEWEIS. Da der Beweis der Aussage sich in $Z(G)$ abspielt, nehmen wir zur Abkürzung der Notation $Z(G) = G$ an. Ist G zyklisch, so gibt es offenbar ein Element der Ordnung p. Andernfalls, sei $g \in G$ mit $\{1\} \subsetneq \langle g \rangle \subsetneq G$. Dann hat per Induktion wegen $|G| = |\langle g \rangle| \cdot |G/\langle g \rangle|$ nun $\langle g \rangle$ oder $G/\langle g \rangle$ ein Element der Ordnung p. Im ersten Fall ist man fertig. Im zweiten Fall betrachtet man das Urbild eines solchen Elements unter dem kanonischen Homomorphismus $\nu\colon G \to G/\langle g \rangle$ und die davon erzeugte zyklische Untergruppe in G. Deren Ordnung wird von p geteilt, enthält also ein Element der Ordnung p.

Jede Untergruppe in $Z(G)$ ist offenbar ein Normalteiler in G. □

SATZ 3.2 (Cauchy). *Es sei G eine endliche Gruppe, deren Ordnung durch die Primzahl p geteilt wird. Dann enthält G ein Element der Ordnung p.*

BEWEIS. Der Beweis von Lemma 4.7 zeigt die Richtigkeit des Satzes von Cauchy unter der Zusatzvoraussetzung, dass G abelsch ist. Den allgemeinen Fall führt man hierauf zurück: Induktion nach $n = |G|$. Für $n = 1$ ist die Aussage klar. Sei $n > 1$. Wir nehmen an, dass keine echte Untergruppe U von G mit $p \mid |U|$ existiert (andernfalls sind wir per Induktionsvoraussetzung fertig). Sei $g \in G$ mit $g \notin Z(G)$. Dann ist der Zentralisator $Z(g)$ eine echte Untergruppe von G. Da dessen Ordnung nicht von p geteilt wird, teilt p den Index $[G : Z(g)] = |C(g)|$. Aus der Klassengleichung

$$|G| = |Z(G)| + \sum_{|C(x)|>1} |C(x)|$$

folgt $p \mid |Z(G)|$. Nach Annahme gilt dann aber $Z(G) = G$, d. h. G ist abelsch. In dem Fall ist uns die Aussage, wie bereits erwähnt, schon bekannt. □

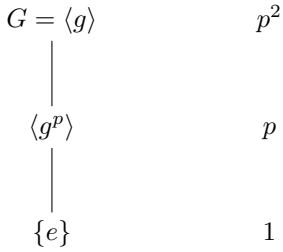
4. Gruppen kleiner Ordnung

Mit Hilfe des Satzes von Cauchy können wir für eine ganze Reihe kleiner Ordnungen sämtliche Gruppen dieser Ordnung bestimmen. Wir wollen bis zur Ordnung 15 sehen, wie weit wir mit unseren jetzigen Fähigkeiten kommen. Sei also G eine endliche Gruppe der Ordnung n.

- $n = 1$ klar.

- $n = 2, 3, 5, 7, 11, 13$. Hier ist n eine Primzahl. Wir wissen, dass diese Gruppen zyklisch sind, isomorph zu $\mathbb{Z}_n$, und außer $\{e\}$ und G keine weiteren Untergruppen haben. $G = \langle g\rangle$, $g^n = e$. Wir haben also auch den sog. Untergruppenverband von G bestimmt (d. h. die Menge aller Untergruppen von G, geordnet mit der Inklusion.)

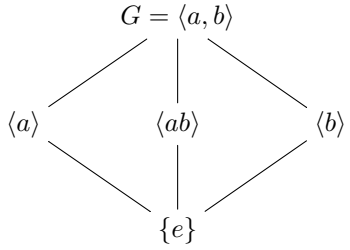
- $n = 4, 9$. Hier ist $n = p^2$ für eine Primzahl p, daher ist G abelsch (nach Folgerung I.4.8). Elemente $e \neq G$ haben die Ordnung p oder p^2. Nur zwei Fälle sind möglich:
  (a) Es gibt ein $g \in G$ der Ordnung $n = p^2$. In diesem Fall ist G zyklisch, $G = \langle g\rangle$, $g^n = e$. Ferner ist der Untergruppenverband linear:



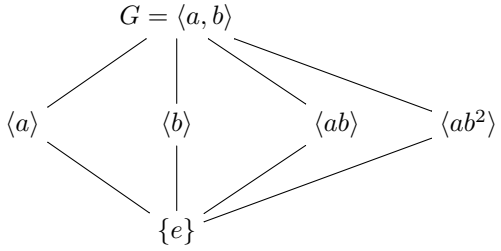
  (b) Jedes $e \neq g \in G$ hat die Ordnung p. Jedes solche Element liegt daher in genau einer Untergruppe U der Ordnung p. Abzählen

$$|G \setminus \{e\}| = p^2 - 1 = (p+1)(p-1) = (p+1)|U \setminus \{e\}|$$

  zeigt, dass G genau $p + 1$ Untergruppen der Ordnung p hat und dies alle echten Untergruppen von G sind.
    (b1) $n = 4$ ($p = 2$). $G = \langle a, b\rangle$, $a^2 = b^2 = e$, $ab = ba$. G ist die sog. Kleinsche Vierergruppe, $G \simeq \mathbb{Z}_2 \times \mathbb{Z}_2$. Untergruppenverband:

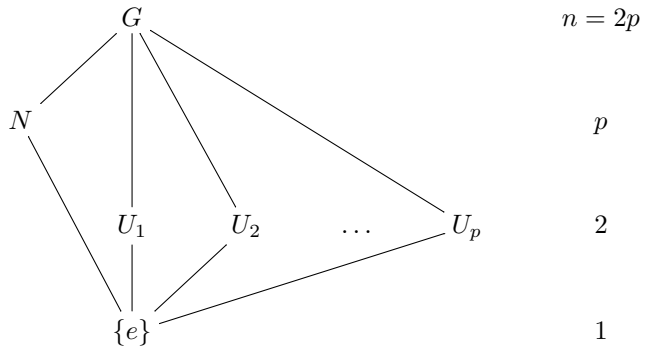


    (b2) $n = 9$ ($p = 3$). $G = \langle a, b\rangle$, $a^3 = b^3 = e$, $ab = ba$. G ist isomomorph zu $\mathbb{Z}_3 \times \mathbb{Z}_3$. Untergruppenverband:



Bemerkung: Mit ähnlicher Argumentation ist jede Gruppe der Ordnung $n = p^2$ entweder zu $\mathbb{Z}_n$ oder zu $\mathbb{Z}_p \times \mathbb{Z}_p$ isomorph. Diese Gruppen sind daher sämtlich direkte Produkte von zyklischen Gruppen. Der Hauptsatz über endliche abelsche Gruppen sagt, dass die letztgenannte Eigenschaft allgemeiner für alle endlichen abelschen Gruppen gilt.

- $n = 6, 10, 14$. Diese Ordnungen haben die Form $n = 2p$, wobei p eine ungerade Primzahl ist. Der Satz von Cauchy sagt uns, dass es sowohl ein Element g der Ordnung 2 als auch ein Element h der Ordnung p gibt. Folgende Fälle sind möglich (für Details vgl. Vorlesung):
  (a) G hat ein Element der Ordnung $n = 2p$. Dann ist $G \simeq \mathbb{Z}_n$ zyklisch.
  (b) Jedes $e \neq x \in G$ hat entweder die Ordnung 2 oder die Ordnung p. Sei, wie oben, g eines der Ordnung 2, h der Ordnung p. Es hat $N = \langle h \rangle$ als Untergruppe der Ordnung p den Index 2, ist also Normalteiler in G (vgl. Übungen). Man zeigt, dass N die einzige Untergruppe der Ordnung p ist. Somit haben alle Elemente aus $G \setminus N$ die Ordnung 2, bilden damit (zusammen mit e) p Untergruppen $U_1, \ldots, U_p$ der Ordnung 2. Wir haben den Untergruppenverband ermittelt:



  Darstellung durch Erzeugende und Relationen: $N = \langle h \rangle$, $h^p = e$, $U_1 = \langle g \rangle$, $g^2 = e$. Man zeigt nun, dass

$$\varphi \colon N \times U_1 \to G,\ (n, u) \mapsto nu$$

  bijektiv ist. Es lässt sich also jedes $x \in G$ eindeutig in der Form

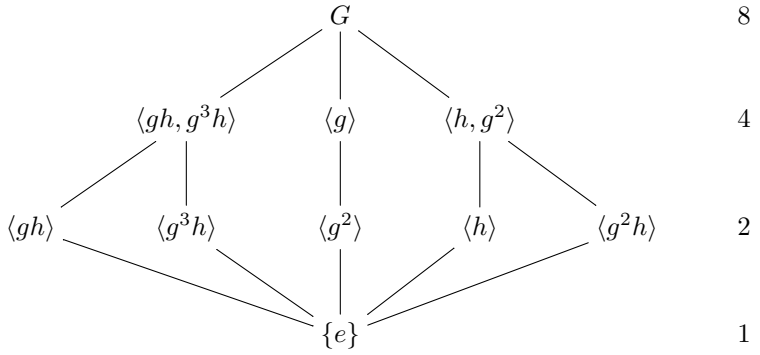
$$x = h^i g^j \quad 0 \leq i \leq p-1,\ 0 \leq j \leq 1$$

  schreiben. Ferner gilt

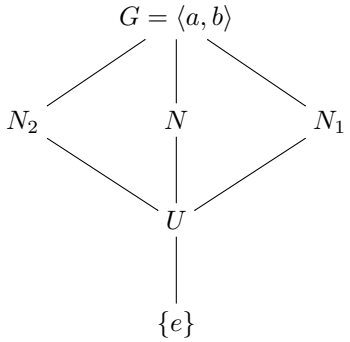
$$ghg^{-1} = h^i$$

  für ein $0 \leq i \leq p-1$. Man sieht aber, dass nur $i = 1$ und $i = p-1$ möglich sind. Im Fall $i = 1$ gilt $gh = hg$, und G ist abelsch, $G \simeq \mathbb{Z}_p \times \mathbb{Z}_2 \simeq \mathbb{Z}_{2p}$ (Übung), also zyklisch. Im Fall $i = p-1$ gilt $G = \langle g, h \rangle$ mit Relationen $g^2 = e = h^p$, $ghg^{-1} = h^{p-1}$. Dies liefert die sog. Diedergruppe D_p (vom Grad p und der Ordnung $2p$).
- $n = 8 = 2^3$. [...] Der interessante Fall ist hier, dass G eine zyklische Untergruppe N der Ordnung 4 hat, die automatisch Normalteiler von G ist. $N = \langle g \rangle$, $g^4 = e$. Es gibt dann zwei Fälle:
  (a) In $G \setminus N$ gibt es ein Element h der Ordnung 2. Es folgt $G = \langle g, h \rangle$ mit $g^4 = e = h^2$, und ferner folgt $hgh^{-1} = g^3$. Es handelt sich also um die

Diedergruppe D_4. Der Untergruppenverband sieht wie folgt aus:



(b) In $G \setminus N$ hat jedes Element die Ordnung 4. Hier zeigt man, dass G die Quaternionengruppe ist:



$a^4 = e$, $b^2 = a^2$, $ba = a^{-1}b$. Hier sind alle Untergruppen Normalteiler.

- $n = 12 = 2^2 \cdot 3$. Hier gibt es als abelsche Gruppen

$$\mathbb{Z}_4 \times \mathbb{Z}_3,\ \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3,\ \mathbb{Z}_{12}$$

  und drei nichtabelsche
  - A_4 alternierende Gruppe;
  - D_6 Diedergruppe;
  - sog. dizyklische Gruppe ($\langle a, b\rangle$, $a^6 = e$, $b^2 = a^3$, $ba = a^{-1}b$).
- $n = 15 = 3 \cdot 5$. Hier ist jede Gruppe zyklisch, siehe Übungen.

5. Ringe und Körper

Definition 5.1. Ring (mit Eins 1_R). Kommutativer Ring. (Siehe Vorlesung.)

Beispiele 5.2. (a) $\mathbb{Z}$.
(b) Jeder Körper, insbesondere $\mathbb{Q}$, $\mathbb{R}$ und $\mathbb{C}$.
(c) $\mathrm{End}_K(V)$ für einen K-Vektorraum V.
(d) $\mathrm{M}_n(K)$. Für $n \geq 2$ nicht kommutativ.
(e)* $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z} = \{[0], [1], \ldots, [n-1]\}$ mit

$$[x] \cdot [y] \overset{def}{=} [xy]$$

ist ein kommutativer Ring mit n Elementen.
(f)* K ein Körper, $K[X]$ der Ring der Polynome über K in der Unbestimmten X.

Definition 5.3. Ein Ring R, für den $R^\times = R \setminus \{0\}$ bzgl. Multiplikation eine Gruppe ist, heißt Schiefkörper. Ist R zusätzlich kommutativ, so heißt R ein Körper.

BEISPIELE 5.4. (1) $\mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$ sind Körper. Weitere Körper wie

$$\mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$$

und

$$\mathbb{Q}[i] = \{a + bi \mid a, b \in \mathbb{Q}\}$$

erhält man als Teilkörper von $\mathbb{R}$ bzw. $\mathbb{C}$.

(2) Die Ringe $\mathbb{Z}$ und $\mathrm{M}_n(K)$ $(n \geq 2)$ sind keine (Schief-) Körper.

(3) Die Menge

$$\mathbb{H} = \left\{ \begin{pmatrix} a & b \\ -\bar{b} & \bar{a} \end{pmatrix} \mid a, b \in \mathbb{C} \right\}$$

bildet bzgl. Matrizenaddition und -multiplikation einen Schief-Körper, den Schiefkörper der (Hamiltonschen) Quaternionen. — Für $(a, b) \neq (0, 0)$ ist

$$\begin{pmatrix} a & b \\ -\bar{b} & \bar{a} \end{pmatrix}^{-1} = \frac{1}{|a|^2 + |b|^2} \begin{pmatrix} \bar{a} & -b \\ \bar{b} & a \end{pmatrix}.$$

(4)* Ist p eine Primzahl, so ist $\mathbb{Z}_p = \mathbb{Z}/p\mathbb{Z}$ ein Körper mit genau p Elementen.

(5)* Ist K ein endlicher Körper, so ist $|K| = p^n$ eine Primzahlpotenz.

(6)* Sind K und L endliche Körper mit $|K| = |L|$, so sind K und L isomorph.

(7)* Ist K ein Körper, so ist

$$K(X) = \left\{ \frac{f}{g} \mid f, g \in K[X],\ g \neq 0 \right\}$$

ein Körper, der Körper der rationalen Funktionen über K in der Unbestimmten X.

LEMMA 5.5. *Jeder Schiefkörper K ist nullteilerfrei, d. h. $x \cdot y = 0$ impliziert $x = 0$ oder $y = 0$.*

BEWEIS. Ist $xy = 0$ und $x \neq 0$, so folgt

$$y = 1 \cdot y = (x^{-1}x)y = x^{-1}(xy) = 0.$$

□

DEFINITION 5.6. Ein kommutativer Ring mit $0 \neq 1$ heißt Integritätsbereich, wenn er nullteilerfrei ist.

BEISPIELE 5.7. (1) $\mathbb{Z}$.

(2)* Allgemeiner ist jeder Unterring eines Körpers K nullteilerfrei.

(3)* $K[X]$ ist nullteilerfrei (K ein Körper).

(4)* Jeder Integritätsbereich lässt sich in einen Körper einbetten, damit als Unterring eines Körpers auffassen. (Beweis später.)

SATZ 5.8. *Jeder endliche Integritätsring R ist ein Körper.*

BEWEIS. Sei $a \in R$, $a \neq 0$. Die Abbildung

$$\lambda_a \colon R \to R,\ x \mapsto ax$$

ist – da a kein Nullteiler ist – injektiv, und wegen der Endlichkeit von R auch surjektiv. Insbesondere gibt es ein $x \in R$ mit $1 = \lambda_a(x) = ax$. Also ist a invertierbar. □

DEFINITION 5.9. Sei $R = (R, +, \cdot)$ ein Ring mit Einselement. Sei K ein Körper. Dann heisst R eine K-Algebra, wenn R bzgl. einer Abbildung

$$K \times R \to R,\ (\alpha, r) \mapsto \alpha \cdot r = \alpha r$$

zusätzlich ein K-Vektorraum ist, so dass gilt

$$\alpha(rs) = (\alpha r)s = r(\alpha s) \quad \text{für alle } \alpha \in K,\ r, s \in R.$$

Beispiele 5.10. (1) $\mathrm{End}_K(V)$ für einen K-Vektorraum V.
(2) $\mathrm{M}_n(K)$ ist eine K-Algebra der Dimension n^2.
(3) $\mathcal{C}([0,1],\mathbb{R})$ stetige reelle Funktionen auf $[0,1]$ ist eine unendlichdimensionale $\mathbb{R}$-Algebra.
(4)* $K[X]$ ist eine unendlichdimensionale K-Algebra.

Satz 5.11. *Jede endlichdimensionale nullteilerfreie K-Algebra $R \neq 0$ (K ein Körper) ist ein Schiefkörper.*

Beweis. Sei $a \in R$, $a \neq 0$. Die Abbildung

$$\lambda_a \colon R \to R,\ x \mapsto ax$$

ist K-linear und – da a kein Nullteiler ist – injektiv, und wegen der Endlichdimensionalität von R auch surjektiv. Insbesondere gibt es ein $x \in R$ mit $1 = \lambda_a(x) = ax$. Aus denselben Gründen gibt es ein $y \in R$ mit $1 = \lambda_x(y) = xy$. Es folgt

$$a = a \cdot 1 = a(xy) = (ax)y = 1 \cdot y,$$

d. h. $ax = 1 = xa$, und damit ist a invertierbar. □

Definition 5.12. Seien R und S Ringe. Eine Abbildung $f \colon R \to S$ heisst (Ring-) Homomorphismus, falls

$$f(x+y) = f(x) + f(y) \quad \text{für alle } x,\, y \in R$$
$$f(x \cdot y) = f(x) \cdot f(y) \quad \text{für alle } x,\, y \in R$$
$$f(1_R) = 1_S$$

gilt. Ist F zusätzlich bijektiv, so heisst f ein Isomorphismus (von Ringen). Zwei Ringe R und S heissen isomorph (Notation: $R \simeq S$), falls es einen Isomorphismus $f \colon R \to S$ gibt.

Definition 5.13. Unterring = Teilring. Teilkörper / Körpererweiterung. (Siehe Vorlesung.)

Beispiele 5.14. (1) $\mathbb{Z}$ ist Teilring von $\mathbb{Q}$. $\mathbb{Q}$ ist ein Teilkörper von $\mathbb{R}$.
(2) Sei $f \colon R \to S$ ein Ringhomomorphismus. Dann ist $\mathrm{Bild}(f)$ ein Unterring von S.
(3) Sei R ein Ring. Dann ist durch $h \colon \mathbb{Z} \to R$, $n \mapsto n \cdot 1 = \ldots$ ein Ringhomomorphismus. Dessen Bild $\mathbb{Z} \cdot 1$ ist der kleinste Unterring von R.
(4) $A = \mathcal{C}([0,1],\mathbb{R})$. Sie $x \in [0,1]$. Dann ist $e_x \colon A \to \mathbb{R}$, $f \mapsto f(x)$ ein (surjektiver) Ringhomomorphismus.
(5) Ist S ein Unterring von R, so ist die Einbettung $j \colon S \to R$, $x \mapsto x$ ein Ringhomomorphismus.

6. Ideale und Faktorringe

Satz 6.1. *Sei $f \colon R \to S$ ein Homormorphismus von Ringen. Dann hat*

$$I = \mathrm{Kern}(f) = \{r \in R \mid f(r) = 0_s\}$$

folgende Eigenschaften:

(I1) *$(I,+)$ ist eine Untergruppe von $(R,+)$;*
(I2) *$R \cdot I \subseteq I$ und $I \cdot R \subseteq I$.*

Beweis. Klar. □

Definition 6.2. Eine Teilmenge $I \subseteq R$ eines Rings R heisst Ideal, falls sie obige Eigenschaften (I1) und (I2) erfüllt.

Lemma 6.3. *Sei R ein kommutativer Ring und $a \in R$. Dann ist $I = Ra = \{ra \mid r \in R\}$ ein Ideal in R.*

Ra heißt (das von a erzeugte) Hauptideal.

SATZ 6.4. *Im Ring $\mathbb{Z}$ ist jedes Ideal ein Hauptideal.*

BEWEIS. Wir hatten schon gesehen, dass die abelsche Gruppe $(\mathbb{Z}, +)$ nur zyklische Untergruppen besitzt, allesamt von der Form $\mathbb{Z}\cdot n$ ($n \in \mathbb{Z}$). Da jede Ideal in $\mathbb{Z}$ insbesondere eine Untergruppe von $\mathbb{Z}$ ist, folgt sofort die Behauptung. □

DEFINITION 6.5. Ein Integritätsbereich, in welchem jedes Ideal ein Hauptideal ist, heißt Hauptidealring (oder -bereich).

BEISPIELE 6.6. Beispiele für Hauptidealringe:

(1) $\mathbb{Z}$
(2) Jeder Körper.
(3)* Der Polynomring $K[X]$ (K Körper). (Dies wird später gezeigt.)

SATZ 6.7. *Ein kommutativer Ring R ist genau dann ein Körper, wenn er genau zwei Ideale hat.*

BEWEIS. (1) Seien $\{0\}$ und R die einzigen beiden Ideale in R (also insbesondere $R \neq \{0\}$). Sei $a \in R$ mit $a \neq 0$. Dann ist das von a erzeugte Hauptideal Ra ungleich $\{0\}$, also muss $Ra = R$ gelten. Insbesondere gibt es ein $r \in R$ mit $1 = ra$. Es folgt, dass a invertierbar ist.

(2) Sei R ein Körper. Dann sind die Ideale $\{0\}$ und R verschieden. Sei $I \neq \{0\}$ ein Ideal. Es gibt ein $a \in I$ mit $a \neq 0$. Da a invertierbar ist, gilt $1 = a^{-1}a \in Ra \subseteq I$. Ist nun $r \in R$ beliebig, so folgt $r = r \cdot 1 \in I$. Also gilt $I = R$. □

SATZ UND DEFINITION 6.8. *Sei R ein Ring und $I \subseteq R$ ein Ideal. Dann wird die Faktorgruppe R/I von $(R, +)$ nach I zu einem Ring vermöge der Multiplikation*

$$[x] \cdot [y] \stackrel{def}{=} [xy],$$

wobei hier $[x]$ für $x \in R$ die Nebenklasse $x + R \in R/I$ bezeichnet. Es ist $1_{R/I} = [1_R]$. Der Ring R/I heisst der Faktorring von R nach dem Ideal I (oder: modulo I).

BEWEIS. Ähnlich wie im Gruppenfall ist hier der wesentliche Punkt zu zeigen, dass die Multiplikation wohldefiniert ist. Dazu verwendet man die Idealeigenschaft. (Details siehe Vorlesung.) □

SATZ 6.9 (Homomorphiesatz für Ringe). *Seien R und S Ringe, und sei $f\colon R \to S$ ein Ringhomomorphismus. Dann ist $I = \mathrm{Kern}(f)$ ein Ideal in R. Es gibt genau einen Ringhomomorphismus $\bar{f}\colon R/I \to S$ mit $\bar{f} \circ \nu = f$, wobei $\nu\colon R \to R/I$, $a \mapsto [a]$ der natürliche surjektive Ringhomomorphismus ist. Ferner ist $\bar{f}$ injektiv.*

BEWEIS. Der Homomorphiesatz für Gruppen liefert einen eindeutigen Gruppenhomomorphismus $\bar{f}\colon R/I \to S$, zwischen den additiven abelschen Gruppen $(R/I, +)$ und $(S, +)$, für den $\bar{f} \circ \nu = f$ gilt, und $\bar{f}$ ist injektiv. Es ist nur noch zu zeigen, dass $\bar{f}$ auch ein Ringhomomorphismus ist. Dies rechnet man leicht nach. (Siehe Vorlesung für Details.) □

7. Der Faktorring $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$

SATZ 7.1. *Für $n \geq 1$ sind äquivalent:*

(1) *$\mathbb{Z}_n$ ist ein Körper.*
(2) *$\mathbb{Z}_n$ ist ein Integritätsbereich.*
(3) *n ist eine Primzahl.*

BEWEIS. (1)⇔(2): Da $\mathbb{Z}_n$ endlich ist, folgt dies aus Satz 5.8 und Lemma 5.5.

(2)⇒(3): Sei $\mathbb{Z}_n$ integer und n keine Primzahl. Dann gibt es $a, b \in \mathbb{Z}$ mit $1 < a$, $b < n$ mit $n = a \cdot b$. Für die Klassen in $\mathbb{Z}_n$ folgt dann $[a] \neq 0$, $[b] \neq 0$, aber $[a] \cdot [b] = [n] = [0]$, Widerspruch.

(3)⇒(2): Sei $n = p$ eine Primzahl. Wir verwenden folgende Eigenschaft einer Primzahl: teilt p ein Produkt ab, so teilt p einen der Faktoren, a oder b. Seien nun a, $b \in \mathbb{Z}$ mit $[a] \cdot [b] = [0]$. Dann $[ab] = [a][b] = [0]$, also $ab \in \mathbb{Z} \cdot p$. Das bedeutet $p \mid ab$, also teilt p einen der Faktoren, was $[a] = 0$ oder $[b] = 0$ bedeutet. □

$\mathbb{F}_p = \mathbb{Z}_p$. Anwendung: Jeder endliche Körper K enthält p^n Elemente. Enthält einen zu $\mathbb{F}_p$ isomorphen Teilkörper. (Siehe Vorlesung für Details.)

KAPITEL III

Gruppenaktionen

Lernziele:

- Das Konzept einer Gruppenaktion begreifen.
- Einige wichtige Beispiele von Gruppenaktionen kennen.
- Bahnenlemma und Bahnenzerlegung; Satz von Lagrange und die Klassengleichung als Spezialfälle.
- Die Sylowsätze verstehen. Eine grobe Vorstellung von der Beweisidee haben.
- Satz von Poincaré und seine Hauptanwendungsfälle.
- Eine Vorstellung haben (Beispiele!), wie diese Sätze zur Klassifikation von (einfachen) Gruppen verwendet werden können.
- Die Definitionen von einfachen und von auflösbaren Gruppen kennen.

1. Grundlegende Eigenschaften und Beispiele

DEFINITION 1.1. Sei G eine Gruppe und M eine Menge. Unter einer Aktion (oder auch: Operation) von G auf M verstehen wir eine Abbildung

$$G \times M \to M,\ (g, m) \mapsto g.m,$$

die den folgenden Bedingungen genügt:

(A1) $e.m = m$ für alle $m \in M$;
(A2) $g.(h.m) = (g \cdot h).m$ für alle $g,\ h \in G,\ m \in M$.

BEISPIELE 1.2. (1) $\mathrm{GL}_n(K)$ operiert auf K^n.
(2) Gruppe G operiert auf sich selbst durch (Links-) Multiplikation.
(3) Gruppe G operiert auf sich selbst durch Konjugation.

DEFINITION 1.3. Sei $G \times M \to M$, $(g, m) \mapsto g.m$ eine Gruppenaktion und sei $m \in M$.

(a) $B = G.m = \{g.m \mid g \in G\}$ heißt die G-Bahn von m (unter der Aktion von G).
(b) Mit $M/G = \{G.m \bmod m \in M\}$ bezeichnen wir die Menge aller G-Bahnen von M, den sog. Bahnenraum.
(c) Die Menge $\mathrm{St}(m) = \{g \in G \mid g.m = m\}$ ist eine Untergruppe von G; sie heißt die Standuntergruppe von m.

LEMMA 1.4 (Bahnenlemma). *G operiere auf M. Sei $m \in M$.*

(a) *Die Abbildung*

$$\varphi\colon G/\mathrm{St}(m) \to G.m,\ g \cdot \mathrm{St}(m) \mapsto g.m$$

ist eine Bijektion. Falls G endlich ist, ist also $|G.m|$ stets ein Teiler von $|G|$.
(b) *Ist $m' = g.m$, so ist*

$$\mathrm{St}(m') = g\,\mathrm{St}(m)g^{-1}.$$

BEWEIS. (Vgl. Vorlesung.) □

SATZ 1.5 (Bahnenzerlegung). (a) *Zwei Bahnen sind gleich oder disjunkt.*
(b) *Es gilt*

$$M = \coprod_{B \in M/G} B.$$

BEWEIS. (Vgl. Vorlesung.) □

BEISPIELE 1.6. (1) Die Gruppe $\mathbb{T} = \{z \in \mathbb{C} \mid |z| = 1\}$ operiert auf der Menge $\mathbb{C}$ der komplexen Zahlen durch Multiplikation

$$\mathbb{T} \times \mathbb{C} \to \mathbb{C},\ (t, x) \mapsto tx.$$

Die Bahnen sind Kreise um 0 mit einem Radius $r \geq 0$. Dieses Beispiel verdeutlicht besonders gut die Bahnenzerlegung. Wir sehen hier auch, dass die Bahnen unterschiedliche Mächtigkeiten haben können.

(2) Sei U eine Untergruppe der Gruppe G. Dies liefert die U-Aktion auf G,

$$U \times G \mapsto G,\ (u, g) \mapsto ug.$$

Die Bahnen sind hier die Linksnebenklassen Ug von U, die Standuntergruppen sind trivial. Alle Bahnen haben die gleich Mächtigkeit, da $U \to Ug$, $u \mapsto ug$ bijektiv. Falls G endlich ist liefert die Bahnenzerlegung

$$|G| = |U| \cdot |G/U|,$$

den bekannten Satz von Lagrange.

(3) G operiert auf G durch Konjugation

$$(g, x) \mapsto gxg^{-1}.$$

Die Bahn zu $x \in G$ ist die Konjugationsklassen $C(x) = \{gxg^{-1} \mid g \in G\}$, die gleichmächtig zu $G/N(x)$, wobei $N(x)$ die Standuntergruppe $\{g \in G \mid gxg^{-1} = x\}$ ist, also der Zentralisator von x. Die Bahnenzerlegung führt – für endliches G – zur Klassengleichung.

(4) Sei σ eine Permutation von $1, \ldots, n$. Die zyklische Gruppe $G = \langle\sigma\rangle$ operiert auf $\{1, \ldots, n\}$. Die Bahn von i enthalten wird duch Bildung der Sequenz

$$\sigma(i),\ \sigma^2(i), \ldots,\ \sigma^j(i) = i \quad j > 0 \text{ minimal.}$$

Die Zahlen $1, \ldots, n$ werden dadurch in disjunkte Bahnen zerlegt. Dies korrespondiert zu sog. Zykelzerlegung von σ.

2. Die Sylowsätze

SATZ 2.1 (1. Sylowscher Satz). *Sei $|G| = p^n \cdot m$ mit p prim, m teilerfremd zu p, und $n \geq 1$. Dann besitzt G mindestens eine Untergruppe P der Ordnung p^n.*

BEWEIS. Induktion nach $|G|$. Für $|G| = 1$ ist alles klar. Wir nehmen an, dass für Gruppen einer Ordnung $< |G|$ die Aussage gilt und zeigen sie für G. Wir können $p \mid |G|$ annehmen. Sei $Z = Z(G)$ das Zentrum von G. Dann operiert G auf der Komplementmenge $G \setminus Z$ durch Konjugation

$$G \times \big(G \setminus Z\big) \to G \setminus Z,\ (g, x) \mapsto gxg^{-1}.$$

Die Bahnen der Operation sind die Konjugationsklassen $C(g)$ nichtzentraler Elemente g, deren Standuntergruppe $\mathrm{St}(g) = Z(g) = \{h \in G \mid hg = gh\}$ die Zentralisatoren von g sind. Für nichtzentrales g gilt $Z(g) \neq G$. Zwei Fälle treten auf:

1. Fall: Es gibt ein $g \in G \setminus Z$, so dass p^n die Ordnung von $Z(g)$ teilt. Wegen $Z(g) \neq G$ lässt sich auf $Z(g)$ die Induktionsvoraussetzung anwenden: Es hat dann $Z(g)$, folglich auch G, eine Untergruppe der Ordnung p^n.

2. Fall: Für kein $g \in G \setminus Z$ ist p^n ein Teiler von $|Z|$. Wegen

$$p^n \cdot m = |G| = |Z(g)| \cdot |C(g)|$$

(Bahnenlemma) muss dann p ein Teiler von $|C(g)|$ sein; dies für jedes $g \in G \setminus Z$. Da

$$G \setminus Z = \coprod C(g)$$

(Bahnenzerlegung) ist dann p ein Teiler von $|G \setminus Z| = |G| - |Z|$ und p folglich ein Teiler von Z. Nach dem Satz von Cauchy (nur die kommutative Version benötigt) hat Z eine Untergruppe U der Ordnung p. Wegen $U < Z$ ist U ein Normalteiler in G, also können

wir die Faktorgruppe G/U bilden und auf G/U die Induktionsvoraussetzung anwenden. Es gibt also eine Untergruppe $\overline{P}$ von G/U der Ordnung p^{n-1}. Definieren wir – mittels des natürlichen Homomorphismus $\nu\colon G \to G/U$ – die Untergruppe P von G als Urbild $P = \nu^{-1}(\overline{P})$, so folgt

$$P/U = \nu(P) = \overline{P},$$

also $|P| = |U| \cdot |\overline{P}| = p \cdot p^{n-1} = p^n$. □

Jede solche Untergruppe heisst p-Sylowgruppe von G.

Satz 2.2 (2. Sylowscher Satz). *Je zwei p-Sylowgruppen von G sind konjugiert.*

Beweis. Wir zeigen etwas mehr: Ist P eine p-Sylowgruppe und Q eine p-Untergruppe von G, so gibt es ein $g \in G$ mit $Q \subseteq gPg^{-1}$.

Wir lassen Q durch Linksmultiplikation auf der Menge $M = G/P = \{gP \mid g \in G\}$ der Rechtsnebenklassen operieren:

$$Q \times G/P \to G/P,\ (q, gP) \mapsto qgP.$$

Es ist klar, dass dies wohldefiniert ist und eine Gruppenaktion darstellt. Hierdurch wird $M = G/P$ in Q-Bahnen zerlegt. Die einelementigen fassen wir als Menge

$$M^Q = \{m \in M \mid q.m = m \text{ für alle } q \in Q\}$$

der Fixpunkte von M zusammen. Es folgt

$$M = M^Q \sqcup \big(B_1 \sqcup \ldots \sqcup B_r\big),$$

wobei $B_1, \ldots, B_r$ die verschiedenen Q-Bahnen mit > 1 Elementen bezeichnen.

$M = G/P$ hat eine zu p teilerfremde Elementanzahl. Jedes $|B_i| > 1$ teilt die Ordnung von Q (Bahnenlemma), wird daher von p geteilt. Somit ist p ein Teiler von $|M \setminus M^Q| = |M| - |M^Q|$, und da p kein Teiler von $|M|$ ist, folgt $M^Q \neq \emptyset$. Sei nun $gP \in M^Q$. Dann folgt $qgP = gP$ für alle $q \in Q$, was

$$Q \subseteq gPg^{-1}$$

bedeutet. □

Insbesondere sind alle p-Sylowgruppen von G isomorph.

Satz 2.3 (3. Sylowscher Satz). *Sei $|G| = p^n \cdot m$ mit p prim, m teilerfremd zu p, und $n \geq 1$. Die Anzahl $\alpha(p)$ der p-Sylowgruppen von G ist ein Teiler von m und von der Form $\alpha(p) = 1 + kp$ für ein $k \geq 0$.*

Beweis. Sei $\mathcal{U}(G)$ die Menge aller Untergruppen von G. Darauf operiert G durch Konjugation

$$G \times \mathcal{U}(G) \to \mathcal{U}(G),\ (g, U) \mapsto gUg^{-1}.$$

Nach dem 2. Sylowschen Satz bilden dabei die p-Sylowgruppen von G eine einzige Bahn

$$B = \{gPg^{-1} \mid g \in G\},$$

wobei P beliebig gewählte p-Sylowgruppe ist. Nach Bahnenlemma ist somit $\alpha(p) = |B|$ ein Teiler von $|G|$. Genauer ist $\alpha(p)$ der Index der Standuntergruppe

$$N(P) = \{g \in G \mid gPg^{-1} = P\}$$

in G, welche man den Normalisator von P nennt. Um die Anzahl $\alpha(p)$ besser einzugrenzen, lassen wir nun P auf $M = G/N(P) = \{gN(P) \mid g \in G\}$ operieren,

$$P \times G/N(P) \to G/N(P),\ (p, gN(P)) \mapsto pgN(P).$$

In diesem Fall ist die Fixpunktmenge

$$M^P = \{N(P)\}$$

einelementig: Denn $pgN(P) = gN(P)$ für alle $p \in P$ bedeutet gerade $g \in N(P)$. (Beweis hierfür: Aus $pgN(P) = gN(P)$ für alle $p \in P$ folgt $Q := g^{-1}Pg < N(P)$. Und da P Normalteiler in $N(P)$ ist (klar!), sowie P und Q beide p-Sylowgruppen von $N(P)$ sind, also – in $N(P)$ – zueinander konjugiert (nach dem 2. Sylowschen Satz), folgt $Q = P$. Damit $g^{-1}Pg = P$, und damit $g \in N(P)$.) Die P-Bahnenzerlegung

$$M = M^P \sqcup \big(B_1 \sqcup \ldots \sqcup B_r\big)$$

liefert Bahnen B_i, deren Mächtigkeiten $|B_i| > 1$ alle durch p teilbar sind, also

$$\alpha(p) = 1 + k \cdot p \quad \text{für ein } k \geq 0.$$

Ferner folgt wegen $P < N(P) < G$ und aus $\alpha(p) = [G : N(P)]$ mit dem Satz von Lagrange

$$|G| = |N(P)| \cdot [G : N(P)] = |P| \cdot [G : N(P)] \cdot [N(P) : P],$$

und damit $\alpha(p) \mid q = [G : N(P)] \cdot [N(P) : P]$. □

3. Eine Anwendung: Gruppen der Ordnung 15 sind zyklisch

Sei G eine Gruppe der Ordnung $15 = 3 \cdot 5$. Für die Anzahlen $\alpha(3)$ bzw. $\alpha(5)$ der 3- bzw. 5-Sylowgruppen gilt nach dem dritten Sylowschen Satz $\alpha(3) \mid 5$, $\alpha(5) \mid 3$, und zusätzlich $\alpha(3) = 1 + \ell 3$ sowie $\alpha(5) = 1 + k5$ für $\ell, k \geq 0$. Also ist nur $\alpha(3) = 1 = \alpha(5)$ möglich. Das heisst, es gibt genau eine Untergruppe U der Ordnung 3 und genau eine Untergruppe V der Ordnung 5. Jedes Element in $G \setminus (U \cup V)$ hat die Ordnung 15, d. h. erzeugt G.

Allgemeiner:

Satz 3.1. *Seien $p < q$ Primzahlen mit $p \nmid (q-1)$. Dann ist jede Gruppe der Ordnung $n = pq$ zyklisch, d. h. isomorph zu $\mathbb{Z}_{pq}$.*

Beweis. Es gilt $\alpha(q) \in \{1, p\}$ sowie $\alpha(q) = 1 + \ell q$ für ein $\ell \geq 0$. Wegen $p < q$ kann nur $\alpha(q) = 1$ gelten. Weiter gilt $\alpha(p) \in \{1, q\}$ und $\alpha(p) = 1 + kp$ für ein $k \geq 0$. Wäre $\alpha(p) = q$, so folgte $kp = (q-1)$, Widerspruch zu der Annahme, dass $p \nmid (q-1)$ gilt. Also gibt es genau eine p- und genau eine q-Sylowgruppe von G. Jedes Element außerhalb dieser hat die Ordnung pq. Davon gibt es $pq - p - q + 1 = (p-1)(q-1) \geq q - 1 \geq 4$ viele. □

4. Die Anzahl der Bahnen

Die Gruppe G operiere auf der Menge M. Für $g \in G$ sei $\mathrm{Fix}(g) = \{m \in M \mid g.m = m\}$ die Menge aller Fixpunkte von g in M.

Satz 4.1 (Fixpunktformel). *Die endliche Gruppe G operiere auf der endlichen Menge M.*

$$|M/G| = \frac{1}{|G|} \sum_{g \in G} |\,\mathrm{Fix}(g)|.$$

In Worten: Die Anzahl der Bahnen ist gleich dem Mittelwert der Anzahl der Fixpunkte.

Beweis. Sei

$$F = \{(g, m) \mid g \in G,\ m \in M,\ g.m = m\}.$$

Es gilt

$$F = \coprod_{g \in G} \{g\} \times \mathrm{Fix}(g) = \coprod_{m \in M} \mathrm{St}(m) \times \{m\},$$

also

$$|F| = \sum_{g \in G} |Fix(g)| = \sum_{m \in M} |\,\mathrm{St}(m)|.$$

Seien $B_1, \ldots, B_r$ die verschiedenen Bahnen, $r = |M/G|$. Für alle Punkte einer Bahn B_i sind die Standuntergruppen konjugiert, haben also dieselbe Elementanzahl. Es folgt

$$|F| = \sum_{m \in M} |\operatorname{St}(m)| = \sum_{i=1}^{r} |B_i| \cdot |\operatorname{St}(m_i)| = r \cdot |G|$$

mit $m_i \in B_i$. Setzt man alles zusammen, folgt die Behauptung. □

Beispiel 4.2. Die symmetrische Gruppe S_n operiert auf $\{1, \ldots, n\}$ mit einer Bahn. Folglich ist

$$1 = \frac{1}{n!} \sum_{\sigma \in S_n} |\operatorname{Fix}(\sigma)|.$$

Daher hat eine Permutation "im Durchschnitt" einen Fixpunkt.

5. Einfache Gruppen

Definition 5.1. Eine Gruppe G heisst einfach, wenn $G \neq \{e\}$ gilt, und wenn G und $\{e\}$ die einzigen Normalteiler von G sind.

Satz 5.2. *Eine endliche abelsche Gruppe ist einfach genau dann wenn sie von Primzahlordnung ist.*

Wir konzentrieren uns bei der Untersuchung einfacher Gruppen daher auf den nichtabelschen Fall.

Satz 5.3. *Es gibt keine einfache Gruppe der Ordnung p^2 bzw. pq (p, q prim).*

Beweis. (a) Jede Gruppe der Ordnung p^2 ist abelsch. Eine abelsche Gruppe ist aber nur abelsch, wenn $|G|$ ein Primzahl ist.

(b) Sei G von der Ordnung pq mit $p < q$ prim. Wir hatten weiter oben gesehen, dass $\alpha(q) = 1$ gilt; das bedeutet, dass es genau eine q-Sylowgruppe U von G gibt. Da alle konjugierten eine q-Sylowgruppe wieder eine q-Sylowgruppe ist, folgt, dass U ein Normalteiler ist. Also ist G nicht einfach. □

Als wichtiges Argument halten wir fest (die Umkehrung folgt aus dem zweiten Sylowschen Satz):

Lemma 5.4. *Sei U eine p-Sylowgruppe der endlichen Gruppe G. Dann gilt*

$$U \text{ ist Normalteiler} \;\Leftrightarrow\; \alpha(p) = 1.$$

Der Fall pq im obigen Resultat kann verallgemeinert werden:

Satz 5.5. *Es gibt keine einfache Gruppe der Ordnung ap (p prim, $1 < a < p$).*

Beweis. Die Teiler von $|G|$ sind

$$\{\text{Teiler von } a\} \cup \{\text{Teiler von } a\} \cdot p.$$

Davon ist nur 1 kongruent 1 modulo p, also $\alpha(p) = 1$. Somit ist *die* p-Sylowgruppe Normalteiler. □

Die Gruppe G operiere auf der Menge M. Wir sagen, dass diese Operation transitiv ist, wenn es genau eine G-Bahn von M gibt: $M = G.m$ (für ein, und damit alle, $m \in M$). Anders formuliert: Zu m, $m' \in M$ gibt es stets $g \in G$ mit $m' = g.m$.

Satz 5.6 (Poincaré). *Sei G eine nicht-abelsche einfache Gruppe, die transitiv auf einer endlichen Menge M operiert, mit $n = |M| \geq 2$. Dann ist G isomorph zu einer Untergruppe der alternierenden Gruppe A_n.*

BEWEIS. Für jedes $g \in G$ bezeichne

$$g_M \colon M \to M,\ m \mapsto g.m$$

die Operation von g auf M. Wir haben schon früher gesehen (Beweis vom Satz von Cayley), dass

$$\varphi \colon G \to S(M),\ g \mapsto g_M$$

ein Gruppenhomomorphismus ist. Da $|M| \geq 2$ und G transitiv operiert, ist φ nicht trivial (d. h. $\mathrm{Kern}(\varphi) \neq G$). Da G einfach ist, folgt $\mathrm{Kern}(\varphi) = \{e\}$, also ist φ injektiv. Wegen $|M| = n$ können wir $S(M)$ mit S_n identifizieren und erhalten somit eine Einbettung

$$\varphi \colon G \to S_n.$$

Komponiert mit der Signatur $\mathrm{sgn} \colon S_n \to \mathbb{Z}_2$ ergibt einen Homomorphismus $\mathrm{sgn} \circ \varphi \colon G \to \mathbb{Z}_2$, der wegen der Voraussetzung an G nicht surjektiv sein kann (andernfalls hätte G eine Untergruppe vom Index 2, die dann ein Normalteiler wäre). Also ist $\mathrm{sgn} \circ \varphi$ der triviale Homomorphismus und

$$G \simeq \varphi(G) < A_n.$$

□

FOLGERUNG 5.7. *Sei $n \geq 2$. Sei G eine nicht-abelsche einfache Gruppe. Es gelte eine der drei Bedingungen:*

(i) *G hat eine Untergruppe U vom Index n; oder*
(ii) *G hat eine n-elementige Konjugationsklasse $C(g)$; oder*
(iii) *es gibt einen Primteiler p von $|G|$ mit $\alpha(p) = n$.*

Dann ist G zu einer Untergruppe von A_n isomorph.

BEWEIS. G operiert transitiv auf

(i) $G/U = \{gU \mid g \in G\}$ via Linksmultiplikation; bzw.
(ii) $C(g)$ via Konjugation; bzw.
(iii) der Menge der p-Sylowgruppen von G via Konjugation.

In jedem der drei Fälle folgt die Behauptung nun aus dem Satz von Poincaré. □

SATZ 5.8. *Es gibt keine nicht-abelsche einfache Gruppe G mit $1 \leq |G| < 60$.*

BEWEIS. Wir können Primzahlpotenzen nach Lemma II.3.1 sowie Ordnungen ap (p prim, $1 < a < p$) ausschließen. Bleiben die Ordnungen

$$12,\ 18,\ 24,\ 30,\ 36,\ 40,\ 45,\ 48,\ 50,\ 54,\ 56.$$

(a) 18, 50, 54 haben die Form $2 \cdot p^k$ ($2 \neq p$ prim). Die p-Sylowgruppe hat Index 2, ist also Normalteiler.

(b) 12, 24, 48 haben die Form $3 \cdot p^k$ ($p = 2$ prim). Die p-Sylowgruppe hat Index 3, Widerspruch zu Poincaré (Folgerung 5.7).

(c) 40, 45 haben die Form $5 \cdot p^k$ (p prim). Die p-Sylowgruppe hat daher den Index 5. Somit ist G isomorph zu einer Untergruppe von A_5, aber $|G| \nmid 60$, Widerspruch.

(d) 36. Hier hat eine 3-Sylowgruppe Index 4, also $G < A_4$, Widerspruch.

(e) 30. Übung.

(f) 56. Übung. □

SATZ 5.9. *Jede einfache Gruppe der Ordnung 60 ist isomorph zur alternierenden Gruppe A_5.*

BEWEIS. Sei G einfach mit $|G| = 60$. Da 60 keine Primzahl ist, ist G nicht abelsch. Da $60 = 2^2 \cdot 3 \cdot 5$ folgt $\alpha(5) \in \{1, 6\}$. Wegen der Einfachheit von G scheidet $\alpha(5) = 1$ aus, somit gilt $\alpha(5) = 6$. Ferner ist $\alpha(2) \in \{3, 5, 15\}$ und $\alpha(3) \in \{4, 10\}$. Wegen des Satzes von

Poincaré kommen nur $\alpha(2) = 15$ und $\alpha(3) = 10$ infrage. (Im Falle $\alpha(2) = 5$ wäre $G < A_5$, also $G \simeq A_5$; im dem Fall wären wir also fertig.) Also:

$$\alpha(2) = 15,\ \alpha(3) = 10,\ \alpha(5) = 6.$$

Wir zeigen nun, dass G eine Untergruppe vom Index 5 besitzt. Dazu untersuchen wir die 15 2-Sylowgruppen von G, die je 4 Elemente haben. Falls je zwei verschiedene 2-Sylowgruppen $U \neq V$ einen trivialen Durchschnitt haben, folgt

$$|G| \geq 1 + 15 \cdot 3 + 10 \cdot 2 + 6 \cdot 4 = 90,$$

Widerspruch. Also gibt es zwei 2-Sylowgruppen $U \neq V$ mit $e \neq x \in U \cap V$. Als Untergruppen der Ordnung 4 sind U und V abelsch, somit umfasst der Zentralisator $Z(x)$ sowohl U als auch V, $[G : Z(x)]$ ist daher ein echter Teiler von $[G : U] = 3 \cdot 5$. Wegen des Satzes von Poincaré ist $[G : Z(x)] = 3$ nicht möglich. $[G : Z(x)] = 1$ ist ebenfalls nicht möglich, da dies sonst $e \neq x \in Z(G)$ impliziert und $Z(G)$ dann ein nichttrivialer Normalteiler von G wäre.

Also ist $[G : Z(x)] = 5$, und nach dem Satz von Poincaré G dann isomorph zu A_5. □

6. Einfachheit der alternierenden Gruppe A_5

LEMMA 6.1. (a) *Für $n \geq 3$ wird A_n von 3-Zykeln erzeugt.*
(b) *(Cauchy) Für $n \geq 5$ sind je zwei 3-Zykeln in A_n zueinander konjugiert.*

BEWEIS. In den Übungen. □

SATZ 6.2 (Jordan). *Für $n \geq 5$ ist die alternierende Gruppe A_n einfach.*

BEWEIS. Sei $N \neq \{e\}$ ein Normalteiler in A_n. Wir zeigen, dass N einen 3-Zykel enthält. Aus Lemma 6.1 folgt dann $N = A_n$.

Sei $1 \neq \sigma \in N$. Es gibt eine Darstellung

$$\sigma = \sigma_1 \circ \ldots \circ \sigma_r$$

von σ in disjunkte Zykeln (vgl. Bahnenzerlegung). Da disjunkte Zykeln miteinander kommutieren, können wir sie der Länge nach ordnen, also ohne Einschränkung gelte $\ell(\sigma_1) \geq \ell(\sigma_2) \geq \ldots \geq \ell(\sigma_r) \geq 2$, wobei $\ell(\sigma_i) = \ell_i$, wenn σ_i ein ℓ_i-Zykel ist.

1. Fall: $\ell_1 \geq 4$. Sei etwa $\sigma_1 = (a\ b\ c\ d \ldots)$. Mit $\tau = (a\ b\ c) \in A_n$ gilt

$$(a\ d\ b) = (b\ c\ d)(c\ b\ a) = (\sigma\tau\sigma^{-1})\tau^{-1} = \sigma(\tau\sigma^{-1}\tau^{-1}) \in N$$

(vgl. Übungen).

2. Fall: $\ell_1 = 3$. Im Falle $\sigma = \sigma_1$ ist die Behauptung richtig. Sei also $r \geq 2$, seien $\sigma_1 = (a\ b\ c)$ und $\sigma_2 = (d\ e\ f)$ oder $\sigma_2 = (d\ e)$. Mit $\tau = (a\ b\ d) \in A_n$ folgt

$$(a\ d\ c\ e\ b) = (b\ c\ e)(d\ b\ a) = (\sigma\tau\sigma^{-1})\tau^{-1} = \sigma(\tau\sigma^{-1}\tau^{-1}) \in N.$$

Nimmt man $(a\ d\ c\ e\ b)$ statt σ, so können wir den 1. Fall anwenden.

3. Fall: $\ell_1 = 2$. Dann sind $\sigma_1, \ldots, \sigma_r$ disjunkte Transpositionen, und $r \geq 2$, etwa $\sigma_1 = (a\ b)$, $\sigma_2 = (c\ d)$. Sei $e \neq a, b, c, d$ (möglich wegen $n \geq 5$). Für $\tau = (a\ c\ e) \in A_n$ folgt

$$(b\ d\ \sigma(e))(e\ c\ a) = (\sigma\tau\sigma^{-1})\tau^{-1} = \sigma(\tau\sigma^{-1}\tau^{-1}) \in N.$$

Gilt dabei $\sigma(e) = e$, so ist dies Element $(a\ b\ d\ e\ c)$, und wir können den 1. Fall anwenden. Gilt $\sigma(e) \neq e$, so sind $(b\ d\ \sigma(e))$ und $(e\ c\ a)$ disjunkt (denn $\sigma(e) \neq \sigma(d) = c$ und $\sigma(e) \neq \sigma(b) = a$). Nimmt man daher $(b\ d\ \sigma(e))(e\ c\ a)$ statt σ, so folgt die Behauptung aus dem 2. Fall. □

SATZ 6.3. *Es gibt keine nicht-abelsche einfache Gruppe G mit $60 < |G| < 168$.*

BEWEIS. (Skizze.) Mit ähnlichen Argumenten (Sylow & Poincaré) kann man fast alle Ordnungen n zwischen 60 und 168 abarbeiten. In der überwiegenden Majorität der Fälle liefern bereits die Sylowsätze einen Primteiler p von $|G|$ mit $\alpha(p) = 1$. Es bleiben dann noch die Ordnungen

$$72,\ 80,\ 90,\ 96,\ 105,\ 108,\ 112,\ 120,\ 132,\ 144,\ 150,\ 160$$

zu behandeln. Eine hypothetische einfache Gruppe hat für die Fälle

$$72,\ 80,\ 96,\ 108,\ 160$$

eine Untergruppe vom Index 3, 4 oder 5 per Sylow (im Falle $n = 72$ ist $\alpha(3) = 4$, dann $G < A_4$). Es bleiben etwas hartnäckigere Fälle

$$90,\ 105,\ 112,\ 120,\ 132,\ 144,\ 150$$

zu behandeln.

(a) 90, 120, 150 haben $\alpha(5) = 6$, liefern also eine Einbettung $G < A_6$ mit zugehörigem Index 4, 3 bzw. 360/150. Die letzte Möglichkeit ist absurd, aber auch Index 4 bzw. 3 treten für Untergruppen der A_6 nicht auf, da sie einfach ist (verwende Poincaré).

(b) 105 (Übung!) $= 3 \cdot 5 \cdot 7$. Bei angenommener Einfachheit liefern die Sylowsätze $\alpha(5) = 21$, $\alpha(7) = 15$, und dann $|G| \geq 21 \cdot 4 + 15 \cdot 6$, Widerspruch.

(c) 132 (Übung!) $= 2^2 \cdot 3 \cdot 11$ ähnlich: $\alpha(2) \geq 11$, $\alpha(3) = 22$, $\alpha(11) = 12$.

(d) Es bleiben also $112 = 2^4 \cdot 7$ und $144 = 2^4 \cdot 3^2$ als besonders hartnäckige Überlebenskünstler übrig. Mit einer Variante des Beweises von Satz 5.9 erhält man (bei angenommener Einfachheit) in diesen Fällen jeweils eine Untergruppe vom Index ≤ 4, im Widerspruch zum Satz von Poincaré. □

BEMERKUNG 6.4. (1) Die $\mathrm{GL}_3(\mathbb{F}_2)$ ist einfach von der Ordnung 168.

(2) Bis zur Ordnung 1000 sind die Ordnungen 360, 504 und 660 die einzigen weiteren, zu denen nicht-abelsche einfache Gruppen existieren.

Ohne Beweis:

SATZ 6.5 ($p^\alpha q^\beta$-Satz von Burnside). *Es gibt keine einfache Gruppe der Ordnung $p^\alpha q^\beta$ (p, q prim, α, $\beta \geq 1$).*

Die endlichen einfachen Gruppen bilden die Bausteine der endlichen Gruppen in folgendem Sinn:

SATZ 6.6. *Jede endliche Gruppe G besitzt eine Kompositionsreihe. Das heisst, es gibt eine Kette*

$$\{e\} = U_0 \subseteq U_1 \subseteq U_2 \subseteq \ldots \subseteq U_r = G$$

von Untergruppen, wobei für jedes $i = 1, \ldots, r$ gilt:

(1) *die Untergruppe U_{i-1} ist ein Normalteiler von U_i; und*
(2) *die Faktorgruppe U_i/U_{i-1} ist einfach.*

Die Einfachheit von U_i/U_{i-1} kann man nämlich so ausdrücken, dass U_{i-1} ein *maximaler* Normalteiler in U_i ist. Ist G nun eine endliche Gruppe, so sind sicherlich $\{e\}$ und G Normalteiler in G. Ist dabei $G/\{e\} \simeq G$ nicht einfach, so gibt es einen Normalteiler N zwischen $\{e\}$ und G, und wegen der Endlichkeit von G kann man dann auch einen solchen finden, so dass zwischen N und G kein weiterer Normalteiler von G liegt. Es ist dann der Faktor G/N einfach. Nun setzt man das Verfahren für N fort (Induktion).

7. Auflösbare Gruppen

DEFINITION 7.1. Eine Gruppe G heißt auflösbar, falls es eine Kette von Untergruppen $\{e\} = U_0 \subseteq U_1 \subseteq U_2 \subseteq \ldots \subseteq U_{n-1} \subseteq U_n = G$ gibt, so dass für jedes $i = 1, \ldots, n$ gilt:

(1) U_{i-1} ist ein Normalteiler in U_i; und
(2) die Faktorgruppe U_i/U_{i-1} ist abelsch.

LEMMA 7.2. (1) *Eine Untergruppe H einer auflösbaren Gruppe G ist auflösbar.*
(2) *Seien $\pi\colon G \to H$ ein surjektiver Gruppenhomomorphismus. Ist G auflösbar, so ist auch H auflösbar. (Faktorgruppen auflösbarer Gruppen modulo einem Normalteiler sind auflösbar.)*
(3) *Sei N ein Normalteiler in der Gruppe G. Sind N und G/N auflösbar, so ist dies auch G.*

BEWEIS. (1) Sei $\{e\} = U_0 \subseteq U_1 \subseteq U_2 \subseteq \ldots \subseteq U_{n-1} \subseteq U_n = G$ eine Kette von Untergruppen mit U_{i-1} ist ein Normalteiler in U_i, und die Faktorgruppe U_i/U_{i-1} ist abelsch ($i = 1, \ldots, n$). Sei $V_i \stackrel{def}{=} U_i \cap H$. Dann ist offenbar V_{i-1} Normalteiler in V_i, und es ist

$$\frac{V_i}{V_{i-1}} = \frac{U_i \cap H}{U_{i-1} \cap H} = \frac{U_i \cap H}{U_{i-1} \cap (U_i \cap H)} \simeq \frac{U_{i-1}(U_i \cap H)}{U_{i-1}} \subseteq \frac{U_i}{U_{i-1}}$$

als Untergruppe einer abelschen Gruppe abelsch.

(2) Sei $\{e\} = U_0 \subseteq U_1 \subseteq U_2 \subseteq \ldots \subseteq U_{n-1} \subseteq U_n = G$ eine Kette von Untergruppen mit U_{i-1} ist ein Normalteiler in U_i, und die Faktorgruppe U_i/U_{i-1} ist abelsch ($i = 1, \ldots, n$). Es ist dann $\{e\} = \pi(U_0) \subseteq \pi(U_1) \subseteq \pi(U_2) \subseteq \ldots \subseteq \pi(U_{n-1}) \subseteq \pi(U_n) = H$ eine Kette von Untergruppen. Sei $i \in \{1, \ldots, n\}$. Sei $h \in \pi(U_i)$. Es gibt ein $g \in U_i$ mit $\pi(g) = h$. Es folgt $h\pi(U_{i-1})h^{-1} = \pi(gU_{i-1}g^{-1}) = \pi(U_{i-1})$, also ist $\pi(U_{i-1})$ ein Normalteiler von $\pi(U_i)$. Ferner ist offenbar $\pi(U_i)/\pi(U_{i-1}) = \pi(U_i/U_{i-1})$ abelsch.

(3) Seien $N/N = U_0/N \subseteq U_1/N \subseteq U_2/N \subseteq \ldots \subseteq U_{n-1}/N \subseteq U_n/N = G/N$ und $\{e\} = V_0 \subseteq V_1 \subseteq V_2 \subseteq \ldots \subseteq V_{m-1} \subseteq V_m = N$ Ketten von Untergruppen, jeweils Normalteiler in der nächst größeren, mit abelschen Faktoren. Setzt man diese Ketten zusammen, so erhält man

$$\{e\} = V_0 \subseteq V_1 \subseteq \ldots \subseteq V_{m-1} \subseteq V_m = N = U_0 \subseteq U_1 \subseteq \ldots \subseteq U_{n-1} \subseteq U_n = G,$$

wobei die Faktoren V_i/V_{i-1} und

$$\frac{U_i}{U_{i-1}} \simeq \frac{U_i/N}{U_{i-1}/N}$$

abelsch sind. □

FOLGERUNG 7.3. *Für $n \geq 5$ ist die symmetrische Gruppe S_n nicht auflösbar.*

BEWEIS. Mit S_n wäre auch die Untergruppe A_n auflösbar. Für $n \geq 5$ ist A_n aber einfach und nicht abelsch, also nicht auflösbar. □

Ohne Beweis:

SATZ 7.4 (Feit-Thompson 1963). *Jede Gruppe ungerader Ordnung ist auflösbar.*

Insbesondere hat jede nicht-abelsche einfache Gruppe gerade Ordnung.

LEMMA 7.5. *Sei G eine endliche, auflösbare Gruppe. Dann gibt es eine Kette von Untergruppen $\{e\} = U_0 \subseteq U_1 \subseteq U_2 \subseteq \ldots \subseteq U_{n-1} \subseteq U_n = G$ mit U_{i-1} ist ein Normalteiler in U_i, und die Faktorgruppe U_i/U_{i-1} ist zyklisch von Primzahlordnung ($i = 1, \ldots, n$).*

BEWEIS. (In den Übungen.) □

BEISPIEL 7.6. (1) Jede abelsche Gruppe ist auflösbar.
(2) Jede endliche p-Gruppe ist auflösbar.

BEWEIS. (In den Übungen.) □

KAPITEL IV

Einführung in die Ringtheorie

Lernziele:

- Euklidische Ringe als Verallgemeinerung von Ringen mit Division mit Rest auffassen.
- Teilbarkeit in Integritätsbereichen. Irreduzible und Primelemente. Faktorisierungen. ggT.
- Überblick zwischen verschiedenen Ringkonzepten (euklidisch, Hauptidealring, faktoriell) haben und deren Beziehungen zueinander kennen. Wichtigste Beispiele kennen.
- Polynomringe. Division mit Rest. Einsetzen. Abspalten von Nullstellen als Linearfaktoren.
- Das Konzept des Quotientenkörpers eines Integritätsbereichs.
- Den Satz von Gauss und das Kriterium von Eisenstein kennen; letzteres auch an Beispielen anwenden können.

1. Euklidische Ringe

In diesem Abschnitt werden wir nur *kommutative* Ringe R betrachten, d. h. es gilt $x \cdot y = y \cdot x$ für alle x, $y \in R$.

Erinnerung: Ein kommutativer Ring R mit $1 \neq 0$ heisst Integritätsbereich, wenn aus $rs = 0$ stets $r = 0$ oder $s = 0$ folgt (r, $s \in R$).

DEFINITION 1.1. Ein Integritätsbereich R zusammen mit einer Größenfunktion $\sigma\colon R\setminus\{0\} \to \mathbb{N}_0$ heißt euklidischer Ring, wenn folgendes gilt: Zu allen Elementen a, $b \in R$ mit $b \neq 0$ gibt es q, $r \in R$ mit $a = qb + r$, mit $r = 0$ oder $\sigma(r) < \sigma(b)$.

BEISPIEL 1.2. $\mathbb{Z}$ ist ein euklidischer Ring mit Größenfunktion $\sigma = |-|$.

Erinnerung: Sei R ein kommutativer Ring. Eine Teilmenge $I \subseteq R$ heißt Ideal, falls $(I, +)$ Untergruppe von $(R, +)$ ist, und falls $R \cdot I \subseteq I$ (und $I \cdot R \subseteq I$) gilt. Ein Ideal I heißt Hauptideal, falls es ein $a \in R$ gibt mit $I = Ra$. Ein Integritätsbereich heißt Hauptidealring, falls dessen Ideale sämtlich Hauptideale sind.

SATZ 1.3. *Jeder euklidische Ring R ist ein Hauptidealring.*

BEWEIS. Sei $I \subseteq R$ ein Ideal. Ist $I = \{0\}$, so wird I von 0 erzeugt. Sei $I \neq \{0\}$. Wähle $a \in I$ mit $\sigma(a)$ minimal. Es gilt $Ra \subseteq I$. Sei umgekehrt $b \in I$. Dann gibt es q, $r \in R$ mit $b = qa + r$, wobei $r = 0$ oder $\sigma(r) < \sigma(a)$ gilt. Weil auch $r = b - qa \in I$ gilt, muss $r = 0$, gelten, also $b = qa \in Ra$. □

2. Teilbarkeit und Faktorisierung

DEFINITION 2.1. Sei R ein Integritätsbereich. (0) Seien a, $b \in R$. Wir sagen, dass a ein Teiler von b ist (oder a teilt b; a ist ein Faktor von b; b ist ein Vielfaches von a; Schreibweise: $a \mid b$), falls $b \in Ra$ gilt, falls es also ein $r \in R$ gibt mit $b = ra$.

(1) Ein $r \in R$ heißt Einheit (invertierbar), falls es ein $s \in R$ gibt mit $rs = 1$ ($= sr$). Die Einheiten in R bilden eine (abelsche) Gruppe $E(R)$.

(2) Ein $u \in R$ heißt irreduzibel, falls $u \neq 0$ keine Einheit ist, und falls aus $u = ab$ folgt, dass a oder b eine Einheit ist.

(3) Ein $p \in R$ heißt prim (Primelement), falls $p \neq 0$ keine Einheit ist, und falls aus $ab \in Rp$ folgt, dass $a \in Rp$ oder $b \in Rp$ gilt. (Also: $p \mid ab \Rightarrow p \mid a$ oder $p \mid b$.)

(4) Gilt $Ra = Rb$, so heißen a und b assoziiert ($a \sim b$). Äquivalent dazu: Es gibt eine Einheit u mit $a = ub$.

LEMMA 2.2. *Jedes Primelement p in einem Integritätsbereich ist irreduzibel.*

BEWEIS. Es gelte $p = ab$. Dann $ab \in Rp$. Es folgt etwa, dass $a \in Rp$ gilt, $a = rp$. Dann $p = rpb$, also $p(1 - rb) = 0$, und es folgt $1 - rb = 0$ bzw. $1 = rb$. Also ist b eine Einheit. □

DEFINITION 2.3. Ein Integritätsbereich R heißt faktoriell, falls jede Nichteinheit $r \neq 0$ ein Produkt von Primelementen ist, $r = p_1 p_2 \dots p_r$ (p_i prim, $r \geq 1$).

LEMMA 2.4. *Sei R ein Integritätsbereich. Es gelte*

$$p_1 p_2 \dots p_r = q_1 q_2 \dots q_s$$

mit Primelementen $p_1, \dots, p_r$ und $q_1, \dots, q_s$. Dann gilt $r = s$, und nach evtl. Umnummerierung $p_i \sim q_i$.

BEWEIS. p_1 teilt das Produkt $q_1 q_2 \dots q_s$, und da p_1 prim ist, einen dieser Faktoren (diese Eigenschaften von Primelementen gilt auch für mehr als zwei Faktoren per Induktion); nach Umnummerierung können wir $p_1 \mid q_1$ annehmen, etwa $ap_1 = q_1$. Da q_1 als Primelement irreduzibel ist und p_1 keine Einheit ist, muss a eine Einheit sein, d. h. $p_1 \sim q_1$. Kürzen (Nullteilerfreiheit!) von p_1 liefert $p_2 \dots p_r = (aq_2)q_3 \dots q_s$, und mit q_2 ist auch aq_2 prim. Die Aussage folgt nun per Induktion. □

SATZ 2.5. *Für einen Integritätsbereich R sind folgende Aussagen äquivalent:*

(1) *R ist faktoriell.*
(2) *Jede Nichteinheit $\neq 0$ ist ein Produkt von irreduziblen Elementen, die bis auf Umnummerierung und Assoziiertheit eindeutig bestimmt sind.*
(3) *Jede Nichteinheit $\neq 0$ ist ein Produkt von irreduziblen Elementen, und jedes irreduzible Element in R ist prim.*

BEWEIS. (1)⇒(3) Nach 2.2 ist jede Nichteinheit $\neq 0$ ein Produkt von irreduziblen Elementen. Sei q irreduzibel. Dann ist $q = p_1 \dots p_r$ mit p_i prim. Da q irreduzibel folgt $q \sim p_i$ für ein i, und damit ist q prim.

(3)⇒(1) klar.

(2)⇒(3) Sei q irreduzibel. Gelte $ab \in Rq$, etwa $ab = cq$. Zerlegt man a, b und c in irreduzible Elemente und nutzt die Eindeutigkeit aus, so erhält man, dass $a \in Rq$ oder $b \in Rq$ gilt. Also ist q prim.

(3)⇒(2) Da jedes irreduzible Element prim ist, und Zerlegungen in Primelemente eindeutig sind (bis auf Assoziiertheit) nach 2.4, folgt auch die Eindeutigkeit der Zerlegung in irreduzible Elemente. □

SATZ 2.6. *Jeder Hauptidealring ist faktoriell.*

BEWEIS. (1) Jedes irreduzible Element ist prim (sog. Euklid's Lemma.): Sei p irreduzibel. Gelte $ab \in Rp$ und $a \notin Rp$. Dann gilt $Rp \subsetneq Rp + Ra = Rc$ für ein $c \in R$, da R Hauptidealring. Dann $p \in Rc$, also $p = dc$. Fall d Einheit, nicht möglich wegen $Ra \neq Rc$. Also c Einheit, $Rc = R$. Also $1 = rp + sa$. Dann $b = rbp + sab \in Rp$.

(2) Jede Nichteinheit $\neq 0$ ist ein Produkt von irreduziblen Elementen: Sei $r \neq 0$ Nicheinheit. Angenommen, r ist nicht Produkt von irreduziblen Elementen. Dann ist r selbst nicht irreduzibel. Also gibt es Nichteinheiten a, b ($\neq 0$) mit $r = ab$. Dann ist a oder b

nicht irreduzibel. Setzt man dies fort, so erhält man (!) eine unendliche, echt aufsteigende Kette

$$Ra_1 \subsetneq Ra_2 \subsetneq Ra_3 \subsetneq \cdots \subsetneq Ra_n \subsetneq Ra_{n+1} \subsetneq \dots$$

Dann ist

$$I = \bigcup_{n\geq 1} Ra_n$$

ein Ideal, also ein Hauptideal, $I = Rc$. Es gibt ein n mit $c \in Ra_n$. Es folgt $Ra_n = Ra_{n+1}$, Widerspruch. □

Wir haben also die Beziehungen

$$\text{euklidisch} \quad \Rightarrow \quad \text{Hauptidealring} \quad \Rightarrow \quad \text{faktoriell.}$$

Die Umkehrungen gelten i. a. nicht.

FOLGERUNG 2.7. *$\mathbb{Z}$ ist faktoriell.*

3. Polynomringe

Definition von Polynomen über einem kommutativen Ring K als Funktionen (Folgen) $f = (f_n)_{n\geq 0} \colon \mathbb{N}_0 \to K$ mit endlichem Träger, d. h. $f_n = 0$ für "fast alle" (d. h. bis auf endliche viele) $n \geq 0$. Schreibe $0 = (0, 0, 0, \dots)$, $1 = (1, 0, 0, \dots)$.

SATZ 3.1. *Die Menge aller Polynome über K wird zu einem kommutativen Ring mit 1 durch folgende Addition und Multiplikation*

$$(f_n) + (g_n) = (f_n + g_n)$$

und

$$(f_n) \cdot (g_n) = (\sum_{i=0}^{n} f_i g_{n-i})_n.$$

BEWEIS. Nachrechnen. □

BEMERKUNG 3.2. Sei R der Ring der Polynome über K. Dann ist $a \mapsto (a, 0, 0, \dots)$ ein injektiver Ringhomomorphismus $K \to R$. Identifiziere K als Teilring (-körper) von R vermöge dieses Homomorphismus.

Schreibe $T := (0, 1, 0, 0, \dots) \in R$. Dann gilt $T^0 = 1 \in R$, $T^2 = (0, 0, 1, 0, 0, \dots)$, $T^3 = (0, 0, 0, 1, 0, \dots)$, usw.

SATZ 3.3. *Jedes vom Nullpolynom verschiedene Polynom f über K hat eine Darstellung $f = a_0 + a_1T + a_2T^2 + \cdots + a_nT^n$ mit $n \geq 0$ und eindeutigen Koeffizienten $a_0, a_1, \dots, a_n \in K$, wobei $a_n \neq 0$.*

BEWEIS. Klar. □

Bezeichnung: $R = K[T]$ heisst der Polynomring über K in der Unbestimmten T. $n = \operatorname{grad} f$.

SATZ 3.4. *Sei K ein Integritätsbereich. Seien $f, g \in K[T]$ vom Nullpolynom verschieden. Dann gilt*

(1) $\operatorname{grad}(f \cdot g) = \operatorname{grad}(f) + \operatorname{grad}(g)$. *(Insbesondere $fg \neq 0$.)*
(2) *$K[T]$ ist ein Integritätsbereich.*

BEWEIS. (1) Sei $f = a_mT^m + \cdots + a_1T + a_0$ und $= b_nT^n + \cdots + b_1T + b_0$ mit $a_m, b_n \neq 0$, also $\operatorname{grad}(f) = m$ und $\operatorname{grad}(g) = n$. Dann gilt $fg = a_mb_nT^{m+n} + \dots$, wobei alle weiteren Summanden kleineren Grad als $m + n$ haben. Da K nullteilerfrei ist, gilt $a_mb_n \neq 0$, also ist $\operatorname{grad}(fg) = m + n = \operatorname{grad}(f) + \operatorname{grad}(g)$.
(2) folgt aus (1). □

SATZ 3.5 (Polynomdivision mit Rest). *Sei K ein Körper. Seien f, $g \in K[T]$ mit $g \neq 0$. Dann gibt es eindeutig bestimmte q, $r \in K[T]$ mit*

$$f = qg + r,$$

wobei $r = 0$ oder $r \neq 0$ und $\operatorname{grad}(r) < \operatorname{grad}(g)$.

BEWEIS. (Siehe Vorlesung.) □

FOLGERUNG 3.6. *Für einen Körper K ist $K[T]$ ist ein euklidischer Ring mit Größenfunktion $\sigma = \operatorname{grad}$. Insbesondere ist $K[T]$ ein Hauptidealring und faktoriell.*

BEMERKUNG 3.7. Der obige Beweis der Polynomdivision mit Rest funktioniert auch in beliebigen kommutativen Ringen mit 1, wenn man nur voraussetzt, dass der Leitkoeffizient von g eine Einheit ist.

SATZ 3.8 (Universelle Eigenschaft des Polynomrings). *Der Polynomring $K[T]$ hat folgende universelle Eigenschaft: Sei S ein Ring und $s \in S$. Sei $\varphi\colon K \to S$ ein Ringhomomorphismus. Dabei sei S ein kommutativer Ring, oder es gelte allgemeiner, dass $\varphi(a)s = s\varphi(a)$ gilt für alle $a \in K$. Dann gibt es genau einen Ringhomomorphismus $\overline{\varphi}\colon K[T] \to S$ mit $\overline{\varphi}_{|K} = \varphi$ und $\overline{\varphi}(T) = s$.*

BEWEIS. Definiere $\overline{\varphi}(\sum_{i=1}^{n} a_i T^i) = \sum_{i=1}^{n} \varphi(a_i) s^i$. □

3.9 (Einsetzen). Häufig ist $\varphi\colon K \longrightarrow S$ eine natürliche Einbettung $\iota\colon a \mapsto a$. Man schreibt dann: $\bar{\iota}(f) = f(s)$. In die Unbestimmte T wird das Element $s \in S$ *eingesetzt*. Ist s fest, so ist $f \mapsto f(s)$, $K[T] \longrightarrow S$ ein Ringhomomorphismus, der sogenannte Einsetzungshomomorphismus. Ein $s \in S$ heißt Nullstelle von f (in S), falls $f(s) = 0$ gilt.

Bemerkung: Man denke etwa an den Satz von Cayley-Hamilton aus der Linearen Algebra: $A \in \mathrm{M}_n(K)$, $\chi_A \in K[T]$ das charakteristische Polynom, dann $\chi_A(A) = 0$. Die Matrix A ist also eine Nullstelle des Polynoms χ_A im Ring $S = \mathrm{M}_n(K)$.

SATZ 3.10. *Sei K ein Körper. Sei $f \in K[T]$ ($f \neq 0$) ein Polynom vom Grad n. Sei $c \in K$ eine Nullstelle von f in K. Dann gilt*

$$f = q \cdot (T - c),$$

mit $q \in K[T]$ vom Grad $n - 1$. Insbesondere hat f in K höchstens n Nullstellen.
(Gilt auch über Integritätsbereichen, vgl. 3.7.)

FOLGERUNG 3.11. *Sei K ein unendlicher Körper. Dann ist $K[T]$ isomorph zum Ring $\operatorname{Pol}(K, K)$ aller Polynomfunktionen $f\colon K \to K$, $c \mapsto a_0 + a_1 c + a_2 c^2 + \cdots + a_n c^n$ mit Koeffizienten in K.*

BEWEIS. Jedes $f \in K[T]$ liefert eine eindeutige Polynomfunktion $c \mapsto f(c)$. Diese Zuordnung ist offenbar surjektiv und ein Homorphismus von Ringen. Weil K unendlich ist, ist diese Zuordnung auch injektiv nach dem vorherigen Satz. □

BEISPIEL 3.12. Sei $K = \mathbb{F}_2$ der Körper mit zwei Elementen 0 und 1. Da Polynom $f = T^2 + T \in K[T]$ ist verschieden vom Nullpolynom, aber die zugehörige Polynomfunktion $K \to K$, $a \mapsto f(a)$ ist die Nullfunktion, denn es gilt $f(0) = 0$ und $f(1) = 1 + 1 = 0$, also $f(a) = 0$ für alle $a \in K$.

4. Quotientenkörper

Bemerkung: Ist R Teilring eines Körpers K, so ist R ein Integritätsbereich. Es gilt auch die Umkehrung:

SATZ 4.1. *Sei R ein Integritätsbereich. Dann gibt es einen Körper K, so dass R mit einem Teilring von K identifiziert werden kann.*

BEWEIS. Sei X die Menge aller Paare (a, b) mit a, $b \in R$, $b \neq 0$. Wir erklären eine Äquivalenzrelation $\sim$ auf X durch

$$(a, b) \sim (c, d) \quad \Leftrightarrow \quad ad = bc.$$

[Nachrechnen, dass dies eine Äquivalenzrelation ist.]

Sei $K = X/\sim$ die Menge der Äquivalenzklassen. Wir schreiben $\left[\frac{a}{b}\right]$ für die Klasse von (a, b).

Auf K wird nun eine Addition und eine Multiplikation wie folgt erklärt:

$$\left[\frac{a}{b}\right] + \left[\frac{c}{d}\right] \overset{def}{=} \left[\frac{ad + bc}{bd}\right]$$

und

$$\left[\frac{a}{b}\right] \cdot \left[\frac{c}{d}\right] \overset{def}{=} \left[\frac{ac}{bd}\right].$$

Man prüft nach, dass dies *wohldefiniert* ist, d. h. nicht von der Auswahl der Repräsentanten der Klasse abhängt. Wir zeigen dies nur für die (schwierigere) Addition: Gilt $(a, b) \sim (a', b')$ und $(c, d) \sim (c', d')$, so folgt $(ad + bc, bd) \sim (a'd' + b'c', b'd')$ [kurz demonstrieren], und dies zeigt die Wohldefiniertheit.

Man sieht das diese "Bruchrechenregeln" K zu einem kommutativen Ring machen mit Nullelement $\left[\frac{0}{1}\right]$ und Einselement $\left[\frac{1}{1}\right]$. Es ist $\left[\frac{a}{b}\right] = 0$ genau dann, wenn $a = 0$ ist. Daher ist jedes $\left[\frac{a}{b}\right] \neq 0$ invertierbar mit Inversem $\left[\frac{b}{a}\right]$.

Es ist offenbar $\iota\colon R \to K$, $a \mapsto \left[\frac{a}{1}\right]$ ein injektiver Ringhomomorphismus. □

BEMERKUNG 4.2. Identifizieren wir R via ι mit einem Teilring des oben konstruierten Körpers K, so folgt, dass jedes Element von K von der Form ist $ab^{-1} = a/b$ mit a, $b \in R$, $b \neq 0$. In K gibt es dann keinen kleineren Körper, der R enthält. Man nennt K auch den Quotientenkörper oder den Körper der Brüche von R. Der bestimmte Artikel ist gerechtfertigt, denn ist L irgendein Körper, der aus den Elementen ("Brüchen") ab^{-1} mit a, $b \in R$, $b \neq 0$ besteht, so konstruiert man einen offensichtlichen Isomorphismus von K nach L, der alle Elemente aus R festläßt.

BEISPIELE 4.3. (1) $\mathbb{Q}$ ist Quotientenkörper von $\mathbb{Z}$.

(2) $K(T)$ sei der Körper der Brüche des Polynomrings $K[T]$. Er besteht aus allen (formalen) Brüchen von Polynomen $f(T)/g(T)$, wobei $g \neq 0$ ist. Dieser Körper heißt auch der rationale Funktionenkörper in einer Unbestimmten über K.

5. Faktorisierung von Polynomen: Der Satz von Gauss

DEFINITION 5.1 (ggT). Sei R Integritätsbereich. Seien a und $b \in R$. Ein $d \in R$ heißt ein größter gemeinsamer Teiler (ggT) von a und b, falls

(1) $a \in Rd$ und $b \in Rd$, und

(2) Ist $d' \in R$ mit $a \in Rd'$ und $b \in Rd'$, so folgt $d \in Rd'$.

Die Definition wird in naheliegender Weise auf mehr als zwei Elemente erweitert.

Offenbar gilt: Sind d_1 und d_2 ggT's von a und b (falls existent), so gilt $d_1 \sim d_2$ (und umgekehrt). Ist $a \neq 0$ und $b = 0$, so ist a ein ggT von a und b. Ist 1 ein ggT von a und b, so heißen a und b auch teilerfremd.

In faktoriellen Ringen hat man die Existenz des ggT (von Elementen $\neq 0$):

LEMMA 5.2. *Sei R faktoriell. Seien $a = up_1^{m_1} \dots p_r^{m_r}$ und $b = vp_1^{n_1} \dots p_r^{n_r}$, mit $p_1, \dots, p_r$ paarweise nicht-assoziierte Primelemente und u, $v \in E(R)$, m_i, $n_j \geq 0$. (Alle Elemente $\neq 0$ lassen sich auf diese Weise schreiben.) Dann ist ein ggT von a und b gegeben durch $p_1^{k_1} \dots p_r^{k_r}$, wobei $k_i = \min(m_i, n_i)$.*

BEWEIS. Klar. □

LEMMA 5.3. *Sei R faktoriell, und seien a, $b \in R$ nicht beide 0. Dann sind a und b teilerfremd genau dann, wenn es kein Primelement $p \in R$ gibt mit $a \in Rp$ und $b \in Rp$.*

BEWEIS. Klar. □

DEFINITION 5.4. Sei R faktoriell. Der Inhalt $I(f)$ eines Polynoms $f = \sum_{i=0}^{n} a_i T^i \in R[T]$, $f \neq 0$ ist der ggT seiner Koeffizienten. (Dies ist nicht paarweise gemeint!) (Ist nur bis auf eine Einheit eindeutig definiert!) Ein Polynom f mit $\operatorname{grad}(f) \geq 1$ heißt primitiv, falls $I(f) = 1$ gilt.

Bemerkung: Ein Polynom $f \in R[T]$ mit $f \neq 0$ heisst normiert, falls der Leitkoeffizient $= 1$ ist. Ein normiertes Polynom vom Grad ≥ 1 ist immer primitiv.

SATZ 5.5. *Sei R faktoriell. Seien f, $g \in R[T]$ ungleich null. Dann gilt (bis auf Einheiten) $I(fg) = I(f)I(g)$.*

BEWEIS. Zunächst kann man ohne Einschränkung annehmen, dass sowohl f wie auch g einen Grad ≥ 1 hat. Schreibt man $f = I(f)f'$ und $g = I(g)g'$, so sind f' und g' primitiv, es gilt $I(fg) = I(f)I(g)I(f'g')$, und es genügt daher zu zeigen:

Sind f und g primitiv, so ist auch fg primitiv.

Seien $f = \sum_{i=0}^{m} a_i T^i$ und $g = \sum_{i=0}^{n} b_i T^i$ mit $a_m \neq 0$ und $b_n \neq 0$. Dann ist

$$fg = \sum_{i=0}^{m+n} (\sum_{j=0}^{i} a_j b_{i-j}) T^i.$$

Schreibe $c_i = \sum_{j=0}^{i} a_j b_{i-j}$ Sei p ein beliebiges Primelement. Sei r die größte ganze Zahl mit $0 \leq r \leq m$, $a_r \neq 0$ und p teilt nicht a_r. Ebenso sei s die größte ganze Zahl mit $0 \leq s \leq n$, $b_s \neq 0$ und p teilt nicht b_s. Es ist

$$c_{r+s} = a_r b_s + a_{r+1} b_{s-1} + \cdots + a_{r-1} b_{s+1} + \ldots$$

Da p das Produkt $a_r b_s$ nicht teilt, aber alle anderen Summanden auf der rechten Seite, teilt p nicht c_{r+s}. Es gibt also kein Primelement, welches alle Koeffizienten c_i gleichzeitig teilt, daher sind sie teilerfremd. □

Ist K ein Körper und $f \in K[T]$, so bedeutet f irreduzibel genau folgendes: (1) $\operatorname{grad}(f) \geq 1$, und (2) ist $f = gh$, so ist $\operatorname{grad}(g) = 0$ oder $\operatorname{grad}(h) = 0$. Ist R (nur) ein faktorieller Ring, so kann es auch irreduzible $f \in R[T]$ vom Grad 0 geben, nämliche gerade die irreduziblen Elemente in R.

LEMMA 5.6. *Sei R faktoriell und sei K der Quotientenkörper von R. Ist $f \in R[T]$ vom Grad ≥ 1 und irreduzibel, so ist f auch irreduzibel in $K[T]$.*

BEWEIS. Sei f vom Grad ≥ 1 und irreduzibel über R, aber reduzibel über K. Man kann also schreiben $f = gh$ mit g, $h \in K[T]$, und mit $\operatorname{grad}(g)$, $\operatorname{grad}(h) \geq 1$. Multipliziert man mit dem Hauptnenner a der Koeffizienten von g und mit dem Hauptnenner b der Koeffizienten von h, so erhält man $abf = (ag)(bh)$ mit a, $b \in R$, $a \neq 0$, $b \neq 0$ und ag, $bh \in R[T]$. Schreibt man $ag = I(ag)g'$ und $bh = I(bh)h'$, so sind g' und h' primitiv, und $abf = I(ag)I(bh)g'h'$. Da f irreduzibel in $R[T]$ (und vom Grad ≥ 1), ist f primitiv. Vergleich der Inhalte beider Seiten liefert (bis auf Einheit) $ab = I(ag)I(bh)$. Kürzen liefert $f = g'h'$ mit g', $h' \in R[T]$ primitiv. Dies ergibt eine nicht-triviale Zerlegung von f in $R[T]$, Widerspruch. □

SATZ 5.7 (Gauss). *Ist R ein faktorieller Ring, so ist dies auch $R[T]$.*

BEWEIS. Sei K der Quotientenkörper von R. Sei $f \in R[T]$, $f \neq 0$. Wir wissen, dass $K[T]$ als euklidischer Ring faktoriell ist. Es hat also f in $K[T]$ eine Zerlegung $f = q_1 q_2 \ldots q_r$ mit Primelementen $q_i \in K[T]$. Zieht man Nenner und gemeinsame Teiler der Zähler heraus, so erhält man $f = cp_1 p_2 \ldots p_r$ mit $c \in K$, $c \neq 0$, und primitiven, irreduziblen

Polynomen $p_i \in R[T]$ (da irreduzibel in $K[T]$). Man kann schreiben $c = a/b$ mit teilerfremden a und b, und erhält $bf = ap_1p_2 \dots p_r$. Der Inhalt der rechten Seite ist a, der der linken Seite wird von b geteilt. Also muss b eine Einheit in R sein, damit zerlegt sich f schon über R in irreduzible Polynome. Ist $f = p'_1p'_2 \dots p'_s$ ein zweite solche Darstellung, so sind die p'_j primitiv oder vom Grad 0. Die primitiven p'_j sind nach Lemma 5.6 auch irreduzibel über K, dort stimmen sie bis auf Einheiten in K (und Umnummerierung) mit den p_i überein, und obiges Argument zeigt nochmal, dass die p_i schon über R zu den p'_j assoziiert sind. □

6. Ein Irreduzibilitätskriterium

Satz 6.1 (Kriterium von Eisenstein). *Sei R ein faktorieller Ring mit Quotientenkörper K. Sei $f \in R[T]$, $f = a_0 + a_1T + \dots + a_nT^n$ vom Grad $n \geq 1$. Es gebe ein Primelement $p \in R$ mit*

(1) $p \nmid a_n$. *(Etwa: f normiert.)*
(2) $p \mid a_i$ $(i = 0, \dots, n-1)$.
(3) $p^2 \nmid a_0$.

Dann ist f irreduzibel in $K[T]$.

Beweis. Schreibe $f = I(f)f'$ mit f' primitiv. Zu zeigen genügt, dass f' in $R[T]$ irreduzibel ist. Da $I(f)$ nicht von p geteilt wird, gelten bzgl. Teilbarkeit durch p für f' dieselben Bedingungen wie für f. Man kann also ohne Einschränkung annehmen, dass f selbst primitiv ist, und zu zeigen genügt (vgl. Lemma 5.6), dass f irreduzibel in $R[T]$ ist. Angenommen, $f = gh$ in $R[T]$ mit $g = \sum_{i=0}^{r} b_iT^i$ und $h = \sum_{i=0}^{s} c_iT^i$ mit $b_r \neq 0$ und $c_s \neq 0$. Dann ist

$$f = \sum_{i=0}^{r+s} (\sum_{j=0}^{i} b_jc_{i-j})T^i.$$

Da $a_0 = b_0c_0$ durch p aber nicht durch p^2 teilbar ist, gilt etwa $p \mid b_0$ und $p \nmid c_0$. Da $a_n = b_rc_s$ nicht durch p teilbar ist, ist b_r nicht durch p teilbar. Sei k der kleinste Index mit $p \nmid b_k$. Da in

$$a_k = b_0c_k + b_1c_{k-1} + \dots + b_{k-1}c_1 + b_kc_0$$

auf der rechten Seite nur der Summand b_kc_0 nicht durch p geteilt wird, folgt, dass a_k nicht durch p geteilt wird, Widerspruch zur Annahme $p \mid a_k$ $(k < n)$. □

Beispiel 6.2. Sei $f = 2T^5 + 15T^4 + 9T^3 + 6 \in \mathbb{Z}[T]$. Nach dem Kriterium von Eisenstein (mit $p = 3$) ist f irreduzibel in $\mathbb{Q}[T]$.

KAPITEL V

Algebraische Körpererweiterungen

Lernziele:

- Körpererweiterungen; Ring- und Körperadjunktionen.
- Das Konzept einer algebraischen Körpererweiterung und Charakterisierungen. Minimalpolynome (auf exakte Sprechweise achten!) und Charakterisierungen.
- Gradsatz. (Ubiquitär!)
- Satz von Kronecker.
- Konstruktion von K-Isomorphismen mit Hilfe von Nullstellen von Minimalpolynomen.
- Minimalpolynome von algebraischen Elementen berechnen können.
- Konstruktionen mit Zirkel und Lineal. Definition. Kennzeichnung der konstruierbaren komplexen Zahlen und Anwendung auf die (Nicht-) Lösbarkeit einiger antiker Probleme.
- Die Kenntnis der Existenz und der Eindeutigkeit des algebraischen Abschlusses eines Körpers. (Ohne Beweise.)

1. Algebraische und transzendente Elemente

L/K eine Körpererweiterung, $x \in L$. (Man beachte, dass bei dieser Schreibweise L/K keine Faktorbildung meint!) Sei $K[x]$ die Teilmenge von L bestehend aus den Elementen der Form

$$a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n$$

mit $n \geq 0$ und $a_i \in K$.

PROPOSITION 1.1. *$K[x]$ ist der bzgl. Inklusion $\subseteq$ der kleinste Unterring von L, der K und x enthält.*

BEWEIS. Offensichtlich. □

DEFINITION 1.2. $K[x]$ entsteht aus K durch Ringadjunktion des Elementes $x \in L$. "K adjungiert x."

Statt ab^{-1} schreiben wir häufig auch a/b, oder $\frac{a}{b}$.
Analog: $K(x)$ die Menge aller in L gebildeten Quotienten

$$q = \frac{a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n}{b_0 + b_1 x + b_2 x^2 + \cdots + b_m x^m}$$

mit $a_i, b_j \in K$ und $b_0 + b_1 x + b_2 x^2 + \cdots + b_m x^m \neq 0$. Also besteht $K(x)$ aus den Elementen der Form a/b mit $a, b \in K[x]$, $b \neq 0$.

PROPOSITION 1.3. *$K(x)$ ist der bzgl. Inklusion kleinste Teilkörper von L, welcher K und x enthält.*

BEWEIS. Offensichtlich. □

DEFINITION 1.4. $K(x)$ heißt der aus K durch Adjunktion des Elementes $x \in L$ gebildete Teilkörper von L.

BEISPIEL 1.5. (a) Die Zahlen $a + b\sqrt{2}$ mit a, $b \in \mathbb{Q}$ bilden einen Teilkörper K des Körpers $\mathbb{R}$. Es gilt $K = \mathbb{Q}[\sqrt{2}] = \mathbb{Q}(\sqrt{2})$.

(b) Im Körper $\mathbb{C}$ ist

$$\mathbb{Q}(i) = \mathbb{Q}[i] = \{a + bi \mid a, b \in \mathbb{Q}\}.$$

(c)* Es lässt sich zeigen (tiefsinnig!), dass $\mathbb{Q}[\pi] \subsetneq \mathbb{Q}(\pi)$ gilt. (π ist "transzendent", Satz von Lindemann 1882.) Ähnliches gilt für die Eulersche Zahl e.

DEFINITION 1.6 (Algebraische Elemente). Sei L/K eine Körpererweiterung. Ein $x \in L$ heisst algebraisch über K, wenn x einer (normierten) polynomialen Gleichung

$$x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 = 0$$

mit $a_0, a_1, \ldots, a_{n-1} \in K$ genügt; es ist also x Nullstelle des normierten Polynoms

$$f = T^n + a_{n-1}T^{n-1} + \cdots + a_1 T + a_0 \in K[T],$$

$f(x) = 0$. Andernfalls heisst x transzendent über K.

Eine Körpererweiterung L/K heisst algebraisch, falls jedes $x \in L$ algebraisch über K ist. Anderfalls heisst L/K transzendente Körpererweiterung.

DEFINITION 1.7 (Minimalpolynom). Sei L/K eine Körpererweiterung, und sei $x \in L$ algebraisch über K. Es gibt dann, nach Definition, ein normiertes Polynom $f \in K[T]$, $f \neq 0$, mit $f(x) = 0$. Dann gibt es auch ein solches f minimalen Grades, und dies heisst das Minimalpolynom von x über K. (Dies ist offenbar eindeutig bestimmt.) Wir schreiben auch $f = \mathrm{MIPO}(x/K)$.

SATZ 1.8 (Charakterisierungen des Minimalpolynoms). *Sei L/K eine Körpererweiterung, sei $x \in L$ und $f \in K[T]$ ein normiertes Polynom. Dann sind äquivalent:*

1. *f ist das Minimalpolynom von x über K, d. h. $0 \neq f \in K[T]$ ist minimalen Grades mit $f(x) = 0$.*
2. *f ist irreduzibel über K und es gilt $f(x) = 0$.*
3. *$f(x) = 0$, und f teilt jedes Polynom $g \in K[T]$ mit $g(x) = 0$.*

BEWEIS. (1)⇒(2) Ist f nicht irreduzibel, so gibt es $g, h \in K[T]$ mit $\mathrm{grad}(g), \mathrm{grad}(h) \geq 1$ mit $f = gh$. Es gilt dann $g(x) = 0$ oder $h(x) = 0$, wobei g und h kleineren Grad als f haben.

(2)⇒(1) Sei f irreduzibel, und sei $g \in K[T]$ minimalen Grades mit $g(x) = 0$. Schreibe $f = qg + r$ mit $r = 0$, oder $\mathrm{grad}(r) < \mathrm{grad}(g)$. Wegen $r(x) = 0$ ist nur $r = 0$ möglich, also $f = qg$. Da f irreduzibel ist, folgt, dass q ein konstantes Polynom $\neq 0$ ist, und auch f hat minimalen Grad.

(1)⇒(3) Folgt wie im vorherigen Beweisteil per Division (durch f) mit Rest.

(3)⇒(1) Klar. □

Zusammen mit dem Homomorphiesatz erhalten wir:

FOLGERUNG 1.9. *Das Minimalpolynom f von x über K erzeugt (als Ideal) den Kern des Einsetzungshomomorphismus $K[T] \to L$, $g(T) \mapsto g(x)$. Insbesondere gilt $K[x] \simeq K[T]/fK[T]$, und $K[x]$ ist ein Körper.*

Die letzte Aussage folgt aus dem folgenden Lemma.

LEMMA 1.10. *Sei R ein Hauptidealring und $p \in R$ irreduzibel (= prim). Dann ist R/pR ein Körper.*

Hier interessiert uns die Aussage für den Spezialfall $R = K[T]$ (K ein Körper).

BEWEIS. Zeige, dass Elemente $\neq 0$ in R/pR invertierbar sind. Sei $x \in R$, so dass $[x] \in R/pR$ ungleich null ist. Das bedeutet gerade $x \notin pR$. Dann gilt $pR \subsetneq Rp + Rx = Ry$ für ein geeignetes y, da R ein Hauptidealring ist. Dann gibt es z mit $p = zy$. Da p

irreduzibel ist und obige Inklusion strikt ist, folgt, dass y eine Einheit ist, und damit $Rp + Rx = R$. Es gibt also r, s mit $rp + sx = 1$, und es folgt $[1] = [r][p] + [s][x] = [s][x]$, also ist $[x]$ invertierbar in R/pR. □

Sei L/K eine Körpererweiterung. Dann ist L insbesondere ein K-Vektorraum. Insbesondere steht das ganze Repertoire der Linearen Algebra (lineare Gleichungen, Matrizen, etc.) zur Untersuchung von L/K bereit. Insbesondere ist $\dim_K L$ definiert (endlich oder unendlich).

DEFINITION 1.11. Sei L/K eine Körpererweiterung. Die Dimension $\dim_K(L)$ heisst auch der (Körper-) Grad von L über K und wird mit $[L : K]$ bezeichnet. Eine Körpererweiterung L/K heisst endlich, falls $[L : K]$ endlich ist. Allgemeiner schreiben wir auch für einen kommutativen Ring R, der K als Teilring enthält, $[R : K] = \dim_K(R)$.

SATZ 1.12. *Sei L/K eine endliche Körpererweiterung. Dann ist L/K algebraisch.*

Genauer gilt: Ist $[L : K] = n$, so gibt es zu jedem $x \in L$ ein normiertes Polynom $f \in K[T]$ vom Grad n mit $f(x) = 0$.

BEWEIS. Sei $x \in L$. Wegen $[L : K] = n$ sind die $n + 1$ Elemente

$$1,\ x,\ x^2, \ldots,\ x^n$$

linear abhängig über K. Es gibt also $b_0, \ldots, b_n \in K$ nicht alle null mit

$$b_0 + b_1 x + \cdots + b_n x^n = 0.$$

Nach evtl. Multiplikation mit einer Potenz von x können wir $b_n \neq 0$ annehmen. Mit $a_i = b_i b_n^{-1}$ folgt dann die Behauptung. □

SATZ 1.13. *Sei L/K eine Körpererweiterung, und sei $x \in L$. Dann sind äquivalent:*

(1) *x ist algebraisch über K.*
(2) *$[K[x] : K]$ ist endlich.*
(3) *$K(x) = K[x]$.*
(4) *$K[x]$ ist ein Teilkörper von L.*

BEWEIS. (1)⇒(2), (3): Ist x algebraisch über K, so gibt es eine natürliche Zahl n und Elemente $a_0, \ldots, a_n \in K$ mit

$$x^n = a_0 + a_1 x + \cdots + a_{n-1} x^{n-1}. \tag{1.1}$$

Es folgt, dass $K[x]$ als K-Vektorraum von $1,\ x, \ldots,\ x^{n-1}$ erzeugt wird, also $[K[x] : K] \leq n$. Mit Folgerung 1.9 ergibt sich $K(x) = K[x]$.

(2)⇒(1): Wie im Beweis von Satz 1.12: Ist $n = [K[x] : K] < \infty$, so sind $1,\ x,\ x^2, \ldots,\ x^n$ linear abhängig, und es folgt, dass x algebraisch über K ist.

(3)⇒(1): Gilt $K(x) = K[x]$, so ist $K[x]$ ein Körper, und insbesondere ist x invertierbar in $K[x]$ (der Fall $x = 0$ ist uninteressant). Es gibt also eine natürliche Zahl und Elemente $b_0, \ldots, b_{n-1} \in K$ mit

$$x^{-1} = b_0 + b_1 x + \cdots + b_{n-1} x^{n-1}.$$

Multiplikation der Gleichung mit x zeigt dann, dass x einer Polynomgleichung über x genügt, x ist also algebraisch über K.

(3)⇔(4): Klar. □

FOLGERUNG 1.14. *Sei L/K eine Körpererweiterung und $x \in L$ algebraisch über K. Dann ist die Körpererweiterung $K(x)/K$ algebraisch.*

BEWEIS. Für alle $y \in K(x)$ gilt $[K(y) : K] \leq [K(x) : K] < \infty$. □

FOLGERUNG 1.15. *Sei L/K eine Körpererweiterung, sei $x \in L$ algebraisch über K mit $f = \mathrm{MIPO}(x/K)$. Dann gilt $[K(x) : K] = \mathrm{grad}(f)$. Ferner gilt mit $n = \mathrm{grad}(f)$, dass $1,\ x,\ x^2, \ldots,\ x^{n-1}$ eine K-Basis von $K(x)$ ist.*

BEWEIS. Es gilt $K(x) = K[x]$. Ist $f = T^n + a_{n-1}T^{n-1} + \cdots + a_1T + a_0$, so folgt wegen $f(x) = 0$, dass der K-Vektorraum $K[x]$ von den n Elementen

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

erzeugt wird; da f minimalen Grades ist, folgt sofort, dass diese Elemente auch linear unabhängig über K sind. Also $[K(x) : K] = n = \mathrm{grad}(f)$. □

Ist x algebraisch über K, so heisst der Körpergrad $[K(x) : K]$ auch der Grad des Elements x über K.

DEFINITION 1.16. Eine Körpererweiterung L/K heisst einfach, falls es ein $x \in L$ gibt mit $L = K(x)$. Ist in diesem Fall x algebraisch über K, so heisst sie einfach algebraisch, und x ein primitives (=erzeugendes) Element von L/K; andernfalls heisst L/K einfach transzendent.

BEISPIEL 1.17. $\mathbb{C}/\mathbb{R}$ ist wegen $\mathbb{C} = \mathbb{R}[i]$ einfach algebraisch. $\mathbb{Q}(\pi)/\mathbb{Q}$ ist einfach transzendent.*

Anmerkung: Gezeigt wird später (Satz vom primitiven Element): Jede endliche Körpererweiterung $L/\mathbb{Q}$ besitzt ein primitives Element.

SATZ 1.18. *Sei L/K eine Körpererweiterung und $\alpha \in L$ transzendent über K. Dann ist $K(\alpha) \simeq K(T)$; genauer: Es gibt einen Isomorphismus $K(T) \xrightarrow{\sim} K(\alpha)$, der T auf α schickt und auf K wie die Identität wirkt.*

BEWEIS. Definiere $K(T) \to K(\alpha)$, $f(T)/g(T) \mapsto f(\alpha)/g(\alpha)$, wobei $g(T) \neq 0$ gilt. Da α transzendent über K ist, folgt dann auch $g(\alpha) \neq 0$. Man prüft unmittelbar nach, dass dies wohldefiniert ist (unabhängig von der Darstellung des Bruches), ein Homomorphismus von Ringen, und nach Definition von $K(\alpha)$ ist die Abbildung auch surjektiv. Weil $K(T)$ ein Körper ist, ist sie offenbar auch injektiv. □

Anmerkung* Es folgt etwa, dass $\mathbb{Q}(\pi) \simeq \mathbb{Q}(T) \simeq \mathbb{Q}(e)$ gilt.

$K[x_1, x_2] \overset{def}{=} (K[x_1])[x_2]$ und $K(x_1, x_2) \overset{def}{=} (K(x_1))(x_2)$. Induktiv werden $K[x_1, \ldots, x_n]$ und $K(x_1, \ldots, x_n)$ definiert. Dies ist der kleinste Teilring (bzw. -körper), der K und $\{x_1, \ldots, x_n\}$ enthält.

2. Konstruktion einfacher algebraischer Körpererweiterungen

In Folgerung 1.9 hatten wir ein algebaisches Element $x \in L$ und dessen Minimalpolynom über K betrachtet, wobei L/K eine schon gegebene Körpererweiterung war. Der folgende wichtige Satz ist gewissermaßen eine Umkehrung davon, der uns zeigt, wie man einfache algebraische Körpererweiterungen "abstrakt" konstruieren kann, d. h. *ohne* in einem evtl. schon gegebenen Oberkörper zu argumentieren.

SATZ 2.1 (Kronecker). *Sei K ein Körper. Sei $f \in K[T]$ normiert und irreduzibel vom Grad n. Dann ist $L = K[T]/fK[T]$ eine Körpererweiterung von K vom Grad $[L : K] = n$. Die Klasse $t = [T]$ von T in L ist eine Nullstelle von f in L, und es gilt $L = K(t)$. Ferner ist f das Minimalpolynom von t über K.*

BEWEIS. Nach Lemma 1.10 ist $L = K[T]/fK[T]$ ein Körper. Offenbar ist $a \mapsto [a] = a + fK[T]$ ein injektiver Ringhomomorphismus $K \to K[T]/fK[T]$, womit K als Teilkörper von L identifiziert wird.

Die Klassen $[1], [T], \ldots, [T^{n-1}]$ sind eine K-Basis von L: Denn ist $[g] = g + fK[T] \in L$, so zeigt Division mit Rest, $g = qf + r$, dass $[g] = [r]$, und $r = 0$ oder $\mathrm{grad}(r) < n$, d. h. r wird von $1, T, \ldots, T^{n-1}$ erzeugt. Ist $\sum_{i=0}^{n-1} a_i[T^i] = 0$, so ist $\sum_{i=0}^{n-1} a_iT^i \in fK[T]$, aber aus Gradgründen geht nur $\sum_{i=0}^{n-1} a_iT^i = 0$, also alle $a_i = 0$.

Ist $t = [T]$, so ist dann $L = K(t)$ unmittelbar klar. Einsetzen ergibt $f(t) = f([T]) = [f] = [0]$. Da f irreduzibel über K ist, ist f das Minimalpolynom von t über K (vgl. 1.8). □

3. Der Gradsatz

Der folgende Satz ist von ähnlich grundlegender Bedeutung wie der Satz von Lagrange in der Gruppentheorie:

SATZ 3.1 (Gradsatz). *Sei $K \subseteq L \subseteq M$ ein Körperturm. $[M : K]$ ist genau dann endlich, wenn $[M : L]$ und $[L : K]$ endlich sind. In dem Fall gilt*

$$[M : K] = [M : L] \cdot [L : K].$$

Dieser Satz hat eine ähnlich grundlegende Wichtigkeit in der Theorie der Körpererweiterungen wie der Satz von Lagrange in der Gruppentheorie. Man beweist dazu die folgende stärkere Aussage. (Beweis einfach.)

ZUSATZ 3.2. *Sei $K \subseteq L \subseteq M$ ein Körperturm. Ist $l_1, \ldots, l_p$ eine K-Basis von L und $m_1, \ldots, m_q$ eine L-Basis von M, so ist die pq-elementige Menge*

$$\{l_i m_j \mid i = 1, \ldots, p,\ j = 1, \ldots, q\}$$

eine K-Basis von M.

BEISPIEL 3.3. $x = \sqrt{i}$ ist Nullstelle des Polynoms $T^4 + 1$. Es gilt $\sqrt{i} = \frac{1}{2}(\sqrt{2} + i\sqrt{2})$. Schauen wir uns die Körpererweiterung $\mathbb{Q}(i, \sqrt{2})/\mathbb{Q}$ an. Es gilt $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$. Weil $\mathbb{Q}(\sqrt{2}) \subseteq \mathbb{R}$ und $i \notin \mathbb{R}$, gilt auch $[\mathbb{Q}(i, \sqrt{2}) : \mathbb{Q}(\sqrt{2})] = 2$, und damit nach dem Gradsatz

$$[\mathbb{Q}(i, \sqrt{2}) : \mathbb{Q}] = [\mathbb{Q}(i, \sqrt{2}) : \mathbb{Q}(\sqrt{2})] \cdot [\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2 \cdot 2 = 4.$$

Es ist 1, $\sqrt{2}$ eine $\mathbb{Q}$-Bais von $\mathbb{Q}(\sqrt{2})$ und 1, i eine $\mathbb{Q}(\sqrt{2})$-Basis von $\mathbb{Q}(i, \sqrt{2})$. Nach dem Zusatz ist deswegen

$$1,\ i,\ \sqrt{2},\ i\sqrt{2}$$

eine $\mathbb{Q}$-Basis von $\mathbb{Q}(i, \sqrt{2})$. Außerdem gilt $\mathbb{Q}(\sqrt{i}) = \mathbb{Q}(i, \sqrt{2})$: Wegen $\sqrt{i} = \frac{1}{2}(\sqrt{2} + i\sqrt{2}) \in \mathbb{Q}(i, \sqrt{2})$, also $\mathbb{Q}(\sqrt{i}) \subseteq \mathbb{Q}(i, \sqrt{2})$. Sollte diese Inklusion echt sein, so muss $[\mathbb{Q}(\sqrt{i}) : \mathbb{Q}] < 4$ ein Teiler von 4 sein, also $= 1$ oder $= 2$. Offenbar kann er nicht $= 1$ sein. Er kann aber auch nicht $= 2$ sein, denn sonst müsste $i = \sqrt{i}^2$ sich als LKB über $\mathbb{Q}$ in 1, $\sqrt{i} = \frac{1}{2}(\sqrt{2} + i\sqrt{2})$ darstellen lassen. Da aber 1, i, $\sqrt{2}$, $i\sqrt{2}$ linear unabhängig über $\mathbb{Q}$ sind, ist dies nicht möglich. Es folgt $[\mathbb{Q}(\sqrt{i} : \mathbb{Q}] = 4$, und da mit $f = T^4 + 1 \in \mathbb{Q}[T]$ ein normiertes Polynom vom Grad 4 ist mit $f(x) = 0$, gilt $\mathrm{MIPO}(x/\mathbb{Q}) = T^4 + 1$.

FOLGERUNG 3.4. *Sei L/K eine Körpererweiterung. Sind $x_1, \ldots, x_n$ sämtlich algebraisch über K, so gilt*

$$K(x_1, \ldots, x_n) = K[x_1, \ldots, x_n],$$

und dies ist eine endliche Körpererweiterung von K.

BEWEIS. Induktion nach n. Für $n = 1$ wissen wir die Aussage schon. Es ist

$$\begin{aligned} K[x_1, \ldots, x_n] &= K[x_1, \ldots, x_{n-1}][x_n] \\ &\overset{IV}{=} K(x_1, \ldots, x_{n-1})[x_n] \\ &\overset{1.12}{=} K(x_1, \ldots, x_{n-1})(x_n) \\ &= K(x_1, \ldots, x_n). \end{aligned}$$

□

FOLGERUNG 3.5. *Sei L/K eine Körpererweiterung. Äquivalent sind:*

(1) *L/K ist endlich.*
(2) *Es gibt über K algebraische Elemente $x_1, \ldots, x_n \in L$ mit $L = K(x_1, \ldots, x_n)$.*

BEWEIS. (2)⇒(1) Nach der vorstehenden Folgerung.

(1)⇒(2) Ist L/K endlich, so gibt es eine endliche K-Basis $y_1, \ldots, y_m \in L$. Damit gilt insbesondere $L = K(y_1, \ldots, y_m)$, und wegen $[K(y_i) : K] \leq [L : K] < \infty$ sind alle y_i algebraisch über K. □

SATZ 3.6 (Algebraischer Abschluss). *L/K sei Körpererweiterung. Es gilt*

(1) *Die über K algebraischen Elemente bilden einen Teilkörper $\overline{K}$ von L.*
(2) *$\overline{K}$ ist der größte Teilkörper von L, der über K algebraisch ist.*
(3) *Jedes Element aus L, welches über $\overline{K}$ algebraisch ist, liegt in $\overline{K}$. Kurz: $\overline{\overline{K}} = \overline{K}$.*

BEWEIS. (1) Seien $x, y \in L$ algebraisch über K. Dann gilt $x + y \in K(x, y)$, also $[K(x + y) : K] \leq [K(x, y) : K] < \infty$, und analoges gilt für $x \cdot y$. Ist $x \neq 0$, so gilt $x^{-1} \in K(x)$, also auch $[K(x^{-1} : K] \leq [K(x) : K] < \infty$. Also sind $x + y$, xy und x^{-1} algebraisch über K, und es folgt, dass $\overline{K}$ ein Körper ist.

(2) ist trivial.

(3) Sei $x \in L$ algebraisch über $\overline{K}$. Dann gibt es ein normiertes $f \in \overline{K}[T]$ mit $f(x) = 0$. Sei etwa $f = T^n + a_{n-1}T^{n-1} + \cdots + a_1T + a_0$, wobei $a_0, \ldots, a_{n-1}$ algebraisch über K sind. Dann ist offenbar x algebraisch über $M = K(a_0, \ldots, a_{n-1})$. Es folgt

$$[K(x) : K] \leq [M(x) : K] = [M(x) : M] \cdot [M : K] < \infty,$$

weil beide Faktoren endlich sind. Also ist x algebraisch über K. □

BEISPIEL 3.7. $\overline{\mathbb{Q}}$ in $\mathbb{C}$ (oder $\mathbb{R}$) ist die Menge der algebraischen komplexen (bzw. reellen) Zahlen.

SATZ 3.8 (Transitivität algebraischer Erweiterungen). *Es sei $K \subseteq L \subseteq M$ ein Körperturm. Die Erweiterung M/K ist genau dann algebraisch, wenn die beiden Erweiterungen M/L und L/K beide algebraisch sind.*

BEWEIS. (1) Seien M/L und L/K algebraisch. Dann gilt $L \subseteq \overline{K}$, dem algebraischen Abschluss von K in M. Sei $x \in M$. Dies ist algebraischh über L, also erst recht über $\overline{K}$. Nach dem Resultat zuvor gilt dann $x \in \overline{K}$, also ist x algebraisch über K. Es folgt, dass M/K algebraisch ist.

(2) Sei umgekehrt M/K algebraisch. Jedes $x \in M$ ist über K, also erst recht über L algebraisch. Also ist M/L algebraisch. Da jedes Element von M algebraisch über K ist, ist insbesondere jedes Element von L algebraisch über K. Also ist auch L/K algebraisch. □

SATZ 3.9. *Für eine Körpererweiterung L/K sind äquivalent:*

(1) *L/K ist algebraisch.*
(2) *Jeder Ring R mit $K \subseteq R \subseteq L$ (Teilringe) ist ein Körper.*

BEWEIS. (1)⇒(2) Sei R ein Zwischenring. Sei $x \in R$, $x \neq 0$. Es ist x algebraisch über K, und es folgt

$$x^{-1} \in K(x) = K[x] \subseteq R.$$

Also ist x in R invertierbar.

(2)⇒(1) Sei $x \in L$. Aus (2) folgt $K[x] = K(x)$, also x algebraisch über K. □

4. Berechnung des Minimalpolynoms

BEISPIEL 4.1. Betrachte $L = \mathbb{Q}(\sqrt{i})/\mathbb{Q}$. Nach Beispiel 3.3 ist 1, i, $\sqrt{2}$, $i\sqrt{2}$ eine $\mathbb{Q}$-Basis von L.

(1) Sei $x = 2i + \sqrt{2}$. Wir wollen das Minimalpolynom von x über $\mathbb{Q}$ berechnen. Dazu stellen wir die Elemente 1, x, $x^2, \ldots$ als Linearkombination in der oben gegebenen Basis dar. Die Koeffizienten schreiben wir als Spalten einer Matrix:

1	x	x^2	x^3	x^4
1	0	-2	0	-28
0	2	0	4	0
0	1	0	-10	0
0	0	4	0	-16

Da nach dem Gradsatz $[L : \mathbb{Q}] = 4$, müssen wir hier maximal bis x^4 gehen und stellen x^4 (sofern dies nicht schon vorher möglich ist), als Linearkombination in den vorherigen Potenzen von x dar. Hier sehen wir, dass die ersten vier Spaltenvektoren linear unabhängig sind, also 1, x, x^2, x^3 sind linear unabhängig. Daher muss MIPO$(x/\mathbb{Q})$ den Grad 4 haben, und man sieht, indem man die letzte Spalte als LKB der vorderen Spalten darstellt, $x^4 = -4x^2 - 36$, und damit MIPO$(x/\mathbb{Q}) = T^4 + 4T^2 + 36$.

(2) $x = 1 + \sqrt{2} + i$.

1	x	x^2	x^3	x^4
1	1	2	4	0
0	1	2	8	24
0	1	2	2	0
0	0	2	6	16

Man sieht $x^4 = 4x^3 - 4x^2 - 8$, also MIPO$(x/\mathbb{Q}) = T^4 - 4T^3 + 4T^2 + 8$.

LEMMA 4.2. *Es sei L/K eine Körpererweiterung und $0 \neq x \in L$. Dann haben die Elemente x und $1/x$ denselben Grad über K.*

BEWEIS. $K(x) = K(1/x)$. □

BEISPIEL 4.3. Minimalpolynom von $x = 1 + i + \sqrt{2}$ über $\mathbb{Q}$ ist $T^4 - 4T^3 + 4T^2 + 8$, das von $1/x$ ist $T^4 + 1/2T^2 - 1/2T + 1/8$.

5. Arithmetische Eigenschaften des Körpers $\mathbb{Q}$

SATZ 5.1. *Jede rationale Zahl x, welche einer normierten Polynomgleichung*

$$x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 = 0 \tag{5.1}$$

mit ganzzahligen Koeffizienten $a_0, \ldots, a_{n-1} \in \mathbb{Z}$ genügt, ist notwendig in $\mathbb{Z}$ gelegen. Ferner ist solch ein x ein Teiler von a_0.

FOLGERUNG 5.2. *Sei a eine ganze Zahl, welche sich für gegebenes $n \geq 2$ in $\mathbb{Z}$ nicht als n-te Potenz schreiben läßt (d. h. wir nehmen $a \neq k^n$ für jedes $k \in \mathbb{Z}$ an). Dann ist die Gleichung*

$$x^n - a = 0$$

nicht in $\mathbb{Q}$ lösbar. Anders formuliert: $\sqrt[n]{a} \notin \mathbb{Q}$.

BEISPIEL 5.3. Die Gleichung $x^{11} - 10x^6 + 3 = 0$ ist nicht in $\mathbb{Q}$ lösbar.

BEWEIS VON SATZ 5.1. Schreibe $x = a/b$ mit teilerfremden $a, b \in \mathbb{Z}$, $b \neq 0$. Multiplikation von (5.1) mit b^n liefert

$$a^n + \sum_{i=1}^{n} a_{n-i} a^{n-i} b^i = 0,$$

also

$$a^n = -b \sum_{i=1}^{n} a_{n-i} a^{n-i} b^{i-1}.$$

Es folgt $b \mid a^n$. Wäre nun $b \neq 1$, dann gäbe es einen Primfaktor p von b, und p wäre dann auch ein Primfaktor von a, Widerspruch. Also gilt $b = 1$, und damit $x = a \in \mathbb{Z}$. Ferner gilt

$$x \cdot \left(-x^{n-2} - a_{n-1}x^{n-2} - \cdots - a_2 x - a_1\right) = a_0,$$

also $x \mid a_0$. □

6. Konstruktionen mit Zirkel und Lineal

- Dreiteilung des Winkels.
- Verdoppelung des Würfels (Delisches Problem).
- Quadratur des Kreises.
- Konstruktion des regelmäßigen n-Ecks.

DEFINITION 6.1. Es sei M eine Teilmenge von $\mathbb{C}$, welche die Punkte 0 und 1 enthält.

(1) Eine Gerade G heißt unmittelbar aus M konstruierbar, wenn es Elemente z_1, $z_2 \in M$ mit $z_1 \neq z_2$ so gibt, dass z_1, $z_2 \in G$.

(2) Ein Kreis heißt unmittelbar aus M konstuierbar, wenn es Elemente z_0, z_1, z_2 in M so gibt, dass K der Kreis um z_0 mit Radius $|z_1 - z_2|$ ist.

(3) Ein Punkt $z \in \mathbb{C}$ heißt unmittelbar aus M konstruierbar, wenn es A und B mit $z \in A \cap B$ so gibt, dass A und B jeweils eine unmittelbar aus M konstruierbare Gerade oder einen unmittelbar aus M konstruierbaren Kreis bedeuten.

DEFINITION 6.2. Wir setzen $M^{(0)} = M$ und erklären rekursiv $M^{(n+1)}$ als die Menge der unmittelbar aus $M^{(n)}$ konstruierbaren Punkte aus $\mathbb{C}$. Definitionsgemäß heißt dann

$$K(M) = \bigcup_{n \in \mathbb{N}} M^{(n)}$$

die Menge der ausgehend von M mit Zirkel und Lineal konstruierbaren Punkte.

Wir nennen ein $z \in \mathbb{C}$ (schlechthin) (mit Zirkel und Lineal) konstruierbar, wenn z ausgehend von der Menge $\{0, 1\}$ konstruierbar ist.

SATZ 6.3. *Sei* $0, 1 \in M \subseteq \mathbb{C}$. *Dann ist* $K(M)$ *der kleinste Teilkörper* K *von* $\mathbb{C}$ *mit folgenden Eigenschaften (1)-(3):*

(1) $M \subseteq K$;
(2) $z \in K \Rightarrow \overline{z} \in K$;
(3) *Ist* $z \in \mathbb{C}$ *Lösung einer quadratischen Gleichung* $z^2 + az + b = 0$ *mit Koeffizienten* $a, b \in K$, *so folgt* $z \in K$.

Kurz: $K(M)$ ist der kleinste Teilkörper von $\mathbb{C}$, der M enthält und unter komplexer Konjugation und Quadratwurzelziehen abgeschlossen ist.

BEWEIS. (0) $K(M)$ ist ein Teilkörper von $\mathbb{C}$: Sind z und w in $K(M)$, so erhält man $z - w$ als Schnittpunkt des Kreises um z mit Radius $|w|$ und des Kreises um $-w$ mit Radius $|z|$. Sei $z \in \mathbb{C}$, $z \neq 0$. In Polarkoordinaten, $z = re^{i\alpha}$. Dann gilt offenbar

$$z \in K(M) \quad \Leftrightarrow \quad r,\, e^{i\alpha} \in K(M).$$

Seien nun $z = re^{i\alpha}$ und $w = se^{i\beta}$ in $K(M) \setminus \{0\}$. Wir wollen zeigen, dass dann auch $z/w \in K(M)$ gilt. Dazu genügt es zu zeigen, dass r/s und $e^{i(\alpha-\beta)}$ in $K(M)$ sind.

(a) Für r/s können wir $r \neq s$ annehmen. Es ist $i \in K(M)$, und dann $1 + i \in K(M)$. Sei A die Gerade durch 0 und $1+i$. Sei $a \in A$ Schnittpunkt des Kreises um 0 mit Radius r mit A, und b der Schnittpunkt mit dem Kreis um 0 mit Radius s. Wir können annehmen, dass a und b im ersten Quadranten liegen. Sei B die Gerade durch 1 und b. Wir können dann eine Parallele B' konstruieren, die durch den Punkt a geht. Der Schnittpunkt von B' mit der reellen Achse heiße c. Der Strahlensatz sagt uns nun

$$\frac{r}{s} = \frac{|a|}{|b|} = \frac{c}{1}.$$

Der konstruierte Punkt $c \in K(M)$ ist also r/s.

(b) Mit $w = e^{i\beta}$ ist auch $\overline{w} = e^{i(-\beta)}$ in $K(M)$. Wir müssen also nur eine Winkeladdition konstruieren. Das ist einfach.

Es folgt, dass $K(M)$ ein Teilkörper von $\mathbb{C}$ ist.

(1) $M \subseteq K$ ist klar.

(2) Die einfache Konstruktion haben wir eben schon verwendet.

(3) Sei $z \in K(M) \setminus \{0\}$. Wir zeigen $\sqrt{z} \in K(M)$. Schreibe $z = re^{i\alpha}$. Es ist $\sqrt{z} = \sqrt{r}e^{i\alpha/2}$. Die Winkelhalbierung ist einfach zu konstruieren. Es sind r, 0 und -1 in $K(M)$. Der Mittelpunkt der Strecke zwischen -1 und r ist $\frac{r+1}{2}$. Wir schlagen einen Kreis B um diesen Punkt, so dass -1 und r die Schnittpunkte von B mit der reellen Achse sind. Der Schnittpunkt von B mit der imaginären Achse heiße a. Die Punkte -1, r und a bilden die Ecken des rechtwinkligen Dreiecks im Thaleskreis, die Länge der Verbindung zwischen 0 und a bildet die Höhe h des Dreiecks. Der Höhensatz (mehrfache Anwendung des Satzes von Pythagoras) sagt $h^2 = |-1| \cdot r$. Es ist also $h = |a| \in K(M)$ Quadratwurzel von r.

Gilt $z^2 + az + b = 0$ mit a, $b \in K(M)$, so gilt $z = -\frac{a}{2} \pm \sqrt{\frac{a^2}{4} - b}$, also $z \in K(M)$ nach dem vorherigen Argument.

(4) Sei nun K ein Teilkörper von $\mathbb{C}$, der die Eigenschaft (1)-(3) erfüllt. Wir haben $K(M) \subseteq K$ zu zeigen. Dazu zeigen wir per Induktion, dass $M^{(n)} \subseteq K$ gilt für jedes $n \geq 0$: Es gilt $M^{(0)} = M \subseteq K$ nach (1). Sei $n \geq 0$, und wir nehmen an, wir hätten bereits $M^{(n)} \subseteq K$ gezeigt. Wir zeigen $M^{(n+1)} \subseteq K$: Sei $z \in M^{(n+1)}$, also $z \in A \cap B$, mit drei möglichen Fällen:

(a) A und B sind Geraden; a_1, $a_2 \in A$, $a_1 \neq a_2$, b_1, $b_2 \in B$, $b_1 \neq b_2$, und a_1, a_2, b_1, $b_2 \in M^{(n)} \subseteq K$. Es gilt

$$A = \{a + tc,\, t \in \mathbb{R}\}, \quad B = \{b + sd,\, s \in \mathbb{R}\},$$

mit $a = a_1$, $c = a_2 - a_1$, $b = b_1$, $d = b_2 - b_1 \in K$. Man kann dies auch so schreiben:

$$A = \{w \in \mathbb{C} \mid \overline{c}(w-a) = c(\overline{w-a})\},\ A = \{w \in \mathbb{C} \mid \overline{d}(w-b) = d(\overline{w-b})\},$$

denn ist $\overline{c}(w-a)$ reell, so erhält man mit $t := \overline{c}(w-a)/\overline{c}c \in \mathbb{R}$, dass $w = a + tc$ gilt. Es ist also $(z, \overline{z})^t$ Lösung des linearen Gleichungssystems

$$\begin{pmatrix} \overline{c} & -c \\ \overline{d} & -d \end{pmatrix} \begin{pmatrix} z \\ \overline{z} \end{pmatrix} = \begin{pmatrix} -c\overline{a} + \overline{c}a \\ -d\overline{b} + \overline{d}b \end{pmatrix},$$

und da alle Koeffizienten in K sind, gilt z, $\overline{z} \in K$.

(b) A ist Gerade und B ein Kreis. Konkret:

$$\begin{aligned} A: &\quad \overline{b}(w-a) - b(\overline{w-a}) = 0 \\ B: &\quad (w-c)(\overline{w-c}) = s, \end{aligned}$$

mit a, $b \in K$, $b \neq 0$ (wie oben) und $c \in K$ und $s = |p-q|^2$, p, $q \in M^{(n)} \subseteq K$. Nutzt man nun $z \in A \cap B$, so sieht man, dass z Nullstelle eines quadratischen Polynoms $f \in K[T]$ ist, also wegen (3) folgt $z \in K$.

(c) A und B sind Kreise. Konkret:

$$\begin{aligned} A: &\quad (w-a)(\overline{w-a}) = r \\ B: &\quad (w-b)(\overline{w-b}) = s, \end{aligned}$$

mit a, b, r, $s \in K$ mit $a \neq b$. Nutzt man $z \in A \cap B$, zieht die erste Gleichung von der zweiten ab, so erhält man mit $c := r - s + b\overline{b} - a\overline{a}$, dass z den Gleichungen

$$(\overline{b-a})z + (b-a)\overline{z} = c, \quad (z-b)(\overline{z-b}) = s$$

genügt und wir nun Fall (b) anwenden können.

In jedem Fall ergibt sich also $z \in K$. Damit $M^{(n+1)} \subseteq K$, und schließlich $K(M) \subseteq M$. □

Satz 6.4. *Für eine komplexe Zahl z sind äquivalent:*

(1) *z ist konstruierbar, d. h. $z \in K(\{0,1\})$.*

(2) *Es gibt einen Körperturm*

$$\mathbb{Q} = K_0 \subset K_1 \subset K_2 \subset \cdots \subset K_{n-1} \subset K_n$$

mit Schritten vom Grad $[K_i : K_{i-1}] = 2$ *(für alle* $1 \leq i \leq n$*), welcher* z *erreicht, d. h.* $z \in K_n$*.*

FOLGERUNG 6.5. *Jede konstruierbare komplexe Zahl* z *ist algebraisch über* $\mathbb{Q}$ *und der Grad* $[\mathbb{Q}(z) : \mathbb{Q}]$ *ist eine Potenz von* 2*.*

FOLGERUNG 6.6. *Die Zahl* π *ist nicht konstruierbar. Damit ist die Quadratur des Kreises nicht lösbar.*

BEWEIS. π ist nicht algebraisch. (Satz von Lindemann 1882.) □

FOLGERUNG 6.7. *Die Zahl* $\sqrt[3]{2}$ *ist nicht konstruierbar. Damit ist die Verdoppelung des Würfels nicht lösbar.*

BEWEIS. Für $\alpha = \sqrt[3]{2}$ gilt (vgl. Kriterium von Eisenstein) $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 3$. □

FOLGERUNG 6.8. *Die Zahl* $\cos 20^\circ$ *ist nicht konstruierbar. Damit ist die Dreiteilung des Winkels nicht lösbar.*

BEWEIS. Man zeigt, dass für $\alpha = \cos 20^\circ$ gilt $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 3$. Also ist α nicht konstruierbar. Andererseits ist offenbar der Winkel 60° (d. h. $z = e^{\pi/3}$) konstruierbar. □

Die Nichtlösbarkeit der Verdoppelung des Würfels und der Dreiteilung des Winkels wurde zuerst von L. P. Wantzel 1837 gezeigt.

FOLGERUNG 6.9. *Das reguläre* 5*-Eck ist mit Zirkel und Lineal konstruierbar.*

BEWEIS. Vgl. Übungen. □

BEMERKUNG 6.10. Es gilt, dass das reguläre n-Eck genau dann konstruierbar ist, wenn $\varphi(n)$ eine Potenz von 2 ist. Hier ist φ die Eulersche φ-Funktion, welche bei gegebener Primzahlfaktorisierung

$$n = p_1^{r_1} \cdots p_t^{r_t}$$

durch

$$\varphi(n) = \left(p_1^{r_1} - p_1^{r_1-1}\right) \cdots \left(p_t^{r_t} - p_t^{r_t-1}\right)$$

erklärt ist. Für den Nachweis dieses Satzes benötigt man stärkere Hilfsmittel aus der Galoistheorie über sog. Kreisteilungskörper. (Aus Zeitgründen muss der Beweis leider entfallen.)

Beweis von Satz 6.4. Wir nehmen von nun an $M = \{0, 1\}$ an. Dann ist die Eigenschaft (2), Abgeschlossenheit gegenüber Konjugation, in Satz 6.3 nicht nötig, sondern automatisch erfüllt. Dies folgt aus dem folgenden allgemeineren Lemma.

LEMMA 6.11. *Sei* $\varphi\colon \mathbb{C} \to \mathbb{C}$ *ein Ringautomorphismus des Körpers* $\mathbb{C}$*. Sei* $K \subseteq \mathbb{C}$ *der kleinste Teilkörper von* $\mathbb{C}$*, der abgeschlossen ist unter Lösungen von quadratischen Gleichungen. Dann gilt* $\varphi(K) \subseteq K$*.*

BEWEIS. Setze $K' = \varphi^{-1}(K)$. Seien $f' = T^2 + a'T + b' \in K'[T]$ und $x \in \mathbb{C}$ mit $f'(x) = 0$. Dann gilt mit $a = \varphi(a')$, $b = \varphi(b')$, $y = \varphi(x)$ und $f = T^2 + aT + b \in K[T]$:

$$f(y) = \varphi(f'(x)) = \varphi(0) = 0.$$

Wegen der Abgeschlossenheit von K folgt $y \in K$ und damit $x = \varphi^{-1}(y) \in K'$. Also ist auch K' abgeschlossen unter Lösungen von quadratischen Gleichungen, und wegen der Minimalitätseigenschaft von K folgt $K \subseteq K'$. Sei nun $x \in K$. Dann gilt $x \in K'$, also $x = \varphi^{-1}(y)$ für ein $y \in K$. Es folgt $\varphi(x) = y \in K$. Es folgt $\varphi(K) \subseteq K$. □

$z \in \mathbb{C}$ heißt erreichbar, wenn es einen Körperturm

$$\mathbb{Q} = K_0 \subset K_1 \subset \cdots \subset K_n$$

in $\mathbb{C}$ gibt, so dass alle $[K_i : K_{i-1}] = 2$ gilt $(1 \leq i \leq n)$, welcher z erreicht, d. h. $z \in K_n$. Mit $\widehat{\mathbb{Q}}$ bezeichnen wir die Menge aller erreichbaren $z \in \mathbb{C}$.

SATZ 6.12. *$\widehat{\mathbb{Q}}$ ist ein Teilkörper von $\mathbb{C}$ mit folgenden Eigenschaften:*

- *Genügt $z \in \mathbb{C}$ einer quadratischen Gleichung über $\widehat{\mathbb{Q}}$, so gilt schon $z \in \widehat{\mathbb{Q}}$.*

BEWEIS. Seien z, $w \in \widehat{\mathbb{Q}}$. Es gibt Körpertürme

$$\mathbb{Q} = K_0 \subset K_1 \subset \cdots \subset K_n$$

und

$$\mathbb{Q} = L_0 \subset L_1 \subset \cdots \subset L_m$$

mit $[K_i : K_{i-1}] = 2$ und $[L_j : L_{j-1}] = 2$, mit $z \in K_n$ und $w \in L_m$. Es gibt α_i vom Grad 2 über K_{i-1} mit $K_i = K_{i-1}(\alpha_i)$ und β_j vom Grad 2 über L_{j-1} mit $L_i = L_{j-1}(\beta_j)$. Es ist dann $K_i = \mathbb{Q}(\alpha_1, \ldots, \alpha_i)$ und $L_j = \mathbb{Q}(\beta_1, \ldots, \beta_j)$. Man betrachtet nun den Körperturm

$$\mathbb{Q} \subset \mathbb{Q}(\alpha_1) \subset \cdots \subset \mathbb{Q}(\alpha_1, \ldots, \alpha_n) \subseteq \mathbb{Q}(\alpha_1, \ldots, \alpha_n, \beta_1) \subseteq \cdots \subseteq \mathbb{Q}(\alpha_1, \ldots, \alpha_n, \beta_1, \ldots, \beta_m),$$

wobei in dem größten der Körper die Elemente z und w, und somit auch $z - w$ und z/w (sofern $w \neq 0$) liegen. Jedes β_j hat den Grad 2 über L_{j-1}, also einen Grad ≤ 2 über $K_n(\beta_1, \ldots, \beta_{j-1})$. Lässt man Indizes j mit $L_j = L_{j-1}$ aus, so erhält man einen Körperturm mit Gradschritten 2, der $z - w$ und z/w erreicht.

Sei nun $z \in \mathbb{C}$ eine Lösung von $z^2 + az + b = 0$, wobei a, $b \in \widehat{\mathbb{Q}}$ gilt. Dann werden a und b von einem gemeinsamen Körperturm der obigen Form erreicht, etwa a, $b \in K_n$. Es ist dann $z \in K_{n+1} := K_n(\sqrt{a^2/4 - b})$ und $[K_{n+1} : K_n] \leq 2$. □

SATZ 6.13. *Für $M = (\{0, 1\})$ gilt $K(M) = \widehat{\mathbb{Q}}$.*

BEWEIS. "$\subseteq$" Beide Teilkörper, $K(M)$ und $\widehat{\mathbb{Q}}$, sind abgeschlossen bzgl. Lösungen von quadratischen Gleichungen, und nach Satz 6.3 (und Lemma 6.11) ist $K(M)$ der kleinste solche. Also folgt $K(M) \subseteq \widehat{\mathbb{Q}}$.

"$\supseteq$" Sei

$$\mathbb{Q} = K_0 \subset K_1 \subset \cdots \subset K_n$$

ein Körperturm in $\mathbb{C}$ mit $[K_i : K_{i-1}] = 2$ für $1 \leq i \leq n$. Man zeigt induktiv für $i = 0, \ldots, n$, dass $K_i \subseteq K(M)$ gilt. Für $i = 0$ ist dies wegen $K_0 = \mathbb{Q}$ klar. Es sei bereits gezeigt, dass $K_{i-1} \subseteq K(M)$ gilt. Sei $z \in K_i$. Wir können $z \notin K_{i-1}$ annehmen. Dann erfüllt z wegen $[K_i : K_{i-1}] = 2$ eine quadratische Gleichung $z^2 + az + b = 0$ mit a, $b \in K_{i-1}$. Es folgt a, $b \in K(M)$, und nach Satz 6.3 folgt $z \in K(M)$. □

7. Isomorphie einfacher algebraischer Erweiterungen

DEFINITION 7.1. Seien L/K und L'/K Körpererweiterungen. Ein Isomorphismus $\sigma\colon L \to L'$ heißt ein K-Isomorphismus, wenn $\sigma_{|K} = 1_K$ gilt. (Äquivalent: σ ist K-linear.)

Ist dabei $L = L'$, so heißt σ ein K-Automorphismus.

Allgemeiner definiert man: Ist $i\colon K \to K'$ ein Isomorphismus von Körpern, und sind L/K und L'/K' Körpererweiterungen, so heißt ein Isomorphismus $\sigma\colon L \to L'$ ein Isomorphismus von Körpererweiterungen, falls $\sigma_{|K} = i$ gilt.

SATZ 7.2. *Seien $K(\alpha)/K$ und $K(\beta)/K$ einfache algebraische Körpererweiterungen, so dass α und β dasselbe Minimalpolynom $f \in K[T]$ haben. Dann gibt es einen K-Isomorphismus $\sigma\colon K(\alpha) \xrightarrow{\sim} K(\beta)$ mit $\sigma(\alpha) = \beta$.*

BEWEIS. Es habe f den Grad n. Jedes $x \in K(\alpha)$ läßt sich nach Folgerung 1.15 eindeutig schreiben

$$x = a_0 + a_1\alpha + a_2\alpha^2 + \cdots + a_{n-1}\alpha^{n-1}$$

$(a_0, \ldots, a_{n-1} \in K)$. Definiere

$$\sigma(x) \stackrel{def}{=} a_0 + a_1\beta + a_2\beta^2 + \cdots + a_{n-1}\beta^{n-1}.$$

Wieder nach 1.15 ist σ bijektiv, und es gilt $\sigma(x+y) = \sigma(x) + \sigma(y)$ für alle $x, y \in K(\alpha)$. Zu zeigen bleibt $\sigma(xy) = \sigma(x)\sigma(y)$ für alle $x, y \in K(\alpha)$. Nach 1.15 gibt es $g, h, p \in K[T]$ vom Grad $\leq n-1$ (sofern nicht das Nullpolynom) mit $x = g(\alpha)$, $y = h(\alpha)$ und $xy = p(\alpha)$. Es ist $(gh-p)(\alpha) = g(\alpha)h(\alpha) - p(\alpha) = xy - xy = 0$. Nach Satz 1.8 gilt, dass $gh - p$ von f geteilt wird, etwa $gh = qf + p$. Entweder $p = 0$, oder $\operatorname{grad}(p) < \operatorname{grad}(f)$, und daher ist p der Rest bei Division von gh durch f. Da auch $f(\beta) = 0$, folgt $\sigma(xy) = p(\beta) = g(\beta)h(\beta) = \sigma(x)\sigma(y)$. □

Manchmal ist es nützlich, vorstehende Aussage allgemeiner zu haben: Für einen Ringhomomorphismus $f\colon R \to S$ definiere $f^*\colon R[T] \to S[T]$ durch

$$f^*(\sum_{i=0}^{n} a_i T^i) = \sum_{i=0}^{n} f(a_i) T^i.$$

SATZ 7.3. *Seien K und L Körper und $i\colon K \to L$ ein Isomorphismus. Seien $K(\alpha)/K$ und $L(\beta)/L$ einfache algebraische Körpererweiterungen. Sei $f \in K[T]$ das Minimalpolynom von α über K und $g \in L[T]$ das Minimalpolynomen von β über L. Gilt $i^*(f) = g$, so gibt es einen Isomorphismus von Erweiterungen $j\colon K(\alpha)/K \to L(\beta)/L$ mit $j(\alpha) = \beta$.*

BEWEIS. Analog zum Beweis des vorstehenden Satzes. □

ÜBUNG 7.4. Man zeige die Umkehrung von Satz 7.2: Seien $K(\alpha)$ und $K(\beta)$ zwei einfach algebraische Körpererweiterungen, und es gebe einen K-Isomorphismus $\sigma\colon K(\alpha) \xrightarrow{\sim} K(\beta)$ mit $\sigma(\alpha) = \beta$. Man zeige, dass α und β selbes Minimalpolynom über K haben.

8. Algebraischer Abschluss

In Satz 3.6 wurde gezeigt, dass ein Körper *innerhalb* eines vorgegebenen Erweiterungskörpers einen algebraischen Abschluss besitzt. Es gibt aber auch einen algebraischen Abschluss eines Körpers schlechthin.

DEFINITION 8.1. Ein Körper K heißt algebraisch abgeschlossen, falls jedes Polynom $f \in K[T]$ vom Grad ≥ 1 eine Nullstelle in K besitzt.

Es folgt dann, dass jedes Polynom $0 \neq f \in K[T]$ vollständig in Linearfaktoren zerfällt: $f = c \cdot (T - a_1) \cdot \ldots \cdot (T - a_n)$ mit $c \in K^\times$, und $a_1, \ldots, a_n \in K$ (nicht notwendig paarweise verschieden). Offenbar gilt für einen Körper K: Genau dann ist K algebraisch abgeschlossen, wenn jedes irreduzible $f \in K[T]$ den Grad 1 hat.

BEISPIEL 8.2. Der Körper $\mathbb{C}$ der komplexen Zahlen ist algebraisch abgeschlossen. Dies ist der sog. Fundamentalsatz der Algebra, der am elegantesten in der Funktionentheorie bewiesen wird.

Der Körper $\mathbb{R}$ der reellen Zahlen ist nicht algebraisch abgeschlossen, denn z. B. hat das Polynom $T^2 + 1 \in \mathbb{R}[T]$ keine reelle Nullstelle.

Wir skizzieren hier den Beweis, dass sich jeder Körper in einen algebraisch abgeschlossenen Körper einbetten läßt. Dazu bedarf es zweier Techniken, die wir verwenden, ohne detailliert darauf einzugehen:

(1) Polynomringe $R[X_i : i \in I]$ in einer beliebigen "Zahl" von Unbestimmten X_i $(i \in I)$, wobei I eine beliebige Indexmenge ist, also auch unendlich sein darf. In jedem Polynom kommen allerdings immer nur Monome vor, die aus nur endlich vielen der Variablen bestehen.

(2) Das Lemma von Zorn. Es ist äquivalent zum Auswahlaxiom und besagt, dass jede nichtleere (partiell) geordnete Menge $(X, \leq)$, die induktiv ist, ein maximales Element enthält. Dabei heißt induktiv, dass jede total geordnete Teilmenge L von X eine obere Schranke $s \in X$ hat (d. h. für alle $x \in L$ gilt $x \leq s$). Mit dem Lemma von Zorn zeigt man z. B. die Existenz von Basen in (beliebigen, auch nicht endlich erzeugten) Vektorräumen. Oder die folgende Aussage: Ist R ein (kommutativer) Ring und $I \subsetneq R$ ein Ideal, so gibt es ein maximales Ideal M mit $I \subseteq M \subsetneq R$. (Es ist dann der Faktorring R/M ein Körper; dies folgt so wie in 1.10.) Beweis: Sei $\mathcal{X}$ die Menge aller Ideal J mit $I \subseteq J \subsetneq R$. Diese Menge ist nichtleer (da sie I enthält), und induktiv geordnet: Sei $\mathcal{L} \subseteq \mathcal{X}$ total geordnet. Dann ist $S = \bigcup_{J \in \mathcal{L}} J$ ein Ideal. Es gilt $S \in \mathcal{X}$, denn $S = R$ würde $1 \in S$ und damit $1 \in J$ und $J = R$ für ein $J \in \mathcal{X}$ nach sich ziehen. Offenbar ist S eine obere Schranke für $\mathcal{L}$. Nach dem Lemma von Zorn gibt es ein maximales Element $M \in \mathcal{L}$, und es folgt die Behauptung.

SATZ 8.3. *Sei K ein Körper. Dann gibt es einen algebraisch abgeschlossenen Körper L, der K als Teilkörper enthält.*

BEWEIS. (Skizze.) Konstruiere einen Körper L_1, in dem jedes Polynom $f \in K[T]$ vom Grad ≥ 1 eine Nullstelle enthält. (Die Konstruktion geht auf Emil Artin zurück.) Für jedes solche Polynom f sei X_f eine Unbestimmte. Wir betrachten den Polynomring in diesen unendlich vielen Variablen,

$$R = K[X_f : f \in K[T]; \operatorname{grad}(f) \geq 1].$$

Jedes Element in R ist eine endlich Linearkombination von Monomen in den X_f [dabei kommen jeweils nur endlich viele Variablen vor]. Sei $I \subseteq R$ das Ideal, welches erzeugt wird von allen Polynomen in R von der Form $f(X_f)$ ($f \in K[T]$ vom Grad ≥ 1), also in jeweils einer Variablen.

Dieses Ideal I ist nicht ganz R: Sonst hätte man eine Darstellung

$$\sum_{i=1}^{n} g_i(X_1, \ldots, X_N) f_i(X_i) = 1$$

(nur endlich viele Variablen sind involviert, wobei wir abkürzend $X_i = X_{f_i}$ schreiben). Mit Satz 2.1 sieht man, dass es einen Erweiterungskörper E von K gibt, in dem alle Polynome $f_i(X_i)$ eine Nullstelle α_i besitzen (Übung!). Setzt man für alle X_i dann α_i ein, so erhält man $0 = 1$, Widerspruch.

Da $I \subsetneq R$ gibt es (nach dem Zornschen Lemma) ein maximales Ideal $M \subsetneq R$, welches I enthält. Es ist dann der Faktorring R/M ein Körper (folgt ähnlich wie in 1.10). Sei $\pi\colon R \longrightarrow R/M$ die kanonische Surjektion. Für jedes f vom Grad ≥ 1 hat dann das Polynom $\pi^*(f)$ eine Nullstelle in R/M (nämlich $[X_f] \stackrel{def}{=} X_f + M$, denn: $\pi^*(f)([X_f]) = [f(X_f)] = [0]$, weil $f(X_f) \in I \subseteq M$), und dies ist eine Körpererweiterung von $\pi(K)$. Bis auf Identifizierung (via π) gibt es also eine Körpererweiterung E_1/K, in der jedes Polynom $f \in K[T]$ vom Grad ≥ 1 ein Nullstelle besitzt.

Induktiv konstruiert man Körpererweiterungen

$$E_1 \subseteq E_2 \subseteq E_3 \subseteq \ldots,$$

so dass jedes Polynom $f \in E_n[T]$ vom Grad ≥ 1 eine Nullstelle in E_{n+1} besitzt. Definiere dann L als die Vereinigung $\bigcup_{n \geq 1} E_n$. Dies ist offenbar wieder ein Körper, und jedes Polynom $f \in L[T]$ vom Grad ≥ 1 hat eine Nullstelle in L. □

FOLGERUNG 8.4. *Sei K ein Körper. Dann gibt es eine algebraische Körpererweiterung L/K, wobei L algebraisch abgeschlossen ist.*

BEWEIS. Sei E/K eine Körpererweiterung, so dass E algebraisch abgeschlossen ist. Sei L die Vereinigung aller Teilerweiterungen, die algebraisch über K sind, also (in der Notation von Satz 3.6) $L = \overline{K}$. Dann ist L algebraisch über K. Sei $f \in L[T]$ vom Grad ≥ 1. Dann hat f eine Nullstelle $\alpha \in E$, und nach Satz 3.6 ist α ist algebraisch über L. Ebenfalls nach Satz 3.6 ist α auch algebraisch über K. Es folgt $\alpha \in L$. □

DEFINITION 8.5. Sei K ein Körper. Ein algebraisch abgeschlossener Körper L, so dass L/K algebraisch ist, heißt ein algebraischer Abschluss von K. Wir schreiben dafür auch $\overline{K}$.

Wir zeigen nun die Eindeutigkeit eines algebraischen Abschlusses (bis auf K-Isomorphie).

LEMMA 8.6. *Sei $\sigma\colon K \to L$ ein injektiver Körperhomomorphismus von K in einen algebraisch abgeschlossenen Körper L. Sei $E = K(\alpha)$, wobei α algebraisch über K ist mit*

Minimalpolynom $f \in K[T]$. Dann ist die Anzahl der möglichen Fortsetzungen von σ auf $K(\alpha)$ gleich der Anzahl der verschiedenen Nullstellen von $\sigma^*(f)$ in L.

BEWEIS. Sei β eine Nullstelle von $\sigma^*(f)$ in L. Sei $x = \sum_{i=0}^{n-1} a_i\alpha^i \in K(\alpha)$. Definiere $\overline{\sigma}(x) \stackrel{def}{=} \sum_{i=0}^{n} \sigma(a_i)\beta^i$. Dies definiert einen injektiven Körperhomomorphismus $\overline{\sigma}\colon K(\alpha) \to L$ mit $\overline{\sigma}_{|K} = \sigma$ (wie im Beweis von Satz 7.2). Für jede andere Nullstelle β' von $\sigma^*(f)$ in L erhält man analog eine weitere Fortsetzung. Sei umgekehrt $\tau\colon K(\alpha) \to L$ eine Fortsetzung von σ. Dann ist $\beta = \tau(\alpha) \in L$, und $\sigma^*(f)(\beta) = \tau(f(\alpha)) = \tau(0) = 0$, also ist β eine Nullstelle von $\sigma^*(f) \in L[T]$. Ferner gilt für $x = \sum_{i=0}^{n-1} a_i\alpha^i \in K(\alpha)$ auch

$$\tau(x) = \sum_{i=0}^{n-1} \tau(a_i)(\tau(\alpha))^i = \sum_{i=0}^{n-1} \sigma(a_i)\beta^i = \overline{\sigma}(x).$$

□

SATZ 8.7. *Sei E/K eine algebraische Erweiterung, sei $\sigma\colon K \to L$ ein injektiver Körperhomomorphismus in einen algebraisch abgeschlossenen Körper L. Dann gibt es eine Fortsetzung von σ auf E.*

BEWEIS. Sei S die Menge aller Paare (F, τ), wobei F ein Zwischenkörper von E/K ist und τ eine Fortsetzung von σ auf F. Für zwei solcher Paare (F, τ) und (F', τ') definiere $(F, \tau) \leq (F', \tau')$ falls $F \subseteq F'$ gilt und $\tau'_{|F} = \tau$. Es gilt $S \neq \emptyset$. Diese Menge ist induktiv geordnet, d. h. ist $\{(F_i, \tau_i)\}$ eine total geordnete Teilmenge, so sei $F = \cup_i F_i$ und definiere τ auf F, so dass es auf F_i gleich τ_i ist. Dies ist eine obere Schranke für die total geordnete Teilmenge. Man kann dann Zorn's Lemma anwenden, und erhält damit, dass S ein maximales Element (F, τ) enthält. Wir zeigen $F = E$. Andernfalls gäbe es ein $x \in E \setminus F$. Man kann nach dem vorherigen Lemma τ fortsetzen auf $F(x) \supsetneq F$, im Widerspruch zur Maximalität von (F, τ). □

FOLGERUNG 8.8. *Sei K ein Körper, und seien L und L' zwei algebraische Abschlüsse von K. Dann gibt es einen K-Isomorphismus $\sigma\colon L \stackrel{\sim}{\to} L'$.*

BEWEIS. Da L/K algebraisch ist, gibt es nach dem vorherigen Satz eine Fortsetzung $\sigma\colon L \to L'$ von $i\colon K \to L'$, $i(x) = x$ für alle $x \in K$. Es ist nur zu zeigen, dass σ surjektiv ist. Es ist aber das Bild $\sigma(L) \simeq L$ algebraisch abgeschlossen, und L' ist algebraisch über $\sigma(L)$. Also folgt $\sigma(L) = L'$. □

KAPITEL VI

Galoistheorie

Lernziele:

- Den Hauptsatz der Galoistheorie samt seiner genauen Voraussetzungen kennen und verstehen. Die dort vorkommenden Begriffe kennen und erläutern können.
- Die Begriffe Zerfällungskörper, galoissche, separable und normale Körpererweiterung kennen. Klassen von Beispielen kennen.
- Eine Hand voll Beispiele von galoisschen bzw. nicht-galoisschen Körpererweiterungen und deren Galoisgruppen kennen.
- Die Sätze von Artin und des primitiven Elements kennen und deren Relevanz für den Beweis des Hauptsatzes verstehen.
- Die Klassifikation endlicher Körper.
- Das ausführliche Beispiel am Ende des Kapitels verstehen.

1. Die Galoisgruppe einer Körpererweiterung

DEFINITION 1.1 (Galoisgruppe). Sei L/K eine Körpererweiterung. Die Menge aller K-Automorphismen $\sigma\colon L \to L$ ist ein Gruppe, wobei die Verknüpfung durch Komposition von Abbildungen gegeben ist. Diese Gruppe heißt die Galoisgruppe der Körpererweiterung L/K und wird mit $\mathrm{Gal}(L/K)$ bezeichnet.

LEMMA 1.2. *Sei L/K und L'/K' Körpererweiterungen und $i\colon K \to K'$ ein Isomorphismus. Sei $\sigma\colon L/K \to L'/K'$ ein Isomorphismus von Erweiterungen. Ist $f \in K[T]$ und $x \in L$ eine Nullstelle von f, so ist $\sigma(x)$ eine Nullstelle von $i^*(f)$.*

BEWEIS. Sei $f = \sum_{j=0}^{n} a_j T^j$. Dann gilt

$$i^*(f)(\sigma(x)) = \sum_{j=0}^{n} i(a_j)(\sigma(x))^j = \sum_{j=0}^{n} \sigma(a_j)\sigma(x^j) = \sigma(\sum_{j=0}^{n} a_j x^j) = \sigma(f(x)) = \sigma(0) = 0.$$

□

SATZ 1.3. *Seien $K(x)/K$ und $K'(x')/K'$ einfache algebraische Körpererweiterungen und $i\colon K \to K'$ ein Isomorphismus. Sei $f \in K[T]$ dass Minimalpolynom von x über K, und es gelte, dass $i^*(f)$ dass Minimalpolynom von x' über K' ist. Dann ist die Anzahl der Fortsetzungen $\sigma\colon K(x) \to K'(x')$ von i gleich der Anzahl der verschiedenen Nullstellen von f in $K(x)$.*

BEWEIS. (Folgt ähnlich wie in Lemma V.8.6.) Seien $x = x_1, x_2, \ldots, x_s$ die verschiedenen Nullstellen von f in $L = K(x)$. Nach Satz V.7.3 gibt es einen Isomorphismus $\sigma\colon K(x) \to K'(x')$, der i fortsetzt und mit $\sigma(x) = x'$. Nach dem vorherigen Lemma überführt σ die verschiedenen Nullstellen $x_1, \ldots, x_s$ von f in die verschiedenen Nullstellen $\sigma(x_1), \ldots, \sigma(x_s)$ von $i^*(f)$. Ist nun $\tau\colon K(x) \to K'(x')$ ein beliebiger Isomorphismus, der i fortsetzt, so gibt es wieder nach dem vorherigen Lemma ein j mit $\tau(x) = \sigma(x_j)$. Da $1, x, \ldots, x^{n-1}$ eine K-Basis von $K(x)$ ist und τ eine Fortsetzung von $i\colon K \to K'$, ist τ durch das Bild $\tau(x)$ schon eindeutig festgelegt. Es gibt für τ also genau s Möglichkeiten. □

Spezialisiert man auf $K = K'$, $x = x'$ und $i = 1_K$, so erhält man:

FOLGERUNG 1.4. *Sei $K(x)/K$ eine einfach algebraische Körpererweiterung, und sei $f \in K[T]$ das Minimalpolynom von x über K. Dann ist die Ordnung von* $\mathrm{Gal}(K(x)/K)$ *gleich der Anzahl der verschiedenen Nullstellen von f in $K(x)$. Insbesondere gilt*

$$|\operatorname{Gal}(K(x)/K)| \leq \operatorname{grad}(f) = [K(x) : K].$$

Es wird ein wichtiges Ziel sein, diese Aussage auf beliebige endliche Körpererweiterungen zu verallgemeinern.

BEMERKUNG 1.5. Die vorherige Aussage (und ihr Beweis) liefert ein Konstruktionsverfahren für $\mathrm{Gal}(K(x)/K)$; die Elemente von $\mathrm{Gal}(K(x)/K)$ korrespondieren mit den (verschiedenen) Nullstellen von f in $K(x)$; sind $x_1, \ldots, x_s \in K(x)$ die verschiedenen Nullstellen von f in $K(x)$, so induziert die Festsetzung $\sigma_i(x) = x_i$ ein eindeutig bestimmtes Element von $\mathrm{Gal}(K(x)/K)$.

BEISPIELE 1.6. (1) Betrachte $\mathbb{C}/\mathbb{R}$. Es ist $\mathbb{C} = \mathbb{R}(i)$. Das Minimalpolynom $f = T^2 + 1$ von i über $\mathbb{R}$ hat die Nullstellen i und $-i$ (die beide in $\mathbb{R}(i)$ liegen). Es gibt also die Möglichkeiten $i \mapsto i$ und $i \mapsto -i$. Dies liefert die $\mathbb{R}$-Automorphismen $1_{\mathbb{C}}$ (die Identität) und τ definiert durch $\tau(a + bi) = a - bi$ (es ist also τ die komplexe Konjugation). $\mathrm{Gal}(\mathbb{C}/\mathbb{R}) = \{1, \tau\} = \langle\tau\rangle$.

(2) Betrachte $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$. Hierbei bezeichnet $\sqrt[3]{2}$ die eindeutig bestimmte positive reelle dritte Wurzel aus 2. Die komplexen Nullstellen des Minimalpolynoms $T^3 - 2$ von $\alpha = \sqrt[3]{2}$ über $\mathbb{Q}$ sind $\alpha, e^{2\pi i/3}\alpha, e^{4\pi i/3}\alpha$. Wegen $\mathbb{Q}(\sqrt[3]{2}) \subseteq \mathbb{R}$ liegt davon nur α in $\mathbb{Q}(\sqrt[3]{2})$. Also besteht $\mathrm{Gal}(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q})$ nur aus dem neutralen Element.

(3) Betrachte $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}$. Die komplexen Nullstellen des Minimalpolynoms $T^4 - 2$ von $\alpha = \sqrt[4]{2}$ über $\mathbb{Q}$ sind $\alpha, i\alpha, -\alpha, -i\alpha$. Davon sind nur α und $-\alpha$ in $\mathbb{Q}(\sqrt[4]{2})$. Also besteht $\mathrm{Gal}(\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q})$ aus dem neutralen Element und dem $\mathbb{Q}$-Automorphismus σ der α auf $-\alpha$ schickt; dieser ist auf beliebigen Elementen von $\mathbb{Q}(\sqrt[4]{2})$ definiert durch

$$\sigma(a + b\alpha + c\alpha^2 + d\alpha^3) = a - b\alpha + c\alpha^2 - d\alpha^3.$$

(4) Betrachte $\mathbb{Q}(i, \sqrt[4]{2})/\mathbb{Q}(i)$. (Übung.) Es ist $f = T^4 - 2$ ein Polynom über $\mathbb{Q}(i)$, welches $\sqrt[4]{2}$ als Nullstelle hat. Wegen

$$8 = 2 \cdot 4 = [\mathbb{Q}(i, \sqrt[4]{2}) : \mathbb{Q}(\sqrt[4]{2})] \cdot [\mathbb{Q}(\sqrt[4]{2}) : \mathbb{Q}] = [\mathbb{Q}(i, \sqrt[4]{2}) : \mathbb{Q}] = [\mathbb{Q}(i, \sqrt[4]{2}) : \mathbb{Q}(i)] \cdot [\mathbb{Q}(i) : \mathbb{Q}]$$

folgt $[\mathbb{Q}(i, \sqrt[4]{2}) : \mathbb{Q}(i)] = 4$, und damit ist f auch das Minimalpolynom von $\sqrt[4]{2}$ über $\mathbb{Q}(i)$. Alle Nullstellen $\alpha, i\alpha, -\alpha, -i\alpha$ (mit $\alpha = \sqrt[4]{2}$) liegen in $\mathbb{Q}(i, \sqrt[4]{2})$. Sei σ der $\mathbb{Q}(i)$-Automorphismus von $\mathbb{Q}(i, \sqrt[4]{2})$, der durch $\sigma\colon \alpha \mapsto i\alpha$ bestimmt ist. Dann gilt $\sigma^2\colon \alpha \mapsto -\alpha$, $\sigma^3\colon \alpha \mapsto -i\alpha$ und $\sigma^4 = 1_L$. Es ist also $\mathrm{Gal}(\mathbb{Q}(i, \sqrt[4]{2})/\mathbb{Q}(i))$ zyklisch von der Ordnung 4, erzeugt von σ.

DEFINITION 1.7 (Fixkörper). Sei L ein Körper und G eine Gruppe von Automorphismen $\sigma\colon L \to L$. Dann ist $L^G = \{x \in L \mid \sigma(x) = x \text{ für alle } \sigma \in G\}$ ein Teilkörper von L, der Fixkörper von G.

Insbesondere: Ist L/K eine Körpererweiterung und $U \subseteq \mathrm{Gal}(L/K)$ eine Untergruppe der Galoisgruppe, so ist der Fixkörper L^U ein Zwischenkörper von L/K.

BEMERKUNG 1.8. Sei L/K eine Körpererweiterung mit Galoisgruppe $G = \mathrm{Gal}(L/K)$. Es gilt $L^G \supseteq K$ und $\mathrm{Gal}(L/L^G) = \mathrm{Gal}(L/K)$, wie man leicht nachrechnet.

DEFINITION 1.9 (Galoiserweiterung). Eine endliche Körpererweiterung L/K heißt galoissch, oder Galoiserweiterung, falls $L^{\mathrm{Gal}(L/K)} = K$ gilt.

BEISPIELE 1.10. (1) $\mathbb{C}/\mathbb{R}$. Sei $G = \mathrm{Gal}(\mathbb{C}/\mathbb{R})$. Es ist $\mathbb{C}^G = \{z \in \mathbb{C} \mid z = \bar{z}\} = \mathbb{R}$. Also ist $\mathbb{C}/\mathbb{R}$ galoissch.

(2) Es ist $G = \{1\}$ die Galoisgruppe von $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$. Also gilt $\mathbb{Q}(\sqrt[3]{2})^G = \mathbb{Q}(\sqrt[3]{2}) \neq \mathbb{Q}$, d. h. diese Körpererweiterung ist nicht galoissch.

(3) Es ist $G = \{1, \sigma\}$ (wie oben beschrieben) die Galoisgruppe von $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}$. Es ist dann

$$\mathbb{Q}(\sqrt[4]{2})^G = \{x \mid \sigma(x) = x\} = \{a + c\sqrt{2} \mid a, c \in \mathbb{Q}\} = \mathbb{Q}(\sqrt{2}),$$

also ist diese Körpererweiterung nicht galoissch.

(4) $\mathbb{Q}(i, \sqrt[4]{2})/\mathbb{Q}(i)$ ist galoissch. (Übung.) Wir haben eben schon gezeigt, dass die Galoisgruppe G zyklisch ist mit Erzeuger $\sigma\colon \alpha \mapsto i\alpha$. Es folgt weiter:

$$L^G = \{x \in \mathbb{Q}(i, \sqrt[4]{2}) \mid \sigma(x) = x\}.$$

Jedes Element $x \in \mathbb{Q}(i, \sqrt[4]{2})$ lässt sich schreiben als

$$x = x_0 + x_1\alpha + x_2\alpha^2 + x_3\alpha^3$$

mit eindeutige x_0, x_1, x_2, $x_3 \in \mathbb{Q}(i)$. Damit ist

$$\sigma(x) = x_0 + x_1 i\alpha - x_2\alpha^2 - x_3 i\alpha^3,$$

Es folgt damit $x \in L^G$ genau dann, wenn $x_1 = ix_1$, $x_2 = -x_2$ und $x_3 = -ix_3$, also, wenn $x = x_0 \in \mathbb{Q}(i)$ gilt. Also $L^G = \mathbb{Q}(i)$. Damit ist die Körpererweiterung $\mathbb{Q}(i, \sqrt[4]{2})/\mathbb{Q}(i)$ galoissch.

2. Der Hauptsatz der Galoistheorie (Formulierung)

Sei L/K eine Körpererweiterung mit Galoisgruppe $G = \mathrm{Gal}(L/K)$. Bezeichne mit $\mathcal{Z}$ die Menge aller Zwischenkörper M von L/K, also so, dass $K \subseteq M \subseteq L$ ein Körperturm ist. Bezeichne mit $\mathcal{U}$ die Menge aller Untergruppen von G. Beides sind geordnete Mengen bzgl. der Inklusion.

Wir betrachten folgende Abbildungen:

$$\Phi\colon \mathcal{Z} \to \mathcal{U},\ M \mapsto \mathrm{Gal}(L/M).$$

$$\Psi\colon \mathcal{U} \to \mathcal{Z},\ U \mapsto L^U.$$

Satz 2.1 (Hauptsatz der Galoistheorie). *Sei L/K eine Galoiserweiterung vom Grad $n = [L : K]$ und mit Galoisgruppe $G = \mathrm{Gal}(L/K)$. Dann gilt:*

(1) *Es ist $|G| = n$.*
(2) *Die Abbildungen*

$$\Phi\colon \mathcal{Z} \to \mathcal{U},\ M \mapsto \mathrm{Gal}(L/M)$$

und

$$\Psi\colon \mathcal{U} \to \mathcal{Z},\ U \mapsto L^U$$

sind ordnungs-umkehrend und zueinander invers.
(3) *Für jeden Zwischenkörper M von L/K ist die Körpererweiterung L/M galoissch; dagegen ist M/K galoissch genau dann, wenn $\Phi(M) = \mathrm{Gal}(L/M) \subseteq G$ ein Normalteiler ist. In diesem Fall hat man eine kanonische Isomorphie von Gruppen*

$$\mathrm{Gal}(M/K) \simeq \frac{\mathrm{Gal}(L/K)}{\mathrm{Gal}(L/M)}.$$

Bemerkung 2.2. Die Bedingung im Hauptsatz, dass die Körpererweiterung galoissch ist, ist offenbar notwendig. Denn wäre $L^G \supsetneq K$, so würde $K \in \mathcal{Z}$ nicht im Bild von Ψ liegen.

Plan: Auf dem Weg zum Beweis des Hauptsatzes werden wir weitere wichtige Ergebnisse beweisen. Es werden die Begriffe *normale* und *separable* Körpererweiterung eingeführt. Es wird sich dann zeigen:

Satz 2.3. *Sei L/K eine endliche Körpererweiterung. Dann sind äquivalent:*

(1) *L/K ist galoissch.*
(2) *$|\mathrm{Gal}(L/K)| = [L : K]$.*
(3) *L/K ist normal und separabel.*

Zwei herausragende Sätze werden die Hauptachsen der Beweise des Hauptsatzes und von Satz 2.3 bilden:

- Der Satz vom primitiven Element. *Jede separable Erweiterung ist einfach.*
- Der Satz von Artin. *Sei L ein Körper und G eine endliche Gruppe von Automorphismen von L. Dann ist die Erweiterung L/L^G normal und separabel mit Galoisgruppe $\mathrm{Gal}(L/L^G) = G$ und mit $[L : L^G] = |G|$.*

3. Zerfällungskörper

DEFINITION 3.1 (Zerfällungskörper). Sei K ein Körper und $f \in K[T]$. Ein Erweiterungskörper L von K heißt ein Zefällungskörper von f über K, falls

(1) f zerfällt über L in Linearfaktoren, d. h. $f = a(T-a_1)\cdot\ldots\cdot(T-a_n)$ mit $a \in K^\times$ und $a_1, \ldots, a_n \in L$; und
(2) es gilt $L = K(a_1, \ldots, a_n)$.

Die zweite Bedingung ist offenbar gleichwertig dazu, dass es in L keinen kleineren Körper gibt, über dem f zerfällt. Außerdem gilt offenbar $[L : K] < \infty$.

BEISPIEL 3.2. Sei $f = T^3 - 2 \in \mathbb{Q}[T]$. Die komplexen Nullstellen von f sind $\sqrt[3]{2}$, $\sqrt[3]{2}e^{2\pi i/3}$, $\sqrt[3]{2}e^{4\pi i/3}$. Ein Zerfällungskörper von f über $\mathbb{Q}$ ist gegeben durch

$$L = \mathbb{Q}(\sqrt[3]{2}, \sqrt[3]{2}e^{2\pi i/3}, \sqrt[3]{2}e^{4\pi i/3}) = \mathbb{Q}(\sqrt[3]{2}, e^{2\pi i/3}).$$

SATZ 3.3 (Existenz von Zerfällungskörpern). *Sei K ein Körper und $f \in K[T]$. Dann gibt es einen Zerfällungskörper L von f über K.*

BEWEIS. 1. Beweis: Über dem algebraischen Abschluss zerfällt f komplett in Linearfaktoren, $f = a\prod_{i=1}^n (T - a_i)$. Dann ist $L \stackrel{def}{=} K(a_1, \ldots, a_n)$ ein Zerfällungskörper von f über K.

2. Beweis: Man kann den Existenzsatz des algebraischen Abschlusses meiden. Stattdessen beweist man per Induktion nach $n = \mathrm{grad}(f)$. Für $n = 1$ ist nichts zu zeigen. Sei $n > 1$. Es hat f einen irreduziblen Faktor $f_1 \in K[T]$. Nach Satz 2.1 gibt es einen Erweiterungskörper $L_1 = K(a_1)$ von K mit $f_1(a_1) = 0$. In $L_1[T]$ gilt dann $f = (T - a_1)g$. Nach Induktionsvoraussetzung hat g einen Zerfällungskörper L/L_1. Dann ist offenbar L ein Zerfällungskörper von f über K. □

SATZ 3.4. *Sei $i\colon K \to K'$ ein Körperisomorphismus, sei $f \in K[T]$. Sei L ein Zerfällungskörper von f über K, sei L' ein Zerfällungskörper von $f' = i^*(f)$ über K'. Dann gibt es einen Isomorphismus von Erweiterungen $\sigma\colon L/K \to L'/K'$ mit $\sigma_{|K} = i$. Es gibt $\leq [L : K]$ solcher Isomorphismen. Zerfällt f in L in paarweise verschiedene Nullstellen, so ist die Anzahl $= [L : K]$.*

BEWEIS. Existenz. Induktion nach $n = \mathrm{grad}(f)$. Für $n = 1$ ist nichts zu zeigen. Sei $n > 1$. Es gibt einen irreduziblen Faktor f_1 von f in $K[T]$. Dann ist $f_1' = i^*(f_1)$ ein irreduzibler Faktor von f'. Sei x eine Nullstelle von f_1 in L und x' eine Nullstelle von $i^*(f_1)$ in L'. Nach Satz V.7.3 gibt es einen Isomorphismus $\sigma_1\colon K(x) \to K'(x')$, der i fortsetzt und x auf x' abbildet. Schreibe $f = (T - x)g$ und $f' = (T - x')g'$ mit $f \in K(x)[T]$ und $f' \in K'(x')[T]$. Dann gilt $f' = i^*(f) = \sigma_1^*(f) = \sigma_1^*(T - x)\sigma_1^*(g) = (T - x')\sigma_1^*(g)$, also $g' = \sigma_1^*(g)$. Offenbar ist L Zerfällungskörper von g über $K(x)$ und L' Zerfällungskörper von g' über $K(x')$. Man wendet nun die Induktionsvoraussetzung auf g an.

Anzahl. Auch dies beweist man per Induktion, mit Lemma 1.2 und Satz 1.4, indem man $L/K(x)$ und $K(x)/K$ betrachtet. □

Spezialisiert man auf $K = K'$ und $i = 1_K$, so erhält man:

FOLGERUNG 3.5 (Eindeutigkeit des Zerfällungskörpers). *Seien L und L' Zerfällungskörper des Polynoms f über K. Dann gibt es einen K-Isomorphismus $\sigma\colon L \to L'$.* □

DEFINITION 3.6. Sei L/K eine Körpererweiterung und $f \in K[T]$. Sei $a \in L$ eine Nullstelle von f. Die Vielfachheit e von a in L ist die natürliche Zahl $e \geq 1$ mit $f = (T-a)^e \cdot g$, wobei $g \in L[T]$ gilt mit $g(a) \neq 0$. Die Nullstelle a heisst einfach, falls $e = 1$ gilt.

ÜBUNG 3.7. Sei K ein Körper. Definiere $D\colon K[T] \to K[T]$ durch

$$\sum_{i=0}^{n} a_i T^i \mapsto \sum_{i=1}^{n} i a_i T^{i-1}.$$

Schreibe $D^n = D \circ D \circ \cdots \circ D$ (n-mal). Man zeige:

(a) D ist K-linear.
(b) $D(fg) = fD(g) + D(f)g$ für alle f, $g \in K[T]$.
(c) Sei $0 \neq f \in K[T]$, sei a eine Nullstelle von f. Die Vielfachheit von a ist die kleinste natürliche Zahl $n \geq 1$ mit $D^n(f)(a) \neq 0$.
(d) Ein Polynom $0 \neq f \in K[T]$ hat in beliebigen Erweiterungskörpern von K nur einfache Nullstellen genau dann, wenn $\mathrm{ggT}(f, D(f)) = 1$ gilt.
(e) Sei $\mathbb{Q} \subseteq K \subset L$ ein Körper. Sei $x \in L$ algebraisch über K mit Minimalpolynom $f \in K[T]$. Dann ist x eine einfache Nullstelle von f.

4. Endliche Körper

Auf dem Weg zum Beweis der Hauptsatzes der Galoistheorie legen wir eine kurze Pause ein und nutzen unsere bisherigen Techniken, um als Anwendung die endlichen Körper vollständig zu beschreiben.

DEFINITION 4.1. Sei K ein Körper. Gibt es keine ganze Zahl $n \geq 1$ mit $n \cdot 1_K = 0$, so ist die Charakteristik von K gleich 0, also $\mathrm{Char}(K) = 0$. Gibt es eine solche Zahl n, so ist die kleinste solche Zahl eine Primzahl p, und diese ist dann die Charakteristik von K. Im ersten Fall ist der Primkörper $\Pi(K)$, der kleinste in K enthaltene Teilkörper, isomorph zu $\mathbb{Q}$, im zweiten Fall ist es ein Körper mit p Elementen. (Vgl. Übungen.)

Sei K ein Körper und $p = \mathrm{Char}(K)$ eine Primzahl. Die Abbildung $\mu\colon \mathbb{Z} \to \Pi(K)$, $n \mapsto n \cdot 1_K$ ist offenbar ein Ringhomomorphismus mit $\mathrm{Kern}(\mu) = p\mathbb{Z}$. Der Homomorphiesatz für Ringe liefert nun:

PROPOSITION 4.2. *Sei K ein Körper von Primzahlcharakteristik p. Dann ist der Primkörper $\Pi(K)$ zum Restklassenkörper $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ isomorph.*

BEWEIS. Es ist $\mathbb{Z}/p\mathbb{Z} \xrightarrow{\sim} \mathrm{Bild}(\mu) \subseteq \Pi(K) \subseteq K$. Nach Lemma 1.10 ist $\mathbb{Z}/p\mathbb{Z}$ ein Körper, also auch $\mathrm{Bild}(\mu)$. Da der Primkörper $\Pi(K)$ der kleinste Teilkörper von K ist, folgt $\Pi(K) = \mathrm{Bild}(\mu)$. □

Die folgende Aussage hatten wir schon an früherer Stelle bewiesen.

SATZ 4.3. *Sei K ein endlicher Körper. Dann gibt es eine Primzahl p und eine natürliche Zahl $n \geq 1$ mit $|K| = p^n$.*

BEWEIS. Die Charakteristik von K ist eine Primzahl p, und es ist $n \overset{def}{=} [K : \Pi(K)] < \infty$. D. h. K ist ein n-dimensionaler Vektorraum über dem Körper $\Pi(K) = \mathbb{F}_p$, hat also p^n Elemente. □

SATZ 4.4. *Sei K ein Körper, und G eine endliche Untergruppe der Einheitengruppe $E(K) = (K \setminus \{0\}, \cdot)$. Dann ist G zyklisch.*

BEWEIS. $G = E(K)$ ist eine abelsche Gruppe. Sei $n = |G|$. Dann gilt $x^n = 1$ für jedes $x \in G$. Sei $m \overset{def}{=} \min\{i \geq 1 \mid x^i = 1 \text{ für alle } x \in G\}$. Es gilt also $x^m = 1$ für jedes $x \in G$, d. h. jedes $x \in G$ ist Nullstelle des Polynoms $T^m - 1 \in \Pi(K)[T]$. Man hat also (mind.) n Nullstellen, andererseits hat es höchsten m Nullstellen. Es folgt $m = n$.

Zu zeigen ist noch, dass es ein $x \in G$ der Ordnung m gibt: Sei $m = p_1^{\alpha_1} \dots p_r^{\alpha_r}$ die Primfaktorzerlegung von m ($p_1, \dots, p_r$ paarweise verschieden prim, $\alpha_i \geq 1$). Wegen der Minimalität ist m ein Teiler des kgV's der Ordnungen aller Elemente von G, also gibt es zu jedem i ein $g_i \in G$, dessen Ordnung von $p_i^{\alpha_i}$ geteilt wird. Ist $k_i p_i^{\alpha_i} = |g_i|$, so hat $g_i^{k_i}$ die Ordnung $p_i^{\alpha_i}$. Das Element $g \stackrel{def}{=} g_1 g_2 \dots g_r$ hat dann die Ordnung $p_1^{\alpha_1} \dots p_r^{\alpha_r} = m$, was zu zeigen war. □

Satz 4.5. *Sei K ein endlicher Körper mit $q = p^n$ Elementen (p prim). Dann ist K ein Zerfällungskörper des Polynoms $T^q - T \in \mathbb{F}_p[T]$.*

Beweis. Ist $x \in K$, $x \neq 0$, also $x \in E(K)$, so gilt nach dem kleinen Satz von Fermat $x^{q-1} = 1$, damit $x^q = x$. Letzteres gilt auch für $x = 0$. Die q verschiedenen Elemente aus K sind also gerade die Nullstellen $x_1, \dots, x_q$ des Polynoms $T^q - T \in \Pi(K)[T]$. Da sicherlich auch $K = \Pi(K)(x_1, \dots, x_q)$ gilt, ist K der Zerfällungskörper des Polynoms $T^q - T$ über $\Pi(K) \simeq \mathbb{F}_p$. □

Satz 4.6. *Sei $q = p^n$ (mit p prim und $n \geq 1$).*

(1) *Es gibt einen Körper K mit q Elementen.*
(2) *Je zwei Körper mit q Elementen sind isomorph.*

Beweis. (1) Sei K Zerfällungskörper des Polynoms $f = T^q - T \in \mathbb{F}_p[T]$. Die Menge N der Nullstellen von f in K bildet einen Teilkörper von K: Denn sind $x, y \in K$ Nullstellen von f, so gilt wegen $p \mid \binom{q}{i}$ für $1 \leq i \leq q-1$

$$(x+y)^q = \sum_{i=0}^{q} \binom{q}{i} x^i y^{q-i} = x^q + y^q = x + y,$$

$$(xy)^q = x^q y^q = xy,$$

und ebenso für $x \neq 0$, $(x^{-1})^q = (x^q)^{-1} = x^{-1}$, und $(-x)^q = -x$ (unterscheide die Fälle p gerade bzw. ungerade). Also ist N ein Teilkörper von K. Da aber f schon über N in Linearfaktoren zerfällt, gilt $N = K$. Damit besteht K aus den Nullstellen von f. Nun ist $D(f) = qT^{q-1} - 1 = -1$, und daher ist $\mathrm{ggT}(f, D(f)) = 1$ und es hat f nur einfache Nullstellen, vgl. Übung 3.7. Damit hat f genau q verschiedene Nullstellen, und K ist ein Körper mit q Elementen.

(2) Folgt aus Satz 4.5 und der Eindeutigkeit des Zerfällungskörpers (genauer Satz 3.4). □

Ein Körper mit $q = p^n$ Elementen wird auch mit $\mathbb{F}_q$ bezeichnet.

5. Separabilität

Definition 5.1. Ein irreduzibles Polynom $f \in K[T]$ heißt separabel, falls es im algebraischen Abschluss $\overline{K}$ (oder in seinem Zerfällungskörper) nur einfache Nullstellen hat. Dabei heißt eine Nullstelle $a \in \overline{K}$ einfach, falls $f = (T-a)g$ in $\overline{K}[T]$ und $g(a) \neq 0$ gilt. Ein beliebiges Polynom $f \in K[T]$ heißt separabel, wenn jeder seiner irreduziblen Faktoren separabel ist.

Definition 5.2. Sei L/K eine Körpererweiterung, sei $x \in L$ algebraisch über K. Dann heißt x separabel über K, falls das Minimalpolynom von x über K separabel ist. Eine endliche Körpererweiterung L/K heißt separabel, falls jedes $x \in L$ separabel über K ist.

Lemma 5.3. *Sei K ein Körper und $f \in K[T]$ irreduzibel. Genau dann hat f in jedem Erweiterungskörper von K nur einfache Nullstellen, wenn $D(f) \neq 0$ gilt.*

BEWEIS. (Vgl. Übung 3.7.) Gilt $D(f) \neq 0$, muss wegen $\operatorname{grad}(D(f)) \leq \operatorname{grad}(f) - 1$ der ggT von f und $D(f)$ eine Einheit sein. Nach Übung 3.7 hat f in jedem Erweiterungskörper von K nur einfache Nullstellen. Ist dies umgekehrt der Fall, so ist nach Übung 3.7. der ggT von f und $D(f)$ eine Einheit, also muss $D(f) \neq 0$ gelten. □

SATZ 5.4. *Eine endliche Körpererweiterung L/K von einem Körper K der Charakteristik null ist separabel.*

BEWEIS. Sei $x \in L$ und $f = T^n + \sum_{i=0}^{n-1} a_i T^i$ das Minimalpolynom von x über K. Dann ist $D(f) = n \cdot T^{n-1} + \cdots \neq 0$. Also ist x separabel über K. □

LEMMA 5.5. *Sei $K \subseteq F \subseteq L$ ein Körperturm. Ist L/K separabel, so sind auch L/F und F/K separabel.*

BEWEIS. Sei L/K separabel. Sei $x \in L$. Das Minimalpolynom g von x über F ist (in $F[T]$) ein Teiler des Minimalpolynoms f von x über K. Mit f hat dann aber erst recht g nur einfache Nullstellen. Trivialerweise ist F/K separabel. □

SATZ 5.6. *Sei L/K eine endliche Körpererweiterung. Sei $i\colon K \to \overline{K}$ ein injektiver Körperhomomorphismus (in den algebraischen Abschluß von K). Dann gibt es mindestens eine und höchstens $[L : K]$ verschiedene Fortsetzungen $\sigma\colon L \to \overline{K}$. Es gibt genau $[L : K]$ Fortsetzungen genau dann, wenn L/K eine separable Erweiterung ist.*

BEWEIS. Wir betrachten zunächst den separablen Fall. Per Induktion nach $n = [L : K]$. Für $n = 1$ ist die Aussage klar. Sei $n > 1$. Sei $\alpha \in L$, aber $\alpha \notin K$. Das Minimalpolynom f von α über K hat in $\overline{K}$ nur einfache Nullstellen. Ist $L = K(\alpha)$, so hat f genau n verschiedene Nullstellen und die Aussage folgt aus Lemma V.8.6. Gilt $L \neq K(\alpha)$, so sind $L/K(\alpha)$ und $K(\alpha)/K$ nach dem vorherigen Lemma separabel und jeweils vom Grad $< n$. Nun hat per Induktionsvoraussetzung (bzw. nach Lemma V.8.6) i die Fortsetzungen $\tau_1, \ldots, \tau_s\colon K(\alpha) \to \overline{K} = \overline{K(\alpha)}$, wobei $s = [K(\alpha) : K]$. Jedes τ_i hat nun per Induktionsannahme $[L : K(\alpha)]$ viele Fortsetzungen auf L, also gibt es insgesamt $[L : K(\alpha)] \cdot [K(\alpha) : K] = [L : K]$ viele.

Um im allgemeinen Fall $\leq$ (und ≥ 1) zu bekommen geht man genauso per Induktion vor. Im nicht-separablen Fall findet man ein Element $\alpha \in L$, $\alpha \notin K$, welches nicht separabel über K ist. Dann hat i nach Lemma V.8.6 $< [K(\alpha) : K]$ viele Fortsetzungen auf $K(\alpha)$, und daher $< [L : K]$ Fortsetzungen auf L. □

Erinnerung: Für eine algebraische Körpererweiterung L/K heisst $\alpha \in L$ ein primitives Element, falls $L = K(\alpha)$ gilt.

SATZ 5.7 (Satz vom primitiven Element). *Sei L/K eine endliche Körpererweiterung.*

(1) *Es gibt ein $\alpha \in L$ mit $L = K(\alpha)$ genau dann, wenn es nur endlich viele Zwischenkörper von L/K gibt.*
(2) *Ist L/K separabel, so gibt es ein $\alpha \in L$ mit $L = K(\alpha)$.*

BEWEIS. (1) "⇒" Gelte $L = K(\alpha)$. Sei F ein Zwischenkörper von L/K. Sei $f = \sum_{i=0}^{n} a_i T^i$ das Minimalpolynom von α über F und setze $E = K(a_0, a_1, \ldots, a_n)$. Dann gilt $F = E$: Denn $F \supseteq E$ ist klar. Es ist f offenbar irreduzibel auch über E, und ist daher das Minimalpolynom von x über E. Es ist $L = F(\alpha)$ und $L = E(\alpha)$, und es folgt $[L : F] = \operatorname{grad}(f) = [L : E]$, und aus dem Gradsatz folgt dann $F = E$. – Nun ist f ein Teiler des Minimalpolynoms von α über K. Also gibt es für E wie oben nur endlich viele Möglichkeiten.

"⇐" Es habe L/K nur endlich viele Zwischenkörper. Ist K ein endlicher Körper, so auch L, und L/K ist einfach da die Einheitengruppe $E(L)$ zyklisch ist. Also kann man im folgenden annehmen, dass K unendlich ist. Seien $\alpha, \beta \in L$. Durchläuft c die unendlich

vielen Elemente aus K, gibt es nur endlich viele verschiedene Körper $K(\alpha + c\beta)$. Es gibt also c_1, $c_2 \in K$ mit $c_1 \neq c_2$ und

$$F \stackrel{def}{=} K(\alpha + c_1\beta) = K(\alpha + c_2\beta).$$

Das bedeutet, dass $\alpha + c_1\beta$ und $\alpha + c_2\beta$ im selben Körper F liegen, also auch $(c_1 - c_2)\beta \in F$, damit $\beta \in F$, und dann auch $\alpha \in F$. Es folgt $K(\alpha, \beta) = F = K(\alpha + c_1\beta)$, also wird $K(\alpha, \beta)$ schon von einem Element erzeugt.

Allgemein ist L von der Form $K(a_1, \ldots, a_n)$. Per Induktion führt man dies aber auf den gerade behandelten Fall zweier Erzeuger zurück.

(2) Sei nun L/K separabel. Auch hier können wir annehmen, dass K ein unendlicher Körper ist, und wegen Lemma 5.5 per Induktion auch annehmen, dass $L = K(\alpha, \beta)$ gilt. Seien $\sigma_1, \ldots, \sigma_n \colon L \to \overline{K}$ die verschiedenen Fortsetzungen von 1_K auf L, wobei $n = [L : K]$ gilt (nach Satz 5.6). Betrachte das Polynom

$$f = \prod_{i \neq j} \big(\sigma_i(\alpha) + \sigma_i(\beta)T - \sigma_j(\alpha) - \sigma_j(\beta)T\big) \in \overline{K}[T].$$

Für $i \neq j$ gilt $\sigma_i \neq \sigma_j$, und da $L = K(\alpha, \beta)$, folgt $\sigma_i(\alpha) \neq \sigma_j(\alpha)$ oder $\sigma_i(\beta) \neq \sigma_j(\beta)$, also $f \neq 0$. Da K unendlich ist, gibt es ein $c \in K$ mit $f(c) \neq 0$. Also sind die Elemente $\sigma_i(\alpha + c\beta)$ verschieden ($i = 1, \ldots, n$), und Nullstellen des Minimalpolynoms von $\alpha + c\beta$ über K. Also gilt $n \leq [K(\alpha + c\beta) : K] \leq [L : K] = n$, also folgt $L = K(\alpha + c\beta)$. □

Satz 5.8 (Transitivität separabler Erweiterungen). *Sei $K \subseteq F \subseteq L$ ein Körperturm mit $[L : K] < \infty$. Sind L/F und F/K separabel, so ist auch L/K separabel.*

Beweis. Folgt mit dem Gradsatz aus Satz 5.6. □

6. Normalität

Definition 6.1. Eine endliche Körpererweiterung L/K heißt normal, falls für jedes (normierte) irreduzible Polynom $f \in K[T]$ gilt: Hat f eine Nullstelle $\alpha \in L$, so zerfällt f über L in Linearfaktoren.

Satz 6.2. *Sei L/K eine endliche Körpererweiterung. Die folgenden Aussagen sind äquivalent:*

(1) *L/K ist normal.*
(2) *L/K ist Zerfällungskörper eines Polynoms in $K[T]$.*

Beweis. (1)⇒(2) Sei L/K normal. Schreibe $L = K(\alpha_1, \ldots, \alpha_n)$. Für jedes $i = 1, \ldots, n$ sei f_i das Minimalpolynom von α_i über K. Sei $f = f_1 \ldots f_n$. Jedes f_i ist irreduzibel und zerfällt über L in Linearfaktoren, da L/K normal. Da L von den Nullstellen von f über K erzeugt wird, ist L ein Zerfällungskörper von f über K.

(2)⇒(1) Es sei L Zerfällungskörper eines Polynoms $f \in K[T]$. Sei $g \in K[T]$ irreduzibel, ohne Einschränkung normiert. Es habe g eine Nullstelle $\alpha \in L$. Sei $M \supseteq L$ ein Zerfällungskörper von fg über K. Sei β eine weitere Nullstelle von g in M. Sei $\gamma = \alpha$ oder $\gamma = \beta$. Dann gilt

$$[L(\gamma) : L] \cdot [L : K] = [L(\gamma) : K] = [L(\gamma) : K(\gamma)] \cdot [K(\gamma) : K].$$

Nun sind $K(\alpha)$ und $K(\beta)$ nach Satz V.7.2 K-isomorph. Außerdem ist $L(\gamma)$ offenbar ein Zerfällungskörper von f über $K(\gamma)$. Daher gibt es nach Satz 3.4 einen Isomorphismus von $L(\alpha)$ nach $L(\beta)$, der obigen K-Isomorphismus fortsetzt. Man bekommt $[L(\alpha) : K(\alpha)] = [L(\beta) : K(\beta)]$, was zusammen $[L(\alpha) : K] = [L(\beta) : K]$ und schließlich durch Kürzen $[L(\alpha) : L] = [L(\beta) : L]$ ergibt. Da $\alpha \in L$, folgt $1 = [L(\alpha) : L] = [L(\beta) : L]$, was aber $\beta \in L$ bedeutet. Also liegen alle Nullstellen von g in L. □

Folgerung 6.3. *Sei L/K eine endliche Körpererweiterung. Die folgenden Aussagen sind äquivalent:*

(1) *L/K ist normal und separabel.*
(2) *L ist Zerfällungskörper eines separablen Polynoms in $K[T]$.*

BEWEIS. (1)⇒(2) ergibt sich sofort aus dem vorherigen Satz und aus der Definition eines separablen Polynoms.

(2)⇒(1) Sei $L = K(\alpha_1, \ldots, \alpha_r)$ Zerfällungskörper eines separablen Polynoms in $f \in K[T]$, wobei die α_i die Nullstellen von f in L sind. Nach dem vorherigen Satz ist L/K normal. Jedes α_i ist Nullstelle eines irreduziblen Faktors f_i von f. Da f_i separabel über K ist, folgt dass jedes α_i separabel über K ist. Per Induktion und der Transitivität der Separabilität genügt es zu zeigen, dass $K(\alpha)/K$ separabel ist, wenn das Minimalpolynom von α über K separabel ist. Dies folgt aber aus Lemma V.8.6 und Satz 5.6. □

SATZ 6.4. *Sei L/K eine endliche Körpererweiterung. Äquivalent sind:*

(1) *L/K ist normal.*
(2) *Ist F/L eine Körpererweiterung und $\sigma\colon F \to F$ ein K-Automorphismus, so gilt $\sigma(L) \subseteq L$.*

BEWEIS. (1)⇒(2) Sei L/K normal, F/L eine Körpererweiterung und $\sigma \in \mathrm{Gal}(F/K)$. Sei $\alpha \in L$. Das Minimapolynom f von α über K zerfällt über L in Linearfaktoren. Da $\beta = \sigma(\alpha)$ auch eine Nullstelle von f ist, folgt $\sigma(\alpha) \in L$.

(2)⇒(1) Sei $g \in K[T]$ irreduzibel, und es habe g eine Nullstelle α in L. Ohne Einschränkung sei g normiert. Es ist L von der Form $L = K(x_1, \ldots, x_n)$. Dabei kann man annehmen, dass $x_1 = \alpha$ gilt. Für jedes $i = 1, \ldots, n$ sei f_i das Minimalpolynom von x_i über K; also $f_1 = g$. Setze $f = f_1 \cdot \ldots \cdot f_n$. Sei $F \supseteq L$ Zerfällungskörper von f über K.

Sei $\beta \in F$ eine weitere Nullstelle von g. Nach Satz V.7.2 gibt es einen K-Isomorphismus $i\colon K(\alpha) \to K(\beta)$ mit $i(\alpha) = \beta$. Da offenbar F auch Zerfällungskörper von f über $K(\alpha)$ und über $K(\beta)$ ist, gibt es nach Satz 3.4 einen (K-) Automorphismus $\sigma\colon F \to F$, der i fortsetzt. Nach Voraussetzung gilt dann $\sigma(L) \subseteq L$. Es folgt $\beta = i(\alpha) = \sigma(\alpha) \in L$, d. h. alle Nullstellen von g liegen schon in L. □

7. Der Satz von Artin

LEMMA 7.1. *Sei L/K eine algebraische Körpererweiterung, und es gebe eine natürliche Zahl $n \geq 1$, so dass jedes Element α von L separabel und vom Grad $\leq n$ über K ist. Dann gilt $[L : K] \leq n$.*

BEWEIS. Sei $\alpha \in L$ so dass $m = [K(\alpha) : K]$ maximal ist. Es gilt $m \leq n$. Behauptung: Es gilt $L = K(\alpha)$. Andernfalls gibt es ein $\beta \in L$ mit $\beta \notin K(\alpha)$. Dann ist $K(\alpha, \beta)$ eine endliche Körpererweiterung, die (trivialerweise) separabel ist. Nach dem Satz vom primitiven Element gibt es ein $\gamma \in L$ mit $K(\alpha, \beta) = K(\gamma)$. Es ist aber $[K(\gamma) : K] = [K(\alpha, \beta) : K(\alpha)] \cdot [K(\alpha) : K] > m$, Widerspruch. □

SATZ 7.2 (E. Artin). *Sei L ein Körper und G eine endliche Gruppe von Automorphismen von L, der Ordnung n. Sei $K = L^G$ der Fixkörper. Dann ist L/K eine normale und separable Körpererweiterung vom Grad $[L : K] = n$ und mit Galoisgruppe $\mathrm{Gal}(L/K) = G$.*

BEWEIS. Sei $\alpha \in L$. Sei $\sigma_1, \ldots, \sigma_r \in G$ ein maximales System, so dass $\sigma_1(\alpha), \ldots, \sigma_r(\alpha)$ verschieden sind. Sei

$$f = \prod_{i=1}^{r} \big(T - \sigma_i(\alpha)\big) \in L[T].$$

Sei $\sigma \in G$. Dann permutiert σ die Elemente $\sigma_1(\alpha), \ldots, \sigma_r(\alpha)$, und daher gilt $\sigma^*(f) = f$. Die Koeffizienten von f bleiben also fix unter allen $\sigma \in G$, und daher liegen die Koeffizienten in $K = L^G$, d. h. $f \in K[T]$. Ferner gilt $f(\alpha) = 0$. Da f nur einfache Nullstellen hat, folgt, dass α separabel über K ist. Ferner ist $[K(\alpha) : K] \leq r \leq n$. Mit dem vorherigen Lemma folgt $[L : K] \leq n$.

Ist $\alpha \in L$ Nullstelle eines irreduziblen Polynoms $g \in K[T]$, so ist dieses (bis auf Normierung) das Minimalpolynom von α über K und daher ein Teiler von obigem Polynom f, und zerfällt daher in $L[T]$ (wie f) komplett in Linearfaktoren. Daher ist L/K auch normal.

Nach dem Satz vom primitiven Element gibt es ein $\alpha \in L$ mit $L = K(\alpha)$.

Es gilt $G \subseteq \mathrm{Gal}(L/K)$: Denn jedes $\sigma \in G$ fixiert jedes $x \in K = L^G$. Es ist $|\mathrm{Gal}(L/K)|$ nach Folgerung 1.4 die Anzahl der verschiedenen Nullstellen des Minimalpolynoms g von α über K, also mit obigen Bezeichnungen $\leq r \leq n = |G|$. Es folgt $G = \mathrm{Gal}(L/K)$.

Aus Folgerung 1.4 folgt außerdem $n = |\mathrm{Gal}(L/K)| \leq [L : K]$. Damit ist alles bewiesen. □

FOLGERUNG 7.3. *Sei L/K eine endliche Körpererweiterung. Dann gilt $|\mathrm{Gal}(L/K)| \leq [L : K]$. (Genauer ist $|\mathrm{Gal}(L/K)|$ ein Teiler von $[L : K]$.) Es gilt Gleichheit genau dann, wenn L/K eine Galoiserweiterung ist.*

BEWEIS. Sei $G = \mathrm{Gal}(L/K)$ und L^G der Fixkörper. Zunächst ist festzuhalten, dass G endlich ist. Denn sei $\tau\colon L \to \overline{K}$ ein festgewählter injektiver Körperhomomorphismus, der 1_K fortsetzt (existiert!). Sind $\sigma, \sigma' \in G$ mit $\sigma \neq \sigma'$, so sind $\tau \circ \sigma \neq \tau \circ \sigma'$ ebenso Fortsetzungen von 1_K. Nach Satz 5.6 gibt es aber höchstens $[L : K]$ viele solcher Fortsetzungen, insbesondere ist $|G| \leq [L : K]$ endlich.

Nach dem vorherigen Satz und dem Gradsatz ist $|G| = [L : L^G] \mid [L : K]$. Wiederum mit dem Gradsatz folgt

$$|G| = [L : K] \;\Leftrightarrow\; [L^G : K] = 1 \;\Leftrightarrow\; L^G = K \;\Leftrightarrow\; L/K \text{ galoissch.}$$

□

FOLGERUNG 7.4. *Sei L/K eine Galoiserweiterung. Dann ist L/K separabel und normal.*

BEWEIS. Für $G = \mathrm{Gal}(L/K)$ gilt $L^G = K$, und die Behauptung folgt unmittelbar aus dem Satz von Artin. □

8. Charakterisierung von Galoiserweiterungen

SATZ 8.1. *Sei L/K eine endliche Körpererweiterung. Dann sind äquivalent:*

(1) *L/K ist galoissch.*
(2) *L/K ist normal und separabel.*
(3) *Es gilt $|\mathrm{Gal}(L/K)| = [L : K]$.*

BEWEIS. Folgerung 7.3 zeigt die Äquivalenz von (1) und (3). Es fehlt nur noch der Beweis von (2)⇒(3). Ist L/K separabel und vom Grad n, so ist nach dem Satz vom primitiven Element $L = K(\alpha)$ einfach. Sei f das Minimalpolynom von α über K. Dann hat wegen der Normalität und der Separabilität f genau n verschiedene Nullstellen in L, und $|\mathrm{Gal}(L/K)| = n$ folgt aus Folgerung 1.4. □

FOLGERUNG 8.2. *Sei L/K galoissch und M ein Zwischenkörper. Dann ist L/M galoissch.*

BEWEIS. Es ist L/K normal und separabel. Dann ist L/M nach Lemma 5.5 separabel, und offenbar ist L als Zerfällungskörper eines Polynoms f über K auch Zerfällungskörper von f über M, also ist L/M auch normal. □

FOLGERUNG 8.3. *Jede Galoiserweiterung ist einfach algebraisch.*

BEWEIS. Da Galoiserweiterungen insbesondere separabel sind, folgt die Aussage aus dem Satz vom primitiven Element.

□

9. Der Hauptsatz der Galoistheorie (Beweis)

LEMMA 9.1. *Sei L/K eine Körpererweiterung und M ein Zwischenkörper. Ist $\sigma \in \mathrm{Gal}(L/K)$, so ist*

$$\mathrm{Gal}(L/\sigma(M)) = \sigma \,\mathrm{Gal}(L/M)\sigma^{-1}.$$

BEWEIS. Übung. □

SATZ 9.2 (Hauptsatz der Galoistheorie). *Sei L/K eine Galoiserweiterung vom Grad $n = [L : K]$ und mit Galoisgruppe $G = \mathrm{Gal}(L/K)$. Dann gilt:*

(1) *Es ist $|G| = n$.*
(2) *Die Abbildungen*

$$\Phi\colon \mathcal{Z} \to \mathcal{U},\ M \mapsto \mathrm{Gal}(L/M)$$

und

$$\Psi\colon \mathcal{U} \to \mathcal{Z},\ U \mapsto L^U$$

sind ordnungs-umkehrend und zueinander invers.
(3) *Für jeden Zwischenkörper M von L/K ist die Körpererweiterung L/M galoissch; dagegen ist M/K galoissch genau dann, wenn $\Phi(M) = \mathrm{Gal}(L/M) \subseteq G$ ein Normalteiler ist. In diesem Fall hat man eine kanonische Isomorphie von Gruppen*

$$\mathrm{Gal}(M/K) \simeq \frac{\mathrm{Gal}(L/K)}{\mathrm{Gal}(L/M)}.$$

BEWEIS. (1) Folgt aus Satz 8.1.

(2) Sei M ein Zwischenkörper, also $M \in \mathcal{Z}$. Es ist L/M galoissch nach Folgerung 8.2. Mit $U = \mathrm{Gal}(L/M) \in \mathcal{U}$ folgt also $L^U = M$. Mit anderen Worten, es gilt $\Psi\Phi(M) = M$, also $\Psi \circ \Phi = 1_{\mathcal{Z}}$.

Sei umgekehrt U eine Untergruppe von G. Dann gilt nach dem Satz von Artin $\mathrm{Gal}(L/L^U) = U$, mit anderen Worten $\Phi\Psi(U) = U$. Damit gilt auch $\Phi \circ \Psi = 1_{\mathcal{U}}$.

(3) Der erste Teil wurde schon gezeigt. Sei M/K galoissch (äquivalent: normal). Sei $\sigma \in G$. Nach Satz 6.4 gilt dann $\sigma(M) = M$, also $\sigma_{|M} \in \mathrm{Gal}(M/K)$. Wegen

$$\mathrm{Gal}(L/\sigma(M)) = \sigma \,\mathrm{Gal}(L/M)\sigma^{-1}$$

folgt, dass $\mathrm{Gal}(L/M)$ ein Normalteiler in G ist.

Ist umgekehrt $\mathrm{Gal}(L/M)$ ein Normalteiler in G, so folgt aus dieser Formel $\mathrm{Gal}(L/\sigma(M)) = \mathrm{Gal}(L/M)$, also $\Phi(\sigma(M)) = \Phi(M)$ für jedes $\sigma \in G$. Aus Teil (2) folgt $\sigma(M) = M$ für jedes $\sigma \in G$, also ist M/K normal (also galoissch) nach Satz 6.4.

Sind diese Bedingungen nun erfüllt, so ist $\sigma \mapsto \sigma_{|M}$ ein Gruppenhomomorphismus $\rho\colon G = \mathrm{Gal}(L/K) \to \mathrm{Gal}(M/K)$. Dessen Kern ist offenbar gerade durch $\mathrm{Gal}(L/M)$ gegeben. Ferner ist ρ surjektiv aufgrund der Liftungseigenschaft von Zerfällungskörpern. Es induziert ρ nach dem Homomorphiesatz also einen Isomorphismus $\mathrm{Gal}(L/K)/\mathrm{Gal}(L/M) \xrightarrow{\sim} \mathrm{Gal}(M/K)$. □

10. Ein Beispiel

BEISPIEL 10.1. Wir betrachten die Körpererweiterung $L = \mathbb{Q}(i, \sqrt[4]{2})$ über $K = \mathbb{Q}$.

(1) Offenbar ist L der Zerfällungskörper des separablen Polynoms $f = T^4 - 2$ über $\mathbb{Q}$, denn die komplexen Nullstellen von f sind $\alpha = \sqrt[4]{2}$, $i\alpha$, $-\alpha$, $-i\alpha$, und es ist $L = \mathbb{Q}(\alpha, i\alpha, -\alpha, -i\alpha)$. Daher ist L/K galoissch.

(2) Es gilt $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 4$, denn $T^4 - 2$ ist nach Eisenstein das Minimalpolynom von α über $\mathbb{Q}$. Es ist $\mathbb{Q}(\alpha) \subseteq \mathbb{R}$, also $i \notin \mathbb{Q}(\alpha)$. Andererseits ist i Nullstelle des Polynoms $T^2 + 1 \in \mathbb{Q}(\alpha)[T]$, und daher gilt $[\mathbb{Q}(\alpha, i) : \mathbb{Q}(\alpha)] = 2$. Es folgt daher

$$[L : K] = [\mathbb{Q}(\alpha, i) : \mathbb{Q}(\alpha)] \cdot [\mathbb{Q}(\alpha) : \mathbb{Q}] = 2 \cdot 4 = 8.$$

(3) Betrachte die Zwischenkörper $\mathbb{Q}(\alpha)$ und $\mathbb{Q}(i)$. Über diesen ist L jeweils einfach, erzeugt von i bzw. von α mit Minimalpolynomen T^2+1 über $\mathbb{Q}(\alpha)$ bzw. T^4-2 über $\mathbb{Q}(i)$. Nach Satz V.7.2 gibt es einen $\mathbb{Q}(i)$-Automorphismus σ von L mit $\sigma(\alpha) = i\alpha$ und einen $\mathbb{Q}(\alpha)$-Automorphismus τ von L mit $\tau(i) = -i$. Insbesondere sind dies K-Automorphismen, also σ, $\tau \in \mathrm{Gal}(L/K)$.

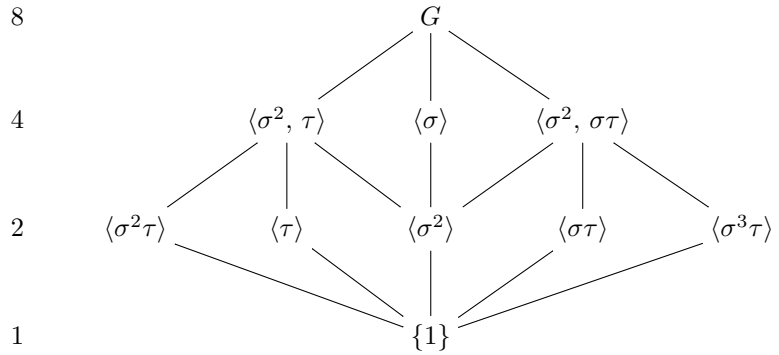
Automorphismus	Wirkung auf α	Wirkung auf i
1	α	i
σ	$i\alpha$	i
σ^2	$-\alpha$	i
σ^3	$-i\alpha$	i
τ	α	$-i$
$\sigma\tau$	$i\alpha$	$-i$
$\sigma^2\tau$	$-\alpha$	$-i$
$\sigma^3\tau$	$-i\alpha$	$-i$

Da dies 8 verschiedene K-Automorphismen sind, sind dies auch schon alle Elemente von $G = \mathrm{Gal}(L/K)$. Die abstrakte Beschreibung von G ist

$$G = \langle \sigma, \tau \mid \sigma^4 = 1 = \tau^2, \tau\sigma = \sigma^3\tau \rangle.$$

Dies ergibt also die Diedergruppe D_4 vom Grad 4, vgl. II.4.

(4) Wir erhalten den folgenden Untergruppenverband von G:



(5) Wir berechnen die Fixkörper der Untergruppen. Es ist $L^G = \mathbb{Q}$ und $L^{\{1\}} = L$. Schreibe jedes $x \in L$ in der Form

$$x = x_0 + x_1\alpha + x_2\alpha^2 + x_3\alpha^3 + x_4 i + x_5 i\alpha + x_6 i\alpha^2 + x_7 i\alpha^3$$

mit rationalen Koeffizienten.

Es ist

$$\begin{aligned} L^{\langle \sigma^2, \tau \rangle} &= \{x \in L \mid \sigma^2(x) = x = \tau(x)\} \\ &= \{x \in L \mid x_1 = x_3 = x_5 = x_7 = 0,\ x_4 = x_6 = 0\} \\ &= \{x = x_0 + x_2\sqrt{2}\} \\ &= \mathbb{Q}(\sqrt{2}). \end{aligned}$$

Ebenso

$$\begin{aligned} L^{\langle \sigma \rangle} &= \{x \in L \mid \sigma(x) = x\} \\ &= \{x \in L \mid x_1 = x_5 = 0,\ x_2 = 0 = x_6,\ x_3 = -x_7 = 0\} \\ &= \{x = x_0 + x_4 i\} \\ &= \mathbb{Q}(i). \end{aligned}$$

Ferner

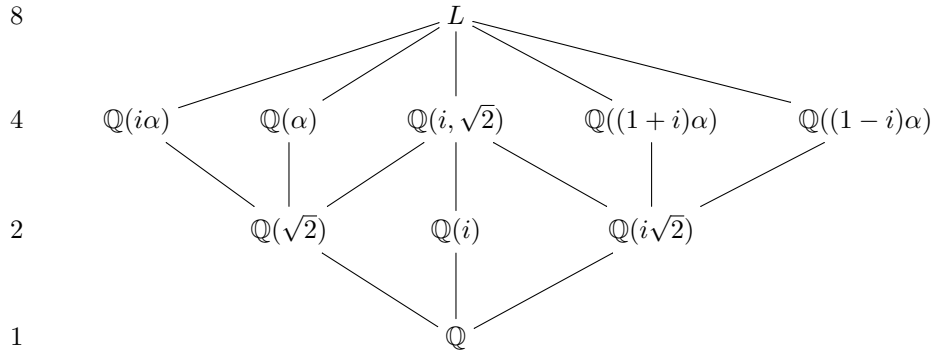
$$\begin{aligned} L^{\langle\sigma^2,\,\sigma\tau\rangle} &= \{x \in L \mid \sigma^2(x) = x = \sigma\tau(x)\} \\ &= \{x \in L \mid x_1 = x_3 = x_5 = x_7 = 0,\, x_2 = x_4 = 0\} \\ &= \{x = x_0 + x_6 i\sqrt{2}\} \\ &= \mathbb{Q}(i\sqrt{2}). \end{aligned}$$

Es sind noch die Fixkörper der Untergruppen der Ordnung 2 zu berechnen. Wir demonstrieren dies nur am folgenden Beispiel:

$$\begin{aligned} L^{\langle\sigma\tau\rangle} &= \{x \in L \mid \sigma\tau(x) = x\} \\ &= \{x \in L \mid x_1 = x_5,\, x_2 = 0 = x_4,\, x_3 = -x_7,\} \\ &= \{x = x_0 + x_1(1+i)\alpha + x_6 i\alpha^2 + x_3(1-i)\alpha^3\} \\ &= \{x = x_0 + x_1(1+i)\alpha + x_6/2((1+i)\alpha)^2 - x_3/2((1+i)\alpha)^3\} \\ &= \mathbb{Q}((1+i)\alpha). \end{aligned}$$

Analog ergibt sich $L^{\langle\sigma^2\rangle} = \mathbb{Q}(i, \sqrt{2})$, $L^{\langle\tau\rangle} = \mathbb{Q}(\alpha)$, $L^{\langle\sigma^2\tau\rangle} = \mathbb{Q}(i\alpha)$ und $L^{\langle\sigma^3\tau\rangle} = \mathbb{Q}((1-i)\alpha)$.

(6) Der Hauptsatz der Galoistheorie liefert daher den Zwischenkörperverband:



(7) Da (außer G und $\{1\}$) gerade die Untergruppen $\langle\sigma^2, \tau\rangle$, $\langle\sigma\rangle$, $\langle\sigma^2, \sigma\tau\rangle$ (vom Index 2) und $\langle\sigma^2\rangle$ Normalteiler von G sind, folgt aus dem Hauptsatz der Galoistheorie, dass von den Zwischenkörpern (außer $\mathbb{Q}$ und L selbst) genau die Zwischenkörper $\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(i)$, $\mathbb{Q}(i\sqrt{2})$ und $\mathbb{Q}(i, \sqrt{2})$ normal (äquivalent: galoissch) über $\mathbb{Q}$ sind.

KAPITEL VII

Auflösung algebraischer Gleichungen

Lernziele:

- Auflösbarkeit von (Polynom-) Gleichungen durch Radikale definieren können.
- Charakterisierung der Auflösbarkeit als Anwendung des Hauptsatzes der Galoistheorie.
- Prinzipiell ein nicht-auflösbares Beispiel kennen und erläutern können.

Wir nehmen im folgenden der Einfachheit halber an, dass alle vorkommenden Körper die Charakteristik 0 *haben. Insbesondere ist dann jedes über* K *algebraische Element separabel.*

1. Die Polynome $T^n - a$

DEFINITION 1.1. Eine Körpererweiterung L/K heißt einfache Radikalerweiterung, falls es ein $a \in L$ gibt mit $L = K(a)$ und mit $a^k \in K$ für eine natürliche Zahl $k \geq 1$.

Gilt hierbei $a^k = b \in K$, so schreibt man auch $a = \sqrt[k]{b}$ und $L = K(\sqrt[k]{b})$. Es bezeichnet also $\sqrt[k]{b}$ *eine* Nullstelle von $T^k - b$.

1.2. Sei K ein Körper, sei $n \geq 1$ eine natürliche Zahl. Ein $\zeta \in K$ heißt n-te Einheitswurzel, falls $\zeta^n = 1$ gilt. Die Menge der n-ten Einheitswurzeln in K bilden eine Gruppe $\mu_n(K)$, eine Untergruppe der Einheitengruppe $E(K)$. Da jede n-te Einheitswurzel in K Nullstelle des Polynoms $T^n - 1 \in K[T]$ ist, hat $\mu_n(K)$ endliche Ordnung $\leq n$. Aus Satz VI.4.4 folgt, dass $\mu_n(K)$ eine zyklische Gruppe ist. Ist $\zeta \in \mu_n(K)$ von der Ordnung n, so heißt ζ eine primitive n-te Einheitswurzel.

Mit $E_n(K)$ bezeichnen wir einen Zerfällungskörper des Polynoms $T^n - 1$ über K. Er wird von den (primitiven) n-ten Einheitswurzeln erzeugt, und $E_n(K) = K(\zeta)$ mit ζ primitive n-te Einheitswurzel. Man nennt $E_n(K)$ auch den n-ten Kreisteilungskörper über K.

SATZ 1.3. *Sei* K *ein Körper der Charakteristik* 0*, und* K *enthalte eine primitive* n*-te Einheitswurzel* ζ*.*

(1) *Jede Körpererweiterung der Form* $K(\sqrt[n]{a})/K$ *mit* $a \in K$ *ist eine Galoiserweiterung mit zyklischer Galoisgruppe, deren Ordnung* n *teilt.*
(2) *Ist* L/K *eine endliche Galoiserweiterung mit zyklischer Galoisgruppe und* $n = [L : K]$*, so ist* L *Zerfällungskörper eines Polynoms* $T^n - a$ *für ein* $a \in K$*.*

BEWEIS. (1) Sei $a \neq 0$. Ist y eine Nullstelle von $T^n - a$, so sind alle Nullstellen von $T^n - a$ von der Form $y\zeta^k$ für eine ganze Zahl k, also ist $K(y) = K(\sqrt[n]{a})$ Zerfällungskörper des Polynoms $T^n - a$, also $K(\sqrt[n]{a})/K$ galoissch. Jedes $\sigma \in \mathrm{Gal}(K(y)/K)$ ist durch das Bild $\sigma(y) = y\zeta^k$, also durch $k \bmod n$ eindeutig bestimmt. Man bekommt damit einen injektiven Gruppenhomomorphismus $\mathrm{Gal}(K(y)/K) \to \mathbb{Z}/n\mathbb{Z}$.

(2) Sei σ ein erzeugendes Element der Galoisgruppe G. Zu jedem $y \in L$ betrachten wir die sogenannte Lagrangsche Resolvente

$$R(\zeta, y) = \sum_{i=0}^{n-1} \zeta^i \sigma^i(y).$$

Behauptung: *Es gibt ein $y \in L$ mit $R(\zeta, y) \neq 0$.*

Nehmen wir das zunächst an. Wegen $\zeta \in K$ gilt $\sigma(\zeta) = \zeta$. Da außerdem $\sigma^n = 1_L$ gilt, folgt

$$\sigma\big(R(\zeta, y)\big) = \sum_{i=0}^{n-1} \zeta^i \sigma^{i+1}(y) = \zeta^{-1} \sum_{i=1}^{n} \zeta^i \sigma^i(y) = \zeta^{-1} R(\zeta, y).$$

Es ergibt sich

$$\sigma^i\big(R(\zeta, y)\big) = \zeta^{-i} R(\zeta, y)$$

für $i = 1, \ldots, n$. Ist nun $\tau = \sigma^i$ ein K-Automorphismus von L, der $R(\zeta, y)$ festlässt, so folgt wegen $R(\zeta, y) \neq 0$, dass $\tau = 1_L$ gelten muss. Es ist also $U \overset{def}{=} \mathrm{Gal}\Big(L/K\big(R(\zeta, y)\big)\Big) = \{1\}$. Aus dem Hauptsatz der Galoistheorie folgt $K\big(R(\zeta, y)\big) = L^U = L^{\{1\}} = L$. Ferner ist

$$\sigma\big(R(\zeta, y)^n\big) = \Big(\sigma\big(R(\zeta, y)\big)\Big)^n = \zeta^{-n} R(\zeta, y)^n = R(\zeta, y)^n,$$

also $R(\zeta, y)^n \in L^G = K$. Dies bedeutet aber, dass $R(\zeta, y) = \sqrt[n]{\big(R(\zeta, y)\big)^n}$ ein Radikal über K ist. –

Es bleibt obige Behauptung zu beweisen. Es genügt zu zeigen: Sind $a_0, \ldots, a_{n-1} \in L$ und gilt

$$\sum_{i=0}^{n-1} a_i \sigma^i(y) = 0$$

für alle $y \in L$, so gilt $a_0 = a_1 = \cdots = a_{n-1} = 0$. Angenommen, dies ist falsch. Dann sei s die kleinste ganze Zahl, so dass

$$\sum_{i=0}^{s} a_i \sigma^i(y) = 0$$

für alle y gilt mit $a_0, \ldots, a_s$ und mit $a_s \neq 0$. Es gilt offenbar $0 < s < n$. Es können offenbar nicht alle Koeffizienten a_i mit $0 \leq i < s$ verschwinden. Es sei $0 \leq t < s$ die größte ganze Zahl mit $a_t \neq 0$. Wähle ein $z \in L$ mit $\sigma^t(z) \neq \sigma^s(z)$. Dann gilt

$$\sum_{i=0}^{s} a_i \sigma^i(z) \sigma^i(y) = \sum_{i=0}^{s} a_i \sigma^i(zy) = 0$$

und

$$\sum_{i=0}^{s} a_i \sigma^s(z) \sigma^i(y) = 0.$$

Subtraktion ergibt: Für jedes $y \in L$ gilt

$$\sum_{i=0}^{t} a_i \big(\sigma^i(z) - \sigma^s(z)\big) \sigma^i(y) = 0.$$

Wegen $a_t\big(\sigma^t(z) - \sigma^s(z)\big) \neq 0$ ist dies ein Widerspruch zu Minimalität von s. □

2. Auflösbarkeit von Gleichungen

DEFINITION 2.1. Sei K ein Körper und $f \in K[T]$ ein separables Polynom. (Im Fall $\mathrm{Char}(K) = 0$ ist die Separabilität automatisch.) Sei L ein Zerfällungskörper von f über K. Es ist L/K eine Galoiserweiterung. Sei $\mathrm{Gal}(f/K) \stackrel{def}{=} \mathrm{Gal}(L/K)$, die Galoisgruppe von f über K.

Wegen der Eindeutigkeit eines Zerfällungskörpers bis auf K-Isomorphie, ist die Galoisgruppe $\mathrm{Gal}(f/K)$ (bis auf Isomorphie) eindeutig bestimmt.

DEFINITION 2.2. Eine Körpererweiterung L/K heißt Radikalerweiterung, falls es einen Körperturm

$$K = K_0 \subseteq K_1 \subseteq K_2 \subseteq \cdots \subseteq K_{n-1} \subseteq K_n = L$$

gibt, so dass K_i/K_{i-1} eine einfache Radikalerweiterung ist für jedes $i = 1, \ldots, n$.

DEFINITION 2.3. Sei $f \in K[T]$. Die Gleichung $f(x) = 0$ heißt auflösbar (durch Radikale; über K), falls der Zerfällungskörper von f über K in einer Radikalerweiterung von K liegt.

BEISPIELE 2.4. (1) Sei $f = T^2 + aT + b \in K[T]$. Die Nullstellen lassen sich in einem Zerfällungskörper L über K beschreiben als $x = -a/2 \pm \sqrt{a^2/4 - b}$. Es ist also $L = K\big(\sqrt{a^2/4 - b}\big)$ (es wird nur $\mathrm{Char}(K) \neq 2$ benötigt), und dies ist eine Radikalerweiterung. Es ist also die Gleichung $f(x) = 0$ auflösbar. (Die Normierung stellt keine Einschränkung dar.)

(2) (Cardanische Formeln; Cardano 1545, Tartaglia 1515, del Ferro um 1500) Sei $f = T^3 + aT^2 + bT + c \in \mathbb{Q}[T]$. Durch Substitution $T = T - \frac{a}{3}$ bekommt man ein Polynom

$$f = T^3 + pT + q$$

mit rationalen Koeffizienten. Es genügt, die Nullstellen für solch ein Polynom zu bestimmen. Die 3 Nullstellen x, y und z dieses Polynoms sind gegeben durch $x = a + b$, $y = \varepsilon^2 a + \varepsilon b$, $z = \varepsilon a + \varepsilon^2 b$, wobei

$$a = \sqrt[3]{-\frac{q}{2} + \sqrt{\left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3}}\,, \quad b = -\frac{p}{3a} \quad \text{und} \quad \varepsilon = -\frac{1}{2} + \frac{1}{2} i\sqrt{3}.$$

Man sieht, dass der Zerfällungskörper $L = \mathbb{Q}(x, y, z)$ von f in einer Radikalerweiterung liegt:

$$\mathbb{Q} \subset \mathbb{Q}(a_1) \subset \mathbb{Q}(a_1, a_2) \subset \mathbb{Q}(a_1, a_2, a_3)$$

mit

$$a_1 = \sqrt{\left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3},\ a_2 = \sqrt[3]{-\frac{q}{2} + a_1},\ a_3 = \varepsilon,$$

und es gilt $L \subset \mathbb{Q}(a_1, a_2, a_3)$.

(3) Auch für Polynome f vom Grad 4 über $\mathbb{Q}$ gibt es Formeln, die zeigen, dass die Gleichung $f(x) = 0$ durch Radikale auflösbar ist. (Ferrari 1540.)

Es wird sich zeigen, dass dies allgemein für Polynome vom Grad ≥ 5 (über $\mathbb{Q}$) nicht mehr richtig ist. Dies geht auf Abel (1824) zurück (auch Ruffini). Um dieses Problem dem Hauptsatz der Galoistheorie zugänglich zu machen, benötigen wir die folgende Aussage.

SATZ 2.5. *Es gelte* $\mathrm{Char}(K) = 0$. *Jede Radikalerweiterung L/K ist in einer galoisschen Radikalerweiterung N/K enthalten.*

BEWEIS. Induktion nach $n = [L : K]$. Für $n = 1$ ist die Aussage offenbar richtig. Sei nun $n \geq 2$. Nach Definition einer Radikalerweiterung gibt es einen Zwischenkörper L' von L/K, so dass L'/K eine Radikalerweiterung ist und mit $L = L'(x)$ mit $x \in L$ und

$x^s = y \in L'$ für ein $s \geq 2$, und $[L : L'] \geq 2$. Nach der Induktionsvoraussetzung gibt es eine normale Radikalerweiterung N'/K mit $L' \subset N'$. Sei N Zerfällungskörper des Polynoms

$$g = \prod_{\sigma \in \mathrm{Gal}(N'/K)} \big(T^s - \sigma(y)\big)$$

über N'. Man kann das so einrichten, dass $x \in N$ gilt, da x Nullstelle von g ist. Da N'/K galoissch ist, gilt $g \in K[T]$. Außerdem ist N' Zerfällungskörper eines Polynoms f über K. Es folgt, dass N Zerfällungskörper von fg über K ist. Damit ist N/K normal. Außerdem gilt $L = L'(x) \subseteq N'(x) \subseteq N$. Offensichtlich ist N/N' eine Radikalerweiterung (es werden sukzessive nur s-te Wurzeln von Elementen aus N' hinzuadjungiert). Da N'/K eine Radikalerweiterung ist, ergibt sich dies auch für N/K. □

Satz 2.6 (Auflösbarkeitskriterium). *Sei K ein Körper der Charakteristik 0. Sei $f \in K[T]$. Genau dann ist die Gleichung $f(x) = 0$ auflösbar, wenn die Gruppe* $\mathrm{Gal}(f/K)$ *auflösbar ist.*

Beweis. (1) Sei zunächst die Gleichung $f(x) = 0$ auflösbar. Sei M Zerfällungskörper von f über K. Dieser ist in einer galoisschen Radikalerweiterung L/K enthalten. Da M/K als Zerfällungskörper normal ist, hat man nach dem Hauptsatz der Galoistheorie eine Isomorphie von Gruppen $\mathrm{Gal}(M/K) \simeq \mathrm{Gal}(L/K)/\mathrm{Gal}(L/M)$. Es gibt also einen surjektiven Gruppenhomomorphismus $\pi\colon \mathrm{Gal}(L/K) \to \mathrm{Gal}(M/K)$. Es genügt daher nach Lemma III.7.2 zu zeigen, dass $\mathrm{Gal}(L/K)$ auflösbar ist.

Es gibt einen Körperturm

$$K = L_0 \subseteq L_1 \subseteq \cdots \subseteq L_{s-1} \subseteq L_s = L$$

mit $L_i = L_{i-1}(a_i)$ und $a_i^{n_i} \in L_{i-1}$ für eine natürliche Zahl $n_i \geq 2$ $(i = 1, \ldots, s)$. Sei $n = n_1 n_2 \ldots n_s$. Definiere $K' = E_n(K)$, $L'_i = E_n(L_i)$ $(i = 1, \ldots, n)$, $L' = E_n(L)$. Offenbar kann man dabei $L'_{i-1} \subseteq L'_i$ annehmen. Man erhält einen Körperturm

$$K' = L'_0 \subseteq L'_1 \subseteq \cdots \subseteq L'_{s-1} \subseteq L'_s = L'.$$

Hierbei ist jedes L'_i/L'_{i-1} eine einfache Radikalerweiterung. Ist L Zerfällungskörper eines Polynoms g über K, so ist L' Zerfällungskörper von $g \cdot (T^n - 1)$ über K, also ist L'/K galoissch. Da auch L/K galoissch ist, gilt nach dem Hauptsatz der Galoistheorie, dass $\mathrm{Gal}(L'/L)$ ein Normalteiler in $\mathrm{Gal}(L'/K)$ ist und

$$\mathrm{Gal}(L/K) \simeq \mathrm{Gal}(L'/K)/\mathrm{Gal}(L'/L)$$

ist als homomorphes Bild von $\mathrm{Gal}(L'/K)$ auflösbar, wenn gezeigt wird, dass $\mathrm{Gal}(L'/K)$ auflösbar ist.

Es ist $\mathrm{Gal}(K'/K)$ isomorph zu einer Untergruppe von $E(\mathbb{Z}/n\mathbb{Z})$: denn ist $\zeta \in K'$ eine feste primitive n-te Einheitswurzel, so sei $\phi\colon \mathrm{Gal}(E_n(\mathbb{Q})/\mathbb{Q}) \to E(\mathbb{Z}/n\mathbb{Z})$, $\sigma \mapsto [k] = k \bmod n$, wobei $1 \leq k < n$ gilt mit $\sigma(\zeta) = \zeta^k$; da $\sigma(\zeta)$ wieder primitiv ist, gilt, dass k teilerfremd zu n ist, also ist $[n]$ eine Einheit in $\mathbb{Z}/n\mathbb{Z}$; es ist leicht zu zeigen, dass ϕ einen injektiven Gruppenhomomorphismus definiert. – Also ist $\mathrm{Gal}(K'/K)$ abelsch und damit auflösbar. Ebenso folgt aus dem Hauptsatz

$$\mathrm{Gal}(K'/K) \simeq \mathrm{Gal}(L'/K)/\mathrm{Gal}(L'/K'),$$

und daher genügt zu zeigen, dass $\mathrm{Gal}(L'/K')$ auflösbar ist.

Wir beweisen dies durch Induktion nach s. Der Vorteil ist nun, dass durch das Vorhandensein der n-ten (und daher auch der n_i-ten) Einheitswurzeln die Erweiterungen L'_i/L'_{i-1} galoissch sind mit zyklischen Galoisgruppen nach Satz 1.3, insbesondere sind sie abelsch. Der Fall $s = 0$ ist trivial. Sei also $s \geq 1$. Es ist L'_1/K' galoissch, also nach dem Hauptsatz $\mathrm{Gal}(L'/L'_1)$ Normalteiler in $\mathrm{Gal}(L'/K')$ mit

$$\mathrm{Gal}(L'_1/K') \simeq \mathrm{Gal}(L'/K')/\mathrm{Gal}(L'/L'_1).$$

Nun ist $\mathrm{Gal}(L_1'/K')$ als abelsche Gruppe auflösbar, und $\mathrm{Gal}(L'/L_1')$ ist auflösbar nach Induktionsvoraussetzung. Also ist nach Lemma III.7.2 auch $\mathrm{Gal}(L'/K')$ auflösbar.

(2) Sei L Zerfällungskörper von f über K. Sei $\mathrm{Gal}(L/K)$ auflösbar. Seien $p_1, \ldots, p_r$ die Primteiler von $[L : K]$, und setze $n = p_1 \ldots p_r$. Setze $K' = E_n(K)$ und $L' = E_n(L)$, wobei L' als Erweiterungskörper von K' aufgefasst werden kann. Als Zerfällungskörper des Polynoms $f \cdot (T^n - 1)$ über K ist L' über K galoissch. Zu zeigen genügt, dass L'/K eine Radikalerweiterung ist.

Es gibt einen injektiven Gruppenhomomorphismus $\mathrm{Gal}(L'/K') \to \mathrm{Gal}(L/K)$, $\sigma \mapsto \sigma_{|L}$. Denn L/K ist normal, also gilt $\sigma(L) = L$ für jedes $\sigma \in \mathrm{Gal}(L'/K')$ nach Satz VI.6.4. Ist $\sigma_{|L}$ die Identität, so wird jedes Element aus $L \cup K'$ fest gehalten. Es ist aber offenbar $L' = L(K')$, also ist $\sigma = 1_{L'}$. Dies zeigt die Injektivität.

Es ist also mit $\mathrm{Gal}(L/K)$ auch die Untergruppe (bis auf Isomorphie) $\mathrm{Gal}(L'/K')$ auflösbar. Zu zeigen genügt, dass L'/K' eine Radikalerweiterung ist. Da K'/K eine Radikalerweiterung ist, folgt dies dann auch für L'/K.

Wir zeigen nun, dass L'/K' eine Radikalerweiterung ist. Da $G = \mathrm{Gal}(L'/K')$ auflösbar ist, gibt es nach Lemma III.7.5 eine Kette von Untergruppen

$$\{1\} = U_0 \subset U_1 \subset \ldots \subset U_{t-1} \subset U_t = G,$$

so dass U_{j-1} ein Normalteiler in U_j ist und die Faktorgruppe U_j/U_{j-1} zyklisch von Primzahlordnung q_j $(j = 1, \ldots, t)$. Dabei ist q_j ein Teiler von $[L' : K']$, also auch von $[L : K] = n$. Es ist also $q_j = p_i$ für ein i. Also enthält K' alle q_j-ten Einheitswurzeln. Übergang zu den Fixkörpern liefert nach dem Hauptsatz der Galoistheorie einen Körperturm

$$K' = K_t' \subset K_{t-1}' \subset \ldots \subset K_1' \subset K_0' = L'.$$

Dabei ist jede Erweiterung K_{j-1}'/K_j' galoissch (denn $\mathrm{Gal}(L'/K_{j-1}') = U_{j-1}$ ist Normalteiler in $U_j = \mathrm{Gal}(L'/K_j')$) mit zyklischer Galoisgruppe

$$\mathrm{Gal}(K_{j-1}'/K_j') \simeq U_j/U_{j-1}$$

von Primzahlordnung q_j. Aus Satz 1.3 (2) folgt, dass $K_{j-1} = K_j(a_j)$ für ein $a_j \in K_{j-1}$ und $a_j^{q_j} \in K_j$. Also ist L'/K' eine Radikalerweiterung. □

3. Nichtauflösbare Gleichungen

3.1. Sei $f \in K[T]$ separabel. Seien $a_1, \ldots, a_m$ die verschiedenen Nullstellen von f in einem Zerfällungskörper L. Für jedes $\sigma \in \mathrm{Gal}(f/K)$ gilt $\sigma(\{a_1, \ldots, a_m\}) = \{a_1, \ldots, a_m\}$, d. h. σ ist eine Permutation der Elemente $a_1, \ldots, a_m$. Offenbar lässt nur $\sigma = 1_L$ alle a_i fest. Man erhält damit einen injektiven Gruppenhomomorphismus $\mathrm{Gal}(f/K) \to S(X) = S_m$, in die symmetrische Gruppe der Menge $X = \{a_1, \ldots, a_m\}$.

Ist $f \in K[T]$ irreduzibel, ohne Einschränkung normiert, so operiert $\mathrm{Gal}(f/K)$ *transitiv* auf der Menge X, d. h. sind $a_i, a_j \in X$, so gibt es ein $\sigma \in \mathrm{Gal}(f/K)$ mit $\sigma(a_i) = a_j$. Denn es ist f das Minimalpolynom sowohl von a_i als auch von a_j, und die Aussage ergibt sich aus Satz V.7.2 und Satz VI.3.4.

Zunächst das "positive" Ergebnis:

Bemerkung 3.2. Sei K ein Körper der Charakeristik 0 und $f \in K[T]$ ein Polynom vom Grad ≤ 4. Dann ist die Gleichung $f(x) = 0$ auflösbar. Denn $G = \mathrm{Gal}(f/K)$ ist zu einer Untergruppe der symmetrischen Gruppe S_n mit $n \leq 4$ isomorph. Die S_n für $n \leq 4$ sind auflösbar. Es ist etwa

$$\{e\} \subset V_4 \subset A_4 \subset S_4$$

eine Kette von Untergruppen mit sukzessiven Normalteilern, so dass die entsprechenden Faktorgruppen abelsch sind. Hier bei ist V_4 die Gruppe, die erzeugt wird von den Transpositionen (1 2) und (3 4).

Ziel des Abschnitts ist der folgende Satz, den wir weiter unten beweisen werden.

SATZ 3.3. *Sei p eine Primzahl und $f \in \mathbb{Q}[T]$ irreduzibel und vom Grad p. Es habe f genau zwei nicht-relle Nullstellen. Dann ist* $\mathrm{Gal}(f/\mathbb{Q}) \simeq S_p$. *Für $p \geq 5$ ist insbesondere die Gleichung $f(x) = 0$ nicht auflösbar.*

FOLGERUNG 3.4. *Sei $f = T^5 - 6T + 3 \in \mathbb{Q}[T]$. Dann ist die Gleichung $f(x) = 0$ nicht auflösbar.*

BEWEIS. Das Polynom ist irreduzibel nach Eisenstein. Nach Aufgabe 8 von Übungsblatt 12 hat f genau zwei nicht-reelle Nullstellen. □

LEMMA 3.5. *Die symmetrische Gruppe S_n ($n \geq 2$) wird von der Transposition $\tau = (1\ 2)$ und dem n-Zykel $\sigma = (1\ 2\ \ldots\ n)$ erzeugt.*

BEWEIS. Sei G die Untergruppe von S_n, die von σ und τ erzeugt wird. Dann enthält G auch

$$\sigma\tau\sigma^{-1} = (2\ 3),\ \sigma^2\tau\sigma^{-2} = (3\ 4),\ \ldots,$$

also alle Transpositionen der Form $(i\ i{+}1)$. Aber dann enthält G auch die Transpositionen

$$(1\ 2)(2\ 3)(1\ 2) = (1\ 3),\ (1\ 3)(3\ 4)(1\ 3) = (1\ 4),\ \ldots,$$

also alle Transpositionen der Form $(1\ i)$. Aber dann enthält G auch eine beliebige Transposition $(i\ j) = (1\ i)(1\ j)(1\ i)$. Da jede Permutation in S_n ein Produkt von Transpositionen ist, folgt $G = S_n$. □

BEWEIS VON SATZ 3.3. Wegen Charakteristik 0 hat f genau p verschiedene Nullstellen $x_1, x_2, \ldots, x_p$ im Zerfällungskörper $L \subseteq \mathbb{C}$. Es ist $[\mathbb{Q}(x_1) : \mathbb{Q}] = p$. Die Ordnung der Gruppe $G = \mathrm{Gal}(f/\mathbb{Q})$ ist also ein Vielfaches von p. Wie oben beschrieben kann man G als Untergruppe von S_p auffassen. Nach dem Satz von Cauchy hat G ein Element σ der Ordnung p. Die einzigen Elemente der Ordnung p in S_p sind p-Zykel. Sind etwa x_1 und x_2 die nicht-reellen Nullstellen, so gilt $x_2 = \overline{x_1}$. Da $L/\mathbb{Q}$ normal, induziert komplexe Konjugation einen $\mathbb{Q}$-Automorphismus $\tau\colon L \to L$, also ein Element der Ordnung 2, welches der Transposition $\tau = (1\ 2)$ entspricht. Nach evtl. Potenzierung von σ und Umnummerierung der reellen Nullstellen $x_3, \ldots, x_p$ kann man annehmen, dass σ der p-Zykel $\sigma = (1\ 2\ \ldots\ p)$ ist. Nach dem vorherigen Lemma folgt dann aber $G = S_p$. Wir haben früher gesehen, dass S_p für $p \geq 5$ nicht auflösbar ist (Folgerung III.7.3). □

Literaturverzeichnis

[1] G. Fischer, *Lehrbuch der Algebra*. (2. Auflage.) Vieweg+Teubner, Wiesbaden, 2011.
[2] J. S. Jantzen, J. Schwermer, *Algebra*. Springer-Verlag, Berlin, 2006.
[3] C. Karpfinger, K. Meyberg, *Algebra*. (3. Auflage) Springer Spektrum, Berlin, 2013.
[4] S. Lang, *Algebra*. Springer-Verlag, New York, 2002.
[5] H.-J. Reiffen, G. Scheja, U. Vetter: *Algebra*. Bibliographisches Institut, Mannheim, 1984.
[6] I. Stewart: *Galois Theory*. (2nd edition.) Chapman & Hall, London, 1989.