Algebra und Zahlentheorie
Wintersemester 2021/2

Prof. Dr. Annette Huber-Klawitter

Fassung vom 2. Februar 2022

Dies ist ein Vorlesungsskript und kein Lehrbuch.
Mit Fehlern muss gerechnet werden!

Math. Institut
Ernst-Zermelo-Str. 1
79104 Freiburg

0761-888 5495
annette.huber@math.uni-freiburg.de

Kapitel 0

Einleitung

Was in dieser Vorlesung anders ist: wir arbeiten ein ganzes Semester, um einen wirklich großen Satz zu beweisen. Natürlich wird das Argument in viele Teilschritte zerlegt. Die Werkzeuge, die wir in diesem Zusammenhang bereitlegen, sind aber auch von unabhängigem Interesse.

Unser Hauptthema ist die Frage nach Lösungsformeln für Gleichungen.

Lösen von Gleichungen höheren Grades

Lineare und quadratische Gleichungen sind teilweise Schulstoff, wurden aber auch in den ersten beiden Semestern behandelt. (Beachte: quadratische Gleichungen werden über die Theorie der bilinearen Abbildungen auf lineare Algebra zurückgeführt). Diese Dinge sind (natürlich nicht der der Sprache der linearen Algebra) sehr alt, im Zweifelsfall geht es auf die Antike zurück.

Lösungsformeln für Gleichungen 3.ten und 4.ten Grades in einer Variablen wurden im 16. Jahrhundert in Italien gefunden. Man benötigt imaginäre Zahlen, selbst wenn die Lösungen reell sind. So wurden die komplexen Zahlen erfunden!

Cardanosche Formeln:

$$x^3 + px + q = 0$$

hat die *Diskriminante* $D = 4p^3 + 27q^2$. Für $D > 0$ hat die Gleichung genau eine reelle Lösung, nämlich (wenn ich richtig abgeschrieben habe):

$$\sqrt[3]{-\frac{q}{2} + \sqrt{A}} + \sqrt[3]{-\frac{q}{2} - \sqrt{A}}, \qquad A = \left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3$$

Die Formel für $D < 0$ und $D = 0$ ist ähnlich. Die allgemeine Gleichung dritten Grades kann immer in die obige Form gebrachte werden.

Im Grad 4 wird es noch umfangreicher, aber Sie finden die Lösung in Formelsammlungen oder auf Wikipedia.

Offensichliche Frage: Wie sieht die Lösungsformel für die Gleichung 5.ten Grades aus? Überraschende Antwort:

Theorem 0.1 (Galois 1830-32)**.** *Es gibt keine Lösungsformeln für allgemeine Gleichungen vom Grad größer 4.*

Beweis: Hauptziel dieser Vorlesung. □

Weitere Gegenstände:

Konstruktion mit Zirkel und Lineal

Damit sind wir definitiv in der Antike: Wie aus der Schule bekannt, kann man Quadrate oder gleichseitige Dreiecke mit Zirkel und Lineal konstruieren. Auch die Methode zur Winkelhalbierung kennen Sie sicher. Für einige klassische Probleme fanden die Griechen jedoch keine Methode.

Das gleichseitige n-Eck: Gesucht ist eine Konstruktionsmethode für das gleichseitige n-Eck.

Für $n = 2, 3, 4, 5, 6$ sind die Verfahren aus der Schule bekannt (naja, für 5 vielleicht nicht). Algebraisch formuliert geht es um die Lösungen der Gleichung $x^n = 1$ in $\mathbb{C}$. Auch auf diese Frage lässt sich Galois' Theorie anwenden.

Theorem 0.2. *Für allgemeines n ist dies unmöglich.*

Quadratur des Kreises: Gegeben ist ein Kreis. Mit Zirkel und Lineal soll ein Quadrat mit gleichem Flächeninhalt konstruiert werden.

Algbraischer: konstruiere $\sqrt{\pi}$. Auch dies ist unmöglich! Der Freiburger Mathematiker Lindemann bewies 1882 die Transzendenz von π.

Bekanntlich kann jeder Winkel mit Zirkel und Lineal halbiert werden. Hingegen:

Dreiteilung des Winkels: Gegeben sei ein beliebiger Winkel. Ist es möglich, ihn mit Zirkel und Lineal in drei gleiche Teile zu teilen? **Antwort:** Nein, z.B. nicht für den 60-Grad-Winkel, denn das regelmäßige 9-Eck kann nicht konstruiert werden.

Delisches Problem: Gegeben ist ein Würfel. Ist es möglich, mit Zirkel und Lineal einen Würfel von doppeltem Volumen zu konstruieren?

Algebraischer: Seitenlänge 1, also Volumen 1. Gesucht ist eine Konstruktion von $\sqrt[3]{2}$. Auch dies stellt sich als unmöglich heraus.

Zahlentheorie

Das Lösen von Gleichungen über $\mathbb{Z}$, $\mathbb{Q}$ oder den Restklassenringen $\mathbb{Z}/n\mathbb{Z}$ ist Gegenstand der Zahlentheorie. Wir werden einigen der grundlegenden Tatsachen wie chinesischen Restsatz und Eindeutigkeit der Primfaktorzerlegung begegnen, aber auch weiterführenden Resultaten.

Kleiner Satz von Fermat: Sei p eine Primzahl, $a \in \mathbb{Z}$ nicht durch p teilbar. Dann ist p ein Teiler von $a^{p-1} - 1$.

Quadratisches Reziprozitätsgesetz: Seien p und q ungerade Primzahlen. Dann gibt es einen Zusammenhang zwischen der Lösbarkeit der Gleichung $X^2 = p \mod q$ und $X^2 = q \mod p$.

Plan der Vorlesung:

- algebraische Grundbegriffe (Gruppe, Ring, Körper)
- Strukturtheorie von endlichen Gruppen bis zu den Sylowsätzen
- Grundlagen der Theorie der Lösungen von Polynomgleichungen über beliebigen Körpern. Wir studieren dies, indem wir Inklusionen von Körpern $K \subset L$ betrachten. Wichtigste Invariante ist die *Galoisgruppe*

$$\mathrm{Gal}(L/K) = \{f : L \to L \mid f|_K = \mathrm{id}, f \text{ Körperhomomorphismus } \}$$

- Galoistheorie und Lösung der obigen Probleme.

Literatur

Moderne Algebra wurde von Emmy Noether in Göttingen (1920-30er Jahre) begründet. Studiert werden Strukturen und ihre Eigenschaften: Gruppen, Ringe, Algebren,.... Sie haben diese Art Mathematik in der Vektorraumtheorie kennengelernt.

B.L. van der Waerden: Moderne Algebra, Springer Verlag (von 1940, das erste Buch, das die neue Sprache benutzt)

E. Artin: Galoissche Theorie, Verlag Harri Deutsch (das Original, von dem die ganze Welt abschreibt)

S. Bosch: Algebra, Springer Verlag.

S. Lang: Algebra, Addison Wesley (sehr gute Stoffauswahl, deutlich umfangreicher als die Vorlesung).

N. Bourbaki: Algebra (Axiomatik in Reinkultur. Eher zum Nachschlagen).

R. Schulze-Pillot: Einführung in die Algebra und Zahlentheorie, Springer Verlag. (geht nicht so weit wie die Vorlesung, dafür stärkere Betonung der zahlentheoretischen Aspekte)

oder jedes andere deutschsprachige Lehrbuch mit dem Titel Algebra.

Meine Hauptquelle: Skript der Fernuni Hagen von Prof. Scharlau.

Kapitel 1

Grundbegriffe der Gruppentheorie

Zur Erinnerung:

Definition 1.1. *Eine* Gruppe *ist ein Paar bestehend aus einer Menge G und einer Abbildung (genannt* Multiplikation*)*

$$\begin{aligned} m : G \times G &\to G \\ (a, b) &\mapsto ab \end{aligned}$$

so dass gilt

(i) (Assoziativgesetz) Für alle $a, b, c \in G$ gilt

$$(ab)c = a(bc) \ .$$

(ii) (neutrales Element) Es gibt ein Element $e \in G$ mit

$$ae = ea = a \text{ für alle } a \in G \ .$$

(iii) (inverses Element) Für jedes $a \in G$ gibt es ein $b \in G$ mit

$$ab = ba = e \ .$$

Wir schreiben $b = a^{-1}$.

Bemerkung. Das neutrale Element und die Inversen sind eindeutig.

Paare (G, m) mit (i) (manchmal (i) und (ii)) nennt man oft *Halbgruppe* oder *Monoid*.

Definition 1.2. *Eine Gruppe heißt* kommutativ *oder auch* abelsch*, wenn zusätzlich gilt:*

(iv) Für alle $a, b \in G$ gilt

$$ab = ba \ .$$

Meist schreibt man dann $a + b$ statt ab.

Beispiel. (i) $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{Q} \setminus \{0\}, \cdot)$, $(\{x \in \mathbb{R} \mid x > 0\}, \cdot)$,..., $\mathbb{R}^n$, überhaupt jeder Vektorraum nach Definition.

(ii) Weiter in linearer Algebra: sei K ein Körper.

$$\mathrm{GL(n, K)} = \mathrm{GL}_n(K) = \{\text{invertierbare } n \times n\text{-Matzrizen }\}$$

die *allgemeine lineare Gruppe* (general linear group).

$$\mathrm{SL}_n(K) = \{A \in \mathrm{GL}_n(K) \mid \det A = 1\}$$

die *spezielle lineare Gruppe.*

$$\mathrm{O}_n(K) = \{A \in \mathrm{GL}_n(K) \mid AA^t = E_n\}$$

die orthogonale Gruppe.

(iii) Sei V ein Vektorraum über dem Körper K.

$$\mathrm{Aut}_K(V) = \{f : V \to V \mid f \text{ linear, bijektiv }\}$$

mit der Komposition von Abbildungen.

Beweis: Assoziativität: Seien $f, g, h \in \mathrm{Aut}_K(V)$.

Behauptung. *Assoziativität:* $(f \circ g) \circ h = f \circ (g \circ h)$

Die linke Seite angewendet auf $v \in V$:

$$((f \circ g) \circ h)(v) = (f \circ g)(h(v)) = f(g(h(v))) \ .$$

Die rechte Seite angewendet auf $v \in V$:

$$(f \circ (g \circ h))(v) = f((g \circ h)(v)) = f(g(h(v))) \ .$$

Behauptung. *Neutrales Element ist die identische Abbildung.*

Sie ist linear, bijektiv, hat die gewünschte Eigenschaft.

Behauptung. *Sei $f : V \to V$ bijektiv. Die inverse Abbildung g ist gegeben durch:*

$$g(v) = \textit{Urbild von } v \textit{ unter } f$$

- g ist wohldefiniert.

- g ist linear: nach Definition ist $g(\lambda v + \mu w)$ das Element mit

$$f(g(\lambda v + \mu w)) = \lambda v + \mu w$$

f bildet $\lambda g(v) + \mu g(w)$ ab auf

$$\begin{aligned} f(\lambda g(v) + \mu g(w)) &= \lambda f(g(v)) + \mu f(g(v)) \ (f \text{ linear}) \\ &= \lambda v + \mu w \ (\text{Def. von } g) \end{aligned}$$

Es folgt die Behauptung.

- g ist bijektiv: $g(v) = g(w) \Rightarrow v = f(g(v)) = f(g(w)) = w$, also injektiv. Sei $v \in V$ beliebig. $w = f(v)$. Nach Definition ist $g(w) = v$, also ist g surjektiv.

Damit liegt g in $\mathrm{Aut}_K(V)$. $f(g(v)) = v = g(f(v))$ gilt nach Definition. □

Übrigens: sei $\dim_K V = n$. Die Wahl einer Basis von V induziert einen Isomorphismus $V \cong K^n$. Die darstellende Matrix zu $f : V \to V$ induziert einen Isomorphismus

$$\mathrm{Aut}_K(V) \cong \mathrm{GL}_n(K)$$

(wenn wir schon gesagt hätten, was ein Gruppenisomorphismus ist).

(iv) Sei M eine Menge.

$$S(M) = \{\alpha : M \to M \mid \alpha \text{ bijektiv } \}$$

heißt *symmetrische Gruppe* oder *Permutationsgruppe*. Insbesondere für $M = \{1, 2, \ldots, n\}$

$$S_n = S(\{1, 2, \ldots, n\})$$

(v) Wir betrachten ein regelmäßiges n-Eck in der Ebene. Die *Diedergruppe* ist die Symmetriegruppe dieses n-Ecks, z.B. Spiegelungen, Drehungen.

(vi) Die *Galoisgruppe* ist eine Art Symmetriegruppe der Lösungen einer Gleichung.

$$(x^2 + 1)(x - 1) = x^3 - x^2 + x - 1$$

hat die Wurzeln $1, \pm i$. Offensichtlich sind $\pm i$ symmetrisch. Diese Idee werden wir später genauer verfolgen...

Gruppen tauchen also überall auf, wo es Symmetrien gibt.

Definition 1.3. *Eine* Untergruppe $H \subset G$ *ist eine Teilmenge einer Gruppe, so dass die Multiplikation in* G *aus* H *eine Gruppe macht.*

Bemerkung. Es genügt, dass H nicht leer ist, sowie abgeschlossen unter Multiplikation und Inversenbildung.

Beispiel. $\mathrm{O}_n(K) \subset \mathrm{GL}_n(K)$ ist eine Untergruppe. $\mathbb{Z} \subset \mathbb{C}$ auch.

Definition 1.4. *Ein* Gruppenhomomorphismus *ist eine Abbildung*

$$f : G \to H$$

von Gruppen G, H, so dass für alle $a, b \in G$ gilt

$$f(ab) = f(a)f(b) \ .$$

Der Kern *von f ist*

$$\mathrm{Ker}(f) = \{a \in G \mid f(a) = e_H\} \ .$$

Das Bild *von f ist*

$$\mathrm{Im}(f) = \{b \in H \mid \text{ es gibt } a \in G \text{ mit } f(a) = b\} \ .$$

Ein Gruppenhomorphismus heißt Isomorphismus*, wenn er bijektiv ist. Ein Isomorphismus $f : G \to G$ heißt* Automorphismus.

Beispiel.

- $\mathrm{Aut}(G)$, die Menge der Automorphismen der Gruppe G, ist selbst eine Gruppe. (Selber Beweis wie für $\mathrm{Aut}_K(V)$.) Insbesondere ist die Umkehrabbildung eines Isomorphismus ein Gruppenisomorphismus.
- $\iota : G \to G$ mit $\iota(a) = a^{-1}$ ist ein Gruppenhomorphisms
$$\iota(ab) = (ab)^{-1} = b^{-1}a^{-1} = \iota(b)\iota(a)$$
genau dann, wenn G kommutativ ist.
- $V \cong K^n$ ein Vektorraumisomorphismus $\Rightarrow \mathrm{Aut}_K(V) \cong \mathrm{GL}_n(K)$ ein Gruppenisomorphismus.
- $\det : \mathrm{GL}_n(K) \to K^*$ ist ein surjektiver Gruppenhomomorphismus mit $\mathrm{Ker}(\det) = \mathrm{SL}_n(K)$.

Satz 1.5. *Kern und Bild eines Gruppenhomomorphismus sind Gruppen.*

Beweis: Betrachte $f : G \to H$. Seien $a, b \in \mathrm{Ker}\, f$.

$$f(ab) = f(a)f(b) = ee = e$$

also gilt $ab \in \mathrm{Ker}\, f$.

$$f(a^{-1})f(a) = f(a^{-1})e = f(a^{-1})$$
$$f(a^{-1}a) = f(e) = e$$

Beide Zeilen gleich, also $a^{-1} \in \mathrm{Ker}\, f$. Die Aussagen fürs Bild sind Übungsaufgabe. □

Gilt auch die Umkehrung?
$H \subset G$ eine Untergruppe $\Rightarrow H$ ist Bild der Inklusion $i : H \to G$, $i(h) = h$. Gibt es auch einen Gruppenhomorphismus $G \to G'$ mit Kern H? Später!

Lemma 1.6. *Sei $f : G \to H$ ein Gruppenhomomorphismus mit* $\mathrm{Ker}(f) = \{e\}$. *Dann ist f injektiv.*

Beweis: Angenommen $f(a) = f(b)$ für $a, b \in G$. Dann folgt

$$e = f(a)f(b)^{-1} = f(a)f(b^{-1}) = f(ab^{-1})$$

Also liegt ab^{-1} im Kern, d.h. $ab^{-1} = e$, also $a = b$. □

Produkte und Faktorgruppen

Wie kann man aus Gruppen neue Gruppen konstruieren?

Definition 1.7 (Satz)**.** *Seien G_1, G_2 Gruppen. Das* direkte Produkt $G = G_1 \times G_2$ *ist die Menge der Paare $(g_1, g_2) \in G_1 \times G_2$ mit der komponentenweisen Multiplikation.*

$$(g_1, g_2)(h_1, g_2) = (g_1h_1, g_2h_2)$$

Beweis: (i) (Assoziativität)

$$(g_1, g_2)\left((h_1, h_2)(k_1, k_2)\right) = (g_1, g_2)(h_1k_1, h_2k_2) = (g_1h_1k_1, g_2h_2k_2)$$
$$\left((g_1, g_2)(h_1, h_2)\right)(k_1, k_2) = (g_1h_1, g_2h_2)(k_1, k_2) = (g_1h_1k_1, g_2h_2k_2)$$

(ii) neutrales Element ist (e_1, e_2).

(iii) $(g_1, g_2)^{-1} = (g_1^{-1}, g_2^{-1})$.

□

Dasselbe funktioniert auch mit beliebig vielen, sogar unendlichen vielen Faktoren. Woran erkennt man, ob eine Gruppe ein direktes Produkt von Untergruppen ist?

Definition 1.8. *Seien $X, Y \subset G$ Untermengen. Dann heißt*

$$XY = \{xy \in G \mid x \in X, y \in Y\}$$

Produkt von X und Y.

Auch wenn X und Y Untegruppen sind, ist XY im allgemeinen keine Untergruppe!

Satz 1.9. *Sei G eine Gruppe, $H, K \subset G$ Untergruppen mit $H \cap K = \{e\}$, $hk = kh$ für alle $h \in H$, $k \in K$ und $G = HK$. Dann ist*

$$\mu : H \times K \to G; (h, k) \mapsto hk$$

ein Isomorphismus.

Beweis: Zunächst: Gruppenhomomorphismus.

$$\mu(h,k)\mu(h',k') = (hk)(h'k') = hkh'k'$$
$$\mu((h,k)(h',k')) = \mu(hh',kk') = hh'kk'$$

Die beiden stimmen überein, da $kh' = h'k$.
Nun: injektiv, also $\mathrm{Ker}(\mu) = (e,e)$. Sei $(h,k) \in \mathrm{Ker}(\mu)$, also $hk = e$. Also $h = k^{-1} \in K$. Nach Vorraussetzung $h \in H$, also $h \in H \cap K = \{e\}$. Also gilt $h = e$. Analog sieht man $k = e$.
Zuletzt: surjektiv. Es ist $\mathrm{Im}(\mu) = HK$. Nach Vorraussetzung $HK = G$. □

Beispiel. $G = \mathbb{Z}/6\mathbb{Z}$ = Restklassen modulo 6 = $\{\overline{0}, \overline{1}, \overline{2}, \ldots, \overline{5}\}$.
H gerade Zahlen modulo 6 = $\{\overline{0}, \overline{2}, \overline{4}\}$.
K durch 3 teilbare Zahlen modulo 6 = $\{\overline{0}, \overline{3}\}$.
Offensichtlich gilt $H \cap K = \{0\}$. Elemente vertauschen, denn G ist kommutativ.

$$HK = \{\overline{0}, \overline{2}, \overline{4}, \overline{3}, \overline{3}+\overline{2} = \overline{5}, \overline{3}+\overline{4} = \overline{1}\} = G$$

Also:

$$H \times K \cong G$$

Übrigens: $H \cong \mathbb{Z}/3\mathbb{Z}$ via $\overline{2} \mapsto \overline{1}$ und $K \cong \mathbb{Z}/2\mathbb{Z}$ via $\overline{3} \mapsto \overline{1}$. Also:

$$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \cong \mathbb{Z}/6\mathbb{Z}$$

Bemerkung. $\mathbb{Z}/6\mathbb{Z}$ ist der Quotient von $\mathbb{Z}$ nach der Untergruppe $6\mathbb{Z}$, dies ist eine weitere Konstruktionsmöglichkeit von Gruppen. Allgemeiner:

Definition 1.10. *Sei G eine Gruppe, H eine Untergruppe. Die Teilmengen*

$$gH = \{gh \mid h \in H\} \text{ für ein } g \in G$$
$$Hg = \{hh \mid h \in H\} \text{ für ein } g \in G$$

heißen Linksnebenklassen *bzw.* Rechtsnebenklassen *von H in G. Mit G/H bzw. $H\backslash G$ bezeichnen wir die Menge der Linksnebenklassen bzw. Rechtsnebenklassen.*

Zwei Elemente von G/H sind gleich, wenn sie als Teilmengen von G übereinstimmen, also diesselben Elemente haben.

Bemerkung. Wenn G abelsch ist, z.B. für $\mathbb{Z}$, so gilt natürlich $gH = Hg$ und $H\backslash G = G/H$.

Lemma 1.11. *Zwei Linksnebenklassen sind entweder gleich oder disjunkt. Jede Nebenklasse enthält gleiche viele Elemente, nämlich so viele wie H.*

Beweis: Seien $g_1, g_2 \in G$. Angenommen es gibt $x \in g_1H \cap g_2H$. Also

$$x = g_1h_1 = g_2h_2$$

mit geeigneten $h_1, h_2 \in H$. Dann folgt

$$g_1 = g_2 h_2 h_1^{-1} \in g_2 H.$$

Hieraus folgt wiederum

$$g_1 h = g_2 h_2 h_1^{-1} h \in g_2 H \text{ für alle } h \in H \Rightarrow$$
$$g_1 H \subset g_2 H \ .$$

Aus Symmetriegründen gilt auch $g_2 H \subset g_1 H$, also sind die Nebenklassen gleich. Die Abbildung:

$$H \to gH \ ; h \mapsto gh$$

ist bijektiv, daher stimmen die Anzahlen überein. □

Definition 1.12. *Die Anzahl der Elemente von G heißt* Ordnung $|G|$. *Die Anzahl der Linksnebenklassen von H in G heißt* Index $[G : H]$.

Ordnung und Index können auch unendlich sein.

Satz 1.13. *Es gilt $|G| = [G : H]|H|$. (Dabei ist mit je zweien auch die dritte Zahl endlich.)*

Beweis: Jede Nebenklasse hat $|H|$ Elemente, es gibt $[G : H]$ viele. □

Bemerkung. (i) Da dasselbe auch mit Rechtsnebenklassen funktioniert, gibt es genauso viele Rechts- wie Linksnebenklassen (wenn alle Zahlen endlich). Nachtrag: Die Aussage gilt auch im unendlichen Fall, da $gH \mapsto Hg^{-1}$ eine Bijektion ist.

(ii) Die Ordnung einer Untergruppe teilt die Ordnung von G. Ist $|G| = p$ eine Primzahl (etwa $\mathbb{Z}/p\mathbb{Z}$), so gibt es keine Untergruppen außer G und $\{e\}$, die trivialen Untergruppen.

Definition 1.14. *Sei $g \in G$. Die* Ordnung *von g ist die Ordnung der kleinsten Untergruppe, die g enthält*

$$\langle g \rangle = \{e, g, g^{-1}, g^2, g^{-2}, \dots\}$$

Bemerkung. Wenn $|g| \neq \infty$, dann ist sie die kleinste natürliche Zahl mit $g^n = e$.

Proof. Wenn $\langle g \rangle$ endlich ist, so gibt es $n > m$ mit $g^n = g^m$. Es folgt $g^{n-m} = e$, d.h. es gibt eine Potenz von g, die gleich dem neutralen Element ist. Sei nun $n_0 \geq 1$ der kleinste solche Exponent. Dann sind die Elemente $e, g, \dots, g^{n_0-1}$ paarweise verschieden, denn für $n, m < n_0$ mit $n > m$ ist $n - m < n_0$. Gleichzeitig ist die Menge unter Multiplikation abgeschlossen, und $(g^n)^{-1} = g^{n_0-n}$. Es handelt sich um eine Untergruppe.
Es gilt also

$$\langle g \rangle = \{e, g, \dots, g^{n_0-1}\}$$

und die Menge hat n_0 Elemente. □

Korollar 1.15. *Die Ordnung von g teilt $|G|$. Es gilt $g^{|G|} = e$ für alle $g \in G$.*

Beweis: Wir wenden Satz 1.13 auf die Untergrupp $\langle g \rangle$ an, also $|G| = |g|m$ für ein $m \in \mathbb{N}$. Mit der Bemerkung folgt

$$g^{|G|} = (g^{|g|})^m = e^m = e.$$

□

Erinnerung: Sei p eine Primzahl. Dann ist

$$\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z} = \{\overline{0}, \overline{1}, \ldots, \overline{p-1}\}$$

ein Körper mit der Addition und Multiplikation von Restklassen modulo p.

Beweis: Einziges Problem ist die Existenz von Inversen bezüglich der Multiplikation. Multiplikation mit einem $a \in \mathbb{F}_p^*$ ist eine injektive Abbildung. Da die Menge endlich ist, ist jede injektive Abbildung auch surjektiv. Es existiert das Urbild von 1. Das ist das inverses Element von a. □

Insbesondere:

Korollar 1.16 (Kleiner Satz von Fermat)**.** *Sei p eine Primzahl, a kein Vielfaches von p. Dann gilt*

$$a^{p-1} \equiv 1 \mod p$$

Beweis: $G = \mathbb{F}_p \setminus \{0\}$ ist eine Gruppe mit der Multiplikation. $|G| = p - 1$. Die Restklasse $\overline{a}$ liegt in G, denn $a \neq 0 \mod p$. □

Zurück zum Quotienten G/H. Ist diese Menge eine Gruppe? Versuch: seien $g_1H, g_2H \in G/H$.

$$(g_1H)(g_2H) = (g_1g_2)H \in G/H \ .$$

Einfach: assoziativ, Existenz von neutralem, inversen Elementen.
Problem: Ist dies unabhängig von der Wahl von g_1, g_2? Sei $g_2H = g_2'H$, d.h. $g_2' = g_2h$ für ein $h \in H$. Dann folgt

$$(g_1H)(g_2'H) = g_1g_2'H = g_1g_2hH = g_1g_2H$$

denn $hH = H$.
Sei $g_1H = g_1'H$, d.h. $g_1' = g_1h$ für ein $h \in H$.

$$(g_1'H)(g_2H) := g_1'g_2H = g_1hg_2H \stackrel{?}{=} g_1g_2H$$

Wir brauchen also:

$$hg_2H = g_2H$$

Definition 1.17. *Eine Untergruppe $N \subset G$ heißt* Normalteiler*, wenn*

$$Ng = gN \text{ für alle } g \in G \ .$$

(äquivalent: $g^{-1}Ng = N$, $g^{-1}Ng \subset N$.) Wir schreiben: $N \triangleleft G$.

Beispiel. (i) Wenn G abelsch ist, so sind alle Untergruppen normal.

(ii) $G = G_1 \times G_2$. Dann sind $G_1 \times \{e\}$ und $\{e\} \times G_2$ Normalteiler.

$$G_1 \times \{e\}(g_1, g_2) = G_1 g_1 \times \{g_2\}$$
$$(g_1, g_2)G_1 \times \{e\} = g_1 G_1 \times \{g_2\}$$

ok, denn $G_1 g_1 = G_1 = g_1 G_1$.

(iii) $\mathrm{SL}_2(K) \triangleleft \mathrm{GL}_2(K)$ z.z. $A^{-1}SA \in \mathrm{SL}_2(K)$ für alle $S \in \mathrm{SL}_2(K)$, $A \in \mathrm{GL}_2(K)$. Es gilt

$$\det(A^{-1}SA) = \det(A)^{-1} \det(S) \det A = \det S = 1 \ .$$

Satz 1.18. *Sei $N \triangleleft G$ ein Normalteiler. Dann ist G/N mit der Multiplikation*

$$g_1 N \cdot g_2 N = g_1 g_2 N$$

eine Gruppe, die Faktorgruppe*. Die Quotientenabbildung*

$$G \to G/N \ ; g \mapsto gN$$

ist ein Gruppenhomomorphismus mit Kern N.

Beweis: Wir haben bereits gesehen, dass die Multiplikation wohldefiniert ist. eN ist das neutrale Element. $g^{-1}N$ ist invers zu gN. □

Also ist jeder Normalteiler Kern eines Homomorphismus!

Satz 1.19 (Homomorphiesatz)**.** *Sei $f : G \to H$ ein Gruppenhomomorphismus. Dann ist $N = \mathrm{Ker}\, f$ ein Normalteiler von G, und f induziert einen eindeutigen injektiven Homomorphismus*

$$\overline{f} : G/N \to H \ ,$$

so dass f als $G \to G/N \to H$ faktorisiert. $\overline{f}$ definiert einen Isomorphismus $G/N \cong \mathrm{Im}\, f = \mathrm{Im}\, \overline{f}$.

Beispiel. $\det : \mathrm{GL}_n(K) \to K^*$ ist surjektiv (betrachte z.B. Diagonalmatrix $(a, 1, \ldots, 1)$). Der Kern $\mathrm{SL}_n(K)$ ist ein Normalteiler. Es gilt also

$$\mathrm{GL}_n(K)/\mathrm{SL}_n(K) \cong K^*$$

Beweis des Homomorphiesatzes:

Behauptung. $g^{-1}ng \in \operatorname{Ker} f$ *für alle* $g \in G$, $n \in \operatorname{Ker} f$.

$$f(g^{-1}ng) = f(g^{-1})f(n)f(g) = f(g^{-1})f(g) = f(g^{-1}g) = f(e) = e$$

Behauptung. $\overline{f}$ *ist eindeutig.*

Einzige Möglichkeit ist $\overline{f}(gN) = f(g)$.

Behauptung. $\overline{f}$ *ist wohldefinierte Abbildung.*

Wenn $gN = g'N$, d.h. $g' = gn$ mit $n \in \operatorname{Ker} f$, so gilt

$$f(g') = f(gn) = f(g)f(n) = f(g)e$$

Behauptung. $\overline{f}$ *ist Gruppenhomomorphismus.*

Für alle $g_1, g_2 \in G$

$$\overline{f}(g_1N \cdot g_2N) = f(g_1g_2) = f(g_1)f(g_2) = \overline{f}(g_1)\overline{f}(g_2)$$

Behauptung. $\overline{f}$ *is injektiv.*

Sei $g \in G$ mit $\overline{f}(gN) = e \Leftrightarrow f(g) = e \Leftrightarrow g \in N$, d.h. $gN = eN$.
Außerdem ist $G/N \to \operatorname{Im} f$ surjektiv, also ein Isomorphismus. □

Keineswegs ist jede Untergruppe Kern eines Gruppenhomomorphismus. Es muss schon ein Normalteiler sein.
Mit Normalteilern und Faktorgruppen kann man rechnen wie mit Brüchen.

Satz 1.20 (1. Isomorphiesatz)**.** *Sei G eine Gruppe, $H \subset G$ eine Untergruppe, $K \triangleleft G$ ein Normalteiler. Dann ist $H \cap K \triangleleft H$. Es gilt $HK = KH$, und dies ist eine Untegruppe. Es gibt einen kanonischen Isomorphismus*

$$H/H \cap K \cong HK/K \ .$$

Beweis: $K \triangleleft G$ bedeutet: für alle $g \in G$, $k \in K$ existiert $k' \in K$ so dass $gk = k'g$. Dies gilt insbesondere für alle $g \in H$.

Behauptung. $h(H \cap K)h^{-1} \subset H \cap K$ *für alle* $h \in H$.

$\subset H$ ist klar, da sich alles in H abspielt. $\subset K$ gilt, denn $h(H \cap K)h^{-1} \subset hKh^{-1} \subset K$ sogar für alle $h \in G$.

Behauptung. HK *ist Untergruppe.*

abgeschlossen unter Inversenbildung: für alle $h \in H$, $k \in K$ existiert $k' \in K$

$$(hk)^{-1} = k^{-1}h^{-1} = h^{-1}k' \in HK$$

abgeschlossen unter Multiplikation: für alle $h_1, h_2 \in H$, $k_1, k_2 \in K$ existiert $k' \in K$

$$(h_1k_1)(h_2k_2) = h_1(k_1h_2)k_2 = h_1(h_2k')k_2 \in HK$$

Wir definieren $\phi : H \to G/K$ via $h \mapsto hK$. Dies ist ein Gruppenhomomorphismus.

Behauptung. $\phi(H) = HK/K$

$\subset$ ist klar. Es gilt $HK/K = \{hK \mid h \in H\}$, denn $hkK = hK$ für alle $h \in H$, $k \in K$. Also ist auch $\supset$ klar.

Behauptung. $\mathrm{Ker}(\phi) = H \cap K$.

$$\mathrm{Ker}(\phi) = \{h \in H \mid hK = K \Leftrightarrow h \in K\} = H \cap K$$

Also faktorisiert ϕ über $\overline{\phi} : H/H\cap K \to HK/K$, und diese Abbildung ist sowohl injektiv als auch surjektiv. □

Bemerkung. Die Vorraussetzung $K \lhd G$ ist zu stark. Gereicht hätte auch: $h^{-1}Kh \subset K$ für alle $h \in H$.

Satz 1.21 (2. Isomorphiesatz)**.** *Sei G eine Gruppe und $K, H \lhd G$ Normalteiler mit $K \subset H$. Dann ist K normal in H, und es gibt einen kanonischen Isomorphismus*

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

Beweis: Wir betrachten $G \to G/H$. K ist enthalten im Kern, also existiert eine Abbildung

$$p : G/K \to G/H$$

(Beweis wie in 1.19). Sie ist surjektiv.

Behauptung. $\mathrm{Ker}\, p = \{hK \mid h \in H\} = H/K$

Sei $gK \in G/K$ mit $gH = p(gK) = H$. Dann ist $g \in H$.
Nach Satz 1.19 sind wir nun fertig. □

Einige Begriffe zum Schluss:

Definition 1.22. *Sei G eine Gruppe, $S \subset G$ eine Teilmenge. Der* Normalisator *von S in G ist*

$$N_S = \{g \in G \mid g^{-1}Sg = S\}$$

Der Zentralisator *von S in G ist*

$$Z_S = \{g \in G \mid g^{-1}sg = s \text{ für alle } s \in S\}$$

Der Zentralisator von G heißt Zentrum

Bemerkung. Es handelt sich um Untergruppen. Das Zentrum ist eine abelsche Untergruppe und ein Normalteiler.

Kapitel 2

Wichtige Beispiele von Gruppen

Erzeuger und Relationen

Beispiel. G sei erzeugt von den Elementen a, b mit den Relationen $a^2 = e$, $b^2 = a$. Man überlegt sich:

Der Erzeuger a ist überflüssig. G wird erzeugt von b mit der Relation $e = (a^2) = b^4$.

- Die Gruppe hat also die Elemente

$$\{e, b, b^2, b^3, b^4\}$$

Es könnte natürlich $e = b$ sein. Wir verabreden aber, dass das nicht passiert, wenn wir eine Gruppe durch Erzeuger und Relationen angeben.

Beispiel. G sei erzeugt von den Elementen a, b mit den Relationen $a^2 = b^2 = (ab)^3 = e$. Es gilt $a^{-1} = a$, $b^{-1} = b$. Die Gruppe hat die Elemente

$$\{e, a = babab, ab = baba, aba = bab, abab = ba, ababa = b\}$$

(Übungsaufgabe. Kennen Sie diese Gruppe?)

Wir formalisieren.

Definition 2.1. *Sei S eine Menge. Die* freie Gruppe *über S ist die Menge $F(S)$ aller Äquivalenzklassen von Worten*

$$s_1^{\varepsilon_1} s_2^{\varepsilon_s} \dots s_k^{\varepsilon_k}$$

mit $k \geq 0$ variabel, $\varepsilon_i = \pm 1$, $s_i \in S$ modulo der Äquivalenzrelation erzeugt von

$$ws^{-1}s^1w' \sim ww' \; ; ws^1s^{-1}w' \sim ww' \text{ für alle Worte } w, w'.$$

Die Gruppenmultiplikation ist das Aneinanderhängen von Worten. Das leere Wort ist das neutrale Element. $s = s^1$ *und* s^{-1} *sind zueinander invers.*

Beispiel. $S = \{a\}$. Dann ist

$$F(S) = \{e, a, a^{-1}, aa, a^{-1}a^{-1}, aaa, a^{-1}a^{-1}a^{-1}, \dots\} \cong \mathbb{Z} \ .$$

$S = \{a, b\}$. Dann ist

$$F(S) = \{e, a, b, a^{-1}, b^{-1}, ab, ab^{-1}, a^{-1}b, a^{-1}b^{-1}, ba, ba^{-1}, \dots\} \ .$$

Beispiel. Sei $X = \mathbb{C} \setminus \{z_1, \dots, z_n\}$ als topologischer Raum, $x \in X$. Dann gilt für die Fundamentalgruppe:

$$\pi_1(X, x) \cong F(\{\gamma_1, \dots, \gamma_n\})$$

wobei γ_i ein einfach geschlossener Weg um z_i ist.

Definition 2.2. *Sei G eine Gruppe, $S \subset G$ eine Teilmenge. Wir sagen, dass G* von *S* erzeugt wird*, wenn die natürliche Abbildung*

$$F(S) \to G \ ; \textit{Wort} \mapsto \textit{Produkt}$$

surjektiv ist. Die Gruppe G heißt endlich erzeugt*, wenn es eine endliche Teilmenge S gibt, die G erzeugt.*
Sei $R \subset F(S)$ eine Teilmenge. Wir sagen, dass G von S erzeugt wird mit Relationen R, wenn

$$F(S)/N(R) \to G$$

ein Isomorphismus ist, wobei $N(R)$ der kleinste Normalteiler von $F(S)$ ist, der R enthält.

Beispiel. $G = \mathbb{Z} \times \mathbb{Z}$. Wir wählen

$$S = \{s_1, s_2\} = \{(1, 0), (0, 1)\} \ .$$

Die Abbildung $F(S) \to \mathbb{Z} \times \mathbb{Z}$ ist surjektiv, denn $s_1 \dots s_1 s_2 \dots s_2 \mapsto (n, 0) + (0, m) = (n, m)$, wobei n die Anzahl der s_1, m die Anzahl der s_2 im Wort. Wir wählen

$$R = \{s_1 s_2 s_1^{-1} s_2^{-1}\} \ .$$

In $F(S)/N(R)$ gilt dann $\overline{s}_1\overline{s}_2\overline{s}_1^{-1}\overline{s}_2^{-1} = \overline{e} \Leftrightarrow \overline{s}_1\overline{s}_2 = \overline{s}_2\overline{s}_1$. Also können alle Worte nach Potenzen von $\overline{s}_1$ und $\overline{s}_2$ umsortiert werden. $\mathbb{Z} \times \mathbb{Z}$ kann mit zwei Erzeugern und einer Relation geschrieben werden.

Bemerkung. Jede Gruppe ist Quotient einer freien Gruppe, z.B.

$$F(G) \to G \ ; g \mapsto g$$

mit sehr vielen Relationen. Das Studium der Gruppen ist also das Studium der Normalteiler von freien Gruppen.

Theorem 2.3 (ohne Beweis, schwer)**.** *Untergruppen von freien Gruppen sind frei.*

Es ist sehr einfach, eine Gruppe durch Erzeuger und Relationen zu definieren. Aber:

Problem. Sei G von einer endliche Menge S erzeugt mit einer endlichen Menge von Relationen R. Sei $w \in F(S)$ ein Wort. Gilt $w = e$ in G?

Es ist unmöglich, einen allgemeinen Algorithmus anzugeben, der dieses Problem entscheidet! Interpretation in der Informatik:

- R ist eine Sprache mit dem Alphabet S.
- w ist ein Programm.
- $w = e$ bedeutet, dass das Programm gültig ist.

In der Logik oder theoretischen Informatik wird bewiesen, dass es keinen Algorithmus gibt, der die Gültigkeit von Programmen testet (es sei denn man stellt Zusatzbedingunen an R). In der Informatik wird meist nicht über Gruppen, sondern über Halbgruppen gesprochen (ohne inverse Elemente). Sie heißen dort *Semi-Thue Systeme*.

Zyklische Gruppen

Definition 2.4. *Eine Gruppe heißt* zyklisch*, falls sie von einem Element erzeugt wird.*

Beispiel. (i) $(\mathbb{Z}, +)$ ist zyklisch. Erzeuger sind 1 oder auch -1.

(ii) $7\mathbb{Z}$ ist zyklisch mit Erzeuger ± 7.

(iii) $\mathbb{Z}/7\mathbb{Z}$ ist zyklisch mit Erzeuger $1 + 7\mathbb{Z}$.

(iv) Die Gruppe der 5-ten Einheitswurzeln

$$\{z \in \mathbb{C} \mid z^5 = 1\} = \{\exp(2\pi ik/5) \mid k \in \mathbb{Z}\}$$

ist zyklisch mit Erzeuger $\exp(2\pi i/5)$.

(v) G eine Gruppe, $g \in G$. Die von g erzeugte Untergruppe ist zyklisch (vergleiche Definition 1.14).

Lemma 2.5. *(i) Eine Gruppe ist zyklisch, genau dann, wenn es einen surjektiven Gruppenhomomorphismus $p : \mathbb{Z} \to G$ gibt.*

(ii) Jede unendliche zyklische Gruppe ist isomorph zu $\mathbb{Z}$. Jede endliche zyklische Gruppe der Ordnung n ist isomorph zu $\mathbb{Z}/n\mathbb{Z}$.

(iii) Jede Untergruppe von $\mathbb{Z}$ ist von der Form $n\mathbb{Z}$ für ein $n \in \mathbb{N}_0$.

Bemerkung. Vergleiche den Beweis der Bemerkung nach 1.14.

Beweis: Sei $g \in G$ ein Erzeuger. Wir setzen $p(k) = g^k$. Dies ist ein Gruppenhomormorphismus. Er ist surjektiv nach Definition. Dies zeigt (i).
Wir betrachten nun den Kern K dieses Homomorphismus. Ist $K = \{0\}$, so ist $\mathbb{Z} \cong G$, die Ordnung ist unendlich. Ist $K \neq \{0\}$, so enthält er ein Element $n \neq 0$, d.h. $g^n = e$. Damit ist die Ordnung von G endlich. Wir haben bereits gesehen, dass $|g| \in K$.

Behauptung. *Alle Elemente von K sind Vielfache von $|g|$.*

Angenommen, dies ist nicht der Fall. Sei $H = |g|\mathbb{Z} \subset K$. Ist $m < 0$ in $K \setminus H$, dann auch $-m$. Sei nun m das kleinste positive Gegenbeispiel, also die kleinste positive Zahl in $K \setminus H$. Dann ist $m - |g| \in K$ und sogar in H, da $0 < m - |g| < m$. Dann ist auch $m = (m - |g|) + |g|$ ein Element von H. Dies beendet den Beweis von (ii).
Sei nun $H \subset \mathbb{Z}$ beliebige Untergruppe. Da $\mathbb{Z}$ abelsch ist, handelt es sich um einen Normalteiler. Wir betrachten $G = \mathbb{Z}/H$. Diese Gruppe ist zyklisch, also auch der Kern. Das ist aber einfach H. □

Satz 2.6. *Sei p eine Primzahl und G eine Gruppe der Ordnung p. Dann gilt $G \cong \mathbb{Z}/p\mathbb{Z}$, insbesondere ist G abelsch. Jedes Element ungleich e ist ein Erzeuger.*

Beweis: Sei $g \in G$ mit $g \neq e$. Die Ordnung von g, d.h. die Ordnung der von g erzeugten Untergruppe $\langle g \rangle$, ist ein Teiler von $|G| = p$. Da die Ordnung von g nicht 1 ist, muss sie p sein. Es folgt $\langle g \rangle = G$. Damit ist G zyklisch von der Ordnung p. Nach Lemma 2.5 c) ist $G \cong \mathbb{Z}/p$. □

Sind $H_1, H_2 \subset \mathbb{Z}$ Untergruppen, so gilt also $H_1 = a_1\mathbb{Z}$ und $H_2 = a_2\mathbb{Z}$. Die Bedingung $H_1 \subset H_2$ ist äquivalent zu $a_1 \in a_2\mathbb{Z}$, also dazu dass $a_2 | a_1$ (lies: teilt).

Lemma 2.7. *Seien $n, m \in \mathbb{Z} \setminus \{0\}$. Dann gilt:*

(i) $n\mathbb{Z} + m\mathbb{Z} = \mathrm{ggT}(n, m)\mathbb{Z}$

(ii) $n\mathbb{Z} \cap m\mathbb{Z} = \mathrm{kgV}(n, m)\mathbb{Z}$.

Beweis: Man beachte, dass

$$n\mathbb{Z} + m\mathbb{Z} = \{ni + mj \mid i, j \in \mathbb{Z}\}$$

wirklich eine Untergruppe von $\mathbb{Z}$ ist, und damit die kleinste Untergruppe die n und m enthält. Die Frage ist also nur, was der Erzeuger ist. Ebenso ist $n\mathbb{Z} \cap m\mathbb{Z}$ die größte Untergruppe, die in $n\mathbb{Z}$ und $m\mathbb{Z}$ enthalten ist.

Wir haben bereits bemerkt, dass sich Enthaltenseinsrelationen für Gruppen in Teilbarkeitsrelationen für Erzeuger übersetzen. Die größte gemeinsame Untergruppe übersetzt sich in das kleinste gemeinsame Vielfache, die kleinste gemeinsame Obergruppe in den größten gemeinsamen Teiler. □

Bemerkung. Standardnotation ist $(n, m) = n\mathbb{Z} + m\mathbb{Z}$, aber auch $\mathrm{ggT}(n, m) = (n, m)$. Nach dem Lemma ist das widerspruchsfrei.
Wir haben also nebenbei die *Existenz* des ggTs bewiesen. Es ist einerseits die größte natürliche Zahl, die n und m teilt. Gleichzeitig wird sie von allen anderen Teilern geteilt, denn es gibt $a, b \in \mathbb{Z}$ mit

$$\mathrm{ggT}(n, m) = an + bm.$$

Versteckt in den Beweisen ist der *euklidische Algorithmus* zur Bestimmung des ggTs. Wir finden es durch wiederholte Divison mit Rest. Interessanterweise hängt also das ggT nur von additiven Struktur von $\mathbb{Z}$ ab, nicht von der Ringstruktur.

Korollar 2.8. *$g \in G$ habe die Ordnung n. Dann hat g^m die Ordnung $n/\mathrm{ggT}(n, m)$.*

Beweis: Ohne Einschränkung ist $G = \langle g\rangle \cong \mathbb{Z}/n\mathbb{Z}$ mit $g = 1 + n\mathbb{Z}$. Aus g^m wird die Nebenklasse $m + n\mathbb{Z}$. Wir bestimmen die Untergruppe $\langle m + n\mathbb{Z}\rangle \subset \mathbb{Z}/n\mathbb{Z}$ und ihren Index.
Sei $\phi : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ und $H = \phi^{-1}(\langle m+n\mathbb{Z}\rangle)$ das Urbild der von $m+n\mathbb{Z}$ erzeugten Gruppe. Nach dem Homomorphiesatz 1.19 gilt

$$\langle m + n\mathbb{Z}\rangle = H/n\mathbb{Z}\ .$$

Dies ist eine Untergruppe von $\mathbb{Z}$, die m und n enthält, also $H = n\mathbb{Z} + m\mathbb{Z} = \mathrm{ggT}(n, m)\mathbb{Z}$. Weiter gilt

$$[\mathbb{Z}/n\mathbb{Z} : \langle m + n\mathbb{Z}\rangle] = |(\mathbb{Z}/n\mathbb{Z})/\langle m + n\mathbb{Z}\rangle| = |(\mathbb{Z}/n)/(H/n\mathbb{Z})|$$

Nach dem 2. Noetherschen Isomorphiesatz 1.21 gilt außerdem

$$(\mathbb{Z}/n)/(H/n\mathbb{Z}) \cong \mathbb{Z}/H = \mathbb{Z}/\,\mathrm{ggT}(n, m)\mathbb{Z}\ .$$

Es folgt

$$|\langle m + n\mathbb{Z}\rangle| = \frac{|\mathbb{Z}/n\mathbb{Z}|}{[\mathbb{Z}/n\mathbb{Z} : \langle m + n\mathbb{Z}\rangle]} = \frac{n}{\mathrm{ggT}(n, m)}.$$

□

Lemma 2.9 (Chinesischer Restsatz)**.** *Seien n und m teilerfremd. Dann gilt*

$$\mathbb{Z}/nm\mathbb{Z} \cong \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}\ .$$

Beweis: Wir betrachten die Abbildung $\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ mit $i \mapsto (i+n\mathbb{Z}, i+m\mathbb{Z})$. Sie hat den Kern

$$\{i \in \mathbb{Z} \mid i \in n\mathbb{Z}, i \in m\mathbb{Z}\} = n\mathbb{Z} \cap m\mathbb{Z} \overset{2.7}{=} \mathrm{kgV}(n,m)\mathbb{Z} = nm\mathbb{Z} \ .$$

Nach 1.19 erhalten wir einen injektiven Homomorphismus $\mathbb{Z}/nm\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$. Da beide Gruppen die Ordnung nm haben, handelt es sich um einen Isomorphismus. □

Theorem 2.10 (Elementarteilersatz)**.** *Jede endlich erzeugte abelsche Gruppe ist direktes Produkt von endlich vielen zyklischen Gruppen.*

$$G \cong \mathbb{Z} \times \mathbb{Z} \times \cdots \times \mathbb{Z} \times \mathbb{Z}/n_1 \times \cdots \times \mathbb{Z}/n_k$$

Die Anzahl r der Faktoren $\mathbb{Z}$ ist eindeutig. Die $n_i > 0$ können als Primzahlpotenzen gewählt werden, dann sind sie eindeutig bis auf Anordnung. Sie können auch mit der Bedingung $n_i \mid n_{i-1}$ gewählt werden, dann sind sie eindeutig. Dies sind die Elementarteiler.

Beweis: Nicht in dieser Vorlesung, da eigentlich ein Satz über Moduln über dem Ring $\mathbb{Z}$ oder allgemeiner für Moduln über Hauptidealringen. □

Permutationsgruppen

Wir studieren das Beispiel (iv) nach 1.2: Sei M eine Menge.

$$S(M) = \{\alpha : M \to M \mid \alpha \text{ bijektiv } \}$$

heißt *symmetrische Gruppe* oder *Permutationsgruppe*. Insbesondere für $M = \{1, 2, \ldots, n\}$

$$S_n = S(\{1, 2, \ldots, n\})$$

Bemerkung. Jede (endliche) Gruppe ist Untergruppe einer (endlichen) Permutationsgruppe, nämlich

$$\iota : G \to S(G); g \mapsto \tau_g$$

wobei $\tau_g : G \to G$, $\tau_g(h) = gh$.

mit $\tau_g : G \to G$, $\tau_g(h) = gh$. Die Abbildung τ_g ist bijektiv, denn $\tau_{g^{-1}}$ ist eine Umkehrabbildung. Die Abbildung ι ist also wohldefiniert.

Die Strukturtheorie der Permutationsgruppen ist also genau kompliziert wie die Theorie aller Gruppen! Es lohnt sich, sich mit ihnen ein wenig zu beschäftigen.

Definition 2.11. *Elemente der S_n heißen* Permutationen. *Man schreibt $\alpha \in S_n$ in der Form*

$$\begin{pmatrix} 1 & 2 & \ldots & n \\ \alpha(1) & \alpha(2) & \ldots & \alpha(n) \end{pmatrix}$$

Ein Zykel *der Länge k ist ein Folge $(m_1\ m_2\ \dots\ m_k)$ mit $m_i \in \{1,\dots,n\}$ paarweise verschieden. Er steht für die Abbildung*

$$m_1 \mapsto m_2\ , m_2 \mapsto m_3\ , \dots, m_k \mapsto m_1, j \mapsto j \text{ für } j \neq m_1, \dots, m_k\ .$$

Ein Zykel der Länge 2 heißt Transposition.

Bemerkung. Es gilt $(m_1\ m_2\ \dots\ m_k) = (m_2\ m_3\ \dots\ m_k\ m_1)$. Ein Zyklus der Länge k hat die Ordnung k. Jede Permuation kann als Produkt von disjunkten Zyklen geschrieben werden. Diese Darstellung ist eindeutig bis auf die Reihenfolge.

Beispiel.

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 3 & 4 & 1 & 6 & 5 \end{pmatrix} = (1\ 2\ 3\ 4)(5\ 6)$$

Lemma 2.12. *S_n hat $n!$ Elemente. Die Gruppe S_n wird von Transpositionen erzeugt.*

Beispiel. $(1\ 2\ 3) \in S_3$. Es gilt $(1\ 2)(2\ 3) = (1\ 3)(1\ 2) = (1\ 2\ 3)$.

Beweis: 1 hat n mögliche Bilder. 2 hat $n-1$ mögliche Bilder (alle Zahlen außer dem Bild der 1). 3 hat $n-2$ mögliche Bilder, etc. Schließlich gibt es für n ein mögliches Bild. Dies ergibt

$$n(n-1)(n-2)\dots 1 = n!$$

Möglichkeiten.
Sei $\sigma = \begin{pmatrix} 1 & 2 & \dots & n \\ \alpha(1) & \alpha(2) & \dots & \alpha(n) \end{pmatrix}$. Sei $F(\sigma)$ die Anzahl der i mit $i \neq \sigma(i)$. Angenommen $1 \neq \sigma(1)$ und $i \mapsto 1$. Wir betrachten

$$\sigma' = \sigma(1\ i) = \begin{pmatrix} 1 & 2 & \dots & i & \dots & n \\ 1 & \sigma(2) & \dots & \sigma(1) & \dots & \sigma(n) \end{pmatrix}$$

Die übrigen Einträge von σ' sind wie bei σ. Also gilt $F(\sigma') < F(\sigma)$. Durch Wiederholen dieses Verfahrens erreicht man

$$\sigma\tau_1 \dots \tau_k = \mathrm{id} \Leftrightarrow \sigma = \tau_k^{-1} \dots \tau_1^{-1} = \tau_k \dots \tau_1$$

mit Transpositionen τ_i. □

Satz 2.13. *Es gibt einen eindeutigen Gruppenhomomorphismus $\varepsilon : S_n \to \{\pm 1\}$, der Transpositionen auf -1 abbildet.*

Definition 2.14. *Eine Permutation σ heißt* gerade *bzw.* ungerade, *falls $\varepsilon(\sigma) = 1$ bzw. -1. Der Kern von ε, d.h. die Untergruppe der geraden Permutationen, heißt* alternierende Gruppe *A_n.*

Bemerkung. Wenn σ Produkt von k Transpositionen ist, dann ist σ gerade bzw. ungerade genau dann wenn k gerade bzw. ungerade ist, denn es gilt $\varepsilon(\sigma) = (-1)^k$.

Beweis: Die Eindeutigkeit folgt aus dem Lemma und der Formel in der Bemerkung. Wir zeigen die Existenz. Wir assoziieren zu jeder Permutation eine Matrix durch Permutation der Basisvektoren. Konkret sei $e_i \in \mathbb{R}^n$ der i-te Einheitsspaltenvektor.

$$M : S_n \to \mathrm{GL}_n(\mathbb{R}); \sigma \mapsto \begin{pmatrix} e_{\sigma(1)} & e_{\sigma(2)} & \dots & e_{\sigma(n)} \end{pmatrix}$$

Behauptung. *M ist ein Gruppenhomomorphismus.*

Nach Definition gilt $M(\sigma\sigma')(e_i) = e_{\sigma\sigma'(i)}$. Anderseits ist $M(\sigma) \circ M(\sigma')(e_i) = M(\sigma)(e_{\sigma'(i)}) = e_{\sigma\sigma'(i)}$.
Wir definieren $\varepsilon = \det \circ M$. Dies ist ein Gruppenhomorphismus. Für eine Transposition τ gilt $\det M(\tau) = -1$, da die Determinante alternierend ist und $\det \mathrm{id} = 1$. □

Bemerkung. Dieser Beweis ist natürlich ein wenig gemogelt. Je nach Methode in der linearen Algebra benutzt man die Leibniz-Formel, um die die Existenz der Determinante zu zeigen. In dieser kommt bereits das Vorzeichen der Permuation vor. All dies wollen wir aus der linearen Algebra voraussetzen.

Beispiel. (i) Es gilt $S_1 = \{e\}$, $S_2 = \{e, (12)\} \cong \mathbb{Z}/2$, $A_2 = \{e\}$.

(ii) $S_3 = \{e, (1\ 2), (1\ 3), (2\ 3), (1\ 2\ 3), (1\ 3\ 2)\}$, $A_3 = \{e, (1\ 2\ 3), (1\ 3\ 2)\} \cong \mathbb{Z}/3\mathbb{Z}$.

(iii) Die S_4 hat 24 Elemente, die A_4 hat 12. In A_4 gibt es den Normalteiler $\{e, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Dies ist die Kleinsche Vierergruppe.

Definition 2.15. *Eine Gruppe heißt* einfach*, wenn sie keine Normateiler außer sich selbst und $\{e\}$ hat.*

Beispiel. $\mathbb{Z}/p\mathbb{Z}$ für p prim ist einfach.

Satz 2.16. *Für $n \geq 5$ ist die alternierende Gruppe einfach.*

Dieser Satz ist zentral für unser Hauptziel. Polynomgleichungen bis Grad 4 haben Lösungsformeln, genau weil dieser Satz erst ab $n = 5$ gilt.

Beweis: Sei $e \neq \sigma \in A_n$, N der von σ erzeugte Normalteiler von A_n.

Behauptung. $N = A_n$.

Was wir wissen: Mit σ liegen auch alle σ^n in N. Da N ein Normalteiler ist, d.h. $\gamma N \gamma^{-1} = N$ für alle $\gamma \in A_5$, gilt auch $\gamma\sigma\gamma^{-1} \in N$.
Wir wir suchen: S_n wird von Transpositionen erzeugt, A_n also von Elementen der Form $(a\ b)(c\ d)$. Dabei gibt es 2 Fälle: $\{a, b\} \cap \{c, d\} = \emptyset$ oder $\neq \emptyset$, d.h. $(a\ b)(a\ c) = (a\ c\ b)$ ein 3-Zykel.
1. Fall: Sei $\sigma = (1\ 2\ 3) \in N$. Für $\gamma \in S_n$ gilt

$$\gamma(1\ 2\ 3)\gamma^{-1} = (\gamma(1)\ \gamma(2)\ \gamma(3))$$

(Übungsaufgabe). Ist also σ' ein 3-Zykel, so gibt es $\gamma \in S_n$ mit

$$\gamma\sigma\gamma^{-1} = \sigma' \ .$$

Falls $\gamma \in A_n$, so liegt σ' in N. Sollte das gewählte γ ungerade sein, so korrigiert man mit der Transposition $(\gamma(4)\ \gamma(5))$:

$$(\gamma(4)\ \gamma(5))\gamma(1\ 2\ 3)\gamma^{-1})(\gamma(4)\ \gamma(5)) = (\gamma(4)\ \gamma(5))(\gamma(1), \gamma(2), \gamma(3))(\gamma(5)\ \gamma(4)) = \sigma' \ .$$

Auch in diesem Fall liegt also σ' in N. Mit σ enthält N alle 3-Zykel. Weiterhin gilt

$$(1\ 2\ 3)(1\ 2\ 4) = (1\ 3)(2\ 4) \ .$$

Mit anderen Produkten von 3-Zykeln erhält man auch alle anderen Erzeuger der A_n. Damit ist dieser Fall abgeschlossen. Gleichzeitig:

Was wir wissen: A_n wird als Normalteiler in A_n von einem beliebigen 3-Zykel erzeugt.

2. Fall: $\sigma = (1\ 2)(3\ 4)$. Wir betrachten

$$\sigma' = (1\ 2\ 5)\sigma(5\ 2\ 1\ ) = (2\ 5)(3\ 4) \in N \ .$$

Mit σ und σ' liegt auch

$$\sigma\sigma' = (1\ 2)(2\ 5) = (1\ 2\ 5)$$

in N. Damit ist auch dieser Fall abgeschlossen.

Allgemeiner Fall: Wir schreiben $\sigma = \sigma_1\sigma_2 \ldots \sigma_m$ als Produkt von disjunkten Zykeln abnehmender Länge. Ohne Einschränkung: $\sigma_1 = (1\ 2\ 3\ \ldots\ k)$. Falls $k \geq 4$, so bilden wir

$$[(1\ 2\ 3)\sigma(3\ 2\ 1)]\sigma^{-1} = (1\ 2\ 3)\sigma_1(3\ 2\ 1)\sigma_1^{-1} = (1\ 2\ 3)(4\ 3\ 2) = (1\ 2\ 4)(3) \in N \ .$$

Falls $k = 3$ und $m \geq 2$, so ist ohne Einschränkung $\sigma_2 = (4\ 5\ 6)$ oder $\sigma_2 = (4\ 5)$. Damit

$$\begin{aligned}[(1\ 2\ 4)\sigma(4\ 2\ 1)]\sigma^{-1} = (1\ 2\ 4)\sigma_1\sigma_2(4\ 2\ 1)\sigma_2^{-1}\sigma_1^{-1} \\ = (1\ 2\ 4)(5\ 3\ 2) = (1\ 2\ 5\ 3\ 4) \in N\end{aligned}$$

und wir sind fertig nach dem Fall $k = 5$.

Falls $k = 2$, so ist nach Voraussetzung σ ein Produkt einer geraden Anzahl von Transpositionen. Den Fall $m = 2$ haben wir bereits betrachtet, sei nun $m \geq 4$. Ohne Einschränkung ist $\sigma = (1\ 2)(3\ 4)(5\ 6)\ldots(2m-1\ 2m)$.

$$[(1\ 2\ 5)\sigma(5\ 2\ 1)]\sigma^{-1} = (1\ 2\ 5)(6\ 1\ 2) = (1\ 5)(2\ 6)$$

und wir sind fertig nach dem 2. Fall. □

Einfache Gruppen sind so wichtig, da sie die Bausteine aller Gruppen sind.

Definition 2.17. *Sei G eine Gruppe. Eine* Kompositionsreihe *der Länge n ist eine Folge von Untergruppen*

$$\{e\} = G_n \lhd G_{n-1} \lhd G_{n-2} \lhd \ldots \lhd G_1 \lhd G_0 = G$$

mit G_{i+1} ein Normalteiler von G_i und G_i/G_{i+1} einfach.

Beispiel. Für $n \geq 5$ ist

$$\{e\} \lhd A_n \lhd S_n$$

eine Kompositionsreihe, denn S_n/A_n hat Ordnung 2, ist also einfach.

Für beliebige Gruppen braucht eine Kompositionsreihe nicht zu existieren.

Lemma 2.18. *Sei G eine endliche Gruppe. Dann existiert eine Kompositionsreihe für G.*

Beweis: Angenommen G ist nicht einfach. Dann gibt es einen Normalteiler $\{e\} \neq N \neq G$. Entweder N ist einfach, oder es gibt einen Normalteiler zwischen $\{e\}$ und N. Entweder G/N ist einfach, oder es gibt einen nichttrivialen Normalteiler $\overline{N}' \lhd G/N$. Dann ist $N' = p^{-1}(\overline{N}') \subset G$ ein Normalteiler zwischen N und G. ($p : G \to G/N$ die natürliche Projektion.) Dieses Verfahren endet irgendwann, da die Ordnungen der Faktorgruppen immer kleiner werden.

Sauberes Argument: Induktion nach der Ordnung $m = |G|$. Für $m = 1$ ist nichts zu zeigen. Sei nun $m > 1$. Wenn G einfach ist, so ist nichts zu zeigen. Andernfalls gibt es einen nichttrivialen Normalteiler $N \lhd G$. Nach Induktionsvoraussetzung gibt es Kompositionsreihen für N und G/N.

$$\{e\} \lhd N_n \lhd \ldots \lhd N_k = N$$
$$\{e\} = \overline{N}_k \lhd \ldots \lhd \overline{N}_0 = G/N$$

Wir setzen $N_i = p^{-1}(\overline{N}_i)$ für $i \leq k$. Für $i \geq k$ sind die Quotienten N_i/N_{i+1} einfach nach Voraussetzung. Für $i < k$ gilt $N_i/N_{i+1} \cong \overline{N}_i/\overline{N}_{i+1}$ (2. Noetherscher Isomorphiesatz 1.21) . Diese Quotienten sind ebenfalls einfach. □

Selbst im einfachsten Fall (z.B. $\mathbb{Z}/6\mathbb{Z}$) ist die Kompositionsreihe nicht eindeutig.

Theorem 2.19 (Jordan-Hölder)**.** *Besitzt G eine Kompositionsreihe, so haben alle Kompositionsreihen die selbe Länge. Die einfachen Subquotienten sind eindeutig bis auf Isomorphie und Anordnung.*

Beweis: (Nur Spezialfall) Angenommen, $\{e\} \lhd N \lhd G$ und $\{e\} \lhd H \lhd G$ sind zwei Kompositionsreihen. Wir betrachten $H \cap N \subset N$. Dies ist der Kern von $N \to G/H$, also ein Normalteiler. Da N einfach ist, folgt $H \cap N = \{e\}, N$.

Ist $N \subset H$, so ist $H/N \subset G/N$ ein Normalteiler. Da G/N einfach ist, folgt $H/N = G/N$ (damit $H = G$, unmöglich) oder $H/N = N/N$, dh. $N = H$. In diesem Fall sind die Kompositionsreihen gleich.

Ist $N \cap H = \{e\}$, so ist die Abbildung $N \to G/H$ injektiv. Das Bild ist ein Normalteiler von G/H, also isomorph zu H/H (damit $N = \{e\}$, unmöglich) oder ganz G/H. Die Abbildung ist ein Isomorphismus. Umgekehrt erhält man $H \cong G/N$.

Der allgemeine Beweis benutzt keine anderen Ideen, ist aber technisch auszuschreiben und wird Ihnen erspart.

Referenz: Lang, Kapitel I, §3. Lemma 3.3 bis Theorem 3.5. □

Bemerkung. Alle endlichen einfachen Gruppen sind bekannt. Es gibt einige unendliche Serien (z. B. $\mathbb{Z}/p\mathbb{Z}$ für p prim und A_n für $n \geq 5$) und endlich viele "sporadische" Gruppen. Die größte sporadische Gruppe heißt *Monster*. Sie hat

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

(54 Stellen) Elemente. Sie wurde von Fischer und Griess 1982 entdeckt.

Der Beweis der Klassifikation ist extrem schwer und lang und über viele Artikel verstreut.

Literatur: R. Borcherds, What is the Monster?, Notices of the AMS, Vol. 49, October 92, p.1076.

Kapitel 3

Operationen von Gruppen auf Mengen

Der Begriff der Gruppe ist rein abstrakt, aber viele Beispiele ($S(M)$, $\mathrm{GL}_n(K)$, Diedergruppe) haben mit Symmetrien von Objekten zu tun.

Definition 3.1. *Sei G eine Gruppe, M eine Menge. Eine* Operation *von G auf M ist eine Abbildung*

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

so dass gilt:

(i) $e \cdot m = m$ *für alle* $m \in M$.

(ii) $g(hm) = (gh)m$ *für alle* $g, h \in G$, $m \in M$.

Bemerkung. Es folgt $g(g^{-1}m) = (gg^{-1})m = em = m$.

Beispiel. (i) $\mathrm{GL}_n(K) \times K^n \to K^n$ mit $(A, v) \mapsto Av$ (Matrixmultiplikation).

(ii) $S(M) \times M \to M$ mit $(\sigma, m) \mapsto \sigma(m)$ (Anwenden der Permutation).

(iii) $G = \mathbb{R}$, $M = \mathbb{R}^2$, $\alpha(x, y)$ das Bild von (x, y) unter der Drehung um $(0, 0)$ um den Winkel α. Algebraisch kann man das so ausdrücken $(x, y) = x + iy \in \mathbb{C}$, $\alpha(x, y) = \exp(i\alpha)(x + iy) \in \mathbb{C}$.

(iv) $G = \mathbb{R}^2$, $M = \mathbb{R}^2$, Punkte aus M werden um Elemente aus G verschoben.

(v) Die Gruppenmultiplikation $G \times G \to G$ ist auch eine Operation von G auf G.

(vi) Die Konjugationsabbildung $c : G \times G \to G$ mit $c(g, h) = ghg^{-1}$ ist eine Operation von G auf G.

Bemerkung. Eigentlich haben wir eine *Linksoperation* definiert. Bei einer *Rechtsoperation*

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

gilt $m(gh) = (mg)h$. Die Abbildung des zweiten Beispiels ist *keine* Rechtsoperation! Versuch: $i\sigma := \sigma(i)$.

$$i(\sigma \circ \tau) = (\sigma \circ \tau)(i) = \sigma(\tau(i)) = \sigma(i\tau) = (i\tau)\sigma \; ,$$

falsche Reihenfolge! Wenn G kommutativ ist, so ist jede Linksoperation auch eine Rechtsoperation.

Lemma 3.2. *Die Angabe einer Operation von G auf M ist äquivalent zur Angabe eines Gruppenhomomorphismus $G \to S(M)$.*

Beweis: Gegeben sei $G \times M \to M$. Wir definieren $\alpha : G \to S(M)$ durch $\alpha(g)(m) = gm$.
$\alpha(g)$ ist bijektiv, denn $\alpha(g^{-1}$ ist invers zu α.
α ist ein Gruppenhomomorphismus, denn für alle $m \in M$ gilt

$$(\alpha(g) \circ \alpha(h))(m) = \alpha(g)(\alpha(h)(m)) = g(hm) = (gh)m = \alpha(gh)m$$

Ist umgekehrt $\alpha : G \to S(M)$ ein Gruppenhomomorphismus, so definiert man $G \times M \to M$ durch $(g, m) \mapsto \alpha(g)(m)$. Wir überprüfen die Axiome einer Operation.

$$em = \alpha(e)(m) = \mathrm{id}(m) = m$$
$$(gh)m = \alpha(gh)(m) = \alpha(g) \circ \alpha(h)(m) = \alpha(g)(hm) = g(hm) \; .$$

□

Im Spezialfall der Operation $G \times G \to G$ durch Gruppenmultiplikation haben wird diesen Satz schon einmal betrachtet (Einbettung einer Gruppe in eine $S(M)$). Im Beweis von Satz 2.13 (Vorzeichen einer Permutation) wurde die Operation $S_n \times \mathbb{R}^n \to \mathbb{R}^n$ betrachtet, die durch lineare Fortsetzung der Permuation der Basisvektoren entsteht.

Definition 3.3. *Eine Operation einer Gruppe G auf einem K-Vektorraum V, so dass die Abbildungen $\alpha(g) : V \to V$ K-linear sind, heißt* Darstellung *von G.*

Darstellungen von Gruppen tauchen beim Lösen von linearen Differentialgleichungen auf, z.B. in der Quantenmechanik.

Definition 3.4. *Sei $G \times M \to M$ eine Operation. Die* Standgruppe *von $m \in M$ ist*

$$G_m = \{g \in G \mid gm = m\} \; .$$

Die Bahn *von $m \in M$ ist*

$$Gm = \{gm \in M \mid g \in G\}$$

Die Operation heißt transitiv*, wenn es nur eine Bahn gibt. Ein* Fixpunkt *ist ein $m \in M$ mit Standgruppe $G_m = G$. Die Menge der Fixpunkte wird mit M^G bezeichnet. Die Operation ist* treu*, wenn*

$$\{e\} = \{g \in G \mid gm = m \text{ für alle } m \in M\} = \bigcap_{m \in M} G_m$$

Beispiel. (i) $G = S_n$, $M = \{1, \ldots, n\}$. Es gilt $S_n \cdot 1 = M$, z.B. $(1\ i)1 = i$, d.h. die Operation ist transitiv. Die Standgruppe G_1 ist die Menge der Permuationen, die 1 nicht bewegen, also $S(\{2, \ldots, n)) \cong S_{n-1}$. Die Operation ist treu.

(ii) Operation von $\mathbb{R}$ auf $\mathbb{R}^2$ durch Drehungen um 0. Sei $(x, y) \in \mathbb{R}^2$. Die Standgruppe ist die Menge der Vielfachen von 2π. Im Fall $(x, y) = (0, 0)$ ist die Standgruppe ganz $\mathbb{R}$. Die Bahn eines Elementes (x, y) ist der Kreis um 0 mit dem Radius $|(x, y)| = \sqrt{x^2 + y^2}$. Die Operation ist weder transitiv noch treu, aber sie hat einen Fixpunkt.

(iii) Sei $H \subset G$ eine Untergruppe, die durch die Gruppenultiplikation auf G operiert. Sei $g \in G$.

$$H_g = \{h \in H | hg = g\} = \{e\}$$

Die Operation ist treu. Die Bahn Hg ist die Rechtsnebenklasse von g.

Satz 3.5. *G operiere auf M. Dann sind zwei Bahnen entweder gleich oder disjunkt. M ist disjunkte Vereinigung der Bahnen.*

Beweis: Wörtlich wie der Beweis von Lemma 1.11 (Zerlegung einer Gruppe in Nebenklassen). □

Beispiel. Sei $\langle\sigma\rangle \subset S_n$ von einem Element erzeugt. Die Zyklenzerlegung von σ entspricht der Zerlegung von $\{1, \ldots, n\}$ in Bahnen von $\langle\sigma\rangle$.

Korollar 3.6. *Gehören x, y zur selben Bahn Gz, so ist*

$$Gx = Gy = Gz$$

Beweis: $x \in Gx \cap Gz \Rightarrow Gx = Gz$ und $y \in Gy \cap Gz \Rightarrow Gy = Gz$ □

Korollar 3.7. *Sei $G \times M \to M$ eine Operation auf einer endlichen Menge M. Seien $x_1, \ldots, x_n$ Elemente der verschieden Bahnen. Dann gilt*

$$|M| = \sum_{i=1}^{n} |Gx_i| \ .$$

Lemma 3.8. *Die Operation von G auf M ist genau dann treu, wenn die zugehörige Abbildung $\alpha : G \to S(M)$ injektiv ist.*

Beweis: Sei $g \in \operatorname{Ker}\alpha$, d.h.

$$\alpha(g) = \mathrm{id} \Leftrightarrow gm = m \text{ für alle } m \in M$$

Nach Definition folgt die Behauptung. □

Umgangsprachlich: Wenn die Operation transitiv ist, dann weiss die Gruppe alles über die Menge. Wenn sie treu ist, so weiss die Menge alles über die Gruppe.

Lemma 3.9. *Sei $G \times M \to M$ eine Operation, $m \in M, g \in G$ und $m' = gm$. Dann gilt*

$$G_{m'} = gG_m g^{-1} \ .$$

Sei M endlich. Dann gilt

$$|Gm| = [G : G_m]$$

d.h. die Anzahl der Elemente der Bahn ist gleich dem Index der Standgruppe.

Beweis: Wir definieren einen Gruppenhomomorphismus $c_g : G_m \to G_{m'}$ via $h \mapsto ghg^{-1}$. Man überprüft leicht: für $h \in G_m$ gilt

$$(ghg^{-1})(m') = ghm = gm = m' \ ,$$

d.h. die Abbildung ist wohldefiniert. Sie ist invers zu $c_{g^{-1}} : G_{m'} \to G_m$, also bijektiv. Mit anderen Worten, alle Elemente von $G_{m'}$ sind von der Form $gG_m g^{-1}$.
Sei G/G_m die Menge der Nebenklassen (keine Gruppe!). Wir geben eine Bijektion

$$\beta : G/G_m \to Gm$$

an. Sei $\beta(gG_m) = gm$.

Behauptung. *β ist wohldefiniert.*

Sei $gG_m = g'G_m$, dann ist $g' = gh$ mit $h \in G_m$. Es folgt

$$\beta(g'G_m) = g'm = ghm = gm = \beta(gG_m) \ .$$

Das Bild liegt nach Definition in der Bahn Gm.

Behauptung. *β ist bijektiv.*

Die Surjektivität ist klar. Sei $\beta(gG_m) = \beta(g'G_m)$, d.h. $gm = g'm$. Dann ist $h = g^{-1}g'$ ein Element der Standgruppe G_m, bzw. $g' = gh$ mit $h \in G_m$. Es folgt $g'G_m = gG_m$. □

Ist die Operation transitiv und die Standgruppe eines (also jedes) Punktes trivial ($\{e\}$), so nennt man sie auch *einfach transitiv*. Die Wahl eines Punktes $m_0 \in M$ induziert dann eine bijektive Abbildung $G \to M$ via $g \mapsto gm_0$. Trotzdem ist G nicht das Gleiche wie M!

Beispiel. M die Ebene (wie in der Schule), G die Gruppe der Translationen. Die Operation ist einfach transitiv. M und G werden mit Vektoren, d.h. Elementen von $\mathbb{R}^2$ identifiziert. In der Schule spricht man von "Ortsvektoren" und "Verschiebevektoren". Die Wahl des Punktes $m_0 \in M$ ist die Wahl des Nullpunktes des Koordinatensystems.

Satz 3.10 (Klassenformel oder Bahnformel)**.** *G operiere auf einer endlichen Menge M. Sei $x_1, \ldots, x_n$ ein Vertretersystem der Bahnen. Dann gilt*

$$|M| = \sum_{i=1}^{n} [G : G_{x_i}] \ .$$

Beweis: Korollar 3.7 und Lemma 3.9. □

Das ist banal, aber ein sehr starkes Hilfsmittel!

Beispiel. Sei $|G| = p^n$ für eine Primzahl p. Dann ist jeder Index $[G : G_{x_i}]$ eine Potenz von p. Dieser Index ist entweder durch p teilbar oder gleich 1. Im letzteren Fall gilt $G = G_{x_i}$, d.h. x_i ist ein Fixpunkt. Also:

$$|M| = |M^G| + \text{Vielfaches von } p \ .$$

Kapitel 4

Grundbegriffe der Ringtheorie

Unser Ziel ist das Studium von Körpern, dafür brauchen wir aber auch etwas Ringtheorie, vor allem den Polynomring. Diesselben Argumente funktionieren auf für $\mathbb{Z}$, also das zentrale Objekt der Zahlentheorie.

Definition 4.1. *Ein* Ring *ist eine Menge A mit zwei Verknüpfungen $+$, $\cdot$, so dass gilt:*

(i) $(A, +)$ *ist eine abelsche Gruppe mit trivialem Element* 0.

(ii) $\cdot$ *ist assoziativ.*

(iii) (Distributivgesetz) Für alle $a, b, c \in A$ gilt

$$a(b+c) = a \cdot b + a \cdot c \ ; \ (b+c)a = b \cdot a + c \cdot a \ .$$

A heißt kommutativ*, wenn $a \cdot b = b \cdot a$ für alle $a, b \in A$. Wir sagen, A* "hat eine Eins"*, wenn es ein neutrales Element der Multiplikation gibt.*

Auf französisch heißt Ring "anneau", daher ist der Buchstabe A üblich.

Beispiel. (i) $\mathbb{Z}$, alle Körper.

(ii) $k[X] = \{a_n X^n + a_{n-1} X^{n-1} + \cdots + a_0 \mid n \in \mathbb{N}_0, a_i \in k\}$ der *Polynomring* über dem Körper k (oder dem Ring k). Formal sauber: $k[X]$ ist der k-Vektorraum mit Basis Elemente mit dem Namen X^i für $i \geq 0$. Wir definieren die Multiplikation als die eindeutige k-bilineare Abbildung mit

$$X^i \cdot X^j := X^{i+j}$$

(iii) endliche Ringe, z.B. $\mathbb{Z}/n\mathbb{Z}$

Diese Ringe sind kommutativ mit Eins.

(iv) $M_n(k)$ der Ring der $n \times n$-Matrizen über einem Körper k. (nicht-kommutativ, aber mit Eins.)

(v) $C(I) = \{f : I \to \mathbb{R} \text{ stetig }\}$, wobei $I \subset \mathbb{R}$ ein Intervall.
$C_c(\mathbb{R}) = \{f : \mathbb{R} \to \mathbb{R} \text{ stetig, mit kompaktem Träger}\}$, d.h. für $f \in C_c(\mathbb{R})$ existiert $N > 0$ mit $f(x) = 0$ für alle $|x| > N$. Dieser Ring hat keine Eins, da die konstante Funktion $f = 1$ nicht kompakten Träger hat.

(vi) Varianten: $C^2(I)$ zweimal stetig differenzierbare Funktionen, $C^\infty(I)$ unendlich oft stetig differenzierbare Funktionen, ebenso $C^\infty(U)$ für $U \subset \mathbb{R}^n$ offen etc.

(vii) $L^2(\mathbb{R}^n) = \{f : \mathbb{R}^n \to \mathbb{R} \mid f \text{ messbar }, \int_{\mathbb{R}^n} |f|^2 < \infty\}/\{f \mid \int_{\mathbb{R}^n} |f|^2 = 0\}$, Gegenstand der Funktionalanalysis.

Definition 4.2. *Sei k ein Körper. Eine* k-Algebra *ist ein Ring A, der gleichzeitig ein k-Vektorraum ist, so dass*

$$\lambda(a \cdot b) = (\lambda a)b \text{ für alle } \lambda \in k, a, b \in A \ .$$

Beispiel. $k[X]$, $M_n(k)$ sind k-Algebren. $\mathbb{C}$ ist eine $\mathbb{R}$-Algebra.

Definition 4.3. *Ein* Ringhomomorphismus $f : A \to B$ *ist eine Abbildung mit*

$$f(a + a') = f(a) + f(a'), f(a \cdot a') = f(a) \cdot f(a') \text{ für alle } a, a' \in R \ .$$

Ab jetzt: Alle Ringe kommutativ mit Eins, alle Homomorphismen bilden Eins auf Eins ab.

Beispiel. A eine k-Algebra mit Eins.

$$k \to A \ ; \lambda \to \lambda \cdot 1_A$$

ist ein Ringhomomorphismus.

Beweis: $\lambda 1_A + \mu 1_A = (\lambda + \mu)1_A$, da A ein k-Vektorraum.
$(\lambda 1_A)(\mu 1_A) = \lambda(1_A(\mu 1_A)) = \lambda(\mu 1_A) = (\lambda\mu)1_A$, A eine k-Algebra, 1_A neutral. □

Die Abbildung ist injektiv genau dann, wenn $1_A \neq 0_A$.

Beweis: $\lambda 1_A = 0 \Rightarrow \lambda^{-1}(\lambda 1) = \lambda^{-1}0 = 0$ und $\lambda^{-1}(\lambda 1) = 1_k 1_A = 1_A$. □

Definition 4.4. *Eine Teilmenge $I \subset A$ heißt* Ideal*, wenn I eine Untergruppe von A ist und*

$$A \cdot I = \{a \cdot u \mid a \in A, u \in I\} \subset I \ .$$

Beispiel. Sei A ein Ring, $f \in A$. Dann ist $(f) = Af = \{af | a \in A\}$ ein Ideal. Solche Ideale heißen *Hauptideale*. Ist $A = k$ ein Körper, so sind die einzigen Ideale die Hauptideale (0) und (1).

Beweis: Sei $I \subset k$ ein Ideal, $f \in I \setminus \{0\}$. Wegen der Idealeigenschaft liegt dann $f^{-1}f = 1$ ebenfalls in I. Wieder wegen der Idealeigenschaft ist $(1) = k$. □

Satz 4.5. *(i) Sei $f : A \to B$ ein Ringhomomorphismus. Dann ist*

$$\operatorname{Ker} f = \{a \in A \mid f(a) = 0\}$$

ein Ideal.

(ii) Sei $I \subset A$ ein Ideal. Dann ist die Faktorgruppe A/I ein Ring (der Restklassenring *mit der Multiplikation*

$$(a + I)(b + I) = ab + I \ .$$

Die Abbildung $f : A \to A/I$ via $a \mapsto a + I$ ist ein Ringhomomorphismus.

(iii) Sei $f : A \to B$ ein Ringhomomorphismus. Dann faktorisiert f eindeutig als $A \to A/\operatorname{Ker} f \xrightarrow{\overline{f}} B$, und $\overline{f}$ ist injektiv.

Ideal spielen also in der Ringtheorie die Rolle von Normalteilern in der Gruppentheorie.

Beweis: (i) Der Kern ist eine Untergruppe als Kern eines Gruppenhomomorphismus. Wir überprüfen die Idealeigenschaft. Sei $a \in A$, $k \in \operatorname{Ker} f$.

$$f(ak) = f(a)f(k) = f(a)0 = 0 \Rightarrow ak \in \operatorname{Ker} f \ .$$

(ii) $I \subset A$ ist ein Normalteiler, da A abelsch. Also ist A/I eine abelsche Gruppe.

Behauptung. *Die Multiplikation ist wohldefiniert.*

Sei $a, b \in A$. Sei $a + I = a' + I$, d.h. es gibt $u \in I$ mit $a' = a + u$.

$$(a' + I)(b + I) := a'b + I = (a + u)b + I = ab + ub + I = ab + I$$

da $ub = bu \in I$, da I ein Ideal.

Behauptung. *A/I erfüllt das Distributivgesetz.*

$$(a + I)(b + I + c + I) = (a + I)(b + c + I) = a(b + c) + I$$
$$(a + I)(b + I) + (a + I)(c + I) = (ab + I) + (ac + I) = ab + ac + I$$

Beide Ausdrücke sind gleich nach dem Distributivgesetz für A.

(iii) Sei $f : A \to B$ ein Ringhomomorphismus. Dann ist f insbesondere ein Gruppenhomomorphismus. Nach Satz 1.19 existiert $\overline{f}$ und ist injektiv.

Behauptung. $\overline{f}$ *ist ein Ringhomomorphismus.*

Es war $\overline{f}(a + \operatorname{Ker} f) = f(a)$. Also

$$\begin{aligned}\overline{f}((a + \operatorname{Ker} f)(b + \operatorname{Ker} f)) &= \overline{f}(ab + \operatorname{Ker} f) \\ &= f(ab) = f(a)f(b) = \overline{f}(a + \operatorname{Ker} f)\overline{f}(b + \operatorname{Ker} f)\ .\end{aligned}$$

□

Bemerkung. Für nichtkommutative Ringe liegen die Dinge etwas komplizierter.

Beispiel. k ein Körper, $A = k[X]$.

(i) $I = \{a_2X^2 + a_3X^3 + \dots a_nX^n \dots n \geq 2, a_i \in k\}$ = Vielfache von X^2. Dann ist $k[X]/I = k[X]/X^2 \cong \{(a_0, a_1) \mid a_i \in k\} = k^2$ als abelsche Gruppe via $\sum a_iX^i \mapsto (a_0, a_1)$. Dabei hat k^2 die Multiplikation

$$\begin{aligned}(a_0, a_1)(b_0, b_1) = (a_0+a_1X)(b_0+b_1X) = a_0b_0+(a_0b_1+a_1b_0)X+a_1b_1X^2 \\ = (a_0b_0, a_0b_1 + a_1b_0)\end{aligned}$$

Man beachte: $(0, 1)(0, 1) = (0, 0)$.

(ii) I = Vielfache von X^2+1. $A/I = \{(a_0, a_1) \mid a_i \in k\}$ mit der Multiplikation

$$\begin{aligned}(a_0, a_1)(b_0, b_1) = (a_0+a_1X)(b_0+b_1X) = a_0b_0+(a_0b_1+a_1b_0)X+a_1b_1X^2 \\ = (a_0b_0 - a_1b_1) + (a_0b_1 + a_1b_0)X = (a_0b_0 - a_1b_1, a_0b_1 + a_1b_0)\end{aligned}$$

Für $k = \mathbb{R}$ ist $A/I \cong \mathbb{C}$ via $X \mapsto i$.

(iii) Sei k ein Körper, $I \subset k$ ein Ideal. Eine Möglichkeit ist $I = \{0\}$. Andernfalls sei $0 \neq \lambda \in I$. Dann gilt $\lambda^{-1}\lambda \in I$, also $1 \in I$, also $I = k$.

(iv) Die Ideale in $\mathbb{Z}$ sind alle von der Form $n\mathbb{Z}$ für ein $n \in \mathbb{Z}$, denn dies sind die einzigen Untergruppen und es handelt sich um Ideale. Wir erhalten als Quotienten die endlichen Ringe $\mathbb{Z}/n\mathbb{Z}$. Für $n = p$ Primzahl erhalten wir den Körper $\mathbb{F}_p$.

Wann sind Quotienten von Ringen Körper? Sei $A \to k$ surjektiv, k ein Körper. Dann ist der Kern m ein besonderes Ideal: Ist $m \subset I \subset A$ ein weiteres Ideal, so ist das Bild in k ein Ideal, also gleich m oder A.

Definition 4.6. *Ein Ideal $m \subset A$ heißt* maximal, *wenn $m \neq A$, und das einzige echte größere Ideal von A ist der ganze Ring A.*

Wir ordnen also die Menge der Ideale ungleich A bezüglich der Inklusion. Darin sind die maximalen Ideale die maximalen Elemente. Ein Ring kann viele maximale Ideale haben!

Satz 4.7. *Sei A ein kommutativer Ring mit Eins, m ein Ideal. Dann ist A/m ein Körper genau dann, wenn m maximales Ideal ist.*

Beweis: Sei m maximal. A/m ist also ein Ring mit $1 \neq 0$, da $A \neq m$.

Behauptung. *In $A/m \setminus \{0+m\}$ existieren multiplikative Inverse.*

Sei $a+m \in A/m$ mit $a \notin m$, d.h. $a+m \neq 0+m$. Wir betrachten $aA+m$. Dies ist ein Ideal und echt größer als m. Nach Vorraussetzung an m folgt dann $aA+m=A$. Insbesondere gibt es $b \in A$ und $c \in m$ mit $ab+c=1$. Es folgt

$$(a+m)(b+m) = ab+m = (1-c)+m = 1+m$$

wegen $c \in m$. Also ist $(b+m)$ invers zu $(a+m)$.
Umgekehrt sei A/m ein Körper. Sei $I \supset m$ ein Ideal.

Behauptung. *$I = A$ oder $I = m$.*

Wir betrachten $\phi : A \to A/m$. Das Bild $\phi(I)$ ist ein Ideal von A/m. Nach dem Beispiel folgt $\phi(I) = 0+m$ oder $\phi(I) = A/m$. Es gilt

$$\phi^{-1}\phi(I) = I + m = I$$

also im ersten Fall $I = \phi^{-1}(0) = m$, im zweiten Fall $I = \phi^{-1}(A/m) = A$. □

Satz 4.8. *Sei A ein Ring, $I \subset A$ ein Ideal ungleich A. Dann gibt es ein maximales Ideal $m \supset I$.*

Diese Aussage ist überraschend tief! Wichtigstes Hilfsmittel ist das Zornsche Lemma. Sei M eine Menge. Eine *partielle Ordnung* auf M ist eine Relation $\leq$ mit

- (reflexiv) $x \leq x$ für alle $x \in M$;
- (transitiv) $x \leq y, y \leq z \Rightarrow x \leq z$ für alle $x, y, z \in M$;
- (antisymmetrisch) $x \leq y, y \leq x \Rightarrow x = y$ für alle $x, y \in M$.

Beispiel. A ein Ring, $M = \{I \subset A \mid I \text{ Ideal}, \ I \neq A\}$ mit der Ordnung $\leq = \subset$.

Eine Ordnung heißt *total*, wenn für $x, y \in M$ entweder $x \leq y$ oder $y \leq x$ gilt.
Ein Element $m \in M$ heißt *maximal*, wenn $m \leq x \Rightarrow m = x$ für alle $x \in M$. Ein Element $m \in M$ heißt *obere Schranke* für $N \subset M$, wenn $x \leq m$ für alle $x \in N$.

Lemma 4.9 (Zornsches Lemma)**.** *Sei $M \neq \emptyset$ eine partiell geordnete Menge. Jede total geordnete Teilmenge von M habe eine obere Schranke in M. Dann besitzt M ein maximales Element.*

Idee: Man nimmt ein Element. Ist es nicht maximal, so gibt es ein größeres. Ist dieses nicht maximal, so gibt es wieder ein größeres, etc. Man erhält eine ganze Kette. Diese hat eine obere Schranke. Ist dieses Element nicht maximal, so etc.

Trotz des Namens handelt es sich um ein **Axiom der Mengenlehre**! Es ist unabhängig von den übrigen Axiomen der Zermelo-Fränkel-Mengenlehre. Es gibt verschiedene äquivalente Formulierungen, die teilweise plausibel, teilweise paradox sind.

Beweis von Satz 4.8. Sei M die Menge der Ideale ungleich A, die I enthalten. M ist partiell geordnet durch die Inklusion. Wegen $I \in M$ ist die Menge nicht leer. Sei $N \subset M$ eine total geordnete Teilmenge.

$$J_N = \bigcup_{J \in N} J \ .$$

Behauptung. *J_N ist ein Ideal und liegt in M.*

Sei $u \in J_N$, $a \in A$. Dann gibt es $J \in N$ mit $u \in J$. Es folgt $au \in J$, da J ein Ideal ist, also auch $au \in J_N$.
Sei $u_1, u_2 \in J_N$. Dann gibt es J_1, J_2 in N mit $u_i \in J_i$. N ist total geordnet, ohne Einschränkung $J_1 \subset J_2$. Also liegen u_1, u_2 beide in J_2. Damit auch $u_1 + u_2 \in J_2 \subset J_N$.
Offensichtlich gilt $I \subset J_N$. Wäre $J_N = A$, so gälte $1 \in J_N$, also $1 \in J$ für ein $J \in N$. Dann wäre aber $J = A$, und das war ausgeschlossen.
Damit ist J_N eine obere Schranke für N. Nach dem Zornschen Lemma hat M ein maximales Element. Dies ist das gesuchte maximale Ideal. □

Da jeder Ring wenigstens das Nullideal hat, können wir uns nun leicht Körper als Quotienten von Ringen konstruieren.

Bemerkung. In den beiden für uns wichtigsten Ringen ($k[X]$ und $\mathbb{Z}$) folgt die Existenz von maximalen Idealen ohne Zornsches Lemma. Es wird ein Nebenprodukt der Strukturtheorie sein.

Definition 4.10. *Seien $a_1, a_2, \ldots, a_n \in A$ Elemente eines Rings A. Dann ist*

$$(a_1, \ldots, a_n) = Aa_1 + \ldots Aa_n = \{b_1 a_1 + \ldots b_n a_n \mid b_i \in A\}$$

das von den a_i erzeugte Ideal. Im Fall $n = 1$ heißt (a_1) Hauptideal*.*
Ein Ring heißt Hauptidealring*, wenn jedes Ideal ein Hauptideal ist und zusätzlich gilt: Falls $ab = 0$ in A, dann ist $a = 0$ oder $b = 0$.*

Beispiel. Wir haben bereits gesehen, dass Körper und $\mathbb{Z}$ Hauptidealringe sind. Im Fall von $\mathbb{Z}$ beruhte dies auf Division mit Rest. Dasselbe Argument funktioniert auch für $k[X]$.

Beispiel. $k[X,Y] = \{\sum_{i,j=0}^{n} a_{ij} X^i Y^j \mid a_{ij} \in k\}$ ist kein Hauptidealring, denn (X,Y) wird *nicht* von einem einzigen Polynom erzeugt.
Auch viele andere Ringe nicht, etwa $\mathbb{Z}[\sqrt{-5}] = \{a + b\sqrt{-5} \mid a, b \in \mathbb{Z}\}$ ist keiner, wohl aber $\mathbb{Z}[i]$ (keine Beweise, Hinweis $(1+\sqrt{-5})(1-\sqrt{-5})$). Dies führt in die algebraische Zahlentheorie.

Direkter Beweis von Satz 4.8 für Hauptidealringe: Sei A ein Hauptidealring. Sei $I \subsetneq A$ ein Ideal. Angenommen I ist nicht in einem maximalen Ideal enthalten. Dann ist insbesondere I nicht maximal, also gibt es $I \subsetneq I_1 \subsetneq A$. Auch I_1 ist nicht maximal also finden wir ein I_2 etc. Wir konstruieren eine Kette von Idealen

$$I \subsetneq I_1 \subsetneq I_2 \subsetneq I_3 \subsetneq \cdots \subsetneq .A$$

Sei $J = \bigcup I_n$. Wie im ersten Beweis des Satzen sehen wir, dass J ein Ideal ist. Da A ein Hauptidealring ist, gilt $J = (x)$ für ein $x \in J$. Dieses liegt in I_n für in n. Es folgt

$$J = (x) \subset I_n \subsetneq I_{n+1} \subset J.$$

Dies ist ein Widerspruch. □

Polynomringe

Sei von nun an k ein Körper.

Satz 4.11. *Sei k ein Körper. Dann ist $k[X]$ ein* Hauptidealring*, d.h. jedes Ideal ist von der Form $(P) = \{QP \mid Q \in k[X]\}$ für ein Polynom $P \in k[X]$.*

Der Beweis des Satzes braucht etwas Vorarbeit.

Definition 4.12. *Sei $P = a_0 + \cdots + a_n X^n$ mit $a_n \neq 0$. Dann ist* $\deg(P) = n$ *der* Grad *von P. Für $P = 0$ setzen wir* $\deg P = -\infty$.

Bemerkung. Es gilt offensichtlich:

$$\deg(P+Q) \leq \max(\deg P, \deg Q)$$
$$\deg(PQ) = \deg P + \deg Q$$

Satz 4.13 (Euklidischer Algorithmus)**.** *Seien $P, Q \in k[X]$ zwei Polynome, $Q \neq 0$. Dann gibt es (eindeutige) Polynome P_1, R mit* $\deg R < \deg Q$*, so dass*

$$P = P_1 Q + R\ .$$

Beweis: Zunächst zur Existenz. Der Fall $P = 0$ ist trivial. Ist $\deg P < \deg Q$, so löst

$$P = 0 \cdot Q + P$$

die Aufgabe. Sei nun $\deg P \geq \deg Q$. Wir schließen weiter mit Induktion nach $n = \deg P$.

$$P = a_n X^n + \ldots a_0\ ;\ Q = b_m X^m + \ldots b_0$$

Sei $H = \frac{a_n}{b_m} X^{n-m}$. Damit folgt

$$\deg(P - HQ) < n$$

denn der höchste Koeffizient (der von X^n) ist $a_n - \frac{a_n}{b_m} b_m = 0$. War $n = 0$, so bedeutet dies $P = HQ$, also den Induktionsanfang. Sonst gibt es nach Induktionsvorraussetzung H_1 mit

$$P - HQ = H_1 Q + R \text{ mit } \deg(R) < \deg Q \ .$$

Es folgt

$$P = (H + H_1)Q + R \text{ mit } \deg(R) < \deg Q \ .$$

Mit $P_1 = H + H_1$ haben wir das Problem gelöst.
Es fehlt die Eindeutigkeit. Seien

$$P = P_1 Q + R_1 \text{ und } P = P_2 Q + R_2 \text{ mit } \deg(R_i) < \deg Q \ .$$

Differnzbildung liefert

$$0 = (P_1 - P_2)Q + (R_1 - R_2) \Rightarrow (P_2 - P_1)Q = R_1 - R_2 \ .$$

Der Grad der rechten Seite ist echt kleiner als $\deg Q$. Dies ist nur möglich, falls $P_2 - P_1 = 0$. Damit ist auch $R_1 - R_2 = 0$. □

Bemerkung. Wir haben ausgenutzt, dass k ein Körper ist!
In dieser Induktion steckt natürlich die Polynomdivision wie in der Schule (?).

Beispiel.

$$\begin{array}{llll}
(X^4 & +3X^3 & +2X^2 & \\
X^4 & & -X^2 & \\
\hline
 & 3X^3 & +3X^2 & \\
 & 3X^3 & & -3X \\
\hline
 & & 3X^2 & +3X \\
 & & 3X^2 & & -3 \\
\hline
 & & & & 3X+3
\end{array}
\qquad) : (X^2 - 1) = X^2 + 3X + 3$$

Wir erhalten $P_1 = X^2 + 3X + 3$, $R = 3X + 3$.

Beweis von Satz 4.11. Sei $I \subset k[X]$ ein Ideal. Fall $I = 0$, so ist $I = (0)$, also ein Hauptideal. Sei nun $Q \in I$ mit $Q \neq 0$ ein Element von minimalem Grad.

Behauptung. $I = (Q)$.

Sei $P \in I$ beliebig. Mit euklidischem Algorithmus erhalten wir

$$P = P_1 Q + R \Rightarrow R = P - P_1 Q \in I \ .$$

Nach Wahl von R gilt $\deg R < \deg Q$, aber Q hatte minimalen Grad. Es folgt $R = 0$, also ist P ein Vielfaches von Q. □

Bemerkung. Vergleichen Sie mit dem Beweis von Lemma 2.5 (ii) (Klassifikation der Untergruppen von $\mathbb{Z}$)!

Lemma 4.14. *Sei $P \in k[X]$, $P \neq 0$. Dann hat $k[X]/(P)$ die k-Dimension* $\deg P$.

Beweis: Sei $n = \deg P - 1$. Wir betrachten die Abbildung

$$\phi : k^{n+1} \to k[X]/(P) \ ; \ (a_0, \ldots, a_n) \mapsto a_0 + a_1 X + \ldots a_n X^n + (P)$$

Dies ist eine k-lineare Abbildung.

Behauptung. *ϕ ist injektiv.*

Sei $\phi(a_0, \ldots, a_n) = 0 + (P)$, d.h. P teilt $Q = a_0 + a_1 X + \ldots a_n X^n$. Da der Grad von P echt größer ist als der Grad von Q, muss $Q = 0$ sein.

Behauptung. *ϕ ist surjektiv.*

Sei $Q + (P)$ ein beliebiges Element von $k[X]/(P)$. Nach euklidischem Algorithmus gibt es Q_1 und R mit $\deg R < \deg P = n + 1$, so dass

$$Q = Q_1 P + R \ .$$

Also ist $Q + (P) = Q_1 P + R + (P) = R + (P)$. Letzteres liegt offensichtlich im Bild von ϕ. □

Definition 4.15. *Sei A ein Ring. Ein Element $a \in A$ heißt* Einheit*, wenn es invertierbar ist bezüglich der Multiplikation. Die Menge der Einheiten wird A^* notiert.*

Ein Element heißt unzerlegbar*, wenn es keine Einheit ist und nicht als nichttriviales Produkt geschrieben werden kann, d.h. falls $a = a_1 a_2$, so ist a_1 oder a_2 eine Einheit.*

Bemerkung. Es gilt

$$\mathbb{Z}^* = \{\pm 1\}, \qquad k[X]^* = k^* = k \setminus \{0\} \ .$$

Ein Element des Polynomrings ist genau dann Einheit, wenn $\deg P = 0$.

Die positiven unzerlegbaren Elemente von $\mathbb{Z}$ sind die Primzahlen.

Ein Polynom $P \in k[X]$ mit $\deg P > 0$ heißt *irreduzibel*, falls es unzerlegbar ist, d.h. P nicht von der Form $P = P_1 P_2$ mit $\deg P_1, \deg P_2 > 0$ ist.

Bemerkung. Im allgemeinen ist der Erzeuger eines Hauptideals nur eindeutig bis auf Multiplikation mit einer Einheit. In $\mathbb{Z}$ ist der Erzeuger eines Ideals eindeutig bestimmt, wenn man verlangt, dass er positiv ist. Er ist das eindeutig bestimmte minimale positive Element in I (Ausnahme $I = 0$).

Definition 4.16. *Ein Polynom heißt* normiert*, falls der höchste Koeffizient* 1 *ist, also*

$$P = X^n + a_{n-1}X + \cdots + a_0 \ .$$

Der Erzeuger Q eines Ideals $I \subset k[X]$ ist eindeutig bestimmt, wenn man verlangt, dass er normiert ist. Er ist das eindeutig bestimmte normierte Element von minimalem Grad in I (Ausnahme $I = 0$).

Satz 4.17. *Sei A ein Hauptidealring, $a \in A$ unzerlegbar. Dann ist der Ring $A/(a)$ ein Körper.*

Beweis: Zu zeigen ist, dass (a) maximales Ideal ist. Die Teilbarkeitsbeziehungen Elementen übersetzen sich genau in Enthaltenseinsrelationen von Idealen. Also (a) maximal bezüglich $\subset$ genau dann wenn a minimal bezüglich Teilbarkeit. □

Bemerkung. Der Satz ist falsch, wenn A kein Hauptidealring ist. Dann ist $X \in k[X, Y]$ unzerlegbar, aber $k[X, Y]/(X) \cong k[X]$ ist kein Körper. Das Ideal (X) ist maximal unter den Hauptidealen, aber nicht unter allen Idealen. Z.B. $(X) \subsetneq (X, Y)$.

Korollar 4.18. *Sei $P \in k[X]$. Der Ring $k[X]/(P)$ ist genau dann ein Körper, wenn P ein irreduzibles Polynom ist.*

Wie steht es mit der Zerlegung von Polynomen in unzerlegbare Faktoren?

Lemma 4.19. *Sei A ein Hauptidealring, a unzerlegbar. Dann ist a* prim*, d.h. wenn ein Produkt $a_1 \dots a_n$ durch a teilbar ist, dann auch einer der Faktoren.*

Beweis: Es genügt den Fall $n = 2$ zu betrachten. Angenommen, a teilt weder a_1 noch a_2.
Wir betrachten das Ideal

$$I_1 := (a, a_1) = (s_1) \ ,$$

denn alle Ideal sind Hauptideale. Es gilt

$$a = t_1 s_1 \ .$$

Da a unzerlegbar ist, ist s_1 oder t_1 eine Einheit. Im zweiten Fall ist mit s_1 auch a ein Teiler von a_1, Widerspruch. Also ist s_1 Einheit, ohne Einschränkung $s_1 = 1$. Analog folgt

$$I_2 := (a, a_2) = (1) \ .$$

Konkret:

$$1 = x_i a + y_i a_i$$

mit $x_i, y_i \in A$. Multiplikation liefert

$$1 = x_1 x_2 a^2 + x_1 a y_2 a_2 + x_2 a y_1 a_1 + y_1 y_2 a_1 a_2 \ .$$

Mit $a_1 a_2 = a$ ist demnach a ein Teiler von 1, ein Widerspruch. □

Theorem 4.20 (Primfaktorzerlegung)**.** *Sei A ein Hauptidealring, $a \in A$ ungleich 0. Dann gibt es eine Darstellung*

$$a = u a_1 \dots a_n$$

mit einer Einheit u und unzerlegbaren Elementen a_i. Diese Darstellung ist eindeutig bis auf Reihenfolge und Wahl von a_i bis auf Einheit. Mit anderen Worten, die Darstellung als Produkt von maximalen Idealen

$$(a) = (a_1) \dots (a_n)$$

ist eindeutig bis auf Reihenfolge.

Bemerkung. Wir haben Einheiten als unzerlegbare Elemente ausgeschlossen, damit der Satz gelten kann! Insbesondere ist 1 keine Primzahl.

Wir verzichten auf den Beweis für allgemeine A, sondern behandeln nur den für uns entscheidenden Fall $A = k[X]$. Der andere besonders wichtige Fall $A = \mathbb{Z}$ geht genauso.

Theorem 4.21 (Primfaktorzerlegung)**.** *Jedes Polynom $P \neq 0$ kann eindeutig (bis auf Reihenfolge) in der Form*

$$P = a P_1^{e_1} P_2^{e_2} \dots P_n^{e_n}$$

geschrieben werden, wobei $a \in k$, $n \geq 0$, $P_i \in k[X]$ irreduzibel und normiert, $e_i > 0$.

Beweis: Existenz: Wenn P nicht irreduzibel ist, zerlegen wir es in zwei Faktoren. Sollten diese nicht irreduzibel sein, zerlegen wir weiter, etc. Der Prozess endet nach endlich vielen Schritten, da jeweils der Grad heruntergeht.

Eindeutigkeit: a ist der höchste Koeffizient von P, ohne Einschränkung $a = 1$. Sei

$$P = P_1^{e_1} P_2^{e_2} \dots P_n^{e_n} = Q_1^{f_1} Q_2^{f_2} \dots Q_m^{e_m}$$

mit irreduziblen P_i, Q_j. Dann teilt P_1 das rechte Produkt, also ein Q_j, ohne Einschränkung Q_1. Da P_1 und Q_1 beide irreduzibel und normiert, folgt $P_1 = Q_1$. Wir teilen durch P_1 und fahren mit Induktion fort. □

Ab jetzt dürfen Sie mit gutem Gewissen Teilbarkeitsargumente in $\mathbb{Z}$ benutzen.

Korollar 4.22. *Sei P ein Polynom vom Grad n. Dann hat P höchstens n Nullstellen in k.*

Beweis: Sei $a \in k$ mit $P(a) = 0$ in k. Mit euklidischem Algorithmus folgt

$$P = P_1(X - a) + R \text{ , } \deg R < 1,$$

also ist R konstant. Einsetzen von a in die Gleichung ergibt

$$0 = P(a) = P_1(a)(a - a) + R(a) = R(a) \ .$$

Demnach ist $R = 0$ und $X - a$ ist ein Teiler von P. Da die Zerlegung in irreduzible Faktoren eindeutig ist, gibt es höchstens n Nullstellen. □

Da wir Körper konstruieren wollen, benötigen wir Kriterien, um zu entscheiden, ob ein Polynom irreduzibel ist.

Beispiel.

- $X^2 + 1 \in \mathbb{R}[X]$, denn $\mathbb{R}[X]/(X^2 + 1) \cong \mathbb{C}$ ist ein Körper. Oder: Wäre $X^2 + 1$ nicht irreduzibel, dann ist es Produkt von Linearfaktoren, also hätte es eine Nullstelle, also $a \in \mathbb{R}$ mit $a^2 = -1$. Dies ist unmöglich, denn Quadrate sind in $\mathbb{R}$ immer positiv.
- $X^2 + 1 \in \mathbb{C}[X]$ ist nicht irreduzibel, denn $X^2 + 1 = (X + i)(X - i)$.
- $X^4 - 2 \in \mathbb{Q}[X]$ ist ebenfalls irreduzibel.

  Beweis: Sei $a = \frac{p}{q}$ mit $p, q \in \mathbb{Z}$ teilerfremd. Es folgt $p^4 = 2q^4$, also 2 teilt p. Also teilt 2^4 die rechte Seite, insbesondere 2^3 teilt q^4. Es folgt 2 teilt q. Widerspruch zu p und q teilerfremd! Demnach hat $X^4 - 2$ keine Nullstellen. Ist es auch irreduzibel? Es könnte noch Produkt von zwei Faktoren vom Grad 2 sein, ohne Einschränkung beide normiert.

  $$X^4 - 2 = (X^2 + a_1X + a_0)(X^2 + b_1 + b_0) =$$
  $$X^4 + (b_1 + a_1)X^3 + (b_0 + a_0 + a_1b_1)X^2 + (a_1b_0 + b_1a_0)X + a_0b_0$$

  Es folgt $0 = b_1 + a_1$, d.h. $b_1 = -a_1$. Ebenso $0 = b_0 + a_0 + a_1b_1 = b_0 + a_0 - a_1^2$, d.h. $b_0 = -a_0 + a_1^2$. Weiter

  $$0 = a_1b_0 + b_1a_0 = a_1(-a_0 + a_1^2) - a_1a_0 = a_1(a_1^2 - 2a_0)$$

  Also ist entweder $a_1 = 0$. Dann folgt $b_1 = 0, b_0 = -a_0$ und $-2 = a_0b_0 = -a_0^2$ ist unmöglich in $\mathbb{Q}$ (Übungsaufgabe). Oder es ist $a_1^2 = 2a_0$, also $a_0 = \frac{1}{2}a_1^2, b_0 = -\frac{1}{2}a_1^2 + a_1^2 = \frac{1}{2}a_1^2$. Es folgt $-2 = a_0b_0 = -\frac{1}{4}a_1^4$ d.h. $8 = a_1^4$, aber 8 ist keine 4-te Potenz (Übungsaufgabe). □

Systematischer:

Satz 4.23 (Gauß)**.** *Sei $P \in \mathbb{Z}[X]$ ein Polynom. Wenn $P = QR$ in $\mathbb{Q}[X]$ mit $\deg Q, \deg R > 0$, dann gilt bereits $P = Q'R'$ mit ganzzahligen Polynomen Q', R', $Q' = \beta Q$, $R' = \gamma R$ für $\beta, \gamma \in \mathbb{Q}$.*

Beweis: Sei $Q = b_m X^m + \cdots + b_0$, $R = c_k X^k + \cdots + c_0$. Sei β der Hauptnenner der b_i, γ der Hauptnenner der c_j. Sei $\alpha = \beta\gamma$. Wir betrachten $\alpha P = \beta Q \gamma R = Q'R'$. Dabei sind $b'_j = \beta b_j$, $c'_i = \gamma c_i$ ganz.
Sei p ein Primteiler von α. Wir reduzieren die Gleichung modulo p underhalten

$$0 = \overline{Q'}\,\overline{R'} \in \mathbb{F}_p[X].$$

Es folgt $\overline{Q'} = 0$ oder $\overline{R'} = 0$, d.h. entweder alle b'_i oder alle c'_j sind durch p teilbar.
Wenn q alle b'_i teilt, so kann der Faktor aus α und Q' gekürzt werden. Induktiv erreicht man $\alpha = \pm 1$. □

Oft kennt man nur die einfachere Form:

Korollar 4.24. *Sei $P \in \mathbb{Z}[X]$ normiert, $\alpha \in \mathbb{Q}$ eine Nullstelle von P. Dann liegt α in $\mathbb{Z}$.*

Beweis: Nach Vorraussetzung ist $P = (X - \alpha)Q$ mit $Q \in \mathbb{Q}[X]$ ebenfalls normiert. Nach dem Gaußkriterium folgt $P = (\beta X - \beta\alpha)(\gamma Q)$ mit ganzzahligen Faktoren, also liegen auch die Koeffizienten $\beta, \beta\alpha, \gamma \in \mathbb{Z}$. Für den höchsten Koeffizienten gilt $1 = \beta\gamma$, also $\beta, \gamma = \pm 1$. Es folgt $\alpha \in \mathbb{Z}$. □

Sehr nützlich ist die folgende Variante:

Satz 4.25 (Eisensteinkriterium)**.** *Sei $P = a_n X^n + \cdots + a_0 \in \mathbb{Q}[X]$, $n \geq 1$, $a_i \in \mathbb{Z}$. Sei p eine Primzahl mit $p \mid a_0, \ldots a_{n-1}$, p kein Teiler von a_n, p^2 kein Teiler von a_0. Dann ist P irreduzibel.*

Beispiel. $P = X^4 - 2$ mit $p = 2$.

Beweis: Sei $P = QR$ mit $Q = b_m X^m + \cdots + b_0$, $R = c_k X^k + \cdots + c_0$. Nach dem Gaußkriterium können b_i, c_j in $\mathbb{Z}$ gewählt werden. Wir reduzieren modulo p und erhalten in $\mathbb{F}_p[X]$ die Gleichung

$$\overline{Q}\,\overline{R} = \overline{P} = \overline{a} X^n, \overline{a} \neq 0$$

Hieraus folgt $\overline{Q} = \overline{b_m} X^m$, $\overline{R} = \overline{c_k} X^k$, d.h. alle anderen Koeffizienten sind durch p teilbar. Insbesondere ist $b_0 c_0$ durch p^2 teilbar, Widerspruch. □

Beispiel. Sei p eine Primzahl, $P = 1 + X + X^2 + \cdots + X^{p-1} = \frac{X^p - 1}{X - 1}$. Trick: Wir ersetzen X durch $Y + 1$. Man erhält

$$P(Y) = \frac{(Y+1)^p - 1}{Y} = \frac{\sum_{i=0}^{p} \binom{p}{i} Y^i - 1}{Y} = \sum_{i=1}^{p} \binom{p}{i} Y^{i-1}$$

Jeder der Binomialkoeffizienten ist durch p teilbar, da dieser Faktor durch den Nenner nicht weggekürzt wird. Der konstante Term ist p, also nicht durch p^2 teilbar. Das Eisensteinkriterium greift, also ist $P(Y)$ irreduzibel. Dann ist aber auch $P(X)$ irreduzibel.

Kapitel 5

Grundbegriffe der Körpertheorie

Basics

Der Vollständigkeit halber:

Definition 5.1. *Ein* Körper *ist ein Ring K (kommutativ mit Eins), in dem $0 \neq 1$ und $(K \setminus \{0\}, \cdot)$ eine Gruppe ist. Ein* Körperhomomorphismus *ist eine Abbildung*

$$\alpha : K \to L \ ,$$

die ein Ringhomomorphismus von Ringen mit Eins, also $\alpha(1) = 1$, zwischen zwei Körpern ist.

Beispiel. (i) $\mathbb{Q}, \mathbb{R}, \mathbb{C}$.

(ii) $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ für p eine Primzahl.

(iii) k ein Körper. $k(X) = \left\{ \frac{P}{Q} \mid P, Q \in k[X], Q \neq 0 \right\}$ mit der Isomorphie, Addition und Multiplikation von Brüchen.

(iv) $\overline{\mathbb{Q}} = \{ z \in \mathbb{C} \mid \ z$ ist Nullstelle eines Polynoms in $\mathbb{Q}[X] \}$. (Übungsaufgabe, wird sehr gerne in Prüfungen gefragt)

(v) $k((X)) = \left\{ \sum_{i=n}^{\infty} a_i X^i \mid n \in \mathbb{Z}, a_i \in k \right\}$ mit der Addition und Muliplikation von Reihen (Übungsaufgabe)

Satz 5.2. *Alle Körperhomomorphismen sind injektiv.*

Beweis: Der Kern eines Ringhomomorphismus ist ein Ideal, also in diesem Fall 0 oder der ganze Körper. Da 1 nicht im Kern liegt, muss es das Nullideal sein. □

Wegen der Injektivität identifizieren wir oft einen Körper mit seinem Bild unter einem Körperhomomorphismus.

Definition 5.3. *Sei L ein Körper, $K \subset L$ eine Teilmenge, die mit der Addition und Multiplikation von L zu einem Körper wird. K heißt* Teilkörper *von L und L ein* Erweiterungskörper *von K. Wir sagen, L/K (lies: L über K) ist eine* Körpererweiterung.

Beispiel. $\mathbb{C}/\mathbb{R}$, $\mathbb{R}/\mathbb{Q}$, $\mathbb{F}_p(X)/\mathbb{F}_p$.

Definition 5.4. *Ein Element $a \in L$ heißt* algebraisch *über K, falls es ein Polynom $0 \neq P \in K[X]$ gibt mit $P(a) = 0$. Das Element a* erfüllt die algebraische Gleichung *P. Die Erweiterung L/K heißt* algebraisch*, wenn alle Elemente von L algebraisch über K sind.*

Beispiel. (i) K/K ist algebraisch, denn $a \in K$ erfüllt die Gleichung $X - a \in K[X]$.

(ii) $\overline{\mathbb{Q}} = \{z \in \mathbb{C} \mid z \text{ ist algebraisch über } \mathbb{Q}\}$ enthält i als Nullstelle von $X^2 + 1$, $\sqrt{3}$, $\sqrt[7]{26 + \sqrt[3]{1/5}}$ als Nullstelle von $(X^7 - 26)^3 = 1/5$.

(iii) $X \in \mathbb{F}_p(X)$ ist nicht algebraisch über $\mathbb{F}_p$.

Frage: Seien $a, b \in L/K$ algebraisch. Sind $a + b, ab$ algebraisch?

Entscheidende Idee: Wenn L/K eine Körpererweiterung ist, dann ist L ein K-Vektorraum! Damit können wir alle Begriffe und Resultate der linearen Algebra ins Rennen schicken.

Definition 5.5. *Sei L/K eine Körpererweiterung. $[L : K] = \dim_K L$ heißt Grad der Erweiterung. Ist er endlich, so heißt die Erweiterung* endlich.

Bemerkung. Der Grad der Körpererweiterung ist ein weiteres Beispiel für eine *Invariante* einer mathematischen Struktur. Wir haben bereits kennengelernt:

- Die Ordnung einer endlichen Gruppe.
- Der Grad eines Polynoms.
- Der Betrag einer ganzen Zahl.

Jede dieser Invarianten war ein wertvolles Hilfsmittel beim Studium der Objekte. Auch unsere neue, einfache Invariante wird große Konsequenzen haben, etwa bei den Fragen nach der Konstruierbarkeit mit Zirkel und Lineal. Später werden wir mit der Galoisgruppe eine raffiniertere Invariante von L/K studieren.

Satz 5.6. *Sei L/K endliche Körpererweiterung. Dann ist L/K algebraisch.*

Beispiel. $\mathbb{C}/\mathbb{R}$

Beweis: Sei $[L : K] = n$, $a \in L$. Dann ist die Menge $\{1, a, a^2, a^3, \ldots, a^n\}$ linear abhängig über K (Ausnahme: $a^i = a^j$ für ein $i < j \leq n$, dann ist a Nullstelle von $X^i - X^j$), denn sie hat mehr Elemente als die Dimension ist. Also existieren Elemente $a_0, \ldots, a_n \in K$, nicht alle gleichzeitig 0 mit

$$a_0 1 + a_1 a + \ldots a_n a^n = 0 \ .$$

Also ist a Nullstelle von $P = a_0 + a_1 X + \ldots a_n X^n$. □

Die Umkehrung gilt nicht! $\overline{\mathbb{Q}}/\mathbb{Q}$ ist unendlich (später). Dennoch ist der Zusammenhang sehr eng. Wir bezeichnen mit $K[a] \subset L$ den kleinsten Teilring, der K und a enthält, mit $K(a) \subset L$ den kleinsten Teilkörper, der K und a enthält.

Satz 5.7. *Sei L/K Körpererweiterung, $a \in L$. Dann sind äquivalent:*

(i) a ist algebraisch über K.

(ii) $K[a]$ ist endlich-dimensional als K-Vektorraum.

(iii) $K[a]$ ist ein Körper.

(iv) $K(a)$ ist endlich-dimensional als K-Vektoraum.

Für den Beweis führen wir einige weitere Begriffe ein. Der Ring $K[a]$ ist das Bild des Ringhomomorphismus

$$K[X] \to L; \sum a_i X^i \mapsto \sum a_i a^i.$$

Sei $I \subset K[X]$ der Kern. Dies sind die Polynome mit Nullstelle a. Nach Definition ist also $I \neq 0$ genau dann, wenn a algebraisch ist.

Definition 5.8. *Sei L/K eine Körpererweiterung, $a \in L$ algebraisch. Dann heißt der eindeutige normierte Erzeuger des Kerns des Einsetzungshomomorphismus $K[X] \to K[a]$* Minimalpolynom von a. *Wir schreiben* $\mathrm{Min}(a) \in K[X]$.

Mit anderen Worten: Das Minimalpolynom ist das Polynom kleinsten Grades mit Nullstelle a. Es teilt alle anderen Polynome, die von a erfüllt werden. Wir haben damit gezeigt:

$$K[a] \cong K[X]/\mathrm{Min}(a).$$

Beweis von Satz 5.7: Wir betrachten den Einsetzungshomomorphismus. Wie oben sei I der Kern. Nach dem Homorphiesatz gilt

$$K[X]/I \cong K[a].$$

Falls a nicht algebraisch ist, so ist also $K[X] \cong K[a]$, insbesondere $\dim_K K[a] = \infty$. Es handelt sich nicht um einen Körper und $\dim_K K(a) \geq \dim_K K[a] = \infty$.

Falls a algebraisch ist, so gilt nach Lemma 4.14, $\dim_K K[a] = \deg(\mathrm{Min}(a)) < \infty$. Wir zeigen, dass es sich nun um einen Körper handelt. Sei $b \in K[a]$, $b \neq 0$. Wir betrachten die K-lineare Abbildung

$$K[a] \to K[a]; x \mapsto bx.$$

Sie ist injektiv, denn $bx = 0$ im Körper L impliziert $b = 0$ oder $x = 0$. Als injektiver Automorphismus eines endlich-dimensionalen K-Vektorraums ist die Abbildung auch surjektiv. Sei b' das Urbild von 1. Dies ist das gesuchte Inverse von b. Da $K[a]$ nun ein Körper ist, gilt sogar $K[a] = K(a)$ und auch letzterer ist endlich-dimensional über K. □

Korollar 5.9. *Sei L/K eine Körpererweiterung und $a \in L$ algebraisch über K. Dann ist* $\mathrm{Min}(a)$ *irreduzibel.*

Beweis: Wir haben gesehen, dass in dieser Situation $K[X]/\mathrm{Min}(a)$ isomorph ist zu dem Körper $K[a]$. Also erzeugt $\mathrm{Min}(a)$ ein maximales Ideal. Das ist genau für irreduzible Polynome der Fall. □

Satz 5.10 (Gradformel)**.** *Sind M/L und L/K endliche Körpererweiterungen, so auch M/K. Es gilt*

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

Beweis: Sei $y_1, \ldots, y_n$ eine L-Basis von M und $x_1, \ldots, x_m$ eine K-Basis von L.

Behauptung. $\{x_i y_j \mid i = 1, \ldots, n, j = 1, \ldots m\}$ *ist eine K-Basis von M.*

Sei $y \in M$. Dann ist

$$y = \sum_{j=1}^{m} a_j y_j \text{ für gewisse } a_j \in L \ .$$

$a_j \in L$. Dann ist

$$a_j = \sum_{i=1}^{n} b_{ij} x_i \text{ für gewisse } b_{ij} \in K \ .$$

Es folgt

$$y = \sum_{j=1}^{m} \sum_{i=1}^{n} b_{ij} x_i y_j \ ,$$

die $x_i y_j$ erzeugen M. Sei

$$\sum_{i,j} a_{ij} x_i y_j = 0 \in M \text{ mit } a_{ij} \in K$$

Dann ist $\sum_j (\sum_k a_{ij} x_i) y_j = 0$ eine Relation mit Koeffizienten in L. Wegen linearer Unabhängigkeit der y_j folgt $sum_i a_{ij} x_i = 0$. Wegen linearer Unabhängigkeit der x_i in L folgt $a_{ij} = 0$ für alle i, j. □

Korollar 5.11. *Sei L/K eine Körpererweiterung, $a, b \in L$ seien algebraisch über K. Dann sind $a+b, a-b, ab, a^{-1}$ alle algebraisch über K.*

Beweis: Sei a algebraisch, also $K(a)/K$ endlich. b ist algebraisch über K, also erst recht über $K(a)$, also ist $K(a)(b)/K(a)$ endlich. Nach dem Satz ist dann auch $K(a)(b)/K$ endlich. Die genannten Elemente liegen alle in $K(a,b) = K(a)(b)$. □

Damit haben wir endlich geklärt, dass $\overline{\mathbb{Q}}$ ein Körper ist.

Korollar 5.12. *Seien M/L und L/K algebraische Körpererweiterungen. Dann ist auch M/K algebraisch.*

Beweis: Sei $a \in M$. Da M/L algebraisch, gibt es ein Minimalpolynom $X^n + a_{n-1}X^{n-1} + \cdots + a_0 \in L[X]$. Dann ist a algebraisch über $K(a_0, \ldots, a_{n-1})$, liegt also in der endlichen Erweiterung $K(a_0, \ldots, a_{n-1}, a)/K$. □

Konstruktion von Körpererweiterungen

Bisher sind wir davon ausgegangen, dass gewisse Elemente oder Körpererweiterungen algebraisch sind und haben deren Eigenschaften konstruiert. Nun wenden wir uns der Konstruktion von algebraischen Erweiterungen zu. Sei also K ein Körper, $P \in K[X]$ ein Polynom. Wir suchen einen Erweiterung L/K, in der P eine Nullstelle a hat. Unsere bisherigen Überlegungen sagen, dass dann $K[a] \cong K[X]/\operatorname{Min}(a)$ und $\operatorname{Min}(a)$ ist ein irreduzibler Faktor von P.

Satz 5.13. *Sei K ein Körper, $P \in K[X]$ ein irreduzibles Polynom vom Grad n, $L = K[X]/(P)$. Dann ist L/K eine endliche Erweiterung vom Grad n. Das Polynom P hat eine Nullstelle in L.*

Beweis: Da P irreduzibel ist, ist $L = K[X]/P$ ein Körper. Nach Lemma 4.14 hat er den Grad n.
Sei ξ die Nebenklasse von X in $K[X]/P$. Mit anderen Worten: $\xi = \pi(X)$, wobei $\pi : K[X] \to K[X]/(P)$ die kanonische Projektion. Es gilt

$$P(\xi) = P(\pi(X)) = \pi(P) = 0 \in L$$

denn π ist ein Ringhomomorphismus. □

Bemerkung. Eigentlich haben wir nur einen Körperhomomorphismus $K \to L$. Wir identifizieren K mit seinem Bild.

Beispiel. $K = \mathbb{R}$, $P = X^2 + 1$, $L = K[X]/(X^2+1) \cong \mathbb{C}$.

Korollar 5.14. *Sei $P \in K[X]$ ein nicht-konstantes Polynom. Dann existiert eine algebraische Erweiterung von L/K, in der P in Linearfaktoren zerfällt.*

$$P(X) = a \prod_{i=1}^{n} (X - \alpha_i) \ , \ \alpha_i \in L, n = \deg P \, a \in K.$$

Man kann L so wählen, dass $[L : K] \leq n!$.

Beweis: Induktion nach n für alle Körper gleichzeitig. Der Fall $n = 1$ ist trivial. Sei Q ein irreduzibler Faktor von P. Es ist $1 \leq \deg Q \leq \deg P$. Nach Satz 5.13 gibt es eine Erweiterung L_1/K mit $[L_1 : K] = m \leq n$, so dass Q (und damit auch P) eine Nullstelle α_1 in L_1 hat. Über L_1 gilt

$$P(X) = (X - \alpha_1)P_1(X) \ , \ P_1(X) \in L_1(X) \ .$$

Nach Induktionsvoraussetzung gibt es L/L_1 mit $[L : L_1] \leq (n-1)!$, so dass P_1 (und damit auch P) in Linearfaktoren zerfällt. Aus der Gradformel 5.10 folgt

$$[L : K] = [L : L_1][L_1 : K] \leq (n-1)! \cdot n \ .$$

□

Definition 5.15. *Ein Körper K heißt* algebraisch abgeschlossen, *wenn jedes nicht-konstante Polynom $P \in K[X]$ über K eine Nullstelle hat.*

Bemerkung. Äquivalent sind: Jedes nicht-konstante Polynom $P \in K[X]$ zerfällt in Linearfaktoren. Die einzige algebraische Erweiterung von K ist K selbst.

Beispiel. $\mathbb{C}$, $\overline{\mathbb{Q}}$ (beides nicht-trivial!)

Satz 5.16. *Sei K ein Körper. Dann gibt es einen algebraischen Erweiterungskörper $\overline{K}/K$, der algebraisch abeschlossen ist. Er ist eindeutig bis auf Isomorphie.*

Beweis: Sei $\mathcal{P} \subset K[X]$ die Menge der nicht-konstanten Polynome. Sei

$$\mathcal{X} = \{X_f \mid f \in \mathcal{P}\}$$

eine Menge von Unbestimmten. $R = K[\mathcal{X}]$ sei der kommutative Polynomring in den Variablen X_f. Seine Elemente sind endliche K-Linearkombinationen von Monomen der Form

$$X_{f_1} X_{f_2} \dots X_{f_n} \ ,$$

wobei f_i's auch mehrfach vorkommen dürfen, und Produkte in unterschiedlicher Reihenfolge identifiziert werden. Das Element $X_f \in K[\mathcal{X}] = R$ kann in ein Polyonom $P \in K[X] \subset R[X]$ eingesetzt werden. Man erhält ein Element von R. Sei $J \subset R$ das Ideal, dass von den Elementen $f(X_f)$ für $f \in I$ erzeugt wird.

Behauptung. *$J \neq R$.*

Sonst ist $1 \in J$, also $1 = \sum_{i=1}^{n} g_i f_i(X_{f_i})$ mit $g_i \in K[\mathcal{X}]$. Sei L/K ein Erweiterungkörper, in dem f_i für $i = 1, \dots n$ die Nullstelle α_i haben (gibt es nach Satz 5.13). Über diesem Körper setzen wir α_i für X_{f_i} ein. Wir erhalten die Gleichung $1 = 0$, Widerspruch.

Nach Satz 4.8 hat R ein maximales Ideal M, das J enthält. Wir setzen $L_1 = R/M$. Dies ist ein Körper. Sei

$$K \to L_1$$

die Abbildung, die einem Element die Nebenklasse des konstanten Polynoms zuordnet. Dies ist ein Körperhomomorphismus. Wir fassen L_1 als Erweiterung von K auf. In L_1 hat $f \in \mathcal{P} \subset K[X]$ die Nullstellen $X_f + M$.
Iterativ konstruieren wir L_2/L_1, in dem alle nichtkonstanten Polynome in $L_1[X]$ eine Nullstelle haben, etc.

$$K \subset L_1 \subset L_2 \subset \dots$$

Behauptung. *$L = \bigcup L_i$ ist algebraisch abgeschlossen.*

Sei $P \in L[X]$. Die Koeffizienten liegen in verschiedenen L_i, also alle in dem größten vorkommenden L_i. Dann hat P eine Nullstelle in L_{i+1}.

Behauptung. *L/K is algebraisch.*

Es genügt zu zeigen, dass L_{i+1}/L_i algebraisch ist. Dies gilt, da die Ringerzeuger X_f algebraisch sind, nämlich Nullstelle von f.
Die Eindeutigkeit werden wir erst später zeigen. □

Kapitel 6

Konstruktion mit Zirkel und Lineal

Im antiken Griechenland war Mathematik Geometrie. Rationale Zahlen waren z.B. Verhältnisse von Streckenlängen. Die Entdeckung irrationaler Zahlen stürzte sie in eine Krise. Geometrie war wiederum Konstruktion mit Zirkel und Lineal.

Ansatz: Die Ebene wird identifiziert mit $\mathbb{C}$. Die Frage ist also, welche komplexen Zahlen mit Zirkel und Lineal aus einer Teilmenge $M \subset \mathbb{C}$ konstruiert werden können.

Erlaubt sind die folgenden Operationen:

(i) Festlegen einer Geraden durch zwei bereits konstruierte Punkte;

(ii) Festlegen eines Kreises mit Mittelpunkt bereits konstruiert und Radius der Abstand zweier konstruierter Punkte;

(iii) Schnitt von zwei konstruierten Geraden oder zweier konstruierter Kreise oder einer konstruierten Gerade mit einem konstruiertem Kreis.

Aus der Schule ist bekannt, wie z.B. mit Zirkel und Lineal das Lot von einem Punkt auf eine Gerade konstruiert werden kann. Zweifache Anwendung erlaubt die Konstruktion einer Parallele zu einer gegebenen Geraden.

Lemma 6.1. *Die Menge der Punkte in $\mathbb{C}$, die man mit Zirkel und Lineal aus $0, 1$ konstruieren kann, ist ein Teilkörper von $\mathbb{C}$.*

Beweis: Sei K die Menge dieser Punkte. Nach Vorraussetzung gilt $0, 1 \in K$.

Behauptung. *Sei $u + iv \in K$ $(u, v \in \mathbb{R})$. Dann ist $-u - iv \in K$.*

Konstruktion: Spiegelung am Nullpunkt.

Behauptung. *$a, b \in K$. Dann ist $a + b \in K$.*

Konstruktion: Konstruktion des Parallelogramms, das von a, b aufgespannt wird.

Behauptung. *Sei $x + iy \in K$. Dann liegen $x, y \in K$.*

Senkrechte Projektion auf die Achse durch $0, 1$ liefert x, als Differenz iy, durch Kreisschlagen y.

Behauptung. *$a, b \in K$. Dann ist $ab \in K$.*

$a = u+iv, b = x+iy \in K$, $(u, v, x, y \in \mathbb{R})$. $ab = (ux-vy)+i(uy+vx)$. Es genügt also, den Fall $a, b \in \mathbb{R} \cap K$ zu betrachten. Konstruktion durch Strahlensatztrick: Zwei Geraden, auf einer a, der anderen b und 1 abtragen. In b Parallele zur Geraden durch $1, a$.

Behauptung. *$a \in K \setminus \{0\}$. Dann liegt $a^{-1} \in K$.*

$a = u+iv$ mit $u, v \in \mathbb{R}$. Dann ist $a^{-1} = \frac{u-iv}{u^2+v^2}$. Es genügt also, den Fall $a \in K \cap \mathbb{R}$ zu betrachten. Dies geht wieder mit Strahlensatztrick. □

Um die Fragen nach Konstruierbarkeit zu beantworten, müssen wir also Eigenschaften des Körpers K studieren.

Lemma 6.2. *Sei $K \subset \mathbb{C}$ ein Teilkörper, $a \in K$. Dann ist $\sqrt{a}$ mit Zirkel und Lineal aus K konstruierbar.*

Beweis: Sei zunächst $a \in K \cap \mathbb{R}$ und $a > 0$. Wir betrachten den Thaleskreis über $[-1, a]$ und betrachten den Schnitt $z_0 = ih$ mit der imaginären Achse. Sei p die Strecke $[-1, z_0]$, q die Strecke $[a, z_0]$. Satz des Phythagoras:

$$(1+a)^2 = p^2 + q^2 \qquad 1 + h^2 = p^2 \qquad a^2 + h^2 = q^2$$
$$\Rightarrow 1 + 2a + a^2(1+a)^2 = 1 + 2h^2 + a^2 \Rightarrow a = h^2$$

Für allgemeines a arbeitet man in Polarkoordinaten. Die Wurzel aus $|a|$ und die Winkelhalbierende können mit Zirkel und Lineal konstruiert werden. □

Theorem 6.3. *Ein Element $z \in \mathbb{C}$ ist genau dann mit Zirkel und Lineal konstruierbar, wenn es eine Kette von Körpererweiterungen*

$$\mathbb{Q} = K_0 \subset K_1 \subset K_2 \subset \cdots \subset K_n$$

gibt mit $z \in K_n$, $[K_i : K_{i-1}] = 2$. Insbesondere ist z algebraisch über $\mathbb{Q}$ und $[\mathbb{Q}(z) : \mathbb{Q}]$ ist eine Potenz von 2.

Beweis: Wir beginnen mit der Hinrichtung. Sei K_n wie im Theorem. Wir zeigen, dass z mit Zirkel und Lineal konstruiert werden kann.

Beweis durch vollständige Induktion über n. Der Fall $n = 0$ folgt aus Lemma 6.1. Seien nun alle Elemente von K_n mit Zirkel und Lineal konstruierbar, $a \in K_{n+1} \setminus K_n$. Es gilt $K_n \subset K_n(a) \subset K_{n+1}$. Da die Erweiterung den Grad 2 hat, muss $K_{n+1} = K_n(a)$ gelten. Gleichzeitig ist $[K_n(a) : K_n]$ der Grad des Minimalpolynoms von a, also löst a eine quadratische Gleichung. Wir benutzen

die Lösungsformel. Mit dem Lemma 6.2 ist dann a und mit 6.1 auch ganz $K_n(a)$ mit Zirkel und Lineal konstruierbar.

Damit haben wir eine Richtung des Theorems gezeigt. Interessanter ist die Umkehrung.

Für diesen Beweis nennen wir ein Element von $\mathbb{C}$ *erreichbar*, wenn es in einem Körper K_n wie im Theorem liegt.

Behauptung. *$z_1, \dots z_n$ erreichbar $\Rightarrow$ alle Elemente von $\mathbb{Q}(z_1, \dots, z_n)$ sind erreichbar.*

Sei $z_1 \in K_n$ mit $\mathbb{Q} = K_0 \subset \cdots \subset K_n$ mit $K_i = K_{i-1}(\sqrt{a_{i-1}})$ und $z_2 \in L_m$ mit $\mathbb{Q} = L_0 \subset \cdots \subset L_m$. Setze $L_{m+i} = L_{m+i-1}(\sqrt{a_{i-1}})$. Es gilt $[L_{m+i} : L_{m+i-1}] = 1, 2$. Damit sind alle Elemente von L_{n+m} erreichbar. Dieser Körper enthält aber z_1 und z_2, also auch $\mathbb{Q}(z_1, z_2)$. Für mehr Elemente funktioniert das gleiche Argument.

Behauptung. *Mit z sind auch $\overline{z}$ und $|z|^2$ erreichbar.*

Hat man eine Kette von Körpern für z, so erhält man durch Anwenden von komplexer Konjugation eine Kette von Körpern für $\overline{z}$. Wegen $|z|^2 = z\overline{z} \in \mathbb{Q}(z, \overline{z})$ ist dann auch das Betragsquadrat erreichbar.

Behauptung. *Sei $z \in \mathbb{C}$ mit Zirkel und Lineal konstruierbar. Dann ist z erreichbar.*

Induktion über die Anzahl der benötigten Konstruktionsschritte. Der letzte Schritt der Konstruktion ist einer der folgenden:

(i) Schnitt zweier Geraden, die durch je zwei erreichbare Punkte festgelegt werden;

(ii) Schnitt einer Geraden, die durch zwei erreichbare Punkte festgelegt wird, mit einem Kreis mit erreichbarem Mittelpunkt und Radius der Abstand zweier erreichbarer Punkte;

(iii) Schnitt zweier Kreise mit erreichbaren Mittelpunkten Radius der Abstand zweier erreichbarer Punkte.

(i) Seien z_1, z_2, z_2, z_4 erreichbar. Sei l_1 eine Gerade durch z_1, z_2. Die Gerade wird beschrieben durch $t \mapsto z_1 + t(z_2 - z_1)$. Ebenso sei l_2 die Gerade durch z_3, z_4, Gleichung $z \mapsto z_3 + t(z_4 + z_3)$. Der Schnitt löst die Gleichung

$$z_1 + t_1(z_2 - z_1) = z_3 + t_2(z_4 + z_3).$$

Tatsächlich handelt es sich um 2 lineare Gleichungen - Realteil und Imaginärteil - für die beiden Unbekannten $t_1, t_2 \in \mathbb{R}$. Die Lösung liegt sogar in $\mathbb{Q}(z_1, z_2, z_3, z_4, \overline{z}_1, \overline{z}_2, \overline{z}_3, \overline{z}_4)$, ist also erreichbar.

(ii) Seien z_1 und z_2 erreichbar, r der Abstand zweier erreichbarer Punkte, also r^2 erreichbar. Sei l gegeben durch z_1, z_2, Gleichung $t \mapsto z_1 + t(z_2 - z_1)$. k sei ein Kreis um z_0 mit Radius r, Gleichung $|x - z_0|^2 = (x - z_0)(\overline{x}_0 - \overline{z_0}) = r^2$. Der Schnitt löst die Gleichung

$$(z_1 + t(z_2 - z_0))(\overline{z}_1 + t(\overline{z}_2 - \overline{z}_1)) = r^2 \ .$$

Dies ist eine quadratische Gleichung in $\mathbb{Q}(z_1, z_2, \overline{z}_1, \overline{z}_2, r^2)$. Nach Vorraussetzung und dem vorherigen sind die Elemente dieses Körpers erreichbar. Der Schnitt liegt in einer quadratischen Erweiterung, ist also ebenfalls erreichbar.

(iii) Seien z_1, z_2, r_1^2, r_2^2 erreichbar. Sei k_1 ein Kreis um z_1 mit Radius r_1, Gleichung

$$|x - z_1|^2 = (x - z_1)(\overline{x} - \overline{z_1}) = r_1^2 \ .$$

Sei k_1 ein weiterer Kreis um z_2 mit Radius r_2, Gleichung

$$|x - z_2|^2 = (x - z_2)(\overline{x} - \overline{z_1}) = r_1^2 \ .$$

Explizite Rechnung zeigt, dass die Schnittpunkte Koordinaten in einer quadratischen Erweiterung von $\mathbb{Q}(z_1, z_2, \overline{z}_1, \overline{z}_2, r_1^2, r_2^2)$ liegen, also ebenfalls erreichbar sind.

Nebenrechnung: $z_1 = u_1 + iv_1$, $z_2 = u_2 + iv_2$, $x = s + it$. Dann lauten die Gleichungen

$$s^2 - 2su_1 + u_1^2 + t^2 - 2tv_1 + v_1^2 = r_1^2$$
$$s^2 - 2su_2 + u_2^2 + t^2 - 2tv_2 + v_2^2 = r_2^2$$

Wir bilden die Differenz und erhalten eine lineare Relation zwischen s und t. Diese können wir benutzen, um eine der Variablen aus der ersten Gleichung zu eleminieren. Es bleibt eine quadratische Gleichung.

□

Anwendungen

Quadratur des Kreises: Gesucht ist ein Quadrat, dessen Flächeninhalt mit dem des Einheitskreis übereinstimmt, also mit Seitenlänge $\sqrt{\pi}$.

Unmöglich: π ist nicht algebraisch, also auch $\sqrt{\pi}$ nicht. Die Aussage ist nicht trivial, vergleiche S. Lang, Algebra, Appendix 1 S. 867. Der erste Beweis stammt von Ferdinand von Lindemann 1882, hier in Freiburg.

Kubusverdopplung: Gesucht ist ein Würfel mit doppeltem Volumen zum gegebenen Würfel.

Unmöglich. Die Zahl $\sqrt[3]{2}$ hat das Minimalpolynom $X^3 - 2$. Jeder Körper, der diese Zahl enthält, hat also einen Teilkörper vom Grad 3 über $\mathbb{Q}$. Nach der Gradformel für Körpererweiterungen passiert dies nicht für Körper mit Grad eine Potenz von 2.

Regelmäßiges n-Eck: Gesucht ist eine Konstruktion des regelmäßigen n-Ecks. Unmöglich im allgemeinen. Sei p eine Primzahl. Die Ecken des p-Ecks sind p-te Einheitswurzeln $\varepsilon_k = \exp(\frac{2\pi ik}{p})$. Sie sind Nullstellen von $X^p - 1 = (X - 1)(X^{p-1} + X^{p-2} + \dots 1)$. Der zweite Faktor ist nach Eisensteinkriterium irreduzibel. Also gilt $[\mathbb{Q}(\varepsilon_1) : \mathbb{Q}] = p - 1$. Ist ε_1 konstuierbar, so muss $p - 1$ eine Potenz von 2 sein, also

$$p = 2^m + 1 \ .$$

Sei $m = 2^k n$ mit ungeradem n.

$$p = 1 - (-2^{2^k})^n$$

wird von $1 - (-2^{2^k})$ geteilt, denn $1 - X$ teilt $1 - X^n$. Dies wäre keine Primzahl. Also:

$$p = 1 + 2^{2^k} \ .$$

Primzahlen von dieser Form heißen *Fermatsche Primzahlen.*

k	p
0	3
1	5
2	17
3	257
4	65537

Fermat vermutete, alle diese Zahlen seien Primzahlen. Tatsächlich ist die nächste, $k = 5$, $p = 641 \cdot 6700417$ (Euler). Es sind keine weiteren Fermatschen Primzahlen bekannt. Auf jeden Fall ist das p-Eck für $p = 7, 11, \dots$ *nicht* konstruierbar. Die Frage nach Konstruierbarkeit von regelmäßigen n-Ecken ist gelöst modulo der Bestimmung der Fermatschen Primzahlen.
Tatsächlich gilt allgemeiner:

Satz 6.4. *Das regelmäßige n-Eck ist genau dann mit Zirkel und Lineal konstruierbar, wenn $n = 2^m p_1 \dots p_i$ mit verschiedenen Fermatschen Primzahlen p_j ist.*

Beweis: Bosch, Algebra 6.4 Satz 5, später. □

Beispiel. $n = 9$. Minimalpolynom einer 9-ten Einheitswurzel

$$(X^9 - 1) : (X^3 - 1) = X^6 + X^3 + 1$$

(Übungsaufgabe, oder später). Der Grad ist wieder keine Potenz von 2.

Winkeldreiteilung: Gesucht ist eine Konstruktion zur Dreiteilung eines beliebigen Winkels.

Unmöglich. Wir betrachten 60°. Dreiteilung wäre die Konstruktion eines regelmäßigen $6 \cdot 3 = 18$-Ecks, daraus erhält man das 9-Eck. Das geht aber nicht, siehe oben.

Aus unseren bisherigen Überlegung wissen wir noch nicht, wie z.B. das regelmäßige 17-Eck zu konstruieren ist. Dafür müssen wir eine Kette von Zwischenkörpern in $\mathbb{Q}(\varepsilon_{17})/\mathbb{Q}$ konstuieren. Dies wird eine Anwendung von Galoistheorie und der Strukturtheorie von 2-Gruppen sein. Im Falle des einfacheren $\mathbb{Q}(\varepsilon_5)$ geht es noch mit Raten:

$$\mathbb{Q} \subsetneq \mathbb{Q}(\varepsilon_5 + \overline{\varepsilon}_5) \subsetneq \mathbb{Q}(\varepsilon_5) \ .$$

Kapitel 7

Exkurs: Aufbau der Zahlbereiche

Jetzt ist eine Gelegenheit, um zusammenzufassen, wie der Zahlbegriff aufgebaut ist:

$$\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$$

Wir skizzieren die Argumente. Vollständig würden sie extrem viel Zeit in Anspruch nehmen, sind aber meist sehr einfach.

Natürliche Zahlen

Definition 7.1 (Peano Axiome)**.** *Die* natürlichen Zahlen *sind eine Menge* $\mathbb{N}$ *zusammen mit einer Abbildung ("Nachfolger")*

$$\mathbb{N} \to \mathbb{N} \; ; n \mapsto n'$$

so dass

(i) Die Nachfolgerabbildung injektiv ist;

(ii) Sie hat als Bild $\mathbb{N} \setminus \{1\}$ *für ein Element* 1

(iii) Jede Teilmenge X *von* $\mathbb{N}$ *mit*

$$1 \in X \;\wedge\; x \in X \Rightarrow x' \in X$$

ist gleich $\mathbb{N}$*.*

Die Existenz einer solchen Menge folgt aus den Axiomen der Mengenlehre, z.B. in dem man für jede Menge definiert $M' = M \cup \{M\}$ und $1 = \{\emptyset\}$. Um diesen Beweis zu führen, müssten wir in die Axiome der Mengenlehre einsteigen, dafür ist diese Vorlesung nicht der richtige Ort.

Die natürlichen Zahlen sind durch die obigen Axiome eindeutig charakterisiert.

Auf den natürlichen Zahlen definieren wir weitere Strukturen:

(i) Addition durch $n + 1 = n'$ und $n + m' = (n + m)'$

(ii) Multiplikation durch $1n = n$ und $n'm = n + nm$

(iii) $\leq$ durch $a \leq b$, falls $a = b$ oder es gibt c mit $a + c = b$

Lemma 7.2. *(i) Addition und Multiplikation sind assoziativ und kommutativ und erfüllen das Distributivgesetz.*

(ii) Es gilt die Kürzungsregel:

$$a + c = b + c \Rightarrow a = b$$

(iii) $\leq$ *ist eine totale Ordnung.*

(iv) Ist $a \leq b$*, so folgt* $a + c \leq b + c$ *und* $ac \leq bc$*.*

(v) Jede Teilmenge von $\mathbb{N}$ *hat bezüglich* $\leq$ *ein kleinstes Element.*

Beweis: Alle Beweise werden mit vollständiger Induktion geführt. Wir zeigen als Beispiel einen Spezialfall des Kommutativgesetzes der Addition.

Behauptung. *Für alle* $n \in \mathbb{N}$ *gilt* $n + 1 = 1 + n$*.*

Die Behauptung lautet $n' = 1 + n$. Wir zeigen dies mit Induktion nach n. Genauer: Sei X die Teilmenge der Elemente von $\mathbb{N}$, für die die Formel gilt. Es ist $1 \in X$, denn $1' = 1 + 1$ nach Definition. Sei $x \in X$. Wir betrachten x'. Die Behauptung lautet nach Definition

$$(x')' = 1 + x' = (1 + x)'$$

Nach Voraussetzung gilt $x' = 1 + x$, also auch die Behauptung. Nach dem Induktionsaxiom ist nun $X = \mathbb{N}$, die Aussage gilt allgemein. □

Ganze Zahlen

Wir erhalten die ganzen Zahlen aus den natürlichen, indem wir für jedes Element formal ein additives Inverses hinzufügen. Man nennt diesen Prozess allgemein *Gruppenkomplettierung* einer Halbgruppe. Alternativ definieren wir die ganzen Zahlen als freie Gruppe in einem Erzeuger 1. Beide Versionen sind durch eine universelle Eigenschaft charakterisiert und daher eindeutig. Wir geben statt dessen die Konstruktion an, das ist dann auch der Existenzbeweis.

Definition 7.3. *Sei* $\mathbb{Z}$ *die Menge der Äquivalenzklassen von Paaren* $(a, b) \in \mathbb{N}^2$ *mit der Äquivalenzrelation*

$$(a, b) \sim (c, d) \Leftrightarrow a + d = c + b$$

Wir definieren $i : \mathbb{N} \to \mathbb{Z}$ *via* $n \mapsto (n', 1)$*.*

Lemma 7.4. *$\sim$ ist wohldefiniert und die Abbildung $\mathbb{N} \to \mathbb{Z}$ injektiv.*

Beweis: Folgt aus der Kürzungseigenschaft. □

Lemma 7.5. *Addition und Multiplikation setzen sich eindeutig nach $\mathbb{Z}$ fort, so dass das Distributivgesetz erhalten bleibt und (b, a) additives Inverses von (a, b) ist. Die Relation $\leq$ setzt sich zu einer Totalordnung von $\mathbb{Z}$ fort. Für $a \leq b$ in $\mathbb{Z}$ und $c \in \mathbb{Z}$ gilt $a + c \leq b + c$. Mit $c \in \mathbb{N}$ gilt $ac \leq bc$.*

Es gilt also $(a, b) = i(a) - i(b)$. Wir schreiben meist a statt $i(a)$ und betrachten $\mathbb{N}$ als Teilmenge von $\mathbb{Z}$.

Beweis: Wir definieren die Addition komponentenweise und die Multiplikation durch

$$(a, b)(c, d) = (a - b)(c - d) = ac - bc - ad + bd = (ac + bd, ad + bc)$$

Der Rest ist mühsam, aber einfach. □

Die ganzen Zahlen sind ein Hauptidealring, wie wir bereits bewiesen haben. Es gilt Eindeutigkeit der Primfaktorzerlegung.

Rationale Zahlen

Aus den ganzen Zahlen erhalten wir die rationalen durch *Lokalisierung* bzw. *Bruchkalkül*. Dies ist ein allgemeines Verfahren für Ringe, um formal eine Menge von Elemente invertierbar zu machen bezüglich der Multiplikation. Auch dies hat eine universelle Eigenschaft. In der kommutativen Algebra wird dies allgemein studiert.
Wir geben die Konstruktion an:

Definition 7.6. *Sei $\mathbb{Q}$ die Menge der Äquivalenzklassen von Paaren $(a, b) \in \mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$ mit der Äquivalenzrelation*

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

Wir schreiben a/b oder $\frac{a}{b}$ für die Äquivalenzklasse von (a, b).

Um zwei Brüche zu vergleichen, bringen wir sie auf einen Hauptnenner und vergleichen dann die Zähler.

Lemma 7.7. *$\sim$ ist eine Äquivalenzrelation. Die Abbildung $a \mapsto a/1$ ist eine injektive Abbildung $\mathbb{Z} \to \mathbb{Q}$.*

Beweis: $\mathbb{Z}$ nullteilerfrei. □

Lemma 7.8. *$\mathbb{Q}$ trägt eindeutig eine Struktur als total geordneter Körper, so dass $\mathbb{Z} \to \mathbb{Q}$ ein ordnungserhaltender Ringhomomorphismus unitärer Ringe ist.*

$\mathbb{Q}$ trägt zusätzlich einen Absolutbetrag mit

$$|a| = \begin{cases} a & a \geq 0 \\ -a & a \leq 0 \end{cases}$$

der die Axiome einer Norm erfüllt. Bezüglich dieses Betrages erhält $\mathbb{Q}$ die Struktur eine metrischen Raumes, und wir können nun über Cauchyfolgen sprechen.

Lemma 7.9. *$\mathbb{Q}$ ist nicht vollständig.*

Beweis: Analysis 1. □

Reelle Zahlen

Die reellen Zahlen sind definiert als Komplettierung von $\mathbb{Q}$ bezüglich des Absolutbetrages.

Lemma 7.10. *Sei $\mathcal{R}$ die Menge der Cauchyfolgen von rationalen Zahlen, $\mathcal{M}$ das Ideal der Nullfolgen von rationalen Zahlen. Dann ist*

$$\mathbb{R} = \mathcal{R}/\mathcal{M}$$

ein vollständiger totalgeoordneter Körper mit Absolutbetrag. Die Abbildung $\mathbb{Q} \to \mathbb{R}$, die eine Zahl auf die konstante Folge abbildet, ist injektiv mit dichtem Bild. Die reellen Zahlen sind archimedisch, d.h. zu je $a \in \mathbb{R}$ und $c > 0$ gibt es $n \in \mathbb{N}$ mit $n|a| > c$.

Beweis: $\mathbb{R}$ ist ein Ring. Z.z. ist, dass jede Cauchyfolge, die keine Nullfolge ist, ein Inverses hat. Sei (a_n) Cauchyfolge, aber keine Nullfolge. Sei $\varepsilon > 0$. Dann gibt es n_0, so dass $|a_n| > \varepsilon$ für $n \geq n_0$. Wir definieren $b_n = a_n^{-1}$ für $n \geq n_0$ und $b_n = 1$ für $n < n_0$. Man überprüft, dass dies eine Cauchyfolge ist, invers zu (a_n).
Der Rest ist Übungsaufgabe. □

Die obigen Eigenschaften charakterisieren $\mathbb{R}$ eindeutig. Häufig findet man auch eine andere Konstruktion aus $\mathbb{Q}$:

Definition 7.11. *Ein* Dedekindscher Schnitt *ist ein Paar (A, B) von nichtleeren Teilmengen von $\mathbb{Q}$, so dass $a < b$ für jedes $a \in A$, $b \in B$; $A \cup B = \mathbb{Q}$ und A hat kein maximales Element.*

(i) Jede ratinoale Zahl $r \in \mathbb{Q}$ definiert einen Dedekindschen Schnitt durch $r \mapsto (\{a \in \mathbb{Q} | a < r\}, \{b \in \mathbb{Q} | b \geq r\})$. Wir identifizieren r mit dem zugehörigen Schnitt.

(ii) Für zwei Dedekindsche Schnitte (A, B) und (C, D) definieren wir $(A, B) < (C, D)$ falls $A \subsetneq C$.

(iii) $(A, B) + (C, D) = (A + C, \mathbb{Q} \setminus \{A + C\})$

(iv) Für $(A,B),(C,D) > 0$ *setzen wir* $(A,B)(C,D) = (X,Y)$ *mit*

$$X = \{p \in \mathbb{Q} | p \leq rs, \text{ für } r,s > 0, r \in A, s \in C\}$$

und Y *das Komplement.*

Lemma 7.12. *Die Menge der Dedekindschen Schnitte ist ein totalgeordneter Körper, der* $\mathbb{Q}$ *als dichten Unterkörper enthält. Er ist isomorph zu* $\mathbb{R}$*.*

Beweis: Zunächst überprüft man die Gruppenaxiome für die Addition. Insbesondere findet man auch negative Inverse. Ist $r \in \mathbb{Q}$, so ist dies der Dedekindsche Schnitt zu $-r$. Ist $(A,B) \notin \mathbb{Q}$, so ist $(-B,-A)$ das additive Inverse. Damit ist klar, wie die Multiplikation von positiven Schnitten auf alle Schnitte fortzusetzen ist. Wieder überprüft man die Körperaxiome.

Der Dedekindsche Schnitt (A,B) kann dann aufgefasst werden als $\inf B$. Hieraus folgt leicht die Existenz von Infima für nach unten beschränkte Mengen von Schnitten oder von Suprema für nach oben beschränkte Mengen von Schnitten. Es gilt also das Supremumsaxiom, das in einem totalgeordneten Körper äquivalent zum Vollständigkeitsaxiom ist.

Das archimedischen Axiom ist leicht zu überprüfen. Zusammen ist dadurch $\mathbb{R}$ charakterisiert. □

Der Vorteil dieses Zugangs ist, dass man nicht über Cauchyfolgen, Ideale oder andere Begriffe der höheren Mathematik sprechen muss. Der Zugang über Cauchyfolgen hat den Vorteil, dass er sich auf andere topologische Körper oder Vektorräume verallgemeinert.

$\mathbb{R}$ ist vollständig, aber nicht algebraisch abgeschlossen. Immerhin:

Lemma 7.13. *Jede positive Zahl hat in* $\mathbb{R}$ *eine Quadratwurzel. Jedes Polynom von ungeradem Grad hat in* $\mathbb{R}$ *eine Nullstelle.*

Beweis: Übungsaufgabe aus Analysis 1, Zwischenwertsatz. □

Komplexe Zahlen

Definition 7.14. $\mathbb{C}$ *ist definiert als* $\mathbb{R}[X]/X^2+1$*.*

Theorem 7.15. $\mathbb{C}$ *ist algebraisch abgeschlossen. Durch* $|a+bi| = \sqrt{a^2+b^2}$ *wird* $\mathbb{C}$ *zu einem vollständigen normierten Körper.*

Beweis: Funktionentheorie oder gegen Ende des Semesters. □

Bemerkung. $\mathbb{C}$ ist nicht mehr total geordnet. Genauer: Es gibt keine Anordnung, die mit Multiplikation verträglich ist in der Art, die wir für $\mathbb{Q}$ und $\mathbb{R}$ verlangt haben.

Kapitel 8

Körperhomomorphismen

Wir wissen schon, dass alle Körperhomomorphismen injektiv sind. Es gibt aber im allgemeinen mehrere Möglichkeiten. Von besonderem Interesse sind die Automorphismen.

Charakteristik

Definition 8.1. *Sei K ein Körper.*

$$F = \bigcap_{K' \subset K} K'$$

der Schnitt über alle Teilkörper heißt Primkörper *von K.*

Bemerkung. Offensichtlich ist F ein Körper.

Satz 8.2. *Der Primkörper ist entweder isomorph zu $\mathbb{Q}$ oder isomorph zu $\mathbb{F}_p$ für eine Primzahl p.*

Definition 8.3. *Wir sagen, K hat* Charakteristik 0 bzw. p*, wenn der Primkörper $\mathbb{Q}$ bzw. $\mathbb{F}_p$ ist.*

Beweis: Wir betrachten $\alpha : \mathbb{Z} \to K$, $1 \mapsto 1$. Dies ist ein Ringhomomorphismus.
1. Fall: α ist injektiv, d.h. $\alpha(n) \neq 0$ für $n \neq 0$. Durch $\alpha(n/m) = \alpha(n)\alpha(m)^{-1} \in K$ wird ein injektiver Ringhomomorphismus $\mathbb{Q} \to K$ definiert (offensichtlich wohldefiniert). Dann ist $\alpha(\mathbb{Q}) \subset K$ ist ein Teilkörper von K, der isomorph zu $\mathbb{Q}$ ist. Ebenso $\alpha(\mathbb{Q}) \subset K' \subset K$ für alle Teilkörper K', also $\alpha(\mathbb{Q}) = F$.
2. Fall: $\operatorname{Ker}\alpha = \mathbb{Z}n$ mit $n > 0$. Dann ist $\operatorname{Im}\alpha \cong \mathbb{Z}/n\mathbb{Z}$ als Ring. Es ist $n \neq 1$, denn $1 \neq 0$ in K. Sei n zerlegbar, $n = mk$. Dann gilt $\alpha(m)\alpha(k) = 0$ in K. Dies ist ein Körper, also ist ein Faktor Null, z.B. $\alpha(m) = 0$, d.h. $m \in \mathbb{Z}n$. Zusammen ist $m = \pm n$. Daher ist m eine Primzahl. $\operatorname{Im}\alpha \cong \mathbb{F}_p$ ist auch in allen Teilkörpern von K enthalten, also der Primkörper. □

Bemerkung. Die Charakteristik ist der Erzeuger von $\operatorname{Ker}\alpha$.

Lemma 8.4. *Sei F ein Primkörper. Dann gibt es nur einen Körperhomomorphismus $\alpha : F \to F$, nämlich die Identität.*

Beweis: $\alpha(1) = 1$, $\alpha(2) = 2$ etc., also α die Identität auf $\mathbb{Z} \cdot 1_F$. Im Fall $\mathbb{F}_p$ sind wir damit fertig. Im Fall $F = \mathbb{Q}$ ist $\alpha(n/m) = \alpha(n)\alpha(m)^{-1}$ ebenfalls die Identität. □

Lemma 8.5. *Seien K, L Körper mit unterschiedlicher Charakteristik. Dann gibt es keinen Körperhomomorphismus $\alpha : K \to L$.*

Beweis: Sei F der Primkörper von K. Dann ist via

$$F \subset K \xrightarrow{\alpha} L$$

eine Kopie von F in L enthalten. Der Primkörper von L ist in $\alpha(F)$ enthalten. Es gibt aber keine nichttrivialen Inklusionen zwischen verschiedenen Primkörpern. □

Hier einige Beispiele für nichttriviale Körperhomomorphismen.

Beispiel. $K = \mathbb{C}$, $x + iv \mapsto x - iv$ für $x, y \in \mathbb{R}$.

Satz 8.6. *Sei K ein Körper mit* $\operatorname{Char} K = p > 0$, *$n \in \mathbb{N}$. Dann ist die Abbildung*

$$\phi_n : K \to K \ ; x \mapsto x^{p^n}$$

ein Körperhomomorphismus, der Frobeniushomomorphismus*. Sein Bild $\phi_n(K)$ ist ein Teilkörper von K.*

Beweis: Wegen $\phi_n = \phi_1 \circ \cdots \circ \phi_1$ genügt es, $n = 1$ zu betrachten. Wir schreiben $\phi := \phi_1$. Es ist $\phi(1) = 1^p = 1$ und $\phi(-1) = (-1)^p = -1$ (klar, falls p ungerade; $p = 2 \Rightarrow -1 = 1$). Seien $x, y \in K$. Es gilt

$$\phi(xy) = (xy)^p = x^p y^p = \phi(x)\phi(y)$$

Die Verträglichkeit mit der Addition ist schwieriger.

$$\phi(x+y) = (x+y)^p = x^p + \binom{p}{1} x^{p-1}y + \binom{p}{2} x^{p-1}y^2 + \ldots \binom{p}{p-1} xy^{p-1} + y^p$$

Der Binomialkoeffizient $\binom{p}{i}$ ist für $i \neq 0, 1$ durch p teilbar. Also ist er Null in K nach Definition der Charakteristik. Es folgt

$$\phi(x+y) = x^p + y^p = \phi(x) + \phi(y) \ .$$

Das Bild eines Körpers ist immer ein Körper. □

Bemerkung. Wenn $|K| < \infty$, dann ist ϕ_n bijektiv, denn jede injektive Abbildung ist auch surjektiv.

Beispiel. $K = \mathbb{F}_p$. Dann ist $\phi_1 = \mathrm{id}$, also $x^p = x$. Dies ist wieder der kleine Satz von Fermat, vergleiche Korollar 1.16.
$K = \mathbb{F}_p(X) = \{\frac{P}{Q} \mid P, Q \in k[X], Q \neq 0\}$. Wir betrachten $\phi_1 : K \to K$.

Behauptung. *X liegt nicht im Bild von ϕ_1.*

Angenommen, $X = \phi_1(P/Q) = P^p/Q^q$. Ohne Einschränkung haben P und Q keine Faktoren gemeinsam. Dann gilt $P^p = XQ^p$. Da in $k[X]$ eindeutige Primfaktorzerlegung gilt, folgt $X \mid P$, dann $X^p \mid XQ^p$, also $X \mid Q$, Widerspruch. In diesem Falls gilt also $\phi_1(K) \subset K$ ist ungleich K, aber isomorph zu K.

Existenz von Homomorphismen

Wir wissen, dass jeder Körper K in einem algebraisch abgeschlossenen Körper $\overline{K}$ enthalten ist (Satz 5.16). Wir wollen zeigen, dass jede algebraische Erweiterung von K als Teilkörper von $\overline{K}$ aufgefasst werden kann.

Definition 8.7. *Eine Erweiterung L/K heißt* einfach, *falls $L = K(a)$ für ein $a \in L$.*

Satz 8.8. *Sei $K' = K(a)/K$ einfache algebraische Körpererweiterung, L ein Körper,*

$$\sigma : K \to L$$

ein Körperhomomorphisms, $P \in K[X]$ das Minimalpolynom von a.

(i) Ist $\sigma' : K' \to L$ eine Fortsetzung von σ, so ist $\sigma'(a)$ eine Nullstelle von $\sigma(P)$.

(ii) Ist $b \in L$ eine Nullstelle von $\sigma(P)$, so gibt es genau eine Fortsetzung σ' von σ nach K' mit $\sigma'(a) = b$.

Bemerkung. Am wichtigsten ist der Fall $\sigma = \subset$.

Beweis: Sei $P(X) = \sum_{i=0}^{n} a_i X^i$ mit $a_i \in K$. Anwenden von σ liefert

$$\sigma(P)(X) = \sum_{i=0}^{n} \sigma(a_i) X^i \in L[X] \ .$$

Nach Vorraussetzung gilt

$$P(a) = \sum_{i=0}^{n} a_i a^i = 0 \ .$$

Anwenden des Körperhomomorphismus σ' liefert

$$\sigma'(P(a)) = \sum_{i=0}^{n} \sigma'(a_i)\sigma'(a)^i = \sigma(P)(\sigma'(a)) = 0 \ .$$

Umgekehrt betrachtet man den Ringhomomorphismus

$$s : K[X] \to L \; ; \sum_{i=0}^{k} \sigma(b_i) X^i \mapsto \sum_{i=0}^{k} \sigma(b_i) b^i \; .$$

Das Polynom P liegt im Kern, denn

$$s(P) = \sum_{i=0}^{k} \sigma(b_i) b^i = 0$$

nach Voraussetzung. Also faktorisiert s über den Ringhomomorphismus

$$\overline{s} : K[X]/(P) \to L \; .$$

Der Homomorphismus $\pi : K[X]/(P) \to K(a)$ mit $X \mapsto a$ ist ein Ismorphismus, da P das Minimalpolynom von a ist. Die gesuchte Abbildung σ' ist gegeben durch $\overline{s} \circ \pi^{-1}$. Offensichtlich bildet sie a auf b ab. □

Bemerkung. Eine Fortsetzung σ' von σ nach K' ist also *nicht* eindeutig. Es gibt soviele Fortsetzung wie Nullstellen von $\sigma(P)$, also höchsten $\deg(P)$ viele.

Definition 8.9. *Sei $P \in K[X]$ ein Polynom. Eine Erweiterung L/K heißt* Zerfällungskörper*, wenn P über L in Linearfaktoren zerfällt,*

$$P(X) = (X - a_1)(X - a_2) \dots (X - a_n)$$

und $L = K(a_1, a_2, \dots, a_n)$.

Beispiel. Das irreduzible Polynom $X^4 - 2 \in \mathbb{Q}[X]$ hat die Nullstellen

$$\sqrt[4]{2}, -\sqrt[4]{2}, i\sqrt[4]{2}, -i\sqrt[4]{2} \; .$$

Der Zerfällungskörper ist $\mathbb{Q}(\sqrt[4]{2}, i)$.

Korollar 8.10. *Sei $P \in K[X]$ ein Polynom, L und L' Zerfällungskörper. Dann sind L und L' isomorph.*

Beweis: Wir betrachten $\sigma : K \subset L$ die Inklusion. Es gilt also $\sigma(P) = P$. Es ist

$$P(X) = (X - a_1)(X - a_2) \dots (X - a_n) \text{ mit } a_i \in L \; .$$

Sei P_1 das Minimalpolynom von a_1 über K. Dann teilt P_1 das Polynom P, also hat P_1 auch eine Nullstelle b_1 in L. Nach dem Satz 8.8 existiert eine Fortsetzung

$$\sigma_1 : K(a_1) \to L \; .$$

Sei P_2 das Minimalpolynom von a_2 über $K(a_1)$. Dann teilt P_2 wieder P und $\sigma_1(P_2)$ teilt $\sigma_1(P) = \sigma(P) = P$. Also hat $\sigma_1(P)$ eine Nullstellte $b_2 \in L$. Nach dem Satz 8.8 existiert eine Fortsetzung

$$\sigma_2 : K(a_1, a_2) \to L \; .$$

Dies wiederholen wir und erhalten schließlich

$$\sigma_n : L' = K(a_1, \ldots, a_n) \to L \ .$$

Das Bild von σ_n ist ein Teilkörper von L, in dem gilt

$$\begin{aligned} P(X) = \sigma_n(P(X)) &= \sigma_n((X - a_1)(X - a_2) \ldots (X - a_n)) \\ &= (X - \sigma_n(a_1))(X - \sigma_n(a_2)) \ldots (X - \sigma_n(a_n)) \ . \end{aligned}$$

D.h. P zerfällt in Linearfaktoren. Da L ein Zerfällungskörper ist, ist σ_n surjektiv. Als Körperhomomorphismus ist es eh injektiv. □

Korollar 8.11 (vergleiche Satz 5.16)**.** *Sei K ein Körper, K_1 und K_2 seien zwei algebraische Abschlüsse. Dann gibt es einen Isomorphismus $K_1 \to K_2$, der mit der Inklusion von K verträglich ist.*

Beweis: Zornsches Lemma! Sei

$$M = \{(F, \tau) \mid K \subset F \subset K_1, \tau : F \to K_2, \tau|_K = \mathrm{id}\}$$

wobei F die Zwischenkörper und τ die Körperhomomorphismen durchläuft. Diese Menge ist partiell geordnet durch

$$(F, \tau) \leq (F', \tau') \Leftrightarrow F \subset F', \tau'|_F = \tau \ .$$

Es gilt $M \neq \emptyset$, denn $(K, \mathrm{id}) \in M$. Sei nun $I \subset M$ total geordnet. Wir bilden

$$F_I = \bigcup_{(F,\tau) \in I} F \ .$$

Da I total geordnet ist, ist dies ein Teilkörper von K_1. Wir definieren

$$\tau_I(f) = \tau(f) \text{ wobei } f \in F, (F, \tau) \in I \ .$$

Wegen unserer Definition der partiellen Ordnung ist τ_I wohldefiniert und ein Körperhomomorphismus. Das Paar (F_I, τ_I) ist die gesuchte obere Schranke für I. Nach Zornschem Lemma hat M nun ein maximales Element (F_m, τ_m).

Behauptung. $F_m = K_1$

Angenommen, es gibt $a \in K_1 \setminus F_m$. Da K_1 algebraisch über K ist, ist a erst recht algebraisch über F_m. Sei P das Minimalpolynom. Da K_2 algebraisch abgeschlossen ist, hat $\tau_m(P)$ eine Nullstelle in K_2. Nach Satz 8.8 gibt es dann eine Fortsetzung von τ_m nach $F_m(a)$. Dies ist ein Widerspruch zur Maximalität.

Behauptung. $\tau_m : K_1 \to K_2$ *ist bijektiv.*

Die Injektivität ist klar. Das Bild ist ein algebraischer Abschluss von K, also ganz K_2. □

Nun kommen wir zur zentralen Definition des zweiten Teils des Semesters:

Definition 8.12. *Sei L/K algebraisch. Dann heißt*

$$\mathrm{Gal}(L/K) = \{\sigma : L \to L \mid \textit{Körperisom. mit } \sigma|_K = \mathrm{id}\}$$

Galoisgruppe *von L/K:*

Bemerkung. Offensichtlich ist es eine Gruppe.

Beispiel. $\mathrm{Gal}(\mathbb{C}/\mathbb{R}) = \{\mathrm{id}, \bar{\cdot}\}$ wobei $\bar{\cdot}$ die komplexe Konjugation ist, denn $\mathbb{C} = \mathbb{R}(i)$, $\sigma(i)$ ist Nullstelle von X^2+1, also $\sigma(i) = \pm i$. Also ist $\mathrm{Gal}(\mathbb{C}/\mathbb{R}) \cong \mathbb{Z}/2$.

Lemma 8.13. *Sei $[L:K] = n$. Dann ist $|\mathrm{Gal}(L/K)| \leq n$.*

Beweis: Da L/K endlich ist, ist jeder Körperhomomorphismus automatisch ein Isomorphismus (Dimensionen abzählen!). Sei $L = K(a_1, \ldots, a_k)$. Nach Satz 8.8 und der nachfolgenden Bemerkung gilt

$$|\{\sigma_1 : K(a_1) \to L \mid \sigma_1|_K = \mathrm{id}\}| \leq [K(a_1) : K]$$
$$|\{\sigma_2 : K(a_1, a_2) \to L \mid \sigma_2|_{K(a_1)} = \sigma_1\}| \leq [K(a_1, a_2) : K(a_1)]$$

etc. Die Behauptung folgt aus der Gradformel. □

Damit ist $\mathrm{Gal}(L/K)$ eine *endliche Gruppe*. Wir werden Gruppentheorie zum Studium von L/K verwenden.

Definition 8.14. *Eine endliche Körpererweiterung L/K heißt* galois, *wenn* $|\mathrm{Gal}(L/K)| = [L:K]$.

Beispiel.

(i) $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}$. Das Minimalpolynom von $\sqrt[4]{2}$ über $\mathbb{Q}$ ist $X^4 - 2$. Es hat über $\mathbb{Q}(\sqrt[4]{2})$ zwei Nullstellen. Also hat die Galoisgruppe nur 2 Elemente. Die Erweiterung ist nicht galois.

(ii) Sei $L = K(\sqrt{a})$ mit $\sqrt{a} \notin K$. Das Minimalpolynom ist also $X^2 - a$. Es zerfällt in L in die Linearfaktoren $(X - \sqrt{a})(X + \sqrt{a})$. In Charakteristik ungleich 2 hat die Galoisgruppe zwei Elemente, die Erweiterung ist galois. In Charakteristik 2 ist aber $\sqrt{a} = -\sqrt{a}$. Die Galoisgruppe hat nur ein Element, die Erweiterung ist wieder nicht galois.

Kapitel 9

Beispiele für Galoisgruppen

Wir behandeln einige Beispiele, die für das Problem der Auflösbarkeit von Polynomgleichungen relevant sind.

Zyklotomische Körper

Definition 9.1. *Sei L ein Körper. Ein Element $\zeta \in L$ mit $\zeta^d = 1$ heißt d-te* Einheitswurzel. *Es heißt* primitive d-te Einheitswurzel*, falls ζ die Ordnung d (bezüglich der Multiplikation) hat. Es sei $\mu_d(L)$ die Gruppe der d-ten Einheitswurzeln von L.*

Beispiel. (i) $\zeta = \exp(2\pi i/d)$ ist primitive d-te Einheitswurzel in $\mathbb{C}$.

(ii) Ist $\mathbb{F}$ ein Körper mit q Elementen, so sind alle Elemente ungleich 0 schon $q-1$-te Einheitswurzeln, denn $\mathbb{F}^*$ ist eine Gruppe mit $q-1$ Elementen.

Lemma 9.2. *Sei L ein Körper, der eine primitive d-te Einheitswurzel ζ enthält. Dann ist $\mu_d(L) \cong \mathbb{Z}/d\mathbb{Z}$. Dabei werden die primitiven d-ten Einheitswurzeln abgebildet auf*

$$(\mathbb{Z}/d\mathbb{Z})^* = \{x \in \mathbb{Z}/d\mathbb{Z} \mid \text{es gibt } y \in \mathbb{Z}/d\mathbb{Z}, xy = 1\} \ .$$

Beweis: Die d-ten Einheitswurzeln sind genau die Nullstellen von $X^d - 1$. Jede der d Potenzen von ζ ist eine solche, also ist $\mu_d(L)$ zyklisch. bzw. isomorph zu $\mathbb{Z}/d\mathbb{Z}$. Dabei werden die primitiven d-ten Einheitswurzeln auf die Erzeuger abgebildet, siehe das folgende Lemma. □

Wir tragen aus der Theorie der zyklischen Gruppen nach:

Lemma 9.3. *Die Erzeuger der Gruppe $\mathbb{Z}/d\mathbb{Z}$ sind die Restklassen, die teilerfremd zu d sind. Dies sind gleichzeitig die Elemente der multiplikativen Gruppe $(\mathbb{Z}/d\mathbb{Z})^*$.*

Beweis: Sei $x \in \mathbb{Z}/d\mathbb{Z}$. Die Ordnung von x ist $d/\operatorname{ggT}(x,d)$ nach Korollar 2.8. Ein Element ist also genau dann Erzeuger, wenn $\operatorname{ggT}(x,d) = 1$. Nach Lemma 2.7 (i) gilt dann $1 \in x\mathbb{Z} + d\mathbb{Z}$, d.h. es gibt y, e mit

$$1 = xy + de \Rightarrow 1 = xy \in \mathbb{Z}/d\mathbb{Z} \ .$$

Damit ist x Einheit des Rings $\mathbb{Z}/d\mathbb{Z}$. □

Bemerkung. Die Ordnung von $(\mathbb{Z}/d\mathbb{Z})^*$ wird mit $\phi(d)$ bezeichnet (Eulersche ϕ-Funktion).

Satz 9.4 (Zyklotomische Erweiterungen)**.** *Sei K Körper und $L = K(\zeta)$ für eine primitive d-te Einheitswurzel ζ.*
Dann ist L der Zerfällungskörper von $X^d - 1$. Die Erweiterung ist galois mit

$$\operatorname{Gal}(L/K) \cong H \subset (\mathbb{Z}/d\mathbb{Z})^* \ .$$

Insbesondere ist die Galoisgruppe abelsch.

Bemerkung. Sei ζ eine primitive d-te Einheitswurzel in $\mathbb{C}$. Dann gilt sogar

$$\operatorname{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q}) \cong (\mathbb{Z}/d\mathbb{Z})^*$$

(Beweis später mit Hilfe von etwas mehr Galoistheorie).

Beweis: Das Polynom $X^d - 1$ hat die Nullstellen $1, \zeta, \zeta^2, \ldots, \zeta^{d-1}$. Insbesondere ist L Zerfällungskörper.
Sei $P \in K[X]$ das Minimalpolynom von ζ. Dann ist P ein Teiler von $X^d - 1$ und zerfällt über L in Linearfaktoren. Die Nullstellen sind paarweise verschiedenen. Daher gibt es $\deg P$ viele Elemente der Galoisgruppe und die Erweiterung ist galois.
Die Abbildung $\sigma \in \operatorname{Gal}(K(\zeta)/K)$ ist eindeutig festgelegt durch den Wert $\sigma(\zeta)$. Dies ist ebenfalls eine primitive d-te Einheitswurzel, also von der Form ζ^{n_σ}. Die Abbildung

$$\operatorname{Gal}(L/K) \to (\mathbb{Z}/d\mathbb{Z})^*, \quad \sigma \mapsto n_\sigma$$

ist daher injektiv.

Behauptung. *Dies ist ein Gruppenhomomorphismus.*

Seien $\sigma, \tau \in \operatorname{Gal}(L/K)$. Es gilt

$$(\sigma\tau)(\zeta) = \sigma(\tau(\zeta)) = \sigma(\zeta^{n_\tau}) = (\sigma(\zeta))^{n_\tau} = (\zeta^{n_\sigma})^{n_\tau} = \zeta^{n_\sigma n_\tau} \ ,$$

also $n_{\sigma\tau} = n_\sigma n_\tau$. □

Bemerkung. Der Isomorphismus $\operatorname{Gal}(L/K) \to H$ hängt nicht von der Wahl der primitiven Einheitswurzel ζ ab.

n-te Wurzeln

Satz 9.5 (Kummer-Erweiterungen)**.** *Sei K ein Körper, der eine primitive d-te Einheitswurzel enthält. Sei $a \in K$, $L = K(\beta)$, wobei β eine Nullstelle von $X^d - a$ ist.*

Dann ist L Zerfällungskörper von $X^d - a$. Die Erweiterung ist galois, und $\mathrm{Gal}(L/K)$ ist isomorph zu einer Untergruppe von $\mathbb{Z}/d\mathbb{Z}$, insbesondere abelsch.

Beweis: Sei ζ eine primitive d-te Einheitswurzel in K. Die Gleichung $\beta^d = a$ impliziert $(\zeta^n\beta)^d = a$, also hat $X^d - a$ in L die Nullstellen $\beta, \zeta\beta, \ldots, \zeta^{d-1}\beta$. Dies sind d verschiedene Zahlen, also zerfällt $X^d - a$ über L in Linearfaktoren. Das Minimalpolynom P von β teilt $X^d - a$, hat also $\deg P$ verschiedene Nullstellen. Daher ist die Erweiterung galois.
Wir betrachten

$$\mathrm{Gal}(L/K) \to L^*, \quad \sigma \mapsto \frac{\sigma(\beta)}{\beta} \ .$$

Diese Abbildung ist injektiv, denn $\sigma(\beta)$ legt σ fest.

Behauptung. *Dies ist ein Gruppenhomomorphismus.*

Sei $\sigma(\beta) = \zeta^{n_\sigma}\beta$, $\tau(\beta) = \zeta^{n_\tau}\beta$. Dann ist

$$\frac{\sigma\tau(\beta)}{\beta} = \frac{\sigma(\zeta^{n_\tau}\beta)}{\beta} = \frac{\zeta^{n_\tau}\sigma(\beta)}{\beta} = \frac{\zeta^{n_\tau}\zeta^{n_\sigma}\beta}{\beta} = \zeta^{n_\tau + n_\sigma}.$$

Andererseits

$$\frac{\sigma(\beta)}{\beta}\frac{\tau(\beta)}{\beta} = \zeta^{n_\sigma}\zeta^{n_\tau} \ .$$

Insgesamt ist $\mathrm{Gal}(L/K)$ isomorph zu einer Untergruppe von $\mu_d(K) \cong \mathbb{Z}/d\mathbb{Z}$. □

Endliche Körper

Sei $\mathbb{F}_q$ ein Körper mit q Elementen. Sei $\mathbb{F}_p$ der Primkörper ($\mathbb{Q}$ kommt nicht in Frage, da $\mathbb{Q}$ unendlich ist). Dann hat $\mathbb{F}_q$ einen endlichen Grad n über $\mathbb{F}_p$, also ist $\mathbb{F}_q \cong \mathbb{F}_p^n$ als Vektorraum und hat $q = p^n$ viele Elemente.
Die multiplikative Gruppe $\mathbb{F}_q^*$ hat $q - 1$ Elemente. Nach Korollar 1.15 gilt dann $x^{q-1} = 1$ für alle $x \in \mathbb{F}_q^*$ oder äquivalent $x^q = x$ für alle $x \in \mathbb{F}_q$. Das Polynom $X^q - X$ zerfällt also über $\mathbb{F}_q$ in Linearfaktoren. Genauer: Es hat q paarweise verschiedene Nullstellen. Daher ist $\mathbb{F}_q$ ein Zerfällungskörper von $X^q - X$. Als solcher ist $\mathbb{F}_q$ *eindeutig*. Es gibt also höchstens einen Körper mit p^n Elementen.
Wie steht es mit der Existenz? Sei $q = p^n$ für eine Primzahl p. Sei $\mathbb{F}$ ein Zerfällungkörper von $P = X^q - X$ über $\mathbb{F}_p$. Darin sei $\mathbb{F}_q$ die *Menge* der Nullstellen. Wir behaupten, dass es sich um einen Teilkörper handelt, d.h. die Menge ist abgeschlossen unter $+, -, \cdot, :$. Um dies zu zeigen, wechseln wir den Standpunkt. Wir erinnern uns an den Frobeniushomomorphismus ϕ_n, der x auf x^{p^n}

abbildet. Die Nullstellen von P sind die Elemente mit $\phi_n(x) = x$. Es folgt z.B. für $x, y \in \mathbb{F}_q$

$$\phi_n(x+y) = \phi_n(x) + \phi_n(y) = x + y$$

und daher $x+y \in \mathbb{F}_q$. Also besteht der Zerfällungskörper genau aus den Nullstellen von P. Wieviele sind es? Könnte es doppelte Nullstellen geben? Wir greifen etwas vor. Wenn $a \in \mathbb{F}$ eine doppelte Nullstelle von p, ist dann ist a auch eine Nullstelle von $P' = qX^{q-1} - 1 = -1$. Das ist unmöglich.
Wir haben gezeigt:

Satz 9.6. *Die Ordnung eines endlichen Körpers ist eine Primzahlpotenz. Für jede Primzahl p und $n \geq 1$ gibt es (bis auf Isomorphie) genau einen Körper mit p^n Elementen, den Zerfällungskörper von $X^{p^n} - X$.*

Der Körper mit q Elementen heißt üblicherweise $\mathbb{F}_q$.

Bemerkung. $\mathbb{F}_{p^n}$ und $\mathbb{Z}/p^n\mathbb{Z}$ haben nichts miteinander zu tun (außer für $n = 1$)!

Nun wollen wir die Galoisgruppe berechnen. Sei weiter $q = p^n$. Wir kennen bereits einen Körperhomomorphismus $\mathbb{F}_q \to \mathbb{F}_q$, nämlich den Frobenius ϕ_1. Wir wissen, dass $\phi_1^n = \phi_n = \mathrm{id}$ auf $\mathbb{F}_q$. Die Ordnung von ϕ_1 ist also ein Teiler von n. Sei m diese Ordnung. Dann sind alle Elemente von $\mathbb{F}_q$ Nullstellen des Polynoms $X^{p^m} - X$. Dessen Grad ist aber zu klein, falls $m < n$. Es folgt also $m = n$. Die Galoisgruppe enthält ein Elment der Ordnung n. Da die Galoisgruppe höchstens $n = [\mathbb{F}_q : \mathbb{F}_p]$ Elemente hat, folgt

$$\mathrm{Gal}(\mathbb{F}_q/\mathbb{F}_p) = \langle \phi_1 \rangle$$

und die Erweiterung ist galois.

Satz 9.7. *Sei $q = p^n$. Dann ist $\mathbb{F}_q/\mathbb{F}_p$ galois. Die Galoisgruppe ist zyklisch und wird vom Frobenius ϕ_1 erzeugt.*

Wir werden später auch das komplementäre Ergebnis zeigen: Die Gruppe $\mathbb{F}_q^*$ ist zyklisch der Ordnung $q - 1$.

Galoisgruppe S_5

Nicht alle Galoisgruppen sind abelsch!

Satz 9.8. *Sei $P = X^5 - 4X + 2$, L der Zerfällungskörper von P über $\mathbb{Q}$. Dann ist*

$$\mathrm{Gal}(L/\mathbb{Q}) \cong S_5 \ .$$

Zur Vorbereitung brauchen wir weitere Sätze der Gruppentheorie:

Lemma 9.9. *Sei G eine endliche Gruppe, p ein Primteiler der Gruppenordnung. Dann enthält G ein Element der Ordnung p.*

Beweis: Wir beginnen mit dem abelschen Fall. Sei $b \in G$, $b \neq e$. Dann ist $\langle b \rangle \subset G$ eine Untergruppe. Falls $|b| = np$, so ist b^n ein Element der Ordnung p. Andernfalls handelt es sich um einen echten Normalteiler und p teilt die Ordnung von $\overline{G} = G/\langle b \rangle$. Nach Induktionsvoraussetzung hat $\overline{G}$ ein Element $\overline{a}$ mit Ordnung p. Sei $a \in G$ ein Urbild. Die Abbildung $\langle a \rangle \to \langle \overline{a} \rangle$ ist surjektiv (beachte: $\langle a \rangle \subset G$, $\langle \overline{a} \rangle \subset \overline{G}$). Also ist die Ordnung ein Vielfaches von p.

Auch für den allgemeinen Fall argumentieren wir mit Induktion nach $|G|$. Falls $|G| = p$, so G zyklisch der Ordnung p. Insbesondere existieren Elemente der Ordnung p. Die Aussage sei wahr für alle Gruppen mit Ordnung kleiner als $|G|$, also auch für alle Untergruppen $H \subsetneq G$. Wird ihre Ordnung von p geteilt, so haben sie ein Element der Ordnung p.

Wir führen nun einen indirekten Beweis. Wenn G kein Element der Ordnung p hat, so gilt das auch für jede Untergruppe. Für jede Untergruppe $H \subsetneq G$ ist p kein Teiler von $|H|$, also komplementär ein Teiler von $[G : H]$. Wir betrachten nun die Operation von G auf sich selbst durch

$$G \times G \to G; \quad (g, h) \mapsto ghg^{-1}.$$

Nach der Bahnformel 3.10 gilt

$$|G| = \sum_{i=1}^{n} [G : G_{x_i}],$$

wobei $x_1, \ldots, x_n$ ein Vertretersystem der Bahnen durchläuft. Die Fixpunkte sind diejenigen Elemente mit $ghg^{-1} = h$ für alle $g \in G$, also die Elemente des Zentrums. Für alle anderen Bahnen ist die Standgruppe echt kleiner als G, ihr Index wird von p geteilt. Zusammen folgt, dass p die Ordnung von $Z(G)$ teilt. Das Zentrum ist abelsch, diesen Fall hatten wir vorab erledigt. □

Lemma 9.10. *Sei $G \subset S_5$ eine Untergruppe, die ein Element der Ordnung 5 und eine Transposition enthält. Dann ist $G = S_5$.*

Beweis: Ohne Einschränkung enthält G das Elemente (1 2 3 4 5) und damit auch

$$\langle (1\ 2\ 3\ 4\ 5) \rangle = \{e, (1\ 2\ 3\ 4\ 5), (1\ 3\ 5\ 2\ 4), (1\ 4\ 2\ 5\ 3), (1\ 5\ 4\ 3\ 2)\}\ .$$

Diese Untergruppe operiert transitiv auf der Menge $\{1, 2, \ldots, 5\}$. Ohne Einschränkung ist die Transposition in G gleich (1 2). Damit enthält G auch die Elemente

$$(1\ 2)(1\ 2\ 3\ 4\ 5) = (1)(2\ 3\ 4\ 5)$$
$$(1\ 2)(1\ 3\ 5\ 2\ 4) = (1\ 3\ 5)(2\ 4)$$

G enthält Elemente der Ordnung $5, 4, 6$, also ist die Ordnung von G ein Vielfaches von 60. Die Gruppe S_5 hat die Ordnung $5! = 120$. Angenommen $|G| = 60$. Dann ist G ein Normalteiler von S_5 und $G \cap A_5$ ein Normalteiler von A_5.

Da die A_5 einfach ist, folgt $G \cap A_5 = \{e\}, A_5$. Der erste Fall scheidet aus, da $(12345) \in A_5$. Also ist $G \cap A_5 = A_5 \Rightarrow G = A_5$. G enthält jedoch die Transposition (1 2). Es bleibt der Fall $|G| = 120 \Rightarrow G = S_5$. □

Beweis von Satz 9.8. Nach Eisensteinkriterium für $p = 2$ ist das Polynom irreduzibel. Seien $A = \{\alpha_1, \alpha_2, \alpha_3, \alpha_4, \alpha_5\}$ die Nullstellen von P in $\mathbb{C}$. Wir untersuchen P mittels Kurvendiskussion.

x	-2	-1	0	1	2
$P(x)$	-22	5	2	-1	26

Also hat P mindestens drei reelle Nullstellen. Wir bestimmen die Anzahl der Maxima und Minima aus der Ableitung $P' = 5X^4 - 4$. Sie hat Nullstellen in $x = \pm\sqrt[4]{\frac{4}{5}}$, also genau ein Maximum und ein Minimum. P hat genau drei reelle Nullstellen. Die beiden anderen sind komplex.
Wir betrachten die Operation

$$\mathrm{Gal}(L/\mathbb{Q}) \times A \to A, (\sigma, \alpha) \mapsto \sigma(\alpha) \ .$$

Sie definiert einen Gruppenhomomorphismus

$$\phi : \mathrm{Gal}(L/\mathbb{Q}) \to S(A) \cong S_5 \ .$$

Diese Abbildung ist injektiv, denn σ wird durch die Werte auf den Wurzeln von P bestimmt.
Auf $L \subset \mathbb{C}$ operiert die komplexe Konjugation. Sie definiert $\sigma_2 \in \mathrm{Gal}(L/\mathbb{Q})$. Sie hält die reellen Nullstellen fest und vertauscht die beiden komplexen, d.h. σ_2 ist eine Transposition.
Die Operation von $\mathrm{Gal}(L/K)$ auf A ist transitiv. Nach der Bahnformel ist $5 = |A|$ ein Teiler von $|\mathrm{Gal}(L/K)|$. Nach Lemma 9.9 hat $\mathrm{Gal}(L/K)$ ein Element der Ordnung 5. Dies gilt dann auch für das Bild von ϕ. Nach Lemma 9.10 ist die $\phi(G) = S_5$. □

Kapitel 10

Normale und separable Körpererweiterungen

Es gibt verschiedene äquivalente Charakterisierungen von galoisschen Körpererweiterungen. Diese wollen wir verstehen. Es geht dabei vor allem um das Abzählen der Nullstellen von Minimalpolynomen.

Separabilität

Definition 10.1. *(i) Ein irreduzibles Polynom in $K[X]$ heißt* separabel*, falls es keine doppelten Nullstellen über dem algebraischen Abschluss hat.*

(ii) Ein beliebiges Polynom heißt separabel, wenn alle irreduziblen Faktoren separabel sind.

(iii) Sei L/K eine Körpererweiterung. $\alpha \in L$ heißt separabel *über K, falls sein Minimalpolynom separabel ist.*

Beispiel. (i) $X^2 + 1 \in \mathbb{R}[X]$

(ii) $(X - \alpha)^n \in \mathbb{Q}[X]$ ebenfalls separabel, da $X - \alpha$ separabel.

(iii) Jedes Element von $\mathbb{C}/\mathbb{R}$ ist separabel.

Wir benötigen ein Kriterium! Wir erinnern uns an Analysis: Eine Funktion hat genau dann eine doppelte Nullstelle in $x \in \mathbb{R}$, wenn die Ableitung in x verschwindet.

Definition 10.2. *Sei K ein Körper,*

$$P(X) = a_0 + a_1 X + a_2 X^2 + \cdots + a_n X^n \in K[X] \ .$$

Die Ableitung *von P ist*

$$P'(X) = a_1 + 2a_2 X + \cdots + n a_n X^{n-1} \ .$$

Lemma 10.3 (Rechenregeln)**.** $P, Q \in K[X]$, $\lambda \in K$.

(i) $(P+Q)' = P' + Q'$.

(ii) $(P \cdot Q)' = P \cdot Q' + P' \cdot Q$.

(iii) $(\lambda P)' = \lambda P'$.

Die Ableitung ist eine K-lineare Abbildung $K[X] \to K[X]$, die die Leibniz-Regel erfüllt.

Beweis: $P = \sum_{i=0}^{n} a_i X^i$, $Q = \sum_{j=0}^{n} b_j X^j$, $\lambda \in K$.

$$(P+Q)' = \Big(\sum (a_i + b_i) X^i\Big)' = \sum i(a_i + b_i) X^{i-1}$$
$$= \sum i a_i X^{i-1} + \sum i b_i X^{i-1} = P' + Q'$$

$$(PQ)' = \left(\sum_i a_i X^i \sum_j b_j X^i\right)' = \left(\sum_{i,j} a_i b_j X^{i+j}\right)'$$
$$= \sum_{i,j} (i+j) a_i b_j X^{i+j-1} = \sum j a_i b_j X^{i+j-1} + \sum i a_i b_j X^{i+j-1}$$
$$= \sum a_i X^i \sum j b_j X^{j-1} + \sum i a_i X^{i-1} \sum b_j X^j = P'Q + PQ'$$

(iii) ist Spezialfall von (ii), denn $\lambda' = 0$. □

Lemma 10.4. *Sei $P \in K[X]$. Ein Element $\alpha \in \overline{K}$ ist doppelte Nullstelle von P, genau dann wenn $P(\alpha) = 0$ und $P'(\alpha) = 0$. Sei P irreduzibel. Dann ist P separabel, genau dann wenn $P' \neq 0$ als Element von $K[X]$.*

Beweis: Man beachte, dass P' über K und über $\overline{K}$ übereinstimmen. Sei $P(X) = (X - \alpha) \prod (X - \alpha_i)$ mit $\alpha, \alpha_i \in \overline{K}$. Nach Produktregel gilt

$$P' = 1 \cdot \prod (X - \alpha_i) + (X - \alpha) \Big(\prod (X - \alpha_i)\Big)'$$

und daher

$$P'(\alpha) = \prod (\alpha - \alpha_i)\ .$$

Daher ist

$$P'(\alpha) = 0 \Leftrightarrow \alpha = \alpha_i \text{ für ein } i.$$

Sei nun P irreduzibel, P nicht separabel, d.h. es gibt ein $\alpha \in \overline{K}$, welches mehrfache Nullstelle von P ist. Dieses α ist gemeinsame Nullstelle von P und P'. Es gilt $\deg P' < \deg P$ und P ist das Minimalpolynom von α. Daher ist $P' = 0$. □

Gibt es das überhaupt? Ja! X^p-1 in Charakteristik p hat Ableitung 0! Tatsächlich ist aber $X^p - 1 = (X-1)^p$, also trotzdem separabel. Wir halten fest:

Korollar 10.5. *Sei* $\operatorname{Char} K = 0$. *Dann sind alle Polynome in* $K[X]$ *separabel.*

Beweis: Offensichtlich $\deg P' = \deg P - 1$, also $P' \neq 0$ für irreduzible Polynome. □

Lemma 10.6. *Sei* $\operatorname{Char} K = p > 0$, $P \in K[X]$. *Es gilt* $P' = 0$ *genau dann, wenn*

$$P(X) = a_0 + a_p X^p + a_{2p} X^{2p} \dots a_{np} X^{np},$$

d.h. $P(X) \in K[X^p]$.

Beweis: $P(X) = \sum a_i X^i$, $P' = \sum i a_i X^i$. $P' = 0$ bedeutet $i a_i = 0$ für alle i, also $i = 0$ in K oder $a_i = 0$. Nach Definition der Charakteristik ist $i = 0$ in K, genau wenn $i = kp$ für $k \in \mathbb{N}$. □

Nachdem wir dieses Kriterium geklärt haben, kommen wir zurück zu Körpererweiterungen.

Definition 10.7. *Sei* L/K *endlich. Die Anzahl der Körperhomomorphismen*

$$\operatorname{Hom}_K(L, \overline{K}) = \{\sigma : L \to \overline{K} | \sigma|_K = \mathrm{id}\}$$

in einen algebraischen Abschluss von K *heißt* Separabilitätsgrad $[L : K]_s$ *von* L/K. *Eine endliche Körpererweiterung* L/K *heißt* separabel, *wenn* $[L : K]_s = [L : K]$ *ist.*

Beispiel. Sei $L = K(\alpha)$. Dann ist L/K genau dann separabel, wenn $\operatorname{Min}(\alpha) \in K[X]$ in $\overline{K}$ so viele Nullstellen hat wie $\deg \operatorname{Min}(\alpha)$, d.h. wenn es keine doppelten Nullstellen in $\overline{K}$ hat.

Lemma 10.8 (Gradformel)**.** *Seien* $K \subset F \subset L]$ *endliche Erweiterungen. Dann gilt*

$$[L : K]_s = [L : F]_s [F : K]_s.$$

Beweis: Jede Einbettung $\sigma : L \to \overline{K}$ definiert durch Einschränken auch eine Einbettung $\sigma|_F : F \to \overline{K}$. Wir fassen $\overline{K}$ via dieser Einbettung als algebraischen Abschluss von F auf. Die Anzahl der möglichen Fortsetzungen ist gleich $[L : F]_s$. □

Korollar 10.9. *Sei* L/K *endlich.*

(i) $[L : K]_s \leq [L : K]$.

(ii) L/K *ist genau dann separabel, wenn alle Elemente separabel sind.*

(iii) Ist F *ein Zwischenkörper, also* $K \subset F \subset L$, *so ist* L/K *genau dann separabel, wenn* L/F *und* F/K *separabel sind.*

Beweis: Falls $L = K(\alpha)$, so gilt die Abschätzung. Für allgemeines $L = K(\alpha_1, \ldots, \alpha_n)$ erhalten wir sie durch Anwenden der Gradformel für Grad und Separabilitätsgrad.
Sei F ein Zwischenkörper. Wir haben

$$[L : F]_s[F : K]_s \leq [L : F][F : K] = [L : F].$$

Gleichheit gilt genau dann, wenn wir in beiden Faktoren Gleichheit haben.
Sei $\alpha \in L$. Ist L/K separabel, dann auch $K(\alpha)/K$. Im einfachen Fall bedeutet dies genau, dass das Minimalpolynom von α separabel ist. Für die Umkehrung bemerken wir: Wenn ein Polynom separabel ist über K, dann auch über allen algebraischen Erweiterungen F. Ist also $L = K(\alpha_1, \ldots, \alpha_n)$ mit separablen α_i, so ist jede der Erweiterungen $K(\alpha_1, \ldots, \alpha_i)/K(\alpha_1, \ldots, \alpha_{i-1})$ separabel. Dann ist auch L/K separabel. □

Definition 10.10. *Ein Körper heißt* vollkommen*, wenn alle Polynome (und damit alle algebraischen Körpererweiterungen) separabel sind.*

Beispiel. Körper der Charakteristik 0, algebraisch abgeschlossene Körper.

Satz 10.11. *Sei K ein endlicher Körper. Dann ist K vollkommen.*

Beweis: Sei $\phi : K \to K$ der Frobenius, $x \mapsto x^p$. Nach Satz 8.6 und der nachfolgenden Bemerkung ist dies ein *bijektiver* Körperhomomorphismus. Sei

$$P = \sum a_{ip} X^{ip} \in K[X]$$

mit $P' = 0$. Sei $b_i = \phi^{-1} a_{ip}$, d.h. $b_i^p = a_{ip}$. Dann gilt

$$(\sum b_i X^i)^p = \sum b_i^p X^{ip} = P \ .$$

Insbesondere ist P nicht irreduzibel. Umgekehrt sind irreduzible Polynome separabel. □

Normale Erweiterungen

Definition 10.12. *Eine Körpererweiterung L/K heißt* normal*, wenn jedes irreduzible Polynom $P \in K[X]$, welches in L ein Nullstelle hat, über L in Linearfaktoren zerfällt.*

Beispiel. $\overline{K}/K$ ist normal.

Korollar 10.13. *Eine endliche Erweiterung ist genau dann normal, wenn*

$$|\operatorname{Gal}(L/K)| = [L : K]_s.$$

Sie ist galois genau dann, wenn sie normal und separabel ist.

Beweis: Wir fixieren eine Injektion $L \subset \overline{K}$. Dies definiert eine injektive Abbildung

$$\mathrm{Gal}(L/K) \to \mathrm{Hom}_K(L, \overline{K}).$$

Sei L/K normal. Jeder Homomorphismus $\sigma \in \mathrm{Hom}_K(L, \overline{K})$ hat bereits Bild in L, denn die Nullstellen aller Minimalpolynome liegen in L. Insbesondere stimmen die Anzahlen überein.

Umgekehrt folgt aus der Gleichheit der Anzahlen die Gleichheit der Mengen. Jede Nullstelle eines Minimalpolynoms eines $\alpha \in L$ taucht als $\sigma(\alpha)$ auf, muss also nun in L liegen.

Ist L/K zusätzlich separabel, so ist $[L : K] = [L : K]_s$. □

Lemma 10.14. *Sei L/K endlich und normal. Dann gibt es $P \in K[X]$, so dass L der Zerfällungskörper von P ist. Ist L/K zusätzlich separabel, so kann P separabel gewählt werden.*

Beweis: Da die Erweiterung endlich ist, gilt $L = K(\alpha_1, \ldots, \alpha_n)$. Sei P_i das Minimalpolynom von α_i, $P = \prod P_i$. Da L normal ist, zerfällt P über L in Linearfaktoren. Zerfällt P über einem Teilkörper, so enthält dieser die α_i, ist also gleich L.

Ist L/K zusätzlich separabel, so sind alle P_i separabel, also auch P. □

Tatsächlich gilt auch die Umkehrung!

Satz 10.15. *Sei L/K Zerfällungskörper von $P \in K[X]$. Dann ist die Erweiterung normal. Ist P zusätzlich separabel, so ist L/K galois.*

Beweis: Es ist $L = K(\alpha_1, \ldots, \alpha_n)$, wobei

$$P = (X - \alpha_1)(X - \alpha_2) \ldots (X - \alpha_n).$$

Wir betrachten die Kette

$$K \subset K(\alpha_1) \subset \cdots \subset K(\alpha_1, \ldots, \alpha_n).$$

Wir fixieren eine Einbettung $L \to \overline{K}$ und benutzen sie, um schrittweise

$$\mathrm{Hom}_K(K(\alpha_1, \ldots, \alpha_i), L) \subset \mathrm{Hom}_K(\alpha_1, \ldots, \alpha_i), \overline{K})$$

zu vergleichen. In jedem Schritt haben wir Gleichheit, da das Minimalpolynom von α_i in $K(\alpha_1, \ldots, \alpha_{i-1})[X]$ ein Teiler von P ist und daher alle Nullstellen des Minimalpolynoms bereits in L liegen. Für $i = n$ erhalten wir die Behauptung.

Ist P separabel, so sind alle α_i separabel. In jedem Schritt ist die Erweiterung separabel, daher insgesamt separabel. □

Korollar 10.16. *Sei L/K endlich, normal, $K \subset F \subset L$ ein Zwischenkörper. Dann ist L/F normal.*

Beweis: Sei L Zerfällungskörper von P über K. Dann ist L auch Zerfällungkörper von P über F. □

Bemerkung. Wie man am Beispiel $\mathbb{Q} \subset \mathbb{Q}(\sqrt[4]{2}) \subset \mathbb{Q}(\sqrt[4]{2}, i)$ sieht, ist F/K nicht immer normal.

Korollar 10.17. *Sei L/K endlich. Dann existiert N/L endlich, so dass N/K normal ist.*

Beweis: $L = K(\alpha_1, \ldots, \alpha_n)$, $P = \prod P_i$ Produkt der Minimalpolynome P_i der α_i. Sei N der Zerfällungskörper von P. □

Definition 10.18. *Sei L/K eine Körpererweiterung. Die* normale Hülle *N/L ist eine Erweiterung N/L, so dass N/K normal ist, und minimal mit dieser Eigenschaft, d.h. für alle Zwischenkörper $N/N'/L$ mit N'/K normal folgt $N' = N$.*

Lemma 10.19. *Die normale Hülle ist eindeutig bis auf Isomorphie.*

Beweis: Seien P, N wie im Beweis des Korollars und N' eine weitere normale Hülle. Über N' zerfällt P in Linearfaktoren. Nach Satz 8.8 existiert ein Homomorphismus $\sigma : N \to N'$, der mit der Inklusion von L verträglich ist. Das Bild von σ ist normal über K, also ist σ surjektiv. □

Galois-Erweiterungen

Wenn eine Gruppe G auf einer Menge M operiert, so bezeichnetete M^G die Menge der Fixpunkte von G,

Definition 10.20. *Sei L ein Körper, $G \subset \mathrm{Aut}(L) = \{\sigma : L \to L \mid \text{Körperisom.}\}$. Dann heißt*

$$L^G = \{\alpha \in L \mid \sigma(\alpha) = \alpha \text{ für alle } \alpha \in G\}$$

Fixkörper *von G.*

Bemerkung. Dies ist wirklich ein Körper.

Lemma 10.21. *Sei L Körper, $H \subset \mathrm{Aut}(L)$ eine endliche Gruppe von Körperautomorphismen.Dann gilt*

$$[L : L^H] = |H|$$

Die Erweiterung L/L^H ist galois mit Galoisgruppe H.

Beweis: Sei $K = L^H$. Es gilt $H \subset \mathrm{Gal}(L/K)$ und daher

$$|H| \leq |\mathrm{Gal}(L/K)| \leq [L : K]$$

Aus der behaupteten Gleichheit folgt dann auch die Aussage über die Galoisgruppe.

Sei $n = |H|$ und $r = [L : L^H]$ (wir erlauben a priori $r = \infty$). Angenommen $n < r$. Sei $H = \{\sigma_1, \ldots, \sigma_n\}$ und $b_1, \ldots, b_r$ eine K-Basis von L. Wir betrachten das lineare Gleichungssystem über L

$$\sum_j x_j \sigma_i(b_j) = 0 \text{ für alle } i = 1, \ldots, n.$$

Da wir mehr Unbekannte als Gleichungen haben, gibt es eine nicht-triviale Lösung $(x_1, \ldots, x_r)$. Sei $N = N(x_1, \ldots, x_r)$ die Anzahl der j mit $x_j \neq 0$. Nach Vorraussetzung ist $N \geq 1$. Wir wählen die Lösung so, dass $N(x_1, \ldots, x_r)$ minimal. Ohne Einschränkung ist $x_1 = 1$.
Wir wenden σ_k auf unsere Gleichungen an und erhalten:

$$0 = \sigma_k \left(\sum_j x_j \sigma_i(b_j) \right) = \sum_j \sigma_k(x_j) \sigma_k \circ \sigma_i(b_j) \text{ für alle } i.$$

Die $\sigma_k \circ \sigma_i$ durchlaufen ganz H, also $\sigma_k \circ \sigma_i = \sigma_{i'}$ für genau ein i'.

$$0 = \sum_j \sigma_k(x_j) \sigma_{i'}(b_j) \text{ für alle } i'.$$

Mit anderen Worten, auch $(\sigma_k(x_1), \ldots, \sigma_k(x_n))$ ist eine Lösung unseres Gleichungssystems.
Wir betrachten das Tupel

$$y_j = x_j - \sigma_k(x_j).$$

Es ist eine neue Lösung mit echt kleinerem $N(y_j)$, denn $y_1 = 1 - \sigma_k(1) = 0$. Nach Wahl von $(x_1, \ldots, x_r)$ muss dann $y_j = 0$ für alle j gelten, d.h.

$$x_j = \sigma_k(x_j) \text{ für alle } j.$$

Da das für alle k gilt, erhalten wir $x_j \in K$. Speziell für $\sigma_k = \mathrm{id}$ erhalten wir

$$0 = \sum_j x_j b_j$$

im Widerspruch zur K-linearen Unabhängigkeit der b_j. Die Annahme war falsch, also gilt $n = r$. □

Damit wissen wir alles, was wir über die Charakterisierung von Galois-Erweiterungen wissen müssen.

Theorem 10.22. *Sei L/K endliche Körpererweiterung. Dann sind äquivalent.*

(i) *L/K ist galois;*

(ii) $|\operatorname{Gal}(L/K)| = [L : K]$*;*

(iii) *L/K ist normal und separabel;*

(iv) $L^{\mathrm{Gal}(L/K)} = K$.

Bemerkung. Die Äquivalenz von (ii) und (iv) ist bereits der wichtigste Teil des Hauptsatzes der Galoistheorie. Es gibt einen wesentlich eleganteren Beweis von Artin, der ohne die Begriffe normal und separabel auskommt.

Beweis: (i)⇔(ii) war unsere Definition. Die Äquivalenz von (ii) und (iii) haben wir bereits in Korollar 10.13 festgehalten.
Wir betrachten

$$K \subset L^{\mathrm{Gal}(L/K)} \subset L,$$

Die zweite Erweiterung hat Grad $|\operatorname{Gal}(L/K)|$, also mit der Gradformel

$$[L : K] = |\operatorname{Gal}(L/K)|[L^{\mathrm{Gal}(L/K)} : K].$$

Die Erweiterung L/K ist genau dann galois, wenn die erste Erweiterung Grad 1 hat. □

Kapitel 11

Hauptsatz der Galoistheorie

Wir fixieren nun eine endliche Erweiterung L/K und betrachten die Menge der Zwischenkörper F mit $K \subset F \subset L$. Wie hängen die Galoisgruppen zusammen?

(i) Es gilt nach Definition $\mathrm{Gal}(L/F) \subset \mathrm{Gal}(L/K)$.

(ii) Schränkt man ein Element $\sigma \in \mathrm{Gal}(L/K)$ ein auf F, so erhält man einen Homomorphismus $\sigma : F \to L$. Das Bild wird im allgemeinen *nicht* in F liegen. Dies ist aber erfüllt, falls F/K normal ist, d.h. dann erhalten wir einen Homomorphismus $\mathrm{Gal}(L/K) \to \mathrm{Gal}(F/K)$.

Umgekehrt definiert jede Untergruppe H von $\mathrm{Gal}(L/K)$ einen Zwischenkörper, nämlich L^H. Wir haben also zwei Abbildungen
Dann gibt es zwei Abbildungen

$$\begin{array}{ccccc} \mathcal{G} & \stackrel{\kappa}{\to} & \mathcal{K} & \stackrel{\gamma}{\to} & \mathcal{G} \\ G & \mapsto & L^G & & \\ & & F & \mapsto & \mathrm{Gal}(L/F) = \{\sigma \in \mathrm{Gal}(L/K) \mid \sigma \mid_F = \mathrm{id}\} \end{array}$$

Wann sind die beiden Zuordnungen zueinander invers? Im Spezialfall $H = \mathrm{Gal}(L/K)$ bedeutet dies $L^{\mathrm{Gal}(L/K)} = K$, d.h. die Erweiterung muss galois sein!

Theorem 11.1 (Hauptsatz der Galois-Theorie)**.** *Sei L/K eine endliche Galoiserweiterung von Körpern.*

(i) Dann sind die obigen Abbildungen κ und γ inklusionsumkehrend und invers zueinander. Insbesondere sind beide Abbildungen bijektiv.

(ii) Für jeden Zwischenkörper ist L/F galois, und es gilt $[L : F] = |\mathrm{Gal}(L/F)|$. Für jede Untergruppe $H \subset \mathrm{Gal}(L/K)$ gilt

$$[L : L^H] = |H|, [L^H : K] = [\mathrm{Gal}(L/K) : H] \ .$$

(iii) Für $L \supset F \supset K$ ist F/K normal (und dann auch galois), genau dann wenn $H = \mathrm{Gal}(L/F)$ ein Normalteiler von $\mathrm{Gal}(L/K)$ ist. In diesem Fall ist

$$\mathrm{Gal}(F/K) \cong \mathrm{Gal}(L/K)/\mathrm{Gal}(L/F) \ .$$

Beweis: Wir betrachten $L \supset F_1 \supset F_2 \supset K$. Dann ist

$$\mathrm{Gal}(L/F_2) = \{\sigma \in \mathrm{Gal}(L/K) \mid \sigma \mid_{F_2} = \mathrm{id}\} \supset \mathrm{Gal}(L/F_1) = \{\sigma \in \mathrm{Gal}(L/K) \mid \sigma \mid_{F_1} = \mathrm{id}\} \ .$$

Umgekehrt seien $\mathrm{Gal}(L/K) \supset H_1 \supset H_2$. Dann ist

$$L^{H_1} = \{x \in L \mid \sigma(x) = x \text{ für alle } \sigma \in H_1\} \subset L^{H_2} = \{x \in L \mid \sigma(x) = x \text{ für alle } \sigma \in H_2\} \ .$$

Sei nun F ein Zwischenkörper. Nach Vorraussetzung ist L/K normal und separabel, also ist auch L/F normal und separabel. Nach Satz 10.22 ist also L/F galois und

$$\kappa\gamma(F) = L^{\mathrm{Gal}(L/F)} = F \ .$$

Ebenfalls nach Satz 10.22 ist $[L : F] = |\mathrm{Gal}(L/F)|$.

Sei H eine Untergruppe von $\mathrm{Gal}(L/K)$. Wir setzen $F = L^H$. Dann ist $H \subset \mathrm{Gal}(L/F)$. Nach Satz 10.21 ist $[L : L^H] = |H|$.

Als Zwischenkörper ist L/L^H galois, also $[L : L^H] = \mathrm{Gal}(L/H)$. Da $H \subset \mathrm{Gal}(L/L^H)$, folgt Gleichheit. Mit anderen Worten,

$$\gamma\kappa(H) = \mathrm{Gal}(L/L^H) = H \ .$$

Die Formel für $[L^H : K]$ folgt aus der Indexformel für Untergruppen und der Gradformel für Zwischenkörper. Damit sind (i) und (ii) gezeigt.

Wir betrachten $L/F/K$. Angenommen, F/K ist normal. Dann respektiert jedes $\sigma \in \mathrm{Gal}(L/K)$ den Teilkörper F, da Elemente auf andere Nullstellen desselben Minimalpolynoms abgebildet werden. Wir erhalten eine Abbildung

$$\mathrm{Gal}(L/K) \to \mathrm{Gal}(F/K)$$

mit Kern $\mathrm{Gal}(L/F)$. Sie ist surjektiv, denn L/K ist normal, also lässt sich jedes Element von $\mathrm{Gal}(F/K)$ fortsetzen. Nach der Anzahlformel in (ii) ist F/K nun galois.

Sei umgekehrt $\mathrm{Gal}(L/F)$ ein Normalteiler. Wir zeigen, dass F/K normal ist. Sei $\alpha \in F$, $P = \mathrm{Min}(\alpha) \in K[X]$. Über L zerfällt P in Linearfaktoren. Sei α' eine weitere Nullstelle. Da L/K normal ist existiert ein $\sigma \in \mathrm{Gal}(L/K)$ mit $\sigma(\alpha) = \alpha'$. Wir wollen zeigen, dass $\alpha' = \sigma(\alpha) \in F$, d.h. invariant unter $\mathrm{Gal}(L/F)$. Sei also $\tau \in \mathrm{Gal}(L/F)$. Nach Voraussetzung ist

$$\sigma^{-1}\tau\sigma \in \mathrm{Gal}(L/F) \Rightarrow \sigma^{-1}\tau\sigma(\alpha) = \alpha \Rightarrow \tau\sigma(\alpha) = \sigma(\alpha) \ .$$

□

Korollar 11.2. *L/K galois. Dann gibt es nur endlich viele Zwischenkörper.*

Beweis: Eine endliche Gruppe hat nur endliche viele Untergruppen. □

Beispiel. Wir bestimmen die Teilkörper von $\mathbb{Q}(\sqrt[4]{2})$. Wir erraten: $\mathbb{Q}(\sqrt{2})$. Gibt es andere?
Sei K die normale Hülle von $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}$, also der Zerfällungskörper von X^4-2. Explizit ist $K=\mathbb{Q}(\sqrt[4]{2},i)$. Er ist galois über $\mathbb{Q}$. Wir bestimmen die Galoisgruppe $G=\mathrm{Gal}(K/\mathbb{Q})$. Jedes $\sigma: K\to K$ ist eindeutig durch die Werte auf $\sqrt[4]{2}$ und i bestimmt. Es gilt

$$\sigma(\sqrt[4]{2})\in\{\pm\sqrt[4]{2},\pm i\sqrt[4]{2}\}\ ,\ \sigma(i)\in\{\pm i\}\ .$$

Die Galoisgruppe hat also 8 Elemente. Sei

$$\tau(\sqrt[4]{2})=i\sqrt[4]{2}\ ,\ \tau(i)=i\ .$$

Dieses Element hat die Ordnung 4, denn

$$\tau^2(\sqrt[4]{2})=\tau(i\sqrt[4]{2})=ii\sqrt[4]{2}=-\sqrt[4]{2}\ .$$

Sei ι die komplexe Konjugation, also

$$\iota(\sqrt[4]{2})=\sqrt[4]{2}\ ,\ \iota(i)=-i\ .$$

Dieses Element hat die Ordnung 2. Es gilt

$$G=\{\tau^j,\iota\tau^j\mid j=0,1,2,3\}\ .$$

Ist die Gruppe kommutativ?

$$\iota\tau(\sqrt[4]{2})=\iota(i\sqrt[4]{2})=-i\sqrt[4]{2}\ ,\ \tau\iota(\sqrt[4]{2})=\tau(\sqrt[4]{2})=i\sqrt[4]{2}\ .$$

Nein, es gilt $\iota\tau=\tau^3\iota$. Damit haben wir die Gruppe in Erzeugern und Relationen vollständig beschrieben. Der Teilkörper $\mathbb{Q}(\sqrt[4]{2})$ ist der Fixkörper der Untergruppe $\{\mathrm{id},\iota\}$. Sie ist kein Normalteiler, wie es der Hauptsatz vorhersagt. Schließlich ist der Körper nicht normal über $\mathbb{Q}$. Teilkörper von $\mathbb{Q}(\sqrt[4]{2})$ entsprechen also Untergruppe von G, die ι enthalten. Sei H eine solche Untergruppe. Mit $\tau^3=\tau^{-1}$ oder $\iota\tau$ oder $\iota\tau^3$ enthält die Gruppe auch τ und ist damit ganz G.

$$H=\{\mathrm{id},\iota,\tau^2,\iota\tau^2\}$$

ist die einzige nichttriviale Möglichkeit. Daher ist $K^H=\mathbb{Q}(\sqrt{2})$ tatsächlich der einzige Teilkörper von $\mathbb{Q}(\sqrt[4]{2})$.

Korollar 11.3 (Satz vom primitiven Element)**.** *Sei L/K endlich und separabel. Dann ist $L=K(a)$ für ein $a\in L$, d.h. die Erweiterung ist einfach.*

Beweis: Falls K endlich ist, so gilt die Aussage, da die Gruppe L^* zyklisch ist (siehe nächstes Kapitel). Sei also K unendlich.
Es gilt $L = K(a_1, \ldots, a_n)$. Wir beweisen die Aussage mit Induktion nach n, daher ist der wesentliche Fall $n = 2$. Wir betrachten die unendlich vielen Elemente $a_1 + xa_2$ mit $x \in K$ und die von ihnen erzeugten Teilkörper. Da L/K separabel ist, gibt es nur endlich viele Teilkörper der normalen Hülle, also auch nur endlich viele Zwischenkörper von L/K. Es gibt also $x_1 \neq x_2$ mit

$$K(a_1 + x_1 a_2) = K(a_1 + xa_2)$$

Dieser Teilkörper enthält auch $(x_1 - x_2)a_2$, also auch a_2 und dann auch a_1. Er ist also gleich $K(a_1, a_2)$. Wir haben ein primitives Element gefunden. □

Lösung von Gleichungen durch Radikale

Sei $P \in \mathbb{Q}[X]$. Wir fassen $P(X) = 0$ als Gleichung auf und suchen eine Lösungsformel in Termen von $+, -, \cdot, :$ und Wurzeln $\sqrt[n]{\cdot}$, so wie es für Gleichungen vom Grad 2, 3 und 4 funktioniert.

Definition 11.4. *$\alpha \in \overline{\mathbb{Q}}$ kann durch* Radikale *ausgedrückt werden, wenn es in einem Körper $K \subset \overline{\mathbb{Q}}$ liegt mit*

$$K = K_n \supset K_{n-1} \supset \cdots \supset K_0 = \mathbb{Q} \ ,$$

wobei $K_i = K_{i-1}(\sqrt[n_i]{a_i})$ für ein $a_i \in K_i$.
Ein Körper heißt durch Radikale auflösbar*, wenn er in einem solchen K_n enthalten ist.*
Ein Polynom heißt durch Radikale auflösbar*, wenn alle seine Wurzeln durch Radikale ausgedrückt werden können, d.h. wenn sein Zerfällungskörper durch Radikale auflösbar ist.*

Wir wollen das Problem mit Galoistheorie angehen. Wir haben gesehen (zyklotomische Erweiterungen Satz 9.4 und Kummererweiterungen Satz 9.5), dass Wurzelerweiterungen abelsche Galoisgruppen haben.

Definition 11.5. *Eine Gruppe G heißt auflösbar, wenn es eine Kette*

$$\{e\} = G_0 \subset G_1 \subset \cdots \subset G_n = G$$

von Untergruppen gibt, so dass G_i ein Normalteiler von G_{i+1} ist und der Quotient G_{i+1}/G_i abelsch.

Lemma 11.6. *Mit G sind auch alle Untergruppen und Quotienten auflösbar.*

Beweis: Sei $H \subset G$ eine Untergruppe. Wir betrachten die Kette der $H_i = G_i \cap H$. Dann ist H_i ein Normalteiler von H_{i+1} und die Abbildung

$$H_{i+1}/H_i = H \cap G_{i+1}/H \cap G_i \to G_{i+1}/G_i$$

ist injektiv. Als Untergruppe einer abelschen Gruppe ist H_{i+1}/H_i abelsch, also H auflösbar.

Sei N ein Normalteiler von G, $H = G/N$. Wir setzen H_i das Bild von G_i unter der Projektion $G \to H$. Nach dem Noetherschen Isomorphiesatz gilt $H_i = G_i/G_i \cap N \cong G_iN/N$. Wieder ist H_i ein Normalteiler in H_{i+1}. Die Projektion

$$G_{i+1}/G_i \to H_{i+1}/H_i$$

ist surjektiv. Als Bild einer abelschen Gruppe ist H_{i+1}/H_i abelsch. Damit ist H auflösbar. □

Theorem 11.7. *Sei $K/\mathbb{Q}$ eine endliche Erweiterung mit normaler Hülle L. Dann sind äquivalent:*

(i) K ist durch Radikale auflösbar.

(ii) $\mathrm{Gal}(L/\mathbb{Q})$ ist auflösbar.

Beweis: Wir zeigen nur die Richtung (i) nach (ii). Die Rückrichtung ist typischer Gegenstand der Kummertheorie, vergleich z.B Bosch.

Wir haben $K \subset K_n$ und

$$K_n \supset K_{n-1} \supset \cdots \supset K_0 = \mathbb{Q} \ ,$$

wie in der Definition. Um den Hauptsatz anwenden zu können, brauchen wir Galoiserweiterungen.

Behauptung. *Es gibt eine endliche Erweiterung L_i/K_i, die normal über $\mathbb{Q}$ ist, und so dass L_i aus K_i durch Adjungieren von Wurzeln entsteht.*

Wir arbeiten uns der Kette entlang. Nach Induktionsvorausaussetzung haben wir L_i gefunden. Es ist Zerfällungskörper eines Polynoms $R \in \mathbb{Q}[X]$.

Es ist $K_{i+1} = K_i(\alpha)$ für ein α, das die Gleichung $X^{n_i} - a_i$, $a_i \in K_i$ erfüllt. Wir betrachten das Polynom

$$P = \prod_{\sigma \in \mathrm{Gal}(L_i/\mathbb{Q})} (X^{n_i} - \sigma(a_i)) \in L_i[X] \ .$$

Das Polynom ist invariant unter der Operation von $\mathrm{Gal}(L_i/\mathbb{Q})$ und die Erweiterung ist galois, also gilt $P \in \mathbb{Q}[X]$. Wir wählen für L_{i+1} den Zerfällungskörper von von RP. Er ist normal über $\mathbb{Q}$ und entsteht aus L_i durch Adjungieren der Wurzeln von P, also von n_i-ten Wurzeln. Dies beendet den Induktionsbeweis.

Ohne Einschränkung ist also $K_n/\mathbb{Q}$ normal. Dann folgt $L \subset K_n$ nach der Eigenschaft einer universellen Hülle. Sei $N = \prod n_i$, ζ eine primitive N-te Einheitswurzel. Dann ist $K_n(\zeta)$ normal über $\mathbb{Q}$. Wir betrachten die Körperkette $L_i = K_i(\zeta)$. Wegen $L_{i+1} = L_i(\sqrt[n_i]{a_i})$ ist dies wieder eine Kette von Körpern wie in der Definition. Auch $L_0 = \mathbb{Q}(\zeta)/\mathbb{Q}$ entsteht durch Adjungieren einer Wurzel, nämlich $\zeta = \sqrt[N]{1}$. Außerdem bleibt $K \subset L_n$. Die Erweiterungen L_{i+1}/L_i sind

nun Kummererweiterungen wie in Satz 9.5, denn L_i enthält mit ζ auch eine primitive n_i-te Einheitswurzel. Alle L_{i+1}/L_i sind galois mit abelscher Galoisgruppe.
Sei $H_i = \mathrm{Gal}(L_n/L_i)$ die Folge von Untergruppen zur Körperkette. Nach dem Hauptsatz der Galoistheorie ist H_{i+1} ein Normalteiler von H_i, und es gilt

$$\mathrm{Gal}(L_{i+1}/L_i) \cong H_i/H_{i+1}.$$

Damit ist $\mathrm{Gal}(L_n/\mathbb{Q})$ auflösbar. Als Quotient ist dann auch $\mathrm{Gal}(L/\mathbb{Q})$ auflösbar. □

Satz 11.8. *Sei $P = X^5 - 4X + 2$. Dieses P ist nicht durch Radikale auflösbar.*

Beweis: Der Zerfällungskörper von P hat nach Lemma 9.8 Galoisgruppe S_5. Nach dem Teil des Theorems, den wir gezeigt haben, impliziert die Auflösbarkeit von P die Auflösbarkeit von S_5. Mit S_5 wäre auch die Untergruppe A_5 auflösbar. Diese ist aber einfach und nicht-abelsch. Sie hat keine abelschen Quotienten, ist also keineswegs auflösbar. □

Kapitel 12

Zyklotomische Körper und das quadratische Reziprozitätsgesetz

Unser Ziel ist es Körper der Form $\mathbb{Q}(\zeta)$ zu verstehen, wobei ζ eine primitive d-te Einheitswurzel ist. Wir wissen aus Kapitel 7, dass $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q}) \subset (\mathbb{Z}/d\mathbb{Z})^*$ gilt. Unser Ziel ist Gleichheit zu beweisen. Wir erinnern uns auch an die Eulersche ϕ-Funktion:

$$\phi(n) = |(\mathbb{Z}/n\mathbb{Z})^*|.$$

Lemma 12.1. *Seien n, m teilerfremd. Dann gilt $\phi(nm) = \phi(n)\phi(m)$. Sei $n = p^k$ eine Primzahlpotenz. Dann gilt $\phi(n) = (p-1)p^{k-1}$. Für jedes $n \geq 1$ gilt*

$$\sum_{d|n} \phi(d) = n \ .$$

Beweis: Nach dem chinesischen Restsatz gilt

$$\mathbb{Z}/(nm)\mathbb{Z} \cong \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z} \ .$$

Die Abbildung ist ein Ringhomorphismus. Ein Element in $\mathbb{Z}/nm\mathbb{Z}$ ist invertierbar bezüglich der Multiplikation, genau dann wenn es invertierbar ist modulo n und m.

$$(\mathbb{Z}/nm\mathbb{Z})^* \cong (\mathbb{Z}/n\mathbb{Z})^* \times (\mathbb{Z}/m\mathbb{Z})^* \ .$$

In $\mathbb{Z}/p^k$ sind genau die Vielfachen von p nicht teilerfremd zu p^k. Es gilt

$$\phi(p^k) = p^k - p^{k-1} = (p-1)p^{k-1} \ .$$

Für die Summenformel zählen wir die Elemente der zyklischen Gruppe $\mathbb{Z}/n\mathbb{Z}$ ab. Es gibt $\phi(n)$ viele Elemente der Ordnung n.

Jedes Element der Gruppe hat eine Ordnung $d|n$. Alle Elemente der Ordnung d liegen in einer zyklischen Gruppe mit d Elemente, die dann $\phi(d)$ Erzeuger hat, d.h. Element der Ordnung d. □

Wir tragen auch endlich nach:

Lemma 12.2. *Sei K algebraisch abgeschlossen, d teilerfremd zur Charakteristik. Dann hat ist die Gruppe der d-ten Einheitswurzeln $\mu_d(K)$ zyklisch von Ordnung d.*

Bemerkung. Ist k ein Körper mit Charakteristik teilerfremd zu d und K der Zerfällungskörper von $X^d - 1$ über k, so enthält K also eine primitive d-te Einheitswurzel. Dies gilt insbesondere für $\mathbb{F}_q$ mit $d = q - 1$. Also ist $\mathbb{F}_q^*$ zyklisch.

Beweis: Wir zeigen, dass es genau $\phi(d) = |(\mathbb{Z}/d\mathbb{Z})^*|$ viele Elemente der Ordnung d gibt. Wir argumentieren mit Induktion nach d. Für $d = 1$ ist die Aussage klar. Das Polynom $P = X^d - 1$ ist separabel, denn seine Ableitung dX^{d-1} hat keine Nullstelle mit P gemeinsam. Es hat also in K genau d Nullstellen. Jede von ihnen hat als Ordnung einen Teiler d' von d. Nach Induktionsvoraussetzung hat $\mu_{d'}(K)$ gerade $\phi(d')$ Elemente. Wir ziehen von d die Anzahl der Elemente von echt kleinerer Ordnung ab und erhalten

$$d - \sum_{d'|d, d' \neq d} \phi(d') = \phi(d)$$

□

Wir werden dies benutzen, um den Fall von Charakteristik Null zu verstehen.

Definition 12.3. *Sei ζ eine primitive d-te Einheitswurzel in $\overline{\mathbb{Q}}$, $\Phi_d \in \mathbb{Z}[X]$ ihr normiertes Minimalpolynom. Der Körper $\mathbb{Q}(\zeta_d)$ heißt* zyklotomischer Körper *oder Kreisteilungskörper.*

Wir wollen nun Φ_d bestimmen. Mit anderen Worten: Wir wollen $X^d - 1$ über $\mathbb{Q}$ in irreduzible Faktoren zerlegen. Für jeden Teiler d' von d erhalten wir den Teiler $X^{d'} - 1$, der sich selbst wieder in irreduzible Faktoren zerlegen lässt. Für Primzahlen p wissen wir bereits (Beispiel zum Eisensteinkriterium, Satz 4.25):

$$\Phi_p(X) = X^{p-1} + X^{p-2} + \cdots + 1$$

Beispiel. $d = 6$ hat die Teiler $1, 2, 3$. Daher gilt

$$\begin{aligned}
X^2 - 1 &= (X-1)(X+1) = \Phi_1\Phi_2 \\
X^3 - 1 &= (X-1)(X^2+X+1) = \Phi_1\Phi_3 \\
X^6 - 1 &= (X^3-1)(X^3+1) = (X-1)(X^2+X+1)(X+1)(X^2-X+1) \\
&= \Phi_1\Phi_3\Phi_2\Phi_6
\end{aligned}$$

denn $\Phi_6 = X^2 - X + 1$ ist irreduzibel.

Dieses Beispiel illustriert, dass alle Φ_d als Teiler eines normierten ganzzahligen Polynoms ganzzahlig sind (Gauß-Lemma 4.23). Die obigen Überlegungen gelten über jedem Grundkörper. Über $\mathbb{Q}$ gibt es keine weiteren Zerlegungen mehr!

Satz 12.4. *Alle primitiven d-ten Einheitswurzeln in $\overline{\mathbb{Q}}$ sind Nullstellen von Φ_d. Es gilt*

$$\deg \Phi_d = \phi(d) = |(\mathbb{Z}/d\mathbb{Z})^*|,$$
$$\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q}) \cong (\mathbb{Z}/d\mathbb{Z})^*.$$

Beweis: Wir haben gesehen, dass es genau $|(\mathbb{Z}/d\mathbb{Z})^*|$ primitive d-te Einheitswurzeln in $\overline{\mathbb{Q}}$ gibt. Wenn jede von ihnen Nullstelle von Φ_d ist, dann ist $\deg \Phi(d) \geq |(\mathbb{Z}/d\mathbb{Z})^*|$. Nach Satz 9.4 ist $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$ isomorph zu einer Untergruppe von $|(\mathbb{Z}/d\mathbb{Z})^*|$. Da die Erweiterung normal (und separabel) ist, folgt $\deg \Phi(d) \leq |(\mathbb{Z}/d\mathbb{Z})^*|$, also Gleichheit und die Berechnung der Galoisgruppe. Zu zeigen ist also die erste Behauptung.

Behauptung. *Sei p eine Primzahl, die d nicht teilt. Dann sind ζ und ζ^p Nullstellen von Φ_d.*

Nach Voraussetzung ist ζ Nullstelle von Φ_d. Sei

$$X^d - 1 = \Phi_d H$$

die Zerlegung in $\mathbb{Q}[X]$. Da Φ_d normiert ist und $X^d - 1$ ganzzahlig, sind auch Φ_d und H ganzzahlig und normiert (Satz von Gauß 4.23). Angenommen, ζ^p ist nicht Nullstelle von Φ_d. Dann ist es Nullstelle von H. Also ist ζ eine Nullstelle von $H(X^p)$. Da Φ_d das Minimalpolynom ist, folgt

$$\Phi_d \mid H(X^p) \ .$$

Wir reduzieren die Polynome modulo p. Sei $\overline{\Phi}_d$ die Reduktion von Φ_d, $\overline{H}$ die von H. Es gilt also in $\mathbb{F}_p[X]$:

$$X^d - 1 = \overline{\Phi}_d \overline{H} \ , \overline{\Phi}_d \mid \overline{H}(X^p) = \overline{H}^p \ .$$

Jede Nullstelle von $\overline{\Phi}_d$ in $\overline{\mathbb{F}}_p$ ist auch eine Nullstelle von $\overline{H}$, also eine doppelte Nullstelle von $X^d - 1$. Da p kein Teiler von d ist, hat aber $X^d - 1$ keine doppelten Nullstellen. Der Widerspruch zeigt, dass ζ^p Nullstelle von Φ_d ist.
Man beachte, dass Φ_d dann auch das Minimalpolynom von ζ^p ist. Sei ζ^i eine primitive d-te Einheitswurzel. Wir zerlegen $i = p_1 \dots p_k$ in Primfaktoren (Wiederholungen erlaubt). Da i teilerfremd zu d ist, teilt kein p_i die Zahl d. Nach dem bereits gezeigten sind auch $\zeta^{p_1}, (\zeta^{p_1})^{p_2}, \dots, \zeta^i$ Nullstellen von Φ_d. □

Mit anderen Worten: $X^d - 1$ hat die nur die offensichtlichen Teiler.

Beispiel. $d = 12$. Die Teiler von 12 sind $1, 2, 3, 4, 6$. Die teilerfremden Zahlen sind $1, 5, 7, 11$. Also hat Φ_{12} den Grad 4. Es gilt

$$X^{12} - 1 = \Phi_{12}\Phi_6\Phi_4\Phi_3\Phi_2\Phi_1 \ ,$$
$$(X^6 - 1) = \Phi_6\Phi_3\Phi_2\Phi_1 \ , (X^{12} - 1)/(X^6 - 1) = \Phi_{12}\Phi_4 = X^6 + 1 \ ,$$
$$(X^4 - 1) = \Phi_4\Phi_2\Phi_1 \ , \Phi_4 = (X^4 - 1)/(X^2 - 1) = X^2 + 1$$
$$\Phi_{12} = (X^6 + 1)/(X^2 + 1) = X^4 - X^2 + 1$$

Bemerkung. Haupttrick des Beweises war das Element von $G = \mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$ mit $\zeta \mapsto \zeta^p$ zu betrachten, wobei p teilerfremd zu d. Dahinter steckt ein Lift der Frobeniusabbildung nach Charakteristik 0, d.h. eine Einbettung

$$\mathrm{Gal}(\mathbb{F}_q/\mathbb{F}_p) \to G$$

wobei $\mathbb{F}_q$ der Zerfällungskörper von $X^d - 1$ über $\mathbb{F}_p$.

Wir kommen nun zu den Anwendungen.

Korollar 12.5 (vergleiche Satz 6.4)**.** *Das regelmäßige n-Eck ist genau dann mit Zirkel und Lineal konstruierbar, wenn $n = 2^m p_1 \dots p_i$ mit Fermatschen Primzahlen p_j ist.*

Beweis: Sei ζ eine primitive n-te Einheitswurzel. Angenommen, ζ ist mit Zirkel und Lineal konstruierbar. Nach Theorem 6.3 ist dann $[\mathbb{Q}(\zeta) : \mathbb{Q}] = \phi(n)$ eine Potenz von 2. Sei $n = 2^m p_1^{m_1} \dots p_i^{m_i}$ die Primfaktorzerlegung von n. Dann gilt

$$\phi(n) = 2^{m-1} p_1 (p_1^{m_1 - 1}) \dots p_i (p_i^{m_i - 1}).$$

In der Primfaktorzerlegung von n darf also keine Primzahl ungleich 2 mit höherer Multiplizität vorkommen. Für die vorkommenden p_j muss $p_j - 1$ eine Potenz von 2 sein. Wie in Kapitel 6 sind dies genau die Fermatschen Primzahlen.

Sei umkehrt n so, dass $\phi(n)$ eine Potenz von 2 ist. Dann ist $|\mathrm{Gal}(\mathbb{Q}(\zeta) : \mathbb{Q})|$ eine Potenz 2^N von 2. Die Gruppe enthält nach Lemma 9.9 ein Element g der Ordnung 2. Sei $H = \langle g \rangle$, $K_{N-1} = \mathbb{Q}(\zeta)^H$. Die Erweiterung $\mathbb{Q}(\zeta)/K_{N-1}$ hat Grad 2. Da $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$ abelsch ist, ist H ein Normalteiler. Nach dem Hauptsatz der Galoistheorie ist $K_{N-1}/\mathbb{Q}$ galois mit Grad 2^{N-1} und abelscher Galoisgruppe. Wir wiederholen das Argument und finden die Kette von Zwischenkörpern, die in Theorem 6.3 verlangt wird, damit ζ konstruierbar ist. □

Beispiel. Konstruktion des regelmäßigen 5-Ecks: Sei $\zeta = \exp(2\pi i/5)$. Das Minimalpolynom von ζ ist $X^4 + X^3 + X^2 + X + 1$. Die Erweiterung $\mathbb{Q}(\zeta)/\mathbb{Q}$ ist galois. Die Elemente der Galoisgruppe sind durch ein $i \in (\mathbb{Z}/5\mathbb{Z})^*$ bestimmt. Die Zuordnung ist $\sigma_i(\zeta) = \zeta^i$. Die Gruppe $(\mathbb{Z}/5\mathbb{Z})^*$ ist zyklisch mit Erzeuger 2, denn es ist $2^2 = 4, 2^3 = 8 = 3, 2^4 = 6 = 1$. Hierin ist $2^2 = 4$ ein Element der Ordnung 2. Wir betrachten den Fixkörper von $H = \langle \sigma_4 \rangle$. Wegen

$$\sigma_4(\zeta) = \zeta^4 = \zeta^{-1} = \overline{\zeta}$$

operiert σ_4 als komplexe Konjugation. Der Fixkörper enthält Er enthält $\alpha = \zeta+\zeta^{-1}$, den dieses Element ist invariant unter σ_4. Das Element ist nicht invariant unter σ_2, denn sonst wäre

$$\zeta + \zeta^{-1} = \zeta^2 + \zeta^{-2} \Rightarrow \zeta^3 + \zeta = \zeta^4 + 1$$

Vergleich mit dem Minimalpolynom von ζ ergibt einen Widerspruch. Die gesuchte Kette von Körpern ist also

$$\mathbb{Q} \subset \mathbb{Q}(\alpha) \subset \mathbb{Q}(\zeta) \ .$$

Das Minimalpolynom von ζ über $\mathbb{Q}(\alpha)$ ist

$$(X - \zeta)(X - \iota(\zeta)) = X^2 - \alpha X + 1 \ .$$

Die Galoisgruppe von $\mathbb{Q}(\alpha)/\mathbb{Q}$ ist $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})/H$. Sie enthält die Identität und die Restklasse von $\sigma : \zeta \mapsto \zeta^2$. Also ist das Minimalpolynom von α über $\mathbb{Q}$

$$(X-\alpha)(X-\sigma(\alpha)) = X^2-(\zeta+\zeta^{-1}+\zeta^2+\zeta^{-2})+(\zeta+\zeta^{-1})(\zeta^2+\zeta^{-2}) = X^2+X-1 \ .$$

Die Lösungsformel für quadratische Gleichungen sagt nun, welche Quadratwurzeln wir konstruieren müssen.
Dasselbe Verfahren funktioniert natürlich auch für das 17-Eck.

Quadratische Reste

Definition 12.6. *Sei p eine Primzahl, $a \in \mathbb{Z}$ teilerfremd zu p. Die Zahl a heißt* quadratischer Rest modulo p, *wenn die Gleichung*

$$x^2 = a \mod p$$

lösbar ist. Sie heißt andernfalls Nichtrest.

Offensichtlich hängt die Eigenschaft nur von der Restklasse $\overline{a} \in \mathbb{F}_p^*$ ab. Die quadratischen Reste sind die Elemente von $(\mathbb{F}_p^*)^2$.

Lemma 12.7. *Sei p ungerade. Dann gibt es in $\mathbb{F}_p$ genauso viele quadratische Reste wie Nichtreste. Die Untergruppe $(\mathbb{F}_p^*)^2 \subset \mathbb{F}_p^*$ hat den Index 2.*

Beweis: Wir wenden den Homomorphiesatz an. Der surjektive Gruppenhomomorphismus $\mathbb{F}_p^* \to (\mathbb{F}_p^*)^2$ mit $x \mapsto x^2$ hat den Kern $\{\pm 1\}$. Dies Menge hat 2 Elemente, wenn $p \neq 2$. Hieraus erhalten wir $[\mathbb{F}_p^* : \{\pm 1\}] = |(\mathbb{F}_p^*)^2| = (p-1)/2$. □

Definition 12.8 (Legendre-Symbol)**.** *Sei p eine ungerade Primzahl, $a \in \mathbb{Z}$. Wir definieren das* Legendre-Symbol

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & a \text{ quadratischer Rest} \mod p \\ -1 & a \text{ quadratischer Nichtrest} \mod p \\ 0 & p|a \end{cases}$$

Lemma 12.9. *Sei a prim zu p. Dann gilt*

$$\left(\frac{a}{p}\right) = a^{(p-1)/2}$$

Die Abbildung

$$\mathbb{F}_p^* \to \{\pm 1\} \qquad a \mapsto \left(\frac{a}{p}\right)$$

ist ein Gruppenhomomorphismus. Das Legendre-Symobl ist multiplikativ.

Beweis: Wir nutzen den Isomorphismus $\mathbb{F}_p^* \cong \mathbb{Z}/2n\mathbb{Z}$ mit $n = (p-1)/2$. Der surjektive Gruppenhomomorphismus

$$\mathbb{Z}/2n\mathbb{Z} \xrightarrow{a \mapsto na} n\mathbb{Z}/2n\mathbb{Z} \cong \mathbb{Z}/2\mathbb{Z}$$

hat als Kern genau die geraden Zahlen. Diese entsprechen in $\mathbb{F}_p^*$ den Quadraten, also ist dies die Definition des Legendre-Symbols.

Aus der Formel sehen wir, dass wir einen Gruppenhomorphismus definiert haben. Die Fortsetzung auf $p|a$ ist ebenfalls multiplikativ: wenn ein Faktor durch p teilbar ist, dann auch das Produkt. □

Theorem 12.10 (Quadratisches Reziprozitätsgesetz)**.** *Seien p, q zwei ungerade Primzahlen. Dann gilt*

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$$

Dieser Satz erlaubt extrem effiziente Berechnung von Legendre-Symbolen.

Beispiel. Ist 7 ein quadratischer Rest modulo 17? Wir berechnen

$$\begin{aligned}\left(\frac{7}{17}\right) &= \left(\frac{17}{7}\right)(-1)^{8\cdot 3} = \left(\frac{3}{7}\right) \\ &= \left(\frac{7}{3}\right)(-1)^{3\cdot 1} = -\left(\frac{1}{3}\right) = -1\end{aligned}$$

Beweis: Wir interpretieren $G = \mathbb{F}_p^*$ als Galoisgruppe von $\mathbb{Q}(\zeta_p)/\mathbb{Q}$. Wir schreiben σ_q für das eindeutige Element $\zeta_p \mapsto \zeta_p^q$.

Die Untergruppe $H = \mathbb{F}_p^{*2}$ ist die eindeutige Untergruppe vom Index 2. Sei $F = \mathbb{Q}(\zeta_p)^H$. Da dies eine quadratische Erweiterung von $\mathbb{Q}$ ist, ist sie von der Form $\mathbb{Q}(\sqrt{D})$ für $D \in \mathbb{Q}$. Die Galoisgruppe von $\mathbb{Q}(\sqrt{D})/\mathbb{Q}$ ist dann G/H. Es ist also $\sigma_q \in H$ genau dann, wenn $\sigma_q(\sqrt{D}) = \sqrt{D}$. Tatsächlich sogar

$$\left(\frac{q}{p}\right) = \frac{\sigma_q(\sqrt{D})}{\sqrt{D}}$$

da die Elemente von G/H durch ihre Wirkung auf $\sqrt{D}$ eindeutig bestimmt sind. Daher ist es unsere erste Aufgabe, D zu bestimmen. Nach dem nächsten Lemma hat $D = (-1)^{\frac{p-1}{2}} p$ die Quadratwurzel

$$\alpha = \sum_{x \in \mathbb{F}_p^*} \left(\frac{x}{p}\right) \zeta_p^x \in \mathbb{Q}(\zeta_p).$$

Daher ist $F = \mathbb{Q}(\alpha)$.
Der Körperhomomorphismus σ_q respektiert den Ganzheitsring $\mathcal{O} = \mathbb{Z}[\zeta_p] \cong \mathbb{Z}[X]/\Phi_p(X)$ und das Ideal $q\mathcal{O}$. Er induziert induziert also einen Ringhomomorphismus

$$\overline{\sigma}_q : \mathcal{O}/q\mathcal{O} \to \mathcal{O}/q\mathcal{O}$$

Da wir nun in Charakteristik q sind, folgt

$$\overline{\sigma}_q(\overline{a}) = \overline{a}^q \text{ für alle } a \in \mathcal{O}/q\mathcal{O}$$

Insbesondere

$$\sigma_q(\alpha) = \left(\frac{q}{p}\right) \alpha = \alpha^q \mod q\mathcal{O}$$

In dieser Gleichung wollen wir durch α teilen. Wir verifizieren dafür, dass α invertierbar ist in $\mathcal{O}/q\mathcal{O}$. Wegen $\alpha^2 = \pm p$ genügt es, dass zu zeigen, dass p invertierbar ist. Dies gilt, da $\mathcal{O}/q\mathcal{O}$ eine $\mathbb{F}_q$-Algebra ist und p invertierbar in $\mathbb{F}_q$.
Hieraus folgt $\mod q\mathcal{O}$:

$$\left(\frac{q}{p}\right) = \alpha^{q-1} = (\alpha^2)^{\frac{q-1}{2}} = \left[(-1)^{\frac{p-1}{2}} p\right]^{\frac{q-1}{2}}$$
$$= (-1)^{\frac{p-1}{2}\frac{q-1}{2}} p^{\frac{q-1}{2}} \overset{12.9}{=} (-1)^{\frac{p-1}{2}\frac{q-1}{2}} \left(\frac{p}{q}\right)$$

Beide Seiten sind ± 1 und unterscheiden sich um ein Vielfaches von q. Dann sind sie bereits gleich. □

Lemma 12.11. *Sei ζ_p eine primitive p-te Einheitswurzel. Dann gilt für*

$$\alpha = \sum_{x \in \mathbb{F}_p^*} \left(\frac{x}{p}\right) \zeta_p^x$$

die Gleichung

$$\alpha^2 = (-1)^{\frac{p-1}{2}} p$$

Beweis:

$$\alpha^2 = \sum_{x,y \in \mathbb{F}_p^*} \left(\frac{xy}{p}\right) \zeta_p^{x+y}$$

Wir setzen $x = x'y$ und erhalten

$$\begin{aligned}\alpha^2 &= \sum_{x',y\in\mathbb{F}_p^*} \left(\frac{x'y^2}{p}\right) \zeta_p^{x'y+y} \\ &= \sum_{x'\in\mathbb{F}_p^*} \left(\frac{x'}{p}\right) \sum_{y\in\mathbb{F}_p^*} \zeta_p^{(x'+1)y}\end{aligned}$$

Für $x' = -1$ erhalten wir den Beitrag $\left(\frac{-1}{p}\right)(p-1)$. Für $x' \neq -1$ ist $\zeta_p^{x'+1}$ eine primitive p-te Einheitswurzel. Beim Summieren über die Potenzen erhalten wir -1, das das Minimalpolynom $X^{p-1} + X^{p-2} + \cdots + X + 1$ ist. Insgesamt also den Beitrag $-\left(\frac{x'}{p}\right)$. Es gilt also

$$\alpha^2 = \left(\frac{-1}{p}\right)(p-1) - \sum_{x'\in\mathbb{F}_p^*} \left(\frac{x'}{p}\right) + \left(\frac{-1}{p}\right)$$

Die mittlere Summe verschwindet, da das Legendre-Symobol genauso oft $+1$ wie -1 ist. □

Noch mächtiger wird das Reziprozitätsgesetz durch die beiden Ergänzungssätze.

Satz 12.12 (Ergänzungssätze)**.** *Sei q ungerade Primzahl. Dann gilt*

$$\begin{aligned}\left(\frac{-1}{q}\right) &= (-1)^{\frac{q-1}{2}} \\ \left(\frac{2}{q}\right) &= (-1)^{\frac{q^2-1}{8}}\end{aligned}$$

In der ersten Formel kommt es nur auf die Restklasse von p modulo 4 an, in der zweiten auf die Restklasse modulo 8.

Beweis: Die erste Formel ist ein Spezialfall von Lemma 12.9. Wir betrachten die zweite und wiederholen den Beweis des Reziprozitätsgesetzes. Sei ζ_8 primitive 8-te Einheitswurzel. Sie hat das Minimalpolynom $\Phi_8(X) = X^4 + 1$, also die Rechenregel $\zeta_8^4 = -1$. Dann gilt

$$\zeta_8 + \zeta_8^{-1} = \sqrt{2}$$

Wir betrachetn σ_q. Es gilt $\sigma_q(\sqrt{2}) = \varepsilon_q\sqrt{2}$ mit einem Vorzeichen ε_q. Durch elementare Rechnung mit $q \mod 8$ verifiziert man die Formel $\varepsilon_q = (-1)^{\frac{q^2-1}{8}}$: Die Werte für q sind $1, 3, 5, 7$. Man erhält in dieser Reihenfolge

$$(-1)^{\frac{q^2-1}{8}} = 1, -1, -1, 1.$$

Es gilt jeweils:

$$\varepsilon_q\zeta_8 + \varepsilon_q\zeta_8^{-1} = \zeta_8^q + \zeta_8^{-q}.$$

Offensichtlich ist $\varepsilon_1 = \varepsilon_7 = 1$. Für $q = 3$:

$$\zeta_8^3 + \zeta_8^{-3} = \zeta_8^{-1}\zeta_8^4 + \zeta_8\zeta_8^{-4} = -\zeta_8^{-1} - \zeta_8$$

also $\varepsilon_3 = -1$. Genauso für $q = 5$.
Anderseits gilt modulo $q\mathbb{Z}[\zeta_8]$

$$\varepsilon_q\sqrt{2} = \sigma_q(\sqrt{2}) = \sqrt{2}^q \Rightarrow \varepsilon_q = \sqrt{2}^{q-1} = 2^{\frac{q-1}{2}}$$

und mit Lemma 12.9 (sogar ganzzahlig)

$$\left(\frac{2}{q}\right) = \varepsilon_q$$

□

Bemerkung. Wir dehnen das Legendre-Symobl multiplikativ auf zum Jacobi-Symbol $\left(\frac{a}{b}\right)$ für b ungerade. Man verifiziert elementar, dass das Reziprozitätsgesetz und die Ergänzungsätze auch für das Jacobi-Symobol gelten.

Beispiel. Wir betrachten die Primzahlen 1231 und 1549.

$$\begin{aligned}
\left(\frac{1231}{1549}\right) &= \left(\frac{1549}{1231}\right)(-1)^{\frac{1548}{2}\frac{1230}{2}} = \left(\frac{318}{1231}\right) = \left(\frac{2}{1231}\right)\left(\frac{159}{1231}\right) \\
&= (-1)^{\frac{1231^2-1}{8}}\left(\frac{1231}{159}\right)(-1)^{\frac{1230}{2}\frac{158}{2}} = \left(\frac{118}{159}\right) = \left(\frac{2}{159}\right)\left(\frac{59}{159}\right) \\
&= (-1)^{\frac{159^2-1}{8}}\left(\frac{159}{59}\right)(-1)^{\frac{158}{2}\frac{58}{2}} = \left(\frac{41}{59}\right) \\
&= \left(\frac{59}{41}\right)(-1)^{\frac{58}{2}\frac{40}{2}} = \left(\frac{18}{41}\right) = \left(\frac{2}{41}\right)\left(\frac{3^2}{41}\right) \\
&= (-1)^{\frac{41^2-1}{8}} = +1
\end{aligned}$$

Bemerkung. Das Reziprozitätsgesetz wurde zuerst von Gauß bewiesen. Er war so begeistert, dass er immer wieder neue Beweise suchte – insgesamt 8. Unser Beweis ist der "richtige", da dies die Version ist, die sich auf das allgemeine Reziprozitätsgesetz für abelsche Erweiterungen von Zahlkörpern (endlich über $\mathbb{Q}$) verallgemeinert. Verallgemeinerungen auf den nicht-abelschen Fall sind Gegenstand aktueller Forschung, Stichwort Langlands-Programm.

Kapitel 13

Die Sylow-Sätze

Wir benutzen systematisch die Operation von G durch durch *Konjugation* auf sich selbst. Abgeleitet erhält man daraus auf der Menge der Untergruppen.

$$G \times G \to G \; ; (g,h) \mapsto ghg^{-1}$$

$$G \times \mathcal{U} \to \mathcal{U} \; ; (g,H) \mapsto gHg^{-1}$$

für die Menge $\mathcal{U}$ der Untergruppen von G. Auf beide Situationen wird die Bahnformel angewendet.

Definition 13.1. *Sei p eine Primzahl. Eine endliche Gruppe heißt p-Gruppe, falls die Ordnung von G eine Potenz von p ist.*

Bemerkung. Jede Untergruppe und jeder Quotient einer p-Gruppe ist ebenfalls eine p-Gruppe. Jedes direkte Produkt von p-Gruppen ist eine p-Gruppe.

Wir wollen zunächst die Struktur von p-Gruppen verstehen, dann die p-Gruppen, die in einer beliebigen endlichen Gruppe enthalten sind.

Korollar 13.2. *Sei G eine p-Gruppe. Dann ist das Zentrum $Z(G)$ ungleich $\{e\}$.*

Beweis: Sei $M = G$ mit Operation durch Konjugation. Wir verwenden die Formel des letzen Beispiels:

$$|M| = |M^G| + \text{Vielfaches von } p \; .$$

Dann ist $|M| = |G|$, also eine Potenz von p. Es gilt

$$M^G = \{h \in G \mid ghg^{-1} = g \text{ für alle } g \in G\} = Z(G) \; .$$

Also ist die Ordnung von $Z(G)$ ebenfalls durch p teilbar. Als Untergruppe enthält $Z(G)$ wenigstens ein Element, nämlich e. Also muss $Z(G)$ wenigstens p Elemente haben, jedenfalls mehr als eines. □

Man beachte, dass $Z(G)$ abelsch ist und ein Normalteiler von G.

Satz 13.3. *Sei $|G| = p^n$. Dann gibt es eine Kette von Normalteilern $N_i \triangleleft G$*

$$\{e\} = N_0 \subset N_1 \subset N_2 \subset \cdots \subset N_n = G$$

mit $|N_i| = p^i$ und $N_i/N_{i-1} \cong \mathbb{Z}/p$.

Bemerkung. I.a. gibt es *nicht* für jeden Teiler der Gruppenordnung eine Untergruppe!

Beweis: **Prinzip:** Sei G eine Gruppe, $N \triangleleft G$ und $\overline{N'} \triangleleft G/N$ ebenfalls ein Normalteiler. Dann ist $N' = \{g \in G \mid gN \in \overline{N'}\}$ ein Normalteiler von G (nämlich der Kern der Abbildung $G \to G/N \to (G/N)/\overline{N'}$, Satz 1.19). Es gilt

$$N'/N \cong \overline{N}' \text{ und } G/N' \cong (G/N)/\overline{N'}$$

(Satz 1.19 und 2. Isomorphiesatz 1.21).
Dieses Prinzip erlaubt es, den Satz mit Induktion über die Gruppenordnung zu beweisen. Sei G eine p-Gruppe. Das Korollar liefert einen nichttrivialen Normalteiler $Z(G)$. Ist $Z(G) \neq G$ sind wir nach Induktionsvoraussetzung fertig. Ist $Z(G) = G$, so ist insbesondere G abelsch.
Sei $g \in G$ ein Element ungleich $\{e\}$. Sei $N = \langle g \rangle$ die von g erzeugte Untergruppe. Ist N echt kleiner als G, so schließen wir wieder mit vollständiger Induktion.
Übrig bleibt der Fall $G = \langle g \rangle$ zyklisch, also $G \cong \mathbb{Z}/p^n\mathbb{Z}$. In diesem Fall können wir die Kette direkt angeben, nämlich

$$N_i = p^{n-i}\mathbb{Z}/p^n\mathbb{Z} \ .$$

□

Beispiel.

$$\mathbb{Z}/p^2\mathbb{Z} \supset p\mathbb{Z}/p^2\mathbb{Z} \supset \{(0,0)\}$$

oder

$$\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z} \supset \mathbb{Z}/p\mathbb{Z} \times \{0\} \supset \{(0,0)\} \ .$$

Definition 13.4. *Sei G eine endliche Gruppe. Sei p eine Primzahl, $|G| = p^r m$, wobei m teilerfremd zu p ist. Eine Untergruppe $H \subset G$ heißt p-Sylowgruppe von G, falls $|H| = p^r$.*

Theorem 13.5 (Erster Sylowsatz)**.** *Sei G endliche Gruppe, p eine Primzahl. Dann gibt es eine p-Sylowgruppe.*

Bemerkung. Damit existieren auch Untergruppen der Ordnung p^i mir $i \leq r$ (mit r wie in der Definition).

Korollar 13.6. *Sei G eine endliche Gruppe und p ein Primteiler der Gruppenordnung. Dann enthält G ein Element der Ordnung p.*

Beweis: Aus dem ersten Sylowsatz: Es gibt eine p-Sylowgruppe, also auch eine Untergruppe der Ordnung p. Diese ist zyklisch, der Erzeuger ist das gesuchte Element. □

Bemerkung. Wir haben das Korollar bereits direkt bewiesen als Lemma **??**.

Beweis des ersten Sylowsatzes. Wir wollen wieder die Operation von G auf sich ausnutzen. Es gilt wie schon im Fall der p-Gruppen

$$p^r m = |G| = |Z(G)| + \sum_{i_1}^{n} [G : G_{x_i}]$$

wobei x_i ein geeigenetes System von Elementen ist, nämlich Vertreter der Bahnen, die keine Fixpunkte sind. Zunächst kann man hier mit Teilbarkeitsargumenten nichts machen. Aber:

Beweis durch vollständige Induktion nach der Gruppenordnung $n = p^r m$, Indirekter Beweis im Induktionsschritt. Angenommen G hat keine p-Sylowgruppe. Dann hat G auch keine Untergruppe der Ordnung $n' = p^r m'$ mit $m' < m$ (denn die hätte nach Induktionsvorausetzung eine Untergruppe der Ordnung p^r.) Wegen

$$p^r m = |H|[G : H]$$

teilt also p den Index $[G : H]$ jeder echten Untergruppe von G. Nun ist die obige Formel sehr hilfreich, nämlich $p^r m = |Z(G)| +$ Vielfaches von p. Es folgt $p \mid Z(G)$. Nach dem Korollar, das wir ja für abelsche Gruppen direkt bewiesen haben, hat $Z(G)$ ein Element a der Ordnung p. Da a im Zentrum liegt, ist $\langle a \rangle$ ein Normalteiler von G. Es gilt $|G/\langle a \rangle| = p^{r-1} m$. Nach Induktionsvoraussetzung hat $G/\langle a \rangle$ eine p-Sylowgruppe $\overline{H}$. Sei

$$H = \{g \in G \mid \overline{g} = g\langle a \rangle \in \overline{H}\}$$

Die Projektion $H \to \overline{H}$ ist surjektiv mit Kern $\langle a \rangle$. Es gilt also

$$|H| = |\overline{H}| \cdot |\langle a \rangle| = p^{r-1} p \ .$$

□

Bemerkung. Der Beweis ist überhaupt nicht konstruktiv!

Theorem 13.7 (Zweiter und dritter Sylowsatz)**.** *Sei G eine endliche Gruppe.*

(i) Sei $H \subset G$ eine p-Gruppe. Dann ist H in einer p-Sylowgruppe enthalten.

(ii) Je zwei p-Sylowgruppen sind konjugiert, insbesondere isomorph.

(iii) Die Anzahl der p-Sylowgruppen teilt $|G|$ und ist kongruent zu 1 molulo p.

Proof. Sei S die Menge der p-Sylowgruppen von G. Wir betrachten die Operation von G auf S durch Konjugation.

$$G \times S \to S \; ; (g, P) \mapsto gPg^{-1} \; .$$

Sie ist wohldefiniert, denn $|gPg^{-1}| = |P|$, also ist dies wieder eine p-Sylowgruppe. Wir bestimmen die Standgruppe:

$$G_P = \{g \in G \mid gPg^{-1} = P\} \supset P$$

Also ist $[G : G_P]$ ein Teiler von $[G : P]$, also teilerfremd zu p. Sei $T = G \cdot P$ die Bahn von P bezüglich der Operation. Es gilt

$$|T| = [G : G_P] \qquad \text{nach Lemma 3.9}$$

also teilerfremd zu p.
Sei nun H eine p-Gruppe der Ordnung größer 1. Wir schränken die Operation ein

$$H \times T \to T$$

Nach dem Beispiel zur Bahnformel 3.10 gilt

$$|T| = |T^H| + \text{ Vielfaches von } p \; .$$

Da p teilerfremd zu $|T|$ ist, folgt $T^H \neq \emptyset$. Also: es gibt $P_1 \in T \subset S$ eine p-Sylowgruppe, so dass

$$hP_1h^{-1} = P_1 \text{ für alle } h \in H \; .$$

Nach dem ersten Isomorphisatz 1.20 folgt

$$HP_1/P_1 \cong H/H \cap P_1$$

Dies ist eine p-Gruppe. P_1 ist nach Voraussetzung eine p-Gruppe, also nun auch HP_1. Es gilt $P_1 \subset HP_1$ und P_1 ist eine p-Sylowgruppe, also folgt $P_1 = HP_1 \Rightarrow H \subset P_1$.
Damit haben wir die erste Behauptung gezeigt. Wenn wir das Ergebnis an auf eine p-Sylowgruppe H an, so haben wir $H \subset P_1$, also $H = P_1 \in T$. Dies ist die zweite Behauptung. Damit ist $S = T$, die Operation von G auf S ist transitiv.
Die Anzahlformel ist für die transitive Operation von G auf S ergibt $|S| = [G : G_P]$. Dies ist ein Teiler von $|G|$. Die Bahnformel für die Operation von $H = P$ auf $S = T$

$$|S| = |S^P| + \text{Vielfaches von } p \; .$$

Dabei ist $S^P = \{P\}$, da wir $H \subset P_1$ für alle $P_1 \in S^P$ gezeigt haben. □

Bemerkung. Es gibt genau eine p-Sylowgruppe $\Leftrightarrow$ Sie ist ein Normalteiler.

Beispiel. (i) Sei G eine Gruppe der Ordnung 15. Wir betrachten die Anzahl der 5-Sylowgruppen. Sie liegt in

$$\{1, 3, 5, 15\} \cap \{1, 6, 11, 16\} \ .$$

Also gibt es einen Normalteiler N_5 der Ordnung 5. Die Anzahl der 3-Sylowgruppen liegt in

$$\{1, 3, 5, 15\} \cap \{1, 4, 7, 10, 13\}$$

Also gibt es einen Normalteiler N_3 der Ordnung 3. Wir betrachten

$$G \to G/N_3 \times G/N_5 \ .$$

Die Abbildung ist injektiv, denn der Kern ist $N_3 \cap N_5$, also teilt seine Ordnung 3 und 5. Die Abbildung ist auch surjektiv, denn $|G| = 15 = 5 \cdot 3 = |G/N_3| \cdot |G/N_5|$. Wir haben gezeigt: Es gibt nur eine Gruppe der Ordnung 15, nämlich $\mathbb{Z}/15$.

(ii) Jede Gruppe der Ordnung 30 hat einen echten Normalteiler, d.h. sie ist nicht einfach: Die Teiler von 30 sind $1, 2, 3, 5, 6, 10, 15, 30$. Man bestimmt die Anzahl der 5-Sylowgruppen. Sie ist 1 oder 6. Im ersten Fall haben wir unseren Normalteiler gefunden. Im anderen Fall bestimmen wir die Anzahl der Elemente der Ordnung 5: In jeder Untergruppe der Ordnung 5 sind es 4. Der Schnitt von je zweien der Untergruppen ist eine Untergruppe, besteht also nur aus e. Damit gibt es insgesamt $6 \cdot 4 = 24$ Elemente der Ordnung 5. Nun betrachten wir die Anzahl der 3-Sylowgruppen. Es sind 1 oder 10. Ist es eins, so haben wir einen Normalteiler. Andernfalls gibt es $10 \cdot 2 = 20$ Elemente der Ordnung 3. Damit hätte G wenigstens $20 + 24$ Elemente statt 30.

Anwendungen in der Galoistheorie

Korollar 13.8 (Fundamentalsatz der Algebra)**.** $\mathbb{C}$ *ist algebraisch abgeschlossen.*

Beweis: Wir verwenden:

(i) Sei $P \in \mathbb{R}[X]$ ungerade, dann hat P eine reelle Nullstelle. (Zwischenwertsatz)

(ii) Sei $P \in \mathbb{C}[X]$ quadratisch, dann zerfällt P in Linearfaktoren. (Lösungsformel).

Sei nun $L/\mathbb{C}$ endlich.

Behauptung. $L = \mathbb{C}$.

Ohne Einschränkung ist $L/\mathbb{R}$ galois (normale Hülle). Sei $G = \mathrm{Gal}(L/\mathbb{R})$, P eine 2-Sylowgruppe von G, $F = L^P$. Nach dem Hauptsatz der Galoistheorie ist $[F : \mathbb{R}] = [G : P]$, also ungerade. Sei $\alpha \in F$. Sein Minimalpolynom ist irreduzibel und ungerade, nach (i) also linear. Damit ist $F = \mathbb{R}$. Dann ist auch $G' = \mathrm{Gal}(L/\mathbb{C}) \subset \mathrm{Gal}(L/\mathbb{R})$ eine 2-Gruppe. Falls G' nicht-trivial, so enthält sie eine Untergruppe mit Index 2. Ihr Fixkörper $L^{G'}$ ist eine quadratische Erweiterung von $\mathbb{C}$. Nach (ii) gibt es so etwas aber nicht. Daher ist $L = \mathbb{C}$. □

Zirkel und Lineal

Korollar 13.9. *Eine Zahl $z \in \mathbb{C}$ ist mit Zirkel und Linear aus $0, 1$ konstruierbar, genau dann wenn es in einer Galoiserweiterung $K/\mathbb{Q}$ enthalten ist mit $[K : \mathbb{Q}]$ eine Potenz von 2.*

Beweis: Wir haben bereits gesehen (Theorem 6.3), dass z konstruierbar ist, genau dann wenn es in einem Körper K_n liegt, für den es eine Kette quadratischer Erweiterungen gibt

$$\mathbb{Q} = K_0 \subset K_1 \subset K_2 \cdots \subset K_n \ .$$

Sei nun K wie im Korollar. Dann ist die Galoisgruppe $G = \mathrm{Gal}(K/\mathbb{Q})$ eine 2-Gruppe. Nach dem Struktursatz für 2-Gruppen gibt es eine Kette von Normalteilern N_i mit Index 2^i. Deren Fixkörper sind die gesuchte Kette von Zwischenkörpern.

Umgekehrt existiere die Körperkette. Offensichtlich ist $[K_n : \mathbb{Q}] = 2^n$. Wenn $K_n/\mathbb{Q}$ normal ist, so sind wir fertig. Im allgemeinen Fall gehen wir ie im Beweis von Theorem 11.7 vor und finden eine Kette von Körpern L_i mit $L_i/\mathbb{Q}$ normal, $K_i \subset L_i$ und L_i entsteht aus L_{i-1} durch Adjungieren von Quadratwurzeln. Dann ist $K = L_n$ die gesuchte Galoiserweiterung. □

Inhaltsverzeichnis

0 Einleitung **1**

1 Grundbegriffe der Gruppentheorie **5**

2 Wichtige Beispiele von Gruppen **17**

3 Operationen von Gruppen auf Mengen **29**

4 Grundbegriffe der Ringtheorie **35**

5 Grundbegriffe der Körpertheorie **49**

6 Konstruktion mit Zirkel und Lineal **57**

7 Exkurs: Aufbau der Zahlbereiche **63**

8 Körperhomomorphismen **69**

9 Beispiele für Galoisgruppen **75**

10 Norm. und sep. Körpererweiterungen **81**

11 Hauptsatz der Galoistheorie **89**

12 Zyklotom. Körper u. quadrat. Reziprozität **95**

13 Die Sylow-Sätze **105**