Algebra I
Wintersemester 2006/07

Prof. Dr. Annette Huber-Klawitter

Fassung vom 31. Januar 2007

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

Math. Institut
Augustusplatz 10/11
04109 Leipzig

0341-97 32 185
huber@mathematik.uni-leipzig.de

Kapitel 0

Einleitung

Die Vorlesung lineare Algebra:

- Eine Menge Vokabeln (Vektorraum, lineare Abbildung, Skalarprodukt,...)
- Die wichtigsten Werkzeuge der Mathematik - so wie Hammer und Schraubenzieher für den Schreiner.

Dieses Semester:

- noch mehr Vokabeln und noch mehr Werkzeuge.
- aber vor allem: wir werden die Werkzeuge benutzen, um eine Reihe sehr alter und sehr tiefer Probleme zu lösen!

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 Gleichungen 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.
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):

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

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!
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. □

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.
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 die unmöglich, wohl aber für gewisse wie z.B. $n = 17$.*

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! (Lindemann 1882: π ist transzendent).
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.

Plan der Vorlesung:

- algebraische Grundbegriffe (Gruppe, Ring, Körper)
- 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*

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

- Strukturtheorie von endlichen Gruppen bis zu den Sylowsätzen
- 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).

oder jedes andere deutschsprachige Lehrbuch mit dem Titel Algebra.
Meine Hauptquelle: Skript der Fernuni Hagen von Prof. Scharlau.

Kapitel 1

Grundstrukturen

Gruppen

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.

Noch ein wichtiges Beispiel:

Definition 1.3. *Sei n eine natürliche Zahl. Zwei ganze Zahlen a und b heißen* kongruent modulo *n, wenn ihre Differenz durch n teilbar ist. Wir schreiben a* mod *n (oft auch $a(n)$) für die Äquivalenzklasse von a. Die Menge der Restklassen modulo n wird mit C_n bezeichnet, die Restklassengruppe modulo n*

C_n hat n Elemente, vertreten durch die Zahlen $0, 1, \ldots, n-1$.

Lemma 1.4. *Seien $\overline{a}$, $\overline{b}$ Restklassen modulo n, $a \in \overline{a}$ und $b \in \overline{b}$ Repräsentanten. Dann wird C_n mit der Verknüpfung*

$$\overline{a} + \overline{b} = a + b \mod n, \overline{a}\overline{b} = ab \mod n$$

zu einer abelschen Gruppe.

Beweis: Alle Axiome folgen aus den entsprechenden Axiomen für $\mathbb{Z}$. Z.B.

$$\overline{a} + (\overline{b} + \overline{c}) = a + (b + c) \mod n = (a + b) + c \mod n = (\overline{a} + \overline{b}) + \overline{c}$$

Das Problem liegt woanders: Sind die Verknüpfungen wohldefiniert? Seien a, a', b, b' Zahlen mit $a = a' \mod n$, $b = b' \mod n$, d.h. n teilt $a' - a$ und $b' - b$. Es gilt

$$a' + b' = a + b \mod n$$

denn $a' + b' - a - b = (a' - a) + (b' - b)$ ist durch n teilbar. □

Definition 1.5. *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 Gruppenhomomorphismus heißt Isomorphismus*, wenn er bijektiv ist. Ein Isomorphismus* $f : G \to G$ *heißt* Automorphismus*.*

Ist f ein Gruppenhomomorphismus, so gilt automatisch $f(e_G) = e_H$ und $f(g^{-1}) = f(g)^{-1}$.

Beweis: Es gilt

$$f(e_G) = f(e_G e_G) = f(e_G)f(e_G)$$

Multiplikation mit $f(e_G)^{-1}$ ergibt dann

$$e_H = f(e_G)^{-1}f(e_G) = f(e_G)^{-1}(f(e_G)f(e_G)) = e_H f(e_G) = f(e_G)$$

Weiterhin gilt

$$f(g^{-1})f(g) = f(g^{-1}g) = f(e_G) = e_H$$

Wegen der Eindeutigkeit des Inversen ist dann auch $f(g^{-1}) = f(g)^{-1}$. □

Lemma 1.6. *Ein Gruppenhomomorphismus* $f : G \to H$ *ist injektiv genau dann, wenn der Kern nur aus* $\{e_G\}$ *besteht.*

Beweis: Wenn die Abbildung injektiv ist, dann besteht das Urbild von e_H (nach Definition der Kern) nur aus einem Element. Da es e_G enthält, muss er also gleich $\{e_G\}$ sein. Sei umgekehrt der Kern trivial. Seien $g, g' \in G$ mit $f(g) = f(g') \Leftrightarrow f(g)^{-1}f(g') = e_H$. Dann gilt

$$f(g^{-1}g') = f(g^{-1})f(g') = f(g)^{-1}f(g') = e_H$$

also $g^{-1}g' \in \mathrm{Ker}\, f = \{e_G\}$. Hierausfolgt $g^{-1}g' = e_G \Leftrightarrow g = g'$. Die Abbildung ist injektiv. □

Sie kennen diesen Beweis bereits von linearen Abbildungen.
Wir werden uns später noch viel ausführlicher mit Gruppen, vor allem endlichen Gruppen beschäftigen. Jetzt geht es uns aber um Ringe und Körper.

Ringe

Definition 1.7. *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 $a, b \in A$. 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).

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 1.8. *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.

Ab jetzt: Alle Ringe kommutativ mit Eins, $1 \neq 0$!

Definition 1.9. *Ein* Ringhomomorphismus *(genauer: Homomorphismus von Ringen mit Eins) $f : A \to B$ ist eine Abbildung mit*

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

und $f(1) = 1$.

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.

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

Lemma 1.10. *Sei n eine natürliche Zahl. Dann wird die Menge der Restklassen modulo n mit der von $\mathbb{Z}$ induzierten Addition und Multiplikation zu einem kommutativen Ring mit 1. Er wird mit $\mathbb{Z}/n\mathbb{Z}$ bezeichnet.*

Beweis: Nach Lemma 1.4 ist die Addition wohldefiniert und die Gruppenaxiome sind erfüllt. Nun geht es um die Wohldefiniertheit der Multiplikation. Sei $a = a' \mod n$, $b = b' \mod n$, also $n \mid a' - a, b' - b$. Dann gilt $a'b' = ab \mod n$, denn

$$a'b' - ab = a'b' - a'b + a'b - ab = a'(b' - b) + (a' - a)b$$

ist durch n teilbar. □

Beispiel. Die Restklassenabbildung

$$\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z} \qquad a \mapsto a \mod n$$

ist ein Ringhomomorphismus. Seien $n \mid N$. Dann ist die natürliche Abbildung

$$\mathbb{Z}/N\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}, \qquad a \mod N \mapsto a \mod n$$

ein Ringhomomorphismus.

Beweis: Die Eigenschaften sind offensichtlich erfüllt. Im zweiten Fall muss aber die Wohldefiniertheit überprüft werden: Aus $a = a' \mod N$ folgt tatsächlich $a = a' \mod n$, wenn $n \mid N$. □

Da wir gerade dabei sind:

Satz 1.11 (Chinesischer Restsatz). *Seien n, m teilerfremde natürliche Zahlen. Dann ist die natürliche Abbildung*

$$\mathbb{Z}/nm\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$$

ein Ringisomorphismus, wenn Addition und Multiplikation auf $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ komponentenweise definiert sind.

Beweis: Beide Ringe haben gleichviele Elemente, nämlich nm. Es genügt daher, die Injektivität zu zeigen.
Aus dem vorherigen Beispiel folgt, dass die natürliche Abbildung ein Ringhomomorphismus ist. Wir bestimmen den Kern. Sei $a \in \mathbb{Z}$ mit $a = 0 \mod n$ und $a = 0 \mod m$, d.h. $n \mid a$ und $m \mid a$. Da n und m teilerfremd sind, folgt auch $nm \mid a$, also $a = 0 \mod nm$. □

Bemerkung. Dieser scheinbar einfache Beweis benutzt Eigenschaften von $\mathbb{Z}$, die keineswegs auf der Hand liegen! Warum gilt eigentlich der Satz von der Eindeutigkeit der Primfaktorzerlegung?

Definition 1.12. *Eine Teilmenge $I \subset A$ heißt* Ideal*, wenn I eine Untergruppe von A ist und*

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

Ein Ideal ungleich A heißt echtes Ideal*.*

Beispiel. Sei $a \in A$. Dann ist die Menge

$$(a) = \{ba \mid b \in A\}$$

ein Ideal, das von a erzeugte *Hauptideal*. Man schreibt auch Aa oder aA.

Beispiel. Sei K ein Körper, $I \subset K$ ein Ideal. Dann gilt $I = 0$ oder $I = K$: Sei $a \neq 0$ ein Element von I, $b \in K$ beliebig. Da $a \neq 0$ gibt es ein multiplikatives Inverses a^{-1} von a in K. Dann gilt

$$b = (ba^{-1})a \in I$$

denn I ist ein Ideal, d.h. $K \subset I$.

Lemma 1.13. *Sei $f : A \to B$ ein Ringhomomorphismus. Dann ist*

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

ein echtes Ideal.

Beweis: Seien $a, \in A$, $k, k' \in \operatorname{Ker} f$. Dann gilt

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

Wegen $f(1) = 1$ und $1 \neq 0$ liegt 1 nicht im Kern, also $\operatorname{Ker} f \neq A$. □

Definition 1.14. *Sei $I \subset A$ ein Ideal. Dann heißen die Teilmengen $a + I = \{a + u \mid u \in I\}$ Nebenklassen von I. Die Menge der Nebenklassen wird mit A/I bezeichnet.*

Lemma 1.15. *Sei $I \subset A$ ein Ideal, $a, b \in A$. Äquivalent sind:*

(i) $a \in b + I$

(ii) $b \in a + I$

(iii) $a - b \in I$

(iv) $a + I = b + I$

Beweis: $a \in b + I$ ist Äquivalenz zur Existenz eines $u \in I$ mit $a = b + u \Leftrightarrow a - b = u \in I$. Ebenso für b.
Wegen $a + 0 \in a + I$ folgt aus (i) die Inklusion $a + I \subset b + I$, aus (ii) dann die umgekehrte. □

Bemerkung. Für ganze Zahlen gilt also $x = y \mod n$ genau dann, wenn $x + (n) = y + (n)$.

Satz 1.16. *(i) Sei $I \subset A$ ein echtes Ideal. Dann ist A/I ein Ring mit der Addition und Multiplikation*

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

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

(ii) 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 mit $\operatorname{Im}(f) = \operatorname{Im}(\overline{f})$.

Beispiel. Es gilt $\mathbb{Z}/n\mathbb{Z} = \mathbb{Z}/(n)$.

Beweis: Zu (i): Wie im Fall $\mathbb{Z}/(n)$ folgen alle Axiome aus den Axiomen für A. Zu überprüfen ist die *Wohldefiniertheit der Verknüpfungen*. Auch dies geht genau wie im Spezialfall.

Behauptung. *Addition und Multiplikation sind wohldefiniert.*

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

$$(a' + b) - (a + b) = u \in I$$
$$a'b - ab = (a + u)b - ab = ub \in I$$

da I ein Ideal. Damit gilt nach Lemma 1.15 $a + b + I = a' + b + I$ und $ab + I = a'b + I$.
Zu (ii): Sei $f : A \to B$ ein Ringhomomorphismus, $I = \operatorname{Ker} f$. Wir setzen

$$\overline{f}(a + I) = f(a) \text{ für alle } a \in A$$

Dies ist die einzige Möglichkeit, die angegebene Faktorisierung zu erhalten.

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

Sei $a + I = a' + I$, also $u = a - a' \in \operatorname{Ker} f$. Dann gilt

$$f(a) - f(a') = f(a - a') = f(u) = 0 \Leftrightarrow f(a) = f(a')$$

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

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

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

Die Rechnung für die Addition ist noch einfacher.

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

$\overline{f}$ ist ein Gruppenhomomorphismus, also müssen wir nur den Kern bestimmen. Sei $a + I \in \operatorname{Ker} \overline{f}$. Nach Definition gilt also $a \in \operatorname{Ker} f = I$. Nach Lemma 1.15 folgt $a + I = 0 + I$. □

Der entsprechende Satz für Vektorräume - mit demselben Beweis - wurde in der linearen Algebra gezeigt.

Bemerkung. Ist A eine k-Algebra und I ein Ideal und Untervektorraum, so ist A/I sogar eine k-Algebra.

Bemerkung. Für nichtkommutative Ringe liegen die Dinge etwas komplizierter.

Körper

Definition 1.17. *Ein* Körper *ist ein Ring K (kommutativ mit Eins, $0 \neq 1$), in dem $K \setminus \{0\}$ eine Gruppe ist bezüglich der Multiplikation. Ein* Körperhomomorphismus *ist eine Abbildung*

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

die ein Ringhomomorphismus zwischen zwei Körpern ist. Ein Körperisomorphismus *ist ein bijektiver Körperhomomorphismus. Ein* Körperautomorphismus *ist ein Körperisomorphismus $\alpha : K \to K$.*

Auf englisch heißt Körper "field´´, daher wird oft auch der Buchstabe F benutzt.

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

(ii) $\mathbb{F}_2, \mathbb{F}_3$.

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

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

Lemma 1.18. *Sei p ein Primzahl. Dann ist $\mathbb{Z}/p\mathbb{Z}$ ein Körper. Wir schreiben $\mathbb{F}_p$.*

Beweis: Einziges Problem ist die Existenz von Inversen bezüglich der Multiplikation. Sei $\overline{a} \in \mathbb{F}_p \setminus \{0\}$. Wir betrachten die Abbildung

$$A : \mathbb{F}_p \to \mathbb{F}_p \qquad \overline{x} \mapsto \overline{ax}$$

Behauptung. *Diese Abbildung ist injektiv.*

A ist ein Gruppenhomomorphismus ($\overline{a}(\overline{x}+\overline{y}) = \overline{ax}+\overline{ay}$), daher genügt es, den Kern zu betrachten. Sei daher $\overline{ax} = 0$ in $\mathbb{F}_p$. Sei a ein Repräsentant von $\overline{a}$, x einer von $\overline{x}$. Nach Voraussetzung gilt $ax = 0 \mod p$, also $p \mod ax$. Da p ein Primzahl ist, folgt $p \mid a$ oder $p \mid x$. Im ersten Fall wäre $a = 0 \mod p$, ein Widerspruch zur Voraussetzung. Also folgt $p \mid x$ bzw. $x = 0 \mod p$. Damit ist der Kern trivial und die Abildung injektiv.
Da $\mathbb{F}_p$ nur endlich viele Elemente hat, ist die Abbildung A dann auch surjektiv, d.h. für alle $\overline{y} \in \mathbb{F}_p$ gibt es ein $\overline{x}$ mit $\overline{ax} = \overline{y}$. Insbesondere gilt dies auch für $\overline{y} = 1 \mod p$. □

Satz 1.19. *Alle Körperhomomorphismen sind injektiv.*

Beweis: Sei $x \in K \setminus \{0\}$ mit $\alpha(x) = 0$. Es folgt

$$\alpha(x^{-1}x) = \alpha(x^{-1})\alpha(x) = 0 \ .$$

Aber $\alpha(1) = 0$ ist nicht erlaubt. □

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

Definition 1.20. *Sei L ein Körper, $K \subset$ 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 ist eine* Körpererweiterung.

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

Damit kommen wir zum zentralen Begriff dieser Vorlesung:

Definition 1.21. *Ein Element $a \in L$ heißt* algebraisch *über K, falls es ein Polynom $0 \neq P \in K[X]$ gibt mit $P(a) = 0$. Wir sagen: a erfüllt die algebraische Gleichung P. Andernfalls heißt a* transzendent. *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 $\mathbb{F}_p$.

(iv) e und π sind nicht algebraisch über $\mathbb{Q}$. (ohne Beweis)

Frage: Seien $a, b \in L/K$ algebraisch. Ist $a+b, ab$ algebraisch? Zur Beantwortung dieser Frage holen wir ein wenig aus.

Definition 1.22. *Ein Ideal $m \subset A$ heißt* maximal*, wenn $m \neq A$, und das einzige echt größere Ideal ist der ganze Ring A.*

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

Satz 1.23. *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

$$aA + m = \{ax + u \mid x \in A, u \in m\} \subset A.$$

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. Wir werden zeigen, dass $I = A$ oder $I = m$. Dafür betrachten wir $\phi : A \to A/m$.

Behauptung. *Das Bild $\phi(I)$ ist ein Ideal von A/m.*

Sei $u \in I$, $a \in A$. Dann gilt

$$(a + m)(u + m) = au + m \in \phi(I)$$

da $au \in I$. Die Eigenschaft bezüglich der Addition folgt genauso.
Nach Beispiel 1 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 $I = \phi^{-1}(A/m) = A$. □

Kapitel 2

Polynomringe

Sei von nun an k ein Körper. Wir studieren nun den Polynomring $k[X]$. Allgemeiner:

Definition 2.1. *Sei S eine Menge. Der Polynomring über S ist der Polynomring in den Unbestimmten $\{X_s \mid s \in S\}$, d.h. die Menge der endlichen formalen Linearkombinationen der Monome $X_{s_1}^{n_1} X_{s_2}^{n_2} \dots X_{s_k}^{n_k}$ mit $k \in \mathbb{N}_0, s_i \in S, n_i \in \mathbb{N}$ mit der offensichtlichen Addition und kommutativen Multiplikation. Formal: Sei V der k-Vektorraumraum mit Basis S, $k[S] = \mathrm{Sym}(V)$ die symmetrische Algebra über V. Wir schreiben X_s für das Bild des Basisvektors zu s unter der natürlichen Abbildung $V \to \mathrm{Sym}(V)$.*

Zur Erinnerung: Ist A ein Ring, $a \in A$, so heißt $Aa = (a)$ das von a erzeugte Hauptideal.

Satz 2.2. *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 $P \in k[X]$.*

Beispiel. $k[X,Y] = \{\sum_{i,j=0}^{n} a_{ij} X^i Y^j \mid n \in \mathbb{N}, a_{ij} \in k\}$ 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). Dies führt in die algebraische Zahlentheorie.

Die wesentliche Schritte des Beweises kennen Sie bereits aus der linearen Algebra, wir behandeleln es aber nocheinmal ausführlich. Dieselben Argumente funktionieren übrigens auch für $\mathbb{Z}$.

Definition 2.3. *Sei $P = a_0 + \dots + a_n X^n$ 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 2.4 (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.

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

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

Beweis von Satz 2.2. Sei $I \subset k[X]$ ein Ideal. Falls $I = 0$, 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. □

Definition 2.5. *Ein Polynom heißt* normiert*, falls der höchste Koeffizient* 1 *ist, also*

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

Bemerkung. Der Erzeuger Q eines Ideals I ist eindeutig bestimmt, wenn man verlangt, dass er normiert ist. Er ist das eindeutig bestimmte normierte Element von minimalem Grad in I (Ausnahme $I = 0$).
Offensichtlich übersetzen sich Enhaltenseinsrelationen für Ideale in Teilbarkeitseigenschaften von Erzeugern.

Lemma 2.6. *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 2.7. *Ein Polynom $P \in k[X]$ mit* $\deg P > 0$ *heißt* irreduzibel*, falls P nicht von der Form $P = P_1 P_2$ mit* $\deg P_1, \deg P_2 > 0$ *ist.*

Korollar 2.8. *Sei $P \in k[X]$. Der Ring $k[X]/(P)$ ist genau dann ein Körper, wenn P ein irreduzibles Polynom ist.*

Beweis: Wir müssen zeigen, dass (P) ein maximales Ideal ist. Wegen $\deg P > 0$ ist $(P) \neq k[X]$. Sei $(P) \subset J \subset k[X]$ ein Ideal, also $J = (Q)$. Dies bedeutet, dass Q ein Teiler von P ist. Also: (P) maximal $\Leftrightarrow$ P hat keine echten Teiler. □

Damit haben wir eine sehr wichtige Erkenntnis gewonnen:

Korollar 2.9. *Sei $P \in k[X]$ ein nichtkonstantes Polynom. Dann gibt es eine Körpererweiterung L von k, so dass P in L eine Nullstelle hat.*

Beweis: Sei Q ein irreduzibler Faktor von P. Wir setzen $L = k[Y]/(Q)$. Nach Korollar 2.8 ist dies ein Körper. Die natürliche Abbildung $k \to k[Y] \to k[Y]/(Q) = X$ ist ein Ringhomomorphismus, also ein Körperhomomorphismus und identifiziert k mit einem Teilkörper von L.

Behauptung. *Die Nebenklasse $\overline{Y} = Y + (Q)$ ist Nullstelle von Q.*

Sei $Q = a_n X^n + \cdots + a_0$ mit $a_n \neq 0$. Dann gilt

$$Q(\overline{Y}) = a_n(Y + (Q))^n + \cdots + a_0 = a_n Y^n + \cdots + a_n + (Q) = Q + (Q) = 0 + (Q)$$

Dann ist $\overline{Y}$ auch Nullstelle von P, wie behauptet. □

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

Lemma 2.10. *Sei P irreduzibel. Dann ist P* prim*, d.h. wenn ein Produkt $Q_1 \dots Q_n$ durch P teilbar ist, dann auch einer der Faktoren.*

Beweis: Es genügt den Fall $n = 2$ zu betrachten. Angenommen, P teilt weder Q_1 noch Q_2. Wir betrachten das Ideal

$$I_1 := (P, Q_1) = k[X]P + k[X]Q_1 = (S_1) \ ,$$

denn alle Ideal sind Hauptideale nach 2.2. S_1 ist ein Teiler des irreduziblen Polynoms P, also ist S_1 konstant oder $S_1 = P$. Der zweite Fall scheidet aus, da P kein Teiler von Q_1 ist. Also ist S_1 konstant, ohne Einschränkung $S_1 = 1$. Analog folgt

$$I_2 := (P, Q_2) = (1) \ .$$

Konkret:

$$1 = A_i P + B_i Q_i$$

mit $A_i, B_i \in k[X]$. Multiplikation liefert

$$1 = A_1 A_2 P^2 + A_1 P B_2 Q_2 + A_2 P B_1 Q_1 + B_1 B_2 Q_1 Q_2 \ .$$

Mit $Q_1 Q_2 = P$ ist demnach P ein Teiler von 1, ein Widerspruch. □

Theorem 2.11 (Primfaktorzerlegung). *Jedes Polynom $P \neq 0$ kann eindeutig (bis auf Reihenfolge) in der Form*

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

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

Beweis: Existenz ist klar. 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 P_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. □

Bemerkung. Man beachte die Anlalogie zu $\mathbb{Z}$: die normierten irreduziblen Polynome entsprechen den (positiven) Primzahlen, die Elemente von $k \setminus 0$ entsprechen ± 1. Dies mach übrigens deutlich, warum 1 *keine* Primzahl ist! Der Beweis der Eindeutigkeit der Primfaktorzerlegung in $\mathbb{Z}$ ist analog zum obigen Argument. Aber es geht uns hier ja um Polynomgleichungen, nicht um zZahlentheorie.

Korollar 2.12. *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: $X^2 + 1$ nicht irreduzible, 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.

$$\begin{aligned} X^4 - 2 &= (X^2 + a_1 X + a_0)(X^2 + b_1 + b_0) = \\ &X^4 + (b_1 + a_1)X^3 + (b_0 + a_0 + a_1 b_1)X^2 + (a_1 b_0 + b_1 a_0)X + a_0 b_0 \end{aligned}$$

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

$$0 = a_1 b_0 + b_1 a_0 = a_1(-a_0 + a_1^2) - a_1 a_0 = a_1(a_1^2 - 2a_0)$$

Also ist entweder $a_1 = 0$. Dann folgt $b_1 = 0, b_0 = -a_0$ und $-2 = a_0 b_0 = -a_0^2$ 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 $-2 = a_0 b_0 = -\frac{1}{4}a_1^4$ d.h. $8 = a_1^4$, aber 8 ist keine 4-te Potenz (Übungsaufgabe). □

Systematischer:

Satz 2.13 (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 $Q = Q = b_m X^m + \cdots + b_0$, $R = c_k X^k + \cdots + c_0$. 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 q ein Primteiler von α.

Behauptung. *Entweder alle b'_i oder alle c'_j sind durch q teilbar.*

Angenommen dies ist falsch. Dann existieren kleinste Indices i, j so dass b'_i und c'_j nicht durch q teilbar sind.

$$\alpha a_{i+j} = b'_0 c'_{i+j} + \cdots + b'_{i-1} c'_{j+1} + b'_i c'_j + b'_{i+1} c'_{j-1} + \cdots + b'_{i+j} c'_0$$

Wenn der erste Index kleiner als i ist oder der zweite kleiner als j, so ist der Summand durch q teilbar. Übrig bleibt nur ein Summand $b'_i c'_j$. Ein Faktor muss durch q teilbar sein, im Widerspruch zur Wahl von i und j.
Dies zeigt die Behauptung. 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 2.14. *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 auch $\beta, \gamma \in \mathbb{Z}$. Für den höchsten Koeffizienten gilt $1 = \beta\gamma$, also $\beta, \gamma = \pm 1$. Es folgt $\alpha \in \mathbb{Z}$. □

Wichtiger ist die folgende Variante:

Satz 2.15 (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. Es gilt

$$a_i = \sum_{j=0}^{i} b_j c_{i-j} \ .$$

p teilt $a_0 = b_0 c_0$, also teilt p entweder b_0 oder c_0 (nicht beide!). Ohne Einschränkung sei b_0 durch p teilbar.
p teilt $a_1 = b_0 c_1 + b_1 c_0$, also teilt p auch b_1. Ebenso folgt p teilt b_i für alle i. Insbesondere teilt p auch $a_n = b_m c_k$, ein Widerspruch zur Vorraussetzung. □

Beispiel. (zyklotomische Polynome, sehr wichtig!) 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

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

Das Eisensteinkriterium greift, also ist $P(Y)$ irreduzibel. Dann ist aber auch $P(X)$ irreduzibel.

Kapitel 3

Endliche und algebraische Körpererweiterungen

Wir erinnern uns (Definition 1.21): Sei L/K eine Körpererweiterung. Ein Element $a \in L$ heißt *algebraisch* über K, falls es ein Polynom $0 \neq P \in K[X]$ gibt mit $P(a) = 0$. a erfüllt die algebraische Gleichung P. Die Erweiterung L/K heißt *algebraisch*, wenn alle Elemente von L algebraisch über K sind.
Entscheidende Idee:

Definition 3.1. *Sei L/K eine Körpererweiterung. $[L : K] = \dim_K L$ heißt Grad der Erweiterung. Ist er endlich, so heißt die Erweiterung* endlich.

Beispiel. Sei K ein Körper, $P \in K[X]$ ein irreduzibles Polynom vom Grad n, $L = K[X]/(P)$. Dann ist L/K nach Korollar 2.8 und Lemma 2.6 eine endliche Körpererweiterung vom Grad $\deg P$.

Satz 3.2. *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 bekommt man alle algebraischen Elemente auf diesem Weg.

Lemma 3.3. *Sei L/K eine Körpererweiterung, $a \in L$. Der K-lineare Einsetzungshomomorphismus*

$$\phi_a : K[X] \to L, \quad X \mapsto a$$

hat den Kern

$$I = \{P \in K[X] \mid P(a) = 0\}$$

Es gilt $I \neq 0$ genau dann, wenn a algebraisch über K ist. In diesem Fall wird I von einem irreduziblen Polynom erzeugt. Es wird von einem irreduziblen Element erzeugt.

Definition 3.4. *Ist a algebraisch, so heißt der normierte Erzeuger von I* Minimalpolynom *von a. Wir schreiben* $\mathrm{Min}(a)$.

Das Minimalpolynom ist das normierte Polynom kleinsten Grades mit Nullstelle a. Es teilt alle anderen Polynome, die von a erfüllt werden.

Beweis: ϕ_a ist die Abbildung

$$\phi_a \left(\sum_{i=0}^{n} a_i X \right) = \sum_{i=0} a_i a^i$$

Dies ist offensichtlich ein Ringhomomorphismus. Nach Definition ist ist $I = \mathrm{Ker}\, \phi_a$, also ein echtes Ideal. Wir erhalten eine injektive Abbildung $\overline{\phi}_a : K[X]/I \to L$. Nach Definition von algebraischen Elementen ist $I \neq 0$ genau dann, wenn a algebraisch ist.
Sei nun a algebraisch. Nach 2.2 ist $I = (P_0)$ für ein Polynom $P \neq 0$. Angenommen, $P = P_1 P_2$. Dann folgt

$$P_1(a)P_2(a) = P(a) = 0 \in L \ .$$

Da L ein Körper ist, folgt ohne Einschränkung $P_1(a) = 0$, also $P_1 \in I = (P)$. Dann ist P_1 Teiler und Vielfaches von P, also muss $\deg P_2 = 0$ sein. Das bedeutet, dass P irreduzibel ist. □

Definition 3.5. *Let L/K eine Körpererweiterung, $a \in L$. Wir bezeichnen mit $K[a] \subset L$ den kleinsten Teilring, der K und a enthält, $K(a) \subset L$ den kleinsten Teilkörper, der K und a enthält.*

Satz 3.6. *Sei L/K Körpererweiterung, $a \in K$. Dann sind äquivalent:*

(i) a ist algebaisch über K.

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

(iii) $K(a)$ ist endlich als K-Vektoraum.

(iv) $K(a) = K[a]$

In diesem Fall ist $[K(a) : K] = \deg \mathrm{Min}(a)$.

Beweis: Sei I wie in Lemma 3.3. Nach Definition ist $K[a]$ das Bild des injektiven Ringhomomorphismus $K[X]/I \to L$. Wir setzen (i) voraus. Nach dem letzten Lemma ist $K[X]/I$ ein Körper, nach Lemma 2.6 endlich über K. Damit gilt (ii) und (iii) mit $K(a) = K[a]$.
Angenommen, (i) ist falsch. Dann ist $I = 0$, die Abbildung $K[X] \to K[\alpha]$ ist ein Isomorphismus, insbesondere ist der Ring nicht endlich dimensional. $K(\alpha)$ ist noch größer.
Ist a algebraisch, so gilt also $K[X]/(\mathrm{Min}(a)) \cong K(a)$. Dieser Körper hat nach Lemma 2.6 den Grad $\deg \mathrm{Min}(a)$. □

Satz 3.7. *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 3.8. *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 3.9. *Seien M/L und L/K algebraische Körpererweiterungen. Dann ist auch M/K algebraisch.*

Beweis: Sei $a \in M$, also nach Voraussetzung algebraisch über L. Sei $\mathrm{Min}_L(a) \in L[X]$ das Minimalpolynom. Sei

$$\mathrm{Min}_L(X) = a_n X^n + \cdots + a_0$$

Dann ist a auch algebraisch über $K' = K(a_n, \ldots, a_0)$, d.h. $K'(a)/K'$ ist endlich. Da alle a_i algebraisch über K sind, ist K'/K endlich, also auch $K'(a)/K$. Damit ist a algebraisch über K. □

Korollar 3.10. *Sei $P \in K[X]$ ein nicht-konstantes Polynom. Dann existiert eine algebraische Erweiterung L/K, in der P in Linearfaktoren zerfällt.*

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

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 2.9 gibt es eine Erweiterung L_1/K in der Q (und damit auch P) eine Nullstelle a_1 hat. Nach Konstruktion oder nach Satz 3.6 hat dieser Körper (oder nach Satz 3.6 der Teilkörper $K(a_1)$) Grad $\deg P \leq n$. 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 3.7 folgt

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

□

Definition 3.11. *Ein Körper K heißt* algebraisch abgeschlossen*, wenn jedes Polynom $P \in K[X]$ über K in Linearfaktoren zerfällt.*

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

Beispiel. $\mathbb{C}$, $\overline{\mathbb{Q}}$

Beweis: Im Fall $\mathbb{C}$ ist dies der Fundamentalsatz der Algebra, der meist in der Funktionentheorie bewiesen wird. Wir wollen später auch einen Beweis studieren. Unter dieser Voraussetzung zerfällt dann jedes Polynom mit Koeffizienten in $\mathbb{Q}$ in $\overline{\mathbb{Q}}$ in Linearfaktoren. Sei P ein Polynom mit Koeffizienten in $\overline{\mathbb{Q}}$. Dieses hat in $\mathbb{C}$ eine Nullstelle α. Die Körpererweiterung $\overline{\mathbb{Q}}(a)/\overline{\mathbb{Q}}$ ist algebraisch. Nach Korollar 3.9 ist dann $\overline{Q}(a)$ (insbesondere also a) algebraisch über $\mathbb{Q}$. Damit liegt a bereits in $\overline{\mathbb{Q}}$, der Körper ist algebraisch abgeschlossen. □

Theorem 3.12. *Sei K ein Körper. Dann gibt es einen algebraischen Erweiterungskörper $\overline{K}/K$, der algebraisch abeschlossen ist.*

Tatsächlich ist $\overline{K}$ eindeutig bis auf Isomorphie. Das muss aber noch etwas warten. Wesentliche Zutat ist der folgenden Satz:

Satz 3.13. *Sei A ein Ring, $I \subset A$ ein Ideal ungleich A. Dann gibt es ein maximales Ideal $m \supset I$.*

Beweis von Theorem 3.12. Sei $I_0 \subset K[X]$ die Menge der nicht-konstanten Polynome. Sei $\mathcal{X} = \{X_f \mid f \in I_0\}$ 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 3.10). In diesem Körper setzen wir α_i für X_{f_i} ein. Wir erhalten die Gleichung $1 = 0$, Widerspruch.
Nach Satz 3.13 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 jedes nicht-konstante $f \in I_0 \subset K[X]$ die Nullstelle $X_f + M$. Sei I_1 die Menge der nicht-konstanten Polynome in $L_1[X]$. Iterativ konstruieren wir L_2/L_1, in dem alle Polynome in $I_1 \subset L_1[X]$ eine Nullstelle haben, etc.

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

Behauptung. *$L = \bigcup_{i=1}^{n} L_i$ 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. □

Das Zornsche Lemma und Existenz von maximalen Idealen

Die Existenz von maximalen Idealen ist erstaunlich tief. Der Beweis benutzt das Zornsche Lemma.

Bemerkung. Vergleichen Sie mit dem Beweis der Existenz von Basen in beliebigen Vektorräumen.

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 3.14 (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 3.13. 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. □

Kapitel 4

Konstruktionen mit Zirkel und Lineal

Definition 4.1. *Gegeben sei eine Punktmenge M in der Ebene.*

(i) Eine Gerade ist (mit Lineal) konstruierbar aus M, wenn sie durch zwei Punkt aus M geht.

(ii) Ein Kreis ist (mit Zirkel) konstruierbar aus M, wenn er als Mittelpunkt einen Punkt aus M hat und als Radius den Abstand von zwei Punkten aus M.

(iii) Ein Punkt ist (mit Zirkel und Lineal) konstruierbar aus M, wenn er Schnitt von zwei konstruierbaren Geraden oder von zwei konstruierbaren Kreisen oder einer konstruierbaren Gerade mit einem konstruierbaren Kreis ist.

Die Menge $\overline{M}$ der mit Zirkel und Lineal aus M konstruierbaren Punkte ist die kleineste Teilmenge der Ebene, die M und alle aus $\overline{M}$ konstruierbaren Punkte enthält.

Mit anderen Worten: $\overline{M}$ enthält alle Punkte, die mit endlich vielen Schnittkonstruktionen Kreis/Gerade der angegebenen Art aus M konstruiert werden können.
Seien $P \neq Q$ zwei Punkte in der Ebene. Wir suchen nach $\overline{\{P, Q\}}$. Aus der Schule ist bekannt: Gegeben eine Gerade G und ein Punkt P. Dann kann durch P ein Lot auf G oder eine Parallele zu G konstruiert werden.
Ansatz: Die Ebene wird identifiziert mit $\mathbb{C}$, $P = 0, Q = 1$. Die Frage ist also, welche komplexen Zahlen mit Zirkel und Lineal konstruiert werden können.

Lemma 4.2. *Die Menge der Punkte in $\mathbb{C}$, die man mit Zirkel und Lineal aus $0, 1$ konstruieren kann, ist ein Teilkörper von $\mathbb{C}$. Mit einer Zahl α sind auch* $\mathrm{Re}\alpha$, $\mathrm{Im}\alpha$ *und $|\alpha| \in K$.*

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 $x, y, |x + iy| \in K$.*

Konstruktion: Den Betrag erhält man direkt duch Kreisschlagen. 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. □

Satz 4.3. *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 Länge der Strecke $[-1, z_0]$, q die Länge der 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 4.4. *Ein Element $z \in \mathbb{C}$ ist genau dann mit Zirkel und Lineal konstruierbar, wenn es eine Kette von Körpererweiterungen*

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

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.

Bemerkung. Die Bedingung $[\mathbb{Q}(z) : \mathbb{Q}]$ Potenz von 2 ist fast hinreichend für die Konstruierbarkeit - aber nicht ganz. Wir werden später darauf zurückkommen.

Beweis von Theorem 4.4.

Behauptung. *Sei $z \in K_n$ wie im Theorem. Dann ist z mit Zirkel und Lineal konstruierbar.*
Beweis durch vollständige Induktion über n. Der Fall $n = 0$ folgt aus 4.2. 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. Mit dem Lemma 4.3 ist dann a und mit 4.2 auch ganz $K_n(a)$ mit Zirkel und Lineal konstruierbar.
Damit haben wir eine Richtung des Theorems gezeigt. Interessanter ist die Umkehrung.
Wir nennen ein Element von $\mathbb{C}$ erreichbar (keine Standardterminologie), wenn es die Eigenschaften des Theorems erfüllt.

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

Ad (i) Seien z_1, z_2, z_2, z_4 erreichbar. Sei l_1 eine Gerade durch $z_1, z_2 \in K$. 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.

Ad (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 Voraussetzung und dem vorherigen sind die Elemente dieses Körpers erreichbar. Der Schnitt liegt in einer quadratischen Erweiterung, ist also ebenfalls erreichbar.

Ad (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_2 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 biquadratischen Erweiterung (quadratische gefolgt von quadratisch) von $\mathbb{Q}(z_1, z_2, \overline{z}_1, \overline{z}_2, r_1^2, r_2^2)$ liegen, also ebenfalls erreichbar sind.

Im einzelnen:

$$\begin{aligned}
&z_1 = u_1 + iv_1, z_2 = u + iv_1, x = a + ib \Rightarrow \\
&(a - u_1)^2 + (b - v_1)^2 = r_1^2 \Rightarrow (a - u_1)^2 = r_1^2 - (b - v_1)^2 \Rightarrow \\
&\qquad\qquad a = u_1 \pm \sqrt{r_1^2 - (b - v_1)^2} \\
&(a - u_2)^2 + (b - v_2)^2 = r_2^2 \Rightarrow (u_1 \pm \sqrt{r_1^2 - (b - v_1)^2})^2 + (b - v_2)^2 = r_2^2 \Rightarrow \\
&\qquad\qquad u_1^2 \pm 2u_1\sqrt{r_1^2 - (b - v_1)^2} + r_1^2 - (b - v_1)^2 + (b - v_2)^2 = r_2^2
\end{aligned}$$

Die letzte Gleichung enhält keinen quadratischen Term in b mehr. Durch Rationalmachen erhalten wir eine quadratische Gleichung für b, deren Lösung in einer quadratischen Erweiterung von $\mathbb{Q}(u_1, v_1, u_2, v_2, r_1^2, r_2^2)$ liegt. a liegt dann in einer quadratischen Erweiterung von $\mathbb{Q}(u_1, v_1, u_2, v_2, r_1^2, r_2^2, b)$. Damit sind dann a und b und deshalb auch $a + bi$ erreichbar.

□

Quadratur des Kreises: Gegeben ist ein Kreis. Dann ist es nicht möglich, mit Zirkel und Lineal ein Quadrat mit gleichem Flächeninhalt zu konstruieren.

Beweis: Ohne Einschränkung handelt es sich um den Einheitskreis mit Flächeninhalt π. Gesucht ist eine Konstruktion von $\sqrt{\pi}$, aber π ist nicht algebraisch und damit auch $\sqrt{\pi}$ nicht. Die Aussage ist nicht trivial, vergleiche S. Lang, Algebra, Appendix 1 S. 867.

Alternativ: Hardy, Writht, an Introduction to the Theory of Numbers, Abschnitt 11.14
Lorenz: Einführung in die Algebra I, §17. □

Kubusverdopplung: Gegeben ist ein Würfel. Dann ist es nicht möglich, mit Zirkel und Lineal einen Würfel von doppeltem Volumen zu konstruieren.

Beweis: Ohne Einschränkung betrachten wir den Einheitswürfel. Zu konstruieren ist also $\sqrt[3]{2}$. Diese Zahl hat das Minimalpolynom $X^3 - 2$ (Eisensteinkriterium!). 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 Potzen von 2. □

Regelmäßiges n-Eck: Sei n eine natürliche Zahl. Dann ist es im allgemeinen nicht möglich, das regelmäßige n-Eck mit Zirkel und Lineal zu konstruieren.

Beweis: 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 $[\mathbb{Q}(\varepsilon_1) : \mathbb{Q}] = p - 1$. Die Frage ist also, wann $p - 1$ eine Potenz von 2 ist, also

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

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

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

wird von $1 - (-2^{2^k})$ geteilt, denn $1 - X$ teilt $1 - X^n$. Dies ist nur eine Primzahl, wenn $n = 1$. 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

Auf jeden Fall ist das p-Eck für $p = 7, 11, \dots$ nicht konstruierbar. □

Bemerkung. Fermat vermutete, alle diese Zahlen der Form $1+2^{2^k}$ seien Primzahlen. Tatsächlich ist die nächste, $k = 5$, $p = 641 \cdot 6700417$ (Euler). Es sind keine weiteren Fermatschen Primzahlen bekannt. In einem gewissen Sinn ist als die Frage nach der Konstruierbarkeit des n-Ecks noch nicht vollständig gelöst!

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

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

Beweis: Sei ω_9 eine primitive 9-te Einheitswurzel, d.h. $\omega_9^3 \neq 1$. Das Polynom $X^6 + X^3 + 1$ genau dann irreduzibel, wenn $[\mathbb{Q}(\omega_9) : \mathbb{Q}] = 6$. Da das Minimalpolynom unser Polynom teilt, kommen nur die Grade $1, 2, 3, 6$ in Frage.
Das Minimalpolynom von $\omega_3 = \omega_9^3$ ist $X^2 + X + 1$, also enthält $\mathbb{Q}(\omega_9)$ einen Teilkörper vom Grad 2 über $\mathbb{Q}$. Wegen der Gradformel ist dann $[\mathbb{Q}(\omega_9) : \mathbb{Q}]$ ein Vielfaches von 2.
Sei $\alpha = \omega_9 + \omega_9^{-1} = \omega_9 + \overline{\omega}_9$. Es erfüllt das Polynom $X^3 - 3X + 1$, denn

$$(\omega_9 + \omega_9^{-1})^3 = \omega_3 + 3\omega_9 + 3\omega_9^{-1} + \omega_3^{-1} = -1 + \alpha$$

Dieses Polynom ist irreduzibel über $\mathbb{Q}$, denn wenn es Teiler hätte, dann müsste es eine ganzzahlige Nullstelle haben. Dies ist aus Paritätsgründen unmöglich. Daher gilt $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 3$ und $\mathbb{Q}(\omega_9)$ enthält einen Teilkörper vom Grad 3.
Insgesamt teilt 6 den Körpergrad, also ist er gleich 6. □

Winkeldreiteilung: Gegeben ist ein Winkel. Dann ist es im allgemeinen nicht möglich, ihn mit Zirkel und Lineal in drei gleiche Teile zu teilen.

Beweis: 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. □

Prinzip: Wir ordnen den Körpern Invarianten zu (hier eine Zahl, den Grad). Unterscheiden sich die Invarianten, so unterscheiden sich die Körper. Um weitergehende Fragen zu verstehen, brauchen wir feinere Invarianten. Wir werden eine Invariante mit Werten in der Kategorie der Gruppen betrachten, nämlich

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

Es wird sich herausstellen, dass diese Gruppe höchstens $[L : K]$ Elemente hat, also für endliche Erweiterung eine Gruppe mit endlich vielen Elementen ist.

Kapitel 5

Existenz und Fortsetzbarkeit von Körperhomomorphismen

Seien K_1, K_2 Körper. Wir wollen die Menge der Körperhomomorphismen $K_1 \to K_2$ verstehen. Besonders intessant wird der Fall K_2 algebraisch abgeschlossen oder $K_1 = K_2$.
Wir beginnen mit einigen einfachen Spezialfällen.

Charakteristik

Definition 5.1. *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 5.2. *Der Primkörper ist entweder isomorph zu $\mathbb{Q}$ oder isomorph zu $\mathbb{F}_p$ für eine Primzahl p.*

Definition 5.3. *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). $\alpha(\mathbb{Q}) \subset K$ 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 5.4. *Sei F ein Primkörper. Dann gibt es nur einen Körperhomomorphismus $\alpha : K \to K$, nämlich die Identität.*

Beweis: $\alpha(1) = 1$, $\alpha(2) = 2$ etc., also α die Identität auf $\mathbb{Z} \cdot 1_K$. Im Fall $\mathbb{F}_p$ sind wir damit fertig. Im Fall $K = \mathbb{Q}$ ist $\alpha(n/m) = \alpha(n)\alpha(m)^{-1}$ ebenfalls die Identität. □

Lemma 5.5. *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 5.6. *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. $\phi_1(1) = 1^p = 1$ und $\phi_1(-1) = (-1)^p = -1$ (klar, falls p ungerade; $p = 2 \Rightarrow -1 = 1$. Seien $x, y \in K$. Es gilt

$$\phi_1(xy) = (xy)^p = x^p y^p = \phi_1(x)\phi_1(y)$$

Die Verträglichkeit mit der Addition ist schwieriger.

$$\phi_1(x+y) = (x+y)^p = x^p + \binom{p}{1}x^{p-1}y + \binom{p}{2}x^{p-1}y^2 + \ldots \binom{p}{p-1}xy^{p-1} + y^p$$

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

$$\phi_1(x+y) = x^p + y^p = \phi_1(x) + \phi_1(y) \; .$$

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 $x^p = x$. Elementarer ausgedrückt, haben wir einen alten Satz gezeigt:

Korollar 5.7 (Kleiner Satz von Fermat). *Sei p eine Primzahl, $x \in \mathbb{Z}$. Dann gilt*

$$x^p = x \mod p$$

Beispiel. $K = \mathbb{F}_p(X) = \{\frac{P}{Q} \mid P, Q \in \mathbb{F}_p[X], Q \neq 0\}/\sim$. Wir betrachten wieder $\phi_1 : K \to K$.

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 Fortsetzungen

Wir wissen, dass jeder Körper K in einem algebraisch abgeschlossenen Körper $\overline{K}$ enthalten ist (Theorem 3.12). Wir wollen zeigen, dass jede algebraische Erweiterung von K als Teilkörper von $\overline{K}$ aufgefasst werden kann. Wieder beginnen wir mit einen Spezialfall.

Definition 5.8. *Eine Erweiterung L/K heißt* einfach, *falls $L = K(a)$ für ein $a \in L$.*

Ist $\sigma : K \to L$ ein Körperhomomorphismus, so ist

$$\sigma : K[X] \to L[X]; \quad \sum a_i X^i \mapsto \sigma(a_i) X^i$$

ein Ringhomomorphismus.

Satz 5.9. *Sei $K' = K(a)/K$ einfache algebraische Körpererweiterung,*

$$\sigma : K \to L$$

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 σ eine Inklusion.

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 sei $b \in L$ eine Nullstelle von $\sigma(P)$. Man betrachtet den Ringhomomorphismus

$$s : K[X] \to L \ ; \sum_{i=0}^{k} b_i X^i \mapsto \sum_{i=0}^{k} \sigma(b_i) b^i \ .$$

Das Polynom P liegt im Kern, denn

$$s(P) = \sum_{i=0}^{k} \sigma(b_i) b^i = 0$$

nach Voraussetzung. Also faktorisiert s nach Satz 1.16 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. s und damit $\overline{s}$ sind die einzigen möglichen Definitionen. □

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 5.10. *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 $\mathbb{Q}(\sqrt[4]{2}, i)$.

Nach Satz 3.10 existiert für jedes Polynom ein Zerällungskörper. Tatsächlich ist er eindeutig bis auf Isomorphismus:

Korollar 5.11. *Sei $P \in K[X]$ ein Polynom, L und L' Zerfällungskörper von P. Dann sind L und L' isomorph über K, d.h. es gibt einen Isomorphismus $\sigma : L' \to L$ mit $\sigma|_K = \mathrm{id}$.*

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 5.9 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 $\sigma_1(P_2)$ eine Nullstellte $b_2 \in L$. Nach dem Satz 5.9 existiert eine Fortsetzung

$$\sigma_2 : K(a_1, a_2) \to L \ .$$

Dies wiederholen wir und erhalten schließlich

$$\sigma_n : L' = K(a_1, \dots, a_n) \to L \ .$$

Das Bild von σ_n ist ein Teilkörper von L, in dem gilt

$$\begin{aligned} P(X) = \sigma_n(P(X)) &= \sigma_n((X - a_1)(X - a_2) \dots (X - a_n)) \\ &= (X - \sigma_n(a_1))(X - \sigma_n(a_2)) \dots (X - \sigma_n(a_n)) \ . \end{aligned}$$

D.h. P zerfällt in Linearfaktoren. Da L ein Zerfällungskörper ist, ist σ_n surjektiv. Als Körperhomomorphismus ist es eh injektiv. □

Korollar 5.12 (vergleiche Satz 3.12). *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 5.9 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. □

Definition 5.13. *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 $\sigma(i) = \pm i$.

Lemma 5.14. *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 5.9 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 5.15. *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 $(X - \sqrt{a})(X + \sqrt{a})$. Ist $\operatorname{Char} K \neq 2$, so gibt es also zwei Körperhomomorphismen $L \to L$ über K, 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.

Beispiele

Definition 5.16. *Sei L ein Körper. $\zeta \in L$ mit $\zeta^d = 1$ heißt d-te* Einheitswurzel. *Es heißt* primitive d-te Einheitswurzel, *falls $\zeta^i \neq 1$ für $1 \leq i < d$. Es sei $\mu_d(L)$ die Gruppe der d-ten Einheitswurzeln von L.*

Beispiel. $\zeta = \exp(2\pi i/d)$ ist primitive d-te Einheitswurzel in $\mathbb{C}$. (Die erste Ecke des regelmäßigen n-Ecks. C_d war die Gruppe der Restklassen modulo d.

Lemma 5.17. *Sei p eine Primzahl, ζ eine primitive p-te Einheitswurzel in $\mathbb{C}$. Dann ist $[\mathbb{Q}(\zeta) : \mathbb{Q}]$ galois. Die Galoisgruppe ist isomorph zu $\mathbb{F}_p^*$.*

Beweis: Das Minimalpolynom von ζ ist $X^{p-1}+\cdots+1 = (X^p-1)/(X-1)$. Insbesondere ist $[\mathbb{Q}(\zeta) : \mathbb{Q}] = p - 1$. Es hat in $\mathbb{Q}(zeta)$ die Nullstellen $\zeta, \zeta^2, \ldots, \zeta^{p-1}$ (alle Ecken des p-Ecks außer 1). Dies sind $p - 1$ viele, also alle. Nach Satz 5.9 gehört zu jeder dieser Einheitswurzeln genau ein Körperhomomorphismus $\mathbb{Q}(\zeta) \to \mathbb{Q}(\zeta)$, der die Identität auf $\mathbb{Q}$ iduziert. Dies sind $p - 1$ Elemente in der Galoisgruppe.
Nun schauen wir genauer hin. Für $i \in \mathbb{Z}$ teilerfremd zu p sei $\sigma_i : \mathbb{Q}(\zeta) \to \mathbb{Q}(\zeta)$ der eindeutige Körperhomomorphismus mit $\sigma_i(\zeta) = \zeta^i$.

Behauptung. *Die Abbildung $\mathbb{F}_p^* \to \operatorname{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$ mit $i \mod p \mapsto \sigma_i$ ist ein Gruppenhomomorphismus.*

Ist $i = j \mod p$, also $i = j + kp$, so gilt

$$\sigma_i(\zeta) = \zeta^i = \zeta^{k+kp} = \zeta^j(\zeta^p)^k = \zeta^j = \sigma_j(\zeta)$$

Also ist die Zuordnung wohldefiniert. Weiter gilt

$$\sigma_i(\sigma_j(\zeta)) = \sigma_i(\zeta^j) = \sigma_i(\zeta)^j = (\zeta^i)^j = \zeta^{ij} = \sigma_{ij}(\zeta)$$

Damit ist es ein Gruppenhomomorphismus. Im ersten Teil des Beweises haben wir gezeigt, dass die Abbildung surjektiv ist. Da beiden Gruppen gleich viel Elemente haben, ist sie sogar bijektiv. □

Allgemein gilt sogar: Sei ζ eine primitive d-te Einheitswurzel in $\mathbb{C}$. Dann gilt

$$\operatorname{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q}) \cong (\mathbb{Z}/d)^*$$

(Beweis wahrscheinlich erst nächstes Semester aus Zeitmangel).

Ziel

Zwei Körpererweiterungen mit unterschiedlicher Galoisgruppe müssen verschieden sein. Um mehr Galoisgruppen zu berechnen, müssen wir aber viel mehr über (endliche) Gruppen wissen.

Kapitel 6

Grundbegriffe der Gruppentheorie

Bisher haben wir nur die Begriffe Gruppe, Gruppenhomomorphismus und Kern/Bild definiert und gezeigt, dass ein Homomorphismus genau dann injektiv ist, wenn der Kern trivial ist.
Noch ein paar Beispiele:

Beispiel. (i) 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

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

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

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

(ii) Sei M eine Menge.

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

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

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

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

(iv) Für eine natürliche Zahl $n \geq 1$ war C_n die Gruppe der Restklassen von $\mathbb{Z}$ modulo n (bezüglich der Addition). Dies ist eine abelsche Gruppe mit n Elementen. Die natürliche Abbildung $\mathbb{Z} \to C_n$ ist ein surjektiver Gruppenhomomorphismus.

(v) $\mathrm{Aut}(G)$, 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.

(vi) $\iota : G \to G$ 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.

(vii) $\det : \mathrm{GL}_n(K) \to K^*$ ist ein surjektiver Gruppenhomomorphismus mit $\mathrm{Ker}\det = \mathrm{SL}_n(K)$.

(viii) sgn : $S_n \to \{\pm 1\}$, das Vorzeichen einer Permutation, ist ein Gruppenhomomorphismus. (Vergleiche LA 1 oder später)

Gruppen tauchen überall auf, wo es Symmetrien gibt!

Definition 6.1. *Eine* Untergruppe $H \subset G$ *ist eine Teilmenge einer Gruppe, so dass die Multiplikation aus* H *eine Gruppe macht.*

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

Beispiel. (i) $\mathrm{O}_n(K) \subset \mathrm{GL}_n(K)$ ist eine Untergruppe.

(ii) $\mathbb{Z} \subset \mathbb{C}$

(iii) Nach Definition ist jeder Untervektorraum eines Vektorraums zunächst eine Untergruppe.

(iv) Ist L/K eine Körpererweiterung, so sind $K \subset L$ (bezüglich der Addition) und $K^* \subset L^*$ (bezügliche der Multiplikation) Untergruppen.

(v) Sei L ein Körper, $\mu_d(L)$ die Menge der d-ten Einheitswurzeln. Dies ist eine Untergruppe von L^*. Die Gruppe ist endlich, da $X^d - 1$ höchstens d Nullstellen hat.

Satz 6.2. *Kern und Bild eines Gruppenhomomorphismus sind Gruppen.*

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

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

also gilt $ab \in \operatorname{Ker} f$.

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

Beide Zeilen gleich, also $a^{-1} \in \operatorname{Ker} f$. 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 Gruppenhomomorphismus $G \to G'$ mit Kern H? Später!
Wie kann man aus Gruppen neue Gruppen konstruieren?

Definition 6.3 (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.*

$$(g_1, g_2)(h_1, g_2) = (g_1 h_1, g_2 h_2)$$

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

□

Beispiel. Seien n, m teilerfremde natürliche Zahlen. Dann gilt nach dem Chinesischen Restsatz 1.11

$$C_n \times C_m \cong C_{nm}$$

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

Definition 6.4. *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 Untergruppen sind, ist XY im allgemeinen keine Untergruppe!

Satz 6.5. *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. $G = C_6$ Restklassen modulo 6, also $G = \{\overline{0}, \overline{1}, \overline{2}, \ldots, \overline{5}\}$.
H gerade Zahlen modulo 6, also $H = \{\overline{0}, \overline{2}, \overline{4}\}$.
K durch 3 teilbare Zahlen modulo 6, $K = \{\overline{0}, \overline{3}\}$.
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:

$$H \times K \cong G$$

Außerdem gilt $H \cong C_3$ via $\overline{2} \mapsto \overline{1}$ und $K \cong C_2$ via $\overline{3} \mapsto \overline{1}$. Also wieder:

$$C_2 \times C_3 \cong C_6$$

Bemerkung. C_6 ist der Quotient von $\mathbb{Z}$ nach der Untergruppe $6\mathbb{Z}$, also eine weitere Konstruktionsmöglichkeit von Gruppen. Allgemeiner:

Definition 6.6. *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.*

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

Lemma 6.7. *Zwei Linksnebenklassen sind entweder gleich oder disjunkt. Jede Nebenklasse enthält gleiche viele Elemente, nämlich so viele wie H.*

Beweis: 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

$$g_1 = g_2h_2h_1^{-1} \in g_2H \Rightarrow$$
$$g_1h = g_2h_2h_1^{-1}h \in g_2H \Rightarrow$$
$$g_1H \subset g_2H \ .$$

Aus Symmetriegründen gilt auch $g_2H \subset g_1H$, also sind die Nebenklassen gleich. Die Abbildung:

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

ist bijektiv, daher stimmen die Anzahlen überein. □

Definition 6.8. *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 6.9 (Euler-Lagrange). *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).

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

Definition 6.10. *Sei $g \in G$. Die* Ordnung *von g ist die Ordnung der kleinsten Untergruppe, die g enthält*

$$< g >= \{e, g, g^{-1}, g^2, g^{-2}, \dots\}$$

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

Korollar 6.11. *Die Ordnung von g teilt $|G|$. Es gilt $g^{|G|} = e$ für alle $g \in G$.*

Das hat konkrete Folgen für die Körpertheorie:

Korollar 6.12. *Sei K ein endlicher Körper mit q Elementen. Dann gilt*

$$x^{q-1} = 1 \text{ für alle } x \in K^* \text{ und } x^q = x \text{ für alle } x \in K$$

K ist Zerfällungskörper von $X^{q-1} - 1 \in \mathbb{F}_p[X]$. Insbesondere ist K eindeutig bis auf Isomorphismus durch seine Anzahl bestimmt.

Beweis: K^* ist eine Gruppe mit $q-1$ Elenten. Die zweite Gleichung folgt durch Multiplikation mit x und gilt dann auch für $x = 0$. Das Polynom hat in K $q-1$ verschiedene Nullstellen, zerfällt also in Linearfaktoren. In jedem Teilkörper von K fehlen einige der Nullstellen, damit ist K tatsächlich der Zerfällungskörper. Nach Satz 5.11 ist dieser eindeutig. □

Definition 6.13. *Der Körper mit q Elementen wird mit $\mathbb{F}_q$ bezeichnet.*

Für $q = p$ eine Primzahl finden wir hier den kleinen Satz von Fermat 5.7 wieder - mit einem anderen Beweis!
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 6.14. *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 6.15 (universelle Eigenschaft). *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 6.16. *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:

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

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

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.*

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

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

Sei $\overline{f}(gN) = e \Leftrightarrow f(g) = e \Leftrightarrow g \in N$, 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.

Satz 6.17 (1. Isomorphisatz). *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 Untergruppe. Es gibt einen kanonischen Isomorphismus*

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

Beweis: $K \triangleleft G$ bedeutet $gk = k'g$ für alle $g \in G$, 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:

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

abgeschlossen unter Multiplikation:

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

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 $hkK = hK$. 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 6.18 (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 6.16). 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 6.16 sind wir nun fertig. □

Einige Begriffe zum Schluss:

Definition 6.19. *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.

Zyklische Gruppen

Definition 6.20. *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 dem Erzeuger 1 mod 7.

(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 Gruppe ist zyklisch (vergleiche Definition 6.10).

Lemma 6.21. *(i) Eine Gruppe ist zyklisch, genau dann, wenn es einen surjektiven Gruppenhomomorphismus $p : \mathbb{Z} \to G$ gibt.*

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

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

Bemerkung. Eigentlich ist das der Beweis der Bemerkung nach 6.10.

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).
Sei $H \subset \mathbb{Z}$ eine Untergruppe. Für $h \in H$ und $a \in \mathbb{Z}$ gilt dann $ah \in H$, also ist H ein Ideal. Die Ideale von $\mathbb{Z}$ sind von der behaupteten Form, denn $\mathbb{Z}$ ist ein Hauptidealring (Beweis wie für Polynomringe, vergleiche Übungsaufgabe). Konkret ist n die kleinste natürliche Zahl, die in H enthalten ist (oder 0).
Nach (i) und Satz 6.16 ist jede zyklische Gruppe isomorph zu $\mathbb{Z}/H$ für einen Normalteiler $H \subset \mathbb{Z}$. Alle Untergruppen sind Normalteiler. Sie wurden also in (ii) bestimmt. Im Fall $n = 0$ erhält man $\mathbb{Z}/\{0\} \cong \mathbb{Z}$ eine unendliche Gruppe. In jedem anderen Fall ist die Faktorgruppe C_n endlich und hat die Ordnung $n > 0$. □

Satz 6.22. *Sei p eine Primzahl und G eine Gruppe der Ordnung p. Dann gilt $G \cong C_p$, insbesondere ist G abelsch.*

Beweis: Sei $g \in G$ mit $g \neq e$. Die Ordnung von g, d.h. die Ordnung der von g erzeugten Untergruppe $< g >$, ist ein Teiler von $|G| = p$. Da die Ordnung von g nicht 1 ist, muss sie p sein. Es folgt $< g >= G$. Damit ist G zyklisch von der Ordnung p. Nach Lemma 6.21 c) ist $G \cong \mathbb{Z}/p$. □

Lemma 6.23. *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.
Allgemeiner: seien $a\mathbb{Z}$, $b\mathbb{Z}$ beliebige Untergruppen von $\mathbb{Z}$. Die Inklusion $a\mathbb{Z} \subset b\mathbb{Z}$ bedeutet $a = xb$ mit $x \in \mathbb{Z}$, d.h. sie ist äquivalent zu b teilt a. 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.

Korollar 6.24. *$g \in G$ habe die Ordnung n. Dann hat g^m die Ordnung $n/\mathrm{ggT}(n,m)$.*

Beweis: Ohne Einschränkung ist $G =< g >\cong C_n$ mit $g = 1 \mod n$. Aus g^m wird die Nebenklasse $m \mod n$. Sei $\phi : \mathbb{Z} \to C_n$ und $H = \phi^{-1}(< m \mod n >)$ das Urbild der von $m \mod n$ erzeugten Gruppe. Dies ist eine Untergruppe von $\mathbb{Z}$, die m und n enthält, also $H = n\mathbb{Z} + m\mathbb{Z} = \mathrm{ggT}(n,m)\mathbb{Z}$. Es folgt $< m \mod n >= H/n\mathbb{Z}$ nach 6.16. Weiter gilt

$$C_n/ < m \mod n >= C_n/(H/n\mathbb{Z}) \cong \mathbb{Z}/H$$

nach dem 2. Noetherschen Isomorphiesatz 6.18. Es gilt also

$$[C_n :< m \mod n >] = |\mathbb{Z}/H| = \mathrm{ggT}(n,m)\ .$$

Nach dem Satz von Euler-Lagrange 6.9 folgt

$$| < m \mod n > | = |C_n|/[C_n :< m \mod n >] = n/\mathrm{ggT}(n,m).$$

□

Theorem 6.25 (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 aus Anordnung. Sie können auch mit der Bedingung $n_i \mid n_{i-1}$ gewählt werden, dann sind sie eindeutig. Dies sind die Elementarteiler.

Beweis: Algebra II, da eigentlich ein Satz über Moduln über dem Ring $\mathbb{Z}$. □

Kapitel 7

Wichtige Beispiele von Gruppen

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 $M = \{1, 2, \ldots, n\}$

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

Satz 7.1. *Jede (endliche) Gruppe ist Untergruppe einer (endlichen) Permutationsgruppe.*

Beweis: Wir wählen $M = G$. Wir definieren

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

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

Behauptung. *ι ist ein Gruppenhomomorphismus.*

Seien $g, g', h \in G$.

$$[\iota(g) \circ \iota(g')](h) = \iota(g)(\iota(g')(h)) = \tau_g(\tau'_g(h)) = g(g'h)$$
$$\iota(gg')(h) = \tau_{gg'}(h) = (gg')h$$

Nach dem Assoziativgesetz stimmen die beiden Ausdrücke überein.

Behauptung. *ι ist injektiv.*

Sei $\iota(g) = \tau_g$ die identische Abbildung. Dann gilt $gh\tau_g(h) = h$ für alle $h \in G$, insbesondere für $h = e$. Es folgt $g = e$. □

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

Definition 7.2. *Elemente der S_n heißen* Permutationen. *Man schreibt $\alpha \in S_n$ in der Form*

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

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*

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

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 7.3. *S_n hat $n!$ Elemente. S_n wird von Transpositionen erzeugt.*

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

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 Fehlstände, d.h. die Anzahl der i mit $i \neq \sigma(i)$. Angenommen $1 \neq \sigma(1)$ und $i \mapsto 1$. Wir betrachten

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

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

Beweis: Die Eindeutigkeit folgt aus dem Lemma. Der Existenzbeweis ist aufwendiger und wurde in der Linearen Algebra geführt. □

Definition 7.5. *Eine Permutation* σ *heißt gerade bzw. ungerade, falls* $\operatorname{sgn}(\sigma) = 1$ *bzw.* -1*. Der Kern von* sgn*, 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 $\varepsilon(\sigma) = (-1)^k$.

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

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

(iii) Die S_4 hat 24 Elemente, die A_4 hat 12. In A_4 gibt es den Normalteiler $\{e, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}$.

Satz 7.6. *Für* $n \geq 5$ *hat* A_n *keine Normalteiler als* $\{e\}$ *und* A_n*.*

Definition 7.7. *Eine solche Gruppe heißt* einfach*.*

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

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 $\gamma \in A_n$, gilt auch $\gamma\sigma\gamma^{-1} \in N$.
Was 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

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

(Übungsaufgabe). Mit geeignetem $\gamma \in S_n$ erhält man so alle 3-Zykel. Falls $\gamma \in \mathbb{A}_n$, 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. Weiterhin gilt

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

Man erhält also 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.
3. Fall: $\sigma = (1\ 2\ 3\ 4\ 5)$.

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

Allgemeiner Fall: Wir schreiben $\sigma = \sigma_1\sigma_2\ldots\sigma_m$ als Produkt von diskunkten 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 $\sigma_2 = (4\ \ldots\ k')$. Damit

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

und wir sind fertig nach dem 3. Fall. Falls $k = 2$, so ist nach Voraussetzung σ ein Produkt einer geraden Anzahl von disjunkten 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. □

Bemerkung. Einfache Gruppen sind so wichtig, da sie die Bausteine aller Gruppen sind: Ist G eine endliche Gruppe, so gibt es 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 $H_i = G_i/G_{i+1}$ einfach. Dabei sind die H_i bis auf Reihenfolge eindeutig durch G bestimmt.
Alle endlichen einfachen Gruppen sind bekannt. Es gibt einige unendliche Serien (z. B. C_p für p prim und A_n für $n \geq 5$) und endliche 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. Das Projekt, den Beweis besser organisiert aufzuschreiben, läuft seit langem.

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

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

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

(Übungsaufgabe. Kennen Sie diese Gruppe?)

Wir formalisieren.

Definition 7.8. *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

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

Definition 7.9. *Sei G eine Gruppe, $S \subset G$ eine Teilmenge. Wir sagen, dass G von S erzeugt wird, wenn die natürliche Abbildung*

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

surjektiv ist. 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

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

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

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

Beispiel. $G = \mathbb{Z} \times \mathbb{Z}$. Wir wählen $S = \{s_1, s_2\} = \{(1,0),(0,1)\}$. $F(S) \to \mathbb{Z} \times \mathbb{Z}$ 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 $F(S)/N$ gilt dann $s_1 s_2 s_1^{-1} s_2^{-1} = e \Leftrightarrow s_1 s_2 = s_2 s_1$. Also können alle Worte nach Potenzen von s_1 und s_2 umsortiert werden. $\mathbb{Z} \times \mathbb{Z}$ kann mit zwei Erzeugern und einer Relation geschrieben werden.

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.*

Kapitel 8

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 8.1. *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) $G = (V, +)$ die additive Gruppe eines Vektorraums, $M = A$ ein affiner Raum über V. Dies ist nach Definition eine Abbildung

$$V \times A \to A$$

welche die Operationseigenschaft hat.

(vi) Sei L/K eine algebraische Körpererweiterung, $G = \mathrm{Gal}(L/K)$. Dann operiert G auf L.

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

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

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 8.2. *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 $G \times G \to G$ die Gruppenmultiplikation haben wird diesen Satz schon bewiesen, siehe Satz 7.1 (Einbettung einer Gruppe in eine $S(M)$.

Definition 8.3. *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.*

Analog zu Lemma 8.2 erhält man dann einen Gruppenhomomorphismus $\alpha : G \to \mathrm{GL}(V)$. Darstellungen von Gruppen tauchen beim Lösen von linearen Differentialgleichungen auf, z.B. in der Quantenmechanik.

Definition 8.4. *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. Sie heißt* einfach transitiv*, wenn sie transitiv ist und $G_m = \{e\}$ für all $m \in M$. 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, aber nicht einfach transitiv.

(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.

(iv) V ein Vektorraum, A ein affiner Raum unter V. Nach Definition ist dies eine Menge mit einer einfach transitiven Operation von $(V, +)$. Insbesondere ist die Operation treu.

(v) Die Operation von $\mathrm{Gal}(L/K)$ auf L ist treu, denn eine Abbildung $\sigma : L \to L$ mit $\sigma(x) = x$ für alle $x \in L$ ist die Identität. Sei $P \in K[X]$, $x \in L$ eine Nullstelle von P. Dann ist die Bahn von x in der Menge der Nullstellen von P enthalten. Die Menge der Fixpunkte $L^{\mathrm{Gal}(L/K)}$ ist ein Teilkörper von L, der K enthält, ein sogenannter Zwischenkörper.

Satz 8.5. *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 $< \sigma > \subset S_n$ von einem Element erzeugt. Die Zyklenzerlegung von σ enspricht der Zerlegung von $\{1, \ldots, n\}$ in Bahnen von $< \sigma >$.

Korollar 8.6. *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 8.7. *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 8.8. *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 eine Operation transitiv, so ist sie also einfach transitiv genau dann, wenne eine Standgruppe (und damit alle) trivial sind. 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! Genau das ist der Witz an affinen Räumen.

Satz 8.9 (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 8.7 und Lemma 8.8. □

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:

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

Lemma 8.10. *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.

Kapitel 9

Normale und separable Körpererweiterungen

Hauptziel dieser Vorlesung ist der Beweis des **Hauptsatzes der Galoistheorie:**
Sei L/K eine endliche Galoiserweiterung. Dann ist die Zuordnung $H \mapsto L^H$ von Untergruppen $H \subset \mathrm{Gal}\,/L/K)$ in Zwischenkörper von L/K bijektiv.
Außerdem müssen wir natürlich besser verstehen, wann eine Erweiterung galois ist.
Sei nun L/K eine algebraische Körpererweiterung. Wir betrachten die Operation

$$\mathrm{Gal}(L/K) \times L \to L$$

Lemma 9.1. *Seien $\alpha, \alpha' \in L$ in derselben Bahn bezüglich der Operation der Galoisgruppe. Dann haben sie dasselbe Minimalpolynom über K.*

Beweis: Nach Vorraussetzung existiert $\sigma : L \to L$ mit $\sigma(\alpha) = \alpha'$. Sei P das Minimalpolynom von α, P' das von α'. Nach 5.9 gilt

$$P(\alpha') = \sigma(P)(\alpha') = 0 \Rightarrow P|P' \ .$$

Ebenso folgt $P' \mid P$, also unterscheiden sich P und P' höchstens um einen Faktor aus K^*. □

Definition 9.2. *Sei L/K eine Körpererweiterung. Zwei Elemente $\alpha, \alpha' \in L$ heißten* konjugiert*, wenn sie dassselbe Minimalpolynom haben.*

Die Bahnen bestehen also stets aus konjugierten Elementen. Die Bahn von α hat höchstens $\deg \mathrm{Min}(\alpha)$ viele Elemente.

Beispiel. Sei $L = K(a)$. Dann sind die Elemente der Galoisgruppe eindeutig durch die Bilder von a bestimmt, d.h. die Bahn von a sind genau die zu a konjugierten Elemente. Die Erweiterung ist genau dann galois, wenn es davon $\deg \mathrm{Min}(a)$ viele gibt.

Normale Erweiterungen

Definition 9.3. *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.

Satz 9.4. *Sei L/K normal. Dann stimmen die Konjugationsklassen mit den Bahnen überein.*

Beweis: Seien α, α' konjugiert. Dann existiert $\sigma : K(\alpha) \to L$ mit $\sigma(\alpha) = \alpha'$. Wegen der Normalität kann dieser nach ganz L fortgesetzt werden. Dies ist das gesuchte Element der Galoisgruppe. □

Lemma 9.5. *Sei L/K endlich und normal. Dann gibt es $P \in K[X]$, so dass L der Zerfällungskörper von P ist.*

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. □

Tatsächlich gilt auch die Umkehrung!

Satz 9.6. *Sei L/K Zerfällungskörper von $P \in K[X]$. Dann ist die Erweiterung normal.*

Beweis: Sei $Q \in K[X]$ irreduzibel mit Nullstelle $\alpha \in L$. Sei L_1/L der Zerfällungskörper von Q, $\beta \in L_1$ ein Nullstelle von Q.

Behauptung. $\beta \in L$.

Wir betrachten die Körpertürme

$$K \subset K(\alpha) \subset L$$

und

$$K \subset K(\beta) \subset L(\beta)$$

α und β haben das Minimalpolynom Q über K. Also existiert nach Satz 5.9 ein Isomorphismus

$$\sigma : K(\alpha) \to K(\beta) \ .$$

L ist der Zerfällungskörper von $P \in K(\alpha)[X]$. $L(\beta)$ ist der Zerfällunskörper von $\sigma(P) = P \in K(\beta)[X]$. Also existiert wie in 5.11 eine Fortsetzung

$$\sigma' : L \to L(\beta) \ ,$$

von σ, die ein Isomorphismus ist. Insbesondere haben L und $L(\beta)$ den gleichen Grad über K. Es folgt $\beta \in L$. □

Korollar 9.7. *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 9.8. *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 9.9. *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 5.9 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. □

Gilt $|\operatorname{Gal}(L/K)\alpha| = \deg \operatorname{Min}(\alpha)$? Sicher nicht, wenn die Erweiterung nicht normal ist. Aber auch dann könnten noch zwei Nullstellen des Minimalpolynoms gleich sein!

Separable Erweiterungen

Definition 9.10. *Ein irreduzibles Polynom in $K[X]$ heißt* separabel, *falls es keine doppelten Nullstellen über dem algebraischen Abschluss hat. Ein beliebiges Polynom heißt separabel, wenn alle irreduziblen Faktoren separabel sind. Sei L/K eine Körpererweiterung. $\alpha \in L$ heißt* separabel *über K, falls sein Minimalpolynom separabel ist. L/K heißt separabel, wenn alle Elemente von L separabel über K sind.*

Beispiel. (i) $X^2 + 1 \in \mathbb{R}[X]$

(ii) $(X - \alpha)^n \in \mathbb{Q}[X]$ ebenfalls separabel, da $X - \alpha$ separabel.

(iii) $\mathbb{C}/\mathbb{R}$ separabel.

Wir benötigen ein Kriterium!

Definition 9.11. *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 9.12 (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: $P = \sum_{i=0}^{n} a_i X^i$, $Q = \sum_{j=0}^{n} b_j X^j$, $\lambda \in K$.

$$(P+Q)' = \left(\sum (a_i + b_i) X^i\right)' = \sum i(a_i + b_i) X^{i-1}$$
$$= \sum i a_i X^{i-1} + \sum i b_i X^{i-1} = P' + Q'$$

$$(PQ)' = \left(\sum_i a_i X^i \sum_j b_j X^i\right)' = \left(\sum_{i,j} a_i b_j X^{i+j}\right)'$$
$$= \sum_{i,j} (i+j) a_i b_j X^{i+j-1} = \sum j a_i b_j X^{i+j-1} + \sum i a_i b_j X^{i+j-1}$$
$$= \sum a_i X^i \sum j b_j X^{j-1} + \sum i a_i X^{i-1} \sum b_j X^j = P'Q + PQ'$$

(iii) ist Spezialfall von (ii), denn $\lambda' = 0$. □

Lemma 9.13. *Sei $P \in K[X]$. $\alpha \in \overline{K}$ ist doppelte Nullstelle von P, genau dann wenn $P'(\alpha) = 0$. 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

$$P' = 1 \cdot \prod (X - \alpha_i) + (X - \alpha) \left(\prod (X - \alpha_i)\right)'$$

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 $P = 0$. □

Korollar 9.14. *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. □

Definition 9.15. *Ein Körper heißt* vollkommen, *wenn alle Polynome (und damit alle algebraischen Körpererweiterungen) separabel sind.*

Beispiel. Körper der Charakteristik 0, algebraisch abgeschlossene Körper.

Lemma 9.16. *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 $k \in \mathbb{N}$. □

Satz 9.17. *Sei* K *ein endlicher Körper. Dann ist* K *vollkommen.*

Beweis: Sei $\phi : K \to K$ der Frobenius, $x \mapsto x^p$. Nach Satz 5.6 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. □

In Termen der Operation

$$\operatorname{Gal}(L/K) \times L \to L$$

bedeutet dies: Wenn L/K normal und separabel, dann hat die Bahn von α genau $\deg \operatorname{Min}(\alpha)$ viele Elemente.

Kapitel 10

Galoistheorie

Wenn eine Gruppe G auf einer Menge M operiert, so bezeichnetete M^G die Menge der Fixpunkte von G,

Definition 10.1. *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.

Satz 10.2. *Sei L/K endliche Körpererweiterung. Dann sind äquivalent.*

(i) *L/K ist galois;*

(ii) $|\mathrm{Gal}(L/K)| = [L : K]$*;*

(iii) *L/K ist normal und separabel;*

(iv) $L^{\mathrm{Gal}(L/K)} = K$*.*

Beweis: (i)⇔(ii) war unsere Definition. Es gelte nun (iii). Wir wollen (iv) zeigen. Wie wir bereits überlegt haben hat die Bahn von α genau $\deg \mathrm{Min}(\alpha)$ viele Elemente. Also ist α ein Fixpunkt, genau dann wenn $\deg \mathrm{Min}(\alpha) = 1$, also $\alpha \in K$.
Es gelte (iv). Wir wollen (iii) zeigen. Sei $\alpha \in L$. Wir bestimmen zunächst das Minimalpolynom von α. Sei A die Bahn von α unter der Operation von $\mathrm{Gal}(L/K)$. Wir betrachten

$$P(X) = \prod_{\beta \in A} (X - \beta) \in L[X] \ .$$

Behauptung. $P(X) \in K[X]$.

Wegen $K = L^{\mathrm{Gal}(L/K)}$ genügt es zu zeigen, dass $P = \sigma(P)$ für alle $\sigma \in \mathrm{Gal}(L/K)$. Nach Definition

$$\sigma(P) = \prod_{\beta \in A} (X - \sigma(\beta)) = \prod_{\sigma^{-1}\gamma \in A} (X - \gamma) = P \ ,$$

denn mit γ durchläuft auch $\sigma^{-1}\gamma$ die gesamte Bahn von α. α ist eine Nullstelle von P. Alle Elemente in der Bahn von α haben ebenfalls das gleiche Minimalpolynom, also ist P tatsächlich das Minimalpolynom von α. Es zerfällt über L in einfache Linearfaktoren. Da dies für alle Minimalpolynome gilt, ist die Erweiterung normal und separabel.
Wir setzen (iii) voraus. Eine Wiederholung des Beweises von Lemma 5.14 ($|\mathrm{Gal}(L/K)| \leq [L : K]$) zeigt Gleichheit, falls die Erweiterung normal und separabel ist. Es folgt auch leicht aus dem nächsten Satz.
Zuletzt zeigt man die Implikation von (ii) nach (iv). Dies ist tief! Es folgt aus dem nächsten Satz. □

Satz 10.3. *Sei L ein Körper, $G \subset \mathrm{Aut}(L)$ eine endliche Untergruppe, $K = L^G$. Dann gilt*

$$[L : K] = |G| \ .$$

Ende des Beweises von Satz 10.2. Es gelte (iii) oder äquivalent (iv), $K = L^{\mathrm{Gal}(L/K)}$. Dann ist (ii) die Aussage des letzten Satzes.
Umgekehrt sei (iv) falsch. Wir haben $L \subset L^{\mathrm{Gal}(L/K)} \subset K$, also nach der Gradformel und dem letzten Satz

$$[L : K] = [L : L^{\mathrm{Gal}(L/K)}][L^{\mathrm{Gal}(L/K)} : K] > [L : L^{\mathrm{Gal}(L/K)}] = |\mathrm{Gal}(L/K)| \ .$$

Damit ist (ii) falsch. Dies beendet den Beweis von 10.2 □

Bemerkung. Der Beweis liefert im Galois-Fall eine Konstruktionsmethode für das Minimalpolynom.

Der harmlos aussehende Satz 10.3 ist in Wirklichkeit der Kern des Hauptsatzes der Galoistheorie und alles andere als trivial!

Der wichtigste Teil des Beweises

Beweis von 10.3. Sei $G = \{\sigma_1, \ldots, \sigma_n\}$, $K = L^G$ und $B = \{b_1, \ldots, b_r\}$ eine Basis von L/K. Hier ist a priori auch $r = \infty$ möglich. Zu zeigen ist $r = n$.

Behauptung. $r \geq n$.

1. Beweis: Es gilt $G \subset \mathrm{Gal}(L/K)$ und daher

$$n \leq |\mathrm{Gal}(L/K)| \leq [L : K] = r \ .$$

Behauptung. $r \leq n$.

Angenommen, $r > n$. Wir betrachten das lineare Gleichungssystem

$$\sum_j x_j \sigma_i(b_j) = 0 \text{ für alle } i.$$

Da wir mehr Unbekannte als Gleichungen haben, gibt es eine nicht-triviale Lösung $(x_1, \ldots, x_n)$. Wir wenden σ_k auf unsere Gleichungen an und erhalten:

$$0 = \sigma_k \left(\sum_j x_j \sigma_i(b_j) \right) = \sum_j \sigma_k(x_j) \sigma_k \circ \sigma_i(b_j) \text{ für alle } i,$$

oder, da $\sigma_k \circ \sigma_i$ ganz G durchläuft:

$$0 = \sum_j \sigma_k(x_j) \sigma_i(b_j) \text{ für alle } i.$$

Mit anderen Worten, auch $\sigma_k(x_j)$ ist eine Lösung unseres Gleichungssystems. Sei $N(x_j)$ die Anzahl der j mit $x_j \neq 0$. Nach Vorraussetzung ist $N \geq 1$. Ohne Einschränkung ist $x_1 = 1$. Wir betrachten das Tupel

$$y_j = x_j - \sigma_i(x_j).$$

Es ist eine neue Lösung mit echt kleinerem $N(y_j)$, denn $y_1 = 0$. Allgemein ist

$$y_j = 0 \Leftrightarrow x_j = \sigma_i(x_j) \ .$$

Gälte dies für alle σ_i, so wäre $x_j \in K$. Das ist aber ein Widerspruch zu linearen Unabhängigkeit der b_j (man betrachtet die Gleichung für $\sigma_1 = \mathrm{id}$). Also gibt es ein σ_i, so dass ein $y_j \neq 0$. Auch die neuere Lösung ist nicht-trivial. Wir erreichen schließlich eine nicht-triviale Lösung mit $N(x_j) = 1$. Der nicht-triviale Eintrag kann als 1 gewählt werden, liegt also in K. Wie wir bereits gesehen haben, ist dies ein Widerspruch zur linearen Unabhängigkeit der b_j. □

Der Hauptsatz

Sei L/K eine Körpererweiterung. Sei $\mathcal{G}$ die Menge der Untergruppen von $\mathrm{Gal}(L/K)$ und $\mathcal{K}$ die Menge der Zwischenkörper von L/K. Dann gibt es zwei Abbildungen

$$\begin{array}{ccccc} \mathcal{G} & \xrightarrow{\kappa} & \mathcal{K} & \xrightarrow{\gamma} & \mathcal{G} \\ G & \mapsto & L^G & & \\ & & F & \mapsto & \mathrm{Gal}(L/F) = \{\sigma \in \mathrm{Gal}(L/K) \mid \sigma \mid_F = \mathrm{id}\} \end{array}$$

Theorem 10.4 (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 $L \supset F_1 \supset F_2 \subset K$. 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

$$L^{H_1} = \{x \in L \mid \sigma(x) = x \text{ für alle } x \in H_1\} \subset L^{H_2} = \{x \in L \mid \sigma(x) = x \text{ für alle } x \in H_2\} \ .$$

Sei nun F ein Zwischenkörper. Nach Vorraussetzung ist L/K normal und separabel, also ist auch L/F normal und separabel, denn das Minimalpolynom von α in $F[X]$ teilt das Minimalpolynom von α in $K[X]$. Nach Satz 10.2 ist also L/F galois und

$$\kappa\gamma(F) = F^{\mathrm{Gal}(L/F)} = F \ .$$

Ebenfalls nach Satz 10.2 ist $[L : F] = |\mathrm{Gal}(L/F)$.
Sei H eine Untergruppe von $\mathrm{Gal}(L/K)$. Nach Satz 10.3 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.
Wie 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. Wie 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. Sei $\alpha \in F$, $\sigma \in \mathrm{Gal}(L/K)$. Wir wollen zeigen, dass $\sigma(\alpha) \in F$, d.h. invariant unter $\mathrm{Gal}(L/F)$. Sei also $\tau \in \mathrm{Gal}(L/F)$. Nach Voraussetzung ist

$$\sigma^{-1}\tau\sigma \in \mathrm{Gal}(L/F) \Rightarrow \sigma^{-1}\tau\sigma(\alpha) = \alpha \ .$$

Also liegen alle Konjugierten von α über L bereits in F, die Erweiterung F/K ist normal. □

Korollar 10.5. *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 $\mathbb{Q}$. Die Galoisgruppe hat Erzeuger σ, τ mit $\sigma^4 = \tau^2 = \mathrm{id}$ und $\tau\sigma = \sigma^3\tau$. (Übungsaufgabe)

$$G = \{\mathrm{id}, \sigma, \sigma^2, \sigma^3, \tau, \tau\sigma, \tau\sigma^2, \tau\sigma^3\}$$

Der Teilkörper $\mathbb{Q}(\sqrt[4]{2})$ ist der Fixkörper der Untergruppe $\{\mathrm{id}, \tau\}$. 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 τ enthalten. Sei H eine solche Untergruppe. Mit $\sigma^3 = \sigma^{-1}$ oder $\tau\sigma$ oder $\tau\sigma^3$ enthält die Gruppe auch σ und ist damit ganz G.

$$H = \{\mathrm{id}, \tau, \sigma^2, \tau\sigma^2\}$$

ist die einzige nichttriviale Möglichkeit. Daher ist $K^H = \mathbb{Q}(\sqrt{2})$ tatsächlich der einzige Teilkörper von $\mathbb{Q}(\sqrt[4]{2})$.

Artins Beweis

Artins Beweis kommt ohne Minimalpolynome und die Begriffe separabel, normal aus. Die Überlegungen zu Fortsetzbarkeit von Körperhomomorphismen entfallen ebenfalls. Das ist also viel eleganter!

Definition 10.6. *Sei G eine Gruppe, L ein Körper. Ein Gruppenhomomorphismus*

$$\chi : G \to L^* = L \setminus \{0\}$$

heißt Charakter.

Charaktere kann man als spezielle Elemente von

$$\mathrm{Abb}(G, L) = \{f : G \to L \mid f \text{ mengentheoretische Abbildung}\}$$

auffassen. Dies ist ein L-Vektorraum.

Satz 10.7. *Sein $\chi_1, \ldots, \chi_n : G \to L^*$ verschiedene Charaktere. Dann sind sie linear unabhängig als Elemente von* $\mathrm{Abb}(G, L)$.

Beweis: Induktion nach n. Der Fall $n = 1$ ist wahr, denn $\chi_1 \neq 0$. Seien nun $\chi_1, \ldots, \chi_{n-1}$ linear unabhängig, aber $\chi_1, \ldots, \chi_{n-1}, \chi_n$ linear abhängig, d.h. es gibt $\alpha_1, \ldots, \alpha_{n-1} \in L$ mit

$$\alpha_1\chi_1 + \cdots + \alpha_{n-1}\chi_{n-1} = \chi_n \in \mathrm{Abb}(G, L) \ ,$$

d.h. für alle $g \in G$ gilt

$$\alpha_1\chi_1(g) + \cdots + \alpha_{n-1}\chi_{n-1}(g) = \chi_n(g) \in L \ .$$

In dieser Gleichung ersetzen wir g durch gh, also

$$\alpha_1\chi_1(g)\chi_1(h) + \cdots + \alpha_{n-1}\chi_{n-1}(g)\chi_{n-1}(h) = \chi_n(g)\chi_n(h) \in L \ .$$

Diese Gleichung multiplizieren wir mit $\chi(h^{-1}) = \chi_n(h)^{-1}$:

$$\alpha_1\chi_1(g)\frac{\chi_1(h)}{\chi_n(h)} + \cdots + \alpha_{n-1}\chi_{n-1}(g)\frac{\chi_{n-1}(h)}{\chi_n(h)} = \chi_n(g) \in L \ .$$

Wir bilden die Differenz zur ersten Gleichung für g:

$$\alpha_1\chi_1(g)\left(1 - \frac{\chi_1(h)}{\chi_n(h)}\right) + \cdots + \alpha_{n-1}\chi_{n-1}(g)\left(1 - \frac{\chi_{n-1}(h)}{\chi_n(h)}\right) = 0 \in L \ .$$

Diese Gleichung gilt für alle g (und festes h), aber die χ_i für $i \leq n-1$ sind linear unabhängig. Es folgt

$$\alpha_i\left(1 - \frac{\chi_i(h)}{\chi_n(h)}\right) = 0 \ .$$

Wären alle $\alpha_i = 0$, so wäre $\chi_n = 0$. Also gibt es ein i_0 mit $\alpha_{i_0} \neq 0$. Es folgt

$$1 = \frac{\chi_{i_0}(h)}{\chi_n(h)} \Leftrightarrow \chi_n(h) = \chi_{i_0}(h) \ .$$

Dies gilt für alle $h \in G$, also ist $\chi_n = \chi_{i_0}$, Widerspruch. □

$$n \leq |\operatorname{Gal}(L/K)| \leq [L : K] = r \ .$$

Artins Beweis von Satz 10.3. Sei $K = L^G$. Die Ungleichung $r = [L : K] \geq |G| = r$ zeigt man wie oben. Wir wenden den letzten Satz an auf die Gruppe L^* und die Charaktere $\sigma_i : L^* \to L^*$ für

$$\{\sigma_1, \ldots, \sigma_n\} \in G \subset \mathrm{Aut}(L) \ .$$

Angenomen, $r < n$. Wir betrachten das lineare Gleichungssystem

$$\begin{aligned}
\sigma_1(b_1)x_1 + \sigma_2(b_1)x_2 + \ldots \sigma_n(b_1)x_n &= 0 \\
\sigma_1(b_2)x_1 + \sigma_2(b_2)x_2 + \ldots \sigma_n(b_2)x_n &= 0 \\
&\ldots \\
\sigma_1(b_r)x_1 + \sigma_2(b_r)x_2 + \ldots \sigma_n(b_r)x_n &= 0
\end{aligned}$$

Da wir mehr Unbekannte als Gleichungen haben, gibt es eine nicht-triviale Lösung $(x_1, \ldots, x_n)$, d.h.

$$\sum_i x_i \sigma_i(b_j) \text{ für alle } j,$$

Sei $b = \sum \alpha_j b_j$ mit $\alpha_j \in K$ ein beliebiges Element von L. Es folgt

$$\sum_i x_i \sigma(\sum_j \alpha_j b_j) = \sum_{i,j} \alpha_j x_i \sigma_i(b_j) = 0 \ .$$

Dies ist ein Widerspruch zur linearen Unabhängigkeit der σ_i. □

Daraus folgt dann die Äquivalenz von (ii) und (iv) in Satz 10.2 und auch der Hauptsatz der Galoistheorie.

Kapitel 11

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 11.1. *$\alpha \in \overline{\mathbb{Q}}$ 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. Wann hat $X^d - a$ doppelte Nullstellen? Die Ableitung ist dX^{d-1}. Für $a \neq 0$ und $\operatorname{Char} K$ teilerfremd zu d hat sie keine gemeinsamen Nullstellen mit $X^d - a$. Daher setzen wir jetzt stets d teilerfremd zu K oder noch einfacher $\operatorname{Char} K = 0$ voraus.

Satz 11.2 (Zyklotomische Erweiterungen). *Sei K ein Körper mit Charakteristik teilerfremd zu d, ζ eine primitive d-te Einheitswurzel, $L = K(\zeta)/K$. Dann ist L der Zerfällungskörper von $X^d - 1$. Es gibt einen Isomorphismus*

$$\operatorname{Gal}(L/K) \cong H \subset (\mathbb{Z}/d)^* \ .$$

Insbesondere ist die Galoisgruppe abelsch.

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 von P sind primitive d-te Einheitswurzeln, denn nicht-primitive Einheitswurzeln teilen einen anderen Faktor von $X^d - 1$. $\sigma \in \mathrm{Gal}(K(\zeta)/K)$ ist eindeutig festgelegt durch $\sigma(\zeta) = \zeta^{n_\sigma}$. Die Abbildung

$$\mathrm{Gal}(L/K) \to (\mathbb{Z}/d)^*, \quad \sigma \mapsto n_\sigma$$

ist injektiv.

Behauptung. *Dies ist ein Gruppenhomomorphismus.*

Seien $\sigma, \tau \in \mathrm{Gal}(L/K)$. 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 $n_{\sigma\tau} = n_\sigma n_\tau$. □

Satz 11.3 (Kummer-Erweiterungen). *Sei K ein Körper der Charakteristik 0, der eine primitive d-te Einheitswurzel enthält, wobei d teilerfremd zur Charakteristik. Sei $a \in K^*$, $L = K(\beta)$, wobei β eine Nullstelle von $X^d - a$ ist. Dann ist L Zerfällunskörper von $X^d - a$ und $\mathrm{Gal}(L/K)$ ist isomorph zu einer Untergruppe von $\mathbb{Z}/d$, insbesondere abelsch.*

Beweis: Sei ζ eine primitive d-te Einheitswurzel in K. $\beta^d = a$ 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, denn die Ableitung dX^{d-1} hat mit $X^d - a$ keine gemeinsame Nullstelle. Also zerfällt $X^d - a$ über L in verschiedene Linearfaktoren. 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 $\mathrm{Gal}(L/K)$ isomoph zu einer Untergruppe von $\mu_d(K) \cong \mathbb{Z}/d\mathbb{Z}$. □

Aber z.b. $\mathbb{Q}(\sqrt[4]{2} + i) = \mathbb{Q}(\sqrt[4]{2}, i)/\mathbb{Q}$ ist galois über $\mathbb{Q}$, aber die Galoisgruppe ist nicht abelsch! Statt dessen:

Definition 11.4. *Eine Gruppe G heißt auflösbar, wenn es eine Kette*

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

von Untergruppen gibt, so dass G_i ein Normalteiler von G_{i+1} ist und der Quotient G_{i+1}/G_i abelsch.

Lemma 11.5. *Mit G sind auch alle Untergruppe 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 11.6. *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), Gegenrichtung nächstes Semester.
Wir haben $K \subset K_n$ und

$$K_n \supset K_{n-1} \supset \cdots \supset K_0 = \mathbb{Q} \ ,$$

wie in der Definition.

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.*

Nach Induktionsvoraussetzung können wir ohne Einschränkung annehmen, dass K_{i-1} normal über $\mathbb{Q}$ ist, der Zerfällungskörper eines Polynoms R. Es ist $K_i = K_{i-1}(\alpha)$, wobei α die Gleichung $X^{n_i} - a_i$, $a_i \in K_{i-1}$ erfüllt. Wir betrachten das Polynom

$$P = \prod_{\sigma \in \mathrm{Gal}(K_i/\mathbb{Q})} (X^{n_i} - \sigma(a_i)) \in K_i[X] \ .$$

Das Polynom ist invariant unter der Operation von $\mathrm{Gal}(K_i/\mathbb{Q})$ und die Erweiterung ist galois, also gilt $P \in \mathbb{Q}[X]$. Wir wählen für L_i den Zerfällungskörper von RP. Er ist normal über $\mathbb{Q}$ und entsteht aus K_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 $\zeta = \sqrt[N]{1}$. Weiterhin gilt $K \subset L_n$.
Die Erweiterungen L_{i+1}/L_i sind nun Kummererweiterungen wie in Satz 11.3, 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. □

Bemerkung. Insbesondere ist also ein irreduzibles Polynom durch Radikale auflösbar, wenn eine Nullstelle durch Radikale ausgedrückt werden kann.

Satz 11.7. *Sei $P = X^5 - 4X + 2$, L der Zerfällungskörper von P. Dann gilt*

$$\mathrm{Gal}(L/\mathbb{Q}) \cong S_5$$

P ist nicht durch Radikale auflösbar.

Im Beweis benötigen wir noch eine Aussage aus der Theorie der endlichen Gruppen, den wir erst im nächsten Kapitel beweisen werden. Es ist eine Konsequenz des ersten Sylowsatzes.

Lemma 11.8. *Sei G eine endliche Gruppe und p eine Primzahl, die $|G|$ teilt. Dann gibt es in G eine Element der Ordnung p.*

Beweis: Wir setzen zunächst die Berechnung der Galoisgruppe voraus. Nach dem Teil des Theorems, den wir gezeigt haben, implziert die Auflösbarkeit von P die Auflösbarkeit von S_5. Mit S_5 wäre auch die Untergruppe A_5 auflösbar. Diese ist aber einfach und nichtabelsch. Sie hat keine abelschen Quotienten, ist also keineswegs auflösbar.
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 $\sigma_2 \in \mathrm{Gal}(L/\mathbb{Q})$. Daher enthält das Bild von ϕ ein Element der Ordnung 2.
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 dem Lemma hat $\mathrm{Gal}(L/K)$ ein Element der Ordnung 5. Dies gilt dann auch für das Bild von ϕ.

Behauptung. *Eine Untergruppe $G \subset S_5$, die ein Element der Ordnung 5 und ein Element der Ordnung 2 enthält, ist gleich S_5.*

Ohne Einschränkung enthält G das Elemente (1 2 3 4 5) und damit auch

$$< (1\ 2\ 3\ 4\ 5) >= \{e, (1\ 2\ 3\ 4\ 5), (1\ 3\ 5\ 2\ 4), (1\ 4\ 2\ 5\ 3), (1\ 5\ 4\ 3\ 2) >\} \ .$$

Ohne Einschränkung enthält G ein Element (1 ?) und sogar ohne Einschränkung (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. Dann ist $G \cap A_5$ 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 $(1\ 2\ 3\ 4\ 5) \in G \cap A_5$. Also ist $G \cap A_5 = A_5 \Rightarrow G \supset A_5$. G enthält jedoch die Transposition (1 2). Es bleibt der Fall $|G| = 120 \Rightarrow G = S_5$.

□

Kapitel 12

Die Sylow-Sätze und Anwendungen

Definition 12.1. *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. Entscheidendes Hilfsmittel sind die Operationen durch *Konjugation* (Übungsaufgaben):

$$G \times G \to G \; ; (g,h) \mapsto ghg^{-1}$$

und für M die Menge der Untergruppen von G

$$G \times M \to M \; ; (g,M) \mapsto gMg^{-1} \; .$$

Auf beide Situationen wird die Bahnformel angewendet.

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

wobei die Menge $\{x_1, \ldots, x_n\}$ aus jeder Bahn genau ein Element enthält. Wir hatten uns bereits überlegt, das im Fall einer p-Gruppe folgt

$$|M| = |M^G| \mod p.$$

Korollar 12.2. *Sei G eine p-Gruppe. Dann ist das Zentrum $Z(G)$ ungleich $\{e\}$.*

Beweis: Wir verwenden die obige Formel für die Operation von G auf sich durch Konjugation. 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 eine Normalteiler von G.

Satz 12.3. *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!

Beispiel.

$$Z/p^2 \subset p\mathbb{Z}/p^2\mathbb{Z} \subset \{(0,0)\}$$

oder

$$\mathbb{Z}/p \times \mathbb{Z}/p \subset \mathbb{Z}/p \times \{0\} \subset \{(0,0)\} \ .$$

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 6.16). Es gilt

$$N'/N \cong \overline{N}' \text{ und } G/N' \cong (G/N)/\overline{N'}$$

(Satz 6.16 und 2. Isomorphiesatz 6.18).
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 $N =< g >$ die von g erzeugte Untergruppe. Ist N echt kleiner als G, so schließen wir wieder mit vollständiger Induktion.
Übrig bleibt der Fall $G =< g >$ zyklisch, also $G \cong \mathbb{Z}/p^n$. In diesem Fall können wir die Kette direkt angeben, nämlich

$$N_i = p^{n-i}\mathbb{Z}/p^n\mathbb{Z} \ .$$

□

Konstruktionen mit Zirkel und Lineal

Wir wissen bereits (Theorem 4.4), dass $z \in \mathbb{C}$ genau dann mit Zirkel und Lineal konstruierbar ist, wenn es eine Kette von quadratischen Erweiterungen

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

gibt mit $z \in K_n$.

Korollar 12.4. *$z \in \mathbb{C}$ ist genau dann mit Zirkel und Lineal konstruierbar, wenn die normale Hülle K von $\mathbb{Q}(z)$ als Grad eine Potenz von 2 hat.*

Beweis: Sei z konstruierbar, also gibt es eine Kette

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

mit $z \in K_n$. Offensichtlich ist $[K_n : \mathbb{Q}]$ eine Potenz von 2. Wie im Beweis von Theorem 11.6 entsteht dann auch die normale HÜlle L von $K_n/\mathbb{Q}$ durch sukkzessives Adjungieren von Quadratwurzeln. Also ist auch $[L : \mathbb{Q}]$ eine Potenz von 2. Nach Voraussetzung ist $\mathbb{Q}(z) \subset K_n$ und daher auch $K \subset L$. Dann ist auch $[K : \mathbb{Q}] \mid [L : \mathbb{Q}]$ eine Potenz von 2.
Sei umgekehrt 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. □

Damit können wir genau bestimmen, welche Einheitswurzln (und damit welche regelmäßigen n-Ecke) mit Zirkel und Lineal konstruierbar sind.

Definition 12.5. *Eine Primzahl heißt* Fermatsche Primzahl*, wenn*

$$p = 1 + 2^{2^k} \qquad k = 0, 1, \ldots$$

k	p
0	p=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 $p = 7, 11, \ldots$ nicht konstruierbar. Die Frage nach Konstruierbarkeit von regelmäßigen n-Ecken ist gelöst modulo der Bestimmung der Fermatschen Primzahlen.

Satz 12.6. *Das regelmäßige n-Eck ist genau dann mit Zirkel und Lineal konstruierbar, wenn $n = 2^m p_1 \ldots p_i$ mit Fermatschen Primzahlen p_j ist.*

Beweis: Sei ζ_n eine primitive n-te Einheitswurzel. Nach dem Korollar ist z genau dann mit Zirkel und Lineal konstruierbar, wenn $[\mathbb{Q}(\zeta_n) : \mathbb{Q}]$ eine Potenz von 2 ist.
1. Fall $n = p$ **Primzahl:** Nach Lemma 5.17 ist $\mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q}) \cong \mathbb{F}_p^*$, hat also $p - 1$ Elemente. Wann ist

$$p = 2^m + 1?$$

Für $m = 0$ erhalten wir $p = 2$. Sei nun $m > 0$. Wir zerlegen $m = 2^k m'$ mit ungeradem m', dann wird

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

von $1-(-2^{2^k})$ geteilt, denn $1-X$ teilt $1-X^{m'}$. Dies wäre keine Primzahl falls $m' > 1$. Damit ist p eine Fermatsche Primzahl.
2. Fall $n = p^m$ **Primzahlpotenz**: Sei zunächst $n = p^m$. Dann ist $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \subset (\mathbb{Z}/p^m\mathbb{Z})^*$. Die invertierbaren Elemente in $\mathbb{Z}/p^m\mathbb{Z}$ sind diejenigen, die teilerfremd zu p sind. Davon gibt es

$$p^m - p^{m-1} = (p-1)p^{m-1}$$

viele. Da $\mathbb{Q}(\zeta_p) \subset \mathbb{Q}(\zeta_{p^m})$ ist $p-1$ ein Teiler von $[\mathbb{Q}(\zeta_n) : \mathbb{Q}]$. Wieder muss p eine Fermatsche Primzahl sein oder 2. Ist $m > 1$, so ist Der Körpergrad echt größer als $p-1$, also durch p teilbar. Dies ist dann nur für $p = 2$ erlaubt.
3. Fall n **allgemein:** Ist m ein Teiler von n, so gilt $\mathbb{Q}(\zeta_m) \subset \mathbb{Q}(\zeta_n)$. Wir betrachten die Zerlegung von

$$n = p_1^{n_1} \dots p_k^{n_k}$$

in Primzahlpotenzen. Nach den bisher betrachteten Fällen dürfen hier nur die im Satz angegebenen vorkommen. Umgekehrt ist die Galoisgruppe enthalten in

$$(\mathbb{Z}/n\mathbb{Z})^* \cong (\mathbb{Z}/p_1^{n_1})^* \times \dots \times (\mathbb{Z}/p_k 7 n_k)^*$$

(chinesischer Restsatz). Dies ist dann eine Potenz von 2. □

Sylowsätze

Definition 12.7. *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 12.8 (Erster Sylowsatz). *p-Sylowgruppen existieren.*

Bemerkung. Damit existieren auch Untergruppen der Ordnung p^i mir $i \leq r$ (mit r wie in der Definition).

Korollar 12.9. *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.
Direkter Beweis im abelschen Fall: Es genügt ein Element der Ordnung pk mit zu finden, denn dessen k-te Potenz hat Ordnung p. Wir führen den Beweis mit vollständiger Induktion. Sei $b \neq e$ beliebig. Wenn p die Ordnung von b teilt, sind wir fertig. Andernfalls teilt p die Ordnung von $\overline{G} = G/ < b >$. Nach Induktionsvoraussetzung existiert ein $\overline{a} \in \overline{G}$ mit Ordnung p. Sei $a \in G$ ein Urbild. Die Abbildung $< a > \to < \overline{a} >$ ist surjektiv (beachte: $< a > \subset G$, $< \overline{a} > \subset \overline{G}$). Also ist die Ordnung ein Vielfaches von p. □

Damit haben wir den Beweis von Lemma 11.8 nachgetragen.

Korollar 12.10 (Fundamentalsatz der Algebra). $\mathbb{C}$ *ist algebraische 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 $G = \mathrm{Gal}(L/R)$, 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 $F = \mathbb{R}$. Als 2-Gruppe enthält $G = P$ eine Untergruppe mit Index 2. Ihr Fixkörper ist eine quadratische Erweiterung von $\mathbb{C}$. Nach (ii) gibt es so etwas aber nicht. Es muss $G = P = \{\mathrm{id}\}$ sein. □

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 Korlollar, das wir ja für abelsche Gruppen direkt bewiesen haben, hat $Z(G)$ ein Element a der Ordnung p. Da a im Zentrum liegt, ist $< a >$ ein Normalteiler von G. Es gilt $|G/ < a > | = p^{r-1} m$. Nach Induktionsvoraussetzung hat $G/ < a >$ eine p-Sylowgruppe $\overline{H}$. Sei

$$H = \{g \in G \mid g < a > \in \overline{H}\}$$

Es gilt

$$|H| = |\overline{H}| \cdot | < a > | = p^{r-1}p \ .$$

□

Bemerkung. Der Beweis ist überhaupt nicht konstruktiv!

Theorem 12.11 (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.

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: Es sind $6 \cdot 4 = 24$. 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.

Beweis des zweiten und dritten Sylowsatzes. 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

$$|T| = [G : G_P] \qquad \text{nach Lemma 8.8}$$

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 8.9 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 6.17 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. Die Anzahlformel ist für die transitive Operation von G auf S ergibt $|S| = [G : G_P]$. 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. □

Kapitel 13

Schluss

Nachträge

Satz 13.1. *Sei ζ_d eine primitive d-te Einheitwurzel in $\mathbb{C}$ mit Minimalpolynom Φ_d über $\mathbb{Q}$. Dann gilt $\Phi_d \in \mathbb{Z}[X]$, $\deg \Phi = |(\mathbb{Z}/d\mathbb{Z})^*| =: \phi(d)$ und $\mathrm{Gal}(\mathbb{Q}(\zeta_d)/\mathbb{Q}) \cong (\mathbb{Z}/d\mathbb{Z})^*$.*

Beweis: Da ζ_d eine Nullstelle von $X^d - 1$ ist, ist Φ_d ein Teiler von $X^d - 1$. Nach dem Gauß-Lemma ist dann auch Φ_d ganzzahlig.
Es gibt genau $|(\mathbb{Z}/d)^*|$ primitive d-te Einheitswurzeln gibt. Wenn sie alle Nullstellen von Φ_d sind, dann ist $\phi(d) \geq |(\mathbb{Z}/d)^*|$. Nach Satz 11.2 ist $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$ isomorph zu einer Untergruppe von $|(\mathbb{Z}/d)^*|$. Da die Erweiterung normal (und separabel) ist, folgt $\phi(d) \leq |(\mathbb{Z}/d)^*|$, also Gleichheit und die Berechnung der Galoisgruppe.

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 (Gaußlemma 2.13). 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. □

Lemma 13.2. *Sei L/K eine Körpererweiterung, $a \in L$ separabel. Dann ist $K(a)/K$ separabel. Zerfällungskörper von separablen Polynomen sind galois.*

Beweis: Sei E/K Zerfällungskörper des separablen Polynoms P. Der Beweis der Implikation separabel und normal $\Rightarrow$ galois funktioniert bereits unter dieser Voraussetzung: Es werden nur die Minimalpolynome der Nullstellen von P benutzt, die dann keine mehrfachen Nullstellen haben. Ist a separabel, so ist $K(a)$ enthalten im Zerfällungskörper E des separablen Polynoms $\mathrm{Min}(a)$. Dann ist auch $K(a)/K$ separabel. □

Satz 13.3 (Satz vom primitiven Element). *Sei L/K endlich und separabel. Dann ist L einfach.*

Beweis: Alle Erweiterungen von endlichen Körpern sind Einheitswurzelerweiterungen, also einfach. Sei also ab jetzt L unendlich.
Die normale Hülle von L ist separabel über K, also galois. Nach dem Hauptsatz der Galoistheorie hat L/K also nur endlich viele Zwischenkörper. Es ist $L = K(a_1, \dots, a_n)$. Induktiv genügt zu zeigen:

Behauptung. *$K(\alpha, \beta)/K$ ist einfach.*

Wir betrachten

$$\{\alpha + c\beta \mid c \in K\}$$

Diese Menge hat unendlich viele Elemente. Andererseits ist die Menge der Körper

$$K(\alpha + c\beta) \subset K(\alpha, \beta)$$

endlich. Also gibt es $c_1 \neq c_2$ in K mit

$$K(\alpha + c_1\beta) = K(\alpha + c_2\beta) = F$$

Er enthält mit $\alpha + c_i\beta$ auch die Differenz $(c_1 - c_2)\beta$, also auch β. Damit muss auch α in F liegen. Dies zeigt $F = K(\alpha, \beta)$. □

Ausblick

Konzentriert man sich auf *Zahlkörper* ($K/\mathbb{Q}$ endlich), so nennt man das algebraische Zahlentheorie. Die *abelschen Erweiterungen* (galois und Galoisgruppe abelsch) sind gut verstanden. Unsere Überlegungen zum zyklotomischen Polynom - Ausnutzen des Frobenius für eine Hilfsprimzahl p - sind typisch für dieses Gebiet. Tatsächlich:

Theorem 13.4 (Kronecker-Weber). *Sei $F/\mathbb{Q}$ abelsch. Dann ist $F \subset \mathbb{Q}(\zeta_n)$ für eine primitive n-te Einheitswurzel n.*

Die Beschreibung der auftretenden Galoisgruppen und der Eigenschaften der Erweiterungen ist *Klassenkörpertheorie*. Man fasst dies auf als Beschreibung der Gruppenhomomorphismen

$$\mathrm{Gal}(\overline{K}/K) \to \mathrm{GL}_1(R) = \mathbb{R}^*$$

Sie entsprechen gewisssen Darstellungen der $\mathrm{GL}_1(\mathbb{A})$, wobei $\mathbb{A}$ der Ring der *Adele* von K ist.

Vermutung 13.5 (Langlands). *Die Gruppenhomomorphismen*

$$\mathrm{Gal}(\overline{K}/K) \to \mathrm{GL}_n(\mathbb{R})$$

entsprechen gewissen Darstellungen der $\mathrm{GL}_n(\mathbb{A})$.

Theorem 13.6 (Drinfeld, Lafforgue). *Die Langlandsvermutung gilt im Funktionenkörperfall, d.h. für endliche Erweiterungen von $\mathbb{F}_p(X)$.*

Der Beweis brachte Drinfeld 1990 (n=2) und Lafforgue 2002 (allgemeiner Fall) die Fields-Medaille ein. Dies ist die höchste Auszeichnung in der Mathematik. Sie wird alle 4 Jahre anlässlich des ICM vergeben.
Funktionenkörper haben eine geometrische Interpretation als Funktionen auf einer kompakten Kurve über $\mathbb{F}_p$. Die Methoden für den Beweis stammen aus der algebraischen Geometrie.

Algebra II

Wir werden uns in erster Linie mit kommutativer Algebra beschäftigen, also Theorie von kommutativen Ringen mit 1. Die wichtigsten Beispiel für mich sind die Ganzheitsringe wie $\mathbb{Z}, \mathbb{Z}[i], \mathbb{Z}[\sqrt{2}], \mathbb{Z}[\zeta_d]$ (algebraische Zahlentheorie) und die Polynomringe $k[X_1, \ldots, X_n]$ (algebraische Geometrie).

Inhaltsverzeichnis

0 Einleitung **1**

1 Grundstrukturen **5**

2 Polynomringe **15**

3 Endliche und alg. Körpererw. **23**

4 Konstruktionen mit Zirkel und Lineal **29**

5 Körperhomomorphismen **35**

6 Grundbegriffe der Gruppentheorie **43**

7 Wichtige Beispiele von Gruppen **55**

8 Operationen von Gruppen auf Mengen **61**

9 Norm. und sep. Körpererweiterungen **67**

10 Galoistheorie **73**

11 Lösung von Gleichungen durch Radikale **81**

12 Die Sylow-Sätze und Anwendungen **87**

13 Schluss **95**