

Algebra I

Wintersemester 2002/03

Prof. Dr. Annette Huber-Klawitter

Fassung vom 4. Februar 2003

**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

Was ist Algebra?

Im engeren Sinne

Die Theorie des Lösens von Gleichungen.

Beispiel. lineare Gleichungssysteme in mehreren Variablen — lineare Algebra, Stoff des 1. und 2. Semesters.

Beispiel. $ax^2 + bx + c = 0$ mit $a, b, c \in \mathbb{R}$ fest — Schulstoff

$$x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$$

reell falls $b^2 - 4ac \geq 0$.

Auch für Polynomgleichungen 3.ten und 4.ten Grades gibt es (grässliche) Lösungsformeln. Man benötigt imaginäre Zahlen, selbst wenn die Lösungen reell sind. So wurden die komplexen Zahlen erfunden!

Satz 0.1 (Fundamentalsatz der Algebra, Gauß 1799). *Jede Polynomgleichung*

$$a_0x^n + a_1x^{n-1} + \dots + a_n = 0$$

mit $a_0, \dots, a_n \in \mathbb{C}$ hat eine Lösung in \mathbb{C} .

Beweis: Siehe LA bei Prof. Kühn. Wir werden ebenfalls einen Beweis sehen, gegen Ende des Semesters. Der eleganteste Beweis kommt aus der Funktionentheorie. \square

Jahrhundertlang suchte man nach Lösungsformeln wie denen für quadratische Gleichungen.

Theorem 0.2 (Galois 1830-32). *Das ist im allgemeinen unmöglich.*

Beweis: Stoff dieser Vorlesung. □

Die Lösbarkeit von Gleichungen in ganzen oder rationalen Zahlen ist Gegenstand der Zahlentheorie. Hier sind noch viele Fragen offen!

Theorem 0.3 (Wiles 1995). *Für $n \geq 3$ hat $x^n + y^n = z^n$ keine Lösung in natürlichen Zahlen $\mathbb{N} = \{1, 2, 3, \dots\}$.*

Dies ist die berühmte “Fermatsche Vermutung” oder “großer Satz von Fermat”.

Beweis: Normalerweise nicht im Rahmen des Studiums. Grundlagen: Zahlentheorie, algebraische Geometrie, Modulformen. □

Literaturempfehlung: Simon Singh, Fermats letzter Satz.

Abstrakte/moderne Algebra

Sie 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. Viele dieser Strukturen werden überall in der Mathematik gebraucht.

Beispiel. (i) Lösungen von Differentialgleichungen führen auf Darstellungen von Gruppen.

(ii) Symmetriebetrachtungen bei Riemannschen Mannigfaltigkeiten führen auf Liegruppen.

Diese Art Algebra wird auch als Werkzeug eingesetzt.

Beispiel. Gibt es eine stetige bijektive Abbildung $\mathbb{R}^2 \rightarrow \mathbb{R}^3$? Versuchen Sie es mal selbst! Der heutige Beweis verwendet algebraische Topologie.

Der axiomatische Standpunkt

Andere Gebiete sind ähnlich aufgebaut wie die Algebra: z.B. Wahrscheinlichkeitstheorie, Topologie. Man destilliert Eigenschaften in Axiome und beweist ihre Konsequenzen.

Vorteil: klarer logischer Aufbau. Oft sehr mächtig. Wenn man nur wenige Voraussetzungen hat, dann müssen die Beweise einfach sein!

Nachteil: als Studierender weiß man nicht so recht, wofür das gut ist. Oft stecken die wichtigsten Einsichten in der Definition (Beispiel: Definition von Limiten).

Überblick über die geplante Vorlesung

Wir werden abstrakte Algebra treiben, und sie auf die klassischen Fragen über Lösbarkeit von Gleichungen anwenden.

- 1. Teil:** Grundbegriffe der Gruppentheorie, vor allem der endlichen Gruppen. Höhepunkt werden die Sylow-Sätze sein.
- 2. Teil:** Grundbegriffe der Theorie der Körpererweiterungen.
- 3. Teil:** Galois-Theorie: die Anwendung der Gruppentheorie in der Theorie der Körpererweiterungen. z.B. Beweis von Theorem 0.2.

Literatur

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

- S. Bosch:** Algebra, Springer Verlag. (oder jedes andere deutschsprachige Lehrbuch mit diesem Titel)
- E. Artin:** Galoissche Theorie, Verlag Harri Deutsch (das Original, von dem die ganze Welt abschreibt)
- S. Lang:** Algebra, Addison Wesley (sehr gute Stoffauswahl, deutlich umfangreicher als die Vorlesung).
- N. Bourbaki:** Algebra (Axiomatik in Reinkultur. Eher zum Nachschlagen).

Kapitel 1

Grundbegriffe der Gruppentheorie

Zur Erinnerung:

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

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

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

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

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

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

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

die *spezielle lineare Gruppe*.

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

die *orthogonale Gruppe*.

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

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

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 $f : V \rightarrow V$ bijektiv. Die inverse Abbildung g ist gegeben durch:*

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

- 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

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

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 $\text{Aut}_K(V)$. $f(g(v)) = v = g(f(v))$ gilt nach Definition. \square

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

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

(wenn wir wüssten, was ein Gruppenisomorphismus ist).

- (iv) Sei M eine Menge.

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

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

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

- (v) Wir betrachten ein regelmäßiges n -Eck in der Ebene. Die *Diedergruppe* ist die Symmetriegruppe dieses n -Ecks, z.B. Spiegelungen, Drehungen.
- (vi) Die *Galoisgruppe* ist eine Art Symmetriegruppe der Lösungen einer Gleichung.

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

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

Gruppen tauchen also überall auf, wo es Symmetrien gibt.

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

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

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

Definition 1.4. Ein Gruppenhomomorphismus ist eine Abbildung

$$f : G \rightarrow H$$

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

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

Der Kern von f ist

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

Das Bild von f ist

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

Ein Gruppenhomomorphismus heißt Isomorphismus, wenn er bijektiv ist. Ein Isomorphismus $f : G \rightarrow G$ heißt Automorphismus.

Beispiel. • $\text{Aut}(G)$, die Menge der Automorphismen der Gruppe G , ist selbst eine Gruppe. (Selber Beweis wie für $\text{Aut}_K(V)$.) Insbesondere ist die Umkehrabbildung eines Isomorphismus ein Gruppenisomorphismus.

- $\iota : G \rightarrow G$ mit $\iota(a) = a^{-1}$ ist ein Gruppenhomomorphismus

$$\iota(ab) = (ab)^{-1} = b^{-1}a^{-1} = \iota(b)\iota(a)$$

genau dann, wenn G kommutativ ist.

- $V \cong K^n$ ein Vektorraumisomorphismus $\Rightarrow \text{Aut}_K(V) \cong \text{GL}_n(K)$ ein Gruppenisomorphismus.
- $\det : \text{GL}_n(K) \rightarrow K^*$ ist ein surjektiver Gruppenhomomorphismus mit $\text{Ker det} = \text{SL}_n(K)$.

Satz 1.5. Kern und Bild eines Gruppenhomomorphismus sind Gruppen.

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

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

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

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

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

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

Gilt auch die Umkehrung?

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

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

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

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

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

Wie kann man aus Gruppen neue Gruppen konstruieren?

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

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

Beweis: (i) (Assoziativität)

$$\begin{aligned} (g_1, g_2) ((h_1, h_2)(k_1, k_2)) &= (g_1, g_2)(h_1k_1, h_2k_2) = (g_1h_1k_1, g_2h_2k_2) \\ ((g_1, g_2)(h_1, h_2))(k_1, k_2) &= (g_1h_1, g_2h_2)(k_1, k_2) = (g_1h_1k_1, g_2h_2k_2) \end{aligned}$$

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

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

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

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

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

Produkt von X und Y .

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

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

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

ein Isomorphismus.

Beweis: Zunächst: Gruppenhomomorphismus.

$$\begin{aligned} \mu(h, k)\mu(h', k') &= (hk)(h'k') = hkh'k' \\ \mu((h, k)(h', k')) &= \mu(hh', kk') = hh'kk' \end{aligned}$$

Die beiden stimmen überein, da $kh' = h'k$.

Nun: injektiv, also $\text{Ker}(\mu) = (e, e)$. Sei $(h, k) \in \text{Ker}(\mu)$, also $hk = e$. Also $h = k^{-1} \in K$. Nach Voraussetzung $h \in H$, also $h \in H \cap K = \{e\}$. Also gilt $h = e$. Analog sieht man $k = e$.

Zuletzt: surjektiv. Es ist $\text{Im}(\mu) = HK$. Nach Voraussetzung $HK = G$. □

Beispiel. $G = \mathbb{Z}/6 =$ Restklassen modulo 6 = $\{\bar{0}, \bar{1}, \bar{2}, \dots, \bar{5}\}$.

H gerade Zahlen modulo 6 = $\{\bar{0}, \bar{2}, \bar{4}\}$.

K durch 3 teilbare Zahlen modulo 6 = $\{\bar{0}, \bar{3}\}$.

Offensichtlich gilt $H \cap K = \{0\}$. Elemente vertauschen, denn G ist kommutativ.

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

Also:

$$H \times K \cong G$$

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

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

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

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

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

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

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

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

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

Beweis: 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:

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

ist bijektiv, daher stimmen die Anzahlen überein. \square

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

Ordnung und Index können auch unendlich sein.

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

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

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 \mathbb{Z}/p), so gibt es keine Untergruppen außer G und $\{e\}$, die trivialen Untergruppen.

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

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

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

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

Erinnerung: Sei p eine Primzahl. Dann ist

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

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

Beweis: Einziges Problem ist die Existenz von Inversen bezüglich der Multiplikation. Multiplikation mit einem $a \in \mathbb{F}_p^*$ ist eine injektive Abbildung. Da die Menge endlich ist, also auch surjektiv, also existiert ein inverses Element. \square

Insbesondere:

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

$$a^{p-1} = 1 \pmod{p}$$

Beweis: $G = \mathbb{F}_p \setminus \{0\}$ ist eine Gruppe mit der Multiplikation. $|G| = p - 1$. Die Restklasse \bar{a} liegt in G , denn $a \not\equiv 0 \pmod{p}$. \square

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 $g_2H = g'_2H$, d.h. $g'_2 = g_2h$ für ein $h \in H$. Dann folgt

$$(g_1H)(g'_2H) = g_1g'_2H = g_1g_2hH = g_1g_2H$$

denn $hH = H$.

Sei $g_1H = g'_1H$, d.h. $g'_1 = g_1h$ für ein $h \in H$.

$$(g'_1H)(g_2H) := g'_1g_2H = g_1hg_2H \stackrel{?}{=} g_1g_2H$$

Wir brauchen also:

$$hg_2H = g_2H$$

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

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

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

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

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

$$\begin{aligned} G_1 \times \{e\}(g_1, g_2) &= G_1g_1 \times \{g_2\} \\ (g_1, g_2)G_1 \times \{e\} &= g_1G_1 \times \{g_2\} \end{aligned}$$

ok, denn $G_1g_1 = G_1 = g_1G_1$.

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

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

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

$$g_1N \cdot g_2N = g_1g_2N$$

eine Gruppe, die Faktorgruppe. Die Quotientenabbildung

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

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 . \square

Also ist jeder Normalteiler Kern eines Homomorphismus!

Satz 1.19. Sei $f : G \rightarrow H$ ein Gruppenhomomorphismus. Dann ist $N = \text{Ker } f$ ein Normalteiler von G , und f induziert einen eindeutigen injektiven Homomorphismus

$$\bar{f} : G/N \rightarrow H ,$$

so dass f als $G \rightarrow G/N \rightarrow H$ faktorisiert. \bar{f} definiert einen Isomorphismus $G/N \cong \text{Im } f = \text{Im } \bar{f}$.

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

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

Beweis:

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

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

Behauptung. \bar{f} ist eindeutig.

Einzigste Möglichkeit ist $\bar{f}(gN) = f(g)$.

Behauptung. \bar{f} ist wohldefinierte Abbildung.

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

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

Behauptung. \bar{f} ist Gruppenhomomorphismus.

$$\bar{f}(g_1N\bar{g}_2N) = f(g_1g_2) = f(g_1)f(g_2) = \bar{f}(g_1)\bar{f}(g_2)$$

Behauptung. \bar{f} is injektiv.

Sei $\bar{f}(gN) = e \Leftrightarrow f(g) = e \Leftrightarrow g \in N$, d.h. $gN = eN$.

Außerdem ist $G/N \rightarrow \mathrm{Im} f$ surjektiv, also ein Isomorphismus. \square

Keineswegs ist jede Untergruppe Kern eines Gruppenhomomorphismus. Es muss schon ein Normalteiler sein.

Satz 1.20 (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 $\phi : H \rightarrow G/K$ 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. $\text{Ker}(\phi) = H \cap K$.

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

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

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

Satz 1.21 (2. Isomorphiesatz). *Sei G eine Gruppe und $K, H \triangleleft G$ 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 $G \rightarrow G/H$. K ist enthalten im Kern, also existiert eine Abbildung

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

(Beweis wie in 1.19). Sie ist surjektiv.

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

Sei $gK \in G/K$ mit $gH = p(gK) = H$. Dann ist $g \in H$.

Nach Satz 1.19 sind wir nun fertig. \square

Einige Begriffe zum Schluss:

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

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

Der Zentralisator von S in G ist

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

Der Zentralisator von G heißt Zentrum

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

Kapitel 2

Wichtige Beispiele von Gruppen

Erzeuger und Relationen

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

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

- Die Gruppe hat also die Elemente

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

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

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

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

(Übungsaufgabe. Kennen Sie diese Gruppe?)

Wir formalisieren.

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

$$s_1^{\varepsilon_1} s_2^{\varepsilon_2} \dots s_k^{\varepsilon_k}$$

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

$$F(S) \rightarrow G ; \text{Wort} \mapsto \text{Produkt}$$

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

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

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.

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

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

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

Beispiel. $G = \mathbb{Z} \times \mathbb{Z}$. Wir wählen $S = \{s_1, s_2\} = \{(1, 0), (0, 1)\}$. $F(S) \rightarrow \mathbb{Z} \times \mathbb{Z}$ 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 Zusatzbedingungen an R . In der Informatik wird meist nicht über Gruppen, sondern über Halbgruppen gesprochen (ohne inverse Elemente). Sie heißen dort *Semi-Thue Systeme*.

Zyklische Gruppen

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

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

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

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

(iv) Die Gruppe der 5-ten Einheitswurzeln

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

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

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

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

Bemerkung. Eigentlich ist das der Beweis der Bemerkung nach 1.14.

Beweis: Sei $g \in G$ ein Erzeuger. Wir setzen $p(k) = g^k$. Dies ist ein Gruppenhomomorphismus. Er ist surjektiv nach Definition. Dies zeigt (i).

Sei $H \subset \mathbb{Z}$ eine Untergruppe. Wenn $H = \{0\}$, so wählen wir $n = 0$. Andernfalls sei $n > 0$ die kleinste natürliche Zahl in H .

Behauptung. n erzeugt H .

Sei $m \in H$. Dann gibt es $q, r \in \mathbb{Z}$ mit $0 \leq r < n$, so dass

$$m = qn + r$$

(Division mit Rest). Wegen $n, m \in H$ gilt auch $r \in H$. Nach Wahl von n und r muss $r = 0$ sein. Also liegt m in $n\mathbb{Z}$. Dies zeigt (ii).

Nach (i) und Satz 1.19 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 $\mathbb{Z}/n\mathbb{Z}$ endlich und hat die Ordnung $n > 0$. \square

Satz 2.6. Sei p eine Primzahl und G eine Gruppe der Ordnung p . Dann gilt $G \cong \mathbb{Z}/p\mathbb{Z}$, insbesondere ist G abelsch.

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

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

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

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

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. \square

Bemerkung. Standardnotation ist $(n, m) = n\mathbb{Z} + m\mathbb{Z}$, aber auch $\text{ggT}(n, m) = (n, m)$. Nach dem Lemma ist das widerspruchsfrei.

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

Beweis: Ohne Einschränkung ist $G = \langle g \rangle \cong \mathbb{Z}/n\mathbb{Z}$ mit $g = 1 + n\mathbb{Z}$. Aus g^m wird die Nebenklasse $m + n\mathbb{Z}$. Sei $\phi: \mathbb{Z} \rightarrow \mathbb{Z}/n$ und $H = \phi^{-1}(\langle m + n\mathbb{Z} \rangle)$ das Urbild der von $m + n\mathbb{Z}$ erzeugten Gruppe. Dies ist eine Untergruppe von \mathbb{Z} , die m und n enthält, also $H = n\mathbb{Z} + m\mathbb{Z} = \text{ggT}(n, m)\mathbb{Z}$. Es folgt $\langle n + m\mathbb{Z} \rangle = H/n\mathbb{Z}$ nach 1.19. Weiter gilt

$$(\mathbb{Z}/n)/\langle m + n\mathbb{Z} \rangle = (\mathbb{Z}/n)/(H/n\mathbb{Z}) \cong \mathbb{Z}/H$$

nach dem 2. Noetherschen Isomorphiesatz 1.21. Es gilt also

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

Nach der Gradformel 1.13 folgt $|\langle m + n\mathbb{Z} \rangle| = |\mathbb{Z}/n|/[\mathbb{Z}/n : \langle m + n\mathbb{Z} \rangle] = n/\text{ggT}(n, m)$. \square

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

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

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

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

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

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

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

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

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

Permutationsgruppen

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

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

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

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

Satz 2.11. *Jede (endliche) Gruppe ist Untergruppe einer (endlichen) Permutationsgruppe.*

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

$$\iota : G \rightarrow S(G) \quad g \mapsto \tau_g$$

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

Behauptung. ι ist ein Gruppenhomomorphismus.

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

$$\begin{aligned} [\iota(g) \circ \iota(g')](h) &= \iota(g)(\iota(g')(h)) = \tau_g(\tau_{g'}(h)) = g(g'h) \\ \iota(gg')(h) &= \tau_{gg'}(h) = (gg')h \end{aligned}$$

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 $g = e$. \square

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

Definition 2.12. 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 Permutation kann als Produkt von disjunkten Zyklen geschrieben werden. Diese Darstellung ist eindeutig bis auf die Reihenfolge.

Beispiel.

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

Lemma 2.13. 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

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

mit Transpositionen τ_i . □

Satz 2.14. *Es gibt einen eindeutigen Gruppenhomomorphismus $\varepsilon : S_n \rightarrow \{\pm 1\}$, der Transpositionen auf -1 abbildet.*

Definition 2.15. *Eine Permutation σ heißt gerade bzw. ungerade, falls $\varepsilon(\sigma) = 1$ bzw. -1 . Der Kern von ε , d.h. die Untergruppe der geraden Permutationen, heißt alternierende Gruppe A_n .*

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

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

$$M : S_n \rightarrow \text{GL}_n(\mathbb{R}); \sigma \mapsto (e_{\sigma(1)} \quad e_{\sigma(2)} \quad \dots \quad e_{\sigma(n)})$$

Behauptung. *M ist ein Gruppenhomomorphismus.*

Nach Definition gilt $M(\sigma\sigma')(e_i) = e_{\sigma\sigma'(i)}$. Andererseits ist $M(\sigma) \circ M(\sigma')(e_i) = M(\sigma)(e_{\sigma'(i)}) = e_{\sigma\sigma'(i)}$.

Wir definieren $\varepsilon = \det \circ M$. Dies ist ein Gruppenhomomorphismus. Für eine Transposition τ gilt $\det M(\tau) = -1$, da die Determinante alternierend ist und $\det \text{id} = 1$. □

Bemerkung. Dieser Beweis ist natürlich ein wenig gepfuscht. Für die Existenz der Determinante benötigt man die Leibnitz-Formel und für diese das Vorzeichen der Permutationen. All dies wollen wir aus der linearen Algebra voraussetzen.

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

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

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

Definition 2.16. Eine Gruppe heißt einfach, wenn sie keine Normalteiler außer sich selbst und $\{e\}$ hat.

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

Satz 2.17. Für $n \geq 5$ ist die alternierende Gruppe 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 $\gamma \sigma \gamma^{-1} \in N$.

Wir wir suchen: S_n wird von Transpositionen erzeugt, A_n also von Elementen der Form $(a\ b)(c\ d)$. Dabei gibt es 2 Fälle: $\{a, b\} \cap \{c, d\} = \emptyset$ oder $\neq \emptyset$, d.h. $(a\ b)(a\ c) = (a\ c\ b)$ ein 3-Zykel.

1. Fall: Sei $\sigma = (1\ 2\ 3) \in N$. Für $\gamma \in S_n$ gilt

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

(Übungsaufgabe). Mit geeignetem $\gamma \in S_n$ erhält man so alle 3-Zykel. Falls $\gamma \in A_n$, 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 suchen: 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: $\sigma = (1\ 2\ 3\ 4\ 5)$.

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

Allgemeiner Fall: Wir schreiben $\sigma = \sigma_1 \sigma_2 \dots \sigma_m$ als Produkt von diskunkten Zykeln abnehmender Länge. Ohne Einschränkung: $\sigma_1 = (1\ 2\ 3\ \dots\ k)$. 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 $m > 2$, so ist ohne Einschränkung $\sigma_2 = (4\ \dots\ k')$. 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 Transpositionen. Den Fall $m = 2$ haben wir bereits betrachtet, sei nun $m \geq 4$. Ohne Einschränkung ist $\sigma = (1\ 2)(3\ 4)(5\ 6)\dots(2m-1\ 2m)$.

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

und wir sind fertig nach dem 2. Fall. \square

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

Definition 2.18. Sei G eine Gruppe. Eine Kompositionsreihe der Länge n ist eine Folge von Untergruppen

$$\{e\} = G_n \triangleleft G_{n-1} \triangleleft G_{n-2} \triangleleft \dots \triangleleft G_1 \triangleleft G_0 = G$$

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

Für beliebige Gruppen braucht eine Kompositionsreihe nicht zu existieren. Selbst im einfachsten Fall (z.B. $\mathbb{Z}/6$) ist sie nicht eindeutig.

Lemma 2.19. Sei G eine endliche Gruppe. Dann existiert eine Kompositionsreihe für G .

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

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

$$\begin{aligned} \{e\} \triangleleft N_n \triangleleft \dots \triangleleft N_k &= N \\ \{e\} = \bar{N}_k \triangleleft \dots \triangleleft \bar{N}_0 &= G/N \end{aligned}$$

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

Theorem 2.20 (Jordan-Hölder). *Besitzt G eine Kompositionsreihe, so haben alle Kompositionsreihen die selbe Länge. Die einfachen Subquotienten sind eindeutig bis auf Isomorphie und Anordnung.*

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

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

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

Der allgemeine Beweis ist technisch und wird Ihnen erspart.

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

Bemerkung. Alle endlichen einfachen Gruppen sind bekannt. Es gibt einige unendliche Serien (z. B. \mathbb{Z}/p 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.

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

Kapitel 3

Operationen von Gruppen auf Mengen

Der Begriff der Gruppe ist rein abstrakt, aber viele Beispiele ($S(M)$, $GL_n(K)$, Diedergruppe) haben mit Symmetrien von Objekten zu tun.

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

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

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) $GL_n(K) \times K^n \rightarrow K^n$ mit $(A, v) \mapsto Av$ (Matrixmultiplikation).

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

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

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

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

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

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

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

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

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

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

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

Beweis: Gegeben sei $G \times M \rightarrow M$. Wir definieren $\alpha : G \rightarrow S(M)$ durch $\alpha(g)(m) = gm$.

$\alpha(g)$ ist bijektiv, denn $\alpha(g^{-1})$ ist invers zu $\alpha(g)$.

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

$$em = \alpha(e)(m) = \text{id}(m) = m$$

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

□

Im Spezialfall der Operation $G \times G \rightarrow G$ die Gruppenmultiplikation haben wird diesen Satz schon bewiesen, siehe Satz 2.11 (Einbettung einer Gruppe in eine $S(M)$). Im Beweis von Satz 2.14 (Vorzeichen einer Permutation) wurde die Operation $S_n \times \mathbb{R}^n \rightarrow \mathbb{R}^n$ betrachtet, die durch lineare Fortsetzung der Permutation der Basisvektoren entsteht.

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

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

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

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

Die Bahn von $m \in M$ ist

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

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

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

Beispiel. (i) $G = S_n$, $M = \{1, \dots, n\}$. 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 Permutationen, die 1 nicht bewegen, also $S(\{2, \dots, n\}) \cong S_{n-1}$. Die Operation ist treu.

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

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

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

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

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

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

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

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

$$Gx = Gy = Gz$$

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

Korollar 3.7. Sei $G \times M \rightarrow M$ eine Operation auf einer endlichen Menge M . Seien x_1, \dots, x_n Elemente der verschiedenen Bahnen. Dann gilt

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

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

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

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

Nach Definition folgt die Behauptung. \square

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

Lemma 3.9. *Sei $G \times M \rightarrow M$ 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 $c_g : G_m \rightarrow G_{m'}$ 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 $c_{g^{-1}} : G_{m'} \rightarrow G_m$, 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

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

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 $g'G_m = gG_m$. \square

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

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

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

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

Beweis: Korollar 3.7 und Lemma 3.9. □

Das ist banal, aber ein sehr starkes Hilfsmittel!

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

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

Kapitel 4

Die Sylow-Sätze

Definition 4.1. 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):

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

und für M die Menge der Untergruppen von G

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

Auf beide Situationen wird die Bahnformel angewendet.

Korollar 4.2. Sei G eine p -Gruppe. Dann ist das Zentrum $Z(G)$ ungleich $\{e\}$.

Beweis: Wir verwenden die Formel des letzten Beispiels:

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

für die Operation von G auf sich durch Konjugation. Dann ist $|M| = |G|$, also eine Potenz von p . Es gilt

$$M^G = \{h \in G \mid ghg^{-1} = h \text{ für alle } g \in G\} = Z(G)$$

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. \square

Man beachte, dass $Z(G)$ abelsch ist und eine Normalteiler von G .

Satz 4.3. 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.

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

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 $G \rightarrow G/N \rightarrow (G/N)/\overline{N'}$, Satz 1.19). Es gilt

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

(Satz 1.19 und 2. Isomorphiesatz 1.21).

Dieses Prinzip erlaubt es den Satz mit Induktion über die Gruppenordnung zu beweisen. Sei G eine p -Gruppe. Das Korollar liefert einen nichttrivialen Normalteiler $Z(G)$. Ist $Z(G) \neq G$ sind wir nach Induktionsvoraussetzung fertig. Ist $Z(G) = G$, so ist insbesondere G abelsch.

Sei $g \in G$ ein Element ungleich $\{e\}$. Sei $N = \langle g \rangle$ die von g erzeugte Untergruppe. Ist N echt kleiner als G , so schließen wir wieder mit vollständiger Induktion.

Übrig bleibt der Fall $G = \langle g \rangle$ zyklisch, also $G \cong \mathbb{Z}/p^n$. In diesem Fall können wir die Kette direkt angeben, nämlich

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

□

Definition 4.4. Sei G eine endliche Gruppe. Sei p eine Primzahl, $|G| = p^r m$, wobei m teilerfremd zu p ist. Eine Untergruppe $H \subset G$ heißt p -Sylowgruppe von G , falls $|H| = p^r$.

Theorem 4.5 (Erster Sylowsatz). p -Sylowgruppen existieren.

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

Korollar 4.6. Sei G eine endliche Gruppe und p ein Primteiler der Gruppenordnung. Dann enthält G ein Element der Ordnung p .

Beweis: Aus dem ersten Sylowsatz: Es gibt eine p -Sylowgruppe, also auch eine Untergruppe der Ordnung p . Diese ist zyklisch, der Erzeuger ist das gesuchte Element.

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 $\overline{G} = G / \langle b \rangle$. Nach Induktionsvoraussetzung existiert ein $\overline{a} \in \overline{G}$ mit Ordnung p . Sei $a \in G$ ein Urbild. Die Abbildung $\langle a \rangle \rightarrow \langle \overline{a} \rangle$ ist surjektiv (beachte: $\langle a \rangle \subset G$, $\langle \overline{a} \rangle \subset \overline{G}$). Also ist die Ordnung ein Vielfaches von p . \square

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 geeignetes 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 Induktionsvoraussetzung eine Untergruppe der Ordnung p^r .) Wegen

$$p^r m = |H|[G : H]$$

teilt also p den Index $[G : H]$ jeder echten Untergruppe von G . Nun ist die obige Formel sehr hilfreich, nämlich $p^r m = |Z(G)| +$ Vielfaches von p . Es folgt $p \mid |Z(G)|$. Nach dem Korollar, das wir ja für abelsche Gruppen direkt bewiesen haben, hat $Z(G)$ ein Element a der Ordnung p . Da a im Zentrum liegt, ist $\langle a \rangle$ ein Normalteiler von G . Es gilt $|G / \langle a \rangle| = p^{r-1} m$. Nach Induktionsvoraussetzung hat $G / \langle a \rangle$ eine p -Sylowgruppe \overline{H} . Sei

$$H = \{g \in G \mid g \langle a \rangle \in \overline{H}\}$$

Es gilt

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

\square

Bemerkung. Der Beweis ist überhaupt nicht konstruktiv!

Theorem 4.7 (Zweiter und dritter Sylowsatz). *Sei G eine endliche Gruppe.*

- (i) *Sei $H \subset G$ eine p -Gruppe. Dann ist H in einer p -Sylowgruppe enthalten.*
- (ii) *Je zwei p -Sylowgruppen sind konjugiert, insbesondere isomorph.*

(iii) Die Anzahl der p -Sylowgruppen teilt $|G|$ und ist kongruent zu 1 modulo 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

$$G \rightarrow G/N_3 \times G/N_5 .$$

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.

$$G \times S \rightarrow S ; (g, P) \mapsto gPg^{-1} .$$

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

$$|T| = [G : G_P] \quad \text{nach Lemma 3.9}$$

also teilerfremd zu p .

Sei nun H eine p -Gruppe der Ordnung größer 1. Wir schränken die Operation ein

$$H \times T \rightarrow T$$

Nach dem Beispiel zur Bahnformel 3.10 gilt

$$|T| = |T^H| + \text{Vielfaches von } p .$$

Da p teilerfremd zu $|T|$ ist, folgt $T^H \neq \emptyset$. Also: es gibt $P_1 \in T \subset S$ eine p -Sylowgruppe, so dass

$$hP_1h^{-1} = P_1 \text{ f\"ur alle } h \in H .$$

Nach dem ersten Isomorphiesatz 1.20 folgt

$$HP_1/P_1 \cong H/H \cap P_1$$

Dies ist eine p -Gruppe. P_1 ist nach Voraussetzung eine p -Gruppe, also nun auch HP_1 . Es gilt $P_1 \subset HP_1$ und P_1 ist eine p -Sylowgruppe, also folgt $P_1 = HP_1 \Rightarrow H \subset P_1$.

Damit haben wir die erste Behauptung gezeigt. Wenn wir das Ergebnis an auf eine p -Sylowgruppe H an, so haben wir $H \subset P_1$, also $H = P_1 \in T$. Dies ist die zweite Behauptung. Die Anzahlformel ist f\"ur die transitive Operation von G auf S ergibt $|S| = [G : G_P]$. Die Bahnformel f\"ur die Operation von $H = P$ auf $S = T$

$$|S| = |S^P| + \text{Vielfaches von } p .$$

Dabei ist $S^P = \{P\}$, da wir $H \subset P_1$ f\"ur alle $P_1 \in S^P$ gezeigt haben. \square

Übersicht Gruppentheorie

Begriffe: Gruppe, Untergruppe, Gruppenhomomorphismus, Kern, Bild, direktes Produkt, Nebenklassen, Normalteiler, Ordnung, Index, Zentrum, freie Gruppe, Erzeuger, Relationen, zyklische Gruppe, symmetrische Gruppe, alternierende Gruppe, Operation, Bahn, Standgruppe, p -Gruppe, Sylowgruppe

Sätze: Faktorgruppe, Gradformel, Faktorisierung von Gruppenhomomorphismen, Gradformel, Isomorphiesätze $HN/N \cong H/H \cap N$, $(G/N)/(K/N) \cong G/K$, Klassifikation der zyklischen Gruppen, kleiner Satz von Fermat, chinesischer Restsatz, Existenz des Vorzeichens von Permutationen, A_n einfach f\"ur $n \geq 5$, Bahnformel, Struktur von p -Gruppen, Sylowsätze

Kapitel 5

Grundbegriffe der Ringtheorie

Unser Ziel ist das Studium von Körpern, dafür brauchen wir aber auch etwas Ringtheorie, vor allem den Polynomring.

Definition 5.1. Ein Ring ist eine Menge A mit zwei Verknüpfungen $+$, \cdot , so dass gilt:

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

(ii) \cdot ist assoziativ.

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

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

A heißt kommutativ, wenn $a \cdot b = b \cdot a$ für alle $a, b \in A$. 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) $k[X] = \{a_n X^n + a_{n-1} X^{n-1} + \dots + a_0 \mid n \in \mathbb{N}_0, a_i \in k\}$ der Polynomring über dem Körper k (oder dem Ring k).

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

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) $C(I) = \{f : I \rightarrow \mathbb{R} \text{ stetig} \}$, wobei $I \subset \mathbb{R}$ ein Intervall.

$C_c(\mathbb{R}) = \{f : \mathbb{R} \rightarrow \mathbb{R} \text{ stetig, mit kompaktem Träger} \}$, 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) $L^2(\mathbb{R}^n) = \{f : \mathbb{R}^n \rightarrow \mathbb{R} \mid f \text{ messbar, } \int_{\mathbb{R}^n} |f|^2 < \infty\} / \{f \mid \int_{\mathbb{R}^n} |f|^2 = 0\}$, Gegenstand der Funktionalanalysis.

Definition 5.2. Sei k ein Körper. Eine k -Algebra ist ein Ring A , der gleichzeitig ein k -Vektorraum ist, so dass

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

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

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

Definition 5.3. Ein Ringhomomorphismus $f : A \rightarrow B$ ist eine Abbildung mit

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

Beispiel. A eine k -Algebra mit Eins.

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

ist ein Ringhomomorphismus.

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

$(\lambda 1_A)(\mu 1_A) = \lambda(\mu 1_A) = \lambda(\mu 1_A) = (\lambda \mu) 1_A$, A eine k -Algebra, 1_A neutral. \square

Die Abbildung ist injektiv.

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

Definition 5.4. Eine Teilmenge $I \subset A$ heißt Ideal, wenn I eine Untergruppe von A ist und

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

Satz 5.5. (i) Sei $f : A \rightarrow B$ ein Ringhomomorphismus. Dann ist

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

ein Ideal.

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

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

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

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

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

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

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

Behauptung. *Die Multiplikation ist wohldefiniert.*

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

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

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

Behauptung. *A/I erfüllt das Distributivgesetz.*

$$\begin{aligned} (a + I)(b + I + c + I) &= (a + I)(b + c + I) = a(b + c) + I \\ (a + I)(b + I) + (a + I)(c + I) &= (ab + I) + (ac + I) = ab + ac + I \end{aligned}$$

Beide Ausdrücke sind gleich nach dem Distributivgesetz für A .

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

Behauptung. *\bar{f} ist ein Ringhomomorphismus.*

Es war $\bar{f}(a + \text{Ker } f) = f(a)$. Also

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

□

Bemerkung. Für nichtkommutative Ringe liegen die Dinge etwas komplizierter.

Beispiel. k ein Körper, $A = k[X]$.

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

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

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

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

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

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

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

Wann sind Quotienten von $k[X]$ Körper? Allgemein:

Definition 5.6. Ein Ideal $m \subset A$ heißt maximal, wenn $m \neq A$, und das einzige echte größere Ideal von A ist der ganze Ring A .

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

Satz 5.7. Sei A ein kommutativer Ring mit Eins, m ein Ideal. Dann ist A/m ein Körper genau dann, wenn m maximales Ideal ist.

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

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

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

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

wegen $c \in m$. Also ist $(b + m)$ invers zu $(a + m)$.

Umgekehrt sei A/m ein Körper. Sei $I \supset m$ ein Ideal.

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

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

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

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

Satz 5.8. Sei A ein Ring, $I \subset A$ ein Ideal ungleich A . Dann gibt es ein maximales Ideal $m \supset I$.

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

- (reflexiv) $x \leq x$ für alle $x \in M$;

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

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

Eine Ordnung heißt *total*, wenn für $x, y \in M$ entweder $x \leq y$ oder $y \leq x$ gilt.

Ein Element $m \in M$ heißt *maximal*, wenn $m \leq x \Rightarrow m = x$ für alle $x \in M$. Ein Element $m \in M$ heißt *obere Schranke* für $N \subset M$, wenn $x \leq m$ für alle $x \in N$.

Lemma 5.9 (Zornsches Lemma). *Sei $M \neq \emptyset$ eine partiell geordnete Menge. Jede total geordnete Teilmenge von M habe eine obere Schranke in M . Dann besitzt M ein maximales Element.*

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

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

Beweis von Satz 5.8. Sei M die Menge der Ideale ungleich A , die I enthalten. M ist partiell geordnet durch die Inklusion. Wegen $I \in M$ ist die Menge nicht leer. Sei $N \subset M$ eine partiell 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. \square

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

Polynomringe

Sei von nun an k ein Körper. Noch etwas allgemeine Notation:

Definition 5.10. Seien $a_1, a_2, \dots, a_n \in A$ Elemente eines Rings A . Dann ist

$$(a_1, \dots, a_n) = Aa_1 + \dots + Aa_n = \{b_1a_1 + \dots + b_na_n \mid b_i \in A\}$$

das von den a_i erzeugte Ideal. Im Fall $n = 1$ heißt (a_1) Hauptideal.

Satz 5.11. Sei k ein Körper. Dann ist $k[X]$ ein Hauptidealring, d.h. jedes Ideal ist von der Form $(P) = \{QP \mid Q \in k[X]\}$ für ein Polynom $P \in k[X]$.

Beispiel. $k[X, Y] = \{\sum_{i,j=1}^n a_{ij}X^iY^j \mid a_{ij} \in k\}$ ist kein Hauptidealring, denn (X, Y) wird nicht von einem einzigen Polynom erzeugt.

Auch viele andere Ringe nicht, etwa $\mathbb{Z}[\sqrt{5}] = \{a + b\sqrt{5} \mid a, b \in \mathbb{Z}\}$ ist keiner, wohl aber $\mathbb{Z}[i]$ (keine Beweise). Dies führt in die algebraische Zahlentheorie.

Der Beweis des Satzes braucht etwas Vorarbeit.

Definition 5.12. Sei $P = a_0 + \dots + a_nX^n$ 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:

$$\begin{aligned} \deg(P + Q) &\leq \max(\deg P, \deg Q) \\ \deg(PQ) &= \deg P + \deg Q \end{aligned}$$

Satz 5.13 (Euklidischer Algorithmus). Seien $P, Q \in k[X]$ zwei Polynome, $Q \neq 0$. Dann gibt es (eindeutige) Polynome P_1, R mit $\deg R < \deg Q$, so dass

$$P = P_1Q + R.$$

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 $n = \deg P$.

$$P = a_nX^n + \dots + a_0; \quad Q = b_mX^m + \dots + b_0$$

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 Induktionsvoraussetzung H_1 mit

$$P - HQ = H_1Q + R \text{ mit } \deg(R) < \deg Q.$$

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

$$P = P_1Q + R_1 \text{ und } P = P_2Q + R_2 \text{ mit } \deg(R_i) < \deg Q .$$

Differenzbildung 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 $R_1 - R_2 = 0$. \square

Bemerkung. Wir haben ausgenutzt, dass k ein Körper ist!

In dieser Induktion steckt natürlich die Polynomdivision wie in der Schule.

Beispiel.

$$\begin{array}{r} (X^4 + 3X^3 + 2X^2) : (X^2 - 1) = X^2 + 3X + 3 \\ \underline{X^4} \\ 3X^3 \\ \underline{3X^3} \\ 2X^2 \\ \underline{2X^2} \\ 0 \end{array}$$

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

Beweis von Satz 5.11. Sei $I \subset k[X]$ ein Ideal. Fall $I = 0$, so ist $I = (0)$, also ein Hauptideal. Sei nun $Q \in I$ mit $Q \neq 0$ ein Element von minimalem Grad.

Behauptung. $I = (Q)$.

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

$$P = P_1Q + R \Rightarrow R = P - P_1Q \in I .$$

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 . \square

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

Definition 5.14. 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 Enthaltenseinsrelationen für Ideale in Teilbarkeits-eigenschaften von Erzeugern.

Lemma 5.15. *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

$$\phi : k^{n+1} \rightarrow k[X]/(P) ; (a_0, \dots, a_n) \mapsto a_0 + a_1X + \dots + a_nX^n + (P)$$

Dies ist eine k -lineare Abbildung.

Behauptung. ϕ ist injektiv.

Sei $\phi(a_0, \dots, a_n) = 0 + (P)$, d.h. P teilt $Q = a_0 + a_1X + \dots + a_nX^n$. 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

$$Q = Q_1P + R .$$

Also ist $Q + (P) = Q_1P + R + (P) = R + (P)$. Letzteres liegt offensichtlich im Bild von ϕ . \square

Definition 5.16. *Ein Polynom $P \in k[X]$ mit $\deg P > 0$ heißt irreduzibel, falls P nicht von der Form $P = P_1P_2$ mit $\deg P_1, \deg P_2 > 0$ ist.*

Korollar 5.17. *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. \square

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

Lemma 5.18. *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 5.11. 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. \square

Theorem 5.19 (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

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

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. \square

Bemerkung. Man beachte die Analogie zu \mathbb{Z} : die normierten irreduziblen Polynome entsprechen den (positiven) Primzahlen, die Elemente von $k \setminus 0$ entsprechen ± 1 . Dies macht übrigens deutlich, warum 1 *keine* Primzahl ist!

Korollar 5.20. *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

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

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. \square

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 irreduzibel, dann ist es Produkt von Linearfaktoren, also hätte es eine Nullstelle, also $a \in \mathbb{R}$ mit $a^2 = -1$. Dies ist unmöglich, denn Quadrate sind in \mathbb{R} immer positiv.

- $X^2 + 1 \in \mathbb{C}[X]$ ist nicht irreduzibel, denn $X^2 + 1 = (X + i)(X - i)$.
- $X^4 - 2 \in \mathbb{Q}[X]$ ist ebenfalls irreduzibel.

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

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

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

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

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

Systematischer:

Satz 5.21 (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 $Q = Q = b_mX^m + \dots + b_0, R = c_kX^k + \dots + c_0$. 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.

$$\alpha a_{i+j} = b'_0c'_{i+j} + \dots + b'_{i-1}c'_{j+1} + b'_ic'_j + b'_{i+1}c'_{j-1} + \dots + b'_{i+j}c'_0$$

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 $b'_ic'_j$. 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 $\alpha = \pm 1$. \square

Oft kennt man nur die einfachere Form:

Korollar 5.22. Sei $P \in \mathbb{Z}[X]$ normiert, $\alpha \in \mathbb{Q}$ eine Nullstelle von P . Dann liegt α in \mathbb{Z} .

Beweis: Nach Voraussetzung 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 $\alpha \in \mathbb{Z}$. \square

Wichtiger ist die folgende Variante:

Satz 5.23 (Eisensteinkriterium). Sei $P = a_n X^n + \dots + a_0 \in \mathbb{Q}[X]$, $n \geq 1$, $a_i \in \mathbb{Z}$. Sei p eine Primzahl mit $p \mid a_0, \dots, a_{n-1}$, 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 $Q = b_m X^m + \dots + b_0$, $R = c_k X^k + \dots + c_0$. 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 $a_n = b_n c_n$, ein Widerspruch zur Voraussetzung. \square

Beispiel. Sei p eine Primzahl, $P = 1 + X + X^2 + \dots + X^{p-1} = \frac{X^p - 1}{X - 1}$. 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 6

Grundbegriffe der Körpertheorie

Exkurs: Unsere Ziele

Ziel der Vorlesung ist die Lösung einiger uralter mathematischer Probleme. Wir haben dafür bereits einen Werkzeugkasten bereitgestellt:

- Gruppen und Faktorgruppen (Kapitel 1)
- A_n ist einfach für $n \geq 5$ (Satz 2.17)
- Sylowsätze (Theorem 4.5 und Theorem 4.7)
- Konstruktion von Körpern aus dem Polynomring (Korollar 5.17)

Lösbarkeit von Polynomgleichungen: Sei $P \in \mathbb{Q}[X]$ ein Polynom, $z \in \mathbb{C}$ eine Nullstelle von P . Kann man z mit plus, mal, geteilt und Wurzeln durch Elemente von \mathbb{Q} ausdrücken?

Beispiel. $X^2 + pX + q$ mit $p, q \in k$. Dann ist $z = -\frac{1}{2}p \pm \frac{1}{2}\sqrt{p^2 - 4q}$.
 $X^3 + pX + q$. Dann ist (Cardanische Lösungsformel):

$$z \in \left\{ u + v, -\frac{u+v}{2} + \frac{u-v}{2}i\sqrt{3}, -\frac{u+v}{2} - \frac{u-v}{2}i\sqrt{3} \right\} ;$$
$$u = \sqrt[3]{-\frac{q}{2} + \sqrt{D}}, v = -\frac{p}{3u}, D = \left(\frac{p}{3}\right)^3 + \left(\frac{q}{2}\right)^2 .$$

Konstruktion mit Zirkel und Lineal

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

Quadratur des Kreises: Gegeben sei ein Kreis. Ist es möglich, mit Zirkel und Lineal ein Quadrat mit demselben Flächeninhalt zu konstruieren?

Konkreter: Ohne Einschränkung hat der Kreis den Radius 1, also die Fläche π (wußten die Griechen auch schon!). Gesucht ist eine Konstruktion von $\sqrt{\pi}$.

Dreiteilung des Winkels: Gegeben sei ein (beliebiger) Winkel. Ist es möglich, ihn mit Zirkel und Lineal in drei Teile zu teilen?

Für manche Winkel geht das natürlich, z.B. rechte Winkel. Halbierung ist ganz einfach! Eng verwandt ist die nächste Frage:

Konstruktion des regelmäßigen n -Ecks: Wie konstruiert man ein regelmäßiges n -Eck mit Zirkel und Lineal? $n = 3, 4$ klar. $n = 5$ geht auch...

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

Konkreter: Seitenlänge 1, also Volumen 1, gesucht ist eine Konstruktion von $\sqrt[3]{2}$.

Antwort auf alle Fragen: **Nein!** (Manchmal in Spezialfällen)

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

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

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

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

Konstruktion: Spiegelung am Nullpunkt.

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

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

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

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

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

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

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

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

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

Auch die Zahlen, die durch plus, mal, geteilt und Wurzeln durch Elemente von \mathbb{Q} ausgedrückt werden können, bilden einen Teilkörper von \mathbb{C} .

Basics

Der Vollständigkeit halber:

Definition 6.2. 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

$$\alpha : K \rightarrow L ,$$

die ein Ringhomomorphismus zwischen zwei Körpern mit $\alpha(1) = 1$ ist.

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

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

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

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

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

Satz 6.3. Alle Körperhomomorphismen sind injektiv.

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

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

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

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

Definition 6.4. Sei L ein Körper, $K \subset L$ eine Teilmenge, die mit der Addition und Multiplikation von L zu einem Körper wird. K heißt Teilkörper von L und L ein Erweiterungskörper von K . Wir sagen, L/K ist eine Körpererweiterung.

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

Definition 6.5. 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.

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 $X^2 + 1$, $\sqrt[3]{3}$, $\sqrt[7]{26 + \sqrt[3]{1/5}}$ als Nullstelle von $(X^7 - 26)^3 = 1/5$.

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

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

Entscheidende Idee:

Definition 6.6. Sei L/K eine Körpererweiterung. $[L : K] = \dim_K L$ heißt Grad der Erweiterung. Ist er endlich, so heißt die Erweiterung endlich.

Satz 6.7. 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 $\{1, a, a^2, a^3, \dots, a^n\}$ 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 $a_0, \dots, a_n \in K$, nicht alle gleichzeitig 0 mit

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

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

Die Umkehrung gilt nicht! $\overline{\mathbb{Q}}/\mathbb{Q}$ ist unendlich (später).

Satz 6.8. Sei K ein Körper, $P \in K[X]$ ein irreduzibles Polynom vom Grad n , $L = K[X]/(P)$. Dann ist L/K eine endliche Erweiterung vom Grad n . Das Polynom P hat eine Nullstelle in L .

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

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

Beweis: Sei $\pi : K[X] \rightarrow K[X]/(P)$ die Projektion. Sei $\xi = \pi(X)$. Nach Lemma 5.15 hat L die K -Dimension n , dies ist also der Körpergrad. Es gilt

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

denn π ist ein Ringhomomorphismus. □

Tatsächlich bekommt man alle algebraischen Elemente auf diesem Weg.

Lemma 6.9. Sei L/K eine Körpererweiterung, $a \in L$ algebraisch über K . Dann ist

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

ein Ideal ungleich 0. Es wird von einem irreduziblen Element erzeugt.

Definition 6.10. In der Situation des Lemmas heißt der normierte Erzeuger von I Minimalpolynom von a .

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

Beweis: Sei $P, Q \in I$. $P(a) + Q(a) = 0 + 0 = 0$, also $P + Q \in I$. Sei $R \in K[X]$. $(RP)(a) = R(a)P(a) = R(a)0 = 0$, also $RP \in I$. Damit ist I Ideal. Wir erhalten eine injektive Abbildung $K[X]/I \rightarrow L$.

Nach 5.11 ist $I = (P_0)$ für ein Polynom P_0 . Da I algebraisch ist, ist $P_0 \neq 0$. Angenommen, $P = P_1P_2$. 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 $\deg P_2 = 0$. Das bedeutet, dass P irreduzibel ist. \square

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 6.11. Sei L/K Körpererweiterung, $a \in K$. Dann sind äquivalent:

- (i) a ist algebraisch über K .
- (ii) $K[a]$ ist endlich als K -Vektorraum.
- (iii) $K(a)$ ist endlich als K -Vektorraum.

Beweis: Sei I wie im Lemma. Nach Definition ist $K[a]$ das Bild des injektiven Ringhomomorphismus $K[X]/I \rightarrow L$. Wir setzen (i) voraus. Nach dem letzten Lemma ist nach dem letzten Lemma ist $K[X]/I$ ein Körper, nach Lemma 6.8 endlich über K . Damit gilt (ii) und (iii) mit $K(a) = K[a]$.

Angenommen, (i) ist falsch. Dann ist $I = 0$, die Abbildung $K[X] \rightarrow K[a]$ ist ein Isomorphismus, insbesondere ist der Ring nicht endlich dimensional. $K(a)$ ist noch größer. \square

Satz 6.12. Sind M/L und L/K endliche Körpererweiterungen, so auch M/K . Es gilt

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

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

Behauptung. $\{x_i y_j \mid i = 1, \dots, n, j = 1, \dots, m\}$ 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 $\sum_j (\sum_k a_{kj} x_k) y_j = 0$ 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 . \square

Korollar 6.13. 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 $K(a, b) = K(a)(b)$. \square

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

Korollar 6.14. Seien M/L und L/K algebraische Körpererweiterungen. Dann ist auch M/K algebraisch.

Korollar 6.15. Sei $P \in K[X]$ ein nicht-konstantes Polynom. Dann existiert eine algebraische Erweiterung von L/K , in der P in Linearfaktoren zerfällt.

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

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 6.8 gibt es eine Erweiterung L_1/K mit $[L_1 : K] = m \leq n$, so dass Q (und damit auch P) eine Nullstelle α_1 in L_1 hat. Über L_1 gilt

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

Nach Induktionsvoraussetzung gibt es L/L_1 mit $[L : L_1] \leq (n-1)!$, so dass P_1 (und damit auch P) in Linearfaktoren zerfällt. Aus der Gradformel 6.12 folgt

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

□

Definition 6.16. 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. $\mathbb{C}, \overline{\mathbb{Q}}$ (beides nicht-trivial!)

Satz 6.17. Sei K ein Körper. Dann gibt es einen algebraischen Erweiterungskörper \overline{K}/K , der algebraisch abgeschlossen ist. Er ist eindeutig bis auf Isomorphie.

Beweis: Sei $I = (X) \subset K[X]$ das Ideal der nicht-konstanten Polynome. Sei $\mathcal{X} = \{X_f \mid f \in I\}$ 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

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

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 Polynom $P \in K[X] \subset R[X]$ 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 Erweiterungskörper, in dem f_i für $i = 1, \dots, n$ die Nullstelle α_i haben (gibt es Satz 6.8). In diesem Körper setzen wir α_i für X_{f_i} ein. Wir erhalten die Gleichung $1 = 0$, Widerspruch.

Nach Satz 5.8 hat R ein maximales Ideal M , das J enthält. Wir setzen $L_1 = R/M$. Dies ist ein Körper. Sei

$$K \rightarrow L_1$$

die Abbildung, die einem Element die Nebenklasse des konstanten Polynoms zuordnet. Dies ist ein Körperhomomorphismus. wir fassen L_1 als Erweiterung von K auf. In L_1 hat $f \in (X) \subset K[X]$ die Nullstellen $X_f + M$.

Iterativ konstruieren wir L_2/L_1 , in dem alle Polynome in $(X) \subset L_1[X]$ eine Nullstelle haben, etc.

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

Behauptung. $L \cup L_i$ ist algebraisch abgeschlossen.

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

Behauptung. L/K is algebraisch.

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

Die Eindeutigkeit werden wir erst später zeigen. \square

nocheinmal Zirkel und Lineal

Zurück zur Konstruierbarkeit mit Zirkel und Lineal. Nach Lemma 6.1 bilden die Zahlen, die mit Zirkel und Lineal konstruierbar sind einen Körper.

Theorem 6.18. *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. Wir werden später zeigen, dass z genau dann konstruierbar ist, wenn $[\mathbb{Q}(z) : \mathbb{Q}]$ eine Potenz von 2 ist.

Lemma 6.19. *Sei $K \subset \mathbb{C}$ ein Teilkörper, $a \in K$. Dann ist \sqrt{a} mit Zirkel und Lineal aus K konstruierbar.*

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

$$\begin{aligned} (1+a)^2 &= p^2 + q^2 & 1+h^2 &= p^2 & a^2+h^2 &= q^2 \\ &\Rightarrow 1+2a+a^2(1+a)^2 & &= 1+2h^2+a^2 & \Rightarrow a &= h^2 \end{aligned}$$

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

Korollar 6.20. *Sei $z \in K_n$ wie im Theorem. Dann ist z mit Zirkel und Lineal konstruierbar.*

Beweis: Beweis durch vollständige Induktion über n . Der Fall $n = 0$ folgt aus 6.1. Seien nun alle Elemente von K_n mit Zirkel und Lineal konstruierbar, $a \in K_{n+1} \setminus K_n$. Es gilt $K_n \subset K_n(a) \subset K_{n+1}$. Da die Erweiterung den Grad 2 hat, muss $K_{n+1} = K_n(a)$ gelten. Gleichzeitig ist $[K_n(a) : K_n]$ der Grad des Minimalpolynoms von a , also löst a eine quadratische Gleichung. Mit dem Lemma 6.19 ist dann a und mit 6.1 auch ganz $K_n(a)$ mit Zirkel und Lineal konstruierbar. \square

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

Beweis von Theorem 6.18. Wir nennen ein Element von \mathbb{C} erreichbar, wenn es die Eigenschaften des Satzes erfüllt.

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

Sei $z_1 \in K_n$ mit $\mathbb{Q} = K_0 \subset \dots \subset K_n$ mit $K_i = K_{i-1}(\sqrt{a_{i-1}})$ und $z_2 \in L_m$ mit $\mathbb{Q} = L_0 \subset \dots \subset L_m$. 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 \bar{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 \bar{z} . Wegen $|z|^2 = z\bar{z} \in \mathbb{Q}(z, \bar{z})$ 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.
- (i) Seien z_1, z_2, z_3, 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 $\mathbb{Q}(z_1, z_2, z_3, z_4, \bar{z}_1, \bar{z}_2, \bar{z}_3, \bar{z}_4)$, ist also erreichbar.

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

$$(z_1 + t(z_2 - z_0))(\bar{z}_1 + t(\bar{z}_2 - \bar{z}_0)) = r^2 .$$

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

- (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 $|x - z_1|^2 = (x - z_1)(\bar{x} - \bar{z}_1) = r_1^2$. Sei k_2 ein weiterer Kreis um z_2 mit Radius r_2 , Gleichung $|x - z_2|^2 = (x - z_2)(\bar{x} - \bar{z}_2) = r_2^2$. Explizite Rechnung zeigt, dass die Schnittpunkte Koordinaten in einer quadratischen Erweiterung von $\mathbb{Q}(z_1, z_2, \bar{z}_1, \bar{z}_2, r_1^2, r_2^2)$ liegen, also ebenfalls erreichbar sind.

□

Quadratur des Kreises: π ist nicht algebraisch, also auch $\sqrt{\pi}$ nicht. Die Aussage ist nicht trivial, vergleiche S. Lang, Algebra, Appendix 1 S. 867.

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

Regelmäßiges p -Eck: Sei p eine Primzahl. Die Ecken des p -Ecks sind p -te Einheitswurzeln $\varepsilon_k = \exp\left(\frac{2\pi i k}{p}\right)$. 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 .

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

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

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

Primzahlen von dieser Form heißen Fermatsche Primzahlen.

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

Satz 6.21. *Das regelmäßige n -Eck ist genau dann mit Zirkel und Lineal konstruierbar, wenn $n = 2^m p_1 \dots p_i$ mit Fermatschen Primzahlen p_j ist.*

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

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

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

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

Winkeldreiteilung: 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.

Kapitel 7

Körperhomomorphismen

Charakteristik

Definition 7.1. 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 7.2. Der Primkörper ist entweder isomorph zu \mathbb{Q} oder isomorph zu \mathbb{F}_p für eine Primzahl p .

Definition 7.3. Wir sagen, K hat Charakteristik 0 bzw. p , wenn der Primkörper \mathbb{Q} bzw. \mathbb{F}_p ist.

Beweis: Wir betrachten $\alpha : \mathbb{Z} \rightarrow K, 1 \mapsto 1$. 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 $\mathbb{Q} \rightarrow K$ 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: $\text{Ker } \alpha = \mathbb{Z}n$ mit $n > 0$. Dann ist $\text{Im } \alpha \cong \mathbb{Z}/n\mathbb{Z}$ 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. Im $\alpha \cong \mathbb{F}_p$ ist auch in allen Teilkörpern von K enthalten, also der Primkörper. \square

Bemerkung. Die Charakteristik ist der Erzeuger von $\text{Ker } \alpha$.

Lemma 7.4. Sei F ein Primkörper. Dann gibt es nur einen Körperhomomorphismus $\alpha : K \rightarrow K$, 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. \square

Lemma 7.5. *Seien K, L Körper mit unterschiedlicher Charakteristik. Dann gibt es keinen Körperhomomorphismus $\alpha : K \rightarrow L$.*

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. \square

Hier einige Beispiele für nichttriviale Körperhomomorphismen.

Beispiel. $K = \mathbb{C}$, $x + iv \mapsto x - iv$ für $x, y \in \mathbb{R}$.

Satz 7.6. *Sei K ein Körper mit $\text{Char } K = p > 0$, $n \in \mathbb{N}$. Dann ist die Abbildung*

$$\phi_n : K \rightarrow K ; x \mapsto x^{p^n}$$

ein Körperhomomorphismus, der Frobeniushomomorphismus. Sein Bild $\phi_n(K)$ ist ein Teilkörper von K .

Beweis: Wegen $\phi_n = \phi_1 \circ \dots \circ \phi_1$ 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.

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

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. \square

Bemerkung. Wenn $|K| < \infty$, dann ist ϕ_n bijektiv, denn jede injektive Abbildung ist auch surjektiv.

Beispiel. $K = \mathbb{F}_p$. Dann ist $\phi_1 = \text{id}$, also $x^p = x$. Dies ist wieder der kleine Satz von Fermat, vergleiche Korollar 1.16.

$K = \mathbb{F}_p(X) = \left\{ \frac{P}{Q} \mid P, Q \in k[X], Q \neq 0 \right\}$. Wir betrachten $\phi_1 : K \rightarrow K$.

Behauptung. X liegt nicht im Bild von ϕ_1 .

Angenommen, $X = \phi_1(P/Q) = P^p/Q^p$. Ohne Einschränkung haben P und Q keine Faktoren gemeinsam. Dann gilt $P^p = XQ^p$. Da in $k[X]$ eindeutige Primfaktorzerlegung gilt, folgt $X \mid P$, dann $X^p \mid XQ^p$, also $X \mid Q$, Widerspruch. In diesem Falls gilt also $\phi_1(K) \subset K$ ist ungleich K , aber isomorph zu K .

Existenz von Homomorphismen

Wir wissen, dass jeder Körper K in einem algebraisch abgeschlossenen Körper \overline{K} enthalten ist (Satz 6.17). Wir wollen zeigen, dass jede algebraische Erweiterung von K als Teilkörper von \overline{K} aufgefasst werden kann.

Definition 7.7. Eine Erweiterung L/K heißt einfach, falls $L = K(a)$ für ein $a \in L$.

Satz 7.8. Sei $K' = K(a)/K$ einfache algebraische Körpererweiterung,

$$\sigma : K \rightarrow L$$

ein Körperhomomorphismus, $P \in K[X]$ das Minimalpolynom von a .

(i) Ist $\sigma' : K' \rightarrow L$ 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 Voraussetzung gilt

$$P(a) = \sum_{i=0}^n a_i a^i = 0.$$

Anwenden des Körperhomomorphismus σ' liefert

$$\sigma'(P(a)) = \sum_{i=0}^n \sigma'(a_i) \sigma'(a)^i = \sigma(P)(\sigma'(a)) = 0.$$

Umgekehrt betrachtet man den Ringhomomorphismus

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

Das Polynom P liegt im Kern, denn

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

nach Voraussetzung. Also faktorisiert s über den Ringhomomorphismus

$$\bar{s} : K[X]/(P) \rightarrow L .$$

Der Homomorphismus $\pi : K[X]/(P) \rightarrow K(a)$ mit $X \mapsto a$ ist ein Isomorphismus, da P das Minimalpolynom von a ist. Die gesuchte Abbildung σ' ist gegeben durch $\bar{s} \circ \pi^{-1}$. Offensichtlich bildet sie a auf b ab. \square

Bemerkung. Eine Fortsetzung σ' von σ nach K' ist also nicht eindeutig. Es gibt soviele Fortsetzung wie Nullstellen von $\sigma(P)$, also höchstens $\deg(P)$ viele.

Definition 7.9. Sei $P \in K[X]$ ein Polynom. Eine Erweiterung L/K heißt Zerfällungskörper, wenn P über L in Linearfaktoren zerfällt,

$$P(X) = (X - a_1)(X - a_2) \dots (X - a_n)$$

und $L = K(a_1, a_2, \dots, a_n)$.

Beispiel. Das irreduzible Polynom $X^4 - 2 \in \mathbb{Q}[X]$ hat die Nullstellen

$$\sqrt[4]{2}, -\sqrt[4]{2}, i\sqrt[4]{2}, -i\sqrt[4]{2} .$$

Der Zerfällungskörper ist $\mathbb{Q}(\sqrt[4]{2}, i)$.

Korollar 7.10. Sei $P \in K[X]$ ein Polynom, L und L' Zerfällungskörper. Dann sind L und L' isomorph.

Beweis: Wir betrachten $\sigma : K \subset L$ die Inklusion. Es gilt also $\sigma(P) = P$. Es ist

$$P(X) = (X - a_1)(X - a_2) \dots (X - a_n) \quad a_i \in L' .$$

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 7.8 existiert eine Fortsetzung

$$\sigma_1 : K(a_1) \rightarrow L .$$

Sei P_2 das Minimalpolynom von a_2 über $K(a_1)$. Dann teilt P_2 wieder P und $\sigma_1(P_2)$ teilt $\sigma_1(P) = \sigma(P) = P$. Also hat $\sigma_1(P)$ eine Nullstelle $b_2 \in L$. Nach dem Satz 7.8 existiert eine Fortsetzung

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

Dies wiederholen wir und erhalten schließlich

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

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. \square

Korollar 7.11 (vergleiche Satz 6.17). *Sei K ein Körper, K_1 und K_2 seien zwei algebraische Abschlüsse. Dann gibt es einen Isomorphismus $K_1 \rightarrow K_2$, der mit der Inklusion von K verträglich ist.*

Beweis: Zornsches Lemma! Sei

$$M = \{(F, \tau) \mid K \subset F \subset K_1, \tau : F \rightarrow K_2, \tau|_K = \text{id}\}$$

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 $(K, \text{id}) \in M$. 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 7.8 gibt es dann eine Fortsetzung von τ_m nach $F_m(a)$. Dies ist ein Widerspruch zur Maximalität.

Behauptung. $\tau_m : K_1 \rightarrow K_2$ ist bijektiv.

Die Injektivität ist klar. Das Bild ist ein algebraischer Abschluss von K , also ganz K_2 . \square

Definition 7.12. *Sei L/K algebraisch. Dann heißt*

$$\text{Gal}(L/K) = \{\sigma : L \rightarrow L \mid \text{Körperisom. mit } \sigma|_K = \text{id}\}$$

Galoisgruppe von L/K :

Bemerkung. Offensichtlich ist es eine Gruppe.

Beispiel. $\text{Gal}(\mathbb{C}/\mathbb{R}) = \{\text{id}, \bar{\cdot}\}$ wobei $\bar{\cdot}$ die komplexe Konjugation ist, denn $\mathbb{C} = \mathbb{R}(i)$, $\sigma(i)$ ist Nullstelle von $X^2 + 1$, also $\sigma(i) = \pm i$. Also ist $\text{Gal}(\mathbb{C}/\mathbb{R}) \cong \mathbb{Z}/2$.

Lemma 7.13. *Sei $[L : K] = n$. Dann ist $|\text{Gal}(L/K)| \leq n$.*

Beweis: Da L/K endlich ist, ist jeder Körperhomomorphismus automatisch ein Isomorphismus (Dimensionen abzählen!). Sei $L = K(a_1, \dots, a_k)$. Nach Satz 7.8 und der nachfolgenden Bemerkung gilt

$$\begin{aligned} |\{\sigma_1 : K(a_1) \rightarrow L \mid \sigma_1|_K = \text{id}\}| &\leq [K(a_1) : K] \\ |\{\sigma_2 : K(a_1, a_2) \rightarrow L \mid \sigma_2|_{K(a_1)} = \sigma_1\}| &\leq [K(a_1, a_2) : K(a_1)] \end{aligned}$$

etc. Die Behauptung folgt aus der Gradformel. \square

Damit ist $\text{Gal}(L/K)$ eine *endliche Gruppe*. Wir werden Gruppentheorie zum Studium von L/K verwenden.

Definition 7.14. Eine endliche Körpererweiterung L/K heißt *galois*, wenn $|\text{Gal}(L/K)| = [L : K]$.

Beispiel. (i) $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}$. Das Minimalpolynom von $\sqrt[4]{2}$ über \mathbb{Q} ist $X^4 - 2$. Es hat über $\mathbb{Q}(\sqrt[4]{2})$ zwei Nullstellen. Also hat die Galoisgruppe nur 2 Elemente. Die Erweiterung ist nicht galois.

(ii) Sei $L = K(\sqrt{a})$ mit $\sqrt{a} \notin K$. Das Minimalpolynom ist also $X^2 - a$. Es zerfällt in L in die Linearfaktoren $(X - \sqrt{a})(X + \sqrt{a})$. In Charakteristik 2 ist aber $\sqrt{a} = -\sqrt{a}$. Die Galoisgruppe hat nur ein Element, die Erweiterung ist wieder nicht galois.

Beispiele

Definition 7.15. Sei L ein Körper. $\zeta \in L$ mit $\zeta^d = 1$ heißt *d-te Einheitswurzel*. Es heißt *primitive d-te Einheitswurzel*, falls ζ die Ordnung d (bezüglich der Multiplikation) hat. Es sei $\mu_d(L)$ die Gruppe der *d-ten Einheitswurzeln* von L .

Beispiel. $\zeta = \exp(2\pi i/d)$ ist primitive *d-te Einheitswurzel* in \mathbb{C} .

Lemma 7.16. Sei L ein Körper der Charakteristik 0. Dann ist $\mu_d(\mathbb{C}) \cong \mathbb{Z}/d$. Dabei werden die primitiven *d-ten Einheitswurzeln* abgebildet auf

$$(\mathbb{Z}/d)^* = \{x \in \mathbb{Z}/d \mid \text{es gibt } y \in \mathbb{Z}/d, xy = 1\}.$$

Beweis: Es genügt $L = \mathbb{Q}(\zeta)$ zu betrachten oder $L = \mathbb{C}$. Die Gleichung $X^d - 1$ hat die d Nullstellen $\exp(2\pi in/d)$ für $n \in \mathbb{Z}/d$. Dies liefert den Gruppenisomorphismus $\mu_d(\mathbb{C}) \cong \mathbb{Z}/d$. Die primitiven Einheitswurzeln entsprechen den Zahlen n , die teilerfremd zu d sind. Sei x eine solche Zahl. Nach Lemma 2.7 (i) gilt dann $1 \in x\mathbb{Z} + d\mathbb{Z}$, d.h. es gibt y, e mit

$$1 = xy + de \Rightarrow 1 = xy \in \mathbb{Z}/d.$$

\square

Satz 7.17 (Zyklotomische Erweiterungen). Sei K ein Körper der Charakteristik 0, ζ eine primitive d -te Einheitswurzel, $L = K(\zeta)/K$. Dann ist L der Zerfällungskörper von $X^d - 1$. Es gibt einen Isomorphismus

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

Insbesondere ist die Galoisgruppe abelsch.

Bemerkung. Sei ζ eine primitive d -te Einheitswurzel in \mathbb{C} . Dann gilt

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

(Beweis wahrscheinlich erst nächstes Semester aus Zeitmangel).

Beweis: Das Polynom $X^d - 1$ hat die Nullstellen $1, \zeta, \zeta^2, \dots, \zeta^{d-1}$. 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 $X^d - 1$. $\sigma \in \text{Gal}(K(\zeta)/K)$ ist eindeutig festgelegt durch $\sigma(\zeta) = \zeta^{n_\sigma}$. Die Abbildung

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

ist injektiv.

Behauptung. Dies ist ein Gruppenhomomorphismus.

Seien $\sigma, \tau \in \text{Gal}(L/K)$. 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 7.18 (Kummer-Erweiterungen). Sei K ein Körper der Charakteristik 0, der eine primitive d -te Einheitswurzel enthält. Sei $a \in K$, $L = K(\beta)$, wobei β eine Nullstelle von $X^d - a$ ist. Dann ist L Zerfällungskörper von $X^d - a$ und $\text{Gal}(L/K)$ 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 $\beta, \zeta\beta, \dots, \zeta^{d-1}\beta$. Nach Lemma 7.16 sind dies d verschiedene Zahlen, also zerfällt $X^d - a$ über L in Linearfaktoren. Wir betrachten

$$\text{Gal}(L/K) \rightarrow L^*, \quad \sigma \mapsto \frac{\sigma(\beta)}{\beta} .$$

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 $\text{Gal}(L/K)$ isomorph zu einer Untergruppe von $\mu_d(K) \cong \mathbb{Z}/d$. \square

Nicht alle Galoisgruppen sind abelsch!

Lemma 7.19. Sei $P = X^5 - 4X + 2$, L der Zerfällungskörper von P über \mathbb{Q} . Dann ist

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

Beweis: 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.

$$\begin{array}{c|c|c|c|c|c} x & -2 & -1 & 0 & 1 & 2 \\ \hline P(x) & -22 & 5 & 2 & -1 & 26 \end{array}$$

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

$$\text{Gal}(L/\mathbb{Q}) \times A \rightarrow A, (\sigma, \alpha) \mapsto \sigma(\alpha).$$

Sie definiert einen Gruppenhomomorphismus

$$\phi : \text{Gal}(L/\mathbb{Q}) \rightarrow S(A) \cong S_5.$$

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 $\sigma_2 \in \text{Gal}(L/\mathbb{Q})$. Daher enthält das Bild von ϕ ein Element der Ordnung 2.

Die Operation von $\text{Gal}(L/K)$ auf A ist transitiv. Nach der Bahnformel ist $5 = |A|$ ein Teiler von $|\text{Gal}(L/K)|$. Nach den Sylowsätzen hat $\text{Gal}(L/K)$ 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

$$\langle (1\ 2\ 3\ 4\ 5) \rangle = \{e, (1\ 2\ 3\ 4\ 5), (1\ 3\ 5\ 2\ 4)(1\ 4\ 2\ 5\ 3)(1\ 5\ 4\ 3\ 2)\} .$$

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 das Produkt von zwei ungeraden Permutationen gerade ist. Also ist $G \cap A_5 = A_5 \Rightarrow G = A_5$. G enthält jedoch die Transposition $(1\ 2)$. Es bleibt der Fall $|G| = 120 \Rightarrow G = S_5$. \square

Kapitel 8

Normale und separable Körpererweiterungen

Es gibt verschiedene äquivalente Charakterisierungen von galoisschen Körpererweiterungen. Diese wollen wir verstehen.

Normale Erweiterungen

Definition 8.1. 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. \bar{K}/K ist normal.

Lemma 8.2. 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 $L = K(\alpha_1, \dots, \alpha_n)$. 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 . \square

Tatsächlich gilt auch die Umkehrung!

Satz 8.3. 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 7.8 ein Isomorphismus

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

L ist der Zerfällungskörper von $P \in K(\alpha)[X]$. $L(\beta)$ ist der Zerfällungskörper von $\sigma(P) = P \in K(\beta)[X]$. Also existiert wie in 7.10 eine Fortsetzung

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

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

Korollar 8.4. *Sei L/K endlich. Dann existiert N/L endlich, so dass N/K normal ist.*

Beweis: $L = K(\alpha_1, \dots, \alpha_n)$, $P = \prod P_i$ Produkt der Minimalpolynome P_i der α_i . Sei N der Zerfällungskörper von P . \square

Definition 8.5. *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 8.6. *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 7.8 existiert ein Homomorphismus $\sigma : N \rightarrow N'$, der mit der Inklusion von L verträglich ist. Das Bild von σ ist normal über K , also ist σ surjektiv. \square

Andere Interpretation:

Sei L/K eine Körpererweiterung. Wir betrachten die Operation

$$\text{Gal}(L/K) \times L \rightarrow L.$$

Was sind die Bahnen?

Lemma 8.7. *Seien $\alpha, \alpha' \in L$ in derselben Bahn bezüglich der Operation der Galoisgruppe. Dann haben sie dasselbe Minimalpolynom über K .*

Beweis: Nach Voraussetzung existiert $\sigma : L \rightarrow L$ mit $\sigma(\alpha) = \alpha'$. Sei P das Minimalpolynom von α , P' das von α' . Nach 7.8 gilt

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

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

Definition 8.8. *Sei L/K eine Körpererweiterung. Zwei Elemente α, α' heißen konjugiert, wenn sie dasselbe Minimalpolynom haben.*

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

Satz 8.9. *Sei L/K normal. Dann stimmen die Konjugationsklassen mit den Bahnen überein.*

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

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

Separable Erweiterungen

Definition 8.10. *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 8.11. *Sei K ein Körper,*

$$P(X) = a_0 + a_1X + a_2X^2 + \cdots + a_nX^n \in K[X].$$

Die Ableitung von P ist

$$P'(X) = a_1 + 2a_2X + \cdots + na_nX^{n-1}.$$

Lemma 8.12 (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 $K[X] \rightarrow K[X]$, die die Leibniz-Regel erfüllt.

Beweis: $P = \sum_{i=0}^n a_i X^i$, $Q = \sum_{j=0}^n b_j X^j$, $\lambda \in K$.

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

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

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

Lemma 8.13. *Sei $P \in K[X]$. $\alpha \in \bar{K}$ 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 \bar{K} übereinstimmen. Sei $P(X) = (X - \alpha) \prod (X - \alpha_i)$ mit $\alpha, \alpha_i \in \bar{K}$. 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 $\alpha \in \bar{K}$, 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 8.14. *Sei $\text{Char } K = 0$. Dann sind alle Polynome in $K[X]$ separabel.*

Beweis: Offensichtlich $\deg P' = \deg P - 1$, also $P' \neq 0$ für irreduzible Polynome. □

Definition 8.15. *Ein Körper heißt vollkommen, wenn alle Polynome (und damit alle algebraischen Körpererweiterungen) separabel sind.*

Beispiel. Körper der Charakteristik 0, algebraisch abgeschlossene Körper.

Lemma 8.16. Sei $\text{Char } K = p > 0$, $P \in K[X]$. 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: $P(X) = \sum a_i X^i$, $P' = \sum i a_i X^{i-1}$. $P' = 0$ 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 $k \in \mathbb{N}$. \square

Satz 8.17. Sei K ein endlicher Körper. Dann ist K vollkommen.

Beweis: Sei $\phi : K \rightarrow K$ der Frobenius, $x \mapsto x^p$. Nach Satz 7.6 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

$$\left(\sum b_i X^i \right)^p = \sum b_i^p X^{ip} = P.$$

Insbesondere ist P nicht irreduzibel. Umgekehrt sind irreduzible Polynome separabel. \square

Andere Interpretation: Sei L/K normal und separabel. Wir betrachten die Operation:

$$\text{Gal}(L/K) \times L \rightarrow L$$

- (i) Die Bahn von $\alpha \in L$ hat $\deg \text{Min}(\alpha)$ viele Elemente.
- (ii) Falls $L = K(\alpha)$ galois.
- (iii) Ein Spezialfall: $\alpha \in L \setminus K \Rightarrow \deg \text{Min}(\alpha) > 1 \rightarrow$ kein Fixpunkt.

Galois-Erweiterungen

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

Definition 8.18. Sei L ein Körper, $G \subset \text{Aut}(L) = \{\sigma : L \rightarrow L \mid \text{Körperisom.}\}$. Dann heißt

$$L^G = \{\alpha \in L \mid \sigma(\alpha) = \alpha \text{ für alle } \sigma \in G\}$$

Fixkörper von G .

Bemerkung. Dies ist wirklich ein Körper.

Satz 8.19. Sei L/K endliche Körpererweiterung. Dann sind äquivalent.

- (i) L/K ist galois;
- (ii) $|\text{Gal}(L/K)| = [L : K]$;

(iii) L/K ist normal und separabel;

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

Beweis: (i) \Leftrightarrow (ii) war unsere Definition. Es gelte nun (iii). Wir wollen (iv) zeigen. Wie wir bereits überlegt haben hat die Bahn von α genau $\deg \text{Min}(\alpha)$ viele Elemente. Also ist α ein Fixpunkt, genau dann wenn $\deg \text{Min}(\alpha) = 1$, 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 $\text{Gal}(L/K)$. Wir betrachten

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

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

Wegen $K = L^{\text{Gal}(L/K)}$ genügt es zu zeigen, dass $P = \sigma(P)$ für alle $\sigma \in \text{Gal}(L/K)$. 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 7.13 ($|\text{Gal}(L/K)| \leq [L : K]$) 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. \square

Satz 8.20. Sei L ein Körper, $G \subset \text{Aut}(L)$ eine endliche Untergruppe, $K = L^G$. Dann gilt

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

Ende des Beweises von Satz 8.19. Es gelte (iii) oder äquivalent (iv), $K = L^{\text{Gal}(L/K)}$. Dann ist (ii) die Aussage des letzten Satzes.

Umgekehrt sei (iv) falsch. Wir haben $L \subset L^{\text{Gal}(L/K)} \subset K$, also nach der Gradformel und dem letzten Satz

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

Damit ist (ii) falsch. Dies beendet den Beweis von 8.19 \square

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

Der harmlos aussehende Satz 8.20 ist in Wirklichkeit der Kern des Hauptsatzes der Galoistheorie und alles andere als trivial!

Kapitel 9

Hauptsatz der Galoistheorie

Der wichtigste Teil des Beweises

Definition 9.1. Sei G eine Gruppe, L ein Körper. Ein Gruppenhomomorphismus

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

heißt Charakter.

Charaktere kann man als spezielle Elemente von

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

auffassen. Dies ist ein L -Vektorraum.

Satz 9.2. Seien $\chi_1, \dots, \chi_n : G \rightarrow L^*$ verschiedene Charaktere. Dann sind sie linear unabhängig als Elemente von $\text{Abb}(G, L)$.

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

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

d.h. für alle $g \in G$ gilt

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

In dieser Gleichung ersetzen wir g durch gh , also

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

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

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

Wir bilden die Differenz zur ersten Gleichung für g :

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

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. \square

Bemerkung. Näheres Hinsehen zeigt, dass wir Satz 9.2 doch nicht brauchen!

Beweis von 8.20. Sei $G = \{\sigma_1, \dots, \sigma_n\}$, $K = L^G$ und $B = \{b_1, \dots, b_r\}$ 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 $G \subset \text{Gal}(L/K)$ und daher

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

Artins Beweis mit Satz 9.2: Wir wenden den letzten Satz an auf die Gruppe L^* und die Charaktere $\sigma_i : L^* \rightarrow L^*$ für

$$\{\sigma_1, \dots, \sigma_n\} \in G \subset \text{Aut}(L).$$

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

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

Da wir mehr Unbekannte als Gleichungen haben, gibt es eine nicht-triviale Lösung (x_1, \dots, 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

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

Dies ist ein Widerspruch zur linearen Unabhängigkeit der σ_i .

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, \dots, 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 Voraussetzung 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 $\sigma_1 = \text{id}$). 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 . \square

Bemerkung. Artins Beweis kommt ohne Minimalpolynome und die Begriffe separabel, normal aus. Das ist also viel eleganter!

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

$$\begin{array}{ccc} \mathcal{G} & \xrightarrow{\kappa} & \mathcal{K} & \xrightarrow{\gamma} & \mathcal{G} \\ G & \mapsto & L^G & & \\ & & F & \mapsto & \text{Gal}(L/F) = \{\sigma \in \text{Gal}(L/K) \mid \sigma|_F = \text{id}\} \end{array}$$

Theorem 9.3 (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 $[L : F] = \text{Gal}(L/F)$.
Für jede Untergruppe $H \subset \text{Gal}(L/K)$ gilt

$$[L : L^H] = |H|, [L^H : K] = [\text{Gal}(L/K) : H] .$$

(iii) Für $L \supset F \supset K$ ist F/K normal (und dann auch galois), genau dann wenn $H = \text{Gal}(L/F)$ ein Normalteiler von $\text{Gal}(L/K)$ ist. In diesem Fall ist

$$\text{Gal}(F/K) \cong \text{Gal}(L/K) / \text{Gal}(L/F) .$$

Beweis: Wir betrachten $L \supset F_1 \supset F_2 \subset K$. Dann ist

$$\begin{aligned} \text{Gal}(L/F_2) &= \{ \sigma \in \text{Gal}(L/K) \mid \sigma|_{F_2} = \text{id} \} \supset \text{Gal}(L/F_1) = \\ & \{ \sigma \in \text{Gal}(L/K) \mid \sigma|_{F_1} = \text{id} \} . \end{aligned}$$

Umgekehrt seien $\text{Gal}(L/K) \supset H_1 \supset H_2$. Dann ist

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

Sei nun F ein Zwischenkörper. Nach Voraussetzung 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 8.19 ist also L/F galois und

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

Ebenfalls nach Satz 8.19 ist $[L : F] = |\text{Gal}(L/F)|$.

Sei H eine Untergruppe von $\text{Gal}(L/K)$. Nach Satz 8.20 ist $[L : L^H] = |H|$. Als Zwischenkörper ist L/L^H galois, also $[L : L^H] = \text{Gal}(L/L^H)$. Da $H \subset \text{Gal}(L/L^H)$, folgt Gleichheit. Mit anderen Worten,

$$\gamma\kappa(H) = \text{Gal}(L/L^H) = H .$$

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 $\sigma \in \text{Gal}(L/K)$ den Teilkörper F , da Elemente auf andere Nullstellen desselben Minimalpolynoms abgebildet werden. Wie erhalten eine Abbildung

$$\text{Gal}(L/K) \rightarrow \text{Gal}(F/K)$$

mit Kern $\text{Gal}(L/F)$. Sie ist surjektiv, denn L/K ist normal, also läßt sich jedes Element von $\text{Gal}(F/K)$ fortsetzen. Nach der Anzahlformel in (ii) ist F/K nun galois.

Sei umgekehrt $\text{Gal}(L/F)$ ein Normalteiler. Sei $\alpha \in F$, $\sigma \in \text{Gal}(L/K)$. Wir wollen zeigen, dass $\sigma(\alpha) \in F$, d.h. invariant unter $\text{Gal}(L/F)$. Sei also $\tau \in \text{Gal}(L/F)$. Nach Voraussetzung ist

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

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

Korollar 9.4. L/K galois. Dann gibt es nur endlich viele Zwischenkörper.

Beweis: Eine endliche Gruppe hat nur endlich viele Untergruppen. \square

Beispiel. Wir bestimmen die Teilkörper von $\mathbb{Q}(\sqrt[4]{2})$. Wir erraten: $\mathbb{Q}(\sqrt{2})$. Gibt es andere?

Sei K die normale Hülle von $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}$, also der Zerfällungskörper von $X^4 - 2$. Explizit ist $K = \mathbb{Q}(\sqrt[4]{2}, i)$. Er ist galois über \mathbb{Q} . Wir bestimmen die Galoisgruppe $G = \text{Gal}(K/\mathbb{Q})$. $\sigma : K \rightarrow K$ ist eindeutig durch die Werte auf $\sqrt[4]{2}$ und i bestimmt. Es gilt

$$\sigma(\sqrt[4]{2}) \in \{\pm\sqrt[4]{2}, \pm i\sqrt[4]{2}\}, \sigma(i) \in \{\pm i\}.$$

Die Galoisgruppe hat also 8 Elemente. Sei

$$\tau(\sqrt[4]{2}) = i\sqrt[4]{2}, \tau(i) = i.$$

Dieses Element hat die Ordnung 4, denn

$$\tau^2(\sqrt[4]{2}) = \tau(i\sqrt[4]{2}) = ii\sqrt[4]{2} = -\sqrt[4]{2}.$$

Sei ι die komplexe Konjugation, also

$$\iota(\sqrt[4]{2}) = \sqrt[4]{2}, \iota(i) = -i.$$

Dieses Element hat die Ordnung 2. Es gilt

$$G = \{\tau^i, \iota\tau^i \mid i = 0, 1, 2, 3\}.$$

Ist die Gruppe kommutativ?

$$\iota\tau(\sqrt[4]{2}) = \iota(i\sqrt[4]{2}) = -i\sqrt[4]{2}, \tau\iota(\sqrt[4]{2}) = \tau(\sqrt[4]{2}) = i\sqrt[4]{2}.$$

Nein, es gilt $\iota\tau = \tau^3\iota$. Damit haben wir die Gruppe in Erzeugern und Relationen vollständig beschrieben. Der Teilkörper $\mathbb{Q}(\sqrt[4]{2})$ ist der Fixkörper der Untergruppe $\{\text{id}, \iota\}$. Sie ist kein Normalteiler, wie es der Hauptsatz vorhersagt. Schließlich ist der Körper nicht normal über \mathbb{Q} . Teilkörper von $\mathbb{Q}(\sqrt[4]{2})$ entsprechen also Untergruppe von G , die ι enthalten. Sei H eine solche Untergruppe. Mit $\tau^3 = \tau^{-1}$ oder $\iota\tau$ oder $\iota\tau^3$ enthält die Gruppe auch τ und ist damit ganz G .

$$H = \{\text{id}, \iota, \tau^2, \iota\tau^2\}$$

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

Korollar 9.5 (Fundamentalsatz der Algebra). \mathbb{C} ist algebraisch abgeschlossen.

Beweis: Wir verwenden:

- (i) Sei $P \in \mathbb{R}[X]$ ungerade, dann hat P eine reelle Nullstelle. (Zwischenwertsatz)
- (ii) Sei $P \in \mathbb{C}[X]$ quadratisch, dann zerfällt P in Linearfaktoren. (Lösungsformel).

Sei nun L/\mathbb{C} endlich.

Behauptung. $L = \mathbb{C}$.

Ohne Einschränkung ist L/\mathbb{R} galois (normale Hülle). Sei $G = \text{Gal}(L/\mathbb{R})$, P eine 2-Sylowgruppe von G , $F = L^P$. Nach dem Hauptsatz der Galoistheorie ist $[F : \mathbb{R}] = [G : P]$, also ungerade. Sei $\alpha \in F$. Sein Minimalpolynom ist irreduzibel und ungerade, nach (i) also linear. Damit ist $F = \mathbb{R}$. 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 $G = P = \{\text{id}\}$ sein. \square

Korollar 9.6. Eine Zahl $z \in \mathbb{C}$ ist mit Zirkel und Linear aus $0, 1$ konstruierbar, genau dann wenn es in einer Galoiserweiterung K/\mathbb{Q} enthalten ist mit $[K : \mathbb{Q}]$ eine Potenz von 2.

Beweis: Wir haben bereits gesehen (Theorem 6.18), dass z konstruierbar ist, genau dann wenn es in einem Körper K_n liegt, für den es eine Kette quadratischer Erweiterungen gibt

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

Sei nun K wie im Korollar. Dann ist die Galoisgruppe $G = \text{Gal}(K/\mathbb{Q})$ eine 2-Gruppe. Nach dem Struktursatz für 2-Gruppen gibt es eine Kette von Normalteilern N_i mit Index 2^i . Deren Fixkörper sind die gesuchte Kette von Zwischenkörpern.

Umgekehrt existiere die Körperkette. Offensichtlich ist $[K_n : \mathbb{Q}] = 2^n$. Wenn K_n/\mathbb{Q} normal ist, so sind wir fertig. Allgemein sei K die normale Hülle von K_n/\mathbb{Q} .

Behauptung. $[K : K_n]$ ist eine Potenz von 2.

Sei L_i die normale Hülle von K_i/\mathbb{Q} . Wir argumentieren mit vollständiger Induktion. Sei $K_{i+1} = K_i(\alpha_i)$. Dabei sei $\alpha_i^2 = a_i \in K_i$. Wir setzen

$$P = \prod_{\sigma \in \text{Gal}(L_i/\mathbb{Q})} (X^2 - \sigma(a_i)) \in L_i[X] .$$

Das Polynom ist invariant unter der Operation von $\text{Gal}(L_i/\mathbb{Q})$, hat also Koeffizienten in $L_i^{\text{Gal}(L_i/\mathbb{Q})} = \mathbb{Q}$, denn der Körper ist galois über \mathbb{Q} . Sei L_i Zerfällungskörper von $R \in \mathbb{Q}[X]$. Wir wählen E_{i+1} als den Zerfällungskörper von RP . Er entsteht aus L_i durch Adjungieren von Wurzeln aus P , also durch Adjungieren von Quadratwurzeln. Daher ist $[E_{i+1} : L_i]$ eine Potenz von 2. Die normale Hülle L_{i+1} von K_{i+1}/\mathbb{Q} ist in E_{i+1} enthalten, also ist auch ihr Grad über \mathbb{Q} eine Potenz von 2. \square

Beispiel. Konstruktion des regelmäßigen 5-Ecks: Sei $\zeta = \exp(2\pi i/5)$. Das Minimalpolynom von ζ ist $X^4 + X^3 + X^2 + X + 1$. Die Erweiterung $\mathbb{Q}(\zeta)/\mathbb{Q}$ ist galois. Die Elemente der Galoisgruppe sind durch ein $i \in (\mathbb{Z}/5)^*$ bestimmt. Die Zuordnung ist $\sigma_i(\zeta) = \zeta^i$. Die Gruppe $(\mathbb{Z}/5)^*$ ist zyklisch mit Erzeuger 2, denn es ist $2^2 = 4, 2^3 = 8 = 3, 2^4 = 6 = 1$. Sie hat eine Untergruppe der Ordnung 2, erzeugt von $2^2 = 4$. Sei $H \subset \text{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$ die entsprechende Untergruppe, erzeugt von $\iota : \zeta \mapsto \zeta^4 = \zeta^{-1}$, also der komplexen Konjugation. Wir bestimmen $\mathbb{Q}(\zeta)^H$. Der Körper ist quadratisch über \mathbb{Q} . Er enthält $\alpha = \zeta + \zeta^{-1}$, den dieses Element ist invariant unter ι . Das Element ist nicht invariant unter $\zeta \mapsto \zeta^2$, denn sonst wäre

$$\zeta + \zeta^{-1} = \zeta^2 + \zeta^{-2} \Rightarrow \zeta^3 + \zeta = \zeta^4 + 1$$

Vergleich mit dem Minimalpolynom von ζ ergibt einen Widerspruch. Die gesuchte Kette von Körpern ist also

$$\mathbb{Q} \subset \mathbb{Q}(\alpha) \subset \mathbb{Q}(\zeta) .$$

Das Minimalpolynom von ζ über $\mathbb{Q}(\alpha)$ ist

$$(X - \zeta)(X - \iota(\zeta)) = X^2 - \alpha X + 1 .$$

Die Galoisgruppe von $\mathbb{Q}(\alpha)/\mathbb{Q}$ ist $\text{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})/H$. Sie enthält die Identität und die Restklasse von $\sigma : \zeta \mapsto \zeta^2$. Also ist das Minimalpolynom von α über \mathbb{Q}

$$(X - \alpha)(X - \sigma(\alpha)) = X^2 - (\zeta + \zeta^{-1} + \zeta^2 + \zeta^{-2}) + (\zeta + \zeta^{-1})(\zeta^2 + \zeta^{-2}) = X^2 + X - 1 .$$

Die Lösungsformel für quadratische Gleichungen sagt nun, welche Quadratwurzeln wir konstruieren müssen.

Dasselbe Verfahren funktioniert natürlich auch für das 17-Eck.

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 $\sqrt[n]{}$, so wie es für Gleichungen vom Grad 2, 3 und 4 funktiniert.

Definition 9.7. $\alpha \in \overline{\mathbb{Q}}$ kann durch Radikale ausgedrückt werden, wenn es in einem Körper $K \subset \overline{\mathbb{Q}}$ liegt mit

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

wobei $K_i = K_{i-1}(\sqrt[n_i]{a_i})$ für ein $a_i \in K_i$.

Ein Körper heißt durch Radikale auflösbar, wenn er in einem solchen K_n enthalten ist.

Ein Polynom heißt durch Radikale auflösbar, wenn alle seine Wurzeln durch Radikale ausgedrückt werden können, d.h. wenn sein Zerfällungskörper durch Radikale auflösbar ist.

Wir wollen das Problem mit Galoistheorie angehen. Wir haben gesehen (zyklotomische Erweiterungen Satz 7.17 und Kummererweiterungen Satz 7.18), dass Wurzelerweiterungen abelsche Galoisgruppen haben.

Definition 9.8. 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 9.9. 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

$$H_{i+1}/H_i = H \cap G_{i+1}/H \cap G_i \rightarrow G_{i+1}/G_i$$

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 $G \rightarrow H$. Nach dem Noetherschen Isomorphiesatz gilt $H_i = G_i/G_i \cap N \cong G_i N/N$. Wieder ist H_i ein Normalteiler in H_{i+1} . Die Projektion

$$G_{i+1}/G_i \rightarrow H_{i+1}/H_i$$

ist surjektiv. Als Bild einer abelschen Gruppe ist H_{i+1}/H_i abelsch. Damit ist H auflösbar. \square

Theorem 9.10. Sei K/\mathbb{Q} eine endliche Erweiterung mit normaler Hülle L . Dann sind äquivalent:

- (i) K ist durch Radikale auflösbar.
- (ii) $\text{Gal}(L/\mathbb{Q})$ 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 Erweiterung endliche 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, K_{i-1} normal über \mathbb{Q} ist.

Es ist $K_i = K_{i-1}(\alpha)$, das die Gleichung $X^{n_i} - a_i$, $a_i \in K_{i-1}$ erfüllt. Wir betrachten das Polynom

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

Das Polynom ist invariant unter der Operation von $\text{Gal}(K_i/\mathbb{Q})$ und die Erweiterung ist galois, also gilt $P \in \mathbb{Q}[X]$. Sei K_{i-1} Zerfällungskörper von R . 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 Wurzeln, nämlich $\zeta = \sqrt[N]{1}$. Weiterhin gilt $K \subset L_n$. Die Erweiterungen L_{i+1}/L_i sind nun Kummererweiterungen wie in Satz 7.18, 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 $H_i = \text{Gal}(L_n/L_i)$ die Folge von Untergruppen zur Körperkette. Nach dem Hauptsatz der Galoistheorie ist H_{i+1} ein Normalteiler von H_i , und es gilt

$$\text{Gal}(L_{i+1}/L_i) \cong H_i/H_{i+1}.$$

Damit ist $\text{Gal}(L_n/\mathbb{Q})$ auflösbar. Als Quotient ist dann auch $\text{Gal}(L/\mathbb{Q})$ auflösbar. \square

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

Satz 9.11. Sei $P = X^5 - 4X + 2$. Dieses P ist nicht durch Radikale auflösbar.

Beweis: Der Zerfällungskörper von P hat nach Lemma 7.19 Galoisgruppe S_5 . Nach dem Teil des Theorems, den wir gezeigt haben, impliziert die Auflösbarkeit von P die Auflösbarkeit von S_5 . Mit S_5 wäre auch die Untergruppe A_5 auflösbar. Diese ist aber einfach und nichtabelsch. Sie hat keine abelschen Quotienten, ist also keineswegs auflösbar. \square

Endliche Körper und Einheitswurzeln

Sei p eine Primzahl. Wir betrachten endliche Körper der Charakteristik p .

Satz 9.12. Für jedes $n \geq 1$ enthält $\overline{\mathbb{F}_p}$ genau einen Teilkörper \mathbb{F}_{p^n} mit p^n Elementen. Die Körpererweiterung $\mathbb{F}_{p^n}/\mathbb{F}_p$ ist galois mit zyklischer Galoisgruppe erzeugt vom Frobenius ϕ mit $\phi(x) = x^p$.

Beweis: Sei \mathbb{F} ein Teilkörper mit p^n Elementen. Alle Elemente von \mathbb{F}^* erfüllen das separable Polynom $X^{p^n-1} - 1$, da \mathbb{F}^* eine Gruppe mit $p^n - 1$ Elementen

ist. Über \mathbb{F} zerfällt P in Linearfaktoren, über einem kleineren Körper nicht, da P keine doppelten Nullstellen hat. Damit ist der einzige Kandidat für \mathbb{F} die Menge der Nullstellen von P zusammen mit 0, also die Menge der Nullstellen von $X^{p^n} - X$. Dies ist die Menge der Fixpunkte von $\phi_n \in \text{Gal}(\overline{\mathbb{F}_p}/\mathbb{F}_p)$ mit $\phi_n(x) = x^{p^n}$. Als Fixpunkte eines Körperhomomorphismus bilden sie einen Körper. Dies zeigt die Existenz von \mathbb{F} .

Da \mathbb{F}_p vollkommen ist, ist \mathbb{F}_{p^n} als Zerfällungskörper galois über \mathbb{F}_p . Die Galoisgruppe hat n Elemente. Wir betrachten die Untergruppe, die vom Frobenius ϕ erzeugt wird. Sei m die Ordnung von ϕ . Dann gilt

$$\phi^m(x) = x^{p^m} = x \text{ für alle } x \in \mathbb{F}_{p^n} .$$

Das Polynom $X^{p^m} - X$ ist separabel, hat also höchstens p^m Nullstellen. Damit ist $m \geq n$. Also ist die Ordnung n . Die Galoisgruppe wird von ϕ erzeugt. \square

Bemerkung. \mathbb{F}_{p^n} und \mathbb{Z}/p^n haben nicht das geringste miteinander zu tun!!!

Definition 9.13. Sei ζ eine primitive d -te Einheitswurzel in $\overline{\mathbb{Q}}$, $\Phi_d \in \mathbb{Z}[X]$ ihr normiertes Minimalpolynom und $\phi(d) = \deg \Phi(d)$.

Satz 9.14. Alle primitiven d -ten Einheitswurzeln in $\overline{\mathbb{Q}}$ sind Nullstellen von Φ_d . Es gilt

$$\phi(d) = |(\mathbb{Z}/d)^*| , \text{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q}) \cong (\mathbb{Z}/d)^* .$$

Beweis: Wir wissen aus Kapitel 7, dass es 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 7.17 ist $\text{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$ 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 (Satz von Gauß 5.21). 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 . \square

Mit anderen Worten: $X^d - 1$ hat die nur die offensichtlichen Teiler.

Beispiel. $d = 12$. Die Teiler von 12 sind 1, 2, 3, 4, 6. Die teilerfremden Zahlen sind 1, 5, 7, 11. Also hat Φ_{12} den Grad 4. Es gilt

$$\begin{aligned} X^{12} - 1 &= \Phi_{12}\Phi_6\Phi_4\Phi_3\Phi_2\Phi_1, \\ (X^6 - 1) &= \Phi_6\Phi_3\Phi_2\Phi_1, (X^{12} - 1)/(X^6 - 1) = \Phi_{12}\Phi_4 = X^6 + 1, \\ (X^4 - 1) &= \Phi_4\Phi_2\Phi_1, \Phi_4 = (X^4 - 1)/(X^2 - 1) = X^2 + 1 \\ \Phi_{12} &= (X^6 + 1)/(X^2 + 1) = X^4 - X^2 + 1 \end{aligned}$$

Lemma 9.15. *Seien n, m teilerfremd. Dann gilt $\phi(nm) = \phi(n)\phi(m)$. Sei $n = p^k$ eine Primzahlpotenz. Dann gilt $\phi(n) = (p - 1)p^{k-1}$.*

Beweis: Nach dem chinesischen Restsatz gilt

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

Die Abbildung ist ein Ringhomomorphismus. Ein Element in \mathbb{Z}/nm ist invertierbar bezüglich der Multiplikation, genau dann wenn es invertierbar ist modulo n und m .

$$(\mathbb{Z}/nm)^* \cong (\mathbb{Z}/n)^* \times (\mathbb{Z}/m)^*.$$

In \mathbb{Z}/p^k sind genau die Vielfachen von p nicht teilerfremd zu p^k . Es gilt

$$\phi(p^k) = p^k - p^{k-1} = (p - 1)p^{k-1}.$$

\square

Korollar 9.16 (vergleiche Satz 6.21). *Das regelmäßige n -Eck ist genau dann mit Zirkel und Lineal konstruierbar, wenn $n = 2^m p_1 \dots p_i$ mit Fermatschen Primzahlen p_j ist.*

Beweis: Sei ζ eine primitive n -te Einheitswurzel. Nach Korollar 9.6 ist ζ genau dann mit Zirkel und Lineal konstruierbar, wenn $[\mathbb{Q}(\zeta) : \mathbb{Q}] = \phi(n)$ eine Potenz von 2 ist. Sei $n = 2^m p_1^{m_1} \dots p_i^{m_i}$ die Primfaktorzerlegung von n . Nach dem Lemma ist

$$\phi(n) = 2^{m-1} p_1 (p_1^{m_1-1}) \dots p_i (p_i^{m_i-1}).$$

In der Primfaktorzerlegung von n darf also keine Primzahl ungleich 2 mit höherer Multiplizität vorkommen. Für die vorkommenden p_j muss $p_j - 1$ eine Potenz von 2 sein. Wie in Kapitel 6 sind dies genau die Fermatschen Primzahlen. \square

Kapitel 10

Ausblicke

Natürlich sind immer noch viele Fragen zur Galoistheorie offen.

Das inverse Problem der Galoistheorie

Vermutung 10.1. *Jede endliche Gruppe kommt als Galoisgruppe einer endlichen Erweiterung über \mathbb{Q} vor.*

Es ist recht einfach, Galoiserweiterungen K/\mathbb{Q} mit Galoisgruppe S_n zu konstruieren, siehe unser Beispiel mit S_5 . Jede endliche Gruppe G ist Untergruppe einer S_n , also taucht nach dem Hauptsatz jede Gruppe auf als Galoisgruppe eines $\text{Gal}(K/F)$, K, F beide endlich über \mathbb{Q} . Für die eigentliche Frage hilft es nicht weiter!

Lemma 10.2. *Es gibt eine Galoiserweiterung F/\mathbb{Q} mit $\text{Gal}(F/\mathbb{Q}) \cong \mathbb{Z}/p^n$.*

Beweis: Sei ζ_{p^n} eine primitive p^n -te Einheitswurzel. Wir wissen, dass

$$\text{Gal}(\mathbb{Q}(\zeta_{p^n})/\mathbb{Q}) \cong (\mathbb{Z}/p^n)^* .$$

Der Kern K der Abbildung $(\mathbb{Z}/p^n)^* \rightarrow (\mathbb{Z}/p)^*$ hat p^{n-1} Elemente. Tatsächlich ist er zyklisch (ohne Beweis). Da p^n und $(p-1)$ teilerfremd sind, gilt nach dem Elementarteilersatz $(\mathbb{Z}/p^n)^* \cong (\mathbb{Z}/p)^* \times p^{n-1}$. Sei F der Fixkörper der Untergruppe $(\mathbb{Z}/p)^*$. Nach dem Hauptsatz der Galoistheorie hat er Galoisgruppe \mathbb{Z}/p^{n-1} . \square

Wie steht es mit $G = \mathbb{Z}/p \times \mathbb{Z}/p$?

Theorem 10.3 (Kronecker-Weber). *Sei F/\mathbb{Q} galois mit abelscher Galoisgruppe. Dann ist $F \subset \mathbb{Q}(\zeta_n)$ für eine primitive n -te Einheitswurzel.*

Wir müssen also unter Teilkörpern der $\mathbb{Q}(\zeta_n)$ suchen. Potenzen von p reichen nicht, das hat der letzte Beweis gezeigt. Wo kann ein zweiter Faktor p herkommen? Wenn p ein Teiler von $p' - 1$ ist, wobei p' eine andere Primzahl ist, dann

hat $\text{Gal}(\mathbb{Q}(\zeta_{p'})/\mathbb{Q}) \cong (\mathbb{Z}/p')^*$ eine Untergruppe mit Index p' (Elementarteilersatz, Theorie der abelschen p -Gruppen). In $\mathbb{Q}(\zeta_{pp'})$ gibt es dann den gesuchten Körper.

Es bleibt die Frage: Gibt es eine Primzahl, die 1 ist modulo p ?

Theorem 10.4 (Dirichletscher Dichtesatz). *Es gibt unendlich viele Primzahlen, die 1 modulo p sind.*

Tatsächlich haben wir gezeigt:

Satz 10.5. *Es gibt eine Galoisweiterung F/\mathbb{Q} mit $\text{Gal}(F/\mathbb{Q}) \cong (\mathbb{Z}/p)^n$.*

Beweis: Wir finden F als Teilkörper von $\mathbb{Q}(\zeta_{p_1 \dots p_n})$, wobei die p_i alle Primzahlen sind, die 1 modulo p sind. \square

Mit ähnlichen Argumenten findet man alle endlichen abelschen Gruppen. Allgemein ist das inverse Problem der Galoistheorie ein Forschungsgegenstand. Meines Wissens ist es über \mathbb{Q} noch nicht für alle einfachen Gruppen gelöst (ohne Gewähr).

Das Langlands-Programm

Sei K ein globaler Körper, d.h. eine endliche Erweiterung von \mathbb{Q} oder $\mathbb{F}_p(X)$. Die Galoisweiterungen von K mit abelscher Galoisgruppe sind gut verstanden. Dies ist Inhalt der *Klassenkörpertheorie*. Man kann sie auffassen als Beschreibungen aller Gruppenhomomorphismen

$$\text{Gal}(\overline{K}/K) \rightarrow \text{Gl}_1(\mathbb{R}) = \mathbb{R}^* ,$$

die über einen endlichen Quotienten faktorisieren. Sie entsprechen gewissen Darstellungen einer Gruppe $\text{Gl}_1(\mathbb{A})$ wobei \mathbb{A} der Ring der Adele ist.

Vermutung 10.6 (Langlands). *Die Gruppenhomomorphismen*

$$\text{Gal}(\overline{K}/K) \rightarrow \text{Gl}_n(\mathbb{R})$$

entsprechen eindeutig gewissen Darstellungen von $\text{Gl}_n(\mathbb{A})$.

In Wirklichkeit ist die Vermutung natürlich sehr viel präziser. Im Fall von $K = \mathbb{Q}$ ist die Vermutung weit offen. Ein Spezialfall für $n = 2$ ist die Shimura-Taniyama Vermutung, die Wiles et.al. vor einigen Jahren bewies.

Theorem 10.7 (Drinfeld, Lafforgue). *Die Langlandsvermutung gilt im Fall von Erweiterungen von $\mathbb{F}_p(X)$.*

Der Beweis brachte Drinfeld 1990 (Fall $n = 2$) 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.

Milnor-Vermutung

Die zweite Fields-Medaille ging 2002 an Voevodsky für den Beweis der Milnor-Vermutung.

Theorem 10.8 (Voevodsky, Milnor-Vermutung). *Sei K ein Körper. Dann ist die natürliche Abbildung*

$$K_M^*(K)/2 \rightarrow H^*(K, \mathbb{Z}/2)$$

ein Isomorphismus.

Hierin ist $K_M^*(K)$ *Milnor K -Theorie*. Man kann die abelsche Gruppe explizit mit Erzeugern und Relationen definieren: Erzeuger sind Ausdrücke der Form $\{a_1, a_2, \dots, a_n\}$ mit $a_i \in K^*$, $n \in \mathbb{N}_0$. Es gelten die Rechenregeln

$$\begin{aligned} \{a_1, a_2, \dots, a_i, \dots, a_n\} + \{a_1, a_2, \dots, b_i, \dots, a_n\} &= \{a_1, a_2, \dots, a_i b_i, \dots, a_n\}, \\ \{a_1, a_2, \dots, a_n\} &= 0, \text{ falls } a_i + a_j = 1 \text{ für ein Paar von Indices.} \end{aligned}$$

Auf der rechten Seite steht *Galoiskohomologie*, die hier nicht definiert werden soll. Sie hängt nur von $\text{Gal}(\overline{K}/K)$ ab.

Die entsprechende Vermutung für beliebige Zahlen n statt 2 steht wohl kurz vor einem Beweis.

Algebra II

Es wird wesentlich prosaischer zugehen:

- (i) Noch etwas Galoistheorie, insbesondere für die Rückrichtung von Theorem 9.10.
- (ii) Ringe und Moduln. Moduln über Ringen entsprechen Vektorräumen über Körpern. Insbesondere werden wir den Elementarteilersatz zeigen.
- (iii) Homologische Algebra. Das ist die Theorie, die benötigt wird, um systematisch Invarianten zu produzieren und mit ihnen zu rechnen. Sie entstand beim Studium von topologischen Räumen, ist aber in vielen Zusammenhängen anwendbar. Ein Beispiel ist Galoiskohomologie, siehe 10.8.

Was sonst noch gut für die Allgemeinbildung wäre: nichtkommutative Theorie!

- Darstellungstheorie von Gruppen, also der Abbildungen $G \rightarrow \text{Gl}(V)$ wobei V ein Vektorraum ist. Etwas eleganter, aber eigentlich das Gleiche: die Theorie der halbeinfachen Algebren.
- Klassifikation der Lie-Algebren: Lie-Algebren sind keine Ringe, statt des Assoziativgesetzes erfüllen sie die Jacobi-Regel. Sie tauchen auf als Tangentialräume von Liegruppen (Gruppen, die gleichzeitig Mannigfaltigkeiten sind wie $\text{Gl}_n(\mathbb{R})$).
- Theorie der quadratischen Formen, also der bilinearen Abbildungen $V \times V \rightarrow K$, (V ein K -Vektorraum).

All diese Themen sind im Buch von Lang behandelt.

Zusammenfassung

Diese Vorlesung hatte - hinter all den Definitionen und Lemmata - zwei Themen:

- Operationen von Gruppen: dies führte zum Beweis der beiden tiefsten Sätze der Vorlesung, nämlich der Sylowsätze und des Hauptsatzes der Galoistheorie;
- Invarianten: die Ordnung einer Gruppe, eines Elementes, der Grad einer Körpererweiterung, die Galoisgruppe einer Erweiterung. Dies sind Beispiele eines der erfolgreichsten Prinzips der Mathematik überhaupt!

Inhaltsverzeichnis

0	Einleitung	1
1	Grundbegriffe der Gruppentheorie	5
2	Wichtige Beispiele von Gruppen	15
3	Operationen von Gruppen auf Mengen	25
4	Die Sylow-Sätze	31
5	Grundbegriffe der Ringtheorie	37
6	Grundbegriffe der Körpertheorie	49
7	Körperhomomorphismen	61
8	Norm. und sep. Körpererweiterungen	71
9	Hauptsatz der Galoistheorie	77
10	Ausblicke	89