Elemente der Algebra

Rainer Vogt

Wintersemester 2007/2008

Inhalt der Veranstaltung ist die Behandlung schulrelevanter Konzepte der Algebra vom höheren Standpunkt aus mit dem Ziel, ein kritisches Verständnis für Eigenschaften der ganzen, rationalen und reellen Zahlen zu vermitteln, die von vielen Lehrern als selbstverständlich und Gottgegeben angesehen werden. Darüber hinaus wollen wir soweit über den Schulstoff hinausgehen, dass ein kleiner Eindruck für die Dinge entsteht, mit der sich moderne Mathematik beschäftigt.

Wir setzen für diese Vorlesung die Inhalte des Grundkurses Mathematik voraus. Insbesondere wird auf das Kapitel über algebraische Strukturen zurückgegriffen. Hörer sollten auch mit Äquivalenzrelationen und den daraus abgeleiteten Äquivalenzklassen vertraut sein.

Inhaltsverzeichnis

I Monoide und Gruppen 4

1 Die Axiome 4

2 Unterstrukturen 9

3 Homomorphismen 13

4 Faktorgruppen 18

5 Produkte 24

6 Diedergruppen 28

7 Permutationsgruppen 32

8 Operationen von Gruppen auf Mengen 38

9 p-Gruppen und die Sylowsätze 42

II Ringe und Körper 48

10 Grundlagen 48

11 Teilerlehre in Ringen 53

12 Ringe in quadratischen Erweiterungen 60

13 Polynomringe 67

14 Algebraische Körpererweiterungen 72

III Konstruktionen mit Zirkel und Lineal 77

15 Unterkörper konstruierbarer reeller Zahlen 77

16 Die klassischen Probleme **82**

Teil I
Monoide und Gruppen

1 Die Axiome

Wir rekapitulieren kurz die Axiomensysteme für Monoide und Gruppen und direkte elementare Folgerungen aus diesen.

1.1 Definition: Ein *Monoid* ist eine Menge M mit einer Verknüpfung

$$M \times M \to M, \quad (x, y) \mapsto x * y,$$

so dass folgende Axiome erfüllt sind:

(A) Die Verknüpfung ist assoziativ: Für alle $x, y, z \in M$ gilt

$$(x * y) * z = x * (y * z)$$

(N) Die Verknüpfung besitzt ein neutrales Element: Es gibt ein Element $e \in M$, so dass für alle $x \in M$ gilt

$$e * x = x * e = x.$$

Eine *Gruppe* ist ein Monoid, der folgendes weitere Axiom erfüllt:

(I) Jedes $x \in M$ besitzt ein inverses Element $\overline{x}$, so dass

$$x * \overline{x} = e = \overline{x} * x.$$

Erfüllt ein Monoid oder eine Gruppe das Kommutativgesetz

(K) für alle x, y aus M gilt $x * y = y * x$

spricht man von einem (einer) *abelschen* oder *kommutativen* Monoid (Gruppe).

1.2 Erste Beispiele

(1) $(\mathbb{N}_0, +)$, $(\mathbb{N}, \cdot)$, $(\mathbb{Z}, \cdot)$ sind kommutative Monoide.

(2) $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{Q}^*, \cdot)$, $(\mathbb{R}^*, \cdot)$ sind kommutative Gruppen. Hier ist $\mathbb{Q}^* = \mathbb{Q}\backslash\{0\}$ und $\mathbb{R}^* = \mathbb{R}\backslash\{0\}$.

(3) Ist M eine beliebige Menge, dann ist die Menge $\mathrm{Abb}(M, M)$ aller Abbildungen $M \to M$ unter der Komposition ein Monoid. Hat M mindestens zwei Elemente, ist $(\mathrm{Abb}(M, M), \circ)$ nicht kommutativ.

(4) Ist $\mathcal{P}(M)$ die Potenzmenge der Menge M, d.h. die Menge aller Teilmengen von M, dann sind $(\mathcal{P}(M), \cap)$ und $(\mathcal{P}(M), \cup)$ kommutative Monide, und $((\mathcal{P}(M), \triangle)$ mit $A \triangle B = (A\backslash B) \cup (B\backslash A)$ eine kommutative Gruppe.

(5) $S^1 = \{(\cos\alpha, \sin\alpha) \in \mathbb{R}^2; \alpha \in \mathbb{R}\} \subset \mathbb{R}^2$ ist der Einheitskreis. Dann ist $(S^1, *)$ mit $(\cos\alpha, \sin\alpha) * (\cos\beta, \sin\beta) = (\cos(\alpha+\beta), \sin(\alpha+\beta))$ eine kommutative Gruppe.

Wir wollen uns jetzt mit den Axiomen befassen. Den Beweis der meisten elementaren Resultate überlassen wir dem Leser. Viele davon findet man auch im Grundkurs.

Das Assoziativgesetz (A) bedeutet, dass das "Produkt" von n Elementen

$$a_1 * a_2 * \ldots * a_n$$

unabhängig von der Klammerung ist. Z.B. kann man ein Produkt aus vier Elementen auf fünf verschiedene Arten klammern, und aus Axiom (A) folgt, dass alle fünf Produkte gleich sind.

$$\begin{aligned}(a_1 * a_2) * (a_3 * a_4) &= a_1 * [a_2 * (a_3 * a_4)] = a_1 * [(a_2 * a_3) * a_4] \\ &= [a_1 * (a_2 * a_3)] * a_4 = [(a_1 * a_2) * a_3] * a_4\end{aligned}$$

Bei jedem Gleichheitszeichen wurde (A) einmal angewandt.

Dieses Beispiel zeigt aber auch, dass hier etwas zu beweisen ist. Denn um von $(a_1 * a_2) * (a_3 * a_4)$ nach $a_1 * [(a_2 * a_3) * a_4]$ zu gelangen, muß (A) zweimal angewandt werden, und im allgemeinen Fall ist das noch erheblich komplizierter.

1.3 Übung Allgemeines Assoziativgesetz: Genügt die Verknüpfung $*$ auf M dem Axiom (A), dann ist das "Produkt"

$$a_1 * a_2 * \ldots * a_n$$

unabhängig von der Klammerung.

Aufgabe: Beweisen Sie 1.3.

Hinweis: Definieren Sie zunächst induktiv das "Standardprodukt" $\prod_{i=1}^{n} a_i$ durch:

$$\prod_{i=1}^{1} a_i = a_1 \text{ und } \prod_{i=1}^{n+1} a_i = \left(\prod_{i=1}^{n} a_i\right) * a_{n+1}, \quad n \geq 1$$

(d.h. das Standardprodukt klammert von links). Zeigen Sie:

(1) $(\prod_{i=1}^{n} a_i) * \left(\prod_{j=1}^{m} a_{n+j}\right) = \prod_{i=1}^{m+n} a_i$ (Induktion nach m)

(2) Ist $x = a_1 * \ldots * a_n$ mit beliebiger Klammerung, dann ist $x = \prod_{i=1}^{n} a_i$ (Induktion nach n).

Da das Produkt unabhängig von der Klammerung ist, werden wir in Zukunft weitgehend auf Klammern verzichten.

Beim allgemeinen Kommutativgesetz muß man entsprechend vorgehen. Wir werden später darauf eingehen.

1.4 Definition: Sei $(M, *)$ ein Monoid mit neutralem Element e, und sei $x \in M$. Ein Element $y \in M$ heißt *Linksinverses* von x, wenn $y * x = e$, und *Rechtsinverses* von x, wenn $x * y = e$

1.5 Bemerkung: Ein Element eines Monids kann mehrere verschiedene Linksinverse oder Rechtsinverse haben.

1.6 Beispiel: Sei $f \in (\mathrm{Abb}(\mathbb{N}_0, \mathbb{N}_0), \circ)$ definiert durch $f(n) = 2n$ und $g_k : \mathbb{N}_0 \to \mathbb{N}_0$ mit $k \in \mathbb{N}_0$ durch

$$g_k(n) = \begin{cases} \dfrac{n}{2}, & \text{falls } n \text{ gerade ist} \\ k, & \text{falls } n \text{ ungerade ist} \end{cases}$$

Dann gilt $g_k \circ f = id$. Also ist jedes g_k linkinvers zu f.

Aber es gilt

1.7 Übung: Sei $(M, *)$ ein Monoid. Zeigen Sie:

(i) Das neutrale Element von M ist eindeutig bestimmt. D.h. sind e und e' neutrale Elemente, dann ist $e = e'$.

(ii) Besitzt ein Element $x \in M$ sowohl linkinverse als auch rechtsinverse Elemente, dann sind diese alle gleich. Insbesondere besitzt x genau ein inverses Element. Wir bezeichnen dieses mit x^{-1}.

(iii) Ist $(M, *)$ eine Gruppe, dann ist das inverse von $x \in M$ eindeutig bestimmt, bezeichnet mit x^{-1}.

Für den Nachweis, dass ein gegebenes Verknüpfungsgebilde eine Gruppe ist, braucht man nicht die Axiome in voller Stärke nachzuweisen.

1.8 Satz: Für eine Menge G mit assoziativer Verknüpfung $*$ sind folgende Aussagen äquivalent.

(i) G ist eine Gruppe.

(ii) G besitzt ein linksneutrales Element e_l, d.h. für alle $x \in G$ gilt $e_l * x = x$; und jedes x aus G besitzt ein linksinverses, d.h. ein Element $\overline{x}$, so dass $\overline{x} * x = e_l$.

(iii) G besitzt ein rechtsneutrales Element e_r und jedes $x \in G$ besitzt ein Rechtinverses.

(iv) Für alle $a, b \in G$ gibt es Elemente x und y in G, so dass

$$x * a = b \text{ und } a * y = b.$$

Beweis: (1) $\Rightarrow$ (2) und (1) $\Rightarrow$ (3) ist klar.
(1) $\Rightarrow$ (4): Nehme $x = b * a^{-1}$ und $y = a^{-1} * b$.
(2) $\Rightarrow$ (1): Sei $\overline{x}$ ein Linksinverses von x und $\overline{\overline{x}}$ ein Linksinverses von $\overline{x}$. Dann gilt

$$\begin{aligned} x * \overline{x} &= e_l * x * \overline{x} = (\overline{\overline{x}} * \overline{x}) * x * \overline{x} = \overline{\overline{x}} * (\overline{x} * x) * \overline{x} = \overline{\overline{x}} * (e * \overline{x}) \\ &= \overline{\overline{x}} * \overline{x} = e_l \end{aligned}$$

Also ist $\overline{x}$ auch rechtsinvers. Weiter gilt

$$x * e_l = x * (\overline{x} * x) = (x * \overline{x}) * x = e_l * x = x$$

Der Beweis (3) $\Rightarrow$ (1) ist analog.
(4) $\Rightarrow$ (2): Nach Voraussetzung gibt es zu $a \in G$ ein Element e_a, so dass $e_a * a = a$. Wir zeigen, dass e_a linksneutral ist: Sei also $b \in G$ beliebig. Dann gibt es ein $y \in G$, so dass $a * y = b$. Es folgt

$$e_a * b = e_a * a * y = a * y = b.$$

Also ist e_a linkneutral.
Weiter gibt es nach Voraussetzung zu jedem $b \in G$ ein x, so dass $x * b = e_a$. Also ist x linksinvers zu b. $\square$

1.9 Beispiel: Sei $M = \{e, a\}$ mit folgender Verknüpfung

$$\begin{array}{lll} e * e = e & , & a * e = e \\ e * a = a & , & a * a = a \end{array}$$

Man prüft leicht nach, dass $*$ assoziativ ist. Außerdem ist e linksneutral und $a * e = e$, $e * e = e$, d.h. e ist rechtsinvers zu a und e. Aber M ist *keine* Gruppe, denn e ist nicht rechtsneutral.

Zum Schluss dieses einführenden Paragraphen gehen wir auf eine Struktur ein, die zwischen Monoid- und Gruppenstruktur liegt.

1.10 Definition: Ein Monoid $(M, *)$ erfüllt die *Kürzungsbedingung*, wenn aus jeder Gleichung $x * a = x * b$ und jeder Gleichung $a * y = b * y$ folgt, dass $a = b$.

1.11 Satz: Ein endlicher Monoid M, der die Kürzungsbedingung erfüllt, ist eine Gruppe.

Beweis: Es genügt zu zeigen, dass jedes $a \in M$ ein Linksinverses hat. Die Abbildung

$$f : M \to M, \quad x \mapsto x * a$$

ist injektiv. Denn ist $f(x) = f(y)$, also $x * a = y * a$, dann folgt aus der Kürzungsbedingung $x = y$

Da M endlich ist, ist f auch surjektiv. Folglich gibt es ein $x \in M$, so dass $f(x) = e$, also $x * a = e$. □

2 Unterstrukturen

Betrachtet man Mengen mit zusätzlicher Struktur, stellt sich die Frage, auf welche Teilmengen sich die Struktur vererben lässt.

2.1 Definition: (1) Sei $(M, *, e)$ ein Monoid. Eine Teilmenge $A \subset M$ heißt *Untermonid*, wenn $*$ eine Monoidstruktur auf A definiert mit e als neutralem Element. D.h.

(i) für alle $a, b \in A$ gilt $a * b \in A$,

(ii) $e \in A$.

(2) Sei $(G, *, e)$ eine Gruppe. Eine Teilmenge $A \subset M$ heißt *Untergruppe*, wir schreiben $H < G$, wenn $*$ eine Gruppenstruktur auf H definiert mit e als neutralem Element und denselben Inversen. D.h.

(i) für alle $a, b \in H$ gilt $a * b \in H$,

(ii) $e \in H$,

(iii) mit $a \in H$ ist auch $a^{-1} \in H$.

(3) Untergruppen von M und Untermonoide von G sind analog definiert.

2.2 Übung: Sei $(G, *, e)$ eine Gruppe. Zeigen Sie: $H \subset G$ ist genau dann Untergruppe von G, wenn

(i) $H \neq \emptyset$,

(ii) $a, b \in H \Rightarrow a * b^{-1} \in H$.

2.3 Beispiele: (1) Ist $(M, *, e)$ ein Monoid, dann sind M und $\{e\}$ Untermonoide, genannt die trivialen Untermonoide.

(2) Auf dem Einheitsintervall $[0, 1]$ definieren wir eine Monoidstruktur durch $x * y = \max(x, y)$. Die Teilmenge $\{1\}$ erfüllt dann die Bedingung (i) für einen Untermonoid, aber nicht die Bedingung (ii).

(3) $\{e\}$ und G sind die trivialen Untergruppen einer Gruppe $(G, *, e)$.

(4) $(\mathbb{Z}, +)$ ist Untergruppe von $(\mathbb{Q}, +)$ und $(\mathbb{R}, +)$.

2.4 Satz: Ist $(G, *)$ eine Gruppe und $H \subset G$ ein endlicher Untermonoid von G, dann ist H eine Untergruppe von G.

Beweis: In einer Gruppe gilt die Kürzungsregel. Daher ist H ein Monoid, der die Kürzungsregel erfüllt. Nach 1.11 ist H eine Gruppe. □

2.5 Satz: Ist $(M, *, e)$ ein Monoid, dann ist die Teilmenge M^* der invertierbaren Elemente von M eine Untergruppe von $(M, *)$.

Beweis: Wir müssen die Bedingungen für eine Untergruppe nachweisen:

(i) sind a und b invertierbar, dann ist auch $a * b$ invertierbar. Das Inverse ist $b^{-1} * a^{-1}$ (Achten Sie auf die Reihenfolge!).

(ii) e ist invertierbar, da $e^{-1} = e$.

(iii) Ist a invertierbar, dann auch a^{-1}, denn $(a^{-1})^{-1} = a$.

□

2.6 Beispiele: (1) $(\mathbb{N}_0, +)^* = \{0\}$, $(\mathbb{Z}, \cdot)^* = \{\pm 1\}$.

(2) Für eine beliebige Menge M gilt

$$(\mathrm{Abb}(M, M), \circ)^* = \Sigma_M = \text{ Gruppe der Permutationen von } M.$$

Wir wollen jetzt ein elementares Verfahren zum Auffinden von Untergruppen und Untermonoiden vorstellen. Dazu benötigen wir den folgenden Satz, dessen einfachen Beweis wir dem Leser überlassen.

2.7 Satz: Sei $\{U_j, j \in J\}$ eine Familie von Untermonoiden (Untergruppen) eines Monoids $(M, \cdot)$ (bzw. einer Gruppe $(G, \cdot)$). Dann ist

$$\bigcap_{j \in J} U_j$$

ebenfalls eine Untermonoid (bzw. eine Untergruppe). □

2.8 Definition: Sei G eine Gruppe und $A \subset G$ eine beliebige Teilmenge. Die *von A erzeugte Untergruppe* ist die kleinste Untergruppe von G, die A enthält: Wir bezeichnen sie mit $\langle A \rangle$. Dann ist $\langle A \rangle$ charakterisiert durch

(1) $A \subset \langle A \rangle$

(2) Ist $U < G$ Untergruppe, so dass $A \subset U$, dann gilt $\langle A \rangle < U$.

Gilt $G = \langle A \rangle$, heißt A *Erzeugendensystem* von G.

2.9 Satz: Sei $A \subset G$ Teilmenge einer Gruppe G. Dann gilt

(1) $\langle A\rangle$ existiert. Genauer gilt

$$\langle A\rangle = \bigcap\{U; U \text{ ist Untergruppe von } G, \text{ und } A \subset U\}$$

(2) Falls $A = \emptyset$, gilt $\langle A\rangle = \{e\}$
Falls $A \neq \emptyset$, gilt

$$\langle A\rangle = \{x_1 \cdot \ldots \cdot x_n \in G; \quad n \in \mathbb{N}, \quad x_i \in A \text{ oder } x_i^{-1} \in A \text{ für jedes } i\}$$

Beweis: Der Durchschnitt $D = \bigcap\{U < G; A \subset U\}$ ist nicht leer, weil G selbst die Bedingung an U erfüllt. Da $A \subset U$ für alle betrachteten U, ist $A \subset D$. Nach 2.7 ist D Untergruppe von G, und weil $\langle A\rangle$ eine Untergruppe von G ist, die A enthält, folgt $D \subset \langle A\rangle$. Aus 2.8.2 folgt aber $D \subset \langle A\rangle$, so dass $\langle A\rangle = D$.
Teil (2) ist dem Leser als Übungsaufgabe überlassen. □
Besonders einfach ist der Fall $A = \{x\}$. Wir schreiben kürzer $\langle x\rangle$ für $\langle\{x\}\rangle$. Nach 2.8.2 gilt

$$\langle x\rangle = \{x^k \in G; \quad x \in \mathbb{Z}\}$$

Solche Untergruppen nennt man *zyklische* Untergruppen.

2.10 Definition: Eine Gruppe $(G, \cdot)$ heißt *zyklisch*, wenn es ein $x \in G$ gibt, so dass $G = \langle x\rangle$. Wir nennen x einen *Erzeuger* von G.

2.11 Beispiel: $(\mathbb{Z}, +)$ ist eine unendliche zyklische Gruppe. Es gilt

$$\mathbb{Z} = \langle 1\rangle = \langle -1\rangle$$

Sowohl 1 als auch -1 erzeugen $\mathbb{Z}$. Man beachte hier, dass die k-te "Potenz" das k-fache ist, weil die Verknüpfung additiv geschrieben wird.

2.12 Definition: Ist $(G, \cdot)$ eine Gruppe, dann nennt man die Anzahl $|G|$ ihrer Elemente die *Ordnung* von G. Für $x \in G$ nennt man die Ordnung der Untergruppe $\langle x\rangle$ auch *Ordnung von* x, bezeichnet mit $\mathrm{ord}(x)$.

2.13 Aufgabe: Sei $(G, \cdot)$ eine Gruppe und seien $x, y \in G$ und $n \in \mathbb{N}$.
Zeigen Sie:

(1) $\mathrm{ord}(x)$ ist die kleinste Zahl $k \in \mathbb{N}$, so dass $x^k = e$. Gibt es kein solches k, ist $\mathrm{ord}(x) = \infty$.

(2) $x^n = e \iff \mathrm{ord}(x)$ teilt n

(3) $\mathrm{ord}(x^{-1}) = \mathrm{ord}(x) = \mathrm{ord}(y^{-1} \cdot x \cdot y)$

(4) $\mathrm{ord}(x \cdot y) = \mathrm{ord}(y \cdot x)$

(5) $\mathrm{ord}(x^n) = \mathrm{ord}(x)/d$, wobei $d = \mathrm{ggT}(n, \mathrm{ord}(x))$

Zum Abschluss bestimmen wir alle Untergruppen von $(\mathbb{Z}, +)$ (s. auch Grundkurs).

2.14 Satz: Für jedes $k \in \mathbb{N}_0$ ist $k \cdot \mathbb{Z} = \{k \cdot n; n \in \mathbb{Z}\}$ eine Untergruppe von $(\mathbb{Z}, +)$ und jede Untergruppe U von ($\mathbb{Z}$ ist von dieser Form.

Beweis: Nach 2.9.2 ist $k \cdot \mathbb{Z} = \langle k \rangle$. Also ist $k \cdot \mathbb{Z}$ Untergruppe von $\mathbb{Z}$.

Sei nun $U < \mathbb{Z}$ eine Untergruppe. Ist $U \neq \{0\}$, enthält U positive Elemente, denn mit x ist auch $-x$ in U. Sei $k > 0$ das kleinste positive Element in U. Dann gilt $k \cdot \mathbb{Z} = \langle k \rangle \subset U$. Sei nun umgekehrt $x \in U$. Wir teilen mit Rest.

$$x = q \cdot k + r \quad \text{mit } 0 \leq r < k.$$

Da x und k in U sind, ist auch $x - q \cdot k = r \in U$. Da aber k das kleinste Element > 0 in U ist und $r < k$, folgt $r = 0$. Also $x = q \cdot k = k \cdot q \in k \cdot \mathbb{Z}$. Folglich ist $U = k \cdot \mathbb{Z}$. □

3 Homomorphismen

Will man Mengen mit Struktur miteinander vergleichen und eine Theorie darüber entwickeln, betrachtet man strukturerhaltende Abbildungen zwischen ihnen.

3.1 Definition: Eine Abbildung $f : (M, \cdot) \to (N, *)$ von Monoiden heißt *Homomorphismus*, wenn

(1) $f(x \cdot y) = f(x) * f(y) \quad \forall x, y \in M$

(2) $f(e_M) = e_N$, wobei $e_M \in M$ und $e_N \in N$ die neutralen Elemente sind.

Eine Abbildung $f : (G, \cdot) \to (H, *)$ von Gruppen heißt *Homomorphismus*, wenn

(1) $f(x \cdot y) = f(x) * f(y) \quad \forall x, y \in G$

(2) $f(e_G) = e_H$

(3) $f(x^{-1}) = (f(x))^{-1} \quad \forall x \in G$

Bei Gruppen genügt es, nur die Bedingung (1) zu kontrollieren:

3.2 Für eine Abbildung $f : (G, \cdot) \to (H, *)$ von Gruppen gilt:

$$f \text{ ist Homomorphismus} \iff f(x \cdot y) = f(x) * f(y) \quad \forall x, y \in G$$

Beweis:: "$\Rightarrow$" ist klar. Für "$\Leftarrow$" sind Bedingungen (2) und (3) zu zeigen:
(2) $f(e_G) = f(e_G \cdot e_G) = f(e_G) * f(e_G)$.
Multiplizieren wir mit $f(e_G)^{-1}$, erhalten wir $e_H = e_H * f(e_G) = f(e_G)$.
(3) $e_H = f(e_G) = f(x \cdot x^{-1}) = f(x) * f(x^{-1})$. Multiplizieren wir von links mit $(f(x))^{-1}$, erhalten wir $(f(x))^{-1} = f(x^{-1})$. □

Wie bei Abbildungen zwischen Mengen, spielen injektive, surjektive und bijektive Abildungen eine besondere Rolle. Sie haben in unserem Fall spezielle Namen.

3.3 Definition: Ein Homomorphismus $f : G \to H$ von Monoiden oder Gruppen heißt

(1) *Monomorphismus*, wenn f injektiv ist,

(2) *Epimorphismus*, wenn f surjektiv ist,

(3) *Isomorphismus*, wenn f bijektiv ist, wir schreiben $G \cong H$.

Ein Homomorphismus $f : G \to G$ heißt *Endomorphismus*, ist f außerdem bijektiv, heißt f *Automorphismus*.

3.4 Übung: Zeigen Sie

(1) Ist $f : G \to H$ ein Isomorphismus, dann ist auch die Umkehrabbildung $f^{-1} : H \to G$ ein Isomorphismus.

(2) Die Identität und die Komposition zweier Homomorphismen sind Homomorphismen.

3.5 Beispiele:

(1) Sei $(G, \cdot)$ eine beliebige Gruppe und $x \in G$ fest gewählt. Dann ist

$$f : (\mathbb{Z}, +) \to (G, \cdot), \qquad k \mapsto x^k$$

ein Gruppenhomomorphismus. Dabei definieren wir

$$\begin{array}{rcll} x^k & = & x \cdot x \cdot \ldots \cdot x & k \text{ Faktoren, falls } k > 0 \\ & = & e_G & , \text{ falls } k = 0 \\ & = & (x^{-1})^{|k|} & , \text{ falls } k < 0 \end{array}$$

(2) Ist G zyklische Gruppe, so dass $G = \langle x \rangle$, dann ist f aus (1) ein Epimorphismus.

(3) Die Abbildungen

$$\begin{array}{ll} (\mathbb{R}, +) \to (\mathbb{R}_+^*, \cdot), & x \mapsto 2^x \\ (\mathbb{R}_+^*, \cdot) \to (\mathbb{R}, +), & x \mapsto \log_2 x \end{array}$$

sind zueinander inverse Isomorphismen. Dabei setzen wir

$$\begin{array}{l} \mathbb{R}_+ = \{x \in \mathbb{R}; x \geq 0\} \quad ; \quad \mathbb{R}_- = \{x \in \mathbb{R}; x \leq 0\} \\ \mathbb{R}^* = \{x \in \mathbb{R}; x \neq 0\} \\ \mathbb{R}_+^* = \{x \in \mathbb{R}; x > 0\} \end{array}$$

Aus 3.4 folgt

3.6 Ist G ein Monoid oder eine Gruppe, dann ist die Menge $End(G)$ der Endomorphismen von G ein Monoid unter der Komposition, und für die Menge der invertierbaren Elemente in $End(G)$ gilt

$$End(G)^* = Aut(G) := \{f : G \to G; f \text{istAutomorphismus}\}.$$

3.7 Beispiel: $End(\mathbb{Z},+) \cong (\mathbb{Z},\cdot)$ als Monoid
$Aut(\mathbb{Z},+) \cong (\{\pm 1\},\cdot)$ als Gruppen

Beweis:: Definiere

$$\varphi : End(\mathbb{Z}) \to \mathbb{Z}, \qquad \varphi(f) = f(1)$$

(1) Da f eine Homomorphismus ist, gilt

$$f(n) = f(1 + \ldots + 1) = n \cdot f(1) \quad \text{für } n > 0 \qquad (*)$$

weiterhin

$$f(-n) = -f(n) = (-n) \cdot f(1) \text{ und } f(0) = 0 = 0 \cdot f(1).$$

Also ist f eindeutig durch $f(1)$ festgelegt. Folglich ist φ injektiv.

(2) φ ist ein Homomorphismus von Monoiden, denn

$$\begin{aligned} \varphi(g \circ f) = (g \circ f)(1) = \; & g(f(1)) \overset{(*)}{=} f(1) \cdot g(1) \\ & = g(1) \cdot f(1) = \varphi(g) \cdot \varphi(g) \\ \varphi(id_{\mathbb{Z}}) = \; & id_{\mathbb{Z}}(1) = 1 \end{aligned}$$

(3) φ ist surjektiv: Für $k \in \mathbb{Z}$ definieren wir

$$f_k : \mathbb{Z} \to \mathbb{Z}, \quad n \mapsto n \cdot k$$

Man sieht sofort, dass f_k ein Homomorphismus ist und $\varphi(f_k) = f_k(1) = k$. Damit ist der erste Teil gezeigt. Der zweite Teil folgt, weil es sich um die Untergruppen der invertierbaren Elemente handelt.

□

Das letzte Beispiel wirft die Frage aus: Was passiert im allgemeinen Fall mit den invertierbaren Elementen eines Monoids?

3.8 Satz: Ist $f : M \to N$ ein Monoidhomomorphismus, dann definiert die Einschränkung von f auf M^* einen Homomorphismus von Gruppen $f^* : M^* \to N^*$.

Beweis:: Wir müssen nur zeigen: Ist $x \in M^*$, dann ist $f(x) \in N^*$. Es gilt

$$\begin{aligned} e_N = f(e_M) \; & = \; f(x \cdot x^{-1}) = f(x) \cdot f(x^{-1}) \\ & = \; f(x^{-1} \cdot x) = f(x^{-1}) \cdot f(x) \end{aligned}$$

Also ist $f(x^{-1})$ invers zu $f(x)$, d.h. $f(x) \in \mathbb{N}^*$. □

Auch die folgenden Begriffe sind zum Teil aus dem Grundkurs Mathematik bekannt.

3.9 Definition: Sei $f : G \to H$ ein Homomorphismus von Monoiden oder Gruppen. Ist $A \subset G$ und $B \subset H$, so nennen wir

$$f(A) := \{y \in H;\ \exists a \in A \text{ mit } f(a) = y\} = \{f(a);\ a \in A\}$$

das *Bild* von A unter f und

$$\text{Bild} f := f(G)$$

das *Bild* von f. Wir nennen

$$f^{-1}(B) := \{x \in G; f(x) \in B\}$$

das *Urbild* von B unter f und

$$\text{Kern} f := f^{-1}(e_H) = \{x \in G; f(x) = e_H\}$$

den *Kern* von f.

3.10 Satz: (1) Ist $f : G \to H$ ein Monoidhomomorphismus und sind $A \subset G$ und $B \subset H$ Untermonoide, so sind auch $f(A)$ und $f^{-1}(B)$ Untermonoide.

(2) Ist $f : G \to H$ ein Gruppenhomomorphismus und sind $A \subset G$ und $B \subset H$ Untergruppen, dann sind auch $f(A) \subset H$ und $f^{-1}(B) \subset G$ Untergruppen. Insbesonderre ist Kern f eine Untergruppe von G.

(3) Ein *Gruppen*homomorphismus $f : G \to H$ ist genau dann injektiv, wenn Kern $f = \{e_G\}$. □

Beweis:

(1) Sei $A \subset G$ ein Untermonoid. Dann ist $e_G \in A$, also $e_H = f(e_G) \in f(A)$. Seien weiter $x, y \in f(A)$. Dann gibt es $a, b \in A$ mit $f(a) = x$ und $f(b) = y$. Da $a \cdot b \in A$, folgt $x \cdot y = f(a) \cdot f(b) = f(a \cdot b) \in f(A)$. Nach 2.1 ist damit $f(A)$ ein Untermonoid von H.

Sei nun $B \subset H$ ein Untermonoid von H. Da $f(e_G) = e_H \in B$, ist $e_G \in f^{-1}(B)$. Sind weiter $a, b \in f^{-1}(B)$, d.h. $f(a) \in B$ und $f(b) \in B$, dann gilt

$$f(a \cdot b) = f(a) \cdot f(b) \in B, \text{ also } a \cdot b \in f^{-1}(B).$$

(2) Aus (1) wissen wir, dass $f(A)$ Untermonoid von H und $f^{-1}(B)$ Untermonoid von G ist. Wir müssen noch die Existenz von Inversen nachweisen. Sei $x \in f(A)$. Dann gibt es ein $a \in A$ mit $f(a) = x$ Da A eine Untergruppe ist, ist $a^{-1} \in A$. Es folgt $f(a^{-1}) = f(a)^{-1} = x^{-1}$. Also ist $x^{-1} \in f(A)$. Sei nun $a \in f^{-1}(B)$, also $f(a) \in B$. Es gilt $f(a^{-1}) = f(a)^{-1}$. Da B eine Untergruppe ist, ist $f(a)^{-1} \in B$, also $a^{-1} \in f^{-1}(B)$.

(3) $f(e_G) = e_H$. Ist f injektiv, wird e_H von höchstens einem Element getroffen, d.h. Kern f besteht nur aus e_G.

Umgekehrt gelte Kern $f = \{e_G\}$ und $f(a) = f(b)$. Wir müssen zeigen, dass $a = b$ Nun gilt, da $f(a) = f(b)$,

$$f(a \cdot b^{-1}) = f(a) \cdot f(b^{-1}) = f(a) \cdot f(b)^{-1} = e_H.$$

Also folgt $a \cdot b^{-1} \in$ Kern f und damit $a \cdot b^{-1} = e_H$. Es folgt $a = b$.

□

4 Faktorgruppen

Faktorgruppen wurden bereits im Grundkurs behandelt. Sei $U < G$ eine Untergruppe. Wir führen auf G eine Äquivalenzrelation ein:

$$x \sim y \iff x^{-1} \cdot y \in U.$$

Es gilt:

(1) $x \sim x$, denn $x^{-1} \cdot x = e \in U$.

(2) $x \sim y \Rightarrow y \sim x$, denn ist $x^{-1}y \in U$, dann auch $(x^{-1} \cdot y)^{-1} = y^{-1} \cdot x$

(3) $x \sim y \ \wedge \ y \sim z \Rightarrow x \sim z$, denn sind $x^{-1} \cdot y$ und $y^{-1} \cdot z$ aus U, dann ist auch $(x^{-1} \cdot y) \cdot (y^{-1} \cdot z) = x^{-1} \cdot z$ aus U.

Wir erinnern an die Definition der Äquivalenzklassen $\overline{x}$ von x:

$$\overline{x} = \{y \in G; x \sim y\} \subset G.$$

4.1 Behauptung: $\overline{x} = x \cdot U = \{x \cdot u; u \in U\}$, *die Linksnebenklasse* von x bzgl. U, wir sagen auch *modulo* U.

Beweis: $x \cdot U \subset \overline{x}$, denn ist $u \in U$, so folgt $x \sim x \cdot u$, da $x^{-1}(x \cdot u) = u \in U$. Ist umgekehrt $x \sim y$, also $x^{-1} \cdot y = u \in U$, folgt $y = x \cdot u \in x \cdot U$. □

Eine Äquivalenzrelation zerlegt eine Menge in disjunkte Äquivalenzklassen. Also ist G die disjunkte Vereinigung von Linksnebenklassen. Ist G endlich, haben wir also eine endliche Zerlegung

$$G = x_1 \cdot U \sqcup x_2 \cdot U \sqcup \ldots \sqcup x_n \cdot U$$

4.2 Definition und Satz: Sei G eine Gruppe und $x \in G$. Die *Linkstranslation* $l_x : G \to G$ mit x ist definiert durch $l_x(a) = x \cdot a$. Es gilt $l_x \circ l_y = l_{x \cdot y}$ und $l_e = \mathrm{id}$. Insbesondere ist l_x bijektiv mit $l_{x^{-1}}$ als Umkehrabbildung.

Beweis: $(l_x \circ l_y)(a) = l_x(l_y(a)) = x(y \cdot a) = (x \cdot y) \cdot a = l_{x \cdot y}(a)$ und $l_e(a) = e \cdot a = \mathrm{id}(a)$ □

4.3 Folgerung: Bezeichnet $|A|$ die Anzahl der Elemente einer Menge A, dann gilt $|x_i \cdot U| = |U|$ und damit $|G| = n \cdot |U|$. □

Wir erhalten

4.4 Satz (Joseph de Lagrange, 1736-1813): Ist G eine endliche Gruppe und $U < G$ Untergruppe von G, dann ist $|U|$ ein Teiler von $|G|$.

4.5 Bemerkung: Statt Linksnebenklassen $x \cdot U$ kann man auch *Rechtsnebenklassen* $U \cdot x$ betrachten. Sie sind die Äquivalenzklassen der Relation

$$x \sim_r y \iff x \cdot y^{-1} \in U.$$

Da auch die *Rechtstranslation* $r_x : G \to G$, $a \mapsto a \cdot x$ mit x bijektiv ist, erhalten wir dasselbe Ergebnis. Insbesondere ist $|G|/|U|$ sowohl die Anzahl der Links- als auch der Rechtsnebenklassen von U.

4.6 Definition: Die Anzahl $\frac{|G|}{|U|}$ der Link- bzw. Rechtsnebenklassen von U heißt *Index von U in G* und wird oft mit $[G : U]$ bezeichnet. Die Menge der Linksnebenklassen bezeichnen wir mit G/U.

4.7 Anwendungen:

(1) Ist $|G|$ prim, dann ist G zyklisch. Genauer gilt dann $G = \langle x \rangle$, wobei $x \neq e$ aus G beliebig gewählt werden kann.

(2) Sei G endliche Gruppe und $x \in G$, dann gilt $x^{|G|} = e$.

Beweis:

(1) Sei $x \neq e \in G$ und $U = \langle x \rangle$. Dann gilt $|U|$ teilt $|G|$. Da $|U| > 1$, folgt $|U| = |G|$, weil $|G|$ prim ist. Also folgt $G = U = \langle x \rangle$.

(2) Sei $k = ord(x)$. Dann ist $\langle x \rangle$ nach 2.12 eine Untergruppe von G der Ordnung k. Also ist k Teiler von $|G|$, d.h. $|G| = l \cdot k$ mit $l \in \mathbb{N}\backslash\{0\}$. Es folgt $x^{|G|} = x^{k \cdot l} = (x^k)^l = e^l = e$.

□

Wir wollen nun untersuchen, unter welchen Bedingungen die Multiplikation auf G eine Multiplikation auf der Menge G/U der Linksnebenklassen definiert.

Wir untersuchen zunächst ein Beispiel.

4.8 Beispiel: Σ_3 ist die Gruppe der Permutationen, d.h. der bijektiven Abbildungen von $\{1, 2, 3\}$. Aus dem Grundkurs wissen wir, dass $|\Sigma_3| = 3! = 6$. Die Elemente sind gegeben durch

$$\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \sigma^2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \tau = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \sigma \circ \tau = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix},$$

$\sigma^2 \circ \tau = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$ und id, wobei die obere Zeile auf die untere Zeile abgebildet wird. Dann ist $\langle \tau \rangle = \{\mathrm{id}, \tau\} = U$ eine Untergruppe von Σ_3. Nach 4.5 gibt es 3 Links- und 3 Rechtsnebenklassen "modulo U".

Linksnebenklassen: $\mathrm{id} \circ U = U = \{\mathrm{id}, \tau\} = \{\tau^2, \tau\} = \tau \circ U$

$$\begin{aligned} \sigma \circ U &= \{\sigma, \sigma \circ \tau\} = \{\sigma \circ \tau^2, \sigma \circ \tau\} = (\sigma \circ \tau) \circ U \\ \sigma^2 \circ U &= \{\sigma^2, \sigma^2 \circ \tau\} = \{\sigma^2 \circ \tau^2, \sigma^2 \circ \tau\} = (\sigma^2 \circ \tau) \circ U \end{aligned}$$

Rechtsnebenklassen: $\mathrm{id} \circ U = U = \{\mathrm{id}, \tau\} = \{\tau^2, \tau\} = U \circ \tau$

$$\begin{aligned} U \circ \sigma &= \{\sigma, \tau \circ \sigma\} = \{\tau \circ \sigma^2 \circ \tau, \sigma^2 \circ \tau\} = U \circ (\sigma^2 \circ \tau) \\ U \circ \sigma^2 &= \{\sigma^2, \tau \circ \sigma^2\} = \{\tau \circ \sigma \circ \tau, \sigma \circ \tau\} = U \circ (\sigma \circ \tau) \end{aligned}$$

Da $\tau \circ \sigma \neq \sigma \circ \tau$, sehen wir, dass $\sigma \circ U \neq U \circ \sigma$, d.h. die Linksnebenklasse von σ ist verschieden von der Rechtsnebenklasse.

Wenn nun die Verknüpfung auf Σ_3 eine Verbindung auf Σ_3/U definiert, muss für Linksnebenklassen $\overline{x}$ und $\overline{y}$ gelte

$$\overline{x} \cdot \overline{y} = \overline{x \circ y} \qquad (*)$$

Insbesondere müsste gelten

$$\overline{\sigma} \cdot \overline{\sigma^2} = \overline{\sigma^3} = \overline{\mathrm{id}} = U.$$

Da aber $\overline{\sigma} = \overline{\sigma \circ \tau}$, folgt dann

$$U = \overline{\sigma} \cdot \overline{\sigma^2} = \overline{\sigma \circ \tau} \cdot \overline{\sigma^2} = \overline{\sigma \circ \tau \circ \sigma^2} = \overline{\sigma^2 \circ \tau} = (\sigma^2 \circ \tau) \circ U,$$

aber $U \neq (\sigma^2 \circ \tau) \circ U$. Also ist $(*)$ nicht "wohldefiniert', definiert daher keine Verknüpfung auf Σ_3/U.

Sei G nun eine beliebige Gruppe, $U < G$ eine Untergruppe. Gegeben Nebenklassen $\overline{x}, \overline{y}, \in G/U$. Wir müssen untersuchen, unter welchen Bedingungen

4.9

$$\overline{x} \cdot \overline{y} \overset{\text{def.}}{=} \overline{x \cdot y}$$

wohldefiniert ist. Andere Repräsentanten aus $\overline{x}$ sind von der Form $x \cdot u_1$ mit $u_1 \in U$ und entsprechend für y. Es muss also für $u_1, u_2 \in U$ gelten

$$x \cdot y \sim x \cdot u_1 \cdot y \cdot u_2, \quad \text{d.h.} \quad (x \cdot y)^{-1}(x \cdot u_1 \cdot y \cdot u_2) \in U$$

Es muss also ein $u_3 \in U$ geben, so dass

$$y^{-1} \cdot x^{-1} \cdot x \cdot u_1 \cdot y \cdot u_2 = u_3$$

bzw. $y^{-1} \cdot u_1 \cdot y = u_3 \cdot u_2^{-1} \in U$. Also ist 4.9 genau dann wohldefiniert, wenn

$$y^{-1} \cdot U \cdot y \subset U.$$

4.10 Definition: Eine Untergruppe $U < G$ heißt *Normalteiler*, wenn für alle $y \in G$ gilt $y^{-1} \cdot U \cdot y \subset U$, wir schreiben $U \lhd G$.

Da die Bedingung für alle $y \in G$ gelten muss, gilt sie auch für y^{-1}, so dass

$$y \cdot U \cdot y^{-1} = (y^{-1})^{-1} \cdot U \cdot y^{-1} \subset U.$$

Es folgt: $U = y^{-1} \cdot U \cdot y$ und $y \cdot U = U \cdot y$.

4.11 Eine Untergruppe $U < G$ ist genau dann Normalteiler, wenn für alle $y \in G$ gilt $y \cdot U = U \cdot y$, d.h. Links- und Rechtsnebenklassen sind gleich.

Wir fassen zusammen

4.12 Satz: Ist $U \lhd G$ ein Normalteiler, dann definiert

$$\overline{x} \cdot \overline{y} = \overline{x \cdot y}$$

eine Verknüpfung auf den Nebenklassen $\overline{x} \in G/U$.
$(G/U, \cdot)$ ist eine Gruppe mit $\overline{e}$ als neutrales Element und $\overline{x^{-1}}$ als Inversen von $\overline{x}$. Die *Projektion*

$$p : G \to G/U, \quad x \mapsto \overline{x}$$

ist ein Epimorphismus mit Kern U.

Beweis: Wir müssen noch den zweiten Teil zeigen:
Assoziativität: $\overline{x} \cdot (\overline{y} \cdot \overline{z}) = \overline{x} \cdot \overline{y \cdot z} = \overline{x(y \cdot z)} = \overline{(x \cdot y) \cdot z} = \overline{x \cdot y} \cdot \overline{z}$
$= (\overline{x} \cdot \overline{y}) \cdot \overline{z}$
$\overline{e}$ ist linksneutral: $\overline{e} \cdot \overline{x} = \overline{e \cdot x} = \overline{x}$
$\overline{x^{-1}}$ ist linksinvers zu $\overline{x}$: $\overline{x^{-1}} \cdot \overline{x} = \overline{x^{-1} \cdot x} = \overline{e}$
Offensichtlich ist p surjektiv. p ist Homomorphismus:

$$p(x \cdot y) = \overline{x \cdot y} = \overline{x} \cdot \overline{y} = p(x) \cdot p(y)$$

$x \in \operatorname{Kern} p \iff \overline{e} = p(x) = \overline{x} \iff e \sim x \iff e^{-1} \cdot x = x \in U.$ □

4.13 Bemerkung: Sind A, B Teilmengen eines Monoids, dann definieren wir

$$A \cdot B = \{a \cdot b;\ a \in A, b \in B\} \text{ und } A^{-1} = \{a^{-1};\ a \in A\}.$$

Mit diesen Bezeichnungen ist $\overline{x} = x \cdot U$ und $\overline{y} = y \cdot U$. Ist U Normalteiler, dann gilt $y \cdot U = U \cdot y$, und die Verknüpfung 4.9 gilt sogar für Teilmengen von G. Genauer

$$(x \cdot U) \cdot (y \cdot U) = x \cdot U \cdot y \cdot U = x \cdot y \cdot U \cdot U = (x \cdot y) \cdot U.$$

Hier ist natürlich zu zeigen, dass $U \cdot U = U$.

4.14 Aufgabe: (1) Für eine Untergruppe $U < G$ gilt $U \cdot U = U$ und $U^{-1} = U$

(2) Eine Teilmenge $A \subset G$ ist genau dann Untergruppe, wenn $A \neq \emptyset$ und $A \cdot A^{-1} \subset A$.

4.15 Bezeichnung: Ist $U \lhd G$, dann heißt G/U mit der Multiplikation aus 4.12 *Faktorgruppe* von G *modulo* U.

4.16 Beispiele von Normalteilern

(1) $\{e\}$ und G sind Normalteiler von G, die *trivialen* Normalteiler.

(2) Jede Untergruppe einer abelschen Gruppe ist Normalteiler.

(3) Das *Zentrum* $Z(G) = \{g \in G;\ g \cdot x = x \cdot g\ \forall x \in G\}$ ist Normalteiler von G.

(4) Ist $f : G \to H$ ein Homomorphismus und $U \lhd H$, dann ist $f^{-1}(U) \lhd G$. Insbesondere ist Kern $f \lhd G$.

(5) Ist $f : G \to H$ ein *Epi*morphismus und $U \lhd G$, dann ist $f(U) \lhd H$.

(6) Jede Untergruppe von Index 2 ist Normalteiler.

Die Beweise sind dem Leser überlassen.

Als erste Anwendung beschreiben wir die aus dem Grundkurs bekannten Restklassengruppen $\mathbb{Z}/n$ als Faktorgruppen von $(\mathbb{Z}, +)$ und zeigen, dass jede zyklische Gruppe zu einer dieser Faktorgruppen isomorph ist. Dazu benötigen wir noch den

4.17 Isomorphiesatz: Sei $f : G \to H$ ein Homomorphismus. Dann bildet f die ganze Nebenklasse $\overline{x} = x \cdot \operatorname{Kern} f$ auf $f(x)$ ab und definiert daher einen Homomorphismus

$$\overline{f} : G/\operatorname{Kern} f \to H \quad \overline{f}(\overline{x}) = f(x \cdot \operatorname{Kern} f) = f(x)$$

$\overline{f}$ ist ein Monomorphismus und $\overline{f} \circ p = f$. Es folgt

$$\overline{f} : G/\operatorname{Kern} f \cong \operatorname{Bild} f$$

Beweis:: Für $u \in \operatorname{Kern} f$ gilt $f(x \cdot u) = f(x) \cdot f(u) = f(x) \cdot e_H = f(x)$, also $f(x \cdot \operatorname{Kern} f) = \{f(x)\}$. Daher ist die Zuordnung $\overline{f}(\overline{x}) = f(x)$ wohldefiniert. $\overline{f}$ ist ein Homomorphismus, denn

$$\overline{f}(\overline{x} \cdot \overline{y}) = f(\overline{x \cdot y}) = f(x \cdot y) = f(x) \cdot f(y) = \overline{f}(\overline{x}) \cdot \overline{f}(\overline{y})$$

$$\overline{f}(\overline{x}) = e_H \iff f(x) = e_H \iff x \in \operatorname{Kern} f \iff \overline{x} = \overline{e} = \operatorname{Kern} f$$

Also ist $\operatorname{Kern} \overline{f} = \{\overline{e}\}$, d.h. $\overline{f}$ ist injektiv. □

Da $(\mathbb{Z}, +)$ abelsch ist, ist jede Untergruppe $n \cdot \mathbb{Z}$, $n \in \mathbb{N}_0$ ein Normalteiler. x und y aus $\mathbb{Z}$ liegen in derselben Nebenklasse modulo $n \cdot \mathbb{Z}$, wenn $-x+y \in n\mathbb{Z}$, d.h. wenn $y - x$ Vielfaches von n ist. Das gilt genau dann, wenn x und y bei der Division mit n denselben Rest haben. Also sind die Nebenklassen genau die Restklassen und die Verknüpfungsregel

$$\overline{x} + \overline{y} = \overline{x + y}$$

ist ebenfalls gleich. Also

4.18 $\mathbb{Z}/n = \mathbb{Z}/(n \cdot \mathbb{Z})$

$\mathbb{Z}/m$ ist zyklisch von der Ordnung m, erzeugt von $\overline{1}$.

4.19 Satz: Jede zyklische Gruppe G ist isomorph zu einer Gruppe $\mathbb{Z}/m$ (beachte $\mathbb{Z}/0 \cong \mathbb{Z}$). Insbesondere sind zyklische Gruppen derselben Ordnung zueinander isomorph.

Beweis:: Sei $G = \langle x \rangle$. Die Abbildung

$$f : (\mathbb{Z}, +) \to (G, \cdot), \quad k \mapsto x^k$$

ist ein Epimorphismus. Der Kern von f ist eine Untergruppe von $\mathbb{Z}$, also von der Form $m\mathbb{Z}$. Nach dem Isomorphiesatz ist

$$\overline{f} : \mathbb{Z}/m \cong G$$

□

4.20 Bemerkung: Sind x und y in derselben Restklasse modulo m, d.h. $\overline{x} = \overline{y}$ in $\mathbb{Z}/m$, schreibt man oft $x \equiv y \mod m$ (x *kongruent* y modulo m).

5 Produkte

Um eine Gruppe besser verstehen zu können, versucht man oft, sie in kleinere Bausteine zu zerlegen.

5.1 Satz und Definition: Sind G und H Monoide oder Gruppen, dann ist das *Produkt* $G \times H$ mit der Verknüpfung

$$(g_1, h_1) \cdot (g_2, h_2) := (g_1 \cdot g_2, h_1 \cdot h_2)$$

wieder ein Monoid bzw. eine Gruppe. Der Nachweis der Gruppenaxiome (Monoidaxiome) ist trivial.

5.2 Bemerkung: Wir können G und H im Falle von Gruppen als Normalteiler von $G \times H$ auffassen. Die Einbettungen sind gegeben durch

$$\begin{aligned} G \subset G \times H, &\quad g \mapsto (g, e_H) \\ H \subset G \times H, &\quad h \mapsto (e_G, h) \end{aligned}$$

Da $(g_1, h_1) \cdot (g, e_H) \cdot (g_1, h_1)^{-1} = (g_1, h_1) \cdot (g, e_H) \cdot (g_1^{-1}, h_1^{-1}) = (g_1 \cdot g \cdot g_1^{-1}, h_1 \cdot e_h \cdot h_1^{-1}) = (g_1 \cdot g \cdot g_1^{-1}, e_H) \in G$, ist G tatsächlich Normalteiler. Analog verhält es sich für H.
Die beiden Projektionen

$$G \xleftarrow{p_1} G \times H \xrightarrow{p_2} H$$

sind Epimorphismen. Beachte: $\operatorname{Kern} p_1 = H$, $\operatorname{Kern} p_2 = G$ und

$$\overline{p}_2 : (G \times H)/G \cong H, \qquad \overline{p}_1 : (G \times H)/H \cong G$$

Wir wollen nun ein Kriterium dafür angeben, wann eine Gruppe G das Produkt zweier anderer Gruppen ist.

5.3 Definition: Eine Gruppe G heißt *inneres Produkt* zweier Untergruppen U und V, wenn die Abbildung

$$f : U \times V \to G \quad (u, v) \mapsto u \cdot v$$

ein Isomorphismus ist.

5.4 Beispiel: $\mathbb{Z}/6$ ist inneres Produkt von $U = \langle \overline{3} \rangle = \{\overline{0}, \overline{3}\}$ und $V = \langle \overline{2} \rangle = \{\overline{0}, \overline{2}, \overline{4}\}$

$$f : U \times V \to \mathbb{Z}/6, \quad (u, v) \to u + v$$

ist ein Homomorphismus:

$$\begin{array}{rcccl} f((u_1,v_1)+(u_2,v_2)) & = & f(u_1+u_2,v_1+v_2) & = & u_1+u_2+v_1+v_2 \\ & = & u_1+v_1+u_2+v_2 & = & f(u_1,v_1)+f(u_2+v_2) \end{array}$$

f ist surjektiv, denn für $\overline{k} \in \mathbb{Z}/6$ gilt

$$f(k\cdot\overline{3}, k\cdot\overline{4}) = k\cdot\overline{3}+k\cdot\overline{4} = k\cdot\overline{3+4} = k\cdot\overline{1} = \overline{k}$$

Da $|U\times V| = 2\cdot 3 = 6 = |\mathbb{Z}/6|$, ist f bijektiv.
Da $U \cong \mathbb{Z}/2$ und $V \cong \mathbb{Z}/3$, erhalten wir als Folgerung

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

5.5 Satz: U und V seien Untergruppen einer Gruppe G. Dann sind äquivalent

(1) G ist inneres Produkt von U und V

(2) $U \lhd G, \quad V \lhd G, \quad G = U\cdot V, \quad U\cap V = \{e\}$

(3) (a) $\forall x \in G\ \exists | u \in U$ und $\exists | v \in V$ mit $x = u\cdot v$
(b) $u\cdot v = v\cdot u\ \forall u \in U, \forall v \in V$

Wir zeigen zunächst

5.6 Lemma: Mit den Bezeichnungen aus 5.3 und 5.5 gilt

(1) $u\cdot v = v\cdot u\ \forall u\in U,\ \forall v \in V \iff f: U\times V \to G$ ist Homomorphismus

(2) $U \lhd G$, $V \lhd G$, $U\cap V = \{e\} \Rightarrow f: U\times V \to G$ ist Monomorphismus

Beweis::

(1) Da

$$f((u_1,v_1)\cdot(u_2,v_2)) = f(u_1\cdot u_2, v_1\cdot v_2) = u_1\cdot u_2\cdot v_1\cdot v_2$$

und

$$f(u_1,v_1)\cdot f(u_2,v_2) = u_1\cdot v_1\cdot u_2\cdot v_2,$$

ist f genau dann ein Homomorphismus, wenn

$$u_1\cdot u_2\cdot v_1\cdot v_2 = u_1\cdot v_1\cdot u_2\cdot v_2 \quad \forall u_1,u_2\in U, \quad \forall v_1,v_2\in V$$

Gleichheit gilt sicherlich, wenn $u_2\cdot v_1 = v_1\cdot u_2$. Ist umgekehrt f ein Homomorphismus, erhalten wir $u_2\cdot v_1 = v_1\cdot u_2$, indem wir $u_1 = v_2 = e$ setzen.

(2) Sei $u \in U$ und $v \in V$. Da U und V Normalteiler sind, folgt $v^{-1} \cdot u \cdot v \in U$ und $u^{-1} \cdot v^{-1} \cdot u \in V$, da $v^{-1} \in V$ ist. Es folgt

$$u^{-1} \cdot v^{-1} \cdot u \cdot v \in u^{-1} \cdot U = U \text{ und } u^{-1} \cdot v^{-1} \cdot u \cdot v \in V \cdot v = V$$

Also ist $u^{-1} \cdot v^{-1} \cdot u \cdot v \in U \cap V = \{e\}$. Es folgt $u \cdot v = v \cdot u$. Nach (1) ist somit f ein Homomorphismus.

Ist nun $f(u, v) = u \cdot v = e$, so folgt $u = v^{-1} \in U \cap V = \{e\}$, also $u = e$ und $v = e$. Es folgt Kern $f = \{(e, e)\}$, also ist f injektiv.

□

Beweis: 5.5: (1) $\Rightarrow$ (2) Wir erinnern daran, dass wir U und V als Untergruppen von $U \times V$ auffassen können, nämlich als die Untergruppen $U \times \{e\}$ und $\{e\} \times V$. Es gilt

$$f(U \times \{e\}) = U \cdot e = U \quad \text{und} \quad f(\{e\} \times V) = e \cdot V = V.$$

Da f ein Isomorphismus ist und $U \times \{e\}$ und $\{e\} \times V$ Normalteiler von $U \times V$ sind, sind $U = f(U \times \{e\})$ und $V = f(\{e\} \times V)$ Normalteiler in G. Weiter gilt

$$\begin{aligned} &U \cdot V = f(U \times V) = G, \quad \text{weil } f \text{ surjektiv ist} \\ &U \cap V = f(U \times \{e\}) \cap f(\{e\} \times V) = f((U \times \{e\}) \cap (\{e\} \times V)) \\ &= f(\{(e, e)\}) = \{(e, e)\}, \quad \text{weil } f \text{ injektiv ist} \end{aligned}$$

(2) $\Rightarrow$ (1) Nach 5.6.2 ist $f : U \times V \to G$ aus 5.3 ein Monomorphismus. Da außerdem $G = U \cdot V$, ist jedes $x \in G$ von der Form

$$x = u \cdot v = f(u, v)$$

für ein $u \in U$ und ein $v \in V$. Also ist f surjektiv.

(1) $\iff$ (3) Ein Teil der Äquivalenz ist in 5.6.1 bewiesen. Nun ist f aber genau dann bijektiv, wenn es zu jedem $x \in G$ genau ein $u \in U$ und genau ein $v \in V$ gibt, so dass $x = u \cdot v$. □

Als Anwendung zeigen wir

5.7 Satz: Sind k und l teilerfremd, so gilt $\mathbb{Z}/(k \cdot l) \cong \langle \overline{k} \rangle \times \langle \overline{l} \rangle \cong \mathbb{Z}/l \times \mathbb{Z}/k$

Beweis: Da $\mathbb{Z}/(k \cdot l)$ abelsch ist, sind $\langle \overline{k} \rangle$ und $\langle \overline{l} \rangle$ Normalteiler. Da $\langle \overline{k} \rangle$ aus den Restklassen der Vielfachen von k und $\langle \overline{l} \rangle$ aus der Restklassen der Vielfachen von l besteht, besteht $\langle \overline{k} \rangle \cap \langle \overline{l} \rangle$ aus den Restklassen der gemeinsamen Vielfachen von k und l. Da k und l teilerfremd ist, ist $k \cdot l$ das kleinste gemeinsame Vielfache, aber $\overline{k \cdot l} = \overline{0}$. Es folgt $\langle \overline{k} \rangle \cap \langle \overline{l} \rangle = \{\overline{0}\}$. Nach 5.6 ist

$$f : \langle \overline{k} \rangle \times \langle \overline{l} \rangle \to \mathbb{Z}/(kl), \ (x, y) \mapsto x + y$$

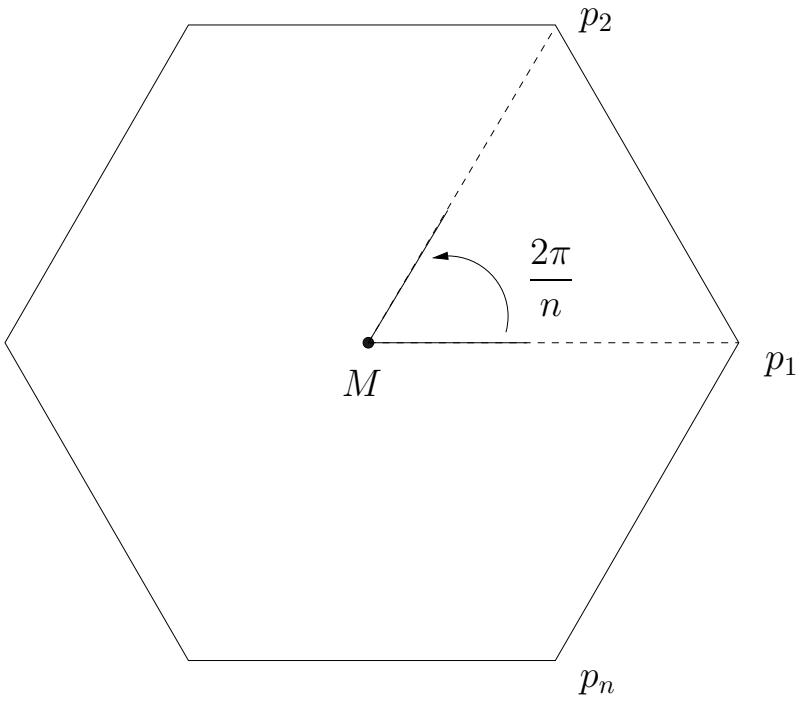
ein Monomorphismus. Da $\operatorname{ord}(\overline{k}) = l$ und $\operatorname{ord}(\overline{l}) = k$ ist $|\langle\overline{k}\rangle \times \langle\overline{l}\rangle| = k \cdot l = |\mathbb{Z}/(kl)|$. Also ist f auch surjektiv, und $\langle\overline{k}\rangle \cong \mathbb{Z}/(l)$ und $\langle\overline{l}\rangle \cong \mathbb{Z}/(k)$.

□

6 Diedergruppen

6.1 Transformationsgruppen: Gelegentlich unterscheidet man zwischen *abstrakten Gruppen* und *Transformationsgruppen*. Abstrakte Gruppen sind gegeben als Menge mit einer Verknüpfung, die eine Gruppenstruktur definiert. Bis jetzt haben wir fast nur abstrakte Gruppen behandelt. Transformationsgruppen dagegen sind Gruppen von Abbildungen einer Menge in sich. Das Standardbeispiel für eine Transformationsgruppe ist die Gruppe Σ_M der Permutationen, also der bijektiven Abbildungen einer Menge M. Wir werden später zeigen, dass jede abstrakter Gruppe als Transformationsgruppe aufgefasst werden kann. Nun ein weiteres Beispiel:

6.2 Die Drehgruppe $\mathcal{R}_\mathbf{n}$ des regulären Ecks:
Gegeben sei ein reguläres n-Eck mit dem Eckpunkten $p_1, \ldots, p_n$. Drehen wir das n-Eck mehrmals um den Winkel $\frac{2\pi}{n}$ um seinen Mittelpunkt M, erhalten wir eine deckungsgleiche Figur. Ist D_k die Drehung um den Winkel $\frac{2\pi k}{n}$, dann



genügt die Komposition von Drehungen den Gleichungen:

(1) $D_k \circ D_l = D_{k+l}$

(2) $D_{n+k} = D_k$

Offensichtlich bilden $D_0 = Id$, $D_1, \ldots, D_{n-1}$ eine Gruppe $\mathcal{R}_n$ mit neutralem Element $D_0 = Id$ und $(D_k)^{-1} = D_{n-k}$ für $k > 0$.
Aus Gleichung (1) folgt, dass

$$D_k = (D_1)^k$$

Also ist jedes Element eine Potenz von D_1, d.h. $\mathcal{R}_n$ ist zyklisch,

$$\mathcal{R}_n =< D_1 >$$

6.3 Die Gruppe $\mathcal{D}_n$ der *Kongruenzabbildungen* des regulären n-Ecks, auch *Diedergruppe* der Ordnung $2n$ genannt.
Nehmen wir das reguläre $n - Eck$ V aus Beispiel 6.2. Eine Kongruenzabbildung bildet die Ecke p_1 auf irgendeine der Ecken $p_1, p_2, \ldots, p_n$ ab. Die übrigen Ecken werden dann im Uhrzeigersinn oder gegen den Uhrzeigersinn von Bild von p_1 aus plaziert. Damit ist jede Kongruenzabbildung entweder eine Drehung oder die Komposition einer Drehung mit einer Spiegelung S an der Achse durch M und p_1. Damit läßt sich jede Kongruenzabbildung als Komposition von Elementen $D := D_1$ und S schreiben. Also wird $\mathcal{D}_n$ von D und S erzeugt: $\mathcal{D}_n =< D, S >$. Die gesuchte Gruppe hat $2n$ Elemente

$$Id = D_0,\ D = D_1,\ D^2 = D_2, \ldots, D^{n-1} = D_{n-1},\ S,\ D \circ S,\ D^2 \circ S \ldots D^{n-1} \circ S$$

Man macht sich sofort klar, dass

(1) $D^n = Id$

(2) $S^2 = Id$

(3) $S \circ D = D^{n-1} \circ S = D^{-1} \circ S$

Durch diese drei Gleichungen wird die Verknüpfung völlig festgelegt. Man sagt: "D und S *erzeugen* $\mathcal{D}_n$ mit den *Relationen* (1), (2), (3)", und schreibt

$$\mathcal{D}_n =< D, S;\ D^n = S^2 = Id,\ S \circ D = D^{-1} \circ S >$$

6.4 Wir wollen die *Verknüpfungstafel* von $\mathcal{D}_3$ aufstellen. In der Tafel stehen die Werte $a * b$, hier also $a \circ b$, wobei die Abbildung b zuerst durchgeführt wird. Induktiv erhält man aus den Relationen die Gleichung

$$S \circ D^k = D^{-k} \circ S$$

Jetzt ist es leicht, die Verknüpfungstafel aufzustellen:

$a\backslash b$	Id	D	D^2	S	$D\circ S$	$D^2\circ S$
Id	Id	D	D^2	S	$D\circ S$	$D^2\circ S$
D	D	D^2	Id	$D\circ S$	$D^2\circ S$	S
D^2	D^2	Id	D	$D^2\circ S$	S	$D\circ S$
S	S	$D^2\circ S$	$D^1\circ S$	Id	D^2	D
$D\circ S$	$D\circ S$	Id	$D^2\circ S$	D	Id	D^2
$D^2\circ S$	$D^2\circ S$	$D\circ S$	S	D^2	D	Id

6.5 Bestimmung der Untergruppen der $\mathcal{D}_3$:

Triviale Untergruppen: $\{Id\}$, $\mathcal{D}_3$

Zyklische Untergruppen:

(1) $< D >=< D^2 >= \{Id, D, D^2\} = \mathcal{R}_3$

(2) $< S >= \{Id, S\}$

(3) $< D\circ S >= \{Id, D\circ S\}$

(4) $< D^2\circ S >= \{Id, D^2\circ S\}$

Von zwei Elementen erzeugte Untergruppen:

Falls D und S in U liegen, folgt $U = \mathcal{D}_3$. Aus (1) wissen wir: Enthält U das Element D oder D^2, enthält U ganz $\mathcal{R}_3$.

Enthält U die Elemente $D^i\circ S$ und D, so enthält U auch $D^{3-i}\circ D^i\circ S = S$, also folgt $U = \mathcal{D}_3$.

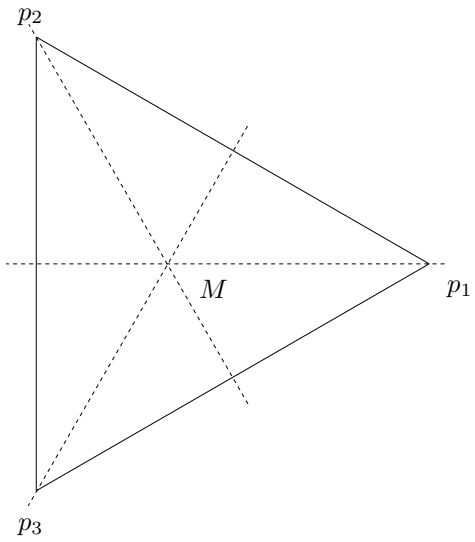
Enthält U die Elemente $D^i\circ S$ und $D^j\circ S$ mit $0 \le i < j \le 2$, so enthält es

$$(D^j\circ S)\circ(D^i\circ S) = D^j\circ D^{-i}\circ S\circ S = D^{j-i}.$$

Wie wir eben gesehen hatten, folgt daraus, dass $U = \mathcal{D}_3$.

Ergebnis: Neben den trivialen Untergruppen enthält $\mathcal{D}_3$ nur die zyklischen Gruppen $(1), \ldots, (4)$.

Die Untergruppen von $\mathcal{D}_3$ haben auch eine geometrische Interpretation. Für die Drehgruppe $\mathcal{R}_3$ ist diese Interpretation klar. Die Untergruppen (2), (3) und (4) sind Spiegelungsgruppen:



$< S >$: Gruppe der Spiegelungen an der Achse $\overline{Mp_1}$

$< D \circ S >$: Gruppe der Spiegelungen an der Achse $\overline{Mp_2}$

$< D^2 \circ S >$: Gruppe der Spiegelungen an der Achse $\overline{Mp_3}$

7 Permutationsgruppen

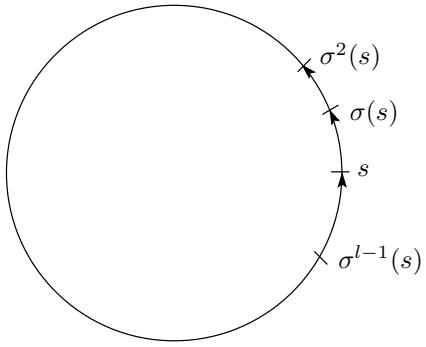
Sei $[n] = \{1, 2, \ldots, n\}$. Dann ist Σ_n die Permutationsgruppe von $[n]$. Sei $\sigma \in \Sigma_n$. Um später mit Permutationen leichter rechnen zu können, suchen wir zunächst eine geeignete Darstellung für σ.

7.1 Die Zykelzerlegung: Sei $s \in [n]$. Wir betrachten die Menge

$$B(s, \sigma) = \{\sigma^k(s);\ k \in \mathbb{Z}\}.$$

Da $\sigma^k(s) \in [n]$, muß es Zahlen $0 \leq k < l$ in $\mathbb{N}$ geben, so dass $\sigma^k(s) = \sigma^l(s)$. Sei l die *kleinste* Zahl, für die es ein solches k gibt.

7.2 Behauptung: $\sigma^l(s) = s$, aber $s, \sigma(s), \sigma^2(s), \ldots, \sigma^{l-1}(s)$ sind verschieden.



D.h. nach l-maligem Anwenden von σ "trifft" man zum erstenmal ein Element, das schon früher aufgetreten ist, und dieses Element ist $s = \sigma^0(s)$, also $k = 0$. Man stellt sich vor, dass man vermöge σ "im Kreis gewandert ist".

Beweis der Behauptung: Seien $0 \leq k < l$ wie oben gewählt, d.h. $\sigma^k(s) = \sigma^l(s)$, und l ist minimal. Wir müssen zeigen, dass $k = 0$ ist. Ist $k > 0$, so folgt $s = \sigma^{-k}(\sigma^k(s)) = \sigma^{-k}((\sigma^l)(s)) = \sigma^{l-k}(s)$, und $0 < l-k < l$. Das widerspricht der Minimalität von l. Also ist $k = 0$.

Wir erhalten

$$B(s, \sigma) = \{s, \sigma(s)), \sigma^2(s), \ldots, \sigma^{l-1}(s)\}$$

So ganz fremd ist uns die Konstruktion $B(s, \sigma)$ nicht. Wir definieren auf $[n]$ eine Relation durch

$$s \sim t \iff \exists\ k \in \mathbb{Z}, \text{ so dass } t = \sigma^k(s)$$

Dann gilt: $s \sim s$, denn $s = \sigma^0(s)$

$s \sim t \Rightarrow t \sim s$, denn $t = \sigma^k(s)$, so ist $s = \sigma^{-k}(t)$

$s \sim t \ \wedge\ t \sim u \Rightarrow s \sim u$, denn ist $t = \sigma^k(s)$ und $u = \sigma^l(t)$, dann ist $u = \sigma^{k+l}(s)$.

Also ist $\sim$ eine Äquvalenzrelation und $B(s, \sigma)$ ist die Äquivalenzklasse von s. Da $[n]$ in disjunkte Äquivalenzklassen zerfällt, haben wir eine Darstellung

$$[n] = B(s_1, \sigma) \sqcup B(s_2, \sigma) \sqcup \ldots \sqcup B(s_r, \sigma).$$

Wir definieren neue Permutationen $\sigma_1, \ldots, \sigma_r \in \Sigma_n$ wie folgt

$$\sigma_i(t) = \begin{cases} \sigma(t) & \text{, falls } t \in B(s_i, \sigma) \\ t & \text{, falls } t \notin B(s_i, \sigma) \end{cases}$$

d.h. σ_i permutiert die Elemente der Klasse $B(s_i, \sigma)$ wie σ und lässt die übrigen Klassen fest. Legt man das Bild 7.2 zugrunde, so permutiert σ_i die Elemente $s_i, \sigma(s_i), \sigma^2(s_i), \ldots, \sigma^{l_i-1}(s_i)$ aus $B(s_i, \sigma)$ zyklisch. Daher ist jedes σ_i ein Zykel in folgendem Sinne.

7.3 Definition: Eine Permutation $\varphi \in \Sigma_n$ heißt *r-Zykel*, wenn es eine r-elementige Teilmenge $T = \{t_1, \ldots, t_r\} \subset [n]$ gibt, so dass φ die Elemente von T zyklisch permutiert, d.h.

$$\varphi(t_i) = \begin{cases} t_{i+1} & 1 \leq i \leq r-1 \\ t_1 & i = r \end{cases}$$

und die übrigen Elemente fest lässt, d.h. $\varphi(s) = s \; \forall s \notin T$. Man nennt T den *Träger* von φ. Nach Definition gilt

$$T = \{t_1, \varphi(t_1), \varphi^2(t_1), \ldots, \varphi^{r-1}(t_1)\}.$$

7.4 Sind $\varphi, \psi \in \Sigma_n$ Zykel mit Trägern T und S, so dass $T \cap S = \emptyset$, so gilt

$$\varphi \circ \psi = \psi \circ \varphi$$

□

Unsere Überlegungen 7.1 zeigen:

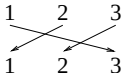
7.5 Satz: Jede Permutation $\sigma \in \Sigma_n$ besitzt eine Zerlegung

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

in *disjunkte* Zykel, d.h. Zykel mit disjunkten Trägern. Die Zerlegung ist bis auf Reihenfolge eindeutig.

7.6 Bezeichnung: Ein Zykel ist eindeutig durch seinen zyklisch *geordneten* Träger definiert, wobei die Ordnung durch die Abbildungsvorschrift 7.3 gegeben ist. Daher benutzen wir oft den Träger als Bezeichnung für einen Zykel.

7.7 Beispiele:

(1) σ :  ist ein Zykel: $\sigma = (1,3,2) = (3,2,1) = (2,1,3)$

(2) Die Permutation $\varphi : \begin{matrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ 2 & 5 & 7 & 4 & 8 & 3 & 6 & 1 & 9 \end{matrix}$

besitzt die Zykelzerlegung $\varphi = (1,2,5,8) \circ (3,7,6) \circ (4) \circ (9)$. Beachte, dass die Permutationen (4) und (9) Identitäten sind. Deshalb ist auch die Beziehungsweise

$$\varphi = (1,2,5,8) \circ (3,7,6)$$

üblich, d.h. 1-Zykel werden in der Zykelzerlegung oft ignoriert. Dabei ist allerdings problematisch, dass man einer so bezeichneten Permutation nicht mehr ansieht, zu welcher Gruppe Σ_n sie gehört.

7.8 Aufgaben:

(1) Ist $\sigma \in \Sigma_n$ ein r-Zykel, so ist $ord(\sigma) = r$

(2) Ist σ das Produkt disjunkter Zykel $\sigma = \sigma_1 \circ \sigma \circ \ldots \circ \sigma_k$, so ist $ord\, \sigma = kgV\{ord(\sigma_1), ord(\sigma_2), \ldots, ord(\sigma_k)\}$

7.9 Bezeichnung: Ein 2-Zykel heißt *Transposition.*

7.10 Satz: Σ_n wird von der Menge $A = \{(i, i+1); i = 1 \ldots, n-1\}$ von Transposition erzeugt, d.h. jede Permutation ist Komposition von Transpositionen aus A.

Beweis:

(i) Jede Permutation ist nach 7.5 Komposition von Zykeln; also genügt es, den Satz für Zykel $(i_1, \ldots, i_k)$ zu zeigen.

(ii) $(i_1, \ldots, i_k) = (i_1, i_k) \circ (i_1, i_{k-1}) \circ \ldots \circ (i_1, i_3) \circ (i_1, i_2)$

Also genügt es, den Satz für beliebige Transpositionen (i, j) und $i < j$ zu zeigen.

(iii) Sei (i, j) Transposition mit $i < j$. Wir beweisen durch Induktion nach $j - i$, dass (i, j) Komposition von Permutation aus A ist. Für $j - i = 1$ ist (i, j) aus A.

Induktionsschritt: $(i, j) = (i, j-1) \circ (j-1, j) \circ (i, j-1)$

$(j-1, j) \in A$, und nach Induktion ist $(i, j-1)$ Komposition von Transpositionen aus A.

□

Als Folgerung können wir nun das allgemeine Kommutativitätsgesetz beweisen, von dem wir im ersten Paragraphen gesprochen haben.

7.11 Allgemeines Kommutativgesetz: Sei $(M, *)$ eine Menge mit einer assoziativen und kommutativen Verknüpfung $*$. Dann gilt für alle $n \in \mathbb{N}$, alle $\sigma \in \Sigma_n$ und alle $a_1, \ldots, a_n$ aus M

$$a_1 * a_2 * \ldots * a_n = a_{\sigma(1)} * a_{\sigma(2)} * \ldots * a_{\sigma(n)}$$

Beweis: Wir definieren $(a_1 * \ldots * a_n) \cdot \sigma = a_{\sigma(1)} * \ldots * a_{\sigma(n)}$. Dann gilt für $\pi, \mu \in \Sigma_n$

$$((a_1 * \ldots * a_n) \cdot \pi) \cdot \mu = (a_1 * \ldots * a_n) \cdot (\pi \circ \mu) \qquad (*)$$

denn setzen wir

$$(a_1 * \ldots * a_n) \cdot \pi = a_{\pi(1)} * \ldots * a_{\pi(n)} = b_1 * \ldots * b_n$$

ist die linke Seite von $(*)$

$$(b_1 * \ldots * b_n) \cdot \mu = b_{\mu(1)} * \ldots * b_{\mu(n)} \equiv a_{\pi\circ\mu(1)} * \ldots * a_{\pi\circ\mu(n)}$$

denn: $b_{\mu(i)} = a_{\pi(k)} \iff k = \mu(i)$. Also $b_{\mu(i)} = a_{\pi(\mu(i))}$. Da σ Komposition von Transpositionen der Form $(i, i+1)$ ist, genügt es also, die obige Gleichung für $\sigma = (i, i+1)$ zu zeigen. Ist aber $\sigma(i, i+1)$, so entsteht $(a_1 * \ldots * a_n) \cdot \sigma$ aus $a_1 * \ldots * a_n$ durch einmaliges Anwenden des Kommutativgesetzes. $\square$

Sei $\sigma \in \Sigma_n$ und $\sigma = \sigma_1 \circ \ldots \circ \sigma_k$ seine bis auf Reihenfolge eindeutige Zykelzerlegung. Ist σ_i ein r_i-Zykel, dann kann man nach Teil (ii) des Beweises von 7.10 das σ_i als Komposition von $r_i - 1$ Transpositionen darstellen. Es folgt

7.12 σ ist die Komposition von $N(\sigma) := (r_1 - 1) + (r_2 - 1) + \ldots + (r_k - 1)$ Transpositionen.

Die Darstellung einer Permutation σ als Komposition von Transpositionen ist weder eindeutig, noch muss die Anzahl der Transpositionen genau $N(\sigma)$ sein. Z.B. gilt

$$(1,2,3) = (1,3) \circ (1,2) = (1,2) \circ (2,3) = (1,2) \circ (1,3) \circ (2,3) \circ (1,2)$$

und $N((1,2,3)) = 3 - 1 = 2$. Aber es gilt

7.13 Satz: Ist σ eine Komposition von l Transpositionen, dann gilt $\overline{l} = \overline{N(\sigma)}$ in $\mathbb{Z}/2$.

Beweis: Sei $\tau_1 = (a, c_1, \ldots, c_k, b, d_1, \ldots, d_l)$, $\lambda_1 = (b, d_1, \ldots, d_l)$ und $\lambda_2 = (a, c_1, \ldots, c_k)$. Dabei ist $k = 0$ und $l = 0$ erlaubt. Man rechnet nach, dass

$$(a, b) \circ (a, c_1, \ldots, c_k, b, d_1, \ldots, d_l) = (b, d_1, \ldots, d_l) \circ (a, c_1, \ldots, c_k) \qquad (A)$$

Komposition mit (a, b) von links ergibt

$$(a, c_1, \ldots, c_k, b, d_1, \ldots, d_l) = (a, b) \circ (b, d_1, \ldots, d_l) \circ (a, c_1, \ldots, c_k) \qquad (B)$$

Sei nun $\sigma = \sigma_1 \circ \sigma_2 \circ \ldots \circ \sigma_r$ die Zykelzerlegung von σ, dann gilt

$$N(\sigma) = N(\sigma_1) + \ldots + N(\sigma_r).$$

Liegen a, b im selben Zykel der Zykelzerlegung, dürfen wir wegen 7.4 annehmen, dass dies σ_1 ist, also ist σ_1 von der Form τ. Damit hat $(a, b) \circ \sigma$ nach (A) die Zykelzerlegung

$$(a, b) \circ \sigma = \lambda_1 \circ \lambda_2 \circ \sigma_2 \circ \ldots \circ \sigma_r$$

Also ist $N(\sigma) = N(\tau) + N(\sigma_2) + \ldots + N(\sigma_r) = k + l + 1 + q$ mit $q = N(\sigma_2) + \ldots + N(\sigma_r)$ und

$$N((a, b) \circ \sigma) = N(\lambda_1) + N(\lambda_2) + q = l + k + q$$

Es folgt: $N((a, b) \circ \sigma) = N(\sigma) - 1$.

Liegen a, b in verschiedenen Zykeln von σ, dürfen wir annehmen, dass σ_1 von der Form λ_1 und σ_2 von der Form λ_2 ist. Nach (B) hat $(a, b) \circ \sigma$ die Zykelzerlegung

$$(a, b) \circ \sigma = \tau \circ \sigma_3 \circ \ldots \circ \sigma_r.$$

Es gilt $N(\sigma) = N(\lambda_1) + N(\lambda_2) + p = l + k + p$ mit $p = N(\sigma_3) + \ldots + N(\sigma_r)$ und $N((a, b) \circ \sigma) = N(\tau) + p = k + l + 1 + p$.

Es folgt $N((a, b) \circ \sigma) = N(\sigma) + 1$.

Da $+\overline{1} = -\overline{1}$ in $\mathbb{Z}/2$, folgt in beiden Fällen

$$\overline{N((a, b) \circ \sigma)} = \overline{N(\sigma)} + \overline{1} \qquad \text{in } \mathbb{Z}/2.$$

Ist nun σ die Komposition von l Transpositionen $\sigma = \tau_1 \circ \ldots \circ \tau_l$ dann folgt, da $N(\mathrm{id}) = 0$

$$\overline{N(\sigma)} = \underbrace{\overline{1} + \ldots + \overline{1}}_{l} + \overline{N(\mathrm{id})} = \overline{l}.$$

□

7.14 Definition und Satz: $\mathrm{sign} : \Sigma_n \to \{\pm 1, \cdot\}$, $\sigma \mapsto (-1)^{N(\sigma)}$ ist ein Epimorphismus. Man nennt $\mathrm{sign}(\sigma) \in \{\pm 1\}$ das *Vorzeichen* oder *Signum* der Permutation σ.

Beweis: Seien $\sigma, \tau \in \Sigma_n$. Dann sind σ und τ die Komposition von $N(\sigma)$ bzw. $N(\tau)$ Transpositionen. Also ist $\sigma \circ \tau$ die Kompostion von $N(\sigma) + N(\tau)$ Transpositionen. Es folgt $\overline{N(\sigma \circ \tau)} = \overline{N(\sigma) + N(\tau)}$ nach 7.13. Also

$$\begin{aligned} \operatorname{sign}(\sigma \circ \tau) &= (-1)^{N(\sigma\circ\tau)} = (-1)^{N(\sigma)+N(\tau)} = (-1)^{N(\sigma)} \cdot (-1)^{N(\tau)} \\ &= \operatorname{sign}(\sigma) \cdot \operatorname{sign}(\tau). \end{aligned}$$

□

7.15 Definition: Der Kern von sign wird *alternierende* Gruppe $A_n \lhd \Sigma_n$ genannt.

A_n besteht aus den *geraden Permutationen*, die Kompositionen einer geraden Anzahl von Transpositiitonen sind. Sie sind u.a. wegen des folgenden Satze von Bedeutung.

7.16 Satz (ohne Beweis): Für $n \neq 4$ besitzt A_n nur die trivialen Normalteiler.

8 Operationen von Gruppen auf Mengen

Wir wollen nun die Interpretation einer abstrakten Gruppe als Transformationsgruppe präzisieren und formalisieren. Das geschieht über den Begriff der Operation einer Gruppe auf einer Menge.

8.1 Definition: Sei $(G, \cdot)$ eine Gruppe und M eine Menge. Eine *Operation* von G auf M *von links* ist eine Abbildung

$$G \times M \to M, \quad (g, x) \mapsto g * x,$$

so dass

(1) $(g_1 \cdot g_2) * x = g_1 * (g_2 * x) \quad \forall g_1, g_2 \in G, \ \forall x \in M$

(2) $e * x = x \quad \forall x \in X$

Eine Operation von *rechts* ist eine Abbildung

$$M \times G \to M, \quad (x, g) \mapsto x * g,$$

so dass

(1) $x * (g_1 \cdot g_2) = (x * g_1) * g_2 \quad \forall g_1, g_2 \in G, \ \forall x \in M$

(2) $x * e = x \quad \forall x \in X$

8.2 Beispiele:

(1) Die Diedergruppe $\mathcal{D}_n$ operiert von links auf dem regulären n-Eck

$$\mathcal{D}_n \times n\text{-Eck} \to n\text{-Eck} \quad (f, x) \mapsto f(x)$$

(2) Ist U Untergruppe von G, dann operiert U von links und rechts auf G.

$$\begin{array}{l} U \times G \to G, \quad (u, g) \mapsto u \cdot g \\ G \times U \to G, \quad (g, u) \mapsto g \cdot u \end{array} \quad \textit{Translationsoperationen}$$

(3) Die *Konjugationsoperatoren* einer Untergruppe U auf der Gruppe G ist definiert durch

$$U \times G \to G, \quad (u, g) \mapsto u \cdot g \cdot u^{-1}.$$

(4) Die Gruppe $\{\pm 1, \cdot\}$ operiert auf $\mathbb{R}^2$ durch

$$\{\pm 1, \cdot\} \times \mathbb{R}^2 \to \mathbb{R}^2, \quad (\pm 1, (x_1, x_2)) \mapsto (\pm x_1, \pm x_2).$$

(5) Die Permutationsgruppe Σ_M operiert auf der Menge M

$$\Sigma_M \times M \to M, \quad (f, x) \mapsto f(x).$$

Das letzte Beispiel ist typisch. Operiert eine Gruppe G auf einer Menge M, kann man jedes Element $g \in G$ als Permutation π_g von M auffassen: wir definieren

$$\pi_g : M \to M, \quad x \mapsto g * x.$$

Dann gilt

$$\pi_{g_1 \cdot g_2} = \pi_{g_1} \circ \pi_{g_2} \text{ und } \pi_e = \mathrm{id}$$

denn $\pi_e(x) = e * x = x = \mathrm{id}(x)$ und

$$\pi_{g_1 \cdot g_2}(x) = (g_1 \cdot g_2) * x = g_1 * (g_2 * x) = \pi_{g_1}(\pi_{g_2}(x)) = (\pi_{g_1} \circ \pi_{g_2})(x).$$

Insbesondere ist π_g bijektiv, denn $\pi_{g^{-1}}$ ist die Umkehrabbildung. Wir erhalten also eine Abbildung

$$\alpha : G \to \Sigma_M, \quad g \mapsto \pi_g.$$

8.3 Satz: Die Abbildung α ist ein Homomorphismus.

Beweis: $\alpha(g_1 \cdot g_2) = \pi_{g_1 \cdot g_2} = \pi_{g_1} \circ \pi_{g_2} = \alpha(g_1) \circ \alpha(g_2)$. □

8.4 Definition: Ist α injektiv, spricht man von einer *effektiven* Operation von G auf M.

Die Linkstranslation von G auf sich selbst

$$G \times G \to G, \quad (g, x) \mapsto g \cdot x$$

ist effektiv. In diesem Fall ist π_g die Linkstranslation $l_g : G \to G$ in der Bezeichnungsweise von 4.2. Gilt $\alpha(g) = l_g = \mathrm{id}$, dann folgt $e = \mathrm{id}(e) = l_g(e) = g \cdot e = g$. Also ist Kern $\alpha = \{e\}$ und α ist injektiv. Wir erhalten den

8.5 Satz von Caley (1821-1895): Jede Gruppe G ist isomorph zu einer Untergruppe der Permutationsgruppe Σ_G.

8.6 Definition: Sei M eine Menge mit Linksoperatoren von G.

(1) $M^G := \{x \in M; g * x = x \quad \forall g \in G\}$ heißt *Fixpunktmenge* der Operation.

(2) Für $x \in M$ heißt

$$G * x := \{g * x; g \in G\} \subset M$$

die *Bahn* oder der *Orbit* von x unter der Operation.

(3) Für $x \in M$ heißt die Menge

$$G_x := \{g \in G;\ g * x = x\} \subset G$$

die *Standuntergruppe* von x.

Wie die Definition schon sagt, ist G_x eine Untergruppe von G. Da $e * x = x$, ist $e \in G_x$. Ist $g \in G_x$, also $g * x = x$, dann folgt

$$g^{-1} * x = g^{-1} * (g * x) = (g^{-1} \cdot g) * x = e * x = x$$

Also ist $g^{-1} \in G_x$. Sind $g_1, g_2 \in G_x$, so gilt

$$(g_1 \cdot g_2) * x = g_1 * (g_2 * x) = g_1 * x = x$$

Also ist $g_1 \cdot g_2 \in G_x$. Nach 2.1.2 ist somit G_x Untergruppe von G.

8.7 Beispiele: (1) Wir betrachten die Konjugationsoperation von G auf sich (Beispiel 8.2.3). Die Fixpunktgruppe ist das *Zentrum* $Z(G)$ von G. Wir erinnern:

$$\begin{aligned} Z(G) &= \{x \in G;\ g \cdot x = x \cdot g\} \\ &= \{x \in G;\ g \cdot x \cdot g^{-1} = x\ \forall g \in G\} \end{aligned}$$

Die Bahn von $x \in G$ wird oft mit x^G bezeichnet und heißt *Konjugationsklasse* von x.

$$x^G = \{g \cdot x \cdot g^{-1};\ g \in G\}$$

Die Standuntergruppe von x wird oft mit $Z(x)$ bezeichnet und heißt *Zentralisator* von x

$$Z(x) = \{g \in G;\ g \cdot x \cdot g^{-1} = x\} = \{g \in G; g \cdot x = x \cdot g\}$$

und besteht aus allen Elementen von G, die mit x kommutieren.

(2) Sei $[n] = \{1, 2, \ldots, n\}$ wie 7.1 und $\sigma \in \Sigma_n$. Dann operiert die Untergruppe $\langle\sigma\rangle < \Sigma_n$ auf $[n]$ durch $(\sigma^k, s) \mapsto \sigma^k(s)$. Die Bahn von s unter dieser Operation in $B(s, \sigma)$ aus 7.1.

Operiert G auf M, können wir eine Relation auf M definieren durch

$$x \sim y \iff \exists\, g \in G \text{ mit } y = g * x$$

$x \sim x$, denn $x = e * x$

$x \sim y \Rightarrow y \sim x$, denn aus $y = g * x$ folgt $g^{-1} * y = x$

$x \sim y \ \wedge \ y \sim z \Rightarrow x \sim z$, denn aus $y = g_1 * x$ und $z = g_2 * y$ folgt

$z = g_2 * (g_1 * x) = (g_1 \cdot g_2) * x$

Also ist $\sim$ eine Äquivalenzrelation. Die Äquivalenzklasse von x ist die Bahn von x, und wir erhalten.

8.8 Zwei Bahnen $G * x$ und $G * y$ sind entweder gleich oder disjunkt. Damit zerfällt M in disjunkte Bahnen.

Zum Abschluss beweisen wir eine wichtige Beziehung zwischen Bahn und Standuntergruppe.

8.9 Satz: Eine *endliche* Gruppe G operiere von links auf einer Menge M. Dann gilt für jedes $x \in M$

$$|G| = |G * x| \cdot |G_x|.$$

Beweis:: Die Abbildung

$$f : G \to G * x, \quad g \mapsto g * x$$

ist surjektiv. Sei $y = g_0 * x$ ein Element aus $G * x$. Dann gilt

$$g_1 \in f^{-1}(y) \iff g_1 * x = g_0 * x \iff (g_0^{-1} \cdot g_1) * x = x \iff g_0^{-1} \cdot g_1 \in G_x$$
$$\iff g_1 \in g_0 \cdot G_x$$

Also $|f^{-1}(y)| = |g_0 \cdot G_x| = |G_x|$, da Linkstranslation mit g_0 bijektiv ist. Damit wird jedes $y \in G * x$ von genau $|G_x|$ Elementen getroffen. Wir erhalten

$$|G| = |G_x| \cdot |G * x|.$$

□

9 p-Gruppen und die Sylowsätze

Sei $\mathcal{P}(G)$ die Potenzmenge von G und $\mathcal{P}_k(G) \subset P(G)$ die Menge der k-elementigen Teilmengen von G. Die Konjugationsoperatoren und die Linkstranslation definieren Operationen.

$$\begin{array}{rll} & G \times \mathcal{P}(G) \to \mathcal{P}(G) & (g, X) \mapsto X^g := g \cdot X \cdot g^{-1} \\ \text{bzw.} & & (g, X) \mapsto g \cdot X \end{array}$$

Da $|g \cdot X| = |X| = |X^g|$, definieren beide Operationen auch Operationen auf $\mathcal{P}_k(G)$.

9.1 (1) X^g heißt *konjugiert* zu X.

(2) Der Orbit von X unter der Konjugation heißt Konjugationsklasse von X.

(3) Die Standuntergruppe $N_G(X) = \{g \in G;\ gXg^{-1} = X\}$ heißt Normalisator von X.

9.2 Definition: Sei p prim. Eine endliche Gruppe G heißt *p-Gruppe*, falls $|G| = p^k$. Ist $|G| = m \cdot p^k$ mit $p \nmid m$, so heißt eine Untergruppe $S < G$ *p-Sylowuntergruppe*, falls $|S| = p^k$.

9.3 Lemma: Operiert eine p-Gruppe G auf einer endlichen Menge M, so gilt

$$|M| \equiv |M^G| \qquad \mod p \quad \text{(vgl.4.20)}$$

Beweis:: M zerfällt in disjunkte Bahnen

$$M = G * x_1 \sqcup \ldots \sqcup G * x_k$$

und $|G * x_i| = \dfrac{|G|}{|G_{x_i}|} = p^{s_i}$, für ein geeignetes s_i nach 8.9.
Folglich ist $|G * x_i| \equiv 0$, falls nicht $G_{x_i} = G$, d.h. falls nicht $x_i \in M^G$. Jedes Element aus M^G bilden selbst je eine vollständige Bahn. Also

$$|M| \equiv |M^G| \qquad \mod p$$

□

9.4 Satz: Sei G eine p-Gruppe, $|G| = p^k$, $k > 0$. Dann ist das Zentrum $Z(G) \neq \{e\}$.

Beweis:: Betrachte die Konjugationsoperation von G auf sich. Dann ist $Z(G)$ die Fixpunktmenge. Also nach 9.3

$$|Z(G)| \equiv |G| = p^k \equiv 0 \qquad \mod p$$

Damit hat $Z(G)$ mindestens p Elemente. □

9.5 Aufgabe: Zeigen Sie: (1) $G/Z(G)$ zyklisch $\Rightarrow G$ abelsch.
(2) $|G| = p^2$, p prim $\Rightarrow G$ abelsch (benutzen Sie 9.4).

9.6 Für jedes fest gewählt $g \in G$ ist

$$\varphi : G \to G, \quad x \mapsto g \cdot x \cdot g^{-1}$$

ein Automorphismus. (Die Abbildung $x \mapsto g^{-1} \cdot x \cdot g$ ist die Umkehrabbildung). Also ist mit U auch $\varphi(U) = g \cdot U \cdot g^{-1}$ eine Untergruppe von G, und ist U Sylowuntergruppe, dann auch $g \cdot U \cdot g^{-1}$.

9.7 Die Sylowsätze: (Ludwig Sylow, 1832-1918, norwegischer Gymnasiallehrer) Sei G eine endliche Gruppe der Ordnung $|G| = p^k \cdot m$ mit $p \nmid m$. Dann gilt:

(1) G besitzt Untergruppen $U_1 < U_2 < \ldots < U_k$ mit $|U_i| = p^i$, insbesondere ist U_k eine p-Sylowuntergruppe S.

(2) Die Anzahl n_p der verschiedenen p-Sylowuntergruppen von G erfüllt

$$n_p \equiv 1 \qquad \mod p, \quad \text{und} \quad n_p \text{ teilt } m.$$

(3) Jede p-Untergruppe H in G ist in einer p-Sylowuntergruppe enthalten.

(4) Alle p-Sylowuntergruppen von G sind konjugiert.

9.8 Lemma: Ist $p \nmid m$, dann gilt für $1 \leq s \leq k$

$$\binom{mp^k}{p^s} = m \cdot p^{k-s} \cdot \binom{mp^k - 1}{p^s - 1}, \quad \text{und} \quad p \nmid \binom{mp^k - 1}{p^s - 1}$$

Beweis::

$$\begin{aligned}
\binom{mp^k}{p^s} &= \frac{m \cdot p^k \cdot (mp^k - 1) \cdot \ldots \cdot (mp^k - p^s + 1)}{p^s \cdot (p^s - 1) \cdot \ldots 1} \\
&= m \cdot p^{k-s} \cdot \binom{mp^k - 1}{p^s - 1} \\
&= m \cdot p^{k-s} \cdot \prod_{i=1}^{p^s - 1} \frac{mp^k - i}{i}
\end{aligned}$$

Wir betrachten die Faktoren im Zähler des Produktes: Für $1 \leq i \leq p^s - 1$ gilt

$$mp^k - i = q \cdot p^r \iff i = mp^k - qp^r$$

(wir wählen r maximal, d.h. $p \nmid q$). Angenommen $r \geq k$, dann klammern wir p^k aus und erhalten $i = p^k(m - qp^{r-k}) \geq p^k$, was wegen $i \leq p^s - 1 < p^k$ unmöglich ist. Also ist $r < k$ und $i = p^r(mp^{k-r} - q)$. Damit läßt sich p^r im Faktor $mp^k - i$ des Zählers gegen p^r im Faktor i des Nenners kürzen, d.h. das Produkt hat nach Kürzen keinen Faktor p im Zähler. □

Beweis von 9.7: Sei $\mathcal{X} = \mathcal{P}_{p^s}(G)$ $1 \leq s \leq k$. Bekanntlich gilt $|\mathcal{X}| = \binom{n}{p^s}$. Unter der Linkstranslation mit $g \in G$ zerfällt $\mathcal{X}$ in disjunkte Orbits, und wir erhalten

$$\binom{n}{p^s} = |\mathcal{X}| = |G \cdot X_1| + \ldots + |G \cdot X_r| = \frac{|G|}{|S_1|} + \ldots + \frac{|G|}{|S_r|}$$

wobei S_i die Standuntergruppe der *Menge* X_i ist, d.h. $g \in S_i$ bildet X_i bijektiv nach X_i ab. Da $p^{k-s+1} \nmid \binom{n}{p^s}$ nach 9.8, gibt es mindestens einen Summanden, etwa $\frac{|G|}{|S_1|}$, der nicht durch p^{k-s+1} teilbar ist. Da $p^k \mid |G|$, folgt $p^s \mid |S_1|$. Sei nun $x \in X_1$. Da S_1 Standuntergruppe von X_1 ist, folgt $S_1 \cdot x \subset X_1$. Aber Rechttranslation mit x ist bijektiv. Es folgt

$$|S_1| = |S_1 \cdot x| \leq |X_1| = p^S. \quad \text{Also } |S_1| = p^s.$$

Mit $s = k$ erhalten wir eine Sylowuntergruppe $S_1 = U_k$ von G.

Wir wenden unsere Überlegungen nun auf U_k an mit $s = k - 1$ und erhalten eine Untergruppe U_{k-1} der Ordnung p^{k-1}. Durch Abwärtsinduktion folgt Teil (1) von 9.7.

Sei nun S eine p-Sylowuntergruppe. Sei nun $H < G$ eine p-Gruppe. Die Zuordnung

$$H \times G/S \to G/S, \quad (h, g \cdot S) \mapsto h \cdot g \cdot S \qquad (*)$$

definiert eine Operation von H auf G/S. Nach 9.3 gilt

$$|(G/S)^H| \equiv |G/S| = m \not\equiv 0 \qquad \text{mod } p.$$

Also besitzt diese Operation Fixpunkte, d.h. es gibt eine Nebenklasse $g \cdot S$ mit $h \cdot g \cdot S = g \cdot S$ für alle $h \in H$. Es folgt

$$\begin{array}{rl} H \cdot g & \subset H \cdot g \cdot S = g \cdot S \\ H & < g \cdot S \cdot g^{-1} \end{array} \qquad (A)$$

Ist H selbst Sylowuntergruppe, so folgt wegen $|H| = p^k = |g \cdot S \cdot g^{-1}|$, dass

$$H = g \cdot S \cdot g^{-1}$$

Das beweist (3) und (4).
Für (2) wenden wir diese Überlegungen auf $H = S$ an. Wir erhalten

$$|G/S| \equiv |(G/S)^S| \mod p$$

und $g \cdot S \in (G/S)^S \iff S = g \cdot S \cdot g^{-1}$ nach (A)
Aber $g \cdot S \cdot g^{-1} = S \iff g \in N_G(S)$, so dass

$$|G/S| \equiv |(G/S)^S| = |N_G(S)/S| \not\equiv 0 \mod p \qquad (**)$$

Betrachten wir jetzt die Bahn $\mathcal{E}$ von S unter der Konjugationsoperation, also die Konjugationsklasse von S. Dann gilt nach 9.7

$$n_p \stackrel{def}{=} |\mathcal{E}| = \frac{|G|}{|N_G(S)|} = \frac{|G/S|}{|N_G(S)/S|} \equiv 1 \mod p$$

wegen $(**)$. Da $m = |G/S| = n_p \cdot |N_G(S)/S|$, folgt n_p teilt m.
Beim letzten Schritt argumentieren wir im Restklassenkörper modulo p. Die Restklassen von $|G/S|$ und $|N_G(S)/S|$ sind gleich und von 0-Klassen verschieden. Die Division im Restklassenkörper ergibt daher die Restklasse von 1. □
Für Anwendungen vermerken wir als Konsequenz aus 9.6 und 9.7.4.

9.9 Hat eine endliche Gruppe G genau eine p-Sylowuntergruppe S, dann ist S Normalleiter.

9.10 Satz: Hat G für jeden Primteiler p von $|G|$ genau eine p-Sylowuntergruppe, dann ist G inneres Produkt seiner Sylowuntergruppen.

Beweis:: Seien $p_1, \ldots, p_k$ die Primteiler von $|G|$ und $S_1, \ldots, S_k$ die zugehörigen Sylowuntergruppen. Durch Induktion nach l zeigen wir, dass

$$f : S_1 \times \ldots \times S_l \to G, \quad (x_1, \ldots, x_l) \mapsto x_1 \cdot \ldots \cdot x_l$$

ein Monomorphismus ist. Da $|S_1 \times \ldots \times S_k| = |G|$, folgt die Behauptung.
Für $l = 1$ ist nichts zu zeigen.
Induktionsschritt von $l-1$ nach l: Nach Induktionsannahme ist

$$U = f(S_1 \times \ldots \times S_{l-1}) = S_1 \cdot \ldots \cdot S_{l-1}$$

eine Untergruppe von G isomorph zu $S_1 \times \ldots \times S_{l-1}$. Da

$$\begin{aligned} g \cdot S_1 \cdot \ldots \cdot S_{l-1} \cdot g^{-1} &= g \cdot S_1 \cdot g^{-1} \cdot g \cdot S_2 \cdot g^{-1} \ldots g \cdot S_{l-1} \cdot g^{-1} \\ &= S_1 \cdot S_2 \cdot \ldots \cdot S_{l-1}, \end{aligned}$$

ist $U \lhd G$. Nach 9.9 ist $S_l \lhd G$. Weiter ist $U \cap S_l$ Untergruppe von U und von S_l. Da $|U|$ und $|S_l|$ teilerfremd sind, folgt $U \cap S_l = \{e\}$. Nach 5.6 ist

$$f : U \times S_l \to G \quad , (u, x) \mapsto u \cdot x$$

injektiv. □

9.11 Satz: Seien $p < q$ Primzahlen und $q \not\equiv 1 \mod p$, dann ist jede Gruppe der Ordnung pq isomorph zu $\mathbb{Z}/pq$.

Beweis:: $n_p = 1 \mod p$ und $n_p \mid q$. Da q prim ist, folgt $n_p = 1$ oder $n_p = q$. Da aber $q \not\equiv 1 \mod p$, erhalten wir $n_p = 1$, $n_q \equiv 1 \mod q$ und $n_q | p$. Da $p < q$, folgt $n_q = 1$.
Nach 9.10 ist $G \cong S_p \times S_q$. Weiter gilt $S_p \times S_q \cong \mathbb{Z}/p \times \mathbb{Z}/q \cong \mathbb{Z}/p \cdot q$ nach 4.19 und 5.7. □

9.12 Beispiel: Ist G eine Gruppe der Ordnung 45, dann ist G abelsch.

Beweis:: $45 = 3^2 \cdot 5$
$n_3 \equiv 1 \mod 3$ und $n_3 \mid 5$. Es folgt $n_3 = 1$.
$n_5 \equiv 1 \mod 5$ und $n_5 \mid 9$. Es folgt $n_5 = 1$.
Also $G \cong S_3 \times S_5$. Da $|S_5| = 5$ ist $S_5 \cong \mathbb{Z}/5$. Da $|S_3| = 9$, ist S_3 nach 9.5 abelsch. Also ist G abelsch. □

Der Beweis von 9.12 lässt sich verallgemeinern:

9.13 Aufgabe: Es seien $p < q$ Primzahlen und G eine Gruppe. Zeigen Sie: G ist abelsch, wenn eine der folgenden Bedingungen erfüllt ist:

(1) $|G| = p^2 \cdot q$ und $q \not\equiv 1 \mod p$ und $p^2 \not\equiv 1 \mod q$

(2) $|G| = p \cdot q^2$ und $q^2 \not\equiv 1 \mod p$

(3) $|G| = p^2 \cdot q^2$ und $p^2 \not\equiv 1 \mod q$ und $q^2 \not\equiv 1 \mod p$

Die Bedeutung dieses Resultats liegt im Struktursatz für endlich erzeugte abelsche Gruppen.

9.14 Struktursatz: Sei G eine endlich erzeugte abelsche Gruppe. Dann gilt:

(1) $G \cong \mathbb{Z}^r \times T$, $r \geq 0$ und T endlich.

(2) Ist $p_1^{k_1} \cdot \ldots \cdot p_s^{k_s}$ mit $p_1 < p_2 < \ldots p_s$ die Primfaktorzerlegung von $|T|$, dann gilt

$$T \cong S_{p_1} \times \ldots \times S_{p_s}$$

wobei S_{p_i} die p_i-Sylowuntergruppe von T ist.

(3) Ist S eine abelsche p-Gruppe, $|S| = p^k$, dann ist S von der Form

$$S \cong \mathbb{Z}/p^{r_1} \times \ldots \times \mathbb{Z}/p^{r_t}$$

$r_1 \leq r_2 \leq \ldots \leq r_t$ und $r_1 + r_2 + \ldots + r_k = k$.

Teil (2) ist ein Spezialfall von 9.10. Die Beweise der Teile (1) und (3) müssen wir aus Zeitgründen schuldig bleiben

Teil II
Ringe und Körper

10 Grundlagen

10.1 Definition: Ein *Ring* ist eine Menge R mit zwei Verknüpfungen, der Addition $+$ und der Multiplikation $\cdot$, so dass folgende Axiome gelten

(1) $(R, +)$ ist abelsche Gruppe. Das neutrale Element bezeichnen wir mit 0.

(2) $(R, \cdot)$ ist ein Monoid. Das neutrale Element bezeichnen wir mit 1.

(3) Es gelten die Distributivgesetze

$$a \cdot (b + c) = a \cdot b + a \cdot c, \quad (b + c) \cdot a = b \cdot a + c \cdot a \quad \forall a, b, c \in R$$

Ist $(R, \cdot)$ kommutativ, sprechen wir von einem *kommutativen Ring*.

Konvention: In dieser Vorlesung betrachten wir nur kommutative Ringe, es sei denn, es wird ausdrücklich von nicht kommutativen Ringen gesprochen.

10.2 Definition: $a \in (R, +, \cdot)$ heißt *Einheit*, wenn a bzgl. der Multiplikation ein rechts- und ein linksinverses Element besitzt (die dann gleich sind). Die Gruppe (s. 2.5) der Einheiten von $(R, \cdot)$ wird mit R^* bezeichnet.

10.3 Definition: Ein *Unterring* von R ist eine Teilmenge $S \subset R$, so dass S unter den Verknüpfungen $+$ und $\cdot$ auf R selbst ein Ring ist und dasselbe Null- und Einselement besitzt.

10.4 Aufgabe: Sei $S \subset R$, dann ist S genau dann Unterring, wenn

(i) $x, y \in S \Rightarrow x + y \in S$ und $x \cdot y \in S$

(ii) $\pm 1 \in S$

10.5 Definition: Seien $a, b \in R \backslash \{0\}$ und sei $a \cdot b = 0$. Dann heißt a *Linksnullteiler* und b *Rechtsnullteiler*. Besitzt R keinerlei Nullteiler, so heißt R *nullteilerfrei*.

10.6 Definition: Ein *Integritätsring* ist ein kommutativer, nullteilerfreier Ring. Ein Ring R, für den $R^* = R \backslash \{0\}$ heißt *Körper*.

10.7 Definition: Eine Abbildung $f : R \to S$ von Ringen heißt *Homomorphismus von Ringen*, wenn

$$f(x+y) = f(x) + f(y) \quad f(x \cdot y) = f(x) \cdot f(y) \quad \forall x, y \in R$$

und

$$f(1_R) = 1_S$$

10.8 Ist $f : R \to S$ ein Ringhomomorphismus und $T \subset S$ ein Unterring, dann ist $f(R)$ ein Unterring von S und $f^{-1}(T)$ ein Unterring von R.

Der Beweis ist dem Leser überlassen.

Sei R ein Ring und U eine Untergruppe von $(R, +)$. Wir fragen uns, unter welchen Bedingungen die Faktorgruppe $(R/U, +)$ von R eine Ringstruktur erbt, so dass die Projektion

$$p : R \to R/U \quad r \mapsto r + U$$

ein Ringhomomorphismus ist. Da $(R, +)$ abelsch ist, existiert die Faktorgruppe $(R/U, +)$.
Wir bezeichnen die Nebenklasse $r + U$ wieder mit $\overline{r}$. Falls R/U ein Ring und p ein Ringhomomorphismus ist, muss gelten

$$\overline{r}_1 + \overline{r}_2 = \overline{r_1 + r_2} \quad \text{und} \quad \overline{r}_1 \cdot \overline{r}_2 = \overline{r_1 \cdot r_2}$$

Aus der Gleichung

$$p(r \cdot u) = p(r) \cdot p(u) = \overline{r} \cdot \overline{0} = \overline{0} = U$$

für $r \in R$ und $u \in U$ folgt

$$r \cdot u \in U \quad \forall r \in R, \quad \forall u \in U$$

Wir fassen diese notwendigen Bedingungen in eine Definition.

10.9 Definition: Sei R ein Ring. Eine Untergruppe U von $(R, +)$ heißt *Ideal*, wenn für $u \in U$ und $r \in R$ gilt $r \cdot u \in U$.

Ist $U \subset R$ ein Ideal, dann gilt für die übliche Multiplikation der Nebenklassen

$$(x+U) \cdot (y+U) = x \cdot y + x \cdot U + U \cdot y + U \cdot U \subset x \cdot y + U + U + U = x \cdot y + U$$

Da die Nebenklassen eine disjunkte Zerlegung von R bilden, wird jedem Paar unter der üblichen Multiplikation *eindeutig* eine Nebenklasse zugeordnet:

$$\overline{x} \cdot \overline{y} = (x + U) \cdot (y + U) \subset xy + U = \overline{x \cdot y}$$

Der folgende Satz ist damit trivial. (Der Beweis ist analog zum Gruppenfall.)

10.10 Satz: (1) Ist $U \subset R$ ein Ideal in einem Ring R, so ist R/U unter

$$\overline{x} + \overline{y} := \overline{x+y} \qquad \overline{x} \cdot \overline{y} := \overline{x \cdot y}$$

mit $\overline{x} = x + U$ ein Ring.

(2) Die Projektion $p : R \to R/U$ ist ein Ringhomomorphismus.

(3) Jedes Ideal ist Kern eines Ringhomomorphismus'. Umgekehrt ist der Kern eines Ringhomomorphismus' ein Ideal.

Der Isomorphisatz 4.17 überträgt sich nun leicht auf Ringe.

10.11 Isomorphisatz: Ist $f : R \to S$ ein Ringhomomorphismus mit

$$\text{Kern}\, f = \{r \in R; f(r) = 0\} = U,$$

dann gibt es genau einen Ringhomomorphismus $\overline{f} : R/U \to S$, so dass $\overline{f} \circ p = f$. Insbesondere gilt

$$\overline{f} : R/U \cong \text{Bild}\, f \quad \text{ als Ringe}$$

Beweis: Aus dem Isomorphisatz für Gruppen wissen wir, dass es genau eine Gruppenhomomorphismus $\overline{f} : (R/U, +)) \to (S, +)$ gibt, so dass $\overline{f} \circ p = f$. Es bleibt also nur zu zeigen, dass $\overline{f}$ ein Ringhomomorphismus ist:
$\overline{f}(\overline{1}) = \overline{f}(p(1)) = f(1) = 1$, also erhält $\overline{f}$ die Eins

$$\begin{aligned} \overline{f}(\overline{r}_1 \cdot \overline{r}_2) &= \overline{f}(p(r_1) \cdot p(r_2)) = \overline{f}(p(r_1 \cdot r_2)) = f(r_1 \cdot r_2) = f(r_1) \cdot f(r_2) \\ &= \overline{f}(p(r_1)) \cdot \overline{f}(p(r_2)) = \overline{f}(\overline{r}_1) \cdot \overline{f}(\overline{r}_2). \end{aligned}$$

□

10.12 Aufgaben:

(1) Ist $\{U_\alpha, \alpha \in A\}$ eine Familie von Idealen in R, dann ist auch $\bigcap\limits_{\alpha \in A} U_\alpha$ ein Ideal

(2) Ist $J_1 \subset J_2 \subset J_3 \subset \ldots$ eine aufsteigende Kette von Idealen in R, dann ist auch $\bigcup\limits_{n=1}^{\infty} J_n$ ein Ideal in R.

(3) Sind I und J Ideale von R, dann ist auch $I + J \subset R$ ein Ideal.

(4) Ist $f : R \to S$ ein Ringhomomorphismus und $J \subset S$ ein Ideal, dann ist $f^{-1}(J) \subset R$ ein Ideal.

Ist f *surjektiv* und I ein Ideal von R, dann ist $f(I)$ ein Ideal von S.

10.13 Definition und Satz: Sei $A \subset R$ eine Teilmenge. Das kleinste Ideal $I(A)$ von R, das A enthält, heißt das von A *erzeugte Ideal*. Es gilt

$$I(A) = \bigcap \{U \subset R;\ U \text{ Ideal },\ A \subset U\}$$

Ein Ideal, das von einem einzigen Element erzeugt wird, heißt *Hauptideal*. Statt $I(\{a\})$ schreiben wir nur (a).

10.14 $(a) = R \cdot a$

Beweis: Da $a \in (a)$ und (a) ein Ideal ist, ist $r \cdot a \in (a)$ für alle $r \in R$, also $R \cdot a \subset (a)$. Weiter ist $R \cdot a$ ein Ideal, denn

(i) $R \cdot a \neq \emptyset$

(ii) mit $r_1 \cdot a$, $r_2 \cdot a \in R \cdot a$ ist $r_1 \cdot a - r_2 \cdot a = (r_1 - r_2) \cdot a \in R \cdot a$. Also ist $R \cdot a$ Untergruppe von $(R, +)$.

(iii) mit $r_1 \cdot a$ ist auch $r \cdot (r_1 \cdot a) = (r \cdot r_1) \cdot a \in R \cdot a$.

$R \cdot a$ enthält $a = 1 \cdot a$. Da (a) das kleinste Ideal ist, das a enthält, folgt $(a) \subset R \cdot a$, insgesamt also $R \cdot a = (a)$. □

10.15 Definition: Ein *Hauptidealring* oder PID (für "principal ideal domain") ist ein Integritätsring, in dem jedes Ideal ein Hauptideal ist.

10.16 Beispiel: $\mathbb{Z}$ ist ein Hauptidealring: Jede Untergruppe $n \cdot \mathbb{Z}$, $n \in \mathbb{N}_0$, ist nach 10.14 ein Hauptideal. Die Faktorringe $\mathbb{Z}/(n \cdot \mathbb{Z})$ sind die aus dem Grundkurs bekannten Restklassenringe.

10.17 Wir wollen uns die Ideale von $\mathbb{Z}$ näher anschauen: $a|b$ bedeute "a teilt b", d.h. es gibt ein x, so dass $a \cdot x = b$. Dann gilt:

(1) $a|b \iff (b) \subset (a)$. Denn: $a|b \iff b \in a \cdot \mathbb{Z} = (a) \iff (b) \subset (a)$

(2) $(a) + (b) = (d)$ mit $d = ggT(a, b)$

Beweis: $d|a$ und $d|b \Rightarrow (a) \subset (d)$ und $(b) \subset (d) \Rightarrow (a) + (b) \subset (d)$. Da $\mathbb{Z}$ ein Hauptidealring ist, gilt $(a) + (b) = (r)$ für ein $r \in \mathbb{N}_0$. Da $(a) \subset (r)$, gilt $r|a$, analog gilt $r|b$. Da nun $d = ggT(a, b)$, folgt $r|d$, also $(d) \subset (r) = (a) + (b)$.

(3) $(a) \cap (b) = (v)$ mit $v = kgV(a,b)$

Beweis: $v = kgV(a,b) \Rightarrow a|v$ und $b|v \Rightarrow (v) \subset (a)$, $(v) \subset (b) \Rightarrow (v) \subset (a) \cap (b)$. Wieder gibt es eine $r \in \mathbb{N}$, so dass $(a) \cap (b) = (r)$. Es folgt $(r) \subset (a)$, $(r) \subset (b)$, also $b|r$ und $a|r$. Da $v = kgV(a,b)$, folgt $v|r$, also $(r) \subset (v)$.

Wir haben somit eine idealtheoretische Interpretation des ggT und kgV.

10.18 Definition: Ein Ring R heißt *einfach*, wenn 0 und R seine einzigen Ideale sind.

10.19 Definition: Ein Ideal J von R heißt *maximal*, wenn $J \neq R$ und aus $J \subset U \subset R$, U Ideal, folgt $J = U$ oder $U = R$.

Die Bedeutung maximaler Ideale dokumentieren folgende Sätze.

10.20 Satz: Ein Ring R ist genau dann einfach, wenn er ein Körper ist.

10.21 Satz: $J \subset R$ ist maximal $\iff$ R/J ist einfach $\iff$ R/J ist ein Körper.

Beweis 10.20: Sei R einfach und $x \in R$, $x \neq 0$. Wir müssen zeigen, dass x^{-1} existiert. $R \cdot x$ ist ein von 0 verschiedenes Ideal, also $R \cdot x = R$. Insbesondere gibt es $r \in R$, so dass $r \cdot x = 1$, d.h. $r = x^{-1}$.

Sei umgekehrt R ein Körper und $J \neq 0$ ein Ideal in R. Dann gibt es ein $x \neq 0$ in J, und weil J ein Ideal ist, folgt $x^{-1} \cdot x = 1 \in J$. Damit ist für jedes $r \in R$ auch $r = r \cdot 1 \in J$, also $R = J$. □

Beweis 10.21: Sei $p : R \to R/J$ die Projektion und $V \neq \{\overline{0}\}$ eine Ideal in R/J. Dann ist $U = p^{-1}(V)$ nach 10.12 ein Ideal in R, und

$$J = p^{-1}(\overline{0}) \subsetneq U \subset R.$$

Ist J maximal, folgt $U = R$ und $V = p(U) = R/J$, d.h. $\{\overline{0}\}$ und R/J sind die einzigen Ideale von R/J.

Ist umgekehrt R/J einfach und $J \subsetneq U \subset R$ ein Ideal, dann ist nach 10.12 auch $p(U)$ ein Ideal von R/J. Da $p(U) \neq \{\overline{0}\}$, ist $p(U) = R/J$. Also gibt es zu jedem $r \in R$ ein $u \in U$, so dass $\overline{u} = p(u) = \overline{r}$, d.h. $r - u = j \in J$. Da $J \subset U$, folgt $r = u + j \in U$, also $U = R$. Damit ist J maximal.

Das beweist die erste Äquivalenz. Die zweite folgt aus 10.20. □

11 Teilerlehre in Ringen

Wir erinnern zunächst an die elementaren Definitionen aus dem Grundkurs.

11.1 Definition: Sei R ein Ring, $a, b, c \in R$.

(1) a *teilt* b, in Zeichen $a|b$, wenn es ein $x \in R$ gibt, so dass $a \cdot x = b$.

(2) a ist *assoziiert* zu b, in Zeichen $a \sim b$, wenn $a|b$ und $b|a$.

(3) c heißt *prim*, wenn $c \neq 0$, $c \notin R^*$ und aus $c|a \cdot b$ folgt, dass $c|a$ oder $c|b$.

(4) c heißt *irreduzibel* , wenn $c \neq 0$, $c \notin R^*$ und aus $c = a \cdot b$ folgt, dass $a \in R^*$ oder $b \in R^*$.

11.2 Lemma: Für $a, b \in R$ und $u \in R^*$ gilt

(0) Ist J ein Ideal, das u enthält, dann gilt $J = R$.

(1) $a = u \cdot b \Rightarrow a \sim b \iff (a) = (b)$.

(2) $\{(a) = R \text{ oder } (a) = (b)\} \overset{(*)}{\Rightarrow} (b) \subset (a) \iff a|b$.
Ist b irreduzibel, gilt auch die Umkehrung von $(*)$.

Beweis: (0) Da $u \in J$ und J ein Ideal ist, liegt jedes $x = (x \cdot u^{-1}) \cdot u$ in J. Also $J = R$.
(1) Aus $a = u \cdot b$ und $b = u^{-1} \cdot a$ folgt $b|a$ und $a|b$, also $a \sim b$. Weiter gilt:

$$a \sim b \iff \{a|b \text{ und } b|a\} \iff \{(b) \subset (a) \text{ und } (a) \subset (b)\}$$

.
(2) Der erste Teil ist trivial. Ist $a|b$, so gibt es ein x mit $a \cdot x = b$. Da b irreduzibel ist, ist entweder $a \in R^*$ oder $x \in R^*$. Ist $a \in R^*$, dann existiert a^{-1}, und für alle $r \in R$ ist $r = (r \cdot a^{-1}) \cdot a \in (a)$, also $(a) = R$. Ist $x \in R^*$, haben wir $a = x^{-1} \cdot x \cdot a = x^{-1} \cdot b \in (b)$, also $(a) \subset (b)$ und mit $(b) \subset (a)$ auch $(a) = (b)$. □

11.3 Satz: Sei $c \neq 0$ und $c \notin R^*$. Dann ist c genau dann prim, wenn $R/(c)$ ein Integritätsring ist.

Beweis: Sei c prim und $\overline{r} \cdot \overline{s} = \overline{0}$ in $R/(c)$. Dann sind $r \cdot s \in (c)$, d.h. $c|r \cdot s$. Da c prim ist, teilt c entweder r und s, d.h. r oder s liegen in (c), so dass $\overline{r} = \overline{0}$ oder $\overline{s} = \overline{0}$.
Sei umgekehrt $R/(c)$ ein Integritätsring und $c|a \cdot b$. Dann folgt $\overline{0} = \overline{a \cdot b} = \overline{a} \cdot \overline{b}$, also $\overline{a} = \overline{0}$ oder $\overline{b} = \overline{0}$, etwa $\overline{a} = \overline{0}$. Dann ist $a \in (c)$, also $c|a$. □

11.4 Lemma: In einem Integritätsring gilt

(1) jedes Primelement ist irreduzibel.

(2) $a \sim b \iff \exists\, u \in R^*$ mit $a = u \cdot b$.

Beweis: (1) Sei c prim und $c = a \cdot b$. Da dann $c|a \cdot b$, folgt $c|a$ oder $c|b$, etwa $c|a$. Dann gibt es ein $r \in R$ mit $c \cdot r = a$. Es folgt $c = a \cdot b = c \cdot r \cdot b$. Da $c \neq 0$, darf man kürzen (R ist Integritätsring), also $1 = r \cdot b$, d.h. $b \in R^*$.
(2) $a \sim b \iff a|b$ und $b|a \iff \exists\, x, y \in R$ mit $a \cdot x = b$ und $b \cdot y = a$. Es folgt $a = b \cdot y = a \cdot x \cdot y$. Ist $a \neq 0$, können wir a kürzen und erhalten $x \cdot y = 1$, d.h. $y \in R^*$. Ist $a = 0$, folgt $b = a \cdot x = 0$ und damit $a = 1 \cdot b$.
Die Rückrichtung wurde bereits in 11.2 gezeigt. □

11.5 Lemma: In einem Hauptidealring R gilt für $b \neq 0$

$$b \text{ irreduzibel} \iff (b) \text{ maximal} \iff b \text{ prim.}$$

Beweis: b irreduzibel $\Rightarrow$ (b) maximal. Dann sei (a) ein Ideal in R mit $(b) \subset (a)$, dann folgt $a|b$ und aus (11.2(2)), dass $(a) = R$ oder $(a) = (b)$
(b) maximal $\Rightarrow$ b prim. Denn nach (10.21) und (10.20) ist $R/(b)$ ein Körper, also insbesondere ein Integritätsring. Nach (11.3) ist b somit prim.
b prim $\Rightarrow$ b irreduzibel: folgt aus (11.4). □
Wir wollen jetzt das Problem der eindeutigen Primfaktorzerlegung angehen.

11.6 Definition: Ein *faktorieller* Ring (UFD= "unique factorization domain") ist ein Integritätsring R, in dem sich jedes $a \neq 0$, $a \notin R^*$ als Produkt von Primelementen schreiben läßt.

11.7 Satz: In einem faktoriellen Ring R gilt

(1) Jedes irreduzibel Element ist prim.

(2) Ist $a \neq 0$, $a \notin R^*$, und sind

$$a = p_1 \cdot \ldots \cdot = q_1 \cdot \ldots \cdot q_s$$

zwei Zerlegungen von a in Primelemente, dann ist $r = s$ und nach einer Umnummerierung der q_i gibt es zu jedem p_i ein $u_i \in R^*$ mit $q_i = u_i \cdot p_i$.

D.h. die Primfaktorzerlegung von a ist bis auf Reihenfolge und Multiplikation mit Einheiten eindeutig.

Beweis: (1) Sei a irreduzibel und p ein Primfaktor von a, also $a = p \cdot x$. Dann gilt $x \in R^*$, da a irreduzibel und $p \notin R^*$ ist. Es folgt $a \sim p$ und somit $(a) = (p)$. Aus 11.3 folgt, dass a prim ist.

(2) $p_1|q_1 \cdot \ldots \cdot q_s$. Da p_1 prim ist, gibt es ein i, so dass $p_1|q_i$ (wende die Definition 11.1.3 induktiv an). Wir nummerieren die q_i so um, dass $p_1|q_1$. Da q_1 irreduzibel ist und $p_1 \notin R^*$, folgt aus (11.2(2)), dass $(p_1) = (q_1)$. Also gibt es ein $u_1 \in R^*$, so dass $q_1 = u_i p_1$ nach (11.4(2)). Es folgt

$$p_1 \cdot p_2 \cdot \ldots \cdot p_r = p_1 \cdot u_1 \cdot q_2 \cdot \ldots \cdot q_s$$

Wir kürzen und erhalten

$$q_2 \cdot \ldots \cdot p_r = (u_1 \cdot q_2) \cdot q_3 \cdot \ldots \cdot q_s$$

Da $(u_1 \cdot q_2)$ ebenfalls prim ist, können wir induktiv fortfahren. Es folgt $r = s$ und die Aussage des Satzes. □

Im Grundkurs wurde gezeigt, dass jedes Element aus $\mathbb{Z}$ eine eindeutige Primfaktorzerlegung im obigem Sinne hat. Damit ist $\mathbb{Z}$ ein UFD. Z.B. gilt

$$6 = 2 \cdot 3 = 3 \cdot 2 = (-2) \cdot (-3) = (-3) \cdot (-2)$$

Um weitere Beispiele faktorieller Ringe zu erhalten, wollen wir zeigen

11.8 Satz: Jeder Hauptidealring ist faktoriell.

Das bedarf einer kleinen Vorbereitung:

11.9 Lemma: Sei R ein Hauptidealring und $J_1 \subset J_2 \subset J_3 \subset \ldots$ eine aufsteigende Idealkette. Dann gibt es ein n, so dass $J_n = J_{n+k}\ \forall k \in \mathbb{N}$. (Einen kommutativen Ring mit dieser Eigenschaft nennt man *noethersch*.)

Beweis:: Nach (10.12) ist $J = \bigcup_{k\in\mathbb{N}} J_k$ ein Ideal. Also gibt es ein $a \in R$, so dass $(a) = J$. Dann gibt es ein n, so dass $a \in J_n$. Es folgt $J_{n+k} \subset J = (a) \subset J_n$. □

11.10 Bemerkung: In einem noetherschen Ring kann es durchaus unendliche streng absteigende Idealketten geben. Da $\mathbb{Z}$ ein Hauptidealring ist, ist $\mathbb{Z}$ noetherisch, aber

$$(p) \supset (p^2) \supset (p^3) \supset (p^4) \supset \ldots$$

p prim, ist eine unendliche streng absteigende Idealkette.

Beweis von 11.8: Sei $x \neq 0$ aus R, $x \notin R^*$. Da in einem Hauptidealring "irreduzibel" und "prim" dasselbe sind, genügt es, x in ein Produkt irreduzibler Elemente zu zerlegen.

Angenommen, das ist unmöglich. Dann besitzt $x = x_0$ eine Zerlegung (sonst wäre es irreduzibel)

$$x_0 = x_1 \cdot y_1 \quad x_1, y_1 \neq 0,\ x_1, y_1 \notin R^*$$

und mindestens eines von x_1 oder y_1 besitzt keine Zerlegung in irreduzible Elemente, etwa x_1. Es folgt $(x_0) \subset (x_1)$. Weiter gilt $(x_0) \neq (x_1)$, denn nach 11.4.2 gibt es sonst ein $u \in R^*$ mit $x_0 = u \cdot x_1$. Es folgt dann $u \cdot x_1 = x_0 = y_1 \cdot x_1$ und nach Kürzen $y_1 = u \in R^*$, ein Widerspruch.

Wir wenden das Argument auf x_1 an und erhalten

$$x_1 = x_2 \cdot y_2 \quad x_2, y_2 \neq 0 \quad x_2, y_2 \notin R^*$$

und x_2 besitzt keine Zerlegung in irreduzible Elemente. Wieder gilt $(x_1) \subsetneqq (x_2)$. Wir fahren fort und erhalten eine unendliche aufsteigende Idealkette

$$(x_0) \subsetneqq (x_1) \subsetneqq (x_2) \subsetneqq (x_3) \subsetneqq \ldots$$

im Widerspruch zu (11.9). □

Um neue Beispiele zu finden, müssen wir also Hauptidealringe konstruieren. Dazu führen wir einen neuen Typ von Ring ein, der Eigenschaften besitzt, die an die ganzen Zahlen erinnern.

11.11 Definition: Ein *euklidischer Ring* ist ein Integritätsring R mit einer Abbildung

$$\delta : R\backslash\{0\} \to \mathbb{N}_0,$$

so dass

(1) $\delta(x) \leq \delta(x \cdot y) \quad \forall x, y \in R\backslash\{0\}$

(2) zu $b \in R\backslash\{0\}$ und $a \in R$ existieren $q, r \in R$, so dass

$$a = q \cdot b + r, \qquad \text{wobei } r = 0 \text{ oder } \delta(r) < \delta(b).$$

11.12 Beispiel: (s. Grundkurs)

(1) $\mathbb{Z}$ mit $\delta(x) = |x|$ ist ein euklidischer Ring.

(2) Der Polynomring $\mathbb{K}[x]$ über einem *Körper* ist euklidisch mit $\delta(f) = \operatorname{grad} f$.

11.13 Satz: Jeder euklidische Ring R ist ein Hauptidealring.

Der Beweis ist praktisch wörtlich derselbe wie für $\mathbb{Z}$ (vgl. Grundkurs): Sei $J \neq 0$ ist Ideal in R. Wähle $a \in J$ derart, dass $\delta(a) = \min\{\delta(x); x \in J\backslash\{0\}\}$. Da $a \in J$, folgt $(a) \subset J$.
Sei umgekehrt $x \in J$ beliebig. Da $a \neq 0$, gibt es $q, r \in R$ mit

$$x = q \cdot a + r, \quad \text{wobei } r = 0 \text{ oder } \delta(r) < \delta(a).$$

$r = x - q \cdot a \in J$, da x und a aus J sind. Nach Wahl von a, kann daher $\delta(r) < \delta(a)$ nicht zutreffen. Es folgt $r = 0$ und damit $x \in (a)$. □
Die euklidische Ringstruktur hat weitere Vorteile.

11.14 Satz: In einem euklidischen Ring R gilt

(1) $\delta(1) \leq \delta(x) \quad \forall x \in R\backslash\{0\}$

(2) $x \in R^* \iff \delta(x) = \delta(1)$

Beweis: (1) Nach (11.11.(1)) gilt $\delta(1) \leq \delta(1 \cdot x) = \delta(x)$.
(2) $x \in R^* \Rightarrow \exists y \in R$ mit $x \cdot y = 1 \Rightarrow \delta(1) \leq \delta(x) \leq \delta(x \cdot y) = \delta(1)$.
Sei umgekehrt $\delta(x) = \delta(1)$. Dann gibt es $q, r \in R$ mit

$$1 = q \cdot x + r, \quad \text{wobei } r = 0 \text{ oder } \delta(r) < \delta(x) = \delta(1).$$

Nach (1) ist $\delta(r) < \delta(1)$ nicht möglich. Also ist $r = 0$ und $q = x^{-1}$. □
In euklidischen Ringen kann man darüber hinaus größte gemeinsame Teiler auf einfache Weise finden. Wir wollen jetzt den Begriff des ggT bzw kgV in beliebigen kommutativen Ringen definieren.

11.15 Definition: Seien $a_1, \ldots, a_n \in R$. Wir nennen $d \in R$ *einen* $ggT(a_1, \ldots, a_n)$, wenn

(i) $d|a_i \; \forall i$

(ii) $r|a_i \; \forall i \Rightarrow r|d$

Wir nennen $v \in R$ *ein* $kgV(a_1, \ldots, a_n)$, wenn

(i) $a_i|v \; \forall i$

(ii) $a_i|r \; \forall i \Rightarrow v|r$

11.16 Aufgaben:

(1) Seien $a_1, \ldots, a_n \in R$. Sei d ein $ggT(a_1, \ldots, a_n)$ und v ein $kgV(a_1, \ldots, a_n)$. Zeigen Sie:

(i) d' ist ein $ggT(a_1, \ldots, a_n) \iff d$ und d' sind assoziiert.

(ii) v' ist ein $kgV(a_1, \ldots, a_n) \iff v$ und v' sind assoziiert.

(2) Sei R ein Hauptidealring und seien $a_1, \ldots, a_n \in R$. Zeigen Sie

(i) d ist $ggT(a_1, \ldots, a_n) \iff (d) = (a_1) + \ldots + (a_n)$

(ii) v ist $kgV(a_1, \ldots, a_n) \iff (v) = (a_1) \cap \ldots \cap (a_n)$

(vgl. (10.17)). Insbesondere gibt es in Hauptidealringen stets größte gemeinsame Teiler und kleinste gemeinsame Vielfache.

11.17 Warnung: In faktoriellen Ringen braucht (11.16) nicht zu gelten! Hier haben wir aber eine andere Möglichkeit, den ggT oder das kgV zu finden, eine Möglichkeit, die man in der Schule für $R = \mathbb{Z}$ intensiv nutzt.

11.18 Satz: In einem faktoriellen Ring existieren $ggT(a_1, \ldots, a_n)$ und $kgV(a_1, \ldots, a_n)$.

11.19 Konstruktion von ggT(a, b), kgV(a, b): Seien

$$a = p_1^{r_i} \ldots p_n^{r_n} \text{ und } b = p_1^{s_1} \ldots p_n^{s_n} \text{ mit } 0 \leq r_i,\ 0 \leq s_i$$

Primfaktorzerlegungen von a und b. Dann ist

$$d = p_1^{t_1} \cdot \ldots \cdot p_n^{t_n} \text{ mit } t_i = \min(r_i, s_i),\ i = 1, \ldots, n$$

ein $ggT(a, b)$ und

$$v = p_1^{u_1} \cdot \ldots \cdot p_n^{u_n} \text{ mit } u_i = \max(r_i, s_i),\ i = 1, \ldots, n$$

ein $kgV(a, b)$.
Der Beweis ist trivial und der allgemeine Fall $ggT(a_1, \ldots, a_n)$ wird entsprechend behandelt.

11.20 Bemerkung: Aus (11.16) erhalten wir: Ist R ein Hauptidealring und $d = ggT(a, b)$, dann besitzt d eine Darstellung

$$d = r \cdot a + s \cdot b \text{ mit } r, s \in R$$

Diese Darstellung findet in der Zahlentheorie viele Anwendungen. In euklidischen Ringen gibt es konstruktive Verfahren für das Auffinden solcher Darstellungen, der uns aus dem Grundkurs vertraute euklidische Algorithmus.

11.21 Der euklidische Algorithmus: Sei R euklidischer Ring .
Sei $r_0 \in R$ und $r_1 \in R\backslash\{0\}$. Wir konstruieren induktiv eine Folge

$$r_0, r_1, r_2, \ldots \quad \text{mit } \delta(r_1) > \delta(r_2) > \ldots \tag{$*$}$$

durch

$$r_{i-1} = q_i \cdot r_i + r_{i+1} \text{ mit } r_{i+1} = 0 \text{ oder } \delta(r_{i+1}) < \delta(r_i). \tag{$**$}$$

Da $\delta(r_1) > \delta(r_2) > \ldots$, muss die Folge abbrechen. D.h. es gibt ein n mit

$$r_n \neq 0, \text{ aber } r_{n+1} = 0.$$

Dann ist

$$r_n = ggT(r_0, r_1).$$

Der Beweis folgt wie im Grundkurs sofort aus $(**)$.
Induktiv konstruiert man eine Darstellung (Abwärtsinduktion)

$$r_n = a_i \cdot r_{i-1} + b_i r_i \quad a_i, b_i \in R,$$

beginnend mit

$$r_n = r_{n-2} - q_{n-1} r_{n-1} \quad \text{aus } (**)$$

Induktionschritt: Sei $r_n = a_i r_{i-1} + b_i r_i$
Aus $(**)$ erhalten wir $r_{i-2} - q_{i-1} r_{i-1} = r_i$. Also

$$r_n = a_i \cdot r_{i-1} + b_i(r_{i-2} - q_{i-1} r_{i-1}) = b_i r_{i-2} + (a_i - b_i q_{i-1}) r_{i-1}$$

So gewinnen wir die Darstellung

$$r_n = ggT(r_0, r_1) = a_1 r_0 + b_1 r_1.$$

11.22 Zur Erinnerung: Für große Zahlen ist (11.21) eine gute Methode, den ggT zu berechnen: $r_0 = 17640$, $r_1 = 2772$

$$\begin{aligned} 17640 &= 6 \cdot 2772 + 1008 \\ 2772 &= 2 \cdot 1008 + 756 \\ 1008 &= 1 \cdot 756 + 252 \\ 756 &= 3 \cdot 252 + 0 \end{aligned}$$

Also: $252 = ggT(17640, 2772)$.

12 Ringe in quadratischen Erweiterungen

Im Grundkurs haben wir Unterkörper

$$\mathbb{Q}(\sqrt{d}) = \{a + b\sqrt{d};\ a, b \in \mathbb{Q}\} \subset \mathbb{R}, \quad d \in \mathbb{N}$$

des Körpers der reellen Zahlen kennen gelernt. Ist d kein Quadrat, ist dies ein Körper, der echt zwischen $\mathbb{Q}$ und $\mathbb{R}$ liegt. Solche Köper nennt man quadratische Erweiterungen von $\mathbb{Q}$.

Ist d negativ, erhält man ebenfalls einen Körper, der aber ein Unterkörper des Körpers der komplexen Zahlen ist.

12.1 Der Körper $\mathbb{C}$ der komplexen Zahlen:

$\mathbb{C}$ besteht aus allen formalen Ausdrücken der Form

$$a + b \cdot i, \quad a, b \in \mathbb{R}$$

und i ist ein fest gewähltes Symbol. Wir definieren

$$\begin{aligned} (a_1 + b_1 \cdot i) + (a_2 + b_2 \cdot i) &= (a_1 + a_2) + (b_1 + b_2) \cdot i \\ (a_1 + b_1 \cdot i) \cdot (a_2 + b_2 \cdot i) &= (a_1 a_2 - b_1 b_2) + (a_1 b_2 + b_1 a_2) \cdot i \end{aligned}$$

D.h. wir rechnen mit diesern fomalen Ausdrücken in der uns bekannten Weise mit der Zusatzinformation, dass

$$i \cdot i = -1.$$

Aus dieser Überlegung folgt, dass $\mathbb{C}$ ein Ring ist mit $0 = 0 + 0 \cdot i$ als neutralem Element der Addition und $1 = 1 + 0 \cdot i$ als neutralem Element der Multiplikation.

Wie üblich schreiben wir

$$a \text{ für } a + 0 \cdot i \text{ und } b \cdot i \text{ für } 0 + b \cdot i.$$

Es folgt, dass $\mathbb{R} = \{a + 0 \cdot i; ; a \in \mathbb{R}\}$ Unterkörper von $\mathbb{C}$ ist. Wir müssen noch zeigen, dass $z = a + b \cdot i$ ein Inverses hat, falls $z \neq 0$. In diesem Fall ist $a^2 + b^2 \neq 0$. Wir ermitteln:

$$z^{-1} = \frac{1}{a + b \cdot i} = \frac{a - bi}{(a + bi) \cdot (a - bi)} = \frac{a - bi}{a^2 - b^2 \cdot i^2} = \frac{a - bi}{a^2 + b^2}.$$

Also $z^{-1} = \dfrac{a}{a^2 + b^2} - \dfrac{b}{a^2 + b^2} \cdot i.$

12.2 Definition: $d \in \mathbb{Z}$ heißt *quadratfrei*, falls $d = -1$ oder falls $|d| > 1$ und für alle Primzahlen p das Quadrat p^2 kein Teiler von $|d|$ ist.

12.3 Bezeichnung und Satz: Sei d quadratfrei. Dann ist

$$\mathbb{Q}(\sqrt{d}) = \{x + y\sqrt{d}; x, y \in \mathbb{Q}\} \subset \mathbb{C}$$

der kleinste Unterkörper von $\mathbb{C}$, der $\mathbb{Q}$ und $\sqrt{d}$ enthält. Man nennt $\mathbb{Q}(\sqrt{d})$ eine *quadratische Erweiterung* von $\mathbb{Q}$.

Beweis:: Ist $\mathbb{K}$ ein Unterkörper von $\mathbb{C}$, der $\mathbb{Q}$ und $\sqrt{d}$ enthält, dann enthält $\mathbb{K}$ offensichtlich $\mathbb{Q}(\sqrt{d})$, weil $\mathbb{K}$ bezüglich der Addition und Multiplikation abgeschlossen ist. Es bleibt also nur zu zeigen, dass $\mathbb{Q}(\sqrt{d})$ ein Unterkörper von $\mathbb{C}$ ist.
$0, 1, -1 \in \mathbb{Q}(\sqrt{d})$. Weiterhin ist $\mathbb{Q}(\sqrt{d})$ additiv und multiplikativ abgeschlossen: Sind $x_1 + x_2\sqrt{d}$, $y_1 + y_2\sqrt{d}$ aus $\mathbb{Q}(\sqrt{d})$ mit $x_1, x_2, y_1, y_2 \in \mathbb{Q}$, so gilt

$$\begin{aligned}(x_1 + x_2\sqrt{d}) + (y_1 + y_2\sqrt{d}) &= (x_1 + y_1) + (x_2 + y_2)\sqrt{d} \\ (x_1 + x_2\sqrt{d}) \cdot (y_1 + y_2\sqrt{d}) &= (x_1y_1 + dx_2y_2) + (x_1y_2 + x_2y_1)\sqrt{d},\end{aligned}$$

und (x_1+y_1), (x_2+y_2), $(x_1y_1+dx_2y_2)$, $(x_1y_2+x_2y_1)$ sind aus $\mathbb{Q}$. Ist $x+y\sqrt{d} \neq 0$ mit $x, y \in \mathbb{Q}$, wo bleibt noch nachzuweisen, dass

$$\frac{1}{x + y\sqrt{d}} \in \mathbb{Q}.$$

Dazu erweitern wir den Bruch mit $x - y\sqrt{d}$ und erhalten

$$\frac{1}{x + y\sqrt{d}} = \frac{x - y\sqrt{d}}{x^2 - dy^2} = \frac{x}{x^2 - dy^2} - \frac{y}{x^2 - dy^2} \cdot \sqrt{d} \in \mathbb{Q}(\sqrt{d})$$

Im Beweis haben wir benutzt, dass $x - y\sqrt{d} \neq 0$, falls $x + y\sqrt{D} \neq 0$. Das ist a priori nicht klar, folgt aber aus dem nächten Lemma, das bereits im Grundkurs bewiesen wurde.

12.4 Lemma: Ist d quadratfrei, dann gilt

(1) $\sqrt{d} \notin \mathbb{Q}$

(2) 1 und $\sqrt{d}$ bilden eine Basis des $\mathbb{Q}$-Vektorraumes $\mathbb{Q}(\sqrt{d})$.

□

Teil (2) wurde im Grundkurs anders formuliert, weil der Begriff des Vektorraumes nicht eingeführt war. Es wurde gezeigt: Aus

$$x_1 + y_1\sqrt{d} = x_2 + y_2\sqrt{d}$$

mit $x_1, x_2, y_1, y_2 \in \mathbb{Q}$ folgt $x_1 = x_2$ und $y_1 = y_2$. D.h. jedes $z \in \mathbb{Q}(\sqrt{d})$ ist eindeutig in der Form $z = x + y\sqrt{d}$ mit $x, y \in \mathbb{Q}$ darstellbar. Aber das ist gerade die Bedingung an eine Basis.
Wir betrachten nun folgende Unterringe $R_d \subset \mathbb{Q}(\sqrt{d})$.

12.5 Definition: Sei $d \in \mathbb{Z}$ quadratfrei. Wir definieren

$$R_d = \{x + y\sqrt{d};\ x, y \in \mathbb{Z}\} \subset \mathbb{Q}(\sqrt{d}), \quad \text{falls } d \equiv 2, 3 \mod 4$$

$$R_d = \left\{\frac{x + y\sqrt{d}}{2};\ x, y \in \mathbb{Z},\ x \equiv y \mod 2\right\} \subset \mathbb{Q}(\sqrt{d}), \quad \text{falls } d \equiv 1 \mod 4$$

Ist $d \equiv 0 \mod 4$, ist $2^2|d$ also d nicht quadratfrei.

12.6 Aufgabe: Zeigen Sie: R_d ist Unterring von $\mathbb{Q}(\sqrt{d}) \subset \mathbb{C}$.

12.7 Bemerkung: (1) $\mathbb{Z}[\sqrt{d}] = \{x + y\sqrt{d};\ x, y \in \mathbb{Z}\}$ ist ebenfalls Unterring von $\mathbb{Q}(\sqrt{d})$. Für quadratfreies $d \not\equiv 1 \mod 4$ ist $R_d = \mathbb{Z}[\sqrt{d}]$.

(2) Die Ringe R_d sind deshalb von Bedeutung, weil sie aus den $z \in \mathbb{Q}(\sqrt{d})$ bestehen, die Lösung einer Gleichung

$$x^2 + ax + b = 0$$

mit $a, b \in \mathbb{Z}$ sind.

Ein zentrales Hilfsmittel zur Untersuchung der Ring R_d ist die Normabbildung:

12.8 Definition: Die Abbildung

$$N : \mathbb{Q}(\sqrt{d}) \to \mathbb{Q}, \quad (x + y\sqrt{d}) \mapsto (x + y\sqrt{d}) \cdot (x - y\sqrt{d}) = x^2 - dy^2$$

heißt *Normabbildung*, und $N(z)$ heißt *Norm* von z.

12.9 Eigenschaften:

(1) $N(z) = 0 \iff z = 0$

(2) $N : (\mathbb{Q}(\sqrt{d}), \cdot) \to (\mathbb{Q}, \cdot)$ ist ein Monoidhomomorphismus

(3) Für $z \in R_d$ gilt $N(z) \in \mathbb{Z}$.

Beweis: (1) Aus 12.4.2 folgt: $z = x + y\sqrt{d} = 0 \iff x = y = 0 \Rightarrow N(z) = 0$. Umgekehrt: $N(z) = 0 \iff x^2 = d \cdot y^2$. Ist $y \neq 0$, folgt $d = \frac{x^2}{y^2} = (\frac{x}{y})^2$. Also ist d Quadrat einer rationalen Zahl und damit $\sqrt{d} \in \mathbb{Q}$, ein Widerspruch zu 12.4(1). Also ist $y = 0$ und damit auch $x = 0$.
(2) Die Abbbildung

$$\tau : \mathbb{Q}(\sqrt{d}) \to \mathbb{Q}(\sqrt{d}), x + y\sqrt{d} \mapsto x - y\sqrt{d}$$

ist ein Körperautomorphism: Sei $z_1 = x_1 + y_1\sqrt{d}$, $z_2 = x_2 + y_2\sqrt{d}$

$$\begin{aligned}
\tau(z_1 + z_2) &= \tau(x_1 + x_2 + (y_1 + y_1)\sqrt{d}) = x_1 + x_2 - (y_1 + y_2)\sqrt{d} \\
&= x_1 - y_1\sqrt{d} + x_2 - y_2\sqrt{d} = \tau(z_1) + \tau(z_2) \\
\tau(z_1 \cdot z_2) &= \tau((x_1x_2 + dy_1y_2) + (x_1y_2 + x_2y_1)\sqrt{d}) \\
&= (x_1x_2 + dy_1y_2) - (x_1y_2 + x_2y_1)\sqrt{d} \\
&= (x_1 - y_1\sqrt{d})(x_2 - y_2\sqrt{d}) = \tau(z_1) \cdot \tau(z_2) \\
\tau(1) &= 1
\end{aligned}$$

$$\begin{aligned}
\text{Es folgt } N(z_1 \cdot z_2) &= z_1 \cdot z_2 \cdot \tau(z_1 \cdot z_2) = z_1 \cdot z_2 \cdot \tau(z_1) \cdot \tau(z_2) \\
&= N(z_1) \cdot N(z_2)
\end{aligned}$$

und $N(1) = 1$.
(3) ist klar, falls $d \neq 1 \mod 4$. Für $d \equiv 1 \mod 4$ erhalten wir

$$N\left(\frac{x + y\sqrt{d}}{2}\right) = \left(\frac{(x + y\sqrt{d})(x - y\sqrt{d})}{4}\right) = \frac{x^2 - dy^2}{4}$$

Da $x \equiv y \mod 2$, folgt $x^2 \equiv y^2 \mod 4$ (nachrechnen!), also $x^2 - dy^2 \equiv x^2 - y^2 \equiv 0 \mod 4$, weil $d \equiv 1 \mod 4$. Damit ist der Zähler durch 4 teilbar. □

12.10 Lemma: Für $z \in R_d$ gilt

(1) $z \in R_d^* \iff N(z) = \pm 1$

(2) $N(z)$ prim $\Rightarrow z$ irreduzibel

Beweis:: (1) Ist $z \in R_d^*$, so ist $N(z) \in \mathbb{Z}^* = \{\pm 1\}$, da N ein Monoidhomomorphismus ist. Ist umgekehrt $z = a + b\sqrt{d}$ und $N(z) = \pm 1$, folgt

$$\pm 1 = (a + b\sqrt{d})(a - b\sqrt{d})$$

Also ist $(a - b\sqrt{d})$ bzw. $-(a - b\sqrt{d})$ invers zu z.
(2) Angenommen $z = z_1 \cdot z_2$. Dann gilt $N(z) = N(z_1) \cdot N(z_2)$. Da $N(z)$ prim ist, ist $N(z_1) = \pm 1$ oder $N(z_2) = \pm 1$. Also ist z_1 oder z_2 Einheit nach (1). $\square$
Lemma 12.10 hat große Ähnlichkeit mit 11.14. Es liegt daher die Vermutung nahe, dass wenigstens einige Ringe R_d mit der Normabbildung euklidisch sind.

12.11 Satz: Für $d = -11, -7, -3, -2, -1, 2, 3$ ist R_d mit

$$\delta : R_d \backslash \{0\} \to \mathbb{N}, \quad z \mapsto |N(z)|$$

ein euklidischer Ring und damit eine Hauptringideal.

Beweis:: Nach 12.9 ist $|N(z)| \in \mathbb{N}\backslash\{0\}$ für $z \in R_d\backslash\{0\}$. Es folgt

$$\delta(z_1 \cdot z_2) = |N(z_1 \cdot z_2)| = |N(z_1)| \cdot |N(z_2)| \geq |N(z_1)| = \delta(z_1) \; \forall z_1, z_2 \in R_d\backslash\{0\}.$$

Sei jetzt $z, y \in R_d$ und $y \neq 0$. Wir suchen q und r in R_d, so dass

$$z = q \cdot y + r \text{ mit } r = 0 \text{ oder } |N(r)| < |N(y)|.$$

Angenommen q und r existieren, dann gilt im Körper $\mathbb{Q}(\sqrt{d})$

$$\frac{z}{y} = q + \frac{r}{y} = a + b\sqrt{d} \text{ mit } a, b \in \mathbb{Q}(\sqrt{d}) \qquad (*)$$

Da N multiplikativ ist, genügt es, ein $q \in R_d$ so zufinden, dass $|N(\frac{r}{y})| < 1$ in $(*)$ ist. Sei nun $q = u + v\sqrt{d}$ mit $u, v \in \mathbb{Z}$. Dann gilt

$$\frac{r}{y} = \frac{z}{y} - q = a + b\sqrt{d} - u - v\sqrt{d} = (a - u) + (b - v)\sqrt{d}.$$

Es folgt: $N(\frac{r}{y}) = (a - u)^2 - d(b - v)^2$.
Da $a, b \in \mathbb{Q}$, können wir $u, v \in \mathbb{Z}$ so wählen, dass $|a - u| \leq \frac{1}{2}$ und $|b - v| \leq \frac{1}{2}$.
Für $d = -1, -2$ folgt dann

$$0 \leq N(\frac{r}{y}) = \frac{1}{4} - d \cdot \frac{1}{4} \leq \frac{1}{4} + 2\frac{1}{4} = \frac{3}{4} < 1$$

Für $d = 2, 3$ folgt

$$-3 \cdot \frac{1}{4} \leq N(\frac{r}{y}) \leq \frac{1}{4}. \quad \text{Also } |N(\frac{r}{y}| \leq \frac{3}{4} < 1$$

Für $d = -3, -7, -11$ ist $d \equiv 1 \mod 4$. Hier setzen wir $q = \frac{u}{2} + \frac{v}{2}\sqrt{d}$ mit $u, v \in \mathbb{Z}$ von gleicher Parität. Wir wählen $v \in \mathbb{Z}$ derart, dass $|b - \frac{v}{2}| \leq \frac{1}{4}$. Dann wählen wir ein u von gleicher Parität, so dass $|a - \frac{u}{2}| \leq \frac{1}{2}$. Eine solche Wahl ist immer möglich. Es gilt

$$\begin{array}{rclcl} |N(\frac{r}{y})| & = & |N\left((a - \frac{u}{2}) + (b - \frac{v}{2})\sqrt{d}\right)| & = & |(a - \frac{u}{2})^2 - d(b - \frac{v}{2})^2| \\ & = & |a - \frac{u}{2}|^2 + |d| \cdot |b - \frac{v}{2}|^2 & \leq & \frac{1}{4} + |d| \cdot \frac{1}{16} = \frac{4 + |d|}{16} < 1 \end{array}$$

□

12.12 Satz: Ist $d < 0$ quadratfrei, so gilt:

(1) $R^*_{-1} = \{\pm 1, \pm i\} \cong \mathbb{Z}/4$ mit $i = \sqrt{-1}$ als Erzeuger.

(2) $R^*_{-3} = \{\pm 1, \pm\frac{1}{2} \pm \frac{1}{2}\sqrt{-3}\} \cong \mathbb{Z}/6$ mit $\frac{1}{2} + \frac{1}{2}\sqrt{-3}$ als Erzeuger.

(3) $R^*_d = \{\pm 1\} \cong \mathbb{Z}/2$, falls $d < 0$, $d \neq -1, -3$.

Beweis:: Sei $z = a + b\sqrt{d}$ mit $a, b \in \mathbb{Z}$. Dann ist $\mathbb{N}(z) = a^2 + |d| \cdot b^2$. Also

$$z \in R^*_d \iff a^2 + |d| \cdot b^2 = 1$$

Ist $|d| \neq 1$, ist diese Gleichung nur für $b = 0$ und $a = \pm 1$ erfüllt. Ist $d = -1$, haben wir die Lösungen $(a, b) \in \{(1, 0), (-1, 0), (0, 1), (0, -1)\}$.
Ist nun $d \equiv 1 \mod 4$ und $z = \frac{a}{2} + \frac{b}{2}\sqrt{d}$ mit $a, b \in \mathbb{Z}$ von gleicher Parität, so gilt

$$z \in R^*_d \iff N(z) = \frac{a^2 + |d| \cdot b^2}{4} = 1 \iff a^2 + |d| \cdot b^2 = 4$$

Ist $d < -3$, ist diese Gleichung nur für $b = 0$ und $a = \pm 2$ erfüllt. Für $d = -3$ haben wir die Lösungen

$$(a, b) \in \{(2, 0), (-2, 0), (1, 1), (-1, 1), (1, -1), (-1, -1)\}$$

Daß R^*_d von den jeweils angegebenen Elementen multiplikativ erzeugt wird, rechnet man nach. □
Für $d > 1$ ist die Situation erheblich komplizierter. Wir geben dafür ein Beispiel an:

12.13 Beispiel: $\varepsilon = 1 + \sqrt{2}$ ist Einheit in $R_2 = \mathbb{Z}[\sqrt{d}]$, denn $N(\varepsilon) = (1 + \sqrt{2}) \cdot (1 - \sqrt{2}) = -1$. Es folgt $\varepsilon^{-1} = -1 + \sqrt{2}$.
Da $\varepsilon > 1$, folgt $1 < \varepsilon < \varepsilon^2 < \varepsilon^3 < \ldots$. Es gibt also unendlich viele verschiedene Einheiten in $\mathbb{Z}[\sqrt{2}]$. Genauer kann man zeigen (ohne Beweis)

$$(\mathbb{Z}[\sqrt{2}])^2 = \{\pm 1\} \cdot \langle \varepsilon \rangle,$$

wobei $\langle \varepsilon \rangle$ die von ε erzeugte Untergruppe der Einheitengruppe ist.

Unter den Ringen R_d gibt es nur wenige faktorielle. Damit ist die Existenz von Primfaktorzerlegung selbst für Unterringe von $\mathbb{C}$ ein echtes Problem. Wir wollen ein Beispiel angeben.

12.14 Satz: $R_{-5} = \mathbb{Z}[\sqrt{-5}] \subset \mathbb{C}$ ist kein faktorieller Ring.

Beweis: $(1 + \sqrt{5})(1 - \sqrt{-5}) = 6 = 2 \cdot 3$.
Behauptung: $(1 \pm \sqrt{-5}),\ 2,\ 3$ sind irreduzibel in $\mathbb{R}_{-5}$.
Beweis: Sei $z \in \mathbb{R}_{-5}$ eine dieser Zahlen. Ist z reduzibel, gibt es Nichteinheiten $x, y \in R_{-5}$, so dass $z = x \cdot y$. Es folgt

$$N(x) \cdot N(y) = N(z) \text{ und } N(x), N(y) > 1.$$

Da $N(z)$ die Werte $6, 4, 9$ hat, je nach z, folgt $N(x) \in \{2, 3\}$. Sei $x = a + b\sqrt{-5}$. Dann gilt

$$N(x) = a^2 + 5b^2.$$

Dieser Wert kann niemals 2 oder 3 sein.
Wäre R_{-5} faktoriell, so wären $2, 3, (1 \pm \sqrt{-5})$ als irreduzible Elemente prim. Damit hätten wir aber zwei Primfaktorzerlegungen von 6, die sich nach 12.12 nicht nur um Multiplikation mit Einheiten unterscheiden. □

13 Polynomringe

Im Grundkurs haben wir polynomiale Abbildungen $\mathbb{R} \to \mathbb{R}$ studiert. Ist $\mathbb{R}[X]$ die Menge dieser Abbildungen, dann haben wir gezeigt, dass $\mathbb{R}[X]$ eine Unterring des Rings $\mathrm{Abb}(\mathbb{R}, \mathbb{R})$ aller Abbildungen $\mathbb{R} \to \mathbb{R}$ ist.

Ist R ein beliebiger Ring, dann braucht der Identitätssatz für Polynome (Grundkurs 12.23) nicht zu gelten. Deshalb müssen wir hier etwas anders vorgehen.

13.1 Definition: Sei R ein Ring. Ein *Polynom* über R ist ein formaler Ausdruck der Form

$$p = a_0 + a_1 X + a_2 X^2 + \ldots + a_n X^n = \sum_{i=0}^{n} a_i X^i$$

mit $a_i \in R$ und einem Symbol X. Ist $a_i = 0$, wird der Summand $a_i X^i$ oft weggelassen. Ist $a_n \neq 0$ nennt man a_n den *Leitkoeffizienten* von p und n den *Grad*, $\mathrm{grad}(p)$, von p. Das *konstante Glied* von p ist a_0. Ein Polynom der Form $p = a_0$ heißt *konstantes Polynom*, das Polynom $p = 0$ heißt *Nullpolynom* und das Polynom $p = 1$ *Einspolynom*.

13.2 Bezeichnung: Mit $R[X]$ bezeichnen wir die Menge aller Polynome über R.

13.3 Seien $p = \sum_{i=0}^{m} a_i X^i$ und $q = \sum_{i=0}^{n} b_i X^i$ Polynome über R und $k = \max(m, n)$. Wir definieren

$$p + q = \sum_{i=0}^{k} (a_i + b_i) \cdot X^i,$$

wobei $a_i = 0$ für $m < i \leq k$ und $b_j = 0$ für $n < j \leq k$, und

$$p \cdot q = \sum_{i=0}^{n+n} c_i X^i \quad \text{mit} \quad c_i = \sum_{j=0}^{i} a_j \cdot b_{i-j}.$$

Das sind dieselben Verknüpfungen wie im Grundkurs definiert, aber hier betrachten wir die Polynome nicht als Abbildungen.

13.4 Satz: Für jeden Ring R ist $(R[X], +, \cdot)$ ein Ring mit $-p = \sum_{i=0}^{m} (-a_i) \cdot X^i$ und dem Null- und Einspolynom als neutralen Elementen der Addition und Multiplikation.

Beweis: Den Beweis aus dem Grundkurs können wie nicht nehmen. Dieser bezog sich auf Abbildungen.

Der explizite Nachweis der Axiome ist einfach, nur die Assoziativität der Multiplikation macht etwas Schwierigkeiten. Um uns das Leben einfacher zu machen, beachten wir, dass

$$c_i = \sum_{j=0}^{i} a_j b_{i-j} = \sum_{j+l=i} a_j \cdot b_l.$$

Sei $r = \sum_{i=0}^{s} u_i X^i$ ein drittes Polynom und $d_t = \sum_{l+w=t} b_l \cdot u_w$. Dann gilt mit den Bezeichnungen von 13.3

$$p \cdot q = \sum_{i=0}^{m+n} c_i X^i \quad \text{und} \quad q \cdot r = \sum_{j=0}^{n+s} d_j X^j.$$

Der i-te Koeffizient von $(p \cdot q) \cdot r$ ist

$$\sum_{v+w=i} c_v \cdot u_w = \sum_{v+w=i} \sum_{j+l=v} a_j b_l u_w = \sum_{j+l+w=i} a_j b_l u_w.$$

Der i-te Koeffizient von $p \cdot (q \cdot r)$ ist

$$\sum_{j+t=i} a_j d_t = \sum_{j+t=i} a_j \cdot \sum_{l+w=t} b_l u_w = \sum_{j+l+w=i} a_j b_l u_w.$$

Wir erhalten $(p \cdot q) \cdot r = p \cdot (q \cdot r)$. □

13.5 Die Abbildung $R \to R[X]$, die r auf das konstante Polynom $p = r$ abbildet, ist ein Ringmonomorphismus. Daher kann man R als Unterring von $R[X]$ auffassen, nämlich als Unterring der konstanten Polynome.

13.6 Gradregeln: Aus 13.3 erhalten wir für $p \neq 0$ und $q \neq 0$

(1) $\operatorname{grad} p + q \leq \max(\operatorname{grad} p, \operatorname{grad} q)$

(2) Ist das Produkt der Leitkoeffizienten ungleich Null (das gilt stets in einem Integritätsring), dann gilt

$$\operatorname{grad}(p \cdot q) = \operatorname{grad} p + \operatorname{grad} q.$$

Aus den Gradregeln folgt sofort

13.7 (1) $R[X]$ ist Integritätsring $\iff$ R ist Integritätsring.

(2) Ist R ein Integritätsring, dann gilt $R[X]^* = R^*$.

(3) $R[X]$ ist niemals ein Körper.

Beweis: (1) "$\Rightarrow$": R ist Unterring von $R[X]$.
"$\Leftarrow$": Ist $p \neq 0$ und $q \neq 0$, dann ist nach 13.6.2 auch $p \cdot q \neq 0$
(2) Ist $p \cdot q = 1$, gilt $\operatorname{grad}(p \cdot q) = 0$ und damit $\operatorname{grad} p = \operatorname{grad} q = 0$ nach 13.6.2.
(3) folgt aus (1) und (2). □

13.8 Beispiel: Ist R kein Integritätring, braucht 13.7.2 nicht zu gelten: In $\mathbb{Z}/4[X]$ haben wir

$$(1 + 2X) \cdot (1 + 2X) = 1 + 4X + 4X^2 = 1.$$

Also ist $(1 + 2X) \in \mathbb{Z}/4[X]^*$.

Eine schöne Eigenschaft von Polynomringen ist, dass man oft dividieren kann.

13.9 Division mit Rest: Sind $f = \sum_{i=0}^{m} a_i X^i$ und $g = \sum_{i=0}^{n} b_i X^i$ Polynome aus $R[X]$, so dass $b_n \in R^*$ ist, dann gibt es Polynome q und r in $R[X]$, so dass

$$f = q \cdot g + r \quad \text{mit } r = 0 \text{ oder } \operatorname{grad}(r) < \operatorname{grad}(g).$$

Der Beweis ist wörtlich derselbe wie der von Satz 12.20 des Grundkurses.

13.10 Ergänzung: Ist R ein Integritätsring, dann sind q und r in 13.5 eindeutig bestimmt.

Der Eindeutigkeitsbeweis ist derselbe wie von Satz 12.27 des Grundkurses.
Aus dem Divisionssatz und den Gradformeln folgt

13.11 Satz: Ist $\mathbb{K}$ ein Körper, dann ist $\mathbb{K}[X]$ ein euklidischer Ring mit

$$\delta = \operatorname{grad} : \mathbb{K}[X] \backslash \{0\} \to \mathbb{N}.$$

Insbesondere ist $\mathbb{K}[X]$ ein Hauptidealring.

13.12 Jedes Polynom $p = \sum_{i=0}^{n} a_i X^i \in R[X]$ definiert eine *polynomiale Abbildung*

$$f_p : R \to R, \quad r \mapsto \sum_{i=0}^{n} a_i \cdot r^i \in R$$

Statt $f_p(r)$ schreiben wir oft kürzer $p(r)$.

13.13 Beispiel: Verschiedene Polynome können dieselbe polynomiale Abbildung definieren: Z.B. definieren alle Polynome $p_k \in \mathbb{Z}/2[X]$

$$p_k = X + X^2 + \ldots + X^{2k}$$

die Nullabbildung $\mathbb{Z}/2 \to \mathbb{Z}/2$. D.h. der Identitätssatz 12.23 des Grundkurses braucht in allgemeinen Polynomringen nicht zu gelten.

Aus den Sätzen 12.17 und 12.19 des Grundkurses und ihren Beweisen erhalten wir

13.14 Satz: Ist R ein Ring, dann ist $(\mathrm{Abb}(R,R), +, \cdot)$ mit der üblichen Addition und Multiplikation von Abbildungen ein Ring und

$$\alpha : R[X] \to \mathrm{Abb}(R,R), \quad p \mapsto f_p$$

ist ein Ringhomomorphismus. □

13.15 Definition: Sei $p \in R[X]$. Ein Element $r \in R$ heißt *Nullstelle* von p, wenn $p(r) = 0$.

Den Beweis des Satzes 12.22 des Grundkurses können wir auf unseren allgemeinen Fall übertragen und erhalten Lemma 13.16 und Satz 13.17.

13.16 Lemma: Ist r eine Nullstelle von $p \in R[X]$, dann ist $X - r$ ein Teiler von p, d.h. es gibt ein $q \in R[X]$, so dass

$$p = q \cdot (X - r).$$

13.17 Satz: Ist R ein Integritätsring und $p \in R[X]$ vom Grad n, dann hat p höchstens n Nullstellen.

Der Beweis des Eindeutigkeitssatzes 12.23 des Grundkurses überträgt sich nun:

13.18 Satz: Ist R ein unendlicher Integritätsring, dann definieren verschiedene Polynome verschiedene polynomiale Abbildungen. D.h. der Ringhomomorphismus $\alpha : R[X] \to \mathrm{Abb}(R,R)$ ist injektiv. □

Für den nächsten Abschnitt benötigen wir Irreduzibilitätskriterien für Polynome. Wir erinnern: Ist $f \in R[X]$ ein Polynom, $f \neq 0$ und $f \notin R[X]^*$, dann heißt f irreduzibel, wenn gilt:

$$f = q \cdot q \Rightarrow p \in R[X]^* \text{ oder } q \in R[X]^*.$$

13.19 Lemma: Ist R ein Integritätsringing und $f = a_0 + a_1X + a_2X^2 + X^3$ aus $R[X]$ reduzibel, dann hat f eine Nullstelle.

Beweis: Sei $f = p \cdot q$ mit $p \notin R[X]^*$ und $q \notin R[X]^*$. Die Polynome p und q sind nicht konstant: Wäre etwa $p = b_0$, dann wäre q von der Form $q = c_2X^2 + c_1X + c_0$, und aus $f = p \cdot q$ folgt dann $b_0 \cdot c_2 = 1$, also $b_0 \in R^*$ und damit $p \in R[X]^*$. Folglich hat p den Grad 1 und q den Grad 2 oder umgekehrt, etwa $p = b_0 + b_1X$ und $q = c_0 + c_1X + c_2X^2$. Da $b_1 \cdot c_2 = 1$, ist $-c_2b_0$ Nullstelle von p:

$$p(-c_2b_0) = b_0 - b_1c_2b_0 = b_0 - b_0 = 0.$$

□

13.20 Satz: Ist $f \in \mathbb{Z}[X]$ irreduzibel, dann ist es auch als Polynom aus $\mathbb{Q}[X]$ irreduzibel.

Beweis: Sei f reduzibel in $\mathbb{Q}[X]$, d.h. $f = g \cdot h$ in $\mathbb{Q}[X]$ mit $g, h \notin \mathbb{Q}[X]^*$. Da $\mathbb{Q}[X] = \mathbb{Q}^*$, sind g und h nicht konstant, d.h. $\operatorname{grad} g \geq 1$ und $\operatorname{grad} h \geq 1$. Wir multiplizieren die Gleichung $f = g \cdot h$ mit dem Hauptnenner a der Koeffizienten von g und h und erhalten eine Gleichung

$(*)$ $\quad a \cdot f = \overline{g} \cdot \overline{h}$ mit $\overline{g}, \overline{h} \in \mathbb{Z}[X]$, $\operatorname{grad} \overline{g} = \operatorname{grad} g$, $\operatorname{grad} \overline{h} = \operatorname{grad} h$.

Sei p ein Primteiler von a. Da $\mathbb{Z}[X]/(p) \cong \mathbb{Z}/p[X]$ ist und $\mathbb{Z}/p[X]$ nach 13.7(1) ein Integritätsring ist, ist p prim in $\mathbb{Z}[X]$ nach 11.3. Also teilt p einen der Faktoren $\overline{g}$ oder $\overline{h}$ in $\mathbb{Z}[X]$. Daher können wir p aus der Gleichung kürzen und erhalten eine neue Gleichung mit denselben Eigenschaften wie $(*)$. Wir fahren fort, bis ganz a gekürzt ist, und erhalten eine Gleichung

$$f = \widetilde{g} \cdot \widetilde{h} \text{ mit } \widetilde{g}, \widetilde{h} \in \mathbb{Z}[X],\ \operatorname{grad} \widetilde{g} = \operatorname{grad} g,\ \operatorname{grad} \widetilde{h} = \operatorname{grad} h.$$

Also ist $f \in \mathbb{Z}[X]$ reduzibel in $\mathbb{Z}[X]$, ein Widerspruch. □

Im Hinblick auf 13.19 zeigen wir noch

13.21 Lemma von Vieta: Ist α eine Nullstelle von $f = a_0 + a_1x + \ldots + a_nX^n \in R[X]$, dann ist α ein Teiler von a_0.

Beweis: Aus $0 = f(\alpha) = a_0 + a_1\alpha + \ldots + a_n\alpha^n$ folgt

$$a_0 = -a_1\alpha - a_2\alpha^2 - \ldots - a_n\alpha^n = \alpha \cdot (-a_1 - a_2\alpha - a_n\alpha^{n-1})$$

□

14 Algebraische Körpererweiterungen

Wir rekapitulieren aus dem Grundkurs

14.1 Definition: Sei $(\mathbb{K}, +, \cdot)$ ein Körper. Ein $\mathbb{K}$-*Vektorraum* ist eine abelsche Gruppe $(V, \boxplus)$ mit einer *Skalarmultiplikation*

$$\mathbb{K} \times V \to V, \quad (k, v) \mapsto k * v,$$

so dass für alle $k, l \in \mathbb{K}$ und alle $v, w \in V$ gilt (Verträglichkeit von $+, \cdot, \boxplus$ und $*$).

(1) $k * (v \boxplus w) = k * w \ \boxplus \ k * w$

(2) $(k + l) * v = k * v \ \boxplus \ l * v$

(3) $(k \cdot l) * v = k * (l * v)$

(4) $1 * v = v$

$\{v_1, \ldots, v_n\} \subset V$ heißt *Erzeugendensystem*, wenn jedes $w \in V$ Linearkombination von $v_1, \ldots, v_n$ ist. Ist jedes w eindeutig als Linearkombination von $v_1, \ldots, v_n$ darstellbar, nennt man $\{v_1, \ldots, v_n\}$ *Basis* von V. Die *Dimension* von V ist die Anzahl der Elemente einer Basis.

14.2 $\{v_1, \ldots, v_n\} \subset V$ ist genau dann Basis, wenn es ein linear unabhängiges Erzeugendensystem ist.

In dieser Vorlesung kommen Vektorräume in folgendem Zusammenhang vor.

14.3 Definition und Satz: Sei $\mathbb{K}$ ein Unterkörper des Körpers $\mathbb{F}$. Wir nennen $\mathbb{K} \subset \mathbb{F}$ auch *Körpererweiterung*. $\mathbb{F}$ ist mit seiner Addition und Multiplikation ein $\mathbb{K}$-Vektorraum. Seine Dimension $\dim_{\mathbb{K}} \mathbb{F}$ heißt auch *Grad* der Körpererweiterung und wird mit $[\mathbb{F} : \mathbb{K}]$ bezeichnet. Ist $[\mathbb{F} : \mathbb{K}]$ endlich, heißt $\mathbb{K} \subset \mathbb{F}$ *endliche Körpererweiterung*.

14.4 Beispiele: (1) $[\mathbb{C} : \mathbb{R}] = 2$. Eine Basis ist $\{1, i\}$.

(2) Ist $d \in \mathbb{Z}$ quadratfrei, dann ist $[\mathbb{Q}(\sqrt{d}) : \mathbb{Q}] = 2$. Eine Basis ist $\{1, \sqrt{d}\}$.

(3) $\mathbb{R}$ ist ein unendlich-dimensionaler $\mathbb{Q}$-Vektorraum, denn jeder n-dimensionale $\mathbb{Q}$-Vektorraum ist abzählbar, während $\mathbb{R}$ überabzählbar ist.

(4) $\mathbb{K}[X]$ ist ein unendlich-dimensionaler $\mathbb{K}$-Vektorraum. Eine Basis ist $\{1, X, X^2, X^3, \ldots\}$.

14.5 Gradschachtelungssatz: Sind $\mathbb{K} \subset \mathbb{L}$ und $\mathbb{L} \subset \mathbb{F}$ endliche Körpererweiterungen, dann ist auch $\mathbb{K} \subset \mathbb{F}$ endliche Körpererweiterung, und es gilt

$$[\mathbb{F} : \mathbb{K}] = [\mathbb{F} : \mathbb{L}] \cdot [\mathbb{L} : \mathbb{K}].$$

Genauer gilt: Ist $\mathcal{B}_1 = \{x_1, \ldots, x_m\}$ eine $\mathbb{K}$-Basis von $\mathbb{L}$ und $\mathcal{B}_2 = \{y_1, \ldots, y_n\}$ eine $\mathbb{L}$-Basis von $\mathbb{F}$, dann ist $\mathcal{B}_3 = \{x_i \cdot y_j; 1 \leq i \leq m, 1 \leq j \leq n\}$ eine $\mathbb{K}$-Basis von $\mathbb{F}$.

Beweis: Aus dem zweiten Teil des Satzes folgt der erste, denn dann wäre $[\mathbb{F} : \mathbb{K}] = m \cdot n$, $[\mathbb{F} : \mathbb{L}] = n$ und $[\mathbb{L} : \mathbb{K}] = m$.
Beweis des zweiten Teils: Sei $z \in \mathbb{F}$. Da $\mathcal{B}_2$ $\mathbb{L}$-Basis ist, gibt es $a_1, \ldots, a_n$ in $\mathbb{L}$, so dass

$$z = a_1 \cdot y_1 + a_2 \cdot y_2 + \ldots + a_n \cdot y_n = \sum_{j=1}^{n} a_j y_j.$$

Da $\mathcal{B}_1$ $\mathbb{K}$-Basis von $\mathbb{L}$ ist, gibt es zu jedem $a_j \in \mathbb{L}$ Elemente $b_{1j}, \ldots, b_{mj} \in \mathbb{K}$, so dass

$$a_j = b_{1j}x_1 + b_{2j}x_2 + \ldots + b_{mj}x_m = \sum_{i=1}^{m} b_{ij}x_i$$

Es folgt

$$z = \sum_{j=1}^{n} a_j y_j = \sum_{j=1}^{n} \left(\sum_{i=1}^{m} b_{ij}x_i \right) y_j = \sum_{j=1}^{n} \sum_{i=1}^{m} b_{ij}(x_i \cdot y_j), \quad b_{ij} \in \mathbb{K}.$$

Also ist $\mathcal{B}_3$ ein Erzeugendensystem für $\mathbb{F}$ als $\mathbb{K}$-Vektorraum. $\mathbb{B}_3$ ist auch linear unabhängig, denn aus

$$0 = \sum_{j=1}^{n} \sum_{i=1}^{m} c_{ij}(x_i \cdot y_j) = \sum_{j=1}^{n} \left(\sum_{i=1}^{m} c_{ij}x_i \right) \cdot y_j$$

mit $c_{ij} \in \mathbb{K}$ folgt für alle j

$$\sum_{i=1}^{m} c_{ij}x_i = 0 \qquad (*)$$

weil die y_j linear unabhängig über $\mathbb{L}$ sind und die Summen $(*)$ in $\mathbb{L}$ liegen. Da die x_i linear unabhängig über $\mathbb{K}$ sind und die c_{ij} in $\mathbb{K}$ liegen, folgt

$$c_{ij} = 0 \quad \text{für alle } 1 \leq i \leq m \text{ und } 1 \leq j \leq n.$$

□

14.6 Definition: Sei $\mathbb{K} \subset \mathbb{F}$ eine Körpererweiterung. $\alpha \in \mathbb{F}$ heißt *algebraisch* über $\mathbb{K}$, wenn es ein $f \neq 0$ in $\mathbb{K}[X]$ gibt, so dass $f(\alpha) = 0$ in $\mathbb{F}$. Gibt es kein solches Polynom, heißt α *transzendent*.

14.7 Beispiele: (1) $\sqrt{2} \in \mathbb{R}$ und $i \in \mathbb{C}$ sind als Nullstellen von $X^2 - 2$ bzw. $X^2 + 1$ algebraisch über $\mathbb{Q}$.

(2) π und e sind transzendent über $\mathbb{Q}$ (der Beweis ist nicht einfach: Für e wurde es 1873 von Charles Hermite (1822-1901) und für π dann 1882 von Carl Louis Ferdinand von Lindemann (1852-1939) bewiesen).

14.8 Lemma: Sei $\mathbb{K} \subset \mathbb{F}$ eine Körpererweiterung und $\alpha \in \mathbb{F}$. Dann ist die *Einsetzabbildung*

$$E_\alpha : \mathbb{K}[X] \to \mathbb{F}, \quad p \mapsto p(\alpha)$$

ein Ringhomomorphismus.

Beweis: Sei $p = \sum_{i=0}^{m} a_i X^i$ und $q = \sum_{i=0}^{n} b_i X^i$ und $k = \max(m, n)$. Dann ist $p + q = \sum_{i=0}^{k} (a_i + b_i) X^i$. Es gilt

$$E_\alpha(p+q) = \sum_{i=0}^{k} (a_i + b_i)\alpha^i = \sum_{i=0}^{m} a_i \cdot \alpha^i + \sum_{i=0}^{n} b_i \cdot \alpha^i = E_\alpha(p) + E_\alpha(q).$$

Analog zeigt man, dass $E_\alpha(p \cdot q) = E_\alpha(p) \cdot E_\alpha(q)$ ist. Ist $p = 1$, folgt $E_a(p) = p(\alpha) = 1$. □

14.9 Folgerung: Ist $\alpha \in \mathbb{F}$ transzendent, dann ist E_α injektiv, da Kern $E_\alpha = \{0\}$. Ist $\alpha \in \mathbb{F}$ algebraisch, ist Kern $E_\alpha \neq \{0\}$.

Da $\mathbb{K}[X]$ ein Hauptidealring ist, wird jedes Ideal, $J \neq \{0\}$ in $\mathbb{K}[X]$ von einem Polynom erzeugt: $J = (f)$. Ist $J = (f) = (g)$, dann unterscheiden sich f und g nach 14.4 um einen Faktor $a \in \mathbb{K}[X]^* = \mathbb{K}^*$, also um einen konstanten Faktor. Damit gibt es genau ein Polynom f mit Leitkoeffizient 1, man nennt solche Polynome *normiert*, so dass $J = (f)$.

14.10 Folgerung: Ist $\alpha \in \mathbb{F}$ algebraisch über $\mathbb{K}$, dann heißt das eindeutig gegebene normierte Polynom $f \in \mathbb{K}[X]$, für das Kern $E_\alpha = (f)$ ist, das *Minimalpolynom* von α über $\mathbb{K}$.

14.11 Satz: Sei $\mathbb{K} \subset \mathbb{F}$ Körpererweiterung, $\alpha \in \mathbb{F}$ algebraisch über $\mathbb{K}$ mit Minimalpolynom f. Dann gilt

(1) f ist irreduzibel in $\mathbb{K}[X]$.

(2) $\mathbb{K}[X]/(f)$ ist ein Körper.

(3) $\mathbb{K}[X]/(f)$ ist isomorph zu Bild(E_α). Folglich ist Bild(E_α) ein Unterkörper von $\mathbb{F}$, bezeichnet mit $\mathbb{K}(\alpha)$.

(4) $\mathbb{K}(\alpha) \subset \mathbb{F}$ ist der kleinste Unterkörper, der $\mathbb{K}$ und α enthält.

(5) $[\mathbb{K}[\alpha] : \mathbb{K}] = \operatorname{grad} f$. Ist $\operatorname{grad} f = n$, dann ist $\{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$ eine $\mathbb{K}$-Basis von $\mathbb{K}(\alpha)$.

Beweis: (1) Angenommen f ist reduzibel, dann gibt es nicht-konstante Polynome $p, q \in \mathbb{K}[X]$ mit $f = p \cdot q$. Da $0 = f(\alpha) = p(\alpha) \cdot q(\alpha)$, ist $p(\alpha) = 0$ oder $q(\alpha) = 0$, etwa $p(\alpha) = 0$. Dann ist $p \in \operatorname{Kern} E_\alpha = (f)$, d.h. f teilt p. Das ist unmöglich, da $\operatorname{grad} p < \operatorname{grad} f$.

(2) Da $\mathbb{K}[X]$ ein Hauptidealring und f irreduzibel ist, ist (f) nach 11.5 maximal und damit $\mathbb{K}[X]/(f)$ ein Körper nach 10.21 und 10.20.

(3) Ist $\overline{p} \in \mathbb{K}[X]/(f)$ die Nebenklasse von p, dann definiert $\overline{p} \mapsto E_\alpha(p) = p(\alpha)$ nach dem Isomorphiesatz 10.11 einen Isomorphismus $\mathbb{K}[X]/(f) \cong \operatorname{Bild} E_\alpha = \mathbb{K}(\alpha)$.

(4) Aus dem Beweis von (3) folgt, dass es zu jedem $z \in \operatorname{Bild} E_\alpha$ ein $p = \sum_{i=0}^{r} b_i X^i \in \mathbb{K}[X]$ gibt, so dass

$$z = p(\alpha) = b_0 + b_1\alpha + \ldots + b_r\alpha^r, \quad b_i \in \mathbb{K} \text{ für alle } i.$$

Der kleinste Unterkörper $\mathbb{U}$ von $\mathbb{F}$, der $\mathbb{K}$ und α enthält, enthält diese Summe, also auch jedes $z \in \operatorname{Bild} E_\alpha$, d.h. $\operatorname{Bild} E_\alpha \subset \mathbb{U}$. Da $\mathbb{K} \subset \operatorname{Bild} E_\alpha$ als Bild der konstanten Polynome und $\alpha = E_\alpha(X) \in \operatorname{Bild} E_\alpha$, ist $\operatorname{Bild} E_\alpha$ ein Unterkörper von $\mathbb{F}$, der $\mathbb{K}$ und α enthält. Es folgt $\operatorname{Bild} E_\alpha = \mathbb{K}(\alpha) = \mathbb{U}$.

(5) Sei $z = p(\alpha) \in \operatorname{Bild} E_\alpha = \mathbb{K}(\alpha)$. Wir teilen p durch f mit Rest

$$p = q \cdot f + r \quad \text{mit } r = 0 \text{ oder } \operatorname{grad} r < \operatorname{grad} f.$$

Dann gilt $z = p(\alpha) = q(\alpha) \cdot f(\alpha) + r(\alpha) = q(\alpha) \cdot 0 + r(\alpha) = r(\alpha)$. Ist $r = 0$, dann ist $z = 0$. Im anderen Fall ist $r = c_0 + c_1X + \ldots c_kX^k$ mit $k < n$ und $c_i \in \mathbb{K}$, also

$$z = c_0 + c_1\alpha + \ldots + c_k\alpha^k \quad k < n,$$

Damit ist $\{1, \alpha, \ldots, \alpha^{n-1}\}$ ein Erzeugendensystem von $\mathbb{K}(\alpha)$ als $\mathbb{K}$-Vektorraum. Das System ist auch linear unabhängig, denn ist

$$0 = b_0 \cdot 1 + b_1\alpha + \ldots + b_{n-1}\alpha^{n-1} = g(\alpha) \text{ mit } g = \sum_{i=0}^{n-1} b_i X \in \mathbb{K}[X],$$

dann ist $g \in \operatorname{Kern} E_\alpha$, also $g \in (f)$. D.h. f teilt g. Das ist aus Gradgründen nur möglich, wenn $g = 0$, d.h. wenn alle $b_i = 0$. $\square$

14.12 Lemma: Ist $\mathbb{K} \subset \mathbb{F}$ eine Körpererweiterung, $\alpha \in \mathbb{F}$ und $f \in \mathbb{K}[X]$ ein irreduzibles normiertes Polynom mit $f(\alpha) = 0$, dann ist f das Minimalpolynom von α.

Beweis: Sei g das Minimalpolynom von α, also $\operatorname{Kern} E_\alpha = (g)$. Dann ist $f \in (g)$, d.h. g teilt f, also $f = q \cdot g$. Da f irreduzibel ist, ist $q \in \mathbb{K}^*$. Da f und g normiert sind, folgt $q = 1$ und $f = g$. $\square$

14.13 Beispiel: $f = x^3 - 2$ ist irreduzibel in $\mathbb{Z}[X]$, denn andernfalls hätte f nach 13.19 eine ganzzahlige Nullstelle. Nach 13.21 kommen dafür nur ± 1 und ± 2 in Frage, und dies sind keine Nullstellen von f. Also ist f das Minimalpolynom von $\sqrt[3]{2}$. Nach 14.11.5 ist

$$\mathbb{Q}(\sqrt[3]{2}) = \{a + b\sqrt[3]{2} + c\sqrt[3]{4};\ a, b, c \in \mathbb{Q}\} \subset \mathbb{R}$$

und jedes $z \in \mathbb{Q}(\sqrt[3]{2})$ ist eindeutig in der Form

$$a + b\sqrt[3]{2} + c\sqrt[3]{4} \quad \text{mit } a, b, c \in \mathbb{Q}$$

darstellbar.

Teil III

Konstruktionen mit Zirkel und Lineal

15 Unterkörper konstruierbarer reeller Zahlen

Sei $\mathbb{E}$ die Ebene, $M \subset \mathbb{E}$ eine Menge von gegebenen Punkten.

15.1 Nach Plato sind bei Konstruktionen mit Zirkel und Lineal folgende Konstruktionsschritte erlaubt:

(1) Zeichnen einer Geraden durch zwei gegebene oder bereits konstruierte verschiedene Punkte.

(2) Zeichnen eines Kreises um einen gegebenen oder bereits konstruierten Punkt mit dem Abstand zweier gegebener oder bereits konstruierter Punkte als Radius.

(3) Hinzufügen der Schnittpunkte der so konstruierten Geraden und Kreise zu den gegebenen oder bereits konstruierten Punkten.

Damit ein Konstruktionsverfahren überhaupt in Gang kommt, muss M mindestens 2 Punkte haben:

15.2 Generelle Voraussetzung: $M \subset \mathbb{E}$ hat mindestens 2 Punkte.

15.3 Definition: Ein Punkt aus $\mathbb{E}$ heißt *aus M konstruierbar*, wenn er in endlich vielen Schritten mit Zirkel und Lineal aus M konstruierbar ist.

Aus der Schule sind folgende Konstruktionen mit Zirkel und Lineal bekannt.

15.4 (1) Ermittlung des Mittelpunktes einer Strecke.

(2) Ermittlung der Mittelsenkrechten einer Strecke.

(3) Fällen des Lotes auf eine Gerade g von einem Punkt außerhalb von g.

(4) Errichten des Lotes in einem Punkt P einer Geraden g.

(5) Konstruktion der Parallelen zu einer Geraden g durch einen Punkt P.

Sei $M \subset \mathbb{E}$ gegeben. Um algebraische Methoden anwenden zu können, identifizieren wir $\mathbb{E}$ mit $\mathbb{R}^2$ wie folgt: Wir wählen zwei verschiedene Punkte aus M und identifizieren die Gerade durch diese Punkte mit der x-Achse. Den einen Punkt nehmen wir als Nullpunkt $(0,0)$, den anderen als $(1,0)$. Damit haben wir die Einheit festgelegt. Die y-Achse ist die Senkrechte zur x-Achse im Punkt $(0,0)$. Weiter identifizieren wir $\mathbb{R}$ mit der x-Achse.

Damit enthält M in Zukunft stets die Punkte $(0,0)$ und $(1,0)$ aus $\mathbb{R}^2$.

15.5 $a = (x,y)$ ist genau dann aus M konstruierbar, wenn $x, y \in \mathbb{R}$ aus M konstruierbar sind (wir erinnern $x, y \in \mathbb{R}$ stehen für $(x,0), (y,0) \in \mathbb{R}^2$).

Beweis: Ist a konstruiert, erhalten wir $(x,0)$ und $(0,y)$, indem wir von a das Lot auf die x-Achs und y-Achse fällen. Der Kreis um $(0,0)$ mit Radius $\overline{(0,0),(0,y)}$ gibt uns dann $(y,0)$.

Sind umgekehrt $(x,0)$ und $(y,0)$ konstruiert, erhalten wir wie eben auch $(0,y)$ und damit (x,y) als Schnittpunkt des Lotes in $(x,0)$ zur x-Achse und des Lotes in $(0,y)$ zur y-Achse. □

15.6 Satz: Sei $\mathbb{K}_M$ die Menge der aus M in endlich vielen Schritten konstruierbaren Elemente von $\mathbb{R}$ (also die konstruierbaren Elemente auf der x-Achse) Dann gilt:

(1) $\mathbb{K}_M \subset \mathbb{R}$ ist ein Unterkörper.

(2) Ist $a \geq 0$ aus $\mathbb{K}_M$, dann ist auch $\sqrt{a} \in \mathbb{K}_M$.

Beweis: s. Grundkurs Satz 12.14.

Aus dem Grundkurs wissen wir weiter

15.7 (1) Jeder Unterkörper $\mathbb{K}$ von $\mathbb{R}$ enthält $\mathbb{Q}$.

(2) Für alle $d \in \mathbb{N}$ gilt $\mathbb{Q}(\sqrt{d}) \subset \mathbb{K}_M$.

Zum Beweis des Hauptresultats benötigen wir

15.8 Lemma: Sei $M \subset \mathbb{R}^2$ und $(0,0), (1,0) \in M$. Sei $\mathbb{K} \subset \mathbb{R}$ ein Unterkörper, der die Koordinaten aller Punkt aus M enthält. Dann gibt es zu jedem Punkt $a = (x,y) \in \mathbb{R}^2$, der sich aus M durch einen einzigen Konstruktionsschritt 15.1 konstruieren lässt, einen Zwischenkörper $\mathbb{K} \subset \mathbb{L} \subset \mathbb{R}$, so dass $x, y \in \mathbb{L}$ und $[\mathbb{L} : \mathbb{K}] \leq 2$.

Beweis: Wir gehen die möglichen Konstruktionsschritte durch:

(1) a ist Schnittpunkt zweier Geraden g_1 und g_2. Dabei geht g_i durch die Punkte (x_i, y_i) und (u_i, v_i), $i = 1, 2$. Dann genügt g_i der allgemeinen Geradengleichung

$$(y - y_i) \cdot (u_i - x_i) = (x - x_i) \cdot (v_i - y_i)$$

Damit sind die Koordinaten (x, y) von a Lösungen des linearen Gleichungssystems

$$\begin{aligned} (y - y_1)(u_1 - v_1) &= (x - x_1)(v_1 - y_1) \\ (y - y_2)(u_2 - v_2) &= (x - x_2)(v_2 - y_2 \end{aligned}$$

dessen Koeffizienten alle in $\mathbb{K}$ liegen. Löst man dieses Gleichungssystem (etwa mit der Einsetzmethode), addiert, subtrahiert, multipliziert und dividiert man die Elemente aus $\mathbb{K}$. Folglich liegen x und y bereits in $\mathbb{K}$. Nehme $\mathbb{L} = \mathbb{K}$.

(2) $a = (x, y)$ ist Schnittpunkt einer Geraden g durch Punkte (x_1, y_1) und (x_2, y_2) aus M mit einem Kreis k um (x_3, y_3) aus M, dessen Radius r der Abstand zweier Punkte (x_4, y_4) und (x_5, y_5) aus M ist. Dann ist

$$r^2 = (x_4 - x_5)^2 + (y_4 - y_5)^2 \in \mathbb{K}$$

und (x, y) ist Lösung des Gleichungssystems

$$\begin{aligned} (y - y_1)(x_2 - x_1) &= (x - x_1)(y_2 - y_1) && \text{I} \\ (x - x_3)^2 + (y - y_3)^2 &= r^2 && \text{II}, \end{aligned}$$

dessen Koeffizienten alle in $\mathbb{K}$ liegen. Wir lösen I nach x oder y auf und setzen in II ein. Da mindestens einer der Faktoren $(x_2 - x_1)$ oder $(y_2 - y_1)$ von 0 verschieden ist, ist das möglich. Können wir I z.B. nach y auflösen, erhalten wir so eine quadratische Gleichung für x mit Koeffizienten in $\mathbb{K}$. Ist die Lösung $x \in \mathbb{K}$, so liegt wegen I mit x auch y in $\mathbb{K}$, und wir nehmen wieder $\mathbb{L} = \mathbb{K}$. Liegt x nicht in $\mathbb{K}$, so ist sein Minimalproblem in $\mathbb{K}[X]$ durch die quadratische Gleichung gegeben, also vom Grad 2. In diesem Fall setzen wir $\mathbb{L} = \mathbb{K}(x)$. Aus Gleichung I folgt, dass dann auch y in $\mathbb{L}$ liegt.

(3) a ist Schnittpunkt zweier Kreise k_i um Punkte $(x_i, y_i) \in M$, deren Radien r_i Abstände von Punkten aus M sind, $i = 1, 2$. Wie in (2) ist $r_i^2 \in \mathbb{K}$. Dann ist (x, y) Lösung des Gleichungssystems

$$\begin{aligned} (x - x_1)^2 + (y - y_1)^2 &= r_1^2 && \text{I} \\ (x - x_2)^2 + (y - y_2)^2 &= r_2^2 && \text{II} \end{aligned}$$

mit Koeffizienten in $\mathbb{K}$. Ziehen wir II von I ab, fallen die quadratischen Terme in x und y weg. Wir können dann nach x oder y auflösen und wie im Fall (2) weiter verfahren. □

Sei $\mathbb{Q}(M) \subset \mathbb{R}$ der kleinste Unterkörper von $\mathbb{R}$, der $\mathbb{Q}$ und und die Koordinaten aller Punkte aus M enthält. Wie in 2.9 kann man zeigen, dass

$$\mathbb{Q}(M) = \bigcap \{\mathbb{K};\ \mathbb{K} \text{ ist Unterkörper von } \mathbb{R} \text{ und } M \subset \mathbb{K}\}.$$

Offensichtlich gilt $\mathbb{Q}(M) \subset \mathbb{K}_M$.

15.9 Konstruierbarkeitskriterium: Sei $M \subset \mathbb{R}^2$ und $(0,0), (1,0)$ aus M.

(i) $a = (x, y)$ ist genau dann aus M konstruierbar, wenn es eine Kette

$$\mathbb{K}_0 = \mathbb{Q}(M) \subset \mathbb{K}_1 \subset \mathbb{K}_2 \subset \ldots \subset \mathbb{K}_n$$

von Unterkörpern von $\mathbb{R}$ gibt, so dass $[\mathbb{K}_i : \mathbb{K}_{i-1}] \leq 2$ für $1 = 1, \ldots n$ und die Koordinaten von a in $\mathbb{K}_n$ liegen.

(ii) Ist $a = (x, y)$ aus M konstruierbar, dann sind x und y algebraisch über $\mathbb{Q}(M)$ und die Grade ihrer Minimalpolynome aus $\mathbb{Q}(M)[X]$ sind Potenzen von 2.

Beweis: Ist a aus M in endlich vielen Schritten konstrierbar, dann gibt es Punkte $a_1, a_2, \ldots, a_n$ aus $\mathbb{R}^2$, so dass $a_n = a$, und a_i aus

$$M_{i-1} = M \cup \{a_1, \ldots, a_{i-1}\}$$

in einem Schritt konstruierbar ist. Sei $\mathbb{K}_0 := \mathbb{Q}(M)$. Nach 15.8 gibt es Körper $\mathbb{K}_i$, so dass

(i) $\mathbb{K}_0 \subset \mathbb{K}_1 \subset \mathbb{K}_2 \subset \ldots \subset \mathbb{K}_n$

(ii) Die Koordinaten von a_i und damit aller Punkte aus M_i liegen in $\mathbb{K}_i$.

(iii) $[\mathbb{K}_i : \mathbb{K}_{i-1}] \leq 2 \quad \forall i = 1, 2, \ldots, n.$

Nach der Gradschachtelungsformel ist

$$[\mathbb{K}_n : \mathbb{K}_0] = [\mathbb{K}_n : \mathbb{Q}(M)] = [\mathbb{K}_n : \mathbb{K}_{n-1}] \cdot [\mathbb{K}_{n-1} : \mathbb{K}_{n-2}] \cdot \ldots \cdot [\mathbb{K}_1 : \mathbb{K}_0]$$

eine Potenz von 2, etwa 2^r für ein $r \leq n$.
Da $\mathbb{K}_0 \subset \mathbb{K}_n$ und $x, y \in K_n$, gilt

$$\mathbb{K}_0 \subset \mathbb{K}_0(x) \subset \mathbb{K}_n, \quad \mathbb{K}_0 \subset \mathbb{K}(y) \subset \mathbb{K}_n$$

Nach der Gradschachtelungsformel gilt

$$2^r = [\mathbb{K}_n : \mathbb{K}_0] = [\mathbb{K}_n : \mathbb{K}_0(x)] \cdot [\mathbb{K}(x), \mathbb{K}_0].$$

Also ist $[\mathbb{K}_0(x), \mathbb{K}_0]$ und damit nach 14.11 auch der Grad des Minimalpolynoms von x in $\mathbb{K}_0[X]$ eine Potenz von 2. Entsprechendes gilt für y.

Das beweist (ii) und die eine Richtung von (i). Sei umgekehrt die Bedingung aus (i) erfüllt. Wir müssen zeigen, dass a konstruiert werden kann. Wir zeigen nun induktiv, dass $\mathbb{K}_i \subset \mathbb{K}_M$ für $0 \leq i \leq n$. Es folgt, dass die Koordinaten von a in $\mathbb{K}_M$ liegen, dass also a aus M konstruiert werden kann.

Wie wir oben angemerkt haben, gilt $\mathbb{K}_0 = \mathbb{Q}(M) \subset \mathbb{K}_M$. Im Induktionsschritt müssen wir zeigen: Ist $\mathbb{K}_{i-1} \subset \mathbb{K}_M$, dann folgt $\mathbb{K}_i \subset \mathbb{K}_M$. Ist $[\mathbb{K}_i : \mathbb{K}_{i-1}] = 1$, gilt $\mathbb{K}_i = \mathbb{K}_{i-1}$, und wir brauchen nichts zu zeigen. Ist $[\mathbb{K}_i : \mathbb{K}_{i-1}] = 2$, ergänzen wir das linear unabhängige Element 1 zu einer $\mathbb{K}_{i-1}$-Basis $\{1, \alpha\}$ von $\mathbb{K}_i$. Dann hat α^2 eine Darstellung $\alpha^2 = a \cdot \alpha + b \cdot 1$ mit $a, b \in \mathbb{K}_{i-1}$. Insbesondere ist α als Lösung einer quadratischen Gleichung mit Koeffizienten in $\mathbb{K}_{i-1}$ nach 15.6 aus $\mathbb{K}_{i-1}$ konstruierbar und damit auch jedes Element von $\mathbb{K}_i$. $\square$

16 Die klassischen Probleme

Die Quadratur des Kreises:

16.1 Theorem: Die Quadratur des Kreise mit Zirkel und Lineal ist nicht möglich.

Beweis: Gegeben sei ein Kreis in der Ebene $\mathbb{E}$ mit Mittelpunkt P und Radius r. Wir zeichnen eine Gerade durch P und wählen das Koordinatensystem so, dass P der Punkt $(0,0)$ und ein Schnittpunkt der Geraden mit dem Kreis der Punkte $(1,0)$ ist. Wir müssen dann aus $M = \{(0,0),(1,0)\}$ ein Quadrat mit dem Flächeninhalt $\pi \cdot 1^2 = \pi$ konstruieren, denn r ist nun die Einheit. Dann wäre $\sqrt{\pi}$ die Grundseite dieses Quadrates. Wäre der Kreis mit Zirkel und Lineal quadrierbar, dann wäre also $\sqrt{\pi}$ und damit auch π aus M konstruierbar. Nach 15.9 wäre somit π algebraisch über $\mathbb{Q}(M) = \mathbb{Q}$, im Widerspruch zum Satz von Lindemann (s. 14.5.2) □

Damit weiß man seit 1882, dass Theorem 16.1 wahr ist.

Die Würfelverdoppelung:

Wärend einer Seuche in Griechenland befragten die betroffenen Bewohner das Orakel des Apoll, wie Abhilfe geschaffen werden könnte. Apoll versprach, die Seuche zu beenden, falls sein würfelförmiger Altar durch einen mit doppelten Volumen ersetzt wird.

Die Griechen machten sich also daran, die Seitenlänge dieses Altars zu konstruieren. Natürlich versuchten sie es zunächst mit Zirkel und Lineal, weil sie folgendes Ergebnis nicht kannten:

16.2 Theorem: Die gefragte Würfelverdopplung ist mit Zirkel und Lineal nicht möglich.

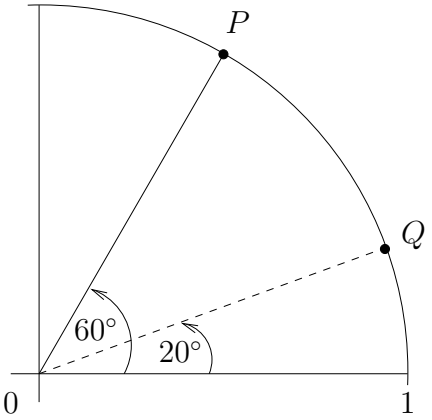
Beweis: Erklären wir die Kantenlänge des gegebenen Würfels zur Einheit, dann enthält M die reellen Zahlen $0, 1, \sqrt{2}, \sqrt{3}$, die letzteren als Flächen- bzw. Raumdiagonale. Zu konstruieren ist die Kantenlänge eines Würfels mit doppeltem Einheitsvolumen, also $\sqrt[3]{2}$.

Sei $M' = \{(0,0),(1,0)\}$. Nach 15.6 sind $\sqrt{2}$ und $\sqrt{3}$ aus M' konstruierbar. Wäre $\sqrt[3]{2}$ aus M konstruierbar, so wäre es auch aus M' konstruierbar. Das Minimalpolynom von $\sqrt[3]{2}$ über $\mathbb{Q}(M') = \mathbb{Q}$ ist nach 14.11 das Polynom $X^3 - 2$, ein Polynom 3. Grades. Nach 15.9 müßte 3 eine Potenz von 2 sein, ein Widerspruch! □

Die Winkeldrittelung:

16.3 Theorem: Nicht jeder Winkel lässt sich mit Zirkel und Lineal dritteln. Insbesondere lässt sich ein Winkel von 60° nicht mit Zirkel und Lineal dritteln.

Beweis: Gegeben ist ein Winkel um 60°. Wir schlagen einen beliebigen Kreis um seinen Scheitelpunkt, den Radius des Kreises erklären wir zur Einheit,



so dass folgende Situation vorliegt. Wir müssen aus den Punkten $(0,0),(1,0)$ und P den Punkt Q konstruieren.
Die Koordinaten von P sind

$$P = (\cos 60°, \sin 60°) = \left(\frac{1}{2}, \frac{1}{2}\sqrt{3}\right).$$

Die Koordinaten von Q sind

$$Q = (\cos 20°, \sin 20°).$$

Da $\frac{1}{2}$ und $\frac{1}{2}\sqrt{3}$ nach 15.6 aus $(0,0)$, $(1,0)$ konstruiert werden können, kann Q genau dann aus $(0,0)$, $(1,0)$ und P konstruiert werden, wenn Q aus $(0,0)$ und $(1,0)$ konstruiert werden kann. Sei also $M = \{(0,0),(1,0)\}$. Wir müssen $\cos 20°$ und $\sin 20°$ aus M konstruieren.

Ist $\cos 20°$ aus M konstruierbar, dann auch $2 \cdot \cos 20°$. Nun folgt aus den Additionstheoremen

$$\cos 3\alpha = 4\cos^3\alpha - 3\cos\alpha.$$

Also

$$1 = 2\cos 60° = 8\cos^3 20° - 6\cos 20° = (2 \cdot \cos 20°)^3 - 3 \cdot (2\cos 20°).$$

Damit ist $2 \cdot \cos 20°$ Nullstelle des Polynoms

$$f = X^3 - 3X - 1.$$

Nach 13.19 und 13.21 ist f irreduzibel in $\mathbb{Z}[X]$ und damit nach 13.20 irreduzibel in $\mathbb{Q}[X]$. Damit ist f nach 14.10 das Minimalpolynom von $2 \cdot \cos 20°$ über $\mathbb{Q}(M) = \mathbb{Q}$. Nach 15.9 müsste der Grad von f aber eine Potenz von 2 sein.

□

Reguläre n-Ecke:

Folgendes Resultat zählt nicht zu den klassischen Problemen, sollte aber jeder Mathematiklehrerin bekannt sein:

16.4 Theorem: (Johann Carl Friedrich Gauß 1777-1855) Das reguläre n-Eck ist genau dann mit Zirkel und Lineal konstruierbar, wenn n eine Primfaktorzerlegung der Form

$$n = 2^r \cdot p_1 \cdot p_2 \cdot \ldots \cdot p_s$$

besitzt, wobei $r \geq 0$ und $p_1, \ldots, p_s$ paarweise verschiedene Primzahlen der Form

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

mit $k \in \mathbb{N}_0$ sind.

16.5 Bemerkung: Die Zahl $F_k = 2^{2^k} + 1$, $k \in \mathbb{N}_0$, heißt k-te *Fermat'sche Zahl* nach Pierre de Fermat (1601-1665). Fermat vermutete 1650, dass alle Fermat'schen Zahlen prim sind. Das ist richtig für $F_0 = 3$, $F_1 = 5$, $F_2 = 17$, $F_3 = 257$, $F_4 = 65537$, aber $F_5 = 641 \cdot 6700417$, wie Euler 1732 zeigte.

Außer $F_0, \ldots, F_4$ sind keine weiteren Fermat'schen Primzahlen bekannt.

16.6 Bemerkung: (1) Ist das reguläre n-Eck konstruierbar, dann ist auch das reguläre $(2n)$-Eck konstruierbar (konstruiere die Winkelhalbierende).

(2) Ist $n = k \cdot l$ mit $k, l > 2$ und ist das reguläre n-Eck konstruierbar, dann sind natürlich auch das reguläre k-Eck und l-Eck konstruierbar.

(3) Sind k und l teilerfremd und sind das reguläre k-Eck und l-Eck konstruierbar, dann ist auch das reguläre $(k \cdot l)$-Eck konstruierbar: Es gibt $a, b \in \mathbb{Z}$, so daß

$$a \cdot k + b \cdot l = 1.$$

Es folgt $\frac{1}{k \cdot l} = a \cdot \frac{1}{l} + b \cdot \frac{1}{k}$. Die Kantenlänge des $(k \cdot l)$-Ecks erhalten wir also durch a-faches Abtragen der Kantenlänge des l-Ecks am Einheitskreis, gefolgt von b-fachen Abtragen der Kantenlänge des k-Ecks.

Also genügt es zu untersuchen, wann das reguläre p^k-Eck konstruiert werden kann, wobei $p > 2$ eine Primzahl ist.

Trotzdem reichen unsere algebraischen Mittel nicht aus, Theorem 16.4 zu beweisen. Man geht wie folgt vor:

(1) Ist $(1,0)$ der erste Eckpunkt und (x,y) der nächste im regulären n-Eck, dann gilt $x = \cos\frac{2\pi}{n}$ und $y = \sin\frac{2\pi}{n}$. Also brauchen wir das Minimalpolynom von $\cos\frac{2\pi}{n}$ oder von $\sin\frac{2\pi}{n}$. Geschickter ist es, (x,y) mit der komplexen Zahl $x + i \cdot y$ zu identifizieren und die Menge der aus M konstruierbaren **komplexen** Zahlen zu betrachten.

(2) Die Ausgangsmenge M ist dann eine Teilmenge von $\mathbb{C}$. Wieder ist die Menge $\mathbb{C}_M$ der aus M konstruierbaren komplexen Zahlen ein Unterkörper von $\mathbb{C}$ (die Beweise sind dieselben wie oben).

(3) Ist $\overline{M} = \{x - i\cdot y : \ x + i\cdot y \in M\}$, dann ist $\overline{M}$ aus M konstruierbar. Das Konstruierbarkeitskriterium überträgt sich fast wörtlich: Man muss nur $\mathbb{Q}(M)$ durch $\mathbb{Q}(M \cup \overline{M})$ ersetzen.

(4) Jetzt benötigt man das Minimalpolynom der komplexen Zahl $\zeta = \cos\frac{2\pi}{n} + i\cdot\sin\frac{2\pi}{n}$ über $\mathbb{Q}$. Aus den Additionstheoremen folgt, dass $\zeta^n = 1$. Daher ist das Minimalpolynom als Faktor von $X^n - 1$ mit nicht allzu großem Aufwand findbar.

(5) Für die hinreichende Aussage von 16.4 müssen wir das Kriterium von 15.9(i) verifizieren. Dafür benötigt man Resultate aus der Galois-Theorie (nach Evariste Galois 1811-1832) und die Sylowsätze 9.7.

16.7 Kurze Geschichte der Konstruktionen:

Euklid (∼325-265 v.Chr.) kannte die Konstruktionen von Dreieck, Quadrat und regulärem 5-Eck.

Erchinger konstruierte auf der Basis der Ergebnisse von Gauß um 1800 herum das reguläre 17-Eck.

Richelot und unabhängig davon Schwendenwein konstruierten gegen 1890 das 257-Eck.

Hermes beschäftigte sich um 1900 ganze 10 Jahre lang mit der Konstruktion des 65537-Ecks, führte sie aber nicht durch.

Bishop hat 1978 die Konstruktion computerisiert.