Einführung in die Algebra

Vorlesung im
Sommersemester 2008
Technische Universität Berlin

gehalten von
Prof. Dr. M. Pohst

Contents

CHAPTER 1

Vorbemerkungen

Gegenstand der Vorlesung sind die Grundstrukturen:
Gruppen, Ringe, Körper.

Herkunft:
aljahr (arabisch) bedeutet Ergänzung, Ausgleich.
$\Rightarrow$ Lösung von Gleichungen

Grundproblem: Gegeben Körper K oder Ring R (kommutativ mit Eins) und Polynom $f(t) \in R[t]$.
Frage: Existiert $x \in R$ mit $f(x) = 0$ (Berechnung!) bzw. Problem der Konstruktion eines Erweiterungskörpers bzw. Oberrings, in dem f eine Nullstelle besitzt.

Beispiel:

(i) $R = \mathbb{Z},\ f(t) = t + 2$ hat Nullstelle $t = -2$.
(ii) $R = \mathbb{Z},\ f(t) = 3t + 2$ hat in R keine Nullstelle, wohl aber in $\mathbb{Q}$.
(iii) $f(t) = t^2 + 1$ hat erst in $\mathbb{C}$ eine Nullstelle (jedoch auch in $\mathbb{Z}[i]$).
(iv) $f(t) = t^4 - 4t^2 + 1$ hat Koeffizienten aus $\mathbb{Z}$.
Gesucht: Ring $R \supseteq \mathbb{Z}$ und $x \in R$ mit $f(x) = 0$.
Es wird geeignete Erweiterung gesucht, in der die Gleichung Nullstellen besitzt. Nullstellen durch Wurzeln ausdrücken:

$$x = \sqrt{2 + \sqrt{3}}$$

Problem:
Darstellung der Nullstellen durch Wurzelausdrücke. Dies geht für Polynome vom Grad ≤ 4, bei Polynomen höheren Grades dagegen i.a. nicht mehr. ($\mathcal{S}_n$ ist für $n \geq 5$ nicht auflösbar!)

Galoistheorie:
Gewisse Erweiterungskörper lassen sich gruppentheoretisch beschreiben.

Hauptsatz der Algebra:
Jedes Polynom mit reellen Koeffizienten besitzt eine Wurzel in $\mathbb{C}$.

Anwendungen: Konstruktion mit Zirkel und Lineal.

Es seien M, N nicht leere Mengen und

$$f\,:\,M\times M\to M,\quad g\,:\,N\times M\to M$$

Abbildungen. f heißt (binäre) innere, g äußere Verknüpfung, N der Operatorbreich von g. Eine Menge mit einer oder mehereren Verknüpfungen heißt algebraische Struktur.
Statt $f(m_1,\,m_2)$ schreibt man kurz: $m_1m_2,\ m_1\circ m_2,\ m_1\cdot m_2$ bzw. $m_1\Box\, m_2$.

Eine innere Verknüpfung heißt kommutativ, falls

$$m_1\circ m_2=m_2\circ m_1\quad\forall m_1,\,m_2\in M,$$

assoziativ, falls

$$(m_1\circ m_2)\circ m_3=m_1\circ(m_2\circ m_3)\quad\forall m_1,\,m_2\,m_3\in M$$

gilt.

Bemerkung:
Ohne Assoziativität sind $(m_1\circ m_2)\circ m_3$ und $m_1\circ(m_2\circ m_3)$ i.a. verschieden. Für die Verknüpfung von 4 Elementen ergeben sich bereits 5 Möglichkeiten für das Resultat.
Definition Eine nicht leere Menge M mit einer (binären) assoziativen inneren Verknüpfung heißt Halbgruppe.

Beispiele:

(i) $(\mathbb{Z},+)$, $(\mathbb{Z},\cdot)$, $(\mathbb{Z}/m\mathbb{Z},+)$, $(\mathbb{Z}/m\mathbb{Z},\cdot)$, $n\times n$-Matrizen bzgl. Addition und Multiplikation.

(ii) Nicht assoziativ ist die Verknüpfung ":" auf $\mathbb{Q}^\times=\mathbb{Q}\backslash\{0\}$:

$$x:(y:z)=\frac{x\,z}{y}$$

ist i.a. nicht gleich

$$(x:y):z=\frac{x}{y\,z}.$$

Gegenbeispiel: $x=y=1,\ z=2$.

Ein Element $e\in M$ heißt Linkseins (Rechtseins), falls $e\circ x=x$ ($x\circ e=x$) für alle $x\in M$ gilt. Ist e sowohl Linkseins als auch Rechtseins, so heißt e Einselement von M.

Bemerkung:

(i) Ein Einselement ist stets eindeutig bestimmt. Sind etwa e, $\tilde e$ Einselemente, so gilt

$$\begin{aligned} e &= e\,\tilde e \quad (\tilde e \text{ als Rechtseins})\\ &= \tilde e \qquad (e \text{ als Linkseins}).\end{aligned}$$

(ii) Linkseinsen hängen natürlich (bei fester Menge) von der Verknüpfung ab:
In $(\mathbb{Z},+)$ ist 0 Einselement, in $(\mathbb{Z},\cdot)$ ist dies 1.

(iii) In einer Halbgruppe besitzt ein Produkt von $n \in \mathbb{Z}^{\geq 2}$ Faktoren bei jeder Beklammerung denselben Wert (Beweis mittels Induktion über n), Klammern können folglich weggelassen werden.

Potenzen lassen sich wie folgt definieren:

$$\begin{aligned} a^1 &:= a, \\ a^{n+1} &:= a \cdot a^n. \end{aligned}$$

Besitzt M ein Einselement e, so setzt man fest: $a^0 = e$.
Hierfür gelten die Rechenregeln

$$\begin{aligned} x^{m+n} &= x^m \circ x^n, \\ (x^m)^n &= x^{mn} \quad (m,\, n \in \mathbb{Z}^{\geq 0}), \end{aligned}$$

die ebenfalls mittels Induktion (etwa nach n) bewiesen werden. Dagegen gilt

$$(x\,y)^n = x^n\,y^n$$

i.a. nur, falls M kommutativ ist, d.h. die Verknüpfung auf M kommutativ ist.
Definition Eine Halbgruppe M mit Einselement e heißt Monoid.

Beispiel: $(2\mathbb{Z}, +)$ ist Monoid, $(2\mathbb{Z}, \cdot)$ nicht.

Strukturgleichheit von algebraischen Strukturen:
Es seien $(X, \circ)$ und $(Y, \square)$ zwei algebraische Strukturen. Dann heißt eine Abbildung

$$f : X \to Y \text{ mit } f(x_1 \circ x_2) = f(x_1) \square f(x_2)$$

Homomorphismus. f heißt $\left\{ \begin{array}{l} \text{Monomorphismus} \\ \text{Epimorphismus} \\ \text{Isomorphismus} \end{array} \right\}$, falls f $\left\{ \begin{array}{l} \text{injektiv} \\ \text{surjektiv} \\ \text{bijektiv} \end{array} \right\}$
ist.
Im Fall $X = Y$, $\circ = \square$ heißt ein Homomorphismus (Isomorphismus) f auch Endomorphismus (Automorphismus).
Beschreibung durch ein Diagramm:

$$\begin{array}{ccc} X \times X & \xrightarrow{\circ} & X \\ {\scriptstyle f\times f}\downarrow & /\!/\!/ & \downarrow{\scriptstyle f} \\ Y \times Y & \xrightarrow{\square} & Y \end{array}$$

///: Diagramm ist kommutativ, d.h. $f \circ = \square\,(f \times f)$.

Bemerkung:
Die Hintereinanderausführung (Produkt) von Homomorphismen ist ein Homomorphismus. Das Produkt zweier Mono-, Epi-, Isomorphismen ist wieder ein Mono-, Epi-, Isomorphismus. Das Inverse eines Isomorphismus ist Isomorphismus.

Zwei algebraische Strukturen heißen isomorph (strukturgleich), falls es zwischen ihnen einen Isomorphismus gibt.

Beispiel:
Es sei M ein Monoid. Dann gibt es zu $a \in M$ genau einen Homomorphismus $f = f_a$ mit

$$f \,:\, \mathbb{N} \to M \;:\; n \mapsto a^n.$$

Definition Es sei M ein Monoid, in dem zu $a \in M$ stets $b \in M$ mit $b \circ a = e$ existiert. Dann heißt M eine Gruppe. b heißt Linksinverses zu a, analog: Rechtsinverses.
Satz Es sei G eine Halbgruppe mit den Eigenschaften

(i) $\exists e \in G \;\forall a \in G \;:\; e \circ a = a$;
(ii) $\forall a \in G \;\exists b \in G \;:\; b \circ a = e$.

Dann ist G eine Gruppe.

Beweis:
$a \in G$ beliebig mit Linksinversem b.
Wir zeigen zunächst:
b ist auch Rechtsinvereses. Zunächst existiert $c \in M$ mit $c \circ b = e$. Hierfür ist dann

$$\begin{aligned} a \circ b &= e \circ (a \circ b) \\ &\overset{\text{(ii)}}{=} (c \circ b) \circ (a \circ b) = c \circ (b \circ a) \circ b \\ &= (c \circ e) \circ b = c \circ (e \circ b) \\ &= c \circ b \\ &= e. \end{aligned}$$

Damit gilt dann auch

$$\begin{aligned} a \circ e &= a \circ (b \circ a) \\ &= e \circ a \\ &= a, \end{aligned}$$

d.h. e ist Rechtseins. Also ist e Einselement, G Monoid und nach (1.3) eine Gruppe.

□

Eigenschaften von Gruppen
(vergleiche Lineare Algebra I)
Das Inverse eines Elements a ist eindeutig bestimmt (Schreibweise: a^{-1}). Zu a, $b \in G$ existieren eindeutig x, $y \in G$ mit

$$\begin{array}{ccc} y \circ a = b & \text{und} & a \circ x = b. \\ (y = b \circ a^{-1}) & & (x = a^{-1} \circ b) \end{array}$$

Zu $a \in G$ ist $(a^{-1})^{-1} = a$, zu a, $b \in G$ ist $(a\,b)^{-1} = b^{-1}\,a^{-1}$.

Es gelten die Kürzungsregeln:

$$a \circ c = b \circ c \;\Rightarrow\; a = b,$$
$$d \circ a = d \circ b \;\Rightarrow\; a = b.$$

Eine Gruppe G heißt kommutativ oder abelsch, falls

$$a \circ b = b \circ a \qquad \forall a,\, b \in G$$

gilt. In diesem Fall schreibt man $\circ$ zumeist als Addition. Ansonsten $\circ$ als Produkt:

$$a \circ b =: a\, b.$$

Lemma Eine Halbgruppe G ist genau dann eine Gruppe, falls zu $a,\, b \in G$ stets $x,\, y \in G$ mit $a \circ x = b$ und $y \circ a = b$ existieren.

Beweis:
$\Rightarrow$ klar,
$\Leftarrow$ Für $a \in G$ existiert stets e mit $e \circ a = a$.
Zu zeigen: $e \circ b = b$ für alle $b \in G$ ($\Rightarrow$ e Linkseins).
Zunächst existiert $x \in G$ mit $a \circ x = b$, und damit wird

$$e \circ b = e \circ (a \circ x) = (e \circ a) \circ x = a \circ x = b.$$

Damit ist (i) von (1.4) erfüllt. Zum Nachweis von (ii) wende man die Voraussetzung für y auf das Paar $(a,\, e)$ an, also gilt die Behauptung nach (1.4).

□

Definition Es sei M eine (nicht leere) Menge.
Eine Teilmenge R von $M \times M$ heißt Relation.
$R \neq \emptyset$ heißt Äquivalenzrelation (auf M), falls gilt:

(i) $a \in M \Rightarrow (a, a) \in R$ (Reflexivität),
(ii) $(a, b) \in R \Rightarrow (b, a) \in R$ (Symmetrie),
(iii) $(a, b)(b, c) \in R \Rightarrow (a, c) \in R$ (Transitivität).

Für $(a, a) \in R$ heißt $K_a := \{b \in M \setminus (a, b) \in R\}$ Äquivalenzklasse zu a. Statt $(a, b) \in R$ schreibt man auch $a \sim b$.

Satz Es sei M eine nicht leere Menge.

(i) Ist R Äquivalenzrelation auf M, so gilt : $M = \bigcup_{a \in M} K_a$ und $K_a \cap K_n = \emptyset$ für $(a, b) \notin R$.
(ii) Ist $M = \bigcup_{i \in I} M_i$ mit nicht leeren Teilmengen M_i, so wird mittels $A \sim b :\Leftrightarrow J_i \in I : a, b \in M_i$ auf M eine Äquivalenzrelation erklärt.

CHAPTER 2

Gruppen

2.1. Definition

Es sei G eine nicht leere Menge mit einer Abbildung $\circ : G \to G$ mit den Eigenschaften:

(i) $\forall a, b, c \in G : (a \circ b) \circ c = a \circ (b \circ c)$,
(ii) $Je \in G \; \forall a \in G : e \circ a = a \circ e = a$,
(iii) $\forall a \in G \; Jb \in G : a \circ b = b \circ a = e$.

Dann heißt $(G, \circ)$, (bzw. G) eine Gruppe, e Einselement von G, b inverses Element zu a (Schreibweise: a^{-1}).

Bemerkungen:

(i) Man beachte die Reihenfolge der Eigenschaften (ii) und (iii)!
(ii) G heißt abelsch (kommutativ), falls $a \circ b = b \circ a \, \forall \, a, b \in G$ gilt.

Wichtige Beispiele von Gruppen sind die sogenannten "Permutationsgruppen". Später werden wir sehen, dass sich jede Gruppe als Permutationsgruppe auffassen lässt.

Beispiel: Die bijektiven Abbildungen einer Menge von n Elementen (etwa $\mathbb{N}_n := \{1, 2, \ldots, n\}$ für $n \in \mathbb{N}$ bilden bzgl. Hintereinanderausführung eine Gruppe S_n, die sogenannte symmetrische Gruppe. Die Elemente von S_n heissen Permutationen.
Schreibweise: $\pi : \mathbb{N}_n \to \mathbb{N}_n$ lässt sich durch die Angabe der Bilder darstellen, mittels $\begin{pmatrix} 1 & 2 & \ldots & n \\ \pi(1) & \pi(2) & \ldots & \pi(n) \end{pmatrix}$.

Beispiele: $\begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$, $\begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$, $\begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}$, $\begin{pmatrix} 1 \\ 1 \end{pmatrix}$.

Das Einzelelement von S_n ist die Identität $id = \begin{pmatrix} 1 & 2 & \ldots & n \\ 1 & 2 & \ldots & n \end{pmatrix}$.

Beim Rechnen mit Permutationen ist die Reihenfolge der Abbildungen ab $n \geq 2$ wichtig:

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \quad \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$

(zunächst wird 1 auf 3, 3 im zweiten Schritt auf 3 abgebildet, 2 wird zuerst auf 2 und diese dann auf 1 abgebildet, 3 auf 1 auf 2), jedoch ist

$$\begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \quad \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$$

verschieden vom ersten "Produkt".
Bemerkung: $\#S_n = n!$ (Der Beweis - etwa mittels vollständiger Induktion - wird dem Leser überlassen.) S_3 wird zur Symmetriegruppe des gleichseitigen Dreiecks, wenn man die Ecken mit $1, 2, 3$ nummeriert.

2.2. Definition

$\pi \in S_n$ mit $\pi(i) = j \neq i$ und $\pi(j) = i$ sowie $\pi(k) = k \; \forall \; k \in \mathbb{N}_n \setminus \{i, j\}$ heißt Transposition (Schreibweise: τ_{i_j}).

Man beachte, dass $\tau_{i_j}^{-1} = \tau_{i_j}$ gilt, d.h. Transpositionen sind zu sich selbst invers.

2.3. Satz

Jede Permutation $\pi \in S_n$ lässt sich als Produkt von höchstens n Transpositionen schreiben.

Beweis: Für $\pi = id$ ist π leeres Produkt von Transpositionen. Sei also $S_n \ni \pi \neq id$. Dann existiert $i_1 \in \mathbb{N}_n$ minimal mit $\pi(i_1) = j_1 > i_1$. $\tau_{i_1 j_1}\pi$ ist dann eine Permutation mit $\pi(k) = k$ für $k = 1, \ldots, i$. Iterierte Anwendung liefert $\tau_{i_k j_k} \cdot \tau_{i_{k-i} j_{k-1}} \cdot \ldots \cdot \tau_{i_1 j_1}\pi = id$ bzw. $\pi = \tau_{i_1 j_1}\, \tau_{i_2 j_2} \cdot \ldots \cdot \tau_{i_k j_k} = \pi$.

□

2.4. Definition

$\pi \in \mathfrak{S}_n$ heißt r-Zyklus, falls es eine Teilmenge $\{i_1, \ldots, i_r\}$ von r Elementen von $\{1, \ldots, n\}$ mit

$$\pi\,(i_\nu) = i_{\nu+1} \;\; (1 \leq \nu < r),\; \pi\,(i_r) = i_1,\; \pi\,(j) = j \;\; \forall j \notin \{i_1, \ldots, i_r\}$$

gibt.
Schreibweise:

$$\pi = (i_1, \ldots, i_r) \text{ statt } \begin{pmatrix} 1 & \ldots & n \\ \pi\,(1) & \ldots & \pi\,(n) \end{pmatrix}.$$

Vereinbarung: id $= (1)$.

Bemerkungen:

(i) Transpositionen sind 2-Zyklen $(i,\, j)$;
(ii) $(i_1 \ldots i_r) = (i_1, \pi(i_1), \ldots, \pi^{r-1}(i_1)),\; \pi^r(i_\nu) = i_\nu \;\; (1 \leq \nu \leq r)$;

Rechenregeln für Zyklen:

2.5. Hilfssatz

(i) $(i_1, \ldots, i_r) = (i_\nu, \ldots, i_r,\ i_1, \ldots, i_{\nu-1})\ \ (1 \leq \nu \leq r)$.
(ii) $(i_1, \ldots, i_r) = (i_1, \ldots, i_\nu)\,(i_\nu, \ldots, i_r)\quad (2 \leq \nu \leq r-1)$, mit Anwendung

$$(i_1, \ldots, i_r) = (i_1, i_2)(i_2, i_3) \cdot \ldots \cdot (i_{r-1}, i_r)\,.$$

(iii) $(i_1, \ldots, i_r)^{-1} = (i_r, i_{r-1}, \ldots, i_1)$,
(iv) $\pi\,(i_1, \ldots, i_r)\,\pi^{-1} = (\pi\,(i_1), \ldots, \pi\,(i_r))\ \ \forall \pi \in \mathfrak{S}_n$.
(v) $r \in \mathbb{N}$ ist minimal mit $(i_1, \ldots, i_r)^r = id$.

Beweis:
Bis auf (iv) sind die Aussagen unmittelbar klar. Es genügt, (iv) für Transpositionen zu zeigen, da gemäß (ii)

$$\pi\,(i_1, \ldots, i_r)\,\pi^{-1} = \prod_{j=1}^{r-1} \pi\,(i_j,\ i_{j+1})\,\pi^{-1}$$

ist. Ist nun $\nu \in \{1, \ldots, n\}$ mit $\pi^{-1}(\nu) \notin \{i_j,\ i_{j+1}\}$, dann bleibt ν invariant. Schließlich ist

$$\pi^{-1}(\nu) = i_{j+1} \Leftrightarrow \nu = \pi\,(i_{j+1})\ \text{ sowie }\ \pi^{-1}(\mu) = i_j \Leftrightarrow \mu = \pi(i_j)\,,$$

also gilt insgesamt:

$$\pi\,(i_j,\ i_{j+1})\,\pi^{-1} = \Big(\pi\,(i_j),\ \pi\,(i_{j+1})\Big).$$

□

2.6. Hilfssatz

$$\begin{aligned} \mathfrak{S}_n &= <(i,\ n)\,|\,1 \leq i < n> \quad (\text{für } n \geq 2). \\ &= <(1,\ i)\,|\,1 < i \leq n> \end{aligned}$$

Beweis:
Bekanntlich ist jede Permutation Produkt von (höchstens n) Transpositionen der Form $(i,\ j)\ \ (1 \leq i < j \leq n)$. Ferner gilt:

$$(i,\ j) = (1,\ i)\,(1,\ j)\,(1,\ i)$$

nach (2.5)(iv) für $i > 1$. Analog gilt

$$(i,\ j) = (j,\ n)\,(i,\ n)\,(j,\ n)$$

für $1 \leq i < j \leq n$.

□

2.7. Definition

Zwei Zyklen $(i_1, \ldots, i_r), (j_1, \ldots, j_s)$ heißen elementfremd, falls

$$\{i_1, \ldots, i_r\} \cap \{j_1, \ldots, j_s\} = \emptyset$$

ist.

2.8. Hilfssatz

Elementfremde Zyklen kommutieren.

Beweis:
Es seien $I = \{i_1, \ldots, i_r\},\ J = \{j_1, \ldots, j_s\}\ K = (\mathbb{N}_n \backslash I) \backslash J,\ I \cap J = \emptyset$. Dann gilt

$$\begin{aligned}(i_1, \ldots, i_r)\,(j_1, \ldots, j_s)\,(\nu) &= \begin{cases} \nu & \text{für } \nu \in K \\ j_{l+1} & \text{für } \nu = j_l\ (1 \le l < s) \\ j_1 & \text{für } \nu = j_s \\ i_{l+1} & \text{für } \nu = i_l\ (1 \le l < r) \\ i_1 & \text{für } \nu = i_r \end{cases} \\ &= (j_1, \ldots, j_s)\,(i_1, \ldots, i_r)\,(\nu).\end{aligned}$$

□

Bemerkung:
Es sei $\pi \in S_n$. Durch $i \sim j :\Leftrightarrow \exists k \in \mathbb{Z} : \pi^k(i) = j$ wird auf $\mathbb{N}_n$ eine Äquivalenzrelation erklärt.

Beweis:
Die Reflexivität ist klar mittels $k = 0$. Für $\pi^k(i) = j$ ist $i = \pi^{-k}(j)$, also gilt auch die Symmetrie. Ist schließlich $\pi^k(i_1) = i_2$ und $\pi^l(i_2) = i_3$, so wird $\pi^{k+l}(i_1) = i_3$, es folgt die Transitivität. Man beachte, dass die Äquivalenzklasse K_i von i aus den Elementen $i, \pi(i), \ldots, \pi^{k_i - 1}(i)$ besteht, falls $k_i \in \mathbb{Z}^{\ge 0}$ minimal mit $\pi^{k_i}(i) = i$ gewählt wird. Es besteht folglich eine Bijektion zwischen den Äquivalenzklassen K_i und den Zyklen $(i, \pi(i), \ldots, \pi^{k_i - 1}(i))$.

□

2.9. Satz

Jede Permutation $\pi \in S_n$ läst sich eindeutig als Produkt elementfremder Zyklen darstellen.

Beweis: Für $\pi = id$ handelt es sich um das leere Produkt. Sei also $\pi \neq id$. Dann existiert $i_1 \in \mathbb{N}_n$ minimal mit $\pi(i_1) = j_1 > i_1$. Bilde $M_1 := \left\{\pi^k(i_1) \mid k \in \mathbb{Z}^{\ge 0}\right\} \ni i_1$. Gemäß der vorangehenden Bemerkung existiert ein minimaler Exponent $l_1 \in \mathbb{N}$ mit $\pi^{l_1}(i_1) = i_1$. Also bildet $(i_1, \pi(i_1), \ldots, \pi^{l_1 - 1}(i_1))$ einen Zyklus.

Nunmehr wählt man $i_2 \in \mathbb{N}_n \setminus (\mathbb{N}_{i_1-1} \cup M_1)$ minimal mit $\pi(i_2) = j_2 > i_2$ und bildet $M_2 := \left\{\pi^k(i_2) \mid k \in \mathbb{Z}^{\geq 0}\right\} \ni i_2$. Wir erhalten so etwa r mehrelementige Zyklen $(i_\kappa, \pi(i_\kappa), \ldots, \pi^{l_\kappa - 1}(i_\kappa)) \quad (1 \leq \kappa \leq r)$.

Zusammen mit den einelementigen Zyklen bilden sie die behauptete Produktdarstellung. Zur Eindeutigkeit beachte man, dass die gefundenen Zyklen als Äquivalenzklassen (vgl. vorangehende Bemerkung) disjunkt sind.

□

Beispiel:
Für

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 \\ 2 & 4 & 6 & 8 & 10 & 12 & 14 & 1 & 3 & 5 & 7 & 9 & 11 & 13 & 15 \end{pmatrix}$$

ist

$$\pi = (1,\, 2,\, 4,\, 8)\ (3,\, 6,\, 12,\, 9)\ (5,\, 10)\ (7,\, 14,\, 13,\, 11).$$

Permutationen lassen sich also als Produkte von Transpositionen (nicht eindeutig) oder als Produkte elementfremder Zyklen (eindeutig) darstellen. Hierfür besteht folgender Zusammenhang:

2.10. Hilfssatz

Ist $\pi \in S_n$ einerseits Produkt von r Transpositionen, andererseits Produkt von c elementfremden Zyklen (einelementige mitgezählt), so besteht der Zusammenhang $r \equiv n - c \bmod 2$.

Beweis: Mittels Induktion nach r. Für $r = 0$ gilt $\pi = id$, welches Produkt von n einelementigen Zyklen ist. Sei nun $r > 0$ und die Behauptung für $1, \ldots, r-1$ bereits bewiesen. Zur Produktdarstellung durch Transpositionen $\pi = \tau_1 \cdot \ldots \cdot \tau_r$ bilden wir $\tilde{\pi} = \tau_1 \cdot \ldots \cdot \tau_{r-1}$. $\tilde{\pi}$ habe die Zyklendarstellung $\tilde{\pi} = (i_{j_1}, \ldots, i_{j_2-1})(i_{j_2}, \ldots, i_{j_3-1}) \ldots (i_{j_{m-1}}, \ldots, i_{j_m-1})$. Nach Induktionsvoraussetzung gilt hierfür $r - 1 \equiv n - m \bmod 2$. Da die Zyklen elementfremd sind, lassen sie sich beliebig umordnen, auch innerhalb eines festen Zyklus kann man jedes Element als Anfangselement einsetzen (vgl. 2.5). Wir können also $\tau_r = (i_{j_1}, i_\mu)$ erreichen, wobei entweder $i_\mu = i_{j_2}$ oder $i_\mu \in \left\{\pi^k(i_{j_1}) \mid k \in \mathbb{Z}^{\geq 0}\right\}$ gilt.

1. Fall. $\mu = j_2$.
Die Zyklen beginnend mit $i_{j_3}, \ldots, i_{j_{m-1}}$ bleiben ungeändert. Dagegen "verschmelzen" die beiden ersten Zyklen zu einem einzigen:

$$\left(i_{j_1}, i_{j_2}, i_{j_2+1}, \ldots, i_{j_3-1}, i_{j_2}, i_{j_1+1}, \ldots, i_{j_2-1}\right).$$

Es geht folglich $r - 1$ auf r sowie m auf $m - 1$, so dass die behauptete Kongruenz erfüllt ist.

2. Fall. $\mu = j_1 + \nu \leq j_2 - 1$.
Die Zyklen beginnend mit $i_{j_2}, \ldots, i_{j_{m-1}}$ bleiben ungeändert. Der erste Zyklus dagegen spaltet in zwei neue elementfremde auf:

$$\left(i_{j_1}, i_{j_1+\nu+1}, \ldots, i_{j_2-1}\right)\left(i_{j_1+1}, i_{j_1+2}, \ldots, i_{j_1+\nu}\right).$$

Es gehen $r-1$ auf r sowie m auf $m-1$, die behauptete Kongruenz ist richtig.

□

Der Hilfssatz besagt, dass die Anzahl der Transpositionen bei der Darstellung einer Permutation zwar nicht eindeutig ist, sie ist jedoch stets gerade oder ungerade.

Bemerkung:
$\operatorname{sig} : S_n \to \langle -1 \rangle : \pi = \tau_1 \cdot \ldots \cdot \tau_r \mapsto (-1)^r$ ist ein Homomorphismus. Für $n \geq 2$ ist sig surjektiv.

2.11. Definition

Eine Teilmenge U einer Gruppe G heißt Untergruppe, falls U mit der Verknüpfung von G für sich bereits eine Gruppe bildet.
(Speziell folgt $e \in U$!)

2.12. Kriterium

Es sei G eine Gruppe und $\emptyset \neq U \subset G$. Dann sind äquivalent:

I U Untergruppe
II (i) $\forall a, b \in U : a\,b \in U$
(Schreibweise: $UU \subseteq U$)
(ii) $\forall a \in U \ \exists b \in U : b\,a = e$.
III $\forall a, b \in U : a\,b^{-1} \in U$.
(Schreibweise: $UU^{-1} \subseteq U$)

Beweis:
I $\Rightarrow$ II: per Definition (1.6);

II $\Rightarrow$ III:
$\forall b \in U \ \exists b^{-1} \in U$ wegen (ii) und der Eindeutigkeit des Inversen in G, dann folgt die Behauptung mittels (i);

III $\Rightarrow$ I:
Für $a = b \in U$ $(\neq \emptyset!)$ ist $aa^{-1} = e \in U$. Für $e, b \in U$ ist $eb^{-1} = b^{-1} \in U$. Für $a, b \in U$ ist $a, b^{-1} \in U$ und damit $a\,(b^{-1})^{-1} = ab \in U$. Das Assoziativgesetz gilt in U wegen $U \subseteq G$.

□

Bemerkung:
Der Durchschnitt von Untergruppen einer Gruppe G ist wieder eine Untergruppe von G. Zu $\emptyset \subset M \subseteq G$ existiert folglich eine kleinste Untergruppe U von G mit $M \subseteq G$, nämlich der Durchschnitt von allen Untergruppen von G, die M enthalten. Diese heißt das Erzeugnis $< M >$ von M in G. Speziell heißt G endlich erzeugt, falls eine endliche Teilmenge M von G mit $G =< M >$ existiert.
Offenbar gilt:

(i) $M \subseteq < M >$, $< M >$ ist Teilmenge jeder Untergruppe, die M enthält.
(ii) Definiere $< \emptyset >=< e >$.
(iii) $< M >= M \Leftrightarrow M$ Untergruppe.

Beispiel:
$G = (\mathbb{Z}, +) =< 1 >$;
$(\mathbb{Q}[t], +)$ ist dagegen nicht endlich erzeugt.

2.13. Lemma

Es sei G eine Gruppe und $\emptyset \neq M \subseteq G$. Dann besteht $< M >$ aus allen endlichen Produkten von Elementen aus $M \cup M^{-1}$ ($M^{-1} := \{a^{-1} \mid a \in M\}$).

Beweis:
Als Untergruppe enthält $< M >$ alle Elemente aus $M \cup M^{-1}$ und damit auch alle endlichen Produkten von solchen Elementen, da $< M >$ bzgl. der Produktbildung abgeschlossen ist. Es bleibt zu zeigen, daß die Menge aller solchen Produkte bereits eine Untergruppe bildet.
Die Assoziativität überträgt sich von G.
Die Abgeschlossenheit ist klar, $e = aa^{-1}$ für $a \in M$, und zu $a_1, \ldots, a_n \in M \cup M^{-1}$ ist

$$(a_1 \cdot \ldots \cdot a_n)^{-1} = a_n^{-1} \cdot \ldots \cdot a_1^{-1}$$

mit $a_1^{-1}, \ldots, a_n^{-1} \in M \cup M^{-1}$.

□

Problem:
Bestimme kleinstes Erzeugendensystem für eine Gruppe. Ein solches existiert i.a. nicht, falls es existiert, ist es nicht eindeutig.

Beispiel:

$$\begin{aligned} (\mathbb{Z}/3\mathbb{Z}, +) &= < 1 + 3\mathbb{Z} > \\ &= < 2 + 3\mathbb{Z} >, \end{aligned}$$

$$\begin{aligned} (\mathbb{Z}, +) &= < 1 > \\ &= < -1 > . \end{aligned}$$

Im folgenden sei G eine Gruppe und U eine Untergruppe von G. Dann wird mittels

$$a \sim b \quad :\Leftrightarrow \quad ab^{-1} \in U$$

auf G eine Äquvalenzrelation erklärt. Es gilt nämlich:

(i) $a \sim a$ wegen $aa^{-1} = e \ \in U$ gilt für alle $a \in G$.

(ii)

$$\begin{aligned} a \sim b &\Leftrightarrow ab^{-1} \in U \\ &\Rightarrow (ab^{-1})^{-1} \in U \\ &\Rightarrow ba^{-1} \in U \\ &\Leftrightarrow b \sim a \qquad \forall a, b \in G. \end{aligned}$$

(iii)

$$\begin{aligned} a \sim b \wedge b \sim c &\Leftrightarrow ab^{-1} \in U \wedge bc^{-1} \in U \\ &\Rightarrow (ab^{-1})(bc^{-1}) = ac^{-1} \in U \\ &\Leftrightarrow a \sim c \qquad \forall a, b, c \in G. \end{aligned}$$

Zu $a \in G$ ist die zugehörige Äquivalenzklasse $Ua := \{ua | u \in U\}$, denn es gilt

$$ua \in Ua \ \Rightarrow \ a(ua)^{-1} = a(a^{-1}u) = u \ \in U.$$

Ua heißt Rechtsnebenklasse von a bzgl. U.
(Entsprechend:

$$a \sim_l b \ \Leftrightarrow \ \exists u \in U \ : \ a^{-1}b = u \text{ oder } b = au$$

führt zu Linksnebenklassen aU.)

Die Mächtigkeit (Anzahl der Elemente) einer Nebenklasse ist gleich der Mächtigkeit (Elementzahl, Ordnung) von U. Bezeichnung: $|U| = (U : 1)$.
Denn für $a \in G$ ist

$$\varphi_a \ : \ U \to Ua \ : \ u \mapsto ua$$

(analog: $\psi_a \ : \ U \to aU \ : \ u \mapsto au$)
bijektiv. Die Surjektivität ist klar, die Injektivität folgt aus den Kürzungsregeln für G:

$$\begin{aligned} ua = \tilde{u}a &\Rightarrow u = \tilde{u}, \\ au = a\tilde{u} &\Rightarrow u = \tilde{u}. \end{aligned}$$

(Folgerung: $Ua = U \ \Leftrightarrow \ a \in U$.)

Bemerkung:

Die Mengen der Linksnebenklassen und die der Rechtsnebenklassen von U in G sind gleichmächtig. Dazu sei $V \subseteq G$ ein Vertretersystem für die Linksnebenklassen von U in G:

$$G = \dot{\bigcup_{a \in V}} aU \ .$$

Wir werden zeigen, dass dann auch

$$G = \dot{\bigcup_{a \in V}} Ua^{-1}$$

gilt. Zunächst ist die Vereinigung der Mengen auf der rechten Seite disjunkt wegen

$$\begin{aligned} aU = bU &\Leftrightarrow b^{-1}aU = U \\ &\Leftrightarrow b^{-1}a \in U \\ &\Leftrightarrow U = Ub^{-1}a \\ &\Leftrightarrow Ua^{-1} = Ub^{-1} \ . \end{aligned}$$

Zudem ist die rechte Seite naturgemäß in der linken Seite enthalten. Ist ferner $g \in G$ beliebig, so liegt g^{-1} in einer Linksnebenklasse aU für ein passendes $a \in V$. Es folgt $g^{-1} = au$ für ein $u \in U$, also $g = u^{-1}a^{-1} \in Ua^{-1}$.
Die Mächtigkeit (Elementzahl) der Menge der verschiedenen Rechtsnebenklassen (Linksnebenklassen) von U in G heißt Index von U in G.
Bezeichnung: $(G : U)$.
Da die Gruppe G disjunkte Vereinigung der Äquivalenzklassen Ua ist, haben wir den folgenden Satz bewiesen:

2.14. Satz (Lagrange)

$$\begin{array}{ccc} (G:1) & = & (G:U)\,(U:1) \\ \| & & \\ \sharp G & & \\ \| & & \\ |G| & & \end{array}$$

2.15. Satz

Es sei G eine Gruppe mit Untergruppen $U \subseteq V$. Dann gilt:

$$(G : U) = (G : V)\,(V : U).$$

Beweis:

Für $|G| < \infty$ ist dies direkte Folge aus (1.9):

$$\begin{aligned}(G:U) &= \frac{(G:1)}{(U:1)} = \frac{(G:V)(V:1)}{(U:1)} \\ &= \frac{(G:V)(V:U)(U:1)}{(U:1)} = (G:V)(V:U).\end{aligned}$$

Sonst seien

$$G = \dot{\bigcup_{\alpha\in I}} a_\alpha V, \quad V = \dot{\bigcup_{\beta\in J}} b_\beta U$$

(disjunkte Zerlegungen in Linksnebenklassen). Es folgt dann, daß

$$G = \bigcup_{\substack{\alpha\in I\\ \beta\in J}} a_\alpha\, b_\beta\, U$$

Zerlegung von G in Linksnebenklassen nach U ist. Es bleibt zu zeigen, daß diese Zerlegung disjunkt ist.
Für

$$\begin{array}{ccc} a_{\tilde\alpha}\, b_{\tilde\beta}\, U & = & a_\alpha\, b_\beta\, U \\ \| & & \| \\ \{a_{\tilde\alpha}\, b_{\tilde\beta}\, \tilde u \mid \tilde u \in U\} & & \{a_\alpha\, b_\beta\, u \mid u \in U\} \end{array}$$

ist

$$a_{\tilde\alpha} \underbrace{b_{\tilde\beta}\, U}_{\subseteq V} = a_\alpha \underbrace{b_\beta\, U}_{\subseteq V} \quad \Rightarrow \quad a_{\tilde\alpha} = a_\alpha$$

und weiter

$$b_{\tilde\beta}\, U = b_\beta\, U \quad \Rightarrow \quad b_{\tilde\beta} = b_\beta.$$

Also gilt:

$$(G:V) = |I|, \quad (G:U) = |I|\,|J|, \quad (V:U) = |J|.$$

□

Die in gewisser Hinsicht einfachsten Gruppen sind die, die von einem einzigen Element erzeugt werden:

$$G = \{a^k \mid k \in \mathbb{Z}\}.$$

2.16. Definition

Eine Gruppe G heißt zyklisch, falls sie von einem Element erzeugt wird.

2.17. Satz

Es sei $G =< a >$ eine zyklische Gruppe. Für $|G| = (G:1) = \infty$ ist dann $G \cong \mathbb{Z}$, für $|G| = (G:1) = m < \infty$ ist $G \cong (\mathbb{Z}/m\mathbb{Z}, +)$.
(Triviale Bemerkung: G zyklisch $\Rightarrow$ G abelsch)

Beweis:
Im Fall $|G| = 1$ besteht G nur aus dem Einselement e. Die Abbildung

$$G \to (\mathbb{Z}/\mathbb{Z}, +) : e \mapsto \mathbb{Z}$$

ist offensichtlich ein Gruppenisomorphismus (vgl. Lineare Algebra I). Im folgenden setzen wir $|G| > 1$ voraus. Wir betrachten den surjektiven Homomorphismus

$$\varphi : (\mathbb{Z}, +) \to G \ : \ k \mapsto a^k.$$

Ist φ nicht injektiv, so existieren $m, n \in \mathbb{Z}$, o.B.d.A. $m > n$, mit $a^m = a^n$ bzw. $a^{m-n} = e$. Also existiert eine kleinste Zahl $f \in \mathbb{N}$ (!) mit $a^f = e$. Wir zeigen: $G = \{e, a, \ldots, a^{f-1}\}$. Ist $m \in \mathbb{Z}$ beliebig, so liefert Division mit Rest $m = Q(m, f)f + R(m, f)$ mit $0 \leq R(m, f) < f$.
Es folgt

$$\begin{aligned} a^m &= a^{Q(m,f)f+R(m,f)} = (a^f)^{Q(m,f)}a^{R(m,f)} \\ &= a^{R(m,f)} \in \{a, a, \ldots, a^{f-1}\}. \end{aligned}$$

Die Elemente $e, a, \ldots, a^{f-1}$ sind aber wegen der Minimalität von f paarweise verschieden!
Ist φ dagegen injektiv, so sind alle Potenzen a^m ($m \in \mathbb{Z}$) verschieden, es ist also $|G| = \infty$.
Die behaupteten Isomorphien folgen nun aus dem Isomorphiesatz für abelsche Gruppen (vgl. Lineare Algebra I), wenn man $\ker\varphi = f\mathbb{Z}$ für φ nicht injektiv bzw. $\ker\varphi = \{0\}$ für φ injektiv beachtet.

□

Bemerkungen:

(i) Jede Untergruppe U einer zyklischen Gruppe G ist zyklisch. Dazu betrachte man für
$G =< a >$ und $U \neq< e >$ die kleinste Potenz a^k ($k \in \mathbb{N}$), die in U enthalten ist.
Für $U =< e >$ setze $k = 0$. Offenbar ist $U =< a^k >$.

(ii) $(\mathbb{Z}, +) \cong (2\mathbb{Z}, +)$.

We list some consequences of Lagrange's Theorem for exponents and orders of elements which will be used later.

2.18. Definition

Let G be an arbitrary group and g an element of G. A natural number m is called **exponent** of g if g^m equals the unit element e of G.
Examples If G is the Klein Four Group then 2 is an exponent of every $g \in G$. If G is finite then $|G|$ is an exponent for every $g \in G$. For $G = (\mathbb{Z}, +)$ the non-zero elements of G have no exponents whereas $0 \in G$ has every natural number as exponent. For $G = \mathbb{Q}^\times := (\mathbb{Q} \setminus \{0\}, \times)$ the element -1 has exponent 2 and the elements g with absolute value greater than 1 (similarly less than 1) have no exponents.

If an element $g \in G$ has an exponent m then it is quite natural to ask for the minimal exponent of g. As we saw in the previous examples the

elements g of the Klein Four Group have minimal exponents either 1 ($g = e$) or 2, whereas the elements g of the cyclic group of order 4 can have minimal exponents 1,2,4. We note that the set of exponents of an element g is a subset of $\mathbb{N}$ and therefore contains a (unique) minimal element if it is not empty.

2.19. Definition

Let G be an arbitrary group and g an element of G. If g has exponents $m \in \mathbb{N}$ then there exists a smallest exponent, the so-called **order** $\mathrm{ord}(g)$ of g. In that case we say that g is of finite order (otherwise infinite).
Remarks As a consequence of Lagrange's Theorem the order of an element g of a group G divides the group order $|G|$ in case G is finite. We observe that $\mathrm{ord}(e) = 1$.

It will turn out useful to establish a few properties of the order function for group elements, especially when discussing finite abelian groups.

2.20. Lemma

Let g be an element of a group G of finite order $m = \mathrm{ord}(g)$. Then we have

$$\mathrm{ord}(g^k) = \mathrm{ord}(g)/\gcd(k, m)$$

for every $k \in \mathbb{Z}$.
Proof We set $c := \gcd(k, m)$ and need to show that $d := m/c$ is the smallest exponent for m^k. Clearly, d is an exponent for m^k because of $(g^k)^d = g^{kd} = g^{mk/c} = (g^m)^{k/c} = e^{k/c} = e$. On the other hand, let f be any exponent for g^k. Because of $e = (g^k)^f = g^{kf}$ the element kf must be a multiple of m, say $kf = lm$ for an appropriate $l \in \mathbb{Z}$. This induces $\frac{k}{c}f = l\frac{m}{c}$ and $\frac{k}{c}$, $\frac{m}{c}$ being coprime we obtain indeed that $\frac{m}{c}$ divides f.
□
We note that we did not impose any conditions on the group G in the previous lemma. If we want to establish a relation between the orders of two group elements and the order of their product then we need to assume that these elements commute. The latter will become clear from the proof and the remarks thereafter.

2.21. Lemma

Let g, h be commuting elements of a group G with coprime orders $m = \mathrm{ord}(g)$ and $n = \mathrm{ord}(h)$. Then the element $gh = hg$ has order mn.
Proof Because of $(gh)^{mn} = g^{mn}h^{mn} = (g^m)^n(h^n)^m = e$ the product mn is an exponent of gh. On the other hand, if f is any exponent of gh we put $c = \gcd(f, m)$, $d := \gcd(f, n)$ and get $e = ((gh)^f)^{m/c} = g^{m(f/c)}h^{fm/c} = h^{fm/c}$, respectively, $e = ((gh)^f)^{n/c} = g^{fn/c}h^{n(f/c)} =$

$g^{fn/c}$. From the first equation we conclude that n divides $f(m/c)$ and since n and m were coprime this yields $n \mid f$. The second equation yields $m \mid f$ analogously and again, n and m being coprime we obtain that mn divides f. Hence, mn is indeed a minimal exponent for gh.
□
If the elements g, h do not commute then the order of their product cannot be obtained so easily. We observe that in the symmetric group $\mathcal{S}_3$ the product of two elements of order 2 has order 3 again (see first page of this chapter). It can even happen that the product of two elements of finite order has an infinite order. To see this we consider $\mathbb{R}$ as affine line and let G be the group of bijective affine mappings from $\mathbb{R}$ onto itself. It contains the 2 reflections $g(x) = 2 - x$ and $h(x) = -x$ of order 2 each. Then $gh \neq hg$, $hg(x) = x + 2$ and $gh(x) = x - 2$ are both translations, hence their order is infinite.
Even the case in which g, h commute but their orders are not coprime is not immediately deducible from the preceding lemmata. We note that the likely assumption $\mathrm{ord}(gh) = \mathrm{lcm}(\mathrm{ord}(g)\,,\, \mathrm{ord}(h))$ is terribly false as the example $h = g^{-1}$ demonstrates.

2.22. Lemma

Let g, h be commuting elements of a group G with orders $m = \mathrm{ord}(g)$ and $n = \mathrm{ord}(h)$. The order of the element $gh = hg$ divides $d := \mathrm{lcm}(m, n)$. There exist exponents u, v such that the element $g^u h^v$ has order d.
Proof As in the proof of the previous lemma one immediately sees that d is an exponent of gh. To show the last statement we consider the prime number decompositions of m, n, respectively. We recall that every natural number can be written as a formal infinite product over all prime numbers in which only finitely many exponents are non-zero. So we assume that

$$m = \prod_{p \in \mathcal{P}} p^{m_p}\ ,\ n = \prod_{p \in \mathcal{P}} p^{n_p}$$

and set

$$u := \prod_{\substack{p \in \mathcal{P} \\ m_p < n_p}} p^{m_p}\ ,\ v := \prod_{\substack{p \in \mathcal{P} \\ n_p \leq m_p}} p^{n_p}\ .$$

Then the orders

$$\mathrm{ord}(g^u) := \prod_{\substack{p \in \mathcal{P} \\ m_p \geq n_p}} p^{m_p}$$

and

$$\mathrm{ord}(h^v) := \prod_{\substack{p \in \mathcal{P} \\ m_p < n_p}} p^{n_p}$$

are mutually prime and the previous lemma yields

$$\operatorname{ord}(g^u h^v) := \prod_{\substack{p\in\mathcal{P}\\ m_p\geq n_p}} p^{m_p} \prod_{\substack{p\in\mathcal{P}\\ m_p<n_p}} p^{n_p} = \operatorname{lcm}(m,n) \ .$$

□

Example Let g, h be commuting elements of a group G with $m := \operatorname{ord}(g) = 540$, $n := \operatorname{ord}(h) = 1008$, respectively. We easily calculate $m = 2^2 3^3 5$, $n = 2^4 3^2 7$, $u = 2^2$, $v = 3^2$, hence we get

$$\operatorname{ord}(g^4) = 135,\ \operatorname{ord}(h^9) = 112,\ \operatorname{ord}(g^4 h^9) = 15120 \ .$$

Folgerungen:
Es sei $G =< a >$ eine zyklische Gruppe der Ordnung k.

(i) Es ist $G =< a^m >$ dann und nur dann, wenn $\operatorname{ggT}(k,\, m) = 1$ ist.

(ii) G besitzt genau $\varphi(k)$ erzeugenden Elemente. Hierbei bezeichnet φ die Eulersche Funktion, die für $k \in \mathbb{N}$ die Anzahl der zu k teilerfremden Zahlen innerhalb $\{1, 2, \ldots, k\}$ angibt. Man beachte:

k	1	2	3	4	5	6
$\varphi(k)$	1	1	2	2	4	2

sowie $\varphi(p) = p - 1$ für Primzahlen p.

2.23. Satz (Kennzeichnungssatz für zyklische Gruppen)

Es sei G eine endliche Gruppe der Ordnung n. Dann gilt:

$$G \text{ zyklisch } \Leftrightarrow \forall\, d \mid n\ \dot{\exists}\, U < G : |U| = d\,.$$

Beweis:
Es sei $G = \langle g \rangle$ mit $\operatorname{ord}(g) = n$. Für $d \mid n$ setze $h = g^{n/d}$ (mit $\operatorname{ord}(h) = d$) und $U = \langle h \rangle$. Um nach der Existenz auch die Eindeutigkeit zu zeigen, nehmen wir an, dass V eine weitere Untergruppe von G von der Ordnung d ist. Für beliebiges $x \in V$ ist dann $e := \operatorname{ord}(x)$ ein Teiler von d. Folglich ist x von der Form $(h^{d/e})^k$ mit $\gcd(k, e) = 1$, also $x \in U$. Damit gilt $V \subseteq U$ und wegen

$$d = (G : V) = (G : U)(U : V) = d(U : V)$$

demnach $(U : V) = 1$, also $U = V$.

" $\Leftarrow$ " Der Beweis erfolgt mittels Induktion nach n. Für $n = 1, 2, 3$ wurde die Aussage bereits verifiziert. Wir schließen von $1, \ldots, n-1$ auf n (für $n \geq 4$). Dabei unterscheiden wir 2 Fälle.

(α) Es ist $(G : 1) = u \cdot v$ mit $u, v \in \mathbb{Z}^{\geq 2}$ und $\gcd(u, v) = 1$.
Hierzu existieren (eindeutige!) Untergruppen U, V von G mit $|U| = u$

und $|V| = v$. Diese sind wegen der Eindeutigkeit unter allen inneren Automorphismen invariant, also Normalteiler. Wir wollen zeigen, dass U (bzw. V) zu jedem Teiler d von u (bzw. d von v) genau eine Untergruppe W der Ordnung d besitzt. Nach Voraussetzung existiert genau eine solche Untergruppe W von G. Wir haben $W < U$ (bzw. $W < V$) zu zeigen. Wir führen den Nachweis lediglich für U. Da $U \triangleleft G$ ist, ist WU Untergruppe von G, die U als Normalteiler enthält. Nach dem 1. Isomorphiesatz folgt $WU/U \cong W/U \cap W$. Dabei ist $(W : U \cap W)$ ein Teiler e von d, der folglich u teilt. Wegen $v = (G : U) = (G : WU)(WU : U) = (G : WU)e$ und $\gcd(u, v) = 1$ muss notwendig $e = 1$ und damit $WU = U$, also $W \subseteq U$ gelten. Demnach sind die Voraussetzungen für G auch für U, V erfüllt. Nach Induktionsvoraussetzung sind $U = \langle x \rangle$, $V = \langle y \rangle$ zyklisch. Wir bilden den "Kommutator" $x^{-1}y^{-1}xy$. Wegen $V \triangleleft G$ liegt er in V, wegen $U \triangleleft G$ auch in U. Da die Ordnungen u von U und v von V teilerfremd sind, gilt $U \cap V = \{e\}$, also auch $x^{-1}y^{-1}xy = e$ bzw. $xy = yx$. Daher kommutieren x, y, es folgt $\mathrm{ord}(xy) = \mathrm{ord}(x)\mathrm{ord}(y) = uv = n$. Hiernach ist $G = \langle xy \rangle$ zyklisch.

(β) Es ist $(G : 1) = p^f$ mit $p \in \mathbb{P}$ und $f \in \mathbb{N}$. In G wählen wir g mit $\mathrm{ord}(g) = p^k$ und k maximal. Ist nun $h \in G$ beliebig mit $\mathrm{ord}(h) = p^l$ $(0 \leq l \leq k)$, so erzeugt h eine zyklische Gruppe der Ordnung p^l. Diese stimmt nach Voraussetzung mit $\langle g^{p^{k-l}} \rangle$ überein. Also ist $h \in \langle g \rangle$ und somit $G = \langle g \rangle$.

□

Bemerkung:
Ist $G = \langle g \rangle$ eine zyklische Gruppe der Ordnung d, so existieren in G gerade $\varphi(d)$ Erzeuger, nämlich g^i mit $1 \leq i < d$ und $\gcd(i, d) = 1$. Der vorangehende Satz liefert somit für $n \in \mathbb{N}$ die Formel:

$$n = \sum_{d|n} \varphi(d)\,.$$

Bemerkung:
Es sei $G =< a >$ unendlich. Dann gilt

$$< a^k >=< a^l > \quad (k, l \in \mathbb{Z})$$

genau dann, wenn $k = \pm l$ ist. Speziell besitzt G genau die beiden Erzeuger a, a^{-1}.

Beweis:
Es existieren $\mu, \nu \in \mathbb{Z}$ mit

$$a^k = a^{l\,\mu}, \quad a^l = a^{k\,\nu},$$

d.h.

$$a^k = a^{k\,\mu\,\nu} \quad \Rightarrow \quad \mu\,\nu = 1 \quad \Rightarrow \quad k = \pm l.$$

□

Beispiel:
Eine wichtige Gruppe mit 2 Erzeugern ist die Diedergruppe:

$$G =< a,\, b \mid a^2 = e,\; b^n = e,\; aba = b^{-1} > \quad (n \in \mathbb{N},\; \sharp G = 2n).$$

Es sei $\mathbb{R}^2$ die reelle Ebene, $n \in \mathbb{N}$.

$$d \,:\, \mathbb{R}^2 \to \mathbb{R}^2$$

bezeichne die Drehung um den Ursprung um den Winkel $\frac{2\pi}{n}$, s die Spiegelung an der y-Achse. Setze $D_n :=< d,\, s >$.
Matrixschreibweise:

$$d = \begin{pmatrix} \cos\frac{2\pi}{n} & -\sin\frac{2\pi}{n} \\ \sin\frac{2\pi}{n} & \cos\frac{2\pi}{n} \end{pmatrix}, \quad s = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}.$$

Relationen zwischen den Erzeugern:

$$d^n = e = \mathrm{id},\; s^2 = e,\; dsd = s \text{ bzw. } sds = d^{-1}.$$

Also läßt sich jedes Element von D_n (beachte (1.8)) in der Form $s^i d^j$ mit $0 \le i \le 1,\; 0 \le j < n$ darstellen,

$$D_n = \{e, d, d^2, \ldots, d^{n-1}, s, sd, \ldots, sd^{n-1}\}.$$

Diese Elemente sind alle verschieden ($d^k = sd^l$ impliziert $d^{k-l} = s$, was unmöglich ist), also gilt $(D_n : 1) = 2n$.

Es sei $x \in G$ fest gewählt. Man betrachte die Abbildung

$$\varphi_x \,:\, G \to G \,:\, a \mapsto xax^{-1}.$$

Diese ist ein Homomorphismus:

$$(xax^{-1})\,(xbx^{-1}) = xabx^{-1}.$$

Injektivität von φ_x :

$$xax^{-1} = xbx^{-1} \quad \Rightarrow \quad a = b.$$

Surjektivität von φ_x: (Einziges) Urbild von $b \in G$ ist $x^{-1}bx$.
Also ist φ_x ein Automorphismus von G, sogenannter innerer Automorphismus, mit Umkehrabbildung

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

Die Automorphismen von G bilden (bzgl. Hintereinanderausführung) eine Gruppe $\mathrm{Aut}\,(G)$. Die inneren Automorphismen bilden hiervon eine Untergruppe $I\,(G)$ gemäß:

φ_x, φ_y innere Automorphismen, dann auch

$$\varphi_x\,(\varphi_y)^{-1} = \varphi_{xy^{-1}}.$$

$I\,(G)$ ist trivial, falls G abelsch ist.

Für Untergruppen U von G gilt i.a. nicht $xUx^{-1} = U$ für alle $x \in G$ (Gegenbeispiel: 2-elementige Untergruppen von $\mathfrak{S}_3$). Untergruppen, die unter allen inneren Automorphismen invariant sind, spielen eine ausgezeichnete Rolle.

2.24. Definition

Eine Untergruppe U von G heißt Normalteiler von G; falls $xUx^{-1} = U$ für alle $x \in G$ ist.

Bemerkungen:

(i) Es genügt in (1.15), $xUx^{-1} \subseteq U$ zu fordern.
(ii) $xUx^{-1} = U \quad \Leftrightarrow \quad xU = Ux$.
(iii) Es sei $\varphi : G \to H$ ein Gruppenhomomorphismus. Dann ist

$$\ker \varphi := \{x \in G \mid \varphi(x) = e_H\}$$

Normalteiler in G. Ist nämlich $a \in G$ beliebig, so gilt

$$\begin{aligned} \varphi(a(\ker \varphi)a^{-1}) &= \varphi(a)\varphi(\ker \varphi)\varphi(a^{-1}) \\ &= \varphi(a)e_H\varphi(a^{-1}) \\ &= \varphi(a)\varphi(a^{-1}) \\ &= \varphi(aa^{-1}) \\ &= \varphi(e_G) \\ &= e_H, \end{aligned}$$

also $a \ker \varphi a^{-1} \subseteq \ker \varphi$.
(iv) Ist U Untergruppe von G mit $(G : U) = 2$, so ist U Normalteiler. Es ist

$$G = U \dot\cup xU = U \dot\cup Ux \text{ für } x \in G \backslash U,$$

also gilt $xU = Ux$ für alle $x \in G$.
(v) $< e >$, G sind stets Normalteiler von G. G heißt einfach, falls es die einzigen sind.
(vi) Es seien $U \subseteq V \subseteq W$ Untergruppen von G; ist dann U Normalteiler in V, so ist U i.a. nicht Normalteiler in W.
(vii) In abelschen Gruppen ist jede Untergruppe Normalteiler.

Schreibweise: $U < G$ für "Untergruppe", $U \lhd G$ für "Normalteiler".

Gruppentypen (bis auf Isomorphie)

$\sharp G$	G
1	$\{e\}$
2	$< x >$ mit $x^2 = e$
3	$< x >$ mit $x^3 = e$
4	$< x >$ mit $x^4 = e$ sowie D_2.
	In D_2 haben alle Elemente die Ordnung 2 .
	D_2 ist die sog. Kleinsche Vierergruppe $\{e, a, b, c\} mit$
	$a^2 = b^2 = c^2 = e,\ ab = c,\ ac = b,\ bc = a,$
	$D_2 \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$
5	$< x >$ mit $x^5 = e$
6	$< x >$ mit $x^6 = e$ sowie
	$D_3 = \{a^\nu b^\mu \mid \nu \in \{0,\ 1\}, \mu \in \{0,\ 1,\ 2\},\ a^2 = b^3 = e,\ aba = b^{-1}\}$,
	D_3 ist die kleinste nicht kommutative Gruppe

Beispiel: Gruppe mit 6 Elementen ist auch

$\mathfrak{S}_3$:

$$e = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} \quad b = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \quad b^2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$
$$a = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \quad ba = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \quad b^2 a = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix},$$

mit $a^2 = e = b^3$.

Anzahl der Elemente vorgegebener Ordnung			
ord	1	2	3
Elementeanzahl	1	3	2
Anzahl der Untergruppen	1	3	1 (ist Normalteiler).

Offenbar ist $\mathfrak{S}_3$ zu D_3 isomorph.

Beispiel:
G Gruppe, Aut (G) ist Gruppe mit Untergruppe $I(G)$.
Wir zeigen: $\forall \varphi \in \text{Aut}\,(G)\ :\ \varphi\, I\,(G)\, \varphi^{-1} \subseteq I\,(G)$ bzw.
$\forall \varphi_x \in I\,(G)\ :\ \varphi\, \varphi_x\, \varphi^{-1} \in I\,(G)$.

Sei $y \in G$ beliebig:

$$\begin{aligned} \varphi\, \varphi_x\, \varphi^{-1}(y) &= \varphi\, \varphi_x\, (\varphi^{-1}(y)) \\ &= \varphi\, (x\, \varphi^{-1}(y)\, x^{-1}) \\ &= \varphi\, (x)\, \varphi\, (\varphi^{-1}(y))\, \varphi\, (x^{-1}) \\ &= \varphi\, (x)\, y\, \varphi\, (x)^{-1} \\ &= \varphi_{\varphi\,(x)}(y), \text{ also ist } \varphi\varphi_x\varphi^{-1} \text{ innerer Automorphismus.} \end{aligned}$$

2.25. Hilfssatz

(i) Der Durchschnitt von Normalteilern von G ist Normalteiler von G,

(ii) $N_1 \lhd G,\ N_2 < G \ \Rightarrow\ N_1 N_2 < G$,
$N_1,\ N_2$ Normalteiler von $G \ \Rightarrow\ N_1 N_2 \lhd G$,

(iii) $\varphi : G \to H$ Homomorphismus,

$$\begin{aligned} V < H &\ \Rightarrow\ \varphi^{-1}(V) < G, \\ V \lhd H &\ \Rightarrow\ \varphi^{-1}(V) \lhd G, \end{aligned}$$

(iv) $\varphi : G \to H$ Epimorphismus,

$$\begin{aligned} U < G &\ \Rightarrow\ \varphi(U) < H, \\ U \lhd G &\ \Rightarrow\ \varphi(U) \lhd H. \end{aligned}$$

Beweis:

(i) $\{N_i\}_{i\in I}$ sei eine Familie von Normalteilern von $G \Rightarrow\ N := \bigcap_{i\in I} N_i$ ist Untergruppe, ferner ist für $x \in G$ und $y \in N$

$$xyx^{-1} \in N_i\ (i \in I) \quad \Rightarrow \quad xyx^{-1} \in N,$$

also $xNx^{-1} \subseteq N$.

(ii) Normalteilereigenschaft:

$$xN_1N_2x^{-1} = xN_1x^{-1}xN_2x^{-1} = N_1N_2\ \forall x \in G,$$

$N_1N_2 \neq \emptyset$ wegen $e \cdot e \in N_1N_2$, ferner ist

$$\begin{aligned} (N_1N_2)\,(N_1N_2)^{-1} &= (N_1N_2)\,N_2^{-1}N_1^{-1} \subseteq N_1N_2^{-1}N_1 \\ &= N_1N_1^{-1}N_2 \subseteq N_1N_2 \text{ (beachte: } N_1^{-1} = N_1,\ N_2^{-1} = N_2 \text{ und } N_1 \lhd G) \end{aligned}$$

$\Rightarrow \quad N_1N_2$ Untergruppe.

(iii) $\varphi^{-1}(V)$ ist Untergruppe:
Trivialerweise ist $e_G \in \varphi^{-1}(V)$. Seien $a,\ b \in \varphi^{-1}(V)\ \Rightarrow$

$$\begin{aligned} \varphi(a),\ \varphi(b) \in V \ &\Rightarrow\ \varphi(a)\,(\varphi(b))^{-1} \in V \\ &\qquad\quad \| \\ &\qquad\quad \varphi(a)\,\varphi(b^{-1}) = \varphi(ab^{-1}). \end{aligned}$$

Sei $x \in G$:

$$\varphi(x\,\varphi^{-1}(V)\,x^{-1}) = \varphi(x)\,V\,\varphi(x)^{-1} = V,$$

also ist

$$x\,\varphi^{-1}(V)\,x^{-1} \subseteq \varphi^{-1}(V).$$

(iv) $\varphi(U)$ ist Untergruppe:
$\varphi(e_G) = e_H$. $(e_G = e_Ge_G\ \Rightarrow\ \varphi(e_G) = \varphi(e_G)\,\varphi(e_G))$.
Seien $\varphi(a),\ \varphi(b) \in \varphi(U)\ \Rightarrow$

$$\varphi(a)\,\varphi(b)^{-1} = \varphi(a)\,\varphi(b^{-1}) = \varphi(ab^{-1})\ \in \varphi(U).$$

Zu $y \in H$ existiert $x \in G$ mit $\varphi(x) = y$. Damit wird

$$\varphi(x)\,\varphi(U)\,\varphi(x)^{-1} = \varphi(xUx^{-1}) = \varphi(U).$$

□

2.26. Satz

Es sei G eine Gruppe mit Normalteiler N. Dann läßt sich

$$G/N := \{gN \mid g \in G\}$$

mittels der Verknüpfung

$$(gN)(hN) = ghN$$

zu einer Gruppe machen, der sogenannten Faktorgruppe. Ihre Ordnung ist $(G/N : 1) = (G : N)$.

Bezeichnung: $\bar{G} = G/N$ mit Elementen $\bar{g} = gN$.

Beweis:
N Normalteiler $\Rightarrow$

$$\begin{aligned}(gN)(hN) &= g(Nh)N \\ &= g(hN)N \\ &= gh(NN) \\ &= ghN,\end{aligned}$$

also ist die Verknüpfung wohldefiniert; das Assoziativgesetz überträgt sich von G; Einselement ist $N = eN$; Inverses zu gN ist $g^{-1}N$. Die Elemente von G/N sind gerade die Linksnebenklassen von N in G.

□

Bemerkung:

(i) Unter den Voraussetzungen von (1.17) ist

$$p : G \to G/N : g \mapsto gN$$

ein Gruppenepimorphismus mit $\ker(p) = N$, der sogenannte kanonische Epimorphismus.

Beweis:
p ist Homomorphismus gemäß Definition der Verknüpfung, p surjektiv ist klar,

$$\text{schließlich ist } \ker(p) = \{g \in G \mid \underset{\Updownarrow}{gN = N}\} = N.$$
$$g \in N$$

(ii) $\emptyset \neq U \subseteq G$ ist dann und nur dann Normalteiler von G, falls U Kern eines Gruppenhomomorphismus $G \to H$ ist.
(

$$U \lhd G \;\Rightarrow\; U = \ker(p) \text{ für } p : G \to G/N;$$

$U = \ker(\varphi)$ für Homomorphismus $\varphi : G \to H$ ist stets Normalteiler in G.)

(iii) Gruppenhomomorphismen von einfachen Gruppen sind trivial oder injektiv. ($\ker(\varphi) \lhd G$; $\ker(\varphi) = G$ ($\Rightarrow$ φ trivial) oder $\ker(\varphi) = e$ ($\Rightarrow$ φ injektiv).)

(iv) Es besteht die exakte Sequenz:

$$e \to N \to G \to G/N \to 1.$$

Beispiel:
In der Topologie und Homologie spielen exakte Sequenzen eine wichtige Rolle. Eine Folge (Sequenz) von Gruppenhomomorphismen

$$G_1 \xrightarrow{\varphi_1} G_2 \xrightarrow{\varphi_2} G_3 \xrightarrow{\varphi_3} \ldots \xrightarrow{\varphi_{n-1}} G_n$$

heißt exakt, falls $\operatorname{Im} \varphi_i = \ker \varphi_{i+1}$ $(1 \leq i \leq n-2)$ ist. Ist Speziell $N \lhd G$, so ist

$$\{e\} \longrightarrow N \xrightarrow{\iota} G \xrightarrow{p} G/N \longrightarrow \{e\}$$

exakt, falls

$$\iota : N \to G : x \mapsto x$$

($\iota = \mathrm{id}_G \mid_N$) die Insertion (Einbettung) von N in G ist. Eine Folge von Gruppenhomomorphismen

$$e \xrightarrow{\iota} G_1 \xrightarrow{\varphi_1} G_2 \xrightarrow{\varphi_2} G_3 \xrightarrow{\varphi_3} e$$

ist genau dann exakt, falls φ_1 injektiv, $\varphi_1(G) = \ker(\varphi_2)$ und φ_2 surjektiv ist.

2.27. Homomorphiesatz (für Gruppen)

Es sei $\varphi : G \to H$ ein (Gruppen)homomorphismus. Dann gilt:

$$G/\ker(\varphi) \cong \varphi(G).$$

(Analoge Aussagen gelten für Ringe, Moduln, Vektorräume).

Beweis:
Definiere

$$\psi : G/\ker(\varphi) \to \varphi(G) : g\ker(\varphi) \mapsto \varphi(g).$$

Die Surjektivität von ψ ist unmittelbar klar.

Zur Injektivität und Wohldefiniertheit von ψ:

$$\begin{aligned} g\ker(\varphi) = h\ker(\varphi) &\Leftrightarrow h^{-1}g \in \ker(\varphi) \\ &\Leftrightarrow \varphi(h^{-1}g) = e \\ &\Leftrightarrow \varphi(h) = \varphi(g) \\ &\Leftrightarrow \psi(h\ker(\varphi)) = \psi(g\ker(\varphi)) \ . \end{aligned}$$

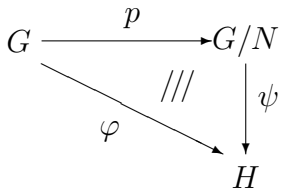
(Von links nach rechts bzw. oben nach unten erhält man die Wohldefiniertheit, in umgekehrter Richtung die Injektivität.)
ψ ist Homomorphismus:

$$\begin{aligned} \psi(g\ker(\varphi)\, h\ker(\varphi)) &= \psi(gh\ker(\varphi)) \\ &= \varphi(gh) \\ &= \varphi(g)\,\varphi(h) \\ &= \psi(g\ker(\varphi))\,\psi(h\ker(\varphi)). \end{aligned}$$

□

2.28. Satz

Es seien $\varphi : G \to H$ ein Gruppenhomomorphismus und N ein Normalteiler von G mit $N \subseteq \ker\varphi$. Dann existiert ein eindeutig bestimmter Homomorphismus $\psi : G/N \to H$ mit



Hierfür ist $\varphi = \psi\, p,\ \psi(G/N) = \varphi(G),\ \ker\psi = \ker\varphi/N$.

Beweis:
Definiere

$$\psi : G/N \to H : gN \mapsto \varphi(g).$$

ψ ist wohldefinert, da $N \subseteq \ker\varphi$ ist;

ψ ist Homomorphismus:

$$\begin{aligned} \psi(gN\,hN) &= \psi(ghN) \\ &= \varphi(gh) \\ &= \varphi(g)\,\varphi(h) \\ &= \psi(gN)\,\psi(hN). \end{aligned}$$

Die Eindeutigkeit von ψ ist klar wegen $\varphi = \psi \circ p$.

$\psi(G/N) = \varphi(G)$ gilt nach Konstruktion.

$$\begin{aligned} \ker \psi &= \{gN \mid \varphi(g) = e_H\} \\ &= \{gN \mid g \in \ker \varphi\} \\ &= \ker \varphi/N. \end{aligned}$$

□

2.29. Satz (1. Isomorphiesatz)

Es seien $U < G,\ N \lhd G$. Dann ist

$$UN/N \cong U/U \cap N$$

(speziell ist also $U \cap N$ Normalteiler in U).

Beweis:
N Normalteiler $\Rightarrow$ UN Untergruppe von G, die U, N umfaßt. N ist Normalteiler in $UN < G$.
Betrachte

$$\varphi : U \to UN/N : u \mapsto uN$$

$$\begin{aligned} UN/N &= \{unN \mid u \in U,\ n \in N\} \\ &= \{uN \mid u \in U\} \end{aligned}$$

φ ist surjektiver Homomorphismus mit

$$\begin{aligned} \ker \varphi &= \{x \in U \mid xN = N\} \\ &= \{x \in U \mid x \in N\} \\ &= U \cap N. \end{aligned}$$

Wende nunmehr(2.27) an!

□

2.30. Satz (2. Isomorphiesatz)

Es seien U, V Normalteiler von G mit $U \subseteq V$. Dann ist V/U Normalteiler in G/U, und es gilt

$$(G/U)\,/\,(V/U) \cong G/V.$$

Beweis:
Betrachte

$$\psi : G/U \to G/V : gU \mapsto gV.$$

Wegen $U \subseteq V$ ist ψ wohldefiniert. ψ ist offenbar Homomorphismus und surjektiv.

$$\begin{aligned} \text{Schließlich ist } \ker \psi &= \{gU \mid g \in G \wedge gV = V\} \\ &= \{gU \mid g \in V\} \\ &= V/U. \end{aligned}$$

Wende nunmehr (2.27) an!

□

Beispiel:
Es seien m, $n \in \mathbb{N}$ mit $n|m$. Dann ist

$$(\mathbb{Z}/m\mathbb{Z}) \,/\, (n\mathbb{Z}/m\mathbb{Z}) \cong \mathbb{Z}/n\mathbb{Z}.$$

Konstruktion von Gruppen aus Gruppen bzw. Zerlegung von Gruppen in Untergruppen führt zum Konzept des direkten Produkts von Gruppen.

2.31. Definition

Es seien $G_1, \ldots, G_n$ Gruppen. Dann heißt

$$G := G_1 \times \ldots \times G_n = \bigtimes_{i=1}^{n} G_i \text{ (oder } \prod_{i=1}^{n} G_i)$$

das äußere direkte Produkt von $G_1, \ldots, G_n$. G wird mittels

$$(g_1, \ldots, g_n) \circ (\tilde{g}_1, \ldots, \tilde{g}_n) = (\underbrace{g_1\tilde{g}_1}_{\in G_1}, \ldots, \underbrace{g_n\tilde{g}_n}_{\in G_n})$$

zu einer Gruppe.
Bei additiver Schreibweise:

$$G_1 \oplus \ldots \oplus G_n = \bigoplus_{i=1}^{n} G_i,$$

die sogenannte äußere direkte Summe.

2.31.1. Bemerkungen und Eigenschaften von direkten Produkten von Gruppen.

(i) $\left|\bigtimes_{i=1}^{n} G_i\right| = \prod_{i=1}^{n} |G_i|$.

(ii) $Z_{\bigtimes_{i=1}^{n} G_i} = \bigtimes_{i=1}^{n} Z_{G_i}$ für die Gruppenzentren

$$Z_G := \{g \in G \mid gx = xg \ \forall x \in G\}.$$

(iii) $G = \bigtimes_{i=1}^{n} G_i$ abelsch $\Leftrightarrow$ $G_1, \ldots, G_n$ abelsch.

(iv) $\pi \in \mathfrak{S}_n \ \Rightarrow \ \bigtimes_{i=1}^{n} G_i \cong \bigtimes_{i=1}^{n} G_{\pi(i)}$ mittels $(g_1, \ldots, g_n) \mapsto (g_{\pi(1)}, \ldots, g_{\pi(n)})$.

(v) $\left(\bigtimes_{i=1}^{n} G_i\right) \times \left(\bigtimes_{j=n+1}^{m} G_j\right) \cong \bigtimes_{i=1}^{m} G_i$ mittels $((g_1, \ldots, g_n), (g_{n+1}, \ldots, g_m)) \mapsto (g_1, \ldots, g_m)$.

(vi) $\varphi_i : G_i \to H_i \begin{cases} \text{Homomorphismus} \\ \text{Isomorphismus} \\ \text{Epimorphismus} \\ \text{Monomorphismus} \end{cases} \Rightarrow$

$$\varphi := \prod_{i=1}^{n} \varphi_i : \bigtimes_{i=1}^{n} G_i \to \bigtimes_{i=1}^{n} H_i : (g_1, \ldots, g_n) \mapsto (\varphi_1(g_1), \ldots, \varphi_n(g_n))$$

$$\text{ist wieder} \begin{cases} \text{Homomorphismus} \\ \text{Isomorphismus} \\ \text{Epimorphismus} \\ \text{Monomorphismus} \end{cases}.$$

(vii) $\varepsilon_i : G_i \to \bigtimes_{i=1}^{n} G_i : g_i \mapsto (e_1, \ldots, e_{i-1}, g_i, e_{i+1}, \ldots, e_n)$ ist eine Einbettung (Monomorphismus). Es gilt

$\varepsilon_i(G_i) \lhd \bigtimes_{j=1}^{n} G_j$ wegen

$$(g_1, \ldots, g_n)\, \varepsilon_i(G_i)\, (g_1, \ldots, g_n)^{-1} = (g_1 e_1 g_1^{-1}, \ldots, \underbrace{g_i G_i g_i^{-1}}_{G_i}, \ldots, g_n e_n g_n^{-1})$$
$$= (e_1, \ldots, e_{i-1}, G_i, e_{i+1}, \ldots, e_n) = \varepsilon_i(G_i).$$

(viii) $\pi_j : \bigtimes_{i=1}^{n} G_i \to G_j : (g_1, \ldots, g_n) \mapsto g_j$ ist eine "Projektion" (Gruppenepimorphismus auf eine Untergruppe) $(1 \leq j \leq n)$.

(ix) Für $\tilde{G}_i := \bigtimes_{\substack{j=1 \\ j \neq i}}^{n} G_j$ ist $\varphi_i : \bigtimes_{j=1}^{n} G_j \to \tilde{G}_i : (g_1, \ldots, g_n) \mapsto (g_1, \ldots, g_{i-1}, g_{i+1}, \ldots, g_n)$ ein Epimorphismus (Projektion) mit Kern $\varepsilon_i(G_i)$. Also ist

$$\bigtimes_{j=1}^{n} \Big/ \varepsilon_i(G_i) \cong \tilde{G}_i,$$

$$\tilde{G}_i \times G_i \cong \bigtimes_{i=1}^{n} G_j.$$

(x) Eine Verallgemeinerung auf unendliche Produkte ist möglich, wenn man die n-Tupel als Abbildung der Menge $\{1, 2, ..., n\}$ auf die Vereinigung der G_i interpretiert. Man erhält dann für beliebige Indexmengen I und Gruppen G_α mit $\alpha \in I$ für das **direkte Produkt** der G_α die Definition:

$$\prod_{\alpha \in I} G_\alpha := \{f : I \to \bigcup_{\alpha \in I} G_\alpha \mid f(\alpha) \in G_\alpha \, \forall \alpha \in I\}.$$

Dieses direkte Produkt enthält eine normale Untergruppe (Beweis als Übung empfohlen), die aus allen solchen Funktionen besteht, für die zusätzlich $f(\alpha) = e_\alpha$ für fast alle $\alpha \in I$ gefordert wird. Diese Untergruppe heißt **direkte Summe** der G_α. Ist die Indexmenge I endlich, stimmen inneres Produkt

und innere Summe offensichtlich überein. Der Fall unendlicher Indexmengen wird allerdings erst später bei Polynomringen gebraucht werden und dort wiederum nur für den Nachweis der Existenz eines algebraischen Abschlusses zu einem gegebenen Körper K.

Das Gegenstück zum äußeren Produkt ist:

2.32. Definition

Es sei G eine Gruppe mit Normalteilern $N_1, \ldots, N_n$. G heißt
direktes inneres Produkt von $N_1, \ldots, N_n$
$\left(G = \dot{\prod}_{i=1}^{n} N_i\right)$, wenn

(i) $G = N_1 \cdot \ldots \cdot N_n$ und
(ii) $N_i \cap \tilde{N}_i = \{e\}$ $(1 \leq i \leq n)$ für $\tilde{N}_i := N_1 \cdot \ldots \cdot N_{i-1} \cdot N_{i+1} \cdot \ldots \cdot N_n$ gilt.

(Additive Schreibweise: $N_1 \dot{+} \ldots \dot{+} N_n = \dot{\sum}_{i=1}^{n} N_i$, direkte innere Summe.)

Zur Auseinanderhaltung beider Begriffe bemerken wir folgendes:
$\mathbb{Z}/2\mathbb{Z} = \{\overline{0}, \overline{1}\}$ hat die Verknüpfungstabelle

$+$	$\overline{0}$	$\overline{1}$
$\overline{0}$	$\overline{0}$	$\overline{1}$
$\overline{1}$	$\overline{1}$	$\overline{0}$

.

Es ist $G = \overbrace{\mathbb{Z}/2\mathbb{Z}}^{G_1} \oplus \overbrace{\mathbb{Z}/2\mathbb{Z}}^{G_2}$ eine additive Gruppe mit Verknüpfungstabelle (Gruppentabelle):

$+$	n	b	c	d
n	n	b	c	d
b	b	n	d	c
c	c	d	n	b
d	d	c	b	n

für die Elemente

$$\begin{aligned} n &= (\overline{0}, \overline{0}) = \overline{0} \oplus \overline{0} \\ b &= (\overline{1}, \overline{0}) = \overline{1} \oplus \overline{0} \\ c &= (\overline{0}, \overline{1}) = \overline{0} \oplus \overline{1} \\ d &= (\overline{1}, \overline{1}) = \overline{1} \oplus \overline{1} \end{aligned} .$$

Also ist G vom Typ $\mathfrak{V}_4$ (Kleinsche Vierergruppe). Die einzigen Untergruppen von G sind

$$\{n\},\ G,\ \underbrace{\{n, b\}}_{N_1},\ \underbrace{\{n, c\}}_{N_2},\ \underbrace{\{n, d\}}_{N_3} \quad \text{mit} \quad N_i \cong G_i\ (i = 1, 2).$$

Offensichtlich ist $G = N_1 \dot{+} N_3 = N_1 \dot{+} N_2 = N_2 \dot{+} N_3$.

Dagegen ist $N_1 \oplus N_3$ zwar zu G isomorph, ist jedoch eine Konstruktion, die nicht mit G verwechselt werden sollte.

Es folgt eine Charakterisierung innerer Produkte:

2.33. Satz

Es sei G eine Gruppe mit Untergruppen $N_1, \ldots, N_n$. Hierfür sind äquivalent:

(i) $g_i g_j = g_j g_i \ \forall g_i \in N_i,\ g_j \in N_j \ (1 \leq i < j \leq n)$, und jedes $g \in G$ läßt sich eindeutig in der Form $g = g_1 \cdot \ldots \cdot g_n$ mit $g_i \in N_i$ schreiben.

(ii) $N_i \lhd G \ (1 \leq i \leq n)$, und G ist direktes inneres Produkt von $N_1, \ldots, N_n$, d.h.

$$G = \dot{\prod_{i=1}^{n}} N_i.$$

Beweis:

(ii) $\Rightarrow$ (i):
Die Normalteilereigenschaft von N_i, N_j liefert:

$$g_i g_j g_i^{-1} \in N_j, \quad g_j g_i^{-1} g_j^{-1} \in N_i;$$

für $i \neq j$ ist demnach

$$g_i g_j g_i^{-1} g_j^{-1} \in N_j N_j \cap N_i N_i = \{e\},$$

also

$$g_i g_j = g_j g_i.$$

Jedes $g \in G$ besitzt eine Produktdarstellung $g = g_1 \cdot \ldots \cdot g_n$ mit $g_i \in N_i$. Zu zeigen bleibt die Eindeutigkeit. Dazu seien $g_i,\ h_i \in N_i \ (1 \leq i \leq n)$ mit

$$g_1 \cdot \ldots \cdot g_n = h_1 \cdot \ldots \cdot h_n$$

bzw.

$$\begin{aligned} g_1^{-1} h_1 &= g_2 \cdot \ldots \cdot g_n \cdot h_n^{-1} \cdot h_{n-1}^{-1} \cdot \ldots \cdot h_2^{-1} \\ &= g_2 h_2^{-1} \cdot \ldots \cdot g_n h_n^{-1} \ \in \tilde{U}_1 \\ &\Rightarrow \ h_1^{-1} g_1 = e \quad \text{bzw.} \quad g_1 = h_1. \end{aligned}$$

Analog folgt $g_i = h_i \ (2 \leq i \leq n)$.

(i) $\Rightarrow$ (ii):
Es ist $h g_i h^{-1} = h_i g_i h_i^{-1} \in N_i$ für $h \in G,\ g_i \in N_i$, da man alle Faktoren $h_j \ (j \neq i)$ an g_i und $h_k (k \neq j)$ vorbeiziehen kann.
Es folgt $h N_i h^{-1} \subseteq N_i$, demnach ist N_i Normalteiler in G. $G = N_1 \cdot \ldots \cdot N_n$ gilt nach Voraussetzung. Ist schließlich $x \in N_i \cap \tilde{N}_i$, so folgt

$$x = g_i = g_1 \cdot \ldots \cdot g_{i-1} \cdot g_{i+1} \cdot \ldots \cdot g_n \quad \Rightarrow \quad e = g_i^{-1} \cdot g_1 \cdot \ldots \cdot g_{i-1} \cdot g_{i+1} \cdot \ldots \cdot g_n$$

mit $g_j \in N_j \ (1 \leq j \leq n)$; wegen der Eindeutigkeit der Darstellung folgt $g_1 = \ldots = g_n = e = x$.

□

Bemerkung:
Wie im obigen Beispiel gilt für das innere direkte Produkt

$$G = \dot{\prod_{i=1}^{n}} N_i,$$

auch

$$G \cong \bigtimes_{i=1}^{n} N_i.$$

Der entsprechende Isomorphismus wird gegeben durch

$$\varphi \,:\, \dot{\prod_{i=1}^{n}} N_i \to \bigtimes_{i=1}^{n} N_i \;:\; g_1 \cdot \ldots \cdot g_n \mapsto (g_1, \ldots, g_n).$$

φ ist Homomorphismus wegen der Vorbeizieheigenschaft, φ surjektiv ist klar, φ injektiv gilt wegen der eindeutigen Darstellung von $e \in G$ als $e \cdot \ldots \cdot e$.

2.34. Hauptsatz über endliche abelsche Gruppen

Theorem Every finite abelian group G is a direct product of cyclic subgroups:

$$G \;=\; \dot{\prod_{i=1}^{l}} G_i \;\;.$$

Additionally, we can postulate that the orders $n_i :=\mid G_i \mid$ have the divisibility properties $n_{i+1} \mid n_i \;\; (1 \leq i < l)$. (The vector $(n_1, ..., n_l)$ is an invariant of the group G; the n_i are said to be **elementary divisors** of G.)

Proof. The proof is by induction on the order n of G. For $n = 1, 2, 3$ the group G itself is cyclic. Therefore we immediately proceed to the induction step $n \longrightarrow n + 1$.
For $G = \langle a_1, ..., a_k \rangle$ the order of each element $g \in G$ is a divisor of $\mathrm{lcm}(\mathrm{ord}(a_1), ..., \mathrm{ord}(a_k)) =: n_1$.
Because of our previous results the group G contains an element A_1 with $\mathrm{ord}(A_1) = n_1$.
We set $G_1 := \langle A_1 \rangle$ and $\tilde{G} := G/G_1$. The order of $\tilde{G}$ is smaller than the order of G.
Because of our induction assumption the group $\tilde{G}$ is a direct product of cyclic subgroups, say

$$\tilde{G} \;=\; \dot{\prod_{i=2}^{l}} \langle b_i G_1 \rangle \;\; (b_i \in G) \;\;,$$

and the orders $n_i =\mid \langle b_i G_1 \rangle \mid$ satisfy

$$n_{i+1} \mid n_i \;\; (2 \leq i < l).$$

(From this it is clear that $A_1, b_2, ..., b_l$ generate G, but the product of the corresponding cyclic subgroups is in general not direct. We therefore need to change the b_i adequately.)

Because of $n_i =| \langle b_i G_1 \rangle |$ the exponent n_i is minimal with the property $b_i^{n_i} \in G_1$, and therefore n_i divides every exponent μ satisfying $b_i^{\mu} \in G_1$. As a consequence we have $n_i \mid \mathrm{ord}(b_i)$. We recall that also $\mathrm{ord}(b_i) \mid n_1$, say $n_1 = \mathrm{ord}(b_i)\lambda_i$ with a suitable integer λ_i.
Let us assume that

$$b_i^{n_i} \;=\; A_1^{m_i} \;\; (0 \le m_i < n_1) \;\; .$$

We want to show that n_i divides m_i.
We have

$$\mathrm{ord}(A_1^{m_i}) \;=\; \frac{n_1}{\gcd(n_1, m_i)} \;=\; \frac{\mathrm{ord}(b_i)\lambda_i}{\gcd(n_1, m_i)} \; .$$

Analogogously, we obtain

$$\mathrm{ord}(b_i^{n_i}) \;=\; \frac{\mathrm{ord}(b_i)}{\gcd(\mathrm{ord}(b_i), n_i)} \;=\; \frac{\mathrm{ord}(b_i)}{n_i} \;\; .$$

The last equations yield

$$n_i \mid n_i\lambda_i \;=\; \gcd(n_1, m_i) \mid m_i \; .$$

We put $A_i := b_i A_1^{-m_i/n_i}$ and obtain $b_i G_1 = A_i G_1$ as well as $\mathrm{ord}(A_i) = n_i$.

We still need to show

$$G \;=\; \dot{\prod_{i=1}^{l}} \langle A_i \rangle \;\; .$$

Because of $G = \langle A_1, b_2, ..., b_l \rangle$ we immediately get $\langle A_1, A_2, ..., A_l \rangle = G$. We have already shown that the product is also direct if the presentations of elements of $x \in G$ as power products of $A_1, ..., A_l$ in the form

$$x \;=\; \prod_{i=1}^{l} A_i^{\mu_i} \;\; (0 \le \mu_i < n_i)$$

are unique.
For this we assume that $x \in G$ has presentations

$$x \;=\; \prod_{i=1}^{l} A_i^{\mu_i} \;=\; \prod_{i=1}^{l} A_i^{\nu_i} \;\; (0 \le \mu_i, \nu_i < n_i) \;\; .$$

This yields

$$A_1^{\mu_1 - \nu_1} \;=\; \prod_{i=2}^{l} A_i^{\nu_i - \mu_i}$$

and therefore also

$$\begin{aligned} G_1 \;&=\; \left(\textstyle\prod_{i=2}^{l} A_i^{\nu_i - \mu_i}\right) G_1 = \textstyle\prod_{i=2}^{l} (A_i G_1)^{\nu_i - \mu_i} \\ &=\; \textstyle\prod_{i=2}^{l} (b_i G_1)^{\nu_i - \mu_i} \;\; . \end{aligned}$$

According to our induction assumption we get

$$\nu_i - \mu_i \ = \ 0 \ \ (2 \leq i \leq l) \ .$$

Then we also must have $\mu_1 - \nu_1 = 0$, hence $\mu_i = \nu_i$ for $1 \leq i \leq l$.
By our construction, the divisibility conditions for the n_i are satisfied, too.
□

Example Let $G = \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/15\mathbb{Z}$ of order 360. The least common multiple of the orders of the 3 cyclic subgroups is 60. An element A_1 of G of order 60 is easily found, for example, we can choose $A_1 = (1 + 4\mathbb{Z}, 2 + 6\mathbb{Z}, 3 + 15\mathbb{Z})$. Then the order of $G/\langle A_1 \rangle$ is 6, that factor group is therefore cyclic, a generator is $(4\mathbb{Z}, 1{+}6\mathbb{Z}, 1{+}15\mathbb{Z})\langle A_1 \rangle$. We set $b_2 = (4\mathbb{Z}, 1 + 6\mathbb{Z}, 1 + 15\mathbb{Z})$ and obtain $b_2^6 = A_1^{12}$. This results in $A_2 = b_2 A_1^{-2}$ and $G = \langle A_1 \rangle \times \langle A_2 \rangle$.

2.35. Group Theory II

In this section we consider groups operating on sets. This is not particularly new. For example, the permutation group S_n acts on the subset $\mathbb{N}_n = \{1, 2, ..., n\}$ of $\mathbb{N}$. Also the group D_n acts on the vertices of a regular n-gon. We see immediately that both actions satisfy the conditions of the subsequent definition. These conditions are essential for establishing a suitable equivalence relation on S with respect to the action of G. The latter is then used for showing the existence of certain subgroups of a given group. The concept is also applied in other areas of mathematics.

Definition 2.1. *Let G be a group and S be a non-empty set. We say that G* **acts on** *S if there is a map*

$$G \times S \to S \ : \ (g, s) \mapsto g \circ s$$

satisfying the following conditions:

(i) $(gh) \circ s \ = \ g \circ (h \circ s) \ \ \forall g, h \in G, \ \forall s \in S,$
(ii) $e \circ s \ = \ s \ \ \forall s \in S$, *$e$ the unit element of G.*

Examples

(i) Let U be a subgroup of a group G, $S \lhd G$ and

$$U \times S \to S \ : \ (g, h) \mapsto ghg^{-1} \ .$$

The 2 conditions of the definition are easily checked:

$$\begin{aligned} g_1 \circ (g_2 \circ h) &= g_1 \circ (g_2 h g_2^{-1}) \\ &= g_1 g_2 \, h \, g_2^{-1} g_1^{-1} \\ &= g_1 g_2 \, h \, (g_1 g_2)^{-1} \\ &= (g_1 g_2) \circ h \end{aligned}$$

for all $g_1, g_2 \in U$, $h \in S$ as well as

$$e \circ h \;=\; h$$

for the unit element e of U.

(ii) Let G be a group and m a natural number satisfying $m \leq |G|$. Let S be a subset of the power set of G consisting of all subsets of G with exactly m elements. The action of G on S is given by $G \times S \to S \;:\; (g, T) \mapsto gT = \{gt | t \in T\}$. We leave it to the reader to verify the conditions of the definition.

If a group G acts on a set S then S decomposes into equivalence classes with respect to the following relation on S. Two elements s, t of S are said to be equivalent (with respect to G), iff there exists $g \in G$ with $g \circ s \;=\; t$. We show that this is indeed an equivalence relation. The relation is clearly reflexive because of the second condition in Definition 2.1 (ii). It is symmetric because $g \circ s = t$ implies $g^{-1} \circ t = s$. For this we need both conditions. Eventually, $g \circ s = t$ and $h \circ t = u$ $(g, h \in G,\; s, t, u \in S)$ yield $(hg) \circ s = h \circ (g \circ s) = h \circ t = u$, hence the transitivity of that relation. The equivalence classes are also called **orbits** . The orbit containing $s \in S$ is denoted by $O(s)$.
We will see that the length of an orbit can be interpreted as a group index of G. For this we introduce the notion of an inertia group.

Definition 2.2. *An action of the group G on the set S is said to be* **transitive** *if there is exactly one orbit in S, namely S itself. For $s \in S$ the subset of G fixing s, i.e. $Stab(s) := \{g \in G \mid g \circ s = s\}$, is called* **stabilizer** *(or inertia group, fix group) of the element s.*

It is easy to see that $\mathrm{Stab}(s)$ is actually a subgroup of G for each $s \in S$. Clearly, the unit element e of G belongs to $\mathrm{Stab}(s)$. If g, h are in $\mathrm{Stab}(s)$, then also h^{-1} and gh^{-1} are in $\mathrm{Stab}(s)$.
In order to establish a connection between the length of an orbit $O(s)$ and the number of elements of G , $\mathrm{Stab}(s)$ we need to consider how the fix groups of elements of an orbit are related.
Let $s, t \in S$ belong to the same orbit, say $O(s)$. Hence, there exists $g \in G$ with $g \circ s = t$. We obtain the following chain of equivalences:

$$\begin{aligned}
\mathrm{Stab}(t) &= \{h \in G \mid h \circ t = t\} \\
&= \{h \in G \mid h\,(g \circ s) = g \circ s\} \\
&= \{h \in G \mid (g^{-1} h g) \circ s = s\} \\
&= \{h \in G \mid g^{-1} h g \in \mathrm{Stab}(s)\} \\
&= \{h \in G \mid h \in g\ \mathrm{Stab}(s) g^{-1}\} \\
&= g\,\mathrm{Stab}(s)\,g^{-1}.
\end{aligned}$$

Hence, the fix groups of any two elements of an orbit are conjugate subgroups of G.

LEMMA 1. *The* **length** $|O(s)|$ *of the orbit* $O(s)$ *equals the group index* $(G : Stab(s))$. *If* G *is finite then the length of every orbit is a divisor of the group order.*

Proof We consider the map

$$\varphi \ : \ O(s) \to \{g\,\mathrm{Stab}(s) \mid g \in G\} \ : \ g \circ s \mapsto g\,\mathrm{Stab}(s) \ .$$

φ is clearly surjective. It is also well defined and injective because of the following chain of equivalences:

$$\begin{aligned} g\,\mathrm{Stab}(s) = h\,\mathrm{Stab}(s) \quad &\Leftrightarrow \quad h^{-1}g \in \mathrm{Stab}(s) \\ &\Leftrightarrow \quad h^{-1}g \circ s = s \\ &\Leftrightarrow \quad g \circ s = h \circ s \ . \end{aligned}$$

Hence, we have established a bijection between the elements $g \circ s$ of the orbit $O(s)$ and the left cosets $g\,\mathrm{Stab}(s)$ of $\mathrm{Stab}(s)$ in G.
□

If G acts on the set S then S decomposes into orbits. Hence, there is a set $R \subset S$ of representatives such that

$$S \ = \ \dot{\bigcup_{r \in R}} O(r) \ . \tag{1}$$

Since that union is disjoint the number of elements in S is obtained as a sum of group indices:

$$|S| \ = \ \sum_{r \in R} (G : \mathrm{Stab}(r)) \ . \tag{2}$$

Those elements $s \in S$ whose orbits $O(s)$ consist of just one element, $O(s) = \{s\}$, are called **fix points** under the action of G. They play a distinguished role. If we denote the set of them by $F(S)$ then the decomposition of S into orbits yields the following relation between the lengths of those orbits.

$$|S| \ = \ |F(S)| \ + \ \sum_{r \in R \setminus F(S)} (G : \mathrm{Stab}(r)) \ . \tag{3}$$

The last equation becomes even more important if we consider the action of a group G on subsets of G by conjugation. Let T be a fixed non-empty subset of G. We put $S \ := \ \{gTg^{-1} \mid g \in G\}$ and define the action of G on S via

$$G \times S \to S \ : \ (h,\, gTg^{-1}) \mapsto hgT(hg)^{-1} \ .$$

Obviously, G operates transitively on S, there exists only one orbit, the set S itself. In this special situation we have

$$\mathrm{Stab}(T) \ = \ \{g \in G \mid gTg^{-1} = T\} \ = \ N_T \ ,$$

that is the fix group of T equals the normalizer N_T of T in G. If T is even a subgroup of G then T has exactly $(G : N_T)$ conjugate subgroups.

In a slightly different situation let G act on the set of its own elements by conjugation. In that case, the set of fixed points $F(G)$ coincides with the center $Z(G)$ of G. The orbits of the elements are called classes of conjugate elements. The stabilizer of an element coincides with its normalizer. The class equation (**??**) becomes

$$|G| \;=\; |Z(G)| \;+\; \sum_{r\in R\setminus Z(G)} (G : N_r) \tag{4}$$

if R again denotes a full set of representatives of the orbits.
These results will now be used to exhibit the existence of subgroups of prime power order in any finite group G.

Definition 2.3. *Let G be a finite group of order $(G : 1) = p^m q$ with $p \in \mathcal{P}$ and $m, q \in \mathbb{N}$, p not dividing q.*

(i) A subgroup of G of order p^a, i.e. $1 \le a \le m$, is called **p-subgroup**.
(ii) A p-subgroup H of maximal p-power, i.e. $(H : 1) = p^m$, is called a **p-Sylow-subgroup**.
(iii) In case $m = 1$ the group G is called a **p-group**.

Remark The center of a p-group is non-trivial, i.e. it contains more than one element. This is an immediate consequence of (**??**) where the left-hand side and also all terms of the second summand of the right-hand side are divisible by p with the consequence that also $\mid Z(G) \mid$ must be divisible by p.

Example Let $G = V_4$ be the Klein Four Group. G is its own p-Sylow-subgroup for the only prime number $p = 2$ dividing the order of G, and G has 3 p-subgroups of order 2.

We want to show the existence of p-subgroups for all finite groups G whose order is divisible by p. For this we start in a slightly more general context. We assume that the order of the given finite group G is $n = p^m q$ for a prime number p not dividing $q \in \mathbb{N}$. From Lagrange's theorem we know that the order of a subgroup of G divides $(G : 1)$. Hence, we assume that k is a positive integer subject to $k > 1$ and $k|(G : 1)$. If there is a subgroup of G of order k then it has to be one of the $\binom{n}{k}$ subsets of G of k elements.
As in the second example in this section let S be the set of all subsets of G of k elements. The group G acts on S by multiplication. For $T \in S$, say $T = \{t_1, ..., t_k\}$, we have

$$G \times S \to S \;:\; g \circ T \mapsto \{gt_1, ..., gt_k\} \;\; .$$

What can we say about the stabilizer of T? If $gT = T$ for some $g \in G$ then $gt_1 = t_j$ for some $j \in \{1, ..., k\}$, and the group element g is uniquely determined by that index j: $g = t_j t_1^{-1}$. Hence, the order of the stabilizer of T is bounded by k.

On the other hand, if $U \in S$ is indeed a subgroup of G then the stabilizer of U equals U because of $g \circ U = U \quad \Leftrightarrow \quad g \in U$. From this we conclude that an element $U \in S$ is a subgroup of G if and only if U equals its stabilizer. In that case the length of the orbit $O(U)$ of U is $|G|/k$.
Now let us assume that the length of the orbit $O(T)$ of $T \in S$ is $|G|/k$. We want to prove that $O(T)$ contains exactly one subgroup U of G. The stabilizer $\mathrm{Stab}(T)$ of T satisfies $\mathrm{Stab}(T)\, x \subseteq T$ for any $x \in T$ and therefore $\mathrm{Stab}(T)\, x = T$ because of $|\mathrm{Stab}(T)| = k$. Hence, $x^{-1}\, \mathrm{Stab}(T)\, x \;=\; x^{-1}T$ is a subgroup in the orbit of T. Also, $O(T)$ can contain at most one subgroup of G. To show this, we assume that $U = gT$ and $V = hT$ are both subgroups of G in $O(T)$. We obtain $U = (gh^{-1})V$ implying $gh^{-1} \in U$, hence also $hg^{-1} \in U$ and therefore $U = hg^{-1}U = hg^{-1}(gh^{-1})V = V$.
For detecting subgroups of order k we therefore just need to check whether S contains an orbit of length $|G|/k$. However, this can require lengthy computations as the following example demonstrates.

Exercise We recommend that the reader generates the subsets of $k \in \{3, 4, 6\}$ elements of the alternating group A_4 to check computationally that A_4 has subgroups of orders 3,4, respectively, but has no subgroup of order 6.

The results of that exercise show that we cannot expect the existence of subgroups of arbitrary order dividing the group order n. It is the merit of the group theoretician L. Sylow (1832-1918) from Norway to have recognized and proved the existence of subgroups of prime power order p^a $(1 \leq a \leq m)$ for prime numbers p with $p^m \;||\; |G|$. The special case $a = 1$ is due to Cauchy and readers not familiar with the subject are advised to assume $a = 1$ at first reading of the following, though the arguments are the same for $a > 1$.
We recall that all we need to prove is the existence of an orbit $O(T)$ of S of length equal to $p^{m-a}q$, a stabilizer belonging to that orbit being a subgroup we are looking for. (If we additionally require $e \in T$ we already have $\mathrm{Stab}(T) = \mathrm{Stab}(T)e = T$.) We already know that $|O(T)| \geq p^{m-a}q$. Since the length of any orbit divides $|G|$ it therefore suffices to exhibit the existence of an orbit whose orbit length is not divisible by p^{m-a+1}. The latter is an easy consequence of the following lemma from elementary number theory and the class equation of the action of G on S.

Lemma 2. *Let $n = p^m q$ for a prime number p not dividing $q \in \mathbb{N}$. Then for $1 \leq a \leq m$ the binomial coefficient $\binom{n}{p^a}$ is divisible by p^{m-a} but not divisible by p^{m-a+1}. The quotient $\binom{n}{p^a} / (p^{m-a}q)$ is congruent to 1 modulo p.*

Proof

$$\binom{n}{p^a} \;=\; \prod_{i=0}^{p^a-1} \frac{n-i}{p^a-i} \;=\; p^{m-a}q \prod_{i=1}^{p^a-1} \frac{p^m q-i}{p^a-i} \;=\; p^{m-a}qx$$

with $x = \binom{n-1}{p^a-1}$. In the product for x we write every index $i \in \{1, ..., p^a-1\}$ in the form $i = p^{l_i}x_i$ with $0 \leq l_i < a$ and x_i not divisible by p. Dividing the numerator and the denominator of the i-th factor of that product by p^{l_i} we obtain
for the numerator:

$$\prod_{i=1}^{p^a-1} \left(p^{m-l_i}q - x_i\right) = u\,p + y \quad (u \in \mathbb{Z}^{\geq 0},\; y = \prod_{i=1}^{p^a-1} (-x_i),\; p \nmid y),$$

and for the denominator:

$$\prod_{i=1}^{p^a-1} \left(p^{a-l_i} - x_i\right) = v\,p + y \quad (v \in \mathbb{Z}^{\geq 0}),$$

and therefore

$$x(vp + y) = up + y \;\;.$$

Because of $p \nmid y$ this yields the result

$$x \equiv 1 \bmod p \;\;.$$

□

The following theorem contains the most important results on the existence of p-subgroups.

THEOREM 3 (Sylow). *Let G be a group of order $n = p^m q$ with $p \nmid m$ and let $1 \leq a \leq m$ $(a \in \mathbb{N})$.*

- *(i) The number of subgroups of G of order p^a is congruent to 1 modulo p, i.e. these subgroups do always exist.*
- *(ii) Let H be a p-Sylow-subgroup of G and U an arbitrary p-subgroup of G. Then one of the conjugates of U is contained in H.*
- *(iii) All p-Sylow-subgroups of G are conjugate. The number of p-Sylow-subgroups of G divides q.*

Proof

(i) We have seen that subgroups of order p^a are in $1-1$-correspondence to the orbits of length $p^{m-a}q$ of the set S of subsets of G with p^a elements under the action of G. Because of the preceding Lemma $|S|$ is not divisible by p^{m-a+1}. Hence, the class equation (**??**) tells us that there are orbits of length $p^{m-a}q$ and it follows that their number is congruent to 1 modulo p.

(ii) Let H be a fixed p-Sylow-subgroup of G. We consider the action of G on the set $S_H := \{gHg^{-1} | g \in G\}$ by conjugation. Obviously, G acts transitively on S_H. The length $|S_H|$ equals

the group index $(G : N_H)$ for the normalizer N_H of H. Since N_H contains H that group index is not divisible by p.

Next let U be an arbitrary p-subgroup of G, say of order p^a. We let U act on S_H by conjugation. S_H decomposes into orbits whose lengths are divisors of p^a. Because of $p \nmid |S_H|$ there must exist orbits of length 1.

Hence, there exists a p-Sylow-subgroup K which is conjugate to H and for which U is contained in the normalizer N_K. Then U and K are both contained in the normalizer N_K of K in G. Also, K is always a normal subgroup of N_K. Hence, we can apply the first isomorphism theorem for groups and get

$$UK/K \cong U/U \cap K \quad .$$

Therefore UK is a supergroup of K for which the index $(U\,K : K)$ equals $(U : U \cap K)$, a p-power. Then also the order of UK is a p-power divisible by $|K|$. K being a p-Sylow-subgroup of G we must necessarily have $UK = K$ and therefore $U \subseteq K$. Since $K = gHg^{-1}$ for a suitable element g of G we obtain

$$g^{-1}Ug \;\subseteq\; g^{-1}Kg \;=\; H \quad .$$

(iii) If we choose U to be a p-Sylow-subgroup, too, then the same considerations as in the previous part of the proof yield that any two p-Sylow-subgroups of G are conjugate, i.e. the orbit S_H already coincides with the set of all p-Sylow-subgroups of G.

We already noted that the orbit length $|S_H| = (G : N_H)$ is not divisible by p. Being a divisor of $|G|$ it must therefore divide q.

□

Remark A p-Sylow-subgroup H of G is a normal subgroup of G if and only if $|S_H| = 1$.

KOROLLAR 4 (Cauchy). *If the order of the finite group G is divisible by the prime number p then G contains a subgroup and therefore an element of order p.*

Proof According to Sylow's theorem G contains a subgroup U with $(U : 1) = p$. U is necessarily cyclic, and all its elements except the unit element have order p.
□

KOROLLAR 5. *A finite group G is a p-group if and only if the order of each of its elements is a p-power.*

Beispiele:

(i) Es sei G eine Gruppe der Ordnung $15 = pq$ mit $p = 3,\ q = 5$. Dann gilt für die Anzahlen n der p-Sylowuntergruppen von G:

$$n_3 \equiv 1 \bmod 3 \text{ und } n_3 \mid 5\,.$$

Notwendigerweise ist $n_3 = 1$. Analog erhält man $n_5 = 1$. Also sind die p-Sylowuntergruppe U und die q-Sylowuntergruppe V von G jeweils Normalteiler. Für $U = \langle x\rangle$ mit $\mathrm{ord}(x) = 3$ und $V = \langle y\rangle$ mit $\mathrm{ord}(y) = 5$ erhält man $x\,y\,x^{-1}y^{-1} \in U \cap V = \{e\}$. Folglich kommutieren x und y. Damit ist $\mathrm{ord}(xy) = \mathrm{ord}(x)\mathrm{ord}(y) = 15$, also $G = \langle xy\rangle$ zyklisch.

(ii) Es sei $G =$ eine Gruppe der Ordnung $21 = pq$ mit $p = 3,\ q = 7$. Wie zuvor ist $n_7 = 1,\ n_3 \in \{1, 7\}$. Für $n_3 = 1$ folgt wiederum, dass G zyklisch ist. Kann auch $n_3 = 7$ auftreten? (G ist dann nicht kommutativ!). Es sei $V = \langle y\rangle$ (Normalteiler!) mit $\mathrm{ord}(y) = 7$ und $U = \langle x\rangle$ eine p-Sylowuntergruppe von G mit $\mathrm{ord}(x) = 3$. Wir betrachten $G = V \,\dot\cup\, xV \,\dot\cup\, x^2V = V \,\dot\cup\, Vx^2 \,\dot\cup\, Vx$, wobei jedes Element in $xV,\ x^2V,\ Vx^2,\ Vx$ notwendig die Ordnung 3 haben muss. Wir setzen an: $x\,y\,x^{-1} = x\,y\,x^2 \stackrel{!}{=} y^\mu$ mit $\mu \in \{0, 1, 2, \ldots, 6\}$. (Offenbar ist $\mu = 0$ nicht möglich.) Wegen $x^3 = e$ folgt $xy = y^\mu x$ und damit $(xy)(xy) = y^\mu x^2 y = y^{\mu+\mu^2}x^2$, $e \stackrel{!}{=} (xy)^3 = y^{\mu+\mu^2}x^2(xy) = y^{1+\mu+\mu^2}$. Wegen $\mathrm{ord}(y) = 7$ muss $1 + \mu + \mu^2 \equiv 0 \bmod 7$ gelten. Dies ist richtig für $\mu \in \{2, 4\}$. (Da wir als Erzeuger von U sowohl x als auch x^2 wählen können und im Fall $\mu = 2$ auch $x^2yx = x^2y\,x^4 = x(x\,y\,x^2) = x\,y^2x^2 = (x\,y\,x^2)^2 = y^4$ erfüllt ist, dürfen wir oBdA $\mu = 2$ annehmen.) Wir haben damit als nicht kommutative Gruppe der Ordnung 21: $G = \langle x, y \mid x^3 = e = y^7,\ x\,y\,x^2 = y^2\rangle$ (Der Nachweis von $\mathrm{ord}(x^iy^j) = 3$ für $i = 1, 2,\ 1 \le j \le 6$, wird als Übung empfohlen.)

(iii) Es sei $p \in \mathbb{P}$ und G eine Gruppe der Ordnung p^2. Ist G abelsch, so ist G isomorph zu $(\mathbb{Z}/p^2\mathbb{Z}, +)$ (zyklisch) bzw. zu $(\mathbb{Z}/p\mathbb{Z}, +) \times (\mathbb{Z}/p\mathbb{Z}, +)$.
Wir zeigen, dass G abelsch ist.
Dazu betrachten wir das Zentrum $U = Z(G)$ von G. Da das Zentrum einer p-Gruppe - wie gezeigt - nicht nur aus dem Einselement besteht, gilt $Z(G) = G$ (folglich G abelsch) oder $\#Z(G) = p$. Im letzteren Fall sei $U = \langle y\rangle$ sowie $G/U = \langle xU\rangle$ mit $\mathrm{ord}(y) = \mathrm{ord}(xU) = p$.
Jedes $g \in G$ hat folglich eine Darstellung $g = x^iy^j$ mit $0 \le i < p,\ 0 \le j < p$. Für $h = x^ky^l \in G$ erhalten wir (wegen $y \in Z(G)$)

$$\begin{array}{rcccl} gh & = & x^iy^jx^ky^l & = & x^{i+k}y^{j+l} \\ & = & x^ky^lx^iy^j & = & hg, \end{array}$$

also ist G notwendig abelsch.

Example We want to determine all non-abelian groups of order 8. G cannot contain an element of order 8 (in that case G would be cyclic) nor can all group elements of G have 2 as exponent (in which case G would be abelian). Hence, G must contain at least one element, say b, of order 4. Then $U = \langle b \rangle$ has index 2 in G and is therefore a normal subgroup. G decomposes into 2 equivalence classes with respect to U, say $G = U \dot\cup Ua$ with $Ua = aU$. Since a is not contained in U the element a^2 is not contained in Ua, therefore it must belong to U. Because of $\mathrm{ord}(a) \mid 4$ we obtain $a^2 = e$ or $a^2 = b^2$. We shall see that both options yield a group of order 8 which is unique up to isomorphism.
Since we are looking for non-abelian groups we need to know what aba^{-1} is. Because of $aU = Ua$ we must have $aba^{-1} \in U$. The option $aba^{-1} = b$ is to be excluded since G would be abelian in that case. The choice $aba^{-1} = e$ is impossible since it yields $b = e$. Finally, a choice $aba^{-1} = b^2$ implies $ab^2a^{-1} = (aba^{-1})^2 = b^4 = e$, hence $b^2 = e$ which is in contradiction with $\mathrm{ord}(b) = 4$. The only remaining possibility is therefore $aba^{-1} = b^{-1}$ yielding $ab^m = b^{-m}a$ for all $m \in \mathbb{N}$.
We now distinguish the two cases $a^2 = e$ and $a^2 = b^2$.

(i) $a^2 = e$ yields $G \cong D_4$.
The generators a, b of G satisfy the relations defining D_4: $a^2 = e = b^4$ and $aba^{-1} = b^{-1}$. For example, these are fulfilled by the matrices

$$b := \begin{pmatrix} \cos(2\pi/4) & -sin(2\pi/4) \\ \sin(2\pi/4) & \cos(2\pi/4) \end{pmatrix}, a := \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} .$$

(ii) $a^2 = b^2$ yields $G \cong Q_8$.
The relations $b^4 = e\,,\ a^2 = b^2\,,\ aba^{-1} = b^{-1}$ are easily seen to be satisfied by the matrices

$$b := \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, a := \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$$

from $\mathbb{C}^{2\times 2}$, where $i^2 = -1$ denotes the imaginary unit. Hence, those 2 matrices generate a group of 8 elements which is isomorphic to the quaternion group.

We note that the special representation of the group elements by matrices in both cases makes it superfluous to test whether the composition (here: matrix multiplication) is associative.
¿From Sylow's theorem we can easily conclude that p-groups do not only contain subgroups for every p-power dividing the group order but also normal subgroups.

PROPOSITION 6. *Let G be a p-group of order p^m and let $a \in \{1, 2, ..., m\}$. Then G contains a normal subgroup of order p^a, moreover, the number of these normal subgroups of G is congruent to 1 modulo p.*

Proof We denote by S the (non-empty) set of subgroups U of G of order p^a. According to the Sylow theorem the number of elements in S is congruent to 1 modulo p. We let G act on S by conjugation. If R denotes a full set of representatives of the corresponding orbits then the class equation reads

$$\mid S \mid = \sum_{U \in R} (G : N_U) \ .$$

Denoting the set of fix points by $F(S)$ we get

$$|S| \equiv |F(S)| \bmod p \ ,$$

and in **??** we proved $|S| \equiv 1 \bmod p$. For any $V \in F(S)$ its normalizer N_V coincides with G. As a consequence, V is a normal subgroup of G.
□
Finally, we apply Sylow's theorem to finite abelian groups.

THEOREM 7. *Let G be a finite abelian group. Then G is the direct sum of its p-Sylow-subgroups.*

Proof Let the prime factor decomposition of the order n of G be

$$n \ = \ \prod_{i=1}^{r} p_i^{m_i} \ .$$

Since G is commutative it has precisely one p_i-Sylow-subgroup U_i for each p_i $(1 \leq i \leq r)$. Writing the composition in G additively we obtain that $U := U_1 + ... + U_r$ is a subgroup of G. We show that this sum of subgroups is direct. Then its order equals the order of G and it must therefore coincide with G.
For this we put

$$\tilde{U}_i := \sum_{\substack{j=1 \\ j \neq i}} U_j$$

and demonstrate $U_i \cap \tilde{U}_i = \{0\}$ for $1 \leq i \leq r$. Every element x of that intersection has an order dividing $p_i^{m_i}$ as well as $\mid G \mid / p_i^{m_i}$. Hence, we must have $x = 0$.
□

2.36. Eigenschaften der alternierenden Gruppe A_n

2.37. Satz

Für $n \geq 3$ wird die alternierende Gruppe von 3-Zykeln erzeugt.
Speziell gilt:

$$\mathfrak{A}_n = < (1,\, 2,\, i) \mid 3 \leq i \leq n > \ .$$

Beweis:

$\mathfrak{A}_n$ besteht aus geraden Permutationen, ihre Elemente sind also Produkte jeweils einer geraden Anzahl von Transpositionen. Also gilt:

$$\mathfrak{A}_n = < (i\,j)\,(k\,l) \mid 1 \le i < j \le n,\ 1 \le k < l \le n > .$$

Die erzeugenden Elemente hierin sind nun Produkte von 3-Zyklen:

(i) $\sharp\{i,j,k,l\} = 2 \ \Rightarrow$ (eventuelles Umnumerieren) $k = i,\ l = j$, also

$$(i,\,j)\,(i,\,j) = \mathrm{id} = (1,\,2,\,3)^3;$$

(ii) $\sharp\{i,j,k,l\} = 3 \ \Rightarrow\ j = k,\ i \neq l$:

$$(i,\,j)\,(j,\,l) = (i,\,j,\,l),$$

(iii) $\sharp\{i,j,k,l\} = 4$:

$$\begin{aligned}(i,\,j)\,(k,\,l) &= ((i,\,j)\,(j,\,k))\,((j,\,k)\,(k,\,l)) \\ &= (i,\,j,\,k)\,(j,\,k,\,l).\end{aligned}$$

Schließlich:

$$(i,\,j,\,k) = (2,\,k,\,i)\,(2,\,i,\,j)$$

und

$$\begin{aligned}(2,\,i,\,j) &= (1,\,j,\,2)\,(1,\,2,\,i) \\ &= (1,\,2,\,j)^2\,(1,\,2,\,i).\end{aligned}$$

□

Beispiel:

$$A_3 = \{(1,\,2,\,3)^k \mid k = 0,\,1,\,2\}, \quad A_2 = \{\mathrm{id}\}.$$

2.38. Hilfssatz

Für $n \ge 5$ sind alle 3-Zyklen von $\mathfrak{A}_n$ konjugiert.

Beweis:
Wir zeigen: Zu (i,j,k) und $(1,2,3)$ existiert $\pi \in \mathfrak{A}_n$ mit

$$\pi\,(1,\,2,\,3)\,\pi^{-1} = (i,\,j,\,k).$$

Wegen $n \ge 5$ existieren $l,\,m \in \mathbb{N}_n$ mit $\sharp\{i,j,k,l,m\} = 5$. Eine der Permutationen

$$\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & \dots & n \\ i & j & k & l & m & \dots & \end{pmatrix} \quad \text{oder} \quad (l,\,m)\,\tau$$

liegt dann in $\mathfrak{A}_5$. Nun gilt:

$$\begin{aligned}\tau\,(1,\,2,\,3)\,\tau^{-1} &= (\tau\,(1),\,\tau\,(2),\,\tau\,(3)) \\ &= (i,\,j,\,k) \\ &= (l,\,m)\,\tau\,(1,\,2,\,3)\,\tau^{-1}(l,\,m).\end{aligned}$$

□

2.39. Satz

Für $n \geq 5$ ist $\mathfrak{A}_n$ einfach.

Bemerkung:
Dies hat weitreichende Konsequenzen. Speziell gilt für

$$p \left| \frac{n!}{2} \quad (n \geq 5) \right.$$

stets, daß mehrere p-Sylow-Untergruppen von $\mathfrak{A}_n$ existieren.

Beweis:
Es sei $N \neq <\mathrm{id}>$ Normalteiler von $\mathfrak{A}_n$ und $n \geq 5$.
Infolge der Vorarbeiten genügt es zu zeigen, dass N einen 3-Zyklus enthält, da dann bereits $N = \mathfrak{A}_n$ folgt.

Dazu sei $\pi \in N,\ \pi \neq \mathrm{id}$, in eindeutiger Darstellung als Produkt elementfremder Zykeln gegeben.

1. Fall:
Es tritt ein r-Zyklus $(i, j, k, l, \ldots)$ mit $r \geq 4$ auf. Für $\tau = (i, j, k)$ liegt dann $\pi\,(\tau\,\pi^{-1}\tau^{-1})$ ebenfalls in N.

$$\begin{aligned} N \ni\ & \pi\,(\tau\,\pi^{-1}\tau^{-1}) \\ & = (i,\ j,\ k,\ l,\ \ldots)\,(\ldots,\ \tau\,(l),\ \tau,\ (k),\ \tau\,(j),\ \tau\,(i)) \\ & = (i,\ j,\ k,\ l,\ \ldots, u)\,(u, \ldots,\ l,\ i,\ k,\ j) \\ & = (i,\ l,\ j) \end{aligned}$$

$\pi\,(\tau\,\pi^{-1}\tau^{-1})$ hat keinen Effekt außerhalb des r-Zykels $(i, j, k, l, \ldots)$.

2. Fall:
In der Faktorisierung von π tritt mindestens ein 3-Zyklus auf. Bei mehreren Faktoren gilt also

$$\pi = (i,\ j,\ k)\,(l,\ m,\ ?)\ \ldots.$$

Setze $\tau = (i, j, l)$ und bilde

$$\begin{aligned} & \pi\,(\tau\,\pi^{-1}\tau^{-1}) \\ & = (i,\ j,\ k)\,(l,\ m,\ ?)\ \ldots\ \ldots\,\tau(k,\ j,\ i)\,(?,\ m,\ l)\,\tau^{-1} \\ & = (i,\ j,\ k)(l,\ m,\ ?)(k,\ l,\ j)(?^{-1},\ m,\ i) \\ & = (i,\ l,\ k,\ m,\ j)\ \in N, \end{aligned}$$

dann weiter mit Fall 1.

3. Fall:
π Produkt elementfremder Transpositionen,
$\pi = (i, j)\,(k, l)\ldots,\ \exists m \in \mathbb{N}_n \backslash \{i, j, k, l\}$.
Setze $\tau = (i, k, m)$ und bilde

$$\begin{aligned} \pi\,(\tau\,\pi^{-1}\tau^{-1}) &= (\pi\,\tau\,\pi^{-1})\tau^{-1} \\ &= (j,\ l,\ \pi\,(m))\,(m,\ k,\ i)\,, \end{aligned}$$

dann weiter mit Fall 2 .

□

2.40. Definition

Eine endliche Gruppe G heißt auflösbar, falls eine Kette von Untergruppen

$$G = G_0 \supset G_1 \supset G_2 \supset \ldots \supset G_n = \{e\}$$

existiert, so daß $G_{i+1} \lhd G_i$ gilt und G_i/G_{i+1} abelsch ist $(1 \leq i < n)$.

Bemerkung:

(i) Existiert eine Kette von Untergruppen

$$G = G_0 \supseteq G_1 \supseteq G_2 \supseteq \ldots \supseteq G_n = \{e\}$$

mit $G_{i+1} \lhd G_i$ und G_i/G_{i+1} abelsch $(0 \leq i < n)$, dann ist G auflösbar.

(ii) Eine solche Untergruppenkette heißt Normalreihe.

Beispiel:
$\mathfrak{S}_3 = G_0 \supset G_1 = \mathfrak{A}_3 \supset \{e\} = G_2$;
$D_n = G_0 \supset G_1 =< b > \supset \{e\} = G_2$;
G abelsch $G = G_0 \supset G_1 = \{e\}$;
$\mathfrak{S}_4 = G_0 \supset G_1 = \mathfrak{A}_4 \supset G_2 = \mathfrak{V}_4 \supset \{e\} = G_3$.

2.41. Hilfssatz

(i) Jede endliche abelsche Gruppe ist auflösbar mit zyklischen Faktorgruppen.

(ii) Eine endliche Gruppe ist genau dann auflösbar, falls eine Untergruppenkette

$$G = G_0 \supset G_1 \supset \ldots \supset G_n = \{e\} \text{ mit } G_{i+1} \lhd G_i$$

und G_i/G_{i+1} zyklisch existiert.

Beweis:

(i) Induktion über $m = (G : 1)$. $m = 1$ ist trivial. Sei also $m > 1$. Ist G selbst zyklisch, so ist nichts zu zeigen. Andernfalls sei $H =< x >$ zyklische Untergruppe von G mit $x \neq \{e\}$. Nach Induktionsvoraussetzung ist dann G/H auflösbar mit zyklischen Faktorgruppen, d.h. es existierten Untergruppe G_i/H $(0 \leq i \leq r)$, $G_0 = G$, $G_r = H$ mit

$$G_i/H \Big/ G_{i+1}/H \cong G_i/G_{i+1}$$

zyklisch. Dann leistet

$$G = G_0 \supset G_1 \supset \ldots \supset G_{r-1} \supset G_r = H \supset \{e\}$$

das gewünschte. (Anderer Beweis direkt mittels (1.25).)

(ii) $\Leftarrow$ klar nach Definition.
$\Rightarrow$ gemäß (i).
G_i/G_{i+1} ist abelsch, falls nicht zyklisch.

$$G_{i_0} = G_i/G_{i+1} \supset \overline{G}_{i_1} \supset \ldots \supset \overline{G}_{i_k} = G_{i+1}$$

mit zyklischer Faktorgruppe

$$\overline{G}_{i_\nu} = G_{i_\nu}/G_{i+1};$$

verfeinere alte Normalreihe mittels

$$G_i = G_{i_0} \supset G_{i_1} \supset \ldots \supset G_{i_{k_i}} = G_{i+1},$$

$$G_{i_\nu}\Big/G_{i_{\nu+1}} \cong \overline{G}_{i_\nu}\Big/G_{i_{\nu+1}}$$

zyklisch.

□

2.42. Hilfssatz

Es sei G eine endliche Gruppe mit Untergruppe H.

(i) Ist G auflösbar, so auch H und im Fall $H \lhd G$ und H auflösbar ist auch G/H auflösbar.
(ii) Ist H Normalteiler und sind H sowie G/H auflösbar, dann ist auch G auflösbar.

Beweis:

(i) Es sei

$$G = G_0 \supset G_1 \supset G_2 \supset \ldots \supset G_n = \{e\}$$

(Normalreihe von G) mit $G_{i+1} \lhd G_i$, G_i/G_{i+1} abelsch. Bilde

$$H_i := G_i \cap H \quad (0 \leq i \leq n).$$

$H_{i+1} \lhd H_i$: Für $x \in H_i$ gilt:

$$x\,H_{i+1}x^{-1} \subseteq x\,G_{i+1}x^{-1} \cap x\,H\,x^{-1} = G_{i+1} \cap H = H_{i+1}.$$

$$H_i/H_{i+1} = H_i/H_i \cap G_{i+1} \overset{(1.20)}{\cong} H_iG_{i+1}/G_{i+1} < G_i/G_{i+1}.$$

Gilt außerdem $H \lhd G$, so bilde mittels $\tilde{G}_i := G_iH < G$ $(0 \leq i \leq n)$ Kette

$$\tilde{G}_0/H \supseteq \tilde{G}_1/H \supseteq \ldots \supset \tilde{G}_n/H = H$$

(Untergruppenkette von G/H). Betrachte Abbildung

$$\varphi : \tilde{G}_i \to G_i/G_{i+1} \ : \ g_u h \mapsto g_i\,G_{i+1}$$

surjektiv. φ ist Homomorphismus:

$$\begin{array}{rcl} \varphi\,(g_iH)\,\varphi\,(\tilde{g}_i\tilde{h}) & = & (g_i\,G_{i+1})\,\tilde{g}_i\,G_{i+1}) \\ & \overset{G_{i+1}\lhd G_i}{=} & g_i\tilde{g}_i\,G_{i+1} \\ & = & \varphi\,(g_i\tilde{g}_ih^k) \\ & = & \varphi\,(g_ih\,\tilde{g}_i\tilde{h}) \end{array}$$

da $k \in H$ beliebig, φ surjektivität ist klar,

$$\ker\varphi = \{g_ih \in \tilde{G}_i \mid g_i \in G_{i+1}\} = G_{i+1}H = \tilde{G}_{i+1}.$$

Also gilt: $\tilde{G}_{i+1} \lhd \tilde{G}_i$ und

$$\tilde{G}_i/\tilde{G}_{i+1} \cong G_i/G_{i+1},$$

also abelsch. Wende nun (1.21) an:

$$(\tilde{G}_i/H)\,\Big/\,(\tilde{G}_{i+1}/H) \cong \tilde{G}_i/\tilde{G}_{i+1}.$$

(ii) H auflösbar:

$$H = H_0 \supset H_1 \supset \ldots \supset H_r = \{e\}$$

mit H_i/H_{i+1} abelsch. G/H auflösbar:

$$G = G_0 \supset G_1 \supset \ldots \supset G_s = H$$

von G mit

$$(G_i/H)\,\Big/\,(G_{i+1}/H) \overset{(1.21)}{\cong} G_i/G_{i+1}$$

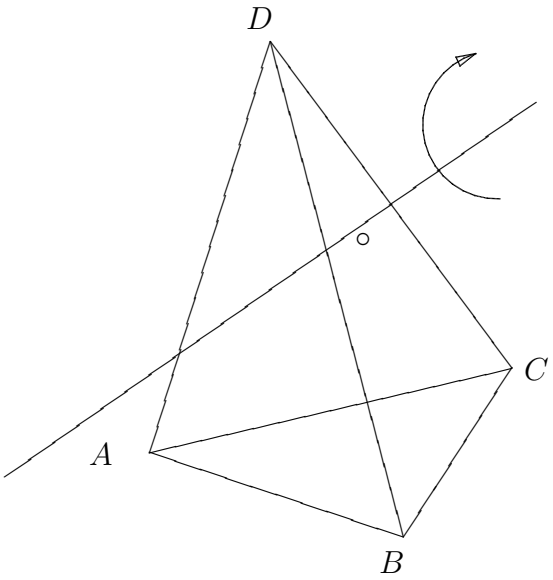
abelsch. Also ist

$$G = G_0 \supset G_1 \supset \ldots \supset G_s = H = H_0 \supset H_1 \supset \ldots \supset H_r = \{e\},$$

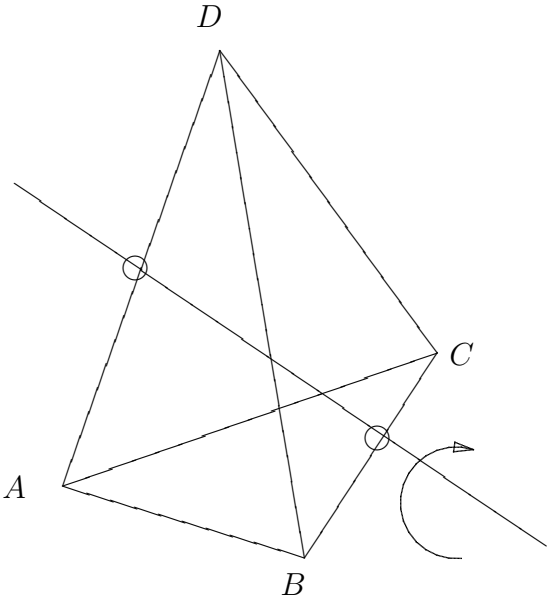
d.h. G auflösbar.

□

Bemerkung: Für $n \geq 5$ ist $\mathfrak{S}_n$ nicht auflösbar, da A_n für $n \geq 5$ nach (1.53) nicht auflösbar ist.



Tetraedergruppe: ($\cong \mathfrak{A}_4$)
Drehungen um Achse durch Eckpunkt und Mittelpunkt der gegenüberliegenden Fläche eines Tetraeders
um A : $(B\,C\,D)$, $(B\,D\,C)$
um B : $(A\,C\,D)$, $(A\,D\,C)$
um C : $(A\,B\,D)$, $(A\,B\,D)$
um D : $(A\,B\,C)$, $(A\,C\,B)$
Und deren Kombinationen: Drehungen um Achsen die durch die Mit-



telpunkte von gegenüberligenden Seiten gehen:

$A \leftrightarrow C,\ B \leftrightarrow D$ $(A\,C)\,(B\,D)$
$A \leftrightarrow D,\ B \leftrightarrow C$ $(A\,D)\,(B\,C)$
$A \leftrightarrow B,\ C \leftrightarrow D$ $(A\,B)\,(C\,D)$
sowie die Identität.

2.43. Hilfssatz

Für $n \in \mathbb{N}$ ist $\mathfrak{S}_{n+1}$ disjunkte Zerlegung von $n+1$ (Links-)Nebenklassen nach $\mathfrak{S}_n$.

$$\left(\iota : \mathfrak{S}_n \to \mathfrak{S}_{n+1} : \begin{pmatrix} 1 & 2 & \dots & n \\ \pi(1) & \pi(2) & \dots & \pi(n) \end{pmatrix} \mapsto \begin{pmatrix} 1 & \dots & n & n+1 \\ \pi(1) & \dots & \pi(n) & \pi(n+1) \end{pmatrix}\right)$$

Beweis:
Setze $\pi(n+1) = \mathrm{id}$ und $\pi(\nu) = (\nu,\, n+1)$ $(1 \le \nu \le n)$. Wir zeigen:

$$\mathfrak{S}_{n+1} = \bigcup_{\nu=1}^{n+1} \pi_\nu \, \mathfrak{S}_n.$$

Sei dazu $\tau \in \mathfrak{S}_{n+1}$ mit $\tau(n+1) = j$. Für $j = n+1$ gilt $\tau \in \pi_{n+1}\,\mathfrak{S}_n$. Andernfalls bildet $(j,\, n+1)\,\tau$ das Element $n+1$ auf sich ab, also ist

$$(j,\, n+1)\,\tau \in \pi_{n+1}\,\mathfrak{S}_n \quad \text{und} \quad \tau \in (j,\, n+1)\,\pi_{n+1}\,\mathfrak{S}_n = (j,\, n+1)\,\mathfrak{S}_n.$$

Wir zeigen noch, daß die Zerlegung disjunkt ist, obwohl dies bereits aus den Elementanzahlen folgt.

$$\begin{aligned} \pi_\nu\,\mathfrak{S}_n = \pi_\mu\,\mathfrak{S}_n \quad &\Leftrightarrow \quad \pi_\mu\pi_\nu\,\mathfrak{S}_n = \mathfrak{S}_n \\ &\Rightarrow \quad \pi_\mu\pi_\nu(n+1) = n+1 \\ &\Rightarrow \quad \pi_\nu(n+1) = \pi_\mu(n+1) \\ &\Leftrightarrow \quad \nu = \mu. \end{aligned}$$

□

Bemerkung: Dies ist ein weiterer Beweis für $\sharp\mathfrak{S}_n = n!$

(i) Das direkte Produkt zyklischer Gruppen mit teilerfremden Ordnungen ist zyklisch.

(ii) Ist G zyklisch mit $(G:1) = m\,n$ und $\mathrm{ggT}\,(m,\,n) = 1$, so gilt

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

(iii) Jede endliche abelsche Gruppe ist direktes Produkt zyklischer Gruppen.

Beweis:

(i) Es sei $G = Z_1 \times Z_2$ mit $Z_1 =< a >,\ Z_2 =< b >,\ |Z_1| = m,\ |Z_2| = n$ und $\mathrm{ggT}\,(m,\,n) = 1$.
Offenbar gilt

$$G = \{(a^\nu,\, b^\mu) \mid o \le \nu < m,\ 0 \le \mu < n\} \text{ mit } a_m = e_1,\ b^n = e_2.$$

Zeige: $\mathrm{ord}((a,\,b)) = m\,n$.
$m\,n$ ist Exponent von $(a,\,b)$ wegen

$$\begin{aligned}(a,\,b)^{mn} &= (a^{mn},\,b^{mn})\\ &= ((a^m)^n,\,(b^n)^m) = (e_1, e_2).\end{aligned}$$

Für jeden Exponent k von $(a,\,b)$ muß auch $a^k = e,\ b^k = e$ gelten, d.h. $m|k$ und $n|k$, folglich $mn|k$.

(ii) Für $G_1 = \mathbb{Z}/m\mathbb{Z},\ G_2 = \mathbb{Z}/n\mathbb{Z}$ ist $G_1 \times G_2$ zyklisch von der Ordnung $m\,n$. Also sind sowohl G als auch $G_1 \times G_2$ isomorph zu $\mathbb{Z}/m\,n\mathbb{Z}$ und damit untereinander isomorph.

Beispiele:

$$\begin{aligned}\mathbb{Z}/6\mathbb{Z} &\cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z};\\ \mathbb{Z}/4\mathbb{Z} &\cong < e > \times \mathbb{Z}/4\mathbb{Z};\\ \mathbb{Z}/2\mathbb{Z} \times \mathfrak{V}_4 &\cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z};\\ \mathbb{Z}/8\mathbb{Z} &\ncong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}\\ &\ncong \mathbb{Z}/2\mathbb{Z} \times \mathfrak{V}_4,\end{aligned}$$

denn nur $\mathbb{Z}/8\mathbb{Z}$ enthält ein Element der Ordnung 8, die letzte Gruppe keins der Ordnung 4.

(iii) Es sei $a_1, \ldots, a_r$ ein Erzeugendensystem für die endliche abelsche Gruppe G, d.h. $G =< a_1, \ldots, a_r >$. Der Beweis wird mittels Induktion über r geführt.

$r = 1$: G ist selbst zyklisch, und es ist nichts zu beweisen.

$r \ge 2$:
Man bilde

$$\mathfrak{M} = \{\,\underline{m} \in (\mathbb{Z}^{\ge 0})^r \mid a_1^{m_1} \cdot \ldots \cdot a_r^{m_r} = e \text{ und } 0 \le m_i < (G:1),\ 1 \le i \le r\}.$$

Für $\mathfrak{M} = \{\,\underline{0}\,\}$ ist G das direkte Produkt von den $< a_i >$ $(1 \le i \le r)$, denn die Schnittbedingung $N_i \cap \tilde{N}_i = \{e\}$ ist erfüllt!

Sei also $\mathfrak{M} \neq \{\underline{0}\}$. Wähle $\underline{n} \in \mathfrak{M}$, welches die kleinste positive Koordinate aller $\underline{m} \in \mathfrak{M}$ enthält. O.B.d.A. (evtl. umnummerieren) sei diese n_1. Für $n_1 = 1$ ist

$$a_1 = \prod_{i=2}^{r} a_i^{-n_i} \ \in < a_1, \ldots, a_r >,$$

d.h. $G =< a_2, \ldots, a_r >$, und wir können die Induktionsvoraussetzung anwenden.

Sei also $n_1 > 1$. Für jedes weitere $\underline{m} \in \mathfrak{M}$, $\underline{m} \neq \underline{0}$, folgt

$$\prod_{i=1}^{r} a_i^{m_i - Q(m_i, n_1)\, n_1} = e,$$

und wegen der Minimalität von $\underline{n}$, damit $R(m_1,\, n_1) = 0$, d.h. wir können $\mathfrak{M}$ ersetzen durch die Teilmenge $\mathfrak{M}$ bestehend aus $\underline{0}$, $\underline{n}$ und allen $\underline{m} \in \mathfrak{M}$ mit erster Koordinate 0.

Nunmehr setzen wir

$$x_1 := a_1 \prod_{i=2}^{r} a_i^{Q(n_i, n_1)}$$

und erhalten

(a) $G =< x_1, a_2, \ldots, a_r >$,

(b) $x_1^{n_1} \prod_{i=2}^{r} a_i^{R(n_i, n_1)} = e$.

Hierin gilt $0 \leq R(n_i,\, n_1) < n_1 \ \ (2 \leq i \leq r)$. Wir wiederholen folglich diesen Prozeß mit $x_1, a_2, \ldots, a_r$ an Stelle von $a_1, \ldots, a_r$. Nach höchstens r-maliger Anwendung führt dies (im ungünstigsten Fall) auf ein Erzeugendensystem $z_1, \ldots, z_r$ mit

$$z_1^{k_1} \prod_{i=2}^{r} z_i^{R(k_i, k_1)} = e \quad \text{und} \quad R(k_i,\, k_1) = 0 \ \ (1 \leq i \leq r).$$

Hierfür ist dann $G =< z_1 > \ \times \ < z_2, \ldots, z_r >$, und wir können wieder die Induktionsvorraussetzung anwenden.

□

2.44. Definition

Es sei G eine Gruppe und S eine nicht leere Menge. Man sagt, daß G auf S operiert (S eine G-Menge ist), falls eine äußere Verknüpfung

$$G \times S \to S \ : \ (g,\, s) \mapsto g \circ s$$

besteht mit

(i) $(g\,h) \circ s = g \circ (h \circ s) \ \ \forall g,\, h \in G,\ \forall s \in S$,

(ii) $e \circ s = s \ \ \forall s \in S$, e Einselement von G.

Beispiele:

(i) (a) G Gruppe, $S \lhd G$ und $G \times S \to S \ : \ (g,\, h) \mapsto ghg^{-1}$.

Hierfür ist $(g_1 g_2,\, h) \mapsto (g_1 g_2)\, h\, (g_1 g_2)^{-1}$ sowie

$$\begin{aligned} g_1 \cdot (g_2 \cdot h) &= g_1 \cdot (g_2 h g_2^{-1}) \\ &= g_1 g_2\, h\, g_2^{-1} g_1^{-1} \text{ und } e \cdot h = h. \end{aligned}$$

(b) $S = M \leq G$ und

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

(ii) (a) $S = \mathbb{R}^n,\ G = (\mathbb{R}, +),\ \underline{u} \in \mathbb{R}^n$ fest und

$$\mathbb{R} \times \mathbb{R}^n \to \mathbb{R}^n \ : \ (s,\, \underline{x}) \mapsto \underline{x} + s\, \underline{u}.$$

(b) $S = \mathbb{R}^n,\ G \leq \mathrm{GL}_n(\mathbb{R})$ mit

$$(A,\, v) \mapsto A\,(v)$$

(iii) $S = \mathbb{R}^2,\ G = \mathbb{Z} \times \mathbb{Z}$ mit

$$G \times \mathbb{R}^2 \to \mathbb{R}^2 \ : \ \left(m,\, n,\, \begin{pmatrix} x \\ y \end{pmatrix}\right) \mapsto \begin{pmatrix} x+m \\ y+n \end{pmatrix}.$$

2.45. Satz

Jede endliche Gruppe G ist isomorph zu einer Permutationsgruppe.
Insbesondere: Ist $|G| = n$, dann ist G isomorph zu einer Untergruppe von $\mathfrak{S}_n$.

Beweis:
$\mathfrak{S}(G)$ bezeichne die Gruppe der bijektiven Abbildungen von G (als Menge) bzgl. Hintereinanderausführung (sog. symmetrische Gruppe, Permutationsgruppe von G). (Für $|G| = n \in \mathbb{N}$ schreibt man kurz $\mathfrak{S}_n$.)
Bilde ab:

$$\varphi \ : \ G \to \mathfrak{S}(G) \ : \ g \mapsto \mathfrak{S} = g\circ,$$

denn

$$\mathfrak{S} \ : \ G \to G \ : \ x \mapsto gx$$

ist bijektive Abbildung von G. φ ist Homomorphismus:

$$gh \mapsto gh\circ = g \circ h\circ,$$

φ ist injektiv

$$\varphi(g) = \mathrm{id} \quad \Rightarrow \quad gx = x \text{ für alle } x \in G \quad \Rightarrow \quad g = e,$$

also gilt mit (1.18):

$$G \cong \varphi(G) < \mathfrak{S}(G).$$

□

Bemerkung:
S G-Menge $\Leftrightarrow$ es existiert ein Homomorphismus $\varphi : G \to \mathfrak{S}(S)$.

Beweis:
"$\Rightarrow$":
Definiere

$$\varphi : G \to \mathfrak{S}(S) : g \mapsto g \circ .$$

Es ist zu zeigen:

$$g\circ : S \to S : x \mapsto gx \text{ ist Bijektion von } S.$$

$g\circ$ ist surjektiv: Urbild von $x \in S$ ist $g^{-1}x$ (wegen $e\,x = x$).
$g\circ$ ist injektiv: $\quad gx = gy \quad \Rightarrow \quad e\,x = e\,y \quad \Rightarrow \quad x = y.$
φ ist Homomorphismus wegen 1.26(i).
"$\Leftarrow$":
Es sei ein Homomorphismus

$$\varphi : G \to \mathfrak{S}(S) : g \mapsto \psi_g$$

gegeben. Definiere äußere Verküpfung

$$G \times S \to S : (g,\, s) \mapsto \psi_g(s) =: g \circ s.$$

Nachweis von (i) und (ii) aus (1.26):
φ Homomorphismus $\Rightarrow$

$$\varphi(e_G) = \mathrm{id}_s \quad \Rightarrow \quad e \circ s = \mathrm{id}_S(s) = s \ \forall s \in S.$$

ψ Homomorphismus $\Rightarrow$

$$\begin{aligned} \psi_{gh} &= \varphi(gh) \\ &= \varphi(g)\,\varphi(h) \\ &= \psi_g\,\psi_h, \end{aligned}$$

also

$$\begin{aligned} (gh) \circ s &= \psi_{gh}(s) \\ &= \psi_g(\psi_h(s)) \\ &= g \circ (h \circ s). \end{aligned}$$

□

2.46. Hilfssatz

Es sei S eine G-Menge. Dann ist

$$x \sim y \quad :\Leftrightarrow \quad \exists g \in G : g \circ s = y$$

eine Äquivalenzrelation auf S.

Beweis:
$\sim$ reflexiv:

$$e \circ x = x \quad \forall x \in S, \text{ setze } g = e;$$

$\sim$ symmetrisch:

$$\begin{aligned} g \circ x = y \quad &\Rightarrow \quad x = e \circ x = g^{-1} \circ (g \circ x) = g^{-1} \circ y \\ &\Rightarrow \quad y \sim x; \end{aligned}$$

$\sim$ transitiv:

$$g \circ x = y \text{ und } h \circ y = z \quad \Rightarrow \quad z = h \circ (g \circ x) = (hg) \circ x.$$

□

Bemerkung:
$x \in S$ so ist die durch x bestimmte Äquvalenzklasse

$$G \cdot x = \{g \cdot x \mid g \in G\}.$$

2.47. Definition

Die Äquvialenzklassen in (1.28) heißen Bahnen (Orbits) von S. G heißt transitiv (über S), falls es genau eine Bahn in S gibt. Für $s \in S$ heißt

$$\mathrm{Stab}(s) = G_s := \{g \in G \mid g \circ s = s\}$$

Stabilisator von s.

Beispiel:
$G = (\mathbb{R}, +),\ X = \mathbb{R}^n,\ g \cdot \underline{x} \in X$ für $\underline{x} \in X,\ g \in G$.
Stabilisator von $x \in X\ :\ G_x = \{g \in G \mid gx = x\}$.

Bemerkungen:

(i) Bahn von $s \in S$ ist $G \circ s := \{g \circ s \mid g \in G\} =: \mathrm{Orb}(s)$.
G transitiv über $S \Leftrightarrow \forall x, y \in S\ \exists g \in G\ :\ y = g \circ x$.

(ii) G_s ist Untergruppe von G, und es gilt $|G \circ s| = (G : G_s)$.
Ist also G endlich, so teilt jede Bahnlänge die Gruppenordnung.

Beweis:
$e \in G_s$, also $G_s \neq \emptyset$. Sind $g,\ h \in G_s$, so ist $h^{-1} \in G_s$ wegen

$$s = h \circ s \quad \Leftrightarrow \quad h^{-1} \circ s = h^{-1}h \circ s = e \circ s = s$$

und folglich

$$(gh^{-1}) \circ s = g \circ (h^{-1} \circ s) = g \circ s = s,$$

also auch $gh^{-1} \in G_s,\ g\,G_s = h\,G_s$. Demnach ist G_s Untergruppe von G.
Betrachte Abbildung

$$\varphi\ :\ G \circ s \to \{g\,G_s \mid g \in G\}\ :\ g \circ s \mapsto g\,G_s.$$

φ ist offensichtlich surjektiv. Zur Wohldefiniertheit und Injektivität von φ:

$$g\,G_s = h\,G_s \quad \Leftrightarrow \quad h^{-1}g \in G_s \quad \Leftrightarrow \quad h^{-1}g \circ s = s \quad \Leftrightarrow \quad g \circ s = h \circ s.$$

□

(iii) s, $\tilde{s}$ Elemente derselben Bahn, dann gehen ihre Stabilisatoren durch einen inneren Automorphismus auseinander hervor. (Solche Untergruppen heißen konjugiert.)

Beweis:
Sei $g \in G$ mit $\tilde{s} = g \circ s$. Dann ist

$$\begin{aligned} G_{\tilde{s}} &= \{h \in G \mid h \circ \tilde{s} = \tilde{s}\} \\ &= \{h \in G \mid h\, g \circ s = g \circ s\} \\ &= \{h \in G \mid (g^{-1}hg) \circ s = s\} \\ &= \{ghg^{-1} \in G \mid h \circ s = s\} \\ &= g\,\{h \in G \mid h \circ s = s\}\, g^{-1} \\ &= g\, G_s g^{-1}. \end{aligned}$$

□

Zur Zerlegung von S in Bahnen:
Wähle Teilmenge V von S mit

$$S = \dot{\bigcup_{v \in V}} G \circ v,$$

sog. Vertretersystem für die Bahnen. Ein Vertretersystem ist also durch folgende beiden Eigenschaften gekennzeichnet:

(i) $\forall x \in S \;\; \exists v \in V \;:\; G \circ v = G \circ x$,
(ii) $\forall u, v \in V \;:\; u \neq v \;\Rightarrow\; G \circ u \cap G \circ v = \emptyset$.

(Beachte: $G \circ u \cap G \circ v$ ist entweder leer oder ganz $G \circ u$ entsprechend der Eigenschaft von Äquivalenzklassen. Ein Element $s \in S$ heißt Fixpunkt, falls $G \circ s = \{s\}$ ist. Dies ist gleichbedeutend damit, daß s in jedem Vertretersystem V vorkommt bzw. mit $G_s = G$.)

Die Menge aller Fixpunkte von S schreiben wir $F(S)$ und erhalten

$$|S| = |F(S)| + \sum_{\substack{s \in V \\ (G:G_s) > 1}} (G : G_s).$$

Hierin ist die Summe eventuell leer.

Ist speziell $|G|$ Potenz einer Primzahl, etwa p^m $(m \in \mathbb{N})$, so gilt:

$$|S| \equiv |F(S)| \bmod p$$

sowie

$$|S| = h\,p + R\,(|S|,\, p) \text{ mit } 0 \leq R\,(|S|,\, p) \leq p - 1.$$

(Für $|S| \not\equiv 0 \bmod p$ besitzt S mindestens $R\,(|S|,\, p)$ Fixpunkte.)

Im folgenden sei G eine Gruppe und $\emptyset \neq T \subseteq G$.
Wir setzen $S := \{\tilde{T} = gTg^{-1} \mid g \in G\}$ und definieren als Operation von G auf S:

$$G \times S \to S \ : \ (h, \tilde{T}) \mapsto h\tilde{T}h^{-1}.$$

Offenbar operiert G transitiv auf S, es gibt nur eine Bahn, nämlich S selber.

1. Behauptung: $G_T = N_T$

Beweis:

$$N_T = \{g \in G \mid gTg^{-1} = T\} = G_T.$$

Also ist $|S| = (G : N_T)$. Insbesondere für $T = U < G$ gibt es genau $(G : N_U)$ verschiedene konjugierte von U.

2. Behauptung: Für $U < G$ ist

$$|\{gUg^{-1} \mid g \in G\}| = (G : N_U).$$

Man kann G auch direkt auf den Elementen von G operieren lassen mittels sog. Konjugation:

$$G \times G \to G \ : \ (h, g) \mapsto hgh^{-1}.$$

Die diesbezüglichen Bahnen heißen Klassen konjugierter Elemente. Hier ist offensichtlich $G_x = N_x \ \forall x \in G$. Überdies gilt:

$$F(G) = \{x \in G \mid gxg^{-1} = x \text{ für alle } g \in G\} = Z(G).$$

Damit erhält man die wichtige Klassengleichung:

2.48. Klassengleichung

$$|G| = |Z(G)| + \sum_{\substack{x \in V \\ (G:N_x)>1}} (G : N_x)$$

für ein Vertretersystem V der Konjugationsklassen.

Ein weiterer Trick:
Operiert G auf X, so auch auf der Potenzmenge $\mathcal{P}(X)$ von X. Ist $Y \subseteq X$, so setze $g \cdot Y = \{g \cdot y \mid y \in Y\}$.

2.49. Definition

Eine endliche Gruppe G heißt p-Gruppe, falls $(G : 1) = p^r$ mit einer Primzahl p und $r \in \mathbb{N}$ gilt.

2.50. Satz

(i) Das Zentrum einer p-Gruppe ist nicht trivial.
(ii) Ist G eine p-Gruppe mit $|G| = p^2$, so ist G zyklisch oder das direkte Produkt zweier zyklischen Gruppen der Ordnung p.

$$\left(\begin{array}{lcl} G & \cong & \mathbb{Z}/p^2\mathbb{Z} \\ G & \cong & \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z} \end{array} \right)$$

Beweis:

(i) Gemäß (1.30) und dem Satz von Lagrange ist $|Z(G)| = p^k$ für ein k mit $1 \leq k \leq r$.

$$|G| = p^r = |Z(G)| + \sum_{i=1}^{r} p^{r_i} \text{ mit } 1 \ \leq r_i$$

$\Rightarrow \ p| \, |Z(G)|$, denn wegen $e \in Z(G) \ \Rightarrow \ |Z(G)| > 1.$)

(ii) Vorbemerkung: Ist $Z(G) \subset G$, so ist $G/Z(G)$ nicht zyklisch.

Indirekt!
Es sei

$$G/Z(G) = \dot{\bigcup}_{\nu \in \mathbb{Z}} \, (a \, Z(G))^{\nu} = \dot{\bigcup}_{\nu \in \mathbb{Z}} \, a^{\nu} \, Z(G).$$

Dann existieren für $g_1, \ g_2 \in G$ Elemente $\nu_i \in \mathbb{Z}, \ b_i \in Z(G)$ mit $g_i = a^{\nu_i} \ b_i \ \ (i = 1, \, 2)$. Also gilt

$$\begin{aligned} g_1 g_2 &= a^{\nu_1} b_1 \, a^{\nu_2} b_2 \\ &= a^{\nu_1 + \nu_2} b_1 b_2 \\ &= a^{\nu_2} a^{\nu_1} b_2 b_1 \\ &= a^{\nu_2} b_2 \, a^{\nu_1} b_1 \\ &= g_2 g_1, \end{aligned}$$

d.h. G ist abelsch im Widerspruch zu $Z(G) \neq G$.

Nach (i) ist demnach G mit $|G| = p^2$ abelsch, denn die einzige Möglichkeit $|Z(G)| = p$ liefert $|G/Z(G)| = p$, d.h. $G/Z(G)$ ist zyklisch. Wende (1.25)(iii) an!

□

Beispiel: Es gibt als Gruppen der Ordnung 4 die zyklische Gruppe und die V_4.

Im folgenden wird die Existenz von gewissen Untergruppen bei endlichen Gruppen mit Hilfe der Sylowschen Sätze bewiesen.

2.51. Definition

Es sei G eine endliche Gruppe. Eine Untergruppe H von G heißt p-Untergruppe von G, falls H eine p-Gruppe ist. H heißt p-Sylow-Untergruppe von G, falls $(H:1)=p^l \ (l\in\mathbb{N},\ p\in\mathbb{P})$ mit $p^l|\,|G|$ mit $p^{l+1}\nmid |G|$ gilt. (Schreibweise: $p^l \,\|\, |G|$)

Beispiel: G sei Gruppe der Ordnung $p^l m$ mit $p\nmid m$.

(i) $p=2,\ l=3,\ m=1\ :$ G selbst ist p-Sylow-Untergruppe.
(ii) $p=2,\ l=2,\ m=1\ :$ G selbst ist p-Sylow-Untergruppe.
Die Anzahl der Untergruppen der Ordnung 2 ist 3 oder 1.

Zum Nachweis der Existenz von Untergruppen im Fall $p|(G:1)$ benötigen wir eine Hilfsaussage aus der elementaren Zahlentheotrie:

2.52. Hilfssatz

Es seien p eine Primzahl, $l,\ n\in\mathbb{N}$ mit $p^l\|n$. Für $n=p^l m$ ist dann

$$\left(\begin{array}{c} n \\ p^\alpha \end{array}\right) = p^{l-\alpha} m x \ \ (\alpha\in\mathbb{Z}^{\geq 0},\ \alpha\leq l,\ x\in\mathbb{N}) \text{ mit } x\equiv 1 \bmod p.$$

Beweis:

$$\left(\begin{array}{c} n \\ p^\alpha \end{array}\right) = \frac{n\,(n-1)\cdot\ldots\cdot(n-(p^\alpha-1))}{p^\alpha\,(p^\alpha-1)\cdot\ldots\cdot(p^\alpha-(p^\alpha-1))} = p^{l-\alpha} m\, x$$

mit

$$x=\prod_{i=1}^{p^\alpha-1}\frac{p^l m-i}{p^\alpha-i} = \left(\begin{array}{c} n-1 \\ p^\alpha-1 \end{array}\right).$$

Jeder Index i läßt sich dabei schreiben als

$$i=p^{m_1}x_i \text{ mit } 0\leq m_i<\alpha,\ x_i\in\mathbb{N},\ p\nmid x_i.$$

Wir erhalten daher nach Kürzen von p^{m_i} für jeden Faktor
für den Zähler:

$$\prod_{i=1}^{p^\alpha-1}\left(p^{l-m_i}m-x_i\right)=\lambda\,p+a \quad (\lambda,\ a\in\mathbb{Z},\ p\nmid a),$$

für den Nenner:

$$\prod_{i=1}^{p^\alpha-1}\left(p^{\alpha-m_i}-x_i\right)=\mu\,p+a \quad (\mu\in\mathbb{Z}),$$

also $x=\dfrac{\lambda\,p+a}{\mu\,p+a}$ oder

$$a\,x\equiv a \bmod p \quad\Rightarrow\quad x\equiv 1 \bmod p.$$

□

2.53. 1. Sylowscher Satz

Es sei G eine Gruppe der Ordnung $n = p^l m$ mit $p \nmid m$ und $0 \leq \alpha \leq l$, $\alpha \in \mathbb{Z}$. Dann besitzt G eine Untergruppe U der Ordnung p^α.

Beweis:
Falls solches U existiert, so ist es sicherlich Element der Menge

$$\mathfrak{M} := \{T \subseteq G \mid |T| = p^\alpha\}.$$

$\mathfrak{M}$ enthält $\binom{n}{p^\alpha}$ Elemente. $\mathfrak{M}$ wird G-Menge mittels

$$G \times \mathfrak{M} \to \mathfrak{M} \ : \ (g, T) \mapsto gT.$$

Dabei zerfällt $\mathfrak{M}$ in Bahnen. Wäre jede Bahnlänge durch $p^{l-\alpha+1}$ teilbar, so auch $\sharp\mathfrak{M}$ im Widerspruch zu (1.34). Also existiert Bahn

$$G \circ T_1 \text{ mit } |G \circ T_1| = (G : G_{T_1}) \ \leq p^{l-\alpha} m.$$

Wegen

$$m\, p^l = (G : 1) = (G : G_{T_1})\, (G_{T_1} : 1) \leq p^{l-\alpha} m\, (G_{T_1} : 1)$$

folgt $(G_{T_1} : 1) \geq p^\alpha$. Andererseits gilt für $a \in T_1$: $G_{T_1} a \subseteq T_1$ und wegen $|G_{T_1}| = |G_{T_1} a|$ auch $|G_{T_1}| \leq |T_1| = p^\alpha$. Also ist G_{T_1} die gesuchte Untergruppe.

□

Bemerkungen:
$O(T)$ bezeichnet im folgenden die Bahn ("orbit") von T.
Nicht alle Bahnlängen sind durch $p^{l-\alpha+1}$ teilbar!

(i) $p^{l-\alpha+1} \nmid |O(T)| \ \Rightarrow \ (G_T : 1) = p^\alpha$
Denn $(G : G_T) \leq p^{l-\alpha} \ \Rightarrow \ (G_T : 1) \geq p^\alpha$.
Andererseits ist für $x \in T$ dann $G_T x \subseteq T$

$$(G_T : 1) = |G_T| = |G_T x| \leq |T| = p^\alpha,$$

also Gleichheit.

(ii) $p^{l-\alpha+1} \nmid |O(T)| \ \Leftrightarrow \ T = U_g$ mit $U \subset G$, $|U| = p^\alpha$ und passendes $g \in G$.
"$\Rightarrow$":
$G_T T = T$, d.h. für beliebiges $x \in T$ ist $G_T x \subseteq T$ bzw. $G_T x = T$ (wegen Elementanzahl) ($|G_T| = p^\alpha$ nach (i)).
"$\Leftarrow$":
Gegeben $U < G$ mit $\sharp U = p^\alpha$, $g \in G$, setze $T = U_G \in \mathfrak{M}$.

$$O(U_g) = \{hU_g \mid h \in G\} = \{\tilde{h} \underbrace{g^{-1} U_g}_{\tilde{U}} \mid \tilde{h} \in G\} = O(\tilde{U})$$

$$|\{\tilde{H} g^{-1} U_g \mid \tilde{h} \in G\}| = (G : G_{\tilde{U}}) = (G : U) = p^{l-\alpha} m.$$

2.54. Korollar (Cauchy)

Ist G eine Gruppe der Ordnung n und wird n von der Primzahl p geteilt, so besitzt G ein Element der Ordnung p.

Beweis:
Gemäß (1.35) besitzt G eine Untergruppe U mit $(U : 1) = p$. U ist dann notwendig zyklisch, und $p-1$ erzeugende Elemente von U leisten das Gewünschte.

□

2.55. Korollar

Eine endliche Gruppe G ist genau dann eine p-Gruppe, wenn für jedes $a \in G$ die Ordnung $ord(a)$ eine p-Potenz ist.

2.56. Lemma

Es sei G eine endliche Gruppe der Ordnung $n = p^l m$ mit einer Primzahl p, die m nicht teilt. Dann ist die Anzahl $N(\alpha)$ aller Untergruppen U der Ordung p^α von G $(0 \leq \alpha \leq k$ fest) kongruent 1 modulo p.

Beweis:
$N_p(\alpha) = N(\alpha) = |\{U < G \mid |U| = p^\alpha\}| \equiv 1 \bmod p$.
Dazu betrachte $T \subseteq G$ mit $|T| = p^\alpha$ und $p^{l-\alpha+1} \nmid |O(T)|$. Sei etwa $T_1 = U_1 g_1$, $T_2 = U_2 g_2$, $T_1 = T_2$?
$T_1 = T_2$ bewirkt: $g_1 \in U_2 g_2$, d.h. $g_1 = u_2 g_2$ mit $u_2 \in U_2$, also $U_1 u_2 g_2 = U_2 g_2$, also $U_1 = U_2 u_2^{-1} = U_2$.
Anzahl der Elemente in $\mathfrak{M}$, deren Bahnen durch $p^{l-\alpha+1}$ teilbar sind:
$\binom{n}{p^\alpha} - H(\alpha)\, p^{l-\alpha} m$, da alle Bahnen durch $p^{l-\alpha+1}$ teilbar sind, auch dir Elementzahl selbst.

$$\begin{aligned} p^{l-\alpha+1} \text{ teilt } p^{l-\alpha} m\,(x - N(\alpha)) &\Rightarrow\ p | m\,(x - N(\alpha)) \\ &\Rightarrow\ p |\,(x - N(\alpha)) \\ &\Rightarrow\ N(\alpha) \equiv 1 \bmod p. \end{aligned}$$

□

2.57. 2. Sylowscher Satz

Es sei G eine endliche Gruppe der Ordnung $n = p^l m$ mit einer Primzahl p, die m nicht teilt. Dann gilt:

(i) Jede p-Untergruppe von G ist in einer passenden p-Sylow-Untergruppe enthalten.
(ii) Je zwei p-Sylow-Untergruppen von G sind konjugiert.
(iii) Die Anzahl der p-Sylow-Untergruppen von G teilt m.

Bemerkung:
Für p-Sylow-Untergruppen P von G gilt:

$$P \lhd G \quad \Leftrightarrow \quad N(l) = 1.$$

Beweis:

(i) Jede p-Untergruppe ist in passender p-Sylow-Untergruppe enthalten.

Betrachte $\mathfrak{N} = \{U < G \mid |U| = p^l\}$, lasse G auf $\mathfrak{N}$ operieren.

Durch "Konjugation": $g \times \mathfrak{N} \to \mathfrak{N} \ : \ (g, U) \mapsto g^{-1}Ug$

Festes $P \in \mathfrak{N}$ hat dabei Bahnlänge $(G : G_p) \not\equiv 0 \bmod p$ (Normalisator $G_p \supseteq P$).

Sei nun $H < G$ mit $\sharp H = p^\alpha$.

H operiert auf den Elementen der Bahn von P unter Konjugation.

$$(o(p) = \{g^{-1}Pg \mid; g \in G\} \supseteq \{h^{-1}Ph \mid h \in H\})$$

$$p \nmid |O(P)| = \sum_{v \in V} (H : H_v) \quad (p\text{-Potenzen})$$

$\Rightarrow$ existiert einelementige Bahn, d.h. $h^{-1}\tilde{P}h = \tilde{P} \quad h \in H$, $\tilde{P} \in O(P)$, d.h. $H < N(\tilde{P})$.

$\tilde{P} \lhd H\tilde{P}$ (Übungsaufgabe)

$\overset{\text{2. Isomorphiesatz}}{\Rightarrow}$ $H\tilde{P}/\tilde{P} \cong H/h \cap \tilde{P} \ \Rightarrow \ |H\tilde{P}|$ ist p-Potenz

$\Rightarrow \ \sharp H\tilde{P} \, (\geq \sharp \tilde{P}) = p^l$, also $H\tilde{P} = \tilde{P} \ \Rightarrow \ H \subseteq \tilde{P}$.

(ii) $\sharp H = p^l \ \Rightarrow$ es gibt nur eine Bahn von p-Sylow-Untergruppe, d.h. alle p-Sylow-Untergruppe sind untereinander konjugiert.

(iii) $N_P(l) = H(L) \, | m$

$$N(L) = |O(P)| = (G : G_p) \, | \, (G : 1),$$

sowie $p \nmid N(l)$.

□

Beispiel:
Bestimmung aller nicht abelschen Gruppen der Ordnung 8. Zunächst gilt allgemein für $|G| = 8 = 2^3 \cdot 1$:
$N(1) \in \{1, 3, 5, 7\}$, $N(2)$ ungerade gemäß (1.38). Ist G nicht abelsch (also erst recht nicht zyklisch), so enthält G kein Element der Ordnung 8, aber notwendig eins — etwa b — der Ordnung 4. Also ist $U =< b >$ Normalteiler und $G = U \dot{\cup} Ua$. Ferner ist $a^2 \notin Ua$ und damit $a^2 = e$ oder $a^2 = b^2$.
Wegen $aU = Ua$ ist jedenfalls $aba^{-1} \in U$. $aba^{-1} = b$ scheidet aus, da G nicht abelsch sein soll. $aba^{-1} = e$ ist wegen der Kürzungsregel unmöglich.

$$aba^{-1} = b^2 \quad \Rightarrow \quad ab^2a^{-1} = (aba^{-1}9 \, (aba^{-1}) = e$$

ebenfalls im Widerspruch zur Kürzungsregel. Also muß notwendig $aba^{-1} = b^{-1}$ gelten.

1. Fall: $a^2 = e$: $G \cong D_4$.

2. Fall: $a^2 = b^2$: $G \cong Q_8$.
(Etwa für $b = i,\ a = j$; dann wird $k = ba,\ -1 = b^2$ mit den üblichen Relationen.)

$n = 8$

Typ	$Z_2 \times Z_2 \times Z_2$	$Z_4 \times Z_2$	Z_8	D_4	Q_8
$N(1)$	7	3	1	5	1
$N(2)$	7	3	1	3	3

Zu Z_2^3:
Es existieren 7 Elemente der Ordnung 2 und ebensoviele Untergruppen der Ordnung 2. Also exitiert $\binom{7}{2} \cdot \frac{1}{3}$ Untergruppen der Ordnung 4.

Zu $Z_4 \times Z_2$:
Untergruppen der Ordnung 2: $< b^2 >,\ < a >,\ < b^2a >$ für $G =< b, a >$ mit $b^4 = a^2 = 1$.
Untergruppen der Ordnung 4: $< b >,\ < ba >,\ < b^2,\ a >$.

Zu Z_8:
Untergruppen der Ordnung 2: $< b^4 >$,
Untergruppen der Ordnung 4: $< b^2 >$ für $G = \{b^\nu \mid 0 \leq \nu \leq 7\}$.

Zu D_4:
Untergruppen der Ordnung 2: $< b^2 >,\ < a >,\ < ab >,\ < ab^2 >,\ < ab^3 >$.
Untergruppen der Ordnung 4: $< b >,\ < b^2,\ a >,\ < b^2,\ ab >$.

Zu Q_8:
Untergruppen der Ordnung 2: $< b^2 >$,
Untergruppen der Ordnung 4: $< b >,\ < a >,\ < ab >$.

2.58. Hilfssatz

Es sei G eine p-Gruppe der Ordnung p^l $(l \in \mathbb{N})$ und es sei $\alpha \in \mathbb{Z},\ 0 \leq \alpha \leq l$. Dann ist die Anzahl der Normalteiler von G von der Ordnung p^α kongruent 1 modulo p. (Es gibt also stets welche!)

Beweis:
Es sei

$$\mathfrak{M} := \{U \mid u < G,\ \sharp U = p^\alpha\}.$$

Wegen (1.38) gilt $|\mathfrak{M}| \equiv 1 \bmod p$. Lasse G auf $\mathfrak{M}$ mittels Konjugation operieren. Es folgt

$$\sharp\mathfrak{M} = \sum_i (G : G_{P_i}) = \sum_i p^{\sigma_i},$$

und mindestens ein σ_i muß hierin verschwinden. Für dieses i gilt $G_{P_i} = N_{P_i} = G$, d.h. P_i ist Normalteiler in G.

□

2.59. Satz

G sei eine endliche abelsche Gruppe.

(i) G ist direktes Produkt seiner p-Sylow-Untergruppen.
(ii) G ist direktes Produkt von zyklischen Gruppen $U_1, \ldots, U_r$ mit $|U_1| \Big| |U_2| \Big| \ldots \Big| |U_r|$ "Elementarteilernormalform".

Beweis:

(i) Es sei

$$|G| = n = p_1^{k_1} \cdot \ldots \cdot p_r^{k_r}$$

die Primfaktorzerlegung der Gruppenordnung. Es bezeichne $G_1, \ldots, G_r$ die p-Sylow-Untergruppen von G (vergleiche (1.38)(i)) mit

$$(G_i : 1) = p_i^{k_i} \quad (1 \leq i \leq r).$$

Wir zeigen: $G_1 \dot{+} \ldots \dot{+} G_r$ ist innere direkte Summe! Dazu setze

$$\tilde{G}_i := \dot{\sum_{\substack{j=1 \\ j \neq i}}^{r}} G_j \quad (1 \leq i \leq r).$$

Gemäß (1.23) bleibt $G_i \cap \tilde{G}_i = \{e\}$ zu zeigen.

Jedes Element aus $G_i \cap \tilde{G}_i = \{e\}$ hat jedoch eine Ordnung, die sowohl $p_i^{k_i}$ als auch

$$\prod_{\substack{j=1 \\ j \neq i}}^{r} p_j^{k_j}$$

teilt. Also gilt notwendig $G_i \cap \tilde{G}_i = \{e\}$. Damit ist $G_1 \dot{+} \ldots \dot{+} G_r$ direkte Summe, also $G_1 \dot{+} \ldots \dot{+} G_r$ Untergruppe von G mit

$$|G_1 \dot{+} \ldots \dot{+} G_r| = \prod_{j=1}^{r} p_j^{k_j} = |G|,$$

also $G = G_1 \dot{+} \ldots \dot{+} G_r$. (Vergleiche (1.25)(iii))

(ii) Beschränkung auf $U =< x >$, $\mathrm{ord}(x) = m$, $V =< y >$, $\mathrm{ord}(y) = n$ und $G = U \dot{+} V = \tilde{U} \dot{+} \tilde{V}$ mit $|\tilde{U}| \Big| |\tilde{V}|$, $\mathrm{ggT}\,(m, n) = c$, $\mathrm{kgV}\,(m, n) = \frac{mn}{c}$.

Erzeuger: $(x,\ y)$

Relationsmatrix: $\begin{pmatrix} m & 0 \\ 0 & n \end{pmatrix}$

Beispiele: $\mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z} \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z}$, $\mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \cong \mathbb{Z}/6\mathbb{Z}$.

In $\mathbb{Z}$ existieren u, v mit $c = um + vn$.

$$\begin{array}{lll}
 & \begin{pmatrix} m & 0 \\ 0 & n \end{pmatrix} & \\
 & \downarrow \qquad \begin{pmatrix} 1 & 0 \\ v & 1 \end{pmatrix} & \\
 & \begin{pmatrix} m & 0 \\ nv & n \end{pmatrix} & \\
\begin{pmatrix} 1 & 0 \\ -u & 1 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ u & 1 \end{pmatrix} & & \\
(x - uy, y) & \begin{pmatrix} m & 0 \\ um + nv & n \end{pmatrix} & \\
\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} & & \\
 & \vdots & \\
(y, x - uy) & \begin{pmatrix} c & n \\ m & 0 \end{pmatrix} & \\
 & \begin{pmatrix} 1 & -\frac{n}{c} \\ 0 & 1 \end{pmatrix} & \\
 & \begin{pmatrix} c & 0 \\ m & -\frac{mn}{c} \end{pmatrix} & \\
\begin{pmatrix} 1 & 0 \\ \frac{m}{c} & 1 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ -\frac{m}{c} & 1 \end{pmatrix} & & \\
\left(y + \frac{m}{c}(x - uy), x - uy\right) & \begin{pmatrix} c & 0 \\ 0 & -\frac{mn}{c} \end{pmatrix} & \\
 & \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} & \\
\left(\frac{m}{c}x + \left(1 - \frac{mn}{c}\right)y, x - uy\right) & \begin{pmatrix} c & 0 \\ 0 & \frac{mn}{c} \end{pmatrix} & \\
\frac{vn}{c} & &
\end{array}$$

$\tilde{u} =< \frac{n}{c}x + \frac{n}{c}vy >$ von der Ordnung c,
$\tilde{v} =< x - uy >$ von der Ordnung $\frac{mn}{c}$.

□

Nützliches Beispiel: **Permutationsgruppen** (vergleiche (1.27)).
Aus der Linearen Algebra setzen wir als bekannt voraus:
$\mathfrak{S}_n$ ist Gruppe der Ordnung $n!$, Definition einer Transposition, jede Permutation ist Produkt von höchstens n Transpositionen, signum einer Permutation π als Anzahl der Fehlstände $i < j$ mit $\pi(i) > \pi(j)$,

signum ist mutiplikativ,

$$\text{sign} \ : \ \mathfrak{S}_n \to Z_2$$

ist Gruppenhomomorphismus, der für $n \geq 2$ surjektiv ist; $\mathfrak{A}_n$ ist Untergruppe der geraden Permutationen,

$$\sharp\mathfrak{A} = \frac{n!}{2} \text{ für } n \geq 2,$$

$\mathfrak{A}_n$ ist Normalteiler in $\mathfrak{S}_n$, sog. alternierende Gruppe.

CHAPTER 3

Ringe

3.1. Definition

Eine nicht leere Menge R mit zwei inneren Verknüpfungen $+$ (Addition), $\cdot$ (Multiplikation) heißt Ring $(R, +, \cdot)$, falls folgende drei Bedingungen erfüllt sind.

(i) $(R, +)$ ist abelsche Gruppe;
(ii) $(R, \cdot)$ ist eine Halbgruppe;
(iii) es gelten die Distributivgesetze:

$$\begin{aligned} x \cdot (y + z) &= (x \cdot y) + (y \cdot z), \\ (x + y) \cdot z &= (x \cdot z) + (y \cdot z) \quad \forall x,\, y,\, z \in R. \end{aligned}$$

Überdies heißt R kommutativ, falls $x \cdot y = y \cdot x \ \forall x,\, y \in R$ gilt. R heißt Ring mit Eins, falls $(R, \cdot)$ Monoid ist.

Bemerkung:
Statt $(R, x, \cdot)$ schreibt man oft kürzer R, statt $x \cdot y$ einfach $x\,y$. Vereinbarungsgemäß geht "Punktrechnung vor Strichrechnung". Das neutrale Element bzgl. $+$ wird als 0 geschrieben. Ein Einselement ist, falls es existiert, stets eindeutig bestimmt.

Beispiel:

(i) $(\mathbb{Z}, +, \cdot)$, $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$, $(\mathbb{C}, +, \cdot)$ sind kommutative Ringe mit Eins, jedoch auch $R = \{0\}$ (pathologischer Ring).
(ii) $(\mathbb{Z}/n\mathbb{Z})$ ist kommutativer Ring mit Eins $(n \in \mathbb{N})$.
(iii) Die Endomorphismen eines Vektorraums V bilden einen Ring mit Einselement id. Dieser ist für $\dim V \geq 2$ nicht kommutativ.
(iv) $R^{n \times n}$ ist Matrizenring über R.

3.1.1. Rechenregeln für Ringe. Für $x,\, y \in R$ gilt (vergleiche Lineare Algebra I):

(i) $0\,x = x\,0 = 0$,
(ii) $(-x)\,y = -(x\,y) = x\,(-y)$,
(iii) $(-x)\,(-y) = x\,y$,
(iv) $(\mathbb{Z},\, R) \to R \ : \ (m,\, x) \mapsto mx = \underbrace{x + \ldots + x}_{m\text{-mal}}$,
$\mathbb{Z}$ operiert auf jedem Ring mittels $(n, x) \mapsto nx$.

Statt $x + (-y)$ schreibt man $x - y$.
Allgemein gilt für $x_i,\ y_j \in R\ (1 \leq i \leq n,\ 1 \leq j \leq m,\ n, m \in \mathbb{N})$:

$$x_1 + \ldots + x_n = \sum_{i=1}^{n} x_i; \qquad x_1 \cdot \ldots \cdot x_n = \prod_{i=1}^{n} x_i;$$

leere Summe $:= 0$; leeres Produkt $:= 1$, falls $1 \in R$;

$$\begin{aligned}
\left(\sum_{i=1}^{n} x_i\right)\left(\sum_{j=1}^{m} y_j\right) &= \sum_{i=1}^{n}\sum_{j=1}^{m} x_i y_j, \\
x^n &= \prod_{i=1}^{n} x, \\
x^{n+m} &= x^n \cdot x^m, \\
(x^n)^m = x^{nm}, & \\
(x+y)^n &= \sum_{i=0}^{n} \binom{n}{i} x^{n-i} y_i
\end{aligned}$$

in kommutativen Ringen mit 1.

3.2. Definition

Eine Teilmenge S von $(R, +, \cdot)$ heißt Teilring (Unterring) von R, falls $(S, +, \cdot)$ selbst Ring ist. In diesem Fall heißt R Oberring (Erweiterungsring) von S.

3.3. Hilfssatz

R sei Ring und $\emptyset \neq S \subseteq R$. Dann sind äquivalent:

(i) S Teilring von R,
(ii) $SS \subseteq S$ und $S + (-S) \subseteq S$.

Beweis:
(i) $\Rightarrow$ (ii): Klar. Beachte

$$\begin{aligned}
SS &= \{xy \mid x \in S,\ y \in S\}, \\
S + (-S) &= \{x - y \mid x,\ y \in S\}.
\end{aligned}$$

(ii) $\Rightarrow$ (i):

$$\begin{aligned}
S + (-S) \subseteq S &\Rightarrow (S, +) \text{ Gruppe}, \\
SS \subseteq S &\Rightarrow (S, \cdot) \text{ Halbgruppe},
\end{aligned}$$

denn die Rechenregeln übertragen sich von R.

□

Beispiele:

(i) Für $n \in \mathbb{N}$ ist $n\mathbb{Z}$ Unterring von $\mathbb{Z}$.
(ii) Die Diagonalmatrizen bilden einen Unterring von $R^{n\times n}$.

Bemerkung: Der Durchschnitt von Teilringen ist Teilring!

Wichtiger als Teilringe sind jedoch Ideale, die in gewisser Weise den Normalteilern in der Gruppentheorie entsprechen!

3.4. Definition

Es sei R ein Ring. $\mathfrak{a} \subseteq R$ heißt Linksideal (bzw. Rechtsideal) von R, falls gilt:

(i) $\mathfrak{a}$ ist Untergruppe von $(R, +)$, d.h. $\mathfrak{a} \neq \emptyset$ und $\mathfrak{a} + (-\mathfrak{a}) \subseteq \mathfrak{a}$.

(ii) $\forall a \in \mathfrak{a} \ \forall x \in R \ : \ x\,a \in \mathfrak{a}$ (bzw. $ax \in \mathfrak{a}$), d.h. $R\,\mathfrak{a} \subseteq \mathfrak{a}$ (bzw. $\mathfrak{a} \supseteq \mathfrak{a}\,R$).

$\mathfrak{a} \subseteq R$ heißt Ideal, falls $\mathfrak{a}$ sowohl Links- als auch Rechtsideal ist.

Bemerkung:

(i) $\{0\}$, R sind stets Ideale von R; Ideale sind Teilringe (Umkehrung i.a. falsch: $\mathbb{Z} \subset \mathbb{Q}$); für $R \ni 1$ und $1 \in \mathfrak{a}$ für ein Links- oder Rechtsideal $\mathfrak{a}$ von R folgt sofort $\mathfrak{a} = R$.

(ii) Der Durchschnitt von (Links- bzw. Rechts-) Idealen ist wieder eins. Zu $A \subseteq R$ existiert folglich ein kleinstes Ideal, welches A umfaßt, das sogenannte von A erzeugte Ideal (A).

Beispiel:
Es sei $\mathfrak{a}$ ein Ideal von $\mathbb{Z}$. Wegen $\mathfrak{a} \neq \emptyset$ und $(-\mathfrak{a}) \subseteq \mathfrak{a}$ gilt entweder $\mathfrak{a} = \{0\}$, oder $\mathfrak{a}$ enthält eine kleinste natürliche Zahl m. Gemäß Division mit Rest gilt, daß m alle Zahlen von $\mathfrak{a}$ teilt. Also ist $\mathfrak{a} = \mathbb{Z}m = m\mathbb{Z}$.

3.5. Hilfssatz

Es sei $\emptyset \neq A \subseteq R$, R Ring. Dann besteht (A) aus allen endlichen Summen von Elementen der Form

$$n\,a,\ x\,a,\ a\,y,\ x\,a\,y \text{ mit } a \in A,\ x, y \in R,\ n \in \mathbb{Z}.$$

Beweis:

(i) Jedes Ideal $\mathfrak{a}$ mit $A \subseteq \mathfrak{a}$ enthält alle in (2.5) angegebenen Elemente.

(ii) Die Menge der in (2.5) angegebenen Elemente ist ein Ideal.

□

3.6. Korollar

Es sei R ein Ring und $\emptyset \neq A \subseteq R$. Dann gilt:

(i) $(A) = \left\{ \sum_{\text{endl.}} x_i \cdot a_i \cdot y_i \;\middle|\; x_i,\ y_i \in R,\ a_i \in A \right\}$ für $R \ni 1$;

(ii) $(A) = \left\{ \sum_{\text{endl.}} x_i \cdot a_i + \sum_{\text{endl.}} m_j \cdot b_j \;\middle|\; x_i \in R,\ m_j \in \mathbb{Z},\ a_i, b_j \in A \right\}$ für R kommutativ;

(iii) $(A) = \left\{ \sum_{\text{endl.}} x_i \cdot a_i \;\middle|\; x_i \in R,\ a_i \in A \right\}$ für R kommutativ mit Eins.

Beweis: Unmittelbar klar nach (2.5)!

3.7. Definition

Ein Ideal $\mathfrak{a}$ eines Ringes R heißt Hauptideal, falls $\mathfrak{a} = (a)$ für $a \in R$ gilt. $\mathfrak{a}$ heißt endlich erzeugbar, falls $\mathfrak{a} = (A)$ mit $\sharp A < \infty$ gilt.

Beispiel:
Alle Ideale in $\mathbb{Z}$ sind Hauptideale.

Bemerkungen:

(i) R kommutativ $\Rightarrow\ (a) = Ra + \mathbb{Z}a$;
(ii) R kommutativ mit Eins $\Rightarrow\ (a) = Ra$;
(iii) R kommutativ ohne Eins: In $R = 2\mathbb{Z}$ ist $(2) = 4\mathbb{Z} + \mathbb{Z}2 = 2\mathbb{Z}$ von $2R = 4\mathbb{Z}$ verschieden;
(iv) $R \ni 1\ \Rightarrow\ (1) = R$.

Arithmetik von Idealen:

3.8. Definition

Die Summe zweier (Links- bzw. Rechts-) Ideale $\mathfrak{a}_1,\ \mathfrak{a}_2$ ist definiert durch:

$$\mathfrak{a}_1 + \mathfrak{a}_2 = \{a_1 + a_2 \mid a_1 \in \mathfrak{a}_1,\ a_2 \in \mathfrak{a}_2\}.$$

Bemerkung:
Die Summe endlich vieler (Links- bzw. Rechts-) Ideale ist wieder eins. Der Durchschnitt von Idealen ist wieder ein Ideal. Es gelten:

$$\mathfrak{a}_i \subseteq \mathfrak{a}_i + \ldots + \mathfrak{a}_n\ (1 \le i \le n), \quad \mathfrak{a}_i + \mathfrak{a}_i = \mathfrak{a}_i, \quad (A_1) + (A_2) = (A_1 \cup A_2).$$

Beispiel:
$R = \mathbb{Z}$:
$Ra + Rb = \{xa + yb \mid x, y \in \mathbb{Z}\} = c\mathbb{Z}$ mit $c = \text{ggT}\,(a, b)$,
$Ra \cap Rb = d\mathbb{Z}$ mit $d = \text{kgV}\,(a, b)$.

3.9. Definition

Das Produkt zweier (Links- bzw. Rechts-) Ideale $\mathfrak{a}_1$, $\mathfrak{a}_2$ ist definiert durch:

$$\mathfrak{a}_1 \cdot \mathfrak{a}_2 = \left\{ \sum_{\text{endl.}} a_{1i}\, a_{2i} \,|\, a_{1i} \in \mathfrak{a}_1,\ a_{2i} \in \mathfrak{a}_2 \right\}.$$

Bemerkung:
Das Produkt endlich vieler (Links- bzw. Rechts-) Ideale ist wieder eins. Es gelten die Rechenregeln:

$$\mathfrak{a}_1\,(\mathfrak{a}_2\mathfrak{a}_3) = (\mathfrak{a}_1\mathfrak{a}_2)\,\mathfrak{a}_3, \quad \mathfrak{a}_1\,(\mathfrak{a}_2 + \mathfrak{a}_3) = \mathfrak{a}_1\mathfrak{a}_2 + \mathfrak{a}_1\mathfrak{a}_3.$$

Ist R kommutativ, so gilt $\mathfrak{a}_1\mathfrak{a}_2 = \mathfrak{a}_2\mathfrak{a}_1$. Sind $\mathfrak{a}_1$, $\mathfrak{a}_2$ Linksideale, so gilt $\mathfrak{a}_1\mathfrak{a}_2 \subseteq \mathfrak{a}_2$; sind $\mathfrak{a}_1$, $\mathfrak{a}_2$ Rechtsideale, so gilt $\mathfrak{a}_1\mathfrak{a}_2 \subseteq \mathfrak{a}_1$, $(A_1)\,(A_2) = (A_1A_2)$ für R kommutativ.

Ist R kommutativer Ring mit Eins und sind a, $b \in R$, so gilt

(i) $(a) + (b) = \{xa + yb \,|\, x,\, y \in R\} = Ra + Rb$.
(ii) $(a)\,(b) = (ab)$, $Ra\,Rb = R\,(Ra)\,b = Rab$.
(iii) $\mathfrak{a} \cap (\mathfrak{b} + \mathfrak{c}) \supseteq \mathfrak{a} \cap \mathfrak{b} + \mathfrak{a} \cap \mathfrak{c}$ mit Gleichheit für $\mathfrak{a} \supseteq \mathfrak{b} \vee \mathfrak{a} \supseteq \mathfrak{c}$.
(iv) für $\mathfrak{a} + \mathfrak{b} = R$ ist $\mathfrak{a} \cap \mathfrak{b} = \mathfrak{a}\mathfrak{b}$.

Beweis:

(i) klar.

(ii) klar.

(iii) $x \in \mathfrak{a} \cap \mathfrak{b},\ y \in \mathfrak{a} \cap \mathfrak{c} \ \Rightarrow\ x + y \in \mathfrak{a}, x + y \in \mathfrak{b} + \mathfrak{c}$.
Gilt oBdA $\mathfrak{a} \supseteq \mathfrak{b}$, so ist für $x \in \mathfrak{a} \cap (\mathfrak{b} + \mathfrak{c})$ zunächst $x = b + c$ mit $b \in \mathfrak{b},\ c \in \mathfrak{c}$.
Wegen $\mathfrak{a} \supseteq \mathfrak{b}$ ist auch $b \in \mathfrak{a}$ und damit $c \in \mathfrak{a}$, also $b \in \mathfrak{a} \cap \mathfrak{b},\ c \in \mathfrak{a} \cap \mathfrak{c}$.

(iv) Es ist

$$\begin{aligned}(\mathfrak{a} + \mathfrak{b})(\mathfrak{a} \cap \mathfrak{b}) &= \mathfrak{a}(\mathfrak{a} \cap \mathfrak{b}) + \mathfrak{b}(\mathfrak{a} \cap \mathfrak{b}) \subseteq \mathfrak{ab} \\ &\subseteq \mathfrak{a} \cap \mathfrak{b},\end{aligned}$$

also $(\mathfrak{a} + \mathfrak{b})(\mathfrak{a} \cap \mathfrak{b}) \subseteq \mathfrak{ab}$;
für $\mathfrak{a} + \mathfrak{b} = R$ gilt offenbar Gleichheit.

□

Bemerkung:
Ein Beispiel für $\mathfrak{a} \cap (\mathfrak{b} + \mathfrak{c}) \supset \mathfrak{a} \cap \mathfrak{b} + \mathfrak{a} \cap \mathfrak{c}$ wird im Anschluß an die Einführung von Polynomringen behandelt.

3.10. Satz

Es sei R ein Ring mit Ideal $\mathfrak{a}$. Dann läßt sich $R/\mathfrak{a}$ mittels

$$(x + \mathfrak{a}) + (y + \mathfrak{a}) =: (x + y) + \mathfrak{a}, (x + \mathfrak{a})(y + \mathfrak{a}) := xy + \mathfrak{a} \quad \forall x, y \in R$$

zu einem Ring machen, dem Faktorring $R/\mathfrak{a}$ oder Restklassenring R modulo $\mathfrak{a}$.

Beweis:
Zunächst ist $(\mathfrak{a}, +)$ additive Untergruppe von $(R, +)$, also $R/\mathfrak{a}$ eine additive Gruppe (vergleiche (1.17)). Wir zeigen: $(R/\mathfrak{a}, \cdot)$ ist Halbgruppe. Zunächst ist $\cdot$ innnere Verknüpfung. Dazu ist die Wohldefiniertheit nachzuweisen. Für

$$x + \mathfrak{a} = \tilde{x} + \mathfrak{a},\ y + \mathfrak{a} = \tilde{y} + \mathfrak{a} \quad \text{folgt} \quad x - \tilde{x},\ y - \tilde{y} \in \mathfrak{a}$$

und somit

$$xy - \tilde{x}\tilde{y} = (x - \tilde{x})\, y + \tilde{x}\,(y - \tilde{y}) \ \in \mathfrak{a},$$

da $\mathfrak{a}$ zweiseitiges Ideal ist. Also folgt $xy + \mathfrak{a} = \tilde{x}\tilde{y} + \mathfrak{a}$. Das Assoziativgesetz bzgl. $\cdot$ überträgt sich von R. Das gleiche gilt für die Distributivgesetze, da ja vertreterweise mit den Idealklassen gerechnet wird.

□

Bemerkung:

(i) Für $1 \in R$ ist $1 + \mathfrak{a}$ Einselement von $R/\mathfrak{a}$. R kommutativ $\Rightarrow$ $R/\mathfrak{a}$ kommutativ.

(ii) Für $x - y \in \mathfrak{a}$ schreibt man $x \equiv y$ modulo $\mathfrak{a}$ ("kongruent"). Hierfür gelten die Regeln:

$$\left.\begin{array}{l} x \equiv y \text{ modulo } \mathfrak{a} \\ u \equiv v \text{ modulo } \mathfrak{a} \end{array}\right\} \Rightarrow x \overset{+}{\underset{\bullet}{}} u \equiv y \overset{+}{\underset{\bullet}{}} v \text{ modulo } \mathfrak{a}.$$

Für $R = \mathbb{Z}$ bedeutet die alte Schreibweise $x \equiv y \bmod n$ gerade $x \equiv y$ modulo $n\mathbb{Z}$, denn sämtliche Ideale von $\mathbb{Z}$ waren ja als Hauptideale nachgewiesen. Die spezielle Äquivalenzrelation $\equiv$ heißt Kongruenzrelation.

3.11. Definition

Es seien R, S zwei Ringe. Unter einem Ringhomorphismus von R nach S versteht man eine Abbildung $f : R \to S$ mit

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

Bemerkung:

(i) Für Ringhomomorphismen $f : R \to S$ ist $\operatorname{Im} f = f(R)$ Unterring von S, $\ker f = f^{-1}(0)$ Ideal in R.

(ii) Ist R ein Ring mit Ideal $\mathfrak{a}$, so ist $p : R \to R/\mathfrak{a} : x \mapsto x + \mathfrak{a}$ ein Ringepimorphismus, der sog. kanonische Epimorphismus. Es ist $\ker p = \mathfrak{a}$.

3.12. Hilfssatz

Eine Teilmenge $\mathfrak{a}$ eines Ringes R ist genau dann ein Ideal, wenn $\mathfrak{a}$ Kern eines Ringhomomorphismus ist.

3.13. Hilfssatz

Es seien R, S Ringe und $f : R \to S$ ein Ringhomomorphismus. Dann gilt:

(i) Ist $\mathfrak{b}$ ein Ideal in S, so ist $f^{-1}(\mathfrak{b})$ Ideal in R, $f^{-1}(\mathfrak{b}) \supseteq \ker f$.

(ii) Ist $\mathfrak{a}$ Ideal in R und f surjektiv, so ist $f(\mathfrak{a})$ Ideal in S.

Beweis:
Gemäß (1.16) gelten die Aussagen bzgl. $+$.

(i) Es sei $s = f(r) \in \mathfrak{b}$ und $x \in R$. Dann ist

$$f(xr) = f(x)\, f(r) \ \in \mathfrak{b},$$

also mit r auch $xr \in f^{-1}(\mathfrak{b})$.

(ii) Es sei $y = f(x)$ mit $x \in \mathfrak{a}$ und $z \in S$. Dann ist $z = f(r)$ für ein $r \in R$ und somit

$$zy = f(r)\, f(x) = f(rx) \ \in f(\mathfrak{a}).$$

□

3.14. Satz

Es seien R, S zwei Ringe.

(i) (Homomorphiesatz)
Ist $\varphi : R \to S$ ein Ringhomomorphismus, dann gilt
$$R/\ker\varphi \cong \varphi(R).$$

(ii) (Erster Isomorphiesatz)
Ist U Unterring und $\mathfrak{a}$ Ideal von R, so gilt
$$(U+\mathfrak{a})/\mathfrak{a} \cong U/U\cap\mathfrak{a}.$$

(iii) (Zweiter Isomorphiesatz)
Für Ideale $\mathfrak{a}$, $\mathfrak{b}$ von R mit $\mathfrak{a}\subseteq\mathfrak{b}$ ist $\mathfrak{b}/\mathfrak{a}$ Ideal von $R/\mathfrak{a}$, und es gilt
$$(R/\mathfrak{a})/(\mathfrak{b}/\mathfrak{a}) \cong R/\mathfrak{b}.$$

3.15. Hilfssatz

Es sei $\mathfrak{a}$ ein Ideal des Ringes R. Die Mengen
$$I(\mathfrak{a}) := \{\mathfrak{b} \mid \mathfrak{b} \text{ Ideal von } R \text{ mit } \mathfrak{b}\supseteq\mathfrak{a}\}$$
und
$$J(\mathfrak{a}) := \{\,\overline{\mathfrak{b}} \mid\ \overline{\mathfrak{b}} \text{ Ideal von } R\backslash\mathfrak{a}\}$$
werden dann mittels $\psi : I(\mathfrak{a}) \to J(\mathfrak{a}) : \mathfrak{b} \mapsto \mathfrak{b}/\mathfrak{a}$ bijektiv aufeinander abgebildet.

Beweis:
Für den kanonischen Epimorphismus $p : R \to R/\mathfrak{a}$ liefert ψ eine Abbildung von $I(\mathfrak{a})$ in $J(\mathfrak{a})$. Für
$$\psi(\mathfrak{b}_1) = \psi(\mathfrak{b}_2) \quad \text{folgt} \quad \mathfrak{b}_1 = \mathfrak{b}_1+\mathfrak{a} = \mathfrak{b}_2+\mathfrak{a} = \mathfrak{b}_2,$$
also ist ψ injektiv. Ist schließlich $\overline{\mathfrak{b}}$ Ideal von $J(\mathfrak{a})$, so ist $p^{-1}(\overline{\mathfrak{b}})$ ein Ideal von R, welches $\mathfrak{a}$ umfaßt, also in $I(\mathfrak{a})$ liegt. Hierfür gilt $\psi(p^{-1}(\overline{\mathfrak{b}})) = \overline{\mathfrak{b}}$ nach Konstruktion.

□

3.16. Definition

Es sei R ein Ring. $0 \neq a \in R$ heißt linker (rechter) Nullteiler, falls $b \in R$ mit $a\,b = 0$ ($b\,a = 0$) für ein $0 \neq b \in R$ existiert. $x \in R$ heißt nilpotent, falls $m \in \mathbb{N}$ mit $x^m = 0$ existiert. Für $1 \in R$ heißt $e \in R$ Einheit (invertierbar), falls e in R ein Linksinverses und ein Rechtsinverses besitzt. $U(R) = R^\times$ bezeichnet die Menge der Einheiten von R.

Bemerkung:

(i) e Einheit $\Rightarrow$ e^{-1} existiert eindeutig.
Sei

$$ae = eb = 1 \quad \Rightarrow \quad a = a \cdot 1 = a\,(eb) = (ae)\,b = 1 \cdot b = b.$$

Für $ae = ea = 1$ und $be = eb = 1$ folgt

$$a = a \cdot 1 = a\,(eb) = (ae)\,b = 1 \cdot b = b.$$

(Vergleiche Gruppentheorie)

(ii) Die Elemente von R, welche keine Nullteiler sind, bilden eine Halbgruppe. Es seien a, b keine Nullteiler; ist dann $x \in R$ mit $abx = 0$ so folgt

$$a\,(bx) = 0 \quad \Rightarrow \quad bx = 0 \quad \Rightarrow \quad x = 0.$$

(iii) Einheiten sind keine Nullteiler und bilden folglich eine multiplikative Untergruppe von R.

$$e \in R^\times,\ x \in R\ :\ ex = 0 \quad \Rightarrow \quad e^{-1}ex = 0 \quad \Rightarrow \quad 1 \cdot x = x = 0.$$

Beispiele:
Bestimme Einheiten, Nullteiler und nilpotente Elemente in
$\mathbb{Z}/12\mathbb{Z},\ \mathbb{Z},\ K^{n\times m},\ R = \{0\}$.

(i) $0 \neq x \in R$ nilpotent $\Rightarrow$ x Nullteiler.
$0 = x^m = \left(x^{m-1}\right) x = x\left(x^{m-1}\right)$, wähle m minimal!

(ii) $\mathbb{Z}/12\mathbb{Z} = \{\,\bar{i} \mid 0 \leq i \leq 11\}$
$\bar{j}^{\,m} \stackrel{?}{=} \bar{0} \ \Rightarrow\ j^m \equiv 0 \bmod 12\ \ (12 = 4 \cdot 3) \ \Rightarrow\ j = 0 \vee 6$
Nilpotente Elemente: $\bar{0}$, $\bar{6}$
Nullteiler: $\bar{6}$, $\bar{2}$, $\bar{4}$, $\bar{8}$, $\overline{10}$, $\bar{3}$, $\bar{9}$
Einheiten: $\bar{1}$, $\bar{5}$, $\bar{7}$, $\overline{11}$ $\ (\bar{1} = \bar{5}^2 = \bar{7}^2 = \overline{11}^2)$

(iii) $R = \mathbb{Z}$
Nilpotente Elemente: 0,
Nullteiler: keine,
Einheiten: ± 1.

(iv) $K^{n\times n}$
Nilpotente Elemente sind z.B. alle oberen $\triangle$-Matrizen mit 0-Diagonale,
Nullteiler: alle singulären Matrizen,
Einheiten: $\mathrm{GL}\,(n,\, K)$.

3.17. Definition

Ein Ring R mit $1 \neq 0$ heißt Schiefkörper, falls $R^\times = R\backslash\{0\}$ ist. Ist R kommutativ, so heißt R Körper.

3.18. Hilfssatz

Ein Ring R ist genau dann ein Schiefkörper, wenn $(R\backslash\{0\}, \cdot)$ Gruppe ist.

Beweis:
$\Rightarrow$: per Definition

$\Leftarrow$:
$R\backslash\{0\}$ enthält Eins e mit $0e = e0 = 0$. Also ist $R^\times = R\backslash\{0\}$.

□

Beispiele:

(i) Körper: $\mathbb{Q}$, $\mathbb{R}$, $(\mathbb{Z}/n\mathbb{Z})$ mit $n \in \mathbb{P}$.
(ii) Schiefkörper: $\mathbb{R}+\mathbb{R}i+\mathbb{R}j+\mathbb{R}k$ Quaternionen (als $\mathbb{R}$-Vektorraum)

Bemerkung:

(i) R Ring mit Eins, $\mathfrak{a}$ Ideal von R mit $\mathfrak{a} \cap R^\times \neq \emptyset$. Dann ist $\mathfrak{a} = R$; denn zu $a \in \mathfrak{a} \cap R^\times$ existiert $a^{-1} \in R$ und $a^{-1}a \in R\mathfrak{a} = \mathfrak{a}$, also $1 \in \mathfrak{a}$ und $R = R\,1 \subseteq \mathfrak{a}$.
(ii) Ein Schiefkörper R enthält nur die Ideale $\{0\}$ und R.
(iii) Ist K ein Schiefkörper und $\varphi : K \to R$ ein Ringhomomorphismus, so ist $\varphi = \mathcal{O}$ oder φ injektiv.
(iv) Es gibt keine endlichen Schiefkörper! (ohne Beweis)

3.19. Hilfssatz

(i) Es sei R ein Ring. Ist $a \in R$ kein Nullteiler, so gilt:

$$ax = ay \;\Rightarrow\; x = y; \quad xa = ya \;\Rightarrow\; x = y \quad \forall x, y \in R.$$

(ii) Ein endlicher nullteilerfreier Ring $R \neq \{0\}$ ist ein Schiefkörper.

Beweis:

(i) $a\,(x - y) = 0 \;\Rightarrow\; x - y = 0 \;\Rightarrow\; x = y$; $\quad (x - y)\,a = 0 \;\Rightarrow\; x - y = 0 \;\Rightarrow\; x = y$.
(ii) Zeige: $(R\backslash\{0\}, \cdot)$ ist Gruppe.

Für $x \in R$, $x \neq 0$, betrachte $\varphi_x : R\backslash\{0\} \to R\backslash\{0\}$: $a \mapsto xa$. φ_x ist injektiv (nach (i)), also wegen R endlich auch surjektiv. Dasselbe gilt für $\psi_x : a \mapsto ax$. Zu $a, b \in R\backslash\{0\}$ existieren folglich eindeutig $x, y \in R\backslash\{0\}$ mit $b = ax = ya$. Gemäß (1.5) ist $R^\times = R\backslash\{0\}$ Gruppe.

□

3.20. Definition

Es sei R ein Ring mit $1 \neq 0$. Existiert dann eine kleinste natürliche Zahl n mit $n\,1 = 0$, so heißt n die Charakteristik $\chi(R)$ von R. Existiert kein solches n, setzt man die Charakteristik $\chi(R)$ zu 0 fest.

Beispiele:
$\chi(\mathbb{Z}) = 0,\ \chi(\mathbb{Z}/n\mathbb{Z}) = n.$

3.21. Satz

Die Charakteristik eines nullteilerfreien unitären ($R \ni 1 \neq 0$) Rings R ist 0 oder eine Primzahl p. Im letzten Fall gilt $px = 0\ \forall x \in R$, sowie $kx = R(k,\, p)\, x$.

Beweis:
Es sei R Ring mit $\chi(R) \neq 0$ und $n \in \mathbb{N}$ die kleinste natürliche Zahl mit $n1 = 0$, also speziell $n \geq 2$. Ist n keine Primzahl, so gilt $n = pq$ mit $p,\, q \in \mathbb{Z}^{\geq 1},\ p < n,\ q < n$ und somit

$$0 = n1 = pq1 = (p1)\,(q1).$$

Da R nullteilerfrei ist, erhält man $p1 = 0$ oder $q1 = 0$ im Widerspruch zur Minimalität von n. Nunmehr ist $0 = n1$, also auch

$$nx = n\,(1x) = (n1)\,x = 0x = 0 \quad \forall x \in R.$$

□

Bemerkung:
Der Durchschnitt von Schiefkörpern ist wieder einer. Also enthält jeder Schiefkörper einen kleinsten Teilkörper, den sogenannten Primkörper.

3.22. Satz

Der Primkörper eines Schiefkörper K ist isomorph zu $\mathbb{Q}$ (für $\chi(K) = 0$) oder zu $\mathbb{Z}/Lp\mathbb{Z}$ für eine Primzahl p (für $\chi(K) = p$).

Beweis:
In K gilt $1 \neq 0$. Der Primkörper von K umfaßt daher alle Elemente der Form $m1$ ($m \in \mathbb{Z}$). Für $\chi(K) = 0$ sind diese alle ungleich 0 für $m \neq 0$. Also existiert $(m1)^{-1}$ und damit $(m1)\,(n1)^{-1}$ im Primkörper. Setze

$$P := \{(m1)\,(n1)^{-1} \mid m \in \mathbb{Z},\ n \in \mathbb{Z},\ n \neq 0\}.$$

Es gilt:

$$(m1)\,(n1)^{-1} = (n1)^{-1}(m1) \text{ wegen } (n1)\,(m1) = (m1)\,(n1) = (mn)\,1,$$
$$(mn1)^{-1} = (m1)^{-1}(n1)^{-1}.$$

Also ist P Körper, der im Primkörper enthalten ist, folglich gleich dem Primkörper.

$$\varphi\ :\ \mathbb{Q} \to P\ :\ \frac{m}{n} \mapsto (m1)\,(n1)^{-1}$$

ist dann ein Ringisomorphismus.
Für $\chi(K) = p$, p Primzahl, ist $p1 = 0$. Für $x = k1$ $(1 \leq k < p)$ existiert (Euklidischer Algorithmus in $\mathbb{Z}$) ein $l \in \mathbb{Z}$ mit $k \cdot l \equiv 1 \bmod p$, also $(k1)(l1) = 1$ in K. Setze

$$P := \{k1 \mid 0 \leq k < p,\ k \in \mathbb{Z}\}.$$

Dies ist bereits der Primkörper von K.

$$\varphi : (\mathbb{Z}/p\mathbb{Z}) \to P : k + p\mathbb{Z} \mapsto k1$$

ist Ringisomorphismus! (φ ist wohldefiniert wegen $(k + pm)\,1 = k1 + p1m1 = k1$.)

□

Wie bei Gruppen kann man für Ringe äußere Produkte (Summen) erklären.

Sind $R_1, \ldots, R_n$ Ringe, so wird $R_1 \times \ldots \times R_n =: \prod_{i=1}^{n} R_i = R$ zu einem Ring mittels

$$\begin{aligned}(x_1, \ldots, x_n) + (y_1, \ldots, y_n) &= (x_1 + x_2, \ldots, x_n + y_n),\\ (x_1, \ldots, x_n) \cdot (y_1, \ldots, y_n) &= (x_1 y_1, \ldots, x_n y_n).\end{aligned}$$

(Vergleiche Eigenschaften bei Gruppen, speziell ist $\varepsilon_i(R_i) = (0, \ldots, 0, R_i, 0, \ldots, 0)$ Ideal von R. Schreibweise: $R_1 \oplus \ldots \oplus R_n$.)
Ist andererseits R ein Ring mit Idealen $\mathfrak{a}_1, \ldots, \mathfrak{a}_n$, so heißt R (innere) direkte Summe von $\mathfrak{a}_1, \ldots, \mathfrak{a}_n$, falls

$$R = \mathfrak{a}_1 + \ldots + \mathfrak{a}_n \quad \text{und} \quad R\mathfrak{a}_i \cap \sum_{\substack{j=1\\ j\neq i}}^{n} \mathfrak{a}_j = \{0\}$$

ist (vgl. (1.23)). (Schreibweise: $R = \mathfrak{a}_1 \dot{+} \ldots \dot{+} \mathfrak{a}_n$)
Ein Element $e \in R$ mit $e \neq 0$ und $e^2 = e$ heißt Idempotente von R.
Zwei Idempotente e, f heißen orthogonal, falls $ef = fe = 0$ ist.

Beispiel:
$R = \mathbb{Z}/6\mathbb{Z}$. Es gilt: $R = <3 + 6\mathbb{Z}> \dot{+} <4 + 6\mathbb{Z}>$.
Hierin sind $e_1 = 3 + 6\mathbb{Z}$ und $e_2 = 4 + 6\mathbb{Z}$ Idempotente. Wir haben hier eine Zerlegung der Eins in orthogonale Idempotente: $1 + 6\mathbb{Z} = (3 + 6\mathbb{Z}) + (4 + 6\mathbb{Z})$.

Bemerkung:
Ringe R mit $1 \in R$ haben mit einer Idempotenten $e \neq 1$ stets eine weitere: $1 - e$. Es gilt

$$\begin{aligned}1 &= e + (1 - e),\\ (1 - e)^2 &= 1^2 - 1 \cdot e - 1 \cdot e + e^2\\ &= 1 - e - e + e\\ &= 1 - e.\end{aligned}$$

$1-e$ und e sind orthogonale Idempotente wegen

$$e\,(1-e) = e - e^2 = 0 = (1-e)\,e.$$

Somit gilt

$$R = R\,1 = R\,(e + (1-e))\& \subseteq \&R\,e \dot{+} R\,(1-e).\& \subseteq \&R$$

, also überall Gleichheit.

Beachte: Orthogonale Idempotente sind Nullteiler.

Es sei R ein kommutativer Ring mit $1 \neq 0$. Zwei Ideale $\mathfrak{a}$, $\mathfrak{b}$ von R mit $\mathfrak{a} + \mathfrak{b} = R$ heißen komaximal. Speziell existieren $e \in \mathfrak{a}$, $f \in \mathfrak{b}$ mit $e + f = 1$. (Allerdings wird nicht gefordert, daß e, f orthogonale Idempotente sind.)

Beispiel: $R = \mathbb{Z}$, $m, n \in \mathbb{Z}$ teilerfremd $\Rightarrow$ $m\mathbb{Z} + n\mathbb{Z} = \mathbb{Z}$ und $mu + nv = 1$ für passende $u,\ v \in \mathbb{Z}$.

3.23. Hilfssatz

Es sei R ein kommutativer Ring mit $1 \neq 0$. Dann gilt für Ideale $\mathfrak{a}, \mathfrak{a}_1, \ldots, \mathfrak{a}_n, \mathfrak{b}_1, \ldots, \mathfrak{b}_n$ mit $\mathfrak{a}_i + \mathfrak{a}_j = R$ ($\mathfrak{a}_i$, $\mathfrak{a}_j$ komaxial) $(1 \leq i < j \leq n)$, $\mathfrak{a} + \mathfrak{b}_i = R$ $(1 \leq i \leq n)$:

(i) $\mathfrak{a} + \mathfrak{b}_1 \cdot \ldots \cdot \mathfrak{b}_n = R$,

(ii) $\mathfrak{a}_1 \cdot \ldots \cdot \mathfrak{a}_n = \mathfrak{a}_1 \cap \ldots \cap \mathfrak{a}_n$.

Beweis:

(i)

$$\begin{aligned} R &= R^n \\ &= \prod_{i=1}^{n} (\mathfrak{a} + \mathfrak{b}_i) \qquad \text{(wegen } 1 \in R\text{)} \\ &= \mathfrak{a}\,(\mathfrak{a}^{n-1} + \ldots) + \mathfrak{b}_1 \cdot \ldots \cdot \mathfrak{b}_n \qquad (R \text{ kommutativ}) \\ &\subseteq \mathfrak{a} + \mathfrak{b}_1 \cdot \ldots \cdot \mathfrak{b}_n \\ &\subseteq R, \end{aligned}$$

also muß überall Gleichheit gelten.

(ii) Beweis per Induktion über n.

$n = 1$: Klar.

$n = 2$: Beweis bereits bei der Einführung der Idealmultiplikation geführt.

$n \to n+1$:

$$\begin{aligned} \mathfrak{a}_1 \cdot \ldots \cdot \mathfrak{a}_{n+1} &= (\mathfrak{a}_1 \cdot \ldots \cdot \mathfrak{a}_n)\,\mathfrak{a}_{n+1} \\ &\overset{(*)}{=} (\mathfrak{a}_1 \cdot \ldots \cdot \mathfrak{a}_n) \cap \mathfrak{a}_{n+1} \\ &\overset{\text{Ind. Vor.}}{=} \bigcap_{i=1}^{n+1} \mathfrak{a}_i \end{aligned}$$

$(*)$: Per Induktionsvoraussetzung für $n = 2$ und (i).

3.24. Chinesischer Restsatz

Es sei R ein kommutativer Ring mit 1. Dann gilt für paarweise komaximale Ideale $\mathfrak{a}_i$ $(1 \le i \le n)$ (d.h. $\mathfrak{a}_i + \mathfrak{a}_j = R$ $(1 \le i < j \le n)$):

$$R/\mathfrak{a}_1 \cdot \ldots \cdot \mathfrak{a}_n \cong \prod_{i=1}^{n} R/\mathfrak{a}_i$$

Lösung simultaner Kongruenzen:

Suche alle x mit

$$\begin{aligned} x &\equiv 2 \bmod 5, \quad \mathfrak{a}_1 = 5\mathbb{Z} \\ x &\equiv 4 \bmod 11, \quad \mathfrak{a}_2 = 11\mathbb{Z} \\ x &\equiv 7 \bmod 12, \quad \mathfrak{a}_3 = 12\mathbb{Z} \end{aligned}$$

oder "ewiger Kalender".

Beweis:
Betrachte Abbildung

$$\phi \,:\, R \to \prod_{i=1}^{n} R/\mathfrak{a}_i \,:\, x \mapsto (x + \mathfrak{a}_1, \ldots, x + \mathfrak{a}_n).$$

Offensichtlich ist ϕ ein Ringhomomorphismus mit $\ker \phi = \mathfrak{a}_1 \cap \ldots \cap \mathfrak{a}_n = \mathfrak{a}_1 \cdot \ldots \cdot \mathfrak{a}_n$. Es bleibt "$\phi$ surjektiv" zu zeigen, dann folgt die Behauptung aus dem Homomorphiesatz für Ringe. Nach Voraussetzung existieren $e_{ij} \in \mathfrak{a}_i,\ e_{ji} \in \mathfrak{a}_j$ mit $1 = e_{ij} + e_{ji}$ $(1 \le i < j \le n)$. Setze

$$\tilde{e}_i := \prod_{\substack{j=1 \\ j \ne i}}^{n} e_{ji} \quad (1 \le i \le n).$$

$$\tilde{e}_i \equiv \begin{cases} 0 \bmod \mathfrak{a}_j \\ 1 \bmod \mathfrak{a}_i \quad (j \ne i). \end{cases}$$

Ist dann $(x_1 + \mathfrak{a}_1, \ldots, x_n + \mathfrak{a}_n) \in \prod_{i=1}^{n} R/\mathfrak{a}_i$ vorgelegt, so ist dies Bild von $x = \sum_{i=1}^{n} x_i\, \tilde{e}_i$. Denn für $\tilde{e}_i$ gilt $\tilde{e}_i \in \mathfrak{a}_j$ $(1 \le j \le n,\, j \ne i)$,

$$\tilde{e}_i \equiv \begin{cases} 1 \bmod \mathfrak{a}_i \\ 0 \bmod \mathfrak{a}_j \quad (j \ne i) \end{cases}.$$

□

$$R/(\mathfrak{a}_1 \cdot \ldots \cdot \mathfrak{a}_n) \;=\; \underset{i=1}{\overset{n}{u}} \Big(R/(\mathfrak{a}_1 \cdot \ldots \cdot \mathfrak{a}_n)\Big)\tilde{e}_i \;\cong\; R/\mathfrak{a}_1 \oplus \ldots \oplus R/\mathfrak{a}_n.$$

Bemerkung:
Der Satz sagt aus, daß sich simultane Kongruenzen nach komaximalen Idealen stets lösen lassen. Er beschreibt die Lösungsmenge und gibt

sogar ein (konstruktives) Verfahren zu ihrer Bestimmung an. ("Zerlegung der Eins in orthogonale Idempotente").

Newton-Verfahren

Eine explizite Berechnung des Urbildes von $(x_1 + \mathfrak{a}_1, \cdots, x_n + \mathfrak{a}_n)$ ist allerdings schneller möglich mit dem folgenden Verfahren, welches der Newton-Interpolation ähnelt.
Setze

$$e_i := \prod_{j=1}^{i-1} e_{ji} \quad (1 < i \leq n)$$

ähnlich zum Beweis sowie $y_1 = x_1$ und iterativ $y_{k+1} = y_k + (x_{k+1} - y_k)e_{k+1} \quad (1 \leq k < n)$.
Dann leistet $x = y_n$ das Gewünschte.
(Dazu beachte man, dass

$$e_{k+1} \equiv \begin{cases} 0 & \bmod \mathfrak{a}_j \quad \text{für } j \leq k \\ 1 & \bmod \mathfrak{a}_{k+1} \end{cases}$$

gilt.)

Beispiel:
Löse $x \equiv 2 \bmod 5,\ x \equiv 4 \bmod 11,\ x \equiv 7 \bmod 12$.
1. Lösungmöglichkeit: Raten.
2. Lösungmöglichkeit: per (2.38)!
$\mathfrak{a}_1 = 5\mathbb{Z},\ \mathfrak{a}_2 = 11\mathbb{Z},\ \mathfrak{a}_3 = 12\mathbb{Z},\ R = \mathbb{Z}$.
$\mathfrak{a}_i + \mathfrak{a}_j = R,\ e_{ij} + f_{ij} = 1$ mit $e_{ij} \in \mathfrak{a}_i$ und $f_{ij} \in \mathfrak{a}_j$.

i	1	1	2	2	3	3
j	2	3	1	3	1	2
e_{ij}	-10	25	11	-11	-24	12
f_{ij}	11	-24	-10	12	25	-11

$$\begin{array}{rcccl} \tilde{e}_1 & = & f_{12}\, f_{13} & = & -264 \\ \tilde{e}_2 & = & f_{21}\, f_{23} & = & -120 \\ \tilde{e}_3 & = & f_{31}\, f_{32} & = & -75 \end{array}.$$

Gesucht sind u, v mit $u \cdot 5 + v \cdot 11 = 1 \ \Rightarrow\ 1 = -2 \cdot 5 + (+11) = 5 \cdot 5 - 2 \cdot 12 = -11 + 12$.

$$\begin{aligned} x &= x_1\tilde{e}_1 + x_2\tilde{e}_2 + x_3\tilde{e}_3 \\ &= -2 \cdot 264 - 4 \cdot 120 - 7 \cdot 275 \\ &= -528 - 480 - 1925 \\ &= -2933; \end{aligned}$$

das Ergebnis ist modulo $5 \cdot 11 \cdot 12 = 660$ eindeutig, also ist die kleinste positive Lösung 367, die betraglich kleinste Lösung -293.
Gesamtlösung ist $367 + 660\mathbb{Z}$.

Nach dem Newton Verfahren verläuft die Berechnung wie folgt:
$e_1 = 1, e_2 = -10, e_3 = -275$,
$y_1 = 2, y_2 = 2 + (4 - 2)(-10) = -18$,

$y_3 = -18 + (7 - (-18))(-275) = -6893 \equiv -293 \bmod 660.$

3.25. Definition

Es sei M eine nicht leere Menge. Eine Relation $\leq$ auf M heißt Halbordnung, falls die Bedingungen

(i) $x \leq x$
(ii) $x \leq y \wedge y \leq x \;\Rightarrow\; x = y$
(iii) $x \leq y \wedge y \leq z \;\Rightarrow\; x \leq z$

$\forall x,\, y,\, z \in M$ erfüllt sind.

Beispiele:

(i) $(\mathbb{Z}, \geq 0)$, $(\mathbb{R}, \geq 0)$, lexikographische Ordung im $\mathbb{R}^n$;
(ii) $(\mathbb{C}, |\ |)$ erfüllt (i), (iii) aber nicht (ii);
(iii) $\mathfrak{P}(M)$ mit $\subseteq$:
$M = \{1, 2\}$ hat $\mathfrak{P}(M) = \{\emptyset, \{1\}, \{2\}, M\}$.
$\emptyset \subseteq \{1\} \subseteq M$, $\emptyset \subseteq \{2\} \subseteq M$. $\{1\}$ ist in $\{2\}$ nicht enthalten.

3.26. Definition

Es sei M eine nicht leere Menge. Eine Halbordung $\leq$ auf M heißt Ordnung, falls für alle $x,\, y \in M$ stets $x \leq y$ oder $y \leq x$ gilt. In diesem Fall heißt M Kette.

Beispiel:
$(\mathbb{R}, \geq)$, nicht aber $(\mathbb{C}, |\ |)$.

3.27. Definition

Es sei $M \neq \emptyset$ und $\leq$ eine Halbordnung auf M. Für $A \subseteq M$ heißt $s(A) \in M$ obere Schranke von A, falls $x \leq s(A)\ \forall a \in A$ gilt. Für $A \subseteq M$ heißt $m(A) \in A$ maximales Element von A, falls aus $a \in A$ und $m(A) \leq a$ stets $a = m(A)$ folgt. Eine Teilmenge X von M heißt induktiv geordnet, falls jede Kette in X eine obere Schranke in X (!) besitzt.

Beispiel:
$A = \{\{1\}, \{2\}, \emptyset\} \subseteq \mathfrak{P}(\{1, 2\})$;
Es ist $s(A) = \{1, 2\}$; sowohl $\{1\}$ als auch $\{2\}$ sind maximale Elemente von A.

3.28. Zornsches Lemma

Jede nicht leere induktiv geordnete Menge besitzt ein maximales Element.

3.29. Definition

Es sei R Ring mit Ideal $\mathfrak{a}$. $\mathfrak{a}$ heißt maximal, falls es kein Ideal $\mathfrak{b}$ mit $\mathfrak{a} \subset \mathfrak{b} \subset R$ gibt.

3.30. Satz

Es sei V ein Vektorraum über dem Körper K und $M \subseteq V$ linear unabhängig. Dann existiert eine Basis B von V mit $M \subseteq B$.

Beweis:
Es bestehe $Q \subseteq P(V)$ aus allen linear unabhängigen Teilmengen von V, die M enthalten. Wegen $M \in Q$ folgt $Q \neq \emptyset$. Ist K eine Kette in Q, so gilt

$$m(K) := \bigcup_{N \in K} N \ \in Q.$$

Denn sind $x_1, \ldots, x_n \in m(K)$, d.h. $x_i \in N_i \ (1 \leq i \leq n)$, so existiert ein maximaler Index j, mit $x_i \in N_j \ (1 \leq i \leq n)$, also sind $x_1, \ldots, x_n$ linear unabhängig.
Nach dem Zornschen Lemma existiert in Q ein maximales Element B. Nach Voraussetzung ist B linear unabhängig. Es bleibt $[B] = V$ zu zeigen.
Ist $x \in V \backslash [B]$, so gilt speziell $x \neq 0$, und $\tilde{B} := B \cup \{x\}$ ist linear abhängig. Also existieren $x_1, \ldots, x_r \in B$ und $\lambda_1, \ldots, \lambda_r, \ \lambda \in K$, nicht alle 0, mit

$$\sum_{i=1}^{r} \lambda_i x_i + \lambda\, x = 0.$$

Für $\lambda \neq 0$ folgt $x \in [B]$. Für $\lambda = 0$ folgt B linear abhängig. Widerspruch!

□

Bemerkung:
Also folgt die Behauptung. Für $M = \emptyset$ liefert dies die Existenz einer Basis von V.

3.31. Satz

Es sei R ein Ring mit $1 \neq 0$ und $\mathfrak{a} \neq R$ ein Ideal von R. Dann ist $\mathfrak{a}$ in einem maximalen Ideal $\mathfrak{m}$ von R enthalten.

Bemerkung:
Für $\mathfrak{a} = \{0\}$ liefert dies die Existenz maximaler Ideale (in Ringen R mit Eins).

Beweis:

Es sei $\mathfrak{M}$ die Menge aller Ideale $\mathfrak{b}$ von R mit $R \supset \mathfrak{b} \supseteq \mathfrak{a}$, dann ist $\mathfrak{M} \neq \emptyset$ induktiv geordnet bzgl. $\subseteq$. (Die Vereinigungsmenge einer aufsteigenden Kette von Idealen ist wieder ein Ideal, welches in unserem Fall 1 nicht enthält.)
Nach dem Zornschen Lemma existiert ein maximales Element $\mathfrak{m}$ aus $\mathfrak{M}$. Wegen $1 \notin \mathfrak{m}$ ist $\mathfrak{m}$ maximales Ideal.

□

Bemerkung:

(i) In $\mathbb{Z}$ sind $p\mathbb{Z}$, p Primzahl, genau die maximalen Ideale.
(ii) Ist R Körper, so ist $\{0\}$ einziges maximales Ideal.

3.32. Satz

Es sei R ein Ring mit Ideal $\mathfrak{m}$. Dann gilt:

(i) $\mathfrak{m} \neq R$ ist maximal $\Leftrightarrow$ $R/\mathfrak{m}$ enthält nur die Ideale $\mathfrak{m}$ und $R/\mathfrak{m}$.
(ii) Ist R kommutativ mit $1 \neq 0$, so ist $\mathfrak{m}$ genau dann maximal, falls $R/\mathfrak{m}$ Körper ist.

Beweis:

(i) Gemäß (2.15).
(ii)

$$\begin{aligned} R/\mathfrak{m} \text{ Körper} &\Leftrightarrow \forall x \in R\backslash\mathfrak{m},\ \exists\, \lambda \in R :\ (x+\mathfrak{m})\,(\lambda+\mathfrak{m}) = 1+\mathfrak{m} \\ &\Leftrightarrow \forall x \in R\backslash\mathfrak{m},\ \exists \lambda \in R :\ \lambda x \equiv 1 \bmod \mathfrak{m} \\ &\Leftrightarrow \forall x \in R\backslash\mathfrak{m},\ \exists m \in \mathfrak{m},\ \exists \lambda \in R :\ \lambda x + m = 1 \\ &\Leftrightarrow Rx + \mathfrak{m} = R\ \ \forall x \in R\backslash\mathfrak{m} \\ &\Leftrightarrow \mathfrak{m} \text{ maximal.} \end{aligned}$$

□

3.33. Definition

Ein kommutativer Ring R mit Eins heißt lokaler Ring, falls R genau ein maximales Ideal besitzt.

3.34. Hilfssatz

R kommutativ mit 1. R lokaler Ring $\Leftrightarrow$ $R\backslash R^\times$ ist Ideal in R.

Beweis:
"$\Leftarrow$":
Jedes Ideal $\mathfrak{a}$ in R mit $\mathfrak{a} \neq R$ beteht aus Nichteinheiten.
"$\Rightarrow$":
Für $x \in R,\ x \notin U(R)$, folgt $Rx = (x) \subseteq \mathfrak{m}$ für ein passendes maximales Ideal $\mathfrak{m}$ von R.

□

Beispiel:
$\dfrac{\mathbb{Z}}{\mathbb{Z}\backslash p\mathbb{Z}} = \left\{ \dfrac{r}{s} \in \mathbb{Q} \,\middle|\, r \in \mathbb{Z},\, p \nmid s \right\}$ ist lokaler Ring mit $\mathfrak{m} = \dfrac{p\mathbb{Z}}{\mathbb{Z}\backslash p\mathbb{Z}}$.

Quotientenbildung bei kommutativen Ringen R**.** Es sei R ein kommutativer Ring und $S \subseteq R$ eine multiplikative Halbgruppe. Als "Brüche" (mit Nennern in S) definiert man die Menge $R \times S$ der geordneten Paare $(r,\, s)$. Wie bei der Konstruktion der rationalen aus den ganzen Zahlen bildet man auf $R \times S$ eine Äquivalenzrelation, deren Klassen dann die gewünschten Brüche bilden. Wegen der möglichen Existenz von Nullteilern muß man allgemeiner

$$(r,\, s) \sim (\tilde{r},\, \tilde{s}) \quad :\Leftrightarrow \quad \exists t \in S \,:\, t\,(r\tilde{s} - \tilde{r}s) = 0 \text{ definieren.}$$

Dies ist tatsächlich eine Äquivalenzrelation, denn Reflexivität und Symmetrie sind klar und bzgl. der Transitivität bemerken wir:

$$\begin{aligned}
&(r_1,\, s_1) \sim (r_2,\, s_2) \,\wedge\, (r_2,\, s_2) \sim (r_3,\, s_3)\\
&\Leftrightarrow\ \exists t_1,\, t_2 \in S \,:\, t_1\,(r_1 s_2 - r_2 s_1) = 0 = t_2\,(r_2 s_3 - r_3 s_2)\\
&\Rightarrow\ \exists t_1,\, t_2 \in S \,:\quad 0 \;=\; t_1 t_2 s_3\,(r_1 s_2 - r_2 s_1) + t_1 t_2 s_1\,(r_2 s_3 - r_3 s_2)\\
&\qquad\qquad\qquad\quad\;\; =\; t_1 t_2 s_2\,(s_3 r_1 - s_1 r_3)\\
&\qquad\qquad\qquad\quad\;\; =\; t\,(s_3 r_1 - s_1 r_3) \;\text{ für }\; t = t_1 t_2 s_2\\
&\Rightarrow\ \exists t \in S \,:\, t\,(s_3 r_1 - s_1 r_3) = 0\\
&\Leftrightarrow\ (r_1,\, s_1) \sim (r_3,\, s_3).
\end{aligned}$$

Die Äquivalenzklassen bilden Brüche:

$$K_{r,s} := \{(\tilde{r},\, \tilde{s}) \in R \times S \mid (r,\, s) \sim (\tilde{r},\, \tilde{s})\} =: \frac{r}{s}.$$

Setze

$$\begin{aligned}
K_{r_1,s_1} + K_{r_2,s_2} &= K_{r_1 s_2 + r_2 s_1,\, s_1 s_2},\\
K_{r_1,s_1} \cdot K_{r_2,s_2} &= K_{r_1 s_1,\, r_2 s_2}.
\end{aligned}$$

(Für die Äquivalenzklassen $\frac{r_1}{s_1}$, $\frac{r_2}{s_2}$ von $(r_1,\, s_1)$, $(r_2,\, s_2) \in R \times S$ definieren wir eine Addition und eine Multiplikation über die Vertreter:

$$\frac{r_1}{s_1} + \frac{r_2}{s_2} := \frac{r_1 s_2 + r_2 s_1}{s_1 s_2}, \qquad \frac{r_1}{s_1} \cdot \frac{r_2}{s_2} := \frac{r_1 r_2}{s_1 s_2}.)$$

Zur Multiplikation: Sind auch $(\tilde{r}_1,\, \tilde{s}_1) \in \frac{r_1}{s_1}$, $(\tilde{r}_2,\, \tilde{s}_2) \in \frac{r_2}{s_2}$, so ist $(r_1 r_2,\, s_1 s_2) \sim (\tilde{r}_1 \tilde{r}_2,\, \tilde{s}_1 \tilde{s}_2)$ wegen

$$\begin{aligned}
&(r_1,\, s_1) \sim (\tilde{r}_1,\, \tilde{s}_1) \,\wedge\, (r_2,\, s_2) \sim (\tilde{r}_2,\, \tilde{s}_2)\\
&\Leftrightarrow\ \exists t_1,\, t_2 \in S \,:\, t_1\,(r_1 \tilde{s}_1 - \tilde{r}_1 s_1) = 0 = t_2\,(r_2 \tilde{s}_2 - s_2 \tilde{r}_2)\\
&\Rightarrow\ \exists t_1,\, t_2 \in S \,:\, 0 = t_1 t_2\,(r_1 r_2 \tilde{s}_1 \tilde{s}_2 - \tilde{r}_1 r_2 s_1 \tilde{s}_2) + t_1 t_2\,(\tilde{r}_1 r_2 s_1 \tilde{s}_2 - \tilde{r}_1 \tilde{r}_2 s_1 s_2)\\
&\Rightarrow\ \exists t_1 t_2 \in S \,:\, 0 = t_1 t_2\,(r_1 r_2 \tilde{s}_1 \tilde{s}_2 - \tilde{r}_1 \tilde{r}_2 s_1 s_2)\\
&\Leftrightarrow\ (r_1 r_2,\, s_1 s_2) \sim (\tilde{r}_1 \tilde{r}_2,\, \tilde{s}_1 \tilde{s}_2);
\end{aligned}$$

für die Addition folgert man aus

$$\begin{aligned}
&\exists t_1,\, t_2 \in S \,:\, 0 = t_1\,(r_1 \tilde{s}_1 - \tilde{r}_1 s_1) = t_2\,(r_2 \tilde{s}_2 - s_2 \tilde{r}_2)\\
&\Rightarrow\ \exists t_1,\, t_2 \in S \,:\, 0 = t_1 t_2\,(r_1 \tilde{s}_1 s_2 \tilde{s}_2 - \tilde{r}_1 s_1 s_2 \tilde{s}_2 + r_2 \tilde{s}_2 s_1 \tilde{s}_1 - s_2 \tilde{r}_2 s_1 \tilde{s}_1)
\end{aligned}$$

$\Rightarrow\ \exists t_1,\, t_2 \in S\,:\ 0 = t_1 t_2\,((r_1 s_2 + r_2 s_1)\,\tilde{s}_1\tilde{s}_2 - (\tilde{r}_1\tilde{s}_2 + \tilde{r}_2\tilde{s}_1)\,s_1 s_2)$
$\Leftrightarrow\ (r_1 s_2 + r_2 s_1,\, s_1 s_2) \sim (\tilde{r}_1\tilde{s}_2 + \tilde{r}_2\tilde{s}_1,\, \tilde{s}_1\tilde{s}_2).$

Die Rechengesetze von R übertragen sich über die Vertreter auf

$$R_S := \left\{ \frac{r}{s} \mid r \in R,\, s \in S \right\} \quad \text{für} \quad \frac{r}{s} = K_{r,s}.$$

Hierfür sind die Assoziativität von Addition und Multiplikation nachzurechnen. Neues Nullelement ist $K_{0,s}$, inverses Element zu $K_{r,s}$ ist $K_{-r,s}$.

Folglich bildet R_S einen kommutativen Ring mit Einselement $\frac{s}{s}$:

$$\frac{r}{s} \cdot \frac{s}{s} = \frac{r}{s} \quad \forall \frac{r}{s} \in R_S.$$

R läßt sich homomorph in R_S abbilden mittels

$$\iota\ :\ R \to R_S\ :\ r \mapsto \frac{rs}{s}$$

für ein beliebiges $s \in S$.
Im Fall, daß $S \neq 0$ keine Nullteiler enthält, ist ι sogar Monomorphismus, also Einbettung, d.h. R_S läßt sich als Ringerweiterung von R auffassen.

Spezialfälle:

(i) $S \ni 0\ \Rightarrow\ R_S$ ist trivial.
(ii) $\emptyset \neq S$ besteht aus allen Nicht-Nullteilern $\neq 0$ von R. In diesem Fall heißt R_S der (vollständige) Quotientenring $\mathfrak{Q}(R)$ von R. Sind speziell alle Elemente $\neq 0$ keine Nullteiler, so ist $\mathfrak{Q}(R)$ ein Körper.

Beispiel:

(i) $R = \mathbb{Z},\ S = \mathbb{Z}\backslash\{0\}\ \Rightarrow\ R_S \cong \mathbb{Q}.$
(ii) $R = \mathbb{Z},\ S = \{2^\nu \mid \nu \in \mathbb{Z}^{\geq 0}\}\ \Rightarrow\ R_S = \{\frac{a}{2^\nu} \mid \nu \in \mathbb{Z}^{\geq 0}\}.$
(iii) $R = \mathbb{Z},\ S = \mathbb{Z}\backslash p\mathbb{Z} \quad (p \in \mathbb{P})\ \Rightarrow\ R_S = \mathbb{Z}_{(p)}$ ("p-Lokalisierung von $\mathbb{Z}$").

3.35. Definition

Es sei R ein kommutativer Ring. Ein Ideal $R \supsetneq \mathfrak{p}$ von R heißt Primideal, falls für $a,\, b \in R$ mit $ab \in \mathfrak{p}$ stets $a \in \mathfrak{p}$ oder $b \in \mathfrak{p}$ folgt.

Beispiele:

(i) $R = \mathbb{Z}$, alle Primideale sind von der Form $p\mathbb{Z}$ mit p Primzahl.
(ii) $\{0\}$ ist Primideal, falls R keine Nullteiler $\neq 0$ besitzt.

3.36. Satz (Charakterisierung von Primidealen)

Es sei R ein kommutativer Ring und $\mathfrak{a} \subsetneq R$ ein Ideal in R. Dann sind äquivalent:

(i) $\mathfrak{a}$ Primideal,
(ii) $\forall a, b \in R$ mit $a \notin \mathfrak{a}$ und $b \notin \mathfrak{a} \Rightarrow ab \notin \mathfrak{a}$,
(iii) Für Ideale $\mathfrak{b}, \mathfrak{c}$ von R mit $\mathfrak{bc} \subseteq \mathfrak{a}$ folgt $\mathfrak{b} \subseteq \mathfrak{a}$ oder $\mathfrak{c} \subseteq \mathfrak{a}$.
(iv) $R\backslash\mathfrak{a}$ ist multiplikative Halbgruppe,
(v) $R/\mathfrak{a}$ ist nullteilerfrei.

Beweis:
(i) $\Rightarrow$ (ii): nach Definition;

(ii) $\Rightarrow$ (iii): Wäre die Aussage falsch, existierten Elemente $b \in \mathfrak{b} \setminus \mathfrak{a},\ c \in \mathfrak{c} \setminus \mathfrak{a}$ mit $b \cdot c \in \mathfrak{a}$ im Widerspruch zur Voraussetzung.

(iii) $\Rightarrow$ (iv): Sind $a, b \in R \setminus \mathfrak{a}$, so folgt $(a) = Ra + \mathbb{Z}a$, $(b) = Rb + \mathbb{Z}b$, $(a)(b) = Rab + \mathbb{Z}ab = (ab)$. Wegen $(a) \not\subseteq \mathfrak{a}$ und $(b) \not\subseteq \mathfrak{a}$ muss $(ab) \not\subseteq \mathfrak{a}$ gelten, also $ab \notin \mathfrak{a}$.

(iv) $\Rightarrow$ (v): für $a + \mathfrak{a}$, $b + \mathfrak{a}$, beide ungleich $\mathfrak{a}$, folgt a, $b \in R\backslash\mathfrak{a}$, damit $ab \in R\backslash\mathfrak{a}$ und

$$(a + \mathfrak{a})(b + \mathfrak{a}) = ab + \mathfrak{a} \neq \mathfrak{a};$$

(v) $\Rightarrow$ (i): es seien a, $b \in R$ mit $ab \in \mathfrak{a}$, also

$$\mathfrak{a} = ab + \mathfrak{a} = (a + \mathfrak{a})(b + \mathfrak{a})$$

und folglich $(a + \mathfrak{a} = \mathfrak{a} \Leftrightarrow a \in \mathfrak{a})$ oder $(b + \mathfrak{a} = \mathfrak{a} \Leftrightarrow b \in \mathfrak{a})$.

□

Bemerkung:

(i) In einem kommutativen Ring mit 1 ist jedes maximale Ideal ein Primideal, also ist jedes Ideal $\mathfrak{a} \subset R$ von R in einem Primideal enthalten.

(ii) In einem kommutativen Ring R mit Primideal $\mathfrak{p}$ bildet $R\backslash\mathfrak{p}$ eine multiplikative Halbgruppe S. Dann heißt

$$R_S = R_{R\backslash\mathfrak{p}} = \frac{R}{R\backslash\mathfrak{p}} =: R_{\mathfrak{p}}$$

Lokalisierung von R bei $\mathfrak{p}$. $R_{\mathfrak{p}}$ ist ein lokaler Ring (siehe Übungsblatt 7).

(Falls $R \ni 1 \ :\ R \to \frac{R}{R\backslash\mathfrak{p}} \ :\ r \mapsto \frac{r}{1}$ ist Ringmonomorphismus.)

Speziell: $R = \mathbb{Z}$, $\mathfrak{p} = p\mathbb{Z}$ für $p \in \mathbb{P}$:

$$R_{(p)} = \left\{ \frac{m}{n} \middle| \, m \in \mathbb{Z},\ n \in \mathbb{Z} \text{ mit } p \nmid n \right\}.$$

(iii) 0 Primideal $\Rightarrow$ R nullteilerfrei.

(iv) $R \ni 1$, $\mathfrak{p}$ Primideal, $R/\mathfrak{p}$ nullteilerfrei:
$R/\mathfrak{p}$ endlich $\Rightarrow$ $R/\mathfrak{p}$ Körper
$\overset{2.29}{\Rightarrow}$ $\mathfrak{p}$ maximales Ideal.

Beispiele:

(i) $\mathfrak{p} = 2\mathbb{Z} \Rightarrow R_{\mathfrak{p}} = \left\{ \frac{a}{b} \,\middle|\, a, b \in \mathbb{Z},\ 2 \nmid b \right\}$.

(ii) $R = 2\mathbb{Z}, \mathfrak{a} = 4\mathbb{Z}$:
$2 \cdot 2 \in \mathfrak{a}$, also ist $\mathfrak{a}$ kein Primideal. $\mathfrak{a}$ ist maximal, denn $x \in R \backslash \mathfrak{a}$ hat die Gestalt $2(2m+1)$,
$(\mathfrak{a}, x) \ni x - 4m = 2$.

3.37. Definition

Ein Ring R, in dem jedes Ideal endlich erzeugt ist, heißt noetherscher Ring.

Beispiel: $R = \mathbb{Z}$, dort ist jedes Ideal Hauptideal.

3.38. Satz (Charakterisierung noetherscher Ringe)

Für Ringe R sind folgende Aussagen äquivalent:

(i) R ist noethersch;
(ii) Jede aufsteigende Kette von Idealen $\mathfrak{a}_1 \subseteq \mathfrak{a}_2 \subseteq \ldots \subseteq \mathfrak{a}_k \subseteq \ldots$ wird stationär (bricht ab), d.h. es existiert $n \in \mathbb{N}$ mit $\mathfrak{a}_{n+i} = \mathfrak{a}_n \ \forall i \in \mathbb{N}$;
(iii) In jeder nicht leeren Menge von Idealen gibt es ein (bzgl. $\subseteq$) maximales Element.

Beweis:
(i) $\Rightarrow$ (ii):
Für eine vorgelegte Kette von Idealen ist deren Vereinigung $\mathfrak{a}$ wieder ein Ideal(!), welches etwa durch $a_1, \ldots, a_m$ erzeugt wird. Für $a_i \in \mathfrak{a}_{j_i}$ $(1 \leq i \leq m)$ gilt dann also $\mathfrak{a}_{j_0} \supseteq (a_1, \ldots, a_m) \supseteq \mathfrak{a}_{j_0}$, $a_i \in \mathfrak{a}_{j_0}$ $(1 \leq i \leq m)$ mit $j_0 := \max\{j_1, \ldots, j_m\}$, und wir erhalten etwa $n = j_0$, d.h. die Kette wird ab $\mathfrak{a}_{j_0}$ stationär.
(ii) $\Rightarrow$ (iii):
Es sei $\mathfrak{M} \neq \emptyset$ eine Menge von Idealen. Wähle $\mathfrak{a}_1 \in \mathfrak{M}$. Ist $\mathfrak{a}_1$ maximal, so sind wir fertig. Ist $\mathfrak{a}_1$ nicht maximal, so exitiert $\mathfrak{a}_2 \in \mathfrak{M}$, $\mathfrak{a}_2 \supset \mathfrak{a}_1$. Man erhält so eine aufsteigende Kette, die nach Voraussetzung stationär werden muß. Das diesbezügliche $\mathfrak{a}_n$ ist dann in $\mathfrak{M}$ maximal.
(iii) $\Rightarrow$ (i):
Es sei $\mathfrak{a}$ ein Ideal von R. Bilde

$$\mathfrak{M} := \{\mathfrak{b} \mid \mathfrak{b} \text{ endlich erzeugtes Ideal in } R \text{ mit } \mathfrak{b} \subseteq \mathfrak{a}\}.$$

Wegen $\{0\} \in \mathfrak{M}$ ist $\mathfrak{M} \neq \emptyset$. Sei $\mathfrak{m}$ maximales Element von $\mathfrak{M}$, etwa $\mathfrak{m} =< a_1, \ldots, a_k >$. Für beliebiges $a \in \mathfrak{a}$ ist $\tilde{\mathfrak{m}} := (a_1, \ldots, a_k, a)$ in $\mathfrak{M}$, also gleich $\mathfrak{m}$, also folgt $\mathfrak{a} = \mathfrak{m}$.

□

Bemerkung:
Es sei R ein noetherscher Ring und $f : R \to S$ ein Ringepimorphismus. Dann ist S noethersch.
(Speziell: Ist $\mathfrak{a}$ ein Ideal von R, so ist $R/\mathfrak{a}$ noethersch.)

Beweis:
Es sei $\mathfrak{a}$ ein Ideal von S, dann ist etwa $f^{-1}(\mathfrak{a}) =< a_1, \ldots, a_k >$, und es folgt $\mathfrak{a} = (f(a_1), \ldots, f(a_k))$.

□

Teilbarkeit in Ringen

Sinnvollerweise sind Nullteiler auszuschließen!
Ferner: $R \ni 1 \neq 0$ und R sollte kommutativ sein.

3.39. Definition

Ein nullteilerfreier, kommutativer Ring $R \neq \{0\}$ heißt Integritätsring.

Bemerkung:
In Integritätsringen gilt die Kürzungsregel (2.19)(i), endliche Integritätsringe sind Körper (2.19)(ii). R kommuativer Ring, $\mathfrak{a} \subset R$ Ideal: $\mathfrak{a}$ Primideal $\Leftrightarrow$ $R/\mathfrak{a}$ Integritätsring nach (2.33).

Beispiel: Alle Ideale $\neq \{0\}$ in $\mathbb{Z}$ und Körper sind Integritätsringe.

3.40. Definition

Es seien R ein Integritätsring mit 1 und $a, b \in R$.
a heißt Teiler von b (a teilt b, b ist Vielfaches von a, $a|b$), falls $c \in R$ mit $b = ac$ existiert.
a heißt assoziiert zu b ($a \sim b$), falls $a|b$ und $b|a$ gilt.
$c \in R$ heißt größter gemeinsamer Teiler (ggT) von a, b, falls $c|a$ und $c|b$ und für alle $d \in R$ mit $d|a$, $d|b$ auch $d|c$ gilt.
a, b heißen teilerfremd, falls ggT $(a, b) \in U(R)$ ist.
$c \in R$ heißt kleinstes gemeinsames Vielfaches (kgV) von a, b, falls $a|c$, $b|c$ und für alle $d \in R$ mit $a|d$, $b|d$ auch $c|d$ gilt.
Ein Element $p \in R \backslash U(R)$, $p \neq 0$, heißt Primelement von R, wenn für alle $a, b \in R$ mit $p|ab$ stets $p|a$ oder $p|b$ folgt.
Ein Element $a \in R \backslash U(R)$, $q \neq 0$ heißt irreduzibel (unzerlegbar), wenn für alle $a, b \in R$ mit $ab = q$ stets $a \in U(R)$ oder $b \in U(R)$ folgt.

Beispiele:

(i) Übliche Definitionen in $\mathbb{Z}$; die zu $a \in \mathbb{Z}$ assoziierten Elemente sind $\pm a$ ($U(R) = \{\pm 1\}$), die Primzahlen sind die Primelemente und stimmen mit den irreduziblen Elemente überein.

(ii) Es sei $R = \mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in \mathbb{Z}\}$. Es gibt unendlich viele assoziierte Elemente $a\,(-1)^h\,(1+\sqrt{2})^k$ $(h \in \{0, 1\},\ k \in \mathbb{Z})$.

$$1+\sqrt{2} = \frac{(1+\sqrt{2})\,(1-\sqrt{2})}{1-\sqrt{2}} = \frac{-1}{1-\sqrt{2}} \quad \Rightarrow \quad \begin{array}{rcl} (1-\sqrt{2})^{-1} & = & -(1+\sqrt{2}), \\ (1+\sqrt{2})^{-1} & = & -(1-\sqrt{2}) \end{array}$$

$((1+\sqrt{2})^k$ $(k \in \mathbb{Z})$ sind alle verschieden!)
$\sqrt{2}$ ist irreduzibel (und sogar Primelement!).
(Denn für $S := \mathbb{Z}[\sqrt{m}]$ $(m \in \mathbb{Z},\ \nexists a \in \mathbb{Z}^{\geq 2} : a^2 | m)$ ist

$$N : \mathbb{Z}[\sqrt{m}] \to \mathbb{Z} : a + b\sqrt{m} \mapsto a^2 - mb^2$$

eine multiplikativer Homomorphismus. Wäre nun $\sqrt{2} = xy$ in $\mathbb{Z}[\sqrt{2}]$, so folgte $N(\sqrt{2}) = -2 = N(x)\,N(y)$ in $\mathbb{Z}$, also $N(x) = \pm 1$ oder $N(y) = \pm 1$. Ist o.B.d.A. $N(x) = \pm 1$, so gilt für $x = u+v\sqrt{2}$: $\pm 1 = (u+v\sqrt{2})\,(u-v\sqrt{2})$, d.h. $x \in U(R)$.)

Der Primelementnachweis verläuft ähnlich.

(iii) Es sei $R = \mathbb{Z}[\sqrt{-5}]$. Hierin ist $U(R) = \{\pm 1\}$ $(= U(\mathbb{Z}))$, wegen

$$N(a + b\sqrt{-5}) = a^2 + 5b^2 = 1 \quad \Leftrightarrow \quad b = 0,\ a = \pm 1.$$

Ferner ist $21 = 3 \cdot 7 = (4+\sqrt{-5})\,(4-\sqrt{-5}) = (1+2\sqrt{-5})\,(1-2\sqrt{-5})$.

Hierin sind die beteiligten Elemente offenbar (!) keine Primelemente, jedoch irreduzibel.

Beweis:

Es ist $N(3) = 9$, für $3 = xy$ mit $x,\ y \notin \{\pm 1\}$ folgt $N(x) = N(y) = 3$, jedoch ist $N(u + v\sqrt{-5}) = u^2 + 5v^2 = 3$ unlösbar in $\mathbb{Z}$. Also ist 3 irreduzibel. Der Nachweis für die anderen Elemente geht analog.

Bemerkung:
Jede Einheit teilt alle Elemente aus R; $x|x$ und $x|0$ für alle $x \in R$; $a \in R$ mit $a|1 \ \Rightarrow\ a$ ist Einheit $(a \in U(R))$; $a, b, x \in R$ und $a|b \ \Rightarrow\ ax|bx$; $a, r_i, x_i \in R$ $(1 \leq i \leq n)$ und $a|x_i$ $(1 \leq i \leq n) \ \Rightarrow\ a \Big| \sum_{i=1}^{n} r_i x_i$; $a, b, c \in R$ und $a|b,\ b|c \ \Rightarrow\ a|c$; $a, b \in R$: $a|b \ \Leftrightarrow\ b \in Ra \ \Leftrightarrow\ Rb \subseteq Ra$; $a, b \in R$:
$a \sim b \ \Leftrightarrow \exists e \in U(R) : b = ae \ \Leftrightarrow\ Ra = Rb$.
Jedes Primelement ist irreduzibel; dies ist eine Konsequenz des folgenden Hilfssatzes.

3.41. Hilfssatz

Es sei R ein Integritätsring mit 1 und $a \in R \backslash U(R),\ a \neq 0$. Dann gilt:

(i) a Primelement $\Leftrightarrow$ Ra Primideal;

(ii) a irreduzibel $\Leftrightarrow$ Ra maximales Hauptideal von R.
(a reduzibel $\Leftrightarrow$ Ra nicht maximal in der Menge der Hauptideale von R.)

Beweis:

(i)

$$\begin{aligned} a \text{ Primelement} &\Leftrightarrow (\forall x, y \in R : a|xy \Rightarrow a|x \vee a|y) \\ &\Leftrightarrow (\forall x, y \in R : xy \in Ra \Rightarrow x \in Ra \vee y \in Ra) \\ &\Leftrightarrow Ra \text{ Primideal.} \end{aligned}$$

(ii)

$$\begin{aligned} a \text{ irreduzibel} &\Leftrightarrow (\forall x, y \in R : a = xy \Rightarrow x \in U(R) \vee y \in U(R)) \\ &\Leftrightarrow (\forall x \in R : Ra \subseteq Rx \Rightarrow x \in U(R) \vee x \sim a) \\ &\Leftrightarrow (\forall x \in R : Ra \subset Rx \Rightarrow x \in U(R)) \\ &\Leftrightarrow Ra \text{ maximales Hauptideal von } R. \end{aligned}$$

□

3.42. Definition

Ein Integritätring mit 1, in dem jedes Ideal Hauptideal ist, heißt Hauptidealring.

Bemerkung:

(i) Hauptidealringe sind noethersch.
(ii) $\mathbb{Z}$ ist Hauptidealring, ebenso sind alle Körper Hauptidealringe.
(iii) Für Elemente $a \neq 0$ in Hauptidealringen gilt:
a Primelement $\Rightarrow$ a irreduzibel $\overset{(2.41)(ii)}{\Rightarrow}$ Ra maximales Hauptideal $\Rightarrow$ Ra Primideal $\overset{(2.41)(i)}{\Rightarrow}$ a Primelement.
Merke: In Hauptidealringen stimmen irreduzible und Primelemente überein. Speziell ist also $\mathbb{Z}[\sqrt{-5}]$ kein Hauptidealring.
(iv) Es seien $d, a_1, \ldots, a_n$ aus einem Hauptidealring R. Dann gilt:

$$d = \mathrm{ggT}\,(a_1, \ldots, a_n) \quad \Leftrightarrow \quad (a_1, \ldots, a_n) = Rd.$$

Dies bedeutet, daß ein größter gemeinsamer Teiler von $a_1, \ldots, a_n$ sich als $d = \sum_{i=1}^{n} r_i\, a_i$ $(r_i \in R)$ darstellen läßt.

Beweis:
Für jeden gemeinsamen Teiler $\tilde{d}$ von $a_1, \ldots, a_n$ gilt:

$$a_i = b_i\, \tilde{d} \quad \Leftrightarrow \quad (a_1, \ldots, a_n) \subseteq R\tilde{d}.$$

Ferner ist $(a_1, \ldots, a_n)$ ein Hauptideal Rd, für das dann $\tilde{d}|d$ und damit $d = \mathrm{ggT}\,(a_1, \ldots, a_n)$ gelten muß.

□

3.43. Satz

In einem Hauptidealring R läßt sich jedes $x \in R\backslash U(R),\ a \neq 0$, als Produkt von Primelementen darstellen.

Beweis:
Gemäß der vorrangehenden Bemerkung (iii) genügt es, eine Darstellung von x als Produkt irreduzibler Elemente nachzuweisen.
Ist x irreduzibel, sind wir fertig. Ansonsten existieren $x_1,\ x_2 \in R\backslash U(R)$ mit $x = x_1 x_2$, und es ist $(x) \subsetneqq (x_i)\ \ (1 \leq i \leq 2)$. Analog versuchen wir $x_1,\ x_2$ zu faktorisieren und erhalten so nach n Schritten x als Produkt von $y_1, \ldots, y_n \in R\backslash U(R)$. Dabei werden die Faktoren so angeordnet, daß im Falle nicht irreduzibler Faktoren diese die höchsten Indizes bekommen. Wegen

$$(x) \subsetneqq (y_2 \cdot \ldots \cdot y_n) \subsetneqq \ldots \subsetneqq (y_{n-1}\, y_n) \subsetneqq (y_n)$$

muß dieser Prozeß abbrechen (R ist als Hauptidealring noethersch), d.h. nach endlich vielen Schritten wird x ein Produkt irreduzibler Elemente.

□

3.44. Definition

Ein Integritätsring mit 1 heißt ZPE-Ring (Ring mit eindeutiger Primelementzerlegung, faktorieller Ring), falls sich jedes $x \in R\backslash U(R),\ x \neq 0$, bis auf Einheiten eindeutig als Produkt irreduzibler Elemente darstellen läßt.
(Aus $x = \varepsilon\, q_1 \cdot \ldots \cdot q_r = \tilde{\varepsilon}\, \tilde{q}_1 \cdot \ldots \cdot \tilde{q}_s$ mit $\varepsilon,\ \tilde{\varepsilon} \in U(R),\ q_i,\ \tilde{q}_j$ irreduzibel folgt $r = s$ und nach eventueller Umnumerierung $q_i \sim \tilde{q}_i\ (1 \leq i \leq r)$.)

3.45. Satz

Für Integritätsringe R mit 1 sind äquivalent:

(i) R ist ZPE-Ring;
(ii) jedes $x \in R\backslash U(R),\ x \neq 0$, ist Produkt irreduzibler Elemente, und jedes irreduzible Element von R ist Primelement;
(iii) jedes $x \in R\backslash U(R),\ x \neq 0$, ist Produkt von Primelementen.

Beweis:
(i) $\Rightarrow$ (ii):
Es bleibt zu zeigen, daß jedes irreduzible Element von R ein Primelement ist. Es seien dazu $a,\ b \in R$ und $\pi \in R$ irreduzibel mit $\pi \mid ab$. Da $a,\ b$ sich eindeutig als Produkte irreduzibler Elemente schreiben lassen, ergibt sich die Zerlegung von ab in irreduzible Elemente aus der von a bzw. b. Nach Voraussetzung muß also ein zu π assoziiertes Element in der Faktorisierung von a oder b auftreten, es folgt $\pi | a$ oder $\pi | b$.
(ii) $\Rightarrow$ (iii): Trivial.
(iii) $\Rightarrow$ (ii):

Ist π irreduzibel, so besitzt π eine Darstellung als Produkt von Primelementen. Diese besteht dann notwendig aus nur einem Faktor.

(ii) $\Rightarrow$ (i):
Es seien

$$x = \varepsilon\, q_1 \cdot \ldots \cdot q_r = \tilde{\varepsilon}\, \tilde{q}_1 \cdot \ldots \cdot \tilde{q}_s$$

mit $\tilde{\varepsilon}$, $\varepsilon \in U(R)$ und q_i, $\tilde{q}_j$ irreduzibel $(1 \leq i \leq r,\ 1 \leq j \leq s)$. Da q_r Primelement ist, muß q_r eins der $\tilde{q}_j$ teilen, also zu ihm assoziiert sein. Wir ordnen nun gegebenenfalls um, so daß $q_r | \tilde{q}_s$ gilt. Daraus folgt

$$\varepsilon\, q_1 \cdot \ldots \cdot q_{r-1} = \hat{\varepsilon}\, \tilde{q}_1 \cdot \ldots \cdot \tilde{q}_{s-1}$$

mit $\hat{\varepsilon} \in U(R)$. Nach r-maliger Anwendung folgt so $r = s$ und bei passender Numerierung $q_i \sim \tilde{q}_i$ $(1 \leq i \leq r)$.

□

Bemerkung:

(i) Als direkte Konseqenz von (2.43) folgt, daß jeder Hauptidealring auch ZPE-Ring ist.

(ii) Wählt man aus jeder Klasse assoziierter Primelemente einen Vertreter aus und bezeichnet die Menge dieser Vertreter mit P so läßt sich in ZPE-Ringen jedes $x \in R,\ x \neq 0$, eindeutig als

$$x = \varepsilon \prod_{p \in P} p^{\nu_p(x)}, \quad y = \eta \prod_{p \in P} p^{\nu_p(y)}$$

$(\nu_p(x) \in \mathbb{Z}^{\geq 0},\ \varepsilon,\ \eta \in U(R)$, nur endlich viele $\nu_p(x)$ ungleich Null, $\nu_p(x)$ ist der genaue Exponent, mit dem p gerade x teilt) schreiben. Für $x,\ y \in R \backslash \{0\}$ folgt dann insbesondere:

$$\begin{aligned} x\, y &= \varepsilon\, \eta \prod_{p \in P} p^{\nu_p(x) + \nu_p(y)}, \\ \mathrm{ggT}\,(x,\ y) &= \prod_{p \in P} p^{\min\{\nu_p(x),\, \nu_p(y)}, \\ \mathrm{kgV}\,(x,\ y) &= \prod_{p \in P} p^{\max\{\nu_p(x),\, \nu_p(y)}, \\ x \,|\, y &\Leftrightarrow \nu_p(x) \leq \nu_p(y)\ \ \forall p \in P. \end{aligned}$$

Ohne Euklidischen Algorithmus ist es i.a. ein schwieriges Problem, wie man in Hauptidealringen ein erzeugendes Element eines Ideals, etwa von $(a_1, \ldots, a_n)$, findet, d.h. einen ggT berechnet. Eine Faktorisierung in Primelemente ist meist zu aufwendig, etwa schon bei großen Zahlen in $\mathbb{Z}$.

3.46. Definition

Ein Integritätsring R heißt euklidischer Ring, wenn es eine Abbildung $v : R\backslash\{0\} \to \mathbb{Z}^{\geq 0}$ gibt, derart daß für beliebige $a,\, b \in R,\; b \neq 0$, zwei Elemente $Q(a,\, b),\, R(a,\, b) \in R$ mit

$$a = Q(a,\, b)\, b + R(a,\, b) \quad \text{und} \quad R(a,\, b) = 0 \quad \text{oder} \quad v(R(a,\, b)) < v(b)$$

gibt.

Bemerkung:

(i) Euklidische Ringe sind Ringe mit Einselement.
Die Menge $\{v(x) \mid x \in R\backslash\{0\}\}$ enthält ein minimales Element $v(x_0)$. Hierfür ist notwendig $R(a,\, x_0) = 0\ \forall a \in R$, also teilt x_0 alle $a \in R$. Ferner ist $0 \neq Q(x_0,\, x_0)$ Linkseins:

$$Q(x_0,\, x_0)\, y = Q(x_0,\, x_0)\, Q(y,\, x_0)\, x_0 = Q(y,\, x_0)\, Q(x_0,\, x_0)\, x_0 = Q(y,\, x_0)\, x_0 = y, \quad \forall y \in R.$$

Da R kommutativ ist, ist $Q(x_0,\, x_0)$ Einselement von R.

(ii) $\mathbb{Z}$ mit $v = |\ \ |$ (Betragsfunktion) und $K[t]$ mit $v = \deg(\ \ )$ sind euklidische Ringe, es existiert der euklidische Algorithmus, der zur Berechnung eines ggT zweier Ringelemente dient. Jeder Körper ist ein euklidischer Ring.

Beispiel: (Übung)
$R = \mathbb{Z}[-1]$ (Gaußsche ganze Zahlen) mit $v : a + b\sqrt{-1} \mapsto a^2 + b^2$.

3.47. Satz

Jeder euklidische Ring R ist Hauptidealring.

Beweis:
Es sei $\mathfrak{a} \neq \{0\}$ ein Ideal von R. Ferner sei $a \in \mathfrak{a}$ mit $v(a) = \min\{v(x) \mid x \in \mathfrak{a},\ x \neq 0\}$. Für $x \in a$ gilt dann $x = Q(x,\, a)\, a$, da notwendig $R(x,\, a)$ verschwinden muß. Also gilt $Ra \subseteq \mathfrak{a} \subseteq Ra$.

□

In this chapter we continue to study the structure of rings. We especially consider special types of rings, group rings, polynomial rings, Artinian and Noetherian rings. All these types of rings are important because of their widespread applicability, especially in the context of calculations with algebraic objects. Polynomials are used to generate algebraic extensions of fields, for defining curves and surfaces. They belong to the most important tools in algebra. Noetherian rings will frequently be used in calculations since their ideals have a finite number of generators, hence arithmetic can be done explicitly with those.

3.48. Group Rings and Polynomial Rings

The study of group rings is a relatively new topic of classical algebra. It was initiated by the idea that rings possess more structural properties than groups, hence, if one associates a suitable ring to a group then the structure of that so-called group ring should reveal structural aspects of the underlying group. We cannot cover this topic in full generality. Hence, we recommend that the reader concentrates on the applications to polynomial rings later in this section.

3.49. Definition

Let S be a semigroup and R be a ring. Then we define a **semigroup ring** $R[S]$ via

$$R[S] := \{f \,:\, S \to R \mid \; f(s) = 0 \text{ for almost all } s \in S\}$$

with operations

$$\begin{aligned} \text{addition} \;\; &: \;\; f+g \,:\, S \to R \,:\, s \mapsto f(s)+g(s) \;\;, \\ \text{multiplication} \;\; &: \;\; f\,g \,:\, S \to R \,:\, s \mapsto \sum_{\substack{t_1 t_2 = s \\ t_1, t_2 \in S}} f(t_1)\, g(t_2) \end{aligned}$$

for all f, $g \in R[S]$.

Whereas the definition of addition is straighforward the notion of multiplication seems to be kind of artificial at first glance. However, if we look at polynomials in one variable t with coefficients in R (for simplicity's sake let us assume that $R = \mathbb{R}$ as in highschool) then S is just the semigroup $(\mathbb{Z}^{\geq 0}, +)$ and a map f designs the coefficient $f(m)$ to the power t^m, i.e. the map f stands for the polynomial $\sum_{i \geq 0} f(i)t^i$, where the formally infinite sum is actually finite because of the condition imposed on f. On the other hand, when we multiply two polynomials given in their usual representation, say $\sum_{i=0}^{n} a_i t^i$ and $\sum_{j=0}^{m} b_j t^j$, it is quite cumbersome to write down their product:

$$\sum_{k=0}^{n+m} (\sum_{l=0}^{k} a_l b_{k-l}) t^k \;\;,$$

where we must additionally require $a_l = 0 \;\; (l > n)$, $b_{k-l} = 0 \;\; (k - l > m)$. This shows why the notion of semigroup rings is advantageous. The advantages will become even more clear when we consider polynomials in several variables. Using the notion of semigroup rings we just choose $S = ((\mathbb{Z}^{\geq 0})^n, +)$ to obtain a polynomial ring over R in n variables. The usual problems, like showing that the order of variables does not matter, are no longer present, this becomes an easy consequence of the analogous property for the direct product of (semi) groups (shown in chapter 2.6).
We leave the verification of the ring axioms for $R[S]$ as an exercise to the reader. As a precedent we establish the law of associativity for

multiplication:
For arbitrary $s \in S$ we have

$$\begin{aligned}
(f\,(g\,h))\,(s) &= \sum_{t_1 t_4 = s} f(t_1)\,(g\,h)\,(t_4) \\
&= \sum_{t_1 t_4 = s} f(t_1) \sum_{t_2 t_3 = t_4} g(t_2)\,h(t_3) \\
&= \sum_{t_1 t_2 t_3 = s} f(t_1)\,g(t_2)\,h(t_3) \\
&= \sum_{t_5 t_3 = s} \left(\sum_{t_1 t_2 = t_5} f(t_1) g(t_2) \right) h(t_3) \\
&= \sum_{t_5 t_3 = s} (f g)\,(t_5)\,h(t_3) \\
&= ((f\,g)\,h)\,(s).
\end{aligned}$$

Next we consider the necessary premises for embedding R, S into $R[S]$.

(i) Let S be a monoid with unit element e. We put

$$\iota_R \,:\, R \to R[S] \,:\, r \mapsto f_r \quad \text{with} \quad f_r(s) = \left\{ \begin{array}{ll} r & \text{for } s = e \\ 0 & \text{otherwise} \end{array} \right\} \;.$$

Then ι_R is a ringmonomorphism because of

$$\begin{aligned}
f_{r+\tilde{r}}(s) &= \left\{ \begin{array}{ll} r + \tilde{r} & \text{for } s = e \\ 0 & \text{otherwise} \end{array} \right\} \\
&= \left\{ \begin{array}{ll} r & \text{for } s = e \\ 0 & \text{otherwise} \end{array} \right\} + \left\{ \begin{array}{ll} \tilde{r} & \text{for } s = e \\ 0 & \text{otherwise} \end{array} \right\} \\
&= f_r(s) + f_{\tilde{r}}(s) \;, \\
f_{r\tilde{r}}(s) &= \left\{ \begin{array}{ll} r\tilde{r} & \text{for } s = e \\ 0 & \text{otherwise} \end{array} \right\} \\
&= \sum_{t_1 t_2 = s} \left\{ \begin{array}{ll} r & \text{for } t_1 = e \\ 0 & \text{otherwise} \end{array} \right\} \left\{ \begin{array}{ll} \tilde{r} & \text{for } t_2 = e \\ 0 & \text{otherwise} \end{array} \right\} \\
&= (f_r\, f_{\tilde{r}})(s) \;,
\end{aligned}$$

and $\ker(\iota_R) = \{0\}$.

(ii) Let R be a unital ring. We put

$$\iota_S \,:\, S \to R[S] \,:\, s \mapsto F_s \quad \text{with} \quad F_s(t) = \left\{ \begin{array}{ll} 1 & \text{for } t = s \\ 0 & \text{otherwise} \end{array} \right\} =: \delta_{ts} \;,$$

where δ_{ts} denotes the **Kronecker symbol** whose value is 1 if both indices coincide and otherwise 0.

ι_S is a homomorphism because of

$$\begin{aligned} F_{s\tilde{s}}(t) &= \delta_{t,s\tilde{s}} \\ &= \left\{ \begin{array}{ll} 1 & \text{for } s\tilde{s} = t \\ 0 & \text{otherwise} \end{array} \right\} \\ &= \sum_{t_1 t_2 = t} \delta_{t_1 s}\, \delta_{t_2 \tilde{s}} \\ &= \sum_{t_1 t_2 = t} \left\{ \begin{array}{ll} 1 & \text{for } t_1 = s \\ 0 & \text{otherwise} \end{array} \right\} \left\{ \begin{array}{ll} 1 & \text{for } t_2 = s \\ 0 & \text{otherwise} \end{array} \right\} \\ &= (F_s\, F_{\tilde{s}})(t) \ . \end{aligned}$$

Obviously, ι_S is injective and therefore a monomorphism.

If additionally S is a monoid then $R[S]$ has a unit element with respect to multiplication, namely F_e:

$$\begin{aligned} (F_e\, f)(t) &= \sum_{t_1 t_2 = t} F_e(t_1)\, f(t_2) \\ &= \sum_{t_1 t_2 = t} \delta_{e t_1}\, f(t_2) \\ &= f(t) \quad \text{for all} \quad f \in R[S] \ . \end{aligned}$$

(iii) In case $R \ni 1$ we obtain

$$R[S] \ = \ \left\{ \sum_{s \in S} a_s\, F_s \ \middle| \ a_s \in R,\ a_s = 0 \text{ for almost all } s \in S \right\} \ .$$

If we identify $s \in S$ with its image $F_s = \iota_S(s)$ this becomes

$$R[S] \ = \ \left\{ \sum_{s \in S} a_s\, s \ \middle| \ a_s \in R,\ a_s = 0 \text{ for almost all } s \in S \right\} \ .$$

Then all calculations in $R[S]$ are easy:

$$\begin{aligned} \alpha \left(\sum_{s \in S} a_s\, s \right) &= \sum_{s \in S} (\alpha\, a_s)\, s \quad \forall \alpha \in R, \\ \sum_{s \in S} a_s\, s + \sum_{s \in S} b_s\, s &= \sum_{s \in S} (a_s + b_s)\, s, \\ \left(\sum_{s \in S} a_s\, s \right) \left(\sum_{t \in S} b_t\, t \right) &= \sum_{s,t \in S} a_s\, b_t\, s\, t \ = \ \sum_{u \in S} \left(\sum_{st = u} a_s\, b_t \right) u. \end{aligned}$$

Examples

(i) $S = \{ t^\nu \mid \nu \in \mathbb{Z}^{\geq 0} \} \cong \mathbb{Z}^{\geq 0}$, R a unital commutative ring.

$$R[S] \ = \ \left\{ \sum_{\nu = 0}^{\infty} a_\nu\, t^\nu \ \middle| \ a_\nu \in R,\ a_\nu \neq 0 \text{ for only finitely many } \nu \right\} =: R[t]$$

is the polynomial ring in the variable t over R. The elements of $R[t]$ are written as

$$f(t) = \sum_{i=0}^{\infty} a_\nu \, t^\nu$$

with $a_\nu \in R$, almost all $a_\nu = 0$. Polynomials in one varable are usually called **univariate** polynomials.

(ii)

$$S = \prod_{i=1}^{n} \{t_i^{\nu_i} \in \mathbb{Z}^{\geq 0}\} \cong (\mathbb{Z}^{\geq 0})^n \,, \; R \text{ a unital commutative ring } .$$

The elements of S can be written in the form $\mathbf{t}^{\underline{\nu}} := t_1^{\nu_1} \cdot \ldots \cdot t_n^{\nu_n}$ with $\underline{\nu} \in (\mathbb{Z}^{\geq 0})^n$. Then

$$R[S] \;=\; \left\{ \sum_{\underline{\nu} \in (\mathbb{Z}^{\geq 0})^n} a_{\underline{\nu}} \mathbf{t}^{\underline{\nu}} \;\middle|\; a_{\underline{\nu}} \in R, a_{\underline{\nu}} \neq 0 \text{ for only finitely many } \underline{\nu} \right\} =: R[\mathbf{t}]$$

is the polynomial ring in n variables $t_1, \ldots, t_n$ over R with elements

$$f(\mathbf{t}) = \sum_{\underline{\nu} \in (\mathbb{Z}^{\geq 0})^n} a_{\underline{\nu}} \mathbf{t}^{\underline{\nu}} \quad (a_{\underline{\nu}} \in R, \text{ almost all } a_{\underline{\nu}} = 0) \;\; .$$

Polynomials in several variables ($n \geq 2$) are usually called **multivariate** polynomials.

(iii) S a group, R a unital ring. $R[S]$ is called **group ring**. Knowledge about the group ring yields information about the group itself. We cite without proof a result of Higman: If G, H are finite abelian groups with $\mathbb{Z}[G] \cong \mathbb{Z}[H]$ then G and H are isomorphic.

As we already mentioned important results on polynomial rings immediately follow from the properties of the semigroup used for their construction.
For example, we get

$$\begin{aligned} R[t_1, ..., t_n, t_{n+1}] &\cong R[t_1, ..., t_n]\,[t_{n+1}], \\ R[t_1, ..., t_n] &\cong R[t_{\pi(1)}, ..., t_{\pi(n)}] \quad \forall \pi \in \mathfrak{S}_n \end{aligned}$$

as an immediate consequence of the corresponding statements for direct products of (semi) groups.

For the elements of the monoid $(\mathbb{Z}^{\geq 0})^n$ we can introduce an ordering via

$$\mathbf{t}^{\underline{\nu}} \geq \mathbf{t}^{\underline{\mu}} \quad \Leftrightarrow \quad \underline{\nu} \geq \underline{\mu} \;\; .$$

There are various possibilities. We just mention the two most popular ones:

(i) lexicographic ordering
We put $\underline{\nu} \geq \underline{\mu}$ if and only if there exists an index $i \in \{1, ..., n\}$ with $\nu_j = \mu_j \ \ (j < i)$ and $\nu_i > \mu_i$. This means that for the smallest index i for which the coordinates of $\underline{\nu}$ and $\underline{\mu}$ differ the i-th coordinate of $\underline{\nu}$ is larger than that of $\underline{\mu}$.
(ii) graded lexicographic ordering
We put $\underline{\nu} \geq \underline{\mu}$ if either $\sum_{i=1}^{n} \nu_i^2 > \sum_{i=1}^{n} \mu_i^2$ or, in case both sums are equal, $\underline{\nu}$ is lexicographically greater than $\underline{\mu}$ (including the case $\underline{\nu} = \underline{\mu}$). Here we first compare the Euclidean lengths of $\underline{\nu}$ and $\underline{\mu}$ and only if they are equal we make use of lexicographic ordering.
For a thorough study of (multivariate) polynomials we need to introduce a few definitions which will be mostly familiar from high school arithmetic.

3.50. Definition

Let

$$f(\mathbf{t}) = \sum_{\underline{\nu} \in (\mathbb{Z}^{\geq 0})^n} a_{\underline{\nu}} \mathbf{t}^{\underline{\nu}}$$

be an element of the polynomial ring $R[\mathbf{t}]$. The single summands $a_{\underline{\nu}} \mathbf{t}^{\underline{\nu}}$ are called **monomials**. The **degree** of a non-zero monomial is defined as the sum of its exponents: $\nu_1 + \ldots + \nu_n$. The **degree** $\deg(f)$ of a non-zero polynomial f is the maximum of the degrees of its monomials. The degree of 0 (as monomial or as polynomial) is formally defined to be $-\infty$. If we have a total ordering on the exponents - and therefore on the monomials - the coefficient of the largest monomial is called **leading coefficient** $l(f)$, sometimes also **headterm**. In case $l(f) = 1$ the polynomial f is called **monic**.

We shortly consider the behavior of the degree function with respect to the addition and multiplication of polynomials. Comparing the degrees of the occuring monomials we immediately see that

$$\begin{aligned} \deg(f+g) &\leq \max\{\deg(f), \deg(g)\} \\ \deg(f\,g) &\leq \deg(f) + \deg(g) \ . \end{aligned}$$

The last inequality becomes an equation, if $l(f)$, $l(g)$ are no zero divisors.
Hence, the degree of the product of two polynomials equals the sum of their degrees over entire rings R. The property to be entire is therefore transfered from R to $R[\mathbf{t}]$:

$$R[\mathbf{t}] \text{ entire ring } \Leftrightarrow \ R \text{ entire ring } \ .$$

Because of the behavior of the degree function mentioned above we also obtain the result that the units of R and of $R[t]$ coincide:

$$f \in U(R[\mathbf{t}]) \ \Leftrightarrow \ f \in U(R) \ .$$

We will consider further properties of rings with respect to whether they transfer from R to $R[\mathbf{t}]$.

Theorem (**Hilbert's Basis Theorem**) Let R be a unital commutative ring. If R is noetherian then also $R[t]$ is noetherian.

Proof Let $\mathbf{A}$ be an ideal of $R[t]$. Then we consider the polynomials of $\mathbf{A}$ of degree $i \in \mathbb{Z}^{\geq 0}$ and put

$$\mathbf{a}_i := \{x \in R \mid x = \mathrm{lc}(f) \text{ for an } f \in \mathbf{A} \text{ with } \deg(f) = i\} \cup \{0\} \ .$$

The $\mathbf{a}_i$ are ideals in R because of

(i) for $f, g \in \mathbf{A}$ with $\deg(f) = \deg(g) = i$ we either have $\mathrm{lc}(f + g) = \mathrm{lc}(f) + \mathrm{lc}(g) \neq 0$ or $\deg(f + g) < i$ and the coefficient of t^i of $f + g$ is zero,

(ii) for $a = \mathrm{lc}(f) \in \mathbf{a}_i,\ r \in R$ we have $ra = 0$ or $rf \in \mathbf{A}$ with $\deg(rf) = i$ and $\mathrm{lc}(rf) = ra \in \mathbf{a}_i$.

Since we can multiply elements of $\mathbf{A}$ by t we obtain

$$\mathbf{a}_0 \subseteq \mathbf{a}_1 \subseteq \ldots \subseteq \mathbf{a}_r \subseteq \ldots \ .$$

Since R is noetherian this chain becomes stationary. Let $r \in \mathbb{Z}^{\geq 0}$ be minimal with $\mathbf{a}_r = \mathbf{a}_{r+k}\ \forall k \in \mathbb{N}$. Since R is noetherian each ideal $\mathbf{a}_i$ has finitely many generators $a_{i1}, \ldots, a_{in_i}$ $(n_i \in \mathbb{N})$ for $0 \leq i \leq r$. We fix elements $f_{ij} \in \mathbf{A}$ with $\deg(f_{ij}) = i$ and $\mathrm{lc}(f_{ij}) = a_{ij}$ for $0 \leq i \leq r,\ 1 \leq j \leq n_i$. We will show that $\mathbf{A} = \mathbf{B}$ for

$$\mathbf{B} \ := \ \langle f_{ij} \mid 0 \leq i \leq r\,,\ 1 \leq j \leq n_i \rangle \ .$$

Clearly, $\mathbf{B}$ is contained in $\mathbf{A}$. On the other hand, let $f \in \mathbf{A}$ with $\deg(f) = d$. The proof of $f \in \mathbf{B}$ is carried out by induction on d. For $d = 0$ there is nothing to show since f is contained in $\mathbf{a}_0 \subseteq \mathbf{B}$. We let therefore be $d > 0$ and assume that all elements of $\mathbf{A}$ of degree less than d belong to $\mathbf{B}$. We need to consider two cases.

(i) For $d > r$ we have

$$\mathbf{a}_d = \langle \mathrm{lc}(t^{d-r} f_{r1}), \ldots, \mathrm{lc}(t^{d-r} f_{rn_r}) \rangle \ ,$$

there exist $\gamma_1, \ldots, \gamma_{n_r} \in R$ such that

$$g \ := \ f - \sum_{i=1}^{n_r} \gamma_i t^{d-r} f_{ri}$$

is a polynomial of $\mathbf{A}$ with $\deg(g) < d$.

(ii) For $d \leq r$ we analogously obtain a polynomial

$$g \ := \ f - \sum_{i=1}^{n_d} \tilde{\gamma}_i f_{di}$$

of degree less than d in $\mathbf{A}$.

According to our induction assumption in both cases the difference polynomial g belongs to the ideal $\mathbf{B}$, hence the polynomial f itself. This finishes the proof of $\mathbf{A} = \mathbf{B}$, the ideal $\mathbf{A}$ is finitely generated and therefore $R[t]$ noetherian.

□

Applying the preceding theorem n times we obtain that for noetherian rings R the polynomial ring in n variables $R[\mathbf{t}]$ is noetherian, too.

A similar discussion whether the properties of a ring R to be a principal ideal ring or a factorial ring transfer to $R[t]$ (and therefore to $R[\mathbf{t}]$) is postponed to the next section.

3.51. Univariate Polynomials

Univariate polynomials play a predominant role among all polynomials. This is mainly due to the fact that polynomial rings in one variable over a field have nicer properties than those with several variables. Also, polynomial rings in $n > 1$ variables could be considered as polynomial rings in one variable over a polynomial ring in $n - 1$ variables as base ring. This is usually not the appropriate approach, however, and therefore we shall consider univariate and multivariate polynomials in separate sections.
We begin with basic properties which will be of importance later on.

3.52. Definition

Let Λ be a unital overring of R, i.e. $1_\Lambda = 1_R$, then for every $x \in \Lambda$ the mapping

$$\Phi_x \,:\, R[t] \to \Lambda \,:\, f(t) \mapsto f(x)$$

is a ring homomorphism with $\Phi_x|_R = \mathrm{Id}_R$. Hence, it leaves every element of R invariant and is therefore called an **R-homomorphism**. Since Φ_x maps a polynomial to a ring element it is also called a **specialization** of the polynomial $f(t)$ to its value $f(x)$.

That Φ_x is indeed a ring homomorphism can be easily verified and is left as an exercise to the reader.

3.53. Definition

Let Λ, R be as in the previous definition. An element $x \in \Lambda$ is called **zero** of $f(t) \in R[t]$, if f is in the kernel of Φ_x. This is clearly tantamount to the more familiar version that $f(t)$ specializes to 0 at x.

Proposition 8. *Let R be a unital entire ring. An R-homomorphism $\varphi \,:\, R[t] \to R[t]$ is an isomorphism exactly for $\varphi(t) = at + b$ with $a \in U(R)$, $b \in R$.*

Before we actually proof this we emphasize that every R-homomorphism $\varphi \,:\, R[t] \to \Lambda$ is uniquely determined by the image $\varphi(t)$. This is because of

$$\varphi\left(\sum_{i=0}^{n} a_i\, t^i\right) \;=\; \sum_{i=0}^{n} \varphi(a_i\, t^i) \;=\; \sum_{i=0}^{n} \varphi(a_i)\, \varphi(t)^i \;=\; \sum_{i=0}^{n} a_i\, \varphi(t)^i \quad .$$

Proof For $\varphi(t) = at + b$ with $a \in U(R)$, $b \in R$ the inverse mapping is given by $\varphi^{-1}(t) = a^{-1}(t - b)$ satisfying $\varphi \circ \varphi^{-1} = \mathrm{Id}_{R[t]}$. On the other hand, if φ is an $R[t]$-isomorphism then φ maps t onto some polynomial of $R[t]$, say $\varphi(t) = g(t) := \sum_{i=0}^{n} a_i t^i \in R[t]$ and φ being surjective there exists $f(t) = \sum_{j=0}^{m} b_j t^j \in R[t]$ with $t = \varphi(f(t))$. This yields

$$t = \varphi(f(t)) = \varphi(\sum_{j=0}^{m} b_j t^j) = \sum_{j=0}^{m} b_j \varphi(t)^j = \sum_{j=0}^{m} b_j g(t)^j = f(g(t))$$

and comparing degrees we obtain

$$1 = \deg(t) = \deg(f(g(t)) = \deg(g)\deg(f) \ .$$

The latter is possible only for $\deg(f) = \deg(g) = 1$, hence $g(t) = at + b$, $f(t) = ct + d$ $(a, b, c, d \in R)$. From

$$\begin{aligned} t &= f(g(t)) \\ &= c\,(at + b) + d \\ &= cat + bc + d \end{aligned}$$

we deduce $1 = ac$, $0 = bc + d$ and therefore $a \in U(R)$.
□

3.54. Definition

Let Λ be a unital overring of the ring R. An element $x \in \Lambda$ is called **algebraic** over R, if the mapping $\varphi_x : R[t] \to \Lambda$ is not injective, i.e. there exists a polynomial $f(t) \in R[t]$ with $f(x) = 0$, x is a zero of a suitable non-constant polynomial of $R[t]$. If x is not algebraic over R it is called **transcendental** over R.

Examples $\sqrt{2} \in \mathbb{R}$ is algebraic over $\mathbb{Z}$ since it is a zero of $f(t) = t^2 - 2 \in \mathbb{Z}[t]$. $e, \pi \in \mathbb{R}$ are transcendental over $\mathbb{Z}$ (respectively $\mathbb{Q}$). For a proof of the last statement the reader is refered to [**?**].
Because of the definition of algebraic elements it is important to characterize zeros of polynomials by purely polynomial ring properties. This is achieved upon showing that we can have division with remainder in polynomial rings and will surely have it in case R is a field.

Proposition 9. *Let us assume that $f(t)$, $g(t)$ are polynomials in $R[t]$ with the leading coefficient of g being a unit in R. Then there exist polynomials $q(t) := q(f,g)(t)$, $r(t) := r(f,g)(t) \in R[t]$ satisfying $f(t) = q(t)g(t) + r(t)$ and $\deg(r) < \deg(g)$. (This includes $r = 0$ with $\deg(r) = -\infty$ since our assumption on $l(g)$ yields $g \neq 0$.)*

Proof Since the polynomials q, r are given explicitly via calculations in R we give an algorithmic proof.
Algorithm (division with remainder for polynomials)
Input Polynomials $f(t)$, $g(t) \in R[t]$ with $l(g) \in U(R)$.
Initilization Set $m := \deg(g)$, $r_0 := f$, $q_0 := 0$, $i := 0$, $\deg(r_i) =:$

m_i.
Step While $k_i := m_i - m \geq 0$ set

$$\begin{aligned} \lambda_i &:= l(r_i)/l(g) \\ r_{i+1} &:= r_i - \lambda_i g(t) t^{k_i} \\ q_{i+1} &:= q_i - \lambda_i t^{k_i} \end{aligned}$$

and increase i by 1.
Output Polynomials $q(t) := q_i(t)$, $r(t) := r_i(t) \in R[t]$ with $f(t) = q(t)g(t) + r(t)$ and $\deg(r) < \deg(g)$.
In each step from the remaining polynomial r_i (initially $f(t)$) the polynomial $(l(r_i)/l(g)g(t)t^{\deg(r_i)-\deg(g)}$ is subtracted. This decreases the degree of the remainder. It can be carried out until the degree of the remainder becomes smaller than $\deg(g)$. The divison of the leading coefficients is always possible in R since we assumed $l(g) \in U(R)$.
□
Remark We note that division with remainder is always possible in case $g(t)$ is monic.

PROPOSITION 10. *Let R be a unital commutative ring, $f(t) \in R[t]$ with $\deg(f) \geq 1$ and Λ be a unital overring of R. $x \in \Lambda$ is a zero of $f(t)$, if and only if $(t - x)$ divides $f(t)$ in $\Lambda[t]$.*

Proof Division with remainder can be carried out in $\Lambda[t]$ since $l(t - x) = 1$ is a unit in Λ. It follows

$$f(t) = Q(f, t - x)\,(t - x) + R(f, t - x)$$

with $\deg(R(f, t - x)) < \deg(t - x) = 1$, hence $R(f, t - x)$ is constant. Now we specialize $t \mapsto x$:

$$\begin{aligned} x \text{ zero} &\Leftrightarrow 0 = f(x) \\ &\Leftrightarrow R(f, t - x)\,(x) = 0 \\ &\Leftrightarrow R(f, t - x) = 0. \end{aligned}$$

□

For division with remainder in polynomial rings (**pseudodivision**) see the detailed exercise 1. Here we just present an illustrative example.

Example For $R = \mathbb{Z}$ the polynomial $f(t) = t^3 - 2$ is not divisible by $g(t) = 2t - 1$ in $R[t]$. However, if we multiply the first polynomial with $l(g)^{deg(f)-deg(g)+1}$ we obtain

$$2^3(t^3 - 2) = (4t^2 + 2t + 1)\,(2t - 1) - 15 \text{ in } \mathbb{Z}[t] \ .$$

(The reader is advised to carry out this example with the algorithm given above.)

If the underlying ring is a field F then division with remainder is always possible in case $g(t)$ is non–zero. Hence, the polynomial ring

$F[t]$ becomes a Euclidean ring with the degree function as Euclidean function.

Theorem A polynomial ring $F[t]$ over a field F is a Euclidean ring.

We note that repeated divison with remainder yields the greatest common divisor of two polynomials exactly as it did for two rational integers. Since $F[t]$ is Euclidean and therefore a principal ideal ring we even obtain a representation of the greatest common divisor in terms of f, g because the principal ideal $\gcd(f,g)$ equals the ideal $f(t)F[t]+g(t)F[t]$ (see exercise ...). This is of importance for finite extensions of fields, for example.

We model repeated division with remainder for two polynomials f, g as follows. A sequence of polynomials $(f_i)_{i\in\mathbb{Z}^{\geq 0}}$ is calculated via $f_0 := f$, $f_1 := g$ and – for $f_{i+1} \neq 0$ – $f_i = q_{i+1}f_{i+1} + f_{i+2}$ by division with remainder.

Let $f(t)$, $g(t) \in F[t]$ be given. If both polynomials are 0 then their greatest common divisor is also 0 by definition. It is represented as $0 = 0 \cdot f + 0 \cdot g$. If $0 = f \neq g$ then the greatest common divisor is $\frac{1}{l)g)}g(t)$. It is represented via $\gcd(f,g) = 0 \cdot f + \frac{1}{l(g)}g$. Analogously, for $0 = g \neq f$ we obtain $\gcd(f,g) = \frac{1}{l(f)}f + 0 \cdot g$. For the more interesting case $fg \neq 0$ we present the following algorithm. We note that we will have $f_i = \lambda_i f_0 + \mu_i f_1$ at each step.

Algorithm (polynomial gcd with presentation)

Input Non–zero polynomials $f(t)$, $g(t) \in F[t]$.

Initialization Set $f_0 := f$, $f_1 := g$, $\lambda_0 := \mu_1 := 1$, $\lambda_1 := \mu_0 := 0$ and $i := 0$.

Step While $f_{i+1} \neq 0$ set

$$\begin{aligned} f_{i+2} &:= f_i - q_i f_{i+1} \text{ (division with remainder)} \\ \lambda_{i+2} &:= \lambda_1 - q_i \lambda_{i+1} \\ \mu_{i+2} &:= \mu_i - q_i \mu_{i+1} \end{aligned}$$

then increase i by 1.

Output $\gcd(f,g) := \frac{1}{l(f_i)}f_i$, $\lambda := \frac{1}{l(f_i)}\lambda_i$, $\mu := \frac{1}{l(f_i)}\mu_i \in F[t]$ with $\gcd(f,g) = \lambda f + \mu g$.

The algorithm is valid as the output polynomial $f_i(t)$ divides $f_{i-1}(t)$ (because of $f_{i+1}(t) = 0$); hence it also divides $f_{i-2}(t), ..., f_1(t), f_0(t)$. On the other hand, any common divisor of $f_0(t)$ and $f_1(t)$ divides $f_2(t)$; hence it also divides $f_3(t), ..., f_i(t)$. Both properties yield $f_i(t) = \gcd(f_0, f_1)$.

After this excursion into computational aspects we proceed with a few consequences of the last theorem. $F[t]$ is a principal ideal ring and a unique factorization ring. For an irreducible polynomial $f(t) \in F[t]$ the factorring $F[t]/f(t)F[t]$ is again a field. In $F[t]$ the number of zeros of a polynomial – counted with respect of their multiplicities – is bounded

by the polynomial degree. (This is also true over entire rings, but not in general, as the example $t^2 - 1 \in (\mathbb{Z}/8\mathbb{Z})[t]$ shows, see exercise ...)

PROPOSITION 11. *For unital commutative rings R the following equivalence holds:*

$$R[t] \text{ principal ideal ring} \quad \Leftrightarrow \quad R \text{ field} \ .$$

Proof We already showed that a polynomial ring over a field is a principal entire ring. To show the opposite direction we consider the ring epimorphism

$$\varphi_0 \ : \ R[t] \to R \ : \ f(t) \mapsto f(0) \ .$$

If $R[t]$ is a principal ideal ring then it is a priori an entire ring and therefore R itself must be an entire ring. The homomorphism theorem for rings tells us that $R \cong R[t]/\ker(\varphi_0)$, hence $\ker(\varphi_0)$ is a prime ideal and therefore maximal in the principal entire ring $R[t]$. Therefore the factorring $R[t]/\ker(\varphi_0)$ is a field. It is isomorphic to R because of the surjectivity of φ_0.
□

Remark An important consequence of this proposition is that polynomial rings in more than one variable are not any more principal ideal rings.

Contrary to this the property of being a factorial ring is transfered from R to $R[t]$. This will be shown below.
Theorem (Gauß) If R is a factorial ring than so is $R[t]$.

The proof of Gauß' theorem is a bit complicated and will be based on preparatory lemmata.

PROPOSITION 12. *Let R be a unital commutative ring. If $\mathfrak{a}$ is an ideal (a prime ideal) of R, then $\mathfrak{a}[t] := \{f(t) = \sum_{i=0}^{n} a_i t^i \in R[t] \mid a_i \in \mathfrak{a} \ \ (0 \leq i \leq n)\}$ is an ideal (a prime ideal) of $R[t]$.*

Proof It is obvious that for an ideal $\mathfrak{a}$ of R also $\mathfrak{a}[t]$ is an ideal of $R[t]$.
Now let us assume that $\mathfrak{a}$ is a prime ideal of R. For

$$f(t) = \sum_{i=0}^{n} a_i t^i, \ g(t) = \sum_{j=0}^{m} b_j t^j \in R[t] \setminus \mathfrak{a}[t] \ ,$$

the polynomials f, g have coefficients a_i, $b_j \notin \mathfrak{a}$ for suitable indices i, j; we choose i, j minimal with this property. Then the coefficient of t^{i+j} of the product of f and g satisfies

$$c_{i+j} := \sum_{k=0}^{i+j} a_k \, b_{i+j-k} \equiv a_i b_j \bmod \mathfrak{a} \ ,$$

and therefore also c_{i+j} is not in the ideal $\mathfrak{a}$. This implies $fg \notin \mathfrak{a}[t]$.
□

3.55. Definition

Let R be a factorial ring and $f(t) = \sum_{i=0}^{n} a_i t^i \in R[t]$ with $\deg(f) \geq 0$. Then $I(f) := \gcd\{a_0, a_1, ..., a_n\}$ is called **content** of $f(t)$. In case $I(f) = 1$ the polynomial $f(t)$ is said to be **primitive**.

Remark If R is factorial then any polynomial $f(t) \in R[t]$ with $\deg(f) \geq 0$ can be written as a product of $I(f)$ and a polynomial $f_p(t) \in R[t]$ which is primitive. The polynomial $f_p(t)$ is also called the primitive part of $f(t)$.

PROPOSITION 13. *If R is factorial then the product of two primitive polynomials of $R[t]$ is primitive.*

Proof Let $f(t)$, $g(t) \in R[t]$ be primitive and $h := f\,g$. If $I(h)$ is not contained in $U(R)$ then there exists a prime element $\pi \in R$ which divides all coefficients of h. Because of **??** the principal ideal $R\pi$ is a prime ideal, hence $R\pi[t]$ is a prime ideal of $R[t]$ according to the previous proposition. ¿From $f\,g \in R\pi[t]$ we conclude that either $f(t)$ or $g(t)$ is contained in $R\pi[t]$, i.e. all coefficients of f or of g are divisible by π contrary to our assumption $I(f) = I(g) = 1$.
□

Remark For arbitrary polynomials f, g over a factorial ring R the content of their product $I(fg)$ equals the product of their contents $I(f)$ and $I(g)$. This is a direct consequence of the last proposition and the remark preceding it.

The next lemma is known as Gauß' lemma in the literature.

LEMMA 14. *Let R be a factorial ring with quotient field $K = \mathfrak{Q}(R)$. If $h(t) \in R[t]$ has a positive degree and a factorisation $h = f_1 f_2$ in $K[t]$, then there is also a factorisation $h = c g_1 g_2$ in $R[t]$ with primitive polynomials g_1, g_2 and $c \in R$. There exist $\alpha_i \in K$ with $\alpha_i f_i = g_i$ $(i = 1, 2)$.*

Proof Let λ_i be the least common multiples of the denominators of the coefficients of f_i $(i = 1, 2)$. We put $\mu_i := I(\lambda_i f_i)$. Then the primitive parts of $g_i := (\lambda_i f_i)_p$ satisfy

$$\lambda_1 \lambda_2\, h = \mu_1 \mu_2\, g_1 g_2 \quad .$$

¿From this we conclude $\lambda_1 \lambda_2\, I(h) = \mu_1 \mu_2$. It follows that $\mu_1 \mu_2 = (\lambda_1 \lambda_2)\, c$ $(c \in R)$, hence, $h = c\, g_1\, g_2$. The last statement is true with $\alpha_i = \frac{\lambda_i}{\mu_i}$ for $i = 1, 2$.
□

Remarks

(i) If $f(t) \in R[t] \setminus R$ is irreducible then f remains irreducible in $\mathfrak{Q}(R)[t]$. For example, if $n \in \mathbb{Z}$ is not a square then $t^2 - n$ is

irreducible in $\mathbb{Z}[t]$. This implies $\sqrt{n} \notin \mathbb{Q}$. Putting it negative: If $f(t) \in R[t]$ is reducible in $K[t]$, then it is also reducible in $R[t]$.

(ii) Let $f, g \in R[t]$ and g primitive with $g \mid f$ in $K[t]$. Then g divides f already in $R[t]$.

(iii) Two primitive polynomials $f, g \in R[t]$ are associated in $K[t]$ if and only if they are associated in $R[t]$.

After this the proof of Gauß' theorem is straightforward.

Proof of 1.54

We recall that the irreducible elements of $R[t]$ belong to two separate classes:

(i) irreducible elements of R,

(ii) irreducible polynomials $f(t) \in R[t]$ of positive degree.

$R[t]$ is a unital entire ring since R has this property. Let $f(t) \in R[t]$ be fixed. Without loss of generality we assume that $\deg(f) > 0$. In the factorial ring $K[t]$, K denoting the quotient field of R, f has a factorisation into irreducible elements: $f = \tilde{q}_1 \cdot \ldots \cdot \tilde{q}_r$ with $\tilde{q}_i \in K[t]$. By Gauß' lemma 7 we obtain from this a factorisation

$$f = c\, q_1 \cdot \ldots \cdot q_r$$

with

$$q_i = \alpha_i \tilde{q}_i \in R[t] \;\; (\alpha_i \in K,\; 1 \leq i \leq r)$$

primitive and irreducible, $c \in R$. Since R was assumed to be factorial also c has a factorisation into irreducible elements in R.

If f admits two such factorisations in $R[t]$, say

$$f = d\, q_1 \cdot \ldots \cdot q_r = c\, p_1 \cdot \ldots p_s \;\; (\deg(q_i) > 0,\; \deg(p_j) > 0),$$

then the q_i, p_j are irreducible in $K[t]$, too, hence we obtain $r = s$ and after a potential reordering $q_i = \alpha_i p_i \;\; (\alpha_i \in K,\; 1 \leq i \leq r)$. The q_i and p_i are therefore associated in $R[t]$. It follows that d is also associated to c. Since R is a factorial ring the theorem follows.

□

Since every polynomial of a factorial ring $R[t]$ is a product of irreducible ones the irreducible polynomials are of special interest. We note that polynomials of degree one are necessarily irreducible. There is an easy test whether a first degree polynomial $at + b$ is a potential divisor of an arbitrary polynomial:

$$(at + b) \mid \left(\sum_{i=0}^{n} a_i\, t^{n-i} \right)$$

obviouslyly implies $a \mid a_0,\; b \mid a_n$.

Example Let us discuss for which $a \in \mathbb{Z}$ the polynomial $f(t) = t^5 + at + 1$ is irreducible in $\mathbb{Q}[t]$. Since f is primitive, irreducibility in $\mathbb{Z}[t]$ and in $\mathbb{Q}[t]$ is tantamount. We therefore need to look for potential

divisors of f in $\mathbb{Z}[t]$ only. If f is not irreducible, it must have a factor of degree either one or two. Having a linear factor means having a zero. We find that $f(1) = a + 2$, $f(-1) = a$, hence f is reducible for $a \in \{-2, 0\}$.
Next we are looking for quadratic factors:

$$t^5 + at + 1 = (t^2 + \alpha\, t + \beta)\,(t^3 + \gamma\, t^2 + \delta\, t + \varepsilon) \ .$$

Calculating the right-hand side and comparing coefficients we get the following system of equations:

$$\alpha + \gamma = 0,\ \delta + \alpha\,\gamma + \beta = 0,\ \varepsilon + \alpha\,\delta + \beta\,\gamma = 0,\ \alpha\,\varepsilon + \beta\,\delta = a,\ \beta\,\varepsilon = 1 \ .$$

We eliminate variables by setting

$$\gamma = -\alpha,\ \delta = \alpha^2 - \beta,\ \varepsilon = \alpha\,(2\beta - \alpha^2)$$

and obtain from the two remaining equations either
$\beta = \varepsilon = 1$ in which case the only solution is $1 = a = \alpha = -\gamma\,,\ \delta = 0$,
or
$\beta = \varepsilon = -1$ in which case there is no solution since the second relation for ε becomes $1 = \alpha(2 + \alpha^2)$.
Hence, the given polynomial is reducible if and only if a is 0,1 or -2.

In general there are very few powerful methods which allow to decide irreducibility of a given polynomial. Here we discuss just two. (For R being a finite field or for $R = \mathbb{Q}$ there are better methods which will be introduced later.)
Theorem (Eisenstein criterion) Let R be a factorial ring and $f(t) = \sum_{i=0}^{n} a_i\, t^i \ \in R[t]$ be a polynomial of positive degree. If R contains a prime element π such that $\pi \mid a_i \ \ (0 \le i < n)$, π^2 **-** a_0 and π **-** a_n, then $f(t)$ is irreducible in $\mathfrak{Q}(R)[t]$.

Proof We assume that $f(t)$ has a factorisation in $\mathfrak{Q}(R)[t]$ into two polynomials of positive degree. According to 7 we also get such a factorisation in $R[t]$. We therefore assume that we have a factorisation in $R[t]$, say $f(t) = g(t)\,h(t)$ with $\deg(g)\deg(h) > 0$. We put

$$g(t) = \sum_{i=0}^{d} b_i\, t^i, \quad h(t) = \sum_{j=0}^{m} c_j\, t^j \ .$$

For the coefficients of the product of g and h we obtain the necessary conditions

$$a_i := \sum_{\substack{k=0 \\ k \le d \\ i-k \le m}}^{i} b_k\, c_i - k \ \ (0 \le i \le n) \ .$$

¿From $a_0 = b_0\, c_0$ and $\pi \mid a_0,\ \pi^2$ **-** a_0 we conclude that π either divides b_0 or c_0 but not both. Without loss of generality (g, h are arbitrary so

far) we assume that $\pi \mid b_0$ and π - c_0. Then we will show by induction that also $\pi \mid b_j \;\; (1 \leq j \leq d)$. Obviously, we have for $d \geq i > 0$:

$$a_i = \sum_{\substack{k=0 \\ i-k \leq m}}^{i} b_k \, c_{i-k} = \sum_{\substack{k=0 \\ i-k \leq m}}^{i-1} b_k \, c_{i-k} + b_i \, c_0 \equiv 0 \bmod \pi$$

because of our induction assumption. We conclude that $\pi | b_i c_0$ and because of π - c_0 therefore $\pi \mid b_i$. Eventually we obtain for $i = d$ that $\pi \mid b_d c_m = a_n$. This is certainly in contradiction to our premises.
□

Example

(i) Let a be an integer. If there exists a prime number p with $p \mid a$ and p^2 - a then the polynomial $t^n - a$ is irreducible in $\mathbb{Q}[t]$ and in $\mathbb{Z}[t]$. Especially, it follows that $\sqrt[n]{a}$ is not rational.

(ii) In $\mathbb{Q}[t]$ the following polynomials are irreducible according to 1.55:

$$\begin{aligned} f_1(t) &= 3\,t^5 - 15 \quad (p = 5), \\ f_2(t) &= 2\,t^{10} - 21 \quad (p = 3,\, 7), \\ f_3(t) &= 5\,t^5 - 12\,t^4 + 24\,t^3 + 2\,t^2 - 4\,t + 34 \quad (p = 2). \end{aligned}$$

We note that only the last two polynomials f_2, f_3 are also irreducible in $\mathbb{Z}[t]$ since the content of f_1 is 3 and therefore not a unit in $\mathbb{Z}$.

(iii) For prime numbers p the p–th roots of unity are zeros of $t^p - 1$, they form a cyclic group of order p. $t^p - 1$ ist reducible since $(t-1) \mid (t^p - 1)$. The formula for the sum of the geometric series tells us that

$$\frac{t^p - 1}{t - 1} = \sum_{i=0}^{p-1} t^i =: \Phi_p[t] \;\; .$$

The polynomial $\Phi_p(t)$ is called p–th cyclotomic polynomial. Its zeros lead to the construction of a regular p–gon, they yield a division of the unit circle into p equal parts. Because $t \mapsto t+1$ is an isomorphism of $R[t]$ (see 1) we conclude that $\Phi_p(t)$ is irreducible if and only if $\Phi_p(t+1)$ is irreducible. This trick of changing the variable allows an easy demonstration of the irreducibility of Φ_p. (We remark that it can be employed also to other polynomials to turn them into polynomials satisfying

the Eisenstein criterion.) We calculate

$$\begin{aligned}\Phi_p(t+1) &= \frac{(t+1)^p-1}{(t+1)-1} \\ &= \frac{\sum_{i=0}^{p}\binom{p}{i}t^i-1}{t} \\ &= t^{p-1}+\sum_{i=1}^{p-1}\binom{p}{i}t^{i-1} \quad ,\end{aligned}$$

and in the resulting monic polynomial the coefficients

$$\binom{p}{i}=\frac{p\cdot(p-1)\cdot\ldots\cdot(p-i+1)}{1\cdot\ldots\cdot i} \quad (1\leq i\leq p-1)$$

are all divisible by p and the lowest one, $\binom{p}{1}=p$, is not divisible by p^2. Hence, $\Phi_p(t+1)$ is irreducible according to Eisenstein's criterion 1.55.

It should be noted that very few polynomials satisfy the premises of Eisenstein's criterion. In practice the following method is more powerful for proving irreducibility.

Theorem (Reduction) Let R, S be two unital entire rings and $\varphi : R \to S$ be a ring homomorphism with $\varphi(1_R)=1_S$. Then φ can be canonically extended to a ring homomorphism $\Phi : R[t]\to S[t]$ with $\Phi|_R=\varphi$ via

$$\sum_{i=0}^{n}a_it^i \mapsto \sum_{i=0}^{n}\varphi(a_i)t^i \quad .$$

Let $f(t)\in R[t]$ with $\deg(\Phi(f))=\deg(f)>0$. If $\Phi(f)$ is irreducible in $S[t]$ then f cannot be written as a product $f=g\,h$ with $\deg(g)\ \deg(h)>0$ in $R[t]$.

Proof

(i) It is easily verified (see exercises) that

$$\Phi\ :\ R[t]\to S[t]\ :\ \sum_{i=0}^{n}a_i\,t^i\mapsto\sum_{i=0}^{n}\varphi\left(a_i\right)t^i$$

is indeed a ring homomorphism. Its kernel is $\ker(\Phi)=\ker(\varphi)[t]$ because of $\Phi|_R=\varphi$.

(ii) If $f=g\,h$ is a proper factorisation, i.e. $(\deg(g)\ \deg(h)>0)$ in $R[t]$, then there is a proper factorisation $\Phi(f)=\Phi(g)\,\Phi(h)$ and $\deg\left(\Phi\left(g\right)\right)\leq\deg\left(g\right)$, $\deg\left(\Phi\left(h\right)\right)\leq\deg\left(h\right)$. Because of $\deg\left(\Phi\left(f\right)\right)=\deg\left(f\right)$ and S being an entire ring we obtain upon comparing degrees that $\Phi\left(g\right)\Phi\left(h\right)$ is a proper factorisation of $\Phi\left(f\right)$. This is a contradiction to our premises.

□

The last theorem is frequently applied in irreducibility tests for polynomials in $\mathbb{Z}[t]$. In that case we choose $R = \mathbb{Z},\ S = \mathbb{Z}/p\mathbb{Z}$ for a prime number p with $p \nmid l(f)$.

Examples

(i) For $f(t) = t^3 + 39t^2 - 4t + 8 \in \mathbb{Z}[t]$ we choose $p = 3\ :\ \Phi(f) = t^3 - t - 1$ is irreducible in $\mathbb{Z}/3\mathbb{Z}[t]$, since it does not have a zero in $\mathbb{Z}/3\mathbb{Z}$.

(ii) For $f(t) = t^2 + (10^{170} + 1)t + (10^{54821} + 343) \in \mathbb{Z}[t]$ we choose $p = 2\ :\ \Phi(f) = t^2 + t + 1$ is irreducible in $\mathbb{Z}/2\mathbb{Z}[t]$. This is of interest since the detection of a zero via the divisors of the constant coefficient is practically impossible in this case.

Our next subject will be the study of calculating solutions of equations. Let R be a unital commutative ring and $f(t) \in R[t]$, say $f(t) = \sum_{i=0}^{n} a_i\, t^{n-i}$. We want to find an element x either in R or in a unital overring Λ which satisfies $f(x) = 0$. If a_0 is not a zero divisor the multiplication by a_o^{n-1} yields:

$$(a_0x)^n + a_1(a_0x)^{n-1} + \ldots + a_n a_0^{n-1} = 0\ .$$

Hence, every solution $y \in R$ of $y^n + a_1y^{n-1} + \ldots + a_n a_0^{n-1} = 0$ corresponds to a solution $x = \frac{y}{a_0}$ in $\mathfrak{Q}(R)$ and vice versa. Therefore we will assume that f is monic from now on. A unital overring Λ of R in which f has a zero is called **solution ring** of the equation $f(x) = 0$.

LEMMA 15. *Let R be a unital commutative ring and $f(t) \in R[t]$ monic of positive degree. Then $\Lambda := R[t]/f(t)R[t]$ is a solution ring of f. We note that R can be embedded into Λ.*

Proof The ring Λ has an R–basis $t^\nu + f(t)R[t]\ \ (0 \le \nu < \deg(f))$, since every polynomial $g(t) \in R[t]$ can be decomposed in $R[t]$ into

$$g(t) = Q(g,f)(t)\, f(t)\ +\ R(g,f)(t) \quad \text{with} \quad \deg(R(g,f)) < \deg(f)$$

by division with remainder. Hence, every residue class modulo $f(t)R[t]$ contains a unique representative of degree less than $\deg(f)$ and that representative can be written as a linear combination of the $t^\nu + f(t)R[t]$ $(0 \le \nu < \deg(f))$ with coefficients in R. Such a presentation is also unique since the difference of two different polynomials of degree $< \deg(f)$ each is again a polynomial of degree $< \deg(f)$. Since that difference is non zero it does not represent the class $f(t)R[t]$.
By construction of Λ we have $f(t + f(t)R[t]) = f(t) + f(t)R[t] = f(t)R[t]$, i.e. $x := t + f(t)R[t]$ is a zero of f in Λ.
An embedding of R into Λ is given by

$$\tau\ :\ R \to \Lambda\ :\ a \mapsto a + f(t)R[t]\ .$$

□

Remark The ring $\Lambda = R[t]/f(t)R[t]$ has the following 3 properties:

(i) Λ is a unital overring of R.
(ii) Λ is generated over R by a zero $x = t + f(t)R[t] \in \Lambda$ of the polynomial f and has an R–basis of $\deg(f)$ elements.
(iii) For every solution ring S in which $f(t)$ has a zero y there exists a ring homomorphism

$$\varphi \,:\, \Lambda \to S \,:\, \sum_{i=0}^{\deg(f)-1} a_i t^i + f(t)R[t] \mapsto \sum_{i=0}^{\deg(f)-1} a_i y^i \ .$$

A unital overring of R with these three properties is called **equation ring** for $f(x) = 0$. We emphasize that in equation rings (and similarly in solution rings) all calculations can be carried out easily. This will be demonstrated now. Let us assume that

$$f(t) \ = \ t^n \ + \sum_{i=1}^{n} \xi_i t^{n-i} \in R[t] \ .$$

Then any $\alpha \in \Lambda$ has a unique presentation

$$\alpha = \sum_{i=0}^{n-1} a_i x^i \ \ (a_i \in R) \ .$$

Two elements α and $\beta = \sum_{j=0}^{n-1} b_j x^j$ of Λ can be added by just adding coefficients:

$$\alpha + \beta \ = \ \sum_{i=0}^{n-1} (a_i + b_i) x^i \ .$$

Multiplication is only slightly more difficult. The immediate result

$$\alpha\beta \ = \ \sum_{k=0}^{2n-2} \left(\sum_{l=0}^{k} a_l b_{k-l} \right) x^k \ \ (a_l = 0 \ \ (l \geq n) \,,\ b_{k-l} = 0 \ \ (k - l \geq n))$$

must however be reduced to powers x^k with $k < n$. But this is exactly what the purpose of a solution ring is. Namely, we recursively obtain basis presentations for all powers of x via

$$\begin{aligned} x^n \ &= \ -\sum_{i=1}^{n} \xi_i x^{n-i} \ , \\ x^{n+1} \ &= \ -\sum_{i=2}^{n} \xi_i x^{n+1-i} - \xi_1 \left(-\sum_{i=1}^{n} \xi_i x^{n-i} \right) \ . \end{aligned}$$

If we assume that we know the coefficients of the presentation

$$x^k \ = \ \sum_{i=0}^{n-1} a_{ki} x^i$$

we get the coefficients $a_{k+1,i}$ of the presentation for x^{k+1} immediately from

$$x^{k+1} \ = \ \sum_{i=1}^{n-1} a_{k,i-1} x^i \ - \ \sum_{i=0}^{n-1} a_{k,n-1} \xi_{n-i} x^i \ ,$$

hence

$$a_{k+1,i} \;=\; a_{k,i-1} - a_{k,n-1}\xi_{n-i} \;\; (0 \le i \le n-1\,,\; a_{k,-1} := 0) \;\; .$$

Examples

(i) Let $R = \mathbb{Z}/8\mathbb{Z}$ and $f(t) = t^2 - 1 \in R[t]$. $\Lambda = R[t]/f(t)R[t]$ has an R–basis $1 + f(t)R[t],\; t + f(t)R[t] =: x$. On the other hand, R itself is a solution ring and we therefore have ring homomorphisms

$$\varphi \;:\; \Lambda \to R \text{ via } t + f(t)R[t] \mapsto \alpha \text{ with } \alpha \in \{1,\, 3,\, 5,\, 7\} \;\; .$$

This situation is enlightened by the following diagram:

$$\begin{array}{ccc}
a(1 + f(t)R[t]) + b(t + f(t)R[t]) & \mapsto & a + \alpha\, b \\
(a(1 + f(t)R[t]) + b(t + f(t)R[t]))(c(1 + f(t)R[t]) + d(t + f(t)R[t])) & \mapsto & (a + \alpha\, b)\,(c + \alpha\, d) \\
\| & & \| \\
ac(1 + f(t)R[t]) + (ad + bc)(t + f(t)R[t]) + bd(1 + f(t)R[t]) & & (ac + \alpha^2 bd) + \alpha\,(ad + bc) \\
\| & & \| \\
(ac + bd)(1 + f(t)R[t]) + (ad + bc)(t + f(t)R[t]) & & (ac + bd) + \alpha\,(ad + bc) \;\; .
\end{array}$$

(ii) If $f(t) = t^3 + pt^2 + qt + r \in R[t]$ has a zero x in Λ then the polynomial $f(t)$ decomposes in $\Lambda[t]$, one factor being $t - x$. Dividing f in $\Lambda[t]$ by $t - x$ we obtain

$$f(t) \;=\; (t - x)\,(t^2 + (p + x)\,t + q + x\,(x + p)) \;\; .$$

Comparing coefficients we get the following relation for r in Λ: $r = -x\,(x\,(x + p) + q)$.

(iii) Let us assume that $t^2 + m$ is irreducible over R (for example, $m = 1$, $R = \mathbb{R}$ or $m = -2$, $R = \mathbb{Z}/5\mathbb{Z}$). Then $\Lambda := R[t]/f(t)R[t]$ has a basis $1,\, x := t + f(t)R[t]$. Therefore we have $R[t]/f(t)R[t] \cong R \times R$. But what does the ring structure on $R \times R$ look like? Addition is clearly done coordinatewise. Multiplication needs to be transfered from Λ, however. Because of $x^2 = -m$ we obtain

$$\begin{aligned}
(a + bx) \cdot (c + dx) \;&=\; ac - mbd + (bc + da)x \;\; \text{, hence} \\
(a,\, b) \cdot (c,\, d) \;&=\; (ac - mbd,\, bc + da)
\end{aligned}$$

in $R \times R$.

KOROLLAR 16. *By a* $(\deg(f) - 1)$*–fold application of the construction in 8 we obtain a ring* $S(f,\, R)$ *(***splitting ring** *of* f *over* R*) with* $\deg(f)!$ *basis elements over* R*.*

PROPOSITION 17. *Let* F *be a field and* $f(t) \in F[t]$ *of positive degree. Then there exists an extension field* E *of* F *in which* f *has a zero.*

Proof In $F[t]$ the polynomial f splits into a product of irreducible polynomials. We assume that g is such an irreducible factor. In case $\deg(g) = 1$ the polynomial g (and therefore f) has a zero in F. Now let us assume that $\deg(g) > 1$. Since $F[t]$ is a principal ideal ring the ideal $g(t)F[t]$ is maximal. Hence, $E := F[t]/g(t)F[t]$ is a field. According to 8 the polynomial g (and therefore f) has a zero in E.
□

Theorem Let F be a field and $f(t) \in F[t]$ of positive degree. Then there exists an extension field E of F such that f splits in $E[t]$ into a product of linear factors:

$$f(t) = l(f) \prod_{i=1}^{\deg(f)} (t - x_i) \quad (x_i \in E) \quad .$$

Hence, all zeros of f are contained in E.

Proof We do this by induction over the degree $n := \deg(f)$ of f. For $n = 0$ the polynomial f is constant and equals its leading coefficient. In this case, the product over the monic linear factors is empty. By induction hypothesis we assume that the theorem is true for all polynomials of degree less than or equal to n. Let $f(t) \in F[t]$ be a polynomial of degree $n + 1$. By 10 there exists an extension field E_1 of F in which f has a zero, say x_1. In $E_1[t]$ the polynomial $f(t)$ therefore splits into two factors: $f(t) = (t - x_1)\, g(t)$, with a polynomial g of degree n and with $l(f) = l(g)$. According to our induction assumption there exists an extension field E of E_1 so that g splits in $E[t]$ into a product of linear factors

$$g(t) = l(g) \prod_{i=2}^{n+1} (t - x_i) \quad (x_2, ..., x_{n+1} \in E) \quad ,$$

hence,

$$f(t) = l(f) \prod_{i=1}^{n+1} (t - x_i) \quad .$$

□

Example Let $f(t) \in F[t]$ be monic. Then f splits in $E[t]$ with zeros $x_i \in E$ in the following way:

$$\begin{aligned} f(t) &= \prod_{i=1}^{n} (t - x_i) \\ &= (t - x_1)\,(t - x_2)\, \ldots\, (t - x_n) \\ &= t^n - t^{n-1} \sum_{i=1}^{n} x_i + t^{n-2} \sum_{i<j} x_i\, x_j \\ &\quad + \ldots + (-1)^{n-k} t^k \sum_{1 \le i_1 < i_2 < \ldots < i_k \le n} x_{i_1} \cdot \ldots \cdot x_{i_k} \\ &\quad + \ldots + (-1)^n\, x_1 \cdot \ldots \cdot x_n \quad . \end{aligned}$$

This will be used in the next section when we discuss elementary symmetric functions.

3.56. Symmetric Polynomials and the Fundamental Theorem of Algebra

3.57. Definition

Let R be a unital commutative ring. A polynomial $f(\mathbf{t}) \in R[\mathbf{t}]$ $(\mathbf{t} = (t_1, ..., t_n))$ is called **symmetric** if it satisfies $f(\mathbf{t}) = f(t_{\pi(1)}, ..., t_{\pi(n)})$ for all $\pi \in \mathfrak{S}_n$. Special symmetric polynomials are

$$\begin{aligned} \sigma_0(\underline{t}) &:= 1 \\ \sigma_j(\underline{t}) &:= \sum_{1 \le i_1 < i_2 < ... < i_j \le n} t_{i_1} \cdot ... \cdot t_{i_j} \quad (1 \le j \le n) \end{aligned}$$

which are called **elementary symmetric functions** in $t_1, ..., t_n$. Here we shortly wrote σ_j instead of the more precise $\sigma_j^{(n)}$.

Examples

(i) Among the elementary symmetric functions

$$\begin{aligned} \sigma_1(\mathbf{t}) &= t_1 + ... + t_n \ , \\ \sigma_2(\mathbf{t}) &= t_1t_2 + ... + t_1t_n + t_2t_3 + ... + t_2t_n + ... + t_{n-1}t_n \ , \\ \sigma_n(\mathbf{t}) &= t_1 ... t_n \end{aligned}$$

are used most frequently.

(ii) Let $f(\mathbf{t}, t) \in R[t_1, ..., t_n, t]$ be monic of degree n with $f(\mathbf{t}, t_i) = 0$ $(1 \le i \le n)$ and R be a factorial ring. Then we obtain

$$\begin{aligned} f(\mathbf{t}, t) &= \prod_{i=1}^{n} (t - t_i) \\ &= \sum_{j=0}^{n} (-1)^{n-j} \, \sigma_{n-j}(\mathbf{t}) \, t^j \\ &= \sum_{i=0}^{n} (-1)^{i} \, \sigma_i(\mathbf{t}) \, t^{n-i} \ . \end{aligned}$$

(iii) Specializing the variables $t_{l+1}, ..., t_n$ to zero we obtain symmetric polynomials

$$\sigma_k^{(l)}(t_1, \ldots, t_n) := \sigma_k(t_1, \ldots, t_l, 0, \ldots, 0) \ (1 \le k \le l) \ .$$

of the same degree. For $k > l$ such a specialization yields zero.

Remark The symmetric polynomials form a subring of $R[t_1, ..., t_n]$. The specialization

$$\Phi_{\underline{\sigma}} \ : \ R[t_1, ..., t_n] \to R[t_1, ..., t_n] \ : \ f \mapsto f(\sigma_1, ..., \sigma_n)$$

maps f onto a symmetric polynomial.
Theorem (Principal theorem for elementary symmetric functions) Let R be a factorial ring. Then every symmetric polynomial $f(\mathbf{t}) \in R[\mathbf{t}]$ can be written as $g(\sigma_1, ..., \sigma_n)$ for a uniquely determined polynomial $g(\mathbf{t}) \in R[\mathbf{t}]$.

Proof We introduce a **weight** w for monomials. For

$$g(\mathbf{t}) = a\, t_1^{m_1} \cdot \ldots \cdot t_n^{m_n} = a\mathbf{t}^{\underline{m}}$$

we set $w(t_k) = k,\ w(g) := \sum_{i=1}^{n} i\, m_i$. Accordingly the **weight of a polynomial** is defined as the maximum of the weights of the occuring monomials. For

$$f(\mathbf{t}) \ = \sum_{\underline{\nu} \in (\mathbb{Z}^{\geq 0})^n} a_{\underline{\nu}} \mathbf{t}^{\underline{\nu}}$$

we set

$$w(f) = \max \{w(\mathbf{t}^{\underline{\nu}}) \mid a_{\underline{\nu}} \neq 0\} \ .$$

Hence, the weight of a polynomial $w(f(\mathbf{t}))$ is exactly the degree of the polynomial $f(\sigma_1, \ldots, \sigma_n)$.

Proof of the existence of a polynomial g.
We show that for every symmetric polynomial $f(\mathbf{t}) \in R[\mathbf{t}]$ of degree d there exists a polynomial $g(\mathbf{t}) \in R[\mathbf{t}]$ of weight $w(g) \leq d$ such that $f(\mathbf{t}) = g(\sigma_1, ..., \sigma_n)$. The proof is by induction on n.
For $n = 1$ we can put $f = g$ because we have $\sigma_1 = t_1$ in this case.
Hence, we assume that we have shown the theorem for polynomials in $n-1$ variables. To obtain the result also for polynomials in n variables we apply induction on the degree d of f.
For $d \leq 0$ the polynomial f is constant and $g = f$ does the job. We now assume that $d > 0$ and that the statement is true for polynomials of degree less than d. Let f be an arbitrary polynomial of degree d. Specializing $t_n \mapsto 0$ in f we obtain $f^{(n-1)}(t_1, ..., t_{n-1})$ of degree at most d. According to our induction hypothesis about the number of variables there exists a polynomial $g_1(t_1, ..., t_{n-1}) \in R[t_1, ..., t_{n-1}] \subseteq R[t_1, ..., t_n]$ of weight $\leq d$ with

$$\begin{aligned} f(t_1, ..., t_{n-1}, 0) \ &= \ g_1(\sigma_1^{(n-1)}, ..., \sigma_{n-1}^{(n-1)}) \\ &\quad\ (\sigma_i^{(n-1)} := \sigma_i(t_1, ..., t_{n-1}, 0)) \ . \end{aligned}$$

We put $h(\mathbf{t}) := f(\mathbf{t}) - g_1(\sigma_1, ..., \sigma_{n-1})$. The polynomial h then is again symmetric of degree $\leq d$. We have $h(t_1, ..., t_{n-1}, 0) = 0$, the polynomial h is therefore divisible by t_n. h being symmetric it is then divisible by all t_i $(1 \leq i \leq n)$. Hence, $R[\mathbf{t}]$ being a factorial ring, h is divisible by σ_n. We therefore get $h(\mathbf{t}) = \sigma_n h_1(\mathbf{t})$ with h_1 again being symmetric. We either have $h_1 = 0$ or $\deg(h_1) = \deg(h) - n < d$. According to our induction assumption on d there exists $g_2 \in R[t_1, ..., t_n]$ of weight

$\leq d-n$ with $h_1(t_1,...,t_n) = g_2(\sigma_1,...,\sigma_n)$. Putting things together we obtain $f(\mathbf{t}) = g(\sigma_1,...,\sigma_n)$ for

$$g(\sigma_1,...,\sigma_n) \;=\; g_1(\sigma_1,...,\sigma_n) \;+\; \sigma_n\, g_2(\sigma_1,...,\sigma_n) \;\;.$$

Proof of uniqueness of g.
To prove uniqueness we show that for $f(\mathbf{t}) \in R[\mathbf{t}]$ with $f(\sigma_1,...,\sigma_n) = 0$ we must have $f = 0$. The proof is by induction on the number n of variables. For $n = 1$ the statement is trivial because of $\sigma_1 = t_1$. Now we assume that uniqueness is guaranteed for polynomials of at most $n-1$ variables. We let $0 \neq f(\mathbf{t}) \in R[\mathbf{t}]$ be a symmetric polynomial in n variables and of minimal degree with $f(\sigma_1,...,\sigma_n) = 0$. We write f as a polynomial in t_n: $f(t_1,...,t_n) = \sum_{i=0}^{k} f_i(t_1,...,t_{n-1})\, t_n^i$. The coefficient $f_0(t_1,...,t_{n-1})$ cannot be zero. Otherwise the polynomial f would be divisible by t_n and therefore – as we saw above – by σ_n in contradiction to our degree assumption. Specializing $t_n \mapsto 0$ we obtain that f_0 is symmetric in $n-1$ variables with

$$0 = f(\sigma_1^{(n-1)},...,\sigma_n^{(n-1)},0) = f_0(\sigma_1^{(n-1)},...,\sigma_{n-1}^{(n-1)}) \;\;,$$

again a contradiction to our induction assumption.
□

Example For $f(t_1,t_2,t_3) = (t_1-t_2)^2\,(t_1-t_3)^2\,(t_2-t_3)^2$ we have

$$\begin{aligned} f(t_1,t_2,0) &= (t_1-t_2)^2\,(t_1t_2)^2 \\ &= ((\sigma_1^{(2)})^2 - 4\,\sigma_2^{(2)})\,(\sigma_2^{(2)})^2 \;\;; \end{aligned}$$

and consequently $h(\mathbf{t}) = \sigma_3\, h_1(\mathbf{t})$ with

$$\begin{aligned} h_1(t_1,t_2,0) &= 18\,\sigma_1^{(2)}\,\sigma_2^{(2)} - 4\,(\sigma_1^{(2)})^3 \\ h_2(\mathbf{t}) &= h_1(\mathbf{t}) - 18\,\sigma_1^{(3)}\,\sigma_2^{(3)} + 4\,\sigma_1^{(3)} \\ &= -27\,t_1t_2t_3 \\ &= -27\,\sigma_3 \;\;. \end{aligned}$$

Putting things together we obtain

$$f(t_1,t_2,t_3) = \sigma_1^2\,\sigma_2^2 - 4\,\sigma_2^3 + \sigma_3\,(18\,\sigma_1\,\sigma_2 - 4\,\sigma_1^3 - 27\,\sigma_3) \;\;.$$

Besides the elementary symmetric functions there is another set of symmetric polynomials, the so–called **power sums**:

$$S_k := S_k(\mathbf{t}) := \sum_{i=0}^{n} t_i^k \;\; (k \in \mathbb{Z}^{\geq 0}) \;\;.$$

Calculations with them are usually easier than with the σ_i. However, a transfer from power sums to elementary symmetric functions is generally possible only in characteristic zero, as we will see below.
Theorem The power sums S_k and the elementary symmetric functions σ_j are connected via **Newton's relations**:

(i)

$$\sum_{i=0}^{k-1}(-1)^i\,\sigma_i(\mathbf{t})\,S_{k-i}(\mathbf{t}) + k\,(-1)^k\,\sigma_k(\mathbf{t}) = 0 \quad (0 \le k \le n) \ ,$$

(ii)

$$\sum_{i=0}^{n}(-1)^i\,\sigma_i(\mathbf{t})\,S_{k-i}(\mathbf{t}) = 0 \quad (k \ge n) \ .$$

Proof The polynomial

$$f(t_1,...,t_n,t) := \sum_{j=0}^{n}(-1)^j\,\sigma_j(\mathbf{t})\,t^{n-j} = \prod_{j=1}^{n}(t-t_j)$$

in $n+1$ variables $t_1,...,t_n,t$ satisfies

$$0 = \sum_{j=0}^{n}(-1)^j\,\sigma_j(\mathbf{t})\,t_i^{n-j} \quad (1 \le i \le n) \ ,$$

respectively,

$$0 = \sum_{j=0}^{n}(-1)^j\,\sigma_j(\mathbf{t})\,t_i^{k-j} \quad (1 \le i \le n,\ k \ge n) \ .$$

Summing up these n equations yields

$$\sum_{j=0}^{n}(-1)^j\,\sigma_j(\mathbf{t})\,S_{k-j}(\mathbf{t}) = 0 \ ,$$

hence 2., respectively 1. in case $k = n$. The remaining part of 1. will now be proved for fixed k via induction on the number of variables n. For the initial value $n = k$ we have already proved it. Therefore we assume that $n > k$ and that the theorem is true for $n-1$ variables. We put

$$F(t_1,...,t_n) := \sum_{i=0}^{k-1}(-1)^i\,\sigma_i(\mathbf{t})\,S_{k-i}(\mathbf{t}) + (-1)^k\,k\,\sigma_k(\mathbf{t}) \ .$$

F is certainly a symmetric function of degree $\le k$ and because of $k < n$ also less than n. By induction assumption we have $F(t_1,...,t_{n-1},0) = 0$. Hence, $F(\mathbf{t})$ is divisible by t_n – and since it is symmetric – also by $\sigma_n(\mathbf{t})$. Because of $\deg(F) < n$ the polynomial F must therefore be 0.
□

Example We list the first few of Newton's relations:

$$\begin{aligned} S_1(\mathbf{t}) &= \sigma_1(\mathbf{t}), \\ S_2(\mathbf{t}) &= \sigma_1(\mathbf{t})\,S_1(\mathbf{t}) - 2\,\sigma_2(\mathbf{t}) \\ &= \sigma_1^2(\mathbf{t}) - 2\,\sigma_2(\mathbf{t}), \\ S_3(\mathbf{t}) &= \sigma_1(\mathbf{t})\,S_2(\mathbf{t}) - \sigma_2(\mathbf{t})\,S_1(\mathbf{t}) + 2\,\sigma_3(\mathbf{t}) \\ &= \sigma_1^3(\mathbf{t}) - 3\,\sigma_1(\mathbf{t})\,\sigma_2(\mathbf{t}) + 3\,\sigma_3(\mathbf{t}) \ . \end{aligned}$$

If the natural numbers are no zerodivisors in R then we can also express the σ_k by the S_k over $\mathfrak{Q}(R)$:

$$\begin{aligned}
\sigma_1(\mathbf{t}) &= S_1(\mathbf{t}), \\
\sigma_2(\mathbf{t}) &= \frac{1}{2}\,(S_1(\mathbf{t})^2 - S_2(\mathbf{t})), \\
\sigma_3(\mathbf{t}) &= \frac{1}{3}\left(S_2(\mathbf{t}) - S_1(\mathbf{t})^3 + 3\,S_1(\mathbf{t})\,\frac{1}{2}\,(S_1(\mathbf{t})^2 - S_2(\mathbf{t}))\right) \\
&= \frac{1}{6}\,(2\,S_3(\mathbf{t}) + S_1(\mathbf{t})^3 - 3\,S_1(\mathbf{t})\,S_2(\mathbf{t}))\ .
\end{aligned}$$

3.58. Definition

The polynomial

$$d(f) := a_0^{2n-2} \prod_{1\le i<j\le n} (t_i - t_j)^2$$

of $R[\mathbf{t}]$ is called **discriminant** of the polynomial

$$f(t) \;=\; a_0 \prod_{i=1}^{n} (t - t_i) \;\in R[\mathbf{t}][t]\ .$$

The exponent of a_0 is chosen minimal such that $d(f)$ belongs to $R[\mathbf{t}]$. This will be shown in the next proposition.

Example A monic quadratic polynomial $t^2 + at + b \in \mathbb{R}[t]$ has the zeros $x_{1,2} = -\frac{a}{2} \pm \sqrt{\frac{a^2-4b}{4}}$. Its discriminant is therefore $(x_1 - x_2)^2 = a^2 - 4b$. We note that the sign of the discriminant decides whether both zeros are real or complex. The discriminant vanishes if and only if both zeros coincide.

Proposition 18. *The discriminant of the polynomial*

$$f(t) \;=\; \sum_{i=0}^{n} a_i t^{n-i} \;=\; a_0 \prod_{i=1}^{n} (t - x_i)$$

satisfies

$$a_0\, d(f) \;=\; (-1)^{\binom{n}{2}} \operatorname{res}(f, f')\ .$$

The discriminant $d(f)$ is an element of R.

Proof The derivative of the given polynomial is

$$f'(t) \;=\; a_0 \sum_{i=1}^{n} \prod_{\substack{j=1 \\ j\neq i}}^{n} (t - x_j)\ .$$

Hence, we obtain

$$f'(x_i) \;=\; a_0 \prod_{\substack{j=1 \\ j\neq i}}^{n} (x_i - x_j)$$

and can easily calculate the resultant of f and f':

$$\begin{aligned}
\operatorname{res}(f,f') &= a_0^{n-1}\prod_{i=1}^{n} f'(x_i) \\
&= a_0^{n-1}\prod_{i=1}^{n}\left(a_0\prod_{\substack{j=1\\ j\neq i}}^{n}(x_i-x_j)\right) \\
&= a_0^{2n-1}\prod_{i=1}^{n}\left(\prod_{j>i}(x_i-x_j)\prod_{j<i}(-(x_j-x_i))\right) \\
&= a_0^{2n-1}(-1)^{\sum_{i=1}^{n}(i-1)}\prod_{1\le i<j\le n}(x_i-x_j)^2 \\
&= (-1)^{\binom{n}{2}}a_0\,d(f)\ .
\end{aligned}$$

To prove the second statement we consider $\operatorname{res}(\frac{f}{a_0},\frac{f'}{a_0})$ as determinant of a $(2n-1)\times(2n-1)$ matrix. The first column of that matrix has entries of $\{0,1,n\}$. The remaining $2n-2$ columns contain – besides zeros – entries of the form

$$\frac{a_i}{a_0}\ \ (1\le i\le n)\ \text{ or }\ (n-i)\,\frac{a_i}{a_0}\ \ (1\le i<n)\ .$$

Hence, upon multiplication with a_0^{2n-2} that resultant belongs to the ring R.
□

For readers familiar with matrices and determinants we give the following proposition as an exercise.

PROPOSITION 19. *In $R[\mathbf{t}]$ the discriminant satisfies*

$$d(f)=a_0^{2n-2}\det\left((S_{i+j-2}(\mathbf{t})_{1\le i,j\le n}\right)\ .$$

(Hint: The proof makes use of Vandermonde's determinant.)

Theorem (Fundamental Theorem of Algebra)
Every polynomial $f(t)\in\mathbb{C}[t]$ of positive degree n has a zero in $\mathbb{C}$. This is tantamount to the statement that f can be factored in $\mathbb{C}[t]$ into linear factors:

$$f(t)=l(f)\prod_{j=1}^{n}(t-x_j)\quad(x_j\in\mathbb{C})\ .$$

We also say that $\mathbb{C}$ is **algebraically closed** since all elements which are algebraic over $\mathbb{C}$ already belong to $\mathbb{C}$.

Proof

(i) In a first step the statement is reduced to polynomials with real coefficients. For $f(t)\in\mathbb{C}[t]$ we form the product of $f(t)$ and its complex conjugate $\overline{f(t)}$ which is obtained from f by

applying complex conjugation to every coefficient. Since that product is invariant under complex conjugation it must be contained in $\mathbb{R}[t]$:

$$g(t) := f(t)\overline{f(t)} \ \in \mathbb{R}[t] \ .$$

Assuming that the statement is true for polynomials in $\mathbb{R}[t]$ we get

$$g(t) := |l(f)|^2 \prod_{j=1}^{2n}(t - c_j) \ .$$

Because of the preceding remark with c_j also $\overline{c_j}$ is a zero of $g(t)$. We order the c_j such that $c_{n+j} = \overline{c_j}$ $(1 \leq j \leq n)$. This yields

$$f(t) = l(f) \prod_{j=1}^{n}(t - c_j) \quad (1 \leq j \leq n) \ .$$

(ii) We need to show that every polynomial of positive degree in $\mathbb{R}[t]$, say $f(t) = t^n + a_1 t^{n-1} + \ldots + a_n \ \in \mathbb{R}[t]$, has a zero in $\mathbb{C}$. It is remarkable that all known proofs for this are not purely algebraic inasmuch as they require some elements from analysis, usually a form of the intermediate value theorem. The intermediate value theorem tells us that a polynomial of $\mathbb{R}[t]$ of odd degree – being interpreted as a continuous function from $\mathbb{R}$ to $\mathbb{R}$ – has a zero in $\mathbb{R}$. Hence, we can assume that $\deg(f) = 2^k q$ with $k \in \mathbb{N}$, $q \in \mathbb{N}$ odd. The proof for the latter is by induction on k. For the initial value $k = 0$ we already saw this. Hence, we assume that $k > 0$ and that the statement is true for degrees of f divisible at most by 2^{k-1}. According to 1.55 there is an extension field K of $\mathbb{R}$ over which $f(t)$ decomposes into a product of linear factors:

$$f(t) = l(f) \prod_{j=1}^{n}(t - x_j) \ .$$

Following an idea of Laplace we consider the polynomials

$$L_r(t) := \prod_{1 \leq \mu < \nu \leq n} (t - x_\mu - x_\nu - r\, x_\mu x_\nu) \ \in K[t] \ \ (r \in \mathbb{R}) \ .$$

We note that the coefficients of $L_r(t)$ are symmetric functions in the zeros x_j. Hence, the coefficients of L_r can be written as polynomials in the elementary symmetric functions $\sigma_j(\mathbf{x}) = (-1)^j a_j$ implying $L_r(t) \in \mathbb{R}[t]$. Then

$$\deg(L_r) = \frac{n}{2}\,(n-1) = 2^{k-1} q\,(2^k q - 1) = 2^{k-1}\tilde{q} \ ,$$

$\tilde{q}$ is odd, and L_r has a zero z_r in $\mathbb{C}$ for every $r \in \mathbb{R}$ according to our induction assumption. For every $r \in \mathbb{R}$ there exist indices

μ, ν with

$$z_r := x_\mu + x_\nu + r\, x_\mu x_\nu \ \in \mathbb{C} \ .$$

Since the number of pairs of indices μ, ν is finite, the number of parameters $r \in \mathbb{R}$ is infinite there must exist $r \neq \tilde{r}$ in R, $1 \leq \mu < \nu \leq n$ with

$$x_\mu + x_\nu + r\, x_\mu x_\nu,\ x_\mu + x_\nu + \tilde{r}\, x_\mu x_\nu \ \in \mathbb{C} \ .$$

This has the consequences $x_\mu x_\nu \in \mathbb{C}$, $x_\mu + x_\nu \in \mathbb{C}$, i.e. x_μ, x_ν are zeros of

$$t^2 - (x_\mu + x_\nu)\, t + x_\mu x_\nu \ \in \mathbb{C}[t] \ ,$$

and therefore also x_μ, x_ν belong to $\mathbb{C}$. Here we use that square roots of complex numbers again belong to $\mathbb{C}$. Hence, $f(t)$ has at least 2 zeros in $\mathbb{C}$.

□

KOROLLAR 20. *Every polynomial $f(t) \in \mathbb{R}[t]$ of positive degree can be decomposed as*

$$f(t) = l(f) \prod_{i=1}^{k} (t - c_i) \prod_{j=1}^{l} q_j(t)$$

with $c_i \in \mathbb{R}$, $q_j(t) = t^2 + u_j t + v_j \in \mathbb{R}[t]$ irreducible $(1 \leq j \leq l))$. This presentation is unique up to the order of the factors.

Proof We let $c_1, ..., c_k$ denote all real zeros of $f(t)$. Then we obtain

$$f(t) = l(f) \prod_{i=1}^{k} (t - c_i)\, g(t) \ ,$$

where the polynomial $g(t) \in \mathbb{R}[t]$ is uniquely determined. Then for every zero $x \in \mathbb{C}$ of $g(t)$ also $\overline{x}$ is a zero. We therefore order the zeros of g appropriately to obtain $g(t) = \prod_{j=1}^{l} (t - z_j)(t - \overline{z_j})$. Then we put

$$q_j(t) = t^2 - (z_j + \overline{z_j})\, t + z_j \overline{z_j} \ \in \mathbb{R}[t] \ \ (1 \leq j \leq l) \ .$$

The uniqueness of that presentation – up to the order of the factors – is a consequence of $\mathbb{R}[t]$ being a factorial ring..

□

KOROLLAR 21. *The irreducible elements of $\mathbb{C}[t]$ are the polynomials of degree one. The irreducible elements of $\mathbb{R}[t]$ are the polynomials of degree one and those polynomials $t^2 + ut + v$ of degree two with $u^2 - 4v < 0$.*

The next theorem is an appendix for readers already familiar with vector spaces. **Theorem** Let Λ be a unital entire commutative overring of $\mathbb{R}$ in which every element is algebraic over $\mathbb{R}$. Then Λ is isomorphic either to $\mathbb{R}$ or to $\mathbb{C}$.

Proof Let us assume that $\Lambda \neq \mathbb{R}$. For $x \in \Lambda \setminus \mathbb{R}$ we obtain a 2–dimensional $\mathbb{R}$–vectorspace $V := \mathbb{R}1 + \mathbb{R}x$. Also there exists $f(t) \in \mathbb{R}[t]$ of positive degree with $f(x) = 0$. Because of the fundamental theorem the minimal polynomial of $x \in \Lambda \setminus \mathbb{R}$ is necessarily of degree 2, say

$$g(t) = t^2 + ut + v \ \in \mathbb{R}[t] \quad (u^2 - 4v < 0) \ .$$

This implies $x^2 = -ux - v$ in Λ. Therefore we can introduce a multiplication in V via

$$\begin{aligned} (a + bx)\,(c + dx) &:= ac + (ad + bc)\,x + (-ux - v)\,bd \\ &= (ac - vbd) + (ad + bc - ubd)\,x \quad . \end{aligned}$$

Thus V becomes a commutative unital entire overring of $\mathbb{R}$ with a 2–element basis. We show that V is isomorphic to $\mathbb{C}$ via

$$a + bx \mapsto a + \frac{b}{2}\,(-u + iD) \quad \text{for} \quad D = \sqrt{4v - u^2} \ .$$

That mapping is a priori surjective and injective and also additive. Its multiplicativity follows from the diagram

$$\begin{array}{ccc} (a+bx)\,(c+dx) & \mapsto & \left(a + \frac{b}{2}\,(-u+iD)\right)\left(c + \frac{d}{2}\,(-u+iD)\right) \\ \| & & \| \\ (ac - bdv) + x\,(bc + ad - ubd) & & ac + (\frac{ad}{2} + \frac{bc}{2})(-u+iD) + \frac{bd}{4}\,(u^2 - 2uDi - D^2) \\ \downarrow & & \| \\ ac - bdv + (bc + ad - ubd)\,\frac{1}{2}\,(-u+iD) & & ac - \frac{u}{2}\,(ad + bc - bdu) - bdv + \frac{i}{2}\,D\,(ad + bc - bdu) \end{array}$$

We still need to prove that $\Lambda = V$. For this we let $y \in \Lambda \setminus \mathbb{R}$ arbitrary, $f(t) \in \mathbb{R}[t]$ with $f(y) = 0$. Making use of $V \cong \mathbb{C}$ we conclude that f decomposes into linear factors $t - \lambda \ \ (\lambda \in V)$, so we get $y = \lambda$ for a suitable choice of λ.

□

Remark The last theorem shows that any $\mathbb{R}$–vectorspace V of dimension r cannot be a field for $r > 2$.

3.59. Multivariate Polynomials and Gröbner Bases

To make the presentation easier we assume in this paragraph that all polynomials have coefficients in a base field F. We emphasize, however, that all concepts which we develop can be generalized to polynomials with coefficients in a Noetherian ring R. In any case, every ideal in the ring of polynomials is finitely generated. The goal of this section is to develop an algorithm for the computation of special sets of generators for arbitrary ideals, so-called Gröbner bases. They have turned out to be one of the strongest tools in computer algebra. For example, using Gröbner bases it is easy to decide whether a polynomial belongs to a given ideal. Another application is to the solution of non linear systems of algebraic equations.

We recall several notations about multivariate polynomials. Usually, we will consider polynomials in n variables, i.e. from $F[t_1, ..., t_n]$ which

we abbreviate by $F[\mathbf{t}]$. Any polynomial $f(\mathbf{t})$ is a finite sum of monomials $m(\mathbf{t}) = a\prod_{i=1}^{n} t_i^{m_i} =: a_{\mathbf{m}}\mathbf{t}^{\mathbf{m}}$. The sum $m_1 + ... + m_n$ is called the **degree** of the monomial $m(\mathbf{t})$. If the coefficient $a \in F$ of $m(\mathbf{t})$ is one the monomial is called monic. We note that the least common multiple lcm and the greatest common divisor gcd of two monic monomials $m(\mathbf{t})$, $k(\mathbf{t})$ are given by

$$\mathrm{lcm}(m,k) \;=\; \prod_{i=1}^{n} t_i^{\max(m_i,k_i)} \;,\; \gcd(m,k) \;=\; \prod_{i=1}^{n} t_i^{\min(m_i,k_i)} \quad .$$

Analogously to the case of univariate polynomials we would like to put the monomials of a polynomial into a specific order. Of course, we can do this with respect to their degrees, but in case $n > 1$ there exist monic monomials of the same degree which do not coincide. For example, we must decide whether $t_1^2 t_2$ or $t_1 t_2^2$ should come first.
This means to introduce a total ordering on the set $\mathcal{S}$ of all monic monomials. Clearly, once the variables have been fixed we can identify each monic monomial with its vector $\mathbf{m} = (m_1, ..., m_n)$ of exponents. This establishes a monoid isomorphism between the multiplicative monoid $\mathcal{S}$ and the additive monoid $(\mathbb{Z}^{\geq 0})^n$. The ordering to be chosen should be compatible with the law of composition of the monoid, i.e. we require that for elements α, β, γ of the monoid the ordering $\alpha > \beta$ implies $\alpha\gamma > \beta\gamma$. Also the property that every non-zero subset of the monoid contains a minimal element will be useful. This element is then unique since we requested a total ordering.
In practice, the following orderings on $\mathcal{S}$ have turned out to be of special interest.

(i) **Lexicographical Ordering** $>_{lex}$
For elements of $(\mathbb{Z}^{\geq 0})^n$ we say that $\mathbf{m} = (m_1, ..., m_n)$ is bigger than $\mathbf{k} = (k_1, ...k_n)$ if there is a smallest index, say i, such that $m_j = k_j$ for $1 \leq j < i$ and $m_i > k_i$.
For example, we have $(1, 2, 0) >_{lex} (0, 3, 4)$ and $(3, 2, 4) >_{lex} (3, 2, 1)$.

(ii) **Inverse Lexicographical Ordering** $>_{ilex}$
For elements of $(\mathbb{Z}^{\geq 0})^n$ we say that $\mathbf{m} = (m_1, ..., m_n)$ is bigger than $\mathbf{k} = (k_1, ...k_n)$ if there is a largest index, say i, such that $m_j = k_j$ for $i < j \leq n$ and $m_i > k_i$.
For example, we have $(4, 7, 4) >_{ilex} (4, 2, 3)$ and $(5, 1, 3) >_{ilex} (4, 1, 3)$.

(iii) **Graded Lexicographical Ordering** $>_{glex}$
For elements of $(\mathbb{Z}^{\geq 0})^n$ we say that $\mathbf{m} = (m_1, ..., m_n)$ is bigger than $\mathbf{k} = (k_1, ...k_n)$ if either $m_1 + ... + m_n > k_1 + ... + k_n$ or $m_1 + ... + m_n = k_1 + ... + k_n$ and $\mathbf{m} >_{lex} \mathbf{k}$. For example, we have $(1, 2, 3) >_{glex} (3, 2, 0)$ and $(1, 2, 4) >_{glex} (1, 1, 5)$.

(iv) **Graded Inverse Lexicographical Ordering** $>_{gilex}$
For elements of $(\mathbb{Z}^{\geq 0})^n$ we say that $\mathbf{m} = (m_1, ..., m_n)$ is bigger

than $\mathbf{k} = (k_1, ...k_n)$ if either $m_1 + ... + m_n > k_1 + ... + k_n$ or $m_1 + ... + m_n = k_1 + ... + k_n$ and $\mathbf{m} >_{ilex} \mathbf{k}$.
For example, we have $(4, 7, 1) >_{gilex} (4, 2, 3)$ and $(1, 4, 3) >_{gilex} (4, 1, 3)$.

It is straightforward that all three orderings are total orderings of $(\mathbb{Z}^{\geq 0})^n$. Also the compatibility of these orderings with addition is immediate. We leave it as an exercise to the reader to show that every non-empty subset of $(\mathbb{Z}^{\geq 0})^n$ has a minimal element. We note that the inverse lexicographical ordering is used to look at the elements of $F[\mathbf{t}]$ as polynomials in the variable t_n with coefficients in $F[t_1, ..., t_{n-1}]$ (recursive representation).
Since every polynomial f is a finite sum of monomials any (total) ordering of the monomials can be used to introduce a (partial) ordering of the polynomials. Especially, we can define the **leading monomial (leading term)** $\mathrm{lt}(f)$ as the largest monomial $a_{\mathbf{m}}\mathbf{t}^{\mathbf{m}}$ occuring in the presentation of f. We denote the corresponding monic part $\mathbf{t}^{\mathbf{m}}$ by $\mathrm{mlt}(f)$ (**monic leading term**) and the coefficient $a_{\mathbf{m}}$ by $\mathrm{lc}(f)$ (**leading coefficient**) of f. The partial ordering on $F[\mathbf{t}]$ is then obtained via

$$f > g \;\Leftrightarrow\; \mathrm{mlt}(f) > \mathrm{mlt}(g) \;\; .$$

With these prerequisites at hand we turn our interest to computations in a polynomial ideal $\mathbf{I}$. We assume that it is given by a finite number of generators, say $f_1, ..., f_k$. Then every element g of $\mathbf{I}$ can be written as

$$g \;=\; \sum_{i=1}^{k} r_i f_i \;\; (r_i \in F[\mathbf{t}]) \;\; .$$

We are interested in elements of small degree of $\mathbf{I}$ since they will play a decisive role for Gröbner bases. In case r_i is not constant the degree of $r_i f_i$ is larger then the degree of f_i. We can therefore expect g to be of small degree only if the sum of the leading monomials of several summands in the presentation of g is zero. If we just consider two polynomials instead of k this phenomenon can be enforced in the following way.

3.60. Definition

For two polynomials $f, g \in F[\mathbf{t}]$ we define their S**-polynomial** $S(f, g)$ as

$$S(f, g) \;:=\; \frac{\mathrm{lcm}(\mathrm{mlt}(f), \mathrm{mlt}(g))}{\mathrm{lt}(f)} f \;-\; \frac{\mathrm{lcm}(\mathrm{mlt}(f), \mathrm{mlt}(g))}{\mathrm{lt}(g)} g \;\; .$$

Hence, the leading term of the S-polynomial $S(f, g)$ is smaller than the least common multiple of the leading terms of f and g. This property will be of importance in a characterization of Gröbner bases in 1.62.

Examples
1. We calculate the S-polynomial of $f = t_1^3t_2^2 - t_1^2t_2^3 + t_1$ and $g = 3t_1^4t_2 + t_2^2$ in $\mathbb{Q}[\mathbf{t}]$ with respect to $>_{glex}$.

$$\begin{aligned} S(t_1^3t_2^2 - t_1^2t_2^3 + t_1, 3t_1^4t_2 + t_2^2) &= \frac{t_1^4t_2^2}{t_1^3t_2^2} f - \frac{t_1^4t_2^2}{3t_1^4t_2} g \\ &= t_1 f - \frac{1}{3} t_2 g \\ &= -t_1^3t_2^3 + t_1^2 - \frac{1}{3} t_2^3 \end{aligned}$$

This computation remains valid for $>_{lex}$.
2. For the polynomials $f = t_1^2 - t_2$ and $g = t_1^3 - t_3$ of $\mathbb{Q}[\mathbf{t}]$ we compute their S-polynomial for two different orderings.
(a) $t_1 > t_2 > t_3$ (lexicographic ordering)

$$S(f, g) = t_1 f - g = -t_1 t_2 + t_3 \ .$$

(b) $t_2 > t_3 > t_1$

$$S(f, g) = t_3 f - t_2 g = -t_2 t_1^3 + t_1^2 t_3 \ .$$

The following lemma will also be used in characterizing Gröbner bases in 1.62.

LEMMA 22. *Let $f, f_1, ..., f_s \in F[\mathbf{t}]$ and $f = \sum_{i=1}^s c_i f_i \ \ (c_i \in F)$ with $\delta = \mathrm{mlt}(f_1) = ... = \mathrm{mlt}(f_s) \neq \mathrm{mlt}(f)$. Then f is also an F-linear combination of the $S(f_i, f_{i+1}) \ \ (1 \leq i < s)$.*

Proof Since the monic leading terms of all f_i coincide the monic leading term of $\sum_{i=1}^s c_i f_i$ either equals δ or it is smaller. According to our assumption $\delta \neq \mathrm{mlt}(f)$ we must therefore have $\sum_{i=1}^s c_i \,\mathrm{lt}(f_i) = 0$. We let $\mathrm{lt}(f_i) = a_i\delta \ \ (a_i \in F^\times)$ and set $b_i := a_i c_i, \ p_i := f_i / \mathrm{lc}(f_i)$ for $(1 \leq i \leq s)$ and obtain

$$\sum_{i=1}^s b_i = 0 \ ,$$

$$S(f_i, f_j) = \frac{\delta}{a_i\delta} f_i - \frac{\delta}{a_j\delta} f_j = \frac{f_i}{a_i} - \frac{f_j}{a_j} = S(p_i, p_j)$$

and eventually

$$\begin{aligned} \sum_{i=1}^s c_i f_i &= \sum_{i=1}^s b_i (f_i / \mathrm{lc}(f_i)) \\ &= b_1(p_1 - p_2) + (b_1 + b_2)(p_2 - p_3) + ... + \\ &\quad (b_1 + ... + b_{s-1})(p_{s-1} - p_s) + (b_1 + ... + b_s)p_s \\ &= \sum_{i=1}^{s-1} (\sum_{j=1}^{i} b_j) S(f_i, f_{i+1}) \ . \end{aligned}$$

□
We note that we have $\mathrm{mlt}(S(f_i, f_j)) < \delta$ in the preceding lemma.

If the leading term of a non-zero polynomial g divides the leading term of a polynomial f ($\mathrm{lt}(g) \mid \mathrm{lt}(f)$), i.e. there exists a monomial h with $\mathrm{lt}(f) = h\,\mathrm{lt}(g)$) then we can subtract hg from f so that this divisibility property is no longer satisfied for the polynomials $f - hg$ and g. We note that $f - hg = S(f, g)$. This remains valid even without the divisibility condition if we set $h = 0$ in case $\mathrm{lt}(g)$ does not divide $\mathrm{lt}(f)$. Repeatedly replacing f by $S(f, g)$ in case $\mathrm{lt}(g)$ divides $\mathrm{lt}(f)$ until this divisibility condition does not hold anymore we say that the polynomial f is **reduced modulo** g. This concept can be easily generalized to the reduction of a polynomial modulo a non-empty finite set of non-zero polynomials.

3.61. Definition

Let $\mathbf{I}$ be a non-zero ideal of $F[t_1, ..., t_n]$ with ordered basis $G = \{g_1, ..., g_k\}$. We say that an element $f \in F[t_1, ..., t_n]$ **reduces to zero modulo** G if the sequence $f_0 = f$,

$$f_i = \text{reduction of } f_{i-1} \text{ modulo } g_i \quad (1 \leq i \leq k)$$

satisfies $f_k = 0$.
We remark that a polynomial which reduces to 0 modulo G necessarily belongs to the ideal $\mathbf{I}$. However, not every element of an ideal must have this property.

Example Let $f = t_1t_2^2 - t_1$ and $G = \{g_1,\ g_2\}$ with $g_1 = t_1t_2 + 1$, $g_2 = t_2^2 - 1$. Then we obtain $f_1 = f - t_2(t_1t_2 + 1) = -t_1 - t_2 = f_2$, and f does not reduce to 0 modulo $\{g_1, g_2\}$. If we change the order of the basis elements, however, we compute $f_1 = f - t_1(t_2^2 - 1) = 0$ and f does reduce to 0 modulo that newly ordered basis. The reason for this phenomenon is that the basis $\{g_1, g_2\}$ is not a Gröbner basis (see definition and theorem below). It does not contain the S-polynomial

$$S(g_1, g_2) = \frac{t_1t_2^2}{t_1t_2}(t_1t_2 + 1) - \frac{t_1t_2^2}{t_2^2}(t_2^2 - 1) = t_1 + t_2 \ .$$

If we add $g_3 := t_1 + t_2$ to the basis we get $G = \{g_1, g_2, g_3\}$ and, clearly, f reduces to 0 modulo G. We note that the same holds for the S-polynomials $S(g_1, g_3)$, $S(g_2, g_3)$.

3.62. Definition

Let $\mathbf{I}$ be a non-zero ideal of $F[t_1, ..., t_n]$ with basis G. If every $f \in \mathbf{I}$ reduces to zero modulo G then G is called a **Gröbner basis** of $\mathbf{I}$.
We remark that Gröbner bases are by no means unique since every superset of a Gröbner basis also satisfies the condition of the definition.

Theorem Let $\mathbf{I}$ be a non-zero ideal of $F[t_1, ..., t_n]$ with basis $G = \{g_1, ..., g_s\}$. Then G is a Gröbner basis for $\mathbf{I}$ if and only if every S-polynomial $S(g_i, g_j)$ $(1 \leq i < j \leq s)$ reduces to 0 modulo G.

Proof If G is a Gröbner basis of $\mathbf{I}$ then every polynomial of $\mathbf{I}$, hence a priori every $S(g_i, g_j)$, reduces to 0 modulo G.
Now let us assume that every S-polynomial $S(g_i, g_j)$ reduces to 0 modulo G but that there exists $f \in \mathbf{I}$ which does not. Obviously, f is not zero. If $0 \neq f$ cannot be reduced modulo G anymore then in the basis representation

$$f = \sum_{i=1}^{s} h_i g_i \quad (h_i \in F[t_1, ..., t_n]) \tag{5}$$

the leading monomial of f is not divisible by any of the leading monomials of the g_i. We assume that (1) is a presentation of f in which the monic part of the largest occuring monomial on the right-hand side is as small as possible, say δ. We observe that $\mathrm{mlt}(f) \neq \delta$. Then we rewrite (1) by separating those summands with monic leading monomial δ from the other terms. We put $J_1 := \{i \mid 1 \leq i \leq s, \mathrm{mlt}(h_i g_i) = \delta\}$ and $J_2 := \{1, ..., s\} \setminus J_1$ and obtain

$$f = \sum_{i \in J_1} h_i g_i + \sum_{i \in J_2} h_i g_i \tag{6}$$

$$= \sum_{i \in J_1} lt(h_i) g_i + \sum_{i \in J_1} (h_i - \mathrm{lt}(h_i)) g_i + \sum_{i \in J_2} h_i g_i \tag{7}$$

so that the leading monomials of the summands in the two last sums are smaller than δ. Because of $\mathrm{mlt}(f) \neq \delta$ the first sum satisfies the prerequisites of the preceding lemma for the polynomial

$$f - \left(\sum_{i \in J_1} (h_i - \mathrm{lt}(h_i)) g_i + \sum_{i \in J_2} h_i g_i \right)$$

if we put $f_i = \mathrm{mlt}(h_i) g_i$ and $c_i = \mathrm{lc}(h_i)$. For $i, j \in J_1$ we set $g_{ij} := \mathrm{lcm}(\mathrm{mlt}(g_i), \mathrm{mlt}(g_j))$ and observe that $g_{ij} > \mathrm{mlt}(S(g_i, g_j))$. Hence, the first sum of (3) becomes an F-linear combination of S-polynomials of the form

$$\begin{aligned} S(\mathrm{mlt}(h_i) g_i, \mathrm{mlt}(h_j) g_j) &= \frac{\delta \, \mathrm{mlt}(h_i) g_i}{\mathrm{mlt}(h_i) \, \mathrm{lt}(g_i)} - \frac{\delta \, \mathrm{mlt}(h_j) g_j}{\mathrm{mlt}(h_j) \, \mathrm{lt}(g_j)} \\ &= \frac{\delta}{\mathrm{lt}(g_i)} g_i - \frac{\delta}{\mathrm{lt}(g_j)} g_j \\ &= \frac{\delta}{g_{ij}} S(g_i, g_j) \quad . \end{aligned}$$

Since the S-polynomials $S(g_i, g_j)$ reduce to zero modulo G they have a basis presentation

$$S(g_i, g_j) \;=\; \sum_{\nu=1}^{s} h_\nu g_\nu$$

with $\mathrm{mlt}(h_\nu g_\nu) \;\leq\; \mathrm{mlt}(S(g_i, g_j))$. Because of $\mathrm{mlt}(\frac{\delta}{g_{ij}} S(g_i, g_j)) < \delta$ inserting those presentations into (3) yields a presentation of f by G in which all occuring monomials are smaller than δ contradicting our assumption.
□
The following algorithm (Buchberger's algorithm) constructs a Gröbner basis from an arbitrary ideal basis.

Buchberger Algorithm

Input A basis $G = \{g_1, ..., g_s\}$ of an ideal $\mathbf{I}$.
Output A Gröbner basis $G = \{g_1, ..., g_t\}$ of $\mathbf{I}$.
Initialization Set $t := s$, $B := \{(i, j) \mid 1 \leq i < j \leq t\}$.
Step If $B \neq \emptyset$ choose (i, j) from B and remove (i, j) from B; reduce $S(g_i, g_j)$ modulo G to f; if $f \neq 0$ add $g_{t+1} := f$ to G and $\{(i, t+1) \mid 1 \leq i \leq t\}$ to B and increase t by 1.

We still need to show that Buchberger's algorithm terminates. For this we consider the sequence of ideals $\mathbf{I}_s := \langle \mathrm{mlt}(g_i) \mid 1 \leq i \leq s \rangle$. We show that every enlargement of G (increase of s) yields a strictly larger ideal $\mathbf{I}_s$. Since any ascending chain of ideals becomes stationary s is bounded.
Let us therefore assume that f is an S-polynomial of two elements of G which is already reduced modulo G but is still non-zero. Hence, f will be inserted into G thus increasing $\sharp G$. We will show that $\mathrm{mlt}(f)$ is not contained in $\mathbf{I}_s$. Namely, if $\mathrm{mlt}(f)$ belongs to $\mathbf{I}_s$ there exists a presentation

$$\mathrm{mlt}(f) \;=\; \sum_{i=1}^{s} h_i \,\mathrm{mlt}(g_i)$$

with polynomials $h_i \in F[\mathbf{t}]$. Comparing monomials on both sides we get a non-empty subset J_1 of $\{1, 2, ..., s\}$ and monomials $a_i \mathbf{t}^{m_i}$ which are summands of h_i such that

$$\mathrm{mlt}(f) \;=\; \sum_{i \in J_1} a_i \mathbf{t}^{\mathbf{m_i}} \,\mathrm{mlt}(g_i) \quad .$$

But then $\mathrm{mlt}(f)$ is a multiple of $\mathrm{mlt}(g_i)$ for $i \in J_1$ and f can be further reduced modulo g_i contradicting our assumption.

We remark that the previous considerations also show that every monomial which is contained in an ideal with a basis of monomials is a linear combination of monomials each summand being divisible by one of the basis elements.

3.63. Multivariate Polynomials – Resultants

Besides Gröbner bases there is another important tool for eliminating variables in a system of polynomial equations: resultants. We introduce them in a generic way, i.e. we assume that their coefficients are algebraically independent over $\mathbb{Z}$. Let $R = \mathbb{Z}[a_0, ..., a_n, b_0, ..., b_m]$ be a polynomial ring in $n + m + 2$ variables. Then the polynomials

$$\begin{aligned} A(t) &= a_0 t^n + a_1 t^{n-1} + ... + a_{n-1} t + a_n \text{ and} \\ B(t) &= b_0 t^m + b_1 t^{m-1} + ... + b_{m-1} t + b_m \end{aligned} \tag{8}$$

of $R[t]$ are said to be **generic** inasmuch as any two polynomials f, g over a unital commutative ring Λ with $\deg(f) \leq n$, $\deg(g) \leq m$ can be obtained as homomorphic images of A, B by mapping

$$1_{\mathbb{Z}} \mapsto 1_\Lambda,\ t \mapsto t,\ a_i \mapsto \alpha_i \in \Lambda,\ b_j \mapsto \beta_j \in \Lambda \ \ (0 \leq i \leq n,\ 0 \leq j \leq m)$$

for suitable elements α_i, β_j of Λ. If S denotes a common splitting ring of A, B over R we obtain

$$A(t) = a_0 \prod_{i=1}^{n} (t - x_i),\ B(t) = b_0 \prod_{j=1}^{m} (t - y_j) \tag{9}$$

in $S[t]$. From this we conclude

$$\frac{a_i}{a_0} \ = \ (-1)^i \sum_{1 \leq j_1 < ... < j_i \leq n} x_{j_1} ... x_{j_i} \ =: \ (-1)^i \sigma_i \ \ (1 \leq i \leq n) \tag{10}$$

with the σ_i being symmetric functions in the zeros of A (so-called elementary symmetric functions). Analogously, we get

$$\frac{b_i}{b_0} \ = \ (-1)^i \sum_{1 \leq j_1 < ... < j_i \leq m} y_{j_1} ... y_{j_i} \ \ (1 \leq i \leq m) \ . \tag{11}$$

It follows that $\mathbb{Z}[a_0, ..., a_n, b_0, ..., b_m] \subseteq \mathbb{Z}[a_0, x_1, ..., x_n, b_0, y_1, ..., y_m]$ and therefore also $a_0, x_1, ..., x_n, b_0, y_1, ..., y_m$ are algebraically independent. ¿From the theorem of Gauß we know that $R[t]$ is a unique factorization domain. Hence, the greatest common divisor of A, B is well defined. Any common zero of A, B is also a zero of $\gcd(A, B)$ and vice versa. Whereas the zeros of A, B usually do not belong to R, the greatest common divisor $\gcd(A, B)$ is calculated in $R[t]$. Hence, the existence of common zeros can be decided without the need of constructing ring extensions of R.

LEMMA 23. *The greatest common divisor of $A, B \in R[t]$ given in (4) is different from 1, if and only if there exist non-zero polynomials $U, V \in R[t]$ satisfying $\deg(U) < m$, $\deg(V) < n$ and $UA = VB$.*

Proof If $C := \gcd(A, B)$ is different from 1 we write $A = C\tilde{A}$, $B = C\tilde{B}$ with $\deg(\tilde{A}) < n$, $\deg(\tilde{B}) < m$ and obtain

$$C\tilde{A}\tilde{B} \ = \ \tilde{B}A \ = \ \tilde{A}B$$

so that we can choose $U = \tilde{B}$, $V = \tilde{A}$.
If U, V with the properties of the lemma exist we consider the factorizations of UA and of VB into prime polynomials. Clearly, not every prime polynomial dividing A can divide V because of $\deg(V) < \deg(A)$. Therefore at least one such prime polynomial must divide B and consequently $\gcd(A, B)$.
□
Setting

$$U(t) = \sum_{i=0}^{m-1} u_i t^{m-1-i}\,,\ V(t) = \sum_{j=0}^{n-1} v_j t^{n-1-j}\ \in R[t] \tag{12}$$

the equation $UA = VB$ yields a linear system of equations for the coefficients u_i, v_j. For the coefficent of t^μ $(0 \le \mu \le m+n-1)$ we obtain

$$\sum_{\max\{0,\mu-n\}\le\nu\le\min\{\mu,m-1\}} u_\nu a_{\mu-\nu} \ = \sum_{\max\{0,\mu-m\}\le\nu\le\min\{\mu,n-1\}} v_\nu b_{\mu-\nu}\ .$$

These are $(m+n)$ equations. Moving everything to the left-hand side we get a homogenous linear system of equations
(13)

$$(u_0,...,u_{m-1},-v_0,...,-v_{n-1}) \begin{pmatrix} a_0 & ... & a_n & & & & & \\ & a_0 & ... & a_n & & & & \\ & & & ... & & & & \\ & & & ... & & & & \\ & & & & a_0 & a_1 & ... & a_n \\ b_0 & b_1 & . & . & . & b_m & & \\ & b_0 & b_1 & . & . & . & b_m & \\ & & & & & & ... & \\ & & & & b_0 & b_1 & ... & b_m \end{pmatrix} = \mathbf{0}$$

We denote the formidable coefficient matrix by Δ. We recall that A, B have a common zero if and only if that homogenous system has a non-trivial solution. Of course, the latter holds exactly for $\det(\Delta) = 0$.

3.64. Definition

The determinant of the coefficient matrix Δ of (9) is called **resultant** of A and B. It is denoted by $\mathrm{res}(A, B)$.
Next we show that $\mathrm{res}(A, B)$ is in the ideal of $R[t]$ generated by A and B. This is of importance when we use resultants for eliminating variables from multivariate polynomials. Looking at the structure of

Δ we immediately find the following identity:

$$\mathbf{v} := \begin{pmatrix} t^{m-1}A \\ t^{m-2}A \\ .. \\ .. \\ t^0 A \\ t^{n-1}B \\ .. \\ .. \\ t^0 B \end{pmatrix} = \Delta \begin{pmatrix} t^{n+m-1} \\ t^{n+m-2} \\ .. \\ .. \\ t^n \\ t^{n-1} \\ .. \\ .. \\ t^0 \end{pmatrix} \quad . \tag{14}$$

Denoting the columns of Δ by $\mathbf{d}_1, ..., \mathbf{d}_{n+m}$ this is tantamount to

$$\mathbf{v} \; = \; \sum_{\kappa=1}^{n+m} t^{n+m-\kappa} \mathbf{d}_\kappa \quad .$$

Then Cramer's rule tells us that

$$\mathrm{res}(A,B) = \det(\Delta) t^0 = \det(\mathbf{d}_1, ..., \mathbf{d}_{m+n-1}, \mathbf{v}) \quad .$$

Calculating the last determinant we note that the variable t only occurs in the last column $\mathbf{v}$ so that we indeed obtain polynomials ϕ, $\psi \in R[t]$ with $\deg(\phi) < m$, $\deg(\psi) < n$ and

$$\phi A \, + \, \psi B \; = \; \mathrm{res}(A,B) \quad . \tag{15}$$

We note that in the first m rows of Δ we have entries zero or coefficients of A and in the last n rows the entries are zero or coefficients of B. According to Laplace's theorem we have

$$\mathrm{res}(A,B) \; = \; \sum_{\pi \in S_{m+n}} \mathrm{sign}(\pi) \Delta(1, \pi(1)) ... \Delta(m+n, \pi(m+n)) \tag{16}$$

if $\Delta(i,j)$ denotes the entry of Δ in row i and column j. Therefore any non-zero summand of the sum in (12) must consist of m factors a_μ (from the first m rows) and n factors b_ν (from the last n rows). We conclude that $\mathrm{res}(A,B)$ is a homogenous polynomial of degree m in the a_μ and of degree n in the b_ν. We can write it in the form

$$\mathrm{res}(A,B) \; = \; a_0^m b_0^n F(\frac{a_1}{a_0}, ..., \frac{a_n}{a_0}, \frac{b_1}{b_0}, ..., \frac{b_m}{b_0}) \quad .$$

According to our remark on the elementary symmetric functions of the zeros of A, respectively B, we know that F can also be written as a polynomial in the variables $x_1, ..., x_n, y_1, ..., y_m$ which we again denote by F. Since the resultant vanishes if zeros of A and B coincide and since $\mathbb{Z}[a_0, x_1, ..., x_n, b_0, y_1, ..., y_m]$ is a factorial ring the polynomial F must be divisible by the polynomials $x_i - y_j \;\; (1 \leq i \leq n, \, 1 \leq j \leq m)$ and therefore by the polynomial

$$\tilde{F} := \prod_{i=1}^{n} \prod_{j=1}^{m} (x_i - y_j) \quad .$$

LEMMA 24. *The resultant res(A, B) of the generic polynomials A, B of (4) coincides with each of the three polynomials*

(i) $a_0^m b_0^n \tilde{F}$,
(ii) $a_0^m \prod_{i=1}^n B(x_i)$,
(iii) $(-1)^{mn} b_0^n \prod_{j=1}^m A(y_j)$.

Proof The equality of the polynomials in the lemma is immediate from (5) :

$$a_0^m b_0^n \tilde{F} \;=\; a_0^m \prod_{i=1}^{n} \left(b_0 \prod_{j=1}^{m} (x_i - y_j) \right) \;=\; (-1)^{mn} b_0^n \prod_{j=1}^{m} \left(a_0 \prod_{i=1}^{n} (y_j - x_i) \right) \quad .$$

We also know that $a_0^m b_0^n \tilde{F}$ divides res(A, B). From 17(2.) we conclude that $a_0^m b_0^n \tilde{F}$ is homogenous of degree n in the b_ν and from (3.) that it is homogenous of degree m in the a_μ. Since res(A, B) has the same properties the quotient of res(A, B) and $a_0^m b_0^n \tilde{F}$ must be constant. The constant will be determined by comparing the coefficients of $a_0^m b_m^n$. In $\det(\Delta)$ we obtain that monomial as the product of all diagonal elements of Δ, it has coefficient 1. But looking at its coefficient in $a_0^m b_0^n \tilde{F}$ we find from 17(2.) that it is 1, too.
□
We list a few direct consequences of the last lemma which will be of help in the actual computation of resultants:

$$\begin{aligned} \mathrm{res}(A, B) &= (-1)^{mn} \mathrm{res}(B, A) \;, \\ \mathrm{res}(rA, B) &= r^m \mathrm{res}(A, B) \;, \\ \mathrm{res}(A, rB) &= r^n \mathrm{res}(A, B) \;\; (r \in R) \;. \end{aligned} \tag{17}$$

If one or even both polynomials involved are constant we get

$$\begin{aligned} \mathrm{res}(a_0, B) &= a_0^m \;, \\ \mathrm{res}(A, b_0) &= b_0^n \;, \\ \mathrm{res}(a_0, b_0) &= 1 \;. \end{aligned} \tag{18}$$

Hence, we will try to evaluate res(A, B) by pseudo-division. In case $\deg(B) > \deg(A)$ we compute $\mathrm{res}(A, B) = (-1)^{mn} \mathrm{res}(B, A)$. Hence, we may assume that $\deg(A) \geq \deg(B)$. Applying pseudo-division we get polynomials $Q = Q(A, B)$, $R = R(A, B) \in R[t]$, $\deg(R) < \deg(B)$ satisfying

$$b_0^{n-m+1} A \;=\; Q\, B \;+\; R \quad . \tag{19}$$

Then the last lemma yields

$$\begin{aligned}
\operatorname{res}(A,B) &= (-1)^{mn} b_0^n \prod_{j=1}^{m} A(y_j) \\
&= (-1)^{mn} b_0^{n-m(n-m+1)} \prod_{j=1}^{m} (Q\,B+R)(y_j) \\
&= (-1)^{mn} b_0^{n-\deg(R)-m(n-m+1)} \left(b_0^{\deg(R)} \prod_{j=1}^{m} R(y_j) \right) \\
&= (-1)^{m(n-\deg(R))} b_0^{n-\deg(R)-m(n-m+1)} \operatorname{res}(R,B) \\
&= (-1)^{mn} b_0^{n-\deg(R)-m(n-m+1)} \operatorname{res}(B,R) \quad . \qquad (20)
\end{aligned}$$

We note that the exponent of b_0 is likely to become negative so that these calculations can only be carried out in the quotient field of R. However, since the resultant itself is an element of R we are guaranteed that the final result will not contain denominators.
In the actual calculation of the resultant of two polynomials we successively replace the polynomial of larger degree via pseudodivision by a polynomial whose degree is less than the original lower degree. In this way we eventually obtain a constant remainder polynomial. If that constant is zero, the original resultant is zero, too. Otherwise the last resultant is evaluated by (14). This leads to the following algorithm.

Algorithm for computing resultants

Input $A, B \in R[t]$ with $\deg(A) \geq \deg(B) > 0$.
Output $\operatorname{res}(A,B) \in R$ and polynomials $\phi, \psi \in R[t]$ satisfying $\phi A + \psi B = \operatorname{res}(A,B)$.
Step 1 (Initialization) Set $\operatorname{res}(A,B) \leftarrow 1$, $F \leftarrow A$, $G \leftarrow B$, $N \leftarrow \deg(A)$, $M \leftarrow \deg(B)$, $\phi_0 \leftarrow 1$, $\psi_1 \leftarrow 1$, $\phi_1 \leftarrow 0$, $\psi_0 \leftarrow 0$.
Step 2 (Pseudo-division) Set $b_0 \leftarrow lc(G)$ and calculate with (15) polynomials $Q = \sum_{i=0}^{N-M} q_i t^{N-M-i}$, $R \in R[t]$. We set $s \leftarrow N - \deg(R)$ and $\operatorname{res}(A,B) \leftarrow \operatorname{res}(A,B)(b_0^{N-M+1})^{-M} b_0^s (-1)^{MN}$ and also $\phi_2 \leftarrow b_0^{N-M+1}\phi_0 - Q\phi_1$, $\psi_2 \leftarrow b_0^{N-M+1}\psi_0 - Q\psi_1$. If R is constant go to 4., else to 3..
Step 3. (Interchange of F, G) Set $F \leftarrow G$, $G \leftarrow R$, $N \leftarrow M$, $M \leftarrow \deg(R)$ as well as $\phi_0 \leftarrow \phi_1$, $\phi_1 \leftarrow \phi_2$, $\psi_0 \leftarrow \psi_1$, $\psi_1 \leftarrow \psi_2$ and go to 2..
Step 4. (Termination) For $R = 0$ set $\operatorname{res}(A,B) = 0$ and $\phi \leftarrow \phi_2$, $\psi \leftarrow \psi_2$; for $R \neq 0$ set $T \leftarrow \operatorname{res}(A,B) R^{M-1}$ and $\operatorname{res}(A,B) \leftarrow TR$, $\phi \leftarrow \phi_2 T$, $\psi \leftarrow \psi_2 T$. Then terminate.

Remarks

(i) The polynomials ϕ, ψ of 11 satisfy $\deg(\phi) \leq \deg(B)-1$, $\deg(\psi) \leq \deg(A) - 1$. The example $A = t^2 + 1$, $B = t^2 + 4$ shows that equality need not hold:

$$9 = \operatorname{res}(A,B) = -3(t^2+1) + 3(t^2+4) \quad .$$

(ii) Instead of operating in the quotient field of R we can keep track of the multipliers b_0 and their exponents in each step separately and calculate their product only at the end knowing that $\mathrm{res}(A, B)$ belongs to R.

Example We want to compute $\mathrm{res}(t^3 + 1, 2t^2 - 2)$ in $\mathbb{Z}[t]$. In the steps of the algorithm the following data are produced:
1. $F = t^3 + 1$, $N = 3$, $G = 2t^2 - 2$, $M = 2$.
2. $2^2(t^3 + 1) = 2t(2t^2 - 2) + 4t + 4$, hence $Q = 2t$, $R = 4t + 4$ yielding $s = 2$, $\mathrm{res}(A, B) = (2^2)^{-2}2^2 = 2^{-2}$.
3. $F = 2t^2 - 2$, $N = 2$, $G = 4t + 4$, $M = 1$.
2. $4^2(2t^2 - 2) = (8t - 8)(4t + 4) + 0$, hence $Q = 8t - 8$, $R = 0$ yielding $s = 2$, $\mathrm{res}(A, B) = 2^{-2}(4^2)^{-1}4^2 = 2^{-2}$.
4. $\mathrm{res}(A, B) = 0$, $\phi = 32(-t + 1)$, $\psi = 16(t^2 - t + 1)$.

Bibliography

[1] Bewersdorff, Jörg, *Algebra für Einsteiger*,Vieweg, 2002.
[2] Birkhoff, Bartee, *Modern Applied Algebra*.
[3] S. Bosch, *Algebra*, Springer, 1993.
[4] N. Bourbaki, *Algebre*, Hermann, Paris 1962.
[5] J. H. Davenport, Y. Siret, E. Tournier, *Computer algebra*, Acad. Press, 1989.
[6] G. Fischer, *Lehrbuch der Algebra*, Vieweg 2008.
[7] I. N. Herstein, *Topics in Algebra*, Xerox Coll. Pub., 1964.
[8] Th. W. Hungerford, *Algebra*, 1974.
[9] N. Jacobson, *Lectures in Abstract Algebra*, Springer GTM, 1974.
[10] R. Kochendörffer, *Einführung in die Algebra*, Dt.Verl.d. Wissenschaften, 1974.
[11] S. Lang, *Algebra*, Addison-Wesley, 1971.
[12] A. Leutbecher, *Zahlentheorie*, Springer, 1996.
[13] F. Lorenz, *Algebra I, II*, BI Wissenschaftsverlag, 1987/90.
[14] K. Meyberg, *Algebra I, II*, Carl Hanser Verlag, 1975.
[15] Mignotte, *Mathematics for Computer Algebra*, Springer, 1992.
[16] E. Scholz, *Geschichte der Algebra*, BI Wissenschaftsverlag, 1990.
[17] G. Stroth, *Algebra*, de Gruyter, 1998.
[18] B. L. van der Waerden, *Algebra I, II*, Springer, 1966/87.
[19] Weber, *Lehrbuch der Algebra*, Vieweg, 1895.