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:

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

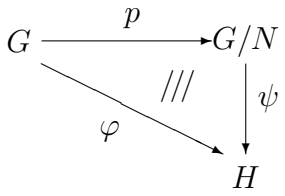
(Von links nach rechts bzw. oben nach unten erhält man die Wohldefiniertheit, in umgekehrter Richtung die Injektivität.)
ψ ist Homomorphismus:

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

□

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(1.18) 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 (1.18) 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 Stab(s) is actually a subgroup of G for each $s \in S$. Clearly, the unit element e of G belongs to Stab(s). If g, h are in Stab(s), then also h^{-1} and gh^{-1} are in Stab(s).
In order to establish a connection between the length of an orbit $O(s)$ and the number of elements of G , 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:

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

Here, the second but last equation is a consequence of $g^{-1}hg = k \;\Leftrightarrow\; gkg^{-1} = h$. 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 (3) 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. $1 \leq a \leq m$, 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 (4) 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 all $x \in T$ 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 $p^{m-a}q$, the stabilizer of 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 $\binom{n}{p^a}/p^{m-a}$ 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 $0 \le l_i < a$ 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:

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

and for the denominator:

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

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 $1 \le a \le m$ $(a \in \mathbb{N})$.*

- *(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 (2) 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.*

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

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

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

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

and in 3 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

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

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 $x = 0$.
□

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.