Einführung in die Algebra

Vorlesung im
Sommersemester 2006
Technische Universität Berlin

gehalten von
Prof. Dr. M. Pohst

CHAPTER 2

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:

(1) $R = \mathbb{Z},\ f(t) = t + 2$ hat Nullstelle $t = -2$.
(2) $R = \mathbb{Z},\ f(t) = 3t + 2$ hat in R keine Nullstelle, wohl aber in $\mathbb{Q}$.
(3) $f(t) = t^2 + 1$ hat erst in $\mathbb{C}$ eine Nullstelle (jedoch auch in $\mathbb{Z}[i]$).
(4) $f(t) = t^4 - 4t^2 + 1$ 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.

CHAPTER 3

Gruppen

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: $m_1 m_2$, $m_1 \circ m_2$, $m_1 \cdot m_2$ 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.

1. Definition

Eine nicht leere Menge M mit einer (binären) assoziativen inneren Verknüpfung heißt Halbgruppe.

Beispiele:

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

(2) 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:

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

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

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

(3) 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.

2. 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 Homo-, 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

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

3. 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.

4. Satz

Es sei G eine Halbgruppe mit den Eigenschaften

(1) $\exists e \in G\ \forall a \in G\,:\, e \circ a = a$;
(2) $\forall a \in G\ \exists b \in G\,:\, b \circ a = e$.

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.

□

4.1. 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

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

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:

$$\begin{aligned} a \circ c = b \circ c &\Rightarrow a = b, \\ d \circ a = d \circ b &\Rightarrow a = b. \end{aligned}$$

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:

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

5. 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).

□

6. Definition

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

7. 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.

8. 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:

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

(2)

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

(3)

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

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 betrachte die Abbildung (!)

$$Ua \mapsto a^{-1}U.$$

Diese ist offensichtlich surjektiv. Zur Injektivität:

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

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:

9. Satz (Lagrange)

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

10. 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

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

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:

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

11. Definition

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

12. 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 $0 \le R(m, f) < f$.

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:

(1) 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 $U =< a^k >$.
(2) $(\mathbb{Z}, +) \cong (2\mathbb{Z}, +)$.

Für beliebige Gruppen G definiert man für $a \in G$ die Ordnung $\mathrm{ord}(a)$ mittels $\mathrm{ord}(a) = (< a >: 1)$. Nach dem Satz von Lagrange ist $\mathrm{ord}(a)$ ein Teiler der Gruppenordnung. $k \in \mathbb{N}$ heißt Exponent zu $a \in G$, falls $a^k = e$ ist. Offenbar gilt, daß $\mathrm{ord}(a)$ jeden Exponenten von a teilt. Dagegen braucht ein Exponent nicht notwendig Teiler der Gruppenordnung zu sein. $(G : 1)$ ist für endliche Gruppen G stets Exponent:

$$a^{(G:1)} = e \quad \forall\, a \in G.$$

Gemäß Definition ist $\mathrm{ord}(a)$ entweder ∞ oder gleich der kleinsten natürlichen Zahl k mit $a^k = e$. Im letzten Fall ist

$$< a >= \{a^m \mid 0 \leq m < k\}.$$

Ist $(G : 1)$ Primzahl, so ist G zyklisch, also isomorph zu $\mathbb{Z}/p\mathbb{Z}$!

13. Lemma

Es sei $a \in G$ mit $\mathrm{ord}(a) = k$ und $m \in \mathbb{Z}$. Dann gilt

$$\mathrm{ord}(a^m) = \frac{k}{\mathrm{ggT}\,(m,\, k)}.$$

Beweis:
Es sei $d = \mathrm{ggT}\,(m,\, k)$. Es folgt

$$(a^m)^{k/d} = (a^k)^{m/d} = e^{m/d} = e,$$

also ist k/d Exponent von a^m. Ist umgekehrt

$$e = (a^m)^j,$$

so folgt $mj \equiv 0 \bmod k$ und $j \equiv 0 \bmod k/d$.

□

Bemerkung: In abelschen Gruppen G gilt:

$$\mathrm{ord}(ab) \mid \mathrm{kgV}\,(\mathrm{ord}(a),\, \mathrm{ord}(b)).$$

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

(1) Es ist $G =< a^m >$ dann und nur dann, wenn $\mathrm{ggT}\,(k,\, m) = 1$ ist.
(2) 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.

14. Satz

Es sei $G =< a >$ mit $(G : 1) = k$. Dann gibt es zu jedem $d \in \mathbb{N}$ mit $d|k$ genau eine Untergruppe U_d von G der Ordnung d.

Beweis:
Für $d|k$ setze $U_d =< a^{k/d} >$. Gemäß (1.13) ist dies eine Untergruppe von G der Ordnung d. Sei $\tilde{U} =< a^m >\ \ (m < k)$ eine weitere Untergruppe von G der Ordnung d. D.h. es ist

$$d = \mathrm{ord}(a^m) = \frac{k}{\mathrm{ggT}\,(k,\, m)},$$

also

$$\mathrm{ggT}\,(k,\, m) = \frac{k}{d}, \quad m = \frac{k}{d}\,\tilde{m}$$

mit $\tilde{m} < d$, d.h. $a^m \in U_d$. Also folgt $U \subseteq U_d$ und wegen $(\tilde{U} : 1) = (U_d : 1)$ damit $\tilde{U} = U_d$.

□

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.

15. Definition

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

Bemerkungen:

(1) Es genügt in (1.15), $xUx^{-1} \subseteq U$ zu fordern.
(2) $xUx^{-1} = U \quad \Leftrightarrow \quad xU = Ux$.
(3) 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 $a \ker \varphi a^{-1} \subseteq \ker \varphi$.
(4) 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 $x \in G$.
(5) $< e >$, G sind stets Normalteiler von G. G heißt einfach, falls es die einzigen sind.
(6) 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.
(7) 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

$\mathfrak{S}_3$:

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

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: $\forall \varphi \in \mathrm{Aut}\,(G)\ :\ \varphi\, I\,(G)\, \varphi^{-1} \subseteq I\,(G)$ bzw.
$\forall \varphi_x \in I\,(G)\ :\ \varphi\, \varphi_x\, \varphi^{-1} \in I\,(G)$.

Sei $y \in G$ beliebig:

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

16. Hilfssatz

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

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

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

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

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

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

Beweis:

(1) $\{N_i\}_{i\in I}$ 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 $xNx^{-1} \subseteq N$.

(2) 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.

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

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

Sei $x \in G$:

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

also ist

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

(4) $\varphi(U)$ 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

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

□

Beispiel: Es gilt $I(G) \lhd \mathrm{Aut}(G)$.

Beweis:
Es seien $\varphi \in \mathrm{Aut}(G)$, $\varphi_y \in I(G)$ und $x \in G$. Dann gilt:

$$\begin{aligned} \varphi\,\varphi_y\,\varphi^{-1}(x) &= \varphi(y\,\varphi^{-1}(x)\,y^{-1}) \\ &= \varphi(y)\,x\,\varphi(y^{-1}) \\ &= \varphi(y)\,x\,\varphi(y)^{-1} \\ &= \varphi_{\varphi(y)}(x). \end{aligned}$$

□

17. 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:

(1) 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,

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

(2) $\emptyset \neq U \subseteq G$ 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.)

(3) 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).)

(4) 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.

18. 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

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

Wohldefiniertheit und Surjektivität von ψ sind unmittelbar klar.
ψ Homomorphismus:

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

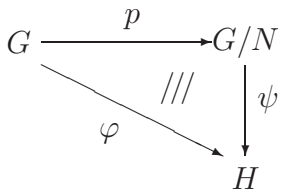
ψ injektiv:

$$\begin{aligned}e_H = \psi(g\ker(\varphi)) = \varphi(g) &\Rightarrow g \in \ker(\varphi) \\ &\Rightarrow g\ker(\varphi) = \ker(\varphi).\end{aligned}$$

□

19. 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.

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

□

20. 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!

□

21. 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.

22. Definition

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

$$G := G_1 \times \ldots \times G_n = \bigtimes_{i=1}^{n} G_i$$

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.

22.1. Bemerkungen und Eigenschaften von direkten Produkten von Gruppen.

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

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

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

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

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

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

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

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

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

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

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

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

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

(9) 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 mit Kern $\varepsilon_i(G_i)$. Also ist

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

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

(10) Verallgemeinerung auf unendliche Produkte ist möglich, falls man fordert, daß fast alle Komponenten das Einselement der betreffenden Gruppe bilden.

Das Gegenstück zum äußeren Produkt ist:

23. Definition

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

(1) $G = N_1 \cdot \ldots \cdot N_n$ und

(2) $N_i \cap \tilde{N}_i = \{e\}$ $(1 \leq i \leq n)$ 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

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

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:

24. Satz

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

(1) $g_i g_j = g_j g_i \ \forall g_i \in N_i,\ g_j \in N_j \ (1 \leq i < j \leq n)$, 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.

(2) $N_i \lhd G \ (1 \leq i \leq n)$, 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.

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

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

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

auch

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

Der entsprechende Isomorphismus wird gegeben durch

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

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

25. Anwendungen (Hauptsatz über endliche abelsche Gruppen)

(1) Das direkte Produkt zyklischer Gruppen mit teilerfremden Ordnungen ist zyklisch.
(2) Ist G zyklisch mit $(G:1) = m\,n$ und $\mathrm{ggT}\,(m,\,n) = 1$, so gilt

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

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

Beweis:

(1) 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 $mn|k$.

(2) 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.

(3) 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

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

Für $\mathfrak{M} = \{\underline{0}\}$ ist G das direkte Produkt von den $< a_i >$ $(1 \leq i \leq r)$, 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.

□

26. 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

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

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

Beispiele:

(1) (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

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

(2) (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

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

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

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

27. 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

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

□

28. 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:

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

$\sim$ 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

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

29. 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:
$G = (\mathbb{R}, +),\ X = \mathbb{R}^n,\ g \cdot \underline{x} = X$ für $\underline{x} \in X,\ g \in G$.
Stabilisator von $x \in X\ :\ G_x = \{g \in G \mid gx = x\}$.

Bemerkungen:

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

(2) 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:

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

□

(3) 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:

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

(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:

30. 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 $g \cdot Y = \{g \cdot y \mid y \in Y\}$.

31. Definition

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

32. Satz

(1) Das Zentrum einer p-Gruppe ist nicht trivial.
(2) 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:

(1) 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 $e \in Z(G) \ \Rightarrow \ |Z(G)| > 1.$)

(2) 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

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

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.

33. 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: $p^l \parallel |G|$)

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

(1) $p = 2,\ l = 3,\ m = 1$: G selbst ist p-Sylow-Untergruppe.
(2) $p = 2,\ l = 2,\ m = 1$: 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:

34. 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

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

□

35. 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!

(1) $p^{l-\alpha+1} \nmid |O(T)| \ \Rightarrow \ (G_T : 1) = p^\alpha$
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.

(2) $p^{l-\alpha+1} \nmid |O(T)| \ \Leftrightarrow \ T = U_g$ 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 $T = U_G \in \mathfrak{M}$.

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

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

36. 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.

□

37. 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.

38. 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.

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

□

39. 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:

(1) Jede p-Untergruppe von G ist in einer passenden p-Sylow-Untergruppe enthalten.
(2) Je zwei p-Sylow-Untergruppen von G sind konjugiert.
(3) 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:

(1) 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 $H\tilde{P} = \tilde{P} \ \Rightarrow \ H \subseteq \tilde{P}$.

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

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

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

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: $< b^2 >$, $< a >$, $< b^2 a >$ 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: $< b >$, $< a >$, $< ab >$.

40. 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.

□

41. Satz

G sei eine endliche abelsche Gruppe.

(1) G ist direktes Produkt seiner p-Sylow-Untergruppen.
(2) 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:

(1) 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))

(2) 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 $c = um + vn$.

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

$\tilde{u} =< \frac{n}{c}x + \frac{n}{c}vy >$ 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.

42. Definition

$\pi \in \mathfrak{S}_n$ heißt r-Zykel, 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:

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

Vereinbarung: id $= (1)$ ist einziger 1-Zykel.

Bemerkungen:
Transpositionen sind 2-Zykel (i, j);

$$(i_1, \ldots, i_r) = (i_1, \pi(i_1), \ldots, \pi^{r-1}(i_1)), \quad \pi^r(i_\nu) = i_\nu \ \ (1 \leq \nu \leq r);$$

$$\mathfrak{V}_4 \cong \{(1), \ (1\,2)\,(3\,4), \ (1\,3)\,(2\,4), \ (1\,4)\,(2\,3)\}$$

als Untergruppe von $\mathfrak{A}_4$.

Rechenregeln für Zykel:

43. Hilfssatz

(1) Zykel entsprechen Bahnen unter der Operation

$$\mathfrak{S}_n \times \{1, \ldots, n\} \to \{1, \ldots, n\} \ : \ \pi \times \nu \mapsto \pi(\nu),$$

d.h. π besitzt genau eine mehrelementige Bahn.

(2) $(i_1, \ldots, i_r) = (i_\nu, \ldots, i_r, \ i_1, \ldots, i_{\nu-1}) \ \ (1 \leq \nu \leq r)$.

(3) $(i_1, \ldots, i_r) = (i_1, \ldots, i_\nu)\,(i_\nu, \ldots, i_r) \quad (2 \leq \nu \leq r-1)$, mit Anwendung

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

(4) $\text{ord}(i_1, \ldots, i_r) = r$,

(5) $(i_1, \ldots, i_r)^{-1} = (i_r, i_{r-1}, \ldots, i_1)$,

(6) $\pi(i_1, \ldots, i_r)\,\pi^{-1} = (\pi(i_1), \ldots, \pi(i_r)) \ \ \forall \pi \in \mathfrak{S}_n$.

Bemerkung: Die Signatur eines r-Zykels ist $(-1)^{r-1}$.

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

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

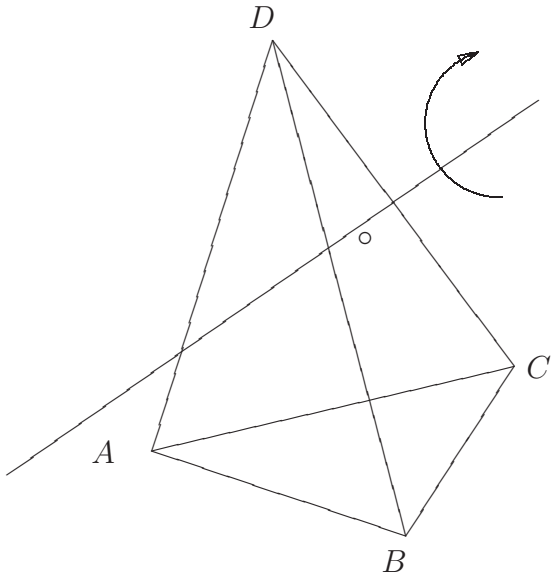
ist. Ist nun $\nu \in \{1, \ldots, n\}$ mit $\pi^{-1}(\nu) \notin \{i_j,\, i_{j+1}\}$, dann bleibt ν invariant. Schließlich ist

$$\pi^{-1}(\nu) = i_{j+1} \quad \Leftrightarrow \quad \nu = \pi\,(i_{j+1}),$$

also gilt insgesamt:

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

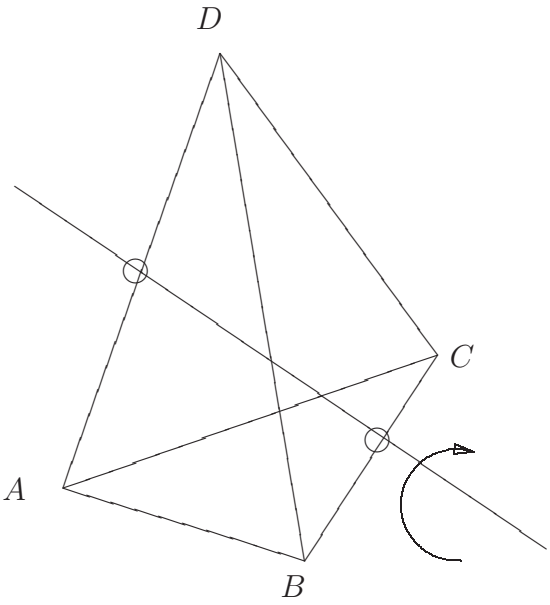
□



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



Mittelpunkte von gegenüberligenden Seiten gehen:

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

44. 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 $\pi\,(\nu) = (\nu,\, n+1) \quad (1 \leq \nu \leq n)$. 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.

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

□

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

45. Hilfssatz

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

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 (1.45)(vi) für $i > 1$. Analog gilt

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

für $1 \leq i < j \leq n$.

□

46. Definition

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

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

ist.

47. Hilfssatz

Elementfremde Zykeln sind vertauschbar.

Beweis:

Es seien $I = \{i_1, \ldots, i_r\},\ J = \{j_1, \ldots, j_s\}$ und $\mathbb{N}_n = \{1, \ldots, n\},\ K = (\mathbb{N}_n \backslash I) \backslash J,\ I \cap J = \emptyset$. Dann gilt

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

□

48. Satz

Jede Permutation $\pi \in \mathfrak{S}_n,\ \pi \neq \mathrm{id}$, läßt sich eindeutig als Produkt elementfremder Zykeln darstellen.

Beweis:

π operiert auf $\mathbb{N}_n$ bzgl. $(\pi, \nu) \mapsto \pi(\nu)$. $\mathbb{N}_n$ zerfällt diesbezüglich in Bahnen $B_1, \ldots, B_{\tilde{k}}$. Nach Weglassen der einelementigen Bahnen verbleiben etwa $B_1, \ldots, B_k$ (bei passender Numerierung) mit

$$B_1 \,\dot\cup\, \ldots \,\dot\cup\, B_k = M_k, \quad B_i = (\nu_i, \pi(\nu_i), \ldots, \pi^{r_i - 1}(\nu_i)) \text{ und } \pi^{r_i}(\nu_i) = \nu_i.$$

Dabei liege

$$\begin{aligned}\nu_1 &:= \min M_k \text{ in } B_1, \\ \nu_2 &:= \min M_k \backslash B_1 \text{ in } B_2, \\ &\vdots \\ \nu_{k-1} &:= \min M_k \backslash (B_1 \,\dot\cup\, \ldots \,\dot\cup\, B_{k-2}) \text{ in } B_{k-1}.\end{aligned}$$

Hierfür ist dann $(\nu_k := \min B_k)$

$$\pi = \Big(\nu_1, \pi(\nu_1), \ldots, \pi^{\sharp B_1 - 1}(\nu_1)\Big)\Big(\nu_2, \pi(\nu_2), \ldots, \pi^{\sharp B_2 - 1}(\nu_2)\Big) \ \ldots\ \Big(\nu_k, \pi(\nu_k), \ldots, \pi^{\sharp B_k - 1}(\nu_k)\Big).$$

Diese Darstellung ist auch eindeutig, da jedes $\nu \in \mathbb{N}_n$ durch π entweder invariant gelassen wird, oder es wird auf ein Element der gleichen Bahn abgebildet, d.h. für $\pi(\nu) \neq \nu$ tritt stets der Zykel

$$\Big(\nu, \pi(\nu), \ldots, \pi^{l_\nu - 1}(\nu)\Big) \text{ auf } \Big(\pi^{l_\nu}(\nu) = \nu\Big).$$

□

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

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

49. 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:

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

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

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

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

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

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

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

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

wie in (ii).

Schließlich:

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

und

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

□

Beispiel:

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

50. Hilfssatz

Für $n \geq 5$ 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 $n \geq 5$ existieren $l,\, m \in \mathbb{N}_n$ mit $\sharp\{i,j,k,l,m\} = 5$. Entweder

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

liegen in $\mathfrak{A}_5$. Nach (1.45)(vi) gilt nun

$$\begin{aligned} \tau\,(1,\,2,\,3) &\overset{(1.45)(\mathrm{vi})}{=} (\tau\,(1),\,\tau\,(2),\,\tau\,(3)) \\ &= (i,\,j,\,k) \\ &\overset{(1.45)(\mathrm{vi})}{=} (l,\,m)\,\tau\,(1,\,2,\,3)\,\tau^{-1}(l,\,m). \end{aligned}$$

□

51. Satz

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

Bemerkung:
Dies hat weitreichende Konsequenzen. Speziell gilt für

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

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

Beweis:
Es sei $N \neq <\mathrm{id}>$ Normalteiler von $\mathfrak{A}_n$ und $n \geq 5$. Gemäß (1.50) und (1.51) genügt es zu zeigen, daß N einen 3-Zykel 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 gemäß (1.49) gegeben.

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

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

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

$$\begin{array}{cccccccc} (i,\,j,\,k,\,l,\,\ldots) & & \pi\,(l), & \pi\,(k), & \pi\,(j) & \pi\,(i) & = (i,\,l,\,j). \\ & (\ldots, & l, & i, & k, & j) & \end{array}$$

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

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

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

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

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

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

Für $\pi\,(m) \neq m$ geht es mit Fall 2 weiter, für $\pi\,(m) = m$ folgt

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

und wir schließen wie im Fall 1.

□

52. 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:

(1) 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.

(2) 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 $G = G_0 \supset G_1 = \{e\}$;
$\mathfrak{S}_4 = G_0 \supset G_1 = \mathfrak{A}_4 \supset G_2 = \mathfrak{V}_4 \supset \{e\} = G_3$.

53. Hilfssatz

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

(2) 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:

(1) 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).)

(2) $\Leftarrow$ 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.

□

54. Hilfssatz

Es sei G eine endliche Gruppe mit Untergruppe H.

(1) Ist G auflösbar, so auch H und im Fall $H \lhd G$ und H auflösbar ist auch G/H auflösbar.

(2) Ist H Normalteiler und sind H sowie G/H auflösbar, dann ist auch G auflösbar.

Beweis:

(1) 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

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

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

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

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

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

$$\begin{aligned} \varphi(g_i H)\,\varphi(\tilde{g}_i \tilde{h}) &= (g_i\, G_{i+1})\,\tilde{g}_i\, G_{i+1}) \\ &\overset{G_{i+1} \lhd G_i}{=} g_i \tilde{g}_i\, G_{i+1} \\ &= \varphi(g_i \tilde{g}_i h^k) \\ &= \varphi(g_i h\, \tilde{g}_i \tilde{h}) \end{aligned}$$

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

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

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:

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

(2) 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.

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] I. N. Herstein, *Topics in Algebra*, Xerox Coll. Pub., 1964.
[7] Th. W. Hungerford, *Algebra*, 1974.
[8] N. Jacobson, *Lectures in Abstract Algebra*, Springer GTM, 1974.
[9] R. Kochendörffer, *Einführung in die Algebra*, Dt.Verl.d. Wissenschaften, 1974.
[10] S. Lang, *Algebra*, Addison-Wesley, 1971.
[11] A. Leutbecher, *Zahlentheorie*, Springer, 1996.
[12] F. Lorenz, *Algebra I, II*, BI Wissenschaftsverlag, 1987/90.
[13] K. Meyberg, *Algebra I, II*, Carl Hanser Verlag, 1975.
[14] Mignotte, *Mathematics for Computer Algebra*, Springer, 1992.
[15] E. Scholz, *Geschichte der Algebra*, BI Wissenschaftsverlag, 1990.
[16] G. Stroth, *Algebra*, de Gruyter, 1998.
[17] B. L. van der Waerden, *Algebra I, II*, Springer, 1966/87.
[18] Weber, *Lehrbuch der Algebra*, Vieweg, 1895.