5.4 Untergruppen

Definition 84

Eine Unteralgebra $\langle T, \circ, 1\rangle$ einer Gruppe $G = \langle S, \circ, 1\rangle$ heißt Untergruppe von G, falls $\langle T, \circ, 1\rangle$ eine Gruppe ist.

Bemerkung: Nicht jede Unteralgebra einer Gruppe ist eine Untergruppe!

Beispiel 85

$\langle \mathbb{N}_0, +, 0\rangle$ ist Unteralgebra von $\langle \mathbb{Z}, +, 0\rangle$, aber keine Gruppe, da es im allgemeinen keine inversen Elemente gibt.

Satz 86

Eine Unteralgebra (bzgl. $\circ$) einer Gruppe ist eine Untergruppe, falls sie unter der Inversenbildung $^{-1}$ abgeschlossen ist.

Beweis:

Folgt sofort aus der Definition. $\square$

Satz 87

Jede Unteralgebra (bzgl. $\circ$) einer endlichen Gruppe ist eine Untergruppe.

Beweis:

Sei $\langle T, \circ, 1\rangle$ eine Unteralgebra einer endlichen Gruppe $\langle S, \circ, 1\rangle$. Sei $b \in T$, $b \neq 1$. Dann gilt:

$$\operatorname{ord}(b) \in \mathbb{N} \setminus \{1\}$$

Sei $m := \operatorname{ord}(b)$. Dann gilt:

$$1 = b^m = b^{m-1} \circ b = b \circ b^{m-1}$$

d. h. $b^{m-1} \in T$ ist das Inverse zu b. $\square$

Satz 88

- *Sei* $G = \langle S, \circ, 1 \rangle$, $b \in G$ *und sei*

$$S_b := \{b^m;\ m \in \mathbb{Z}\} \subseteq S$$

die von b *erzeugte Untergruppe von* G*.* S_b *ist die kleinste Untergruppe, die* b *enthält.*

- *Das Bild einer Gruppe (Halbgruppe, Monoid) unter einem Homomorphismus ist wieder eine Gruppe (Halbgruppe, Monoid).*
- *Seien* $G_1 = \langle S_1, \circ, 1 \rangle$ *und* $G_2 = \langle S_2, \circ, 1 \rangle$ *Untergruppen von* $G = \langle S, \circ, 1 \rangle$*. Dann ist auch*

$$G_1 \cap G_2 = \langle S_1 \cap S_2, \circ, 1 \rangle$$

eine Untergruppe von G*.*

Beweis:

Trivial, lediglich zur letzten Behauptung:

$$a \in S_1 \cap S_2 \;\Rightarrow\; a^{-1} \in S_1 \,\wedge\, a^{-1} \in S_2 \;\Rightarrow\; a^{-1} \in S_1 \cap S_2 .$$

$\square$

5.5 Nebenklassen und Normalteiler

Definition 89

Sei $H = \langle T, \circ, 1\rangle$ eine Untergruppe von $G = \langle S, \circ, 1\rangle$ und sei $b \in G$. Dann heißt

$$T \circ b := \{c \circ b;\ c \in T\} =: H \circ b$$

eine rechte Nebenklasse von H in G und

$$b \circ T := \{b \circ c;\ c \in T\} =: b \circ H$$

eine linke Nebenklasse von H in G (engl.: coset).

Die Anzahl verschiedener Nebenklassen von H in G heißt der Index von H in G:

$$\mathrm{ind}(H) = \mathrm{ind}_G(H).$$

H heißt Normalteiler von G, falls

$$H \circ b = b \circ H \quad \forall b \in G$$

d. h. H ist Normalteiler genau dann, wenn $\forall b \in G : H = b \circ H \circ b^{-1}$ („konjugiert“).

Beispiel 90

Betrachte $\langle \mathbb{Z}_{12}^*, \cdot_{12}, 1\rangle = \langle \{1,5,7,11\}, \cdot_{12}, 1\rangle$. Dann gilt: Die Untergruppe $\langle \{1,5\}, \cdot_{12}, 1\rangle$ ist Normalteiler (folgt aus Definition).

Satz 91

Sei H Untergruppe von G, $b \in G$. Dann ist die Kardinalität von $H \circ b$ gleich der Kardinalität von H (ebenso für $b \circ H$).

Beweis:

Folgt aus der Kürzungsregel: Betrachte die Abbildung

$$H \ni h \mapsto h \circ b \in H \circ b.$$

Diese Abbildung ist surjektiv und injektiv (Kürzungsregel!):

$$h_1 \circ b = h_2 \circ b \Rightarrow h_1 = h_2$$

$\square$

Satz 92

Sei H Untergruppe von G. Dann bildet die Menge der rechten (linken) Nebenklassen von H eine Partition (Zerlegung einer Menge in disjunkte Teilmengen) von G.

Beweis:

Klar ist, dass

$$G \subseteq \bigcup_{b \in G} H \circ b$$

Seien $b, c \in G$ mit $H \circ b \cap H \circ c \neq \emptyset$, etwa $h_1 \circ b = h_2 \circ c$. Dann ist

$$H \circ c = H \circ {h_2}^{-1} \circ h_1 \circ b = H \circ b$$

$\square$

Eigenschaften von Nebenklassen:

H sei Untergruppe von G, $b, c \in G$.

- Zwei Nebenklassen $H \circ b$ und $H \circ c$ sind entweder identisch oder disjunkt.
- Für alle $b \in G$ gilt $|H \circ b| = |H|$.

Satz 93 (Lagrange)

Sei G eine endliche Gruppe und H eine Untergruppe in G. Dann

1. *haben alle Nebenklassen von H in G gleich viele Elemente;*
2. *ist $|G| = \text{ind}_G(H) \cdot |H|$;*
3. *teilt $|H|$ die Kardinalität $|G|$ von G ganzzahlig.*

Beweis:

1. siehe oben;
2. folgt aus Satz 92;
3. folgt aus 2.

$\square$

Mehr zu Joseph-Louis Lagrange!

5.6 Satz von Fermat

Satz 94

Sei $b \in \mathbb{N}_0$ und $p \in \mathbb{N}$ eine Primzahl. Dann gilt:

$$b^p \equiv b \bmod p, \;\; (\textit{falls } b \not\equiv 0 \bmod p \;:\; b^{p-1} \equiv 1 \bmod p)$$

(gemeint ist: die Gleichung $b^p = b$ gilt modulo p)

Beweis:

$\mathbb{Z}_p^* := \{n \in \{1, \ldots, p-1\}; \mathrm{ggT}(n,p) = 1\}$

1. Fall: $b = 0$: $0^p = 0 \bmod p$
2. Fall: $1 \leq b < p$: Betrachte $S_b = \langle \{b^0, b^1, \ldots, b^{\mathrm{ord}(b)-1}\}, \ \cdot \ \rangle$.

   S_b ist Untergruppe von $\mathbb{Z}_p^*$.

   Lagrange: $(\mathrm{ord}(b) =)\ |S_b| \ \big|\ |\mathbb{Z}_p^*| (= p-1)$

   $$\Rightarrow (\exists q \in \mathbb{N})[q \cdot \mathrm{ord}(b)] = p - 1$$

   Da $b^{\mathrm{ord}(b)} = 1$ (Einselement) ist, gilt:

   $$b^p = b^{p-1} \cdot b = b^{q \cdot \mathrm{ord}(b)} \cdot b = 1^q \cdot b = b \bmod p$$
3. Fall: $b \geq p$: Dann gilt:

   $$(\exists q, r \in \mathbb{N}_0, 0 \leq r < p)[b = q \cdot p + r].$$

   Damit:

   $$b^p = (q \cdot p + r)^p \stackrel{(*)}{=} r^p \bmod p \stackrel{(**)}{=} r \bmod p = b \bmod p$$

   $(*)$ Binomialentwicklung, die ersten p Summanden fallen weg, da jeweils $= 0 \bmod p$;
   $(**)$ Fall 1 bzw. 2

$\square$

Die umgekehrte Richtung

Satz 95

Sei $n \in \mathbb{N}$*,* $n \geq 2$*. Dann gilt:*

$$b^{n-1} \equiv 1 \bmod n \text{ für alle } b \in \mathbb{Z}_n \setminus \{0\} \Longrightarrow n \text{ ist prim.}$$

Beweis:

[durch Widerspruch] Annahme: $r|n$ für ein $r \in \mathbb{N}$, $r > 1$. Dann

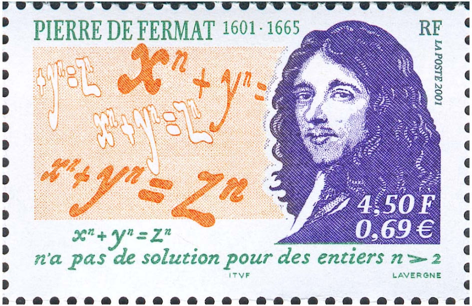
$$r^{n-1} - 1 \equiv (r \bmod n)^{n-1} - 1 \overset{\text{n. V.}}{\equiv} 0 \bmod n\ ,$$

also

$$r^{n-1} - 1 = q \cdot n = q \cdot q' \cdot r \text{ da } r|n\ .$$

Daraus folgt aber, dass $r|1$, n also keinen nichttrivialen Teiler besitzen kann. □

Pierre de Fermat (1601–1665)



Definition 96 (Eulersche phi-Funktion)

Sei $n \in \mathbb{N}$, $n > 1$. Dann bezeichnet

$$\varphi(n) := |\mathbb{Z}_n^*|$$

die Anzahl der zu n teilerfremden Reste.

Satz 97

Sei $n \in \mathbb{N}$, $n > 1$. Dann gilt in der Gruppe $\langle \mathbb{Z}_n^*, \times_n, 1 \rangle$:

$$b^{\varphi(n)} = 1 \text{ *für alle* } b \in \mathbb{Z}_n^* \ .$$

Beweis:

Folgt sofort aus dem Satz von Lagrange (Satz 93)! □

Leonhard Euler (1707–1783)

Leonhard Euler (1707–1783)

5.7 Zyklische Gruppen

Definition 98

Eine Gruppe $G = \langle S, \circ, 1 \rangle$ heißt zyklisch, wenn es ein $b \in G$ gibt, so dass

$$G = S_b$$

wobei $S_b = \langle \{b^i | i \in \mathbb{Z}\}, \circ, 1 \rangle$.

Satz 99

Sei G eine zyklische Gruppe. Falls G unendlich ist, ist G zu $\langle \mathbb{Z}, +, 0 \rangle$ isomorph; falls G endlich ist, dann ist G isomorph zu $\langle \mathbb{Z}_m, +_m, 0 \rangle$ für ein $m \in \mathbb{N}$.

Beweis:

1. Fall: Sei G unendlich. Wir wissen: $G = \{b^i | i \in \mathbb{Z}\}$ für ein geeignetes $b \in G$, nach Voraussetzung. Betrachte die Abbildung

$$h : \mathbb{Z} \ni i \mapsto b^i \in G$$

Behauptung: h ist bijektiv.
Nach Voraussetzung ist h surjektiv.
Die Injektivität beweisen wir mittels Widerspruch.

Annahme: $(\exists i, j, i \neq j)[b^i = b^j]$
Daraus folgt:

$$b^{i-j} = 1$$

Daher ist G endlich, es gilt nämlich:

$$G \subseteq \{b^k; 0 \leq k < |i - j|\}$$

Dies ist ein Widerspruch zur Annahme, G sei unendlich!

Beweis (Forts.):

2. Fall: G endlich:

Wiederum ist die Abbildung h nach Voraussetzung surjektiv. Nach dem Schubfachprinzip

$$(\exists i, j, i \neq j)[b^i = b^j] \; .$$

Nach der Kürzungsregel können wir $j = 0$ wählen. Falls $i > 0$ und i minimal gewählt wird, folgt sofort

$$G \text{ isomorph } \langle \mathbb{Z}_i, +_i, 0 \rangle \; .$$

$\square$

Satz 100

Jede Untergruppe einer zyklischen Gruppe ist wieder zyklisch.

Beweis:

Sei G zyklisch, $H \subseteq G$ Untergruppe von G.

1. Fall: $|G| = \infty$, also $G \cong \langle \mathbb{Z}, +, 0 \rangle$ ($\cong$ isomorph).

   Sei H' die durch den Isomorphismus gegebene Untergruppe von $\langle \mathbb{Z}, +, 0 \rangle$, die H entspricht.

   Zu zeigen ist: H' ist zyklisch.

   Sei $i := \min\Big\{k \in H'; k > 0\Big\}$.

   Die Behauptung ist:
$$H' = S_i.$$
   Es gilt sicher:
$$S_i \subseteq H'.$$
   Falls ein $k \in H' \setminus S_i$ existiert, folgt $k \bmod i \in H'$. Dies stellt einen Widerspruch zur Wahl von i dar. Also ist $H' = S_i$, damit ist gezeigt, dass H' und daher auch H zyklisch ist.

2. Fall: $|G| < \infty$: Der Beweis läuft analog.

$\square$

5.8 Transformationsgruppen

Definition 101

Eine Transformationsgruppe ist eine Gruppe von bijektiven Abbildungen einer Menge U auf sich selbst mit der Komposition $\circ$ als binärem Operator:

$$g \circ f : U \ni x \mapsto g\big(f(x)\big) \in U$$

Satz 102 (Darstellungssatz für Gruppen)

Jede Gruppe ist isomorph zu einer Transformationsgruppe.

Beweis:

Sei $G = \langle S, \circ, 1 \rangle$, $g \in G$. Betrachte die Abbildung

$$\tilde{g} : S \ni a \mapsto g \circ a \in S$$

Aus der Kürzungsregel und der Existenz eines Inversen folgt, dass $\tilde{g}$ eine bijektive Abbildung ist.

Wir betrachten nun $\tilde{G} := \langle \tilde{S}, \circ, \tilde{1} \rangle$ mit $\tilde{S} = \{\tilde{g};\ g \in G\}$. Die Abbildung

$$\tilde{\ } : \ S \ni g \mapsto \tilde{g} \in \tilde{S}$$

ist ein Gruppenisomorphismus. Für $h, g \in G$ gilt:

$$\big(\widetilde{h \circ g}\big)(a) = (h \circ g) \circ a = h \circ (g \circ a) = h \circ \tilde{g}(a) = \tilde{h}\big(\tilde{g}(a)\big) = \big(\tilde{h} \circ \tilde{g}\big)(a)$$

$\square$