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:

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

□

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!):

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

□

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

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

□

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 $|G| = ind_G(H) \cdot |H|$;*
3. *teilt $|H|$ die Kardinalität $|G|$ von G ganzzahlig.*

Beweis:

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

□

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:

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

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

Beweis:

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

1. Fall: $b = 0$: $0^p = 0 \bmod p$
2. Fall: $1 \leq b < p$: Betrachte $S_b = \langle \{b^0, b^1, \ldots, b^{\text{ord}(b)-1}\}, \cdot \rangle$.
   S_b ist Untergruppe von $\mathbb{Z}_p^*$.
   Lagrange: $(\text{ord}(b) =)\ |S_b|\ \big||\mathbb{Z}_p^*|(= p-1)$

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

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

$$b^p = b^{p-1} \cdot b = b^{q \cdot \text{ord}(b)} \cdot b = 1^q \cdot b = b \bmod p$$

3. Fall: $b \geq p$: Dann gilt:

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

   Damit:

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

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

□