2. Faktorgruppen

Definition: Es sei G eine Gruppe und $H \leq G$. Auf G definiert man zwei Relationen $\sim_r$ und $\sim_\ell$ durch $a \sim_r b :\Leftrightarrow ab^{-1} \in H$ und $a \sim_\ell b :\Leftrightarrow a^{-1}b \in H$.

Satz 16: Es sei G eine Gruppe und $H \leq G$. Dann gelten:
(i) $\sim_r$ und $\sim_\ell$ sind Äquivalenzrelationen.
(ii) Die Äquivalenzklasse von $a \in G$ bezüglich $\sim_r$ ist die Menge $Ha = \{ha \mid h \in H\}$ und die Äquivalenzklasse bezüglich $\sim_\ell$ ist die Menge $aH = \{ah \mid h \in H\}$.
(iii) $|aH| = |H| = |Ha|$ $\forall a \in G$.

Beweis: Wir führen den Beweis nur für $\sim_r$. Der Beweis für $\sim_\ell$ kann analog geführt werden.
(i) $aa^{-1} = e \in H$ $\forall a \in G \Rightarrow a \sim_r a$ $\forall a \in G$.
$a \sim_r b \Rightarrow ab^{-1} \in H \Rightarrow ba^{-1} = (ab^{-1})^{-1} \in H \Rightarrow b \sim_r a$.
$a \sim_r b$ und $b \sim_r c \Rightarrow ab^{-1}, bc^{-1} \in H \Rightarrow ac^{-1} = (ab^{-1})(bc^{-1}) \in H \Rightarrow a \sim_r c$.
(ii) Die Äquivalenzklasse von a ist

$$\{x \in G \mid x \sim_r a\} = \{x \in G \mid xa^{-1} \in H\} = \{x \in G \mid x \in Ha\} = Ha.$$

(iii) Die Abbildung $H \to Ha$, $h \mapsto ha$ ist offensichtlich bijektiv.

Definition: Es sei G eine Gruppe und $H \leq G$. Die Mengen Ha (bzw. aH) mit $a \in G$ werden Rechtsnebenklassen (bzw. Linksnebenklassen) von H in G genannt.

Korollar 17: Es sei G eine Gruppe und $H \leq G$. Dann gelten:
(i) G ist disjunkte Vereinigung der Linksnebenklassen (bzw. Rechtsnebenklassen) von H in G.
(ii) Zwei Linksnebenklassen (bzw. Rechtsnebenklassen) von H in G sind entweder disjunkt oder stimmen überein.
(iii) Für $a, b \in G$ gelten $Ha = Hb \Leftrightarrow ab^{-1} \in H$ und $aH = bH \Leftrightarrow a^{-1}b \in H$.
(iv) Die Menge der Linksnebenklassen von H in G und die der Rechtenebenklassen von H in G haben dieselbe Kardinalität.

Beweis: (i) und (ii) Das folgt aus Satz 16 (i) weil diese beiden Eigenschaften für jede Äquivalenzrelation erfüllt sind.
(iii) Zunächst ist $Ha = Hb \Leftrightarrow a \in Hb$. (Einerseits ist $a = ea \in Ha = Hb$. Andererseits folgt aus $a = ea \in Ha$ und $a \in Hb$, dass $Ha \cap Hb \neq \varnothing$ und daher $Ha = Hb$ nach (ii).) Schließlich ist $a \in Hb \Leftrightarrow ab^{-1} \in H$. Die zweite Behauptung kann analog bewiesen werden.

(iv) Die Abbildung $Ha \mapsto a^{-1}H$ ist wohldefiniert und injektiv, da

$$Ha = Hb \overset{\text{(iii)}}{\Leftrightarrow} ab^{-1} \in H \Leftrightarrow (a^{-1})^{-1}b^{-1} \in H \overset{\text{(iii)}}{\Leftrightarrow} a^{-1}H = b^{-1}H$$

(Die Implikationen von links nach rechts zeigen, dass diese Abbildung wohldefiniert ist, die Implikationen von rechts nach links, dass sie injektiv ist.) Da die Abbildung trivialerweise auch surjektiv ist, ist sie bijektiv.

Bemerkungen: 1) Wird die Verknüpfung der Gruppe G additiv geschrieben, so erhält man $a \sim_r b \Leftrightarrow a - b \in H$ und $H + a = \{h + a \mid h \in H\}$ ist Rechtsnebenklasse.
2) Ist die Gruppe G abelsch, so ist $a \sim_r b \Leftrightarrow a \sim_\ell b$, denn

$$a \sim_r b \Leftrightarrow ab^{-1} \in H \Leftrightarrow (ab^{-1})^{-1} \in H \Leftrightarrow ba^{-1} \in H \Leftrightarrow a^{-1}b \in H \Leftrightarrow a \sim_\ell b$$

und daher $aH = Ha \ \forall a \in G$.

Definition: Es sei G eine Gruppe und $H \leq G$. Die Kardinalität der Menge der Rechtsnebenklassen von H in G wird als Index von H in G bezeichnet und man schreibt $[G : H]$ dafür.

Bemerkungen: 1) Nach Korollar 17 (iv) stimmt $[G : H]$ mit der Kardinalität der Linksnebenklassen überein.
2) Für jede Gruppe G ist $[G : G] = 1$, da $ab^{-1} \in G \ \forall a, b \in G \Leftrightarrow a \sim_r b \ \forall a, b \in G$.
3) Für jede Gruppe G ist $\big[G : \{e\}\big] = |G|$, da $ab^{-1} \in \{e\} \Leftrightarrow ab^{-1} = e \Leftrightarrow a = b$.

Beispiel: Es sei $m \in \mathbb{N} \setminus \{0, 1\}$, $G = \mathbb{Z}$ und $H = m\mathbb{Z}$. Dann gilt $a \sim_r b \Leftrightarrow a \equiv b \pmod{m}$, denn

$$a \sim_r b \Leftrightarrow a - b \in m\mathbb{Z} \Leftrightarrow m \mid (a - b) \Leftrightarrow a \equiv b \pmod{m}$$

und die Nebenklassen sind genau die Restklassen modulo m (d.h. die Mengen der Gestalt $a + m\mathbb{Z}$).

Satz 18: Es seien K, H und G drei Gruppen mit der Eigenschaft $K \leq H \leq G$. Dann gilt $[G : K] = [G : H][H : K]$.

Beweis: Es sei $G = \bigcup_{i \in I} Ha_i$ eine Darstellung von G als disjunkte Vereinigung von Nebenklassen, d.h. $a_i \in G \ \forall i \in I$, $Ha_i \cap Ha_j = \varnothing$ für $i, j \in I$, $i \neq j$ und $[G : H] = |I|$. Ebenso sei $H = \bigcup_{j \in J} Kb_j$ eine Darstellung von H als disjunkte Vereinigung von Nebenklassen, d.h. $b_j \in H \ \forall j \in J$, $Kb_i \cap Kb_j = \varnothing$ für $i, j \in J$, $i \neq j$ und $[H : K] = |J|$. Dann ist

$$G = \bigcup_{i \in I} Ha_i = \bigcup_{i \in I} \Big(\bigcup_{j \in J} Kb_j \Big) a_i = \bigcup_{(i,j) \in I \times J} Kb_j a_i.$$

Wir zeigen, dass es sich bei Kb_ja_i (mit $(i,j) \in I \times J$) um disjunkte Nebenklassen handelt. Wenn $Kb_ja_i = Kb_ta_s$, dann $b_ja_i \in Kb_ta_s$, d.h. $\exists k \in K : b_ja_i = kb_ta_s$. Aus $b_j, b_t, k \in H$ folgt $Ha_i = Hb_ja_i = Hkb_ta_s = Ha_s$ und daher $i = s$. Daraus erhält man $b_j = kb_t$ und somit $Kb_j = Kkb_t = Kb_t$ und $j = t$. Also ist

$$[G : K] = |I \times J| = |I| \cdot |J| = [G : H][H : K].$$

Korollar 19 (Satz von Lagrange): Es sei G eine Gruppe und $H \leq G$. Dann gelten;
(i) $|G| = [G : H]|H|$
(ii) Ist G endlich, so $|H| \,\big|\, |G|$.
(iii) Ist G endlich und $a \in G$, so $\mathrm{ord}(a) \,\big|\, |G|$.
(iv) Ist G endlich und $a \in G$, so $a^{|G|} = e$.

Beweis: (i) Setze $K = \{e\}$ in Satz 18.
(ii) Folgt sofort aus (i).
(iii) Setze $H = \langle a \rangle$ in (ii).
(iv) Folgt aus (iii) und Satz 15 (iii).

Beispiele: 1) In der Gruppe $(\mathbb{Z}_5, +)$ kann es nur Elemente bzw. Untergruppen der Ordnung 1 oder 5 geben, da 5 eine Primzahl ist und nur die positiven Teiler 1 und 5 besitzt. Daher ist $\mathrm{ord}(\overline{0}) = 1$ und $\mathrm{ord}(\overline{a}) = 5$ für $a \in \{1, 2, 3, 4\}$. Weiters besitzt $\mathbb{Z}_5$ offenbar nur die Untergruppen $\left\{\overline{0}\right\}$ und $\mathbb{Z}_5$.
2) Völlig analog zeigt man die folgende Verallgemeinerung: Ist p eine Primzahl, so gilt $\mathrm{ord}(\overline{a}) = p \ \forall \overline{a} \in \mathbb{Z}_p \setminus \left\{\overline{0}\right\}$ und $(\mathbb{Z}_p, +)$ besitzt nur die beiden Untergruppen $\left\{\overline{0}\right\}$ und $\mathbb{Z}_p$.
3) In $(\mathbb{Z}_8, +)$ kann es nur Elemente bzw. Untergruppen mit Ordnung in $\{1, 2, 4, 8\}$ geben. (Damit ist aber noch nicht gezeigt, dass es derartige Elemente bzw. Untergruppen tatsächlich gibt.)

Satz 20: Es sei G eine Gruppe und $N \leq G$. Dann sind äquivalent:

(i) Die Partitionen von G in Links- bzw. Rechtsnebenklassen stimmen überein,
(ii) $aN = Na \ \forall a \in G$,
(iii) $aN \subseteq Na \ \forall a \in G$,
(iv) $aNa^{-1} \subseteq N \ \forall a \in G$,
(v) $aNa^{-1} = N \ \forall a \in G$.

Beweis: (i) $\Rightarrow$ (ii) Es sei $a \in G$. Nach Voraussetzung $\exists b \in G : bN = Na$. Daher ist $a \in aN \cap bN$ und nach Korollar 17 (ii) ist $aN = bN = Na$.
(ii) $\Rightarrow$ (iii) Trivial.
(iii) $\Rightarrow$ (iv) $aNa^{-1} = (aN)a^{-1} \subseteq (Na)a^{-1} = N$.

(iv) $\Rightarrow$ (v) Außer $aNa^{-1} \subseteq N$ gilt auch $a^{-1}N(a^{-1})^{-1} \subseteq N$, d.h. $a^{-1}Na \subseteq N$ und daher $N = a(a^{-1}Na)a^{-1} \subseteq aNa^{-1}$.
(v) $\Rightarrow$ (ii) $aN = (aNa^{-1})a = Na$.
(ii) $\Rightarrow$ (i) Trivial.

Definition: Es sei G eine Gruppe. Ein $N \leq G$, das eine (und damit alle) der Bedingungen aus Satz 20 erfüllt, wird Normalteiler (oder normale Untergruppe) von G genannt. Wir schreiben dafür $N \trianglelefteq G$.

Beispiele: 1) Für jede Gruppe G ist $\{e\} \trianglelefteq G$ und $G \trianglelefteq G$.
2) Ist G eine abelsche Gruppe und $H \leq G$, so ist $H \trianglelefteq G$.
3) Ist K ein Körper, so ist $\mathrm{SL}_n(K) \trianglelefteq \mathrm{GL}_n(K)$. Sind nämlich $A, B \in \mathrm{GL}_n(K)$ wobei $\det A = 1$, so ist

$$\det(BAB^{-1}) = \det(B) \cdot \det(A) \cdot \det(B)^{-1} = \det(A) = 1,$$

d.h. $BAB^{-1} \in \mathrm{SL}_n(K)$, womit gezeigt wurde, dass Bedingung (iv) aus Satz 20 erfüllt ist.

Definition: Eine Gruppe G, die außer $\{e\}$ und G keine weiteren Normalteiler besitzt, wird einfach genannt.

Beispiel: Ist p eine Primzahl, so ist $(\mathbb{Z}_p, +)$ einfach.

Satz 21: Es sei G eine Gruppe und $N \trianglelefteq G$. Bezeichnet G/N die Menge der Nebenklassen von N in G, so ist G/N mit der Verknüpfung $(aN) \cdot (bN) = abN$ eine Gruppe der Ordnung $[G : N]$. Ist G abelsch, so ist G/N ebenfalls abelsch.

Bemerkung: Das Produkt $(aN) \cdot (bN)$ ist ein Komplexprodukt (d.h. sind $X, Y \subseteq G$, so setzt man $X \cdot Y = \{xy \mid x \in X, y \in Y\}$).

Beweis: Da $N \trianglelefteq G$, gilt

$$(aN)(bN) = a(Nb)N = a(bN)N = (ab)(NN) = abN.$$

Die Verknüpfung ist daher wohldefiniert, d.h. sind $\overline{a}N = aN$ und $\overline{b}N = bN$, so ist

$$\overline{a}\overline{b}N = (\overline{a}N)(\overline{b}N) = (aN)(bN) = abN.$$

Das Assoziativgesetz gilt, da

$$\big((aN)(bN)\big)(cN) = (ab)cN = a(bc)N = (aN)\big((bN)(cN)\big) \ \forall a, b, c \in G.$$

Neutrales Element ist $eN = N$, da $(aN)(eN) = (eN)(aN) = aN \ \forall a \in G$.
Inverses Element von aN ist $a^{-1}N$, da $(aN)(a^{-1}N) = (a^{-1}N)(aN) = eN = N$.
Ist G abelsch, so ist $(aN)(bN) = abN = baN = (bN)(aN) \ \forall a, b \in G$, d.h. G/N ist abelsch.
Da die Elemente von G/N die Nebenklassen von N in G sind, besitzt G/N genau $[G : N]$ Elemente.

Definition: Ist G eine Gruppe und $N \trianglelefteq G$, so bezeichnet man die in Satz 21 beschriebenen Gruppe G/N als Faktorgruppe von G nach N.

Bemerkung: Schreibt man die Verknüpfung von G additiv, so tut man das auch für die Verknüpfung von G/N, d.h. $(a + N) + (b + N) = (a + b) + N$.

Beispiel: Es sei $m \in \mathbb{N} \setminus \{0, 1\}$. Dann ist $\mathbb{Z}_m = \mathbb{Z}/m\mathbb{Z}$, d.h. die additive Gruppe der Restklassen modulo m ist die Faktorgruppe von $(\mathbb{Z}, +)$ nach dem Normalteiler $(m\mathbb{Z}, +)$.