# Links- und Rechtsnebenklassen einer Untergruppe

**Definition (2.13)**

Sei $(G, \cdot)$ eine Gruppe und $U$ eine Untergruppe. Eine Teilmenge von $G$, die mit einem geeigneten $g \in G$ in der Form

$$gU \quad = \quad \{gu \mid u \in U\}$$

geschrieben werden kann, wird Linksnebenklasse von $U$ genannt. Ebenso bezeichnet man die Teilmengen der Form $Ug = \{ug \mid u \in U\}$ mit $g \in G$ als Rechtsnebenklassen von $U$.

Im Folgenden bezeichnet $G/U$ für die Menge der Links- und $U\backslash G$ die Menge der Rechtsnebenklassen von $U$.

# Gleichmächtigkeit der Linksnebenklassen

**Lemma (2.14)**

Sei $G$ eine Gruppe, $U$ eine Untergruppe von $G$ und $g \in G$ ein beliebiges Element. Dann sind die Abbildungen

$$\tau_g^{\ell} : U \to gU \ , \ h \mapsto gh \qquad \text{und} \qquad \tau_g^{r} : U \to Ug \ , \ h \mapsto hg$$

jeweils bijektiv. Ist $U$ endlich, dann gilt also $|U| = |gU| = |Ug|$ für alle $g \in G$.

Beweis von Lemma 2.14 (nur Bijektivität von $\tau_g^l$ für ein $g \in G$)

(1) Injektivität: Seien $h, h' \in U$ mit $\tau_g^l(h) = \tau_g^l(h')$.

$\Rightarrow gh = gh' \rightarrow g^{-1}gh = g^{-1}gh' \rightarrow eh = eh'$

$\rightarrow h = h'$

(2) Surjektivität: Sei $k \in gU$. Nach Def gibt es ein $h \in U$ mit $k = gh$. $\Rightarrow \tau_g^l(h) = gh = k$.

□

# Zerlegung einer Gruppe in Linksnebenklassen

**Lemma (2.15)**

Sei $G$ eine Gruppe und $U$ eine Untergruppe von $G$. Dann folgt für alle $g, h \in G$ aus $h \in gU$ jeweils $gU = hU$.

**Satz (2.16)**

Sei $G$ eine Gruppe und $U \leq G$. Dann ist sowohl durch $G/U$ als auch durch $U\backslash G$ eine Zerlegung von $G$ gegeben. Die zugehörigen Äquivalenzrelationen auf $G$ sind definiert durch $g \equiv_\ell h \Leftrightarrow h \in gU$ bzw. $g \equiv_r h \Leftrightarrow h \in Ug$.

Beweis von Lemma 2.15:

Seien $g, h \in G$ mit $h \in gU$. z.zg.: $gU = hU$

$h \in gU \Rightarrow \exists u \in U : h = gu$

„⊇" Sei $k \in hU \Rightarrow \exists v \in U$ mit $k = hv \Rightarrow$

$k = (gu)v = g(uv)$ $uv \in U$ (wg. $U \leq G$) $\Rightarrow k \in gU$

„⊆" Es gilt $g = ge = guu^{-1} = hu^{-1}$, und $u^{-1} \in U$

(wg. $U \leq G$) Sei nun $k' \in gU \Rightarrow \exists v' \in U$ mit $k' = gv'$

$\Rightarrow k' = (hu^{-1})v' = h(u^{-1}v')$, und $u^{-1}v' \in U$

$\Rightarrow k' \in hU$ □

Beweis von Satz 2.16

(zeige nun die Zerlegungseigenschaft von $G/U$)

zu überprüfen: (1) $\emptyset \notin G/U$

(2) $G = \bigcup_{A \in G/U} A$ (3) $\forall A, B \in G/U$ :
$A \cap B \neq \emptyset \Rightarrow A = B$

zu (1) Sei $A \in G/U$, z.zg. $A \neq \emptyset$.

$A \in G/U \Rightarrow \exists g \in G : A = gU$ Wegen
$e \in U$ gilt $g = g \cdot e \in gU$, d.h. $gU \neq \emptyset$

zu (2) „$\supseteq$" Nach Def. sind alle $A \in G/U$
Teilmengen von $G$.

„$\subseteq$" Sei $g \in G$. Dann gilt $g \in gU$ (s.o.) und $gU \in G/U$.

Zu (3) Seien $A, B \in G/U$ mit $A \cap B \neq \emptyset$.

z.zg.: $A = B$ $A, B \in G/U \Rightarrow \exists g, h \in G$ mit $A = gU$, $B = hU$. $A \cap B \neq \emptyset \Rightarrow$ $\exists k \in G$ mit $k \in gU$ und $k \in hU$.

$k \in gU \overset{\text{Lemma 2.15}}{\Rightarrow} kU = gU$, ebenso: $k \in hU \Rightarrow$ $kU = hU$ also: $gU = kU = hU$.

Zeige noch: Die Elemente von $G/U$ sind genau die Äquivalenzkl. der Relation $\equiv_l$ auf $G$ gg. durch $g \equiv_l h \Leftrightarrow h \in gU \quad \forall g, h \in G$, insb. ist $\equiv_l$ eine Äquivalenzrelation.

Sei $g \in G$. Definiere $[g]_l = \{h \in G \mid g \equiv_l h\}$

Es gilt $[g]_l = gU$, denn: Sei $h \in G$.

„$\supseteq$" Ang. $h \in gU \rightarrow g \equiv_l h \Rightarrow h \in [g]_l$

„$\subseteq$" Ang $h \in [g]_l \Rightarrow g \equiv_l h \Rightarrow h \in gU$

Die Teilmengen der Form $gU$ bilden also genau die Zerlegung, die auch durch die Teil-

mengen der Form $[g]_1$ gegeben ist.
bekannt aus dem 1. Semester: Ist $Z$ eine
Zerlegung einer Menge, dann erhält man
durch $g \equiv_Z h \iff \exists A \in Z : g, h \in Z$
eine Äquivalenzrelation auf $G$. Ist nun $Z$
gegeben durch $\{[g]_1 \mid g \in G\}$, dann gilt
$g \equiv_1 h \iff g \equiv_Z h$ für alle $g, h \in G$
(wie man unmittelbar überprüft). Mit $\equiv_Z$
ist also auch $\equiv_1$ eine Äquivalenzrelation.

# Ergänzung zu Satz 2.16

Seien $g, h \in G$. Die Relation $\equiv_{\mathcal{Z}}$ in Abhängigkeit von einer Zerlegung $\mathcal{Z}$ der Menge $G$ war definiert durch

$$g \equiv_{\mathcal{Z}} h \;\Leftrightarrow\; \exists\, A \in \mathcal{Z} : (g \in A) \wedge (h \in A) \qquad \forall\, g, h \in G.$$

Ist nun $\mathcal{Z}$ speziell die Menge der Linksnebenklassen von einer Untergruppe $U$, dann kann man die Äquivalenz $g \equiv_\ell h \Leftrightarrow g \equiv_{\mathcal{Z}} h$ folgendermaßen überprüfen:

„$\Leftarrow$“ Nach Voraussetzung gilt $h \in gU$. Also ist $A = gU$ ein Element von $\mathcal{Z}$, das sowohl $g$ als auch $h$ enthält.

„$\Rightarrow$“ Nach Voraussetzung existiert ein $A \in \mathcal{Z}$ mit $g, h \in A$. Weil $A$ eine Linksnebenklasse ist, gilt $A = kU$ für ein $k \in G$. Aus $g, h \in kU$ folgt $gU = hU = kU$ nach Lemma 2.15. Wegen $h \in hU$ gilt also auch $h \in gU$, und damit $g \equiv_\ell h$.

# Repräsentantensysteme von Äquivalenzklassen

**Definition (2.17)**

Sei $X$ eine Menge und $\equiv$ eine Äquivalenzrelation auf $X$. Eine Teilmenge $R \subseteq X$ wird Repräsentantensystem der Äquivalenzklassen von $\equiv$ genannt, wenn durch $R \to X/\equiv,\ x \mapsto [x]$ eine bijektive Abbildung gegeben ist. Mit anderen Worten, in jeder Äquivalenzklasse ist genau ein Element aus $R$ enthalten.

# Zusammenhang zwischen Links- und Rechtsnebenklassen

**Proposition (2.18)**

Sei $G$ eine Gruppe und $U$ eine Untergruppe.Ist $R$ ein Repräsentantesystem der Linksnebenklassen, dann ist $R' = \{g^{-1} \mid g \in R\}$ ein Repräsentantensystem der Rechtsnebenklassen, und durch $g \mapsto g^{-1}$ ist eine Bijektion zwischen $R$ und $R'$ definiert.

Beweis von Prop. 2.18:

geg: Gruppe $G$, Untergruppe $U$

$R$ Repräsentantensystem von $G/U$, d.h. jedes $A \in G/U$ enthält genau ein Element aus $R$

Sei außerdem $R' = \{g^{-1} \mid g \in R\}$

Sei $B \in U\backslash G$, d.h. $B = Ug$ für ein $g \in G$ zzg:

(1) $\exists\, h \in R'$ mit $h \in B$

(2) $\forall\, h, h' \in R'$: $h, h' \in B \Rightarrow h = h'$

zu (1) $R$ Repr.-system der LNK $\Rightarrow \exists\, h_1 \in R$ mit $h_1 \in g^{-1}U$

$\Rightarrow \exists\, u \in U$: $h_1 = g^{-1}u \Rightarrow h_1^{-1} = u^{-1}g \Rightarrow h_1^{-1} \in B$

Sei außerdem $R' = \{g^{-1} \mid g \in R\}$

Sei $B \in U\backslash G$, d.h. $B = Ug$ für ein $g \in G$ z.z.g.:

Nach Def. von $R'$ ist $h := h_1^{-1}$ in $R'$ enthalten.

zu (2) Seien $h, h' \in R'$ mit $h, h' \in B$ z.z.g.: $h = h'$

$h, h' \in R' \Rightarrow \exists\, h_1, h_1' \in R$ mit $h_1^{-1} = h, (h_1')^{-1} = h'$

$h, h' \in B \Rightarrow \exists\, u, u' \in U : h = ug,\ h' = u'g$

$\longrightarrow h_1 = h^{-1} = g^{-1}u^{-1},\ h_1' = (h')^{-1} = g^{-1}u'$

$\Rightarrow h_1, h_1' \in R$ und $h_1, h_1' \in g^{-1}U$ $\overset{R \text{ Rupr.-system}}{\Longrightarrow}$ $h_1 = h_1'$

$\Rightarrow h = h_1^{-1} = (h_1')^{-1} = h'$

noch zu überprüfen: Bijektivität von $\phi : R \to R',\ g \mapsto g^{-1}$

Die Surj. folgt direkt aus der Def. von $R'$. Zur Injektivität:

Seien $g, g' \in R$ mit $\phi(g) = \phi(g') \Rightarrow g^{-1} = (g')^{-1} \Rightarrow (g^{-1})^{-1} = ((g')^{-1})^{-1} \Rightarrow g = g'$. $\square$

# Der Index einer Untergruppe

**Definition (2.19)**

Sei $G$ eine Gruppe und $U$ eine Untergruppe. Die Mächtigkeit $|G/U|$ der Menge $G/U$ wird der Index von $U$ in $G$ genannt und mit $(G : U)$ bezeichnet.

# Der Satz von Lagrange

**Satz (2.20)**

Sei $G$ eine endliche Gruppe und $U$ eine Untergruppe. Dann gilt $|G| = (G : U)|U|$. Insbesondere ist die Ordnung $|U|$ der Untergruppe immer ein Teiler der Gruppenordnung $|G|$.

**Folgerung (2.21)**

Sei $G$ eine Gruppe und $U$ eine Untergruppe. Genau dann ist $G$ endlich, wenn sowohl $U$ als auch $G/U$ endliche Mengen sind (und in diesem Fall gilt dann natürlich der Satz von Lagrange).

Beweis von Satz 2.20:

geg.: endl. Gruppe $G$, $U \leq G$

z.z.g.: $|G| = (G:U) \cdot |U|$

s.o. $\rightarrow$ $G/U$ ist eine Zerlegung von $G$

$\Rightarrow |G| = \sum_{A \in G/U} |A|$ Sei $R \subseteq G$ ein Repräsentantensystem von $G/U$. Dann gilt

$$|G| = \sum_{g \in R} |gU| \overset{\text{Prop (2.14)}}{=} \sum_{g \in R} |U| = |R| \cdot |U|$$

$= (G:U)|U|$. $\square$

# Folgerung aus dem Satz von Lagrange

**Satz (2.22)**

(i) Jede Gruppe von Primzahlordnung ist zyklisch.

(ii) Sei $G$ eine Gruppe, und seien $U, V \subseteq G$ endliche Untergruppen teilerfremder Ordnung. Dann gilt $U \cap V = \{e_G\}$.

# Beweis von Satz 2.22

zu i) Sei $G$ eine endl. Gruppe, $p$ eine Primzahl mit $|G| = p$.

$|G| \geq 2 \Rightarrow \exists\, g \in G \setminus \{e\}$ Behi: $G = \langle g \rangle$

Wende den Satz v. Lagrange auf $U = \langle g \rangle$ an. $\longrightarrow$

$|U| \mid |G| \Rightarrow |U| \mid p \Rightarrow |U| \in \{1, p\}$

1. Fall: $|U| = 1$, d.h. $U = \{e\}$ $\lightning$ da $g \in U$ und $g \neq e$

2. Fall: $|U| = p$ $\quad |U| = p = |G|$, $U \leq G \Rightarrow U = G$

zu ii) Seien $U, V \leq G$ wie angegeb. $m = |U|$, $n = |V| \longrightarrow$

$\mathrm{ggT}(m, n) = 1$ nach Vor. $\quad U \cap V \leq U$ und $U \cap V \leq V$

$\Rightarrow U \cap V$ ist Untergruppe von $U$ und von $V$

Lagrange $\Rightarrow |U \cap V| \mid m$ und $|U \cap V| \mid n$

$\Rightarrow |U \cap V| \mid ggT(m, n) \Rightarrow |U \cap V| = 1$

$\Rightarrow U \cap V = \{e\}$. □

**Definition (3.1)**

Sei $G$ eine Gruppe.

- Die Anzahl $|G|$ der Elemente von $G$ wird die Ordnung von $G$ genannt.
- Ist $g \in G$ ein beliebiges Element, dann bezeichnen wir $\operatorname{ord}(g) = |\langle g \rangle|$ als die Ordnung von $g$.

Aus dem Satz von Lagrange folgt unmittelbar, dass für jedes $g \in G$ einer endlichen Gruppe $G$ die Elementordnung $\operatorname{ord}(g)$ stets ein Teiler der Gruppenordnung $|G|$ ist.

# Die Elemente einer zyklischen Gruppe

**Lemma (3.2)**

Sei $G$ eine Gruppe, $g \in G$ und $m \in \mathbb{N}$ mit $g^m = e_G$. Dann ist die von $g$ erzeugte Untergruppe gegeben durch

$$\langle g \rangle \quad = \quad \{g^r \mid 0 \leq r < m\}.$$

Beweis von Lemma 3.2:

geg.: Gruppe $G$, $g \in G$, $m \in \mathbb{N}$ mit $g^m = e$

z.zg.: $\{g^e \mid e \in \mathbb{Z}\} = \{g^r \mid 0 \leq r \leq m-1\}$

„$\supseteq$" offensichtlich „$\subseteq$" Sei $e \in \mathbb{Z}$. z.zg.: $g^e = g^r$ für ein $r \in \{0, 1, \ldots, m-1\}$ Division mit Rest $\Rightarrow \exists\, q, r \in \mathbb{Z}$ mit $e = qm + r$, wobei $r \in \{0, 1, \ldots, m-1\}$

$$\Rightarrow g^e = g^{qm+r} = g^{qm} \cdot g^r = (g^m)^q \cdot g^r = e^q \cdot g^r$$
$$= e \cdot g^r = g^r$$

□