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 $g \in G$.

Erinnerung Sei X eine Menge.

Zerlegung von X = Teilmenge $\mathcal{Z} \subseteq \mathcal{P}(X)$ (also ein System von Teilmengen von X), so dass gilt

(i) $\emptyset \notin \mathcal{Z}$

(ii) $\bigcup_{A \in \mathcal{Z}} A = X$

(iii) $A, B \in \mathcal{Z}, A \neq B \Rightarrow A \cap B = \emptyset$

äquivalent zu (ii) $\wedge$ (iii). Jedes $x \in X$ ist in genau einem $A \in \mathcal{Z}$ enthalten.

Bsp: $X = \{1,2,3,4,5\} \Rightarrow \mathcal{Z} = \{\{1,3\},\{2,4,5\}\}$ ist

eine Zerlegung

ebenso. $G = S_3$, $U = \langle (12) \rangle$

$G/U = \{ \{id, (12)\}, \{(13), (123)\}, \{(23), (132)\} \}$

$U \backslash G = \{ \{id, (12)\}, \{(13), (132)\}, \{(23), (123)\} \}$

sind beides Zerlegungen von G.

Zerlegungen und Äquivalenzrelationen

Äquivalenzrelation auf einer Menge X = reflexive, symmetrische und transitive Relation auf X

bekannt:

(1) Ist $\equiv$ eine Äquivalenzrelation auf einer Menge X, dann bilden die Äquivalenzklassen bzgl $\equiv$ eine Zerlegung von X. formal:

Äquivalenzklasse von x: $[x] = \{y \in X \mid x \equiv y\}$

$\Rightarrow Z = \{ [x] \mid x \in X \}$ ist Zerlegung von X

(2) Ist umgekehrt Z eine Zerlegung von X, dann ist durch $x \equiv_Z y \Longrightarrow \exists A \in Z$ mit $x, y \in A$ eine Äquivalenzrelation auf X definiert.

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:

geg.: Gruppe G, Untergruppe U, $g, h \in G$ mit $h \in gU$. z.zg.: $gU = hU$

„$\supseteq$" Sei $k \in hU \Rightarrow \exists u \in U$ mit $k = hu$.

$h \in gU \Rightarrow \exists v \in U$ mit $h = gv$

einsetzen $\Rightarrow k = hu = (gv)u = g(uv)$

U Untergr., $u, v \in U \Rightarrow uv \in U$

$k = g(uv)$, $uv \in U \Rightarrow k \in gU$

„$\subseteq$" Sei $k \in gU \Rightarrow \exists u' \in U$ mit $k = gu'$

$h = gv \Rightarrow g = hv^{-1}$ einsetzen $\Rightarrow$

$k = gu' = (hv^{-1})u' = h(v^{-1}u')$

$u', v \in U \overset{U \text{ Untergr.}}{\Rightarrow} u', v^{-1} \in U \overset{U \text{ Untergr.}}{\Rightarrow} v^{-1}u' \in U$

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

$\square$

Beweis von Satz 2.16:

Sei G eine Gruppe, U Untergruppe von G. z.zg:

(1) G/U, $U\backslash G$ sind Zerlegungen von G

(2) Die Zerlegung G/U bzw. $U\backslash G$ ist gegeb. durch $\equiv_l$ bzw. $\equiv_r$ wobei $g \equiv_l h \iff h \in gU$ und $g \equiv_r h \iff h \in Ug$, $\forall g, h \in G$.

Führe den Beweis nur für G/U und $g \equiv_l h$

zu (1) zu überprüfen: (i) $\forall A \in G/U : A \neq \emptyset$

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

$A \cap B \neq \emptyset \Rightarrow A = B$

zu (i) Sei $A \in G/U \Rightarrow \exists g \in G$ mit $A = gU$

Wegen $e_G \in U$ gilt $g = g \cdot e_G \in gU \overset{A=gU}{\Rightarrow} A \neq \emptyset$

zu (ii) „$\supseteq$" klar, da jedes $A \in G/U$ nach Def. eine Teilmenge von G ist

„$\subseteq$" Sei $g \in G$. Dann gilt $g \in gU$ und $gU \in G/U$, siehe oben.

zu (iii) 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 $A = gU$, $B = hU$

$A \cap B \neq \emptyset \Rightarrow \exists k \in A \cap B$

$k \in gU \overset{\text{Lem 2.15}}{\Rightarrow} kU = gU$ $\quad k \in hU \overset{2.15}{\Rightarrow} kU = hU$

$\Rightarrow A = gU = kU = hU = B$

zu (2) Sei $g \in G$. zu zeigen: Die Äquivalenzklasse $[g]_l$ von g bzgl. $\equiv_l$ stimmt überein mit gU.

Nachweis von $[g]_l = gU$:

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

„$\supseteq$" $h \in gU \Rightarrow g \equiv_l h \Rightarrow h \in [g]_l$ □

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

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

zu zeigen: R' ist ein Repräsentantensystem von $U \backslash G$

Sei $Uh \in U \backslash G$ vorgegeben. z.zg.: Uh enthält genau ein Element aus R'

Betrachte $h^{-1}U \in G/U$. Da R ein Repr.-system von G/U ist, existiert ein $g \in R$ mit $g \in h^{-1}U$.

$g \in h^{-1}U \Rightarrow \exists u \in U$ mit $g = h^{-1}u \Rightarrow$

$g^{-1} = (h^{-1}u)^{-1} = u^{-1}(h^{-1})^{-1} = u^{-1}h \in Uh$

insgesamt: $g^{-1} \in R'$ (da $g \in R$) und $g^{-1} \in Uh$

($\Rightarrow$ Existenz)

zu Eindeutigkeit: Ang Uh enthält zwei Elemente aus R'. $\Rightarrow \exists\, g, g_1 \in R$ mit $g^{-1} \in Uh$ und $g_1^{-1} \in Uh$

$g^{-1} \in Uh \Rightarrow \exists u \in U$ mit $g^{-1} = uh$

$g_1^{-1} \in Uh \Rightarrow \exists v \in U$ mit $g_1^{-1} = vh$

$\Rightarrow g = (uh)^{-1} = h^{-1}u^{-1} \in R^{-1}U$, ebenso $g_1 \in h^{-1}U$

$g, g_1 \in h^{-1}U$, $g, g_1 \in R$, R ist Repr-system von G/U

Eindeutigkeit $\Rightarrow g = g_1 \Rightarrow g^{-1} = g_1^{-1}$

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

(1) Surjektivität:

Ist $h \in R'$, dann gilt $h = g^{-1}$ für ein $g \in R$. Es folgt $\phi(g) = h$.

(2) Injektivität:

Seien $g, g' \in R$ mit $\phi(g) = \phi(g')$. Dann folgt $g^{-1} = (g')^{-1}$. Durch Übergang zum Inversen auf beiden Seiten erhalten wir $g = g'$.

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 des Satzes von Lagrange

geg.: endliche Gruppe G, Untergruppe U

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

Verwende: Ist X eine endliche Menge und Z eine Zerlegung von X, dann gilt

$$|X| = \sum_{A \in Z} |A|$$

Sei R ein Repräsentantensystem von G/U

Dann gilt

$$|G| = \sum_{A \in G/U} |A| = \sum_{g \in R} |gU| \overset{\text{Lemma 2.14}}{=}$$

$\uparrow$ G/U ist Zerlegung von G

$$\sum_{g \in R} |U| = |R| \cdot |U| = |G/U| \cdot |U|$$

↑ auf Grund der Bijektion $R \to G/U$

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

□

Bem.: Ist G eine endliche Gruppe, dann gilt:

Ordnung von G = Mächtigkeit von G =

$|G|$ = Elementezahl von G

Z

mma 2.14

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 Prop. 2.22

zu i) Vor. G Gruppe, $p = |G|$ ist Primzahl

z.Zg. G ist zyklisch, d.h. $\exists g \in G : G = \langle g \rangle$

Sei $g \in G \setminus \{e\}$ (existiert, da $|G| = p \geq 2$).

betrachte $U = \langle g \rangle$. Satz von Lagrange $\Rightarrow$

$|G| = (G:U) \cdot |U|$. Da p Primzahl ist,

p

gilt $|U| = p$ oder $|U| = 1$. Ang. $|U| = 1$ $\Rightarrow$

$U = \{e\}$ $\lightning$ denn: $g \in \langle g \rangle \Rightarrow g \in U$, und $g \neq e$

also: $|U| = p = |G| \overset{U \leq G}{\Rightarrow} G = U = \langle g \rangle$

zu (ii) gegeben: G Gruppe, U, V Untergruppen

Vor.: $|U|$ und $|V|$ sind teilerfremd

z.Zg.: $U \cap V = \{e\}$

Betrachte $W = U \cap V$. bekannt: Mit U und V ist auch W eine Untergruppe von G.

W Untergr. von G, $W \leq U \Rightarrow$ W ist Untergruppe von U

Lagrange angewendet auf die Gruppe U und die Untergruppe W

$\Rightarrow |W| \mid |U|$ genauso erhält man $|W| \mid |V|$

$|W| \mid |U|, |W| \mid |V|, |U|, |V|$ sind teilerfremd $\Rightarrow |W| = 1$

$\Rightarrow U \cap V = W = \{e\}$

□

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 $\mathrm{ord}(g) = |\langle g \rangle|$ als die Ordnung von g.