

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

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

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 .

Lemma (2.14)

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

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

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

Notation: $U \leq G$ bedeutet: U ist Untergruppe der Gruppe G

Zerlegung einer Menge X = Mengensystem $\mathcal{Z} \subseteq \mathcal{P}(X)$
mit den Eigenschaften (i) $\emptyset \notin \mathcal{Z}$ (ii) $\bigcup_{A \in \mathcal{Z}} A = X$
(iii) $\forall A, B \in \mathcal{Z} : A \cap B \neq \emptyset \rightarrow A = B$

Zuordnung $\{ \text{Äquivalenzrel. auf } X \} \rightarrow \{ \text{Zerlegungen von } X \}$
Jeder Äquivalenzrel. wird die Menge der Äquivalenzklassen zugeordnet

Ist umgekehrt $\mathcal{Z}$ eine Zerlegung von X , dann ist durch
 $x \equiv_{\mathcal{Z}} y \iff \exists A \in \mathcal{Z} : x \in A \wedge y \in A$ eine Äquivalenzrel. 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 , $U \leq G$, $g, h \in G$ mit $h \in gU$

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

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

$$\stackrel{\text{so}}{\Rightarrow} k = (gu)u' = g(\underbrace{uu'}_{\in U}) \Rightarrow k \in gU$$

" $\subseteq$ " $h = gu \Rightarrow hu^{-1} = g$ Sei $k \in gU \Rightarrow$

$$\exists u'' \in U \text{ mit } k = gu'' \Rightarrow k = (hu^{-1})u'' = h(\underbrace{u^{-1}u''}_{\in U})$$

$$\Rightarrow k \in hU$$

□

Beweis von Satz 2.16 :

geg : Gruppe G , $U \leq G$

G/U Menge der Linksebenklassen von U

z.zg: G/U ist eine Zerlegung von G

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

$$(ii) G = \bigcup_{A \in G/U} A$$

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

zu (i) Jedes $A \in G/U$ hat die Form $A = gU$

für ein $g \in G$. $e \in U \Rightarrow g \cdot e \in A$

$$\Rightarrow g \in A \Rightarrow A \neq \emptyset$$

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

" $\subseteq$ " Sei $g \in G \Rightarrow g \in gU (g.o.)$, und $gU \in A$
 $\Rightarrow g \in \bigcup_{A \in G/U} A$

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 $A = gU, B = hU$ $A \cap B \neq \emptyset \Rightarrow$

$\exists k \in G$ mit $k \in A$ und $k \in B$

$$k \in gU \xrightarrow{(2.15)} kU = gU$$

$$k \in hU \xrightarrow{(2.15)} kU = hU$$

zusammen: $A = gU = kU = hU = B$

Sei $\equiv_l$ die Relation auf G geg.
durch $g \equiv_l h \iff h \in gU$.

U ~~z.z.~~ Für jedes $g \in G$ ist gU genau die
Äquivalenzklasse $[g]_l$, von g bzgl. $\equiv_l$.

Seien $g, h \in G$. Dann gilt die Äquivalenz

$$h \in [g]_l \iff g \equiv_l h \iff h \in gU$$

[Def der Äquivalenzklasse

Also gilt tatsächlich $[g]_l = gU$. □

$$A = B$$

$$= gU$$

A

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 $R \rightarrow X/\equiv$, $x \mapsto [x]$ eine **bijektive** Abbildung gegeben ist. Mit anderen Worten, in jeder Äquivalenzklasse ist genau ein Element aus R enthalten.

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 Repräsentantesystem der Rechtsnebenklassen, und durch $g \mapsto g^{-1}$ ist eine Bijektion zwischen R und R' definiert.

Beweis von Prop. 2.18 :

geg. G Gruppe, U Untergruppe

R Repräsentantensystem von G/U

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

Beh. R' ist ein Repräsentantensystem von $U \backslash G$

zu überprüfen:

(i) Jede Menge $A \in U \backslash G$ enthält mindestens ein Element aus R' .

(ii) Jedes $A \in U \backslash G$ enthält höchstens ein Element aus R' .

zu i) Sei $A \in U \setminus G$ und $g \in G$ mit $A = Ug$.

z.zg: $\exists h \in R'$ mit $h \in A$

Betrachte $g^{-1}U \in G/U$. R ist Repr.-system von G/U

$\Rightarrow \exists h_1 \in R$ mit $h_1 \in g^{-1}U$ $h_1 \in R \Rightarrow h = h_1^{-1}$ liegt in R'

$h_1 \in g^{-1}U \Rightarrow \exists u \in U$ mit $h_1 = g^{-1}u \Rightarrow h = h_1^{-1} = (g^{-1}u)^{-1}$
 $= u^{-1}g \Rightarrow h \in Ug \Rightarrow h \in A$

zu ii) Sei $A \in U \setminus G$ und $g \in G$ mit $A = Ug$.

Seien $h, h' \in A$ mit $h, h' \in R'$ z.zg. $h = h'$

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

$\Rightarrow h^{-1} = g^{-1}u^{-1}, (h')^{-1} = g^{-1}(u')^{-1} \Rightarrow h^{-1}(h')^{-1} \in g^{-1}U$

Aus $h, h' \in R'$ folgt $h^{-1}, (h')^{-1} \in R$.

$h^{-1}, (h')^{-1} \in R, h^{-1}, (h')^{-1} \in g^{-1}U$, R ist Repr.-system
von $G/U \rightarrow h^{-1} = (h')^{-1} \Rightarrow h = h'$

Offenbar ist $R' \rightarrow R, h \mapsto h^{-1}$ die Umkehrabb.
von $R \xrightarrow{\phi} R', g \mapsto g^{-1}$. Also ist ϕ eine Bijektion zwischen
 R und R' . $\square$

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: endliche Gruppe G , $U \leq G$

z.zg: $|G| = (G:U) \cdot |U|$, wobei $(G:U)$ die Anzahl der Linksebenenklassen angibt.

Sei $R \subseteq G$ ein Repräsentantensystem von G/U .

Dann gilt $|R| = (G:U)$, und außerdem

$$|G| = \sum_{A \in G/U} |A| = \sum_{g \in R} |gU| \stackrel{(2.14)}{=} \sum_{g \in R} |U|$$

$\uparrow$
 G/U ist Zerlegung
von G

$$\sum_{g \in R} |U| = |R| \cdot |U| = (G:U) |U|.$$

□

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 $U \cap V = \{e_G\}$.

Dann gilt $|R| = (G:U)$, und außerdem
 $|R| = \sum |A| = \sum |e|U| \stackrel{(2.14)}{=} |U|$

Beweis von Satz 2.22

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

Beh. G ist zyklisch, d.h. $\exists g \in G$ mit $G = \langle g \rangle$

Sei $g \in G \setminus \{e\}$ (existiert wegen $|G| > 1$)

$\langle g \rangle$ ist Untergruppe von $G \xRightarrow{\text{Lagrange}} |\langle g \rangle|$ teilt $p = |G|$

$\rightarrow |\langle g \rangle| \in \{1, p\}$ $|\langle g \rangle| = 1$ ist ausgeschlossen, da

$e, g \in \langle g \rangle$ verschieden sind also: $|\langle g \rangle| = p = |G|$

$\langle g \rangle \subseteq G$
 $\xRightarrow{|\langle g \rangle| = |G|} G = \langle g \rangle$

zu ii) Seien U, V Untergruppen einer Gruppe G , endlich mit teilerfremden Ordnungen $|U|$ und $|V|$. Beh.: $U \cap V = \{e_G\}$

Mit U und V ist auch $U \cap V$ eine Untergruppe von G , wegen $U \cap V \subseteq U$ auch eine Untergruppe von U . Lagrange $\Rightarrow |U \cap V|$ teilt $|U|$
analog: $|U \cap V|$ teilt $|V|$. $|U|, |V|$ teilerfremd $\Rightarrow |U \cap V| = 1 \Rightarrow U \cap V = \{e_G\}$



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