U *Untergruppe von* G

$a \in aU := \{au \mid u \in U\}$ **linke Nebenklasse** von U

$a \in Ua := \{ua \mid u \in U\}$ **rechte Nebenklasse** von U

$\langle n \rangle$ Untergruppe von $\mathbb{Z}_n(+)$

$a + \langle n \rangle = \langle n \rangle + a$ Kongruenzklasse mod A

$$\rho_n(a + in) = \rho_n(a)$$

---

1) $aU = bU \quad \Leftrightarrow \quad b \in aU \quad \Leftrightarrow \quad a^{-1}b \in U$

$a + \langle n \rangle = b + \langle n \rangle$

$b - a = 0 \bmod n$

$b - a \in \langle n \rangle$

$Ua = Ub \quad \Leftrightarrow \quad a^{-1} \quad \Leftrightarrow \quad ba^{-1} \in U$

2) $u \mapsto au$ Bijektion von U auf aU

$u \mapsto ua$ Bijektion von U auf Ua d.h. $|U| = |aU| = |Ua|$

↳ $\Rightarrow$ "gleichmächtig"

3) $G = \bigcup_{a \in G} aU \left(= \bigcup_{u \in G} Ua \right)$

4) Definiere auf G Äquivalenzrelation:

$a \sim_U b \quad \Leftrightarrow \quad ba^{-1} \in U$

i) $a \sim a$ (reflexiv)

ii) $a \sim b \quad \Rightarrow \quad b \sim a$ (symmetrisch)

iii) $a \sim b \sim c \quad \Rightarrow \quad a \sim c$ (transitiv)

$ba^{-1} \in U \quad cb^{-1} \in U \Rightarrow cb^{-1} \in U \Rightarrow cb^{-1}ba^{-1} = ca^{-1} \in U$

$a \equiv b \pmod n$

Äquivalenzklassen

$[a] := \{b \in G \mid a \sim_U b\} \qquad ba^{-1} \in U$

$[a] = Ua \quad b \in Ua,\ b \in aU,\ a^{-1}b \in U$

Die Äquivalenzklassen bilden ein **Partition**, da Menge G:

$$G = \bigcup_{a \in G} Ua$$

4.3. Satz von Lagrange

Sei G eine endliche Gruppe (d.h. $|G| < \infty$) und U Untergruppe von G.

Dann ist $|U|$ Teiler von $|G|$.

Genauer:

Die Anzahl der NK Ua von U in G ist $\frac{|G|}{|U|}$.

Index von U in $G = |G:U| = \frac{|G|}{|U|}$

$|G| = |G:U| \cdot U$

Sei $\varphi: G \to H$ Homomorphismus

$(\varphi: R \to S \quad (\text{Ringhomomorphismus}))$

Kein $\varphi := \{a \in G \mid \varphi(a) = 1_U\}$

(Kein $\varphi := \{a \in R \mid \varphi(a) = 0\}$)

4.4. a) Kein φ ist Untergruppe von G

(Kein φ ist Ideal von R)

Beispiel:

$\rho_n: \mathbb{Z} \to \mathbb{Z}_n$ Homomorphismus

$\ker \rho_n = \langle n \rangle$ (Menge der Vielfachen)

denn $a, b \in \ker \varphi$

$\varphi(a, b^{-1}) = \varphi(a)\varphi(b)^{-1} = 1 \cdot 1 = 1$

$\varphi: R \to S$

$\ker \varphi$ ist Untergruppe von $R(+)$

$a \in \ker \varphi, \ r \in R$

$\varphi(r \cdot a) = \varphi(r) \cdot \varphi(a) = \varphi(r) \cdot 0 = 0$

$(r \in R, \ a \in I \ (\text{Ideal}) \Rightarrow r \cdot a \in I, \ a \cdot r \in I)$

b) Sei $a \in G$ und $U = \ker \varphi$

$\{b \in G \mid \varphi(b) = \varphi(a)\} = Ua \overset{!}{=} a \cdot U$

Beweis:

$\varphi(a) = \varphi(b) \Leftrightarrow \varphi(a)^{-1}\varphi(b) = 1$

$\varphi(a^{-1}) \cdot \varphi(b) = 1$

$\varphi(a^{-1}b) = 1$

$\Leftrightarrow a^{-1}b \in U \quad \Leftrightarrow \quad aU = bU$

$$\varphi(a)=\varphi(b) \quad \Leftrightarrow \quad \varphi(a)\varphi(b^{-1})=1$$
$$\Leftrightarrow \; ab^{-1}\in U \quad \Leftrightarrow \quad Ua=Ub$$

c) φ ist injektiv $\Leftrightarrow$ $\ker\varphi=1$

$\varphi(a)=\varphi(b) \Leftrightarrow aU=bU$ bzw. $Ua=Ub$

Definition: Eine Untergruppe N von G heißt **Normalteiler** von G,
wenn $aN=Na \;\; \forall a\in G$. (falls abelsch sind die UG immer Normalteiler)

- Sei G abelsch, U ist Untergruppe $\Rightarrow U$ ist Normalteiler
- Sei φ Homomorphismus: $\ker\varphi$ ist Normalteiler von G

Bemerkung: $A,B,C\subseteq G$

$AB:=\{ab\,|\,a\in A,b\in B\}$ Komplexprodukt

$(AB)\cdot C=A\cdot(BC)$ (assoziativ)

$(ab)\cdot c=a\cdot(bc)$

N sei Nullteiler von G

Definition der Faktorgruppe G/N:

$G/N:=\{aN\,|\,a\in G\}$

Multiplikation: $(aN)\cdot(bN)=a\underbrace{(Nb)}_{\text{NT}\Rightarrow=bN}N=a(bN)N=ab\cdot NN=ab\cdot N$

Definition:

$(aN)(bN)\overset{\text{def.}}{=}(ab)N$ (wohldefiniert)

4.5. Bezüglich diesem Produkt ist G/N Gruppe

Beweis:

- Assoziativ $(aNbN)(cN)=(abN)(cN)=(ab)cN$
- Einselement $=1N=N$
- Inverses Element $(aN)^{-1}=a^{-1}N$

Beispiel:

$\langle n\rangle$ ist NT von $\mathbb{Z}(+)$

$\mathbb{Z}(+)/\langle n\rangle\cong\mathbb{Z}_n=\{0,1,....,n-1\}$

$(a+\langle n\rangle)+(b+\langle n\rangle)=(a+b)+\langle n\rangle$

Allgemeine Betrachtung:

U Untergruppe von G. Eine Teilmenge G_U heißt **(Links-)Repräsentantensystem** von U in G, wenn G_U aus jeder Nebenklasse aU genau ein Element r_a enthält.

Normiert: $r_a = 1$, wenn $a \in U$

Versuch: Definiere Multiplikation auf G_U

$$r \cdot_U s = t \overset{\text{def.}}{\Leftrightarrow} r \cdot s \in tU$$

"Loop" (1)+(2) gelten, 3) nicht! ⇒Gruppe ohne Assoziativgesetz)

1) neutrales Element 1 $\quad r \in rU$

2) inverses Element: Sei $s \in G_U$ mit $r^{-1} \in sU$, $r^{-1} = su$

3) Assoziativgesetz gilt im Allgemeinen nicht, nur wenn U NT ist.

4.6. Sei N NT von G. Dann ist die Abbildung:

$\psi : G \to G/N$ mit $a \mapsto aN$

Gruppenhomomorphismus

$$\psi(a)\psi(b) = (aN)(bN) = (ab)N = \psi(ab)$$

und es ist $\ker \psi = N$

$$\psi(a) = N \quad aN = N \Leftrightarrow a \in N$$

Insbesondere gilt:

- Normalteiler sind die Kerne der Homomorphismen

4.7. **Homomorphiesatz**

Sei $\varphi : G \mapsto H$ Homomorphismus und $N = \ker \varphi$ $(\to \text{NT})$

Dann ist: $\varphi : G/N \to H$ mit $aN \mapsto \varphi(a)$ wohldefiniert, injektiv und Homomorphismus

d.h. $G/N \overset{\cong}{\underset{\uparrow}{}} \operatorname{im} \varphi$ (↑ Isomorphismus)

Beispiel:

$\rho_n : \mathbb{Z}(+) \to \mathbb{Z}_n(+)$ surjektiv

$\rho_n(a+b) = \rho_n(a) +_n \rho_n(b)$ Homomorphismus

$\ker \rho_n = \langle n \rangle$

$\mathbb{Z}/\langle n \rangle \cong \mathbb{Z}_n$