Vorlesung Algebra

SoSe'21, hhu
K. Halupczok

Teil I: GRUPPEN

A2: Untergruppen, Faktorgruppen

Stichworte: Def. Untergruppe, Zentrum, UGen von $\mathbb{Z}$, die von S erzeugte UG $\langle S\rangle$, zyklische Gruppe, Links-/Rechts-nebenklassen, Index, Satz von Lagrange, Normalteiler, Faktorgruppe G/N, Faktorgruppen von $\mathbb{Z}$ = Restklassengruppen, Kommutator UG

2.1. Einleitung: Gewisse Konzepte von "Unterstrukturen", die z.B. von Untervektorräumen bekannt sind, lassen sich auf die Theorie der Untergruppen übertragen. Bei der Quotientenbildung, analog den Quotientenvektorräumen, ist etwas anders: man benötigt Normalteiler zur Definition von Faktorgruppen. Die Faktorgruppen von $\mathbb{Z}$ sind genau die aus linearer Algebra/elementarer Zahlentheorie bekannten Restklassengruppen in $\mathbb{Z}$. Die Kommutator UG liefert eine Möglichkeit zur "Abelisierung" nichtabelscher Gruppen, vgl. Ü.

2.2. Def.: Sei G Gruppe. $H \subseteq G$ heißt Untergruppe (UG), falls

$$\left.\begin{cases} \text{(i) } e \in H \\ \text{(ii) } a, b \in H \Rightarrow ab,\ a^{-1} \in H \end{cases}\right\} \Leftrightarrow (a, b \in H \Rightarrow ab^{-1} \in H) \wedge H \neq \emptyset$$

2.3. Bsp.: $\{e\}$, G sind UG von G (schreibe auch e statt $\{e\}$!)

2.4. Bsp.: Sei G Gruppe, dann:

$$Z = Z(G) := \{a \in G;\ \forall b \in G : ab = ba\} \quad \text{Zentrum von } G,$$

ist UG von G,

Bew.: $a, b \in Z \Rightarrow \forall c \in G: ab^{-1}c = a(c^{-1}b)^{-1} = a(bc^{-1})^{-1}$
$= acb^{-1} = cab^{-1}$, d.h. $ab^{-1} \in Z$. □

Es gilt: $Z(G) = G \Leftrightarrow G$ abelsch.

2.5. Bsp.: Seien $H_i \subseteq G$ UG $(i \in I)$ von G.

Dann ist $H := \bigcap_{i \in I} H_i$ UG von G.

2.6. **Bsp.:** Die UG von $\mathbb{Z}$:

Sei $0 \neq A \subseteq \mathbb{Z}$ UG von $\mathbb{Z}$,
und $n_0 \in \mathbb{N}$ die kleinste nat. Zahl mit $n_0 \in A$.

Beh.: $A = n_0\mathbb{Z}$ $(:= \{n_0 k;\ k \in \mathbb{Z}\})$

Bew.: „$\supseteq$": ✓ wegen Abgeschl. bzgl. + und Inversenbildung

„$\subseteq$": Sei $a \in A$. Division mit Rest A0.5: $a = m n_0 + r$,
mit $0 \le r < n_0$. Dann:

$r = \underset{A}{\underset{\cap}{a}} - \underset{A}{\underset{\cap}{m n_0}} \in A$, ↯ zur Wahl von n_0, wenn $r \neq 0$ wäre.

Somit: $a = m n_0 \in n_0\mathbb{Z}$. □

Resultat: Die UG von $\mathbb{Z}$ sind genau die Mengen $n\mathbb{Z}$, $n \in \mathbb{N}_0$.

2.7. **Def.:** Sei G Gruppe, $S \subseteq G$ Menge.

$\langle S \rangle := \bigcap_{\substack{H \subseteq G \text{ UG}, \\ S \subseteq H}} H$ heißt die von S erzeugte UG.

2.8. **Lemma:** (i) $\langle S \rangle$ ist die kleinste UG von G, die S umfasst.

(ii) $a \in \langle S \rangle \iff \exists\, n \in \mathbb{N}\ \exists\, s_1, \dots, s_n \in S\ \exists\, \varepsilon_1, \dots, \varepsilon_n \in \{1, -1\}$:

$$a = s_1^{\varepsilon_1} \cdot \ldots \cdot s_n^{\varepsilon_n} \qquad (\!(*)\!)$$

Bew.: (i): Sei $H \subseteq G$ UG mit $S \subseteq H$ $\Rightarrow$ $\langle S \rangle \subseteq H$ nach 2.7.

(ii): „$\Leftarrow$": Jedes a der Gestalt $(\!(*)\!)$ ist in $\langle S \rangle$,
da $\langle S \rangle$ eine UG ist, die S umfasst.

„$\Rightarrow$": Sei $H := \{a \in G;\ a \text{ hat Darst. } (\!(*)\!)\}$, zeigen: $\langle S \rangle \subseteq H$.
zeige dazu nur: H ist UG mit $S \subseteq H$.

Denn: $a, b \in H$, $a = s_1^{\varepsilon_1} \cdot \ldots \cdot s_n^{\varepsilon_n}$, $b = t_1^{\delta_1} \cdot \ldots \cdot t_m^{\delta_m}$

$\Rightarrow a b^{-1} = s_1^{\varepsilon_1} \cdot \ldots \cdot s_n^{\varepsilon_n} \cdot t_m^{-\delta_m} \cdot \ldots \cdot t_1^{-\delta_1} \in H$. □

2.9. Kor.: Sei G abelsche Gruppe, $S := \{a_1, \dots, a_n\} \subseteq G$. Dann:
$$\langle S \rangle = \{a_1^{k_1} \cdot \ldots \cdot a_n^{k_n};\ k_1, \dots, k_n \in \mathbb{Z}\} \quad \text{(mult.)}$$
bzw. $\langle S \rangle = \{k_1 a_1 + \ldots + k_n a_n;\ k_1, \dots, k_n \in \mathbb{Z}\}$ (add.)

Bew.: „$\supseteq$": ✓ nach Lemma 2.8.

„$\subseteq$": $H = $ r.S.$^{\ni e}$ ist UG, die S umfasst: $a, b \in H$
$$\Rightarrow a b^{-1} = a_1^{k_1} \cdot \ldots \cdot a_n^{k_n} \cdot (a_1^{l_1} \cdot \ldots \cdot a_n^{l_n})^{-1} = a_1^{k_1} \cdot \ldots \cdot a_n^{k_n} \cdot a_n^{-l_n} \cdot \ldots \cdot a_1^{-l_1}$$
$$= a_1^{k_1 - l_1} \cdot \ldots \cdot a_n^{k_n - l_n} \in H.$$
Somit $\langle S \rangle \subseteq H$. $\square$

2.10. Def.: Gruppe G zyklisch $:\Leftrightarrow \exists a \in G$ mit $G = \langle a \rangle$ $(= \langle \{a\} \rangle)$.

2.11. Bsp.: In $\mathbb{Z}$: $\langle 1 \rangle = \{m \cdot 1;\ m \in \mathbb{Z}\} = \mathbb{Z} \cdot 1 = \mathbb{Z}$, d.h. $\mathbb{Z}$ ist zyklisch.

2.12. Lemma: Sei $G = \langle a \rangle = \{a^k;\ k \in \mathbb{Z}\}$. Dann gilt:

(i) G ist abelsch,

(ii) $\operatorname{ord}(a) = n \Rightarrow \# G = n$ und $G = \{e = a^0, a = a^1, a^2, \dots, a^{n-1}\}$.

Bew.: (i): $a^k \cdot a^l = a^{k+l} = a^{l+k} = a^l \cdot a^k$ für alle $k, l \in \mathbb{Z}$

(ii): Für $l \in \mathbb{Z}$: $l = mn + r$, $0 \leq r < n \Rightarrow a^l = a^{mn+r} = (a^n)^m a^r = a^r$

$\Rightarrow \# G \leq n$, $G = \{\dots\}$.

Sei $a^i = a^j$, $0 \leq i \leq j < n \underset{A1.21}{\Rightarrow} n \mid (j - i)$, $j - i < n \Rightarrow j - i = 0 \Rightarrow i = j$.

$\Rightarrow \# G \geq n$. $\square$

2.13. Def.: Sei G Gruppe, H UG von G, $a, b \in G$.

Dann: $a \underset{L}{\sim} b :\Leftrightarrow a^{-1} b \in H$.

2.14. Lemma: $\underset{L}{\sim}$ ist Äquivalenzrelation auf G.

Bew.: (i): $a \underset{L}{\sim} a$, da $a^{-1} a = e \in H$,

(ii): $a \underset{L}{\sim} b \Rightarrow a^{-1} b \in H \Rightarrow b^{-1} a \in H \Rightarrow b \underset{L}{\sim} a$,

(iii): $a \underset{L}{\sim} b \wedge b \underset{L}{\sim} c$

$a^{-1} b \in H \wedge b^{-1} c \in H \Rightarrow a^{-1} b b^{-1} c = a^{-1} c \in H \Rightarrow a \underset{L}{\sim} c$. $\square$

2.15. Lemma: $a \underset{L}{\sim} b \Leftrightarrow a^{-1} b \in H \Leftrightarrow b \in aH \Leftrightarrow a \in bH \Leftrightarrow aH = bH$.

2.16. **Def.:** aH heißt Linksnebenklasse von a mod H, analog: Ha Rechts...
$G/H := \{aH;\ a \in G\}$, $[G:H] := \#G/H$ Index von H in G.

2.17. **Satz:** $\#G = \#H \cdot [G:H]$ $(\Rightarrow \#H \mid \#G)$, falls $\#G$ endl.
Bew.: Nach 2.15: Die Äquivalenzklassen von $\sim$ sind genau die Linksnebenklassen.
Sei $a_1, \dots, a_q$ ein Repräsentantensystem für die Linksnebenklassen mod H,
also $G = a_1 H \,\dot\cup \dots \dot\cup\, a_q H$.
Betr. $\varphi: H \longrightarrow aH$
$h \mapsto ah$: φ ist injektiv, denn $ah_1 = ah_2 \Rightarrow h_1 = h_2$.
Daher haben alle Linksnebenklassen gleichviele Elemente, nämlich $\#H$.
Es folgt: $\#G = q \cdot \#H = \#H \cdot [G:H]$. □
„Satz von Lagrange"

2.18. **Kor.:** G endl. Gruppe. Dann: $\mathrm{ord}(a) \mid \#G$ (für bel. $a \in G$).
Bew.: $\mathrm{ord}(a) = \#\langle a\rangle \mid \#G$ nach 2.17. □

2.19. **Kor.:** G endl. Gruppe, $\#G = p$ prim $\Rightarrow G = \langle a\rangle$ mit bel. $a \neq e$, d.h. zyklisch.
Bew.: $e \subsetneq \langle a\rangle \subseteq G \Rightarrow \langle a\rangle = G$, da $1 < \#\langle a\rangle \mid \#G = p$ prim. □

2.20. **Def.:** $N \subseteq G$ UG von G heißt Normalteiler (NT), falls:
$\forall a \in G:\ aNa^{-1} = N$ $(\Leftrightarrow aN = Na)$.

2.21. **Bem.:** $ab = ba$ muss nicht notwendig gelten!
aHa^{-1} ist UG, wenn H UG: $(ah_1a^{-1})(ah_2a^{-1})^{-1} = ah_1a^{-1}ah_2^{-1}a^{-1}$
$= a(h_1h_2^{-1})a^{-1} \in aHa^{-1}$.

2.22. **Bsp.:** In G sind e, G stets NT.

2.23. **Bsp.:** G abelsch, H UG $\Rightarrow H$ NT.
Bew.: $\forall a \in G\ \forall b \in H:\ aba^{-1} = b \Rightarrow aHa^{-1} = H$. □

2.24. **Bsp.:** In G ist $Z(G)$ NT.
Bew.: $Z(G) = \{a \in G;\ \forall b \in G: \underbrace{ab = ba}_{\Leftrightarrow bab^{-1} = a}\} \Rightarrow aZ(G)a^{-1} = Z(G)$ für alle $a \in Z(G)$.
□

2.25 Satz: Sei G Gruppe, $N \leq G$ NT, $\cdot : G/N \times G/N \to G/N$

$$(aN, bN) \mapsto (ab)N$$

$\cdot$ ist wohldefiniert, $(G/N, \cdot, N)$ ist Gruppe.

Bew.: Wohldef.: Sei $a_1 N = a_2 N$, $b_1 N = b_2 N$

$\Rightarrow a_1^{-1} a_2 \in N$, $b_1^{-1} b_2 \in N$

$\Rightarrow (a_1 b_1)^{-1}(a_2 b_2) = \underbrace{b_1^{-1} \underbrace{a_1^{-1} a_2}_{\in N} (b_1}_{\in N,\text{ da } N \text{ NT}} \underbrace{b_1^{-1}) b_2}_{\in N} \in N$

$\Rightarrow (a_1 b_1)N = (a_2 b_2)N$

Gruppenaxiome: $((aN)(bN))(cN) = ((ab)N)(cN) = (a(bc))N$

$= (aN)((bc)N) = (aN)((bN)(cN))$,

$(eN)(aN) = (ea)N = aN$,

$(a^{-1}N)(aN) = (a^{-1}a)N = N \Rightarrow (aN)^{-1} = a^{-1}N$. □

2.26 Def.: $(G/N, \cdot, N)$ heißt Faktorgruppe von G nach N (auch: Quotientengruppe, G mod N, ...)

2.27 Bsp.: Die Faktorgruppen von $\mathbb{Z}$ (auch: "Restklassengruppen")

Die UG von $\mathbb{Z}$ sind genau die Gruppen $m\mathbb{Z}$ ($m \in \mathbb{N}_0$), vgl. Bsp. 2.6, diese sind nach Bsp. 2.23 auch NT.

* $\Rightarrow$ Die Faktorgruppen von $\mathbb{Z}$ sind genau die Gruppen
  $\mathbb{Z}/n\mathbb{Z} \overset{!}{=} \{\underline{0}, \underline{1}, \dots, \underline{n-1}\}$, wobei $\underline{i} := i + n\mathbb{Z}$.

  Bew. von "$\overset{!}{=}$": "$\subseteq$": Sei $m \in \mathbb{Z}$, $m = un + r$ mit $0 \leq r < n$

  $\Rightarrow m - r = un \in n\mathbb{Z} \Rightarrow \underline{m} = \underline{r} \Rightarrow m + n\mathbb{Z} = r + n\mathbb{Z}$

  "$\supseteq$": Sei $\underline{i} = \underline{j}$, $0 \leq j \leq i < n \Rightarrow i - j \in \mathbb{Z}n = \underline{0}$ $(0 \leq j - i < n) \Rightarrow i = j$. □

* Es ist $\underline{i} + \underline{j} = \underline{k}$ mit $\begin{cases} k = i+j, & \text{für } i+j < n, \\ k = i+j-n, & \text{für } i+j \geq n. \end{cases}$

* $\mathbb{Z}/n\mathbb{Z}$ ist zyklisch der Ordnung n.

  Bew.: $k \cdot \underline{1} = \underline{k} = \underline{0} \Leftrightarrow k - 0 = k \in n\mathbb{Z} \Leftrightarrow n \mid k$,

  d.h. $\underline{1}$ hat Ordnung n (vgl. A1.21) $\Rightarrow \mathbb{Z}/n\mathbb{Z} = \langle \underline{1} \rangle$. □

2.28. **Bsp.:** Def.: G Gruppe, $K(G) := \langle \{aba^{-1}b^{-1};\ a,b \in G\} \rangle$
heißt Kommutator UG, $c = aba^{-1}b^{-1} \in K(G)$ heißt Kommutator.

Lemma: $K(G)$ ist NT in G.

Bew.: Da $c^{-1} = (aba^{-1}b^{-1})^{-1} = bab^{-1}a^{-1}$,
ist jedes $k \in K(G)$ Produkt aus Kommutatoren.
Sei $K(G) \ni k = c_1 \cdot \ldots \cdot c_m$, $c_i = a_i b_i a_i^{-1} b_i^{-1}$ $(1 \leq i \leq m)$, $g \in G$.
$\Rightarrow gkg^{-1} = g c_1 \cdot \ldots \cdot c_m g^{-1} = (gc_1g^{-1})(gc_2g^{-1}) \cdot \ldots \cdot (gc_mg^{-1})$.
Nun: $gcg^{-1} = gaba^{-1}b^{-1}g = (gag^{-1})(gbg^{-1})(gag^{-1})^{-1}(gbg^{-1})^{-1} \in K(G)$
$\Rightarrow gkg^{-1} \in K(G) \Rightarrow gK(G)g^{-1} \subseteq K(G)$.
Ferner: $K = g^{-1}gkg^{-1}g \subseteq g^{-1}Kg \Rightarrow g^{-1}K(g^{-1})^{-1} \supseteq K \quad \forall g \in G$.
$\Rightarrow K(G) = g\,K(G)g^{-1}$. $\square$

Bem.: $G/K(G)$ ist abelsche Gruppe. Ü