WS 05/06
Priv.-Doz. Dr. S. Wewers
Andreas Martin

Algebra I

4. Übungsblatt

Aufgabe 1: (1+2+1=4 P)

(a) Sei G eine Gruppe und $H \lhd G$ ein Normalteiler. Zeigen Sie: H ist (als Menge) disjunkte Vereinigung von Konjugiertenklassen von G.

(b) Bestimmen Sie alle Konjugiertenklassen von A_5 (die Angabe eines Vertreters für jede Klasse reicht) und die Anzahl der Elemente jeder Klasse.

(c) Zeigen Sie: A_5 ist eine einfache Gruppe, d.h. $H = \{e\}$ und $H = A_5$ sind die einzigen Normalteiler. (Hinweis: benutzen Sie (a) und (b).)

Lösung:

(a) Es sei M die Menge aller Konjugiertenklassen von G, welche in H enthalten sind. Dann gilt offenbar

$$H \supseteq \bigcup_{C \in M} C \ .$$

Für jedes $h \in H$ und jedes $g \in G$ gilt andererseits, daß $ghg^{-1} \in gHg^{-1} = H$, also ist die Konjugiertenklasse $[h]_{\sim_G}$ von h ganz in H enthalten. Es folgt $h \in [h]_{\sim_G}$ und $[h]_{\sim_G} \in M$. Somit gilt sogar

$$H = \bigcup_{C \in M} C \ .$$

Die Vereinigung ist disjunkt, da zwei verschiedene Konjugiertenklassen stets disjunkt sind.

(b) Es gilt

$$A_5 = \{\sigma \in S_5 \mid Z(\sigma) \in \{[1,1,1,1,1],[1,2,2],[1,1,3],[5]\}\} \ .$$

Nach Blatt 2, Aufgabe 2, sind Elemente verschiedenen Zykeltyps nicht konjugiert. Außerdem zerfallen die Elemente vom Zykeltyp [5] in genau zwei Konjugiertenklassen in A_5, nämlich die Konjugiertenklasse von $(1\ 2\ 3\ 4\ 5)$ und die Konjugiertenklasse von $(1\ 2\ 3\ 5\ 4)$. Wir wollen zeigen, daß die Elemente vom Zykeltyp $[1,2,2]$ bzw. $[1,1,3]$ jeweils eine Konjugiertenklassen in A_5 bilden.

- Zykeltyp $[1,2,2]$: Es gilt für $a,b,c,d,e \in \{1,2,3,4,5\}$ paarweise verschieden
$$\begin{aligned} (b\ c\ d)((a\ b)(c\ d))(b\ c\ d)^{-1} &= (a\ c)(b\ d) \ , \\ ((a\ b)(d\ e))((a\ b)(c\ d))((a\ b)(d\ e))^{-1} &= (a\ b)(c\ e) \ . \end{aligned}$$
Daher sind alle Elemente vom Zykeltyp $[1,2,2]$ konjugiert in A_5.
- Zykeltyp $[1,1,3]$: Es gilt für $a,b,c,d,e \in \{1,2,3,4,5\}$ paarweise verschieden
$$\begin{aligned} ((b\ c)(d\ e))(a\ b\ c)((b\ c)(d\ e))^{-1} &= (a\ c\ b) \ , \\ (c\ d\ e)(a\ b\ c)(c\ d\ e)^{-1} &= (a\ b\ d) \ . \end{aligned}$$
Daher sind alle Zykel vom Typ $[1,1,3]$ konjugiert in A_5.

Also gibt es folgende fünf Konjugiertenklassen in A_5.

Vertreter	Elementezahl
Id	1
(1 2)(3 4)	15
(1 2 3)	20
(1 2 3 4 5)	12
(1 2 3 5 4)	12

(c) Es sei $H \trianglelefteq A_5$ gegeben. Nach (a) ist H Vereinigung von Konjugiertenklassen. Nach (b) gilt also

$$|H| \;=\; 1 + 15\alpha + 20\beta + 12(\gamma + \delta)$$

für gewisse $\alpha, \beta, \gamma, \delta \in \{0, 1\}$. Für diese Summe gibt es somit 12 verschiedene Werte, diese sind

$$1, 13, 16, 21, 25, 28, 33, 36, 40, 45, 48, 60 \,.$$

Nun ist $|H|$ ein Teiler von $|A_5| = 60$. Daher kommt nur $|H| = 1$ oder $|H| = 60$ in Frage, und die Behauptung folgt.

Aufgabe 2: (1+1+2=4 P)

(a) Finden Sie ganze Zahlen $a, b \in \mathbb{Z}$ mit $5a + 7b = 1$.

(b) Sei $G = \mathbb{Z}\cdot 1/5 + \mathbb{Z}\cdot 1/7$ die von den Brüchen $1/7$ und $1/5$ erzeugte Untergruppe von $(\mathbb{Q}, +)$. Zeigen Sie, dass G eine zyklische Gruppe ist, und finden Sie einen Erzeuger.

(c) Zeigen Sie, dass die Gruppen $(\mathbb{Q}, +)$ und $(\mathbb{Q}^\times, \cdot)$ nicht endlich erzeugt sind.

Lösung:

(a) Mit dem Euklidischen Algorithmus wird

$$\begin{aligned} 7 &= 1 \cdot 5 + 2 \\ 5 &= 2 \cdot 2 + 1 \,. \end{aligned}$$

Somit ist

$$1 \;=\; 5 - 2 \cdot 2 \;=\; 5 - 2 \cdot (7 - 1 \cdot 5) \;=\; 3 \cdot 5 - 2 \cdot 7 \;=\; 5a + 7b$$

mit $a := 3$ und $b := -2$.

(b) Es gilt

$$G \;\ni\; b \cdot \frac{1}{5} + a \cdot \frac{1}{7} \;=\; \frac{5a + 7b}{35} \;=\; \frac{1}{35}$$

und somit $\mathbb{Z} \cdot \frac{1}{35} \subseteq G$. Andererseits ist offenbar

$$G \;=\; \mathbb{Z} \cdot \frac{1}{5} + \mathbb{Z} \cdot \frac{1}{7} \;\subseteq\; \mathbb{Z} \cdot \frac{1}{35} \,.$$

Somit folgt $G = \mathbb{Z} \cdot \frac{1}{35}$.

(c)
- Wir nehmen an, $(\mathbb{Q}, +)$ besäße ein endliches Erzeugendensystem

  $$\frac{m_1}{n_1} \,,\; \ldots \,,\; \frac{m_k}{n_k} \,,$$

  wobei $k \in \mathbb{N}$, $m_1, \ldots, m_k \in \mathbb{Z}$ und $n_1, \ldots, n_k \in \mathbb{N}$. Für jedes $z \in \mathbb{Q}$ gibt es also $r_1, \ldots, r_k \in \mathbb{Z}$ so, daß

  $$z \;=\; \sum_{i=1}^{k} r_i \, \frac{m_i}{n_i} \,.$$

  Mit $n := n_1 \cdot \ldots \cdot n_k$ gilt dann folglich

  $$nz \;\in\; \mathbb{Z} \,.$$

  Setzt man speziell $z := \frac{1}{2n}$, so folgte daraus $\frac{1}{2} \in \mathbb{Z}$, ein Widerspruch.

- Wir nehmen an, $(\mathbb{Q}^\times, \cdot)$ besäße ein endliches Erzeugendensystem

$$\frac{m_1}{n_1}\ , \ \dots\ ,\ \frac{m_k}{n_k}\ ,$$

wobei $k \in \mathbb{N}$, $m_1, \dots, m_k, n_1, \dots, n_k \in \mathbb{Z} \setminus \{0\}$. Für jedes $z \in \mathbb{Q}^\times$ gibt es also $r_1, \dots, r_k \in \mathbb{Z}$ so, daß

$$z \ = \ \prod_{i=1}^k \left(\frac{m_i}{n_i}\right)^{r_i} \ .$$

Mit $n := n_1 \cdot \ldots \cdot n_k$, $m := m_1 \cdot \ldots \cdot m_k$ und $r := \max\{|r_1|, \dots |r_k|\}$ gilt dann

$$(nm)^r z \ = \ \prod_{i=1}^k m_i^{r+r_i} n_i^{r-r_i} \ \in \ \mathbb{Z}\ ,$$

denn es gilt $r+r_i \geq 0$ und $r-r_i \geq 0$ für alle i. Es sei nun p eine Primzahl, die nm nicht teilt. Dann sind p und nm teilerfremd. Setzt man $z := \frac{1}{p}$, so gäbe es ein $r \in \mathbb{Z}$ mit $\frac{(nm)^r}{p} \in \mathbb{Z}$, d.h. p wäre ein Teiler von $(nm)^r$. Das ist ein Widerspruch.

Aufgabe 3: (1+2+1=4 P)

(a) Sei $G := \mathbb{Z}$ und $H \subset G$ eine Untergruppe. Zeigen Sie: H is ein direkter Faktor (d.h. es existiert eine Untergruppe $H' \subset \mathbb{Z}$ mit $G = H \oplus H'$) genau dann, wenn $H = \{0\}$ oder $H = \mathbb{Z}$. Hinweis: benutzen Sie die Klassifikation aller Untergruppen von $\mathbb{Z}$ (Satz 1.7.3 bei Lütkebohmert).

(b) Sei $x := (a, b) \in \mathbb{Z}^2$ und $G := \mathbb{Z} \cdot x \subset \mathbb{Z}^2$ die von x erzeugte zyklische Untergruppe. Zeigen Sie: H ist genau dann ein direkter Faktor, wenn a und b teilerfremd sind. Hinweis: sind a und b teilerfremd, so gibt es $c, d \in \mathbb{Z}$ mit $ac + bd = 1$.

(c) Für $a := 17$ und $b := 13$: finde ein Komplement $H' \subset \mathbb{Z}^2$ zu $H = \mathbb{Z} \cdot x \subset \mathbb{Z}^2$.

Lösung:

(a) Wir wollen verwenden, daß alle Untergruppen von $\mathbb{Z}$ von der Form $m\mathbb{Z}$ sind für ein $m \in \mathbb{N}_0$. Es seien nun H und H' zwei nichttriviale Untergruppen von $\mathbb{Z}$. Also gibt es $m, n \in \mathbb{N}$ so, daß $H = m\mathbb{Z}$ und $H' = n\mathbb{Z}$. Dann ist aber

$$H \cap H' \ \supseteq \ (nm)\mathbb{Z} \ \neq \ \{0\}\ .$$

Also kann $\mathbb{Z}$ nicht direkte Summe zweier nichttrivialer Untergruppen sein. Die einzigen Darstellungen von $\mathbb{Z}$ als direkte Summe zweier Untergruppen sind somit

$$\mathbb{Z} \ = \ \mathbb{Z} \oplus \{0\} \ = \ \{0\} \oplus \mathbb{Z}\ .$$

Daraus folgt die Behauptung.

(b) Wir wollen folgendes Lemma beweisen.

Lemma *Es seien $x_1, \dots, x_m \in \mathbb{Z}^n$ Zeilenvektoren und $A \in \mathbb{Z}^{m\times n}$ sei die von diesen Zeilen gebildete Matrix. Dann sind die $x_1, \dots, x_m$ genau dann eine Basis der Gruppe $\mathbb{Z}^n$, wenn $m = n$ und* $\det A = \pm 1$.

Beweis: Es seien $e_1, \dots, e_n$ die Einheitsvektoren in $\mathbb{Z}^n$, aufgefaßt als Zeilen.

- „$\Rightarrow$“: Zunächst gilt $m \leq n$, denn die lineare Unahängigkeit der Zeilen von A über $\mathbb{Z}$ bedeutet auch die lineare Unabhängigkeit im Vektorraum $\mathbb{Q}^n$ über $\mathbb{Q}$ (nach Multiplikation mit dem Hauptnenner der Koeffizienten).

Nach Voraussetzung lassen sich die e_i als Linearkombinationen der x_j schreiben, d.h. es gilt

$$e_i \;=\; \sum_{j=1}^{m} b_{ij} x_j$$

für gewisse $b_{ij} \in \mathbb{Z}$. Schreibt man $B := \begin{pmatrix} b_{11} & \cdots & b_{1m} \\ \vdots & & \vdots \\ b_{n1} & \cdots & b_{nm} \end{pmatrix} \in \mathbb{Z}^{n \times m}$, so erhält man

$$\begin{aligned} B \cdot A \;&=\; \begin{pmatrix} b_{11} & \cdots & b_{1m} \\ \vdots & & \vdots \\ b_{n1} & \cdots & b_{nm} \end{pmatrix} \cdot \begin{pmatrix} x_1 \\ \vdots \\ x_m \end{pmatrix} \;=\; \begin{pmatrix} b_{11}x_1 + \ldots + b_{1m}x_m \\ \vdots \\ b_{n1}x_1 + \ldots + b_{nm}x_m \end{pmatrix} \\ &=\; \begin{pmatrix} e_1 \\ \vdots \\ e_n \end{pmatrix} \;=\; \mathrm{E}_n \; . \end{aligned}$$

Aus der Linearen Algebra wissen wir, daß daraus $m = n$ folgt. Ferner sind $\det A \in \mathbb{Z}$ und $\det B \in \mathbb{Z}$, und es gilt

$$(\det B)(\det A) \;=\; 1 \; .$$

Daraus folgt $\det A = \pm 1$.

- „$\Leftarrow$“: Es gelte also $m = n$ und $\det A = \pm 1$. Nach der Cramerschen Regel gilt $A^{-1} \in \mathbb{Z}^{n \times n}$. Die Gleichung

$$A^{-1} \cdot A \;=\; \mathrm{E}_n$$

zeigt, daß sich die Einheitsvektoren als Linearkombinationen der Zeilen von A schreiben lassen. Also bilden die $x_1, \ldots, x_n$ ein Erzeugendensystem. Ferner sind die Zeilen von A linear unbahängig über $\mathbb{Q}$, also auch über $\mathbb{Z}$. Also handelt es sich um eine Basis von $\mathbb{Z}^n$. $\square$

Für eine Untergruppe $H \leq \mathbb{Z}^2$ mit Basis $x_2, \ldots, x_m$ gilt $\mathbb{Z}^2 = G \oplus H$ genau dann, wenn $x, x_2, \ldots, x_m$ eine Basis von $\mathbb{Z}^2$ bilden.

Also ist G genau dann ein direkter Faktor von $\mathbb{Z}^2$ ist, wenn x sich zu einer Basis von $\mathbb{Z}^2$ ergänzen läßt. Nach obigem Lemma ist das genau dann der Fall, wenn es ein $(c, d) \in \mathbb{Z}^2$ gibt derart, daß

$$ad - bc \;=\; \det \begin{pmatrix} a & b \\ c & d \end{pmatrix} \;=\; \pm 1 \; .$$

Dies ist wiederum äquivalent zur Existenz von $c, d \in \mathbb{Z}$ so, daß $ac + bd = 1$. Daraus folgt die Behauptung.

(c) Nach Teil (b) müssen wir c, d finden so, daß $ad - bc = 1$. Mit dem Euklidischen Algorithmus wird

$$\begin{aligned} 17 \;&=\; 1 \cdot 13 + 4 \\ 13 \;&=\; 3 \cdot 4 + 1 \; . \end{aligned}$$

Also gilt

$$1 \;=\; 13 - 3 \cdot 4 \;=\; 13 - 3 \cdot (17 - 1 \cdot 13) \;=\; 4 \cdot 13 - 3 \cdot 17 \;=\; ad - bc$$

mit $d := -3$ und $c := -4$. Nach obigem Lemma bilden $(17, 13)$ und $(-4, -3)$ eine Basis von $\mathbb{Z}^2$. Also ist

$$H' \;:=\; \mathbb{Z} \cdot (4, 3)$$

ein Komplement zu $H = \mathbb{Z} \cdot (17, 13)$.