Goethe-Universität Frankfurt
Institut für Mathematik

Prof. Dr. Jakob Stix
Martin Lüdtke

Grundlagen der Algebra

Sommersemester 2019

Übungsblatt 2 4. Juni 2019

Aufgabe 5. (4 = 1+1+1+1 Punkte)

Bestimmen Sie jeweils Kern und Bild der folgenden Gruppenhomomorphismen:

(a) $\mathbb{R}^\times \to \mathbb{R}^\times, \quad x \mapsto x^2$;

(b) $\mathbb{Z} \to \mathbb{C}^\times, \quad n \mapsto i^n$;

(c) $\mathrm{Aff}^1(\mathbb{R}) \to \mathbb{R}^\times, \quad aX + b \mapsto a$ (vgl. Aufgabe 2, Blatt 1);

(d) $\mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}, \quad (a, b) \mapsto 2a + 3b$.

Lösungsskizze zu Aufgabe 5:

(a) Der Kern ist $\{1, -1\}$, denn für $x \in \mathbb{R}^\times$ gilt

$$x^2 = 1 \iff (x-1)(x+1) = 0 \iff x = \pm 1.$$

Das Bild ist die Gruppe $\mathbb{R}_{>0}$ der positiven reellen Zahlen: Für alle $x \in \mathbb{R}^\times$ ist $x^2 > 0$, und ein Urbild von $y > 0$ ist die (positive) Quadratwurzel $\sqrt{y}$.

(b) Wir berechnen

$$i^1 = i, \quad i^2 = -1, \quad i^3 = -i, \quad i^4 = 1.$$

Die Ordnung von $i \in \mathbb{C}^\times$ ist also 4 und somit ist $4\mathbb{Z}$ der Kern des Homomorphismus'. Ausführlicher: Schreiben wir $n \in \mathbb{Z}$ in der Form $n = 4k + r$ mit $k \in \mathbb{Z}$ und $0 \leq r < 4$, dann folgt

$$i^n = i^{4k+r} = (i^4)^k \cdot i^r = i^r.$$

Damit ist n genau dann im Kern, wenn $i^r = 1$, also $r = 0$ gilt, und das ist genau dann der Fall, wenn $n \in 4\mathbb{Z}$ ist.
Die Rechnung zeigt auch, dass das Bild $\{\pm 1, \pm i\}$ ist. Dies ist die von i erzeugte Untergruppe von $\mathbb{C}^\times$.

(c) Der Kern besteht aus den Translationen $X + b$ mit $b \in \mathbb{R}$. Das Bild ist $\mathbb{R}^\times$, denn ein Urbild von $a \in \mathbb{R}^\times$ ist durch aX gegeben.

(d) Das Bild ist $\mathbb{Z}$: Es ist nämlich $1 = 2 \cdot (-1) + 3 \cdot 1$ im Bild enthalten. Das Bild ist eine Untergruppe und damit die volle Gruppe $\mathbb{Z}$, da diese von 1 erzeugt wird. Angenommen (a, b) liegt im Kern, also $2a + 3b = 0$. Dann gilt

$$2a = -3b.$$

Die linke Seite ist durch 2 teilbar, damit auch die rechte Seite, und dafür muss b durch 2 teilbar sein. Wir schreiben $b = 2k$ mit $k \in \mathbb{Z}$. Dann gilt $2a = -3 \cdot (2k)$, somit $a = -3k$. Umgekehrt gilt für alle $k \in \mathbb{Z}$:

$$2 \cdot (-3k) + 3 \cdot (2k) = 0.$$

Der Kern ist also

$$\{(-3k, 2k) \; ; \; k \in \mathbb{Z}\}.$$

Aufgabe 6. (4 = 1+1+1+1)

Sei $n \in \mathbb{N}$. Für eine ganze Zahl $a \in \mathbb{Z}$ bezeichne $[a] \coloneqq a + n\mathbb{Z}$ die Restklasse von a in $\mathbb{Z}/n\mathbb{Z}$. Sei $\pi : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$, $a \mapsto [a]$ der Restklassenhomomorphismus.

(a) Bestimmen Sie Kern und Bild von π.

(b) Seien $a, b \in \mathbb{Z}$. Wir sagen, b ist ein Teiler von a (geschrieben $b \mid a$), wenn $a = kb$ für ein $k \in \mathbb{Z}$ gilt. Zeigen Sie: $a\mathbb{Z} \subseteq b\mathbb{Z} \;\Leftrightarrow\; b \mid a$.

(c) Zeigen Sie, dass die Untergruppen von $\mathbb{Z}/n\mathbb{Z}$ in Bijektion zu den Teilern von n in $\mathbb{N}$ stehen.

(d) Wie viele Untergruppen besitzt $\mathbb{Z}/2019\mathbb{Z}$?

Lösungsskizze zu Aufgabe 6:

(a) Für $a \in \mathbb{Z}$ gilt

$$[a] = [0] \;\Leftrightarrow\; a \equiv 0 \bmod n \;\Leftrightarrow\; \exists k \in \mathbb{Z} : a - 0 = kn \;\Leftrightarrow\; a \in n\mathbb{Z}.$$

Somit ist $\ker(\pi) = n\mathbb{Z}$. Das Bild ist $\mathbb{Z}/n\mathbb{Z}$ nach Definition der Gruppe als Menge der Restklassen von ganzen Zahlen modulo n.

(b) Aus $a\mathbb{Z} \subseteq b\mathbb{Z}$ folgt $a \in b\mathbb{Z}$. Umgekehrt, wenn $a \in b\mathbb{Z}$ gilt, dann ist auch die von a erzeugte Untergruppe, also $a\mathbb{Z}$ in $b\mathbb{Z}$ enthalten. Somit gilt:

$$a\mathbb{Z} \subseteq b\mathbb{Z} \;\Leftrightarrow\; a \in b\mathbb{Z} \;\Leftrightarrow\; \exists k \in \mathbb{Z} : a = kb \;\Leftrightarrow\; b \mid a.$$

(c) Die Untergruppen von $\mathbb{Z}/n\mathbb{Z} = \pi(\mathbb{Z})$ stehen in Bijektion zu den Untergruppen von $\mathbb{Z}$, die $\ker(\pi) = n\mathbb{Z}$ enthalten. Jede Untergruppe von $\mathbb{Z}$ ist von der Form $d\mathbb{Z}$ für ein eindeutiges $d \in \mathbb{N}_0$, und gemäß (b) gilt $n\mathbb{Z} \subseteq d\mathbb{Z}$ genau dann, wenn d ein Teiler von n ist.

(d) Gemäß (c) suchen wir die Anzahl der Teiler von 2019. Die Primfaktorzerlegung ist

$$2019 = 3 \cdot 673,$$

die Teiler sind somit $1, 3, 673, 2019$, ihre Anzahl ist vier.

Aufgabe 7. (4 = 2+2 Punkte)

(a) Sei $(A, +)$ eine abelsche Gruppe und $\{a_1, \ldots, a_n\} \subseteq A$ eine endliche Teilmenge. Zeigen Sie:

$$\langle a_1, \ldots, a_n \rangle = \{m_1 a_1 + \ldots + m_n a_n \; ; \; m_1, \ldots, m_n \in \mathbb{Z}\}.$$

(b) Sei $(A, +)$ eine abelsche Gruppe, die von endlich vielen Elementen endlicher Ordnung erzeugt wird. Zeigen Sie, dass A endlich ist.

Lösungsskizze zu Aufgabe 7:

(a) Sei

$$B := \{m_1a_1 + \ldots + m_na_n \ ; \ m_1, \ldots, m_n \in \mathbb{Z}\}.$$

Dies ist eine Untergruppe, denn es gilt

$$0 = 0 \cdot a_1 + \ldots + 0 \cdot a_n \in B,$$

und für $m_1, \ldots, m_n,\ m'_1, \ldots, m'_n \in \mathbb{Z}$ gilt

$$(m_1a_1+\ldots+m_na_n)-(m'_1a_1+\ldots+m'_na_n) = (m_1-m'_1)a_1+\ldots+(m_n-m'_n)a_n \in B.$$

Ferner gilt

$$a_i = 0 \cdot a_1 + \ldots + 1 \cdot a_i + \ldots + 0 \cdot a_n \in B \quad \text{für} \quad i = 1, \ldots, n,$$

also $\{a_1, \ldots, a_n\} \subseteq B$. Ist B' eine weitere Untergruppe von A, die $\{a_1, \ldots, a_n\}$ enthält, dann gilt zunächst $m_ia_i \in B'$ für $i = 1, \ldots, n$ und $m_i \in \mathbb{Z}$, und damit auch $m_1a_1 + \ldots + m_na_n \in B'$ für alle $m_1, \ldots, m_n \in \mathbb{Z}$, also $B \subseteq B'$. Somit ist B die kleinste Untergruppe, die $\{a_1, \ldots, a_n\}$ enthält, also

$$B = \langle a_1, \ldots, a_n \rangle.$$

(b) Angenommen, es gilt $A = \langle a_1, \ldots, a_n \rangle$ und jedes a_i hat endliche Ordnung t_i. Für $m_i \in \mathbb{Z}$ können wir $m_i = k_it_i + r_i$ mit $k_i \in \mathbb{Z}$ und $0 \leq r_i < t_i$ schreiben, dann gilt

$$m_ia_i = k_it_ia_i + r_ia_i = r_ia_i$$

wegen $t_ia_i = 0$. Jedes Element von $A = \langle a_1, \ldots, a_n \rangle$ hat somit eine Darstellung der Form

$$r_1a_1 + \ldots + r_na_n \quad \text{mit} \quad 0 \leq r_i < t_i.$$

Für die r_i gibt es nur endlich viele Möglichkeiten, damit ist A endlich.

Aufgabe 8. (4 = 2+2 Punkte)

Sei $\mathrm{Aff}^1(\mathbb{Z}) \subseteq \mathrm{Aff}^1(\mathbb{Q})$ die Untergruppe der Polynome $aX + b$ mit $a \in \{1, -1\}$ und $b \in \mathbb{Z}$ (vgl. Aufgabe 2, Blatt 1). Seien

$$u(X) := -X, \quad v(X) := -X + 1 \in \mathrm{Aff}^1(\mathbb{Z}).$$

(a) Bestimmen Sie die Ordnungen von u, v und $v \circ u$.

(b) Zeigen Sie, dass $\mathrm{Aff}^1(\mathbb{Z})$ von u und v erzeugt wird.

Lösungsskizze zu Aufgabe 8:

(a) Wir berechnen

$$(u \circ u)(X) = -(-X) = X, \quad (v \circ v)(X) = -(-X + 1) + 1 = X,$$

somit gilt $\mathrm{ord}(u) = \mathrm{ord}(v) = 2$. Es gilt

$$(v \circ u)(X) = -(-X) + 1 = X + 1.$$

Dieses Element hat unendliche Ordnung, denn es gilt

$$(v \circ u)^2 = X + 2, \quad (v \circ u)^3 = X + 3, \quad \text{usw.},$$

induktiv $(v \circ u)^n = X + n \neq X$ für alle $n \in \mathbb{N}$.

(b) Mittels $X+1 = v \circ u$ lassen sich alle Elemente der Form $X+n$ mit $n \in \mathbb{N}$ erzeugen. Das Inverse von $X+1$ ist $X-1$, dadurch lässt sich allgemeiner $X+b$ mit $b \in \mathbb{Z}$ erzeugen. Wegen $-X+b = (X+b) \circ u$ sind alle Elemente von $\mathrm{Aff}^1(\mathbb{Z})$ in der von u und v erzeugten Untergruppe enthalten.
Wir stellen fest, dass die Gruppe $\mathrm{Aff}^1(\mathbb{Z})$ von zwei Elementen endlicher Ordnung erzeugt wird, obwohl die Gruppe selbst unendlich ist, dass also in Aufgabe 7 (b) auf die Voraussetzung nicht verzichtet werden kann, dass die Gruppe abelsch ist.

Abgabe: Am kommenden Dienstag, den **11. Juni 2019**, bis zur Vorlesung in den Kasten im 3. Stock, Institut für Mathematik, Robert-Mayer-Straße 6–8. Downloads von Übungsblättern und Informationen zur Vorlesung unter

`http://www.uni-frankfurt.de/76786679/Grundlagen_der_Algebra`
