Algebra 1 (WS 2026-27) - Problem sheet 1

1.1 In einem abelschem Monoid gilt: $x^n y^n = (xy)^n$.

1.2 Sei S eine Halbgruppe und seien $a_1, \ldots, a_n \in S$. Dann ist das Produkt $a_1 \cdot a_2 \cdots a_n$ unabhängig davon, wie die Klammern gesetzt werden.

1.3 Sei M ein Monoid, und sei $x \in M$ invertierbar.

- x^n ist invertierbar für alle $n \in \mathbb{Z}$, und es gilt: $(x^n)^{-1} = x^{-n}$.
- die Potenzgesetze $x^m \cdot x^n = x^{m+n}$ und $(x^m)^n = x^{mn}$ gelten für alle $m, n \in \mathbb{Z}$

1.4 Zeigen Sie: Ein Monoid G ist genau dann eine Gruppe, wenn für alle $a, b \in G$ jede der Gleichungen $ax = b$ und $ya = b$ genau eine Lösung in G hat.

1.5 Auf $\mathbb{Z}$ definieren wir eine Verknüpfung durch $n*m := (1+n)(1+m)-1 = n+m+nm$.

- Zeigen Sie, dass $(\mathbb{Z}, *)$ ein kommutatives Monoid ist.
- Bestimmen Sie das neutrale Element und alle invertierbaren Elemente.

1.6 Bestimmen Sie für jeden der fünf platonischen Körper die Ordnung der Isometriegruppe diese Körpers.

Solution. (Wir betrachten auch orientierungsumkehrende Isometrien.)

- Eine Isometrie ist eindeutig bestimmt, wenn wir wissen:
  - auf welche Kante eine fest gewählte Kante abgebildet wird;
  - wohin ihre beiden Endpunkte abgebildet werden (2 Möglichkeiten);
  - auf welche der beiden angrenzenden Flächen eine fest gewählte Fläche abgebildet wird (2 Möglichkeiten).

(Für die orientierungserhaltende Isomeitrien brauchen wir die dritte Möglichkeit nicht.)

• Wegen der Symmetrie der platonischen Körper ist jede solche Wahl möglich. Hat der Körper k Kanten, so hat seine Isometriegruppe also $4k$ Elemente.

Körper	Kanten	$\lvert G\rvert$
Tetraeder	6	24
Würfel	12	48
Oktaeder	12	48
Dodekaeder	30	120
Ikosaeder	30	120

1.7 $|S_n| = n!$

1.8 **[10]**

Sei G eine Gruppe. Für $S \subseteq G$ besteht die von S erzeugte Untergruppe $\langle S\rangle$ aus allen Produkten $s_1^{\varepsilon_1} \cdots s_k^{\varepsilon_k}$ mit $s_i \in S$, $\varepsilon_i \in \{-1, 1\}$ und $k \geqslant 0$ (für $k = 0$ erhalten wir e).

Zeigen Sie, dass $\langle S\rangle$ die kleinste Untergruppe von G ist, die S enthält. D.h. falls $H \leqslant G$ und $S \subseteq H$, dann $\langle S\rangle \subset H$.

Solution. Die Menge $\langle S\rangle$ enthält e (für $k = 0$) und alle Elemente von S (für $k = 1$).

Sie ist eine Untergruppe: Produkte von Elementen aus $\langle S\rangle$ liegen wieder in $\langle S\rangle$, indem wir die entsprechenden Ausdrücke hintereinander schreiben. Auch Inverse liegen in $\langle S\rangle$, denn

$$(s_1^{\varepsilon_1} \cdots s_k^{\varepsilon_k})^{-1} = s_k^{-\varepsilon_k} \cdots s_1^{-\varepsilon_1}.$$

Sei nun $H \leqslant G$ mit $S \subseteq H$. Da H unter Produkten und Inversen abgeschlossen ist, enthält H alle Elemente von $\langle S\rangle$. Also $\langle S\rangle \subseteq H$.

1.9 **[10]**

Sei $(G, \cdot)$ eine Gruppe, seien $a, b \in G$ mit $ab = ba$. und $\mathrm{ggT}(\mathrm{ord}(a), \mathrm{ord}(b)) = 1$. Zeigen Sie dass die Untergruppe $\langle a, b\rangle$ zyklisch ist.

Solution. We essentially rewrite the observation that $\mathbb{Z}/a \times \mathbb{Z}/b$ is cyclic, using the multiplicative notation.

Solution. Wir übertragen die Beobachtung, dass $\mathbb{Z}/m \times \mathbb{Z}/n$ für teilerfremde m, n zyklisch ist, in die multiplikative Schreibweise.

Seien $m := \mathrm{ord}(a)$ und $n := \mathrm{ord}(b)$. Da a und b kommutieren, besteht $\langle a, b\rangle$ aus den Elementen $a^i b^j$ mit $0 \leqslant i < m$, $0 \leqslant j < n$. Also gilt $|\langle a, b\rangle| \leqslant mn$.

Wir zeigen, dass die Potenzen $e, ab, \ldots, (ab)^{mn-1}$ paarweise verschieden sind.

Falls $(ab)^i = (ab)^j$ für $0 \leqslant i < j < mn$, dann gilt $a^{j-i} = b^{i-j}$. Die Ordnung dieses

Elements teilt sowohl m als auch n, also ist es e. Somit gilt $m \mid (j-i)$ und $n \mid (j-i)$, also $mn \mid (j-i)$, Widerspruch.

Damit hat $\langle ab \rangle$ mindestens mn Elemente. Es folgt $\langle a, b \rangle = \langle ab \rangle$. .

1.10 Die Matrizen $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ und $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ erzeugen $\mathrm{SL}(2, \mathbb{Z})$.

Solution. Seien $T := \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ und $S := \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$.

• Linksmultiplikation mit T^k addiert das k-Fache der zweiten Zeile zur ersten, und S tauscht die Zeilen gefoltgt von der Multiplizierung der ersten Zeile durch -1.

• Sei $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}(2, \mathbb{Z})$. Wegen $\det(A) = ad - bc = 1$ gilt $\mathrm{ggT}(a, c) = 1$. Mit dem euklidischen Algorithmus können wir daher durch die obigen Zeilenoperationen die erste Spalte auf $\begin{pmatrix} 1 \\ 0 \end{pmatrix}$ oder $\begin{pmatrix} -1 \\ 0 \end{pmatrix}$ bringen. Da $S^2 = -I$ bekommen wir $\begin{pmatrix} 1 \\ 0 \end{pmatrix}$.

• Da die Determinante erhalten bleibt, ist die resultierende Matrix von der Form $\begin{pmatrix} 1 & m \\ 0 & 1 \end{pmatrix} = T^m$.

Somit ist A ein Produkt von Potenzen von S und T.

1.11 Sei $K = \mathbb{Z}/p$, wobei p eine Primzahl ist. Zeigen Sie dass Untergruppen von K^n sind genau die K-lineare Untervektorräume von K^n. Bestimmen Sie dia Anzahl der Untegruppen von K^n.

1.12 Wie viele verschiedene Erzeuger hat eine zyklische Gruppe der Ordnung n?

Solution. Wir nehmen $\mathbb{Z}/n$. Die Klasse $[k]$ ist ein Erzeuger falls $[dk] \neq 0$ wenn $d|n$, $d < n$. Also $n \nmid dk$ wenn $d \mid n$, $d < n$. Das gild gdw $\gcd(n, k) = 1$, also die Antwort ist: genauso viele wie es Zahlen k gibt mit $1 \leqslant k \leqslant n$ mit $\gcd(k, n) = 1$. Dieze Zahl nennt man auch die Eulersche φ-funktion von n, bezeichnet mit $\varphi(n)$. (Z.B. $\varphi(p) = p - 1$ fall p prim ist, was entspricht der Tatsache, dass jedes nichtriviales Element in $\mathbb{Z}/p$ ein Erzeuger ist).

1.13 • Sei $S \subseteq G$ ein Erzeugendensystem von G und sei $T \subseteq G$. Zeigen Sie: Falls $S \subseteq \langle T \rangle$, dann ist auch T ein Erzeugendensystem von G.

• Zeigen Sie dass die Transpositionen $(1\,2), (2\,3), \ldots, (n-1\,n)$ die Gruppe S_n erzeugen. Benutzen Sie dabei die obige Aussage und die Tatsache dass wir schon wissen, dass die Transpositionen $(1\,2), (1\,3), \ldots, (1\,n)$ die Gruppe S_n erzeugen.

1.14 In $\mathrm{SL}(2,\mathbb{Z})$ haben die Matrizen $A = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ und $B = \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}$ die Ordnungen 4 bzw. 3. Zeigen Sie, dass $\langle AB \rangle$ eine unendliche zyklische Untergruppe von $\mathrm{SL}(2,\mathbb{Z})$ ist. Das Produkt zweier Elemente endlicher Ordnung muss also nicht wieder endliche Ordnung haben. Was gilt in abelschen Gruppen?

1.15 **[10]**

Zeigen Sie, dass jede Gruppe G gerader Ordnung $|G| = 2n$ ein Element $g \neq e$ der Ordnung 2 enthält.

Hinweis: Betrachten Sie die Paare g, g^{-1}.

1.16 Sei H eine nichtleere Teilmenge einer endlichen Gruppe G, die unter Multiplikation abgeschlossen ist. Zeigen Sie, dass H eine Untergruppe von G ist. Insbesondere müssen wir die Existenz eines neutralen Elements und der inversen Elemente nicht gesondert überprüfen. Gilt dies auch für unendliche Gruppen?

1.17 Bestimmen Sie ein minimales Erzeugendensystem der multiplikativen Gruppe $(\mathbb{Q}_{>0}, \cdot)$. (D.h. kein echtes Teilsystem soll die Gruppe erzeugen.)

1.18 Sei $\pi = (1\,2\,\ldots\,n) \in S_n$ und $k \geqslant 1$. Zeigen Sie, dass π^k ein Produkt von $d := \mathrm{ggT}(n,k)$ paarweise disjunkten Zyklen ist, die alle die Länge n/d haben.

1.19 Seien $A, B \in M_n(\mathbb{R})$ und $(AB)^m = I_n$ für ein $m \geqslant 1$. Gilt dann notwendigerweise auch $(BA)^m = I_n$?

Solution. Aus $AB^m = I_n$ folgt $\det(A), \det(B) \neq 0$, also sind A und B invertierbar. Wr multplizieren die Gleichheite $(AB)^m = I_n$ auf der rechten Seite durch A^{-1} und auf der linken Seite ducht A, und bekommen wir $(BA)^m = I_n$.