KLAUSUR ZUR ALGEBRA (B3)

18. Februar 2009

MUSTERLÖSUNG

Name:

Matrikelnummer:

Studiengang:

Aufgabe	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**Summe**
Punktzahl								/**50**

Allgemeine Hinweise:

– Bitte schreiben Sie Ihre Lösungen jeweils unter die Aufgabenstellung und ggf. auf die Rückseite. Wenn der Platz nicht ausreicht, bitten Sie die Aufsicht um zusätzliches **Aufgabenpapier**.
– Verwenden Sie immer **für jede Aufgabe ein separates Blatt.**
– Vermerken Sie **auf jedem Blatt Ihren Namen und Ihre Matrikelnummer**.
– Einziges erlaubtes Hilfsmittel ist ein von Ihnen selbst beidseitig handbeschriebenes DIN A4-Blatt.

Wir wünschen viel Erfolg!

Name: **Matrikelnummer:**

Aufgabe 1 **(7 Punkte)**

Welche der folgenden Relationen $\sim$ sind Äquivalenzrelationen auf $\mathbb{Z}$?
Welche sind Kongruenzrelationen auf dem Monoid $(\mathbb{Z}, \cdot)$?

(a) $a \sim b \iff a - b$ ist gerade $(a, b \in \mathbb{Z})$ (2 Punkte)

(b) $a \sim b \iff |a - b| \leq 2$ $(a, b \in \mathbb{Z})$ (2 Punkte)

(c) $a \sim b \iff \exists m, n \in \mathbb{N}_{>0} : a^m = b^n$ $(a, b \in \mathbb{Z})$ (3 Punkte)

Begründen Sie Ihre Antworten.

Lösung. (a) Die angegebene Relation ist natürlich gerade die vom Ideal (2) induzierte Kongruenzrelation. Das genügt als Antwort. Man darf es aber auch nachrechnen: Symmetrie und Reflexivität sind offensichtlich. Für die Transitivität, seien $a, b, c, k, \ell \in \mathbb{Z}$ mit $a - b = 2k$, $b - c = 2\ell$. Dann ist $a - c = a - b + 2\ell = 2k + 2\ell$ gerade. Also ist $\sim$ eine Äquivalenzrelation. Sie ist auch eine Kongruenzrelation. Denn sind $a, b, c, d, k, \ell \in \mathbb{Z}$ mit $a - b = 2k$, $c - d = 2\ell$, so ist $ac - bd = a(d + 2\ell) - d(a - 2k) = 2k + 2\ell$ gerade. Also folgt aus $a \sim b$ und $c \sim d$ auch $ac \sim bd$.

(b) Die Relation $\sim$ ist nicht transitiv. Denn es gilt etwa $0 \sim 2$ und $2 \sim 4$, aber $0 \nsim 4$. Sie ist damit keine Äquivalenzrelation (und schon erst recht keine Kongruenzrelation).

(c) Die Relation $\sim$ ist eine Äquivalenzrelation. Dabei sind Symmetrie und Reflexivität wieder ganz offensichtlich. Für die Transitivität, seien $a, b, c \in \mathbb{Z}$, $k, \ell, m, n \in \mathbb{N}_{>0}$ mit $a^k = b^\ell$ und $b^m = c^n$. Dann ist $a^{km} = b^{\ell m} = c^{\ell n}$, also $a \sim c$.
Aber $\sim$ ist keine Kongruenzrelation. Z.B. gilt $2 \sim 4$ und $3 \sim 3$, aber $6 \nsim 12$. Denn wären $k, \ell \in \mathbb{N}_{>0}$ mit $6^k = 12^\ell$, so wäre $2^k 3^k = 6^k = 12^\ell = 2^{2\ell} 3^\ell$. Aus der Eindeutigkeit der Primfaktorzerlegung würde also $k = 2\ell$ und $k = \ell$ folgen, was wegen $k, \ell > 0$ unmöglich ist. $\square$

Name: **Matrikelnummer:**

Aufgabe 2 **(6 Punkte)**

Sei G eine Gruppe, und sei H eine Untergruppe von G. Setze

$$N = \{h \in H \,;\, \forall g \in G\colon ghg^{-1} \in H\}.$$

Zeigen Sie:

(a) N ist eine Untergruppe von H. (2 Punkte)

(b) N ist normal in G. (2 Punkte)

(c) N ist maximal mit diesen Eigenschaften, d.h. wenn L eine normale Untergruppe von G mit $L \subset H$ ist, dann folgt $L \subset N$. (2 Punkte)

Lösung. (a) Sei $h \in N$. Für alle $g \in G$ gilt dann $gh^{-1}g^{-1} = (ghg^{-1})^{-1}$. Da $ghg^{-1} \in H$ und H eine Untergruppe ist, folgt $gh^{-1}g^{-1} \in H$ und damit $h^{-1} \in N$. Sind $h, h' \in N$ und ist $g \in G$, dann gilt $ghh'g^{-1} = ghg^{-1}gh'g^{-1} \in H$, also $hh' \in N$.

(b) Sei h in N, $g \in G$. Dann gilt $ghg^{-1} \in H$. Ist nun $g' \in G$, dann folgt auch $g'(ghg^{-1})g'^{-1} = (g'g)h(g'g)^{-1} \in H$ und damit $ghg^{-1} \in N$. Also ist N ein Normalteiler.

(c) Sei L ein Normalteiler von G mit $L \subset H$, und sei $h \in L$. Dann gilt für alle $g \in G$: $ghg^{-1} \in L \subset H$, also $h \in N$. □

Name: **Matrikelnummer:**

Aufgabe 3 **(7 Punkte)**

Sei G eine Gruppe, und seien H und K Untergruppen von G.

(a) Zeigen Sie: $G = H \cup K$ genau dann, wenn $G = H$ oder $G = K$ gilt. (3 Punkte)

(b) Die Untergruppen H und K seien konjugiert, d.h. es gebe $g \in G$ mit $H = gKg^{-1}$.
Zeigen Sie: $G = HK$ genau dann, wenn $G = H$ gilt. (4 Punkte)

Lösung. (a) Aus $G = H$ oder $G = K$ folgt natürlich $G = H \cup K$. Für die andere Richtung: Es gelte $G \neq H$ und $G \neq K$, aber $G = H \cup K$. Wähle $g \in G \setminus H$ und $g' \in G \setminus K$. Dann muss $g \in K$, $g' \in H$ gelten. Ferner $gg' \in H$ oder $gg' \in K$. Aber aus $gg' = h$ mit $h \in H$ folgt $g = hg'^{-1} \in H$, ein Widerspruch. Analog folgt aus $gg' \in K$, dass $g' \in K$, Widerspruch.

(b) Ist $G = H$, so $G = HK$ wegen $1 \in K$. Für die umgekehrte Richtung, sei $G = HK$ mit $H \neq G$. Dann muss $H \neq K$ sein, also $g \notin K$. Wähle $h \in H$ und $k \in K$ mit $g = hk$. Dann folgt $H = gKg^{-1} = hkK(hk)^{-1} = hkKk^{-1}h^{-1} = hKh^{-1}$ und damit $K = h^{-1}Hh$ und somit $H = K$, ein Widerspruch. $\square$

Name: **Matrikelnummer:**

Aufgabe 4 **(8 Punkte)**

Sei $\mathbb{Z}[i] = \{a + bi\,;\ a, b \in \mathbb{Z}\}$, $i^2 = -1$, der Ring der gaußschen ganzen Zahlen.

(a) Zeigen Sie, dass $1, -1, i, -i$ die einzigen Einheiten in $\mathbb{Z}[i]$ sind. (3 Punkte)

(b) Zeigen Sie, dass zwei Elemente $x, y \in \mathbb{Z}[i]$ genau dann assoziiert sind, wenn $x^4 = y^4$ gilt. (2 Punkte)

(c) Sei $(1 + i)$ das von $1 + i$ erzeugte Ideal. Bestimmen Sie das Ideal $(1 + i) \cap \mathbb{Z}$. (3 Punkte)

Lösung. (a) Wegen $1, -1, i, -i \in \mathbb{Z}[i]$ und $i(-i) = 1$, sind $1, -1, i, -i$ Einheiten in $\mathbb{Z}[i]$. Es gibt zwei Methoden zu zeigen, dass dies die einzigen Einheiten sind.

(1) Mit der Norm: Für $x = a + bi \in \mathbb{Z}[i]$ ist $N(x) = (a + bi)(a - bi) = a^2 + b^2$. Ist x eine Einheit, so gilt $xx^{-1} = 1$ und damit $1 = N(xx^{-1}) = N(x)N(x^{-1}) = N(x)N(x)^{-1}$, da die Norm multiplikativ ist. Daraus folgt $N(x) = 1$. Aus $a^2 + b^2 = 1$ folgt dann $a = 0, b = \pm 1$ oder $a = \pm 1, b = 0$, was genau $x \in \{1, -1, i, -i\}$ bedeutet.

(2) Durch direktes Rechnen: Sei $x = a + bi \in \mathbb{Z}[i]$ eine Einheit, etwa $x^{-1} = c + di$. Dann gilt $1 = xx^{-1} = (a + bi)(c + di) = ac - bd + (bc + ad)i$, damit $bc + ad = 0$ und $ac - bd = 1$. Ist $b = 0$, so folgt $ac = 1$, also $a = \pm 1$ und damit $x = \pm 1$. Ist $b \neq 0$, so schreibe $c = -\frac{ad}{b}$. Dann folgt $1 = ac - bd = -a\frac{ad}{b} - bd$, also $b = -(a^2 + b^2)d$. Daraus folgt $(a^2 + b^2)|b$, andererseits ist $a^2 + b^2 \geq |b|$. Es folgt $a^2 + b^2 = |b|$, also $a = 0$ und $b = \pm 1$, und somit $x = \pm i$.

(b) Wenn $x, y \in \mathbb{Z}[i]$ assoziiert sind, dann bedeutet dass $x = uy$, $u \in \{1, -1, i, -i\}$. Wegen $u^4 = 1$ gilt dann $x^4 = y^4$. Umgekehrt folgt aus $x^4 = y^4$, dass $\left(\frac{x}{y}\right)^4 = 1$. Damit ist $\frac{x}{y}$ eine vierte Einheitswurzel. Diese sind aber gerade $1, -1, i, -i$, also folgt $\frac{x}{y} \in \{1, -1, i, -i\} = \mathbb{Z}[i]^\times$.

(c) Wieder geht es mit oder ohne Norm:

(1) Wegen $N(x) = x\overline{x}$, gilt $N(x) \in (1 + i) \cap \mathbb{Z}$ für alle $x \in (1 + i)$. Es gilt $N(1 + i) = 2$, also $2 \in (1 + i) \cap \mathbb{Z}$. Andererseits gilt $1 \notin (1 + i)$, da $1 + i$ keine Einheit ist. Also ist $(1 + i) \cap \mathbb{Z} = (2)$, da (2) ein maximales Ideal ist.

(2) Durch direktes Rechnen: Es gilt $(1+i) = \{(a+bi)(1+i); a, b \in \mathbb{Z}\}$. Wir berechnen $(a+bi)(1+i) = a - b + (a + b)i$. Es folgt aus $(a + bi)(1 + i) \in \mathbb{Z}$ also $a = -b$ und damit $(a + bi)(1 + i) = 2a$. Also gilt $(1 + i) \cap \mathbb{Z} = (2)$. $\square$

Name: **Matrikelnummer:**

Aufgabe 5 **(6 Punkte)**

Sei R ein kommutativer Integritätsbereich. Für jedes $x \in R$ sei $\operatorname{ord}(x)$ die Ordnung von x in der additiven Gruppe $(R, +)$. (*Erinnerung:* Dies bedeutet $\operatorname{ord}(x) = \min\{n \in \mathbb{N}_{>0} \, ; \, nx = 0\}$, falls ein $n \in \mathbb{N}_{>0}$ mit $nx = 0$ existiert, sonst $\operatorname{ord}(x) = \infty$.)

Zeigen Sie: Für alle $x, y \in R \setminus \{0\}$ gilt:

(a) $\operatorname{ord}(x) = \operatorname{ord}(y)$; (3 Punkte)

(b) Falls $\operatorname{ord}(x) < \infty$, so ist $\operatorname{ord}(x)$ eine Primzahl. (3 Punkte)

Lösung. (a) Sei $n \in \mathbb{N}_{>0}$ mit $nx = 0$. Dann gilt $0 = (nx)y = x(ny)$ und damit $x = 0$ oder $ny = 0$, da R nullteilerfrei ist. Also $ny = 0$, wegen $x \neq 0$. Damit $\operatorname{ord}(y) \leq \operatorname{ord}(x)$. Die Umkehrung gilt genauso. (Falls $\operatorname{ord}(y) = \infty$, dann zeigt die gleiche Betrachtung dass nicht $\operatorname{ord}(x) < \infty$ gelten kann, und umgekehrt.)

(b) Es sei $n \in \mathbb{N}_{>0}$ mit $nx = 0$ und $mx \neq 0$ für alle $m < n$. Angenommen $n = k\ell$ mit $k, \ell \in \mathbb{N}_{>0}$, dann $kx \neq 0 \neq \ell x$, insbesondere $k, \ell \neq 0$ in R. Andererseits ist $k(\ell x) = 0$, also $k = 0$ oder $\ell x = 0$, da R nullteilerfrei ist, ein Widerspruch. $\square$

Name: **Matrikelnummer:**

Aufgabe 6 **(8 Punkte)**

Sei $n \geq 2$ eine natürliche Zahl.

(a) Zeigen Sie, dass der n-Zyklus $(12 \cdots n)$ als Produkt von $n-1$ Transpositionen geschrieben werden kann. (3 Punkte)

(b) Zeigen Sie, dass $(12 \cdots n)$ nicht als Produkt von k Transpositionen geschrieben werden kann, falls $k \leq n-2$. (5 Punkte)
(*Hinweis:* Sei $k \in \mathbb{N}$ und seien $a_1, \ldots, a_k, b_1, \ldots, b_k \in \{1, \ldots, n\}$ mit $(12 \cdots n) = (a_1 b_1) \cdots (a_k b_k)$. Zeigen Sie, dass die Menge $\{a_1, \ldots, a_k, b_1, \ldots, b_k\}$ höchstens $k+1$ (verschiedene) Elemente enthält.)

Sie erhalten in (b) immer noch 3 Punkte, wenn sie die Behauptung für den Spezialfall $k = n-2$ zeigen können.

Lösung. (a) Es gilt $(12 \cdots n) = (1n)(1(n-1)) \cdots (12)$. Das genügt als Beweis. Man darf die Behauptung auch schön säuberlich mit Induktion zeigen: Für $n = 2$ ist nichts zu zeigen. Sei $n \geq 3$. Dann gilt $(12 \cdots n) = (1n)(12 \cdots n-1)$. Anwenden der Induktionsvoraussetzung auf $(12 \cdots n-1)$ zeigt die Behauptung.

(b) Sei $(12 \cdots n) = (a_1 b_1) \cdots (a_k b_k)$ wie im Hinweis. Behaupte, dass $A_k := \{a_1, \ldots, a_k, b_1, \ldots, b_k\}$ höchstens $k+1$ Elemente enthält. Denn wäre $|A_k| \geq k+2$, dann gäbe es einen Index $i \in \{1, \ldots, k\}$ derart, dass $a_i, b_i \notin \bigcup_{j \neq i} \{a_j, b_j\}$, in Worten: Es gäbe einen Index i derart, dass die Elemente a_i, b_i von den übrigen $k-1$ Transpositionen nicht bewegt werden. (*Beweis* (muss nicht unbedingt ausgeführt werden): Wenn $a_i \in \bigcup_{j \neq i} \{a_j, b_j\}$ oder $b_i \in \bigcup_{j \neq i} \{a_j, b_j\}$ für alle i gilt, dann hat A_k höchstens $k+1$ Elemente. Für $k = 1$ ist die Behauptung ohnehin klar. Sei $k \geq 2$. Nach Induktionsannahme hat $A_{k-1} = \{a_1, \ldots, a_{k-1}, b_1, \ldots, b_{k-1}\}$ höchstens k Elemente. Wegen $a_k \in A_{k-1}$ oder $b_k \in A_{k-1}$ hat dann A_k höchstens $k+1$ Elemente.)
Das ist aber unmöglich. Schreibe der Übersicht halber $\pi = (12 \cdots n)$. Es würde $\pi^\ell(a_i) \in \{a_i, b_i\}$ für alle $\ell \geq 0$ folgen. Tatsächlich ist aber $\{\pi^\ell(a_i)\ ;\ \ell \geq 0\} = \{1, \ldots, n\}$, ein Widerspruch. (Alternatives Argument: Die Transposition $(a_i b_i)$ ist disjunkt zu den übrigen. Wegen der Eindeutigkeit der Zerlegung in disjunkte Zykel müsste sie also in der Zykelzerlegung von $(12 \cdots n)$ vorkommen. Aber $(12 \cdots n)$ ist selbst ein Zykel, Widerspruch.)
Also gezeigt: $|A_k| \leq k+1$. Andererseits folgt aus der Gleichheit $(12 \cdots n) = (a_1 b_1) \cdots (a_k b_k)$ sofort $A_k = \{1, \ldots, n\}$, denn $(12 \cdots n)$ hat keine Fixpunkte; es müssen daher alle Elemente von $\{1, \ldots, n\}$ auf der rechten Seite vorkommen. Also gilt $k+1 \geq n$, wie behauptet. $\square$

Name: **Matrikelnummer:**

Aufgabe 7 **(8 Punkte)**

Sei p eine Primzahl, und sei G eine nicht-abelsche Gruppe der Ordnung p^3. Zeigen Sie:

(a) Das Zentrum Z von G ist zyklisch von Ordnung p. (3 Punkte)

(b) Für die Kommutatorgruppe G' von G gilt $G' = Z$. (3 Punkte)

(c) Nennen Sie ein Beispiel einer nicht-abelschen Gruppe der Ordnung 8 und geben Sie ihr Zentrum an (ohne Beweis). (2 Punkt)

Die folgenden Resultate aus den Übungsaufgaben dürfen Sie ohne Beweis verwenden:
Ist G/Z zyklisch, so ist G abelsch; $Z \neq \{1\}$; Gruppen der Ordnung p^2 sind abelsch; G/G' ist abelsch und G' ist minimal bezüglich dieser Eigenschaft.

Lösung. (a) Nach dem Satz von Lagrange muss die Ordnung des Zentrums ein Teiler von p^3 sein. Es kommen also nur die Ordnungen $1, p, p^2, p^3$ in Frage. Dabei scheidet 1 aus wegen $Z \neq \{1\}$, p^3 scheidet aus, da G sonst abelsch wäre. Die Möglichkeit $|Z| = p^2$ besteht ebenfalls nicht, da sonst G/Z (das Zentrum ist ein Normalteiler!) die Ordnung p hätte (wiederum nach Lagrange) und somit zyklisch wäre. Dann wäre aber G abelsch, ein Widerspruch. Also gilt $|Z| = p$.

(b) Nach (a) hat G/Z die Ordnung p^2 und ist damit abelsch. Aufgrund der Minimalität von G' folgt daraus $G' \subset Z$. Aber Z ist zyklisch von Primzahlordnung. Also hat Z keine Untergruppen außer Z und $\{1\}$. Nun ist $G' = \{1\}$ aber unmöglich, da G nicht abelsch ist. Also gilt $G' = Z$.

(c) Aus Vorlesung und Übungen bekannte Beispiele sind: Die Diedergruppe D_4 und die Quaternionengruppe. Man kann beweisen, dass dies die einzigen nicht-abelschen Gruppen der Ordnung 8 sind. (Die Heisenberggruppe mit Einträgen in $\mathbb{F}_2$ (Aufgabe 24) ist zu D_4 isomorph.)
Sei a die Viertel-Drehung in D_4 (das Element der Ordnung 4). Dann ist $Z = \{1, a^2\}$, d.h. das Zentrum besteht gerade aus der 180-Grad-Drehung. In der Quaternionengruppe ist $Z = \{1, -1\}$.

□