

## KLAUSUR ZUR ALGEBRA UND ZAHLENTHEORIE

22. März 2017

Nachname:

---

Vorname:

---

Matrikelnummer:

---

Studiengang:

---

Aufgabe	1	2	3	4	5	6	7	8	9	Summe
Punktzahl										/60

### Allgemeine Hinweise

- Die Bearbeitungszeit beträgt drei Stunden.
- 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 **kein eigenes Papier**.
- Bitte schreiben Sie **nicht mit Bleistift** und **nicht in roter Farbe**.
- Bitte verwenden Sie **kein Tippex**, keine Tintenkiller oder Ähnliches.
- Verwenden Sie immer **für jede Aufgabe ein separates Blatt**.
- Vermerken Sie **auf jedem Blatt Ihren Namen und Ihre Matrikelnummer**.
- Alle Antworten sind zu begründen und die Lösungswege nachvollziehbar aufzuschreiben.
- Es sind **keine Hilfsmittel** zugelassen.
- Sie dürfen auf Resultate aus der Vorlesung zur Algebra und Zahlentheorie (Wintersemester 2016/17) verweisen (zum Beispiel durch ein Stichwort wie „Chinesischer Restsatz“ oder durch eine kurze Beschreibung des Ergebnisses), es sei denn die Aufgabe besteht gerade darin, ein solches Resultat zu beweisen.

**Wir wünschen viel Erfolg!**

Name:

Matrikelnummer:

---

**Aufgabe 1**

**(6 Punkte)**

- (a) Formulieren Sie den chinesischen Restsatz für ganze Zahlen.  
(b) Bestimmen Sie alle ganzen Zahlen  $a$ , die durch 3 und 7 teilbar sind und außerdem

$$a \equiv 1 \pmod{11}$$

erfüllen.

---

*Lösung.* (a) Sind  $m_1, \dots, m_r \in \mathbb{Z}$  paarweise teilerfremde Zahlen und  $a_1, \dots, a_r \in \mathbb{Z}$  beliebig, dann hat das System von Kongruenzen

$$x \equiv a_i \pmod{m_i} \quad (i = 1, \dots, r)$$

eine Lösung  $x \in \mathbb{Z}$ , die modulo  $m = m_1 \cdots m_r$  eindeutig bestimmt ist.

Ist  $M_i = m/m_i$  und sind  $x_1, \dots, x_r$  Lösungen der Gleichungen  $M_i x_i \equiv a_i \pmod{m_i}$ , dann ist  $x = \sum_{i=1}^r M_i x_i$  eine solche Lösung.

(Der Zusatz, der die Lösung hinschreibt, darf auch weggelassen werden. Die Version über kartesische Produkte wird auch akzeptiert.)

- (b) Wir suchen alle Vielfachen von  $3 \cdot 7 = 21$ , die kongruent 1 modulo 11 sind. Um die Kongruenz

$$21x_3 \equiv 1 \pmod{11}$$

zu lösen, teilen wir 21 durch 11, was Rest 10 ergibt. Das Inverse von 10 modulo 11 ist 10 selbst. Also ist  $21 \cdot 10 = 210$  eine Lösung. Die Lösung ist eindeutig modulo  $3 \cdot 7 \cdot 11 = 231$ . Alle Lösungen sind also  $210 + k \cdot 231$ ,  $k \in \mathbb{Z}$ . (Man kann auch die obige Beschreibung der Lösung verwenden, was auf dasselbe hinausläuft, nur etwas mehr zu schreiben ist.)

□

Name:

Matrikelnummer:

---

**Aufgabe 2**

**(5 Punkte)**

- (a) Bestimmen Sie alle Einheiten im Ring  $\mathbb{Z}/8$ .  
(b) Bestimmen Sie die Struktur der Einheitengruppe  $(\mathbb{Z}/8)^*$ .
- 

*Lösung.* (a) Die Einheiten in  $\mathbb{Z}/8$  sind gerade die Restklassen modulo 8 von Zahlen, die teilerfremd zu 8 sind. Das sind  $\bar{1}$ ,  $\bar{3}$ ,  $\bar{5}$  und  $\bar{7}$ .

(b) Nach (a) hat die Einheitengruppe vier Elemente. Sie ist also nach Vorlesung entweder die Kleinsche Vierergruppe  $C_2 \times C_2$  oder zyklisch der Ordnung vier. Wegen  $\bar{1}^2 = \bar{3}^2 = \bar{5}^2 = \bar{7}^2 = \bar{1}$  hat jedes Element die Ordnung 2. Also liegt der erste Fall vor.

□

Name:

Matrikelnummer:

---

**Aufgabe 3**

**(7 Punkte)**

- (a) Definieren Sie die Begriffe 'irreduzibel' und 'prim' für Elemente in einem Integritätsring.  
(b) Zeigen Sie, dass der Ring  $\mathbb{Z}[\sqrt{-31}]$  nicht faktoriell ist.  
(*Hinweis:* Betrachten Sie etwa Zerlegungen der Zahl 32 in diesem Ring.)
- 

*Lösung.* (a) Sei  $R$  ein Integritätsring. Ein Element  $c \in R$  heißt irreduzibel, wenn es nicht die Null ist und keine Einheit und für jede Zerlegung  $c = ab$  mit  $a, b \in R$  eines der Elemente  $a, b$  eine Einheit ist.

Ein Element  $p \in R$  heißt prim, wenn es nicht die Null ist und keine Einheit und folgendes gilt: Für alle  $a, b \in R$  ist  $p$  genau dann ein Teiler des Produkts  $ab$ , wenn  $p$  ein Teiler von  $a$  oder ein Teiler von  $b$  ist.

- (b) Es gilt  $32 = 2^5 = (1 + \sqrt{-31})(1 - \sqrt{-31})$ . Offenbar ist 2 kein Teiler von  $1 \pm \sqrt{-31}$ . Also ist 2 nicht prim. Es ist aber irreduzibel. Denn ist  $xy = 2$  mit  $x = a + b\sqrt{-31}$  und  $y = c + d\sqrt{-31}$ , so folgt  $x\bar{x}y\bar{y} = x\bar{x}y\bar{y} = 4$  und damit  $(a^2 + 31b^2)(c^2 + 31d^2) = 4$ . Das geht nur für  $b^2 = d^2 = 0$  und dann  $(a, c) = (2, 1)$  oder  $(a, c) = (1, 2)$ .

□

Name:

Matrikelnummer:

---

**Aufgabe 4**

**(6 Punkte)**

(a) Es sei  $C$  eine zyklische Gruppe der Ordnung 120 mit Erzeuger  $g$ . Zeigen Sie, dass

$$\langle g^{42} \rangle = \langle g^{54} \rangle$$

gilt.

(b) Es sei  $a = \frac{1}{2}$  und  $b = \frac{1}{3}$  und sei  $H = \langle a, b \rangle$  die von  $a$  und  $b$  erzeugte Untergruppe der additiven Gruppe  $(\mathbb{Q}, +)$ . Zeigen Sie, dass  $H$  zyklisch ist.

---

*Lösung.* (a) Es gilt  $42 = 6 \cdot 7$  und  $54 = 6 \cdot 9$  und damit  $\text{ggT}(42, 54) = 6$ . Das Element  $h = g^6$  erzeugt laut Vorlesung die eindeutige Untergruppe  $H = \langle h \rangle$  der Ordnung  $120/6 = 20$  von  $C$ . Also liegen  $g^{42} = h^7$  und  $g^{54} = h^9$  beide in  $H$ . Weil 7 und 9 teilerfremd zu 20 sind, sind  $h^7$  und  $h^9$  beides Erzeuger von  $H$ . Insgesamt gilt also  $\langle g^{42} \rangle = \langle g^{54} \rangle = \langle g^6 \rangle$ .

(b) Es gilt  $H = \{ra + sb \mid r, s \in \mathbb{Z}\}$  und deshalb  $a + b = \frac{5}{6} \in H$ . Damit auch  $c = \frac{1}{6} = -\frac{5}{6} + \frac{1}{2} + \frac{1}{2} \in H$ . Wegen  $a = 3c$  und  $b = 2c$  folgt  $H = \langle \frac{1}{6} \rangle$ .

□

Name:

Matrikelnummer:

---

**Aufgabe 5**

**(7 Punkte)**

Es sei  $G$  eine Gruppe, die auf einer Menge  $X$  operiert.

- (a) Definieren Sie die Begriffe 'Bahn' und 'Fixpunkt'.  
(b) Beweisen Sie, dass durch

$$x \sim y \Leftrightarrow \exists g \in G: gx = y$$

für  $x, y \in X$  eine Äquivalenzrelation  $\sim$  auf  $X$  definiert wird.

- (c) Sei  $G$  endlich der Ordnung 65 und  $X$  endlich mit 32 Elementen. Zeigen Sie, dass die Operation einen Fixpunkt besitzt.
- 

*Lösung.* (a) Die Bahn eines Punktes  $x \in X$  ist die Menge

$$Gx = \{gx \mid g \in G\}.$$

Ein Punkt  $x \in X$  heißt Fixpunkt, wenn  $gx = x$  für alle  $g \in G$  gilt (äquivalent wenn  $Gx = \{x\}$ ).

(b) Die Relation ist reflexiv, denn für  $x \in X$  gilt  $x = 1x$ , also  $x \sim x$ . Sie ist symmetrisch, denn aus  $x \sim y$ , etwa  $gx = y$ , folgt  $x = g^{-1}gx = g^{-1}y$  und damit  $y \sim x$ . Sie ist auch transitiv, denn aus  $x \sim y$  und  $y \sim z$  mit etwa  $gx = y$  und  $hy = z$  folgt  $hgx = hy = z$ , also  $x \sim z$ .

(c) Die Ordnung der Bahnen teilt die Gruppenordnung. Als Bahnlängen kommen also nur die Teiler 1, 5, 13, 65 von 65 in Frage. Weil  $X$  nur 32 Elemente hat, kann es keine Bahn mit 65 Elementen geben. Weil  $X$  die disjunkte Vereinigung der Bahnen ist, muss die Summe aller Bahnlängen gleich 32 sein. Die Zahl 32 ist aber nicht als Summe von positiven ganzzahligen Vielfachen von 5 und 13 darstellbar ( $2 \cdot 13 + 5 = 31$ ,  $6 \cdot 5 = 30$ ,  $13 + 3 \cdot 5 = 28$ , andere Kombinationen sind noch kleiner). Also muss es mindestens eine Bahn mit nur einem Element geben, das heißt einen Fixpunkt.

□

Name:

Matrikelnummer:

---

**Aufgabe 6**

**(6 Punkte)**

Geben Sie alle Untergruppen der symmetrischen Gruppe  $S_3$  an. Welche davon sind Normalteiler?

---

*Lösung.* Die Gruppe  $S_3$  hat die Ordnung 6, ihre nicht-trivialen Untergruppen deshalb die Ordnungen 2 und 3. Diese Untergruppen sind also alle zyklisch. Die Untergruppen der Ordnung 2 sind also

$$\langle(12)\rangle = \{\text{id}, (12)\}, \quad \langle(13)\rangle = \{\text{id}, (13)\}, \quad \langle(23)\rangle = \{\text{id}, (23)\}$$

und die Untergruppe der Ordnung 3 ist

$$\langle(123)\rangle = \{\text{id}, (123), (132)\}.$$

Da zwei Permutationen genau dann konjugiert sind, wenn sie die gleiche Zykelstruktur haben, sind die Untergruppen der Ordnung 2 nicht normal, die der Ordnung 3 dagegen schon. (Letztere ist die  $A_3$ ). □

Name:

Matrikelnummer:

**Aufgabe 7**

**(8 Punkte)**

Es sei  $f = x^3 - x + 1 \in \mathbb{Q}[x]$  und sei  $\alpha \in \mathbb{C}$  eine Nullstelle von  $f$ .

- (a) Zeigen Sie, dass  $f$  keine Nullstelle in  $\mathbb{Q}$  hat.
- (b) Stellen Sie  $\alpha^{-1}$  als Linearkombination von  $1, \alpha, \alpha^2$  mit rationalen Koeffizienten dar.
- (c) Bestimmen Sie das Minimalpolynom von  $\alpha^2$  über  $\mathbb{Q}$ .

*Lösung.* (a) Weil  $f$  normiert ist mit ganzzahligen Koeffizienten, ist nach dem Gaußschen Lemma jede Nullstelle von  $f$  in  $\mathbb{Q}$  ganzzahlig. Außerdem teilt jede Nullstelle den konstanten Term. Es kommen also nur 1 und  $-1$  als Nullstellen in Frage. Es gilt aber  $f(1) = 1 \neq 0$  und  $f(-1) = -1 \neq 0$ .

(b) Es gilt  $\alpha^3 - \alpha + 1 = 0$  und damit  $\alpha(-\alpha^2 + 1) = 1$ , also  $\alpha^{-1} = -\alpha^2 + 1$ .

(c) Setze  $\beta = \alpha^2$ . Dann gelten

$$\begin{aligned}\beta &= \alpha^2 \\ \beta^2 &= \alpha^4 = \alpha \cdot \alpha^3 = \alpha(\alpha - 1) = \alpha^2 - \alpha \\ \beta^3 &= \beta \cdot \beta^2 = \alpha^4 - \alpha^3 = \alpha^2 - \alpha - \alpha + 1 = \alpha^2 - 2\alpha + 1.\end{aligned}$$

Daraus sehen wir  $\beta^3 = 2\beta^2 - \beta + 1$ . Also ist  $\beta$  eine Nullstelle von  $g = x^3 - 2x^2 + x - 1$ . Dieses Polynom ist irreduzibel, denn es hat Grad 3 und keine Nullstelle in  $\mathbb{Q}$  (gleiche Argumentation wie in (a)). Also ist es das Minimalpolynom von  $\beta$ .

□

Name:

Matrikelnummer:

---

**Aufgabe 8**

**(7 Punkte)**

- (a) Es sei  $K \subset L$  eine endliche Körpererweiterung und  $f \in K[x]$  ein irreduzibles Polynom vom Grad  $n > 1$ . Zeigen Sie: Falls  $n$  den Grad  $[L : K]$  nicht teilt, dann hat  $f$  keine Nullstelle in  $L$ .
- (b) Es sei  $\alpha = \sqrt[3]{2}$  eine komplexe Kubikwurzel von 2. Ist die Körpererweiterung  $\mathbb{Q} \subset \mathbb{Q}(\alpha)$  eine Galois-Erweiterung? Begründen Sie die Antwort.
- 

*Lösung.* (a) Wäre  $\alpha \in L$  eine Nullstelle von  $f$ , dann würde  $[K(\alpha) : K] = n$  gelten, weil  $f$  irreduzibel ist. Es würde  $[L : K] = [L : K(\alpha)][K(\alpha) : K]$  folgen und damit  $n \mid [L : K]$ .

(b) Es ist keine Galois-Erweiterung. Das Polynom  $x^3 - 2$  hat in  $\mathbb{Q}(\alpha)$  eine Nullstelle. Es zerfällt aber nicht in Linearfaktoren, denn es gilt

$$x^3 - 2 = (x - \alpha)(x^2 + \alpha x + \alpha^2)$$

und der quadratische Faktor hat die Lösungen

$$x = \frac{-1 \pm \sqrt{-3}}{2} \cdot \alpha$$

in  $\mathbb{Q}(\alpha)$ . Wegen  $\sqrt{-3} \notin \mathbb{Q}(\alpha)$  (nach (a)), zerfällt  $x^3 - 2$  also nicht in Linearfaktoren. Weil dieses Polynom in  $\mathbb{Q}[x]$  irreduzibel ist, folgt daraus, dass  $\mathbb{Q}(\alpha)$  nicht normal über  $\mathbb{Q}$  ist.

□

Name:

Matrikelnummer:

---

**Aufgabe 9**

**(8 Punkte)**

- (a) Ist der Körper  $\mathbb{F}_9$  als Ring isomorph zu  $\mathbb{Z}/9$ ? Begründen Sie die Antwort.
  - (b) Welche Teilkörper hat der Körper  $\mathbb{F}_{729}$ ? (*Hinweis:*  $729 = 3^6$ ).
  - (c) Wie sieht die Galois-Gruppe von  $\mathbb{F}_{729}$  über  $\mathbb{F}_3$  aus?
  - (d) Geben Sie zu jedem der Teilkörper aus (b) die zugehörige Untergruppe der Galois-Gruppe an.
- 

*Lösung.* (a) Der Ring  $\mathbb{Z}/9$  ist kein Körper, denn wegen  $\overline{3}\overline{3} = \overline{9} = \overline{0}$  und  $\overline{3} \neq 0$  in  $\mathbb{Z}/9$  ist  $\overline{3}$  ein Nullteiler ungleich 0. Also kann  $\mathbb{Z}/9$  nicht zu  $\mathbb{F}_9$  isomorph sein.

(b) Laut Vorlesung hat  $\mathbb{F}_{729}$  genau einen Teilkörper der Ordnung  $3^k$  für jeden Teiler  $k$  von 6. Also enthält  $\mathbb{F}_{729}$  jeweils eine Kopie von  $\mathbb{F}_3$ ,  $\mathbb{F}_9$  und  $\mathbb{F}_{27}$ .

(c) Laut Vorlesung ist die Galois-Gruppe  $G = \text{Gal}(\mathbb{F}_{729}/\mathbb{F}_3)$  zyklisch der Ordnung 6, erzeugt vom Frobenius-Automorphismus  $\sigma$ .

(d) Die Gruppe  $G$  enthält genau eine Untergruppe der Ordnung 2, erzeugt von  $\sigma^3$ , und eine Untergruppe der Ordnung 3, erzeugt von  $\sigma^2$ . Die erste entspricht dem Zwischenkörper  $\mathbb{F}_{27}$  und die zweite dem Zwischenkörper  $\mathbb{F}_9$ .

□