

## KLAUSUR ZUR ALGEBRA UND ZAHLENTHEORIE

15. Februar 2017

### MUSTERLÖSUNG

**Nachname:**

---

**Vorname:**

---

**Matrikelnummer:**

---

**Studiengang:**

---

| Aufgabe   | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | Summe |
|-----------|---|---|---|---|---|---|---|---|---|-------|
| Punktzahl |   |   |   |   |   |   |   |   |   | /55   |

#### 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**.
- 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**

**(7 Punkte)**

Es seien  $f, g \in \mathbb{Q}[x]$  gegeben durch  $f = x^5 + x^2 - x + 1$  and  $g = x^3 - x^2 + x - 1$ .

- (a) Zerlegen Sie  $g$  in  $\mathbb{Q}[x]$  in seine irreduziblen Faktoren.
  - (b) Geben Sie die Definition eines größten gemeinsamen Teilers zweier Elemente  $a, b$  in einem kommutativen Ring  $R$  an.
  - (c) Bestimmen Sie den größten gemeinsamen Teiler von  $f$  und  $g$  in  $\mathbb{Q}[x]$  und  $p, q \in \mathbb{Q}[x]$  mit  $\text{ggT}(f, g) = pf + qg$ .
- 

*Lösung.* (a) Weil  $g$  normiert ist, sind  $x = \pm 1$  die einzig möglichen Nullstellen in  $\mathbb{Q}$ . Tatsächlich ist  $x = 1$  eine Nullstelle. Division ergibt  $g = (x - 1)(x^2 + 1)$ . Der Faktor  $x^2 + 1$  ist irreduzibel, denn er ist quadratisch und hat keine Nullstelle in  $\mathbb{Q}$ .

(b) Ein Element  $d \in R$  heißt ein größter gemeinsamer Teiler von  $a$  und  $b$ , wenn  $d|a$  und  $d|b$  gelten und außerdem  $e|d$  gilt für jedes  $e \in R$  mit  $e|a$  und  $e|b$ .

(c) Wir verwenden den euklidischen Algorithmus: Division mit Rest ergibt  $f = (x^2 + x)g + (x^2 + 1)$ . Die nächste Division  $g = (x - 1)(x^2 + 1)$  hat Rest 0. Also ist  $x^2 + 1$  bereits der ggT. Die gesuchte Darstellung ist

$$x^2 + 1 = f - (x^2 + x)g,$$

also  $p = 1$  und  $q = -x^2 - x$ .

□

Name:

Matrikelnummer:

---

**Aufgabe 2**

**(5 Punkte)**

Wieviele Elemente  $x$  mit  $x^2 = 1$  gibt es im Ring  $\mathbb{Z}/120$ ?

---

*Lösung.* Nach dem chinesischen Restsatz gilt  $\mathbb{Z}/120 \cong \mathbb{Z}/3 \times \mathbb{Z}/5 \times \mathbb{Z}/8$ . Es genügt also, die Gleichung  $x^2 = 1$  in jedem der Faktoren zu lösen. In  $\mathbb{Z}/3$  sind das die Restklassen  $\bar{1}$  und  $\bar{2} = -\bar{1}$ , ebenso in  $\mathbb{Z}/5$ . Die Einheiten in  $\mathbb{Z}/8$  sind  $\bar{1}, \bar{3}$  und  $\bar{5}$  und  $\bar{7}$ . Alle vier erfüllen die Gleichung. Insgesamt gibt es also  $2 \cdot 2 \cdot 4 = 16$  Lösungen in  $\mathbb{Z}/120$ . □

Name:

Matrikelnummer:

---

**Aufgabe 3**

**(5 Punkte)**

Bestimmen Sie alle Einheiten im Ring  $\mathbb{Z}[i]$  der Gaußschen ganzen Zahlen.

---

*Lösung.* Genau dann ist  $x = a + bi \in \mathbb{Z}[i]$  eine Einheit, wenn es  $y = c + di \in \mathbb{Z}[i]$  mit  $xy = 1$  gibt. Man kann nun entweder ausmultiplizieren und die entstehenden Gleichungen für Real- und Imaginärteil nach  $a, b$  lösen. Oder man benutzt die Multiplikativität des komplexen Absolutbetrags: Falls  $xy = 1$ , dann folgt  $|x||y| = |xy| = 1$ , also

$$(a^2 + b^2)(c^2 + d^2) = 1.$$

Wenn diese Gleichung in  $c, d$  eine Lösung hat, dann muss der erste Faktor gleich 1 sein, also

$$(a = \pm 1 \text{ und } b = 0) \quad \text{oder} \quad (a = 0 \text{ und } b = \pm 1)$$

gelten. Umgekehrt sind  $1, -1, i, -i$  tatsächlich Einheiten, mit Inversen  $1, -1, -i, i$ . □

Name:

Matrikelnummer:

---

**Aufgabe 4**

**(6 Punkte)**

- (a) Geben Sie alle abelschen Gruppen der Ordnung 36 bis auf Isomorphie an (ohne Beweis).  
(b) Zeigen Sie, dass es bis auf Isomorphie genau eine abelsche Gruppe  $G$  gibt, die genau 8 Elemente der Ordnung 3, 18 Elemente der Ordnung 9 und (außer dem neutralen Element) keine Elemente anderer Ordnung enthält.
- 

*Lösung.* (a) Es gilt  $36 = 2^2 \cdot 3^2$ . Die abelschen Gruppen dieser Ordnung sind deshalb

$$C_9 \times C_4, C_3 \times C_3 \times C_4, C_9 \times C_2 \times C_2, C_3 \times C_3 \times C_2 \times C_2$$

- (b) Falls  $G$  existiert, dann hat es insgesamt  $18 + 8 + 1 = 27 = 3^3$  Elemente. Die abelschen Gruppen dieser Ordnung sind  $C_{27}$ ,  $C_3 \times C_9$  und  $C_3 \times C_3 \times C_3$ . In der ersten gibt es ein Element der Ordnung 27, in der letzten kein Element der Ordnung 9. Also kommt nur  $G = C_3 \times C_9$  in Frage. Tatsächlich enthält  $C_9$  genau  $\varphi(9) = 6$  Elemente der Ordnung 9. Deshalb haben  $3 \cdot 6 = 18$  Elemente in  $C_3 \times C_9$  die Ordnung 9, nämlich alle Paare  $(a, b) \in C_3 \times C_9$ , in denen  $b$  die Ordnung 9 hat. Die übrigen  $27 - 1 - 18 = 8$  Elemente von  $C_3 \times C_9$  können nur die Ordnung 3 haben.

□

Name:

Matrikelnummer:

---

**Aufgabe 5**

**(7 Punkte)**

Es sei  $\sigma \in S_{10}$  durch

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 3 & 7 & 9 & 6 & 8 & 4 & 10 & 5 & 1 & 2 \end{pmatrix}$$

gegeben.

- (a) Zerlegen Sie  $\sigma$  in disjunkte Zyklen.
  - (b) Ist  $\sigma$  gerade oder ungerade? Begründen Sie die Antwort.
  - (c) Bestimmen Sie die Ordnung von  $\sigma$ .
  - (d) Finden Sie  $k \in \mathbb{N}$  mit  $k > 10$  derart, dass  $\sigma^k$  die Ordnung 3 hat.
- 

*Lösung.* (a) Es gilt  $\sigma = (1\ 3\ 9)(2\ 7\ 10)(4\ 6)(5\ 8)$ .

- (b) Gerade, denn Dreizykel sind gerade und das Produkt von zwei Transpositionen ist gerade.
- (c) Da die disjunkten Zyklen kommutieren, ist die Ordnung das kleinste gemeinsame Vielfache der Ordnungen aller Zyklen, also  $\text{kgV}(2, 3) = 6$ .
- (d) Da  $\sigma$  die Ordnung 6 hat, hat  $\sigma^i$  ebenfalls die Ordnung 6, wenn  $i$  und 6 teilerfremd sind. In diesem Fall hat dann  $\sigma^{2i}$  die Ordnung 3. Also muss  $k$  gerade und nicht durch 3 teilbar sein. Damit ist  $k = 14$  die kleinste geeignete Zahl.

□

Name:

Matrikelnummer:

---

**Aufgabe 6**

**(8 Punkte)**

Sei  $G = D_6$  die Symmetriegruppe des regelmäßigen Sechsecks. Sei  $a \in G$  eine erzeugende Drehung und  $b \in G$  eine Spiegelung.

- (a) Ist  $G$  eine abelsche Gruppe? Begründen Sie die Antwort.
  - (b) Bestimmen Sie die Untergruppen  $\langle b, ab \rangle$  und  $\langle b, a^2b \rangle$ . Um welche bekannte Gruppe handelt es sich jeweils?
  - (c) Finden Sie eine Untergruppe der Ordnung 4 in  $G$ .
- 

*Lösung.* (a)  $D_6$  ist keine abelsche Gruppe, denn es gilt  $bab^{-1} = a^{-1} = a^5 \neq a$ , also  $ba \neq ab$ .

(b) Es gilt  $b^2 = 1$  und deshalb  $a = ab \cdot b \in \langle a, ab \rangle$ . Also enthält  $\langle b, ab \rangle$  sowohl  $a$  als auch  $b$  und es folgt  $\langle b, ab \rangle = D_6$ . Genauso folgt  $a^2 \in \langle b, a^2b \rangle$  und deshalb  $\langle b, a^2b \rangle = \{\text{id}, a^2, a^4, b, a^2b, a^4b\}$ . Diese Untergruppe ist deshalb isomorph zu  $D_3 \cong S_3$ .

(c) Sei  $H = \langle a^3, b \rangle = \{\text{id}, a^3, b, a^3b\}$ . Jedes dieser Elemente ist zu sich selbst invers. Außerdem liegt das Produkt zweier Elemente von  $H$  wieder in  $H$ . (Es ist eine Kleinsche Vierergruppe.)

□

Name:

Matrikelnummer:

---

**Aufgabe 7**

**(5 Punkte)**

Sei  $\alpha \in \mathbb{C}$  mit  $\alpha^3 = 2$  und sei  $c \in \mathbb{Q}$ . Bestimmen Sie das Minimalpolynom von  $\alpha + c$  über  $\mathbb{Q}$ .

---

*Lösung.* Setze  $\beta = \alpha + c$ . Dann gilt also  $(\beta - c)^3 = \alpha^3 = 2$ . Also ist  $\beta$  eine Nullstelle des Polynoms

$$f = (x - c)^3 - 2 = x^3 - 3cx^2 + 3c^2x - c^3 - 2.$$

Dieses Polynom kann keine Nullstelle in  $\mathbb{Q}$  haben, denn  $f(a) = 0$  für  $a \in \mathbb{Q}$  würde  $(a - c)^3 = 2$  bedeuten, was nicht sein kann. Weil  $f$  den Grad 3 hat, folgt daraus, dass  $f$  irreduzibel ist. Da  $f$  außerdem normiert ist, ist es das Minimalpolynom von  $\beta$ .  $\square$

Name:

Matrikelnummer:

---

**Aufgabe 8**

**(5 Punkte)**

Beweisen Sie, dass jede endliche Körpererweiterung algebraisch ist.

---

*Lösung.* Sei  $K \subset L$  eine endliche Körpererweiterung. Per Definition heißt das, dass  $L$  als  $K$ -Vektorraum endliche Dimension hat. Ist  $\alpha \in L$ , dann kann die Familie  $(1, \alpha, \alpha^2, \dots)$  also nicht linear unabhängig über  $K$  sein. Es gibt also eine endliche lineare Relation  $\sum_{i=0}^n a_i \alpha^i = 0$ , in der nicht alle Koeffizienten 0 sind. Dann ist  $f = \sum_{i=0}^n a_i x^i$  ein Polynom ungleich 0 mit Koeffizienten in  $K$  und mit  $f(\alpha) = 0$ . Also ist  $\alpha$  algebraisch über  $K$ .

□

Name:

Matrikelnummer:

---

**Aufgabe 9**

**(7 Punkte)**

Es sei  $K$  ein Körper mit  $2^{12} = 4096$  Elementen. Zeigen Sie:

- (a) Es gibt ein Element  $\alpha \neq 1$  in  $K$  mit  $\alpha^{13} = 1$ .
  - (b) Es gilt  $K = \mathbb{F}_2(\alpha)$ .
- 

*Lösung.* (a) Die multiplikative Gruppe von  $K$  hat die Ordnung  $4096 - 1 = 4095 = 3^2 \cdot 5 \cdot 7 \cdot 13$ . Also ist 13 ein Teiler von  $|K^*|$ . Damit enthält  $K^*$  ein Element dieser Ordnung.

(b) Wäre  $\mathbb{F}_2(\alpha) \subsetneq K$ , dann müsste  $\alpha$  in einem echten Teilkörper von  $K$  liegen. Laut Vorlesung haben die Teilkörper von  $K$  die Ordnungen  $2^k$  mit  $k|12$ . Weil  $\alpha$  die Ordnung 13 hat, müsste  $2^k - 1$  dann durch 13 teilbar sein. Das ist aber für keine der Zahlen  $2^6 = 64$ ,  $2^4 = 16$ ,  $2^3 = 8$ ,  $2^2 = 4$  der Fall. Das zeigt die Behauptung.

□