Prof. Dr. Daniel Plaumann
Konstantinos Lentzos
Wintersemester 2016/2017

technische universität dortmund

KLAUSUR ZUR ALGEBRA I

15. Februar 2017

MUSTERLÖSUNG

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**.
- 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 I (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 $\mathrm{ggT}(f, g) = pf + qg$.

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 $\overline{1}$ und $\overline{2} = \overline{-1}$, ebenso in $\mathbb{Z}/5$. Die Einheiten in $\mathbb{Z}/8$ sind $\overline{1}, \overline{3}$ und $\overline{5}$ und $\overline{7}$. Alle vier erfüllen die Gleichung. Insgesamt gibt es also $2 \cdot 2 \cdot 4 = 16$ Lösungen in $\mathbb{Z}/120$. □

Name: **Matrikelnummer:**

Aufgabe 3 **(8 Punkte)**

Es sei $I = \{g \in \mathbb{R}[x] \mid g(2-i) = 0\}$ (mit $i = \sqrt{-1} \in \mathbb{C}$).
(a) Geben Sie die Definition eines Ideals in einem kommutativen Ring R.
(b) Zeigen Sie, dass I ein Ideal in $\mathbb{R}[x]$ ist.
(c) Finden Sie $f \in \mathbb{R}[x]$ mit $I = \langle f \rangle$.
(d) Zeigen Sie, dass $\mathbb{R}[x]/I$ zum Körper $\mathbb{C}$ isomorph ist.

Lösung. (a) Ein Ideal ist eine Teilmenge $I \subset R$ mit $I \neq \emptyset$ und folgenden beiden Eigenschaften:
(i) Für alle $a, b \in I$ gilt $a + b \in I$.
(ii) Für alle $r \in R$ und $a \in I$ gilt $ra \in I$.

(b) Es gilt $0 \in I$, also $I \neq \emptyset$. Für $f, g \in I$ folgt $(f+g)(2-i) = f(2-i)+g(2-i) = 0$. Für $r \in \mathbb{R}[x]$ und $f \in I$ gilt außerdem $(rf)(2-i) = r(2-i)f(2-i) = 0$.

(c) Es gilt $(2-i)^2 = 3 - 4i = 4(2-i) - 5$. Für $f = x^2 - 4x + 5$ gilt deshalb $f \in I$. Weil $\mathbb{R}[x]$ ein Hauptidealring ist und f irreduzibel ist, muss $I = \langle f \rangle$ gelten.

(d) Weil f das Minimalpolynom von $2-i$ ist, gilt $\mathbb{R}[x]/I \cong \mathbb{R}(2-i) = \mathbb{C}$. (Man kann das auch mit dem Isomorphiesatz nachprüfen.)

□

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 **(8 Punkte)**

Es sei G eine endliche Gruppe und seien H und K Untergruppen von G.
(a) Zeigen Sie $[H : H \cap K] \leq [G : K]$.
(b) Folgern Sie $[G : H \cap K] \leq [G : H] \cdot [G : K]$.

Lösung. (a) Wenn zwei Elemente $h, h' \in H$ dieselbe Rechtsnebenklasse $hK = h'K$ von K in G bestimmen, dann bedeutet das per Definition $h'h^{-1} \in K$ und damit $h'h^{-1} \in H \cap K$. Also folgt auch $h(H \cap K) = h'(H \cap K)$. Damit kann $H \cap K$ in H nicht mehr Nebenklassen haben als K in G.

(b) Nach Teil (a) gilt $[G : H] \cdot [G : K] \geq [G : H][H : H \cap K]$. Nach dem Satz von Lagrange gilt nun

$$[G : H][H : H \cap K] = \frac{|G|}{|H|} \cdot \frac{|H|}{|H \cap K|} = \frac{|G|}{|H \cap K|} = [G : H \cap K].$$

□

Name: **Matrikelnummer:**

Aufgabe 6 **(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 σ in disjunkte Zykel.

(b) Ist σ gerade oder ungerade? Begründen Sie die Antwort.

(c) Bestimmen Sie die Ordnung von σ.

(d) Finden Sie $k \in \mathbb{N}$ mit $k > 10$ derart, dass σ^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 Zykel kommutieren, ist die Ordnung das kleinste gemeinsame Vielfache der Ordnungen aller Zykel, also $\mathrm{kgV}(2, 3) = 6$.

(d) Da σ die Ordnung 6 hat, hat σ^i ebenfalls die Ordnung 6, wenn i und 6 teilerfremd sind. In diesem Fall hat dann σ^{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 7 **(7 Punkte)**

Beweisen Sie:
(a) Jede endliche Körpererweiterung ist algebraisch.
(b) In einer Körpererweiterung $K \subset L$ bilden die über K algebraischen Elemente von L einen Teilkörper.

Lösung. (a) 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 Koeffzienten in K und mit $f(\alpha) = 0$. Also ist α algebraisch über K.
(b) Seien $\alpha, \beta \in L$ algebraisch. Dann ist $K(\alpha)$ endlich über K und $K(\alpha, \beta) = K(\alpha)(\beta)$ endlich über $K(\alpha)$. Also ist $K(\alpha, \beta)$ endlich über K und damit nach (a) algebraisch. Weil $K(\alpha, \beta)$ die Elemente $\alpha \pm \beta$ und $\alpha\beta$, $\alpha\beta^{-1}$ (falls $\beta \neq 0$) enthält, zeigt das die Behauptung.

□

Name: **Matrikelnummer:**

Aufgabe 8 **(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 α in einem echten Teilkörper von K liegen. Laut Vorlesung haben die Teilkörper von K die Ordnungen 2^k mit $k|12$. Weil α 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.

□

Name: **Matrikelnummer:**

Aufgabe 9 **(5 Punkte)**

Gibt es ein irreduzibles Polynom in $\mathbb{Q}[x]$, das in $\mathbb{C}$ eine mehrfache Nullstelle besitzt? Begründen Sie die Antwort.

Lösung. Es gibt kein solches Polynom. Denn laut Vorlesung müsste ein solches Polynom f eine Nullstelle α mit seiner Ableitung f' gemein haben. Dann haben f und f' aber auch einen gemeinsamen Teiler in $\mathbb{Q}[x]$, nämlich das Minimalpolynom von α. Weil f kleineren Grad als f' hat und irreduzibel ist, ist das unmöglich. □