Prof. Dr. Peter Bürgisser
Jesko Hüttenhain

Technische Universität Berlin, Fakultät II,
Institut für Mathematik, Sekretariat MA 3-2

Übungen zur Vorlesung Algebra 1

Wintersemester 2013, zweite Hälfte

Aufgabenzettel 9

Auf diesem Übungszettel sind insgesamt 100 Punkte erreichbar, für die Gesamtwertung zählt der Zettel jedoch mit den üblichen 50 Punkten, d.h. es können Bonuspunkte erzielt werden, welche für die Gesamtwertung und die Zulassung zählen. Wir wünschen frohe Weihnachten!

Aufgabe 1 (4 Punkte). Sei $\phi : A \to B$ ein Homomorphismus kommutativer Ringe.

(a) Zeige: Wenn $P \subseteq B$ ein Primideal ist, dann ist $\phi^{-1}(P)$ ein Primideal von A.

(b) Zeige anhand eines Beispiels, dass das Urbild maximaler Ideale nicht notwendigerweise maximal sein muss.

Aufgabe 2 (12 Punkte). Sei $\mathbb{K}$ ein endlicher Körper.

(a) Zeige, dass es eine Primzahl p und ein $n \in \mathbb{N}$ gibt, so dass $|\mathbb{K}| = p^n$.

(b) Warum gibt es keinen Integritätsbereich mit genau 55 Elementen?

Aufgabe 3 (8 Punkte). Sei $\phi : A \to B$ ein Homomorphismus kommutativer Ringe.

(a) Zeige, dass ϕ injektiv ist, wenn A ein Körper und $B \neq \{ 0 \}$ ist.

(b) Kann es einen Homomorphismus zwischen Körpern unterschiedlicher Charakteristik geben?

Aufgabe 4 (8 Punkte). Angenommen, $n = pq$ für verschiedene Primzahlen p und q. Angenommen, der Wert $f := \varphi(n) = |\mathbb{Z}_n^\times|$ ist bekannt.

(a) Beschreibe ein Verfahren, um aus diesen Daten die Zahlen p und q zu ermitteln.

(b) Wende Dein Verfahren auf $n = 2329059851$ und $f = 2328954192$ an. Das Verwenden eines Taschenrechners oder eines Computers ist ausdrücklich erlaubt.

Aufgabe 5 (8 Punkte). Sei $f \in \mathbb{F}_2[X]$ und $R := \mathbb{F}_2[X]/(f)$. Bezeichne mit x das Bild von X in R.

(a) Zeige, dass für $f = X^5 + X^2 + 1$ das Inverse von $x + x^2 + x^4$ in R gleich x^3 ist.

(b) Sei $f = X^4 + X^3 + 1$. Zeige, dass $x + 1 \in R^\times$ und berechne $(x + 1)^{-1}$.

Aufgabe 6 (10 Punkte). Sei $\mathbb{K}$ ein Körper. Zeige:

(a) Es gibt in $\mathbb{K}[X]$ unendlich viele normierte Primpolynome.

(b) Falls jedes nicht-konstante Polynom aus $\mathbb{K}[X]$ eine Nullstelle in $\mathbb{K}$ besitzt, so ist $\mathbb{K}$ nicht endlich.

Die Abgabe erfolgt bis **Mittwoch**, den **08.01.2014** in der Übung. Gutes Gelingen!

Im Folgenden gilt, dass die zu beweisenden Aussagen jeder Aufgabe für das Lösen der darauffolgenden Aufgaben sehr hilfreich oder sogar unabdingbar sind. Solche Aussagen dürfen stets verwendet werden, selbst wenn die entsprechende Aufgabe nicht bearbeitet wurde.

Aufgabe 7 ($5+5+4+2=16$ Punkte).

(a) Sei G eine endliche, abelsche Gruppe und $m := \max\{\operatorname{ord}(g) \mid g \in G\}$. Zeige, dass $\forall g \in G\colon\ \operatorname{ord}(g) \mid m$.

(b) Sei $\mathbb{K}$ ein beliebiger Körper. Man zeige, dass es zu jeder natürlichen Zahl $n > 1$ höchstens $n-1$ Elemente der Ordnung n in $\mathbb{K}^\times$ gibt.

(c) Sei $\mathbb{K}$ ein endlicher Körper. Zeige, dass $\mathbb{K}^\times$ zyklisch ist. Verwende dazu die Aufgabenteile (a) und (b).

(d) Was ist die Anzahl der primitiven Elemente in $\mathbb{Z}_p^\times$? Ein primitives Element ist ein $x \in \mathbb{Z}_p^\times$, so dass x ganz $\mathbb{Z}_p^\times$ als Gruppe erzeugt. Siehe auch Aufgabe 1 von Zettel 3. Gib einen Erzeuger von $\mathbb{F}_{11}^\times$ an.

Aufgabe 8 ($5+5+4=14$ Punkte). Sei $\mathbb{K}$ ein endlicher Körper mit $\operatorname{char}(\mathbb{K}) \neq 2$.

(a) Zeige, dass $(\mathbb{K}^\times)^2 := \{a^2 \mid a \in \mathbb{K}^\times\}$ eine Untergruppe von $\mathbb{K}^\times$ vom Index 2 ist.

(b) Sei p eine Primzahl und $\pi : \mathbb{Z} \to \mathbb{Z}_p$ der kanonische Homomorphismus. Zeige, dass $\pi(-1) \in (\mathbb{Z}_p^\times)^2$ genau dann, wenn $p = 2$ oder $4 \mid (p-1)$.

(c) Seien $x, y \in \mathbb{Z}$ so, dass $x^2 + y^2 = p$ eine ungerade Primzahl ist. Zeige, dass dann $p-1$ durch 4 teilbar ist.

Aufgabe 9 ($2+5+3+4+6=20$ Punkte). Sei $i \in \mathbb{C}$ die imaginäre Einheit. Wir betrachten den *Ring der Gaußschen Zahlen* $\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$ zusammen mit $\delta : \mathbb{Z}[i] \to \mathbb{N}$, definiert als

$$\delta(a+bi) := \|a+bi\|^2 = a^2 + b^2.$$

(a) Zeige, dass $\delta(xy) = \delta(x)\delta(y)$ für alle $x, y \in \mathbb{Z}[i]$ gilt. Zeige ferner, dass jedes $x \in \mathbb{Z}[i]$ ein Teiler von $\delta(x) \in \mathbb{Z} \subseteq \mathbb{Z}[i]$ ist.

(b) Zeige, dass $\mathbb{Z}[i]$ ein Euklidischer Ring bezüglich δ ist.

(c) Zeige, dass $2 \in \mathbb{Z}[i]$ nicht irreduzibel ist.

(d) Beschreibe die Einheiten in $\mathbb{Z}[i]$.

(e) Zeige, dass für ein irreduzibles $z \in \mathbb{Z}[i]$ die Norm $d := \delta(z)$ entweder eine Primzahl oder das Quadrat einer Primzahl ist. Welche Form hat z in den beiden Fällen?