8.Übungsblatt zur Algebra

Anne Henke, Sam Thelin, WS 2018

1. (Zum Votieren.) Bob hatte Alice nie zuvor so wütend gesehen, wie in dem Moment, als Eve plötzlich vor der Tür stand. Dabei versteht er nicht, was Alice eigentlich gegen Eve hat. Er selbst findet beide in Ordnung: Alice ist echt lieb, aber dafür hat Eve immer das beste Geschwätz parat. Eine gewaltige Standpauke hat Alice ihm gehalten, für das mit den Zetteln. War doch letztendlich ihr Fehler, solche banalen Krypto-Methoden zu verwenden. Jetzt RSA, ordentliches Zeug. Alice öffentlicher Schlüssel lautet $(2^4 + 1, 55)$. Die Zahlen kommen ihm schon etwas klein vor, aber das macht bestimmt keinen großen Unterschied. Den Monat und den Tag ihres nächsten Treffens muss er jetzt getrennt verschlüsseln: 29. Dezember. Dabei hat Alice ihm alle technischen Hilfsmittel verboten, sogar einen arglosen Taschenrechner darf er nicht benutzen. Sie meinte, dieser Marvin-Typ hat für Eve alles gehackt. Lächerlich. Obendrein hätte er eigentlich nichts dagegen, dass Eve auch dabei wäre. Nur Alices Wutausbruch war echt heftig, der hat ihm ernsthaft Angst gemacht. Also Stift und Papier her. Aber 17 Multiplikationen, und das zweimal. Dabei hat er einen Riesenhunger. Und dass Eve $2^4 + 1$ statt einfach 17 geschrieben hat, das geht ihm schon ganz schön auf den Sack. Blöde Angeberei! Oder? Helfen Sie Bob, das Datum (ohne Taschenrechner!) durch deutlich weniger als 34 Multiplikationen zu verschlüsseln, damit der arme Kerl sich erst einmal etwas beruhigen kann.

2. (Schriftlich, 10 Punkte.)

   (a) Bestimmen Sie Primzahlen $p_1, \ldots, p_n$ und natürliche Zahlen $k_1, \ldots, k_n$ mit

   $$\mathbb{Z}_{360} \simeq \mathbb{Z}_{p_1^{k_1}} \times \cdots \times \mathbb{Z}_{p_n^{k_n}},$$

   und berechnen Sie $|\mathbb{Z}_{360}^\times|$.

   (b) Seien a, b und n ganze Zahlen mit $n \neq 0$, und sei $a \equiv b \mod n$. Zeigen Sie, dass $\mathrm{ggT}(a, n)$ ein Teiler von b ist.

   (c) Zeigen Sie, dass wenn $x^5 \equiv 1 \mod 360$ ist, dann gilt $\mathrm{ggT}(x, 360) = 1$. Folgern Sie, dass 1 die einzige ganze Zahl im Intervall $1 \leq x \leq 360$ ist, die $x^5 \equiv 1 \mod 360$ erfüllt. (*Hinweis:* Welche Ordnungen sind für Elemente in $\mathbb{Z}_{360}^\times$ möglich).

   (d) Wieviele ganze Zahlen im Intervall $1 \leq x \leq 360$ erfüllen $x^2 \equiv 1 \mod 360$? (*Hinweis:* Verwenden Sie Teil (a) und Aufgabe 5(a) auf Übungsblatt 4).

   Begründen Sie jeweils Ihre Antwort.

3. (Schriftlich, 10 Punkte.) Seien R und S kommutative Ringe mit Eins.

   (a) Seien I_1 und I_2 Primideale von R. Beweisen oder widerlegen Sie die folgenden Aussagen.

      i. Das Ideal $I_1 + I_2$ ist immer ein Primideal.

      ii. Das Ideal $I_1 \cap I_2$ ist genau dann ein Primideal, wenn $I_1 \subseteq I_2$ oder $I_2 \subseteq I_1$ gilt.

   (b) Sei I ein Primideal von R und J ein Primideal von S. Ist $I \times J$ ein Primideal von $R \times S$?

   (c) Sei I ein Ideal von R. Gibt es eine inklusionserhaltende Korrespondenz zwischen den Primidealen J von R mit $I \subseteq J$ und den Primidealen von R/I?

   Begründen Sie jeweils Ihre Antwort.

4. (Zum Votieren.) In dieser Aufgabe zeigen wir, dass wenn p eine Primzahl mit $p \equiv 1 \mod 4$ ist, dann existiert $a \in \mathbb{Z}$ mit $a^2 \equiv -1 \mod p$. Sei p zunächst eine ungerade Primzahl.

   (a) Zeigen Sie: Ist $x^2 \equiv 1 \mod p$, dann gilt $x \equiv \pm 1 \mod p$.

   (b) Zeigen Sie, dass die Abbildung $\sigma\colon \mathbb{Z}_p^\times \to \mathbb{Z}_p^\times : x \mapsto x^2$ ein Gruppenhomomorphismus ist. Bestimmen Sie $\mathrm{Ker}(\sigma)$.

   (c) Sie jetzt p eine Primzahl mit $p \equiv 1 \mod 4$. Zeigen Sie, dass $\mathrm{im}(\sigma)$ eine Gruppe gerader Ordnung ist. Folgern Sie, dass es $a \in \mathbb{Z}$ existiert mit $a^2 \equiv -1 \mod p$ (*Hinweis*: Jede Gruppe gerader Ordnung besitzt ein Element der Ordnung 2).

5. (Zum Votieren.) Sei X eine nicht leere, endliche Menge. Wir betrachten den Ring $R = \mathcal{P}(X) = \{U \mid U \subseteq X\}$ mit Addition und Multiplikation definiert durch

$$a + b = (a \cup b) \setminus (a \cap b) \text{ und}$$
$$a \cdot b = a \cap b.$$

   Sei I ein Ideal von R.

   (a) Zeigen Sie: Wenn $a \in I$ und $c \subseteq a$, dann gilt $c \in I$.

   (b) Zeigen Sie: Wenn $a, b \in I$, dann folgt $a \cup b \in I$.

   (c) Folgern Sie: Jedes Ideal I von R hat die Form $I = \mathcal{P}(Y) = \{U \mid U \subseteq Y\}$ für eine Untermenge $Y \subseteq X$.

   (d) Bestimmen Sie alle maximalen Ideale von R.

   (e) Bestimmen Sie alle Primideale von R.

   Begründen Sie jeweils Ihre Antwort.

6. (Zum Selbststudium.) Sei R ein kommutativer Ring mit Eins. Die *Charakteristik* von R, Notation $\mathrm{char}(R)$, ist definiert als die kleinste Zahl $n \in \mathbb{N}_{>0}$ mit

$$0_R = n \cdot 1_R := 1_R + 1_R + \ldots + 1_R$$

   und sie ist definiert als 0, falls $n \cdot 1_R \neq 0$ für alle $n \in \mathbb{N}_{>0}$.

   (a) Gibt es einen Ring R mit $\mathrm{char}(R) = 6$?

   (b) Gibt es einen Integritätsbereich R mit $\mathrm{char}(R) = 6$?

   (c) Gibt es Integritätsbereiche R_1 und R_2 mit $\mathrm{char}(R_1) < \mathrm{char}(R_2)$, sodass ein Ringhomomorphismus $\phi : R_1 \to R_2$ existiert?

   (d) Gibt es Integritätsbereiche R_1 und R_2 mit $\mathrm{char}(R_1) > \mathrm{char}(R_2)$, sodass ein Ringhomomorphismus $\phi : R_1 \to R_2$ existiert?

   (e) Sei p eine Primzahl und sei $\mathrm{char}(R) = p$. Ist die Abbildung $\varphi\colon R \to R, x \mapsto x^p$ ein Ringhomomorphismus?

   Begründen Sie jeweils Ihre Antwort.