D-MATH Algebra I HS20
Prof. Manfred Einsiedler

Serie 4

Euklidische Ringe

1. Sei R ein Integritätsbereich und $f, g \in R \setminus \{0\}$. Seien d, d' zwei grösste gemeinsame Teiler von f und g. Zeigen Sie, dass es eine Einheit $c \in R^\times$ gibt, so dass $d = cd'$. In anderen Worten, ein grösster gemeinsamer Teiler ist bis auf Multiplikation mit einer Einheit eindeutig.

2. Sei n eine positive natürliche Zahl. Bestimmen Sie alle invertierbaren Elemente im Ring $\mathbb{Z}[\sqrt{-n}] = \mathbb{Z} + \sqrt{-n}\mathbb{Z} \subseteq \mathbb{C}$.

   Hinweis: Benutzen Sie eine Normfunktion.

3. Sei R ein kommutativer Ring und sei $\mathrm{Mat}_{nn}(R)$ der Ring der $n \times n$-Matrizen mit Koeffizienten in R mit der üblichen Addition und Multiplikation.

   Definition: Sei S ein nichtkommutativer Ring. Ein *zweiseitiges Ideal in S* ist eine Teilmenge $J \subseteq S$ so dass $0 \in J$ und $j, j' \in J \implies j + j' \in J$ und $j \in J$, $s \in S \implies js,\ sj \in J$.

   (a) Zeigen Sie: Ist $I \subseteq R$ ein Ideal, so ist

   $$\mathrm{Mat}_{nn}(I) := \{M = (m_{ij})_{1 \leqslant i,j \leqslant n} \in \mathrm{Mat}_{nn}(R) | m_{ij} \in I \text{ für alle } 1 \leqslant i, j \leqslant n\}$$

   ein zweiseitiges Ideal in $\mathrm{Mat}_{nn}(R)$.

   (b) Zeigen Sie: Jedes zweiseitige Ideal in $\mathrm{Mat}_{nn}(R)$ ist von der Form $\mathrm{Mat}_{nn}(I)$ für ein geeignetes Ideal $I \subseteq R$.

   Bemerkung: Ist J ein zweiseitiges Ideal in einem nicht-kommutativen Ring S, dann hat S/J wieder eine Ringstruktur. In unserem Beispiel kann man sogar zeigen, dass $\mathrm{Mat}_{nn}(R/I) \cong \mathrm{Mat}_{nn}(R)/\mathrm{Mat}_{nn}(I)$, also, dass der Faktorring wieder ein Matrixring über einem kommutativen Ring ist.

4. (a) (**SAGE**) Schreiben Sie eine Method in SAGE, die den euklidischen Algorithmus implementiert und daher den grössten gemeinsamen Teiler von zwei Elementen berechnet.

   Hinweis: Verwenden Sie hierzu %, um den Rest der Division zu bestimmen. Überspringen Sie Schritt 0 in der Definition des euklidischen Algorithmus, da es keine Rolle spielt und dies die Implementierung einer Normfunktion verhindert. (Frage: Warum?)

(b) Verifizieren Sie mit der obigen Methode Ihre Rechnungen in der Aufgabe 5 (a)-(d).

Hinweis: Hilfreiche Stichwörter, nach denen Sie im Sage Handbuch suchen können: PolynomialRing, FractionField, GF (steht für Galois field). Bei der Verifikation von Aufgabe 5 (d) gibt es Probleme bei der Benutzung von %, falls eines der Argumente des euklidischen Algorithmus' die Variable T ist (dies gibt einen Fehler obwohl T eine Einheit in $K[X]$ ist, % sollte also 0 ausgeben). Sie können diesen Fehler vermeinden, indem Sie vor Anwendung von % überprüfen, ob die Argumente Einheiten sind, und in diesem Fall das richtige Ergebnis direkt ausgeben lassen. Wichtig ist hierbei zu beachten, dass T als Element verschiedener Ringe aufgefasst werden kann und nicht in allen eine Einheit ist.

5. (a) Betrachten Sie die Polynome $p, q \in \mathbb{Q}[X]$ definiert durch

$$p := X^3 - \frac{5}{2}X^2 + \frac{3}{2}X \text{ und } q = 2X^2 - X - 3.$$

Berechnen Sie die Division mit Rest von p durch q.

(b) Finden Sie einen Erzeuger des Hauptideals $(p, q) \subseteq \mathbb{Q}[X]$.

(c) Benutzen Sie Division mit Rest in $\mathbb{F}_3[X]$, wobei $\mathbb{F}_3 = \mathbb{Z}/3\mathbb{Z}$ der Körper mit drei Elementen ist, um zu zeigen, dass die Ideale $(X^4 + 2X + 1)$ und $(X^2 + X - 1)$ in $\mathbb{F}_3[X]$ koprim sind.

Erinnerung: Zwei Ideale $I, J \subseteq R$ in einem Ring R heissen koprim, falls $I + J = R$.

(d) Sei $K = \mathbb{Q}(T)$. Berechnen Sie die Division mit Rest in $K[X]$ von

$$f = X^3 + TX^2 - 1 \text{ durch } g = (1 + T)X^2 - 1.$$

6. Sei K ein unendlicher Körper.

(a) Angenommen $P \in K[X]$ ist ein Polynom, so dass $P(\alpha) = 0$ für alle $\alpha \in K$ gilt. Zeigen Sie, dass $P = 0$ in $K[X]$.

(b) Angenommen $P \in K[X_1, \ldots, X_n]$ ist ein Polynom, so dass $P(\alpha) = 0$ für alle $\alpha = (\alpha_1, \ldots, \alpha_n) \in K^n$ gilt. Zeigen Sie, dass $P = 0$ in $K[X_1, \ldots, X_n]$.

Hinweis: Machen Sie eine Induktion über n und benutzen Sie Aufgabenteil *(a)*.