Übungsblatt 3: Ringe und Polynome

1. Integritätsringe

V 1.1. Zeigen Sie, dass jeder endliche Integritätsring ein Körper ist.

S 1.2. (4 Punkte) Sei R ein Ring und $K \subset R$ ein Teilkörper. Zeigen Sie:
(a) Der Ring R ist auf natürliche Weise ein Vektorraum über K.
(b) Wir nehmen zusätzlich an, dass R ein Integritätsring mit $\dim_K R < \infty$ ist. Dann ist R ein Körper. *Zusatz:* Gilt das auch noch für $\dim_K R = \infty$?

2. Lokalisation

Sei R ein kommutativer Ring und S ein Untermonoid von $(R,\cdot)$, also eine multiplikativ abgeschlossene Teilmenge von R, die die 1 enthält. Wir betrachten auf $R \times S$ die Relation

$$(r,s) \sim (r',s') \quad \Leftrightarrow \quad \exists\, \bar{s} \in S : \ \bar{s}(rs' - r's) = 0$$

V 2.1. (a) Zeigen Sie, dass $\sim$ eine Äquivalenzrelation ist und die Verknüpfungen

$$\frac{r}{s} + \frac{r'}{s'} = \frac{rs' + r's}{ss'} \quad \text{und} \quad \frac{r}{s} \cdot \frac{r'}{s'} = \frac{rr'}{ss'}$$

wohldefiniert sind, wenn wir mit $\frac{r}{s}$ die Äquivalenzklasse des Elements (r,s) bezüglich der Relation $\sim$ bezeichnen.
(b) Folgern Sie, dass die Menge $S^{-1}R$ der Äquivalenzklassen damit zu einem kommutativen Ring wird. Warum ist dies eine Verallgemeinerung der Konstruktion des Bruchkörpers aus der Vorlesung?
(c) Betrachten Sie $R = \mathbb{Z}/6$ mit $S_1 = \{\overline{1}, \overline{3}\}$, $S_2 = R^\times$ und $S_3 = R$. Wieviele Elemente hat $S_i^{-1}R$ für $i \in \{1,2,3\}$? Gibt es noch andere multiplikativ abgeschlossene Mengen in $\mathbb{Z}/6$?

S 2.2. (2 Punkte) Zeigen Sie, dass die Abbildung $R \to S^{-1}R : r \mapsto \frac{r}{1}$ genau dann injektiv ist, wenn $S \subset R^*$ keine Nullteiler von R enthält.

V 2.3. Zeigen Sie, dass die Abbildung $R \to S^{-1}R : r \mapsto \frac{r}{1}$ surjektiv ist, wenn $S \subset R^\times$.

3. Polynomringe

V 3.1. $P \in \mathbb{Z}[X]$ hat keine Nullstellen in $\mathbb{Z}$ wenn $P(0)$ und $P(1)$ ungerade sind.

V 3.2. Man bestimme die Gruppe $\mathbb{Z}/4[X]^\times$ der invertierbaren Elemente in $\mathbb{Z}/4[X]$.

S 3.3. (3 Punkte) Sei $\mathbb{F}_4 := (\mathbb{Z}/2[X])/(X^2+X+1)$.
(a) Bestimmen Sie die Anzahl der Elemente von $\mathbb{F}_4$ und zählen sie diese auf.
(b) Erstellen Sie die Additions- und Multiplikationstafeln von $\mathbb{F}_4$.
(c) Ist der Quotientenring $\mathbb{F}_4$ ein Körper?

4. Polynomielle Abbildungen

Sei $K[X]$ der Polynomring über dem Körper K.
Für $p = \sum_{k=0}^{n} a_k X^k$ sei die Abbildung $f_p : K \to K$ durch $x \mapsto p(x) = \sum_{k=0}^{n} a_k x^k$ gegeben.

4.1. Die Abbildung $\varphi : K[X] \to K^K : p \mapsto f_p$ ist ein Ringhomorphismus.

V 4.2. Wenn K unendlich viele Elemente hat, dann ist φ injektiv, aber nicht surjektiv.

V 4.3. Wenn K endlich ist, dann ist φ surjektiv, aber nicht injektiv.

5. Charakterisierung des Polynomrings über einem Körper

5.1. Ist $R = K[X]$ der Polynomring über einem Körper K, dann definiert der Grad eine surjektive Abbildung $\nu\colon R \to \mathbb{N} \cup \{-\infty\}$, die folgende Eigenschaften erfüllt:
(1) Für $a, b \in R$ mit $b \neq 0$ existieren $c, d \in R$ so dass $a = bc + d$ mit $\nu(d) < \nu(b)$.
(2) Für alle $a, b \in R$ gilt $\nu(ab) = \nu(a) + \nu(b)$ und $\nu(a+b) \leq \sup\{\nu(a), \nu(b)\}$ mit Gleichheit wenn $\nu(a) \neq \nu(b)$.

V 5.2. Sei R ein kommutativer Ring mit einer surjektiven Abbildung $\nu\colon R \to \mathbb{N} \cup \{-\infty\}$, die obige Eigenschaften (1) und (2) erfüllt.
(a) Man zeige $\nu(a) = -\infty \Leftrightarrow a = 0$ und $\nu(a) = 0 \Leftrightarrow a \in R^\times$.
(b) Man zeige, dass $K = \{\, a \in R \mid \nu(a) \leq 0 \,\}$ ein Unterkörper von R ist.
(c) Für $X \in R$ mit $\nu(X) = 1$ ist $R = K[X]$ der Polynomring in X und $\nu = \deg$.

6. Gruppenringe

S 6.1. (2 Punkte) Sei R ein Integritätsring und G eine Gruppe. Wenn es ein Element $g \in G$ endlicher Ordnung gibt, also $g \neq 1$ aber $g^n = 1$ für ein $n \geq 1$, dann hat der Gruppenring $R[G]$ Nullteiler. *Hinweis:* endliche geometrische Reihe.

Eine berühmte Vermutung von Kaplansky fragt nach der Umkehrung: Wenn eine Gruppe G keine Elemente endlicher Ordnung hat, dann hat der Gruppenring $R[G]$ keine Nullteiler. Diese Vermutung ist bis heute offen.

7. Potenzreihenringe

Wir sagen in einem Monoid $(M, \cdot)$ gilt *endliche Zerlegbarkeit* wenn zu jedem $m \in M$ nur endlich viele Paare $(a, b) \in M \times M$ existieren, die $ab = m$ erfüllen Dies gilt zum Beispiel für $(\mathbb{N}, +)$ und $(\mathbb{N}^d, +)$, nicht aber für $(\mathbb{Z}, +)$ und $(\mathbb{Q}_{\geq 0}, +)$.

V 7.1. Sei R ein kommutativer Ring und M ein Monoid, in dem endliche Zerlegbarkeit gilt. Auf der Menge $S = R^M$ aller Abbildungen definieren wir Summe und Produkt wie im Skript angegeben. Man weise nach, dass $(S, +, \cdot)$ ein Ring ist. Der Ring S ist genau dann kommutativ wenn das Monoid M kommutativ ist.

Für das Monoid $(\mathbb{N}, +)$ betrachten wir Abbildungen $f\colon \mathbb{N} \to R$. Wir stellen uns f vor als eine unendliche Summe $\sum_{k=0}^{\infty} f_k X^k$. Hier hat das Summenzeichen $\sum$ nur einen symbolischen Sinn: algebraisch können wir nur Summen für endlich viele Terme definieren. Für Summe und Produkt gilt in dieser Schreibweise

$$\Big(\sum_{k=0}^{\infty} f_k X^k\Big) + \Big(\sum_{k=0}^{\infty} g_k X^k\Big) = \sum_{k=0}^{\infty} (f_k + g_k) X^k$$

$$\Big(\sum_{k=0}^{\infty} f_k X^k\Big) \cdot \Big(\sum_{\ell=0}^{\infty} g_\ell X^\ell\Big) = \sum_{n=0}^{\infty} \Big(\sum_{k+\ell=n} f_k g_\ell\Big) X^n$$

Den so entstehenden Ring $R[[X]]$ nennt man den Ring der *Potenzreihen* über R. Zur Betonung spricht man von *formalen Potenzreihen*, denn anders als in der Analysis umgehen wir hier alle Fragen der Konvergenz: Diese Potenzreihen sind nur formale Ausdrücke und beschreiben nicht etwa Funktionen. Wichtig ist allein, dass sie einen Ring bilden.

V 7.2. Man bestimme die invertierbaren Elemente in $R[[X]]$.
Wenn R ein Integritätsring ist, ist dann auch $R[[X]]$ ein Integritätsring?
Für jedes $n \in \mathbb{N}$ ist $\mathfrak{m}^n = \{\, \sum_{k=n}^{\infty} f_k X^k \mid f_k \in R \}$ ein Ideal in $R[[X]]$.
Ist R ein Körper, so sind $\mathfrak{m}^0, \mathfrak{m}^1, \mathfrak{m}^2, \ldots, \{0\}$ die einzigen Ideale des Rings $R[[X]]$.