Aufgabe 1 (5 Punkte)

Zeigen Sie: Ist K ein Körper, so gibt es unendlich viele normierte irreduzible Polynome über K.

Hinweis: Imitieren Sie den Beweis für die analoge Aussage über Primzahlen.

Lösungsskizze. Für unendliche Körper bilden die Polynome $T-a$ für $a \in K$ schon eine unendliche Familie. Für endliche Körper funktioniert das natürlich nicht.

Nehmen wir aber an, es gäbe nur endlich viele irreduzible normierte Polynome, etwa $F_1, \dots, F_n \in K[T]$. Dann betrachte $G = 1 + \prod_{i=1}^{n} F_i$. Da es zumindest die Linearfaktoren unter den F_i gibt, muss $\deg(G) = \sum_{i=0}^{n} \deg(F_i) \geq 2$, und damit ist G keine Einheit. Nach dem Satz über die Primfaktorzerlegung muss es eine Primfaktorzerlegun $G = G_1 \cdot \dots \cdot G_m$ geben, insbesondere muss G einen irreduziblen Faktor P besitzen. Aber keines der F_i teilt G: Dann würde es ja auch $1 = G - F_i \cdot \prod_{j \neq i} F_j$ teilen und damit eine Einheit sein. Das heißt P ist ein zusätzliches irreduzibles Polynom im Widerspruch zur ursprünglichen Annahme. □

Bemerkung. *Die einzige Zusatzeigenschaft eines eukldischen Rings, die man hier wirklich benutzt ist, dass* $1 + \prod_{i=1}^{n} p_i$ *für keine Ansammlung von irreduziblen Elementen* p_i *eine Einheit ist. Das ist in* $\mathbb{Z}$ *und* $K[T]$ *wahr, aber im Allgemeinen wirklich nicht: Die Faltung, die wir zur Definition der Multiplikation auf* $R[T]$ *benutzt haben, macht auch* $R[\![T]\!] = \mathrm{F}(\mathbb{N}, R)$ *zu einem Ring, dem Ring der (formalen) Potenzreihen, eine Vergrößerung des Polynomrings. Der Grad eine solchen Potenzreihe ist natürlich nicht mehr zu definieren, aber (vielleicht etwas kontraintuitiv) ist* $K[\![T]\!]$ *für einen Körper* K *euklidisch unter der Funktion*

$$K[\![T]\!] \setminus \{0\} \longrightarrow \mathbb{N}, \quad F \longmapsto \min\{n \in \mathbb{N} \mid F_n \neq 0\}$$

und $T \in K[T] \subset K[\![T]\!]$ *das einzige irreduzibles Element von* $K[\![T]\!]$*; insbesonere ist* $T+1 \in K[\![T]\!]$ *eine Einheit (nicht aber natürlich in* $K[T]$*!). Das Inverse ist die echte Potenzreihe*

$$\sum_{i \geq 0} (-1)^i \cdot T^i$$

im Wesentlichen nach der geometrischen Summenformel.

Aufgabe 2 (5 Punkte)

Zeigen Sie: Der $\mathbb{Z}[T]$-Untermodul $\{F \in \mathbb{Z}[T] \mid F(0) \text{ ist gerade}\}$ von $\mathbb{Z}[T]$ lässt sich von zwei Elementen, aber nicht von einem Element erzeugen.

Lösungsskizze. Nennen wir den Untermodul I. Ich behaupte I wir als $\mathbb{Z}[T]$-Modul von 2 und T erzeugt, mit anderen Worten $I = \langle 2, T \rangle_{\mathbb{Z}[T]}$. Zunächst gelten per Definition

$$\mathrm{apf}(2) = \mathrm{const}_2 \quad \text{und} \quad \mathrm{apf}(T) = \mathrm{id}_R,$$

und diese beiden Funktionen werten sich bei 0 zu 2 bzw. 0 aus, beides gerade. Damit gilt $2, T \in I$. Und ist $F = \sum_{i=0}^{n} F_i \cdot T^i \in I$ gegeben, so gilt per Definition $F_0 = F(0) = 2 \cdot k$ für ein $k \in \mathbb{Z}$. Aber damit haben wir

$$F = F_0 + \sum_{i=1}^{n} F_i \cdot T^i = 2 \cdot k + T \cdot \left(\sum_{i=1}^{n} F_i \cdot T^{i-1} \right) \in \langle 2, T \rangle_{\mathbb{Z}[T]}.$$

Es bleibt noch zu zeigen, dass I nicht von einem Element z erzeugt werden kann, also dass $I = \langle z \rangle_{\mathbb{Z}[T]}$ für kein $z \in \mathbb{Z}[T]$ gilt. Nehmen wir an, dass doch. Dann ist jedes Element von I ein Vielfaches von z. Insbesondere gilt $z \mid T$. Aber T ist irreduzibel, also bleiben nur $z \in \{1, -1, T, -1\}$ als Möglichkeiten. Es muss aber ebenso $z \mid 2$ gelten, und aus gleichem Grunde dann $z \in \{1, -1, 2, -2\}$, also $z = 1$ oder $z = -1$, aber weder 1 noch -1 sind überhaupt Elemente von I. □

Die dritte Aufgabe bedarf ein klein wenig Notation: Ist R ein kommutativer Ring, so heißen zwei Elemente $r, s \in R$ *assoziiert*, falls es eine Einheit $u \in R$ gibt mit $u \cdot r = s$. Dies ist eine Äquivalenzrelation $\sim$. Auf den Assoziiertheitsklassen $R/\sim$ definiert

$$X \text{ teilt } Y :\Longleftrightarrow \exists x \in X, y \in Y, r \in R\colon x \cdot r = y$$

eine partielle Ordnung, falls R ein Integritätsbereich ist. Gegeben nun eine Menge $E \subseteq R$, so heißt $r \in R$ ein *größter gemeinsamer Teiler* der Elemente von E, falls $[r] \in R/\sim$ ein größtes Element von

$$\{X \in R/\sim \mid X \text{ teilt } [e] \text{ für jedes } e \in E\}$$

bezüglich der Teilbarkeitsrelation ist.

Aufgabe 3 (5 Punkte)

Sei R ein kommutativer Ring. Zeigen Sie:

a) Assoziiertheit ist wirklich eine Äquivalenzrelation auf R.

b) Ist R ein Integritätsbereich, so ist Teilbarkeit wirklich eine partielle Ordnung auf den Assoziiertheitsklassen in R.

c) Ist R ein Integritätsbereich, $t \in R$ und $E \subseteq R$ mit $\langle E \rangle_R = \langle t \rangle_R$ so ist t ein größter gemeinsamer Teiler der Elemente von E.

Lösungsskizze. a) Wir rechnen die drei definierenden Eigenschaften nach:

1) Reflexivität: $r = 1 \cdot r$ zeigt $r \sim r$.
2) Transitivität: Gilt $r \sim s$, etwa weil $r = u \cdot s$, so folgt $s = 1/u \cdot r$ und damit $s \sim r$, da mit u auch $1/u$ eine Einheit ist.
3) Symmetrie: Und gelten $r \sim s$ und $s \sim t$, etwa weil $r = u \cdot s$ und $s \cdot v \cdot t$, dann folgt

$$r = u \cdot s = (u \cdot v) \cdot t$$

und damit $r \sim t$, weil $u \cdot v$ mit u und v eine Einheit ist.

b) Auch hier rechnen wir die drei definierenden Eigenschaften nach. Es lohnt sich aber vorab zu beweisen, dass auch gilt

$$X \text{ teilt } Y \Longleftrightarrow \forall x \in X, y \in Y, \exists r \in R\colon x \cdot r = y$$

Da Assoziiertheitsklassen nie leer sind (Äquivalenzklassen jeder Äquivalenzrelation auf einer nicht-leeren Menge sind per Definition nicht leer), impliziert die rechte Seite sicherlich die linke. Und teilt X die Klasse Y, etwa weil $x' \cdot r = y'$ für irgendwelche $x' \in X$, $y' \in Y$ und $r \in R$, und sind $x \in X$ und $y \in Y$ beliebig, so gibt es per Definition Einheiten $u, v \in R$ mit $x' = u \cdot x$ und $y = v \cdot y'$. Damit rechnen wir dann

$$y = v \cdot y' = x' \cdot r \cdot y' = x \cdot (u \cdot r \cdot y')$$

was die Behauptung beweist.

1) Reflexivität: Ist X eine Assoziiertheitsklasse, so gilt wie gerade schon gesagt $X \neq \emptyset$. Ist dann $x \in X$, so zeigt $x \cdot 1 = x$, dass X sich selbst teilt.
2) Transitivität: Teilt X die Klasse Y und Y die Klasse Z, wählen wir drei Elemente $x \in X$, $y \in Y$ und $z \in Z$. Dann gilt nach der Vorüberlegung $y = r \cdot x$ und $z = r' \cdot y$ für irgendwelche $r, r' \in R$ und damit

$$z = r' \cdot y = r' \cdot r \cdot x,$$

was beweist, dass X die Klasse Z teilt.

3) Identivität: Teilt X die Klasse Y und Y die Klasse X, so wählen wir $x \in X$ und $y \in Y$. Wieder nach der Vorüberlegung gibt es dann $r, r' \in R$ mit $x \cdot r = y$ und $y \cdot r' = x$. Ist dann $x = 0$ oder $y = 0$, so folgt jeweils auch das andere und damit $X = Y$. Bleibt noch der Fall zu klären, wenn $x \neq 0 \neq y$. Wir haben aber

$$x = y \cdot r' = x \cdot r \cdot r'$$

was nach Kürzen von x (R ist als integer angenommen!) $1 = r \cdot r'$ ergibt, also dass r und r' Einheiten sind. Aber damit folgt $x \sim y$, ergo $X = Y$ wie gewünscht.

c) Da $\langle t \rangle_R$ genau aus den Vielfachen von t besteht, gilt $E \subseteq \langle t \rangle_R$ genau dann, wenn t ein gemeinsamer Teiler von den Elementen von E ist, insbesondere teilt $[t]$ die Klasse $[e]$ für jedes $e \in E$.

Um zu sehen, dass $[t]$ wirklich größt ist, schreiben wir $t = \sum_{e \in I} e \cdot s_e$ für eine endliche Teilmenge $I \subseteq E$ und $s \colon I \to R$ irgendeine Koeffizientenfunktion; das ist möglich genau dann, wenn $t \in \langle E \rangle_R$. Sei nun X irgendeine Assoziiertheitsklasse, die $[e]$ für alle $e \in E$ teilt. Wählen wir uns dann ein $x \in X$, so folgt aus der Vorüberlegung, dass $e = x \cdot r_e$ gilt für irgendwelche Elemente $r_e \in R$. Aber dann haben wir

$$t = \sum_{e \in I} e \cdot s_e = \sum_{e \in I} x \cdot r_e \cdot s_e = x \cdot \sum_{e \in I} r_e \cdot s_e$$

und damit teilt X die Klasse $[t]$ wie gewünscht.

□

Aufgabe 4 (5 Punkte)

Berechnen Sie den größten gemeinsamen Teiler von $T^5+2T^3+2T^2+T+2$ und T^3+2T^2+T+2 in $\mathbb{Q}[T]$ mittels des euklidischen Algorithmus und finden Sie eine Darstellung von ihm als Linearkombination der beiden Polynome.

Lösungsskizze. Wir führen die nötigen Divisionen mit Rest aus:

$$\begin{aligned} T^5+2T^3+2T^2+T+2 &= T^2 \cdot (T^3+2T^2+T+2) - 2T^4 + T^3 + T + 2 \\ -2T^4+T^3+T+2 &= -2T \cdot (T^3+2T^2+T+2) + 5T^3 + 2T^2 + 5T + 2 \\ 5T^3+2T^2+5T+2 &= 5 \cdot (T^3+2T^2+T+2) - 8T^2 - 8 \end{aligned}$$

also

$$T^5+2T^3+2T^2+T+2 = (T^2-2T+5) \cdot (T^3+2T^2+T+2) - 8T^2 - 8$$

und dann

$$\begin{aligned} T^3+2T^2+T+2 &= \frac{-1}{8} \cdot T \cdot (-8T^2-8) + 2T^2 + 2 \\ 2T^2+2 &= \frac{-1}{4} \cdot T \cdot (-8T^2-8) \end{aligned}$$

also

$$T^3+2T^2+T+2 = \left(\frac{-1}{8} T - \frac{1}{4} \right) \cdot (-8T^2-8).$$

Und damit folgt, dass der größte gemeinsame Teiler der beiden Polynome $-8T^2-8$ oder äquivalenterweise T^2+1 ist.

Einsetzen liefert sofort

$$-8 \cdot T^2 - 8 = 1 \cdot (T^5+2T^3+2T^2+T+2) - (T^2-2T+5) \cdot (T^3+2T^2+T+2)$$

als die gewünschte Darstellung (die man natürlich auch noch durch 8 teilen kann). □