Übung zu Algebraische und Geometrische Strukturen in der Mathematik, SoSe 2014

3. Übungsblatt – Lösungsskizze

Aufgabe P8

1. „$\Rightarrow$“: $p \mid q \Rightarrow$ es existiert $s \in k[X]$ mit $p \cdot s = q \Rightarrow q \cdot k[X] = p \cdot s \cdot k[X] \subseteq p \cdot k[X]$
   „$\Leftarrow$“: $q \cdot k[X] \subseteq p \cdot k[X] \Rightarrow q = p \cdot t$ für ein $t \in k[X] \Rightarrow p \mid q$.

2. Ein Element aus $I(p,q)$ ist gegeben durch $p \cdot a + q \cdot b$ für $a, b \in k[X]$ beliebig. $I(p,q)$ ist abgeschlossen unter Addition und Skalarmultiplikation:

$$(p \cdot a + q \cdot b) + (p \cdot a' + q \cdot b') = p \cdot (a + a') + q \cdot (b + b') \in I(p,q)$$
$$\lambda \cdot (p \cdot a + q \cdot b) = p \cdot \lambda \cdot a + q \cdot \lambda \cdot b \in I(p,q).$$

   Ferner gilt

$$s \cdot (p \cdot a + q \cdot b) = p \cdot s \cdot a + q \cdot s \cdot b \in I(p,q)$$

   für ein beliebiges $s \in k[X]$ und $p \cdot a + q \cdot b \in I(p,q)$.

Aufgabe P9

Gilt $p(\alpha) = 0$, dann kann man die Nullstelle abspalten und wir haben $p(X) = (X - \alpha) \cdot q(X)$. Also ist p nicht irreduzibel. Da jedes reelle Polynom von ungeradem Grad eine Nullstelle hat (warum?) ist es somit auch nicht irreduzibel. Das rational Polynom $X^3 - 2$ hat nur $\sqrt[3]{2}$ als Nullstelle, also insbesondere keine rationale Nullstelle. Könnte man es als Produkt von rationalen Polynomen kleineren Grades schreiben hätte es aber ein rationale Nullstelle. Also ist es irreduzibel in $\mathbb{Q}[X]$, nach dem obigen aber nicht irreduzibel in $\mathbb{R}[X]$.

Hat $p \in \mathbb{R}[X]$ einen Grad größer gleich 4, so hat es entweder eine reelle Nullstelle und ist somit nicht irreduzibel. Hat es keine reelle Nullstelle, so treten die komplexen Nullstelle alle in Paaren $\alpha, \overline{\alpha}$ auf. In der Zerlegung in Linearfaktoren kann man also diese Faktoren

$$(X - \alpha)(X - \overline{\alpha}) = X^2 - \underbrace{(\alpha + \overline{\alpha})}_{\in \mathbb{R}} X + \underbrace{\alpha\overline{\alpha}}_{\in \mathbb{R}}$$

zu reellen Polynomen gruppieren und erhält somit eine Zerlegung in reelle Polynome von echt kleinerem Grad. Da Polynome vom Grad 1 nach Definition irreduzibel sind bleiben also nur noch die reellen Polynome vom Grad 2 zu untersuchen. Ein solches Polynom

$$p(X) = aX^2 + bX + c$$

läßt sich genau dann als ein Produkt von zwei Linearfaktoren schreiben, wenn beide Nullstellen reell sind. Das ist nach der *pq*-Formel genau dann der Fall, wenn $\frac{b^2}{4a^2} - \frac{c}{a} \geq 0$ gilt. Also sind die irreduziblen reellen Polynome genau die reellen Polynome vom Grad 1 und die reellen Polynome vom Grad 2 mit $\frac{b^2}{4a^2} - \frac{c}{a} < 0$ (für a, b, c wie oben).

Aufgabe P10

Es ist klar, dass $\mathbb{Z}/n\mathbb{Z}$ ein Ring ist, es bleibt also nur zu zeigen, dass jedes Element ungleich Null multiplikativ invertierbar genau dann wenn n eine Primzahl ist.
„$\Rightarrow$": Wir führen einen Widerspruchsbeweis. Ist n keine Primzahl, dann gilt $n = s \cdot t$ mit $s, t \in \mathbb{Z}$, $1 < s, t < n$. Damit gilt $[s] \cdot [t] = 0$ in $\mathbb{Z}/n\mathbb{Z}$ und gleichzeitig $0 \neq [s]$ und $0 \neq [t]$. Letzteres kann in einem Körper aber nicht sein.
„$\Leftarrow$": Ist $[x] \neq 0$, so ist $x \in \mathbb{Z}$ kein Vielfaches von n, also Teilerfremd zu n, da n als Primzahl vorausgesetzt ist. Daher existieren $s, t \in \mathbb{Z}$ mit

$$x \cdot s + n \cdot t = 1.$$

Da $[n \cdot t] = 0$ in $\mathbb{Z}/n\mathbb{Z}$ gilt haben wir hiermit $[x] \cdot [s] = 1$.
Bemerkung: Die Argumentation funktioniert *wörtlich* genauso um zu zeigen, dass $k[X]/f \cdot k[X]$ genau dann ein Körper ist, wenn f irreduzibel (bzw. prim) ist.

Aufgabe H7

Der Euklidische Algorithmus gibt

$$\begin{aligned} X^4 - 3X^2 - 2X^2 + 3X + 1 &= (X+3)(X^3 - 6X^2 + 8X + 3) + 8X^2 - 24X - 8 \\ X^3 - 6X^2 + 8X + 3 &= (\frac{1}{8}X - \frac{3}{8})(8X^2 - 24X - 8), \end{aligned}$$

also ist

$$\text{ggT}(X^4 - 3X^2 - 2X^2 + 3X + 1, X^3 - 6X^2 + 8X + 3) = X^2 - 3X - 1,$$

(der „normierte Divisor der ersten aufgehenden Division").

Aufgabe H8

1. Für $s \in k[X]$ gilt
$$f \cdot s \in (p \cdot k[X] + q \cdot k[X]) \cdot s \subseteq p \cdot k[X] + q \cdot k[X].$$

2. Sei $g \in p \cdot k[X] + q \cdot k[X]$. Dann gilt $\deg(f) \leq \deg(g)$, also $g = f \cdot s + r$ mit $\deg(r) < \deg(f)$. Damit gilt auch $r = g - f \cdot s \in p \cdot k[X] + q \cdot k[X]$ (vgl. P8), also $r = 0$, da f minimalen Grad hat. Also gilt $g = f \cdot s \in f \cdot k[X]$.

3. Aus Teil 1. und 2. folgt dass
$$f \cdot k[X] = p \cdot k[X] + q \cdot k[X],$$
also existiert ein $s \in k[X]$ mit $f \cdot s = p \in p \cdot k[X] + q \cdot k[X]$ und ein $t \in k[X]$ mit $f \cdot t = q \in p \cdot k[X] + q \cdot k[X]$. Also gelten $f \mid p$ und $f \mid q$. Damit ist f ein Teiler von p und q und es gilt nach Definition von $\text{ggT}(p, q)$ dass $\deg(f) \leq \deg(\text{ggT}(p, q))$.

4. Aus P8 folgt $p \cdot k[X] \subseteq \text{ggT}(p, q) \cdot k[X]$, $q \cdot k[X] \subseteq \text{ggT}(p, q) \cdot k[X]$ und
$$f \cdot k[X] = p \cdot k[X] + q \cdot [X] \subseteq \text{ggT}(p, q) \cdot k[X].$$
Damit existiert ein $s \in k[X]$ mit $f = \text{ggT}(p, q) \cdot s$. Da $\deg(f) \leq \deg(\text{ggT}(p, q))$ gilt und f und $\text{ggT}(p, q)$ normiert sind muss $s = 1$ gelten.

Man bemerke, dass man obige Argumentation wörtlich von der Argumentation in $\mathbb{Z}$ übernehmen kann, wenn man den Betrag einer ganzen Zahl durch den Grad eines Polynoms ersetzt.