Übungsblatt 5: Primfaktorzerlegung in Polynomringen

"Wer vieles bringt, wird manchem etwas bringen."
— Johann Wolfgang von Goethe, Faust I

1. Inhalt und ggT

S 1.1. (2 Punkte) Man bestimme den Inhalt von $P = X^3Y + X^3 + X^2Y^2 - X^2 + XY^3 - XY$ in $\mathbb{Q}[Y][X]$ und anschließend in $\mathbb{Q}[X][Y]$.

V 1.2. Man berechne den ggT folgender Polynome (vgl. Algorithmus 6 im Skript):

(a) $P = 24X^3 - 81$ und $Q = 24X^2 - 72X + 54$ in $\mathbb{Z}[X]$.
Hinweis: Man bestimme den ggT zuerst in $\mathbb{Q}[X]$ und schließe auf $\mathbb{Z}[X]$.

(b) $P = X^3Y^3 + X^4Y - X^2Y^2 - X^3$ und $Q = X^2Y^3 - X^4Y - XY^2 + X^3$ in $\mathbb{Q}[X,Y]$.
Hinweis: Man bestimme den ggT zuerst in $\mathbb{Q}(X)[Y]$ und schließe auf $\mathbb{Q}[X][Y]$.

(c) In beiden Fällen zerlege man P und Q in irreduzible Faktoren.
Primfaktorzerlegungen sind im Allgemeinen schwer. Daher ein *Hinweis:* Man berechne zunächst $P(-Y^2,Y)$ sowie $Q(X,X)$ und $Q(X,-X)$.

2. Das Reduktionsverfahren und seine Grenzen

2.1. Man bestimme alle irreduziblen Polynome vom Grad ≤ 3 über $\mathbb{Z}/2$ und $\mathbb{Z}/3$.

S 2.2. (2 Punkte) Welche der folgenden Polynome sind irreduzibel in $\mathbb{Z}[X]$?

(a) $X^3 + 14X^2 + 19X + 25$
(b) $X^3 + 35X^2 + 18X + 45$
(c) $X^3 + 5X^2 + 7X + 13$

2.3. Man zerlege $X^4 + 1$ in $\mathbb{C}[X]$, $\mathbb{R}[X]$, $\mathbb{Q}[X]$, $\mathbb{Z}[X]$, $\mathbb{Z}/2[X]$, $\mathbb{Z}/3[X]$.

Wir wollen zeigen, dass das Polynom $Q = X^4 + 1 \in \mathbb{Z}/p[X]$ für jede Primzahl p nicht irreduzibel ist.

2.4. Zeigen Sie dazu:

(a) Gibt es ein $a \in \mathbb{Z}/p[X]$ mit $a^2 = -1$, dann ist $Q \in \mathbb{Z}/p[X]$ nicht irreduzibel.

(b) Gibt es ein $b \in \mathbb{Z}/p[X]$ mit $b^2 = 2$, dann ist $Q \in \mathbb{Z}/p[X]$ nicht irreduzibel.

(c) Gibt es ein $c \in \mathbb{Z}/p[X]$ mit $c^2 = -2$, dann ist $Q \in \mathbb{Z}/p[X]$ nicht irreduzibel.

(d) In $\mathbb{Z}/p$ ist mindestens eine der drei Zahlen $-2, -1, 2$ ein Quadrat.
Hinweis: Sie dürfen verwenden, dass $x \in \mathbb{Z}/p^*$ für $p \neq 2$ genau dann ein Quadrat in $\mathbb{Z}/p$ ist, wenn $x^{\frac{p-1}{2}} = 1$ und ein Nichtquadrat, wenn $x^{\frac{p-1}{2}} = -1$.
Zusatz: Wie folgt der Hinweis aus dem kleinen Satz von Fermat?

Somit gibt es Polynome in $\mathbb{Z}[X]$, welche nicht mit dem Reduktionskriterium modulo p als irreduzibel erkannt werden können, obwohl sie irreduzibel sind.

3. Zum Kriterium von Eisenstein

S 3.1. (2 Punkte) Man zerlege die folgenden Polynome in $\mathbb{Z}[X]$:
(a) $X^4 - 4X^3 + 6$
(b) $2X^4 - 6X^3 + 12$
(c) $X^3 + nX + 2$ (in Abhängigkeit von $n \in \mathbb{N}$)

Für das Kriterium von Eisenstein ist manchmal folgender Trick hilfreich:

3.2. Ein Polynom $P \in R[X]$ ist irreduzibel genau dann wenn $P(X+b)$ es ist.

Dies führt uns zu der Frage nach den Automorphismen des Rings $R[X]$ über R:

3.3. Für $a, b \in R$ existiert genau ein Ringhomomorphismus $\varphi_{a,b} \colon R[X] \to R[X]$ mit $\varphi_{a,b}|_R = \mathrm{id}_R$ und $X \mapsto aX + b$. Man zeige, dass $\varphi_{a,b}$ genau dann ein Automorphismus ist, wenn $a \in R^\times$ gilt. In diesem Falle gebe man $\varphi_{a,b}^{-1}$ explizit an.

3.4. Sei R ein Integritätsring und sei $\mathrm{Aut}_R(R[X])$ die Gruppe der Ringautomorphismen $\varphi \colon R[X] \xrightarrow{\sim} R[X]$ mit $\varphi|_R = \mathrm{id}_R$. Man zeige $\mathrm{Aut}_R(R[X]) = \{\, \varphi_{a,b} \mid a \in R^\times, b \in R \,\}$.

4. Reduzible und irreduzible Polynome

In dieser Aufgabe sollen Sie selbst herausfinden, welches Kriterium oder welche Methode am Besten anzuwenden ist. Ein allgemeiner Hinweis: Der Satz von Gauß und die Proposition 6G9 aus dem Skript können auch nützlich sein.

V 4.1. Man zerlege die folgenden Polynome in $\mathbb{Q}[X]$:
(a) $X^4 + 4X^3 + 6X^2 + 4X + 1$
(b) $X^3 + 3X^2 + 6X + 5$
(c) $X^3 + 3X^2 + 5X + 6$
(d) $4X^2 + 4X + 1$
(e) $X^4 + 10X^2 + 1$
(f) $9X^3 + 7X + 3$
(g) $3X^5 + 10X^3 + 50X^2 - 40X + 20$
(h) $2X^3 + 3X^2 + 3X + 1$
(i) $X^8 - 1$

S 4.2. (2 Punkte) Ist $P = X^2 + Y^2 - 1$ irreduzibel in $\mathbb{C}[X,Y]$? und in $\mathbb{Z}/2[X,Y]$?

S 4.3. (2 Punkte) Man zeige: $\sqrt[n]{a}$ mit $a \in \mathbb{N}$, $n \in \mathbb{N}_{\geq 2}$, ist entweder ganz oder irrational.

4.4. Für $n \geq 3$ zerlege man $6X^n - 6X^{n-1} + 24X^2 - 36X + 12$ in $\mathbb{Z}[X]$ in irreduzible Faktoren.

4.5. Man zerlege $2X^5 - 5X^4 - 21X^3 - 15X^2 - 23X - 10$ in $\mathbb{Z}[X]$.