Übungen zur Elementaren Zahlentheorie

Wintersemester 2015/16

Prof. Dr. K. Wingberg
O. Thomas

Blatt 9
Abgabe bis 17.12.2015, 11:00h

Aufgabe 33. *(3·2 Punkte)*
Seien f und g zwei nicht-konstante normierte Polynome mit ganzzahligen Koeffizienten.

(i) f und g sind teilerfremd in $\mathbb{Z}[X]$ genau dann, wenn sie in $\mathbb{C}$ keine gemeinsame Nullstelle besitzen.

(ii) f ist separabel genau dann, wenn $r(f, f') \neq 0$, wobei r die Resultante aus Aufgabe 29 bezeichnet.

(iii) Sei $d \in \mathbb{Z}$ quadratfrei und $\omega \in \mathbb{Q}(\sqrt{d})$ wie in der Vorlesung definiert. Sei h das Minimalpolynom von ω über $\mathbb{Z}$. Bestimme die Primteiler von $r(h, h')$.

Aufgabe 34. *(2.5+2.5+1 Punkte)*
Betrachte $f = X^6 + X^5 - 4X^4 + 2X^3 - 11X^2 + X - 6$.

(i) Faktorisiere f nach dem Algorithmus aus Aufgabe 30.

(ii) Bestimme mit Aufgabe 33, ob f separabel ist.

(iii) Wann eignet sich Aufgabe 30 besser, wann Aufgabe 33, um zu bestimmen, ob ein Polynom separabel ist?

Aufgabe 35. *(1+1+1+1+2 Punkte)*
Sei $K = \mathbb{Q}(\sqrt{d})$ ein quadratischer Zahlkörper. Eine bijektive Abbildung $\sigma\colon K \longrightarrow K$ heißt Körperautomorphismus, falls $\sigma(x + y) = \sigma(x) + \sigma(y)$ und $\sigma(xy) = \sigma(x)\sigma(y)$ für alle $x, y \in K$ gilt.

(i) $\sigma(1) = 1$.

(ii) $\sigma(x) = x$ für alle $x \in \mathbb{Q}$.

(iii) Ist $f \in \mathbb{Q}[X]$ und $f(\alpha) = 0$ mit $\alpha \in K$, so ist auch $f(\sigma(\alpha)) = 0$.

(iv) Ist $\alpha \in \mathcal{O}_K$, so ist auch $\sigma(\alpha) \in \mathcal{O}_K$.

(v) Bestimme alle Körperautomorphismen $\sigma\colon K \longrightarrow K$.

Aufgabe 36. *(2+4 Punkte)*
Sei $K = \mathbb{Q}(\sqrt{d})$ ein quadratischer Zahlkörper und $\sigma\colon K \longrightarrow K$ ein von der Identität verschiedener Körperautomorphismus.

(i) Es gibt ein $\alpha \in K$, sodass $K = \{x\alpha + y\sigma(\alpha) \mid x, y \in \mathbb{Q}\}$.

(ii) Ein $\alpha \in \mathcal{O}_K$ mit $\mathcal{O}_K = \{x\alpha + y\sigma(\alpha) \mid x, y \in \mathbb{Z}\}$ gibt es genau dann, wenn $d \equiv 1 \mod 4$.