Universität Konstanz
Fachbereich Mathematik und Statistik
Sommersemester 2011

Christoph Hanselka
Aaron Kunert
Markus Schweighofer

Lösungsblatt 12 zur Zahlentheorie

Aufgabe 1.

(a) Der Ringhomomorphismus

$$\begin{aligned}\Psi\colon B &\longrightarrow A,\\ p(X) &\longmapsto p(X^2)\end{aligned}$$

ist bijektiv und daher ein Isomorphismus. Da B ein Hauptidealring ist, muss somit auch A ein Hauptidealring sein. Wegen $A \subseteq L$ ist der Quotientenkörper von A ein Teilkörper von L. Dies ist genau der Teilkörper von L, der sowohl alle $p(X^2)$ mit $p \in B$, als auch für $p \neq 0$ deren Inversen enhält. Es ist also

$$\mathrm{qf}(A) = \left\{ \frac{p(X^2)}{q(X^2)} \,\middle|\, p,q \in A, q \neq 0 \right\} = \mathbb{R}(X^2) = L.$$

(b) Es ist $L = K(X)$, dabei hat X über K das Minimalpolynom $Y^2 - X^2 = 0$. Dies zeigt, dass $K \subseteq L$ algebraisch vom Grad 2 ist. Offensichtlich ist wegen $\mathrm{char}(K) = 0$ die Erweiterung $K \subseteq L$ separabel. Weiter zerfällt das Minimalpolynom von X über L in $(Y - X)(Y + X)$, was zeigt, dass die Erweiterung $K \subseteq L$ normal und daher galoisch ist.

(c) Zunächst zeigen wir, dass $A \subseteq B$ eine ganze Ringerweiterung ist. Einerseits ist $B = A(X)$ anderseits ist $(X)^2 - X^2 = 0$ eine Ganzheitsgleichung von X über A. Daher ist $A \subseteq B$ ganz. Weiter ist B ein Hauptidealring und daher ganz abgeschlossen. Gäbe es ein Element $a \in L$ mit $a \notin B$, das ganz über A wäre, so wäre es schon ganz über B und daher in B. Also ist B der ganze Abschluss von A in L.

(d) Wir bestimmen zunächst die Primideale von B. Da B ein Hauptidealring ist, genügt es die irreduziblen Elemente in B zu finden. Da der algebraische Abschluss $\mathbb{C}$ von $\mathbb{R}$ Grad 2 über $\mathbb{R}$ hat, hat jedes irreduzible Polynom von $\mathbb{R}[X]$ Grad 1 oder Grad 2. Ferner ist ein Polynom vom Grad 2 genau dann irreduzibel über $\mathbb{R}$, wenn es keine Nullstellen in $\mathbb{R}$ hat. Daher sind die Primideale von B genau die

$$\begin{aligned}\mathfrak{p}_a &= (X - a), \text{ mit } a \in \mathbb{R}, \text{ sowie}\\ \mathfrak{q}_{b,c} &= ((X - b)^2 + c^2), \text{ mit } b,c \in \mathbb{R}, c > 0.\end{aligned}$$

Der Isomorphismus Ψ bildet die irreduziblen Elemente von B genau auf die irreduziblen Elemente von A ab. Daher sind die Primideale von A genau die

$$\begin{aligned}\mathfrak{p}'_a &= (X^2 - a), \text{ mit } a \in \mathbb{R}, \text{ sowie}\\ \mathfrak{q}'_{b,c} &= ((X^2 - b)^2 + c^2), \text{ mit } b,c \in \mathbb{R}, c > 0.\end{aligned}$$

(e) Wir betrachten zunächst die Zerlegung der Ideale $B\mathfrak{p}'_a$ in B. Dazu unterscheiden wir drei Fälle.

Fall 1: $a > 0$:
Hier ist $(X^2 - a) = (X - \sqrt{a})(X + \sqrt{a}) = (\mathfrak{p}_{\sqrt{a}})(\mathfrak{p}_{-\sqrt{a}})$. Wegen $a \neq 0$ ist daher $e_{\mathfrak{p}'_a}(B) = 1$ und wegen $[L : K] = 2$ ist auch $f_{\mathfrak{p}'_a}(B) = 1$.

Fall 2: $a < 0$:
Hier ist $(X^2 - a)$ selbst ein Primideal in B und daher ist $e_{\mathfrak{p}'_a}(B) = 1$ und es muss $f_{\mathfrak{p}'_a}(B) = 2$ sein.

Fall 3: $a = 0$:
Für $a = 0$ verzweigt sich das Ideal (X^2) in $(X)^2$. Es ist daher $e_{\mathfrak{p}'_0}(B) = 2$ und $f_{\mathfrak{p}'_0}(B) = 1$.

Als nächstes betrachten wir die Zerlegung der $B\mathfrak{q}'_{b,c}$ in B. Offensichtlich hat das Polynom $(X^2 - b)^2 + c^2$ keine Nullstellen in $\mathbb{R}$, daher muss es über B in zwei quadratische Polynome zerfallen. Um den Verzweigungs– bzw. Trägheitsindex zu bestimmen, genügt es zu wissen, ob $(X^2 - b)^2 + c^2$ in zwei gleiche, oder zwei verschiedene quadratische Polynome zerfällt. Im ersten Fall ist dann der Verzweigungsindex 2 und der Trägheitsindex 1 im zweiten Fall sind beide Indizes gleich 1. Angenommen $p := (X^2 - b)^2 + c^2$ ist das Quadrat des Polynoms $q := X^2 + \alpha X + \beta$. Durch Vergleich der jeweiligen Koeffizienten folgert man $\alpha = 0$ und daher ist $p = q^2$ dann und nur dann, wenn $c = 0$ ist.

Aufgabe 2.
Wir wenden den Satz 3.2.2 aus der Vorlesung an. Es ist

$$[\mathcal{O}_K : \mathbb{Z}[d]] = \begin{cases} 1 & \text{falls } d \equiv_{(4)} 2{,}3 \\ 2 & \text{falls } d \equiv_{(4)} 1. \end{cases}$$

Daher lässt sich ausser für den Fall $d \equiv_{(4)} 1$ und $p = 2$ der Satz 3.2.2 stets anwenden. Sei daher zunächst $p \neq 2$ oder $d \equiv_{(4)} 2{,}3$. Das Minimalpolynom von $\sqrt{d}$ über $\mathbb{Q}$ ist $f = X^2 - d$. Über $\mathbb{F}_p$ zerfällt dieses Polynom genau dann, wenn $\overline{f}$ eine Nullstelle hat, also wenn ein $\alpha \in \mathbb{Z}$ existiert mit $\alpha^2 \equiv_{(p)} d$. In diesem Fall ist $\overline{f} = (X - \alpha)(X + \alpha)$. Ist $p \nmid d$, so ist wegen $p \neq 2$ auch $\alpha \neq -\alpha$; ist $p \mid d$, so ist $\overline{f} = X^2$. Anwendung des Satzes 3.2.2 liefert daher:

$$e_p(\mathcal{O}_K) = \begin{cases} 1 & \text{falls } p \nmid d \\ 2 & \text{falls } p \mid d \end{cases}$$

$$f_p(\mathcal{O}_K) = \begin{cases} 1 & \text{falls } \exists \alpha \in \mathbb{Z} : \alpha^2 \equiv_{(p)} d \\ 2 & \text{sonst.} \end{cases}$$

Schließlich betrachten wir den Fall, $d \equiv_{(4)} 1$ und $p = 2$. Auch hier können wir den Satz 3.2.2 anwenden, müssen jedoch den vollen Ganzheitsring $\mathbb{Z}[\frac{1+\sqrt{d}}{2}]$ betrachten. Das Minimalpolynom von $\frac{1+\sqrt{d}}{2}$ ist $f = X^2 - X - \frac{d-1}{4}$. Wir schreiben $d = 4k+1$ für ein $k \in \mathbb{Z}$ und erhalten $f = X^2 - X - k$. In $\mathbb{F}_2$ ist $\overline{f} = X^2 + X + \overline{k}$ reduzibel genau dann, wenn $\overline{f}$ eine Nullstelle besitzt. Dies ist genau dann der Fall, wenn $2 \mid k$. Dann ist $\overline{f} = X(X + 1)$. Daher ergibt sich

$$e_2(\mathcal{O}_K) = 1$$

$$f_2(\mathcal{O}_K) = \begin{cases} 1 & \text{falls } 2 \mid k \\ 2 & \text{falls } 2 \nmid k. \end{cases}$$

Aufgabe 3.
Wir hatten schon auf dem letzten Blatt gesehen, dass $\mathcal{O}_K = \mathbb{Z}[z]$ ist. Daher lässt sich Satz 3.2.2 anwenden. Um die jeweiligen Zerlegungen zu bestimmen genügt es daher, das Polynom $f = X^3 - X + 3$ in $\mathbb{F}_p$ für $p \in \{2{,}3, 5{,}7{,}11\}$ in irreduzible Faktoren zu zerlegen.

$p = 2:$ Es ist $\overline{f} = X^3 + X + 1$. Dieses Polynom hat über $\mathbb{F}_2$ keine Nullstellen und ist daher irreduzibel. Wir erhalten somit

$$2\mathcal{O}_K = (2, z^3 + z + 1) = (2).$$

$p = 3:$ Es ist $\overline{f} = X^3 - X = X(X^2 - 1) = X(X-1)(X+1)$. Daher ist

$$3\mathcal{O}_K = (3, z)(3, z-1)(3, z+1).$$

$p = 5:$ Es ist $\overline{f} = X^3 - X + 3$. Dieses Polynom hat über $\mathbb{F}_5$ keine Nullstellen und ist daher irreduzibel. Also ist

$$5\mathcal{O}_K = (5, z^3 - z + 3) = (5).$$

$p = 7:$ Das Polynom $\overline{f} = X^3 - X + 3$ hat über $\mathbb{F}_7$ die Nullstelle $X = \overline{4}$. Nach Polynomdivision erhalten wir $\overline{f} = (X-4)(X^2 + 4X + 1)$. Da der zweite Faktor keine Nullstelle in $\mathbb{F}_7$ hat, ist dies schon die Primfaktorzerlegung von $\overline{f}$. Wir erhalten daher

$$7\mathcal{O}_K = (7, z-4)(7, z^2 + 4z + 1).$$

$p = 11:$ Das Polynom $\overline{f}$ hat über $\mathbb{F}_{11}$ keine Nullstellen und wir erhalten daher

$$11\mathcal{O}_K = (11, z^3 - z + 3) = (11).$$