G. Nebe, M. Künzer

Übungen Algebra II, Sommersemester 03

Lösung 2

Aufgabe 1.

(a) Sei

$$\mu_{\xi,\mathbf{Q}}(X) \;=\; X^n + a_{n-1}X^{n-1} + \cdots + a_0 \;\in\; \mathbf{Z}[X]\;.$$

Beachte, daß jedes Element von $\mathbf{Z}[\xi]$ ganz über $\mathbf{Z}$ ist.

Sei $\mathfrak{p} \neq 0$ ein Primideal in $R = \mathbf{Z}[\xi]$. Wir behaupten, daß $\mathfrak{p} \cap \mathbf{Z} \neq 0$. Sei $\vartheta \in \mathfrak{p}$, und sei

$$\mu_{\vartheta,\mathbf{Q}}(X) = X^m + b_{m-1}X^{m-1} + \cdots + b_0 \;\in\; \mathbf{Z}[X]$$

Es ist $b_0 \neq 0$, da wegen $\vartheta \neq 0$ kein Faktor X abdividiert werden können darf (allgemeiner, Minimalpolynome von Elementen in Körpererweiterungen sind irreduzibel). Nun ist aber $b_0 = -(\vartheta^m + b_{m-1}\vartheta^{m-1} + \cdots + b_1\vartheta^1) \in \mathfrak{p}$ und somit $0 \neq b_0 \in \mathbf{Z} \cap \mathfrak{p}$.

Ist $\mathfrak{p}$ ein Primideal, dann auch $\mathfrak{p} \cap \mathbf{Z}$. Sei also $\mathfrak{p} \cap \mathbf{Z} = p\mathbf{Z}$, und betrachte

$$\mathbf{Z}[\xi]/p\mathbf{Z}[\xi] \;\simeq\; \mathbf{Z}[X]/(p, X^n{+}a_{n-1}X^{n-1}{+}\cdots{+}a_0) \;\simeq\; \mathbf{F}_p[X]/(X^n{+}a_{n-1}X^{n-1}{+}\cdots{+}a_0)\;.$$

Wir haben also einen surjektiven Ringhomomorphismus

$$\begin{array}{rcl} \mathbf{Z}[\xi] & \xrightarrow{\varphi} & \mathbf{F}_p[X]/(X^n + a_{n-1}X^{n-1} + \cdots + a_0) \\ \xi & \longmapsto & X\;, \end{array}$$

und die Primideale der rechten Seite entsprechen unter Urbildnahme den Primidealen der linken Seite, die p enthalten. Umgekehrt, das Bild eines Primideals in $\mathbf{Z}[\xi]$, das p enthält, ist ein Primideal der rechten Seite.

Die Primideale von $\mathbf{F}_p[X]/(X^n + a_{n-1}X^{n-1} + \cdots + a_0)$ sind die Hauptideale, die von den Primteilern von $X^n + a_{n-1}X^{n-1} + \cdots + a_0$ in $\mathbf{F}_p[X]$ erzeugt werden. Also gibt es ein $f(X) \in \mathbf{Z}[X]$ mit $\varphi(\mathfrak{p}) = (f(X))$, wobei $f(X) \in \mathbf{F}_p[X]$ zu lesen ist, und es wird

$$\mathfrak{p} \;=\; \varphi^{-1}(f(X)) \;=\; (p, f(\xi))\;.$$

(Das ist immer derselbe nützliche Trick.)

(b) Wir zeigen zunächst ein

Lemma. *Sei A eine* endliche *Menge von Primidealen von R, und sei $(\nu_\mathfrak{p})_{\mathfrak{p}\in A}$ ein Tupel nichtnegativer ganzer Zahlen. Dann gibt es ein $x \in R$ mit $v_\mathfrak{p}(x) = \nu_\mathfrak{p}$ für alle $\mathfrak{p} \in A$.*

Beweis. Nach dem Chinesischen Restsatz ist die kanonische Abbildung

$$R \longrightarrow \prod_{\mathfrak{p}\in A} R/\mathfrak{p}^{\nu_\mathfrak{p}+1}$$

surjektiv. Für $\mathfrak{p} \in A$ sei $y_\mathfrak{p} \in \mathfrak{p}^{\nu_\mathfrak{p}} \smallsetminus \mathfrak{p}^{\nu_\mathfrak{p}+1}$ (existent wegen der Eindeutigkeit der Primidealfaktorzerlegung). Sei x ein Urbild des Tupels $(y_\mathfrak{p})_{\mathfrak{p}\in A}$. Dann ist $x \equiv_{\mathfrak{p}^{\nu_\mathfrak{p}+1}} y_\mathfrak{p}$

(wenn unter $y_\mathfrak{p}$ auch ein Repräsentant in R verstanden werde), und wegen $v_\mathfrak{p}(y_\mathfrak{p}) = \nu_\mathfrak{p}$ auch $v_\mathfrak{p}(x) = \nu_\mathfrak{p}$.

Sei nun $\mathfrak{a} \subseteq R$ vorgegeben. Sei $A = \{\mathfrak{p} \text{ prim in } R \ : \ v_\mathfrak{p}(\mathfrak{a}) > 0\}$ die Menge der Primteiler von $\mathfrak{a}$. Das ist wegen $\mathfrak{a} = \prod_{\mathfrak{p}\in A} \mathfrak{p}^{v_\mathfrak{p}(\mathfrak{a})}$ eine endliche Menge. Mit dem Lemma gibt es nun ein $x \in R$ mit $v_\mathfrak{p}(x) = v_\mathfrak{p}(\mathfrak{a})$ für alle $\mathfrak{p} \in A$. Sei X die Menge der Primteiler von x. Mit dem Lemma gibt es auch ein $y \in R$ mit $v_\mathfrak{p}(y) = v_\mathfrak{p}(\mathfrak{a})$ für alle $\mathfrak{p} \in A$ und $v_\mathfrak{p}(y) = 0$ für $\mathfrak{p} \in X \setminus A$. Sei $\mathfrak{b} = (x, y)$. Wir behaupten $\mathfrak{a} = \mathfrak{b}$.

Fall $\mathfrak{p} \in A$. Dann ist $v_\mathfrak{p}(\mathfrak{b}) = \min(v_\mathfrak{p}(x), v_\mathfrak{p}(y)) = \min(v_\mathfrak{p}(\mathfrak{a}), v_\mathfrak{p}(\mathfrak{a})) = v_\mathfrak{p}(\mathfrak{a})$.

Fall $\mathfrak{p} \in X \setminus A$. Dann ist $v_\mathfrak{p}(\mathfrak{b}) = \min(v_\mathfrak{p}(x), v_\mathfrak{p}(y)) = \min(v_\mathfrak{p}(x), 0) = 0 = v_\mathfrak{p}(\mathfrak{a})$.

Fall $\mathfrak{p} \notin X$. Dann ist $v_\mathfrak{p}(\mathfrak{b}) = \min(v_\mathfrak{p}(x), v_\mathfrak{p}(y)) = \min(0, v_\mathfrak{p}(y)) = 0 = v_\mathfrak{p}(\mathfrak{a})$.

(c) Sei R ein Dedekindbereich mit endlich vielen Primidealen, und sei $\mathfrak{a} \subseteq R$ ein Ideal. Nach dem Lemma aus (b) gibt es ein $x \in R$ mit $v_\mathfrak{p}(x) = v_\mathfrak{p}(\mathfrak{a})$ für *alle* Primideale von R. Also ist $(x) = \mathfrak{a}$.

Aufgabe 2.

Wie bei Blatt 1, Aufgabe 1 (a), ist für ein Element $\xi = a + b\sqrt{d} \in \mathcal{Q}(\sqrt{d})$, $a = a(X) \in \mathcal{Q}$, $b = b(X) \in \mathcal{Q}$, nur der Fall $b \neq 0$ von Interesse, und dann ist

$$\mu_{\xi,\mathcal{Q}}(T) \ = \ T^2 - 2aT + (a^2 - db^2) \ .$$

Fall $p > 2$. Aus $2a \in \mathcal{Z}$ folgt $a \in \mathcal{Z}$, und aus $a^2 - db^2 \in \mathcal{Z}$ zunächst $db^2 \in \mathcal{Z}$, und somit $b \in \mathcal{Z}$.

Fall $p = 2$. Wir begnügen uns (notgedrungen) mit der folgenden Betrachtung.

Wir erhalten $\mu_{\xi,\mathcal{Q}}(T) \ = \ T^2 + (a^2 + db^2)$, und ξ ist ganz über $\mathcal{Z}$ genau dann, wenn $a^2 + db^2$ in $\mathcal{Z}$ liegt. Schreiben wir $a = a_1/a_2$ und $b = b_1/b_2$ gekürzt mit $a_1, a_2, b_1, b_2 \in \mathcal{Z}$, so muß also $a_1^2 b_2^2 \equiv_{a_2^2 b_2^2} da_2^2 b_1^2$ sein.

Zunächst folgt aus $a_1^2 b_2^2 \equiv_{a_2^2} 0$ und aus $(a_1, a_2) = 1$, daß $a_2 \mid b_2$. Dann folgt aus $da_2^2 b_1^2 \equiv_{b_2^2} 0$ und aus $(b_1, b_2) = 1$ und aus d quadratfrei, daß $b_2 \mid a_2$. Es folgt $a_2 = b_2 =: c$. Für ein solches ξ muß also c^2 ein Teiler von $a_1^2 + db_1^2$ sein.

Ferner ist $(d, c) = 1$, da ein gemeinsamer Primteiler db_1^2 und folglich auch a_1^2, und mithin a_1 teilte, wohingegen $(a_1, c) = 1$ gilt.

Wenn nun c^2 ein Element $f \in \mathcal{Z}$ teilt, dann teilt c^2 auch f', die Ableitung von f nach X. Denn aus $f = c^2 g$ mit $g \in \mathcal{Z}$ folgt $f' = 2cc'g + c^2 g' = c^2 g'$.

Wenn also c^2 das Element $a_1^2 + db_1^2$ teilt, dann auch $d'b_1^2$. (Weiteres Ableiten bringt nichts, da d' ein Quadrat in $\mathcal{Z}$ ist, und wir so $(d'b_1^2)' = 0$ erhalten.)

Da c teilerfremd zu b_1 ist, teilt c^2 mithin d'. Halten wir fest : Ist $\mathcal{O}$ der ganze Abschluß von $\mathcal{Z}$ in $\mathcal{Q}(\sqrt{d})$, und ist $e^2 = d'$, so wird

$$\mathcal{Z}[\sqrt{d}] \ \subseteq \ \mathcal{O} \ \subseteq \ e^{-1}\mathcal{Z}[\sqrt{d}] \ ,$$

und ist somit ein endlich erzeugter freier $\mathcal{Z}$-Modul (mangels Separabilität von $\mathcal{Q}(\sqrt{d})|\mathcal{Q}$ nicht a priori klar), dessen Basis im allgemeinen wohl schwierig zu bestimmen ist.

Beispiel. Ist d' eine Einheit in $\mathcal{Z}$, so ist $\mathcal{Z}[\sqrt{d}] = \mathcal{O}$. Z.B. ist $\mathcal{Z}[\sqrt{X^2 + X + 1}] = \mathcal{O}$.

Beispiel. Sei $d = X^3 + 1$, also $d' = X^2$ und $e = X$. Ein Element

$$X^{-1}(a_1 + b_1\sqrt{X^3+1})$$

ist ganz über $\mathbf{Z}$ genau dann, wenn

$$X^2 \mid a^2 + b^2(X^3+1)\ .$$

Es folgt $a(0) = b(0)$, und mithin ist $\mathcal{O}$ das $\mathcal{Z}$-lineare Erzeugnis von $\mathcal{Z}[\sqrt{X^3+1}]$ und $X^{-1}(1+\sqrt{1+X^3})$, d.h. wir $\mathcal{O} = \mathcal{Z}\langle 1, X^{-1}(1+\sqrt{1+X^3})\rangle$, oder aber $\mathcal{O} = \mathcal{Z}[X^{-1}(1+\sqrt{1+X^3})] \simeq \mathcal{Z}[T]/(T^2+X)$.

Aufgabe 3.

Um die Klassengruppe von $\mathbf{Z}[\sqrt{-5}]$ zu berechnen, bemühen wir die Tatsache, daß nach Minkowski jede Idealklasse ein Ideal $\mathfrak{a}$ mit

$$\mathrm{N}_{\mathbf{Q}(\sqrt{-5})|\mathbf{Q}}(\mathfrak{a}) \;\le\; \left(\frac{2}{\pi}\right)^s \sqrt{|\Delta_{\mathbf{Q}(\sqrt{-5})|\mathbf{Q}}|} \;=\; \frac{2}{\pi}\sqrt{20} \;<\; 3$$

hat. Wir haben also die Ideale $\mathfrak{a}$ mit Norm 2 zu betrachten. Da $2\mathbf{Z}[\sqrt{-5}] \subseteq \mathfrak{a}$, ist $\mathbf{Z} \cap \mathfrak{a} = 2\mathbf{Z}$. Die Ideale über $2\mathbf{Z}$ entsprechen den 3 Idealen von $\mathbf{F}_2[X]/(X^2+5)$, davon nichttrivial nur $(X+1)$. Dieses entspricht $\mathfrak{a} := (2, 1+\sqrt{-5})$, mit Norm 2. Wäre dieses Ideal ein Hauptideal, so gäbe es ein Element $a+b\sqrt{-5}$ mit Norm $a^2+5b^2 = 2$, wobei $a, b \in \mathbf{Z}$. Dies ist nicht der Fall. Damit gibt es genau zwei Idealklassen, und mithin ist notwendigerweise $\mathrm{Cl}(\mathbf{Z}[\sqrt{-5}]) \simeq C_2$.

Probe. Es muß $\mathfrak{a}^2$ ein Hauptideal sein. In der Tat wird $(2, 1+\sqrt{-5})^2 = (4, 2+2\sqrt{-5}, -4+2\sqrt{-5}) = (2)$ (hätte man auch in $\mathbf{F}_2[X]/(X^2+5)$ sehen können).

Aufgabe 4.

(a) Eine $\mathbf{Z}$-lineare Basis von $\mathbf{Z}[\sqrt{-13}]$ ist gegeben durch $(1, \sqrt{-13})$. Die Diskriminante ergibt sich zu

$$\Delta_{\mathbf{Q}(\sqrt{-13})|\mathbf{Q}} \;=\; \det\begin{pmatrix} \mathrm{Tr}(1) & \mathrm{Tr}(\sqrt{-13}) \\ \mathrm{Tr}(\sqrt{-13}) & \mathrm{Tr}(-13) \end{pmatrix} \;=\; \det\begin{pmatrix} 2 & 0 \\ 0 & -26 \end{pmatrix} \;=\; -52\,,$$

wobei $\mathrm{Tr} = \mathrm{Tr}_{\mathbf{Q}(\sqrt{-13})|\mathbf{Q}}$. Diese berechnet sich alternativ auch als Produkt aller Differenzen der Nullstellen von X^2+13, namentlich $(\sqrt{-13}-(-\sqrt{-13}))((-\sqrt{-13})-\sqrt{-13}) = -52$. Modulo p hat X^2+13 also genau dann mehrfache Nullstellen (man sagt, p verzweigt in $\mathbf{Z}[\sqrt{-13}]$), wenn p die Diskriminante teilt.

Es ist $X^2+13 \equiv_2 (X+1)^2$, also ergibt eine Betrachtung von $\mathbf{F}_2[X]/(X^2+13)$, daß $(2) = (2, 1+\sqrt{-13})^2$. Verzweigung!

Es ist $X^2+13 \equiv_5 X^2+3$ irreduzibel, also ist (5) prim.

Es ist $X^2+13 \equiv_7 (X-1)(X+1)$, also ist $(7) = (7, 1-\sqrt{-13})(7, 1+\sqrt{-13})$.

Es ist $X^2+13 \equiv_{13} X^2$, also ist $(13) = (\sqrt{-13})^2$. Verzweigung!

(b) Die Diskriminante ergibt sich zu

$$\Delta_{\mathbf{Q}((1+\sqrt{-15})/2)|\mathbf{Q}} \;=\; \det\begin{pmatrix} \mathrm{Tr}(1) & \mathrm{Tr}((1+\sqrt{-15})/2) \\ \mathrm{Tr}((1+\sqrt{-15})/2) & \mathrm{Tr}((-7+\sqrt{-15})/2) \end{pmatrix} \;=\; \det\begin{pmatrix} 2 & 1 \\ 1 & -7 \end{pmatrix} \;=\; -15\,,$$

Das Minimalpolynom von $(1+\sqrt{-15})/2$ über $\mathbf{Q}$ ist X^2-X+4.

Es ist $X^2-X+4 \equiv_2 X(X-1)$, also $(2)=(2,(1+\sqrt{-15})/2)(2,(1-\sqrt{-15})/2)$.

Es ist $X^2-X+4 \equiv_3 (X+1)^2$, also $(3)=(3,(3+\sqrt{-15})/2)^2$. Verzweigung!

Es ist $X^2-X+4 \equiv_5 (X+2)^2$, also $(5)=(5,(5+\sqrt{-15})/2)^2$. Verzweigung!

(c) Die Diskriminante wurde bis auf eine Einheit in $\mathbf{Z}$ schon auf Blatt 1 in Aufgabe 2 (a) berechnet, sie beträgt also $\pm p^{p-2}$.

Um das Vorzeichen zu bestimmen, kann man folgende Überlegung anstellen.

$$\begin{aligned}
\Delta_{\mathbf{Q}(\zeta_p)|\mathbf{Q}} &= \textstyle\prod_{i,j\in[1,p-1],\, i\neq j}(\zeta_p^i-\zeta_p^j) \\
&= \textstyle\prod_{i\in[1,p-1]} \Phi_p'(\zeta_p^i) \\
&= \mathrm{N}_{\mathbf{Q}(\zeta_p)|\mathbf{Q}}(\Phi_p'(\zeta_p)) \\
&= \mathrm{N}_{\mathbf{Q}(\zeta_p)|\mathbf{Q}}(\tfrac{p\zeta_p^{-1}}{\zeta_p-1}) \\
&= +p^{p-2}\ ,
\end{aligned}$$

da $\Phi_p'(X)=\frac{pX^{p-1}}{X-1}-\frac{X^p-1}{(X-1)^2}$, und da ζ_p-1 das Minimalpolynom $\Phi_p(X+1)$ und damit die Norm $(-1)^{p-1}\Phi_p(1)=p$ hat.

Betrachten wir das Ideal (2). Das Kreisteilungspolynom $\Phi_p(X)$ hat modulo 2 genau dann einen irreduziblen Faktor von Grad n, wenn $\mathbf{F}_{2^n}$ von einer p-ten Einheitswurzel erzeugt wird. Da $\#\mathbf{F}_{2^n}^*=2^n-1$, enthält $\mathbf{F}_{2^n}$ genau dann eine primitive p-te Einheitswurzel, wenn p ein Teiler von 2^n-1 ist, i.e. wenn $2^n\equiv_p 1$.

Sei d die Ordnung von 2 in $\mathbf{F}_p^*$. Insbesondere ist d ein Teiler von $p-1$. Wir behaupten, daß $\Phi_p(X)$ modulo 2 in $(p-1)/d$ irreduzible Polynome von Grad d zerfällt.

Es hat $\Phi_p(X)$ modulo 2 keinen irreduziblen Teiler von Grad kleiner als d. Nun enthält $\mathbf{F}_{2^d}^*\simeq C_{2^d-1}$ wegen $p\,|\,2^d-1$ aber $p-1$ primitive p-te Einheitswurzeln, und mehr kann es auch in $\mathbf{F}_{2^{p-1}}^*\simeq C_{2^{p-1}-1}$ nicht geben. Damit hat $\Phi_p(X)$ modulo 2 auch keinen irreduziblen Teiler von Grad größer als d.

Sei $\Phi_p(X)\equiv_2 f_1(X)\cdots f_{(p-1)/d}(X)$ eine Zerlegung in irreduzible Faktoren von Grad d. Dann ist dementsprechend

$$(2) \;=\; (2,f_1(\zeta_p))\cdots(2,f_{(p-1)/d}(\zeta_p))\ .$$

Bemerkung: Es gibt in $\mathbf{F}_{2^d}$ genau $(p-1)/d$ Bahnen von primitiven p-ten Einheitswurzeln unter der Operation von $\mathrm{Gal}(\mathbf{F}_{2^d}|\mathbf{F}_2)=\langle x\longmapsto x^2\rangle$ — im Unterschied zu $\mathbf{Q}(\zeta_p)|\mathbf{Q}$, in $\mathbf{Q}(\zeta_p)$ gibt es nur eine solche Bahn. Ein weiterer Unterschied besteht darin, daß man mit der Einheitswurzel auch ihr Minimalpolynom spezifizieren muß, also, zu welchem Faktor des zyklotomischen Polynoms das Element gehört.

Ist etwa β eine primitive siebte Einheitwurzel über $\mathbf{F}_2$, mit Minimalpolynom X^3+X+1, so ist in $\mathbf{F}_8=\mathbf{F}_2(\beta)$ auch $\beta+1$ eine primitive siebte Einheitswurzel. Die Galoisbahn von β ist hingegen gegeben durch $\{\beta,\beta^2,\beta^4=\beta^2+\beta\}$.

Beispiele. $p=31$. Es hat wegen $2^5=32$ das Element 2 die Ordnung 5 in $\mathbf{F}_{31}$. Und in der Tat wird

$$\begin{aligned}
\Phi_{31}(X) \;\equiv_2\; & (X^5+X^3+1)(X^5+X^2+1)(X^5+X^4+X^3+X^2+1) \\
& \cdot(X^5+X^4+X^3+X+1)(X^5+X^4+X^2+X+1) \\
& \cdot(X^5+X^3+X^2+X+1)\ .
\end{aligned}$$

$p = 43$. Es hat wegen $2^{14} = 43 \cdot 381 + 1$ (und 14 minimal mit einer solchen Zerlegung) das Element 2 die Ordnung 14 in $\mathbf{F}_{43}$. Und in der Tat wird

$$\begin{aligned}\Phi_{43}(X) \equiv_2 \; & (X^{14} + X^{11} + X^{10} + X^9 + X^8 + X^7 + X^6 + X^5 + X^4 + X^3 + 1) \\ & \cdot (X^{14} + X^{13} + X^{11} + X^7 + X^3 + X + 1) \\ & \cdot (X^{14} + X^{12} + X^{10} + X^7 + X^4 + X^2 + 1) \; .\end{aligned}$$

Betrachten wir das Ideal (p). Auf Blatt 1, Aufgabe 2 (a) wurde schon festgestellt, daß $(p) = (\zeta_p - 1)^{p-1}$ ist. Und in der Tat ist $\Phi_p(X) = \frac{X^p - 1}{X - 1} \equiv_p \frac{(X-1)^p}{X-1} = (X-1)^{p-1}$. Verzweigung!