G. Nebe, M. Künzer

Übungen Algebra II, Sommersemester 03

Lösung 4

Aufgabe 1. Wir geben eine Lösung in Stichworten. Im folgenden seien $s, s', \ldots, t, t', \cdots \in S$, $m, m', \cdots \in M$, $r, r', \cdots \in R$.

(a) Beachte, daß an verschiedenen Stellen R kommutativ und S Monoid gebraucht wird.

Die Relation $(\sim)$ auf $M \times S$ ist Äquivalenzrelation: Reflexiv mit $t = 1$. Symmetrisch per definitionem. Transitiv: $ms't = m'st$ und $m's''t' = m''s't'$ impliziert $ms''(s'tt') = ms'ts''t' = m'sts''t' = m's''t'st = m''s't'st = m''s(s'tt')$. Die Äquivalenzrelation ist von der Relation $(m, s) \approx (mt, st)$ erzeugt, da aus $ms't = m'st$ folgt, daß $(m, s) \approx (ms't, ss't) = (m'st, ss't) \approx (m', s')$.

(i) Wohldefiniertheit: $(mt)/(st) + (m't')/(s't') = (mts't' + m't'st)/(sts't') = (ms' + m's)/(ss')$.
Null: $0/1 + m/s = m/s$. Assoziativität:

$$\begin{aligned} (m/s + m'/s') + m''/s'' &= (ms's'' + m'ss'' + m''ss')/(ss's'') \\ &= m/s + (m'/s' + m''/s'') \,. \end{aligned}$$

Kommutativität per definitionem. Inverses Element: $m/s + (-m)/s = (ms + (-m)s)/s^2 = 0/1$. (Wir schreiben i.a. *nicht* $m/1 = m$, da $M \longrightarrow S^{-1}M$, $m \longmapsto m/1$ i.a. nicht injektiv ist, d.h. es kann $m \neq 0$, aber $m/1 = 0$ sein. Eine Ausnahme bildet der Fall, in welchem diese Injektivität bekannt und somit eine Identifikation als Teilmenge möglich ist.)

(ii) $S^{-1}R$ Ring: Wohldefiniertheit: $(rt/st)(r't'/s't') = (rtr't')/(sts't') = (rr')/(ss')$. Kommutativität und Assoziativität per definitionem. Eins: $(r/s)(1/1) = r/s$. Distributivität:

$$\begin{aligned} (r/s + r'/s')(r''/s'') &= (rs' + r's)r''/(ss's'') \\ &= (rr''s's'' + r'r''ss'')/(ss''s's'') \\ &= (rr'')/(ss'') + (r'r'')/(s's'') \,. \end{aligned}$$

$S^{-1}M$ Modul über $S^{-1}R$: Wohldefiniertheit:

$$\begin{aligned} (mt/st)(r't'/s't') &= (mtr't')/(sts't') \\ &= (mr')/(ss') \,. \end{aligned}$$

Assoziativität per definitionem. Eins: $(m/s)(1/1) = m/s$. Distributivität:

$$\begin{aligned} (m/s + m'/s')(r''/s'') &= (ms' + m's)r''/(ss's'') \\ &= (mr''s's'' + m'r''ss'')/(ss''s's'') \\ &= (mr'')/(ss'') + (m'r'')/(s's'') \,, \end{aligned}$$

und

$$\begin{aligned}(m/s)(r'/s'+r''/s'') &= m(r's''+r''s')/(ss's'') \\ &= (mr'ss''+mr''ss')/(ss'ss'') \\ &= (mr')/(ss')+(mr'')/(ss'')\ .\end{aligned}$$

Ringmorphismus λ: Es ist $(r+r')\lambda = r\lambda + r'\lambda$, und $(rr')\lambda = (r\lambda)(r'\lambda)$ per definitionem. Ist e.g. $R = \mathbf{Z}/6\mathbf{Z}$ und $S = \{1,3\}$, so ist λ wegen $2 \longmapsto 2/1 = 6/3 = 0/3 = 0/1$ nicht injektiv. (Das Beispiel $R = \mathbf{Z}$ zeigt, daß λ i.a. auch nicht surjektiv ist – ist etwa $s \in S \smallsetminus \{\pm 1\}$, so ist $1/s$ nicht im Bild von λ.)

(iii) Sei $S^{-1}R \xrightarrow{g} A$, $r/s \longmapsto (rf)(sf)^{-1}$. Wohldefiniert:

$$\begin{aligned}(rt)/(st) &\longmapsto (rf)(tf)(sf)^{-1}(tf)^{-1} \\ &= (rf)(sf)^{-1}\ .\end{aligned}$$

Ringmorphismus, da f Ringmorphismus. Es ist $r\lambda g = (r/1)g = (rf)(1f)^{-1} = rf$, d.h. $\lambda g = f$. Eindeutigkeit: Sei $S^{-1}R \xrightarrow{\tilde g} A$ Ringmorphismus mit $\lambda\tilde g = f$, d.h. $(r/1)\tilde g = rf$ stets. Es wird $(sf)(1/s)\tilde g = (s/1)\tilde g \cdot (1/s)\tilde g = ((s/1)(1/s))\tilde g = 1$, also $(1/s)\tilde g = (sf)^{-1}$. Mithin $(r/s)\tilde g = ((r/1)(1/s))\tilde g = (r/1)\tilde g \cdot (1/s)\tilde g = (rf)(sf)^{-1} = (r/s)g$, i.e. $\tilde g = g$. (Beachte, daß λ insbesondere ein Epimorphismus ist, der i.a. nicht surjektiv ist.)

Sei nun $R \xrightarrow{\tilde\lambda} \tilde R$ mit derselben universellen Eigenschaft ausgestattet, und sei $S\tilde\lambda \subseteq \tilde R^*$. Dann gibt es Ringmorphismen $\tilde R \xrightarrow{\tilde g} S^{-1}R$ und $S^{-1}R \xrightarrow{g} \tilde R$, eindeutig mit $\tilde\lambda\tilde g = \lambda$ resp. mit $\lambda g = \tilde\lambda$. Wir behaupten, daß λ und $\tilde\lambda$ sich invertierende Isomorphismen sind. Es ist $\tilde\lambda\tilde g g = \lambda g = \tilde\lambda 1$, also $\tilde g g = 1$. Es ist $\lambda g\tilde g = \tilde\lambda\tilde g = \lambda 1$, also $g\tilde g = 1$.

(iv) Das inverse Bild eines Primideals ist ein Primideal. Wäre $s \in \lambda^{-1}(\mathfrak{p}) \cap S$, so wäre $s/1 \in \mathfrak{p}$, also $\mathfrak{p} = S^{-1}R$, Widerspruch. Damit ist die Abbildung wohldefiniert.

Injektiv: Sei $\lambda^{-1}(\mathfrak{p}) = \lambda^{-1}(\tilde{\mathfrak{p}})$ und sei $r/s \in \mathfrak{p}$. Wir haben $r/s \in \tilde{\mathfrak{p}}$ zu zeigen. Nun ist aber auch $r/1 = (r/s)(s/1) \in \mathfrak{p}$, i.e. $r \in \lambda^{-1}(\mathfrak{p}) = \lambda^{-1}(\tilde{\mathfrak{p}})$, i.e. $r/1 \in \tilde{\mathfrak{p}}$. Daraus folgt $r/s = (r/1)(1/s) \in \tilde{\mathfrak{p}}$.

Surjektiv: Sei $\mathfrak{q} \subseteq R$ ein Primideal mit $\mathfrak{q} \cap S = \emptyset$. Sei $\mathfrak{p} := \{r/s \in S^{-1}R : r \in \mathfrak{q}\}$, was zunächst einmal auf einer wohldefinierten Aussage beruht, denn $r \in \mathfrak{q} \iff rt \in \mathfrak{q}$, da $t \notin \mathfrak{q}$. Es ist $\mathfrak{p} \subseteq S^{-1}R$ ein Ideal, und wir wollen zeigen, daß es ein Primideal ist. Zunächst ist $1/1 \notin \mathfrak{p}$, da ansonsten $1/1 = x/s$ mit $x \in \mathfrak{q}$ implizierte, daß $st = xt$, und $st \notin \mathfrak{q}$, aber $xt \in \mathfrak{q}$, Widerspruch. Sei nun $(r/s)(r'/s') \in \mathfrak{p}$. Es folgt $rr' \in \mathfrak{q}$, und somit $r \in \mathfrak{q}$ oder $r' \in \mathfrak{q}$, mithin $r/s \in \mathfrak{p}$ oder $r'/s' \in \mathfrak{p}$. Damit ist $\mathfrak{p}$ prim, und es bleibt zu zeigen, daß $\lambda^{-1}(\mathfrak{p}) = \mathfrak{q}$. Beide Inklusionen $\subseteq$, $\supseteq$ folgen jedoch aus der Definition von $\mathfrak{p}$.

(b) Es ist $\mathrm{Nil}\,(R) \subseteq \mathfrak{p}$ für jedes Primideal $\mathfrak{p}$. Nehmen wir an, die Inklusion $\subseteq$ sei echt, und sei $x \in \bigcap_{\mathfrak{p} \subseteq R \text{ prim}} \mathfrak{p} \smallsetminus \mathrm{Nil}\,(R)$. Mit $S = \{1, x, x^2, \dots\}$ behaupten wir, daß $S^{-1}R$ nicht der Nullring ist. In der Tat bedeutete $1/1 = 0/1$, daß es ein $m \geq 0$ gäbe mit $1 \cdot 1 \cdot x^m = 0 \cdot 1 \cdot x^m \in R$, was nicht geht, da x nicht nilpotent ist.

Sei $\mathfrak{m}$ ein maximales Ideal in $S^{-1}R$ (Zorn!), sei $\mathfrak{p} = \lambda^{-1}(\mathfrak{m})$. Damit gibt es ein Primideal in R disjunkt zu S, d.h. insbesondere $x \notin \mathfrak{p}$. Widerspruch.

(c) Wohldefiniertheit von $S^{-1}f$: $(mt)/(st) \longmapsto (mt)f/(st) = (mf)t/(st) = mf/s$.

Darüberhinaus ist $S^{-1}(fg) = (S^{-1}f)(S^{-1}g)$ und $S^{-1}1_M = 1_{S^{-1}M}$, i.e. $f \longmapsto S^{-1}f$ ist ein *Funktor* von der *Kategorie* der R-Moduln in die Kategorie der $S^{-1}R$-Moduln.

Lokalisieren exakt: Wir haben $\operatorname{Im} S^{-1}f = \operatorname{Kern} S^{-1}g$ zu zeigen. Die Inklusion $\subseteq$ folgt aus $(S^{-1}f)(S^{-1}g) = S^{-1}(fg) = 0$. Sei $(m/s)S^{-1}g = 0$, i.e. gebe es ein t mit $0 = (mg)t = (mt)g$. Dann ist $mt \in \operatorname{Kern} g = \operatorname{Im} f$. Sei $m'f = mt$. Wir erhalten $(m'/(st))S^{-1}f = m'f/(st) = (mt)/(st) = m/s$.

(d) Da allgemein $(M \oplus N)_{\mathfrak{p}} \simeq M_{\mathfrak{p}} \oplus N_{\mathfrak{p}}$, genügt es, $(\mathbf{Z}/q^n\mathbf{Z})_{(p)}$ zu berechnen für q prim und $n \geq 1$.

Fall $q \neq p$. Für $k \in \mathbf{Z}/q^n\mathbf{Z}$ und $s \in \mathbf{Z} \setminus (p)$ wird $k/s = kq/sq = 0/sq = 0/1$. Also ist $(\mathbf{Z}/q^n\mathbf{Z})_{(p)} = 0$.

Fall $q = p$. Wir behaupten, daß $\mathbf{Z}/p^n\mathbf{Z} \longrightarrow (\mathbf{Z}/p^n\mathbf{Z})_{(p)}$, $k \longmapsto k/1$, bijektiv ist. Injektiv: Ist $k/1 = 0/1$, i.e. gibt es ein $s \in \mathbf{Z} \setminus (p)$ mit $ks \equiv_{p^n} 0$, dann ist auch $k \equiv_{p^n} 0$. Surjektiv: sei k/s vorgegeben mit $s \in \mathbf{Z} \setminus (p)$ und $k \in \mathbf{Z}/p^n\mathbf{Z}$. Seien $u, v \in \mathbf{Z}$ mit $us + vp = 1$. Dann wird $uk/1 = usk/s = (us + vp)k/s = k/s$.

Sei M ein als Menge endlicher $\mathbf{Z}_{(p)}$-Modul, via Einschränkung also ein $\mathbf{Z}$-Modul. Die Abbildung $M \longrightarrow (M|_{\mathbf{Z}})_{(p)}$ ist ein Isomorphismus, mit Umkehrabbildung gegeben durch $ms^{-1} \longleftarrow\!\shortmid m/s$. Also ist M bis auf Isomorphie eine direkte Summe von Moduln der Form $\mathbf{Z}/p^n\mathbf{Z}$ für ein $n \geq 0$.

(e) Sei $m \in M$ und sei $\mathfrak{a} := \{r \in \mathbf{R} \ : \ rm = 0\}$ der Annullator von m. Ist für ein maximales Ideal $\mathfrak{m}$ die Lokalisierung $M_{\mathfrak{m}} = 0$, so heißt dies wegen $m/1 = 0$ insbesondere, daß es ein $t \in R \setminus \mathfrak{m}$ gibt mit $mt = 0$. Dann ist $t \in \mathfrak{a} \setminus \mathfrak{m}$, so daß $\mathfrak{a} \not\subseteq \mathfrak{m}$. Da dies für alle maximalen Ideale $\mathfrak{m} \subseteq R$ gilt, ist $\mathfrak{a} = R$, und somit $m = 0$. Da dies nun wiederum für alle $m \in M$ gilt, ist $M = 0$.

Die zweite Aussage folgt wegen der Exaktheit der Lokalisierung mit Betrachtung von Kern und Cokern.

(f) Sei $j \in \operatorname{Jac}(R)$. Wäre $1 - j$ in einem maximalen Ideal $\mathfrak{m} \subseteq R$ enthalten, so wegen $\operatorname{Jac}(R) \subseteq \mathfrak{m}$ auch $1 = j + (1 - j)$, was aber nicht der Fall ist. Damit ist das Ideal $R(1 - j) = R$, i.e. $1 - j$ eine Einheit.

Sei nun $\operatorname{Jac}(R)M = M$. Sei k die minimale Länge eines R-linearen Erzeugendensystems von M, und sei $m_1, \ldots, m_k$ ein solches. Wir haben $k = 0$ zu zeigen. Nehmen wir an, es sei $k \geq 1$. Schreibe $m_1 = m_1 j_1 + \cdots m_k j_k$. Wir erhalten $m_1 = (m_2 j_2 + \cdots m_k j_k)(1 - j_1)^{-1}$, was zeigt, daß bereits $m_2, \ldots, m_k$ ein Erzeugendensystem von M ist. Widerspruch.

Sei $N \subseteq M$. Aus $\operatorname{Jac}(R)M + N = M$ folgt $\operatorname{Jac}(R)(M/N) = 0$, und somit $N = M$.

Ist $\bar{f}$ epimorph, so ist $\operatorname{Jac}(R)M' + \operatorname{Im} f = M'$, und folglich $\operatorname{Im} f = M'$, i.e. f surjektiv.

Sei $\bar{f}$ nun isomorph, und M' projektiv. Wie eben folgt zunächst, daß f surjektiv ist, und nun insbesondere auch, daß es ein $M \xleftarrow{g} M'$ mit $gf = 1_{M'}$ gibt. (Man sagt, f ist *split epimorph* oder auch *Retraktion*. Entsprechend heißt g *split monomorph* oder auch *Coretraktion*.) Sei K der Kern von $M \xrightarrow{f} M'$. Für f isomorph bleibt $K = 0$ zu zeigen.

Sei L der Kern von $M \xrightarrow{1-fg} M$. Wir behaupten, daß $K \oplus L = M$. Die Gleichung $x = x(1 - fg) + xfg$ zeigt wegen $x(1 - fg) \in K$ und $xfg \in L$, daß $K + L = M$. Sei $x \in K \cap L$. Dann ist $0 = x(1 - fg) = x$. Es folgt $K \cap L = 0$.

Wegen $\bar{f}$ injektiv ist nun $K \subseteq \operatorname{Jac}(R)M$. Also folgt aus $K \oplus L = M$, daß $\operatorname{Jac}(R)M + L = M$, und mit Nakayama, daß $L = M$. Das aber impliziert $K = 0$.

Aufgabe 2.

(a) Da eine Basis von T über R auch eine Basis von ST über S ist, und da die $\operatorname{Tr}_{E|L}(x) = \operatorname{Tr}_{M|K}(x)$ für $x \in M$, ist die Diskriminante von ST über S gleich (1). Es ist mithin $1 \cdot U \subseteq ST$. Da jedenfalls $ST \subseteq U$, ist mithin $U = ST$. Die Diskriminante von E über K ergibt sich mit Blatt 3, Aufgabe 2 zu $(\Delta_{E|K}) = (\Delta_{L|K})^{[E:L]} = (\Delta_{L|K})^{[M:K]}$.

(b) Zunächst einmal treffen wir die Vereinbarung, daß $\zeta_{p^{m+1}}^p = \zeta_{p^m}$ für $m \geq 1$ stets gelte. Alternativ zu Neukirch kann man wie folgt vorgehen.

Berechnen wir das Diskriminantenideal von $\mathbf{Z}[\zeta_{p^m}]$ über $\mathbf{Z}$ induktiv. Wir behaupten, daß es gleich

$$(p)^{p^{m-1}(mp-m-1)}$$

ist, was für $m = 1$ nach Blatt 1, Aufgabe 2 (a) zutrifft. Sei die Aussage zutreffend für das Diskriminantenideal von $\mathbf{Z}[\zeta_{p^{m-1}}]$ über $\mathbf{Z}$, sei dieses also gegeben durch $(p)^{p^{m-2}((m-1)p-m)}$. Es handelt sich um eine lokale Frage (ein Ideal ist bestimmt, wenn man seine Primidealfaktoren kennt), also können wir nach Lokalisierung Blatt 3, Aufgabe 2 anwenden.

Das Diskriminantenideal von $\mathbf{Z}[\zeta_{p^m}]$ über $\mathbf{Z}[\zeta_{p^{m-1}}]$ berechnet sich wegen

$$\mu_{\zeta_{p^m},\mathbf{Q}(\zeta_{p^{m-1}})}(X) = X^p - \zeta_{p^{m-1}} = \prod_{i\in[0,p-1]} (X - \zeta_{p^m}\zeta_p^i)$$

zu

$$\begin{aligned} \left(\prod_{i\in[0,p-1]} \mu'_{\zeta_{p^m},\mathbf{Q}(\zeta_{p^{m-1}})}(\zeta_{p^m}\zeta_p^i)\right) &= \left(\prod_{i\in[0,p-1]} p\zeta_{p^m}^{p-1}\zeta_p^{i(p-1)}\right) \\ &= (p)^p\ . \end{aligned}$$

Damit wird das Diskriminantenideal von $\mathbf{Z}[\zeta_{p^m}]$ über $\mathbf{Z}$ zu

$$\left((p)^{p^{m-2}((m-1)p-m)}\right)^p \left((p)^p\right)^{p^{m-1}(p-1)} = (p)^{p^{m-1}((m-1)p-m+p-1)}\ ,$$

wie behauptet.

Nun zum Ring der ganzen Zahlen $\mathcal{O}$ in $\mathbf{Q}(\zeta_{p^m})$. Nach dem eben gesehenen ist $p^N\mathcal{O} \subseteq \mathbf{Z}[\zeta_{p^m}]$ für ein N groß genug. Nun ist mit $\lambda = \zeta_{p^m} - 1$ wieder $\mathcal{O}\lambda^{p^{m-1}(p-1)} = \mathcal{O}p$, da auch $(\zeta_{p^m}^a - 1)/(\zeta_{p^m} - 1)$ für $a \in \mathbf{Z}$ teilerfremd zu p eine Einheit in $\mathbf{Z}[\zeta_{p^m}]$ und also auch in $\mathcal{O}$ darstellt, und das Produkt über alle solchen Terme $(\zeta_{p^m}^a - 1)$ bis auf Vorzeichen gleich $\Phi_{p^m}(X)|_{X=1} = X^{p^{m-1}(p-1)} + X^{p^{m-1}(p-2)} + \cdots + 1|_{X=1} = p$ ist. Wegen $\mathcal{O}/\mathcal{O}\lambda \simeq \mathbf{Z}/p\mathbf{Z}$ (Verzweigungsindex $e = p^{m-1}(p-1)$ impliziert Trägheitsindex $f = 1$) ist $\lambda\mathcal{O} + \mathbf{Z} = \mathcal{O}$. Dies läßt sich iterieren zu $\lambda^M\mathcal{O} + \mathbf{Z} = \mathcal{O}$ für $M \geq 1$ beliebig, woraus wir $\mathbf{Z}[\zeta_{p^m}] \supseteq \mathcal{O}$ und somit $\mathbf{Z}[\zeta_{p^m}] = \mathcal{O}$ entnehmen. Speziell wird

$$(\Delta_{\mathbf{Q}(\zeta_{p^m})|\mathbf{Q}}) = (p)^{p^{m-1}(mp-m-1)}\ .$$

(c) Im folgenden bezeichnen $p, q \in \mathbf{Z}$ Primzahlen. Wir schreiben $n[p] = p^{v_p(n)}$, so daß $n = \prod_{p|n} n[p]$. Mit (b) ist die Diskriminante von $\mathbf{Q}(\zeta_{n[p]})$ über $\mathbf{Q}$ eine Potenz von

p. Iterierte Anwendung von (a) liefert also, daß der Ring der ganzen Zahlen durch $\prod_{p|n} \mathbf{Z}[\zeta_{n[p]}] = \mathbf{Z}[\zeta_n]$ gegeben ist, und daß

$$(\Delta_{\mathbf{Q}(\zeta_n)|\mathbf{Q}}) \;=\; \prod_{p|n} (p)^{n(v_p(n)-1/(p-1))\prod_{q|n}(1-1/q)} \;.$$

(d) Wir haben $G := \mathrm{Gal}(\mathbf{Q}(\zeta_{24})|\mathbf{Q}) \simeq (\mathbf{Z}/24\mathbf{Z})^* = \{1,5,7,11,13,17,19,23\}$. Den Isomorphismus verwenden wir als Identifikation.

(i) Es ist $\mathbf{Z}[\zeta_{24}]/(2) \simeq \mathbf{F}_2[X]/(X^2+X+1)^4$, und also $(2) = (2, 1+\zeta_{24}+\zeta_{24}^2)^4$. Der Trägheitsindex von $\mathfrak{p} = (2, 1+\zeta_{24}+\zeta_{24}^2) = (1+\zeta_{24}+\zeta_{24}^2)$ ist 2, der Verzweigungsindex ist 4.

Da $\mathfrak{p}$ das einzige Primideal über (2) ist, ist die Zerlegungsgruppe $G_\mathfrak{p} = G$, und der Zerlegungskörper

$$Z_\mathfrak{p} \;=\; \mathbf{Q}\,.$$

Die Faktorisierung von (2) in $\mathbf{Z}$ ist trivial – es liegt ja auch keine Zerlegung vor.

Die Trägheitsgruppe $I_\mathfrak{p}$ besteht aus den Elementen $m \in G$, für die die Operation $\zeta_{24} \longmapsto \zeta_{24}^m$ die triviale Operation modulo $\mathfrak{p}$ induziert. In anderen Worten, wir suchen die Elemente m, für die $X^m - X$ in $\mathbf{F}_2[X]$ durch X^2+X+1 teilbar ist. Wir erhalten $I_\mathfrak{p} = \{1,7,13,19\} = \langle 7, 13\rangle$, und

$$T_\mathfrak{p} \;=\; \mathbf{Q}(\zeta_3)\,.$$

Es ist $\mathbf{Z}[\zeta_3]/(2) \simeq \mathbf{F}_2[X]/(X^2+X+1)$, folglich ist $(2) = (2)^1$ prim in $\mathbf{Z}[\zeta_3]$, hat allerdings Trägheitsindex 2.

In $\mathbf{Z}[\zeta_{24}]$ zerlegt sich (2) dann noch wie schon erwähnt in $(2) = (1+\zeta_{24}+\zeta_{24}^2)^4$, mit Verzweigungsindex 4.

(ii) Es ist $\mathbf{Z}[\zeta_{24}]/(3) \simeq \mathbf{F}_3[X]/(X^2+X-1)^2(X^2-X-1)^2$, und folglich $(3) = (3, \zeta_{24}^2+\zeta_{24}-1)^2(3, \zeta_{24}^2-\zeta_{24}-1)^2$.

Die Zerlegungsgruppe $G_\mathfrak{p}$ von $\mathfrak{p} := (3, \zeta_{24}^2+\zeta_{24}-1)$ besteht aus den Elementen $m \in (\mathbf{Z}/24\mathbf{Z})^*$, für die die Operation $\zeta_{24} \longmapsto \zeta_{24}^m$ das Primideal $\mathfrak{p}$ in sich überführt, i.e. für die $X^{2m}+X^m-1$ in $\mathbf{F}_3[X]$ durch X^2+X-1 teilbar ist. Wir erhalten $G_\mathfrak{p} = \{1,11,17,19\} = \langle 17, 19\rangle$ und

$$\boxed{Z_\mathfrak{p} \;=\; \mathbf{Q}(\sqrt{-2})\,,}$$

wobei $\sqrt{-2} = \zeta_{24}^3 + \zeta_{24}^9$ (beachte, daß unter $\zeta_{24} \longmapsto \zeta_{24}^{17}$ die Elemente $\zeta_8 \longmapsto \zeta_8$ und $\zeta_3 \longmapsto \zeta_3^{-1}$ abgebildet werden; und unter $\zeta_{24} \longmapsto \zeta_{24}^{17}$ die Elemente $\zeta_8 \longmapsto \zeta_8^3$ sowie $\zeta_3 \longmapsto \zeta_3$). Es ist $\mathbf{Z}[\sqrt{-2}]/(3) \simeq \mathbf{F}_3[X]/(X+1)(X-1)$, also

$$\boxed{(3) \;=\; (3, 1+\sqrt{-2})(3, 1-\sqrt{-2}) \;=\; (1+\sqrt{-2})(1-\sqrt{-2}) \;\subseteq \mathbf{Z}[\sqrt{-2}]\,.}$$

Insbesondere haben wir hier nur Zerlegung, keine Verzweigung und keine Trägheit.

Die Trägheitsgruppe ergibt sich zu $I_\mathfrak{p} = \{1, 17\} = \langle 17\rangle$, und somit ist

$$\boxed{T_\mathfrak{p} \;=\; \mathbf{Q}(\zeta_8)\,,}$$

wobei $\zeta_8 = \zeta_{24}^3$.

Zum einen ist

$$\begin{aligned}\mathbf{Z}[\zeta_8]/(1+\sqrt{-2}) &\simeq \mathbf{Z}[\sqrt{-2}][X]/(1+\sqrt{-2}, X^2-\sqrt{-2}X-1)\\ &\simeq \mathbf{F}_3[X]/(X^2+X-1)\,,\end{aligned}$$

und somit bleibt

$$\boxed{(1+\sqrt{-2}) \;=\; (1+\zeta_8+\zeta_8^3)^1 \;\subseteq\; \mathbf{Z}[\zeta_8]}$$

prim, mit Trägheitsindex 2.
Zum anderen ist

$$\begin{aligned}\mathbf{Z}[\zeta_8]/(1-\sqrt{-2}) &\simeq \mathbf{Z}[\sqrt{-2}][X]/(1-\sqrt{-2}, X^2-\sqrt{-2}X-1)\\ &\simeq \mathbf{F}_3[X]/(X^2-X-1)\,,\end{aligned}$$

und somit bleibt auch

$$\boxed{(1-\sqrt{-2}) \;=\; (1-\zeta_8-\zeta_8^3)^1 \;\subseteq\; \mathbf{Z}[\zeta_8]}$$

prim, mit Trägheitsindex 2. (Das hätte man auch daraus folgern können, daß $(1-\sqrt{-2})$ ein galoiskonjugiertes Primideal zu $(1+\sqrt{-2})$ in $\mathbf{Z}[\sqrt{-2}]$ ist.)
Schließlich wird

$$\begin{aligned}\mathbf{Z}[\zeta_{24}]/(1+\zeta_8+\zeta_8^3) &\simeq \mathbf{Z}[\zeta_8][X]/(1+\zeta_8+\zeta_8^3, X^2+\zeta_8^3X-\zeta_8^2)\\ &\simeq \Big(\underbrace{\mathbf{F}_3[Y]/(Y^2+Y-1)}_{=:\,\mathbf{F}_9}\Big)[X]/(X^2-(Y+1)X+Y-1)\\ &= \mathbf{F}_9[X]/(X+Y+1)^2\,,\end{aligned}$$

womit

$$\boxed{(1+\zeta_8+\zeta_8^3) \;=\; (1+\zeta_8+\zeta_8^3, \zeta_8+\zeta_{24}+1)^2 \;=\; (\zeta_{24}^3+\zeta_{24}+1)^2 \;\subseteq\; \mathbf{Z}[\zeta_{24}]\,,}$$

mit Trägheitsindex 1 und Verzweigungsindex 2.
Als Variante davon erhalten wir

$$\begin{aligned}\mathbf{Z}[\zeta_{24}]/(1-\zeta_8-\zeta_8^3) &\simeq \mathbf{Z}[\zeta_8][X]/(1-\zeta_8-\zeta_8^3, X^2+\zeta_8^3X-\zeta_8^2)\\ &\simeq \Big(\underbrace{\mathbf{F}_3[Y]/(Y^2-Y-1)}_{=:\,\mathbf{F}_9}\Big)[X]/(X^2+(1-Y)X-Y-1)\\ &= \mathbf{F}_9[X]/(X+Y-1)^2\,,\end{aligned}$$

womit

$$\boxed{(1-\zeta_8-\zeta_8^3) \;=\; (1-\zeta_8-\zeta_8^3, \zeta_8+\zeta_{24}-1)^2 \;=\; (\zeta_{24}^3+\zeta_{24}-1)^2 \;\subseteq\; \mathbf{Z}[\zeta_{24}]\,,}$$

mit Trägheitsindex 1 und Verzweigungsindex 2.
Insgesamt zerlegt sich (3) in $\mathbf{Z}[\zeta_{24}]$, alternativ zu den eingangs gefundenen Idealerzeugern in den Faktoren, in

$$\boxed{(3) \;=\; (\zeta_{24}^3+\zeta_{24}+1)^2(\zeta_{24}^3+\zeta_{24}-1)^2 \;\subseteq\; \mathbf{Z}[\zeta_{24}]\,.}$$

Probe: Als Element ist $(\zeta_{24}^3+\zeta_{24}+1)^2(\zeta_{24}^3+\zeta_{24}-1)^2 = 3\cdot(2\zeta_{24}^6+\zeta_{24}^4-2\zeta_{24}^2-2) = 3/(\zeta_{24}^2-1)^2$.
Wir merken noch an, daß die Zerlegungsgruppe $G_\mathfrak{q}$ von $\mathfrak{q} := (3, \zeta_{24}^2-\zeta_{24}-1) = (\zeta_{24}^3+\zeta_{24}-1)$ zu $G_\mathfrak{p}$ in G konjugiert ist, und so wegen G abelsch mit $G_\mathfrak{p}$ übereinstimmt. Genauso folgt $I_\mathfrak{q} = I_\mathfrak{p}$.

(iii) Es ist $\mathbf{Z}[\zeta_{24}]/(13) \simeq \mathbf{F}_2[X]/(X^2-2)(X^2+2)(X^2-6)(X^2+6)$, und also

$$\begin{aligned} (13) &= (13,\zeta_{24}^2-2)(13,\zeta_{24}^2+2)(13,\zeta_{24}^2-6)(13,\zeta_{24}^2+6) \\ &= (\zeta_{24}^2-2)(\zeta_{24}^2+2)(13,\zeta_{24}^2-6)(13,\zeta_{24}^2+6)\ , \end{aligned}$$

mit Trägheitsindizes 2 und Verzweigungsindizes 1.

Sei $\mathfrak{p} = (\zeta_{24}^2-2)$. Als Zerlegungsgruppe ergibt sich $G_\mathfrak{p} = \{1,13\} = \langle 13\rangle$, und wir erhalten

$$Z_\mathfrak{p} \;=\; \mathbf{Q}(\zeta_{12})\ ,$$

wobei $\zeta_{12} = \zeta_{24}^2$. Es ist $\mathbf{Z}[\zeta_{12}]/(13) \simeq \mathbf{F}_{13}[X]/(X-2)(X+2)(X-6)(X+6)$, und somit $(13) = (\zeta_{12}-2)(\zeta_{12}+2)(13,\zeta_{12}-6)(13,\zeta_{12}+6)$.

Als Trägheitsgruppe ergibt sich $I_\mathfrak{p} = 1$ (was mangels Verzweigung ja auch der Fall sein muß), und somit

$$T_\mathfrak{p} = \mathbf{Q}(\zeta_{24})\ .$$

Oben haben wir schon gesehen, daß alle Primidealfaktoren von (13) in $\mathbf{Z}[\zeta_{12}]$ auch in $\mathbf{Z}[\zeta_{24}]$ prim bleiben, mit jeweiligem Trägheitsindex 2.