D-MATH | Number Theory I | HS 2023
Prof. Richard Pink

Solutions 10

Different and discriminant

1. Let L/K be a Galois extension of number fields with Galois group Γ, and let $\mathfrak{b}$ be a fractional ideal of $\mathcal{O}_L$. Show that

$$\mathrm{Nm}_{L/K}(\mathfrak{b}) \;=\; K \cap \prod_{\gamma\in\Gamma} {}^{\gamma}\mathfrak{b}.$$

Solution: For any fractional ideal $\mathfrak{b}$ of $\mathcal{O}_L$ we set $N(\mathfrak{b}) := K \cap \prod_{\gamma\in\Gamma} {}^{\gamma}\mathfrak{b}$, which by construction is an A-submodule of K. Since $\mathrm{Nm}_{L/K}(\mathfrak{b})$ is the fractional ideal of $\mathcal{O}_K$ that is generated by the elements $\mathrm{Nm}_{L/K}(b) = \prod_{\gamma\in\Gamma} {}^{\gamma}b$ for all $b \in \mathfrak{b}$, and all these lie in $N(\mathfrak{b})$, we have $\mathrm{Nm}_{L/K}(b) \subset N(\mathfrak{b})$. In particular $N(\mathfrak{b})$ is non-zero.

Also, by construction we have $1 = \mathrm{Nm}_{L/K}(1) \in \mathrm{Nm}_{L/K}(\mathcal{O}_L) \subset \mathcal{O}_K$ and therefore $\mathrm{Nm}_{L/K}(\mathcal{O}_L) = \mathcal{O}_K$. The multiplicativity of the relative norm thus implies that

$$\mathcal{O}_K = \;\mathrm{Nm}_{L/K}(\mathcal{O}_L) \;=\; \mathrm{Nm}_{L/K}(\mathfrak{b}) \cdot \mathrm{Nm}_{L/K}(\mathfrak{b}^{-1}) \;\subset\; N(\mathfrak{b}) \cdot N(\mathfrak{b}^{-1}).$$

On the other hand we compute that

$$N(\mathfrak{b}) \cdot N(\mathfrak{b}^{-1}) = \Big(K \cap \prod_{\gamma\in\Gamma} {}^{\gamma}\mathfrak{b}\Big) \cdot \Big(K \cap \prod_{\gamma\in\Gamma} {}^{\gamma}\mathfrak{b}^{-1}\Big) \subset K \cap \prod_{\gamma\in\Gamma} {}^{\gamma}\mathfrak{b}\,{}^{\gamma}\mathfrak{b}^{-1} = K \cap \mathcal{O}_L = \mathcal{O}_K.$$

In particular this shows that $N(\mathfrak{b}) \subset \frac{1}{a}\mathcal{O}_K$ for any $a \in N(\mathfrak{b}^{-1}) \setminus \{0\}$; hence $N(\mathfrak{b})$ is a fractional ideal of $\mathcal{O}_K$. Also, together we conclude that the inclusion

$$\mathrm{Nm}_{L/K}(\mathfrak{b}) \cdot \mathrm{Nm}_{L/K}(\mathfrak{b}^{-1}) \;\subset\; N(\mathfrak{b}) \cdot N(\mathfrak{b}^{-1})$$

must be an equality. Thus the inclusion of fractional ideals $\mathrm{Nm}_{L/K}(\mathfrak{b}) \subset N(\mathfrak{b})$ is an equality, as desired.

2. Let A be a Dedekind ring with quotient field K. Take finite separable extensions $M/L/K$ and let $C/B/A$ be the respective integral closures of A.

   (a) Prove that $\mathrm{Nm}_{L/K}(\mathrm{Nm}_{M/L}(\mathfrak{c})) = \mathrm{Nm}_{M/K}(\mathfrak{c})$ for any fractional ideal $\mathfrak{c}$ of C.

   (b) Prove that $\mathrm{diff}_{C/A} = \mathrm{diff}_{C/B} \cdot \mathrm{diff}_{B/A}$.

Solution:

(a) For any fractional ideal $\mathfrak{c}$ of C and any $x \in M^\times$ we have

$$\begin{aligned}\mathrm{Nm}_{L/K}(\mathrm{Nm}_{M/L}(x\mathfrak{c})) &= \mathrm{Nm}_{L/K}\big(\mathrm{Nm}_{M/L}(x) \cdot \mathrm{Nm}_{M/L}(\mathfrak{c})\big) \\ &= \mathrm{Nm}_{L/K}(\mathrm{Nm}_{M/L}(x)) \cdot \mathrm{Nm}_{L/K}(\mathrm{Nm}_{M/L}(\mathfrak{c})) \\ &= \mathrm{Nm}_{M/K}(x) \cdot \mathrm{Nm}_{L/K}(\mathrm{Nm}_{M/L}(\mathfrak{c}))\end{aligned}$$

and

$$\mathrm{Nm}_{M/K}(x\mathfrak{c})) = \mathrm{Nm}_{M/K}(x) \cdot \mathrm{Nm}_{M/K}(\mathfrak{c}).$$

Since any fractional ideal of C can be written in the form $x\mathfrak{c}$ for an $x \in M^\times$ and a non-zero ideal $\mathfrak{c} \subset C$, it suffices to prove the desired formula in the case $\mathfrak{c} \subset C$.

In that case choose $z \in \mathfrak{c} \setminus \{0\}$ and set $x := \mathrm{Nm}_{M/K}(z)$. Since $\mathfrak{c} \subset C$ we then have $x \in \mathfrak{c} \setminus \{0\}$ and can therefore write $\mathfrak{c} = (x, w)$ for some $w \in M$. By the lemma from §6.6 we then have

$$\mathrm{Nm}_{M/K}(\mathfrak{c}) = (x, \mathrm{Nm}_{M/K}(w)).$$

On the other hand we have $y := \mathrm{Nm}_{M/L}(z) \in \mathrm{Nm}_{M/L}(\mathfrak{c})$ and therefore $\mathrm{Nm}_{M/L}(\mathfrak{c}) = (y, \mathrm{Nm}_{M/L}(w))$ by the same lemma. Since $x = \mathrm{Nm}_{M/K}(z) = \mathrm{Nm}_{L/K}(y) \in \mathrm{Nm}_{L/K}(\mathrm{Nm}_{M/L}(\mathfrak{c}))$, using the same lemma again implies that

$$\mathrm{Nm}_{L/K}(\mathrm{Nm}_{M/L}(\mathfrak{c})) = (x, \mathrm{Nm}_{K/L}(\mathrm{Nm}_{M/L}(w))) = (x, \mathrm{Nm}_{M/K}(w)).$$

The desired equality follows.

(b) For any element $z \in M$ we have $z \in \mathrm{diff}_{C/A}^{-1}$ if and only if

$$\begin{aligned} & \forall\, c \in C\colon\ \mathrm{Tr}_{M/K}(cz) \in A \\ \iff & \forall\, c \in C\colon\ \forall\, b \in B\colon\ \mathrm{Tr}_{M/K}(bcz) \in A \\ \iff & \forall\, c \in C\colon\ \forall\, b \in B\colon\ \mathrm{Tr}_{L/K}(\mathrm{Tr}_{M/L}(bcz)) \in A \\ \iff & \forall\, c \in C\colon\ \forall\, b \in B\colon\ \mathrm{Tr}_{L/K}(b\,\mathrm{Tr}_{M/L}(cz)) \in A \\ \iff & \forall\, c \in C\colon\ \mathrm{Tr}_{M/L}(cz) \in \mathrm{diff}_{B/A}^{-1}. \end{aligned}$$

Since $\mathrm{Tr}_{M/L}$ is L-linear, multiplying by $\mathrm{diff}_{B/A}^{\pm 1}$ shows that the last condition is equivalent to

$$\forall\, y \in C {\cdot} \mathrm{diff}_{B/A}\colon\ \mathrm{Tr}_{M/L}(yz) \in B.$$

That in turn is equivalent to

$$\begin{aligned} & \forall\, y \in \mathrm{diff}_{B/A}\colon \forall\, c \in C\colon\ \mathrm{Tr}_{M/L}(cyz) \in B \\ \iff & \forall\, y \in \mathrm{diff}_{B/A}\colon yz \in \mathrm{diff}_{C/B}^{-1} \\ \iff & \mathrm{diff}_{B/A} \cdot z \in \mathrm{diff}_{C/B}^{-1} \\ \iff & z \in \mathrm{diff}_{B/A}^{-1}\,\mathrm{diff}_{C/B}^{-1}. \end{aligned}$$

Therefore $\mathrm{diff}_{C/A}^{-1} = \mathrm{diff}_{B/A}^{-1}\,\mathrm{diff}_{C/B}^{-1}$, from which the claim follows.

3. For $K := \mathbb{Q}(\sqrt[3]{2})$ compute the prime factorization of the different $\operatorname{diff}_{\mathcal{O}_K/\mathbb{Z}}$ and verify that a prime ideal of $\mathcal{O}_K$ divides $\operatorname{diff}_{\mathcal{O}_K/\mathbb{Z}}$ if and only if it is ramified over $\mathbb{Z}$.

Solution: By Exercise 3 of Sheet 8 we have $\mathcal{O}_K = \mathbb{Z}[\omega]$ with $\omega := \sqrt[3]{2}$. The minimal polynomial of ω over $\mathbb{Q}$ is $f(X) := X^3 - 2$; hence by Proposition 6.7.3 we have

$$\operatorname{diff}_{\mathcal{O}_K/\mathbb{Z}} = \left(\tfrac{df}{dX}(\omega)\right) = \left(3\omega^2\right).$$

In the solution of Exercise 4 on Sheet 8, we calculated that $\mathcal{O}_K/2\mathcal{O}_K \cong \mathbb{F}_2[X]/(X)^3$ and $\mathcal{O}_K/3\mathcal{O}_K \cong \mathbb{F}_3[X]/(X-2)^3$. Therefore $2\mathcal{O}_K = \mathfrak{p}_2^3$ and $3\mathcal{O}_K = \mathfrak{p}_3^3$ for the prime ideals $\mathfrak{p}_2 := (2,\omega) = (\omega)$ and $\mathfrak{p}_3 := (3, \omega - 2)$. The prime factorization of the different is therefore $\operatorname{diff}_{\mathcal{O}_K/\mathbb{Z}} = \mathfrak{p}_3^3\mathfrak{p}_2^2$.

In particular, the primes $\mathfrak{p}_2$ and $\mathfrak{p}_3$ are totally ramified over $\mathbb{Z}$ and divide the different. Any other prime $\mathfrak{p}$ of $\mathcal{O}_K$ lies over a rational prime $p \neq 2, 3$. The polynomial $f(X) = X^3 - 2$ is then separable modulo p. Thus its decomposition in $\mathbb{F}_p[X]$ has no multiple factors, and so all exponents in the prime factorization of $p\mathcal{O}_K$ are 1. Thus $\mathfrak{p}$ is unramified over $\mathbb{Z}$ and does not divide the different. Together this shows that a prime of $\mathcal{O}_K$ is ramified over $\mathbb{Z}$ if and only if it divides $\operatorname{diff}_{\mathcal{O}_K/\mathbb{Z}}$.

4. Let $K := \mathbb{Q}(\alpha)$ for $\alpha := \sqrt[3]{539}$.

(a) Using Exercise 5 of Sheet 8, show that (7) and (11) are totally ramified in $\mathcal{O}_K$. Let $\mathfrak{p}_7$ and $\mathfrak{p}_{11}$ denote the prime ideals above (7) and (11), respectively.

(b) Using the discriminant, show that $\mathcal{O}_K = \alpha\mathbb{Z} \oplus \beta\mathbb{Z} \oplus \gamma\mathbb{Z}$, where $\beta := \frac{77}{\alpha}$ and $\gamma := \frac{1+2\alpha+\beta}{3}$, and that $\operatorname{disc}(\mathcal{O}_K) = -3 \cdot 7^2 \cdot 11^2$.

(c) Show that $3\mathcal{O}_K = \mathfrak{p}_3^2\mathfrak{p}_3'$ for distinct prime ideals $\mathfrak{p}_3$ and $\mathfrak{p}_3'$.

(d) Show that the different of $\mathcal{O}_K/\mathbb{Z}$ is $\mathfrak{p}_3\mathfrak{p}_7^2\mathfrak{p}_{11}^2$.

*(e) Using the norm, show that $\operatorname{diff}_{\mathcal{O}_K/\mathbb{Z}}$ is not principal and conclude that $\mathcal{O}_K$ is not generated by one element over $\mathbb{Z}$.

Solution:

(a) The minimal polynomial of α is $X^3 - 7^2 \cdot 11$, which is Eisenstein at 11 and therefore irreducible. Thus $[K/\mathbb{Q}] = 3$. On the other hand K is also generated by $\beta := \frac{77}{\alpha}$ which has minimal polynomial $X^3 - 7 \cdot 11^2$ that is Eisenstein at 7. By Exercise 5 of Sheet 8, the primes (7) and (11) are therefore totally ramified in $\mathcal{O}_K$ with decompositions $7\mathcal{O}_K = \mathfrak{p}_7^3$ for $\mathfrak{p}_7 := (7, \beta)$ and $11\mathcal{O}_K = \mathfrak{p}_{11}^3$ for $\mathfrak{p}_{11} := (11, \alpha)$.

(b) Since $\beta = \frac{\alpha^2}{7}$, the elements α, β, γ form a basis of K over $\mathbb{Q}$. We compute the multiplication table for pairs of basis elements:

	α	β	γ
α	7β	$77 = -154\alpha - 77\beta + 231\gamma$	$-51\alpha - 21\beta + 77\gamma$
β	77	11α	$-99\alpha - 51\beta + 154\gamma$
γ	$-51\alpha - 21\beta + 77\gamma$	$-99\alpha - 51\beta + 154\gamma$	$-67\alpha - 31\beta + 103\gamma$

This table shows that $A := \alpha\mathbb{Z} \oplus \beta\mathbb{Z} \oplus \gamma\mathbb{Z}$ is a subring. Since A is finitely generated as a $\mathbb{Z}$-module, it is integral over $\mathbb{Z}$ and hence contained in $\mathcal{O}_K$. Next, we see from the minimal polynomials of α and β that $\mathrm{Tr}_{K/\mathbb{Q}}(\alpha) = \mathrm{Tr}_{K/\mathbb{Q}}(\beta) = 0$. By $\mathbb{Q}$-linearity this implies that $\mathrm{Tr}_{K/\mathbb{Q}}(\gamma) = \frac{1}{3}\mathrm{Tr}_{K/\mathbb{Q}}(1) = 1$. Using the multiplication table we can now calculate the discriminant of A:

$$\begin{aligned}
\mathrm{disc}(A) &= \det\begin{pmatrix} \mathrm{Tr}(\alpha^2) & \mathrm{Tr}(\alpha\beta) & \mathrm{Tr}(\alpha\gamma) \\ \mathrm{Tr}(\beta\alpha) & \mathrm{Tr}(\beta^2) & \mathrm{Tr}(\beta\gamma) \\ \mathrm{Tr}(\gamma\alpha) & \mathrm{Tr}(\gamma\beta) & \mathrm{Tr}(\gamma^2) \end{pmatrix} \\
&= \det\begin{pmatrix} 0 & 231 & 77 \\ 231 & 0 & 154 \\ 77 & 154 & 103 \end{pmatrix} = -17787 = -3\cdot 7^2\cdot 11^2.
\end{aligned}$$

From the lecture course, we know that $\mathrm{disc}(A) = [\mathcal{O}_K : A]^2\,\mathrm{disc}(\mathcal{O}_K)$. Furthermore, both 7 and 11 are ramified in $\mathcal{O}_K$ by (a) and therefore divide $\mathrm{disc}(\mathcal{O}_K)$ by Theorem 6.8.4 (a). Thus $[\mathcal{O}_K : \mathfrak{a}]^2$ must divide $3\cdot 7\cdot 11$, which is only possible for $[\mathcal{O}_K : \mathfrak{a}] = 1$. Therefore $A = \mathcal{O}_K$ with the stated discriminant, as desired.

(c) The multiplication table in (b) shows that $\alpha \equiv \gamma^2 - \gamma - 1 \mod 3\mathcal{O}_K$ and $\beta \equiv \gamma^2 - \gamma + 1 \mod 3\mathcal{O}_K$. Thus $\mathcal{O}_K/3\mathcal{O}_K$ is generated as an $\mathbb{F}_3$-algebra by the residue class of γ. Another direct calculation using the multiplication table shows that $\gamma^3 - \gamma^2 \equiv 0 \mod 3\mathcal{O}_K$. Therefore $\mathcal{O}_K/3\mathcal{O}_K \cong \mathbb{F}_3[X]/(X^3 - X^2) = \mathbb{F}_3[X]/(X^2(X-1))$, where the residue class of γ corresponds to the residue class of X. Thus the maximal ideals (X) and $(X-1)$ of the right hand side correspond to the maximal ideals $\mathfrak{p}_3 := (3,\gamma)$ and $\mathfrak{p}_3' := (3,\gamma-1)$ of $\mathcal{O}_K$, both with residue fields isomorphic to $\mathbb{F}_3$. Since $\mathfrak{p}_3^2\mathfrak{p}_3'/3\mathcal{O}_K$ maps to the ideal $(X)^2(X-1) = (X^3 - X^2) = (0) \subset \mathbb{F}_3[X]/(X^3 - X^2)$ via the isomorphism given above, we have $\mathfrak{p}_3^2\mathfrak{p}_3' \subset 3\mathcal{O}_K$. As both sides have the same norm, we deduce the desired equality.

(d) By Theorem 6.7.6 a prime $\mathfrak{p}$ of $\mathcal{O}_K$ divides the different $\mathrm{diff}_{\mathcal{O}_K/\mathbb{Z}}$ if and only if $\mathfrak{p}$ is ramified over $\mathbb{Z}$. By the multiplicativity of the norm $\mathrm{Norm}(\mathfrak{p})$ then divides $\mathrm{Norm}(\mathrm{diff}_{\mathcal{O}_K/\mathbb{Z}})$, which is equal to $|\,\mathrm{disc}(\mathcal{O}_K)| = 3\cdot 7^2\cdot 11^2$ by Proposition 6.8.2 and part (b). In view of parts (a) and (c) this leaves only the possibilities $\mathfrak{p} = \mathfrak{p}_3$, $\mathfrak{p}_7$, $\mathfrak{p}_{11}$. But the norm of any prime ideal is the order of its residue field, and the residue field is a prime field in each of these cases. Thus the prime factorization of $|\,\mathrm{disc}(\mathcal{O}_K)|$ implies that $\mathrm{diff}_{\mathcal{O}_K/\mathbb{Z}} = \mathfrak{p}_3\mathfrak{p}_7^2\mathfrak{p}_{11}^2$.

*(e) By (a) we have $(\alpha)^3 = (\alpha^3) = (7^2\cdot 11) = \mathfrak{p}_7^6\mathfrak{p}_{11}^3$. By unique prime factorization of ideals this implies that $(\alpha) = \mathfrak{p}_7^2\mathfrak{p}_{11}$. Using (d) it follows that $\mathrm{diff}_{\mathcal{O}_K/\mathbb{Z}} = \mathfrak{p}_3\mathfrak{p}_7^2\mathfrak{p}_{11}^2 = \alpha\mathfrak{p}_3\mathfrak{p}_{11}$, so $\mathrm{diff}_{\mathcal{O}_K/\mathbb{Z}}$ is principal if and only if $\mathfrak{p}_3\mathfrak{p}_{11}$ is principal.

Suppose that $\mathfrak{p}_3\mathfrak{p}_{11} = (\xi)$ for some element $\xi \in \mathcal{O}_K$. Then $|\,\mathrm{Norm}_{K/\mathbb{Q}}(\xi)| = \mathrm{Norm}(\mathfrak{p}_3\mathfrak{p}_{11}) = 3\cdot 11$, and so $\mathrm{Norm}_{K/\mathbb{Q}}(\xi) = \pm 33$. We will show that this is impossible. Write $\xi = a\alpha + b\beta + c\gamma$ with $a,b,c \in \mathbb{Z}$. The Galois conjugates of

α, β, and γ are given in the following table, where ζ_3 is a primitive 3rd root of unity:

$\varphi \in \mathrm{Hom}_{\mathbb{Q}}(K, \bar{\mathbb{Q}})$	$\varphi(\alpha)$	$\varphi(\beta)$	$\varphi(\gamma)$
$\mathrm{id} : \alpha \mapsto \alpha$	α	β	γ
$\varphi_1 : \alpha \mapsto \zeta_3\alpha$	$\zeta_3\alpha$	$\zeta_3^2\beta$	$\frac{1+2\zeta_3\alpha+\zeta_3^2\beta}{3}$
$\varphi_2 : \alpha \mapsto \zeta_3^2\alpha$	$\zeta_3^2\alpha$	$\zeta_3\beta$	$\frac{1+2\zeta_3^2\alpha+\zeta_3\beta}{3}$

We calculate

$$\begin{aligned}\mathrm{Norm}_{K/\mathbb{Q}}(\xi) &= \xi \cdot \varphi_1(\xi) \cdot \varphi_2(\xi)\\ &= 7^2 \cdot 11a^3 + 7 \cdot 11^2b^3 + 2 \cdot 7^2 \cdot 11a^2c - 7 \cdot 11abc + 7 \cdot 11^2b^2c\\ &\quad + 3^2 \cdot 7 \cdot 11ac^2 + 3 \cdot 7 \cdot 11bc^2 + 2 \cdot 3 \cdot 29c^3.\end{aligned}$$

This is congruent to $-c^3 \mod (7)$. Since the only cubes in $\mathbb{F}_7$ are 0 and ±1, it follows that $\mathrm{Norm}_{K/\mathbb{Q}}(\xi)$ is congruent to 0 or ±1 modulo (7). As each of these residue classes is distinct from $\pm33 \equiv \pm5 \mod (7)$, we have obtained the desired contradiction. Therefore no element $\xi \in \mathcal{O}_K$ of norm ±33 exists and $\mathrm{diff}_{\mathcal{O}_K/\mathbb{Z}}$ is not principal in $\mathcal{O}_K$.

Finally, if $\mathcal{O}_K = \mathbb{Z}[\omega]$ and $f(X)$ is the minimal polynomial of ω over $\mathbb{Q}$, by Proposition 6.7.3 $\mathrm{diff}_{\mathcal{O}_K/\mathbb{Z}} = (\frac{df}{dX}(\omega))$. Since $\mathrm{diff}_{\mathcal{O}_K/\mathbb{Z}}$ is not a principal ideal, it follows that $\mathcal{O}_K$ is not generated by a single element over $\mathbb{Z}$.