Solutions 7

Different and Discriminant, Cyclotomic Fields

1. (a) Prove that any Dedekind ring with only finitely many maximal ideals is a principal ideal domain.

   (b) Let A be a discrete valuation ring and B its integral closure in a finite separable field extension of $\mathrm{Quot}(A)$. Deduce from (a) that B is a principal ideal domain.

   Solution: Part (a) is Theorem 60 in section 1-6 of the book [I. Kaplansky: *Commutative Rings.* Revised Edition. The University of Chicago Press, Chicago, Ill.-London. 1974], as every non-zero fractional ideal of a Dedekind ring is invertible.

   For (b) observe that A is a Dedekind ring with precisely one maximal ideal, say $\mathfrak{m}$. By §6 we know that B is a Dedekind ring with only finitely many prime ideals above $\mathfrak{m}$. Any other prime ideal of B must lie above the zero prime ideal of A and hence be zero itself, because the zero ideal of B is already prime and B has Krull dimension 1. Thus B is a Dedekind ring with only finitely many maximal ideals. By (a) it is therefore a principal ideal domain.

2. Let $K := \mathbb{Q}(\alpha)$, where $\alpha := \sqrt[3]{539}$.

   (a) Using exercise 3 of sheet 6, 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 $\mathrm{disc}(\mathcal{O}_K) = -3 \cdot 7^2 \cdot 11^2$.

   (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 $\mathrm{diff}_{\mathcal{O}_K/\mathbb{Z}}$ 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 3 of sheet 6, 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, by §7 Proposition 13, both 7 and 11 divide $\mathrm{disc}(\mathcal{O}_K)$ because they are ramified in $\mathcal{O}_K$ by part (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 $\alpha \equiv \gamma^2 - \gamma - 1 \bmod 3\mathcal{O}_K$ and $\beta \equiv \gamma^2 - \gamma + 1 \bmod 3\mathcal{O}_K$. 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 $\gamma^3 - \gamma^2 \equiv 0 \bmod 3\mathcal{O}_K$. 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 §7 Proposition 11, 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 $\mathrm{Nm}(\mathfrak{p})$ then divides $\mathrm{Nm}(\mathrm{diff}_{\mathcal{O}_K/\mathbb{Z}})$, which is equal to $|\,\mathrm{disc}(\mathcal{O}_K)| = 3 \cdot 7^2 \cdot 11^2$ by §7 Theorem 9 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 $|\operatorname{Nm}_{K/\mathbb{Q}}(\xi)| = \operatorname{Nm}(\mathfrak{p}_3 \mathfrak{p}_{11}) = 3 \cdot 11$, and so $\operatorname{Nm}_{K/\mathbb{Q}}(\xi) = \pm 33$. 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

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

This is congruent to $-c^3 \bmod (7)$. Since the only cubes in $\mathbb{F}_7$ are 0 and ± 1, it follows that $\operatorname{Nm}_{K/\mathbb{Q}}(\xi)$ is congruent to 0 or ± 1 modulo (7). As each of these residue classes is distinct from $\pm 33 \equiv \pm 5 \bmod (7)$, 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 §7 Proposition 3 we have $\mathrm{diff}_{\mathcal{O}_K/\mathbb{Z}} = (\frac{df}{dX}(\omega))$. 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 $\mathbb{Z}$.

3. Let K be a number field, let m be a positive integer, let $G_m(K) := \{x^m \mid x \in K^\times\}$ and let $L_m(K)$ be the group of elements $x \in K^\times$ such that in the prime factorization of (x), all exponents are multiples of m.

   (a) Prove that for every $x \in L_m(K)$, there exists a unique fractional ideal $\mathfrak{a}_x$ such that $(x) = \mathfrak{a}_x^m$.

   (b) Define $S_m(K) := L_m(K)/G_m(K)$ and $\mathrm{Cl}(\mathcal{O}_K)[m] := \{c \in \mathrm{Cl}(\mathcal{O}_K) \mid c^m = 1\}$ and show that the map

   $$\begin{aligned} f : S_m(K) &\to \mathrm{Cl}(\mathcal{O}_K)[m] \\ x &\mapsto [\mathfrak{a}_x] \end{aligned}$$

   is a well-defined group homomorphism.

   (c) Show that f is surjective.

   (d) Find the kernel of f.

   Solution:

   (a) Let $x \in L_m(K)$ and let $(x) = \prod_i \mathfrak{p}_i^{ma_i}$ be the prime factorization of the principal ideal generated by it. Then $\mathfrak{a}_x := \prod_i \mathfrak{p}_i^{a_i}$ satisfies the required property. The uniqueness of $\mathfrak{a}_x$ follows from the uniqueness of the prime factorization.

   (b) Consider the map $\tilde{f} : L_m(K) \to \mathrm{Cl}(\mathcal{O}_K)$, $x \mapsto [\mathfrak{a}_x]$. For any $x, y \in L_m(K)$ we have $(\mathfrak{a}_x\mathfrak{a}_y)^m = \mathfrak{a}_x^m\mathfrak{a}_y^m = (x)(y) = (xy)$ and so $\mathfrak{a}_{xy} = \mathfrak{a}_x\mathfrak{a}_y$, by uniqueness. It follows that $\tilde{f}$ is a homomorphism. Note that $\tilde{f}(x)^m = [\mathfrak{a}_x]^m = [\mathfrak{a}_x^m] = [(x)] = 1$ and hence $\operatorname{Im} \tilde{f} \subset \mathrm{Cl}(\mathcal{O}_K)[m]$. Suppose that $x \in G_m(K)$ and choose $z \in K^\times$ such that $z^m = x$. Then $\mathfrak{a}_x = (z)$ and hence $\tilde{f}(x) = 1$. Therefore $G_m(K) \subset \operatorname{Ker} \tilde{f}$ and $\tilde{f}$ factors through S_m, inducing the map f.

   (c) Let $[\mathfrak{a}] \in \mathrm{Cl}(\mathcal{O}_K)[m]$. Then $\mathfrak{a}^m$ is principal, say $\mathfrak{a}^m = (x)$. But then $x \in L_m(K)$ and $\mathfrak{a} = \mathfrak{a}_x$ by uniqueness. Then $f(x) = [\mathfrak{a}]$ and f is surjective, as desired.

   (d) Take any $x \in L_m(K)$. Then $f(x) = 1$ if and only if $\mathfrak{a}_x = (y)$ for some $y \in K^\times$. By unique factorization of ideals this is equivalent to $\mathfrak{a}_x^m = (y)^m$, and hence to $(x) = (y^m)$, or again to $x = uy^m$ for some unit $u \in \mathcal{O}_K^\times$. Thus $f(x) = 1$ if and only if $x \in \mathcal{O}_K^\times G_m(K)$. Therefore $\operatorname{Ker} f = \mathcal{O}_K^\times G_m(K)/G_m(K)$. Since $\mathcal{O}_K^\times \cap G_m(K) = (\mathcal{O}_K^\times)^m$, the second isomorphism theorem for groups yields a natural isomorphism $\operatorname{Ker} f \cong \mathcal{O}_K^\times/(\mathcal{O}_K^\times)^m$.

*4. (*Hilbert's Theorem 90*) Let L/K be a finite Galois extension of fields whose Galois group is cyclic and generated by σ. Show that for any element $x \in L^\times$ with $\mathrm{Nm}_{L/K}(x) = 1$ there exists an element $y \in L^\times$ with $x = \sigma(y)/y$.

Hint: Set $n := [L/K]$ and consider the map

$$h\colon L \longrightarrow L, \quad z \mapsto h(z) := \sum_{i=0}^{n-1} \sigma^i(z) \cdot \prod_{i<j<n} \sigma^j(x).$$

Solution: By Galois theory σ has finite order n and the elements $\mathrm{id}, \sigma, \ldots, \sigma^{n-1} \in \mathrm{Hom}_K(L,L)$ are L-linearly independent. Since all $\sigma^j(x)$ are non-zero, the map $h \in \mathrm{Hom}_K(L,L)$ is therefore also non-zero. Thus there exists $z \in L$ with $y := h(z) \neq 0$. Using the facts that $\sigma^n = \mathrm{id}$ and $\prod_{0<j\leqslant n} \sigma^j(x) = \mathrm{Nm}_{L/K}(x) = 1$, we compute

$$\begin{aligned}
x \cdot h(z) &= \sigma^n(x) \cdot \sum_{i=0}^{n-1} \sigma^i(z) \cdot \prod_{i<j<n} \sigma^j(x) \\
&= \sum_{i=0}^{n-1} \sigma^i(z) \cdot \prod_{i<j\leqslant n} \sigma^j(x) \\
&= z \cdot \prod_{0<j\leqslant n} \sigma^j(x) + \sum_{i=1}^{n-1} \sigma^i(z) \cdot \prod_{i<j\leqslant n} \sigma^j(x) \\
&= \sigma^n(z) \cdot 1 + \sum_{i=1}^{n-1} \sigma^i(z) \cdot \prod_{i<j\leqslant n} \sigma^j(x) \\
&= \sum_{i=1}^{n} \sigma^i(z) \cdot \prod_{i<j\leqslant n} \sigma^j(x) \\
&= \sigma(h(z)).
\end{aligned}$$

We therefore have $xy = \sigma(y)$ and hence $x = \sigma(y)/y$, as desired.

*5. Set $d := p_1 \cdots p_r$ for prime numbers $2 = p_1 < p_2 < \ldots < p_r$ and consider the imaginary quadratic number field $K := \mathbb{Q}(\sqrt{-d})$. For each i write $p_i\mathcal{O}_K = \mathfrak{p}_i^2$. Show that the subgroup $H := \{\xi \in \mathrm{Cl}(\mathcal{O}_K) \mid \xi^2 = 1\}$ has order 2^{r-1} and is generated by the ideal classes $[\mathfrak{p}_i]$ with the single relation $[\mathfrak{p}_1] \cdots [\mathfrak{p}_r] = 1$.

Solution: Since $d \equiv 2 \bmod (4)$, we have $\mathcal{O}_K = \mathbb{Z}[\sqrt{-d}]$ with discriminant $-4d$. So the prime divisors of the discriminant are $p_1, \ldots, p_r$, and these are precisely the rational primes that ramify in $\mathcal{O}_K$. In particular, for each i we have $p_i\mathcal{O}_K = \mathfrak{p}_i^2$ with a prime ideal $\mathfrak{p}_i$. For later use observe that, since K is imaginary quadratic, for any element $x \in L$ we have $\mathrm{Nm}_{K/\mathbb{Q}}(x) = x\bar{x} \geqslant 0$.

Since $\mathfrak{p}_i^2 = (p_i)$, the ideal class $[\mathfrak{p}_i]$ lies in the subgroup H. Next, the computation $(\sqrt{-d})^2 = (d) = (p_1 \cdots p_r) = \mathfrak{p}_1^2 \cdots \mathfrak{p}_r^2$ implies that $(\sqrt{-d}) = \mathfrak{p}_1 \cdots \mathfrak{p}_r$ and hence $[\mathfrak{p}_1] \cdots [\mathfrak{p}_r] = [(\sqrt{-d})] = 1$ in H. Conversely consider any subset $I \subset \{1, \ldots, r\}$ such that $\prod_{i\in I} [\mathfrak{p}_i] = 1$ in H. Then $\prod_{i\in I} \mathfrak{p}_i = (a + b\sqrt{-d})$ for some non-zero element $a+b\sqrt{-d}\in\mathcal{O}_K$ with $a,b\in\mathbb{Z}$. Computing

$$a^2+b^2d=\big|\mathrm{Nm}_{K/\mathbb{Q}}(a+b\sqrt{-d})\big|=\mathrm{Nm}_{\mathcal{O}_K/\mathbb{Z}}\Big(\prod_{i\in I}\mathfrak{p}_i\Big)=\prod_{i\in I}\mathrm{Nm}_{\mathcal{O}_K/\mathbb{Z}}(\mathfrak{p}_i)=\prod_{i\in I}p_i$$

we deduce that a^2+b^2d divides $\prod_{i=1}^r p_i=d$. In particular $b^2d\leqslant a^2+b^2d\leqslant d$ and hence $|b|\leqslant 1$. If $b=0$, we have $a^2|d$ with d squarefree and therefore $\prod_{i\in I}p_i=a^2=1$ and hence $I=\varnothing$. If $b=\pm1$ we must have $a=0$ and $\prod_{i\in I}p_i=d$ and hence $I=\{1,\ldots,r\}$. Together this implies that the classes $[\mathfrak{p}_i]$ generate a subgroup of H of order 2^{r-1}.

It remains to show that H is generated by the $[\mathfrak{p}_i]$. For this consider an arbitrary ideal class $[\mathfrak{a}]\in H$. Write $\mathfrak{a}^2=(x)$ and $\mathrm{Nm}_{\mathcal{O}_K/\mathbb{Z}}(\mathfrak{a})=(a)$ with $a>0$. Then

$$\mathrm{Nm}_{K/\mathbb{Q}}(x)=\mathrm{Nm}_{\mathcal{O}_K/\mathbb{Z}}((x))=\mathrm{Nm}_{\mathcal{O}_K/\mathbb{Z}}(\mathfrak{a}^2)=\mathrm{Nm}_{\mathcal{O}_K/\mathbb{Z}}(\mathfrak{a})^2=a^2=\mathrm{Nm}_{K/\mathbb{Q}}(a)$$

and hence $\mathrm{Nm}_{K/\mathbb{Q}}(x/a)=1$. By Hilbert Theorem 90 (see the preceding exercise) it follows that $x/a=\bar{y}/y$ for some $y\in K^\times$. The ideal $\mathfrak{b}:=y\mathfrak{a}$ then satisfies

$$\mathfrak{b}^2=y^2\mathfrak{a}^2=(y^2x)=(y\bar{y}a)=(b)$$

with $b:=y\bar{y}a\in\mathbb{Q}^\times$. Thus $\mathfrak{b}^2=(b)=(\,\bar{b}\,)=\overline{(b)}=\overline{\mathfrak{b}^2}=\bar{\mathfrak{b}}^2$ and hence $\mathfrak{b}=\bar{\mathfrak{b}}$.

Now we look at the prime factorization of $\mathfrak{b}$. There are three kinds of non-zero prime ideals of $\mathcal{O}_K$: the ramified primes $\mathfrak{p}_1,\ldots,\mathfrak{p}_r$, the inert primes of the form (p), and the pairs of distinct split primes $\mathfrak{p},\bar{\mathfrak{p}}$ with $\mathfrak{p}\bar{\mathfrak{p}}=(p)$. For any of the third kind the fact that $\mathfrak{b}=\bar{\mathfrak{b}}$ implies that $\mathfrak{p}$ and $\bar{\mathfrak{p}}$ have the same exponent in the prime factorization of $\mathfrak{b}$. Combining these factors thus yields simply a power of p. Together it follows that $\mathfrak{b}$ is a product of some powers of $\mathfrak{p}_1,\ldots,\mathfrak{p}_r$ and some powers of rational primes p. The latter factors form a principal ideal, so the ideal class $[\mathfrak{a}]=[y\mathfrak{a}]=[\mathfrak{b}]$ is a product of powers of the classes $[\mathfrak{p}_1],\ldots,[\mathfrak{p}_r]$, as desired.

Remark: In the lecture we showed that K possesses an everywhere unramified finite extension of the form $L=\mathbb{Q}(\sqrt{p_1^*},\ldots,\sqrt{p_r^*})$ for suitable $p_i^*=\pm p_i$, which is Galois with a Galois group isomorphic to H. Combined with the result of the present exercise this illustrates a part of the theory of the Hilbert class field.

6. Show that for any root of unity $\zeta\in\mathbb{C}$ whose order is not a prime power, the element $1-\zeta$ is a unit in $\mathcal{O}_{\mathbb{Q}(\zeta)}$.

Solution: By assumption the order n of ζ is divisible by distinct primes p_1, p_2. Set $K:=\mathbb{Q}(\zeta)$, and for each $i=1,2$ set $\zeta_i:=\zeta^{n/p_i}$ and $K_i:=\mathbb{Q}(\zeta_i)$. Then ζ_i is a root of unity of order p_i, and so $p_i\in(1-\zeta_i)\mathcal{O}_{K_i}$ by §8 Theorem 3(b). Since $\frac{1-\zeta_i}{1-\zeta}=\sum_{j=0}^{n/p_i-1}\zeta^j\in\mathcal{O}_K$, it follows that $p_i\in(1-\zeta)\mathcal{O}_K$. Since $(p_1,p_2)=(1)$ in $\mathbb{Z}$, we deduce that $1\in(1-\zeta)\mathcal{O}_K$ and hence $(1-\zeta)\mathcal{O}_K=\mathcal{O}_K$. Thus $1-\zeta$ is a unit in $\mathcal{O}_K$, as desired.