Solutions Additional Problems

1. 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 Theorem 3.6.7 (c). 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.

2. Let K be a number field and let S be a finite set of maximal ideals of $\mathcal{O}_K$. For any $\mathfrak{p} \in S$ and $x \in K^\times$ let $\mathrm{ord}_\mathfrak{p}(x)$ denote the exponent of $\mathfrak{p}$ in the prime factorization of the fractional ideal (x). We define the ring of *S-integers in K* to be

$$\mathcal{O}_{K,S} \;:=\; \bigcap_{\mathfrak{p}\notin S} \mathcal{O}_{K,\mathfrak{p}} \;=\; \big\{x \in K \;\big|\; \forall \mathfrak{p} \notin S : \mathrm{ord}_\mathfrak{p}(x) \geqslant 0\big\}.$$

   The group $\mathcal{O}_{K,S}^\times$ is called the group of *S-units in K*.

   (a) Show that the torsion subgroup of $\mathcal{O}_{K,S}^\times$ is $\mu(K)$.

   (b) Let $\mathfrak{p}_1, \ldots, \mathfrak{p}_t$ be the distinct elements of S. Show that the homomorphism

$$\varphi\colon \mathcal{O}_{K,S}^\times \to \mathbb{Z}^t,\; x \mapsto (\mathrm{ord}_{\mathfrak{p}_i}(x))_i$$

   has kernel $\mathcal{O}_K^\times$ and that its image is a free abelian group of rank t.

   (c) Deduce that $\mathcal{O}_{K,S}^\times \cong \mu(K) \times \mathbb{Z}^{r+s+|S|-1}$.

   Solution:

   (a) Since the torsion subgroup of $K^\times$ is $\mu(K)$, the torsion subgroup of $\mathcal{O}_{K,S}^\times$ must be a subgroup of $\mu(K)$. But $\mu(K) \subseteq \mathcal{O}_K^\times \subseteq \mathcal{O}_{K,S}^\times$ and the conclusion follows.

   (b) Clearly $\mathcal{O}_K^\times \subset \ker(\varphi)$. Conversely consider any $x \in \ker(\varphi)$. Then $\mathrm{ord}_\mathfrak{p}(x) \geqslant 0$ for all $\mathfrak{p} \notin S$ by the definition of $\mathcal{O}_{K,S}$ and for all $\mathfrak{p} \in S$ because $\varphi(x) = 0$. Thus the prime factorization of (x) possesses only nonnegative exponents; hence $(x) \subset \mathcal{O}_K$ and so $x \in \mathcal{O}_K$. The same argument for x^{-1} in place of x shows that $x^{-1} \in \mathcal{O}_K$ as well. Together this shows that $x \in \mathcal{O}_K^\times$, proving the first assertion in (b).

For the second let h be the class number of $\mathcal{O}_K$. Then for each i the ideal $\mathfrak{p}_i^h$ is principal, say generated by x_i. By construction we then have $\varphi(x_i) = (0, \ldots, 0, h, 0, \ldots, 0)$ with entry h at i. Varying i this shows that $h\mathbb{Z}^t \subset \mathrm{im}(\varphi)$. Since $\mathrm{im}(\varphi) \subset \mathbb{Z}^t$ it follows that $\mathrm{im}(\varphi)$ is a free abelian group of rank $t = |S|$.

(c) By (b), we obtain a short exact sequence

$$1 \to \mathcal{O}_K^\times \to \mathcal{O}_{K,S}^\times \to \mathrm{im}(\varphi) \cong \mathbb{Z}^t \to 0.$$

Since $\mathrm{im}(\varphi)$ is free of rank t the sequence splits. With Dirichlet's unit theorem $\mathcal{O}_K^\times \cong \mu(K) \times \mathbb{Z}^{r+s-1}$ it follows that $\mathcal{O}_{K,S}^\times \cong \mathcal{O}_K^\times \times \mathbb{Z}^t \cong \mu(K) \times \mathbb{Z}^{r+s+t-1}$.

3. Consider a Dedekind ring A with quotient field K, a finite Galois extension L/K, and let B denote the integral closure of A in L. Consider a subextension K'/K which is also Galois and let A' denote the integral closure of A in K'. Consider a prime $\mathfrak{p}$ of A and a prime $\mathfrak{q} \subset B$ above $\mathfrak{p}$, such that $k(\mathfrak{q})/k(\mathfrak{p})$ is separable. Determine the decomposition of $\mathfrak{p}$ in A' with its numerical invariants r, e, f and its decomposition and inertia groups from the corresponding data in B.

Solution: Set $\Gamma := \mathrm{Gal}(L/K)$ and $\Gamma' := \mathrm{Gal}(L/K')$ and $\Gamma'' := \mathrm{Gal}(K'/K) \cong \Gamma/G'$. Let $I_\mathfrak{q} \triangleleft \Gamma_\mathfrak{q} < \Gamma$ be the inertia group and the decomposition group for $\mathfrak{q}/\mathfrak{p}$. We will show how these groups determine all the desired data.

Set $\mathfrak{p}' := \mathfrak{q} \cap A'$, which is a prime of A' above $\mathfrak{p}$. Plugging in the definitions, we see that the inertia and decomposition groups for $\mathfrak{q}/\mathfrak{p}'$ are $I'_\mathfrak{q} := \Gamma' \cap I_\mathfrak{q} \triangleleft \Gamma'_\mathfrak{q} := \Gamma' \cap \Gamma_\mathfrak{q} < \Gamma'$. Let $I''_{\mathfrak{p}'} \triangleleft \Gamma''_{\mathfrak{p}'} < \Gamma''$ denote the inertia and decomposition groups for $\mathfrak{p}'/\mathfrak{p}$. Since $k(\mathfrak{q})/k(\mathfrak{p}')/k(\mathfrak{p})$ are separable field extensions, we have

$e := e_{\mathfrak{q}/\mathfrak{p}} = \lvert I_\mathfrak{q}\rvert$	$f := f_{\mathfrak{q}/\mathfrak{p}} = [\Gamma_\mathfrak{q} : I_\mathfrak{q}]$	$r := r_{B/\mathfrak{p}} = [\Gamma : \Gamma_\mathfrak{q}]$
$e' := e_{\mathfrak{q}/\mathfrak{p}'} = \lvert I'_\mathfrak{q}\rvert$	$f' := f_{\mathfrak{q}/\mathfrak{p}'} = [\Gamma'_\mathfrak{q} : I'_\mathfrak{q}]$	$r' := r_{B/\mathfrak{p}'} = [\Gamma' : \Gamma'_\mathfrak{q}]$
$e'' := e_{\mathfrak{p}'/\mathfrak{p}} = \lvert I''_{\mathfrak{p}'}\rvert$	$f'' := f_{\mathfrak{p}'/\mathfrak{p}} = [\Gamma''_{\mathfrak{p}'} : I''_{\mathfrak{p}'}]$	$r'' := r_{A'/\mathfrak{p}} = [\Gamma'' : \Gamma''_{\mathfrak{p}'}]$

where $r_{../..}$ denotes the number of primes of .. above ... Since $I'_\mathfrak{q}$ and $\Gamma'_\mathfrak{q}$ are already given by explicit formulas, a complete answer follows from the descriptions:

(a) $\Gamma''_{\mathfrak{p}'} = \Gamma_\mathfrak{q}\Gamma'/\Gamma' \cong \Gamma_\mathfrak{q}/\Gamma'_\mathfrak{q}$.

(b) $I''_{\mathfrak{p}'} = I_\mathfrak{q}\Gamma'/\Gamma' \cong I_\mathfrak{q}/I'_\mathfrak{q}$.

In both statements the last isomorphism results from the first isomorphism theorem. To prove (a) note that $\Gamma_\mathfrak{q}$ stabilizes $\mathfrak{q}$ and A' and hence also $\mathfrak{p}' := \mathfrak{q} \cap A'$. Thus its image $\Gamma_\mathfrak{q}\Gamma'/\Gamma'$ in $\Gamma/\Gamma' \cong \mathrm{Gal}(K'/K)$ is contained in $\Gamma''_{\mathfrak{p}'}$. It follows that

$$e''f'' \;=\; |\Gamma''_{\mathfrak{p}'}| \;\geqslant\; |\Gamma_\mathfrak{q}\Gamma'/\Gamma'| \;=\; |\Gamma_\mathfrak{q}/\Gamma'_\mathfrak{q}| \;=\; \frac{|\Gamma_\mathfrak{q}|}{|\Gamma'_\mathfrak{q}|} \;=\; \frac{ef}{e'f'}.$$

Since $e = e'e''$ and $f = f'f''$, this inequality must be an equality; hence so is the inclusion $\Gamma_{\mathfrak{q}}\Gamma'/\Gamma' \subset \Gamma''_{\mathfrak{p}'}$, proving (a).

Likewise, for (b) observe that $I_{\mathfrak{q}}$ acts trivially on the residue field $k(\mathfrak{q})$ and hence also on the subfield $k(\mathfrak{p}')$. Thus its image $I_{\mathfrak{q}}\Gamma'/\Gamma'$ in $\Gamma/\Gamma' \cong \mathrm{Gal}(K'/K)$ is contained in $I''_{\mathfrak{p}'}$. It follows that

$$e'' \;=\; |I''_{\mathfrak{p}'}| \;\geqslant\; |I_{\mathfrak{q}}\Gamma'/\Gamma'| \;=\; |I_{\mathfrak{q}}/I'_{\mathfrak{q}}| \;=\; \frac{|I_{\mathfrak{q}}|}{|I'_{\mathfrak{q}}|} \;=\; \frac{e}{e'}.$$

Since again $e = e'e''$, the inclusion $I_{\mathfrak{q}}\Gamma'/\Gamma' \subset I''_{\mathfrak{p}'}$ must be an equality, proving (b).

4. Let L/K be a Galois extension of number fields with noncyclic Galois group.

   (a) Show that any prime ideal of $\mathcal{O}_K$ over which lies only one prime ideal of $\mathcal{O}_L$ is ramified in $\mathcal{O}_L$.

   (b) Deduce that there are at most finitely many prime ideals with the property in (a), and in particular no prime ideals of $\mathcal{O}_K$ that are totally inert in $\mathcal{O}_L$.

   Solution:

   (a) Let $\mathfrak{p}$ be a prime ideal of $\mathcal{O}_K$ over which lies only one prime ideal $\mathfrak{q}$ of $\mathcal{O}_L$. Then the decomposition group at $\mathfrak{q}$ is equal to $\mathrm{Gal}(L/K)$, so we have a short exact sequence

   $$1 \to I_{\mathfrak{q}} \to \mathrm{Gal}(L/K) \to \mathrm{Gal}(k(\mathfrak{q})/k(\mathfrak{p})) \to 1.$$

   Since $k(\mathfrak{p})$ is a finite field, the group $\mathrm{Gal}(k(\mathfrak{q})/k(\mathfrak{p}))$ is cyclic; hence it is not isomorphic to $\mathrm{Gal}(L/K)$. Thus the inertia group $I_{\mathfrak{q}}$ is not trivial. By Proposition 6.4.3, it follows that $e = |I_{\mathfrak{q}}| > 1$, as desired.

   (b) By (a), every such prime is ramified. Hence, there are no totally inert primes. Since, by Theorem 6.8.4, there are only finitely many ramified primes, there are only finitely many primes with the property from (a).

5. Let K be a quadratic number field and γ the non-trivial Galois automorphism of $K/\mathbb{Q}$. Show that for every fractional ideal $\mathfrak{a}$ of $\mathcal{O}_K$ the ideal $\mathfrak{a} \cdot \gamma(\mathfrak{a})$ is principal.

   Hint: Prove this first in the case of prime ideals.

   Solution: Let $\mathfrak{p}$ be a maximal ideal of $\mathcal{O}_K$ and p the rational prime under $\mathfrak{p}$. Then $p\mathcal{O}_K = \mathfrak{p}$ or $\mathfrak{p}^2$ or $\mathfrak{p}\mathfrak{p}'$ for a prime ideal $\mathfrak{p}' \neq \mathfrak{p}$. Since $\gamma(\mathfrak{p})$ is also a prime ideal over p, it is equal to $\mathfrak{p}$ in the first two cases. In the first case we thus have $\mathfrak{p} \cdot \gamma(\mathfrak{p}) = p^2\mathcal{O}_K$, and in the second case we have $\mathfrak{p} \cdot \gamma(\mathfrak{p}) = p\mathcal{O}_K$. In the last case the fact that the Galois group transitively permutes the primes over p implies that $\gamma(\mathfrak{p}) = \mathfrak{p}'$. In that case we therefore have $\mathfrak{p} \cdot \gamma(\mathfrak{p}) = p\mathcal{O}_K$. In all cases this shows that $\mathfrak{p} \cdot \gamma(\mathfrak{p})$ is a principal ideal. As any fractional ideal $\mathfrak{a}$ of $\mathcal{O}_K$ is a product of powers of prime ideals, the desired result follows.

6. Consider a prime $p \equiv 3 \bmod (4)$. Show that $K := \mathbb{Q}(\sqrt{-p})$ has odd class number.

   Hint: Use Exercise 5 above and Exercise 5 of Sheet 9.

   Solution: Here K is imaginary quadratic, so the non-trivial Galois automorphism of $K/\mathbb{Q}$ is complex conjugation. Consider any ideal class $[\mathfrak{a}]$ with $[\mathfrak{a}]^2 = 1$. Then $\mathfrak{a} \cdot \bar{\mathfrak{a}}^{-1} = \mathfrak{a}^2 \cdot (\mathfrak{a} \cdot \bar{\mathfrak{a}})^{-1}$, where $\mathfrak{a}^2$ is principal by assumption and $\mathfrak{a} \cdot \bar{\mathfrak{a}}$ is principal by Exercise 5 above. Thus $\mathfrak{a} \cdot \bar{\mathfrak{a}}^{-1} = (b)$ for some $b \in K^\times$. Then the computation

$$(b \cdot \bar{b}) \;=\; \mathfrak{a} \cdot \bar{\mathfrak{a}}^{-1} \cdot \overline{(\mathfrak{a} \cdot \bar{\mathfrak{a}}^{-1})} \;=\; \mathfrak{a} \cdot \bar{\mathfrak{a}}^{-1} \cdot \bar{\mathfrak{a}} \cdot \mathfrak{a}^{-1} \;=\; (1)$$

   shows that $\mathrm{Nm}_{K/\mathbb{Q}}(b) = b \cdot \bar{b} \in \mathbb{Z}^\times$. With $b \cdot \bar{b} \geqslant 0$ this implies that $\mathrm{Nm}_{K/\mathbb{Q}}(b) = 1$. By Exercise 5 on Sheet 9 there therefore exists $c \in K^\times$ such that $b = \bar{c}/c$. Thus the fractional ideal $\mathfrak{b} := c\mathfrak{a}$ satisfies $[\mathfrak{b}] = [\mathfrak{a}]$ and $\mathfrak{b} = \bar{\mathfrak{b}}$.

   Now observe that $-p \equiv 1 \bmod (4)$ implies that $d_K = -p$. Thus p is the only rational prime that is ramified in K, and $(p) = \mathfrak{p}^2$ for the principal ideal $\mathfrak{p} := (\sqrt{-p}) = \bar{\mathfrak{p}}$. Consider the prime decomposition $\mathfrak{b} = \mathfrak{p}^n \cdot \mathfrak{p}_1^{n_1} \cdots \mathfrak{p}_r^{n_r}$ with pairwise distinct primes $\mathfrak{p}, \mathfrak{p}_1, \ldots, \mathfrak{p}_r$. Then each $\mathfrak{p}_i$ is unramified over $\mathbb{Z}$, hence it is either inert and $\mathfrak{p}_i = (p_i)$ for some rational prime p_i, or it is split and $\mathfrak{p}_i\bar{\mathfrak{p}}_i = (p_i)$ for some rational prime p_i. Now the equality $\mathfrak{b} = \bar{\mathfrak{b}} = \bar{\mathfrak{p}}^n \cdot \bar{\mathfrak{p}}_1^{n_1} \cdots \bar{\mathfrak{p}}_r^{n_r}$ and the uniqueness of the prime decomposition implies that each split prime $\mathfrak{p}_i$ occurs with the same exponent as its conjugate $\bar{\mathfrak{p}}_i$. Thus $\mathfrak{b}$ is a product of principal ideals and therefore itself principal.

   This shows that the ideal class group of $\mathcal{O}_K$ possesses no element of order 2 and hence has odd order.