Autumn Semester 2019

# Introduction to Algebraic Number Theory

Lecturer: Prof. Dr. Özlem Imamoglu
Coordinator: Dr. Danylo Radchenko

## Solutions to Exercise Sheet 11

**Exercise 11.1.** Let $K = \mathbb{Q}(\sqrt{2}, \sqrt{3})$. Recall from the lectures that $\mathcal{O}_K = \mathbb{Z}[\gamma]$, where $\gamma = \frac{\sqrt{2}+\sqrt{6}}{2}$. Show that no prime is inert in $K$, i.e., that $(p)$ is not a prime ideal of $\mathcal{O}_K$ for any prime $p$.

(*Hint: Use the fact that for any $p$ one of 2, 3, or 6 is a quadratic residue mod $p$.*)

**Solution.** We compute the minimal polynomial of $\gamma = \frac{\sqrt{2}+\sqrt{6}}{2}$ to be

$$q(x) \;=\; (x - \tfrac{\sqrt{2}+\sqrt{6}}{2})(x - \tfrac{-\sqrt{2}+\sqrt{6}}{2})(x - \tfrac{\sqrt{2}-\sqrt{6}}{2})(x - \tfrac{-\sqrt{2}-\sqrt{6}}{2}) \;=\; x^4 - 4x^2 + 1\,.$$

By Theorem 8.5 from the lectures it is enough to prove that the reduction of $q(x)$ modulo any prime is reducible.

For $p = 2$ and $p = 3$ we check directly that $q(x)$ is reducible modulo $p$. Let $p > 3$. Next, grouping the four linear factors in the definition of $q$ in pairs in all different ways we obtain the following factorizations:

$$\begin{aligned} q(x) &= (x^2 - \sqrt{6}x + 1)(x^2 + \sqrt{6}x + 1) \\ &= (x^2 - \sqrt{2}x - 1)(x^2 + \sqrt{2}x - 1) \\ &= (x^2 - 2 - \sqrt{3})(x^2 - 2 + \sqrt{3})\,. \end{aligned}$$

From this we see that if 2, 3, or 6 is a quadratic residue mod $p$, then $q(x)$ modulo $p$ factors as a product of two quadratic polynomials. Thus it is enough to show that one of 2, 3 or 6 is a quadratic residue mod $p$. But this is easy to see: if both 2 and 3 are non-residues modulo $p$, then $(\frac{2}{p}) = (\frac{3}{p}) = -1$, but since $6 = 2 \cdot 3$, this means that $(\frac{6}{p}) = 1$, so that 6 is a quadratic residue.

**Exercise 11.2.** Let $K = \mathbb{Q}(\alpha)$, where $\alpha$ is a root of $p(x) = x^3 - 10x^2 + 19x - 2$.

(a) Show that $D_K = 43^2$;

(b) Check that $\alpha_2 = \frac{-\alpha^2+7\alpha+4}{2}$ and $\alpha_3 = \frac{\alpha^2-9\alpha+16}{2}$ are roots of $p(x)$, and show that $K$ is a Galois extension;

(c) Show that $(2) = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3$ for distinct prime ideals $\mathfrak{p}_i$;

(d) Conclude that $\mathcal{O}_K$ is not monogenic, i.e., $\mathcal{O}_K \neq \mathbb{Z}[\theta]$ for any $\theta \in K$.

**Solution.**

(a) The discriminant of the polynomial is equal to $2^2 \cdot 43^2$. Since $\beta = \frac{\alpha^2-\alpha}{2}$ is an algebraic integer (its minimal polynomial is $x^3 - 26x^2 + 39x + 2$), and it does not belong to $\mathbb{Z}[\alpha]$, we see that $2 | [\mathcal{O}_K : \mathbb{Z}[\alpha]]$. This means that $D_K$ divides $43^2$, and thus $D_K \in \{1, 43^2\}$. But $D_K$ cannot be equal to 1 by Minkowski's theorem, so $D_K = 43^2$.

(b) We have $p(x) = (x-\alpha)(x^2+(\alpha-10)x+(\alpha^2-10\alpha+19))$. Since $\alpha_2+\alpha_3 = -\alpha+10$, and

$$\alpha_2\alpha_3 \;=\; \frac{-\alpha^4+16\alpha^3-75\alpha^2+76\alpha+64}{4} \;=\; \frac{6\alpha^3-56\alpha^2+74\alpha+64}{4} \;=\; \alpha^2-10\alpha+19\,,$$

we see that $p(x) = (x-\alpha)(x-\alpha_2)(x-\alpha_3)$. This implies that $K$ is the splitting field of $p$, and thus it is Galois over $\mathbb{Q}$.

(c) Since the constant coefficient of $p(x)$ is $-2$, from (b) we get that $2 = (\alpha)(\alpha_2)(\alpha_3)$. Therefore we just need to show that $(\alpha)$, $(\alpha_2)$, and $(\alpha_3)$ are distinct. Since $K$ is Galois, it is enough to check that $(\alpha) \neq (\alpha_2)$.

Suppose that $(\alpha) = (\alpha_2)$. Then $\gamma = \alpha_2/\alpha = \alpha^2 - \frac{21}{2}\alpha + \frac{45}{2}$ is an algebraic integer (and even a unit). However, the minimal polynomial of $\gamma$ is $2x^3 - 49x^2 + 135x - 2$, which is not monic, a contradiction.

(d) Suppose that $\mathcal{O}_K = \mathbb{Z}[\theta]$ for some $\theta$ with minimal polynomial $q(x)$. Since $(2) = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3$ by part (c), Theorem 8.5 from the lectures tells us that $\overline{q}(x) = l_1(x)l_2(x)l_3(x)$, where $\overline{q} \in (\mathbb{Z}/2\mathbb{Z})[x]$ is the reduction of $q$ modulo 2, and $l_1$, $l_2$, and $l_3$ are distinct. However, there are only two different linear polynomials in $(\mathbb{Z}/2\mathbb{Z})[x]$, thus contradicting the assumption that $\mathcal{O}_K = \mathbb{Z}[\theta]$.

**Exercise 11.3.** Let $K = \mathbb{Q}(\sqrt{-D})$, where $D \in \{1, 2, 3, 7, 11, 19, 43, 67, 163\}$. Show that the class number of $K$ is equal to 1.

(*Hint: Cases $D = 1, 2, 3, 11, 19$ where previously considered in Ex. 1.1, Ex. 1.2, Ex. 8.1b. In remaining cases compute the Minkowski bound and factorize small primes into prime ideals.*)

**Solution.** Since the cases $D = 1, 2, 3, 11, 19$ where considered before, assume that $D$ is one of $\{7, 43, 67, 163\}$. Since $-D \equiv 1 \pmod 4$, we have that $|D_K| = D$, and thus the Minkowski bound is $M_K = \frac{2\sqrt{D}}{\pi}$. In case $D = 7$ we have $M_K < 2$, so that all fractional ideals are equivalent to $\mathcal{O}_K$ and in this case $h_K = 1$. This leaves the cases $D \in \{43, 67, 163\}$.

In all three remaining cases we have $M_K \leq 8$. This means that any fractional ideal is equivalent to a product of some integral ideals dividing $(p)$ for $p \in \{2, 3, 5, 7\}$.

For $p = 2$ we see that $(2)$ is a prime ideal by Theorem 8.3 from the lectures since $-43 \equiv -67 \equiv -163 \equiv 5 \pmod 8$.

For $p = 3$ we have $-43 \equiv -67 \equiv -163 \equiv -1 \pmod 3$ and thus $(\frac{-D}{3}) = -1$, so by Theorem 8.2 we get that $(3)$ is a prime ideal in $\mathcal{O}_K$.

For $p = 5$ we have $-43$,$-67$, and $-163$ are congruent to $\pm 2$ modulo 5, and since $(\frac{\pm 2}{5}) = -1$, we see that 5 is inert.

For $p = 7$ we have $-43 \equiv 6 \pmod 7$, $-67 \equiv 3 \pmod 7$, and $-163 \equiv 5 \pmod 7$. Since 3, 5, and 6 are quadratic non-residues modulo 7, we get that $(7)$ is a prime ideal.

Thus we see that in all cases each fractional ideal is equivalent to some product of the ideals $(2)$, $(3)$, $(5)$, or $(7)$, but all of these ideals are principal, hence $h_K = 1$.

**Exercise 11.4.** Let $K = \mathbb{Q}(\alpha)$, where $\alpha$ is an algebraic integer with minimal polynomial $q(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0$. Show that if $q(x)$ is Eisenstein at prime $p$ (i.e., $p||a_0$ and $p|a_j$, $j = 1, \ldots, n-1$), then $p \nmid [\mathcal{O}_K : \mathbb{Z}[\alpha]]$.

**Solution.** Suppose that $p|[\mathcal{O}_K : \mathbb{Z}[\alpha]]$. Then there exists an element $\beta \in \mathcal{O}_K$ such that

$\beta \notin \mathbb{Z}[\alpha]$, but $p\beta \in \mathbb{Z}[\alpha]$. Let

$$\beta \;=\; r_0 + r_1\alpha + \cdots + r_{n-1}\alpha^{n-1}\,.$$

Since $p\beta \in \mathbb{Z}[\gamma]$, we have $pr_i \in \mathbb{Z}$, but since $\beta \notin \mathbb{Z}[\gamma]$, at least one of $r_i$ is not an integer. Write $r_i = \frac{b_i}{p}$ for some integers $b_i$; by definition not all of the $b_j$ are divisible by $p$. Thus we have $b_0 + \cdots + b_{n-1}\alpha^{n-1} \in p\mathcal{O}_K$, and at least one of $b_i$ is not divisible by $p$.

Assume that for some $0 \leq k \leq n-1$ we have $p|b_j$ for all $j < k$ (this is certainly the case for $k = 0$). We claim that then $p|b_k$. If this is indeed the case, then by induction we obtain that all $b_j$ are divisible by $p$, and this contradiction finishes the proof.

Let us prove the claim. Since $p|b_j$ for $j < k$, we have $\beta' = b_k\alpha^k + \cdots + b_{n-1}\alpha^{n-1} \in p\mathcal{O}_K$. Note that $\alpha^n \in p\mathcal{O}_K$ by the Eisenstein condition since $\alpha^n = -a_0 - a_1\alpha - \cdots - a_{n-1}\alpha^{n-1}$ and $p|a_j$ for $j = 0, \ldots, n-1$. Thus, multiplying $\beta'$ by $\alpha^{n-1-k}$ we get that $b_k\alpha^{n-1} \in p\mathcal{O}_K$. After taking the norms we get that $p^n$ divides $b_k^n N_{K/\mathbb{Q}}(\alpha)^{n-1} = \pm b_k^n a_0^{n-1}$ ($a_0$ is the constant term of $q(x)$). However, by the Eisenstein condition $a_0$ is divisible by $p$ but not by $p^2$, hence $p^n | b_k^n a_0^{n-1}$ implies that $p|b_k$. This finishes the proof of the claim.