Autumn Semester 2019

Introduction to Algebraic Number Theory

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

Solutions to Exercise Sheet 6

Exercise 6.1. Let $K = \mathbb{Q}(\sqrt{-30})$ and define $\mathfrak{a} = (2, \sqrt{-30})$ and $\mathfrak{b} = (3, \sqrt{-30})$.

(a) Find the norms of $\mathfrak{a}$, $\mathfrak{b}$, and $\mathfrak{ab}$;

(b) Show that $\mathfrak{a}$, $\mathfrak{b}$, and $\mathfrak{ab}$ are not principal and represent different elements of the ideal class group.

(*Hint: show that* $\mathfrak{a}^2 = (2)$ *and* $\mathfrak{b}^2 = (3)$.)

Solution.

(a) We compute $\mathfrak{a}^2 = (4, 2\sqrt{-30}, -30) = (2, 2\sqrt{-30}) = (2)$. Similarly, $\mathfrak{b}^2 = (9, 3\sqrt{-30}, -30) = (3, 3\sqrt{-30}) = (3)$. Since $N((2)) = 2^2$ and $N((3)) = 3^2$, we get $N(\mathfrak{a}) = 2$ and $N(\mathfrak{b}) = 3$ by multiplicativity of the norm. Again using multiplicativity of the norm we get also $N(\mathfrak{ab}) = N(\mathfrak{a})N(\mathfrak{b}) = 6$.

(b) Assume that $\mathfrak{a}$ is principal. Then $2 = N(\mathfrak{a}) = N_{K/\mathbb{Q}}(\alpha)$ for some $\alpha = a + b\sqrt{-30} \in \mathcal{O}_K$. But $N_{K/\mathbb{Q}}(a + b\sqrt{-30}) = a^2 + 30b^2$ cannot be equal to 2 (since $2 < 30$, we must have $b = 0$, but then $a^2 \neq 2$ since 2 is not a square). Repeating the same reasoning for $\mathfrak{b}$ and $\mathfrak{ab}$ (since $3 < 30$, $6 < 30$, and both 3 and 6 are not squares) we get that all three ideals are not principal.

Clearly, $\mathfrak{a}$ and $\mathfrak{ab}$ represent different ideal classes, since otherwise we would have that $\mathfrak{b}$ is principal, which we have already checked not to be the case. For the same reason, $\mathfrak{b}$ and $\mathfrak{ab}$ represent different classes.

It remains to check that $\mathfrak{a}$ and $\mathfrak{b}$ are from different ideal classes. Suppose that they are the same, then $\mathfrak{ab} \sim \mathfrak{b}^2 = (3)$ (see (a)) is principal, but we have already checked that $\mathfrak{ab}$ is not principal.

Exercise 6.2. Let $K = \mathbb{Q}(\sqrt{5})$ and let $A = \mathbb{Z}[\sqrt{5}]$ (note that $A \neq \mathcal{O}_K$).

(a) Prove that the ideal $\mathfrak{p} = (2, 1 + \sqrt{5})$ in A is maximal, and $|A/\mathfrak{p}| = 2$.

(b) Prove that $\mathfrak{p}^2 = 2\mathfrak{p}$ and $\mathfrak{p}^{-1} = \frac{1}{2}\mathfrak{p}$, so that $\mathfrak{p}\mathfrak{p}^{-1} = \mathfrak{p}$;

(c) Let $\mathfrak{a} = (2)$. Show that $\mathfrak{a} \subseteq \mathfrak{p}$, but there is no ideal $\mathfrak{b}$ such that $\mathfrak{a} = \mathfrak{pb}$ (i.e, $\mathfrak{p} \nmid \mathfrak{a}$).
(*Hint: in (c) suppose that* $\mathfrak{a} = \mathfrak{pb}$ *for some integral ideal* $\mathfrak{b}$ *and use (b) to show that* $\mathfrak{a} = \mathfrak{p}$.)

Solution. (a) A simple calculation shows that $(2, 1 + \sqrt{5}) = \{a + b\sqrt{5} \mid a \equiv b \pmod 2\}$. This implies that $A/\mathfrak{p} \cong \mathbb{Z}/2\mathbb{Z}$ since any element of A is equal mod $\mathfrak{p}$ to either 0 or 1 and $1 \notin \mathfrak{p}$. Since $\mathbb{Z}/2\mathbb{Z}$ is a field, $\mathfrak{p}$ is maximal.

(b) We have $\mathfrak{p}^2 = (4, 2 + 2\sqrt{5}, 6 + 2\sqrt{5}) = (4, 2 + 2\sqrt{5}) = 2(2, 1 + \sqrt{5}) = 2\mathfrak{p}$. Next, $a + b\sqrt{5} \in \mathfrak{p}^{-1}$ if and only if $2a, 2b \in \mathbb{Z}$ and $a + b, a + 5b \in \mathbb{Z}$. This is equivalent to

$2a, 2b \in \mathbb{Z}$ and $2a \equiv 2b \pmod 2$, i.e. $2(a + b\sqrt{5}) \in \mathfrak{p}$. Therefore, $\mathfrak{p}^{-1} = \frac{1}{2}\mathfrak{p}$. Finally, from these identities we get $\mathfrak{p}\mathfrak{p}^{-1} = \frac{1}{2}\mathfrak{p}^2 = \mathfrak{p}$.

(c) The inclusion $\mathfrak{a} \subseteq \mathfrak{p}$ is trivial. Suppose that $\mathfrak{a} = \mathfrak{p}\mathfrak{b}$ for some integral ideal $\mathfrak{b}$. Then multiplying this identity by $\mathfrak{p}$ on both sides we get $2\mathfrak{p} = \mathfrak{a}\mathfrak{p} = \mathfrak{p}^2\mathfrak{b} = 2\mathfrak{p}\mathfrak{b}$. Multiplying this identity by $\frac{1}{2}$ we get $\mathfrak{p} = \mathfrak{p}\mathfrak{b} = \mathfrak{a}$. But this is impossible, since $1 + \sqrt{5} \in \mathfrak{p}$ does not belong to $\mathfrak{a}$.

Exercise 6.3. Let K be a number field and assume that $|Cl_K| = 2$.

(a) Let $a \in \mathcal{O}_K$ be an irreducible element that is not prime. Show that $(a) = \mathfrak{p}_1\mathfrak{p}_2$ for some non-principal prime ideals $\mathfrak{p}_1$, $\mathfrak{p}_2$;

(b) Show that any two factorizations of $a \in \mathcal{O}_K$ into irreducibles have the same number of irreducible factors.

Solution. (a) By unique factorization of ideals we have $(a) = \mathfrak{p}_1 \dots \mathfrak{p}_n$ for some prime ideals $\mathfrak{p}_1, \dots, \mathfrak{p}_n$. Since (a) is not a prime ideal, we must have $n \geq 2$.

Assume that $n \geq 3$. Then by pigeonhole principle some two ideals, say $\mathfrak{p}_1$ and $\mathfrak{p}_2$, represent the same class in Cl_K, and since Cl_K is of order 2, this means that $\mathfrak{p}_1\mathfrak{p}_2$ is principal. If $\mathfrak{p}_1\mathfrak{p}_2 = (b)$, then $b|a$, and since a is irreducible this means that $a = ub$ for some unit u. However, this implies that $(a) = (b) = \mathfrak{p}_1\mathfrak{p}_2$, which contradicts the fact that $(a) = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3$. Therefore, $n = 2$, and $(a) = \mathfrak{p}_1\mathfrak{p}_2$. For the same reason the ideals $\mathfrak{p}_1$ and $\mathfrak{p}_2$ are not principal, since if $\mathfrak{p}_i = (b)$, then $b|a$, and we again arrive at a contradiction.

(b) Consider the prime factorization $(a) = \mathfrak{p}_1 \dots \mathfrak{p}_n$ and let k be the number of principal ideals among $\mathfrak{p}_1, \dots, \mathfrak{p}_n$. Let $a = q_1 \dots q_m$ be any factorization of a into irreducibles. Then $(a) = (q_1) \dots (q_m)$. Assume that $(q_1), \dots, (q_r)$ are prime ideals, and $(q_{r+1}), \dots, (q_m)$ are not prime. Then by part (a) $(q_i) = \mathfrak{p}_{i,1}\mathfrak{p}_{i,2}$ for $i = r+1, \dots, m$, and comparing the two factorizations for (a) we get $n = r + 2(m - r) = 2m - r$. Moreover, the number of principal ideals in the factorization of (a) is equal to $k = r$. From this we see that $m = (n + k)/2$ so that m is independent of the factorization (n and k only depend on a).

Exercise 6.4. In this exercise we give a different definition of the ideal class group. Let K be a number field, $A = \mathcal{O}_K$, and let $\mathcal{I}$ be the set of all integral ideals of A. We say that $\mathfrak{a} \sim \mathfrak{b}$ for $\mathfrak{a}, \mathfrak{b} \in \mathcal{I}$ if there are non-zero elements $x, y \in A$ such that $x\mathfrak{a} = y\mathfrak{b}$.

(a) Show that $\sim$ is an equivalence relation on $\mathcal{I}$;

(b) Show that if $\mathfrak{a} \sim \mathfrak{a}'$ and $\mathfrak{b} \sim \mathfrak{b}'$, then $\mathfrak{a}\mathfrak{b} \sim \mathfrak{a}'\mathfrak{b}'$, and show that there is $\widetilde{\mathfrak{a}} \in \mathcal{I}$ such that $\mathfrak{a}\widetilde{\mathfrak{a}} \sim A$, so that $\mathcal{I}/\sim$ is a group whose identity is the equivalence class of A;

(c) Show that the group $\mathcal{I}/\sim$ is isomorphic to the class group defined in terms of fractional ideals.

Solution. (a) Reflexivity and symmetry are clear. Let $\mathfrak{a}$, $\mathfrak{b}$, $\mathfrak{c}$ be integral ideals with $\mathfrak{a} \sim \mathfrak{b}$ and $\mathfrak{b} \sim \mathfrak{c}$. This means that $x\mathfrak{a} = y\mathfrak{b}$ and $z\mathfrak{b} = w\mathfrak{c}$ for some nonzero $x, y, z, w \in A$. Then $xz\mathfrak{a} = yz\mathfrak{b} = wz\mathfrak{c}$, proving transitivity. Thus $\sim$ is an equivalence relation.

(b) If $x\mathfrak{a} = y\mathfrak{a}'$ and $z\mathfrak{b} = w\mathfrak{b}'$, then $xz\mathfrak{a}\mathfrak{b} = x\mathfrak{a}\, z\mathfrak{b} = y\mathfrak{a}'\, w\mathfrak{b}' = yw\mathfrak{a}'\mathfrak{b}'$. Recall that $\mathfrak{a}\mathfrak{a}^{-1} = A$, where $\mathfrak{a}^{-1} = \{x \in A \mid x\mathfrak{a} \subseteq A\}$ is a fractional ideal. Since $\mathfrak{a}^{-1}$ is a finitely-generated A-submodule of K and for any element $x \in K$ there is a number $n \in A$ (in fact

even $n \in \mathbb{Z}$) such that $nx \in A$, for some $n \in A$ we have $n\mathfrak{a}^{-1} \subseteq A$. If we set $\widetilde{a} = n\mathfrak{a}^{-1}$, then $\mathfrak{a}\widetilde{\mathfrak{a}} = n\mathfrak{a}\mathfrak{a}^{-1} = nA \sim A$ as needed.

(c) Since any integral ideal is itself a fractional ideal, we get a well-defined map of sets $\phi\colon \mathcal{I} \to Cl_K$. Next, if $\mathfrak{a}, \mathfrak{b} \in \mathcal{I}$ are equivalent, i.e., $x\mathfrak{a} = y\mathfrak{b}$, then $\mathfrak{b} = (x/y)\mathfrak{a}$, and thus $\phi(\mathfrak{a}) = \phi(\mathfrak{b})$. In view of (b) this gives a well-defined homomorphism $\overline{\phi}\colon \mathcal{I}/\!\sim \to Cl_K$. This homomorphism is surjective since for any fractional ideal $\mathfrak{a}$ there is some $n \in A$ such that $n\mathfrak{a}$ is an integral ideal, and thus $\overline{\phi}(n\mathfrak{a})$ is equal to the class of $\mathfrak{a}$. Finally, let $\mathfrak{a}$ represent a class in the kernel of $\overline{\phi}$. By definition this means that $\mathfrak{a}$ is principal, but then $\mathfrak{a} \sim A$ and hence the class of $\mathfrak{a}$ is trivial in $\mathcal{I}/\!\sim$. Thus $\ker\overline{\phi}$ is trivial and $\overline{\phi}$ is an isomorphism.