Nontrivial Ideal Class Groups

Seewoo Lee

February 15, 2022

In this note, we will compute the ideal class groups of the following number fields:

$$\mathbb{Q}(\sqrt{226}),\ \mathbb{Q}(\sqrt{-30}),\ \mathbb{Q}(\sqrt{-89}),\ \mathbb{Q}(\sqrt[3]{7}),\ \mathbb{Q}(\alpha),$$

where α is a root of a cubic polynomial $f(x) = x^3 + 11x + 21$.

General method is the following (this follows the argument of [1]): by Minkowski's theorem, for any ideal class A of K, there exists an integral ideal $\mathfrak{a} \in A$ s.t.

$$N(\mathfrak{a}) \leq \frac{n!}{n^n}\left(\frac{4}{\pi}\right)^s \sqrt{|d_K|} =: M_K$$

where $n = [K : \mathbb{Q}]$, s is the number of complex embedding of K and d_K is the discriminant of K. Thus $\mathrm{Cl}(K)$ is generated by the ideal class $[\mathfrak{p}]$ of prime ideals $\mathfrak{p}$ with $N(\mathfrak{p}) \leq M_K$. By the Proposition 8.3. of [4], we know how the prime ideal $(p) \subseteq \mathbb{Z}$ factors in K very well. Now try to find $\alpha \in \mathcal{O}_K$ s.t. the norm $N((\alpha))$ of the principal ideal has only prime factors less than M_K, and this gives a nontrivial relation among ideal classes. We use MATLAB and SAGE for complicated computations that is hard to do by hand. Especially, we can compute norm of any element of given number field. SAGE can even compute ideal class groups of number fields, but we are not going to use this directly.

1 $K = \mathbb{Q}(\sqrt{226}) \Rightarrow \mathrm{Cl}(K) \simeq \mathbb{Z}/8\mathbb{Z}$

Since $226 \equiv 2 \pmod 4$, discriminant of the field is $4 \times 226 = 904$, $\mathcal{O}_K = \mathbb{Z}[\sqrt{226}]$ and the Minkowski bound is $\frac{1}{2}\sqrt{904} < 16$. Hence we look at the primes lying over 2, 3, 5, 7, 11, and 13. Using the Proposition 8.3. of [4], we can determine how the principal ideals $(2), (3), (5), \ldots, (13)$ decompose in $\mathcal{O}_K$:

p	$X^2 - 226 \bmod p$	factorization
2	X^2	$(2, \sqrt{226})^2 = \mathfrak{p}_2^2$
3	$(X-1)(X+1)$	$(3, -1+\sqrt{226})(3, 1+\sqrt{226}) = \mathfrak{p}_3\mathfrak{p}_3'$
5	$(X-1)(X+1)$	$(5, -1+\sqrt{226})(5, 1+\sqrt{226}) = \mathfrak{p}_5{\mathfrak{p}_5}'$
7	$(X-3)(X+3)$	$(7, -3+\sqrt{226})(7, 3+\sqrt{226}) = \mathfrak{p}_7\mathfrak{p}_7'$
11	$X^2 - 6$	(11)
13	$X^2 - 5$	(13)

So $\mathrm{Cl}(K)$ is generated by $[\mathfrak{p}_2], [\mathfrak{p}_3], [\mathfrak{p}_5]$, and $[\mathfrak{p}_7]$, and $[\mathfrak{p}_3'] = [\mathfrak{p}_3]^{-1}$, $[\mathfrak{p}_5'] = [\mathfrak{p}_5]^{-1}$, and $[\mathfrak{p}_7'] = [\mathfrak{p}_7]^{-1}$. Note that $N(\mathfrak{p}_q) = N(\mathfrak{p}_q') = q$ for $q = 2, 3, 5, 7$.

Before we analyze prime ideals, we will compute the unit group first. Since $K = \mathbb{Q}(\sqrt{226})$ is a real quadratic field, its unit group $U_K = \mathcal{O}_K^\times$ is generated by -1 and a fundamental unit $\epsilon = a + b\sqrt{226}$, which satisfies $a^2 - 226b^2 = \pm 1$. The continued fraction of $\sqrt{226}$ is $[15; \overline{30}]$, so $a^2 - 226b^2 = -1$ has an integer solution $(a, b) = (15, 1)$, and $15 + \sqrt{226}$ is the fundamental unit we were looking for. (See [6] for details.)

We will show that $\mathfrak{p}_2 = (2, \sqrt{226})$ is not a principal ideal, so $[\mathfrak{p}_2]$ has order 2 in the class group. If it is a principal ideal that is generated by $\alpha = a + b\sqrt{226}$, then $\mathfrak{p}_2^2 = (2)$ implies $2u = (a + b\sqrt{226})^2$ for some unit $u \in U_K$. By taking a norm on a both side, $N_{K/\mathbb{Q}}(u)$ should be positive and so $u = (15 + \sqrt{226})^{2k}$ for some $k \in \mathbb{Z}$. A unit square can be absorbed into the $(a + b\sqrt{226})^2$ term, so we have $2 = (a + b\sqrt{226})^2$, which is definitely impossible since $\sqrt{2} \notin \mathbb{Z}[\sqrt{226}]$. By the same way, we can prove that $\mathfrak{p}_3, \mathfrak{p}_5, \mathfrak{p}_7$ are not principal. Now we will prove that $\mathrm{Cl}(K)$ is a cyclic group of order 8, generated by the ideal class $[\mathfrak{p}_3]$. Since $N((11 + \sqrt{226})) = 105 = 3 \times 5 \times 7$, it should be a product of three distinct prime ideals which lie over (3), (5) and (7), respectively. Those ideals should contain $11 + \sqrt{226}$, hence we can conclude that

$$(11 + \sqrt{226}) = (3, -1 + \sqrt{226})(5, 1 + \sqrt{226})(7, -3 + \sqrt{226}) = \mathfrak{p}_3\mathfrak{p}_5'\mathfrak{p}_7.$$

Similarly, we can check that

$$(16 + \sqrt{226}) = \mathfrak{p}_2\mathfrak{p}_3'\mathfrak{p}_5', \quad (17 + \sqrt{226}) = \mathfrak{p}_3^2\mathfrak{p}_7'.$$

By these relations, we have $[\mathfrak{p}_5] = [\mathfrak{p}_2][\mathfrak{p}_3]^{-1}$ and $[\mathfrak{p}_7] = [\mathfrak{p}_3]^{-1}[\mathfrak{p}_5] = [\mathfrak{p}_2][\mathfrak{p}_3]^{-2}$. From $[\mathfrak{p}_7] = [\mathfrak{p}_3]^2$, we get $[\mathfrak{p}_2] = [\mathfrak{p}_3]^4$, and since $[\mathfrak{p}_2]$ has order 2, $[\mathfrak{p}_3]$ has order 8. Since $[\mathfrak{p}_5] = [\mathfrak{p}_3]$ and $[\mathfrak{p}_7] = [\mathfrak{p}_3]^2$, $\mathrm{Cl}(K)$ is generated by one element $[\mathfrak{p}_3] = [(3, -1 + \sqrt{226})]$, which has order 8.

2 $K = \mathbb{Q}(\sqrt{-30}) \Rightarrow \mathrm{Cl}(K) \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$

Since $-30 \equiv 2 \pmod 4$, $d_K = 2 \times (-30) = -60$, $\mathcal{O}_K = \mathbb{Z}[\sqrt{-30}]$ and the Minkowski bound is $\frac{4}{\pi}\sqrt{30} < 7$. Hence we look at the primes lying over 2,3, and 5. The ideals $(2), (3), (5)$ decompose in $\mathcal{O}_K$ as follows:

p	$X^2 + 30 \bmod p$	factorization
2	X^2	$(2, \sqrt{-30})^2 = \mathfrak{p}_2^2$
3	$X^2 - 2$	(3)
5	X^2	$(5, \sqrt{-30})^2 = \mathfrak{p}_5^5$

So $\mathrm{Cl}(K)$ is generated by $[\mathfrak{p}_2]$ and $[\mathfrak{p}_3]$. Since both $a^2 + 30b^2 = 2$ and $a^2 + 30b^2 = 5$ don't have integer solution, $\mathfrak{p}_2$ and $\mathfrak{p}_5$ aren't principal and $[\mathfrak{p}_2], [\mathfrak{p}_5]$ have order 2 in $\mathrm{Cl}(K)$.

Now we will show that there's any relation between $[\mathfrak{p}_2]$ and $[\mathfrak{p}_5]$, so that $\mathrm{Cl}(K)$ is a Klein 4-group generated by $[\mathfrak{p}_2]$ and $[\mathfrak{p}_5]$. Since both have order 2, it is enough to show that $[\mathfrak{p}_2] \neq [\mathfrak{p}_5] \Leftrightarrow [\mathfrak{p}_2\mathfrak{p}_5] \neq 1 \Leftrightarrow \mathfrak{p}_2\mathfrak{p}_5$ is not a principal ideal. We have

$$\mathfrak{p}_2\mathfrak{p}_5 = (2, \sqrt{-30})(5, \sqrt{-30}) = (10, 2\sqrt{-30}, 5\sqrt{-30}, -30) = (10, \sqrt{-30}).$$

Assume that this is a principal ideal, i.e. $(10, \sqrt{-30}) = (a + b\sqrt{-30})$ for some $a, b \in \mathbb{Z}$. Then $(10) \subseteq (a + b\sqrt{-30})$ and $(\sqrt{-30}) \subseteq (a + b\sqrt{-30})$ gives $a^2 + 30b^2 | \gcd(100, 30) = 10$, which gives $(a, b) = (1, 0)$, and this generates the unit ideal. Contradiction.

3 $K = \mathbb{Q}(\sqrt{-89}) \Rightarrow \mathrm{Cl}(K) \simeq \mathbb{Z}/12\mathbb{Z}$

Since $-89 \equiv 3 \pmod 4$, $d_K = 4 \times (-89) = -356$, $\mathcal{O}_K = \mathbb{Z}[\sqrt{-89}]$ and the Minkowski bound is $\frac{4}{\pi}\sqrt{89} < 13$. Hence we look at the primes lying over 2, 3, 5, 7, and 11. The ideals $(2), (3), (5), (7), (11)$ decompose in $\mathcal{O}_K$ as follows:

p	$X^2 + 89 \bmod p$	factorization
2	$(X+1)^2$	$(2, -1 + \sqrt{-89})^2 = \mathfrak{p}_2^2$
3	$(X-1)(X+1)$	$(3, -1 + \sqrt{-89})(3, 1 + \sqrt{-89}) = \mathfrak{p}_3\mathfrak{p}_3'$
5	$(X-1)(X+1)$	$(5, -1 + \sqrt{-89})(5, 1 + \sqrt{-89}) = \mathfrak{p}_5\mathfrak{p}_5'$
7	$(X-3)(X+3)$	$(7, -3 + \sqrt{-89})(7, 3 + \sqrt{-89}) = \mathfrak{p}_7\mathfrak{p}_7'$
11	$X^2 + 1$	(11)

So $\mathrm{Cl}(K)$ is generated by $[\mathfrak{p}_2], [\mathfrak{p}_3], [\mathfrak{p}_5]$, and $[\mathfrak{p}_7]$, and $[\mathfrak{p}_3'] = [\mathfrak{p}_3]^{-1}$, $[\mathfrak{p}_5'] = [\mathfrak{p}_5]^{-1}$, and $[\mathfrak{p}_7'] = [\mathfrak{p}_7]^{-1}$. Note that $N(\mathfrak{p}_q) = N(\mathfrak{p}_q') = q$ for $q = 2, 3, 5, 7$. Since $a^2 + 89b^2 = q$ doesn't have integer solution for $q = 2, 3, 5, 7$, $\mathfrak{p}_q$ aren't principal for $q = 2, 3, 5, 7$. We will show that the class group is generated by $[\mathfrak{p}_5]$ and $[\mathfrak{p}_7]$, which have order 3 and 4 respectively. This will prove that $\mathrm{Cl}(K)$ is an order 12 cyclic group generated by $[\mathfrak{p}_5\mathfrak{p}_7]$. We have the following factorizations:

$$\begin{aligned}
(1 + \sqrt{-89}) &= \mathfrak{p}_2\mathfrak{p}_3^2\mathfrak{p}_5' \\
(3 + \sqrt{-89}) &= \mathfrak{p}_2(\mathfrak{p}_7')^2 \\
(6 + \sqrt{-89}) &= (\mathfrak{p}_5')^3 \\
(40 + 3\sqrt{-89}) &= \mathfrak{p}_7^4 \\
(10 + \sqrt{-89}) &= (\mathfrak{p}_3')^3\mathfrak{p}_7'.
\end{aligned}$$

Since the only integer solution of $a^2 + 89b^2 = 49$ is $(a, b) = (\pm 7, 0)$, $\mathfrak{p}_7^2$ is not a principal ideal and $[\mathfrak{p}_7]$ has order 4. Also, we have $[\mathfrak{p}_2] = [\mathfrak{p}_7]^2$. From $[\mathfrak{p}_3]^2 = [\mathfrak{p}_2][\mathfrak{p}_5] = [\mathfrak{p}_7]^2[\mathfrak{p}_5]$ and $[\mathfrak{p}_3]^3 = [\mathfrak{p}_7]^{-1}$, we have $[\mathfrak{p}_3] = [\mathfrak{p}_5]^{-1}[\mathfrak{p}_7]^{-3}$. Thus $\mathrm{Cl}(K)$ is generated by two ideal classes $[\mathfrak{p}_5]$ and $[\mathfrak{p}_7]$, and we can easily check that the ideal class $[\mathfrak{p}_3] = [(3, -1 + \sqrt{-89})] = [\mathfrak{p}_5]^{-1}[\mathfrak{p}_7]^{-3} = [\mathfrak{p}_5]^2[\mathfrak{p}_7]$ became a generator of the group.

4 $K = \mathbb{Q}(\sqrt[3]{7}) \Rightarrow \mathrm{Cl}(K) \simeq \mathbb{Z}/3\mathbb{Z}$

This is one of exercises in [3]. First, we will show that $\mathcal{O}_K = \mathbb{Z}[\sqrt[3]{7}]$. It is clear that $\mathbb{Z}[\sqrt[3]{7}] \subseteq \mathcal{O}_K$. The discriminant of the polynomial $x^3 - 7$ is $-1323 = -3^3 \times 7^2$, so if $(\mathcal{O}_K : \mathbb{Z}[\sqrt[3]{7}])$ is not 1, then its possible prime factors are 3 and 7. Hence it is enough to show that $(\mathcal{O}_K : \mathbb{Z}[\sqrt[3]{7}])$ can't be divided by 3 or 7.

First, assume that $3|(\mathcal{O}_K : \mathbb{Z}[\sqrt[3]{7}])$. Then there exists $\alpha \in \mathcal{O}_K$ s.t. $\alpha \notin \mathbb{Z}[\sqrt[3]{7}]$ but $3\alpha \in \mathbb{Z}[\sqrt[3]{7}]$. So $\alpha = (a + b\sqrt[3]{7} + c\sqrt[3]{49})/3$ for some $a, b, c \in \mathbb{Z}$. By adding elements in $\mathbb{Z}[\sqrt[3]{7}]$, we can assume that $a, b, c \in \{-1, 0, 1\}$. Then

$$\mathrm{Nm}_{K/\mathbb{Q}}(\alpha) = \frac{1}{27}(a^3 + 7b^3 + 49c^3 - 21abc) \in \mathbb{Z},$$

so $27|(a^3 + 7b^3 + 49c^3 - 21abc)$. However, we can check that the only possible combination is $(a, b, c) = (0, 0, 0)$, which contradicts to $\alpha \notin \mathbb{Z}[\sqrt[3]{7}]$. Hence $3 \nmid (\mathcal{O}_K : \mathbb{Z}[\sqrt{7}])$. Similarly, we can prove that $7 \nmid (\mathcal{O}_K : \mathbb{Z}[\sqrt[3]{7}])$, so we have $\mathcal{O}_K = \mathbb{Z}[\sqrt[3]{7}]$,

We know that $n = 3 = r + 2s$ where $r = 1, s = 1$ and $d_K = -1323$ as we mentioned above. Hence the Minkowski bound is $\frac{2}{9}\left(\frac{4}{\pi}\right)\sqrt{1323} < 11$, so we look at the primes lying over 2, 3, 5, and 7. The ideals $(2), (3), (5), (7)$ decompose in $\mathcal{O}_K$ as follows:

p	$X^3 - 7 \bmod p$	factorization
2	$(X-1)(X^2+X+1)$	$(2, -1+\sqrt[3]{7})(2, 1+\sqrt[3]{7}+\sqrt[3]{49}) = \mathfrak{p}_2\mathfrak{q}_2$
3	$(X-1)^3$	$(3, -1+\sqrt[3]{7})^3 = \mathfrak{p}_3^3$
5	$(X-3)(X^2-2X-1)$	$(5, -3+\sqrt[3]{7})(5, -1-2\sqrt[3]{7}+\sqrt[3]{49}) = \mathfrak{p}_5\mathfrak{q}_5$
7	X^3	$(7, \sqrt[3]{7})^3 = (\sqrt[3]{7})^3 = \mathfrak{p}_7^3$

So $\mathrm{Cl}(K)$ is generated by $[\mathfrak{p}_2], [\mathfrak{p}_3], [\mathfrak{p}_5]$, and $[\mathfrak{q}_2] = [\mathfrak{p}_2]^{-1}$, $[\mathfrak{q}_5] = [\mathfrak{p}_5]^{-1}$. Note that $N(\mathfrak{p}_q) = q$ for $q = 2, 3, 5, 7$ and $N(\mathfrak{q}_q) = q^2$ for $q = 2, 5$. We have the following factorizations:

$$(1 + \sqrt[3]{49}) = \mathfrak{p}_2\mathfrak{p}_5^2$$
$$(1 + \sqrt[3]{7} + \sqrt[3]{49}) = \mathfrak{q}_2\mathfrak{p}_3^2$$

From this, we have $[\mathfrak{p}_2] = [\mathfrak{p}_5]^{-2}$ and $[\mathfrak{p}_3] = [\mathfrak{q}_2][\mathfrak{p}_3]^3 = [\mathfrak{q}_2] = [\mathfrak{p}_2]^{-1} = [\mathfrak{p}_5]^2$, so $\mathrm{Cl}(K)$ is generated by the single ideal class $[\mathfrak{p}_5]$. First, we will show that $[\mathfrak{p}_5]^3 = 1$. Consider $\alpha = 5 + 4\sqrt[3]{7} + 2\sqrt[3]{49} \in \mathbb{Z}[\sqrt[3]{7}]$. We have $N(\alpha) = 125$, so we should have $(\alpha) = \mathfrak{p}_5\mathfrak{q}_5$ or $\mathfrak{p}_5^3$. Assume that $(\alpha) \subseteq \mathfrak{q}_5$. Then we also have $(4\sqrt[3]{7} + 2\sqrt[3]{49}) \subseteq \mathfrak{q}_5$, since $5 \in \mathfrak{q}_5$. However, this is impossible since $N(4\sqrt[3]{7} + 2\sqrt[3]{49}) = 840$ can't be divided by $N(\mathfrak{q}_5) = 25$. Thus $(\alpha) = \mathfrak{p}_5^3$ and we get $[\mathfrak{p}_5]^3 = 1$.

Our last claim is that $\mathfrak{p}_5$ is not a principal ideal, so that $[\mathfrak{p}_5]$ has order 3 and $\mathrm{Cl}(K) \simeq \mathbb{Z}/3\mathbb{Z}$. For this, we have to compute the unit group $U_K = \mathcal{O}_K^\times$ first. By Dirichlet's unit theorem, $U_K \simeq \mu(\mathcal{O}_K) \times \epsilon^{\mathbb{Z}}$ where $\mu(\mathcal{O}_K)$ is the finite cyclic group of roots of unity in $\mathcal{O}_K$ and ϵ is a fundamental unit of U_K. From $1 = 8 - 7 = (2 - \sqrt[3]{7})(4 + 2\sqrt[3]{7} + \sqrt[3]{49})$, both $2 - \sqrt[3]{7}$ and $4 + 2\sqrt[3]{7} + \sqrt[3]{49}$ are units. Our claim is that these are fundamental units. To prove this, we use Artin's inequality:

Theorem 1 (Artin)**.** *Let $\mathcal{O}$ be an order in a cubic field K with $r = 1$. Viewing K in $\mathbb{R}$, if $v > 1$ is a unit of $\mathcal{O}^\times$ then $|\mathrm{disc}(\mathcal{O})| < 4v^3 + 24$.*

Corollary 1. *Let $\mathcal{O}$ be an order in a cubic field K with $r = 1$ and let $\epsilon > 1$ be a fundamental unit of K as an element of $\mathbb{R}$. If $u > 1$ is a unit in $\mathcal{O}^\times$ and $4u^{3/m} + 24 < |\mathrm{disc}(\mathcal{O})|$ for some integer $m \geq 2$, then $u = \epsilon^k$ for some $1 \leq k < m$. In particular, if $4u^{3/2} + 24 < |\mathrm{disc}(\mathcal{O})|$, then $u = \epsilon$.*

For the proof of these, see [2]. Since $u = 4+2\sqrt[3]{7}+\sqrt[3]{49}$ satisfies $4u^{3/2}+24 < 1323$, u is a fundamental unit, and since $2 - \sqrt[3]{7} = u^{-1}$, we get $U_K = \pm\epsilon^{\mathbb{Z}}$ for $\epsilon = 2 - \sqrt[3]{7}$. (Note that only real root of unity is ± 1.)

Now assume that $\mathfrak{p}_5$ is a principal ideal generated by $\beta = a + b\sqrt[3]{7} + c\sqrt[3]{49} \in \mathbb{Z}[\sqrt[3]{7}]$. From $\mathfrak{p}_5^3 = (\alpha)$, we have $\alpha v = \beta^3$ for some $v \in U_K$. Since β can be changed by a unit cube without affecting the ideal (β^3), we may assume that $v = 1, \epsilon$, or ϵ^{-1}. Now we can deal with this case by case:

1. $v = 1$. We have $\beta^3 = 5 + 4\sqrt[3]{7} + 2\sqrt[3]{49}$. From

$$\begin{aligned}(a + b\sqrt[3]{7} + c\sqrt[3]{49})^3 &= (a^3 + 7b^3 + 49c^3 + 42abc)\\ &\quad + (3a^2b + 21b^2c + 21c^2a)\sqrt[3]{7}\\ &\quad + (3ab^2 + 21bc^2 + 3ca^2)\sqrt[3]{49},\end{aligned}$$

   we can easily see that it is impossible by comparing coefficient of $\sqrt[3]{7}$. $3a^2b + 21b^2c + 21c^2a$ is a multiple of 3, but 4 isn't.

2. $v = \epsilon = 2 - \sqrt[3]{7}$. $\alpha v = -4 + 3\sqrt[3]{7}$. From $a^3 + 7b^3 + 49c^3 + 42abc = -4$, we have $a^3 \equiv 3 \pmod 7$. However, we can check that 3 is not a cubic residue mod 7, so it is impossible.

3. $v = \epsilon^{-1} = 4 + 2\sqrt[3]{7} + \sqrt[3]{49}$. $\alpha v = 76 + 40\sqrt[3]{7} + 21\sqrt[3]{49}$, so it is impossible since 40 is not a multiple of 3.

Therefore, $\mathrm{Cl}(K)$ is a cyclic group of order 3 generated by the ideal class $[\mathfrak{p}_5] = [(5, -3 + \sqrt[3]{7})]$.

5 $K = \mathbb{Q}[x]/(x^3 + 11x + 21) \Rightarrow \mathrm{Cl}(K) \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$

This is an example found by the MSE user Y. H. Ng (see [5]). Let $f(x) = x^3+11x+21$ and let $\alpha \in \mathbb{R}$ be a root of $f(x)$. Then $K \simeq \mathbb{Q}(\alpha)$. The discriminant of K is same as the discriminant of $f(x)$, which is -17231, a prime. Hence we have $\mathcal{O}_K = \mathbb{Z}[\alpha]$ and the Minkowski bound is $\frac{8}{9\pi}\sqrt{17231} < 38$, so we loot at the primes lying over 2, 3, 5, 7, 11, 13, 17, 23, 31, and 37. These ideals decompose in $\mathcal{O}_K$ as follows:

p	$X^3 + 11X + 21 \bmod p$	factorization
2	$X^3 + X + 1$	(2)
3	$(X-1)X(X+1)$	$(3,\alpha-1)(3,\alpha)(3,\alpha+1) = \mathfrak{p}_3\mathfrak{p}'_3\mathfrak{p}''_3$
5	$X^3 + X + 1$	(5)
7	$X(X^2+4)$	$(7,\alpha)(7,\alpha^2+4) = \mathfrak{p}_7\mathfrak{q}_7$
11	$(X-1)(X^2+X+1)$	$(11,\alpha-1)(11,\alpha^2+\alpha+1) = \mathfrak{p}_{11}\mathfrak{q}_{11}$
13	$(X+3)(X^2-X-4)$	$(13,\alpha+3)(13,\alpha^2-\alpha-4) = \mathfrak{p}_{13}\mathfrak{q}_{13}$
17	$(X-2)(X^2+2X-2)$	$(17,\alpha-2)(17,\alpha^2+\alpha-2) = \mathfrak{p}_{17}\mathfrak{q}_{17}$
19	$(X+7)(X^2-7x+3)$	$(19,\alpha+7)(19,\alpha^2-7\alpha+3) = \mathfrak{p}_{19}\mathfrak{q}_{19}$
23	$(X-8)(X^2+8X+6)$	$(23,\alpha-8)(23,\alpha^2+8\alpha+6) = \mathfrak{p}_{23}\mathfrak{q}_{23}$
29	$(X+4)(X+6)(X-10)$	$(29,\alpha+4)(29,\alpha+6)(29,\alpha-10) = \mathfrak{p}_{29}\mathfrak{p}'_{29}\mathfrak{p}''_{29}$
31	$X^3 + 11x + 21$	(31)
37	$X^3 + 11x + 21$	(37)

So $\mathrm{Cl}(K)$ is generated by $[\mathfrak{p}_3], [\mathfrak{p}'_3], [\mathfrak{p}_{29}], [\mathfrak{p}'_{29}]$ and $[\mathfrak{p}_q]$ for $q = 7, 11, 13, 17, 19, 23$. Note that $N(\mathfrak{p}_q) = q$ for all $q = 3, 7, 11, 13, 17, 19, 23, 29$. As before, we will try to factorize some principal ideals. Good choices for generators are elements which are generators of $\mathfrak{p}_q$, which may give an information about $[\mathfrak{p}_q]$. Norm of an element $\alpha + j \in \mathbb{Z}[\alpha]$ is given by

$$\begin{aligned} N(\alpha + j) &= (\alpha + j)(\alpha' + j)(\alpha'' + j) \\ &= j^3 + (\alpha + \alpha' + \alpha'')j^2 + (\alpha\alpha' + \alpha'\alpha'' + \alpha''\alpha)j + \alpha\alpha'\alpha'' \\ &= j^3 + 11j - 21 \end{aligned}$$

where α', α'' are conjugates of α, i.e. $x^3 + 11x + 21 = (x-\alpha)(x-\alpha')(x-\alpha'')$. From this, we have the following factorizations:

$$\begin{aligned} (\alpha) &= \mathfrak{p}'_3\mathfrak{p}_7 \\ (\alpha - 1) &= \mathfrak{p}_3\mathfrak{p}_{11} \\ (\alpha + 3) &= \mathfrak{p}'_3\mathfrak{p}_{13} \\ (\alpha - 2) &= \mathfrak{p}''_3\mathfrak{p}_{17} \\ (\alpha + 7) &= \mathfrak{p}''_3\mathfrak{p}_7\mathfrak{p}_{19} \\ (\alpha - 8) &= (\mathfrak{p}''_3)^3\mathfrak{p}_{23} \\ (\alpha + 4) &= \mathfrak{p}''_3\mathfrak{p}_{29} \\ (\alpha + 6) &= (\mathfrak{p}'_3)^2\mathfrak{p}'_{29} \end{aligned}$$

This shows that the whole class group is generated by $[\mathfrak{p}_3]$ and $[\mathfrak{p}'_3]$. Our claim is that these are not principal ideals, have order 2, and no relations among them. Thus $\mathrm{Cl}(K) \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ where the generators correspond to these ideal classes. First, they have order dividing 2. In fact, we have

$$\begin{aligned} \mathfrak{p}_3^2 &= (\alpha + 2) \\ (\mathfrak{p}'_3)^2 &= (2\alpha^2 - 3\alpha + 27). \end{aligned}$$

which can be proved by computing their norms.

To show that $\mathfrak{p}_3$ and $\mathfrak{p}_3'$ are not principal, we need to compute a fundamental unit of K as before. One can check that $\alpha^2-\alpha-4$ is a unit with $(\alpha^2-\alpha-4)(16\alpha^2-25\alpha+215)=1$. The real root of the polynomial $x^3+11x+21$ is about -1.5624, so $u=16\alpha^2-25\alpha+215$ satisfies $4u+24<17231$. Hence by the Corollary 1, $u=\epsilon$ or $u=\epsilon^2$ for the fundamental unit $\epsilon>1$ of K. We will show that $u=\epsilon^2$ can not happen by showing that it can't be a quadratic residue mod $\mathfrak{p}_{11}$. Note that there is an isomorphism $\mathbb{F}_{11}\simeq\mathcal{O}_K/\mathfrak{p}_{11}$ induced by $\mathbb{Z}\hookrightarrow\mathcal{O}_K$. (The inverse map is given by $\mathcal{O}_K\to\mathbb{F}_{11}$, which sends α to 1. This is a well-defined homomorphism since $11|f(1)=33$.) Now assume that $u=16\alpha^2-25\alpha+215=\epsilon^2$. From $\epsilon^2=u\equiv 16-25+215=206\equiv 8 \pmod{\mathfrak{p}_{11}}$, 8 should be a quadratic residue mod 11, which is not. Thus $u=\epsilon$ is a fundamental unit of K.

Now assume that $\mathfrak{p}_3=(3,\alpha-1)$ is a principal ideal generated by $\beta=a\alpha^2+b\alpha+c\in\mathbb{Z}[\alpha]$. Since $\mathfrak{p}_3^2=(\alpha+2)$, we have $v(\alpha+2)=\beta^2$ for some $v\in\mathcal{O}_K^\times$. As before, we may assume that $v=1$ or ϵ^{-1}. (We don't have to consider -1 and $-\epsilon^{-1}$ since $\alpha+2>0$ in $\mathbb{R}$.) Note that we have

$$\beta^2=(a\alpha^2+b\alpha+c)^2=(b^2+2ac-11a^2)\alpha^2+(2bc+22ab-21a^2)\alpha+(c^2+42ab).$$

1. $v=1$, $\alpha+2=\beta^2$. Then $c^2+42ab=2$, which is impossible by viewing the equation mod 3.
2. $v=\epsilon^{-1}=\alpha^2-\alpha-4$, $(\alpha^2-\alpha-4)(\alpha+2)=\alpha^2-17\alpha-29=\beta^2$. Then $c^2+42ab=-29$, which is impossible by viewing the equation mod 7.

Thus $\mathfrak{p}_3$ is not a principal ideal and $[\mathfrak{p}_3]\in\mathrm{Cl}(K)$ is an element of order 2.

To show that $\mathfrak{p}_3'=(3,\alpha)$ is not a principal ideal, we will show that $\mathfrak{p}_{13}=(13,\alpha+3)$ is not a principal ideal, since $\mathfrak{p}_3'\mathfrak{p}_{13}=(\alpha+3)$ is a principal ideal. From $(\alpha+3)^2=(\mathfrak{p}_3')^2\mathfrak{p}_{13}^2=(2\alpha^2-3\alpha+27)\mathfrak{p}_{13}^2$, we have $\mathfrak{p}_{13}^2=(-2\alpha^2+9\alpha+19)$. If $\mathfrak{p}_{13}=(\beta)$ for some $\beta=a\alpha^2+b\alpha+c$, then we have $v(-2\alpha^2+9\alpha+19)=\beta^2$ for some $v\in O_K$. As before, we can assume that $v=1$ or ϵ^{-1}. (Note that $-2\alpha^2+9\alpha+19>0$.)

1. $v=1$. $-2\alpha^2+9\alpha+19=\beta^2$. Then $c^2+42ab=19$, which is impossible by viewing the equation mod 3.
2. $v=\epsilon^{-1}=\alpha^2-\alpha-4$. $(\alpha^2-\alpha-4)(-2\alpha^2+9\alpha+19)=40\alpha^2-134\alpha-307$. Then $c^2+42ab=-307$, which is impossible by viewing the equation mod 3.

Thus $[\mathfrak{p}_3']\in\mathrm{Cl}(K)$ is an element of order 2.

Now we have to show that $[\mathfrak{p}_3]\neq[\mathfrak{p}_3']$, which is equivalent to $[\mathfrak{p}_3'']\neq 1$, i.e. $\mathfrak{p}_3''$ is not a principal ideal. Note that we have $(\mathfrak{p}_3'')^2=(-\alpha-1)$ with $-\alpha-1>0$. Assume that $\mathfrak{p}_3''=(\beta)$ for some $\beta=a\alpha^2+b\alpha+c\in\mathcal{O}_K$ and $v(-\alpha-1)=\beta^2$ for some $v\in\mathcal{O}_K^\times$. We may assume that $v=1$ or ϵ^{-1}. (Note that $-\alpha-1>0$.)

1. $v=1$. $-\alpha-1=\beta^2$. Then $c^2+42ab=-1$, which is impossible by viewing the equation mod 3.

2. $v = \epsilon^{-1} = \alpha^2 - \alpha - 4$. $(\alpha^2 - \alpha - 4)(-\alpha - 1) = 16\alpha + 25 = \beta^2$, and the previous argument doesn't work. However, we can check that

$$\alpha^3 + 11\alpha + 21 = \left(\frac{\beta^2 - 25}{16}\right)^3 + 11\left(\frac{\beta^2 - 25}{16}\right) + 21 = \frac{\beta^6 - 75\beta^4 + 4691\beta^2 - 9}{4096} = 0$$

and the polynomial $g(x) = x^6 - 75x^4 + 4691x^2 - 9$ is irreducible over $\mathbb{Q}$. Hence the degree of β is 6, which contradicts to $\beta \in \mathbb{Q}(\alpha)$.

There's another way (and more efficient way) to show this. When we show that u is a fundamental unit, we proved that it can't be a square by reduction it mod 11. Similarly, from $29 | f(10)$, we get a homomorphism $\mathcal{O}_K \to \mathbb{F}_{29}$ that sends α to 10. Under this map, $16\alpha + 25$ maps to $185 = 11 \in \mathbb{F}_{29}$, which is a quadratic nonresidue. Hence $16\alpha + 25$ can't be a square.

Hence we get $[\mathfrak{p}_3] \neq [\mathfrak{p}_3']$. As a result, $\mathrm{Cl}(K) \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ with generators $[\mathfrak{p}_3] = [(3, \alpha - 1)]$ and $[\mathfrak{p}_3'] = [(3, \alpha)]$.

References

[1] K. Conrad, *Class Group Calculations*, `http://www.math.uconn.edu/~kconrad/blurbs/gradnumthy/classgpex.pdf`.

[2] K. Conrad, *Dirichlet's Unit Theorem*, `http://www.math.uconn.edu/~kconrad/blurbs/gradnumthy/unittheorem.pdf`.

[3] D. A. Marcus, *Number fields*, Springer, 1977.

[4] J. Neukirch, *Algebraic number theory*, Springer, 1999.

[5] Y. H. Ng, Answer to the question *noncyclic class group example of a cubic field*, `https://math.stackexchange.com/questions/2949653/noncyclic-class-group-example-of-a-cubic-number-field/2949882#2949882`

[6] E. Weisstein, *Pell's Equation*, `http://mathworld.wolfram.com/PellEquation.html`, Wolfram Mathworld.