CLASS GROUP CALCULATIONS

KEITH CONRAD

1. Introduction

The Minkowski bound says, for a number field K, that each ideal class contains an integral ideal with norm bounded above by

$$\frac{n!}{n^n}\left(\frac{4}{\pi}\right)^{r_2}\sqrt{|\operatorname{disc}(K)|}.$$

In particular, the ideal class group is generated by the prime ideals with norm not exceeding this bound.

We will use the Minkowski bound to compute class groups of some quadratic and cubic number fields. (The computation of class *numbers*, rather than class *groups*, can be obtained by analytic methods. If the class number is prime, then of course the class group is cyclic, but we don't know the class group right away from knowing the class number is, say, 4.) The Minkowski bound specializes in the case of quadratic fields to the following formulas: $(1/2)\sqrt{|\operatorname{disc}(K)|}$ in the real quadratic case ($n = 2$, $r_2 = 0$) and $(2/\pi)\sqrt{|\operatorname{disc}(K)|}$ in the imaginary quadratic case ($n = 2$, $r_2 = 1$).

For a nonzero ideal $\mathfrak{a}$ in $\mathcal{O}_K$, its ideal class will be denoted $[\mathfrak{a}]$ and we write $\sim$ for the equivalence relation on ideals that leads to the class group: $\mathfrak{a} \sim \mathfrak{b}$ means $\mathfrak{b} = \gamma\mathfrak{a}$ for some $\gamma \in K^\times$. We'll usually write $\mathfrak{a} \sim (1)$ as $\mathfrak{a} \sim 1$. Keep in mind the distinction between equality of ideals and equality of ideal classes. For example, if $\mathfrak{a}^2 \sim 1$ and $\mathfrak{a}\mathfrak{b} \sim 1$, this implies $\mathfrak{a} \sim \mathfrak{b}$ (so $\mathfrak{a} = \gamma\mathfrak{b}$ for some γ), *not* $\mathfrak{a} = \mathfrak{b}$.

2. Quadratic fields

Example 2.1. When the Minkowski bound is less than 2, the class group is trivial. For the real quadratic case, the bound is less than 2 when $|\operatorname{disc}(K)| < 16$. For the imaginary quadratic case, the bound is less than 2 when $|\operatorname{disc}(K)| < \pi^2$.

This tells us the following quadratic fields have class number 1: $\mathbf{Q}(\sqrt{2})$, $\mathbf{Q}(\sqrt{3})$, $\mathbf{Q}(\sqrt{5})$, $\mathbf{Q}(\sqrt{13})$, $\mathbf{Q}(i)$, $\mathbf{Q}(\sqrt{-2})$, $\mathbf{Q}(\sqrt{-3})$, and $\mathbf{Q}(\sqrt{-7})$. There are other real and imaginary quadratic fields with class number 1, but the Minkowski bound in the other cases is not less than 2, so we need extra work to show the class number is 1.

Example 2.2. Let $K = \mathbf{Q}(\sqrt{82})$. We will show the class group is cyclic of order 4.

Here $n = 2$, $r_2 = 0$, $\operatorname{disc}(K) = 4 \cdot 82$, so the Minkowski bound is ≈ 9.055. We look at the primes lying over 2, 3, 5, and 7.

The following table describes how (p) factors from the way $T^2 - 82$ factors modulo p.

p	$T^2 - 82 \bmod p$	(p)
2	T^2	$\mathfrak{p}_2^2$
3	$(T-1)(T+1)$	$\mathfrak{p}_3\mathfrak{p}_3'$
5	irred.	prime
7	irred.	prime

Thus, the class group of $\mathbf{Q}(\sqrt{82})$ is generated by $[\mathfrak{p}_2]$ and $[\mathfrak{p}_3]$, with $\mathfrak{p}_2^2 = (2) \sim (1)$ and $\mathfrak{p}_3' \sim \mathfrak{p}_3^{-1}$.

Since $\mathrm{N}_{K/\mathbf{Q}}(10 + \sqrt{82}) = 18 = 2 \cdot 3^2$, and $10 + \sqrt{82}$ is not divisible by 3, $(10 + \sqrt{82})$ is divisible by just one of $\mathfrak{p}_3$ and $\mathfrak{p}_3'$. Let $\mathfrak{p}_3$ be that prime, so $(10 + \sqrt{82}) = \mathfrak{p}_2\mathfrak{p}_3^2$. Thus $\mathfrak{p}_2 \sim \mathfrak{p}_3^{-2}$, so the class group of K is generated by $[\mathfrak{p}_3]$ and we have the formulas

$$[\mathfrak{p}_2]^2 = 1, \quad [\mathfrak{p}_3]^2 = [\mathfrak{p}_2].$$

Therefore $[\mathfrak{p}_3]$ has order dividing 4.

We will show $\mathfrak{p}_2$ is nonprincipal, so $[\mathfrak{p}_3]$ has order 4, and thus K has a class group $\langle[\mathfrak{p}_3]\rangle \cong \mathbf{Z}/4\mathbf{Z}$.

If $\mathfrak{p}_2 = (a + b\sqrt{82})$, then $a^2 - 82b^2 = \pm 2$, so 2 or -2 is $\equiv \Box \bmod 41$. This is no contradiction, since $2 \equiv 17^2 \bmod 41$. We need a different idea.

The idea is to use the known fact that $\mathfrak{p}_2^2$ is principal. If $\mathfrak{p}_2 = (a + b\sqrt{82})$, then $(2) = \mathfrak{p}_2^2 = ((a + b\sqrt{82})^2)$, so

$$2 = (a + b\sqrt{82})^2 u,$$

where u is a unit.

Taking norms here $\mathrm{N}(u)$ must be positive, so $\mathrm{N}(u) = 1$. The unit group of $\mathbf{Z}[\sqrt{82}]$ is $\pm(9 + \sqrt{82})^{\mathbf{Z}}$, with $9 + \sqrt{82}$ having norm -1. Therefore the positive units of norm 1 are the integral powers of $(9 + \sqrt{82})^2$, which are all squares. A unit square can be absorbed into the $(a + b\sqrt{82})^2$ term, so we have to be able to solve $2 = (a + b\sqrt{82})^2$ in integers a and b. This is absurd: it implies $\sqrt{2}$ lies in $\mathbf{Z}[\sqrt{82}]$, which is false. Thus, $\mathfrak{p}_2$ is not principal.

Example 2.3. Let $K = \mathbf{Q}(\sqrt{-14})$. We will show the class group is cyclic of order 4.

Here $n = 2, r_2 = 1$, and $\mathrm{disc}(K) = -56$. The Minkowski bound is ≈ 4.764, so the class group is generated by primes dividing (2) and (3). The following table shows how (2) and (3) factor in $\mathcal{O}_K$ based on how $T^2 + 14$ factors modulo 2 and modulo 3.

p	$T^2 + 14 \bmod p$	(p)
2	T^2	$\mathfrak{p}_2^2$
3	$(T-1)(T+1)$	$\mathfrak{p}_3\mathfrak{p}_3'$

Since $\mathfrak{p}_2^2 \sim 1$, $\mathfrak{p}_2 \sim \mathfrak{p}_2^{-1}$. Since $\mathfrak{p}_3\mathfrak{p}_3' \sim 1$, $\mathfrak{p}_3' \sim \mathfrak{p}_3^{-1}$. Therefore the class group of K is generated by $[\mathfrak{p}_2]$ and $[\mathfrak{p}_3]$.

Both $\mathfrak{p}_2$ and $\mathfrak{p}_3$ are nonprincipal, since they have norm 2 and 3 but the equations $a^2 + 14b^2 = 2$ and $a^2 + 14b^2 = 3$ have no integral solutions.

To find relations between $\mathfrak{p}_2$ and $\mathfrak{p}_3$, we use $\mathrm{N}_{K/\mathbf{Q}}(2 + \sqrt{-14}) = 18 = 2 \cdot 3^2$. The ideal $(2 + \sqrt{-14})$ is divisible by only one of $\mathfrak{p}_3$ and $\mathfrak{p}_3'$, since $2 + \sqrt{-14}$ is not a multiple of 3. Without loss of generality, we may let $\mathfrak{p}_3$ be the prime of norm 3 dividing $(2 + \sqrt{-14})$. Then $\mathfrak{p}_2\mathfrak{p}_3^2 \sim 1$, so

$$\mathfrak{p}_3^2 \sim \mathfrak{p}_2^{-1} \sim \mathfrak{p}_2,$$

so the class group of K is generated by $[\mathfrak{p}_3]$. Since $\mathfrak{p}_2$ is nonprincipal and $\mathfrak{p}_2^2 \sim 1$, $[\mathfrak{p}_3]$ has order 4. Thus, the class group of K is cyclic of order 4.

Example 2.4. Let $K = \mathbf{Q}(\sqrt{-30})$. We will show the class group is a product of two cyclic groups of order 2.

Here $n = 2, r_2 = 1$, and $\mathrm{disc}(K) = -120$. The Minkowski bound is ≈ 6.97, so the class group is generated by primes dividing 2, 3, and 5.

The following table shows how these primes factor into prime ideals.

p	$T^2 + 30 \bmod p$	(p)
2	T^2	$\mathfrak{p}_2^2$
3	T^2	$\mathfrak{p}_3^2$
5	T^2	$\mathfrak{p}_5^2$

For $a, b \in \mathbf{Z}$, $\mathrm{N}_{K/\mathbf{Q}}(a + b\sqrt{-30}) = a^2 + 30b^2$ is never 2, 3, or 5. Therefore $\mathfrak{p}_2$, $\mathfrak{p}_3$, and $\mathfrak{p}_5$ are nonprincipal, so their ideal classes have order 2 in the class group of K. Moreover, since $\mathrm{N}_{K/\mathbf{Q}}(\sqrt{-30}) = 30 = 2 \cdot 3 \cdot 5$, $(\sqrt{-30}) = \mathfrak{p}_2\mathfrak{p}_3\mathfrak{p}_5$. Thus $\mathfrak{p}_2\mathfrak{p}_3\mathfrak{p}_5 \sim 1$, in the class group, so $[\mathfrak{p}_2]$ and $[\mathfrak{p}_3]$ generate the class group.

The relation $\mathfrak{p}_2\mathfrak{p}_3\mathfrak{p}_5 \sim 1$ in the class group can be rewritten as

$$[\mathfrak{p}_2][\mathfrak{p}_3] = [\mathfrak{p}_5]^{-1} = [\mathfrak{p}_5].$$

Since $\mathfrak{p}_5$ is nonprincipal and $[\mathfrak{p}_2]$ and $[\mathfrak{p}_3]$ have order 2 in the class group, $[\mathfrak{p}_2] \neq [\mathfrak{p}_3]$. Therefore the class group of K is $\langle [\mathfrak{p}_2], [\mathfrak{p}_3] \rangle \cong \langle [\mathfrak{p}_2] \rangle \times \langle [\mathfrak{p}_3] \rangle \cong \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$.

Example 2.5. Let $K = \mathbf{Q}(\sqrt{79})$. We will show the class group is cyclic of order 3. (This is the first real quadratic field $\mathbf{Q}(\sqrt{d})$, ordered by squarefree d, with a class number greater than 2.)

Here $n = 2, r_2 = 0$, and $\mathrm{disc}(K) = 4 \cdot 79$. The Minkowski bound is ≈ 8.88, so the class group is generated by primes dividing 2, 3, 5, and 7. The following table shows how these primes factor in $\mathcal{O}_K$.

p	$T^2 - 79 \bmod p$	(p)
2	$(T-1)^2$	$\mathfrak{p}_2^2$
3	$(T+1)(T-1)$	$\mathfrak{p}_3\mathfrak{p}_3'$
5	$(T+2)(T-2)$	$\mathfrak{p}_5\mathfrak{p}_5'$
7	$(T+3)(T-3)$	$\mathfrak{p}_7\mathfrak{p}_7'$

Therefore the class group is generated by $[\mathfrak{p}_2]$, $[\mathfrak{p}_3]$, $[\mathfrak{p}_5]$, and $[\mathfrak{p}_7]$.

Here is a table that factors $|\,\mathrm{N}_{K/\mathbf{Q}}(a + \sqrt{79})|$ for a running from 1 to 10.

a	$\lvert\,\mathrm{N}_{K/\mathbf{Q}}(a + \sqrt{79})\rvert$
1	$2 \cdot 3 \cdot 13$
2	$3 \cdot 5^2$
3	$2 \cdot 5 \cdot 7$
4	$3^2 \cdot 7$
5	$2 \cdot 3^3$
6	43
7	$2 \cdot 3 \cdot 5$
8	$3 \cdot 5$
9	2
10	$3 \cdot 7$

From $a = 9$, we see $\mathfrak{p}_2 = (9 + \sqrt{79}) \sim 1$. From $a = 8$ and $a = 10$, $[\mathfrak{p}_5]$ and $[\mathfrak{p}_7]$ are equal to $[\mathfrak{p}_3]$ or $[\mathfrak{p}_3'] = [\mathfrak{p}_3]^{-1}$. Therefore the class group of K is generated by $[\mathfrak{p}_3]$.

Consider now $a = 5$. Since $5 + \sqrt{79}$ has absolute norm $2 \cdot 27$ and is not divisible by 3, $(5 + \sqrt{79})$ is only divisible by one of $\mathfrak{p}_3$ or $\mathfrak{p}_3'$. Without loss of generality, let $\mathfrak{p}_3$ be that prime, so $(5 + \sqrt{79}) = \mathfrak{p}_2\mathfrak{p}_3^3 \sim \mathfrak{p}_3^3$. Thus, the class group is either trivial or cyclic of order 3.

We will show $\mathfrak{p}_3$ is not principal, so the class group is cyclic of order 3. Our method will be similar to work in Example 2.2. In particular, we need knowledge of the unit group $\mathcal{O}_K^\times$.

Assuming $\mathfrak{p}_3$ is principal, say $\mathfrak{p}_3 = (\alpha)$ for some $\alpha \in \mathbf{Z}[\sqrt{79}]$, we have

$$\begin{aligned}(\alpha^3) &= \mathfrak{p}_3^3 \\ &= (5+\sqrt{79})\mathfrak{p}_2^{-1} \\ &= (5+\sqrt{79})(9+\sqrt{79})^{-1} \\ &= (-17+2\sqrt{79}).\end{aligned}$$

Thus

$$\alpha^3 = (-17+2\sqrt{79})u, \tag{2.1}$$

where u is a unit in $\mathbf{Z}[\sqrt{79}]$. We want to show (2.1) is impossible for all $u \in \mathbf{Z}[\sqrt{79}]^\times$.

In (2.1), changing u by a unit cube doesn't affect solvability of the equation since we can absorb that unit into a change in α. Therefore we can focus on (2.1) where u runs through representatives of the units modulo cubes. A fundamental unit of $\mathbf{Z}[\sqrt{79}]$ is

$$\varepsilon = 80 + 9\sqrt{79}.$$

and modulo cubes of units (note ±1 are both cubes) we have the representatives $u = 1$, ε, and ε^{-1}. (It may seem more natural to use ε^2 instead of ε^{-1}, which are equal modulo unit cubes. The inverse ε^{-1} leads to smaller coefficients in the calculations below.) By a direct calculation,

$$(-17+2\sqrt{79})\varepsilon = 62+7\sqrt{79}, \quad (-17+2\sqrt{79})\varepsilon^{-1} = -2782+313\sqrt{79}.$$

Therefore if (2.1) is possible in $\mathbf{Z}[\sqrt{79}]$ for some α and unit u, one of the three numbers

$$-17+2\sqrt{79}, \quad 62+7\sqrt{79}, \quad -2782+313\sqrt{79} \tag{2.2}$$

is α^3 for some α in $\mathbf{Z}[\sqrt{79}]$. Here are two methods of showing none of these numbers is a cube.

Method 1. Writing $\alpha = a + b\sqrt{79}$ for unknown integers a and b,

$$\alpha^3 = a(a^2 + 3\cdot 79b^2) + b(3a^2+79b^2)\sqrt{79}.$$

Taking ideal norms in the hypothetical equation $(a+b\sqrt{79}) = \mathfrak{p}_3$, $|a^2-79b^2| = 3$, so both a and b are nonzero. Therefore the coefficient $b(3a^2+79b^2)$ of $\sqrt{79}$ in α^3 is, in absolute value, at least $3+79 = 82$. So α^3 can't equal $-17+2\sqrt{79}$ or $62+7\sqrt{79}$ in (2.2).

The remaining option is $\alpha^3 = -2782+313\sqrt{79}$, so

$$b(3a^2+79b^2) = 313,$$

which is a prime number. Thus b, which must be positive by this equation and is less than $3a^2+79b^2$, has to be 1, so $a^2 = (313-79)/3 = 78$, which is impossible.

Method 2. To prove the three numbers in (2.2) are not cubes in $\mathbf{Z}[\sqrt{79}]$, we will show they are not cubes in $\mathbf{Z}[\sqrt{79}]/\mathfrak{p}$ for some prime ideals $\mathfrak{p}$. We need this residue field not to consist entirely of cubes, so we want $3 \mid (\mathrm{N}(\mathfrak{p})-1)$: $\mathrm{N}(\mathfrak{p}) \equiv 1 \bmod 3$. We'll use prime ideals of norm 7 and 43, which both split in $\mathbf{Z}[\sqrt{79}]$ and are 1 mod 3.[1]

Since $T^2 - 79 \equiv (T+3)(T-3) \bmod 7$ and $T^2-79 \equiv (T+6)(T-6) \bmod 43$, we have $(7) = \mathfrak{p}_7\mathfrak{p}_7'$ and $(13) = \mathfrak{p}_{43}\mathfrak{p}_{43}'$, where

$$\sqrt{79} \equiv 3 \bmod \mathfrak{p}_7, \quad \sqrt{79} \equiv -3 \bmod \mathfrak{p}_7', \quad \sqrt{79} \equiv 6 \bmod \mathfrak{p}_{43}, \quad \sqrt{79} \equiv -6 \bmod \mathfrak{p}_{43}'. \tag{2.3}$$

[1] The prime 13 is also split in $\mathbf{Z}[\sqrt{79}]$ and 1 mod 3, but it turns out not to be useful for us.

Using these values, in the table below we compute the numbers in (2.2) modulo $\mathfrak{p}_7$ or $\mathfrak{p}_{43}$, for which the residue fields are uniquely isomorphic to $\mathbf{Z}/7\mathbf{Z}$ and $\mathbf{Z}/43\mathbf{Z}$.

$\mathfrak{p}$	$-17+2\sqrt{79} \bmod \mathfrak{p}$	$62+7\sqrt{79} \bmod \mathfrak{p}$	$-2782+313\sqrt{79} \bmod \mathfrak{p}$
$\mathfrak{p}_7$	3		5
$\mathfrak{p}_{43}$		18	

In $\mathbf{Z}/7\mathbf{Z}$, 3 and 5 are not cubes, so $-17+2\sqrt{79} \bmod \mathfrak{p}_7$ and $-2782+313\sqrt{79} \bmod \mathfrak{p}_7$ are not cubes. In $\mathbf{Z}/43\mathbf{Z}$, 18 is not a cube, so $62+7\sqrt{79} \bmod \mathfrak{p}_{43}$ is not a cube. Thus none of the numbers in (2.2) is a cube in $\mathbf{Z}[\sqrt{79}]$.

Example 2.6. Let $K = \mathbf{Q}(\sqrt{-65})$. We will show its class group is isomorphic to $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/4\mathbf{Z}$.

The Minkowski bound is $(4/\pi)\sqrt{65} \approx 10.26$, so we should factor 2, 3, 5, and 7 in $\mathcal{O}_K = \mathbf{Z}[\sqrt{-65}]$. From the following table, the class group is generated by $[\mathfrak{p}_2]$, $[\mathfrak{p}_3]$, and $[\mathfrak{p}_5]$.

p	$T^2+65 \bmod p$	(p)
2	$(T+1)^2$	$\mathfrak{p}_2^2$
3	$(T+1)(T+2)$	$\mathfrak{p}_3\mathfrak{p}_3'$
5	T^2	$\mathfrak{p}_5^2$
7	T^2+65	(7)

If we factor $\mathrm{N}(a+\sqrt{-65}) = a^2+65$ for small a, looking for only factors of 2, 3, and 5, then we get examples at $a=4$ and $a=5$.

a	a^2+65
1	$3\cdot 11$
2	$3\cdot 23$
3	$2\cdot 37$
4	3^4
5	$2\cdot 3^2\cdot 5$

Since $(4+\sqrt{-65})$ is not divisible by (3), the ideal $(4+\sqrt{-65})$ is divisible by only one of the prime factors of (3). Choose $\mathfrak{p}_3$ as that prime, so

$$(4+\sqrt{-65}) = \mathfrak{p}_3^4.$$

Then

$$(5+\sqrt{-65}) = \mathfrak{p}_2\mathfrak{p}_3'^2\mathfrak{p}_5,$$

so the class group is generated by $[\mathfrak{p}_2]$ and $[\mathfrak{p}_3]$.

Since $\mathfrak{p}_2^2 = (2)$ and $\mathfrak{p}_3^4 = (4+\sqrt{-65})$, $[\mathfrak{p}_2]^2 = [1]$ and $[\mathfrak{p}_3]^4 = [1]$. The ideal $\mathfrak{p}_2$ is nonprincipal, since there is no integral solution to the equation $2 = x^2+65y^2$. The only integral solution to $9 = x^2+65y^2$ is $x = \pm 3$ and $y = 0$, so if $\mathfrak{p}_3^2$ were principal then $\mathfrak{p}_3^2 = (3) = \mathfrak{p}_3\mathfrak{p}_3'$, and that is false ($\mathfrak{p}_3 \neq \mathfrak{p}_3'$). Therefore $[\mathfrak{p}_2]$ has order 2 and $[\mathfrak{p}_3]$ has order 4. Can $[\mathfrak{p}_3]^2 = [\mathfrak{p}_2]$? If so, then $[\mathfrak{p}_2\mathfrak{p}_3^2] = [\mathfrak{p}_2]^2 = [1]$, so $\mathfrak{p}_2\mathfrak{p}_3^2$ is principal. But $18 = x^2+65y^2$ has no integral solution. Therefore $\langle[\mathfrak{p}_2]\rangle$ and $\langle[\mathfrak{p}_3]\rangle$ intersect trivially, so the class group is

$$\langle[\mathfrak{p}_2],[\mathfrak{p}_3]\rangle \cong \langle[\mathfrak{p}_2]\rangle \times \langle[\mathfrak{p}_3]\rangle \cong \mathbf{Z}/2\mathbf{Z}\times\mathbf{Z}/4\mathbf{Z}.$$

3. Cubic fields

Example 3.1. Let $K = \mathbf{Q}(\sqrt[3]{2})$. We will show its class group trivial.

Since $\mathcal{O}_K = \mathbf{Z}[\sqrt[3]{2}]$ and $r_2 = 1$, the Minkowski bound is $(6/27)(4/\pi)\sqrt{108} \approx 2.94$, so we should factor (2) into prime ideals in $\mathcal{O}_K$. We have $(2) = (\sqrt[3]{2})^3$, so $(\sqrt[3]{2})$ is a prime ideal of norm 2, so the only prime ideal of norm less than 2.94 is principal and thus $h(K) = 1$.

Example 3.2. Let $K = \mathbf{Q}(\sqrt[3]{3})$. We will show its class group trivial.

Since $\mathcal{O}_K = \mathbf{Z}[\sqrt[3]{3}]$ and $r_2 = 1$, the Minkowski bound is $(6/27)(4/\pi)\sqrt{243} \approx 4.41$, so we should factor (2) and (3) into prime ideals in $\mathcal{O}_K$.

p	$T^3 - 3 \bmod p$	(p)
2	$(T+1)(T^2+T+1)^2$	$\mathfrak{p}_2\mathfrak{p}_4$
3	T^3	$\mathfrak{p}_3^3$

By the table, there is one prime ideal of norm 2 and one of norm 3. These are $(-1+\sqrt[3]{3})$ and $(\sqrt[3]{3})$ since $-1+\sqrt[3]{3}$ has minimal polynomial $(T+1)^3-3 = T^2+3T^2+3T-2$ with constant term -2 and $\sqrt[3]{3}$ has minimal polynomial $T^3 - 3$ with constant term -3. Since $(2) = \mathfrak{p}_2\mathfrak{p}_4$ with $\mathfrak{p}_2$ being principal, $\mathfrak{p}_4$ is principal too. (Explicitly, $\mathfrak{p}_4 = (2/(-1+\sqrt[3]{3})) = (1+\sqrt[3]{3}+\sqrt[3]{9})$.) Thus all prime ideals of norm less than 4.41 are principal, so $h(K) = 1$.

Remark 3.3. The first pure cubic fields $\mathbf{Q}(\sqrt[3]{d})$ with nontrivial class group are $\mathbf{Q}(\sqrt[3]{7})$ and $\mathbf{Q}(\sqrt[3]{11})$, which have class numbers 3 and 2, respectively.

Example 3.4. Let $K = \mathbf{Q}(\alpha)$, where α is a root of $T^3 - T - 9$. This polynomial is irreducible mod 2, so it's irreducible over $\mathbf{Q}$: K is a cubic field. We will show the class group of K has order 2.

The discriminant of $T^3 - T - 9$ is $-4(-1)^3 - 27(-9)^2 = -2183 = -37 \cdot 59$, which is squarefree, so $\mathcal{O}_K = \mathbf{Z}[\alpha]$ and $\operatorname{disc}(K) = -2183$. The polynomial $T^3 - T - 9$ has one real root, so $r_2 = 1$ and the Minkowski bound is $(6/27)(4/\pi)\sqrt{2183} \approx 13.21$. The table below gives us factorizations of (p) for all primes $p \leq 13$.

p	$T^3 - T - 9 \bmod p$	(p)
2	irred.	prime
3	$T(T-1)(T-2)$	$\mathfrak{p}_3\mathfrak{p}_3'\mathfrak{p}_3''$
5	$(T-3)(T^2+3T+3)$	$\mathfrak{p}_5\mathfrak{p}_{25}$
7	irred.	prime
11	$(T-8)(T^2+8T+8)$	$\mathfrak{p}_{11}\mathfrak{p}_{121}$
13	irred.	prime

From this table the class group of K is generated by $[\mathfrak{p}_3]$, $[\mathfrak{p}_3']$, $[\mathfrak{p}_3'']$, $[\mathfrak{p}_5]$, and $[\mathfrak{p}_{11}]$. To get relations among these ideal classes we will factor $(a+\alpha)$ for some small integers a. The ideal norm is $(a+\alpha)$ is $|\operatorname{N}_{K/\mathbf{Q}}(a+\alpha)|$, which up to sign is the constant term of the minimal polynomial of $a+\alpha$. That minimal polynomial is $(T-a)^3 - (T-a) - 9$, whose constant term is $-a^3 + a - 9 = -(a^3 - a + 9)$, so $|\operatorname{N}_{K/\mathbf{Q}}(a+\alpha)| = |a^3 - a + 9|$.

a	$\lvert a^3 - a + 9\rvert\rvert$
0	3^2
1	3^2
-1	3^2
2	$3 \cdot 5$
-2	3
3	$3 \cdot 11$

From the first three rows in the table above, the ideals (α), $(\alpha+1)$, and $(\alpha-1)$ all have norm 9. They are pairwise relatively prime, since the generators differ by ± 1 and 2, so we can set

$$(\alpha) = \mathfrak{p}_3^2, \quad (\alpha+1) = \mathfrak{p}_3'^2, \quad (\alpha-1) = \mathfrak{p}_3''^2. \tag{3.1}$$

Since $(\alpha - 2)$ has norm 3 and $\alpha - 2 \equiv \alpha + 1 \equiv 0 \bmod \mathfrak{p}_3'$, $\mathfrak{p}_3' = (\alpha - 2)$, so $[\mathfrak{p}_3'] = [1]$.

From the table above and the congruences $\alpha + 2 \equiv \alpha - 1 \equiv 0 \bmod \mathfrak{p}_3''$ and $\alpha + 3 \equiv \alpha \equiv 0 \bmod \mathfrak{p}_3$, we have prime ideal factorizations

$$(\alpha+2) = \mathfrak{p}_3''\mathfrak{p}_5, \quad (\alpha+3) = \mathfrak{p}_3\mathfrak{p}_{11},$$

so in the class group of K, $[\mathfrak{p}_5] = [\mathfrak{p}_3'']^{-1}$ and $[\mathfrak{p}_{11}] = [\mathfrak{p}_3]^{-1}$. Therefore the class group of K is generated by $[\mathfrak{p}_3]$ and $[\mathfrak{p}_3'']$. Since the factorization $(3) = \mathfrak{p}_3\mathfrak{p}_3'\mathfrak{p}_3'' = \mathfrak{p}_3(\alpha-2)\mathfrak{p}_3''$ implies $[\mathfrak{p}_3][\mathfrak{p}_3''] = [1]$, the class group of K is generated by $[\mathfrak{p}_3]$. We have $[\mathfrak{p}_3]^2 = [1]$ by (3.1), so $h(K)$ is 1 or 2. To show the class number of K is 2, we'll show $\mathfrak{p}_3$ is nonprincipal.

Assume $\mathfrak{p}_3$ is principal, say $\mathfrak{p}_3 = (\beta)$ for some $\beta \in \mathbf{Z}[\alpha]$. Then $(\beta^2) = \mathfrak{p}_3^2 = (\alpha)$, so

$$\beta^2 = \alpha u \tag{3.2}$$

for a unit $u \in \mathbf{Z}[\alpha]^\times$. We want to show (3.2) is impossible, and we will do this by following the second method of proving the impossibility of (2.1): we will show $\alpha u \bmod \mathfrak{p}$ is not a square for some prime ideal $\mathfrak{p}$ and all units u.

As in Example 2.5, we need information about the unit group of $\mathbf{Z}[\alpha]$. First let's find a nontrivial unit. Because $\mathfrak{p}_3' = (\alpha - 2)$ and $\mathfrak{p}_3'^2 = (\alpha + 1)$, we have the equation of principal ideals

$$(\alpha + 1) = ((\alpha - 2)^2).$$

Therefore $v := (\alpha-2)^2/(\alpha+1)$ is a unit and $v \neq \pm 1$ since the numerator of v is quadratic in α and the denominator of v is linear in α and $1, \alpha, \alpha^2$ are linearly independent over $\mathbf{Q}$.

Fact: $\mathbf{Z}[\alpha]^\times/\{\pm 1\}$ is infinite cyclic: for a unit ε of infinite order, $\mathbf{Z}[\alpha]^\times = \pm\varepsilon^{\mathbf{Z}}$.

This fact is a special case of Dirichlet's unit theorem. The easier part of the proof of that theorem shows $\mathbf{Z}[\alpha]^\times/\{\pm 1\}$ is either trivial or infinite cyclic, so the fact that we found a unit v besides ± 1 in the cubic field K forces $\mathbf{Z}[\alpha]^\times/\{\pm 1\}$ to be infinite cyclic without needing to rely on the full proof of Dirichlet's unit theorem. It also turns out that in the above fact we can use v for ε, but we will *not* need this.

If (3.2) has a solution β and u, then u only matters modulo unit squares (changing u by a unit square changes β by a unit), so to prove (3.2) is impossible we can focus on (3.2) where u runs over representatives for the units modulo unit squares. From the structure of $\mathbf{Z}[\alpha]^\times$, the unit squares are $\varepsilon^{2\mathbf{Z}}$, so a set of representatives for the units modulo unit squares is ± 1 and $\pm\varepsilon^k$ where k is odd.

In the fact above, we can replace ε by $-\varepsilon$, so without loss of generality $\varepsilon > 0$ under the real embedding of K, which makes the positive units of $\mathbf{Z}[\alpha]$ equal to $\varepsilon^{\mathbf{Z}}$. The unique real root of $T^3 - T - 9$ is positive (it's around 2.24), so the real embedding of K maps α to a positive number (around 2.24) and thus also $v = (\alpha-2)^2/(\alpha+1)$ to a positive number, so $v \in \varepsilon^{\mathbf{Z}}$ by the fact above. We will show v is an *odd* power of ε by showing v is not a square.

In $\mathbf{Z}[\alpha]/\mathfrak{p}_3''$, $\alpha \equiv 1 \bmod \mathfrak{p}_3'$, so $v = (\alpha-2)^2/(\alpha+1) \equiv 1/2 \equiv 2 \bmod \mathfrak{p}_3''$. This is not a square since $\mathbf{Z}[\alpha]/\mathfrak{p}_3'' \cong \mathbf{Z}/3\mathbf{Z}$ and 2 is not a square mod 3. Thus v is not a square in $\mathbf{Z}[\alpha]$, so $v = \varepsilon^k$ where k is odd, and that makes $\pm 1, \pm v$ a set of representatives for the units of $\mathbf{Z}[\alpha]$ modulo unit squares. The impossibility of solving (3.2) is therefore equivalent to none of the four numbers $\pm\alpha$ and $\pm\alpha v$ being squares in $\mathbf{Z}[\alpha]$, and we'll prove this by showing they are not squares in $\mathbf{Z}[\alpha]/\mathfrak{p}_5$.

Recall $\mathfrak{p}_5$ is a prime ideal of norm 5, with $\alpha \equiv 3 \bmod \mathfrak{p}_5$. That makes $v = (\alpha-2)^2/(\alpha+1) \equiv 1/4 \equiv -1 \bmod \mathfrak{p}_5$, so $\pm\alpha \equiv \pm 3 \bmod \mathfrak{p}_5$ and $\pm\alpha v \equiv \mp 3 \bmod \mathfrak{p}_5$. In the field $\mathbf{Z}[\alpha]/\mathfrak{p}_5 \cong \mathbf{Z}/5\mathbf{Z}$, 3 and -3 are not squares. Hence $\pm\alpha$ and $\pm\alpha v$ are not squares in $\mathbf{Z}[\alpha]/\mathfrak{p}_5$ and thus also in $\mathbf{Z}[\alpha]$. This completes the proof that (3.2) is impossible, so $\mathfrak{p}_3$ is not principal.

The examples we looked at here with nontrivial class groups are $\mathbf{Q}(\sqrt{-14})$, $\mathbf{Q}(\sqrt{-30})$, $\mathbf{Q}(\sqrt{-65})$, $\mathbf{Q}(\sqrt{79})$, $\mathbf{Q}(\sqrt{82})$, and $\mathbf{Q}(\alpha)$, where $\alpha^3 - \alpha - 9 = 0$. In each of these cases we had to show certain ideals are not principal, and this was much simpler for the imaginary quadratic fields than for the other examples. That is because the only units in the imaginary quadratic fields are ± 1, while there are infinitely many units in $\mathbf{Z}[\sqrt{79}]$, $\mathbf{Z}[\sqrt{82}]$, and $\mathbf{Z}[\alpha]$. An important lesson is that to compute the ideal class group when it is nontrivial, you need to understand the unit group, and this gets delicate when the unit group is infinite.