CLASS GROUP CALCULATIONS

KEITH CONRAD

The Minkowski bound says, for a number field K, that any 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 various quadratic 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 any 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 $\mathfrak{ab} \sim 1$, this implies $\mathfrak{a} \sim \mathfrak{b}$ (so $\mathfrak{a} = \gamma\mathfrak{b}$ for some γ), *not* $\mathfrak{a} = \mathfrak{b}$.

Example 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. 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 $\mathbf{Z}[\sqrt{82}]$. Thus, $\mathfrak{p}_2$ is not principal.

Example 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 $\operatorname{disc}(K) = -56$. 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 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 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 $\operatorname{disc}(K) = -120$. 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 $[\mathfrak{p}_5]$ each 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, in the class group, $\mathfrak{p}_2\mathfrak{p}_3\mathfrak{p}_5 \sim 1$, 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 a product of two cyclic groups of order 2.

Example 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 $[\mathfrak{p}_3]^{-1}$. 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 now show $\mathfrak{p}_3$ is not principal, so the class group is cyclic of order 3. Our method will be similar to the work with $\mathbf{Q}(\sqrt{82})$. In particular, we need knowledge of the unit group.

Assuming $\mathfrak{p}_3 = (\alpha)$, 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

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

where u is a unit in $\mathbf{Z}[\sqrt{79}]$. A fundamental unit of $\mathbf{Z}[\sqrt{79}]$ is

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

Since α can be changed by a unit cube without affecting the ideal (α^3), we may assume $u = 1, \varepsilon$, or 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.) Negative signs on units can be absorbed into α^3. By a direct calculation,

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

Writing $\alpha = a + b\sqrt{79}$ for unknown integers a and b, we have

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

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 $3 + 79 = 82$. Thus it is impossible to have α^3 equal $-17 + 2\sqrt{79}$ or $(-17+2\sqrt{79})\varepsilon$.

If $\alpha^3 = -2782 + 313\sqrt{79}$, then we must have

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

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 $a^2 = 78$, which is impossible. We have a contradiction, so $\mathfrak{p}_3$ is not principal.

Example 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

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