B3.4 Algebraic Number Theory, Hilary 2020

Exercises 4

In many of these solutions it is worth having to hand the following data. The Minkowski bound is $\frac{1}{2}\sqrt{|\Delta_K|}$ (real quadratic case) and $\frac{2}{\pi}\sqrt{|\Delta_K|}$ (imaginary quadratic case). The descriminant Δ_K, $K = \mathbb{Q}(d)$, is $4d$ if $d \equiv 2, 3 (\mathrm{mod}\, 4)$ and d if $d \equiv 1 (\mathrm{mod}\, 4)$.

Question 1. Find all quadratic fields for which the Minkowski bound is strictly less than 2. What is the class number of these fields?

Solution 1. The full list is $\mathbb{Q}(\sqrt{d})$ where $d = 2, 3, 5, 13$ (real fields) and $d = -1, -2, -3, -7$ (imaginary fields). It follows immediately from Minkowski's theorem that all these fields have class number 1.

Question 2. Show that $\mathrm{Cl}(K)$ is cyclic of order two, where $K = \mathbb{Q}(\sqrt{-37})$.

Solution 2. Since $d \equiv 3 (\mathrm{mod}\, 4)$, $\mathcal{O}_K = \mathbb{Z}[\sqrt{-37}]$ and $\Delta_K = -148$. Therefore $M_K = \frac{2}{\pi}\sqrt{148}$ which, whilst it is less than 11, is sadly a little bigger than 7. Thus generators of $\mathrm{Cl}(K)$ may be found amongst the (ideal) prime factors of $(2), (3), (5)$ and (7). Dealing with this seems, in the light of the last example, as if it could be a formidable challenge. However, this turns out not to be the case.

The minimal polynomial $m(X)$ for $\sqrt{-37}$ is $X^2 + 37$.

Over $\mathbb{F}_2$ this factors as $(X + 1)^2$, so by Dedekind $(2) = \mathfrak{p}^2$ where $\mathfrak{p} = (2, 1 + \sqrt{-37})$ is not principal, and has norm 2.

Over $\mathbb{F}_3$ this is irreducible, since $-37 \equiv -1$ is not a quadratic residue modulo 3. Thus by Dedekind (3) is itself prime (that is, 3 is inert)

Over $\mathbb{F}_5$ it is also irreducible, since $-37 \equiv 3$ is not a quadratic residue modulo 5. Thus by Dedekind, 5 is inert.

Over $\mathbb{F}_7$ it is also irreducible, since $-37 \equiv 5$ is not a quadratic residue modulo 7. Again, by Dedekind 7 is inert.

From the above analysis, it follows straight away that $\mathrm{Cl}(K)$ is cyclic of order two and generated by $[\mathfrak{p}]$.

Question 3. Find $\mathrm{Cl}(K)$, where $K = \mathbb{Q}(\sqrt{-6})$.

Solution 3. This is a quadratic field $\mathbb{Q}(\sqrt{d})$ with $d = 6$. Since $d \equiv 2 (\mathrm{mod}\, 4)$, $\mathcal{O}_K = \mathbb{Z}[\sqrt{-6}]$ and $\Delta_K = -24$. Therefore $M_K = \frac{2}{\pi}\sqrt{24}$ which is definitely less than 5 (but, it turns out, not less than 3). Thus generators of $\mathrm{Cl}(K)$ may be found amongst the (ideal) prime factors of (2) and (3).

The minimal polynomial $m(X)$ for $\sqrt{-6}$ is $X^2 + 6$.

Over $\mathbb{F}_2$ this factors as X^2, so by Dedekind we have $(2) = \mathfrak{p}^2$ where $\mathfrak{p} = (2, \sqrt{-6})$ has norm 2.

Over $\mathbb{F}_3$ this also factors as X^2, so by Dedekind we have $(3) = \mathfrak{q}^2$ where $\mathfrak{q} = (3, \sqrt{-6})$ has norm 3.

Neither $\mathfrak{p}$ nor $\mathfrak{q}$ is principal, since $\mathbf{N}_{K/\mathbb{Q}}(a+b\sqrt{-6}) = a^2+6b^2$ and so there are no elements in $\mathcal{O}_K$ of norm 2 or 3. Therefore, by very simple group theory, $\mathrm{Cl}(K)$ is either C_2 (cyclic of order 2) or $C_2 \times C_2$, and we can decide between these by deciding whether or not $[\mathfrak{p}] = [\mathfrak{q}]$. To do this, note that $\mathfrak{pq}$ contains $2\sqrt{-6}$ and $3\sqrt{-6}$, and hence $\sqrt{-6}$, and so $(\sqrt{-6}) \subseteq \mathfrak{pq}$. The norm of either side is 6, so in fact $(\sqrt{-6}) = \mathfrak{pq}$ and so $[\mathfrak{p}] \sim [\mathfrak{q}]^{-1} \sim [\mathfrak{q}]$ (this last statement follows since $\mathfrak{q}^2$ is principal). Therefore $\mathrm{Cl}(K)$ is cyclic of order 2 and $h_K = 2$.

Question 4. Let K be a number field, other than $\mathbb{Q}$. Show that $\Delta_K > 1$.

Solution 4. Recall Minkowski's theorem, that every ideal class in $\mathcal{O}_K$ contains an ideal $\mathfrak{a}$ with $N(\mathfrak{a}) \leqslant M_K := (\frac{4}{\pi})^{r_2} \frac{n!}{n^n} \sqrt{|\Delta_K|}$. Thus, we must certainly have $M_K \geqslant 1$ and so

$$\Delta_K \geqslant (\frac{\pi}{4})^{2r_2} (\frac{n^n}{n!})^2 \geqslant (\frac{\pi}{4})^n (\frac{n^n}{n!})^2.$$

We claim this is always > 1. For this, we will need some simple bounds on factorials. Noting that $x(n-x) \leqslant (n/2)^2$, we see upon taking products over $x = 1, \ldots, n-1$ that $(n-1)! \leqslant (n/2)^{n-1}$, and so $n! \leqslant 2(n/2)^n$. Substituting into the bounds above gives

$$\Delta_K \geqslant (\frac{\pi}{4})^n 4^n \frac{1}{4} = \frac{1}{4}\pi^n,$$

which is obviously > 1 for all $n \geqslant 2$. (Students could create a bit more work for themselves here by using less appropriate bounds for factorials.)

Question 5. Find $\mathrm{Cl}(K)$, where $K = \mathbb{Q}(\sqrt{-34})$.

Solution 5. The Minkowski bound is $\frac{4}{\pi}\sqrt{34} < 8$. Thus we only need consider primes $\leqslant 7$. The minimal polynomial is $X^2 + 34$, and the ring of integers is $\mathbb{Z}[\sqrt{-34}]$. Applying Dedekind gives

Mod 2: $(2) = (2, \sqrt{-34})^2 = \mathfrak{p}_2^2$, where $\mathfrak{p}_2$ has norm 2 and is not principal (since $2 \neq a^2 + 34b^2$ is not the norm of any element).

Mod 3: $X^2 + 34 = X^2 - 2$ is irreducible, so (3) is inert.

Mod 5: $X^2 + 34 = X^2 - 1 = (X-1)(X+1)$, so $(5) = (5, -1+\sqrt{-34})(5, 1+\sqrt{-34}) = \mathfrak{p}_5\mathfrak{p}_5'$ say. Neither of these ideals is principal.

Mod 7: $X^2 + 34 = (X-1)(X+1)$ so $(7) = (7, -1+\sqrt{-34})(7, 1+\sqrt{-34}) = \mathfrak{p}_7\mathfrak{p}_7'$.

Now let's look in more detail at the prime 5. Note that the only elements of norm 25 are ± 5, and the ideal (5) is not $\mathfrak{p}_5^2$, since it is $\mathfrak{p}_5\mathfrak{p}_5'$ as we have seen. An easy check shows that there is no element of norm 125. So $\mathfrak{p}_5^3$ is not principal either. Note, however, that $\mathbf{N}_{K/\mathbb{Q}}(9+4\sqrt{-34}) = \mathbf{N}_{K/\mathbb{Q}}(9-4\sqrt{-34}) = 625 = 5^4$.

We claim that $9 \pm 4\sqrt{-34}$ are coprime. In the ideal generated by both of these elements, we have 18 and $8\sqrt{-34}$ and hence $8 \times 34 = 272$, and hence $272 - (15 \times 18) = 2$. Then we have $9 = (9 + 4\sqrt{-34}) - (2 \times 2\sqrt{-34})$ and hence, finally 1.

Since $(5) = \mathfrak{p}_5\mathfrak{p}_5'$, one of $(9 \pm 4\sqrt{-34})$ must be $\mathfrak{p}_5^4$, and the other $\mathfrak{p}_5'^4$. Thus $[\mathfrak{p}_5]$ has order 4 in the ideal class group.

Finally, we show that the classes of $[\mathfrak{p}_2], [\mathfrak{p}_7]$, are in the group generated by $[\mathfrak{p}_5]$.

For $[\mathfrak{p}_2]$, observe that

$$\mathbf{N}_{K/\mathbb{Q}}(4+\sqrt{-34}) = 50 = 2 \cdot 5^2,$$

so $(4+\sqrt{-34})$ factors as a product of an ideal of norm 2 (either $\mathfrak{p}_2$ or $\mathfrak{p}_2'$) times two ideals of norm 5. Either way, $[\mathfrak{p}_2]$ is in the group generated by $[\mathfrak{p}_5]$.

For $[\mathfrak{p}_7]$, observe that

$$\mathbf{N}_{K/\mathbb{Q}}(1+\sqrt{-34}) = 35 = 5 \times 7$$

and argue very similarly.

Conclusion: the class group is generated by $[\mathfrak{p}_5]$ and so is cyclic of order 4.

Question 6. Find $\mathrm{Cl}(K)$, where $K = \mathbb{Q}(\sqrt{65})$.

Solution 6. $d \equiv 1 (\mathrm{mod}\, 4)$, and this is a real quadratic field, so the Minkowski bound M_K is $\frac{1}{2}\sqrt{65}$ which is a tiny amount bigger than 4, but certainly less than 5. Thus we can find generators for $\mathrm{Cl}(K)$ from amongst the prime factors of (2) and (3). $\mathcal{O}_K$ has a power integral basis $\mathbb{Z}[\frac{1+\sqrt{65}}{2}]$, and the minimal polynomial of the generator is $X^2 - X - 16$.

Modulo 2, this factors as $X(X+1)$, so we have $(2) = \mathfrak{p}_2\mathfrak{p}_2'$ where $\mathfrak{p}_2 = (2, \frac{1+\sqrt{65}}{2})$, $\mathfrak{p}_2' = (2, \frac{-1+\sqrt{65}}{2})$, and both these ideals have norm 2. We claim neither is principal. Indeed, if they were, then for some $a, b \in \mathbb{Z}$ we would have to have $N(a+b(\frac{1+\sqrt{65}}{2})) = (a+\frac{b}{2})^2 - 65(\frac{b}{2})^2 = \pm 2$, whence $x^2 - 65y^2 = \pm 8$ for some $x, y \in \mathbb{Z}$. This is impossible, working modulo 5.

Modulo 3, the minimial polynomial is $X^2 - X - 1$, which is irreducible. Thus (3) is inert.

The conclusion then is that $\mathrm{Cl}(\mathbb{Q}(\sqrt{65})) \cong \mathbb{Z}/2\mathbb{Z}$, with a generator being $[\mathfrak{p}_2]$ (or $[\mathfrak{p}_2']$).

Remark. Because the course does not include a discussion of units in real quadratic fields, we do not really have the tools for class group calculations in them unless favourable accidents occur, as here. Students should be told more about units if time allows.

Question 7. Find all integer solutions to the equation $y^2 + 74 = x^3$. (You may assume that $h_{\mathbb{Q}(\sqrt{-74})}) = 10$.)

Solution 7. Factor the equation as $(y+\sqrt{-74})(y-\sqrt{-74}) = (x)^3$. We first claim that the two factors are coprime. Any common ideal prime factor $\mathfrak{p}$ must divide $2\sqrt{-74}$.

Suppose first that $\mathfrak{p}|2$. By Dedekind, the prime factorisation of (2) is $(2, \sqrt{-74})^2$. Therefore $\mathfrak{p}|(\sqrt{-74})$, and so $\mathfrak{p}|(y)$; but this means, taking norms, that $2|y$. Then $x^3 \equiv 2 (\mathrm{mod}\, 4)$, which is a contradiction.

Suppose then that $\mathfrak{p}|(\sqrt{-74})$ but $\mathfrak{p} \nmid 2$. Thus we must have $\mathfrak{p}|(37)$ and $N\mathfrak{p} = 37$. As before, $\mathfrak{p}|(y)$. Taking norms, we see that $37|y$. But then we

quickly get a contradiction by looking at the original equation, since 37 will have to divide both x and y and thus 37^2 divides y^2, x^3 and hence 37, a contradiction.

Thus we have an ideal equation $\mathfrak{ab} = (x)^3$, where $\mathfrak{a}, \mathfrak{b}$ are coprime. This implies (by unique factorisation into prime ideals) that $\mathfrak{a}, \mathfrak{b}$ are themselves cubes of other ideals, $\mathfrak{a} = \mathfrak{a}'^3$, $\mathfrak{b} = \mathfrak{b}'^3$. Moreover we know that $[\mathfrak{a}']^3[\mathfrak{b}']^3$ is trivial in the ideal class group. Since this class group has size 10, $[\mathfrak{a}'], [\mathfrak{b}']$ must also be trivial in this group, thus we have

$$(y + \sqrt{-74}) = (a + \sqrt{-74}b)^3$$

for some integers a, b. Comparing coefficients gives

$$y = a^3 - 222ab^2,$$

$$1 = 3a^2b - 74b^3.$$

Factoring the second of these leads to $b = \pm 1$. With $b = 1$ we have $3a^2 = 75$, which implies $a = \pm 5$. With $b = -1$ we get no solution. Thus we get the value

$$y = \pm(5^3 - 222 \times 5) = \pm 985,$$

which then gives the value $x = 99$. (One can get x without a calculator by noting it must be $a^2 + 74b^2$.)

Question 8. Show that the ring of integers in $\mathbb{Q}(2^{1/3})$ is a principal ideal domain (any results about this field established on previous sheets may be used without proof).

Solution 8. We use the fact that $\mathcal{O}_K = \mathbb{Z}[\alpha]$, where $\alpha = 2^{1/3}$, and that $\Delta_K = -108$; both of these facts were established on Sheet 1. K has one real embedding and one pair of complex conjugate embeddings, so the Minkowski bound is $\frac{4}{\pi}\frac{6}{27}\sqrt{108} \approx 2.94\ldots$. Thus we only need check that (2) splits as a product of principal prime ideals. But this is clear, since $(2) = (2^{1/3})^3$, and $(2^{1/3})$ is an ideal of norm two so must be prime.

Question 9. (i) Let Λ be a lattice in $\mathbb{R}^2$ which has no nonzero vector x with $\|x\| \leqslant 1$. Show that $\det(\Lambda) \geqslant \frac{1}{2}\sqrt{3}$.

(ii) Deduce a (small) improvement to the Minkowski bound for imaginary quadratic fields.

(iii) Briefly comment on the implications for the Rabinowicz phenomenon.

Solution 9. (i) Let v be a nonzero vector of shortest length. Then $v = ae_1 + be_2$ (where e_1, e_2 is some integral basis) and we must have a, b coprime, since otherwise $\frac{1}{\gcd(a,b)}v$ would lie in Λ, and this vector is obviously shorter. Set $w = ce_1 + de_2$ with $ad - bc = 1$; then v, w are an integral basis for Λ, because we have transformed by a matrix in $\mathrm{SL}_2(\mathbb{Z})$.

By shrinking (if necessary) and rotating Λ, we may assume that v is in fact the standard basis vector e_1. Now note that every vector in Λ other than

multiples of e_1 has y coordinate $|y| \geqslant \frac{1}{2}\sqrt{3}$: if $(x, y) \in \Lambda$ then we can find $(x', y) \in \Lambda$ with $|x'| \leqslant \frac{1}{2}$ by subtracting appropriate multiples of e_1. Suppose that $w = (x, y)$. Then $\det(\Lambda) = |\begin{vmatrix} 1 & 0 \\ x & y \end{vmatrix}| = |y| \geqslant \frac{1}{2}\sqrt{3}$, as required.

(ii) Recall the discussion of the Minkowski bound for imaginary quadratic field in lectures. The key lemma there was an application of Blichfeldt's lemma with the ball of radius $\sqrt{R}$, leading to the conclusion that if $\pi R \geqslant 4\det(\Lambda)$ then the ball of radius $\sqrt{R}$ contains a nonzero point of Λ. But now we can do better: consider $\Lambda' := \frac{1}{\sqrt{R}}\Lambda$, which has $\det(\Lambda') = \frac{1}{R}\det(\Lambda)$. By (i), Λ' either has a nonzero vector of length $\leqslant 1$ or else $\det(\Lambda') \geqslant \frac{1}{2}\sqrt{3}$. So if $\det(\Lambda) < \frac{1}{2}\sqrt{3}R$, the ball of radius $\sqrt{R}$ contains a nonzero point of Λ. Applying this in the proof of the Minkowski bound, we see that $M'_K = \sqrt{|\Delta_K|/3}$ is a bound which works for imaginary quadratic fields. (Note that $2/\pi \approx 0.637$, $1/\sqrt{3} \approx 0.577$.)

(iii) Working through Section 11.4 of the notes almost verbatim, one gets that if $x^2 + x + a$ is prime for all $x \leqslant \sqrt{a/3}$, then $x^2 + x + a$ is prime for x up to $a - 2$. (The main point of my mentioning this is that it was Question 6 at the IMO in 1987; I had always assumed that one could do this via the Minkowski bound, but it turns out that the Minkowski bound is not quite sharp enough, even for imaginary quadratic fields. Of course there is an "elementary" solution to the IMO question.)

ben.green@maths.ox.ac.uk