Math 129 HW 7

Bryden Cais

April 9, 2002

1. Suppose that $p \leq \frac{-d_K}{4}$. We know that

$$\left\{1, \frac{d_K + \sqrt{d_K}}{2}\right\}$$

is an integral basis for $\mathcal{O}_K$, so that if $\mathrm{N}(x) = p$ for some $x \in \mathcal{O}_K$, then we would have

$$\begin{aligned} p &= \mathrm{N}\left(a + b\left(\frac{d_K + \sqrt{d_K}}{2}\right)\right) \\ &= \left(a + \frac{bd_K}{2}\right)^2 + b^2\frac{-d_K}{4}. \end{aligned}$$

Since $p \leq \frac{-d_K}{4}$, it follows that we in fact have equality, $b = \pm 1$, $d_K = -4p$, and $a = -2bp$.

2. Suppose that $\mathcal{O}_K$ is principal.

   (a) Suppose that $p < \frac{-d_K}{4}$ splits in $\mathcal{O}_K$ as $p = Q_1 Q_2$ for Q_1, Q_2 not necessarily distinct primes. Then we have $Q_1 = (x)$ for some $x \in \mathcal{O}_K$ since $\mathcal{O}_K$ is principal and therefore $\mathrm{N}(x) = p$, contradicting problem 1. Therefore p is inert.

   (b) Suppose that $-d_K > 8$. Part a then tells us that 2 is inert since $2 < -d_K/4$. Therefore 2 does not ramify so that $2 \not| d_K$ which implies that $d_K = d$ and $d \equiv 1 \mod 4$. Therefore, $d \equiv 1$ or $5 \mod 8$. We know that $\mathcal{O}_K = \mathbf{Z}[\frac{1+\sqrt{d}}{2}]$, and therefore that 2 splits if $d \equiv 1 \mod 8$ since the minimal polynomial of $\frac{1+\sqrt{d}}{2}$ is

$$X^2 - X + \frac{1-d}{4},$$

which splits as $X(X-1) \mod 2$. Now if $-d$ is not prime then there exists some $p < \sqrt{-d}$ dividing d_K. This implies that p ramifies in $\mathcal{O}_K$, that is $p = Q^2$. Since $-d > 8$ and $-d \equiv 3 \mod 8$ by the above, we have $-d > 16$ (since we are assuming that d is not prime) and theresore that $\sqrt{-d} < -d_K/4$. Then $p < -d_K/4$ and $p = Q^2$, which contradicts part a. Therefore, $-d$ is prime.

(c) Suppose that $-d_K \geq 28$. Since we have shown that $d_K = d \equiv 5 \mod 8$, we in fact have $-d_K > 28$ so that $7 < -d_K/4$. By part a, the primes $3, 5, 7$ are inert in K. That is, the polynomial

$$X^2 - X + \frac{1-d}{4}$$

is irreducible modulo $3, 5, 7$. From this, we obtain the requirements

$$\begin{aligned} -d &\equiv 1 \mod 3 \\ -d &\equiv 2, 3 \mod 5 \\ -d &\equiv 1, 2, 4 \mod 7. \end{aligned}$$

We combine the first congruence with the requirement that $-d \equiv 3 \mod 8$ from above to obtain

$$\begin{aligned} -d &\equiv 19 \mod 24 \\ -d &\equiv 2, 3 \mod 5 \\ -d &\equiv 1, 2, 4 \mod 7. \end{aligned}$$

The chinese remainder theorem gives a unique solution modulo $2^3 \cdot 3 \cdot 5 \cdot 7 = 840$ to each of the six systems of congruences above. A short computation shows that $-d$ is congruent modulo 840 to one of

$$43, 67, 163, 403, 547, 667.$$

3. Here we shall use the Minkowski bound. We have that every ideal of $\mathcal{O}_K$ is equivalent to some ideal J with

$$\mathrm{N}(J) \leq \lfloor \frac{2}{\pi} \sqrt{|d_K|} \rfloor = \lambda.$$

For $d = -1, -2, -3, -7$ we have $d_K = -4, -8, -3, -7$ and therefore that $\lambda = 2$, so that $\mathcal{O}_K$ is clearly principal for these values of d. For $d = -11, -19$ we have $\lambda = 2$. Since 2 is inert in $\mathcal{O}_K$ by 2b, we see that 2 cannot be the norm of any ideal and therefore every ideal of $\mathcal{O}_K$ is equivalent to some ideal of norm 1; i.e. $\mathcal{O}_K$ is principal for these values of d also. For $d = -43$, we obtain $\lambda = 4$. Since it is enough to check that no ideal has prime norm (since such ideals generate the classgroup), we need only consider the possibilities $\mathrm{N}(J) = 2, 3$. We rule out the first right away using 2b and since $X^2 - X + \frac{1+43}{4} \equiv X^2 - X + 2 \mod 3$ is irreducible, we see that 3 is inert and rule out the second possibility. We then conclude that $\mathcal{O}_K$ is principal. Similarly, for $d = -67$, we need only consider the behavior of $X^2 - X + 17$ modulo $3, 5$. It is readily seen that this polynomial is irreducible in both cases, so that $3, 5$ are inert in $\mathcal{O}_K$ and hence, as before, that $\mathcal{O}_K$ is principal. Finally, we conquer $d = -163$. Minkowski gives $\lambda = 8$ so that we must check the behavior of $X^2 - X + 41$ modulo $3, 5, 7$. We find that this polynomial is irreducible for each modulus, and therefore that $3, 5, 7$ are inert and cannot be the norms of any ideals. Therefore, every $\mathcal{O}_K$ ideal is equivalent to some ideal of norm 1; that is, $\mathcal{O}_K$ is principal.

4. Let's take $N = 909$. We have shown that if $\mathcal{O}_K$ is principal and $-d_K > 28$ then $-d \equiv 43, 67, 163, 403, 547, 667 \mod 840$. We have also shown that $\mathcal{O}_K$ is principal for $-d = 1, 2, 3, 7, 11, 19, 43, 67, 163$. This leaves the values $-d = 5, 6, 403, 547, 667, 883, 907$. When $-d = 5, 6$ we have $-d_K = 20, 24$ respectively so that by 2c we must have $-d_K = d$, which rules out the possibility of principality of $\mathcal{O}_K$ for these values of d. Observe that we have the following factorizations:

$$\begin{aligned}
X^2 - X + 101 &\equiv (X+4)(X+6) \mod 11 \\
X^2 - X + 137 &\equiv (X+2)(X+8) \mod 11 \\
X^2 - X + 167 &\equiv (X+4)(X+6) \mod 11 \\
X^2 - X + 221 &\equiv X(X-1) \mod 13 \\
X^2 - X + 227 &\equiv (X+4)(X+8) \mod 13.
\end{aligned}$$

This shows that 11 is not inert in $\mathcal{O}_K$ for $-d = 403, 547, 667$, so that by 2a, since $11 < -d/4$, we see that $\mathcal{O}_K$ is not principal for these values of d. Similarly, 13 is not inert in $\mathcal{O}_K$ for $-d = 883, 907$ and hence $\mathcal{O}_K$ is not principal for these values of d either. We have shown that the only $-d$ in the range [1,909] for which $\mathcal{O}_K$ is principal are those listed in problem 3.

5. We now compute $\mathrm{Cl}(\mathcal{O}_K)$ for $-d = 6, 14, 21, 23$.

   (a) $-d = 6$. Using Minkowski, we find that every $\mathcal{O}_K$ ideal is equivalent to some ideal J with $\mathrm{N}(J) \leq 3$. Since $-6 \equiv 2 \mod 4$, we have $\mathcal{O}_K = \mathbf{Z}[\sqrt{-6}]$. Since $2, 3$ divide 6, both primes ramify and we find

   $$\begin{aligned} (2) &= (2, \sqrt{-6})^2 = P_2^2 \\ (3) &= (3, \sqrt{-6})^2 = P_3^2. \end{aligned}$$

   Since $(2, \sqrt{-6})(2, \sqrt{-6}) = (\sqrt{-6})$ is principal, we have $[P_2] = [P_3]^{-1}$ where $[P]$ denotes, as usual, the image of P in $\mathrm{Cl}(\mathcal{O}_K)$. Therefore, $\mathrm{Cl}(\mathcal{O}_K)$ is generated by $[P_2]$, and since P_2^2 is principal, we have $[P_2]^2 = [1]$. Therefore,

   $$\mathrm{Cl}(\mathcal{O}_K) \simeq \mathbf{Z}/2\mathbf{Z}.$$

   (b) $-d = 14$. Again, by Minkowski, we find that every $\mathcal{O}_K$ ideal is equivalent to some ideal J with $\mathrm{N}(J) \leq 4$. Since $-14 \equiv 2 \mod 4$, we have $\mathcal{O}_K = \mathbf{Z}[\sqrt{-6}]$. We look at the polynomial $X^2 + 14$ modulo $2, 3$ to determine the factorizations

   $$\begin{aligned} (2) &= (2, \sqrt{-14})^2 = P_2^2 \\ (3) &= (3, \sqrt{-14} - 1)(3, \sqrt{-14} + 1) = P_3 \bar{P}_3. \end{aligned}$$

   Notice that $(2 + \sqrt{-14})(2 - \sqrt{-14}) = 2 \cdot 3^2 = P_2^2 (P_3 \bar{P}_3)^2$. Using the fact that $(2 + \sqrt{-14})$ and $(2 - \sqrt{-14})$ are conjugate, we find that up to relabeling we have the factorization

   $$(2 + \sqrt{-14}) = P_2 P_3^2,$$

   which shows that $[P_3]^2 = [P_2]$. We already know that $P_2^2 = (2)$ is principal, hence that $[P_2]^2 = [1]$. Therefore, $\mathrm{Cl}(\mathcal{O}_K)$ is generated by $[P_3]$, which is of order 4. This shows that

   $$\mathrm{Cl}(\mathcal{O}_K) \simeq \mathbf{Z}/4\mathbf{Z}.$$

(c) $-d = 21$. Minkowski shows that we must only consider the behavior of the primes $2, 3, 5$ in $\mathcal{O}_K$. From the factorizations of $X^2 + 21$ modulo $2, 3, 5$, we find

$$\begin{aligned}
(2) &= (2, \sqrt{-21} - 1)^2 = P_2^2 \\
(3) &= (3, \sqrt{-21})^2 = P_3^2 \\
(5) &= (5, \sqrt{-21} + 2)(5, \sqrt{-21} - 2) = P_5\bar{P}_5.
\end{aligned}$$

From the fact that $(3+\sqrt{-21})(3-\sqrt{-21}) = 2 \cdot 3 \cdot 5$, we see (again using the fact that $(3 + \sqrt{-21})$ and $(3 - \sqrt{-21})$ are conjuagte), that

$$(3 + \sqrt{-21}) = P_2P_3P_5,$$

up to relabeling and units. At any rate, we see that $P_2P_3P_5$ is principal so that $[P_5] = [P_2P_3]^{-1}$. Notice that this implies that $[P_2] \neq [P_3]^{\pm 1}$ since then P_5 would be principal, which it clearly is not (by considering norms: $5 \neq a^2 + 21b^2$ for any integers a, b). In summary, we have shown that $\mathrm{Cl}(\mathcal{O}_K)$ is generated by $[P_2], [P_3]$ with the relations $[P_2]^2 = [P_3]^2 = 1$, and $[P_2], [P_3]^{\pm 1}$ distinct. Therfore,

$$\mathrm{Cl}(\mathcal{O}_K) \simeq \mathbf{V}_4,$$

the Klein–four group.

(d) $-d = 23$. Using Minkowski, we find that every $\mathcal{O}_K$ ideal is equivalent to some ideal J with $\mathrm{N}(J) \leq 3$. In this case, $\mathcal{O}_K = \mathbf{Z}[\frac{1+\sqrt{-23}}{2}] := \mathbf{Z}[\alpha]$, and we look at the irreducible polynomial

$$X^2 - X + \frac{1 + 23}{4} = X^2 - X + 6$$

modulo $2, 3$. This gives the factorizations

$$\begin{aligned}
(2) &= (2, \alpha)(2, \alpha - 1) = P_2\bar{P}_2 \\
(3) &= (3, \alpha)(3, \alpha - 1) = P_3\bar{P}_3.
\end{aligned}$$

Since $\frac{1+\sqrt{-23}}{2}\frac{1-\sqrt{-23}}{2} = 6$ and the two factors are conjugate, we must have

$$\left(\frac{1 + \sqrt{-23}}{2}\right) = P_2P_3$$

up to relabeling. Therefore, $\mathrm{Cl}(\mathcal{O}_K)$ is generated by $[P_2]$. Now, the factorization

$$\frac{3+\sqrt{-23}}{2}\frac{3-\sqrt{-23}}{2} = 2^3$$

tells us that

$$\left(\frac{3+\sqrt{-23}}{2}\right) = P_2^3$$

up to relabeling and units (it cannot be that only a single or double power of P_2 divides $\frac{3+\sqrt{-23}}{2}$, for then we would have $\left(\frac{3+\sqrt{-23}}{2}\right) = P_2^2\bar{P}_2$, up to relabeling, which is impossible since $[P_2]^2[\bar{P}_2] = [P_2]$ is not principal). Therefore, $[P_2]^3 = 1$ so that $[P_2]$ must have order 3. It follows that

$$\mathrm{Cl}(\mathcal{O}_K) \simeq \mathbf{Z}/3\mathbf{Z}.$$

6. Let $d \equiv 1, 2 \mod 4$ be a positive square free integer greater than 4, so that $\mathcal{O}_K = \mathbf{Z}[\sqrt{-d}]$, and suppose that 3 does not divide $|\,\mathrm{Cl}(\mathcal{O}_K)|$. Consider the equation

$$y^2 = x^3 - d$$

which we write as

$$(y - \sqrt{-d})(y + \sqrt{-d}) = x^3.$$

Assume that we have some solution with $x, y \in \mathbf{Z}$. We show first that $(y - \sqrt{-d})$ and $(y + \sqrt{-d})$ are relatively prime principal ideals. For let P be a prime ideal containing $(y - \sqrt{-d})$ and $(y + \sqrt{-d})$. Then $2\sqrt{-d} \in P$ and since $P|x^3$ we must have $P|x$ and therefore $x \in P$. This implies that $\mathrm{N}(P)|\,\mathrm{N}(2\sqrt{-d})$ and $\mathrm{N}(P)|\,\mathrm{N}(x)$, that is, $\mathrm{N}(P)|4d$ and $\mathrm{N}(P)|x^2$ (since $x \in Z$). Clearly x cannot be even since then it would be $0 \mod 8$ and $x^3 - d \equiv 2, 3 \mod 4$, neither of which are squares. Therefore x is odd. Furthermore, $(x, d) = 1$ since if they had a common prime factor, its square would divide y^2 so that, since its cube has to divide x^3, d would not be square free. Thus, $N(P) = 1$ and $(y - \sqrt{-d})$ and $(y + \sqrt{-d})$ are relatively prime. Now let Q be any prime ideal factor of (x). Then $Q^3|(y-\sqrt{-d})(y+\sqrt{-d})$ and therefore Q^3 divides one of $(y-\sqrt{-d})$ or $(y+\sqrt{-d})$. Repeating this process for each prime ideal factor of (x), we find that $J^3 = (y+\sqrt{-d})$ for some ideal J. Since $3 \not| |\mathrm{Cl}(\mathcal{O}_K)|$, $\mathrm{Cl}(\mathcal{O}_K)$ contains no elements of order 3, and therefore J must be principal, say $J = (a + b\sqrt{-d})$ with $a, b \in \mathbf{Z}$. Since the only units of $\mathbf{Z}[\sqrt{-d}]$ are ± 1 (we showed this on an earlier homework) we have

$$y + \sqrt{-d} = \pm(a + b\sqrt{-d})^3,$$

which gives the equations

$$\begin{aligned} y &= \pm a(a^2 - 3db^2) \\ 1 &= \pm b(3a^2 - b^2 d) \end{aligned}$$

from which we obviously have $b = \pm 1$ and $d = 3a^2 \pm 1$. Notice that $d = 5$ has $\mathrm{Cl}(\mathcal{O}_K) \simeq \mathbf{Z}/2\mathbf{Z}$ and therefore satisfies all of our hypotheses on d but that 5 is not of the form $3a^2 \pm 1$ for any integer a. Therefore, the equation $y^2 = x^3 - 5$ has no integer solutions.

7. Let $K = \mathbf{Q}(\sqrt[3]{19})$ and put $R = \mathcal{O}_K$. In an earlier Marcus excercise, we computed a basis for the ring of integers of a pure cubic extension. Using such a result, we determine that an integral basis for R is

$$\left\{1, \alpha, \frac{1 + \alpha + \alpha^2}{3}\right\}$$

where $\alpha = \sqrt[3]{19}$. Using this, it is not difficult to calculate the discriminant of K. It is found to be $-3 \cdot 19^2$. The Minkowski bound is therefore

$$\lambda = \frac{3!}{3^3}\left(\frac{4}{\pi}\right)\sqrt{3 \cdot 19^2} < 10.$$

Marcus kindly tells us that

$$3R = P^2 Q$$

for primes P, Q. We now consider how $2, 5, 7$ split in R. The irreducible polynomial of α is clearly

$$\begin{aligned} X^3 - 19 &\equiv X^3 - 1 \equiv (X-1)(X^2 + X + 1) \mod 2 \\ &\equiv X^3 - 4 \equiv (X+1)(X^2 + 4X + 1) \mod 5 \\ &\equiv X^3 + 2 \mod 7, \end{aligned}$$

where the factors listed above are clearly irreducible. We therefore see that 7 is inert in R while

$$\begin{aligned} 2R &= P_2 Q_2 \\ 5R &= P_5 Q_5 \end{aligned}$$

where Q_2, Q_5 have residual degree 2. In particular, we have a unique primes of norms 2 and 5.

Now it is not difficult to see that

$$\begin{aligned} \mathrm{N}(\alpha - 3) &= -8 \\ \mathrm{N}(\alpha + 1) &= 20 \\ \mathrm{N}(\alpha - 1) &= 18 \\ \mathrm{N}(2\alpha - 5) &= 27 \end{aligned}$$

.

Using the second equality, we find that $(\alpha + 1) = P_5 P_2^2$ or $P_5 Q_2$ up to units. The third equality shows that $(\alpha - 1) = P_2 P^2$ or $P_2 Q^2$ up to units. In either case, since $P^2 Q$ is principal and therefore $[Q] = [P]^{-2}$, we find that $[P_2]$ and hence $[Q_2]$ since $P_2 Q_2 = (2)$ is principal, and hence $[P_5]$, are all powers of $[P]$ so that $[P]$ generates the class group.

Now, using the first equality, we have $P_2^3 = \alpha - 3|$ (up to units) so that, since P_2 is not principal, $\mathrm{Cl}(R)$ contains an element of order 3 and therefore has size divisible by 3. Now both 3 and $(2\alpha - 5)$ have norm 27 so that one of the following factorizations holds:

$$\begin{aligned} 2\alpha - 5 &= P^3 \\ 2\alpha - 5 &= PQ^2 \\ 2\alpha - 5 &= Q^3. \end{aligned}$$

Therefore, in the first two cases, P has order 3, while in the last case it has order 6. Now suppose that $[P]$ has order 6. Then $[Q] = [P]^{-2} = [P]^4$. Similarly, considering the factorizations $(\alpha - 1) = P_2 P^2$ or $P_2 Q^2$, we see that $[P_2] = [P]^4$ in any case. Finally, considering the factorizations $(\alpha + 1) = P_5 P_2^2$ or $P_5 Q_2$, we see that $[P_5] = [P]^4$. By multiplying these ideals together, since each is an even power of P, we see that no ideal J with $\mathrm{N}(J) \leq 9$ is in the same class as P^3. This is impossible by the Minkowski bound since we have assumed that P^3 is not principal. Therefore, there are 3 ideal classes and

$$\mathrm{Cl}(R) \simeq \mathbf{Z}/3\mathbf{Z}.$$

8. Let K be a number field and I an ideal of $R = \mathcal{O}_K$. Since the class group $\mathrm{Cl}(R)$ is finite, some power of I is principal, say $I^m R = \alpha R$ with $\alpha \in R$. Now let $L = K(\sqrt[m]{\alpha})$. Then we certainly have $I^m S = \alpha S = (\sqrt[m]{\alpha} S)^m$. It follows that $I = \sqrt[m]{\alpha} S$ is principal. Clearly, $[L : K] | m$ is finite. Now let $I_1, \ldots, I_k$ be representatives of the equivalence classes of R ideals. We know the list is finite since $\# \mathrm{Cl}(R)$ is finite. We therefore have a finite extension M of K with each $I_j = \alpha_j \mathcal{O}_M$ a principal $\mathcal{O}_M$ ideal. Notice that if $J\tilde{I_j}$ then there exists $\beta \in K$ with $\beta I_j = J$, and consequently $J = \beta \alpha_j \mathcal{O}_M$ is also a principal $\mathcal{O}_M$ ideal. Therefore, every ideal of $\mathcal{O}_K$ is principal in M. As an example, we determine a degree 4 extension of $\mathbf{Q}(\sqrt{-21})$ in which every ideal of $\mathbf{Z}[\sqrt{-21}]$ is principal. We determined above that $\mathrm{Cl}(\mathbf{Z}[\sqrt{-21}]) \simeq \mathbf{V}_4$ is generated by P_2, P_3 with

$$\begin{aligned} P_2^2 &= (2, \sqrt{-21} - 1)^2 = 2 \\ P_3^2 &= (3, \sqrt{-21})^2 = 3. \end{aligned}$$

Notice that if we find an extension of $\mathbf{Q}(\sqrt{-21}])$ in which P_2, P_3 are principal, then every ideal generated by P_2, P_3 will also be principal since these generate the class group. By the above argument, P_2, P_3 are principal in the extension $\mathbf{Q}(\sqrt{-21}, \sqrt{2}, \sqrt{3})$, which is of degree 4 over $\mathbf{Q}(\sqrt{-21})$.

Let $\mathcal{A}$ denote the set of algebraic integers. We show that every finitely generated ideal of $\mathcal{A}$ is principal. Let $I = (a_1, \ldots, a_n)$ be a finitely generated ideal of (A). Let $K = \mathbf{Q}(a_1, \ldots, a_n)$. Then I is an $\mathcal{O}_K$ ideal. Therefore, by the previous problem, there exists a finite extension L of K such that $I\mathcal{O}_L$ is principal, say $I = (\alpha)$. But $\mathcal{O}_L \subset \mathcal{A}$ so that $\alpha \in \mathcal{A}$ and $I = \alpha \mathcal{O}_K$ was principal to begin with. As an example of an ideal of $\mathcal{A}$ that is not finitely generated, consider the ideal I generated by $\sqrt{n}$ for $n = 2, 3, 4, \ldots$. Then I cannot be principal since if $I = (\alpha)$ for some $\alpha \in \mathcal{A}$ then $\sqrt{n} \in \alpha\mathcal{A}$ for every $n \geq 2$ so that $\mathrm{N}(\sqrt{n}) | \mathrm{N}(\alpha)$ for each n. But $\mathrm{N}(\sqrt{n}) = n$, which implies that $\mathrm{N}(\alpha)$ is unbounded. This is impossible and we see that I is not finitely generated since it is not principal.