## 7. Quadratic fields

We now specialise the results of the previous section to the case of extensions of $\mathbb{Q}$ of degree 2. Such a field is of the form $\mathbb{Q}[T]/P(T)$ where $P(T)$ is an irreducible polynomial of degree 2. An order in such a field is generated by 1 and a non-rational element $\alpha$ that satisfies an equation of the type $P(T) = T^2 - bT + c$. Thus every order has the form $R[T]/P(T)$. Now, it is clear that $\mathrm{Trace}(\alpha) = b$ and $\mathrm{Nm}(\alpha) = c$. Moreover, $\mathrm{Trace}(\alpha^2) = \mathrm{Trace}(b\alpha - c) = b^2 - 2c$. Thus the discriminant $D_R$ of $R$ is the determinant of $\left(\begin{smallmatrix} 2 & b \\ b & b^2-2c \end{smallmatrix}\right)$ which is $b^2 - 4c$ (as expected). In particular, we see that $D_R = b^2 \pmod 4$; i. e. the discriminant must be 0 or 1 modulo 4. In the first case, we can replace $\alpha$ by $\alpha + (b-1)/2$ so that we get an element with trace 1. In the second case, we can replace $\alpha$ by $\alpha + b/2$ to get an element with trace 0. Thus we can assume that the equation takes the form $T^2 - T + N$ in the first case and $T^2 + N$ in the second case. An alternative normalisation is to replace $\alpha$ by $\omega_D = (D_R + \sqrt{D_R})/2$ in both cases; this can be done since $D_R + b$ is even in both cases. We thus have a natural basis for $R$. There is also a natural involution on $R$ which sends $\sqrt{D_R}$ to $-\sqrt{D_R}$ or equivalently $\omega_D$ to $D_R - \omega_D$.

### 7.1. **Prime ideals.**

By the earlier analysis, we see that every prime ideal is either ramified (to order 2) or of degree 1 or of degree 2. If the prime lies over 2 then it is not ramified when $D_R$ is odd since, in that case the equation takes the form $T^2 + T$ or $T^2 + T + 1$ modulo 2; both these equations have distinct roots. When $D_R$ is even, the prime over 2 is ramified. When the prime lies over an odd prime $p$, it is clear that the prime is ramified when the discriminant is divisible by $p$. Thus the ramified primes are precisely those that lie over primes $p$ that divide the discriminant. (This is also true for *any* field extension of $\mathbb{Q}$ that is normal in the sense that it contains all the roots of the polynomial that defines it).

If $D_R$ is odd and in the above notation $N$ is even, then the primes lying over 2 and $\mathbb{Z}\cdot 2+\mathbb{Z}\cdot\alpha$ and $\mathbb{Z}\cdot 2+\mathbb{Z}\cdot(1-\alpha)$. When $N$ is odd, then the only prime lying over 2 is $2R$. Now, if $p$ is an odd prime that does not divide the discriminant then either $\mathbb{F}_p[T]/(P(T))$ is isomorphic to $\mathbb{F}_{p^2}$ or it splits into two $\mathbb{F}_p$ factors. The former case occurs when $D_R$ is not a square modulo $p$ and in this case the prime lying over $p$ is just the ideal $pR$; which is principal. In the second case $D_R$ is a square modulo $p$ and we obtain two primes $P_p$ and $Q_p$, lying over $p$; both these have norm $p$ and their product (and intersection) is $pR$. Let $c_p$ be a number between 1 and $p-1$ so that $c_p^2 = D_R \pmod p$; then $a_p = (1 + c_p)/2$ satisfies the equation modulo $p$ in the $D_R$ odd case and $a_p = (c_p)/2$ satisfies the equation modulo $p$ in the $D_R$ even case. Thus we can pick a solution $a_p$ of the equation modulo $p$ in each case and declare that $P_p = \mathbb{Z}\cdot p + \mathbb{Z}\cdot(\alpha - a_p)$. The primes $P_p$ and $Q_p$ are interchanged by the involution.

### 7.2. **Naive computation of the class group.**

As shown earlier, each element of the class group of the order $R$ is represented by an invertible ideal $J$ with $\mathrm{Nm}(J) \leq \delta_R$; here $\delta_R = \sqrt{|D_R|}$ if $D_R > 0$ and $\delta_R = (2/pi)\sqrt{|D_R|}$ if $D_R < 0$. Now, if $\overline{J}$ is the image of $J$ under the involution, then we have seen above (by writing $J$ as a product of primes) that $J \cdot \overline{J} = \mathrm{Nm}\, JR$. Thus the involution acts on the class group by group inversion (which is a group homomorphism for abelian groups!). In particular, we know how to represent inverses in this set of representatives.

From the above discussion we see that one natural set of generators is to pick one prime ideal $P_p$ lying over each split prime $p$ and for each ramified prime $p$. We only need to consider primes satisfying the criterion $p \leq \delta_R$; let $S$ denote the set of such primes. Now we need to write relations. Suppose that $T$ is the (finite) set of all integers $n$ such that (1) $n$ is a multiple of elements of $T$ (2) For each prime divisor $p$ of $n$, $n/p \leq \delta_R$. Each such $n$ can be written uniquely as the norm of an ideal $J_n$ that is a product of the ideals $P_p$. If we find an element $\alpha_n$ in $J_n$ so that $\mathrm{Nm}(\alpha_n) \leq n \cdot \delta_R \cdot$, then $\alpha_n = J_n \cdot I_n$, where $\mathrm{Nm}(I_n) \leq \delta_R$. We can thus write a natural factorisation of the ideal $\alpha_n$ in terms of $P_p$ and $Q_p$. Note that when $n \geq \delta_R$, the existence of such an $\alpha$ is guaranteed by the lemma proved in the previous section. To write these relations, it is sufficient find all numbers less than $\max(T)\delta_R$ which are products of primes in $S$ and write these elements as norms.

Now suppose we have a relation $\prod_{p\in S} P_p^{n_p} = \alpha R$ with $n_p \geq 0$. If $\mathrm{Nm}(\alpha) \geq \delta_R$, then we can find a factor $\prod_{p\in S} P_p^{m_p}$ which has norm $n$ larger than $\delta_R$, but lying in $T$. Then, we can replace the above relation by

$$\overline{I_n} \cdot \prod_{p\in S} P_p^{n_p - m_p} = (\alpha/\alpha_n)\,\mathrm{Nm}(I_n)R$$

Now the left hand side has integral norm and so we have obtained another relation. Moreover, the norm of the left hand side is smaller than the earlier norm. Thus we can always reduce any relation to a product of relations of the type given above.

To write the relations associated with elements of $T$ as above we note that for each $n$ in $T$ we can construct a candidate for $\alpha_n$ as follows. First of all we use Chinese Remainder theorem to find an integer $a_n$ so that $a_n = a_p \pmod{p}$ for every $p$ dividing $n$ (if necessary we can actually use Hensel's lemma to replace $a_p$ by the root of the equation modulo the maximal power of $p$ that divides $n$). Then, elements of the form $x + y\alpha$ are candidates where $y$ is some number less than $n$ and $x$ is the reduction modulo $n$ of $a_n \cdot y$. In addition, we can impose the condition that $x + y\alpha$ lies in a specified region in $\mathbb{R} \cdot K$ with volume $n\delta_R$ (this region is a rectangle in the case $D_R > 0$ and a circle in the case $D_R < 0$). These conditions make the search for $\alpha_n$ effective.

Now the numbers in $T$ could be just short of $\delta_R^2$, so that the norm of $\alpha_n$ could be just short of $\delta_R^3$. This is in general too big a collection of relations to handle. One way to simplify the approach is to make reductions to the set $S$ on the basis of relations found. Thus, if we find that $P_p$ has order $k$ based on relations already found then we do not consider numbers $n$ that are divisible by powers of $p$ larger than $k - 1$. Similarly, if we found a relation expression $P_p$ in terms of smaller primes in the set $S$, then we can drop multiples of $p$ from further choices for $n$ in $T$. Finally, we can use a "Class Number formula" to give an *estimate* in terms of lower and upper bounds for the size of the group. Once we find a group that is the correct range then there are techniques to verify that there are no more relations to be considered.

Thus the techniques described above *could* be used to compute the class group even for large $D_R$. However, the main aim of this section was to show the *possibility* of making the computation. We will need some more effective techniques to deal with finite abelian groups before we can make the computation more efficient.

As a demonstration we now compute the class group of the discriminant 257. The associated polynomial is $T^2 - T - 64$. The initial candidates for the set $S$

consist of the primes $\leq 16$, i. e. the set $\{2, 3, 5, 7, 11, 13\}$. Now, the polynomial becomes $T^2 + T$ modulo 2 so that 2 is split so it is in $S$. Now we have

$$257 \equiv 2 \pmod 3 \qquad \text{and} \qquad 257 \equiv 2 \pmod 5$$

which shows that 3 and 5 are non-split and thus not in $S$. The squares modulo 7 are 1, 4 and 2, while $257 \equiv 5 \pmod 7$; thus 7 is not in $S$ either. We also check that

$$257 \equiv 4 \equiv 2^2 \pmod{11} \qquad \text{and} \qquad 257 \equiv 10 \equiv 6^2 \pmod{13}$$

so that 11 and 13 are in $S$. We then see easily that $T$ is

$$\{22 = 2 \cdot 11, 26 = 2 \cdot 13, 32 = 2^5, 121 = 11^2, 143 = 11 \cdot 13, 169 = 13^2\}$$

We now compute the relations in succession. We lift the above roots $0 \pmod 2$ and $7 \pmod{11}$ (of the equation $T^2 - T - 64$) to the root $18 \equiv -4 \pmod{22}$. Thus a candidate for $\alpha_{22}$ is $\alpha + 4$, which has norm $44 = 2^2 \cdot 11$. Thus we obtain the relation $P_2^2 \cdot P_{11}$. Next we lift the roots $0 \mod 2$ and $10 \mod 13$ to the root $10 \mod 26$. Thus a candidate for $\alpha_{26}$ is $\alpha - 10$ which has norm $26 = 2 \cdot 13$. Thus we obtain the relation $P_2 \cdot P_{13}$. Next we have $\alpha_{32} = \alpha$, which has norm $64 = 2^6$, which gives the relation $P_2^6$. Next, we lift (using Hensel's lemma) the root $7 \pmod{11}$ to the root $18 \pmod{121}$ which gives $\alpha_{121} = \alpha - 18$ which has norm $242 = 2 \cdot 11^2$ so we have a relation $P_2 \cdot P_{11}^2$. Now, we could calculate further but we notice that this says that the class group is a quotient of a group of order 3 that is generated by $P_2$. Since it is clear that this ideal is *not* principal, it follows that the class group in this case *is* $\mathbb{Z}/3\mathbb{Z}$. Note that we did not use the rectangular bounds for the sizes of $\alpha_n$ in this computation since all the numbers were "small" in any case, but in general we would need to use these restrictions as well.

### 7.3. **Binary Quadratic Forms.**

Gauss's approach to ideals (which were not defined in his time!) was to represent elements of the class group (groups were also not defined in his time!) by equivalence classes of quadratic forms. The idea is to make use of the fact that for each ideal $I$ we are actually interested in objects like $\mathrm{Nm}(\alpha)/\mathrm{Nm}(I)$ for some element $\alpha$ in $I$. As seen above, the ideal class is represented by some ideal $J$ with $\mathrm{Nm}(J) = \mathrm{Nm}(\alpha)/\mathrm{Nm}(I)$.

To fix notation, let the quadratic order $R$ be given as $\mathbb{Z} + \mathbb{Z} \cdot \omega$, where $\omega = (D + \sqrt{D})/2$ with $D = D_R$ the discriminant of the order $R$; then $\omega$ satisfies the equation

$$\omega^2 - D \cdot \omega + \frac{D^2 - D}{4} = 0$$

Any non-zero ideal $I$ in $R$ is then of the form $\mathbb{Z} \cdot a + \mathbb{Z} \cdot (b + c\omega)$, where $I \cap \mathbb{Z} = \mathbb{Z} \cdot a$ is the restriction of $I$ to $\mathbb{Z}$; we can assume that $a > 0$. Moreover, by Euclidean division we can subtract a multiple of $a$ from $b$ to ensure that $0 \leq b < a$. Now the fact that $I$ is an ideal gives us

$$\begin{aligned} a \cdot \omega &= p \cdot a + q \cdot (b + c\omega) \\ (b + c\omega) \cdot \omega &= r \cdot a + s \cdot (b + c\omega) \end{aligned}$$

For some integers $p$, $q$, $r$ and $s$. From this we deduce

$$a = qc \qquad \text{and} \qquad 0 = pa + qb$$

$$b + cD = sc \qquad \text{and} \qquad -\frac{D^2 - D}{4} = ra + sb$$

Hence $a = qc$ and $b = -pc$ are multiples of $c$. Moreover, the quadratic expression $b^2+bcD+c^2\frac{D^2-D}{4} = -rac$ is divisible by $ac$. Now, it is clear that $c$ is determined by the condition that $(I+\mathbb{Z})/\mathbb{Z}$ is the subgroup $\mathbb{Z}\cdot(c\omega)$ of $R/\mathbb{Z} \cong \mathbb{Z}\cdot\omega$; or equivalently that $\mathrm{Nm}(I) = ac$, with $a$ determined as before. It follows that any tuple $(a, b, c)$ that satisfies the above conditions uniquely determines an ideal and vice versa.

Now, it is clear that the ideal $c^{-1}I = \mathbb{Z}\cdot q + \mathbb{Z}(-p+\omega)$ is equivalent to $I$ in the class group. Thus, we say the ideal is *primitive* if the representative tuple $(a, b, c)$ satisfies $c = 1$. Clearly, we only need to look at primitive ideals for the purpose of computing the class group; but there are more equivalence relations.

We write a general element of $I$ as $ax + (b + c\omega)y$; its norm is a multiple of $\mathrm{Nm}(I) = ac$. Thus,

$$Q_I(x,y) = \frac{\mathrm{Nm}(ax + (b + c\omega)y)}{\mathrm{Nm}(ac)} = qx^2 + sxy - ry^2$$

(with notation as above) is a form with integer coefficients. Moreover, it is invariant (by construction) under the replacement of $I$ by a rational multiple. We easily check the identity $s^2 + 4qr = D$. Conversely, given any form $Q(x, y) = qx^2 + sxy - ry^2$ satisfying this identity, we note that $s \equiv D \pmod 2$. Thus we can consider the ideal $\mathbb{Z}\cdot q+\mathbb{Z}(s+\sqrt{D})/2$. When $Q(x, y) = Q_I(x, y)$, $s = -2p + D$ so that $(s+\sqrt{D})/2 = -p + \omega$; hence we recover the primitive ideal associated with $I$. However, we not that for a general quadratic form $Q(x, y)$ the integers $q$ and $(s - D)/2$ need not be positive unless we impose this as an additional requirement on the quadratic forms under consideration.

Now, if $I = \mathbb{Z}\cdot u_1 + \mathbb{Z}\cdot u_2$, for some elements $u_1$, $u_2$ in $R$, then the quadratic form $Q_{u_1,u_2}(x,y) = \mathrm{Nm}(xu_1 + yu_2)/\mathrm{Nm}(I)$ is (in general) different from $Q_I(x, y)$. However, it is obtained from $Q_I(x, y)$ by a substitution $(x, y) \mapsto (Ax+By, Cx+Dy)$ where $\left(\begin{smallmatrix} A & B \\ C & D \end{smallmatrix}\right)$ is an integer matrix with integer inverse. One way to obtain a new basis is to consider $I = \alpha\cdot J$ for some ideal $J$ in $R$ and some $\alpha$ in $K$. Then, we write $J = \mathbb{Z}\cdot a' + \mathbb{Z}\cdot(b' + c'\omega)$ as before. Clearly $u_1 = a'\alpha$ and $u_2 = (b' + c'\omega)\alpha$ is another basis of $I$.

Conversely, given a basis $u_1$ and $u_2$ of the ideal $I$, let $d$ be a denominator of $u_2/u_1$; i. e. $d$ is a positive integer so that $du_2/d_1$ lies in $R$. Consider the ideal $J = (d/u_1)\cdot I$, we see that $J = \mathbb{Z}\cdot d + \mathbb{Z}\cdot(du_2/u_1)$ and $J\cap\mathbb{Z} = \mathbb{Z}\cdot d$. Thus, as above we can find $e$ and $f$ so that $0 \le e < d$ and $(du_2/u_1) = nd\pm(e+f\omega)$ for some integer $n$. Thus $J = \mathbb{Z}\cdot d + \mathbb{Z}\cdot(e + f\omega)$. Putting $\alpha = u_1/d$ we see that $u_1 = d\alpha$ and $u_2 = (nd \pm (e + f\omega))\alpha$; in particular, $I = \alpha\cdot J$. Moreover, we have

$$Q_{u_1,u_2}(x,y) = Q_{d,(du_2/u_1)}(x,y) = Q_J(x, nx \pm y)$$

the latter form being clearly equivalent to $Q_J$.

Thus we have shown that $Q_I(x, y)$ and $Q_J(x, y)$ are equivalent under an integer change of co-ordinates for the variables $(x, y)$ if and only if the corresponding ideals are equivalent in the class group. The problem of finding representatives of ideal classes can be replaced by the problems of finding quadratic forms that represent equivalence classes.

We now separate the cases $D < 0$ and $D > 0$. In the first case, we restrict our attention to quadratic forms $Q(x, y) = qx^2 + sxy - ry^2$ (continuing the above notation) such that $q > 0$. Since $D = s^2 + 4qr < 0$, we see that $r < 0$. In fact $Q(x, y) > 0$ for all $(x, y) \neq (0, 0)$. Pictorially, the region $Q(x, y) \le r$ is bounded by an ellipse. Thus, among lattice points we can choose $u_1$ to be an element where the $Q(u_1)$ takes its minimum (non-zero) value. Now, we can complete $u_1$ to a basis by picking a suitable vector $u_2$. The only possible alternative choices for $u_2$ are $nu_1 \pm u_2$ for some integer $n$. Let $u_2$ be so chosen that the value $Q(u_2)$ is minimum in this collection. It is not too difficult to show that the expression for $Q$ in this basis is independent of the finitely many choices available. (In fact for $D| > 4$ the choices of $u_1$ and $u_2$ are unique upto sign). Now, in this basis we get $Q(x, y) = Ax^2 + Bxy + Cy^2$ with $A \leq C$ and $|B| \leq A$. Moreover, if one of these is an equality (which can only happen if $|D| \leq 4$), we have $B \geq 0$ as well. A quadratic form with negative discriminant is said to be *reduced* if it has this special form. Clearly, there are only finitely many such forms for a given $D$; one for each equivalence class of quadratic forms. Thus we have found representatives for the class group.

When $D > 0$, the quadratic forms are indefinite. The locus $Q(x, y) = r$ represents a hyperbola. Now the value 0 is not attained at non-zero $(x, y)$ (else $D$ would have a square root in integers) and the values are all integers. Thus, the absolute value of $Q$ attains a minimum at some point $u_1$ on the lattice. But this $u_1$ is far from unique (in fact there are infinitely many points where $Q$ takes this value. One can show that upto a finite number of choices these are related by an integer change of co-ordinates. Now, as before, $u_1$ can be completed to a basis by a choice of $u_2$. The alternatives for this choice are $nu_1 \pm u_2$ as earlier. Again, there are only finitely many of these with sign opposite to that of $Q(u_1)$ (since the term $n^2Q(u_1)$ in the expansion of the quadratic form will dominate for $n$ large). Among this finite set we choose $u_2$ so that the absolute value of $Q$ is minimum (again with only finitely many options for this choice). Thus, each equivalence class of quadratic forms has been represented upto a finite ambiguity. Moreover, one can bound the ambiguity depending on $D_R$.