

8430 HANDOUT 6: PROOF OF THE MAIN THEOREM

PETE L. CLARK

1. PROOF OF THE MAIN THEOREM FOR MAXIMAL ORDERS

We are now going to take a decisive step forward by proving the Main Theorem on which primes p are represented by the principal quadratic form $q_D(x, y)$ of discriminant $D < 0$, when D is a **fundamental** discriminant, i.e., the discriminant of the full ring of integers of $\mathbb{Q}(\sqrt{D})$. Of course, to solve our original problem of representation of primes by $x^2 + ny^2$ for *arbitrary* n , we need to look also at quadratic orders of not necessarily maximal discriminant. But notice that all our efforts so far have yielded solutions for only finitely many values of n , whereas here we can take n to be any squarefree negative number which is not $3 \pmod{4}$. Here is the result:

Theorem 1. *Let $D < 0$ be a fundamental quadratic discriminant, the discriminant of (the maximal order of) the imaginary quadratic field $K = \mathbb{Q}(\sqrt{D})$. Let $h(K) = \#\text{Pic}(\mathcal{O}(D))$ be the class number of K . Then there exists a monic polynomial $P_D(t) \in \mathbb{Z}[t]$ such that:*

- (a) $P_D(t)$ is irreducible of degree $h(K)$, and has at least one real root.
- (b) A prime number p which is prime to D and to $\text{disc}(P_D)$ is of the form $q_D(x, y)$ iff $\left(\frac{D}{p}\right) = 1$ and the mod p reduction $\overline{P_D}(t) \in \mathbb{F}_p[t]$ has at least one rational root.

The proof occurs in two steps: first we bring our heavy artillery to bear and almost immediately deduce the following result:

Theorem 2. *With notation as above, a prime p prime to D is of the form $q_D(x, y)$ iff p splits completely in the Hilbert class field K^1 of $K = \mathbb{Q}(\sqrt{D})$.*

Then we need to use a bit of comparatively elementary (but slightly tricky) reasoning to get from Theorem 2 to Theorem 1.

Well, second things first:

Proof of Theorem 2: Suppose p is prime to D . We already know that a necessary condition for p to be represented by q_D is the fundamental congruence $\left(\frac{D}{p}\right) = 1$. (Note that this is to be interpreted as the Kronecker symbol when $p = 2$; or just assume p is odd; you're not missing out on much.) Further, we saw that the fundamental congruence buys us precisely a Galois conjugate pair $\mathfrak{p}, \bar{\mathfrak{p}}$ of prime ideals of $\mathcal{O}(D) = \mathcal{O}_K$ lying over p . And we also saw that p is of the form $q_D(x, y)$ iff one of these ideals (equivalently, both) are **principal**.

But now we know more: there is an abelian field extension K^1/K , called the Hilbert class field, which has the following three remarkable properties: (i) its Galois group is isomorphic to $\text{Pic}(\mathcal{O}_K)$, the ideal class group of K ; (ii) it is unramified

at every prime ideal \mathfrak{p} of K ; and (iii) a prime \mathfrak{p} is principal iff its Frobenius element $\tau_{\mathfrak{p}} \in \text{Pic}(\mathcal{O}_K)$ is trivial. As we saw, it immediately follows from Chebotarev Density that the set of principal primes \mathfrak{p} has density $\frac{1}{h(K)}$. Compiling these two conditions, we see that indeed what we want is for the rational prime p to split completely from \mathbb{Q} to K^1 , the Hilbert class field of K . We're done.

As a warmup to deducing Theorem 1, let's first check that the density of the set of primes p which split completely in K^1 is $\frac{1}{2h(K)}$, as we have been claiming for a while now. Again by Chebotarev Density, it suffices to show that the extension K^1/\mathbb{Q} is Galois. (Moreover, it is less obvious but also true that K/\mathbb{Q} being Galois is **necessary** for the density to be $\frac{1}{2h(K)}$: according to Exercise X.X.X, in general the density is the reciprocal of the degree of the Galois closure.)

Proposition 3. *Let K/\mathbb{Q} be a finite Galois extension. Then the Hilbert class field K^1 of K is Galois over \mathbb{Q} .*

Proof: First note that we know (or at least, have been told) that K^1/K is not only Galois but abelian. Of course this does not in itself say anything about K^1/\mathbb{Q} . Anyway, let $\sigma : K^1 \hookrightarrow \overline{\mathbb{Q}}$ be any embedding. What we want to show is that $\sigma(K^1) = K^1$ (this is one of the equivalent conditions of normality; of course separability is not in question). Here's the key observation: since K^1 is the maximal unramified abelian extension of K , it must be that $\sigma(K^1)$ is the maximal unramified abelian extension of $\sigma(K)$. Indeed, applying σ gives an isomorphism from $\text{Aut}(K^1/K)$ to $\text{Aut}(\sigma(K^1)/\sigma(K))$, so $\sigma(K^1)/\sigma(K)$ is an abelian extension with Galois group isomorphic to the class group of $\sigma(K)$. Moreover if $\mathfrak{p}\mathcal{O}_{K^1} = \mathcal{P}_1 \cdots \mathcal{P}_g$ (no ramification!), then again we can just apply σ to get that $\sigma(\mathfrak{p})\mathcal{O}_{\sigma(K^1)} = \sigma(\mathcal{P}_1) \cdots \sigma(\mathcal{P}_g)$: still no ramification. This shows that $\sigma(K^1)/\sigma(K)$ is an unramified abelian extension of the same degree as K^1/K . But, since we assumed K/\mathbb{Q} is Galois, $\sigma(K) = K$, and K^1/K is the **maximal** unramified abelian extension of K , so we must have $\sigma(K^1) \subset K^1$, and by comparing degrees (or even just by symmetry) we get $K^1 = \sigma(K^1)$. Done!

Certainly $K = \mathbb{Q}(\sqrt{D})$ is Galois, so Proposition 3 applies, and we get that K^1/\mathbb{Q} is Galois.

The next thing to show is that we can find an extension F_D/\mathbb{Q} with the property that $[F_D : \mathbb{Q}] = [K_D : K] = h(K)$ and $F_D(\sqrt{D}) = K_D$, i.e., we have a parallelogram of field extensions...

Let us view K^1 as being embedded in the complex numbers. (It is a subtle point, but as an algebraic number theorist I don't myself view number fields as being canonically embedded in the complex numbers: there are, depending on the degree, multiple embeddings, none privileged over the others. But this slightly "naive" perspective – which is the one Cox uses – does not harm: if you like, we pick some embedding of K^1 into \mathbb{C} and proceed that way.) Now we have complex conjugation acting on \mathbb{C} and fixing \mathbb{Q} pointwise; so complex conjugation must act as an automorphism on the Galois extension K^1 . Let $F_D = (K^1)^c = K^1 \cap \mathbb{R}$, the fixed field of complex conjugation. Obviously complex conjugation does not act trivially on K^1 , because it contains the imaginary quadratic field $\mathbb{Q}(\sqrt{D})$; the only other choice is

to have $[K^1 : F_D] = 2$. This field F_D is the one we want.

Since F_D/\mathbb{Q} is separable – no one said it was Galois, and it usually isn't! (more on this later) – it has a primitive element: $F_D = \mathbb{Q}[\alpha]$ for some α . Since every algebraic number is of the form an algebraic integer divided by a positive integer, we can just replace α by $n\alpha$ for an appropriate n to get that $F_D = \mathbb{Q}[\alpha]$ where α is a real algebraic integer.

Finally, we need to show that a prime p , which is prime to D and to the discriminant of P_D , splits completely in $K(1)$ iff $\left(\frac{D}{p}\right) = 1$ and $P_D(x)$ has a root modulo p . One implication is easy: suppose p splits completely in $K(1)$. Then every prime of $K(1)$ lying over p is unramified and has residual degree 1. By multiplicativity of residual degrees, the same behavior holds in any subextension L of $K(1)/\mathbb{Q}$: in particular it holds in $\mathbb{Q}(\sqrt{D})$, giving the fundamental congruence, and it holds in F_D , which by a standard piece of algebraic number theory (“Kummer’s criterion”) implies that P_D splits completely modulo p , which certainly implies that it has a root modulo p . The converse seems more interesting, since we must go from the assumption that P_D has a root mod p to the conclusion that p splits completely in $K(1)$, which, as we have just seen, shows in particular that P_D splits completely mod p . Since F_D/\mathbb{Q} need not be Galois, this at first looks unlikely. But recall that we have something else: the assumption $\left(\frac{D}{p}\right) = 1$. As above, this says that p splits in $\mathbb{Q}(\sqrt{D})$. Now, our assumption that P_D has at least one root mod p means that we assume that there is at least one degree 1 prime \mathfrak{p} of F_D lying over p . But $K(1) = F_D(\sqrt{D})$ and since p splits in $\mathbb{Q}(\sqrt{D})$, \mathfrak{p} splits into two degree one primes $\mathcal{P}, \overline{\mathcal{P}}$ in $K(1)$. Thus \mathcal{P} is a degree one prime lying over p ; since $K(1)/\mathbb{Q}$ is Galois, this means that all primes over p have degree 1, i.e., p splits completely in $K(1)$, qed!

2. FURTHER THEORY OF NONMAXIMAL ORDERS

We revisit the situation of §2.4: suppose R is a one-dimensional Noetherian integral domain with fraction field K . Let \tilde{R} be the integral closure of R in K . Recall that \tilde{R} is a Dedekind domain (the hardest part here is to show that it remains Noetherian!). If $R \neq \tilde{R}$ then the ring R is **singular** in the sense of algebraic geometry: more precisely, by Theorem 2.1c)¹ there exists at least one prime ideal \mathfrak{p} of R such that the localization $R_{\mathfrak{p}}$ is not a discrete valuation ring (= regular, one-dimensional local ring).

If J is an ideal of R , we say an ideal I of R is **prime to J** if $I + J = R$. (More precise terminology would be: I and J are **comaximal**.)

Proposition 4. *Let I and J be nonzero ideals of R . TFAE:*

- (i) I is prime to J : $I + J = R$.
- (ii) $I\tilde{R}$ and $J\tilde{R}$ are coprime ideals in the Dedekind domain \tilde{R} .
- (iii) For all primes \mathfrak{p} containing J , $IR_{\mathfrak{p}} = R_{\mathfrak{p}}$.

¹By this numbering we mean Handout 2, Theorem 1c.

Proof: (i) \implies (ii): Suppose $I + J = R$. Then $I\tilde{R} + J\tilde{R} = (I + J)\tilde{R} = R\tilde{R} = \tilde{R}$. (ii) \implies (i): Assume I and J are not coprime, i.e., $I + J$ is proper. Then since the extension \tilde{R} is integral over R , the proper ideal $I + J$ pushes forward to the proper ideal $\tilde{R}I + \tilde{R}J$. (i) \implies (iii): If $I + J = R$ we may choose $x \in I$, $y \in J$ such that $x + y = 1$. For any prime \mathfrak{p} containing J , we have $y = 1 - x \in \mathfrak{p}R_{\mathfrak{p}}$, so $x = 1 - y$ must be a unit of $R_{\mathfrak{p}}$ (otherwise it would lie in the unique maximal ideal and hence so would $x + y = 1$, contradiction), i.e., $IR_{\mathfrak{p}} \supset xR_{\mathfrak{p}} = R_{\mathfrak{p}}$. (iii) \implies (i): If \mathfrak{p} is any prime ideal containing I , $IR_{\mathfrak{p}} \subset \mathfrak{p}R_{\mathfrak{p}}$, but then by our assumption, \mathfrak{p} does not contain J . In other words, there is no prime ideal \mathfrak{p} containing both I and J , or equivalently, $I + J = R$.

Exercise X.X: Suppose that $R = \mathcal{O}$ is an order in a number field K (so $\tilde{R} = \mathcal{O}_K$, the full ring of integers). Show that an ideal I is prime to a positive integer M – i.e., prime to the principal ideal MR – iff $N(I) = \#\mathcal{O}/I$ is relatively prime to M . (Hint: $M\mathcal{O} + I = \mathcal{O} \iff$ the multiplication by M map on \mathcal{O}/I is surjective.)

It turns out to be very desirable for the set S of singular primes of R to be finite. This is essentially related to the conductor \mathfrak{f} , which is the largest ideal of \tilde{R} which is also an ideal of R :

$$\mathfrak{f} = \{x \in R \mid \tilde{R}x \subset R\}$$

Proposition 5. *Let R be a one-dimensional Noetherian domain with conductor ideal \mathfrak{f} , and let \mathfrak{p} be a nonzero prime ideal of R . Then TFAE:*

- (i) R is nonsingular at \mathfrak{p} , i.e., the localization $R_{\mathfrak{p}}$ is a DVR.
- (ii) \mathfrak{p} **does not** contain \mathfrak{f} .

If either of these conditions hold, then $\tilde{\mathfrak{p}} = \mathfrak{p}\tilde{R}$ is a prime ideal, and $\tilde{R}_{\tilde{\mathfrak{p}}} = R_{\mathfrak{p}}$.

Remarks: (i) The last part says that the pushforward map $\iota_* : \mathcal{I}(R) \rightarrow \mathcal{I}(\tilde{R})$, $I \mapsto \tilde{I} := I\tilde{R}$ is a bijection on prime ideals prime to the conductor.

(ii) This was Proposition 2.24² but the proof was not given there.

Proof: [Neukirch, p. 80].

Proposition 6. *One has $\mathfrak{f} \neq 0$ iff \tilde{R} is finitely generated as an R -module.*

Proof: Suppose that \tilde{R} is finitely generated as an R -module, and for $1 \leq i \leq N$, let $b_i = \frac{a_i}{d_i}$ be a set of generators, with $a_i, d_i \in R$, $d_i \neq 0$. Put $d = \prod_{i=1}^N d_i$. Then $d \in R$, $d \neq 0$, and $db_i \in R$ for all i so that $d\tilde{R} \subset R$, i.e., d is a nonzero element of \mathfrak{f} .

Conversely, if $d \in \mathfrak{f} \setminus \{0\}$, then $d\tilde{R} \subset R$, so $\tilde{R} \subset \frac{1}{d}R$. Now $\frac{1}{d}R$ is, as an R -module generated by the single element $\frac{1}{d}$, so \tilde{R} is a submodule of a finitely generated module over the Noetherian ring R , and therefore it too is finitely generated.

In case $\mathfrak{f} = 0$, **every** prime of R is singular – this is quite pathological. So we had better assume that \tilde{R} is finitely generated over R – recall that we said that R is **almost Dedekind**. (Example: any order in a number field.)

Proposition 7. *a) In an almost Dedekind ring R , any nonzero element $x \in R$ is contained in only finitely many prime ideals.*

b) Therefore the same holds for any nonzero ideal I of R .

²Meaning, Handout 2, Proposition 24.

Proof: Suppose x is in the nonzero prime ideal \mathfrak{p} . By the going up theorem, there exists a prime \mathcal{P} of \tilde{R} such that $\mathcal{P} \cap R = \mathfrak{p}$. If we chose a different prime \mathfrak{p}' , the ideal \mathcal{P}' , having the property that $\mathcal{P}' \cap R = \mathfrak{p}' \neq \mathfrak{p}$, is certainly a different ideal from \mathcal{P} . But viewing x as an element of the Dedekind domain \tilde{R} , we know that there are only finitely many prime ideals of \tilde{R} containing x , so we conclude that there can only be finitely many prime ideals of R containing x , giving part a). Part b) follows immediately, since any nonzero ideal contains a nonzero element.

Corollary 8. *In an almost Dedekind domain, the set of singular primes \mathfrak{p} – i.e., the set of nonzero primes containing the conductor \mathfrak{f} – is finite.*

Definition: A fractional ideal I of R is said to be prime to an ideal J if for all primes $\mathfrak{p} \supset J$, $IR_{\mathfrak{p}} = R_{\mathfrak{p}}$. Note that by Proposition XX, this is compatible with the previous definition for integral ideals.

Exercise X.X: Let I be a fractional ideal of R which is prime to every nonzero prime ideal \mathfrak{p} of R . Show that $I = R$.

Exercise X.X: Let I be a fractional ideal of R which is prime to \mathfrak{f} . Show that the pushed forward fractional ideal $\tilde{I} = \tilde{R}I$ is prime to $\mathfrak{f}\tilde{R} = \mathfrak{f}$.

Theorem 9. *The fractional ideals prime to the conductor \mathfrak{f} form a group under multiplication.*

Proof: Note that this amounts to two statements: first that every fractional ideal prime to \mathfrak{f} is invertible, and second that the product of two fractional ideals prime to \mathfrak{f} is also prime to \mathfrak{f} . The second statement indeed follows readily from the first: if I and J are prime to \mathfrak{f} and $\mathfrak{p} \supset \mathfrak{f}$, then

$$(IJ)R_{\mathfrak{p}} = I(JR_{\mathfrak{p}}) = IR_{\mathfrak{p}} = R_{\mathfrak{p}}.$$

Moreover, if I is prime to \mathfrak{f} by the first statement there exists a fractional ideal I^{-1} such that $I^{-1}I = R$, and then

$$R_{\mathfrak{p}} = RR_{\mathfrak{p}} = (I^{-1}I)R_{\mathfrak{p}} = I^{-1}(IR_{\mathfrak{p}}) = I^{-1}R_{\mathfrak{p}}.$$

For the first statement, we will use the fact that invertible fractional ideals are precisely those which are locally principal (Theorem 2.21). Thus we must show that if I is prime to \mathfrak{f} , then for every nonzero prime ideal \mathfrak{p} of R , we have $IR_{\mathfrak{p}}$ is a principal $R_{\mathfrak{p}}$ -ideal. The very definition of I being prime to \mathfrak{f} is that for the finitely many primes $\mathfrak{p} \supset \mathfrak{f}$ we have $IR_{\mathfrak{p}} = R_{\mathfrak{p}}$, which is certainly a principal $R_{\mathfrak{p}}$ -ideal! We have a right to expect the other primes to be “nicer”. This is expressed in the following

Lemma 10. *For any prime $0 \neq \mathfrak{p}$ not containing \mathfrak{f} , $R_{\mathfrak{p}}$ is a discrete valuation ring.*

Before proving the lemma, recall that a DVR is in particular a PID, so the fractional ideals have no choice but being principal! Thus it suffices to prove the lemma.

Proof of Lemma: Choose a nonzero $d \in \mathfrak{f}$. We claim $R_d (= R[\frac{1}{d}])$ is equal to \tilde{R}_d . Certainly we have $R_d \subset \tilde{R}_d$. Conversely, we may write an arbitrary element of \tilde{R}_d as $\frac{x}{d^k}$ for some $x \in \tilde{R}$, $k \in \mathbb{N}$. But since $d \in \mathfrak{f}$ we have $dx \in R$, so $\frac{x}{d^k} = \frac{dx}{d^{k+1}} \in R_f$. Now, since \mathfrak{p} does not contain \mathfrak{f} , we may choose $d \in \mathfrak{f} \setminus \mathfrak{p}$, so that in localizing at

the prime ideal \mathfrak{p} (remember this means we adjoining inverses of all elements not in \mathfrak{p} !) we get in particular $\frac{1}{d}$, so that

$$R_{\mathfrak{p}} = (R_d)_{\mathfrak{p}} = (\tilde{R}_d)_{\mathfrak{p}R_d} = \tilde{R}_{\tilde{\mathfrak{p}}},$$

and the last ring, being the localization of a Dedekind domain at a nonzero prime ideal, is a DVR (Theorem 2.1). In fact we can prove this result using the other results we have proven: localization of a one-dimensional integrally closed Noetherian domain yields a one-dimensional integrally closed Noetherian domain with a unique prime ideal, which is therefore a PID by Theorem 2.15. It is easy to see that a local PID is a DVR (and anyway, we only used that the localization was a PID).

Theorem 11. a) A fractional ideal I of R which is prime to \mathfrak{f} can be factored uniquely into a product of prime ideals $\mathfrak{p}_1^{\alpha_1} \cdots \mathfrak{p}_r^{\alpha_r}$ with each \mathfrak{p}_i prime to \mathfrak{f} .
 b) The pushforward map from fractional ideals of R prime to \mathfrak{f} to fractional ideals of \tilde{R} prime to \mathfrak{f} is the isomorphism from the free abelian group on the prime ideals of R prime to \mathfrak{f} to the free abelian group on the prime ideals of \tilde{R} prime to $\tilde{\mathfrak{p}}$ induced by the bijection $\mathfrak{p} \mapsto \tilde{\mathfrak{p}}$ of Proposition XX.

Exercise X.X: Prove Theorem XX. (Hint: the hypotheses are such that one can prove everything by working locally.)

Finally, we will need the following result:

Lemma 12. (Local-global principle for fractional ideals) Let R be an almost Dedekind domain. Write $J(R)$ for the group of invertible fractional ideals and $P(R)$ for the subgroup of principal fractional ideals, so (by definition)

$$\text{Pic } R = J(R)/P(R).$$

a) Then the natural map $I \mapsto (I_{\mathfrak{p}})$, gives an isomorphism $J(R) \xrightarrow{\sim} \bigoplus_{\mathfrak{p}} P(R_{\mathfrak{p}})$.
 b) Therefore we have

$$\text{Pic } R \cong \left(\bigoplus_{\mathfrak{p}} P(R_{\mathfrak{p}}) \right) / P(R).$$

Proof: ...

Theorem 13. a) There is a short exact sequence

$$1 \rightarrow R^{\times} \rightarrow \tilde{R}^{\times} \rightarrow \bigoplus_{\mathfrak{p}} \tilde{R}_{\mathfrak{p}}^{\times} / R_{\mathfrak{p}}^{\times} \rightarrow \text{Pic } R \rightarrow \text{Pic } \tilde{R} \rightarrow 1.$$

b) There is a canonical isomorphism

$$\bigoplus_{\mathfrak{p}} \tilde{R}_{\mathfrak{p}}^{\times} / R_{\mathfrak{p}}^{\times} \xrightarrow{\sim} (\tilde{R}/\mathfrak{f})^{\times} / (R/\mathfrak{f})^{\times}.$$

c) Therefore if R is an order in a number field, $\text{Pic}(R)$ is finite, and

$$\frac{\#\text{Pic}(R)}{\#\text{Pic}(\tilde{R})} = \frac{1}{[\tilde{R}^{\times} : R^{\times}]} \cdot \frac{\#(\tilde{R}/\mathfrak{f})^{\times}}{\#(R/\mathfrak{f})^{\times}} \in \mathbb{Z}.$$

Theorem 14. (“Moving lemma”) Let R be an almost Dedekind domain, with conductor \mathfrak{f} . Let I be an invertible fractional R -ideal. Then there exists a fractional R -ideal J which is prime to \mathfrak{f} such that $[I] = [J]$ in $\text{Pic}(R)$.

2.1. Comparing $\text{Pic}(R)$ to $\text{Pic}(\tilde{R})$.

Let $I(R)$ be the group of invertible fractional R -ideals and $P(R)$ the subgroup of principal fractional R -ideals, so by definition $\text{Pic } R = I(R)/P(R)$. We would like to relate this group to $\text{Pic } \tilde{R} = I(\tilde{R})/P(\tilde{R})$, because, in the case of R an order in a number field, it is the latter group which occurs naturally in class field theory, as the Galois group of the Hilbert class field.

First, by XX above, every invertible fractional R -ideal lies in the same class as one which is prime to \mathfrak{f} . Let $I(R, \mathfrak{f})$ be the group of fractional ideals prime to \mathfrak{f} (recall we saw above that all such ideals are invertible). In other words, the composite map

$$I(R, \mathfrak{f}) \hookrightarrow I(R) \rightarrow I(R)/P(R)$$

is an injection; the kernel is evidently the subgroup of principal fractional ideals prime to \mathfrak{f} ; as soon as we name this group – let us call it $P(R, \mathfrak{f})$ – we get an induced isomorphism

$$I(R, \mathfrak{f})/P(R, \mathfrak{f}) \xrightarrow{\alpha} I(R)/P(R) = \text{Pic}(R).$$

But we have also seen that pushing forward ideals gives an isomorphism $I(R, \mathfrak{f}) \rightarrow I(\tilde{R}, \mathfrak{f})$. Moreover, under the canonical isomorphism $I(R, \mathfrak{f}) \cong I(\tilde{R}, \mathfrak{f})$ the subgroup $P(R, \mathfrak{f})$ gets mapped into the subgroup $P(\tilde{R}, \mathfrak{f})$: this just says that the pushforward of a principal fractional ideal prime to \mathfrak{f} is a principal fractional ideal prime to \mathfrak{f} . So, using the standard fact that if $H_1 \subset H_2$ are normal subgroups of G there is a natural surjection $G/H_1 \rightarrow G/H_2$, we get a surjective homomorphism

$$\text{Pic}(R) \xrightarrow{\alpha^{-1}} I(R, \mathfrak{f})/P(R, \mathfrak{f}) \rightarrow I(\tilde{R}, \mathfrak{f})/P(\tilde{R}, \mathfrak{f}) \rightarrow I(\tilde{R})/P(\tilde{R}) = \text{Pic}(\tilde{R}).$$

The kernel, say $K(R)$, consists of the group of fractional R -ideals I prime to \mathfrak{f} whose pushforward \tilde{I} is principal. Note that almost everyone finds it strange at first that the smaller ring R should have the larger Picard group, but this explains it: the pushforward is practically the identity map on the level of ideals prime to \mathfrak{f} , but of course it is easier for a fractional ideal to be principal in the larger ring \tilde{R} than in the smaller ring R .

There are in fact two different things we'd like to do at this point. First we would like to describe this kernel $K(R)$ as explicitly as possible, because we have a short exact sequence

$$0 \rightarrow K(R) \rightarrow \text{Pic}(R) \rightarrow \text{Pic}(\tilde{R}) \rightarrow 0,$$

and in our intended application – in which $R = \mathcal{O}$ is a quadratic order – all of these groups will be finite, so that $\#K(R) = \frac{h(\tilde{R})}{h(R)}$ measures the difference in size between the two Picard groups. But we also wish to regard $\text{Pic}(R)$ as a group of the form $I(\tilde{R}, \mathfrak{f})/\Gamma$, because this will enable us to identify $\text{Pic}(R)$ as the Galois group of an abelian extension $K(R)$ of K .

Let us do the latter task first. Assume $R = \mathcal{O}(D)$ is a quadratic order, so $\mathfrak{f} = fR$. We need to find the image Γ of $P(R, \mathfrak{f})$ under the isomorphism $I(R, \mathfrak{f}) \rightarrow I(\tilde{R}, \mathfrak{f})$. We claim that it is the subgroup generated by principal ideals of the form $x\mathcal{O}_K$, where $\alpha \equiv a \pmod{f\mathcal{O}_K}$ for some integer a relatively prime to f .

Exercise: Show that for $x \in \mathcal{O}_K$, $x \equiv a \pmod{f\mathcal{O}_K}$ for some $a \in \mathbb{Z}$ with $\gcd(a, f) = 1$ iff $x \in \mathcal{O}$, $\gcd(N(x), f) = 1$. (See Cox, p. 146).

Assuming this, we have by definition that $P(\mathcal{O}, f)$ is generated by ideals $x\mathcal{O}$ for $x \in \mathcal{O}$ with $N(x)$ relatively prime to f . Thus Γ is generated by the corresponding ideals $x\mathcal{O}_K$.

Theorem 15. *a) Pushing forward ideals prime to \mathfrak{f} gives a canonical group isomorphism*

$$\frac{I(\mathcal{O}, f)}{P(\mathcal{O}, f)} \rightarrow \frac{I(\mathcal{O}_K, f)}{\Gamma}$$

where Γ is the subgroup generated by principal ideals of the form $x\mathcal{O}_K$ where $x \equiv a \pmod{f\mathcal{O}_K}$ for some a relatively prime to f .

b) Γ contains the subgroup $P(K, f)$ of principal fractional ideals congruent to 1 $\pmod{f\mathcal{O}_K}$. We also have an exact sequence

$$0 \rightarrow I(\mathcal{O}_K, f) \cap P(\mathcal{O}_K)/\Gamma \rightarrow I(\mathcal{O}_K, f)/\Gamma \rightarrow I(K, \mathcal{O}_K)/P(K, \mathcal{O}_K).$$

Exercise: Let $R = \mathcal{O}$ be an order in an arbitrary number field K . Show that the image Γ of $P(R, f)$ contains the subgroup generated by principal ideals $x\tilde{R}$ with $x \equiv 1 \pmod{\mathfrak{f}}$.

Throughout this section, we let $\mathcal{O} = \mathcal{O}(D)$ denote the imaginary quadratic order of discriminant $D = f^2 D_0$, i.e., of fundamental discriminant D_0 and conductor f .

If I is an ideal of \mathcal{O} and x is an element of \mathcal{O} , then we say that I is **prime to x** if the ideals I and $x\mathcal{O}$ are comaximal: $I + x\mathcal{O} = \mathcal{O}$.

Theorem 16. (*“Moving lemma” for proper ideals*) *Let $M \in \mathbb{Z}^+$. For any proper \mathcal{O} -ideal I , there exists an ideal J of \mathcal{O} such that $[I] = [J] \in \text{Pic}(\mathcal{O})$ and J is prime to M .*

Lemma 17. *Let $f(x, y)$ be a primitive integral quadratic form and let $M \in \mathbb{Z}^+$. Then f represents integers prime to M .*

Exercise: Prove Lemma XX. (Suggestion: see 2.18 on p.45 of Cox’s book if you need a hint.)

Proof of Theorem XX: We combine Lemma XX with the last part of the fundamental bijection: $M \in \mathbb{Z}^+$ is represented by a primitive positive definite form f of discriminant D iff $M = N(J)$ for some J with $[J] = [I(f)]$.

Proposition 18. *Any \mathcal{O} -ideal which is prime to f is proper, hence invertible.*

Let I be an \mathcal{O} -ideal which is prime to f , and suppose $x \in K$ is such that $xI \subset I$. Of course $x \in \mathcal{O}_K$ (why?), and thus

$$x\mathcal{O} = x(I + f\mathcal{O}) = xI + xf\mathcal{O} \subset I + f\mathcal{O}_K \subset \mathcal{O} + \mathcal{O} = \mathcal{O}.$$

Thus $x = x \cdot 1 \in \mathcal{O}$. For any positive integer M divisible by f , let $I(\mathcal{O}, M)$ denote the group of fractional ideals generated ...

Corollary 19. *Let M be any integer divisible by f . Then we can represent $\text{Pic}(\mathcal{O})$ as the quotient of the monoid of ideals prime to M by the submonoid of principal ideals prime to M .*

Proof:

3. CONGRUENCES REVISITED

Let us now revisit an issue which was mysterious in our early study of primes of the form $x^2 + ny^2$: to what extent can we determine the set of primes so represented using congruence conditions alone?

We proved that if $h(D) = 1$, then the fundamental congruence $\left(\frac{D}{p}\right) = 1$ is sufficient as well as necessary. Moreover, in each case in which $h(D) = 2$, it transpired that we could find one additional congruence relation that would be sufficient as well as necessary, and more precisely that would suffice to distinguish between the primes represented by the principal form and those represented by the unique non-principal form.

In general things are more complicated. There are some values of D for which $h(D) > 2$ and nevertheless $p = N(q_D)$ is equivalent (for p prime to D , of course) to a set of congruence conditions modulo D . For example, this happens for $D = -84$, where $h(D) = -84$. But it does not happen for $D = -56$ – there is no congruence class $a \pmod{56}$ such that each of the (infinitely many) primes $p \equiv a \pmod{56}$ is of the form $x^2 + 14y^2$. It is natural to wonder whether some congruence condition modulo a multiple of D might be sufficient. Computations suggest that this is not the case, but we haven't yet proved anything along these lines.

If one looks more carefully at such examples, the answer seems to lie in the group structure of $\text{Pic}(\mathcal{O}(D))$. For $D = -84$, the group is $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Indeed the reduced forms are

$$x^2 + 21y^2, 3x^2 + 7y^2, 5x^2 + 4xy + 5y^2, 2x^2 + 2xy + 11y^2,$$

which are all ambiguous classes. However, for $D = -56$, the reduced forms are

$$x^2 + 14y^2, 2x^2 + 7y^2, 3x^2 \pm 2xy + 5y^2,$$

only two of which are ambiguous, so the group is $\mathbb{Z}/4\mathbb{Z}$. This suggests that the problem of when $p = q_D(x, y)$ is solvable by congruences iff $h(D)$ is an elementary 2-group. Let us try to explain this.

Recall that one form of our main result is that (for p prime to D , as usual) $p = q_D(x, y)$ iff p splits completely in the ring class field $K(\mathcal{O}(D))$. In particular the set of such primes has positive density.

Recall that by class field theory over \mathbb{Q} , congruence conditions modulo N translate into conditions on the Frobenius map in the cyclotomic field $\mathbb{Q}(\zeta_N)$. More precisely, for a prime to N , $p \equiv a \pmod{N}$ iff the Frobenius element at p is the automorphism $\zeta_N \mapsto \zeta_N^a$ of $\mathbb{Q}(\zeta_N)$.

Theorem 20. *Let D be an imaginary quadratic order, $K = \mathbb{Q}(\sqrt{D})$, with ring class field $K(\mathcal{O}(D))$. TFAE:*

- (i) $p \equiv 1 \pmod{D}$ implies $p = q_D(x, y)$.
 - (ii) There exists some positive integers N and a prime to N such that every prime $p \equiv a \pmod{N}$ is of the form $q_D(x, y)$.
 - (iii) The Galois group $\text{Gal}(K(\mathcal{O}(D))/\mathbb{Q})$ is abelian.
 - (iv) The Galois group $\text{Gal}(K(\mathcal{O}(D))/K)$ has exponent dividing 2.
- Moreover, there are at least 65 values of n such that $D = -4n$ satisfies these equivalent properties. Conditionally on GRH, there are exactly 65.

We will prove the equivalence of conditions (i) through (iv). See Cox p. 60-61 for a least of the 65 known values of $D = -4n$: such n are called **idoneal numbers**. The proof that there are either 65 or 66 is beyond the scope of our ambitions.

We begin with the following important consequence of Chebotarev density:

Theorem 21. *Let F be a global field, and K and L be finite Galois extensions of F . Suppose that every prime ideal \mathfrak{p} of F which splits completely in K also splits completely in L . Then $K \supset L$.*

Exercise X.X: Let F be any field, and K and L be two Galois extensions (if you are comfortable with infinite Galois extensions, allow K and L to be possibly infinite; if not, stick to finite extensions) contained in a common algebraic closure \overline{F} of F . Then the compositum KL of K and L is Galois.

Proof of Theorem: We take the compositum LK , which by the exercise is also Galois over F . According to Chebotarev's theorem, the density of the set of primes of F which split completely in KL is $\frac{1}{[KL:F]}$, whereas the density of the primes which split completely in K and L respectively are $\frac{1}{[K:F]}$ and $\frac{1}{[L:F]}$. A prime splits completely in both K and L iff it splits completely in the compositum KL , so under our assumption, every prime which splits completely in K splits completely in KL . Comparing densities, this tells us that $[KL:F] = [K:F]$, i.e., $K = KL$ and $L \subset K$.

Exercise X.X: Let F be a global field and K, L be finite separable extensions.

a) Show that TFAE:

- (i) A prime ideal \mathfrak{p} of F splits completely in K iff it splits completely in L .
- (ii) The Galois closures of K and L (over F) are equal.

b) Give an example where these equivalent conditions hold but K is not contained in L and vice versa.

Note the following striking and important special case of this theorem: if K and L are two Galois extensions of F such that a prime splits completely in K iff it splits completely in L , then $K = L$. In other words, if you know which primes split completely in a Galois extension, you know that extension! In fact, the proof shows that you don't need to assume that exactly the same primes split completely in both. Its enough to assume that the density of the set of primes \mathfrak{p} which split in exactly one of the two fields is zero.

Next let us assume that $K(\mathcal{O}(D))/\mathbb{Q}$ is abelian, so by class field theory there exists an N such that $K(\mathcal{O}(D)) \subset \mathbb{Q}(\zeta_N)$. We know that a prime p splits completely in $\mathbb{Q}(\zeta_N)$ iff $p \equiv 1 \pmod{N}$; under our assumption on $K(\mathcal{O}(D))$ this clearly implies

that p splits in $K(\mathcal{O}(D))$. This shows that (iii) implies (ii), and in fact in (ii) we can take $a = 1$.

Let us now show that (ii) implies (iii). Namely, suppose that there exist coprime positive integers a and N such that every prime $p \equiv a \pmod{N}$ is represented by $q_D(x, y)$. Let $F = K(\mathcal{O}(D)) \cap \mathbb{Q}(\zeta_N)$. Then we get a diamond diagram of field extensions, with F at the bottom, $K(\mathcal{O}(D))$ and $\mathbb{Q}(\zeta_N)$ at the sides and the compositum $K(\mathcal{O}(D), \zeta_N)$ at the top. Since both $K(\mathcal{O}(D))$ and $\mathbb{Q}(\zeta_N)$ are Galois over \mathbb{Q} , they are also Galois over their intersection field F . They are then **linearly disjoint** over F , and by basic Galois theory this gives a natural isomorphism

$$\text{Gal}(K(\mathcal{O}(D), \zeta_N)/F) \cong \text{Gal}(K(\mathcal{O}(D))/F) \times \text{Gal}(\mathbb{Q}(\zeta_N)/F).$$

Now p prime to D is represented by q_D iff p splits completely in $K(\mathcal{O}(D))$; in particular the corresponding Frobenius class τ_p must be trivial in $\text{Gal}(K(\mathcal{O}(D))/\mathbb{Q})$ and hence lie in the subgroup $\text{Gal}(K(\mathcal{O}(D))/F)$. This shows that the subgroup of $(\mathbb{Z}/N\mathbb{Z})^\times$ corresponding to $\text{Gal}(\mathbb{Q}(\zeta_N)/F)$ gives congruence classes modulo N into which any p of the form $q_D(x, y)$ must fall. Conversely, the above isomorphism shows that in order for every prime $p \equiv a \pmod{N}$ to split completely in $K(\mathcal{O}(D))$, we need $K(\mathcal{O}(D)) = F$.

Next we show that $\text{Gal}(K(\mathcal{O}(D))/\mathbb{Q})$ is abelian iff it has exponent dividing 2. This is a special case of the following important and beautiful result:

Theorem 22. *The Galois group $\text{Gal}(K(\mathcal{O}(D))/\mathbb{Q})$ fits into a short exact sequence*

$$1 \rightarrow \text{Gal}(K(\mathcal{O}(D))/K) \rightarrow \text{Gal}(K(\mathcal{O}(D))/\mathbb{Q}) \rightarrow \text{Gal}(K/\mathbb{Q}) = \langle c \rangle \rightarrow 1.$$

Moreover lifting the generator c of $\text{Gal}(K/\mathbb{Q})$ to complex conjugation $\sigma \mapsto \bar{\sigma}$ gives a splitting of the sequence, exhibiting $\text{Gal}(K(\mathcal{O}(D))/\mathbb{Q})$ as the semidirect product of the abelian group $\text{Gal}(K(\mathcal{O}(D))/K)$ and the order two group $\text{Gal}(K/\mathbb{Q})$. Moreover, conjugation by c acts as inversion.

Therefore $\text{Gal}(K(\mathcal{O}(D))/\mathbb{Q})$ is what is called a **dihedral** extension of \mathbb{Q} . Since it is given in terms of generators and relators as $\langle a \in \text{Gal}(K(\mathcal{O}(D))/K), c \mid c^2 = 1, cac^{-1} = a^{-1} \rangle$, it is easily seen that the abelianization of this group – i.e., the quotient by the commutator subgroup – is obtained by setting $a = a^{-1}$ for all a ; in other words, the abelianization is an elementary 2-group, a trivial extension of $\text{Pic}(\mathcal{O}(D))/2\text{Pic}(\mathcal{O}(D))$ by $\mathbb{Z}/2\mathbb{Z}$. This shows that $\text{Gal}(K(\mathcal{O}(D))/\mathbb{Q})$ is abelian iff $\text{Gal}(K(\mathcal{O}(D))/K)$ has exponent 2.

We will not give the proof that (ii) \implies (i) here.

In particular, when $D = -4n$, the class group is 2-torsion iff n is an idoneal number, i.e., iff every class is ambiguous.

In fact more is true: put $G(D) = \text{Pic}(\mathcal{O}(D))/2\text{Pic}(\mathcal{O}(D))$, the **genus group**. As we have seen, $G(D) \cong (\mathbb{Z}/2\mathbb{Z})^r$, and r is determined by the number of ambiguous classes, a calculation which we have already seen on the quadratic forms side. On the Galois theory side, we have shown that the maximal abelian subfield of $K(\mathcal{O}(D))$ is generated by quadratic extensions of \mathbb{Q} , i.e., is of the form $\mathbb{Q}(\sqrt{x_1}, \dots, \sqrt{x_n})$. It is equally possible to explicitly compute which x_i 's occur; in

fact it is a bit easier this way. In the case that D is a fundamental discriminant, we want quadratic extensions $\mathbb{Q}(\sqrt{x_i})$ such that $\mathbb{Q}(\sqrt{D}, \sqrt{x_i})/\mathbb{Q}(\sqrt{D})$ is everywhere unramified.

Exercise: a) This occurs when every prime which divides the discriminant of $\mathbb{Q}(\sqrt{x_i})$ also divides D .

b) Deduce that the genus field is a subfield of $\mathbb{Q}(\zeta_N)$, proving (i) \equiv (ii) in this case.

One says that two quadratic forms f_1 and f_2 of discriminant D **lie in the same genus**

$$[I(f_1)] \cong [I(f_2)] \pmod{2} \text{Pic}(\mathcal{O}(D)),$$

i.e., iff the corresponding elements of the genus group $\text{Gal}(G(D)/K)$ agree.

Theorem 23. *For two quadratic forms f_1 and f_2 , TFAE:*

(i) f_1 and f_2 represent the same reduced residue classes modulo D .

(ii) f_1 and f_2 represent the same reduced residue classes modulo N for all N .

(iii) f_1 and f_2 are $\text{GL}_2(\mathbb{Z}_p)$ -equivalent for every prime p .

(iv) f_1 and f_2 are in the same genus.

If the discriminant D is fundamental, these conditions are equivalent to: f_1 and f_2 are $\text{GL}_2(\mathbb{Q}_p)$ -equivalent for all p .

We must omit the proof of this theorem here; parts of it are proved in Cox.

4. SOME THEORY OF SINGULAR MODULI

One of the things to notice about the class number one j -invariants is that they are not just any 13 rational integers. They tend to be divisible by large powers of small primes. As soon as one computes examples of Hilbert class polynomials, one also finds – a bit unfortunately – that the coefficients grow very rapidly with D . There is a whole theory about this: here is just a small piece.

Define

$$\gamma_2(\tau) := \sqrt[3]{j(\tau)} = 12 \frac{g_2(\tau)}{\sqrt[3]{\Delta(\tau)}}.$$

Here we are taking the unique cube root which makes the function real on the positive imaginary axis, as j is.

Theorem 24. *Let D be an imaginary quadratic discriminant which is prime to 3, and write $\mathcal{O}(D) = [1, \tau_0]$ where $\tau_0 = \frac{\sqrt{-D}}{2}$ if $D \equiv 0 \pmod{4}$ and $\tau_0 = \frac{3+\sqrt{-D}}{2}$ if $D \equiv 1 \pmod{4}$. Then $\gamma_2(\tau_0)$ is an algebraic integer, $\mathbb{Q}(\sqrt{-D}, \gamma_2(\tau)) = K(\mathcal{O})$ and $\mathbb{Q}(\gamma_2(\tau_0)) = \mathbb{Q}(j(\tau_0))$.*

This proposition explains why

$$\begin{aligned} j(\sqrt{-1}) &= 12^3, \\ j(\sqrt{-2}) &= 20^3, \\ j\left(\frac{1 + \sqrt{-7}2}{2}\right) &= 15^3. \end{aligned}$$

For the case where $3 \mid D$, see Theorem 12.13 of Cox.

Of course the definition of $\gamma_2(\tau)$ we have given is not helpful for computations. An independent expression of it in terms of certain modular functions of higher level is part of the vast work done by Weber, and is described in Cox's book.

Theorem 25. (*Deuring*) Let $\mathcal{O}(D_1)$ and $\mathcal{O}(D_2)$ be two imaginary quadratic orders in possibly distinct fields K_1 and K_2 . Let \mathfrak{a}_1 and \mathfrak{a}_2 be invertible fractional $\mathcal{O}(D_i)$ -ideals. Let L be a number field containing $j(\mathfrak{a}_1)$ and $j(\mathfrak{a}_2)$. Let p be a prime number and \mathcal{P} a prime ideal of L lying over p . If $K_1 = K_2$ we assume moreover that p does not divide the conductor of either order. Finally, assume $j(\mathfrak{a}_1) \neq j(\mathfrak{a}_2)$. Then: if

$$j(\mathfrak{a}_1) \equiv j(\mathfrak{a}_2) \pmod{\mathcal{P}},$$

then neither $\left(\frac{D_1}{p}\right)$ nor $\left(\frac{D_2}{p}\right)$ equals 1.

In fact this is a theorem relating complex multiplication in characteristic 0 to complex multiplication in characteristic p , but we – alas! – cannot talk about the proof here.

Corollary 26. Let D be an imaginary quadratic discriminant and p a prime.

- a) If p divides the constant term of $P_D(t)$ and $\mathbb{Q}(\sqrt{D}) \neq \mathbb{Q}(\sqrt{-3})$, then $\left(\frac{D}{p}\right) \neq 1$ and either $p = 3$ or $p \equiv 2 \pmod{3}$.
- b) If p divides the discriminant of $P_D(t)$, then $\left(\frac{D}{p}\right) \neq 1$.

Proof: ...

This result implies that in our main theorem, so long as we use the Hilbert class polynomial $P_D(t)$, we do not need to exclude any primes except those which divide D . This seems like a good place to end.