LATTICES, QUADRATIC FORMS, AND IDEALS

ISHAN LEVY

1. Abelian Extensions & Chebotarev

The theorems of class field theory have amazing consequences:

Lemma 1.1 (Abelian Classification)**.** *Let L, L' be finite abelian extensions of a number field K, let m be a modulus for L, L' and let $H_L, H_{L'}$ be the kernels of the Artin maps for L, L', m. Then $L \subset L'$ iff $H'_L \subset H_L$.*

Proof. $L \subset L' \implies H'_L \subset H_L$ by naturality of the Artin map. Conversely, if $H'_L \subset H_L$, then LL' is abelian, as it's Galois group embeds in the product of the Galois groups of L, L'. Then the kernel of the Artin map for LL' is the intersection of that for L, L' since it is the compositum, and since the Artin map is natural. But by uniqueness of the existence theorem, $LL' = L'$ and so $L' \supset L$. □

Note that by the conductor theorem, for any pair L, L', the conditions of the lemma are always satisfied for some large enough modulus. Thus class field theory tells us exactly what the lattice of abelian extensions looks like.

Corollary 1.2 (Kronecker-Weber)**.** *Any abelian extension of $\mathbb{Q}$ is contained in some cyclotomic field.*

Proof. By Artin reciprocity, for some modulus m, which we can assume contains the real embedding by the conductor theorem, the kernel of the Artin map is contained in P_m. But P_m is the kernel of the Artin map for $\mathbb{Q}[\zeta_m]$ so we are done by the lemma above. □

So an abelian extension is essentially determined by the kernel of the Artin map, which is the set of primes that split completely. However, it turns out that the assumption that the extension is abelian is non-essential, and is a consequence of a theorem that is very related to class field theory, the Chebotarev density theorem.

Say that the **natural density** of some set S of primes $\mathfrak{p}$ in K is the limit $\lim_{n\to\infty} \frac{\#\mathfrak{p}\in S, N(\mathfrak{p})<n}{\#\mathfrak{p} \text{ in } K, N(\mathfrak{p})<n}$, when the limit exists. Say that $S \doteq S'$ if the S, S' differ only by finitely many primes. If $S \doteq S'$, then they have the same density, and $\dot{\supset}, \dot{\subset}$. In particular if the density is greater than 0, there are infinitely many primes in S. Suppose L/K is a Galois extension, and C is a conjugacy class in the Galois group.

Theorem 1.3 (Chebotarev density theorem)**.** *Let C be a conjugacy class in the Galois group of L/K. The density of primes in K with Frobenius C is $\frac{|C|}{[L:K]}$.*

In the case of the extension $\mathbb{Q}[\zeta_n]/\mathbb{Q}$, the Frobenius of p is $p \in \mathbb{Z}/n\mathbb{Z}^\times$, so the theorem says that the primes are evenly distributed mod n, which is Dirichlet's theorem.

The Chebotarev density theorem along with the Frobenius, can be used to show that Galois extensions of number fields are up to an automorphism of the algebraic closure, determined by which primes split completely inside of them.

If L/K is a finite extension, then let $\tilde{S}_{L/K}$ be the set of primes $\mathfrak{p}$ in K such that there is a $\mathfrak{P}/\mathfrak{p}$ in L such that residual degree is 1, and let $S_{L/K}$ be the set of primes splitting completely in L. Note that when L is Galois, $\tilde{S}_{L/K} \doteq S_{L/K}$.

Lemma 1.4 (General Classification)**.** *Let L, L' be finite extensions of K, L Galois. Then $S_{L/K} \dot{\supset} \tilde{S}_{L'/K}$ iff $L' \supset L$, and $L' \subset L$ iff $S_{L/K} \subset S_{L'/K}$.*

Proof. Suppose $L' \supset L$, where L is not necessarily Galois. If p is a prime in K and there is a prime $\mathfrak{P}$ over p with residual degree 1, then $\mathfrak{P} \cap L$ is some prime $\mathfrak{p}$in L over p with residual degree 1, so $S_{L/K} \dot{\supset} \tilde{S}_{L'/K}$. Conversely suppose $S_{L/K} \dot{\supset} \tilde{S}_{L'/K}$. If L is Galois, let M be the Galois closure of the compositum of L, L', and let σ be an element of $\mathrm{Gal}(M/L')$. By the Chebotarev density theorem, there are infinitely many primes $\mathfrak{P}_i/p$ in M/L' not ramifying such that the Frobenius element is σ. Since the Frobenius restricts to being trivial on L', $p \in S_{L'/K}$, so $\mathfrak{p}_i \in S_{L/K}$ (for all but finitely many i). Then since L is Galois, $\mathfrak{p}$ splits completely, so its Frobenius must fix L. Thus $\mathrm{Gal}(M/L) \supset \mathrm{Gal}(M/L')$ so $L \subset L'$.

If $S_{L/K} \dot{\supset} S_{L'/K}$, note that $L' \subset L$ iff the Galois closure $\tilde{L}'$ of L' is in L iff $S_{\tilde{L}'/K} \dot{\supset} \tilde{S}_{L/K} \doteq S_{L/K}$ by the first case. But $S_{L'/K} \supset S_{\tilde{L}/K}$ so we are done. □

Corollary 1.5. *The Hilbert class field is unique.*

Proof. This follows from the previous lemma and the definition of the Hilbert class field. □

2. Quadratic forms and ideals

From now on, $n \equiv 2, 1 \pmod 4$ and is square free. Although we have an abstract solution to the problem of $p = x^2 + ny^2$ for any particular n, it remains to actually find the Hilbert class field. This is an unramified extension of degree the class number, so it would be helpful to know how to compute the class number

To help us compute class numbers. Given a negative discriminant of a quadratic field $D \equiv 0, 1 \pmod 4$, $\mathrm{Cl}(D)$ is the set of equivalence classes of quadratic forms of discriminant D, and $\mathrm{Pic}(\mathbb{Q}[\sqrt{D}])$ is the group of ideals modulo principle ones. We

will construct a bijection between the two, which will induce a group structure on $\mathrm{Cl}(D)$, and lets us compute class numbers.

Given a quadratic form $ax^2 + bxy + cy^2$, we can send it to the ideal that is the free abelian group generated by $a, \frac{b+\sqrt{D}}{2}$, denoted $[\frac{-b+\sqrt{D}}{2}, a]$ (check this is an ideal). This can be thought of as a sublattice of the complex plane.

The proof will use ideas related to complex multiplication, which is a tool used to explicitly construct abelian extensions of imaginary quadratic number fields. However complex multiplication will not be explored here. Let $\mathfrak{a}$ be an ideal of $\mathcal{O}_K$, an imaginary quadratic field, viewed as a lattice in $\mathbb{C}$. Given $x \in \mathbb{C}$, let $x\mathfrak{a}$ be the lattice given by multiplying every element of $\mathfrak{a}$ by x. Say that two lattices $\mathfrak{a}, \mathfrak{b}$ are **homothetic** if there is a x such that $\mathfrak{a} = x\mathfrak{b}$.

Lemma 2.1. *Two ideals are in the same ideal class iff they are homothetic as lattices. A lattice L is homothetic to an ideal in $\mathcal{O}_K$ iff $\mathcal{O}_K = \{x \in \mathbb{C} | x\mathfrak{a} \subset \mathfrak{a}\}$.*

Proof. Suppose L is a lattice homothetic to an ideal. Clearly, if $xL \subset L \implies x \in K$. But x also acts as a linear map on $\mathfrak{a}$ as an abelian group, so is the root of the characteristic polynomial, a monic polynomial of degree 2, so $x \in \mathcal{O}_K$. For the converse, change by homothety so $1 \in L$, and observe that L is a fractional ideal.

If two ideals $\mathfrak{a}, \mathfrak{b}$ are in the same ideal class, then $\mathfrak{a} = x\mathfrak{b}, x \in K$, so the two are homothetic. Conversely, if two fractional ideals are homothetic, by scaling by a large enough number, we can assume $\mathfrak{a} \subset \mathfrak{b}$. but then by the first part, the scaling factor for the homothety between $\mathfrak{a}, \mathfrak{b}$ must lie in K, so the ideals are in the same class. □

Exercise 2.1.1. *Can you make a version of the above lemma that works for $\mathbb{Z}[\sqrt{-n}]$ where n is arbitrary?*

Note that $[\frac{-b+\sqrt{D}}{2}, a]$ is homothetic to $[\frac{-b+\sqrt{D}}{2a}, 1]$ which is a fractional ideal, and so the lattice that we get corresponds to $\mathrm{SL}_2(\mathbb{Z})$ acts on both lattices with bases, and and

If $[a, b]$ is a lattice with a choice of generators, it is homothetic to $[\frac{a}{b}, 1]$, where $\frac{a}{b}$ is a not real complex number. In order to get an invariant of the lattice, we observe that we can get all the bases from our original choice by changing $[a, b]$ by some matrix in $\begin{pmatrix} w & x \\ y & z \end{pmatrix} \in \mathrm{GL}_2(\mathbb{Z})$, which sends it to $[wa + bx, ya + zb]$, which is homothetic to $[\frac{wa+bx}{ya+zb}, 1]$. This is the same as forcing $\frac{a}{b}$ for $[\frac{a}{b}, 1]$ to lie in the upper half plane, and only considering matrices in $\mathrm{SL}_2(\mathbb{Z})$. So every lattice is represented by some complex number, modulo the action of $\mathrm{SL}_2(\mathbb{Z})$ in the way described.

Theorem 2.2. *The map $ax^2+bxy+cy^2 \mapsto [a, \frac{-b+\sqrt{D}}{2}]$ gives an isomorphism between the $\mathrm{Cl}(D)$ and the ideal class group of $\mathbb{Z}[\sqrt{-n}]$.*

Proof. If we interpret the ideal class group in terms of homothety classes of ideals, If we change $ax^2+bxy+cy^2$ by an element of $\mathrm{SL}_2(\mathbb{Z})$, then the root of $x^2+bxy+cy^2$ is acted on by the same element of $\mathrm{SL}_2(\mathbb{Z})$ via fractional linear transformations. Thus since the value of the image only depends on the homothety class of the image by the previous lemma, the map is well-defined and injective. For surjectivity, we can assume the ideal is of the form $[\tau, 1]$, and send it to $Q(x,y) = ax^2+bxy+cy^2$, where τ is the root of $Q(x,1)$, and $(a,b,c) = 1$. $\mathrm{disc}(Q) = a^2 \mathrm{disc}(\mu(\tau)) = a^2 \mathrm{disc}[1,\tau] = \mathrm{disc}[1, a\tau]$ so if we show that $[1, a\tau] = \mathbb{Z}[\sqrt{-n}]$, we are done.

To show this, a computation shows that $[1, a\tau] = \{x | x[1,\tau] \subset [1,\tau]\}$, so we are done by the lemma from above. □

3. An example of a Hilbert class field

Let's use these results to find out when $p = x^2+14y^2$. The reduced quadratic forms for the discriminant -56 are $x^2+14y^2, 2x^2+7y^2, 3x^2 \pm 2xy + 5y^2$ so the size of the class group is 4. However, looking at congruence classes is not enough to distinguish x^2+14y^2 from the rest. To find the Hilbert class field of $K = \mathbb{Q}[\sqrt{-14}]$, first note that $K[\sqrt{2}]$ is an unramified extension, since the subfields are $K, \mathbb{Q}[\sqrt{2}], \mathbb{Q}[\sqrt{-7}]$, and the primes $2, 7$ only ramify in two of these. Thus the Hilbert class L field is a degree 2 extension of $K[\sqrt{2}]$. Moreover, $\bar{L}$ satisfies the axioms of the Hilbert class field, so by uniqueness, L is generated over K by a real element, and is the linearly disjoint compositum of a real extension over $\mathbb{Q}$ of degree 4 and K. This extension is a degree 2 extension of $\mathbb{Q}[\sqrt{2}]$ so is of the form $\mathbb{Q}[\sqrt{2}][\sqrt{u}]$ for positive u. u is an algebraic integer of the form $a+b\sqrt{2}$. The minimal polynomial is x^2-u which has discriminant $4u$, so if $p \nmid 4u$ it is unramified. for the prime $\sqrt{2}$, we will have to divide by 2, so we want to use instead an algebraic integer of the form $\frac{\sqrt{u}+b}{2}$. These have minimal polynomials x^2+bx+c where $u = b^2-4c$, so we need u to be a square mod 4 in $\mathbb{Z}[\sqrt{2}]$. $N(u) = \pm 2, \pm 1$ by the first condition, so u is a power of $1+\sqrt{2}$ with a possible extra factor of $\sqrt{2}$. Thus modulo squares, u is either $\sqrt{2}, 1+\sqrt{2}, 2+\sqrt{2}$. A $\sqrt{2}$ factor cannot appear in u because the result will not be a square mod 4. Thus $u = 1+\sqrt{2}$, which has minimal polynomial $x^2-2x-1 = (x-1)^2-2$. Now p splits completely in L iff it does in $\mathbb{Q}[\sqrt{u}]$ and $\mathbb{Q}[\sqrt{-14}]$ so we get the following result:

Theorem 3.1. *Let p be a prime not dividing the discriminant of $(x^2-1)^2-2$or 56. Then $p = x^2+14y^2$ iff $(\frac{-14}{p}) = 1$ and the polynomial $(x^2-1)^2-2$ has a root mod p.*

Exercise 3.1.1. *Which primes are of the form x^2+17y^2?*