# 8430 HANDOUT 5: CHEBOTAREV DENSITY; GLOBAL CLASS FIELD THEORY

PETE L. CLARK

Remark: This handout presents some of the most important results of algebraic number theory. Although our intended application is to the case of $K$ an imaginary quadratic field, $L/K$ a certain finite abelian extension, $R = \mathcal{O}_K$ and $S = \mathcal{O}_L$, whenever it was not obviously inconvenient I have presented the results in more generality. Some of my motivations for doing this are as follows: first, in contrast to the intended "basic graduate level" audience of Part II of Cox's book, this course is a topics course which – while, I hope, being mostly accessible to students with a background in basic graduate algebra – is also intended to be **useful** for students who are now doing or contemplate going on to do thesis work in algebraic number theory and/or arithmetic geometry. For such students – i.e., for at least three out of five – the extra generality I add over Cox's treatment will almost certainly come in handy later in your career. Moreover, Dino has recently taught two topics courses which develop things in a similar level of generality (and, in fact, with even more loving attention to inseparable field extensions), so it would be a disservice to students who took either or both of his courses not to give the natural continuations of some of the topics from Dino's courses.

My recommendation to you is to pay especially close attention to the Frobenius elements and Chebotarev Density – if you really understand the well-definedness of Frobenius elements for unramified primes up to conjugacy, you will be well equipped to appreciate the remarkable *simplicity* of Chebotarev's theorem: it just says that the probability that a conjugacy class $C$ in $\mathrm{Gal}(L/K)$ is the Frobenius conjugacy class of a randomly chosen prime ideal $\mathfrak{p}$ is exactly what equidistribution would predict: $\frac{\#C}{\#\mathrm{Gal}(L/K)}$. What could be simpler?

In contrast, no one has ever accused class field theory of being simple. I think it is fair to say that the material presented in this handout will be best understood and appreciated by patiently parsing the complicated statements and then waiting to see how it will be applied (which is now coming up very soon). You are entitled to be a little confused!

## 1. Decomposition of ideals in separable extensions

The running hypotheses for this section are as follows: $R$ is a Dedekind domain with quotient field $K$, $L/K$ is a **separable** field extension of degree $n$, and $S$ is the integral closure of $R$ in $L$. Recall that $S$ is a Dedekind domain and (by virtue of the separability) is finitely generated as an $R$-module. If $\mathfrak{p}$ is a prime of $R$, then because the extension is integral it follows that $\mathfrak{p}S$ is a proper ideal of $S$. Therefore

it factors, say as

$$\mathfrak{p}S = \prod_{i=1}^{g} \mathcal{P}_i^{e_i}.$$

It turns out to be critically important to understand this factorization, and especially how it changes depending on $\mathfrak{p}$.

The most important case for us is when $K$ is a number field and $R = \mathcal{O}_K$ the full ring of integers, so that $S = \mathcal{O}_L$, the ring of integers in the number field $L$. In particular, this allows us to define the **Frobenius map**. However, we will work our way from the general case to this specific case, delaying the more restrictive hypotheses until the time at which they are needed.

### 1.1. **Discriminant ideal of an extension.**

Our first task is to define the **discriminant** $\Delta(L/K)$, which will be a nonzero ideal of $R$. (If the extension $L/K$ were not separable, this ideal would be zero.) Note that $S$ is a finitely generated (because of the separability!) $R$-module; clearly it is also torsionfree: i.e., if $r \in R, 0 \neq s \in S$ is such that $rs = 0$, then $r = 0$.

Step 1: Suppose $R$ is a PID. Then finitely generated torsion free modules are free; it is easy to see that $S$ has rank $n = [L : K]$, i.e., $S \cong_R R^n$. In particular we can choose a basis for $S$ as an $R$-module, i.e., $x_1, \ldots, x_n \in S$ such that $S = Rx_1 \oplus \ldots \oplus Rx_n$. We define the discriminant $\Delta(x_1, \ldots, x_n)$ to be the determinant of the matrix whose $(i, j)$ entry is $M(i, j) = \mathrm{tr}_{L/K}(x_i x_j)$. Again, if we let $\sigma_1, \ldots, \sigma_n$ be the $n$ embeddings of $L/K$ into $\overline{L}$, then it can be shown that

$$\Delta(x_1, \ldots, x_n) = \det(\sigma_i(x_j))^2,$$

and as before, this shows that for any two integral bases of $S$, the ratio of the discriminants is the square of a unit of $R$. In general $R$ has plenty of units, but no matter what $\Delta(S/R)$ is well-defined as a principal **ideal** of $R$.

Unfortunately, if $R$ is not a PID, then in general $S$ will *not* be free as an $R$-module. Indeed Narkewicz shows that whenever $\mathcal{O}_K$ is not a PID there exists a quadratic extension $L/K$ such that $\mathcal{O}_L$ is not free as an $\mathcal{O}_K$-module. There are two ways of remedying this: the **global** way and the **local way**.

Step 2 (global): We define $\Delta(L/K)$ to be the ideal generated by all elements $\mathrm{disc}(x_1, \ldots, x_n)$ as $(x_1, \ldots, x_n)$ ranges over $n$-tuples $x_1, \ldots, x_n \in S$. (This will give zero unless $x_1, \ldots, x_n$ are $K$-linearly independent, so one may restrict to this case if desired.) With this definition it is easy to show that $\Delta(L/K)$ is nonzero.

Step 3 (local): From the structure theory of modules over a Dedekind domain, the finitely generated torsionfree $R$-module $S$ is at least **locally free**, which suggests we should define the discriminant prime by prime. Namely, define the discriminant of $S_{\mathfrak{p}}/R_{\mathfrak{p}}$, which is an ideal of $R_{\mathfrak{p}}$ and therefore is equal to some power $a_{\mathfrak{p}}$ of the unique maximal ideal $\mathfrak{p}R_{\mathfrak{p}}$. It is not too hard to see that $a_{\mathfrak{p}} = 0$ for all but finitely many primes $\mathfrak{p}$; for instance let $L = K[t]/P(t)$. Then it turns out that the only

primes $\mathfrak{p}$ for which $\mathfrak{p} > 0$ are those dividing the ideal generated by the discriminant of the polynomial $P$ in the usual sense. Therefore the ideal $\prod_{\mathfrak{p} \in \mathcal{P}_R} \mathfrak{p}^{a_\mathfrak{p}}$ is well-defined, and called the **discriminant** ideal.

Example 5.1.1.1: Let $K$ be a number field and $L = K(\sqrt{\alpha})$. Then the discriminant can only be divisible by primes lying over 2 and those dividing $\alpha$.

Example 5.1.1.2: Let $n$ be a positive integer which is either odd or divisible by 4. Let $\zeta_n$ be a primitive $n$th root of unity. Let $K = \mathbb{Q}$ and $L = \mathbb{Q}(\zeta_n)$. Then the discriminant of $L/K$ is divisible precisely by the primes dividing $n$. (Think about why we have made the restriction on $n$.)

## 1.2. **Decomposition of primes.**

Let $\mathfrak{p}$ be any (nonzero) prime (ideal) of $R$. Consider the pushed forward ideal $\mathfrak{p}S$. As in any integral extension of domains, the pushforward of a proper (nonzero) ideal is proper (nonzero), so we get a nontrivial factorization

$$\mathfrak{p}S = \prod_{i=1}^{g} \mathcal{P}_i^{e_i},$$

where the $\mathcal{P}_i$'s are precisely the primes **lying over** $\mathfrak{p}$, i.e., such that $\mathcal{P}_i \cap R = \mathfrak{p}$. We write $e(\mathcal{P}_i/\mathfrak{p})$ for the exponent $e_i$ and call it the **ramification index** of $\mathcal{P}_i$ over $\mathfrak{p}$. We say that $\mathcal{P}_i$ is **ramified** if either $e_i > 1$ or the **residual** field extension $S/\mathcal{P}/R/\mathfrak{p}$ is not separable.[1] We say $\mathfrak{p}$ **ramifies** if some $\mathcal{P}$ lying over $\mathfrak{p}$ is ramfied; otherwise we say $\mathfrak{p}$ is **unramified** in $S/R$.

**Theorem 1.** *A prime $\mathfrak{p}$ of $R$ ramifies iff it divides the discriminant ideal $\Delta(S/R)$. Therefore at most finitely many primes ramify.*

For any prime $\mathcal{P}_i$ lying over $\mathfrak{p}$, we have an obvious composite homomorphism $R \to S \to S/\mathcal{P}_i$, the kernel of which is $\mathcal{P}_i \cap R = \mathfrak{p}$. In other words we get an injection

$$R/\mathfrak{p} \hookrightarrow S/\mathcal{P}_i. \tag{1}$$

Indeed, because nonzero prime ideals in a Dedekind ring are maximal, (1) is a field extension, called the **residual extension**. A finite set of generators for $S$ over $R$ (which, again, necessarily exists because $L/K$ is separable) certainly gives a set of generators for $S/\mathcal{P}_i/R/\mathfrak{p}$, i.e., the **residual degree** $f_i$ is finite.

We have the following simple and important relation:

**Theorem 2.** *For any prime $\mathfrak{p}$ in $R$, in the factorization $\mathfrak{p}S = \prod_{i=1}^{g} \mathcal{P}_i^{e_i}$, we have*

$$\sum_{i=1}^{g} e_i f_i = [L : K]. \tag{2}$$

Proof: See, e.g. [ZS, Corollary, p. 287] for the general case; see almost any text on algebraic number theory (or Matt Baker's online notes) for the case of number fields.

[1] Since in the cases of interest to us, the residual extension is an extension of finite fields hence automatically separable, the reader can safely ignore this part of the definition for the rest of the course. But in general we need the more complicated definition in order for Theorem 1 to hold.

More terminology: an unramified prime $\mathfrak{p}_i$ **splits completely** in $S$ if $g = n$ (equivalently $e_i = f_i = 1$ for all $i$); we say it is **inert** in $S$ if $g = 1$.

It is not hard to prove the following:

**Proposition 3.** *Let $R$ be a Dedekind domain with quotient field $K$, let $K \subset L \subset M$ be field extensions, and let $S$ (resp. $T$) denote the integral closure of $R$ in $L$ (resp. $M$). Let $\mathfrak{p}_3$ be a prime ideal in $T$; let $\mathfrak{p}_2 = \mathfrak{p}_3 \cap S$ and $\mathfrak{p}_1 = \mathfrak{p}_2 \cap R$. Then:*

$$e(\mathfrak{p}_3/\mathfrak{p}_1) = e(\mathfrak{p}_3/\mathfrak{p}_2) \cdot e(\mathfrak{p}_2/\mathfrak{p}_1),$$
$$f(\mathfrak{p}_3/\mathfrak{p}_1) = f(\mathfrak{p}_3/\mathfrak{p}_2) \cdot f(\mathfrak{p}_2/\mathfrak{p}_1).$$

That is, both ramification indices and inertial degrees are multiplicative in towers.

1.3. **Prime decomposition in a Galois extension.** Let us now assume that $L/K$ is **Galois**. This has the following important consequence:

**Theorem 4.** *For any prime $\mathfrak{p}$, the Galois group $G = \mathrm{Gal}(L/K)$ acts transitively on the set of primes $\mathcal{P}_i$ of $S$ lying over $\mathfrak{p}$.*

Proof: Let $\mathcal{P}_i \neq \mathcal{P}_j$ be distinct primes lying over $\mathfrak{p}$. Suppose, for the sake of contradiction, that for all $\sigma \in G$ we have $\sigma\mathcal{P}_i \neq \mathcal{P}_j$. By CRT, there exists $x \in S$ such that $x \equiv 0 \pmod{\mathcal{P}_j}$ and for all $\sigma \in G$, $x \equiv 1 \pmod{\sigma\mathcal{P}_i}$. But $N_{L/K}(x) = \prod_{\sigma \in G} \sigma x$ lies in $S \cap K = R$ and indeed in $\mathcal{P}_j \cap R = \mathfrak{p}$. But for all $\sigma \in G$, $x$ is not in $\sigma^{-1}\mathcal{P}_i$, i.e., $\sigma x \not\in \mathcal{P}_j$. This contradicts the fact that $\prod_{\sigma \in G} \sigma x$ lies in the prime ideal $\mathfrak{p}$.

**Corollary 5.** *If the extension is Galois, then there exist integers $e$ and $f$ such that for all $1 \leq i \leq g$ we have $e_i = e$ and $f_i = f$. Therefore (2) simplifies to*

$$efg = [L : K]. \tag{3}$$

Exercise 5.1.1: Prove Corollary 5.

Let $\mathcal{P}$ be a prime of $S$ lying over $\mathfrak{p}$ in $R$. We define the **decomposition group**

$$D(\mathcal{P}/\mathfrak{p}) = \{\sigma \in \mathrm{Gal}(L/K) \mid \sigma\mathcal{P} = \mathcal{P}\}.$$

In other words, the decomposition group is the stabilizer of $\mathcal{P}$ under the action of $\mathrm{Gal}(L/K)$ on the ideals lying above $\mathfrak{p}$. Because this action is transitive, we have $[\mathrm{Gal}(L/K) : D(\mathcal{P}/\mathfrak{p}] = g$, so

$$\#D(\mathcal{P}/\mathfrak{p}) = ef.$$

In general, the decomposition group does depend upon the choice of $\mathcal{P}$ lying over $\mathfrak{p}$, but only up to conjugacy: we know that any other prime $\mathcal{Q}$ lying over $\mathcal{P}$ is of the form $\mathcal{Q} = \sigma\mathcal{P}$ for some $\sigma \in \mathrm{Gal}(L/K)$, and then as an easy fact of pure group theory we have

$$D(\sigma\mathcal{P}/\mathfrak{p}) = \sigma D(\mathcal{P}/\mathfrak{p})\sigma^{-1}.$$

Exercise 5.1.2: Prove it.

In particular, if we are so fortunate so as to have $\mathrm{Gal}(L/K)$ abelian (and we will be!), the decomposition group will depend only upon $\mathfrak{p}$.

Let us simplify the notation by writing $k = R/\mathfrak{p}$ and $l = S/\mathcal{P}$.

The next key observation is that we have a canonical homomorphism $\Phi : D(\mathcal{P}/\mathfrak{p}) \to \mathrm{Aut}(l/k)$, $\sigma \mapsto \overline{\sigma}$. Namely, for $x + \mathcal{P} \in l$, we define

$$\overline{\sigma}(x + \mathcal{P}) := (\sigma(x) + \mathcal{P}).$$

This is well-defined since if $x - x' \in \mathcal{P}$, $\sigma(x - x') = \sigma(x) - \sigma(x') \in \sigma(\mathcal{P}) = \mathcal{P}$.

We now assume that the residue field $k$ is **perfect**.

**Theorem 6.** *The residual extension $l/k$ is normal, hence Galois since $k$ is perfect. The homomorphism $\Phi : D(\mathcal{P}/\mathfrak{p}) \to \mathrm{Gal}(l/k)$ is surjective. Therefore, writing $I(\mathcal{P}/\mathfrak{p})$ for its kernel, we have a short exact sequence of finite groups*

$$1 \to I(\mathcal{P}/\mathfrak{p}) \to D(\mathcal{P}/\mathfrak{p}) \stackrel{\Phi}{\to} \mathrm{Gal}(l/k) \to 1,$$

*and $\#I(\mathcal{P}/\mathfrak{p}) = e$.*

Proof:[2] First, since $L/K$ is Galois, there exists a degree $[L : K]$ monic polynomial $P(t) \in R[t]$, irreducible over $K$, and splitting completely in $L$, so that $L = K[t]/(P(t))$. The field $l$ is again the splitting field of the (possibly reducible!) polynomial $\overline{P}(t) \in R/\mathfrak{p}[t]$, hence $l/k$ is normal, and thus, by our assumption that $k$ is perfect, is Galois. In particular, since it is finite separable, there is a primitive element, i.e., a single $\overline{\alpha} \in l$ such that $l = k(\overline{\alpha})$. And because it is Galois, the number of automorphisms $s$ of $l/k$ is equal to the number of conjugates of $\overline{\alpha}$. Therefore it is enough to show that every conjugate of $\overline{\alpha}$ is of the form $\Phi(\sigma)(\overline{\alpha})$ for some $\sigma \in D(\mathcal{P}/\mathfrak{p})$.

Invoking CRT, there exists an element $\alpha \in S$ whose class modulo $\mathcal{P}$ is $\overline{\alpha}$ and also satisfies $\alpha \in \mathcal{Q}$ for every other prime $\mathcal{Q}$ lying over $\mathfrak{p}$. (Check that this is equivalent to an assertion about solutions to a system of congruences modulo the various ideals lying over $\mathfrak{p}$.) Suppose $f(t) \in R[t]$ is the minimal polynomial of $\alpha$ over $K$ and let $\overline{g}(t) \in k[t]$ be the minimal polynomial of $\overline{\alpha}$ over $k$. Since every root of $f(t)$ is an $L/K$-Galois conjugate of $\alpha$, there exists a subset $H \subset G$ such that

$$f(t) = \prod_{\sigma \in H} (t - \sigma(\alpha)).$$

Put $H' = H \cap D(\mathcal{P}/\mathfrak{p})$. If $\sigma \in G \setminus D(\mathcal{P}/\mathfrak{p})$, then $\sigma^{-1}$ is also not in $D(\mathcal{P}/\mathfrak{p})$, so $\sigma^{-1}(\mathcal{P}) \neq \mathcal{P}$, and then by our choice of $\alpha$, $\alpha \in \sigma^{-1}(\mathcal{P})$, i.e., $\sigma(\alpha) \in \mathcal{P}$. So

$$\overline{f}(t) = \prod_{\sigma \in H} (t - \overline{\sigma(\alpha)})$$

$$= \prod_{\sigma \in H'} (t - \overline{\sigma(\alpha)}) \prod_{\sigma \notin H'} (t - \overline{\sigma(\alpha)}) = t^{\#H - \#H'} \prod_{\sigma \in H'} (t - \Phi\sigma(\overline{\alpha})).$$

This shows that all nonzero roots of $\overline{f}(t)$ are of the form $\Phi\sigma(\overline{\alpha})$ for some $\sigma \in D(\mathcal{P}/\mathfrak{p})$. But $\overline{f}(\overline{\alpha}) = \overline{f(\alpha)} = 0$, so $\overline{g}(t) \mid \overline{f}(t)$. Since 0 is not a root of $\overline{g}$, we conclude

$$\overline{g}(t) \mid \prod_{\sigma \in H'} (t - \Phi(\sigma)(\overline{\alpha})).$$

This shows that every $l/k$-conjugate of $\overline{\alpha}$ is of the form $\Phi(\sigma)(\overline{\alpha}$ for some $\sigma \in D(\mathcal{P}/\mathfrak{p})$, QED.

[2]The proof of this takes a little while, but is a nice application of the things we've been talking about. Parts of this proof come closely from Matt Baker's notes.

We call $I(\mathcal{P}/\mathfrak{p})$ the **inertia group**. In fact we are most pleased when it is trivial, which according to the theorem happens iff $\mathfrak{p}$ does not ramify in $L$, so in particular for all but finitely many primes.

Let us now assume further that the Dedekind ring $R$ has finite quotients. Recall that the two most important examples of this are $R = \mathcal{O}_K$, the ring of integers in a number field, and $R = \mathbb{F}_p[t]$, a polynomial ring over a finite field – or the integral closure of such an $R$ in a finite separable field extension: i.e., the coordinate ring $k[C]$ of a nonsingular, geometrically integral affine curve over a finite field $k$.

What we are assuming is that $k = \mathbb{F}_q$, and then $l = \mathbb{F}_{q^f}$. So we know that $\mathrm{Gal}(l/k)$ is cyclic of order $f$. In fact we know more than this: we have a **canonical** isomorphism $\mathbb{Z}/f\mathbb{Z} \cong \mathrm{Gal}(l/k)$, i.e., a canonical generator of $\mathrm{Gal}(l/k)$, namely the **Frobenius automorphism** $F : x \mapsto x^q$. The preimage of the Frobenius map $F$ in $D(\mathcal{P}/\mathfrak{p})$ gives a canonical **coset** $\tau_{\mathcal{P}} + I(\mathcal{P}/\mathfrak{p})$. Better yet, for all but the at most finitely many ramified primes $\mathfrak{p}$, the inertia group is trivial, and for such primes we get a canonical **Frobenius element**

$$\tau_{\mathcal{P}} \in D(\mathcal{P}/\mathfrak{p}) \subset \mathrm{Gal}(L/K).$$

The Frobenius element $\tau_{\mathcal{P}}$ depends on the choice of $\mathcal{P}$ lying over $\mathfrak{p}$ only up to conjugacy, so that the **Frobenius conjugacy class** $\tau_{\mathfrak{p}} \subset \mathrm{Gal}(L/K)$ makes sense for any unramified prime. Note that if $L/K$ is abelian, then each Frobenius conjugacy class contains a single element.

Exercise 5.1.3: let $L/K$ be a separable field extension, with Galois closure $M/K$. Show that a prime $\mathfrak{p}$ of $K$ splits completely in $L$ iff it splits completely in $M$.

## 2. Cebotarev Density Theorem

### 2.1. **Final preparations.**

Let $k$ be either $\mathbb{Q}$ or $\mathbb{F}_p(t)$; $\mathfrak{o} = \mathbb{Z}$ or $\mathbb{F}_p[t]$. Let $K/k$ be a finite separable extension and $L/K$ be a finite Galois extension. Let $R$ be the integral closure of $\mathfrak{o}$ in $K$, $S$ the integral closure of $\mathfrak{o}$ in $S$. We further write $\Sigma_R$ (resp. $\Sigma_S$) for the set of nonzero prime ideals of $R$ (resp. of $S$). For brevity, we summarize this situation by saying that $S/R$ is a **Galois extension of global rings**.

Notice that $R$ and $S$ are Dedekind rings with finite quotients, so all of the material of the previous section applies: especially, for any prime $\mathfrak{p}$ in $R$ not dividing $\Delta(S/R)$, we have a Frobenius conjugacy class $\tau_{\mathfrak{p}} \subset \mathrm{Gal}(L/K)$.

We also have (just!) one more thing: we have a norm map on the nonzero integral ideals of $R$, with the property that there are only finitely many ideals of norm less than or equal to any given number.

Let $T \subset \Sigma_R$. We say that $T$ **has a natural density** if

$$\lim_{x \to \infty} \frac{\#\{I \in T \mid N(I) \leq x\}}{\#\{I \in \Sigma_R \mid N(I) \leq x\}}$$

exists; if so we define its natural density $\delta(T) \in [0,1]$ to be the above limit.

We say that $T$ **has a Dirichlet density** if

$$\lim_{s \to 1^+} \frac{\sum_{\mathfrak{p} \in \mathcal{T}} N(\mathfrak{p})^{-s}}{\sum_{\mathfrak{p} \in \Sigma_R} N(\mathfrak{p})^{-s}}$$

exists; if so we define its Dirichlet density $\delta_D(T) \in [0,1]$ to be the above limit.

Exercise 5.2.0: Let $T \subset \Sigma_R$.
a) Show that if $T$ has a natural density, then it has a Dirichlet density and $\delta_D(T) = \delta(T)$.
b) Exhibit a $T$ which has a Dirichlet density but no natural density.

For any group $G$, a **normal subset** $T \subset G$ will be a subset which is invariant under conjugation: for all $\sigma \in G$, $\sigma T \sigma^{-1} = S$.

Exercise 5.2.1: Show that a subset $T$ of $G$ is normal iff it is a disjoint union of conjugacy classes.

A trivial but important remark: if $G$ is abelian, all subsets are normal.

2.2. **The Chebotarev Density Theorem.**

**Theorem 7.** *(Chebotarev, 1922) Let $S/R$ be a Galois extension of global rings, with $G = \mathrm{Gal}(L/K)$. Let $X \subset G$ be a normal subset, and consider the* ***Chebotarev set*** *$T_X \subset \Sigma_R$ of prime ideals $\mathfrak{p}$ which are unramified in $S$ and such that the Frobenius conjugacy class $\tau_{\mathfrak{p}}$ is contained in $X$.*
*a) The set $T_X$ has Dirichlet density $\frac{\#X}{\#G}$.*
*b) If $\mathrm{char}\, K = 0$, then $T_X$ has natural density $\frac{\#X}{\#G}$.*

Exercise 5.2.2: Suppose that you know Chebotarev Density when $T \subset G$ is a single conjugacy class. Deduce the general case.

**Corollary 8.** *For any separable extension $S/R$ of local rings with $[L:K] = n$, the density of the set $\mathcal{S}$ of primes $\mathfrak{p}$ of $R$ which split completely in $S$ is $\frac{1}{\#\,\mathrm{Gal}(M/K)}$, where $M$ is the Galois closure of $L/K$. In particular we have*

$$\frac{1}{n!} \leq \delta(S) \leq \frac{1}{n}.$$

Exercise 5.2.3: Prove Corollary 8. (Hint: use Exercise 5.1.3.)

**Corollary 9.** *(Equidistribution of Frobenius elements in the abelian case) With notation as above, suppose that $G = \mathrm{Gal}(L/K)$ is abelian. Then for any $\sigma \in G$, the set of unramified primes $\mathfrak{p}$ such that $\tau_{\mathfrak{p}} = \sigma$ has density $\frac{1}{\#G}$.*

Rhe "intersection" of Corollaries 8 and 9 is important in of itself: that in an abelian extension $L/K$ of degree $n$, the set of unramified primes $\mathfrak{p}$ of $R$ for which $\tau_{\mathfrak{p}} = 1$ –

i.e., which split completely in $L$ – has density $\frac{1}{n}$.[3]

Example 5.2.1.1: Let $L/K$ be a quadratic extension. Then the set of ramified primes is finite, and the set of primes which split completely and the set of inert primes both have density $\frac{1}{2}$. Applying this in particular to $K = \mathbb{Q}$, $L = \mathbb{Q}(\sqrt{D})$, this gives: for $(p, 4D) = 1$, the set of primes $p$ such that $(\frac{D}{p}) = 1$ and the set such that $(\frac{D}{p}) = -1$ each have density $\frac{1}{2}$.

Example 5.2.1.2: Let $K = \mathbb{Q}$ and $L = \mathbb{Q}(\zeta_n)$, where $\zeta_n$ is (still) a primitive $n$th root of unity. The well-known irreducibility of the cyclotomic polynomials easily implies that $\mathrm{Gal}(L/K) = (\mathbb{Z}/n\mathbb{Z})^\times$, the isomorphism being given by $a \pmod n \mapsto (\zeta_n \mapsto \zeta_n^a)$. Recall that every prime not dividing $n$ is unramified. So for $p$ with $\gcd(p, n) = 1$, there is a well-defined Frobenius element $\tau_p$ in $G$; it is a great exercise to check that under the above isomorphism $\tau_p$ is precisely the class of $p$ in $(\mathbb{Z}/n\mathbb{Z})^\times$. Thus in this very special case we recover the following seminal result:

**Theorem 10.** *(Dirichlet's Theorem) For $n \in \mathbb{Z}^+$ and any $a$ with $\gcd(a, n) = 1$, the set of primes $p$ which are congruent to $a \pmod n$ has density $\frac{1}{\varphi(n)}$.*

Exercise 5.2.4: Let $P(t) \in \mathbb{Z}[t]$ be a monic polynomial of positive degree $d$. For a prime number $\ell$, let $\tilde{P}_\ell \in \mathbb{F}_\ell[t]$ denote the obvious (coefficientwise) modulo $\ell$ reduction of $P$.
a) If $P$ is reducible over $\mathbb{Z}[t]$, then for all $\ell$, $\tilde{P}_\ell$ is reducible over $\mathbb{F}_\ell[t]$. Thus, applying the contrapositive, we get a sufficient condition for irreducibility of $P$: it suffices for $\tilde{P}_\ell$ to be reducible for some $\ell$.
b) Suppose that the degree $d$ is a **prime number**. Show a (much more interesting) converse: the set of primes $\ell$ such that $\tilde{P}_\ell(t)$ is irreducible has positive density.
c)* Find an irreducible quartic (i.e., $d = 4$) polynomial all of whose mod $\ell$ reductions are reducible.
d)** Show that a polynomial as in part c) exists for all composite degrees $d$.[4]

## 2.3. **Some further remarks.**

Theorem 7 was conjectured by Frobenius in 1896. He was able to prove a substantial special case: in the **Frobenius Density Theorem** the subset $T$ must be invariant under conjugation and also have the property that if $\sigma \in T$, so is every other generator of the cyclic subgroup generated by $\sigma$, i.e., for all $i$ prime to the order of $\sigma$, $\sigma^i \in T$. Note that when $G$ is a symmetric group (which is what the Galois group of an extension of global fields will be "with probability 1") the first condition implies the second, since $\sigma^i$ has the same cycle type as $\sigma$. Also Frobenius' theorem applies in the case in which $T$ is a normal sub**group** of $G$; in particular it applies to $T = \{e\}$, giving Corollary 8.

Nikolai Grigorevich Chebotarev was born in 1896 and died in 1947. He proved

[3]This special case was proved much earlier by Frobenius: see below.

[4]This is proved in a 1986 Monthly paper of Brandl. The generalization to polynomials over any global ring is proved in *Irreducible polynomials which are locally reducible everywhere*, Guralnick, Schacher and Sonn, Proc. AMS 133 (2005), 3171-3177.

the density theorem in summer of 1922, having just turned 26, while being physically occupied with rather menial labor (e.g., bringing buckets of cabbages to the market for his mother to sell) in the city of Odessa. He was not able to defend his dissertation (on the density theorem) until 1927.

Stricitly speaking what Chebotarev proved was weaker than Theorem 7: he proved the result when $K$ is a number field and for the Dirichlet density $\delta_D(T_X)$.

The generalization to natural density in the number field case is a significant piece of analytic number theory. Even in the special case of Dirichlet's Theorem (proved in the case of Dirichlet density by....Dirichlet), the version for natural density was not proven until much later by de la Vallée Poussin. Apparently the replacement of Dirichlet density by natural density in the full-fledged Chebotarev Theorem was first done by Hecke (and is sufficiently difficult not to be found in any of the standard texts that I have consulted). It should be noted that in the vast majority of cases the real import of the Density Theorem is to show that the set of primes in question is infinite, and for this it certainly doesn't matter which density is used.

The proof in the function field case – $\operatorname{char} K > 0$ – is not dramatically different, and in some ways it is simpler. It seems to have first been proven by Reichardt in 1936. The argument is similar to Chebotarev's and in some ways simpler.

However, in the function field case it is not always true that the *natural* density $\delta(T_X)$ exists! It turns out that $\delta_D(T_X)$ exists when the extension $L/K$ has trivial constant field extension – i.e., if the algebraic closure of $\mathbb{F}_p$ in $K$ is algebraically closed in $L$ – but there are counterexamples in the general case. This was pointed out to me by Melanie Matchett Wood on 6/19/13, correcting an error in the way Theorem 7 had originally been stated (in spring 2008). Wood also suggests the reference [Ba08] for more information on this phenomenon.

There are **effective** versions of the Chebotarev Density Theorem, i.e., one can give an explicit upper bound on the norm of the least unramified prime $\mathfrak{p}$ whose Frobenius conjugacy class lies in the normal subset $T$ of $\mathrm{Gal}(L/K)$. I have had occasion to look at such estimates in joint work with A.C. Cojocaru: as one might imagine, the estimates depend on all the quantities in question (especially, the discriminant $\Delta(S/R)$) in a somewhat complicated way. What is unconditionally known is somewhat disappointingly weaker than what should be true: if one is willing to assume the Generalized Riemann Hypothesis (GRH) then there are bounds which are a full logarithm better than the unconditional bounds.

## 3. Class Field Theory

### 3.1. The Artin Map.

Let $S/R$ be a Galois extension of global rings, such that $G = \mathrm{Gal}(L/K)$ is **abelian**. Let $\Delta$ be the discriminant of $L/K$. Let $I(\Delta)$ denote the group of all fractional ideals of $R$ which are (in the obvious sense) prime to $\Delta$. Then $I(\Delta)$ is the free abelian group generated by prime ideals $\mathfrak{p}$ not dividing $\Delta$; in particular, because of this freeness, there is a unique homomorphism of abelian groups

$$\mathfrak{r} : I(\Delta) \to \mathrm{Gal}(L/K)$$

which extends the map $\mathfrak{p} \mapsto \tau_{\mathfrak{p}}$ on primes. This map goes by various intimidating names: e.g. **Artin symbol**, **reciprocity map**.

Notice that Chebotarev Density asserts, in particular; that every element of $\mathrm{Gal}(L/K)$ is hit by infinitely many primes $\mathfrak{p}$, so certainly the homomorphism $r$ is **surjective**.

Evidently then $\mathfrak{p}$ induces a canonical isomorphism of groups

$$I(\Delta)/\ker(\mathfrak{r}) \xrightarrow{\sim} \mathrm{Gal}(L/K).$$

Therefore the obvious question to ask – the main question of class field theory – is:

**WHAT IS THE KERNEL OF $\mathfrak{r}$??**

Notice that what is nice about $I(\Delta)$ is that it doesn't make reference to the extension $L$ at all; certainly we can consider $I(\mathfrak{c})$ – the subgroup of fractional ideals prime to $\mathfrak{c}$ – for any (nonzero) integral ideal $\mathfrak{c}$ of $R$. The goal of class field theory is to similarly describe the kernel $\mathfrak{r}$ in terms of "the arithmetic of $K$". Admittedly this a confusing statement, because obviously the abelian extension $L$ has to come into the picture somewhere; it already has by virtue of the discriminant $\Delta$, but we certainly need more information than this, because – as we shall see shortly! – there can be more than one abelian extension $L/K$ with a given discriminant. So things must be a bit more complicated, and indeed they are.

### 3.2. **Moduli and ray class fields.**

What we can do is define a certain **family** $\{K(\mathfrak{m})\}$ of abelian extensions which are parameterized solely by some arithmetic data $\mathfrak{m}$ from $K$ (you are not yet supposed to know what this means; don't worry). These field $K(\mathfrak{m})$ are called **ray class fields** of $K$. Again, it is too much to hope for that every finite abelian extension of $K$ is a ray class field, but what turns out to be true is that every abelian extension $L$ is **contained** in some ray class field – in fact, in infinitely many ray class fields, but there will be a unique **smallest** ray class field containing $L$. The Galois theory of subextensions of abelian extensions behaves beautifully – in particular every subextension is Galois – so that if we know all the ray class fields, we have a good chance at understanding all the finite abelian extensions.

Let me now describe the objects $\mathfrak{m}$ by which ray class fields are parameterized.

For this we need to say something about real places of number fields. Let us say at the outset that our main application of all this will be in the case of $K$ an imaginary quadratic field, in which case there are no real places. So, on a first reading, it might be a good strategic move to simply ignore the entire business about real places, at least until you get to the example of $K = \mathbb{Q}$, which goes a long way towards clarifying what is going on with them.

Anyway, recall that if $K/\mathbb{Q}$ is a number field of degree $d$, say given as $\mathbb{Q}[t]/(P(t))$, then the embeddings of $K$ into $\mathbb{R}$ correspond precisely to the real roots of $P(t)$: in particular there is somewhere between 0 and $[K : \mathbb{Q}]$ such embeddings. Let us label these embeddings $\infty_1, \infty_2, \ldots, \infty_r$. We call such embeddings "real places."

Example 5.3.2.1: $\mathbb{Q}$ has, of course, one real embedding. For a squarefree $D > 1$, the field $\mathbb{Q}(\sqrt{D})$ has two real embeddings: the usual one $a + b\sqrt{D}$, and the one obtained by applying Galois conjugation, namely $a + b\sqrt{D} \mapsto a - b\sqrt{D}$. If $D < 0$ there are, evidently, no real embeddings.

The function field case is simpler: there are no real embeddings to worry about.[5]

Now a **modulus** $\mathfrak{m}$ is a formal product of two different quantities: the first, **finite** part $\mathfrak{m}_0$, is precisely a nonzero integral ideal of $R$, which we further view (as we have before) as a formal product $\prod_{\mathfrak{p}} \mathfrak{p}^{\mathrm{ord}_{\mathfrak{p}}(\mathfrak{m}_0)}$. In the function field case $\mathfrak{m} = \mathfrak{m}_1$; if $K$ is a number field which has real places, then there is also an **infinite part** $\mathfrak{m}_\infty$, which you can think of as a subset of the real places but you write formally as a product: if, say, $\Sigma_S^\infty = \{\infty_1, \ldots, \infty_r\}$ is the set of real places of $K$, then for some subset $Z \subset \Sigma_S^\infty$, we write the corresponding $\mathfrak{m}_2$ as $\prod_{\infty_i \in Z} \infty_i$. The whole modulus is formally written as $\mathfrak{m}_1 \cdot \mathfrak{m}_2$. Let us write simply $\infty$ for the product of all the real places of $K$ (if there are any at all).

For a prime $\mathfrak{p}$ of $R$ and a modulus $\mathfrak{m}$, define $\mathrm{ord}_{\mathfrak{p}} \mathfrak{m}$ just to be $\mathrm{ord}_{\mathfrak{p}}(\mathfrak{m}_0)$.

Example 5.3.2.2: When $R = \mathbb{Z}$, a modulus is either the ideal generated by a positive integer $(n)$, or $(n) \cdot \infty$.

For any modulus $\mathfrak{m}$, we define $I(\mathfrak{m}) = I(\mathfrak{m}_0)$, i.e., fractional ideals prime to the finite part of the modulus. Now we also define a subgroup of $I(\mathfrak{m})$, namely $P(\mathfrak{m})$, to be the subgroup generated by principal fractional ideals $(\alpha)$ with a generator $\alpha$ satisfying:

(i) for all primes $\mathfrak{p}$, $\mathrm{ord}_{\mathfrak{p}}(x - 1) \geq \mathrm{ord}_{\mathfrak{p}} \mathfrak{m}$, and (ii) For all $\infty_i \in \mathfrak{m}_\infty$, $\infty_i(\alpha) > 0$.

Note (i) implies $\alpha \in R$, i.e., these are principal **integral ideals**. So $\alpha^{-1}$ need not be in $R$, and that is why we are taking the subgroup generated by these guys. In fact this is one case where thinking solely in terms of integral ideals seems cleaner:

Exercise 5.3.1: Show that the quotient group $I(\mathfrak{m})/P(\mathfrak{m})$ can be identified with the quotient of the monoid of integral ideals prime to $\mathfrak{m}$ by the submonoid of principal integral ideals $xR$, where $x$ satisfies (i) and (ii) above.

Example 5.3.2.3: Again let $R = \mathbb{Z}$. If $\mathfrak{m} = (n)$, then $P(\mathfrak{m})$ just consists of principal ideals $I$ which can be expressed in the form $(x)$ with $x \equiv 1 \pmod{n}$. Note that the "expressed" is important here; since every nonzero ideal of $\mathbb{Z}$ has precisely two generators – $x$ and $-x$ – what this really says is that $I$ is generated by something which is $\pm 1 \pmod{n}$.

Exercise 5.3.2: Show that $I((n))/P(n)) \cong (\mathbb{Z}/n\mathbb{Z})^\times/(\pm 1)$.

[5]Nevertheless one hears about "real" and "imaginary" function fields: there is in fact a reasonable *analogue* to real embeddings in the function field case. But I had better not say more about this here.

The other kind of modulus is $\mathfrak{m} = (n)\infty$. Then $P(\mathfrak{m})$ consists of principal ideals $I$ which can be expressed in the form $(x)$ with $x > 0$ and $x \equiv 1 \pmod{n}$.

Exercise 5.3.3: a) Show that for $n > 2$, $[P((n)) : P((n)\infty)] = 2$.
b) Show that $I((n)\infty)/P((n)\infty) \cong (\mathbb{Z}/n\mathbb{Z})^\times$.

There is a fairly evident notion of divisibility of moduli: we say that $\mathfrak{m} \mid \mathfrak{m}'$ if the finite part of $\mathfrak{m}$ divides the finite part of $\mathfrak{m}'$ in the usual sense of ideal division and if the set of real places in $\mathfrak{m}$ is a subset of the set of real places in $\mathfrak{m}'$. So e.g. for $K = \mathbb{Q}$ we have $(2) \mid (12) \mid (60\infty)$.

If $L/K$ is a finite extension and $\infty_i$ is a real place of $K$, we say that it is **unramified** in $L$ if every extension of $\infty_i$ to an embedding $\iota : L \hookrightarrow \mathbb{C}$ has $\iota(L) \subset \mathbb{R}$. Otherwise we say that it ramifies. For example, the place $\infty$ of $\mathbb{Q}$ ramifies in an imaginary quadratic field but not in a real quadratic field. More generally, if $K$ is a number field, then $K/\mathbb{Q}$ is unramified at $\infty$ if for every embedding $\iota : K \hookrightarrow \mathbb{C}$ we have $\iota(K) \subset \mathbb{R}$. Such number fields are called **totally real**. (When $[K : \mathbb{Q}] > 2$ this is a stronger condition than just saying that $K$ can be embedded into $\mathbb{R}$.)

At last we can describe the ray class fields $K(\mathfrak{m})$, at least indirectly.

For each modulus $\mathfrak{m}$, there exists a finite abelian extension $K(\mathfrak{m})/K$, called the **$\mathfrak{m}$-ray class field** of $K$, with the following properties:

(RC1) $\mathfrak{p} \mid \Delta(K(\mathfrak{m})/K) \implies \mathfrak{p} \mid \mathfrak{m}$; also if an infinite place $\infty_i$ of $K$ ramifies in $K(\mathfrak{m})$ then $\infty_i \mid \mathfrak{m}$.

In other words, the extension is only ramified at primes (including "infinite primes") dividing the modulus.

In view of (RC1), we may restrict the Artin map to have domain $I(\mathfrak{m})$:

$$\mathfrak{r} : I(\mathfrak{m}) \to \mathrm{Gal}(K(\mathfrak{m})/K).$$

(Chebotarev tells us that this restricted map is still surjective.)

(RC2) The kernel of the restricted Artin map is precisely the subgroup $P(\mathfrak{m})$.

Therefore there is a canonical isomorphism

$$r : I(\mathfrak{m})/P(\mathfrak{m}) \xrightarrow{\sim} \mathrm{Gal}(K(\mathfrak{m})/K).$$

(RC3) If $\mathfrak{m} \leq \mathfrak{m}'$, $K(\mathfrak{m}) \subseteq K(\mathfrak{m}')$.

The relation $\leq$ endows the moduli with the structure of a directed set (a partially ordered set in which any pair of elements is less than or equal to some third element). Therefore by (RC3) the ray class fields form a directed system of fields.

(RC4) $\varinjlim_{\mathfrak{m}} K(\mathfrak{m}) = K^{\mathrm{ab}}$, the maximal abelian extension of $K$.

This is a somewhat fancy way of saying that every finite abelian extension is contained in some ray class field. In fact we can be much more precise than this:

For a finite abelian extension $L/K$, put

$$\Gamma(L) = \mathrm{Ker}(r : I(\Delta(S/R)) \to \mathrm{Gal}(L/K)).$$

(RC5) There exists a unique smallest modulus $\mathfrak{c}$ such that $L \subset K(\mathfrak{m})$. Moreover, tfor this minimal $\mathfrak{c}$: the finite part of $\mathfrak{c}$ is divisible only by primes dividing $\Delta(L/K)$; the infinite part of $\mathfrak{c}$ includes no unramified inifnite places; and $P(\mathfrak{c}) \subset \Gamma(L)$, so that we have a short exact sequence

$$1 \to \Gamma(L)/P(\mathfrak{c}) \to I(\mathfrak{c})/P(\mathfrak{c}) \to \mathrm{Gal}(L/K) \to 1$$

exhibiting the Galois group of an arbitrary finite abelian extension $L/K$ as a quotient of a certain ray class group.

The minimal modulus $\mathbf{c}$ for $L/K$ of (RC5) is called the **conductor** of $L/K$.[6]

The main result of (global) class field theory is that there is indeed a unique family of fields satisfying all of these properties. (This was first shown by Artin, drawing partly on Chebotarev's proof of his density theorem.) There is no way we are going to discuss the proof here. Not only are all known proofs extremely long and difficult, what is worse they are not really enlightening. The essential point is that although the proof of the theorem involves "constructing" the ray class fields in the sense of showing their existence, this construction is in general very far from being constructive or explicit. One of the great open problems in algebraic number theory is to give a reasonable explicit construction of the class fields of a given number field $K$. There are only two cases which are completely understood: the case of $\mathbb{Q}$, which we will give (without proof) as an example below, and the case of an imaginary quadratic field, in which the explicit construction of ray class fields as torsion fields of suitable CM elliptic curves is the ultimate goal of our course.

### 3.3. **The Hilbert Class Field.**

First however let us note the following extremely important special case: take $\mathfrak{m} = 1$, i.e., the "empty modulus."

**Theorem 11.** *Concerning the ray class field $K(1)/K$:*
*a) It is the maximal everywhere unramified abelian extension of $K$.*
*b) The map $r$ induces a canonical isomorphism $I(1)/P(1) = \mathrm{Pic}(R) \xrightarrow{\sim} \mathrm{Gal}(K(1)/K)$.*
*c) A prime ideal $\mathfrak{p}$ of $R$ splits completely in $K(1)$ iff it is a principal ideal of $R$.*

Proof: (RC1) says that $K(1)$ cannot be ramified anywhere (not even at the real places, if any). Moreover, (RC5) implies that any finite everywhere unramified abelian extension $L$ is contained in $K(1)$, establishing a). By definition the Picard group of the Dedekind ring $R$ is the fractional ideals modulo the principal fractional ideals, i.e., $I(1)/P(1)$, so b) follows from (RC2). Similarly part c) follows because a prime splits completely iff its Frobenius element is trivial iff it lies in the kernel $P(1)$ of the Artin map, i.e., is principal.

[6]Yes, we will eventually be able to relate this to the conductor of a quadratic order.

Definition: The extension $K(1)/K$ is called the **Hilbert class field** of $K$.

As Theorem 11 shows, the Hilbert class field has some remarkable (and useful) properties. In particular, the theorem implies that the maximum everywhere unramified abelian extension of $K$ is finite, which is certainly not obvious.[7]

We now have enough firepower to prove our Main Theorem when $n$ is squarefree and congruent to 1 or 2 mod 4, so that $D = -4n$ is the discriminant of the field $\mathbb{Q}(\sqrt{D})$: using Theorems 7 and 11, we will be able to show that the density of the set of primes $p$ of the form $x^2 + ny^2$ is $\frac{1}{2h(-4n)}$, where $h(-4n) = \#\operatorname{Pic}(\mathcal{O}(-4n))$. It would be good to think about this now; the only remaining problem in this case is consolidating the Chebotarev condition for $K^1/K$ and the splitting condition $(\frac{D}{p}) = 1$ coming from the fundamental congruence.

Of course we also have to worry about the case of nonmaximal discriminant, which is where the ray class fields fit in. For any discriminant $D < 0$, we will be able to identify $\operatorname{Pic}(\mathcal{O}(D)$ with the Galois group of some abelian extension $K_D/K$. In fact we will really need to use all the material we have summarized above, since $K_D$ is *not* a ray class field but (like every finite abelian extension!) a subfield of some minimal ray class field. It turns out that the conductor of the extension $K_D$ we're looking for is the conductor $f$ (i.e., the principal ideal $fR$) of the order in the previous sense, so that $\operatorname{Gal}(K_D/K) \cong I(\mathfrak{f})/\Gamma_D$ for a group $\Gamma_D$ properly containing $P(\mathfrak{f})$; the group $\Gamma_D$ will be simultaneously interpretable in terms of certain principal ideals of $\mathcal{O}_K$ and certain principal ideals of $\mathcal{O}(D)$.

### 3.4. **Class field theory over $\mathbb{Q}$.**

But first let us look at the one case where it is easy to at least state what the class fields are: $K = \mathbb{Q}$. Recall that we computed above that if $\mathfrak{m} = n$, the quotient $I(\mathfrak{m}/P(\mathfrak{m})$ is isomorphic to $(\mathbb{Z}/n\mathbb{Z})^\times/\pm 1$, whereas if $\mathfrak{m} = n\infty$, the same quotient is isomorphic to $(\mathbb{Z}/n\mathbb{Z})^\times/\pm 1$.

So we would like to find, or at least to correctly guess, for every positive integer $n$ an abelian extension $\mathbb{Q}(n)/\mathbb{Q}$ whose Galois group is $(\mathbb{Z}/n\mathbb{Z})^\times/\pm 1$ and another abelian extension $\mathbb{Q}(n\infty)/\mathbb{Q}$ with Galois group $(\mathbb{Z}/n\mathbb{Z})^\times$.

If we have made it this far, we would have to guess that $\mathbb{Q}(n\infty) = \mathbb{Q}(\zeta_n)$, wouldn't we? It has the right Galois group and the right ramification properties: the only finite primes at which if ramifies are those dividing $n = \mathfrak{m}$, in accordance with (RC1). In fact in a previous exercise we computed the Artin map in this case, so we can verify that these are the $(n\infty)$-ray class fields: I leave it to you to do so.

What about the moduli $\mathfrak{m} = n$? The point here is that we have not included $\infty$, so that by (RC1) the ray class field $\mathbb{Q}(n)$ is not allowed to ramify at $\infty$: in other words, it must be totally real.

[7]In fact, for some number fields $K$ – not $\mathbb{Q}$, but e.g. for certain quadratic fields – there exist everywhere unramified (non-abelian) extensions of arbitrarily large degree.

Exercise 5.4.1: Figure out what the ray class field $\mathbb{Q}(n)$ is.

Applying (RC3) we get a very important result:

**Theorem 12.** *(Kronecker-Weber) A finite extension $K/\mathbb{Q}$ is abelian iff it is a subfield of some cyclotomic field $\mathbb{Q}(\zeta_n)$. Equivalently, the maximal abelian extension $\mathbb{Q}^{ab}$ of $\mathbb{Q}$ is the (infinite algebraic) extension obtained by adjoining to $\mathbb{Q}$ all roots of unity.*

In particular, we have a single transcendental function, namely $e(t) := e^{2\pi it}$ which maps $\mathbb{R}/\mathbb{Z}$ isomorphically to the unit circle in the complex plane. Then for all $n$, the $n\infty$-ray class field of $\mathbb{Q}$ is obtained by adjoining to $\mathbb{Q}$ the value of the function $e$ at the $n$-torsion points of the one-dimensional torus $\mathbb{R}/\mathbb{Z}$, namely at $\frac{1}{n}, \ldots, \frac{n-1}{n}$ (or also at just $\frac{1}{n}$, of course). Wouldn't it be amazing if all (or a cofinal set) of class fields for any number field $K$ could be obtained just by adjoining special values of a nice transcendental function? This was Kronecker's **Jugendtraum** ("youthful dream.") We will see later that this dream comes true when $K$ is an imaginary quadratic field.[8]

Exercise 5.4.2: a) Notice that $\mathbb{Q}(1) = \mathbb{Q}(\infty)$, which shows that the association of a ray class field to a modulus need not be injective.
b) Find all moduli $\mathfrak{m}$ such that $\mathbb{Q}(\mathfrak{m}) = \mathbb{Q}$.
c) Show that if $n$ is odd, then $\mathbb{Q}(n \cdot \infty) = \mathbb{Q}(2n \cdot \infty)$.
d) Find all pairs $\mathfrak{m} \neq \mathfrak{m}'$ such that $\mathbb{Q}(\mathfrak{m}) = \mathbb{Q}(\mathfrak{m}')$.

Remark: Unfortunately, this exercise implies that the conductor $\mathfrak{c}$ of the $\mathfrak{m}$-ray class field $K(\mathfrak{m})$ may be strictly smaller than $\mathfrak{m}$, unlike what virtually everyone feels entitled to expect. However, Exercise 5.4.2 seems to suggest that the discrepancy is small enough so that we should virtually pretend that $\mathfrak{c}(K(\mathfrak{m})) = \mathfrak{m}$. Watch for this in the quadratic case...

Exercise 5.4.3: Let $p$ be an odd prime. Certainly $\mathbb{Q}(\sqrt{p})/\mathbb{Q}$ is an abelian extension. What is its conductor?

Exercise 5.4.4*: Use class field theory to prove the quadratic reciprocity law.

3.5. **Remarks.**

We have given an exposition of the "ideal class" version of global class field theory. This was indeed the approach of Artin and other early 20th century mathematicians. Around the middle of the 20th century Chevalley developed another approach, using **idéles**: this is a theory which makes more direct contact with **local class field theory**, and also has a more topological (and even Fourier-analytic) flavor. Also in contemporary approaches to class field theory there is much more emphasis on connections to Galois cohomology (and especially, to Brauer groups).

[8]Much of the work on automorphic functions in number theory in the last 50 years has been motivated by a desire to extend this Jugendtraum to other fields. There are indeed some results in this direction, but it is remarkable how much more complicated any other case is – even for e.g. a real quadratic field there is not to my knowledge a complete, satisfactory answer.

All these things are important to learn at some point, but it seems best to see just a taste of what class field theory is, then see it applied to some nontrivial problem, and then perhaps seeing the more sophisticated techonology appearing more helpful/inevitable down the line. (For instance, to properly treat aspects of complex multiplication for non-maximal quadratic orders – an issue which has arisen in our VIGRE group – seems to cry out for the idelic formalism.)

## References

[Ba08] C. Ballot, *Competing prime asymptotic densities in $\mathbb{F}_q[x]$: a discussion*. L'enseignment Mathématique 54 (2008), 303–328.

[ZS] O. Zariski and P. Samuel, *Commutative Algebra: Volume I*. Graduate Texts in Mathematics #28, Springer-Verlag.