Some algebraic number theory and the reciprocity map

Ervin Thiagalingam

September 28, 2015

Motivation

In Weinstein's paper, the main problem is to find a rule (reciprocity law) for when an irreducible polynomial $f \in \mathbb{Z}[X]$ splits modulo a prime p. For quadratic polynomials, splitting happens exactly when the discriminant is a square mod p and this is governed by quadratic reciprocity. Similarly, cubic reciprocity helps to answer the question for cubics. In this talk, I will explain the solution to this problem in the case f has an abelian Galois group given by class field theory and the generalized reciprocity laws obtained from it.

The first step in the solution is to move the problem into the setting of algebraic number theory. Let $f \in \mathbb{Z}[X]$ be an irreducible polynomial of degree n and let K be the splitting field of f so K/Q is a finite Galois extension with $[K : \mathbb{Q}] = n$. Let $\mathcal{O}_K$ be the integral closure of $\mathbb{Z}$ in K. This is the ring of integers in K and it has unique factorization of ideals. We will show that for all but finitely primes, f splitting mod p is equivalent to the prime ideal (p) splitting (completely) into n distinct prime ideals of $\mathcal{O}_K$, i.e. $p\mathcal{O}_K = \mathfrak{P}_1\mathfrak{P}_2 \cdots \mathfrak{P}_n$. We can do this for an extension of number fields L/K and so now the problem is to figure out when a prime in $\mathcal{O}_K$ splits in $\mathcal{O}_L$.

The Galois group $G(L/K)$ acts on the primes $\mathfrak{P}_i$ and permutes them. Using this action, we can associate to all but a finite number of primes in $\mathcal{O}_L$ a conjugacy class of $G(L/K)$ denoted $\mathrm{Frob}_{\mathfrak{p}}$. The conjugacy class determines the splitting of $\mathfrak{p}$ in that $\mathrm{Frob}_{\mathfrak{p}}$ is trivial if and if only if $\mathfrak{p}$ splits. When $G(L/K)$ is abelian, class field theory gives conditions on the prime $\mathfrak{p}$ in terms of generalized congruence relations. Namely, $\mathfrak{p}$ must be a product of a norm from $\mathcal{O}_L$ and a principal ideal generated by a "local" unit. The generalized congruence relations appear when determining the "local" units.

The Ring of Integers $\mathcal{O}_K$

To study extensions of prime ideals, we first need to know some properties of $\mathcal{O}_K$. The most important being unique factorization of ideals. To get there, we introduce a special class of integral domains.

Definition. *A ring R is a Dedekind ring if it is a noetherian integral domain such that the localization $R_{\mathfrak{p}}$ is a discrete valuation ring (DVR) for every non-zero prime ideal $\mathfrak{p}$ of R.*

It is not clear by this definition that $\mathcal{O}_K$ is a Dedekind ring but we have the following characterization.

Theorem. *(Janusz [2], Pg. 13) Let R be an integral domain which is not a field. The following are equivalent statements.*

(1) R is a Dedekind ring.

(2) For each maximal ideal $\mathfrak{p}$ of R, $R_{\mathfrak{p}}$ is a DVR and for each element $a \neq 0$ there exists only a finite number of prime ideals containing a.

(3) R is a noetherian, integrally closed domain and each non-zero prime ideal is a maximal ideal.

We have defined $\mathcal{O}_K$ as the integral closure of $\mathbb{Z}$ in K so it is already an integrally closed domain. To show $\mathcal{O}_K$ is Noetherian, we apply the Primitive Element Theorem. K over $\mathbb{Q}$ is a finite separable (characteristic 0) extension so there exists $\alpha \in K$ so that $K = \mathbb{Q}(\alpha)$. Now, we can assume α is an algebraic integer as follows. K is an algebraic extension of $\mathbb{Q}$ so α is a root of a polynomial in $\mathbb{Q}[X]$. By clearing denominators, we can assume the polynomial is in $\mathbb{Z}[X]$. Now,

$$a_n\alpha^n + a_{n-1}\alpha^{n-1} + \ldots + a_1\alpha + a_0 = 0$$

where $a_i \in \mathbb{Z}$ and $a_n \neq 0$. Then we have:

$$\begin{aligned} 0 &= a_n^{n-1} \cdot (a_n\alpha^n + a_{n-1}\alpha^{n-1} + \ldots + a_1\alpha + a_0) \\ &= (a_n\alpha)^n + a_{n-1}(a_n\alpha)^{n-1} + a_{n-2}a_n(a_n\alpha)^{n-2} \ldots + a_1a_n^{n-2}(a_n\alpha) + a_n^{n-1}a_0 \end{aligned}$$

so $a_n\alpha$ is an algebraic integer. With the existence of a basis of algebraic integers for K over $\mathbb{Q}$, we construct a integral basis for $\mathcal{O}_K$, i.e. a basis as a free abelian group under addition. If we do this any subgroup (including ideals) will also be a free abelian group of at most the same rank (Stewart [1], Pg. 28) and so will be finitely generated.

First we note that we have shown above that for any $\alpha \in K$ there exists an algebraic integer β and non-zero integer c so that $c\alpha = \beta$. So it is now easy to see that the field of fractions of $\mathcal{O}_K$ is K. Moreover, an integral basis for $\mathcal{O}_K$ will also be a basis for K over $\mathbb{Q}$. If $[K : \mathbb{Q}] = n$, we are looking for n independent algebraic integers spanning $\mathcal{O}_K$. The idea is to pick a $\mathbb{Q}$-basis of algebraic integers so that the discriminant is a minimum. The discriminant of any $\mathbb{Q}$-basis $\mathcal{B} = \{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ for K is the $[det(\sigma_i(\alpha_j))]^2$ where the σ_i are the n distinct embeddings of K into $\mathbb{C}$. It is always rational and in the case when $\mathcal{B} \subset \mathcal{O}_K$, it is a positive integer.

Theorem. *(Stewart [1], Pg. 46) Every number field K possess an integral basis, and the additive group of $\mathcal{O}_K$ is free abelian of rank n equal to the degree of K.*

Finally, to show every non-zero prime ideal $\mathfrak{p}$ of $\mathcal{O}_K$ is maximal, its is enough to show that the quotient $\mathcal{O}_K/\mathfrak{p}$ is finite since a finite integral domain is a field. The norm of an ideal $N(\mathfrak{p})$ is defined to be the cardinality of the quotient so we want to show this norm is finite. Let $0 \neq \alpha \in \mathfrak{p}$ so that $N(\alpha) = \alpha\sigma_1(\alpha)\sigma_2(\alpha)\ldots\sigma_{n-1}(\alpha) \in \mathfrak{p}$. Therefore the principal ideal $(N(\alpha)) \subset \mathfrak{p}$ so $\mathcal{O}_K/\mathfrak{p}$ is a quotient of $\mathcal{O}_K/(N(\alpha))$. Since α is an algebraic integer, $N(\alpha)$ is an integer and so as an abelian group $\mathcal{O}_K/(N(\alpha))$ is finite since $\mathcal{O}_K$ is finitely generated and every element in the quotient has order (additive) at most $|N(\alpha)|$. So $\mathcal{O}_K/\mathfrak{p}$ is also finite.

Unique Factorization and the Ideal Class Group

From the equivalences above, all primes ideals in Dedekind rings are maximal. This is actually easy to see since for a prime ideal $\mathfrak{p} \in R$, prime ideals in $R_\mathfrak{p}$ correspond to primes ideals contained in $\mathfrak{p}$. So if $\mathfrak{p}_1 \subset \mathfrak{p}_2$, $\mathfrak{p}_1 R_{\mathfrak{p}_2}$ is a prime ideal. But there are only two prime ideals in a DVR, 0 and the maximal ideal $\mathfrak{p}_2 R_{\mathfrak{p}_2}$. So either $\mathfrak{p}_1 = 0$ or $\mathfrak{p}_1 = \mathfrak{p}_2$. From this, we can get a factorization for an ideal.

Let I be an ideal of R. We show every ideal in R/I contains a product of prime ideals. Suppose there exists an ideal that does not contain a product of prime ideals. Let J be maximal w.r.t. to this property. So J is not prime and there exists $x, y \in R/I$ such that $xy \in J$ but $x, y \notin J$. Then $(J + (x))(J + (y)) = J$ contains a product of primes. So $0 = \mathfrak{p}_1^{a_1} \cdots \mathfrak{p}_n^{a_n}$ in R/I, i.e. $\mathfrak{p}_1^{a_1} \cdots \mathfrak{p}_n^{a_n} \subset I$. Looking at the image of I in $R/(\mathfrak{p}_1^{a_1} \cdots \mathfrak{p}_n^{a_n})$ gives the factorization of I.

Now that we know $\mathcal{O}_K$ is a Dedekind domain we have the fact that any Dedekind ring has unique factorization of ideals into prime ideals. To measure unique factorization in $\mathcal{O}_K$, we would like to form a multiplicative group from the set of ideals which we will be a free abelian group generated by the prime ideals. The technical problem arises from requiring inverses but is remedied by introducing fractional ideals.

Definition. *A fractional ideal of a Dedekind ring R is a non-zero finitely generated R-submodule of its field of fractions K.*

Non-zero ideals are finitely generated R-modules so are also fractional ideals. Fractional ideals $\mathfrak{U}$ are of the form $c^{-1}\mathcal{B}$ for an ideal $\mathcal{B}$ and non-zero $c \in R$. c is obtained by taking the common denominators of the finitely many generators of $\mathfrak{U}$ when written as fractions in R.

The inverse of a fractional ideal $\mathfrak{U}$ is the set $\mathfrak{U}^{-1} = \{x \in K \mid x\mathfrak{U} \subseteq R\}$. $\mathfrak{U}^{-1}$ is also a fractional ideal and $\mathfrak{U}\mathfrak{U}^{-1} = R$.

Theorem. *(Janusz [2], Pg. 18) Any fractional ideal $\mathfrak{U}$ of a Dedekind ring R can be uniquely expressed as a product*

$$\mathfrak{U} = \prod_{i=1}^{n} \mathfrak{p}_i^{a_i},$$

with $\mathfrak{p_1}, \ldots, \mathfrak{p_n}$ distinct prime ideals and $a_1, \ldots, a_n$ positive or negative integers. If $\mathfrak{U}$ is an ideal, the exponents will be positive.

With inverses and ideal multiplication defined, we can now form the ideal class group $C(R)$. First, we have that the set of all fractional ideals $I(R)$ is a free abelian group under multiplication with prime ideals as generators and R as the identity. $P(R)$ is the subgroup of principal fractional ideals of R. The quotient

$$C(R) = {}^{I(R)}\Big/_{P(R)}$$

is the ideal class group of R. The group is trivial if and only if R is a PID. A PID is always a UFD but for Dedekind rings which already have the property that all non-zero prime ideals are maximal, being a UFD implies being a PID. So $C(R)$ measures unique factorization.

In the case of a number field K, we are always working with its unique ring of integers and so we denote C_K as the ideal class group of its ring of integers $\mathcal{O}_K$. C_K turns out to be a finite group and this relies heavily on the embeddings of K into $\mathbb{R}$ and $\mathbb{C}$. The order of C_K is the class number h_K of K.

Finiteness of the Class Number

To show C_k is finite, we follow a proof using Minkowski's bound on convex sets and lattices. The idea is to embed K into complex space in such a way that ideals become lattices and the norm of an ideal corresponds to the volume of the fundamental domain.

Theorem. *(Minkowski's Theorem) Let L be an n-dimensional lattice in $\mathbb{R}^n$ with fundamental domain T, and let X be a bounded symmetric convex subset of $\mathbb{R}^n$. If*

$$v(X) > 2^n v(T)$$

where v denotes the volume, then X contains a non-zero point of L.

To apply Minkowski's Theorem, we embed K as follows. First we write the degree $[K : \mathbb{Q}] = n$ as $s + 2t$ where s is the number of real embeddings of K and t is the number of pairs of complex embeddings. Then we order the monomorphisms of K into $\mathbb{C}$ as $\sigma_1, \sigma_2, \ldots, \sigma_s, \sigma_{s+1}, \overline{\sigma}_{s+1}, \ldots, \sigma_{s+t}, \overline{\sigma}_{s+t}$, where the first monomorphisms are the real embeddings and the others are complex embeddings and their complex conjugates. Now we map $x \in K$ to

$$\sigma(x) = (\sigma_1(x), \sigma_2(x), \ldots, \sigma_s(x), \sigma_{s+1}(x), \ldots, \sigma_{s+t}(x))$$

in the space $L^{st} := \mathbb{R}^s \times \mathbb{C}^t$. The important property of this map is that it takes free abelian subgroups of rank m of K to lattices of dimension m. Ideals of $\mathcal{O}_K$ are free of rank n so are taken to n-dimensional lattices in L^{st} which is also n-dimensional over $\mathbb{R}$. The volume of the fundamental domain is related to the norm of the ideal and the discriminant Δ of K defined as the discriminant an integral basis for $\mathcal{O}_K$ (which is also a $\mathbb{Q}$-basis for K and unique up to a unimodular change of basis matrix). With Minkowski's theorem, we can find an ideal equivalent (differing by a principal fractional ideal) to an ideal $\mathfrak{a}$ with a bounded norm.

Corollary. *(Stewart [1], Pg. 157) Every non-zero ideal $\mathfrak{a}$ of $\mathcal{O}_K$ is equivalent to an ideal whose norm is at most $(\frac{2}{\pi})^t\sqrt{|\Delta|}$.*

Now given a non-zero fractional ideal $\mathfrak{a}$, we know it is of the form $c^{-1}\mathfrak{b}$ for $0 \neq c \in \mathcal{O}_K$ and $\mathfrak{b}$ an ideal of $\mathcal{O}_K$. So $\mathfrak{a}$ is equivalent to the ideal $\mathfrak{b}$ since it differs by the principal ideal $c\mathcal{O}_K$. Applying the corollary gives that $\mathfrak{a}$ is equivalent to an ideal $\mathfrak{c}$ with norm $N(\mathfrak{c}) \leq (\frac{2}{\pi})^t\sqrt{|\Delta|}$. There are only finitely many positive integers less than the bound so finitely many possible norms of $\mathfrak{c}$. For a particular norm $N = N(\mathfrak{c})$, $N \in \mathfrak{c}$ and so $\mathfrak{c}$ divides N (or the ideal $N\mathcal{O}_K$). But by unique factorization, only finitely many ideals can divide N and so there are only finitely many choices for $\mathfrak{c}$. Since any fractional ideal is equivalent to a choice of $\mathfrak{c}$, C_K is finite.

Units

To complete our picture of the ring of integers $\mathcal{O}_K$, we want to know the structure of the units. The connection between principal ideals and elements is governed by units since associate elements will generate the same ideals. Let U_K denote the unit group. We have the following exact sequence:

$$1 \to U_K \to K \to I(K)$$

Theorem. *(Dirichlet's Unit Theorem) $U_K \cong C \times \mathbb{Z}^{s+t-1}$ where C is the finite cyclic group of roots of unity in $\mathcal{O}_K$.*

To show this, we define a homomorphism $l : K^\times \to \mathbb{R}^{s+t}$ by:

$$l(a) = (\ln|\sigma_1(a)|, \ldots, \ln|\sigma_r(a), 2\ln|\sigma_{r+1}(a)), \ldots, 2\ln|\sigma_{r+s}(a)|).$$

This homomorphism maps the unit group to the subspace given by $\sum\limits_{i=1}^{s+t} x_i = 0$. Using the previous embedding of K, σ, we can show that the unit group is mapped to a lattice (of dimension at most $s+t-1$). Using Minkowski's Theorem, we can show that the lattice is of dimension $s+t-1$. The last step is to show that the kernel of l is finite using the old embedding σ on elements of the kernel. It is easy to see all roots of unity are in the kernel and so we are done. The volume of the fundamental domain of the lattice formed by the unit group is called the regulator of K, $\mathrm{reg}(K)$.

Decomposition of Primes

Given an extension $K \subset L$ of number fields, prime ideals in $\mathcal{O}_K$ can factor in $\mathcal{O}_L$. We would like to also include the "factoring" of "infinite" primes.

Theorem. ★ *(Janusz [2], Pg. 30) Let R be a Dedekind ring with quotient field K and let L be a finite dimensional, separable extension of K. Let R' be the integral closure of R in L and let $\mathfrak{p}$ be a non-zero prime ideal of R. Let $\mathfrak{p}R'$ have the factorization $\mathfrak{P}_1^{e_1} \dots \mathfrak{P}_g^{e_g}$. Then*

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

where $f_i = [R'/\mathfrak{P}_i : R/\mathfrak{p}]$. In the case of a Galois extension, all the exponents e_i are equal and all the relative degrees f_i are equal and so we obtain $efg = [L : K]$.

To prove this, we use the fact that R' is a finitely generated R module so the localization $R'_{\mathfrak{p}}$ is finitely generated over $R_{\mathfrak{p}}$. We can then show that a minimal generating set is linearly independent over K using the fact that $R_{\mathfrak{p}}$ is a DVR. The last step is to show that the minimal set has size n. In the Galois case, it is enough to show that the Galois group acts transitively on the prime factors.

Ramification

Definition. *A prime ideal $\mathfrak{p}$ of $\mathcal{O}_K$ is ramified in a finite extension L if a prime ideal $\mathfrak{P}$ lying above it ($\mathfrak{P} \cap K = \mathfrak{p}$) has $e(\mathfrak{P}/\mathfrak{p}) > 1$ where $e(\mathfrak{P}/\mathfrak{p})$ is the exponent in the factorization of $\mathfrak{p}$ in $\mathcal{O}_L$.*

Let If such a prime ideal exists in an extension, we say the extension is ramified at the finite prime $\mathfrak{p}$.

Definition. *An infinite prime of a number field K is an embedding of K into $\mathbb{C}$. It is a real infinite prime if the embedding is real and complex otherwise.*

A finite extension L is said to be ramified at an infinite prime of K if first the infinite prime is real and the embedding extends to a complex embedding of L. We can characterize which finite primes will ramify.

Theorem. *(Janusz [2], Pg. 35) Let R be a Dedekind ring with quotient field K and let L be a finite dimensional, separable extension of K. Let R' be the integral closure of R in L. The prime ideals of R which ramify in R' are those containing the discriminant $\Delta(R'/R)$.*

As we saw before, only finitely many ideals can divide (contain) an integer so there are only finitely many ideals which ramify in an extension.

Decomposition and Inertia Groups

Now we would like to answer the main question of when does a prime ideal split into distinct primes in an extension. We saw that a prime ideal $\mathfrak{p}$ in $\mathcal{O}_{\mathcal{K}}$ will factor and possibly be ramified in an extension. There are subfields between K and L in which the ramification, change in relative degree and splitting happen separately.

Let $\mathfrak{p}$ be a prime ideal in $\mathcal{O}_{\mathcal{K}}$ and $\mathfrak{P}$ a prime above it in $\mathcal{O}_{\mathcal{L}}$. Define the decomposition group of $\mathfrak{P}$ as

$$G(\mathfrak{P}) = \{\sigma \in G(L/K) \mid \sigma(\mathfrak{P}) = \mathfrak{P}\}.$$

$\sigma \in G(\mathfrak{P})$ gives rise to an automorphism $\overline{\sigma}$ of $R' = \mathcal{O}_{\mathcal{L}}/\mathfrak{P}$ over $R = \mathcal{O}_{\mathcal{K}}/\mathfrak{p}$. Define the inertia group $T(\mathfrak{B})$ to be the kernel of this map so

$$T(\mathfrak{B}) = \{\sigma \in G(\mathfrak{B} \mid \sigma(x) \in x + \mathfrak{B}, \forall x \in R'\}.$$

Assuming L is Galois, we have two fixed subfields: the decomposition field $L^{G(\mathfrak{P})}$ and the inertia field $L^{T(\mathfrak{P})}$. Then the splitting of $\mathfrak{p}$ happens between K and $L^{G(\mathfrak{P})}$, the change in relative degree happens between $L^{G(\mathfrak{P})}$ and $L^{T(\mathfrak{P})}$ and ramification happens between $L^{T(\mathfrak{P})}$ and L. ★ More importantly, the Galois group of the extension of finite fields $R' = \mathcal{O}_L/\mathfrak{P}$ and $R = \mathcal{O}_K/\mathfrak{p}$, $G(R'/R)$ is isomorphic to $G(\mathfrak{P})/T(\mathfrak{P})$. The proof involves working in the completions $L_{\mathfrak{P}}$ and $K_{\mathfrak{p}}$ to compute the order of each subgroup. Namely, $|G(\mathfrak{P})| = [L_{\mathfrak{P}} : K_{\mathfrak{p}}] = ef$ and $[G(\mathfrak{P}) : T(\mathfrak{P})] = f$.

Frobenius Elements and the Artin Map

By counting orders of groups, we have $G(R'/R) \cong G(\mathfrak{P})/T(\mathfrak{P})$ but $G(R'/R)$ is the Galois group of an extension of finite fields and so is cyclic. Define the Frobenius element of $\mathfrak{P}$, $\mathrm{Frob}_{\mathfrak{P}}$, to be the coset $\sigma T(\mathfrak{P})$ corresponding to the generator of $G(R'/R)$. Now if $\mathfrak{P}$ is unramified, this is a unique element of $G(\mathfrak{P})$. Moreover, $\mathrm{Frob}'_{\mathfrak{P}}$, for a different prime $\mathfrak{P}'$ above $\mathfrak{p}$, is conjugate. The converse holds as well so we can associate a conjugacy class, $\mathrm{Frob}_{\mathfrak{p}}$ in $G(L/K)$ to each unramified (finite) prime $\mathfrak{p}$. So now by the definition, $\mathfrak{p}$ splits ($f = 1$) if and only if $\mathrm{Frob}_{\mathfrak{p}}$ is trivial (or $\mathrm{Frob}_{\mathfrak{P}}$ is trivial for some prime lying above). If we assume that $G(L/K)$ is also abelian, $\mathrm{Frob}_{\mathfrak{p}}$ is a unique element.

In the abelian case, the unique Frobenius element only depends on the prime $\mathfrak{p}$ which allows us to define a map from the ideals of $\mathcal{O}_K$ to $G(L/K)$. Let S be a finite set of (finite) primes if $\mathcal{O}_K$ containing atleast the ramified primes. Define I_K^S to be the subgroup of the group of fractional ideals containing only ideals divisible by primes outside S. Each $I \in I_K^S$ factors as $I = \mathfrak{p}_1^{e_1} \dots \mathfrak{p}_g^{e_g}$ for $\mathfrak{p}_i \in I_K^S$. Now we can define the Artin map:

$$\left(\frac{L/K}{\bullet}\right) : I_K^S \to G(L/K)$$
$$I \mapsto Frob_{\mathfrak{p}_1}^{e_1} \cdots Frob_{\mathfrak{p}_g}^{e_g}$$

This map is only well defined for abelian extensions since we can always reorder the factorization of an ideal. The Artin map (symbol) generalizes the Legendre symbol and a reciprocity law is a description of the kernel of the Artin map since primes in the kernel are exactly those split.

Properties of the Artin Map

Theorem. ★ *The kernel of the Artin map contains $N(I_L^S(L))$ where $S(L)$ is the finite set of primes of $\mathcal{O}_L$ dividing primes of S.*

Density of Primes

Definition. *Let S be a set of prime ideals of $\mathcal{O}_K$. If there exists a real number δ such that*

$$-\delta \log(s-1) \sim \sum_{\mathfrak{p} \in S} \frac{1}{\mathcal{N}(\mathfrak{p})^s}$$

then we say the Dirichlet density of S is $\delta(S) = \delta$.

Definition. *Let σ be an element of order n in a group G. The division of σ is the collection of all elements of G that are conjugate to some σ^m with m relatively prime to n.*

Theorem. *(Frobenius Density Theorem) Let L be a Galois extension of K and let $\sigma \in G(L/K)$ be an element having t elements in its division. Let S_1 be the set of primes of K which are divisible by a prime of L having Frobenius automorphism in the division of σ. Then S_1 has Dirichlet density $\delta(S_1) = t/|G|$.*

Theorem. *(Janusz [2], Pg. 164) For any finite set of primes S containing atleast the ramified primes, the Artin map is surjective.*

Let $\sigma \in G(L/K)$ so there exists infinitely many primes whose Frobenius automorphism generates $\langle \sigma \rangle$ (G abelian). Since S is finite, we can always find a prime with factors outside of S that still generates $\langle \sigma \rangle$.

Corollary. *Let L_1 and L_2 be Galois extensions of K and let S_i be the set of primes ideals in $\mathcal{O}_K$ that split completely in L_i for $i = 1, 2$. If $S_1 \subset S_2$ (except possibly for a set of density zero) then $L_2 \subset L_1$.*

Let $L = L_1 L_2$. The primes of K that split completely in L are the primes that split completely in both L_1 and L_2, i.e S_1 (except possibly for a set of density zero). Then by the Frobenius density theorem,

$$[L : K]^{-1} = \delta(S_1) = [L_1 : K]^{-1}.$$

So $L_2 \subset L_1$.

The converse is also true. Let $n_1 = [L_1 : K]$ and $n_2 = [L_2 : K]$. Suppose $L_2 \subset L_1$. If $\mathfrak{p} = \mathfrak{Q}_1 \cdots \mathfrak{Q}_n$ in L_2 for $n < n_1$, we have $n_2 = f * n$ where f is the relative degree of $\mathfrak{Q}_i$ over $\mathfrak{p}$. Suppose $\mathfrak{P}$ is above $\mathfrak{Q}_1$. Then $f(\mathfrak{P}/\mathfrak{p}) = f(\mathfrak{P}/\mathfrak{Q}_1) \cdot f > 1$.

Remark: Galois (even non-abelian) extensions of number fields are characterized by which primes split completely in them.

Reciprocity Theorem

A modulus of K is a formal product of primes (finite and infinite)

$$\mathfrak{m} = \prod_{\mathfrak{p}} \mathfrak{p}^{n(\mathfrak{p})}$$

where only finitely many of the $n(\mathfrak{p})$ are non-zero. Moreover, for real infinite primes $n(\mathfrak{p})$ is 0 or 1 and for complex infinite primes, $n(\mathfrak{p}) = 0$. We take S to be the finite set of (finite) primes dividing m and denote I_K^S by $I_K^{\mathfrak{m}}$. The goal is to define congruence relations mod $\mathfrak{m}$ so that for a large enough modulus, we can determine the kernel of the Artin map.

For $\alpha, \beta \in K^\times$, we say $\alpha \equiv \beta \bmod \mathfrak{m}$ if α/β is positive for every real prime/embedding of $\mathfrak{m}$ and $\alpha \in \beta(1 + \mathfrak{p}^{n(\mathfrak{p})}(\mathcal{O}_K)_{\mathfrak{p}})$ for every finite prime $\mathfrak{p}$ with $n(\mathfrak{p}) \neq 0$. Separate the modulus $\mathfrak{m}$ into its finite and infinite parts: $\mathfrak{m} = \mathfrak{m}_0\mathfrak{m}_\infty$. We define two important subgroups of $K^\times$.

$$K_{\mathfrak{m}} = \{a/b \mid a, b \in \mathcal{O}_K, a\mathcal{O}_K \text{ and } b\mathcal{O}_K \text{ are relatively prime to } \mathfrak{m}_0\}$$

$$K_{\mathfrak{m},1} = \{\alpha \in K_{\mathfrak{m}} \mid \alpha \equiv 1 \bmod \mathfrak{m}\}$$

Theorem. *(Artin Reciprocity Theorem) Let $\mathfrak{m}$ be a modulus divisible by all ramified primes. If the exponents of $\mathfrak{m}$ are sufficiently large, then the kernel of the Artin map is $\mathfrak{i}(K_{\mathfrak{m},1})N(I_L^{\mathfrak{m}})$. The smallest modulus for which this is true is called the conductor of L/K, $\mathfrak{f}$.*

The first step is to prove this for cyclic extensions since finite abelian groups are just products of cyclic groups. The condition on the exponents guarantees convergence of the exponential and logarithm maps in the completions. Using the completions and some cohomology of cyclic groups (0^{th} and 1^{st} groups), we can compute the index $[I_K^{\mathfrak{m}} : N(I_L^{\mathfrak{m}})\mathfrak{i}(K_{\mathfrak{m},1})]$ which turns out to be $[L : K]$. We also know that $[I_K^{\mathfrak{m}} : ker(\varphi_{L/K})] = [L : K]$. So it is enough to show either $ker(\varphi_{L/K}) \subset N(I_L^{\mathfrak{m}})\mathfrak{i}(K_{\mathfrak{m},1})$ or $\mathfrak{i}(K_{\mathfrak{m},1}) \subset ker(\varphi_{L/K})$. For cyclic extensions, we can show the first one by working in a larger field with certain roots of unity. When the second (equivalent) condition holds, we say the reciprocity law holds for $(L, K, \mathfrak{m})$.

Concluding Remarks

Classification of Abelian Extensions

Class field theory goes further and classifies all abelian extensions of a number field k by objects internal to K. It gives a correspondence between abelian extensions and certain equivalence classes of subgroups of I_K called ideal groups. The proof relies strongly on the Artin map and the important fact that an extension of a number field is almost determined by which primes split completely. The kernel of the Artin map falls into one of these ideal groups and conversely, for each ideal group, an abelian extension (a class field) exists for which the kernel of the Artin map lies in the ideal group.

The Hilbert Class Field

Definition. *The Hilbert class field $K^{(1)}$ of a number field K is the unique maximal unramified abelian extension of K.*

The existence of $K^{(1)}$ is given by the main result of class field theory (Janusz [2], Pg. 215) which classifies all finite abelian extensions in terms of generalized class groups. The Hilbert class field corresponds to the usual ideal class group in a very strong way.

Theorem. *(Cox [3], Pg. 109) If $K^{(1)}$ is the Hilbert class field of a number field K, then the Artin map*

$$\left(\frac{L/K}{\bullet}\right) : I_K \to Gal(L/K)$$

is surjective, and its kernel is exactly the subgroup P_K of principal fractional ideals. Thus the Artin map induces an isomorphism

$$C_K \xrightarrow{\sim} Gal(L/K).$$

So knowing the class number h_K gives a way of finding $K^{(1)}$ since $[K^{(1)} : K] = h_k$. The final property of the Hilbert class field is what it does to ideals in K.

Theorem. *(Principal Ideal Theorem) Every fractional ideal in K becomes principal when extended to an ideal in $K^{(1)}$.*

We can repeat the process of taking Hilbert class fields to obtain a tower of maximal unramified abelian extensions.

$$K \subseteq K^{(1)} \subseteq K^{(2)} \subseteq \dots$$

It is an amazing fact that this tower can be infinite and moreover, in the "simple" case of a quadratic extension.

Theorem. *(Golod and Shafarevich) $K = \mathbb{Q}(\sqrt{d})$ has an infinite class field tower if d is a square free integer divisible by eight or more primes.*

Explicit Class Field Theory

The classification of abelian extensions of number fields in general is not explicit since the class fields are not constructed. In the case of abelian extensions over $\mathbb{Q}$, we have a concrete picture of the extensions since they are all subfields of cyclotomic extensions. Another large class of number fields that have an explicit class field theory are imaginary quadratic fields and CM (Complex Multiplication) fields. The abelian extensions in this case are described by elliptic curves and their associated modular forms.

One of the reasons why these classes of number fields can be worked with it that these are exactly the fields with a finite number of units. From Dirichlet's Unit Theorem, $K/\mathbb{Q}$ has a finite unit group exactly when $K = \mathbb{Q}$ or K is am imaginary quadratic field. This simplifies some calculations since the regulator is trivial. Even the real quadratic case is difficult and there is still the open problem of determining how many (and which) real quadratic fields have class number 1.

Examples

Quadratic Fields

Now we apply the theory to quadratic number fields K ($[K : \mathbb{Q}] = 2$). K is of the form $\mathbb{Q}(\sqrt{d})$ for d a square-free integer.

Theorem. *(Stewart [1], Pg. 62) Let d be a square-free integer. Then the ring of integers of $\mathbb{Q}(\sqrt{d})$ are:*

(a) $\mathbb{Z}(\sqrt{d})$ if $d \equiv 2, 3$ (mod 4)

(b) $\mathbb{Z}(\frac{1}{2} + \frac{1}{2}\sqrt{d})$ if $d \equiv 1$ (mod 4)

This gives us an integral basis for $\mathcal{O}_K$ so we can compute the discriminant of K. There are of course only two embeddings of K into $\mathbb{C}$ given by sending $\sqrt{d} \mapsto \sqrt{d}$ and $\sqrt{d} \mapsto -\sqrt{d}$. So we have:

$$\Delta = \begin{vmatrix} 1 & \sqrt{d} \\ 1 & -\sqrt{d} \end{vmatrix}^2 = 4d \text{ if } d \equiv 2, 3 (\text{mod } 4)$$

$$\Delta = \begin{vmatrix} 1 & \frac{1}{2} + \frac{1}{2}\sqrt{d} \\ 1 & \frac{1}{2} - \frac{1}{2}\sqrt{d} \end{vmatrix}^2 = d \text{ if } d \equiv 1 (\text{mod } 4)$$

To compute C_K, it will be useful to compute Minkowski's bound $(\frac{2}{\pi})^t \sqrt{|\Delta|}$. The number t of complex embeddings of K is either 0 or 1.

Δ	t	Bound
d	0	$\sqrt{\lvert d\rvert}$
d	1	$\frac{2\sqrt{\lvert d\rvert}}{\pi}$
$4d$	0	$2\sqrt{\lvert d\rvert}$
$4d$	1	$\frac{4\sqrt{\lvert d\rvert}}{\pi}$

We can quickly see that for $d = -7, -3, -2, -1$, C_K is trivial (the bound is less than two). There are some other cases for which it can be shown that $\mathcal{O}_K$ has an Euclidean algorithm and so is a PID and UFD. For small positive d the algorithm involves taking the nearest integer or half-integer approximations.

For $d = -19, -15, -11, -5, 2, 5$, the bound is 2. For $d = 2, 5$, we do have Euclidean algorithms. We show that $h_K = 2$ for $K = \mathbb{Q}(\sqrt{-5})$ and compute the Hilbert class field which will then be of degree 2 over K.

Since 2 is the bound for the norm, we look at the factorization of the ideal generated by 2, $2\mathcal{O}_K$. It is ramified since 2 divides the discriminant $4 \cdot (-5) = -20$. The degree of K is 2 so we have $2\mathcal{O}_K = \mathcal{B}^2$ for some prime ideal $\mathcal{B}$. So $\mathcal{B}$ is the only ideal of norm 2 and so $h_K \leq 2$. Now, K is not a UFD so $h_K = 2$ since we have two distinct factorizations into irreducibles for 6 as $6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$. We know $[K^{(1)} : K] = h_K = 2$ so to find $K^{(1)}$, we are looking for a unramified abelian extension of degree 2. Of course, any degree 2 extension is already abelian.

If we take $K^{(1)} = K(i) = \mathbb{Q}(\sqrt{5}, i)$, we claim it is unramified over K. The discriminant over Q of $K^{(1)}$ can be obtained by taking the integral basis $\{1, i, \frac{1}{2} + \frac{1}{2}\sqrt{5}, (\frac{1}{2} + \frac{1}{2}\sqrt{5})i\}$ to obtain $\Delta = -2^4 5^2$. So the only primes of $\mathbb{Q}$ that ramify are 2 and 5. But each of these already ramify in K. Let $\mathcal{B}$ be a prime lying over 5 in $K^{(1)}$ and $\mathfrak{p} = \mathfrak{P} \cap K$. We have another subfield of interest in $K^{(1)}$, namely $L = \mathbb{Q}(i)$. Let $\mathfrak{p}' = \mathfrak{P} \cap L$. The prime 5 does not ramify in L since the discriminant is -4 so $e(\mathfrak{p}'/3) = 1$. We already know 5 ramifies in K so $e(\mathfrak{p}/3) = 2$. Then we have the following:

$$e(\mathfrak{P}/3) = e(\mathfrak{P}/\mathfrak{p})e(\mathfrak{p}/3) = e(\mathfrak{P}/\mathfrak{p}')e(\mathfrak{p}'/3)$$

Since L is a degree 2 extension, the product formula forces $e(\mathfrak{P}/\mathfrak{p}') \leq 2$. This means $e(\mathfrak{P}/\mathfrak{p}) = 1$ and so primes above 5 do not ramify. We can make a similar argument for primes above 2 using the subfield $\mathbb{Q}(5)$. Finally, K has no real infinite primes so cannot ramify at an infinite prime. So $K^{(1)}$ is the Hilbert class field of K.

For quadratic extensions, Frobenius elements lie in the Galois group $\langle -1 \rangle$. As we expect, quadratic reciprocity governs whether or not $\mathrm{Frob}_{\mathfrak{p}}$ is 1 or -1. To talk about this, we need to discuss cyclotomic fields.

To compute the conductor $\mathfrak{f}$ of a number field, it is useful to work locally and compute "local" conductors. It is also useful to know that $\mathfrak{f}$, being the smallest modulus satisfying the reciprocity law, is only divisible by primes that ramify (further evidence that the bad primes are exactly the ramified primes). We know the discriminant of a quadratic field and so, depending on d mod 4, we have to check locally at the odd primes dividing d and possibly 2. The result is $\mathfrak{f} = (\Delta)$ if $d > 0$ and $\mathfrak{f} = (\Delta)\mathfrak{p}_\infty$ otherwise.

Cyclotomic Fields

Let $K = \mathbb{Q}(\zeta_n)$ and denote the homomorphism of K taking ζ_n to ζ_n^m by σ_m. We know the Galois group $G(K/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^\times$, $\mathcal{O}_K = \mathbb{Z}[\zeta_n]$ and Δ_K is only divisible by primes dividing n. For a prime q not dividing n (so unramified), $Frob_q = \sigma_q$. To see this, write $x \in \mathcal{O}_K$ as $x = \sum\limits_{i=0}^{n-1} a_i \zeta_n^i$ for $a_i \in \mathbb{Z}$ and let $\mathfrak{Q}$ be a prime above q. Then $\mathcal{O}_K/\mathfrak{Q}$ is a finite field of characteristic q so

$$x^q \equiv \sum_{i=0}^{n-1} a_i^q \zeta_n^q i \equiv \sum_{i=0}^{n-1} a_i^q \zeta_n^q i \equiv \sigma_q(x) \pmod{\mathfrak{Q}}$$

So σ_q corresponds to the generator of $\mathcal{O}_K/\mathfrak{Q}$ and $\sigma_q \in G(\mathfrak{Q})$ since for $x \in \mathfrak{Q}$, $\sigma_q(x) \equiv x^q \equiv 0 \pmod{\mathfrak{Q}}$.

Now that we know what the Frobenius elements look like we can easily figure out when they are trivial. Let $n = \prod_{i=1}^r p_i^{k_i}$. Then $Frob_q = \sigma_q = \sigma_1$ if $m|q-1$, i.e. $q \equiv 1 \pmod{m}$.

Example: $K = \mathbb{Q}(\zeta_3)$

Theorem. *(Kronecker-Weber) A number field K is an abelian extension of $\mathbb{Q}$ if and only if $K \subset \mathbb{Q}(\zeta_n)$ for some n.*

We know there exists a modulus $\mathfrak{m}$ so that the reciprocity law holds for K so the kernel of the Artin map on $I_K^{\mathfrak{m}}$ is $\mathfrak{i}(\mathbb{Q}_{\mathfrak{m},1})N(I_K^{\mathfrak{m}})$ which contains $\mathfrak{i}(\mathbb{Q}_{\mathfrak{m},1})$, the kernel of the Artin map on $\mathbb{Q}(\zeta_m)$. So the primes that split in $\mathbb{Q}(\zeta_m)$ also split in K. This is enough to imply $K \subset \mathbb{Q}(\zeta_m)$ by a previous theorem.

Remark: The fields over $\mathbb{Q}$ with nice reciprocity laws (i.e. in terms of some congruence condition) are the abelian ones since they behave like cyclotomic fields.

The smallest n for which $K \subset \mathbb{Q}(\zeta_n)$ turns out to be the conductor of $K/\mathbb{Q}$. One way to see this is to use the classification of abelian extensions. The kernel of the Artin map for both extensions are "defined" mod $\mathfrak{n} = (n)\mathfrak{p}_\infty$ but $ker(\varphi_{\mathbb{Q}(\zeta_n)/\mathbb{Q}})$ is the smallest subgroup defined for $\mathfrak{n}$. This is because $ker(\varphi_{\mathbb{Q}(\zeta_n)/\mathbb{Q}}) = \mathfrak{i}(\mathbb{Q}_{\mathfrak{m},1})$ which is always contained in the kernel of the Artin map.

Quadratic Reciprocity

Let $K = \mathbb{Q}(\sqrt{d})$ where $d = (-1)^{\frac{p-1}{2}}p$ for an odd prime p and let Δ be the discriminant. $d \equiv 1 \bmod 4$ so $\Delta = d$.

Let $\mathfrak{f} = (d)\mathfrak{p}_\infty$ be the conductor of $K/\mathbb{Q}$. We know that $\mathfrak{i}(\mathbb{Q}_{\mathfrak{f},1}) \subset ker(\varphi)$. $\mathbb{Q}_{\mathfrak{f},1} = \{a/b \in \mathbb{Q} | (a,p) = (b,p) = 1, ab^{-1} \equiv 1 \bmod p, a/b > 0\}$ and $I_{\mathbb{Q}}^{\mathfrak{f}} = \{(a/b) | (a,p) = (b,p) = 1\}$. We have a surjective homomorphism from $I_{\mathbb{Q}}^{\mathfrak{f}}$ to $(\mathbb{Z}/p\mathbb{Z})^\times$ with kernel $\mathfrak{i}(\mathbb{Q}_{\mathfrak{f},1})$. So φ reduces to a homomorphism from $(\mathbb{Z}/p\mathbb{Z})^\times \to \{\pm 1\}$, i.e. a quadratic character. It is non-trivial since φ is onto so it must be the Legendre symbol $(-/p)$. But we also know that for an odd prime q, $\varphi(q) = (\Delta/q)$ since q splits in K if and only if Δ is a square mod q. So $(\Delta/q) = (-1/q)^{\frac{p-1}{2}}(p/q) = (q/p)$. Using the fact $(-1/q) = (-1)^{\frac{q-1}{2}}$, we have quadratic reciprocity.

Theorem. *(Kummer's Theorem) Let L/K be number fields and $\mathfrak{p} \in \mathcal{O}_K$. Suppose there is $\theta \in L$ such that the integral closure of $(\mathcal{O}_K)_\mathfrak{p}$ in L is $(\mathcal{O}_K)_\mathfrak{p}[\theta]$. Let $f(X)$ be the minimum polynomial of θ over K. Let $\overline{f}(X)$ be $f(X)$ modulo $\mathfrak{p}$. Suppose*

$$\overline{f}(X) = g_1(X)^{a_1} \cdots g_t(X)^{a_t}$$

is the factorization of $\overline{f}(X)$ as product of distinct irreducible polynomials $g_i(X)$ over $\mathcal{O}_K/\mathfrak{p}$. Then

$$p\mathcal{O}_L = \mathfrak{P}_1^{a_1} \cdots \mathfrak{P}_t^{a_t}$$

for certain prime ideals $\mathfrak{P}_i$ of $\mathcal{O}_L$ corresponding one to one with the irreducible factors $g_i(X)$; the relative degree $f_i(\mathfrak{P}_i/\mathcal{O}_K)$ equals the degree of the polynomial $g_i(X)$.

References

[1] I. Stewart and D. Tall, *Algebraic Number Theory and Fermat's Last Theorem*, A. K. Peters, 2001.

[2] G. J. Janusz, *Algebraic Number Fields*, American Mathematical Society, 1996.

[3] D. A. Cox, *Primes of the Form $x^2 + ny^2$*, John Wiley and Sons, Inc., 1989.