SEMINAR ON CLASS FIELD THEORY

MICHAEL BAKER, RAYMOND CHENG, RITVIK RAMKUMAR

1. Motivation

Class field theory is the study of finite abelian extensions of global and local fields. In particular, it seeks to characterize these abelian extensions in terms of arithmetic data attached to the base field. Probably the most basic example of this is the *Kronecker-Weber theorem*, described below. One thing provided by class field theory is a bijective correspondence between abelian extensions and certain classes of ideals; this can also be formulated in the language of "idèles".

The law of quadratic reciprocity, of which Gauss famously gave 8 proofs, states that

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{(p-1)(q-1)/2}$$

where the Legendre symbol is defined by

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & \text{if } a \equiv 0 \bmod p \\ +1 & \text{if } a \not\equiv 0 \bmod p \text{ and for some integer } x,\ a \equiv x^2 \bmod p \\ -1 & \text{otherwise.} \end{cases}$$

This can actually be viewed as one of the first theorems of class field theory. Although it looks like a harmless curiosity, it is in fact closely related to the splitting of primes in cyclotomic fields. We have the following result.

Theorem 1. *Let* $n = \prod_p p^{\nu_p}$ *be the prime factorization of* n*, and for every prime number* p*, let* f_p *be the smallest positive integer such that* $p^{f_p} \equiv 1 \bmod n/p^{\nu_p}$*. Then in* $\mathbf{Q}(\zeta_n)$ *one has the factorization*

$$p = (\mathfrak{p}_1 \cdots \mathfrak{p}_r)^{\varphi(p^{\nu_p})}$$

where $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ *are distinct prime ideals, all of degree* f_p*.*

The search for "higher reciprocity laws" dominated number theory for a long time. At the heart of class field theory lies a result known as *Artin reciprocity*, which subsumes all of these laws.

Given a number field K (that is, a finite-degree field extension of $\mathbf{Q}$), the elements $\alpha \in K$ for which there exist a monic polynomial $f \in \mathbf{Z}[x]$ such that $f(\alpha) = 0$ are known as *algebraic integers*; they form a subring of K denoted by $\mathcal{O}_K$. In fact, $\mathcal{O}_K$ is a Dedekind domain: an integral domain in which every proper nonzero ideal factors as a product of prime ideals.

If $L \supset K$ is an extension of number fields, then every prime ideal $\mathfrak{p}$ of $\mathcal{O}_K$ generates an ideal $\mathfrak{p}\mathcal{O}_L$ of $\mathcal{O}_L$, which in general is no longer prime. However, it can of course be factorized into primes (that is, prime ideals) in $\mathcal{O}_L$. One of the central goals of algebraic number theory is to understand the splitting behaviour of primes when lifted in this sense.

Here is another angle. Suppose we are given a monic irreducible polynomial $f \in \mathbf{Z}[x]$ of degree n. Then for any prime number p, we can reduce all of the coefficients of f modulo p to obtain a polynomial $\bar{f} \in \mathbf{F}_p[x]$, and factorize $\bar{f}$ into irreducibles, say $\bar{f} = f_1 \cdots f_r$, with $\lambda_i := \deg(f_i)$, numbered in such a way that $\lambda_1 \geqslant \lambda_2 \geqslant \ldots \geqslant \lambda_r$. Then we have $\lambda_1 + \ldots + \lambda_r = n$, so λ is a partition of n. It seems fairly natural to ask whether, given f and λ, we can describe the set of prime numbers p for which the reduction of f mod p has "factorization pattern" λ, in this sense. In particular, for which primes p does $\bar{f}$ split completely into linear factors over $\mathbf{F}_p$?

This innocent question remains to this day only partially understood. The polynomial f gives rise to a finite Galois extension K of $\mathbf{Q}$, namely the one obtained by adjoining all of its roots $\alpha_1, \ldots, \alpha_n$ to $\mathbf{Q}$. This is

called the *splitting field* of f, and we can consider its Galois group $G = \mathrm{Gal}(K|F)$. If G is abelian, then we call K an *abelian extension* of $\mathbf{Q}$, and the famous Kronecker-Weber theorem then tells us that K is contained in some sufficiently large cyclotomic extension, that is, $K \subset \mathbf{Q}(\zeta_N)$ for some sufficiently large integer N; here ζ_N is a primitive Nth root of unity. What is the significance of the least such N? It turns out that the set of primes p for which $\overline{f}$ splits completely admits a very nice characterization in terms of congruences modulo N. This is really what class field theory is all about. Assuming the Galois group is abelian is hardly a mild hypothesis, however, and getting a satisfying answer to the question in general is one of the main goals of the Langlands program! Whoa, how did we go from a simple question about reducing polynomials mod p to automorphic representations, L-functions, harmonic analysis, and all that crazy stuff?

Here are some other considerations which motivated class field theory. Given a number field F, can we find a finite extension $K \mid F$ of class number one? Shafarevich and Golod showed, in the early 1960s, that this is not always possible. However, it was conjectured by Hilbert that there is always an extension $K \mid F$ such that any non-principal ideal in $\mathcal{O}_F$ becomes principal in $\mathcal{O}_K$. This turned out to be true, due to a result called the *Principal Ideal Theorem*, which was proved in the 1930s by Furtwängler.

2. Review: global theory of number fields

We now quickly review the global theory of number fields, as is presented in Chapter I of Neukirch's *Algebraic Number Theory*. Even if you cannot recall the proofs of some of these facts, the point is to establish a common abstraction layer (and, less importantly, notation) which we will later build upon.

2.1. Number fields and integrality.

The starting point is the concept of an *(algebraic) number field*, that is to say, a finite field extension K of $\mathbf{Q}$. Note that many fields of interest, such as $\mathbf{Q}(\sqrt[3]{2})$, are not Galois extensions of $\mathbf{Q}$, since they are not normal[1]. Separability, on the other hand, is automatic in characteristic 0.

We say $\alpha \in K$ is *integral* if it satisfies $f(\alpha) = 0$ for some monic $f \in \mathbf{Z}[x]$. More generally, if $A \subset B$ is an extension of rings, we say $\alpha \in B$ is *integral over* A if $f(\alpha) = 0$ for some monic $f \in A[x]$. B itself is called *integral over* A if all its elements are so. The following fact is crucial: the set

$$\overline{A} = \{b \in B \mid b \text{ integral over } A\}$$

is a ring, called the *integral closure of* A *in* B. Indeed, recall that $b_1, \dots, b_n \in B$ are all integral over A if and only if $A[b_1, \dots, b_n]$ is finitely generated as an A-module.

We say A is *integrally closed in* B if $A = \overline{A}$. Of special interest is the case when A is an integral domain with field of fractions K; we call A simply *integrally closed* if it is integrally closed in K.

We have the following transitivity property: if $C \supset B$ is integral, and $B \supset A$ is integral, then $C \supset A$ is integral.

We will now consider the following situation: A is an integral domain, integrally closed in its field of fractions K, and B is the integral closure of A in a finite extension L of K.

2.2. Trace and norm.

We isolate two quantities of interest attached to an element x of L, namely, its norm and trace. The former often yields useful information about units and prime elements. Define an endomorphism T_x of the K-vector space L by $\alpha \mapsto x\alpha$. Its trace and determinant are called the *trace* $\mathrm{Tr}_{L|K}(x)$ and *norm* $N_{L|K}(x)$ of $x \in L$. We obtain in this way homomorphisms

$$\mathrm{Tr}_{L|K} : L \to K, \qquad N_{L|K} : L^* \to K^*.$$

In the case when $L \mid K$ is separable, we have the following convenient Galois-theoretic interpretation: if $\sigma : L \to \overline{K}$ runs over the K-embeddings of L into an algebraic closure $\overline{K}$ of K, then we have:

$$\mathrm{Tr}_{L|K}(x) = \sum_\sigma \sigma x, \qquad N_{L|K}(x) = \prod_\sigma \sigma x.$$

Another useful fact is that

$$\mathrm{Tr}_{L|K} \circ \mathrm{Tr}_{M|L} = \mathrm{Tr}_{M|K}, \qquad N_{L|K} \circ N_{M|L} = N_{M|K}.$$

[1] This is unfortunate terminology. An extension $K \mid F$ is called *normal* if it is obtained by adjoining to F all the roots of some collection $S \subset F[x]$ of polynomials.

2.3. **Discriminant of a basis.** The *discriminant* of a basis $\alpha_1, \ldots, \alpha_n$ of a separable extension $L \mid K$ is defined by

$$d(\alpha_1, \ldots, \alpha_n) = \det((\sigma_i \alpha_j))^2$$

where σ_i run over the K-embeddings $L \to \overline{K}$. [Alternative definition of the discriminant.] If $L \mid K$ is separable and $\alpha_1, \ldots, \alpha_n$ is a basis, then $d(\alpha_1, \ldots, \alpha_n) \neq 0$, and $(x, y) := \mathrm{Tr}_{L|K}(xy)$ is a nondegenerate bilinear form on the K-vector space L.

2.4. **Integral bases.** An *integral basis* for B over A (or simply an A-*basis for* B) is a collection of elements $\omega_1, \ldots, \omega_n \in B$ such that any $b \in B$ can be expressed uniquely as

$$b = a_1\omega_1 + \ldots + a_n\omega_n, \qquad a_1, \ldots, a_n \in A.$$

Since any integral basis is clearly a basis for $L \mid K$, we have $n = [L : K]$, the degree of the extension. The existence of an integral basis implies B is free as an A-module; it is therefore not surprising that in general they do not exist. However, if A is a PID, and $L \mid K$ is separable, then every finitely generated B-submodule $M \neq 0$ of L is free of rank $n = [L : K]$. In particular, B admits an integral basis over A.

By looking at simple examples like quadratic fields, one might expect that an integral basis of the form $1, \theta, \ldots, \theta^{n-1}$, where $\theta \in K$, always exists. This is called a *power basis*, and the discriminant of such a basis is simply

$$\prod_{i<j} (\theta_i - \theta_j)^2, \qquad \theta_i = \sigma_i\theta.$$

Unfortunately, power bases do not always exist.

2.5. **Ring of integers.** Of primary importance is the integral closure of $\mathbf{Z} \subset \mathbf{Q}$ in a number field K, which we denote $\mathcal{O}_K$. This is called the *ring of integers* of K. By our previous remarks, any finitely generated $\mathcal{O}_K$-submodule $\mathfrak{a}$ of K admits a $\mathbf{Z}$-basis $\alpha_1, \ldots, \alpha_n$. However, the discriminant $d(\alpha_1, \ldots, \alpha_n)$ is actually independent of the choice of basis, so we simply denote it $d(\mathfrak{a})$.

Applying this to the special case of an integral basis $\omega_1, \ldots, \omega_n$ of K, we obtain a fundamental invariant of the number field K:

$$d_K = d(\mathcal{O}_K)$$

which we call the *discriminant of* K.

If $\mathfrak{a} \subset \mathfrak{a}'$ are two nonzero finitely generated $\mathcal{O}_K$-submodules of K, then the index $(\mathfrak{a}' : \mathfrak{a})$ is finite, and

$$d(\mathfrak{a}) = (\mathfrak{a}' : \mathfrak{a})^2 \cdot d(\mathfrak{a}').$$

2.6. **Dedekind domains and unique factorization.** In general, although elements of $\mathcal{O}_K$ always admit factorizations into irreducibles, we do not in general have uniqueness. To salvage this situation we turn to the ideals of $\mathcal{O}_K$. Examination of the properties of $\mathcal{O}_K$ leads us to the general concept of a *Dedekind domain*: a Noetherian integral domain, integrally closed, such that every nonzero prime ideal is maximal. In these rings, every proper nonzero ideal $\mathfrak{a} \subset \mathcal{O}_K$ can be written (essentially) uniquely as a product of prime ideals:

$$\mathfrak{a} = \mathfrak{p}_1^{\nu_1} \cdots \mathfrak{p}_r^{\nu_r}, \qquad \nu_i > 0.$$

You should think of Dedekind domains as "generalized PIDs": if we start with a PID and consider its integral closure in some finite extension of its field of fractions, this will not generally remain a PID, but it will be a Dedekind domain. We also have a kind of generalized Chinese remainder theorem.

2.7. **Fractional ideals and the class group.** If $\mathcal{O}$ is a Dedekind domain, we want every nonzero ideal $\mathfrak{a}$ to have an "inverse". For this reason, writing K for the field of fractions of $\mathcal{O}$, we introduce the notion of a *fractional ideal*: a nonzero finitely generated $\mathcal{O}$-submodule of K.

Of course, any $a \in K^*$ gives rise to a fractional ideal, namely the principal ideal $(a) = a\mathcal{O}$. In particular, any ideal of $\mathcal{O}$ is certainly a fractional ideal; we call these *integral ideals*.

The fractional ideals form an abelian group J_K, which we call the *ideal group* of K. As mentioned before, we have the subgroup P_K of principal ideals. The quotient J_K/P_K is the all-important *ideal class group* $\mathrm{Cl}_K = J_K/P_K$ of K. It fits into the exact sequence

$$1 \to \mathcal{O}^* \to K^* \to J_K \to \mathrm{Cl}_K \to 1.$$

One way to read this is as follows: the class group measures the expansion that takes place in passing from numbers to ideals, whereas the unit group $\mathcal{O}^*$ measures the contraction in this same process.

For a general Dedekind domain, this group could be horrible, but for the ring of integers of a number field K, it is finite. This is one consequence of Minkowski's theory of lattices ("geometry of numbers"). Its order is called the *class number of* K and is denoted h_K.

There are several interesting open problems related to class numbers. A long standing conjecture says that there are infinitely many real quadratic fields with class number 1, but in fact it is not even known whether there are infinitely many algebraic number fields with class number 1! On the other hand, we now know (conjectured by Gauss and proven in the 1950s) that the only imaginary quadratic fields $\mathbf{Q}(\sqrt{d})$, $d < 0$ squarefree, with class number 1, are those with

$$d = -1, -2, -3, -7, -11, -19, -43, -67, -163.$$

These are called *Heegner numbers*.

2.8. **Lattices.** A **lattice** in an n-dimensional $\mathbf{R}$-vector space is a subgroup of the form

$$\Gamma = \mathbf{Z}v_1 + \cdots + \mathbf{Z}v_m$$

with $v_1, \ldots, v_m \in V$ linearly independent; we say they form a *basis* of Γ. The set

$$\Phi = \{x_1v_1 + \ldots + x_mv_m \mid x_i \in \mathbb{R},\ 0 \leqslant x_i < 1\}$$

is called a *fundamental mesh* of the lattice. A lattice is called *complete* if $m = n$.

More intrinsically, a lattice is a discrete subgroup of V. Now, suppose V is an *euclidean* vector space: an n-dimensional real vector space equipped with a symmetric, positive definite bilinear form $\langle -, - \rangle : V \times V \to \mathbf{R}$. Then on V we have a notion of volume (Haar measure); the form $\langle -, - \rangle$ fixes the scaling factor. The cube spanned by an orthonormal basis $e_1, \ldots, e_n$ has volume 1, and more generally, the parallelepiped spanned by n linearly independent vectors $v_1, \ldots, v_n$,

$$\Phi = \{x_1v_1 + \ldots + x_nv_n \mid 0 \leqslant x_i < 1\}$$

has volume $\mathrm{vol}(\Phi) = |\det A|$ where A is the change of basis $e \rightsquigarrow v$. As $(\langle v_i, v_j \rangle) = AA^t$, we can also write $\mathrm{vol}(\Phi) = |\det(\langle v_i, v_j \rangle)|^{1/2}$.

If $\Gamma = \mathbf{Z}v_1 + \ldots + \mathbf{Z}v_n$, then Φ is a fundamental mesh for Γ and we simply write $\mathrm{vol}(\Gamma) = \mathrm{vol}(\Phi)$. This is independent of choice of basis, as the transition matrix passing to a different basis, and its inverse, both have integer coefficients, thus have determinant ± 1.

We say $X \subset V$ is *centrally symmetric* if $x \in X$ implies $-x \in X$. It is *convex* if given $x, y \in X$, the line segment joining them is fully contained in X. With this, we have the following result, known as *Minkowski's Lattice Point Theorem*: Let Γ be a complete lattice in the euclidean space V and X a centrally symmetric, convex subset of V. Suppose $\mathrm{vol}(X) > 2^n \cdot \mathrm{vol}(\Gamma)$. Then X contains at least one nonzero $\gamma \in \Gamma$. This result cannot be improved (the $>$ cannot be replaced with $\geqslant$).

2.9. **Minkowski theory.** Given an algebraic number field $K \mid \mathbf{Q}$, the idea is to interpret its numbers as points in n-dimensional space. Consider the map

$$j : K \to K_{\mathbf{C}} := \prod_\tau \mathbf{C}, \qquad a \mapsto j(a) = (\tau a)$$

arising from the n complex embeddings $\tau : K \to \mathbf{C}$. We equip $K_{\mathbf{C}}$ with the natural hermitian scalar product,

$$\langle x, y \rangle = \sum_\tau x_\tau \overline{y_\tau}.$$

The Galois group $G(\mathbf{C} \mid \mathbf{R})$ is cyclic of order 2, generated by complex conjugation $F : z \mapsto \bar{z}$. Since this acts both on the factors of the product $K_{\mathbf{C}}$ and on the indexing set of τ (to each embedding τ corresponds its conjugate $\overline{\tau} : K \to \mathbf{C}$). In this way we obtain an involution $F : K_{\mathbf{C}} \to K_{\mathbf{C}}$ given by $(Fz)_\tau = \overline{z_{\overline{\tau}}}$. We note

$$\langle Fx, Fy \rangle = \sum_\tau (Fx)_\tau \overline{(Fy)_\tau} = \sum_\tau \overline{x_{\overline{\tau}}} y_{\overline{\tau}} = \overline{\sum_\tau x_{\overline{\tau}} \overline{y_{\overline{\tau}}}} = \overline{\sum_\tau x_\tau \overline{y_\tau}} = F\langle x, y \rangle,$$

that is, $\langle -, - \rangle$ is equivariant under F.

2.10. **Dirichlet's unit theorem.** We now examine the second main problem posed by the ring of integers $\mathcal{O}_K$, namely, its unit group. The main result here is as follows: $\mathcal{O}_K^*$ is the direct product of the finite cyclic group $\mu(K)$ (the group of roots of unity in K) and a free abelian group of rank $r+s-1$, where r is the number of real embeddings $K \to \mathbf{R}$ and s is the number of pairs of conjugate embeddings $\sigma, \overline{\sigma} : K \to \mathbf{C}$. Another way to formulate it: there exist units $\epsilon_1, \ldots, \epsilon_t$, with $t = r+s-1$, called the *fundamental units*, such that any other unit ϵ can be written uniquely as a product

$$\epsilon = \zeta \epsilon_1^{\nu_1} \cdots \epsilon_t^{\nu_t}$$

with a root of unity ζ and integers ν_i.