MATH 776
STATEMENTS OF CLASS FIELD THEORY

ANDREW SNOWDEN

1. Local class field theory

The local Kronecker–Weber theorem tells us that the maximal abelian extension of $\mathbf{Q}_p$ is obtained by adjoing all roots of unity to $\mathbf{Q}_p$. We can use this to determine the abelianization of the absolute Galois group $G_{\mathbf{Q}_p}$. Put

$$K = \bigcup_{n \geq 1} \mathbf{Q}_p(\zeta_{p^n}), \qquad L = \bigcup_{(n,p)=1} \mathbf{Q}_p(\zeta_n) = \bigcup_{n \geq 1} \mathbf{Q}_p(\zeta_{p^n-1}).$$

Then $L/\mathbf{Q}_p$ is unramified, and the maximal unramified extension since its resiude field is $\overline{\mathbf{F}}_p$. We thus see that $\mathrm{Gal}(L/\mathbf{Q}_p) \cong \hat{\mathbf{Z}}$. Now, from basic algebraic number theory, we know that $\mathbf{Q}(\zeta_{p^n})$ is totally ramified as p. We thus have

$$\mathrm{Gal}(\mathbf{Q}_p(\zeta_{p^n})/\mathbf{Q}_p) = \mathrm{Gal}(\mathbf{Q}(\zeta_{p^n})/\mathbf{Q}) \cong (\mathbf{Z}/p^n\mathbf{Z})^\times,$$

and so $\mathrm{Gal}(K/\mathbf{Q}_p) = \mathbf{Z}_p^\times$. Since KL is the maximal abelian extension of $\mathbf{Q}_p$, we find

$$G_{\mathbf{Q}_p}^{\mathrm{ab}} = \mathrm{Gal}(KL/\mathbf{Q}_p) = \hat{\mathbf{Z}} \times \mathbf{Z}_p^\times.$$

The second equality follows from the fact that K and L are linearly disjoint, since K is totally ramified and L is unramified. Recall that

$$\mathbf{Q}_p^\times = \mathbf{Z} \times \mathbf{Z}_p^\times.$$

Thus $\mathbf{Q}_p^\times$ and $G_{\mathbf{Q}_p}^\times$ look very similar! In fact, we can say that $G_{\mathbf{Q}_p}^\times$ is isomorphic to $\widehat{\mathbf{Q}}_p^\times$, the profinite completion of the group $\mathbf{Q}_p^\times$. In fact, this statement generalizes to finite extensions of $\mathbf{Q}_p$, which is essentially the main content of local class field theory:

Theorem 1.1 (Local class field theory)**.** *Let $K/\mathbf{Q}_p$ be a finite extension. Then there exists a unique isomorphism*

$$\varphi\colon \hat{K}^\times \to G_K^{\mathrm{ab}}$$

(called the local Artin map) with the following properties:

- *(a) For any uniformizer π of K, the restriction of $\varphi(\pi)$ to the maximal unramified extension of K is the Frobenius element.*
- *(b) For any finite abelian extension L/K, we have an isomorphism*

$$K^\times / \mathrm{Nm}_{L/K}(L^\times) \to \mathrm{Gal}(L/K)$$

induced by φ.

Date: January 29, 2019.

It follows from (a) that we get a commutative diagram

$$\begin{array}{ccccccccc} 1 & \longrightarrow & U_K & \longrightarrow & \hat{K}^\times & \xrightarrow{v} & \hat{\mathbf{Z}} & \longrightarrow & 1 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 1 & \longrightarrow & I & \longrightarrow & \mathrm{Gal}(K^{\mathrm{ab}}/K) & \longrightarrow & \mathrm{Gal}(K^{\mathrm{un}}/K) & \longrightarrow & 1 \end{array}$$

where $I \subset \mathrm{Gal}(K^{\mathrm{ab}}/K)$ is the inertia group, and the vertical maps are isomorphisms. In fact, there is a more precise statement: the higher unit groups correspond to higher interita groups in a specific manner.

2. Global class field theory

The cyclotomic character yields an isomorphism $\chi\colon \mathrm{Gal}(\mathbf{Q}(\zeta_n)/\mathbf{Q}) \to (\mathbf{Z}/n\mathbf{Z})^\times$. If $p \nmid n$ then p is unramified in $\mathbf{Q}(\zeta_n)$, and so we have a Frobenius element Frob_p in $\mathrm{Gal}(\mathbf{Q}(\zeta_n)/\mathbf{Q})$. Its action on roots of unity is not difficult to determine: we have $\mathrm{Frob}_p(\zeta) = \zeta^p$ (idea: this is true mod p, and prime-to-p roots of unity maps injectively mod p). Thus $\chi(\mathrm{Frob}_p) = p \in (\mathbf{Z}/n\mathbf{Z})^\times$.

This is a simple computation, but it has a remarkable consequence: p and q are two primes such that $p \equiv q \pmod{n}$ then $\mathrm{Frob}_p = \mathrm{Frob}_q$ in $\mathrm{Gal}(\mathbf{Q}(\zeta_n)/\mathbf{Q})$, and conversely. The global Kronecker–Weber theorem implies the same holds for any abelian extension of $\mathbf{Q}$. That is, if $K/\mathbf{Q}$ is a finite abelian extension then there exists some n such that $\mathrm{Frob}_p = \mathrm{Frob}_q$ whenever $p \equiv q \pmod{n}$.

This statement generalizes to arbitrary number fields, and is essentially the main theorem of global class field theory. To formulate the generalization, we need to introduce some terminology. Fix a number field K, and suppose that L/K is a finite extension. Let S be the set of primes of K that ramify in L. Given a prime $\mathfrak{p} \notin S$, we have a well-defined Frobenius element $\mathrm{Frob}_\mathfrak{p} \in \mathrm{Gal}(L/K)$. Let I^S be the group of fractional ideals of K that are relatively prime to S. This group is simply the free abelian group with basis consisting of those primes not in S. We can therefore build a homomorphism

$$\psi\colon I^S \to \mathrm{Gal}(L/K), \qquad \mathfrak{p} \mapsto \mathrm{Frob}_\mathfrak{p}.$$

This is called the **global Artin map** (or, at least, one version of it).

We now want to use this map to precisely formulate the fact that $\mathrm{Frob}_\mathfrak{p}$ is periodic in $\mathfrak{p}$. If K has class number 1, then we could simply ask that there exists some ideal $\mathfrak{m}$ such that $\mathrm{Frob}_\mathfrak{p} = \mathrm{Frob}_\mathfrak{q}$ whenever $\mathfrak{p} = (\alpha)$ and $\mathfrak{q} = (\beta)$ and $\alpha \equiv \beta \pmod{\mathfrak{m}}$. Equivalently, this would say that $\mathfrak{p} = (\beta/\alpha)\mathfrak{q}$, where β/α is an element of $K^\times$ congruent to 1 modulo $\mathfrak{m}$. Formulated in this way, we can generalize to the setting where $\mathfrak{p}$ and $\mathfrak{q}$ are possibly non-principal. In fact, there is one additional idea we need to bring in. In the case $K = \mathbf{Q}$, we have $\mathrm{Frob}_p = \mathrm{Frob}_q$ in $\mathbf{Q}(\zeta_n)$ if and only if $p = q \pmod{n}$. However, both p and $-p$ generate the ideal (p), and we might have $-p = q \pmod{n}$ without $p = q \pmod{n}$. So how do we know which generator to pick? Well, in this case, we can simply say $\mathrm{Frob}_p = \mathrm{Frob}_q$ if and only if $(p) = (\alpha)(q)$ for some positive element $\alpha \in \mathbf{Q}^\times$ that is congruent to 1 modulo n.

This motivates the following definition. A **modulus** for K is a pair $\mathfrak{m} = (\mathfrak{m}_f, \mathfrak{m}_\infty)$ where the finite part $\mathfrak{m}_f$ is an integral ideal, and the infinite part $\mathfrak{m}_\infty$ is a set of real places of K. Given a modulus $\mathfrak{m}$ we let $K^{\mathfrak{m},1}$ be the set of elements $a \in K^\times$ such that $a \equiv 1 \pmod{\mathfrak{m}_f}$ and a is positive at the places in $\mathfrak{m}_\infty$. We also write $S(\mathfrak{m}) = S$ for the set of primes dividing $\mathfrak{m}_f$, and let $I^\mathfrak{m} = I^{S(\mathfrak{m})}$. If $a \in K^{\mathfrak{m},1}$ then the principal ideal (a) belongs to $I^\mathfrak{m}$. We thus have

a group homomorphism $i\colon K^{\mathfrak{m},1} \to I^{\mathfrak{m}}$. We define the **ray class group** $C_{\mathfrak{m}}$ of K to be the quotient $I^{\mathfrak{m}}/K^{\mathfrak{m},1}$. We can now phrase the periodicity statement:

Theorem 2.1 (Reciprocity law)**.** *Let L/K be a finite abelian extension, and let S be the set of primes of K ramifying in L. Then there exists a modulus $\mathfrak{m}$ of K, prime to S, such that the Artin map induces a surjection*

$$C_{\mathfrak{m}} \to \mathrm{Gal}(L/K).$$

In fact, it induces an isomorphism

$$I^S/(i(K^{\mathfrak{m},1}) \cdot \mathrm{Nm}_{L/K}(I_L^S)) \to \mathrm{Gal}(L/K).$$

This theorem gives a lot of information about the Galois group of an abelian extension, but does not tell us what all the abelian extensions are. This is taken care of by the following theorem:

Theorem 2.2 (Existence theorem)**.** *Given any modulus $\mathfrak{m}$ of K, there exists an abelian extension $K_{\mathfrak{m}}/K$ such that the Artin map induces an isomorphism $C_{\mathfrak{m}} \to \mathrm{Gal}(L/K)$.*

The field $K_{\mathfrak{m}}$ in the above theorem is called the **ray class field** associated to $\mathfrak{m}$. Note that, by Galois theory, the existence theorem asserts that every quotient of $C_{\mathfrak{m}}$ is realized as the Galois group of some abelian extension. Also, the reciprocity law tells us that every finite abelian extension is contained in some $K_{\mathfrak{m}}$. Thus, for a general number field, $K_{\mathfrak{m}}$ takes the place of $\mathbf{Q}(\zeta_n)$ and $C_{\mathfrak{m}}$ takes the place of $(\mathbf{Z}/n\mathbf{Z})^\times$ (which is the ray class group for the modulus $((n), \infty)$).

It follows from the above that G_K^{ab} can be described as the inverse limit of $C_{\mathfrak{m}}$'s. We now study this, and give a convenient description of it. For the moment, fix a modulus $\mathfrak{m}$. Let $\mathbf{I}$ be the group of ideles of K, and $\mathbf{I}^{\mathfrak{m}} \subset \mathbf{I}$ be the subgroup consisting of ideles $x = (x_v)$ satisfying the following conditions: (a) for a finite place v dividing $\mathfrak{m}_f$, we have $x_v \in U_{v,n(v)}$, where $n(v)$ is the multiplicity of v in $\mathfrak{m}$; (b) for a real place v in $\mathfrak{m}_\infty$, we have $x_v > 0$. Let $U \subset \mathbf{I}^{\mathfrak{m}}$ be the subgroup consisting of ideles (x_v) such that $x_v \in U_v$ for all finite v.

Lemma 2.3. *We have an isomorphism $\mathbf{I}^{\mathfrak{m}}/(K^{\mathfrak{m},1} \cdot U) = C_{\mathfrak{m}}$.*

Proof. Consider the homomorphism $f\colon \mathbf{I}^{\mathfrak{m}} \to I^{S(\mathfrak{m})}$ defined by $f(x_v) = \prod_{v \nmid \infty} \mathfrak{p}_v^{\mathrm{val}(x_v)}$, where $\mathrm{val}(x_v)$ is the valuation of $x_v \in K_v^\times$. Note that, since $(x_v) \in \mathbf{I}^{\mathfrak{m}}$, we have $\mathrm{val}(x_v) = 0$ if $v \mid \mathfrak{m}$, so f does take values in $I^{S(\mathfrak{m})}$. It is clear that f is surjective. Moreover, it is clear that $\ker(f) = U$. The claim thus follows. □

Lemma 2.4. *The inclusion $\mathbf{I}^{\mathfrak{m}} \subset \mathbf{I}$ induces an isomorphism $\mathbf{I}^{\mathfrak{m}}/K^{\mathfrak{m},1} \to \mathbf{I}/K^\times$.*

Proof. The kernel of the map $\mathbf{I}^{\mathfrak{m}} \to \mathbf{I}/K^\times$ is $K^\times \cap \mathbf{I}^{\mathfrak{m}}$ (intersection computed in $\mathbf{I}$). This is clearly $K^{\mathfrak{m},1}$. Thus the stated map is well-defined and injective. To prove surjectivity, it suffices to show that $\mathbf{I} = \mathbf{I}^{\mathfrak{m}} K^\times$. For this, it suffices to show the following: given elements $x_v \in K_v^\times$ for $v \in S(\mathfrak{m})$ there exists $y \in K^\times$ totally positive such that $y \equiv x_v$ modulo $U_{v,n(v)}$ for all $v \in S(\mathfrak{m})$. This is an easy application of the Chinese remainder theorem. □

We thus see that $\mathbf{C}_K = \mathbf{I}/K^\times$ (the idele class group) maps to each $C_{\mathfrak{m}}$, and does so compatibly. It is clearly not the inverse limit (since $\mathbf{I}/K^\times$ still has the real numbers in it, and is therefore not profinite), but it does surject onto the inverse limit. Thus it surjects onto G_K^{ab}. In fact, we have the following theorem:

Theorem 2.5. *Let K be a number field.*

(a) *We have a unique homomorphism* $\varphi\colon \mathbf{I}_K \to G_K^{\mathrm{ab}}$ *(the global Artin map) such that for every finite place* v*, the restriction of* φ *to* $K_v^\times$ *is the local Artin map* φ_v*. (And for real places,* φ *induces an isomorphism* $K_v^\times/K_{v,>0} \cong G_{K_v}$*.)*
(b) *The kernel of* φ *contains* $K^\times$*.*
(c) *For a finite abelian extension* L/K*, the map* φ *induces an isomorphism*

$$\mathbf{C}_K/\operatorname{Nm}_{L/K}(\mathbf{C}_L) \to \operatorname{Gal}(L/K).$$

In the adelic language, the existence theorem takes the following form:

Theorem 2.6. *Fix an algebraic closure* $\overline{K}$ *of* K*. Then for every open subgroup* U *of* $\mathbf{C}_K$ *of finite index, there exists a unique abelian extension* L *of* K *ontained in* $\overline{K}$ *such that* $\operatorname{Nm}_{L/K}(\mathbf{C}_L) = U$*.*

References

[K] K. Kedlaya. Notes on class field theory. http://www.math.mcgill.ca/darmon/courses/cft/refs/kedlaya.pdf
[W] L. Washington. *Introduction to Cyclotomic Fields*, Chapter 14