Class Field Theory and the Local-Global Property

Noah Taylor
Discussed with Professor Frank Calegari

March 18, 2017

1 Classical Class Field Theory

1.1 Lubin Tate Theory

In this section we derive a concrete description of a relationship between the Galois extensions of a local field K with abelian Galois groups and the open subgroups of $K^\times$. We assume that K is a finite extension of $\mathbb{Q}_p$, $\mathcal{O}_K$ has maximal ideal $\mathfrak{m}$, and we suppose the residue field k of K has size q, a power of p.

Lemma 1.1 (Hensel)**.** *If $f(x)$ is a polynomial in $\mathcal{O}_K[x]$ and $a \in \mathcal{O}_K$ with $\left|\frac{f(a)}{f'(a)^2}\right| < 1$ then there is some a_1 with $f(a_1) = 0$ and $|a - a_1| \leq \left|\frac{f(a)}{f'(a)}\right|$.*

Proof. As in Newton's method, we continually replace a with $a - \frac{f(a)}{f'(a)}$. Careful consideration of the valuation of $f(a)$ shows that it decreases while $f'(a)$ does not, so that $f(a)$ tends to 0. Because K is complete, the sequence of a's we get has a limit a_1, and we find that $f(a_1) = 0$. The statement about the distance between a and a_1 follows immediately. □

We can apply this first to the polynomial $f(x) = x^q - x$ and a being any representative of any element in k to find that K contains the $q-1$'st roots of unity. It also follows that if L/K is an unramified extension of degree n, then $L = K(\zeta)$ for a $q^n - 1$'st root of unity ζ. In particular, L/K is an abelian extension.

Proposition 1.2. *If L/K is unramified, then* $\mathrm{Gal}(L/K)$ *is cyclic, generated by* $\mathrm{Frob} : \zeta \to \zeta^q$*. More generally, there is a unique generator* Frob *for which* $\mathrm{Frob}(x) \equiv x^q \mod \mathfrak{m}$ *for all $x \in \mathcal{O}_L$.*

Proposition 1.3. *The compositum of two abelian extensions of K is another abelian extension of K; the compositum of two unramified extensions of K is another unramified extension of K.*

So we may talk about K^{ab}/K and K^{ur}/K, the maximal abelian and unramified extensions of K. We let π be any uniformizer of K.

Lemma 1.4. *Given a polynomial $f(x) = x^q + \pi x^2 u(x) + \pi x$ for some u, there is a unique power series $F \in \mathcal{O}_K[\![x, y]\!]$ with $F(x, y) = F(y, x)$, $F(x, 0) = x$, $F(F(x, y), z) = F(x, F(y, z))$ and $f(F(x, y)) = F(f(x), f(y))$. Furthermore, for $a \in \mathcal{O}_K$, there is a unique $[a] \in \mathcal{O}_K[\![x]\!]$ with $[a] \equiv ax \mod (x^2)$ and $[a] \circ f = f \circ [a]$.*

Proof. [1] I.2.11. □

Theorem 1.5. *Suppose f is defined as above. Further suppose $\Lambda_{n,f} = \{x : \underbrace{f \circ f \circ \ldots \circ f}_{n}(x) = 0\}$, and $K_{n,f} = K(\Lambda_{n,f})$, and $K_f = \cup_{n=1}^{\infty} K_{n,f}$. Then K_f/K is a totally ramified abelian extension, $K^{ab} = K^{ur} \cdot K_f$ and $K_f \cap K^{ur} = K$. Thus* $\mathrm{Gal}(K^{ab}) = \mathrm{Gal}(K_f) \times \mathrm{Gal}(K^{ur})$.

Proof. The polynomial $\frac{f}{x} \circ f \circ \ldots \circ f$ can be written as $\pi + x \cdot \pi(\ldots) + x^{q^{n-1}(q-1)}$, so it is irreducible by Eisenstein and the roots, $\Lambda_{n,f} \backslash \Lambda_{n-1,f}$, are all conjugates. Noting that $F([a],[b]) \equiv (a+b)x \mod (x^2)$ and $F([a],[b]) \circ f = F(f \circ [a], f \circ [b]) = f \circ F([a],[b])$, and remembering uniqueness, we must have $F([a],[b]) = [a+b]$. Similarly, $[a] \circ [b] = [ab]$. Now $[a](\Lambda_{n,f}) \subseteq \Lambda_{n,f}$ because $[a]$ commutes with f, and since $\underbrace{f \circ f \circ \ldots \circ f}_{k} = [\pi^k]$, we see that $[a](\Lambda_{n,f}) = 0$ if and only if $\pi^n | a$. Then this gives an action of $\mathcal{O}_K/(\pi^n)$ on $\Lambda_{n,f}$. If $x \in \Lambda_{n,f} \backslash \Lambda_{n-1,f}$, then the action sends x everywhere. And since $[b]([a](x)) = [ab](x)$, as long as $\pi \nmid a$, $x \to [a](x)$ is an automorphism of $\Lambda_{n,f}$ and extends to an automorphism of $K_{n,f}$. So $\mathrm{Gal}(K_{n,f}/K) \simeq (\mathcal{O}_K/(\pi^n))^\times$, and is thus abelian. It's easy to check that these are compatible for different n and extend to an isomorphism $K_f \simeq \widehat{\mathcal{O}^\times} = \mathcal{O}^\times$.

The other parts are in [1] I.1-3. □

Proposition 1.6. *The fields $K_{n,f}$ depend not on f but only on the uniformizer π. As long as $f \equiv \pi x \mod (x^2)$ and $\equiv x^q \mod \pi$, different f's give the same fields $K_{n,f}$. Thus we write $K_{n,\pi}$ and K_π instead. And $[a]$, while a priori different symbols for different f, gives the same action on K_π for different f's.*

Theorem 1.7. *There is a map ϕ from $K^\times$ to* $\mathrm{Gal}(K^{ab}/K)$ *which takes uniformizers π to* Frob *when restricted to K^{ur} and, given an abelian extension L/K, can be restricted to $K^\times/N_{L/K}(L^\times) \simeq \mathrm{Gal}(L/K)$. That is, if we restrict ϕ to $\mathrm{Gal}(L/K)$, then the kernel is exactly $N_{L/K}(L^\times)$, the norm subgroup of L over K.*

Proof. The map is given by

$$x = u \cdot \pi^k \to ([u^{-1}], \mathrm{Frob}^k) \in \mathrm{Gal}(K_\pi) \times \mathrm{Gal}(K^{ur}) = \mathrm{Gal}(K^{ab}).$$

This is in fact invariant for different π's. For proof of this theorem and the previous (nonobvious) proposition, see [1] I.3. □

Theorem 1.8. *Any finite-index open subgroup of $K^\times$ is equal to the norm group $N_{L/K}(L^\times)$ of a unique finite abelian extension L/K.*

Example 1.9 (Local Kronecker-Weber). If $K = \mathbb{Q}_p$, we can take $\pi = p$, $f(x) = (x+1)^p - 1$, $F(x,y) = (x+1)(y+1) - 1$, and $[u] = (x+1)^u - 1$, where this exponent is defined because of Lucas' Theorem. This gives $\Lambda_{n,f} = \{\mu_{p^n}^i - 1\}$, and any abelian extension of $\mathbb{Q}_p$ is contained in a cyclotomic extension. The corresponding ϕ takes p to $\begin{cases} \zeta_m \to \zeta_m^p \\ \zeta_{p^n} \to \zeta_{p^n} \end{cases}$ and $x \in \mathcal{O}_K^\times$ to $\begin{cases} \zeta_m \to \zeta_m \\ \zeta_{p^n} \to \zeta_{p^n}^{x^{-1}} \end{cases}$.

Remark 1.10. The key point is not really the construction of ϕ, although that was a major triumph of Tate and Lubin. The main draw of local class field theory is that it describes a certain class of representations of $\mathrm{Gal}(\overline{K}/K)$, namely the one-dimensional ones. It shows that they have this very nice structure: if we complete $K^\times$ with respect to its finite-dimensional quotients to get $\widehat{K^\times}$, this is isomorphic to $\mathrm{Gal}(K^{ab}/K)$. And $\widehat{K^\times}$ has a nice describable structure, namely $\widehat{\mathbb{Z}} \times \mu_K \times (1 + \pi\mathcal{O}_K)$. So we get a description of all 1-dimensional representations of $\mathrm{Gal}(\overline{K}/K)$, an extrinsic property of K depending on its algebraic closure, depending very explicitly on $\widehat{K^\times}$ and hence on only $K^\times$.

1.2 Global Class Field Theory

Let K be a global field. We write K_v to be the completion of K with respect to the absolute value given by v.

Definition 1.11. The **ideles** of K are defined as $\mathbb{I}_K = \prod_v' K_v^\times$ over all places v, where the product is restricted so that for all but finitely many v, the element is in $\mathcal{O}_v^\times$. A basis for the topology is given by $\prod_v' U_v$, U_v open in $K_v^\times$, and the product again restricted so that U_n is almost always $\mathcal{O}_v^\times$.

The diagonal embedding of $K^\times$ into $\mathbb{I}_K$ is discrete, so we can define $C_K = \mathbb{I}_K/K^\times$, the idele class group. This will play the same role as $K^\times$ did in local class field theory.

For a finite extension L/K, we can embed $\mathbb{I}_K$ into $\mathbb{I}_L$: the coordinate of w, a place over v, is a_v. We can go back the other way as well: the norm of an idele $(a_w)_w$ in $\mathbb{I}_L$ is $(\prod_{w|v} N_{L_w/K_v}(a_w))_v$. Note that $N_{L/K}$ takes the embedding of $L^\times$ in $\mathbb{I}_L$ to the embedding of $K^\times$ in $\mathbb{I}_K$, so we can define the norm map from C_L to C_K.

Theorem 1.12. *There is a homomorphism $\phi : C_K \to \mathrm{Gal}(K^{ab}/K)$ which can be restricted to an isomorphism $C_K/N_{L/K}(C_L) \to \mathrm{Gal}(L/K)$ for Galois extensions L/K.*

Proof. We first define a map $\phi_{L/K} : \mathbb{I}_K \to \mathrm{Gal}(L/K)$ for some abelian extension L by taking $\phi_{L/K}((a_v)_v) = \prod_v \phi_v(a_v)$, where ϕ_v is the local map defined above, but restricted from $\mathrm{Gal}(K_v^{ab}/K_v)$ to $\mathrm{Gal}(L_w/K_v)$ to $\mathrm{Gal}(L/K)$. (If v is real infinite, ϕ_v sends positive numbers to the identity and negative numbers to conjugation in $\mathrm{Gal}(\mathbb{C}/\mathbb{R})$; if v is complex infinite then there is no Galois group.) This map is well defined, because all but finitely many v are unramified in the extension, meaning that they only act as powers of Frob; and all but finitely many of those v have $a_v \in \mathcal{O}_{K_v}^\times$, so it is the zeroth power of Frob, or the identity. Thus the product is actually finite.

Notice that $N_{L/K}(\mathbb{I}_L)$ is in the kernel, because all L_w are isomorphic for all w over v since L/K is Galois. So for any v and the section of $\mathbb{I}_L$, $(a_{w_i})_{w_i|v}$, the product of their norms in K_v maps to the identity in the Galois group $\mathrm{Gal}(L_w/K_v)$ because each norm separately does, by definition.

This $\phi_{L/K}$ is functorial in L (that is, $\phi_{L/K}|_{L'} = \phi_{L'/K}$ if $K \subset L' \subset L$) by the local Artin map's own functoriality; we can thus define $\phi : C_K \to \mathrm{Gal}(K^{ab}/K)$ by inverse limit.

Half of the theorem is that the embedding of $K^\times$ is in the kernel of this map; the other half is showing that $N_{L/K}(C_L)$ is the entire rest of the kernel, and that it is surjective. For a proof, see [1] VII.8. □

The next theorem is reminiscent of 1.8 in the local case:

Theorem 1.13. *The map ϕ gives an inclusion-reversing bijection between finite index subgroups of C_K and finite abelian extensions of K.*

Proof. [1] VII.9. □

We can get the global Kronecker Weber theorem now: any abelian extension of $\mathbb{Q}$ is contained in a cyclotomic extension. The proof involves showing that $\mathbb{I}_\mathbb{Q} \simeq \mathbb{Q}^\times \times \mathbb{R}^+ \times \prod_p \mathbb{Z}_p^\times$, so that quotienting by $\mathbb{Q}^\times$ leaves $\mathbb{R}^+ \times \prod_p \mathbb{Z}_p^\times$; and also showing that the subgroups corresponding to adjoining the p^e'th roots of unity are exactly $\mathbb{R}^+ \times (1 + p^e\mathbb{Z}_p) \times \prod_{q \neq p} \mathbb{Z}_q^\times$. Then any finite-index subgroup of $C_\mathbb{Q}$ contains an intersection of a finite number of these groups; thus by inclusion-reversal, the abelian extension must be contained in a cyclotomic extension.

2 Group Cohomology

Here we collect some results about group cohomology that we use later. Much of this was taken from [5] IV and [3] VII-VIII.

Definition 2.1. The cohomology of a group G and some module M can be defined as follows: we take a projective $\mathbb{Z}(G)$-resolution of $\mathbb{Z}$, say $\ldots \to P_1 \to P_0 \to \mathbb{Z} \to 0$. Then we take $C^i = \hom_G(P_i, M)$; this gives a cochain complex $0 \to C^0 \to C^1 \to \ldots$; then $H^i(G, M)$ is defined to be the homology of this complex.

The usual resolution is $P_n = \mathbb{Z}(G^{n+1})$ and the map is $(g_0, \ldots g_n) \to (g_1, \ldots g_n) - (g_0, g_2, \ldots g_n) + \ldots + (-1)^n(g_0, \ldots g_{n-1})$. This can be used (modifying a bit to make the G-homs just plain maps) to calculate $H^0(G, M) = M^G$ and

$$H^1(G, M) = \frac{\{\phi : G \to M | \phi(gh) = \phi(g) + g\phi(h)\}}{\{\phi_m : \phi(g) = gm - m\}}.$$

We also record H^2:

$$H^2(G, M) = \frac{\{\phi : G \times G \to M | g\phi(h, k) + \phi(g, hk) = \phi(gh, k) + \phi(g, h)\}}{\{\phi_\varphi : \phi_\varphi(g, h) = g\varphi(h) - \varphi(gh) + \varphi(g)\}}$$

We now suppose G is finite. We can make the setup a bit more symmetric by taking a complete resolution of $\mathbb{Z}$. For example $P_{-n} = \mathbb{Z}[(G^n)^*]$, the dual space of P_{n+1}, and the map $P_{-n} \to P_{-n-1}$ is

$$(g_1, \ldots g_n)^* \to \sum_{s \in G} \left[(s, g_1, \ldots g_n)^* - (g_1, s, g_2, \ldots g_n)^* + \ldots + (-1)^n (g_1, g_2, \ldots g_n, s)^*\right].$$

And we must define the map from P_0 to P_{-1} to be $g \to \sum_{s \in G} s^*$, irrespective of g. We then define the cochain complex $C^i = \hom_G(P_i, M)$ and then the **Tate cohomology group** $\widehat{H}^i(G, M)$ is the homology of this complex. For example, we get that $\widehat{H}^0(G, M) = M^G / \left\{ \left(\sum_{g \in G} g \right) \cdot m : m \in M \right\}$.

We say $\widehat{H}^{-i-1}$ is the i'th homology group $\widehat{H}_i(G, M)$. In particular, we find that

$$\widehat{H}^{-1}(G, M) = \widehat{H}_0(G, M) = \frac{\{m : \left(\sum_{g \in G} g \right) \cdot m = 0\}}{\langle (g - \mathrm{Id}_G) \cdot m : g \in G, m \in M \rangle}.$$

With a lot more work, we further compute that $\widehat{H}_1(G, \mathbb{Z}) = G/[G, G] = G^{ab}$, the abelianization of G.

Theorem 2.2. *If G is finite and cyclic, then $\widehat{H}^i(G, A)$ is periodic in i with period 2.*

Proof. The proof uses not the standard resolution but the resolution

$$\ldots \xrightarrow{\cdot(g-1)} \mathbb{Z}[G] \xrightarrow{\cdot(1+g+\ldots+g^{n-1})} \mathbb{Z}[G] \xrightarrow{\cdot(g-1)} \mathbb{Z}[G] \xrightarrow{g \to 1} \mathbb{Z} \to 0$$

and its dual. From here it's obvious by definition. □

Theorem 2.3 (Tate)**.** *Suppose G is finite, A is a G-module and we know that for all subgroups H (proper or not) $H^1(H, A) = 0$ and there is an $a \in H^2(G, A)$ for which $H^2(H, A)$ is cyclic generated by the restriction of the domain a from G to H. Then there is a homomorphism $\widehat{H}^r(G, \mathbb{Z}) \simeq \widehat{H}^{r+2}(G, A)$ given by "cupping with a".*

Proof. [5] IV.10.12. □

3 Brauer Groups

Definition 3.1. A **central simple algebra** (CSA) over a field K is an algebra A over K for which the embedding of K into A is the center of A, and has no nontrivial two-sided ideals.

Theorem 3.2 (Wedderburn)**.** *If K is a field, then any finite-dimensional CSA over K is isomorphic to $M_n(D)$ for some division algebra D over K.*

Proof. [1] IV.1.15. □

Definition 3.3. The **Brauer group** of K, called $\mathrm{Br}(K)$, is the set of CSA's over K mod the equivalence of being matrix algebras over the same D, with tensoring as the group operation.

All the things that need to be checked (this is a well-defined operation, the inverse of $[A]$ is $[A^{opp}]$, etc.) are true. We define also the Brauer group $\mathrm{Br}(L/K)$ to be the CSA's $[A]$ for which $[A] \otimes L \simeq M_n(L)$ is trivial in $\mathrm{Br}(L)$; we say that L **splits** these classes.

If L is algebraically closed, then there is no finite-dimensional division algebra D over L, since any element of D generates a field over L, so that any element of D is already in L. Thus, if K is just a field, then tensoring any CSA A over K with $\overline{K}$ gives a matrix algebra $M_n(\overline{K})$ but preserves dimension; therefore, the dimension of A over K is a square.

Theorem 3.4. *Given a CSA A over K, say the centralizer of a subalgebra B is $C(B)$. Then $[B : K] \cdot [C(B) : K] = [A : K]$. In particular, the largest subfields of a division algebra are of dimension equal to the square root of the dimension of A over K. Furthermore, a field L with $[L : K]^2 = [A : K]$ splits A if and only if it can be embedded into A.*

Proof. [1] IV.3.1, IV.3.6. □

Theorem 3.5 (Noether-Skolem)**.** *If f, g are homomorphisms from A to B and A is simple over K and B is a CSA over K, then there is some element $b \in B$ with $f(x) = b \cdot g(x) \cdot b^{-1}$.*

Proof. [1] IV.2.10. □

Let us assume now that L/K is a finite Galois extension. Then I claim that $\mathrm{Br}(L/K) = H^2(\mathrm{Gal}(L/K), L^\times)$. Given a CSA A of dimension $[L : K]^2$ which L splits and therefore embeds into, we can find an element e_σ in A, by 3.5, for which $\sigma(\ell) = e_\sigma \ell e_\sigma^{-1}$. This is unique up to multiplication on the right by elements of L. Then we have $e_\sigma e_\tau = \phi(\sigma, \tau) e_{\sigma\tau}$ for some $\phi(\sigma, \tau)$. By associativity, we require that

$$\sigma(\phi(\tau, \nu))\phi(\sigma, \tau\nu) = \phi(\sigma, \tau)\phi(\sigma\tau, \nu)$$

which is exactly the multiplicative cocycle condition from above. Choosing different e_τ changes the cocycle by a coboundary, so this is a map from $\mathrm{Br}(L/K)$ to $H^2(\mathrm{Gal}(L/K), L^\times)$. There's an inverse; namely, given some cocycle, we can just build the algebra in the exact opposite way. Going the other way produces a CSA, which takes work to check. So it is bijective, and it can be checked (with some difficulty) that the group structure on each is the same. We can prove the statement is true for non-Galois extensions as well, if we take $H^2(\mathrm{Gal}(L/K), L^\times)$ to be defined as $\mathrm{Ker}\big[H^2(\mathrm{Gal}(M/K), M^\times) \to H^2(\mathrm{Gal}(M/L), M^\times)\big]$, the kernel of the restriction map where M is the Galois closure of L over K.

3.1 K local

We now suppose K is local. Then given a central division algebra D, we can extend the absolute value of K to D by, given any $a \in D$, letting $P(x)$ be the characteristic polynomial of a as a transformation of D by left multiplication, and then letting $|a| = \sqrt[[D:K]]{|P(0)|}$. This is multiplicative, and it agrees with the normalized absolute value on any subfield (because the characteristic polynomial of x with respect to a smaller division algebra is just a root of the one we found). So for any x and y, we have (by the non-archimedean property of $|\cdot|$ on $K(x^{-1}y)$)

$$|x+y| = |x| \cdot |x^{-1}y + 1| \geq |x| \cdot \min(|x^{-1}y|, |1|) = \min(|y|, |x|)$$

so that this absolute value is a norm. If the image of $|\cdot|_D$ is $|\mathfrak{p}|^{\frac{1}{e}}$ and that the dimension of $\mathcal{O}_D/\mathfrak{P}_D$ over $\mathcal{O}_K/\mathfrak{p}_K$ is f, then $e \leq \sqrt{[D:K]} =: n$ because the largest subfields of D have dimension n and $|\cdot|$ agrees with the definition on subfields, and $f \leq n$ because we can lift any element of $\mathcal{O}_D/\mathfrak{P}_D$ to a root of unity in $\mathcal{O}_D$ generating a field of dimension f. But $ef \geq n^2$ because $\{1, \pi, \pi^2, \ldots \pi^{e-1}\} \times \{1, \zeta, \zeta^2, \ldots \zeta^{f-1}\}$ form a spanning set for D as a K-vector space, where ζ is a root of unity and π is a uniformizer of D. So $e = f = n$, so there is an embedding of the nth roots of unity into D.

We now define a map Inv as follows: if ζ is a root of unity, we have by 3.5 an element b with $b\zeta b^{-1} = \zeta^q$; we set $\mathrm{Inv}(D) = u \mod \mathbb{Z}$ where $|b| = |\pi|^{nu}$, where again π is a uniformizer. This is well-defined; if we have another root of unity ρ inside D, then by 3.5 again, there is some element c in D with $c\rho c^{-1} = \zeta$; if b' is the element for ρ, then

$$bc\rho c^{-1}b^{-1} = b\zeta b^{-1} = \zeta^q = (c\rho c^{-1})^q = c\rho^q c^{-1} = cb'\rho(b')^{-1}c^{-1}$$

so $c^{-1}b^{-1}cb'$ commutes with ρ. By 3.4, $c^{-1}b^{-1}cb'$ is in $K(\rho)$ and so it has integer norm; thus b and b' have the same norm up to an integer.

Lemma 3.6. Inv *is an isomorphism from* $\mathrm{Br}(K)$ *to* $\mathbb{Q}/\mathbb{Z}$. *Extending the base field by tensoring with* L *multiplies the corresponding invariant by* $[L:K]$. *Therefore, any division algebra of dimension* n^2 *over* K *contains (and is split by) every field extension of degree* n, *and* $\mathrm{Br}(L/K) \simeq \frac{1}{[L:K]}\mathbb{Z}/\mathbb{Z}$.

Proof. [3] XIII.3 Prop 7. □

From here we can give a proof of 1.7. We apply 2.3 to $G = \mathrm{Gal}(L/K)$. Any subgroup of G is given by $\mathrm{Gal}(L/M)$ for some M over K. By Hilbert's Theorem 90, $H^1(H, L^\times)$ is trivial, and $H^2(H, L^\times) = \mathrm{Br}(L/M)$ which is cyclic of order $[L:M]$. And the element with invariant $\frac{1}{[L:K]}$ restricts to the generator for each $\mathrm{Br}(L/M)$. Thus we apply 2.3 to get an isomorphism between $\widehat{H}^{-2}(G, \mathbb{Z}) = G^{ab}$ and $\widehat{H}^0(G, L^\times) = K^\times / N_{L/K}(L^\times)$. This isn't quite as explicit an isomorphism as the one we gave above; it becomes more so if we were to define the isomorphism "cupping" with the generator.

If K is $\mathbb{R}$, then the cohomology description is $H^2(\mathrm{Gal}(\mathbb{C}/\mathbb{R}), \mathbb{C}^\times)$. The cohomology classes here are generated by $\phi(1,1) = \phi(1,\tau) = \phi(\tau,1) = 1$ and $\phi(\tau,\tau) = \pm 1$; thus $\mathrm{Br}(\mathbb{R}) = \mathbb{Z}/2\mathbb{Z} = \frac{1}{2}\mathbb{Z}/\mathbb{Z}$, where the nontrivial class goes to $\frac{1}{2} + \mathbb{Z}$.

3.2 K global

Theorem 3.7 (Albert-Brauer-Hasse-Noether)**.** *There is an exact sequence*

$$0 \to \mathrm{Br}(K) \to \bigoplus_v \mathrm{Br}(K_v) \xrightarrow{\oplus_v \mathrm{Inv}} \mathbb{Q}/\mathbb{Z} \to 0$$

which describes exactly the structure of the Brauer group $\mathrm{Br}(K)$*. This restricts to*

$$0 \to \mathrm{Br}(L/K) \to \bigoplus_v \mathrm{Br}(L_w/K_v) \xrightarrow{\oplus_v \mathrm{Inv}} \frac{1}{[L:K]}\mathbb{Z}/\mathbb{Z}$$

for Galois extensions L/K*.[6]*

This involves a bit of work on cohomology groups. The first key result is that this middle group is the limit of cohomology groups $H^2(\mathrm{Gal}(L/K), \mathbb{I}_L)$ where $\mathrm{Gal}(L/K)$ acts on $\mathbb{I}_L$ by σ sending a in the w-prime position to $\sigma(a)$ in the $\sigma(w)$ position. If we take $\mathbb{I}_{L,S}$ to be the set of ideles for which a_w is a unit in L_w for w dividing v outside S (which contains all archimedean places), then $H^2(\mathrm{Gal}(L/K), \mathbb{I}_L) = \varinjlim H^2(\mathrm{Gal}(L/K), \mathbb{I}_{L,S})$ because cohomology commutes with direct limits. It also commutes with products; so

$$H^2(\mathrm{Gal}(L/K), \mathbb{I}_{L,S}) = \prod_{v\in S} H^2\left(\mathrm{Gal}(L/K), \prod_{w|v} L_w^\times\right) \times \prod_{v\notin S} H^2\left(\mathrm{Gal}(L/K), \prod_{w|v} \mathcal{O}_w^\times\right)$$

We can simplify these two products using so-called "Shapiro's Lemma" to get

$$H^2(\mathrm{Gal}(L/K), \mathbb{I}_{L,S}) = \prod_{v\in S} H^2(\mathrm{Gal}(L_w/K_v), L_w) \times \prod_{v\notin S} H^2(\mathrm{Gal}(L_w/K_v), \mathcal{O}_w^\times)$$

for some $w|v$ (because all Galois groups and places above v are equivalent). Then we can show that for $w|v$ unramified, and thus $\mathrm{Gal}(L_w/K_v)$ cyclic with Frob generator, we have $H^2(\mathrm{Gal}(L_w/K_v), \mathcal{O}_w^\times) = \widehat{H}^0(\mathrm{Gal}(L_w/K_v), \mathcal{O}_w^\times) = \mathcal{O}_v^\times / N_{w/v}(\mathcal{O}_w^\times) = 0$ because the norm group of units of unramified extensions is everything. Thus the product above becomes $\prod_{v\in S} H^2(\mathrm{Gal}(L_w/K_v), L_w^\times) = \prod_{v\in S} \mathrm{Br}(L_w/K_v)$. We now take the direct limit as above to get $H^2(\mathrm{Gal}(L/K), \mathbb{I}_L) = \bigoplus_v \mathrm{Br}(L_w/K_v)$.

Note that the proof works for any dimension: $H^i(\mathrm{Gal}(L/K), \mathbb{I}_L) = \bigoplus_v H^i(\mathrm{Gal}(L_w/K_v), L_w)$. If we look at the long exact sequence given by $0 \to L^\times \to \mathbb{I}_L \to C_L \to 0$ as $\mathrm{Gal}(L/K)$-modules, and remembering Hilbert 90, we get the exact sequence

$$0 \to H^1(\mathrm{Gal}(L/K), C_L) \to H^2(\mathrm{Gal}(L/K), L^\times) \to \bigoplus_v H^2(\mathrm{Gal}(L_w/K_v), L_w) \to H^2(\mathrm{Gal}(L/K), C_L) \to \dots$$

so that the exact sequence of the theorem requires that $H^1(\mathrm{Gal}(L/K), C_L) = 0$. We can prove this in the following way. We reduce to the case of $[L:K]$ being a p-group by embedding $H^1(\mathrm{Gal}(L/K), C_L)$ into $\prod_{p|[L:K]} H^1(G_p, C_L)$, where G_p is a p-Sylow subgroup of $\mathrm{Gal}(L/K)$. It is true that this map is injective. And then we can restrict to cyclic groups of order p by using induction and the inflation-restriction exact sequence $0 \to H^1(\mathrm{Gal}(L/K), C_L) \to H^1(\mathrm{Gal}(M/K), C_M) \to H^1(\mathrm{Gal}(M/L), C_M)$ for some tower of normal extensions $K \subseteq L \subseteq M$.

We will conclude with the two following lemmas:

Lemma 3.8 (First Inequality)**.** *If* L/K *is cyclic, then*

$$h_{2/1}(L/K, C_L) = \frac{\#H^2(\mathrm{Gal}(L/K), C_L)}{\#H^1(\mathrm{Gal}(L/K), C_L)} = [L:K]$$

Proof. [2] V. □

Lemma 3.9 (Second Inequality)**.** *For any Galois extension* L/K*,* $\#\widehat{H^0}(\mathrm{Gal}(L/K), C_L) | [L:K]$.

Proof. [2] VI. □

Combining the two, for cyclic extensions we find that $[L : K] = \#H^2(\mathrm{Gal}(L/K), C_L)$ and $1 = \#H^1(\mathrm{Gal}(L/K), C_L)$. So we're done.

Remark 3.10. We can (with much harder arguments) prove that $H^2(\mathrm{Gal}(L/K), C_L) \simeq \frac{1}{[L:K]}\mathbb{Z}/\mathbb{Z}$ not just for cyclic extensions but for any Galois extension L/K, as in [2] VII, and restriction from L/K to L/M works well with this isomorphism: it multiplies by $[M : K]$. So the hypotheses of Tate's theorem are satisfied, and we can apply it to get an isomorphism $\widehat{H}^{-2}(\mathrm{Gal}(L/K), \mathbb{Z}) \to \widehat{H}^0(\mathrm{Gal}(L/K), C_L)$. This is exactly the isomorphism of class field theory, $\mathrm{Gal}(L/K)^{ab} \simeq C_K/N(C_L)$. And all compatibilities hold with restriction, because they do in the cohomology groups. So this is class field theory.

3.3 Brauer Groups and Artin Reciprocity

We continue to look at the Brauer exact sequence 3.7 as a means to study class field theory.

Theorem 3.11. *For an abelian extension of local fields L/K and any $\chi \in H^1(\mathrm{Gal}(L/K), \mathbb{Q}/\mathbb{Z}) = Hom(\mathrm{Gal}(L/K), \mathbb{Q}/\mathbb{Z})$ and any $a \in L^\times$, the equality below holds:*

$$\chi\left(\phi_{L/K}(a)\right) = \mathrm{Inv}(\delta\chi \cup a)$$

where δ is the connecting homomorphism $H^1(\mathrm{Gal}(L/K), \mathbb{Q}/\mathbb{Z}) \to H^2(\mathrm{Gal}(L/K), \mathbb{Z})$ and $\phi_{L/K}$ is the local reciprocity map.

Proof. [1] III.3.6. □

The main point of this theorem is that it allows us to relate the local map, and hence the global map, to the Brauer invariant. Notice that if we take some global extension L/K, and some $k \in K^\times \subseteq \mathbb{I}_K$, then for any global character $\chi : \mathrm{Gal}(L/K) \to \mathbb{Q}/\mathbb{Z}$,

$$\chi(\phi_{L/K}(k)) = \chi(\prod_v \phi_{L_w/K_v}(k)) = \sum_v \chi_v(\phi_{L_w/K_v}(k)) = \sum_v \mathrm{Inv}(k \cup \delta\chi_v)$$

and the cohomology class $k \cup \delta\chi_v \in H^2(\mathrm{Gal}(L_w/K_v), K_v^\times)$ is represented by $(\sigma, \tau) \to k^{\overline{\chi}(\sigma)+\overline{\chi}(\tau)-\overline{\chi}(\sigma\tau)}$ where $\overline{\chi}$ is some lift of χ to $\mathbb{Q}$. As we vary χ, we look for when the LHS remains 0. The right side of this equality is the sum of the invariants of the local classes of the CSA corresponding to this class. So if the Brauer exact sequence holds, then the sum of the invariants is 0 whatever k and χ are, so k is in the kernel of the Artin map. Conversely, if L/K is cyclic, then for χ taking a generator of $\mathrm{Gal}(L/K)$ to $\frac{1}{[L:K]}$, $k \to k \cup \delta\chi$ is an isomorphism $\widehat{H}^0(\mathrm{Gal}(L/K), L^\times) = K^\times/N(L^\times) \to H^2(\mathrm{Gal}(L/K), L^\times)$ as we know exists from 2.2. Thus the sum of the invariants of any cohomology class is $\chi(\phi_{L/K}(k))$ for some χ and some k, which is 0. We have shown that the Brauer sequence implies the reciprocity statement, and the reciprocity statement implies exactness at the center term of the Brauer sequence in cyclic extensions.

4 Class Formations

The ideas behind these proofs of local and global class field theory are obviously similar. They both involve the use of Tate's Theorem to give the key isomorphism, after proving that the first cohomology groups are 0 and the second cohomology groups are cyclic of exactly the order of the Galois group. To put these in all-encompassing but abstract terms is to discuss the idea of class formations.

Definition 4.1. A **formation** is a group G, a collection of finite-index subgroups $\{G_F\}$ which is conjugate-closed, upward-closed and closed under finite intersection and whose full intersection is trivial, and a G-module A for which the stabilizer of $a \in A$ is one of the G_F. We say $A_F = \{a \in A : g \cdot a = a \forall g \in G_F\}$. We also say that F'/F is a **layer** if $G_{F'} \subseteq G_F$.

The prototypical example, and the only one we discuss, is $G = \mathrm{Gal}(\overline{K}/K)$ and $G_F = \mathrm{Gal}(\overline{K}/F)$ for every finite field extension F/K. The layers are then towers of field extensions: $M \supset L \supset K$. There's a bit more structure on the Galois groups than in general formations: Galois theory says that there's a one-to-one correspondence between Galois groups and field extensions, but there need not be a one-to-one correspondence between fixed submodules A_F of A and the subgroups of G. We'll only be worried about the cohomological properties of G and A.

We say that a layer F'/F is normal if $G_{F'} \trianglelefteq G_F$, and we say $G_{F'/F} = G_F/G_{F'}$. We can then talk about $H^i(G_{F'/F}, A_{F'})$ (for convenience we write $H^i(F'/F)$ instead). We say a formation is a **class formation** if $H^1(F'/F) = 0$ for every normal layer, and $H^2(F'/F) \simeq \frac{1}{[G_F : G_{F'}]}\mathbb{Z}/\mathbb{Z}$ with compatible inclusion maps into $\varinjlim H^2(F'/F) \simeq \mathbb{Q}/\mathbb{Z}$ where the limit is over F' with inflations as the connecting maps (which are injective by inflation-restriction and the triviality of the first cohomology groups). This isomorphism we call the invariant map.

The two examples we've seen are $G = \mathrm{Gal}(\overline{K}/K)$ and $A = \overline{K}^\times$ (K local) or $\varinjlim C_L$ (K global). The main reason we study class formations in generality is that Tate's theorem applies exactly to these cases. It gives the reciprocity map as the cup product with the class in $H^2(G_{L/K}, A_L)$ with invariant $\frac{1}{(G_K : G_L)}$. Casting the whole situation in terms of cohomology allows us to also use maps between cohomology groups, restrictions and inflations and corestrictions to get naturality statements between the two. For example, if $L/K/F$ is a chain of normal layers, then the inclusion $G_{L/K} \to G_{L/F}$ and their abelianizations induces the norm map $A_K/N(A_L) \to A_F/N(A_L)$; the transfer map $G^{ab}_{L/F} \to G^{ab}_{L/K}$ induces the inclusion $A_F/N(A_L) \to A_K/N(A_L)$; conjugation of $G_{L/F}$ by τ induces conjugation of $A_F/N(A_L)$ by τ, and the canonical homomorphism $G_{L/F} \to G_{K/F}$ induces the identity map $A_F/N(A_L) \to A_F/N(A_K)$.

The point is that we can do all this without even knowing anything about what these groups are and what the module is. We get an isomorphism from Tate's theorem $H^i(G_{L/K}, \mathbb{Z}) \to H^{i+2}(L/K)$; this means that the cohomology groups $H^j(L/K)$ are completely described by the cohomology of $\mathbb{Z}$; once we have a class formation, the cohomology groups don't really depend on A anymore. We can even get an existence statement like 1.13 if we assume more (including a topology on the layers), but the statement is not general enough to warrant inclusion here. Really, local class field theory and global class field theory are not so different; their difference in difficulty lies in proving that the module and groups are a class formation. From there it's just abstraction.

This information all came from [2] XIV.

5 Applications

5.1 Gauss's three square theorem

We can prove Gauss's classic 3-square theorem, which says that a positive integer is the sum of 3 integer squares if and only if it is not a power of 4 times a number $7 \mod 8$. If we look at the standard Hamiltonian algebra $\mathbb{H} = \mathbb{Q}(i, j, k)$, since

$$(a + bi + cj + dk)^2 = (a^2 - b^2 - c^2 - d^2) + 2a(bi + cj + dk),$$

a rational number is the square of an element in $\mathbb{H}$ if and only if either it is a square of some rational number or it can be written as $-b^2 - c^2 - d^2$. So $\mathbb{Q}(\sqrt{-e})$ splits $\mathbb{H}$ if and only if $\mathbb{Q}(\sqrt{-e})$ can be

embedded into $\mathbb{H}$ if and only if e is the sum of 3 squares. But the invariants of $\mathbb{H}$ are $\frac{1}{2}$ in the $\mathbb{R}$ and $\mathbb{Q}_2$ places, and 0 everywhere else (because in all places except those two, there's a nontrivial solution to $a^2+b^2+c^2+d^2=0$ by Hensel). Then $\mathbb{Q}(\sqrt{-e})$ splits $\mathbb{H}$ iff $e>0$ and $-e$ is not a square in $\mathbb{Q}_2$ by 3.4, 3.6 and 3.7; but the squares of $\mathbb{Q}_2$ are elements $1 \mod 8$ times powers of 4. So $-e$ is not a square if and only if e is not a power of 4 times an element $7 \mod 8$.

So we proved the statement is true for sums of rational squares; that is, if the conditions hold, then a $\sqrt{-e}$ can be found in $\mathbb{H}$. But we want integer squares. Now given $u=\sqrt{-e}$ inside $\mathbb{H}$, by 3.5 there must be a v with $uv=-vu$. We see that v is also the square root of some rational; we can take it to be the square root of an integer. Then the $\mathbb{Z}$-span of $1,u,v,uv$ is a rank-4 integer subring of $\mathbb{H}$, or an order; by looking at volumes of fundamental parallelopipeds and the well ordering principle, we can find a maximal order $\mathcal{O}$ inside $\mathbb{H}$ containing u and v. Let $\mathcal{O}'$ be spanned by $1,i,j,\frac{1+i+j+k}{2}$. It's clear that this is another maximal order. Let $I=\mathcal{O}\cdot\mathcal{O}'$. Then I is a subgroup of $\mathbb{H}$ that absorbs multiplication from $\mathcal{O}$ on the left and $\mathcal{O}'$ on the right; it's a left fractional ideal of $\mathcal{O}$ and a right fractional ideal of $\mathcal{O}'$.

We can prove that $\mathcal{O}'$ has a left division algorithm with the above norm; thus by the usual arguments in the commutative case (which don't need commutativity), all right fractional ideals of $\mathcal{O}'$, including I, are principal. Say $I=\beta\mathcal{O}'$. Then $\mathcal{O}I=I$ so $\mathcal{O}\beta\subseteq\mathcal{O}\beta\mathcal{O}'=\beta\mathcal{O}'$. Then $\mathcal{O}$ is contained in $\beta\mathcal{O}'\beta^{-1}$; since $\mathcal{O}$ is maximal, it must be equal. We know that $\sqrt{-e}$ is in $\mathcal{O}$; thus $\beta^{-1}\sqrt{-e}\beta$ is inside $\mathcal{O}'$, and so there is a square root of $-e$ inside $\mathcal{O}'$ too. By conjugating with some unit among $i,j,k,\frac{\pm1\pm i\pm j\pm k}{2}$ we can show that we are able to make it an integer quaternion instead of just a half-integer quaternion, so there are integers a,b,c with $a^2+b^2+c^2=e$.

(Definitions taken from [4])

5.2 Division algebras containing K

We can continue the statements made in the previous subsection:

Theorem 5.1. *(i) A field K can be embedded in a central division algebra over $\mathbb{Q}$ if and only if, for any $\ell^k|[K:\mathbb{Q}]$, there are two primes p_1 and p_2 of $\mathbb{Q}$ with $\ell^k|[K_v:\mathbb{Q}_{p_i}]$ for all v over p_i, $i=1,2$. (ii) It can be embedded in a specific division algebra D of dimension n^2 over $\mathbb{Q}$ if and only if $[K:\mathbb{Q}]|n$ and $\frac{n[K_v:\mathbb{Q}_p]\operatorname{Inv}_p(D)}{[K:\mathbb{Q}]}$ is an integer for all p and all v over p.*

Proof. We use the diagram below, where as usual $\mathbb{Q}_\infty=\mathbb{R}$:

$$\begin{array}{ccccc} \operatorname{Br}(\mathbb{Q}) & \xrightarrow{\otimes_{\mathbb{Q}}\mathbb{Q}_p} & \operatorname{Br}(\mathbb{Q}_p) & \xrightarrow{\text{Inv}} & \mathbb{Q}/\mathbb{Z} \\ \Big\downarrow{\scriptstyle \otimes_{\mathbb{Q}}K} & & \Big\downarrow{\scriptstyle \otimes_{\mathbb{Q}_p}K_v} & & \Big\downarrow{\scriptstyle \times[K_v:\mathbb{Q}_p]} \\ \operatorname{Br}(K) & \xrightarrow{\otimes_K K_v} & \operatorname{Br}(K_v) & \xrightarrow{\text{Inv}} & \mathbb{Q}/\mathbb{Z} \end{array}$$

(ii)$\Rightarrow$: By 3.4, the centralizer of K in D contains K, so $[K:\mathbb{Q}]^2|[D:\mathbb{Q}]=n^2$ so certainly $[K:\mathbb{Q}]|n$. Extend K to a maximal subfield of D, say L. Then L splits D again by 3.4, so by the diagram, for any prime w of L over any prime v of K over any prime p, $0=\operatorname{Inv}_w(D\otimes L)=[L_w:\mathbb{Q}_p]\cdot\operatorname{Inv}_p(D)$. Then since $\gcd([L_w:K_v]:w|v)$ divides $[L:K]=\sum_{w|v}[L_w:K_v]$, we know that $\gcd([L_w:\mathbb{Q}_p]:w|v)$ divides $[L:K][K_v:\mathbb{Q}_p]$ so $\operatorname{Inv}_p(D)\frac{n[K_v:\mathbb{Q}_p]}{[K:\mathbb{Q}]}\in\mathbb{Z}$ as required.

(ii)$\Leftarrow$: Let v_i be the (finite) set of primes for which $\operatorname{Inv}_{v_i}(D\otimes K)\neq 0$. We can find $x\in K$ such that x is negative in all infinite primes among these, and so that $x\in v_i\backslash v_i^2$ for all finite v_i, by the Chinese Remainder Theorem. If we let $L=K(x^{\frac{[K:\mathbb{Q}]}{n}})$, then there is a single ramified prime w_i over

each v_i by construction, so $[L_{w_i} : K_{v_i}] = [L : K] = \frac{n}{[K:\mathbb{Q}]}$; thus

$$\mathrm{Inv}_{w_i}(D \otimes L) = [L_{w_i} : K_{v_i}] \mathrm{Inv}_{v_i}(D \otimes K) = \frac{n[K_v : \mathbb{Q}] \mathrm{Inv}_p(D)}{[K : \mathbb{Q}]}$$

so that L splits D. Thus L can be embedded in D, so K can too.

(i) follows from (ii), the exact sequence 3.7, and the following lemma.

Lemma 5.2. *A CSA D over $\mathbb{Q}$ is a division algebra if and only if the LCM of the denominators of $\mathrm{Inv}_p(D)$ is equal to $\sqrt{[D : \mathbb{Q}]}$.*

Proof. In one direction, the division algebra D' that D is a matrix algebra of (by 3.2) has the same invariants as D, and any splitting field L of D' has dimension $\sqrt{[D' : \mathbb{Q}]}$. In order for L to split D', any invariant's denominator must divide the gcd of the indices of the local field extensions of L over $\mathbb{Q}$, which divides their sum $[L : \mathbb{Q}]$. So every invariant's denominator, and hence the LCM of all denominators (which, remember, is $\sqrt{[D : \mathbb{Q}]}$), must divide $[L : \mathbb{Q}] = \sqrt{[D' : \mathbb{Q}]}$. Hence $D = D'$.

In the other direction, we can do the same construction as in (ii)$\Leftarrow$: let p_i be all the primes of $\mathbb{Q}$ whose invariants are not 0, and choose some number x divisible by p_i but not p_i^2 (and is negative if the infinite prime invariant is not 0). If the LCM of the denominators of the invariants is k, we just take $L = \mathbb{Q}(\sqrt[k]{x})$; this field splits D by construction and has dimension k. So $\sqrt{[D : \mathbb{Q}]} | k$, and we proved the other divisibility above. □

□

References

[1] Milne, J. (2013). Class Field Theory [PDF]. Retrieved from Mathematics Site- James Milne: http://jmilne.org/math/

[2] Artin, E., & Tate, J. (1968). Class Field Theory. USA: W.A. Benjamin, Inc.

[3] Serre, JP. (1979). Local Fields. New York: Springer-Verlag.

[4] Clark, P. (2005). Lectures on Shimura Curves 9: Quaternion Orders [PDF]. Retrieved from University of Georgia website: http://math.uga.edu/∼pete/

[5] Cassels, J.W.S., & Frohlich, A. (Eds.) (1968). Algebraic Number Theory. Washington, D.C.: Thompson Book Company, Inc.

[6] Roquette, P. (2004). The Brauer-Hasse-Noether theorem in historical perspective [PDF]. Retrieved from the University of Heidelberg Mathematics website: http://www.mathi.uni-heidelberg.de/.