CLASS FIELD THEORY AND THE MKR DICTIONARY FOR KNOTS

THOMAS KOBERDA

Minor Thesis under the supervision of Richard Taylor
May 8, 2008

Contents

1. Introduction

Class field theory can be summarized as the following: "if K is a local or a global field, then the structure of all abelian extensions of K is explicitly determined by the arithmetic inside of K itself." More precisely, class field theory provides canonical "reciprocity isomorphisms" $G(L,K) \to Gal(L/K)$, where $G(L,K)$ is a group that can be determined from K alone but depends on L, and $K \subset L \subset K^{ab} \subset \overline{K}$ is the inclusion of K inside of its maximal abelian extension sitting inside of a fixed algebraic closure of K. Notice that standard Galois theory gives us $Gal(K^{ab}/K) \cong Gal(\overline{K}/K)^{ab}$.

In this exposition we will treat two distinct approaches to class field theory. The first is through algebraic geometry. There, we will consider extensions of function fields as corresponding to branched covers of algebraic curves. We will deduce class field theory through the use of generalized Jacobians. The program of understanding class field theory geometrically was

initiated by Lang and carried out by Serre, and in essence the theory is the same as from the arithmetic point of view.

The second approach is purely algebraic and mostly follows the work of Serre and Tate. We will begin with tools from Galois cohomology, develop the local theory, and then treat the global theory. Global class field theory uses the local theory in a strong way. We will illustrate this by giving a proof of the Kronecker-Weber theorem, which can be viewed as the first instance of global class field theory, that is based on local class field theory. We will go as far as giving as explicit of a description of the reciprocity map as possible, and we will explain some specific examples.

Finally, we will delve into an analogy between number fields and coverings of S^3 branched over links. All links and knots we consider will be assumed to be tame. We will be able to pass between the PL category and the smooth category without loss of generality.

For the sake of brevity, we will only give references for proofs of many of the results contained herein, and occasionally we will paraphrase the main ideas or give sketches of the proofs.

Any mistakes contained herein are my own. I would like to thank Richard Taylor for agreeing to supervise this minor thesis. I would also like to thank Aaron Silberstein, Jack Huizenga, Jay Pottharst and Sam Isaacson for numerous helpful conversations and advice.

2. Some basic facts

First, some terminology: a global field is a number field or a function field of an algebraic curve over a finite field. A local field is a field with a nontrivial valuation with respect to which it is a locally compact topological field, and whose residue field is finite. Let K be a local or global field, and let L/K be a finite Galois extension. Recall that we have well-defined notions $O_K \subset O_L$, and that these rings are Dedekind domains. The norm of a nonzero ideal $a \subset O_K$ is defined to be $[O_K : a]$. There is also a norm map $N_{L/K} : I_L \to I_K$, the the groups of fractional ideals in O_L and O_K respectively, by $N(P) = p^{f_P}$ if P lies over p, and then we extend multiplicatively. Recall that f_P is the residue index (sometimes called the inertial degree of p in P.) If p is a prime in O_K then $pO_L = P_1^{e_1} \cdots P_m^{e_m}$. The e_i are called ramification degrees. When $(O_L/P_i)/(O_K/p)$ is a finite extension of finite fields, its degree is defined to be f_i. If $[L : K] = n$, then $n = \sum e_i f_i$. This last fact holds for any finite extension. In the case that L/K is Galois, then the ramification and residue degrees are all equal.

Let L/K be a finite Galois extension, K a global field, and let v be a nontrivial valuation on L, with L_v the corresponding completion. The Galois group G acts on the set of valuations on L by precomposition. If (x_i) is a Cauchy sequence for v and $g \in G$ then $(g \cdot x_i)$ is a Cauchy sequence for $g \cdot v = v \circ g^{-1}$. By continuity, we get an isomorphism $g_v : L_v \to L_{g \cdot v}$. We will write G_v for the stabilizer of a valuation v. Now let v be a valuation of K. When it makes sense, L^v will denote the completion of L with respect to any valuation lying over v (in the instances we consider, all such fields will be canonically isomorphic,) and G^v will be the corresponding local Galois group.

We will be making heavy use of many standard facts from algebraic number theory and homological algebra. We state some of them for reference.

2.1. **Results from algebraic number theory.**

Proposition 2.1 (Normal Basis Theorem)**.** *Let K/k be a finite Galois extension. Then K is a free $k[G]$-module.*

Proof. This appears as an exercise in [3]. □

Recall the definition of the discriminant and the different of a finite separable field extension: we have a nondegenerate bilinear form $\langle x, y\rangle = Tr(xy)$ defined on L. It is surjective. If A is a Dedekind domain with fraction field K and B is the integral closure of A in L, then B is a lattice in L. Let B^* be the set of all elements of $y \in L$ such that $\langle y, x\rangle \in A$ for all $x \in B$. This is also a lattice in L and is a B-submodule of L. It is called the codifferent of B over A. It is also the largest B-submodule of L whose trace is contained in A. Since $Tr(B) \subset A$, we have $B^* \supset B$. The codifferent is therefore a fractional ideal of L. Its inverse is called the different $D_{B/A}$. This is an ideal of B. The discriminant $d_{B/A}$ is the norm of the different. If $\{e_i\}$ is a free A-basis for B, then the discriminant is equal to

$$\det(Tr(e_i e_j)) = (\det(\sigma(e_i)))^2,$$

as σ varies over embeddings of L into a fixed algebraic closure of K. The proofs of the next two results can be found in [12].

Proposition 2.2 (Ramification criterion)**.** *Let A be a Dedekind domain with field of fractions K. Suppose that L/K is a finite Galois extension, and let B be the integral closure of A in L. Let P be a prime ideal of B lying over $p \subset A$. L/K is ramified at P if and only if P divides the different $D_{B/A}$, if and only if p divides the discriminant $d_{B/A}$.*

Now let K be a local field with residue field k. Let k'/k be a finite separable extension.

Proposition 2.3. *There is a finite unramified extension K'/K that realizes the first extension on residue fields. This extension is unique up to unique isomorphism and is Galois if and only if k'/k is.*

The existence part of the proposition follows essentially from the primitive element theorem.

Corollary 2.4. *There exists a unique maximal unramified extension K_{nr} of K.*

It is obtained by applying the proposition to the separable closure of k.

Proposition 2.5 (Minkowski's discriminant bound)**.** *Let K be a finite, nontrivial extension of $\mathbb{Q}$. Then $|d_{K/\mathbb{Q}}| > 1$. More precisely, if the degree of the extension is n and $2t$ is the number of imaginary embeddings of K in $\mathbb{C}$, then*

$$1 \leq (\frac{4}{\pi})^t \frac{n!}{n^n} |d_{K/\mathbb{Q}}|^{1/2} \leq (\frac{4}{\pi})^n \frac{n!}{n^n} |d_{K/\mathbb{Q}}|^{1/2}$$

Proof. [3], theorem 36. □

2.2. **Results from homological algebra.** Throughout this exposition, we will take the definition of group (co)-homology and basic constructions for granted. Let $H < G$ be a subgroup, and let A be a G-module. We can view A as an H-module. Hence, the inclusion $H \to G$ induces a map $Res : H^n(G, A) \to H^n(H, A)$, called restriction. If H is a normal subgroup of G then we get that A^H is a G/H-module. Thus, we get a map $Inf : H^n(G/H, A^H) \to H^n(G, A)$ called inflation. Now suppose $[G : H] < \infty$. Let $\{s_i\}$ be a set of coset representatives for G/H and let A be an H-module. If $a \in A^H$ then we let $N(a) = \sum s_i a$ (the norm of a.) This is invariant under G action. We hence get a map $Cor : H^0(H, A) \to H^0(G, A)$. It extends to a map on all cohomology groups (cf. [12].) For the definition of Ver, we continue assuming that $[G : H] < \infty$. Ver gives us a map $G^{ab} \to H^{ab}$. Explicitly, let $\theta : G/H \to G$ be a collection of right coset representatives. Let $x_{t,s}$ be defined by $\theta(t)s = x_{t,s}\theta(ts)$. Ver is obtained by looking at $s \mapsto \prod_t x_{t,s}$ and passing to the quotient. This definition comes from the isomorphism $G^{ab} \cong I_G/I_G^2$, $H^{ab} \cong I_H/I_H^2$, and the norm map (acting as Cor on H_0) $I_G/I_G^2 \to I_G/I_G I_H$.

Let H be a normal subgroup of G and let A be a G-module. There is an exact sequence

$$0 \to H^1(G/H, A^H) \to H^1(G, A) \to H^1(H, A),$$

where the second map is inflation and the third is restriction. The exactness can be verified by diagram chasing. More generally, if $H^i(H, A) = 0$ through dimension $n - 1$, then

$$0 \to H^n(G/H, A^H) \to H^n(G, A) \to H^n(H, A)$$

is exact, with inflation and restriction maps in the same places. For a proof, see [12], proposition VII.6.5.

There is a useful way to keep track of some homological and cohomological data for a finite group in one sequence of cohomology groups, called the Tate cohomology groups. In this subsection, G will always denote a finite group.

Define the norm N of G by $\sum_{g \in G} g \in \mathbb{Z}[G]$. By abuse of notation, we use N to also denote the endomorphism of a G-module induced by multiplication by N. It is clear that the augmentation submodule of A, $I_G A$, lies in the kernel of of N and that the image of N lies in A^G for any G-module A. It follows that N induces a map $N^* : H_0(G, A) \to H^0(G, A)$. Let $\widehat{H}_0(G, A) = ker(N^*)$ and $\widehat{H}^0(G, A) = coker(N^*)$. It can be showed that both of these groups vanish for A relatively projective (equivalently relatively injective in the case of a finite group.)

If $0 \to A \to B \to C \to 0$ is a short exact sequence of G modules, we have the standard long exact sequences on homology and cohomology. Multiplication by N gives us maps from the 0-dimensional groups on homology to the 0-dimensional groups on cohomology. The snake lemma gives us a new exact sequence that connects the dimension 1 and higher groups in homology and cohomology by:

$$\widehat{H}_0(G, A) \to \widehat{H}_0(G, B) \to \widehat{H}_0(G, C) \to \widehat{H}^0(G, A) \to \widehat{H}^0(G, B) \to \widehat{H}^0(G, C).$$

This motivates the definition of Tate cohomology groups, $\{\widehat{H}^n(G,A), n \in \mathbb{Z}\}$. They coincide with $H^n(G,A)$ when $n > 0$, $H_{-n-1}(G,A)$ when $-n > 1$, $coker(N^*)$ when $n = 0$ and $ker(N^*)$ when $n = -1$.

The restriction and corestriction maps all work as before, and if $[G : H] = n$, then $Cor \circ Res = n$ as with usual group cohomology. There also exists a uniquely defined cup product

$$\widehat{H}^p(G,A) \otimes \widehat{H}^q(G,B) \to \widehat{H}^{p+q}(G, A \otimes B).$$

These satisfy certain naturality properties. In particular they are natural transformations and bifunctorial in A and B. We will only mention other properties of the cup product when we require them.

In order to do class field theory in the arithmetic case, we will need to know how to actually compute certain cup products. The following lemmas are all taken from [12], appendix after chapter 11.

Lemma 2.6. *Let A and B be G-modules, $\alpha \in A^G$, and $f : \mathbb{Z} \to A$ a G-homomorphism taking $1 \mapsto \alpha$. Suppose $x \in \widehat{H}^n(G,B)$. Then, viewing α as an element of $\widehat{H}^0(G,A)$, the cup product of α and x is equal to the image of x under*

$$f \otimes 1 : B = \mathbb{Z} \otimes B \to A \otimes B.$$

Lemma 2.7. *Let $\alpha \in A$ with $Na = 0$, and let f be a 1-cocycle $G \to B$, which we identify in notation with its cohomology class. Then, viewing α as an element of $\widehat{H}^{-1}(G,A)$, the cup product of α and f is given by the cohomology class of*

$$c = -\sum_{t \in G} ta \otimes f(t).$$

The augmentation homomorphism gives a short exact sequence

$$0 \to I_G \to \mathbb{Z}[G] \to \mathbb{Z} \to 0.$$

If $g \in G$, we may consider $g - 1$, viewed as an element of $\widehat{H}^{-1}(G, I_G)$. The map $d : g \mapsto g - 1$ gives us a canonical isomorphism $G^{ab} \cong \widehat{H}^{-2}(G, \mathbb{Z})$.

Lemma 2.8. *Identify a 1-cocycle f of G in B and an element g of G with their classes in $\widehat{H}^1(G,B)$ and $\widehat{H}^{-2}(G,\mathbb{Z})$. Then, their cup product is given by the cohomology class of $f(s)$ in $\widehat{H}^{-1}(G,B)$.*

Lemma 2.9. *Let u be a 2-cocycle of G in B, identified with its cohomology class. For all $g \in G$, we have that the cup product of u and s is given by*

$$\sum_{t \in G} u(t,s) \in \widehat{H}^0(G,B).$$

The proofs of all these lemmas go along the following lines: choose an exact sequence of G-modules

$$0 \to B \to B' \to B'' \to 0$$

with B' induced. Using the fact that induced modules are cohomologically trivial, we can express one of the relevant factors in the cup product as a coboundary. Applying lemma 2.6 and the definition of the coboundary operator gives the results.

In particular, to do local class field theory, we will need the following result of Nakayama-Tate:

Theorem 2.10. *Let G be a finite group, A a G-module, and α a 2-cohomology class. Let G_p be a Sylow p-subgroup of G, and suppose that $H^1(G_p, A) = 0$ and $H^2(G_p, A)$ is generated by $Res_{G/G_p}(\alpha)$ and has the same order as G_p. Then for any G-module B with $\mathrm{Tor}(A, B) = 0$, the cup product with a_g, the image of a under the restriction map, induces an isomorphism*

$$\widehat{H}^n(H, B) \to \widehat{H}^{n+2}(H, A \otimes B)$$

for all n and all $H < G$.

Proof. [12], IX.8.14. □

When B above is just $\mathbb{Z}$, we get

Corollary 2.11. *The cup product with a_g gives an isomorphism of $\widehat{H}^n(H, \mathbb{Z})$ and $\widehat{H}^{n+2}(H, A)$.*

2.2.1. *Cohomology of cyclic groups.* Consider $G = \langle s \rangle$. In addition to the previously defined N, let $D = s - 1$. We can compute the cohomology of cyclic groups very easily and explicitly. Let $\{C^i\}$ be the complex that is $\mathbb{Z}[G]$ in each dimension, and the boundary maps $C^i \to C^{i+1}$ are given by multiplication by D and N when i is even and odd respectively. Denote by $C(A)$ the complex $\{C^i\} \otimes_{\mathbb{Z}[G]} A$. An exact sequence of G-modules gives rise to an exact sequence of complexes in a way that preserves the direction of the arrows.

Proposition 2.12. *The cohomology functor $H^q(G, A)$ is isomorphic to the cohomology functor of the complex $C(A)$.*

Proof. [12], VIII.4.6. □

In particular, the cohomology of $C(A)$ is independent of the choice of generator s.

Corollary 2.13. *Let G be a cyclic group. Then $\widehat{H}^q(G, A) = ker(D)/Im(N)$ if q is even, and $ker(N)/Im(D)$ if q is odd.*

For the study of class field theory, we will need the notion of a Herbrand quotient. If G is a finite cyclic group, then the previous corollary tells us that the cohomology of G is periodic with period 2. Suppose that both $H^0(G, A)$ and $H^1(G, A)$ have finite order. Then the Herbrand quotient $h(G, A)$ is defined as $|H^0(G, A)|/|H^1(G, A)|$.

The Herbrand quotient has several nice properties. Let

$$0 \to A \to B \to C \to 0$$

be an exact sequence of G-modules. Then the Herbrand quotient is multiplicative. That is, $h(G, B) = h(G, A)h(G, B)$. If $\mathbb{Z}$ is a trivial G-module, then $h(G, \mathbb{Z}) = |G|$. Also, whenever A is a finite G-module, $h(A) = 1$. Indeed, we have the exact sequence

$$0 \to A^G \to A \to A \to A_G \to 0,$$

where the map $A \to A$ is given by multiplication by D. This sequence shows that A^G and A_G have the same number of elements. We also have the exact sequence

$$0 \to H^1(A) \to A_G \to A^G \to H^0(A) \to 0,$$

where the map $A_G \to A^G$ is multiplication by N. This is seen by modifying the grading on the complex used to compute cohomology of cyclic groups (cf. [12], 8.4.) This establishes the claim.

The Herbrand quotient is much like the Euler characteristic. Recall that in any abelian category with have the notion of the Grothendieck group that constructs a universal abelian group $K(D)$ out of any commutative monoid D. Consider the category $AbGrp$ of abelian groups and let A run through all G-modules in $AbGrp$. If we consider the subcategory $FinAbGrp$ of finite abelian groups, and we suppose that $H^0(G, A)$ and $H^1(G, A)$ belong to $FinAbGrp$, then we can set $h(G, A) = H^0(G, A) - H^1(G, A) \in K(FinAbGrp)$. We need to be careful to use isomorphism classes of abelian and finite abelian groups to make sure that these constructions make sense. Indeed, for any $n \in \mathbb{N}$, there are only finitely many isomorphism classes of abelian groups of order n, so that the isomorphism classes of finite abelian groups forms a set. Therefore, we get an honest commutative monoid when we consider isomorphism classes of finite abelian groups under direct sums.

2.3. **Ramification theory and the Artin representation.** In this subsection, K will denote a field that is complete with respect to a discrete valuation v. O_K will be used to denote the valuation ring, and $U_K = O_K - P_K$ will denote the invertible elements. If L/K is a finite separable extension, $O_L \supset O_K$ is the integral closure of O_K in L. O_L is also a discrete valuation ring, and we have w a valuation on L lying over v. We will assume the extension of residue fields to be separable. We will generally assume the extension to be Galois with group G. Under these assumptions, O_L is generated by a single element x as an O_K-algebra (cf. [12], proposition III.6.12.)

Let $g \in G$. It is obvious that g acts trivially on O_L/P_L^{i+1} if and only if $w(g{\cdot}a{-}a) \geq i{+}1$ for all $a \in O_L$ if and only if $w(g{\cdot}x{-}x) \geq i{+}1$. Let G_i denote the normal subgroup of G that consists of elements that act this way. It is called the i^{th} ramification group. Let $i_G(g) = w(g \cdot x - x)$. Then i_G is a class function, $i_G(g) \geq i + 1$ if and only if $g \in G_i$, and $i_G(gh) \geq \inf(i_G(g), i_G(h))$. Furthermore, for any subgroup H, we can consider the fixed field $F = L^H$. It follows that for all $g \in H$, $i_H(g) = i_G(g)$, and that $H_i = H \cap G_i$.

We will see later that the largest unramified subextention K_r of L is the fixed subfield of the inertia group. It follows that the ramification subgroups of G are equal to those of of its inertia group. Thus, it makes sense to talk about the totally ramified extension L/K_r.

We will suppose now that H is a normal subgroup of G, so that we can talk about $G/H = Gal(F/K)$.

Proposition 2.14. *Let $\pi : G \to G/H$ be the canonical projection, and let e denote the ramification index of P_L when L is viewed as an extension of L^H. Then,*

$$i_{G/H}(\gamma) = \frac{1}{e} \sum_{\pi(g)=\gamma} i_G(g).$$

Proof. [12], proposition IV.1.3. □

Now let π denote a uniformizing element for L.

Lemma 2.15. *Let $i \geq 0$. An element $g \in G_0$, the inertia group of G, belongs to G_i if and only if $g \cdot \pi/\pi \equiv 1 \pmod{P_L^i}$.*

Proof. Clearly we can consider only the totally ramified case. It turns out that then π generates A_L as an A_K algebra (cf. [12], I.6.18.) Since $w(\pi) = 1$, it follows that $i_G(g) = 1 + w(g \cdot \pi/\pi - 1)$. □

Now consider $U_L \subset O_L$. We write $U_L^0 = U_L$, and $U_L^i = 1 + P_L^i$. It turns out that these are closed subgroups of U_L which form a base of neighborhoods of 1 in the topology induced by L^*. U_L is closed, so we may write $U_L = \varprojlim U_L/U_L^i$.

Proposition 2.16. *$U_L/U_L^1 = \overline{L}^*$ and for $i \geq 1$, $U_L^i/U_L^{i+1} \cong P_L^i/P_L^{i+1}$. The latter quotients are noncanonically isomorphic to the additive group $\overline{L}$.*

Proof. The first two statements are obvious. The third follows since P_L^i/P_L^{i+1} is a one-dimensional vector space over $\overline{L}$. □

We can describe the quotients U_L^i/U_L^{i+1} more canonically: let $V = P_L/P_L^2$, and consider $V^i := V^{\otimes i}$, the i^{th} tensor algebra. There is a canonical map $V^i \to P_L^i/P_L^{i+1}$ taking $v_1 \otimes \cdots \otimes v_i \mapsto v_1 \cdots v_i$. This is obviously a nonzero map of $\overline{L}$-vector spaces and is a bijection since P_L/P_L^2 is 1-dimensional.

We can easily characterize the successive quotients G_i/G_{i+1}: they are isomorphic to U_L^i/U_L^{i+1} via $g \mapsto g \cdot \pi/\pi$. In particular the inertia group is solvable. Furthermore, the isomorphism is independent of the choice of uniformizing parameter. Denote this isomorphism by θ_i.

Notice that since G_i is normal in G_0, G_0 acts on G_i/G_{i+1} by conjugation. The proof of the following statement is not difficult:

Proposition 2.17. *If $g \in G_0$ and $h \in G_i/G_{i+1}$, then $\theta(ghg^{-1}) = \theta_0(g)^i\theta_i(h)$.*

We will now define a function that will be important in the study of class field theory and describe some of its properties. Let $x \geq -1$ be a real number. By G_x we mean G_i, where i is the smallest integer greater than x. It is clear that $g \in G_x$ if and only if $i_G(g) \geq x + 1$. Define $\varphi(x)$ by

$$\varphi(x) = \int_0^x \frac{dt}{[G_0 : G_t]}.$$

We will call φ is Herbrand function associated to a field extension. When $-1 \leq t \leq 0$, then $[G_0, G_t] = [G_{-1} : G_0]^{-1}$. In particular, if $g_i = |G_i|$ and $k \leq x \leq k + 1$, we have

$$\varphi(x) = \frac{1}{g_0}(\sum_{i=1}^{k} g_i + (x - k)g_{k+1}).$$

Note that φ is continuous, piecewise linear, increasing, concave and satisfies $\varphi(0) = 0$. Furthermore, if φ_l and φ_r denote the left and right derivatives of φ, then if x is not an integer these are both equal to $1/[G_0 : G_x]$. Otherwise, they are $1/[G_0 : G_x]$ and $1/[G_0 : G_{x+1}]$ respectively. φ is easily seen

to be a homeomorphism of $[1,\infty)$ to itself. An interesting property of φ is the following:

Theorem 2.18 (Hasse-Arf)**.** *Let G be an abelian group. If $G_i \neq G_{i+1}$ then $\varphi(i)$ is an integer.*

Proof. [12], V.7. □

Let ψ denote the inverse of φ. Then ψ is continuous, piecewise linear, increasing, convex and satisfies $\psi(0) = 0$. The inverse function theorem shows that the derivatives of ψ are inverses of those of φ. If we write $G^y = G_{\psi(y)}$, then

$$\psi(y) = \int_0^y [G^0 : G^t]\, dt.$$

If H is a normal subgroup of G, it follows that $(G/H)^y = G^y H/H$. Let $K \subset F = L^H$. The fundamental property of φ and ψ that will allow us to justify this claim is the following:

Proposition 2.19 ([12], proposition IV.3.15)**.** *$\varphi_{L/K} = \varphi_{F/K} \circ \varphi_{L/K}$ and $\psi_{L/K} = \psi_{L/F} \circ \psi_{F/K}$.*

The proof of this proposition follows from several lemmas, all of which can be found in [12], IV.3. None of the proofs are difficult. Notice that the properties of φ and ψ mentioned above characterize them. It follows that:

Lemma 2.20.

$$\varphi_{L/K}(x) = \frac{1}{g_0} \sum_{g \in G} \inf(i_G(g), x+1) - 1.$$

Now let $\pi : G \to G/H$ be the canonical projection. Let $b(g) = \sup_{x \in \pi^{-1}(g)} i_G(x)$.

Lemma 2.21. $i_{G/H}(g) - 1 = \varphi_{L/K}(b(g) - 1)$.

Lemma 2.22 (Herbrand's theorem)**.** *Let $y = \varphi_{L/F}(x)$. Then $G_x H/H = (G/H)_y$.*

Indeed, $g \in G_x H/H$ if and only if $b(g) - 1 \geq x$ if and only if $\varphi_{L/F}(b(g) - 1) \geq \varphi_{L/K}(x)$ if and only if $i_{G/H}(g) - 1 \geq \varphi_{L/F}(x)$ if and only if $g \in (G/H)_y$.

Let $e_{F/K}$ and $e_{L/F}$ be the corresponding ramification indices of the tower $K \subset F \subset L$. To see why proposition 2.19 holds, note that if $x \geq -1$ is not an integer, then the derivative of $\varphi_{F/K} \circ \varphi_{L/F}$ can be computed via the chain rule, giving us

$$(|(G/H)_y|/e_{F/K})(|H_x|/e_{L/F}),$$

where $y = \varphi_{L/K}(x)$. It follows from Herbrand's theorem that this is just $|G_x|/e_{L/K} = \varphi'_{L/K}(x)$, giving us the transitivity formula for φ and ψ. Combining proposition 2.19 and Herbrand's theorem justifies the claim.

Now, let $f = [\overline{L} : \overline{K}]$ be the residue degree. Let $a_G(g) = -f \cdot i_G(g)$ for $g \neq 1$ and $f \sum_{g \neq 1} i_G(g)$ for $g = 1$. From the definition of i_G, it follows that a_G is a class function. Since $\sum_{g \in G} a_G(g) = 0$, it follows that the inner product $(a_G, 1_G)$ vanishes. In fact, if χ is any character on G, (φ, a_G) is a nonnegative integer. That is, a_G is a character of an irreducible representation of G, called the Artin representation.

Proposition 2.23. *The character a_G is induced as a function by a_{G_0}.*

This follows easily from the definitions of induction and i_G. For a character χ of G, we write $f(\chi) = (a_G, \chi)$. The prime ideal $P_K^{f(\chi)}$ is called the conductor of χ. When χ has degree one, corresponding to a cyclic extension of K, then the conductor of χ is the conductor of the extension.

Recall that if G is any group, we can consider R_G, the regular representation. The trivial representation occurs with multiplicity one, and we call the representation $R_G - 1_G$ the augmentation representation, denoted U_G. we write u_G for its character. We will write u_i for u_{G_i} and u_i^* for the induced characters of G.

Proposition 2.24.

$$a_G = \sum_{i=1}^{\infty} \frac{1}{[G_0 : G_i]} u_i^*.$$

Proof. [12], proposition VI.2.2. □

3. The perspective of curves

Let X be an algebraic curve over a field k. That is, X is given by a field K of transcendence degree 1 over the base field k. We will generally assume in this section that all curves are nonsingular. Many of the results generalize to the case of singular curves, but we will not give indications as to how this is achieved.

3.1. **Jacobians and their generalizations.** Let X be a projective, nonsingular curve over $\mathbb{C}$ for the moment. Then X is diffeomorphic to a Riemann surface of some genus g. Let $\{\omega_1, \ldots, \omega_g\}$ be a basis for $\Omega^1(X)$, the space of holomorphic differentials on X and let $p \in X$ be a fixed point. Since holomorphic 1-forms are closed, they have well-defined integrals about homology classes in $H_1(X, \mathbb{Z})$. Recall that a functional $\lambda : \Omega^1(X) \to \mathbb{C}$ is called a period if it is given by:

$$\omega \mapsto \int_{[c]} \omega$$

for some homology class $[c]$. Let Λ denote the subgroup of periods in $\Omega^1(X)^*$, and recall that the Jacobian of X is defined by:

$$J(X) = \frac{\Omega^1(X)^*}{\Lambda}.$$

We thus have a canonical map (often called the Abel-Jacobi map in the case of complex curves) $X \to J(X)$ given as follows: for $q \in X$, choose a path $\gamma_q : I \to X$ with $\gamma_q(0) = p$ and $\gamma_q(1) = q$. We then define the canonical map f by:

$$q \mapsto (\int_{\gamma_q} \omega_1, \ldots, \int_{\gamma_q} \omega_g) \pmod{\Lambda}.$$

If X is a complete non-singular curve of genus $g > 0$ over an arbitrary field k, we need to define the Jacobian differently, since integration ceases to make sense. The constructions below will allow us to make precise analogies between class field theory for algebraic curves and global class field theory.

The Jacobian (or more generally, the Albanese variety,) is characterized by its universal property:

Proposition 3.1. *Let X be a smooth projective variety. There exists an abelian variety $Alb(X)$ called the Albanese variety of X and a map $\alpha : X \to Alb(X)$ with the following universal property: if T is a complex torus and $f : X \to T$ is a morphism, then there is a unique map $F : Alb(X) \to T$ such that $f = F \circ \alpha$.*

Proof. We take the proof given in [1], theorem V.13. The proof is done over $\mathbb{C}$, but the result generalizes to other fields. The construction of the Albanese variety exactly parallels that of the Jacobian of a curve.

From Hodge theory we get a map $i : H_1(X, \mathbb{Z}) \to (H^0(X, \Omega^1_X))^*$ defined by $\langle i(\gamma), \omega \rangle = \int_\gamma \omega$, whose image is a lattice by which the quotient is an abelian variety. Let $A = Alb(X)$ be the quotient. For ease of notation we write the image of i as H, and $H^0(X, \Omega^1_X) = \Omega$.

Now let $p \in X$ be a fixed point. For each $x \in X$ we can choose a path c_x from p to x. It is obvious that the form $\omega \mapsto \int_{c_x} \omega$ is a well-defined element of A. Call it $\alpha(x)$.

It is easy to see that α is analytic in the neighborhood of a point $q \in X$. Indeed, let c be a path from p to q and let U be a neighborhood of q that is isomorphic to a ball $B \subset \mathbb{C}^n$. We can identify U and B. For each $x \in U$, we write $\alpha(x) = \alpha(c_x)$, where c_x is the concatenation of the fixed path from p to q with the segment connecting q and x. The map $\alpha : U \to \Omega^*/H$ is evidently analytic.

Now, there is a canonical isomorphism $\delta : \Omega \to H^0(A, \Omega^1_A)$. This is a general fact about complex tori, which we will explain. If V/Γ is a complex torus, then the tangent and cotangent spaces at the origin are canonically identified with V and V^* respectively (similarly for tangent and cotangent sheaves.) The explicit isomorphism $V^* \to H^0(V/\Gamma, \Omega^1_{V/\Gamma})$ is given thus: $x \in V^*$ defines a function that satisfies $x(v+\gamma) = x(v)+C$ for C a constant, $\gamma \in \Gamma$ and for all $v \in V$. Thus, the differential dx will be a global 1-form. This isomorphism is denoted δ.

We will now show that α induces an isomorphism $\alpha^* : H^0(A, \Omega^1_A) \to H^0(X, \Omega^1_X)$. It clearly suffices to show that $\alpha^*(\delta\omega) = \omega$ for $\omega \in \Omega$. This can be seen by computing α^* locally, noting that if $\gamma(x)$ is a local family of paths from p to x, then

$$d(\langle \omega, \gamma(x) \rangle) = d(\int_\gamma \omega) = \omega(x).$$

Now let T be any complex torus and let $f : X \to T$ be any morphism. Suppose that F exists, as in the statement of the proposition. Then, $F^* : H^0(T, \Omega^1_T) \to H^0(A, \Omega^1_A)$ is the induced map. F^* is determined uniquely since α^* is an isomorphism. It follows that F is determined up to a translation. Since we fixed a basepoint, we have uniqueness.

To prove the existence of F, we must use the following fact about complex tori: Let $u : T_1 \to T_2$ be any morphism between complex tori $T_1 = V_1/\Gamma_1$ and $T_2 = V_2/\Gamma_2$. Then u is composed of a translation and a group homomorphism. The group homomorphism, on the other hand, is induced by a linear map $\ell : V_1 \to V_2$ satisfying $\ell(\Gamma_1) \subset \Gamma_2$.

To justify this fact, we note that u induces a map U on the universal covers such that $U(x+\gamma) - U(x) \in \Gamma_2$ for all $\gamma \in \Gamma_1$ and all $x \in V_1$. In particular, the partial derivatives of U are invariant under translation be elements of Γ_1, so they define holomorphic, i.e. constant, functions on T_1. It follows that U is affine.

Returning to the proof, let $T = V/\Gamma$. It clearly suffices to show that u, the composite of δ (for V) and f^*, viewed as a map $V^* \to \Omega$ satisfies ${}^t u(H) \subset \Gamma$.

$$\langle {}^t u(i(\gamma)), v^* \rangle = \langle i(\gamma), u(v^*) \rangle = \int_\gamma f^*(\delta v^*) = \int_{f_*\gamma} \delta v^*.$$

Now let $h : \Gamma \to H_1(T, \mathbb{Z})$ be the canonical isomorphism. Then

$$\int_{f_*\gamma} \delta v^* = \langle h^{-1}(f_*\gamma), v^* \rangle,$$

completing the proof. □

It is possible to use the machinery of complex geometry to prove that the Jacobian of a curve is its Albanese variety (cf. [1], chapter V.) When the base field is not $\mathbb{C}$, one can construct an algebraic group with the same universal property and call it the Jacobian.

Let S be a finite subset of X. To each element P of S we associate a positive integer n_P. We call this data a modulus m of the curve X. When we study the class field theory of a number field, we will have an analogous notion. The modulus can be viewed as a divisor $\sum_S n_P \cdot P$. Let f be a rational function of X satisfying $f \equiv 1 \pmod{m}$, and let $F : X \to G$ be a morphism, where G is an algebraic group. If (f) is the divisor of f, then we can make sense of $F((f))$ by defining the image of a divisor of a point to be its image under F, and then extending by linearity. We will suppose now that F is defined outside of S. We then define $F((f))$ by

$$\sum_{P \in X - S} v_P(f) F(P).$$

We say that m is the modulus of the map F if $F((f)) = 0$ for all rational functions f satisfying $f \equiv 1 \pmod{m}$.

Proposition 3.2 ([11], theorem I.1.1)**.** *For any rational map $F : X \to G$, that is regular outside a finite set S, F has a modulus supported on S.*

Proposition 3.3 ([11], theorem I.1.2)**.** *For any modulus m, there is a commutative algebraic group J_m and a rational map $F_m : X \to J_m$ with the following universal property: for any rational map $F : X \to G$ that admits m as a modulus, there is a unique affine homomorphism $\theta_m : J_m \to G$ such that $F = \theta_m \circ F_m$.*

Given this setup, the Jacobian will be defined much like the idèle class group for a number field. It can also be defined through purely geometric methods. To see how the ideal-theoretic definition is reconciled with the analytic definition, we can give a description of the case of elliptic curves.

Let $L \subset \mathbb{C}$ be a subfield. Let $f(x) = x^3 + ax^2 + bx + c \in L[x]$ be a separable polynomial. Let $g(x, y) = y^2 - f(x)$, and let $E(L)$ be the subvariety

of $\mathbb{P}^2(L)$ defined by g after homogenizing. Let $L(E)$ be the corresponding function field. $E(L)$ can be viewed as a union of finite points and a point at infinity. There is a bijection between points in $E(L)$ and degree one valuations of $L(E)$. A point should be thought of as giving rise to a valuation by associating to a function its order of vanishing at the point. The reverse correspondence is less obvious. Given a degree one valuation v of $L(E)$, let w be the valuation on $L(X)$ lying below v. The theory of valuations on $L(X)$ (cf. [3]) shows that w can be canonically associated a polynomial $(x-p) \in L[x]$. It follows that v is nonnegative on $L[x]$. Writing $X = x_1 + p$, we have

$$y^2 = f(X) = f(x_1 + p) = f(p) + h(x_1)$$

with $h \in x \cdot L[x]$. Combining these observations shows that $y^2 - f(p) \in P_v$, the associated prime ideal. $y^2 \in O_v$, and so $y - q \in P_v$ for some $q \in L$, so that $q^2 - f(p) \in P_v$. We let $v \mapsto (p, q)$ be the reverse correspondence. It is in fact well-defined.

Let $\mathrm{Div}(L(E))$ denote the free abelian group on valuations of $L(E)$. Hence, $\mathrm{Div}(E(L)) \cong I_E \oplus \mathbb{Z}v_\infty$, where I_E is the group of fractional ideals (note that we are considering the integral closure of $L[x]$ inside $L(E)$.) If i is the canonical map $L(E)^* \to \mathrm{Div}(L(E))$, then we form the class group C_E as the quotient.

Let $f : E(L) \to C_E$ be given by $p \mapsto v_p - v_\infty$. Then f is injective (cf. [3], theorem 55) and the image is closed under the group law on C_E. By the universal property of the Jacobian, we have that f is induced as a composition of the canonical map of $E(L)$ into its Jacobian followed by a map F from the Jacobian to C_E. Since f is injective, F must be injective. Since f is regular, it follows that $f(E(L))$ is isomorphic to the Jacobian of $E(L)$. Notice that the image consists precisely of degree zero classes of divisors. This will motivate the general definition of the Jacobian.

The Jacobian can be defined geometrically using symmetric powers. This approach gives a functorial viewpoint. Let $Y = X^g$ denote the g-fold symmetric product of X with itself. It exists. If X is flat over a scheme S then $(X/S)^g$ is also flat over S, and the construction is compatible with base changes. If X/k is a smooth curve then X^g is also smooth (cf. [13].) One can define a rational map $Y \times Y \to Y$ that is a composition law, making Y into a "bi-rational group." One could then use the following general result:

Lemma 3.4. *For any bi-rational group Y defined over a field k, there exists a unique algebraic group G defined over an extension K/k that is K-birationally isomorphic to Y.*

Proof. [16], V.15. □

For more exposition on this approach, see [5], for example.

It is possible to define this group structure in a more functorial manner, and we will choose this approach. Let X/S be a scheme over S. A closed subscheme D is called a relative effective Cartier divisor of X if D is flat over S and its ideal sheaf is an invertible O_X-module. The contravariant functor $\mathrm{Div}^g_{X/S} : (Sch/S) \to (Sets)$ is given by

$$T \mapsto \{\text{relative effective Cartier divisors of degree } g \text{ of } X_T/T\},$$

where $X_T/T = (X/S) \times_S T$. This functor is also compatible with base changes.

Proposition 3.5. *If X is a smooth curve, then $X^g \cong \mathrm{Div}^g_{X/S}$.*

Proof. [13], theorem 4.1. □

Now, let C_m be the group of divisors not supported on S modulo principal ones given by (f) with $f \equiv 1 \pmod m$. Let C_m^0 be the subgroup of C_m consisting of degree 0 classes. If C^0 is the group of classes of degree 0, there is a natural surjective homomorphism $C_m^0 \to C^0$. The kernel L_m of this map consists of principal divisors (f) such that f is invertible at all points of S. For every $P_i \in S$ we can look at invertible elements modulo those congruent to 1 (mod m). These form a commutative algebraic group $R_{m,i}$. Let R_m be the product of these. If G^m denotes the multiplicative group of the field, then $L_m \cong R_m/G^m$. Writing $J = C^0$, we obtain

$$0 \to R_m/G^m \to C_m^0 \to J \to 0.$$

We write $C_m^0 = J_m$ and call this the generalized Jacobian. Notice that in spirit, this is the same object as we constructed for elliptic curves.

If G, G' are connected, commutative algebraic groups and $\theta : G' \to G$ is surjective with finite kernel, we say that θ is an isogeny. If the corresponding field extension is separable, we call θ separable. Let Γ be the kernel of θ. Then $G \cong G'/\Gamma$.

Let $f : U \to G$ be a regular map, with U an algebraic variety. Let U' be the preimage of G' under f, that is to say the fibered product $U \times_G G'$. The projection $U' \to U$ is an unramified cover with Galois group Γ.

Proposition 3.6 ([11], theorem 4)**.** *Every abelian cover of an irreducible algebraic variety is the preimage of an isogeny.*

The idea of the proof is to reduce the problem to Kummer theory and Artin-Schreier theory to write the isogeny as a composition of maps of the form $x \mapsto x^n$ and $x \mapsto x^p - x$.

3.2. **Class field theory.** The results above allow us to derive class field theory for function fields. We will forego the explicit description of reciprocity maps for the sake of brevity. A survey of the results in geometric class field theory can be found in [6].

Let K be a number field and X a complete nonsingular curve defined over K.

Proposition 3.7. *Let $x \in X$ be a K-rational point. There is a maximal abelian unramified covering $\pi : X' \to X$ that is defined over K such that the preimage of x consists of $\deg(X'/X)$ distinct K-rational points.*

In particular this cover is finite.

Proposition 3.8. *The maximal abelian unramified cover of $K(X)$ is given by the composite of the maximal abelian extension K^{ab} of K and the cover asserted above.*

By the previous subsection, abelian covers of X correspond to covers of the Jacobian.

Lemma 3.9. *Let $\theta : G' \to G$ be a separable isogeny, defined over K. Then, the following three conditions are equivalent:*

(1) *The extension $K(G')/K(G)$ defined by θ is Galois.*
(2) *The extension $K(G')/K(G)$ defined by θ is abelian.*
(3) *The kernel of θ is contained in the K-points of G'.*

When these conditions are satisfied, the Galois group of the extension is given by the group of translations $x \mapsto x + a$ as a varies over elements of the kernel.

Proof. [11], proposition VI.6.6. □

If $J' \to J$ is a cover of the Jacobian of a curve X satisfying the conditions of the lemma, we can describe kernels of isogenies via certain subgroups of J. Let $x \in J$ have order n, and suppose it is rational over some finite extension of K. Consider $G = Gal(\overline{K}/K)$. Suppose that the subgroup generated by x is G-isomorphic to μ_n, the group of n^{th} roots of unity. Then, we say that x is a μ-point. x is then rational over $K(\mu_n)$. A subgroup of J is a μ-group if all of its points are μ-points. It turns out that μ-subgroups of J are in bijective correspondence with finite K-rational subgroups of coverings of J.

Proposition 3.10 ([6], theorem 5.3)**.** *The maximal μ-subgroup is finite.*

This result is equivalent to the finiteness of the geometric cover mentioned in proposition 3.7.

3.3. **The Artin representation and algebraic curves.** We follow [12], VI.4. Let k be an algebraically closed field of characteristic p, Y a projective, non-singular, connected algebraic curve over k, and let G be a finite group of automorphisms of Y. Let $\pi(Y) = X = Y/G$, let $L = k(Y)$ and let $K = k(X)$. L/K is a Galois extension with Galois group G. Points on the curves correspond to local rings that are discrete valuation rings, and hence can have valuations assigned canonically. The elements of G that fix a point P form the decomposition group D_P. Let t be a uniformizing parameter at P. For $1 \neq g \in D_P$, we write

$$i_P(g) = v_P(g \cdot t - t).$$

It is not difficult to see that $i_P(g)$ is in fact the multiplicity of $P \times P$ in $\Gamma_g \cap \Delta$, the intersection of the diagonal and the graph of g.

We define a_P as before. Extending it by zero outside of the decomposition group of P, and fixing $Q \in X$, we write

$$a_Q = \sum_{\pi(P)=Q} a_P.$$

It is true that if P lies above Q, then a_Q is induced by a_P, and that a_Q is the character of a representation of G. We call this representation the Artin representation of G at Q.

It is also possible to interpret the Artin representation as a generalization of the Hurwitz formula using ℓ-adic cohomology, but we shall not do this.

4. The perspective of arithmetic

4.1. **Galois cohomology.** Let K/k be a finite Galois extension with Galois group G. We get a canonical G-module structure on the additive group K and on the multiplicative group K^*. It will often be possible to give G-module structures to (possibly nonabelian) groups that are canonically associated to K. The first result in Galois cohomology is the following:

Proposition 4.1. *For all integers n, $\widehat{H}^n(G,K) = 0$.*

The proof of this statement just follows from the normal basis theorem.

Proposition 4.2. $H^1(G,K^*) = 0$.

Proof. [12], X.1.2. □

Corollary 4.3 (Hilbert's Theorem 90)**.** *If $G = \langle s \rangle$ is a cyclic group and $x \in K^*$ with norm 1, then there exists a $y \in K^*$ satisfying $x = y/s(y)$.*

The proof of this statement follows immediately from the determination of the cohomology of a cyclic group along with the cocycle condition.

Similar arguments using noncommutative cohomology show that

$$H^1(G, GL_n(K)) = H^1(G, SL_n(K)) = \{1\}.$$

We will see later that these statements are just generalizations of Hilbert's Theorem 90.

4.1.1. *Cohomology of profinite groups.* This section is taken essentially from [12], X.3. Let K/k be a Galois extension. G is topologized by taking finite index subgroups to be a base of neighborhoods of the identity. G is thus a profinite group and is equal to $\varprojlim Gal(L/k)$, where L varies over all finite subextensions of k in K. If A is a G-module, we call it a topological G-module if $A = \cup A^H$ as H varies over all open normal subgroups of G. Equivalently, for all $a \in A$, $\{g | g \cdot a = a\}$ is an open subgroup of G. We may therefore make sense of the expression $H^n(G/H, A^H)$ for any n. The inflation homomorphisms allow us to then define

$$H^n(G,A) = \varinjlim H^n(G/H, A^H).$$

We will perform some calculations below for $\widehat{\mathbb{Z}}$, the profinite completion of $\mathbb{Z}$. Note that the Chinese remainder theorem shows that $\widehat{\mathbb{Z}} \cong \prod_p \mathbb{Z}_p$, as p ranges over all prime numbers.

4.1.2. *Artin-Schreier and Kummer theory.* First, let k be a field of characteristic p. Consider the isogeny $x \mapsto x^p - x$. We obtain the following short exact sequence:

$$0 \to \mathbb{F}_p \to k \to k \to 0.$$

Let K/k be a finite abelian extension. We obtain the same exact sequence as above with K replacing k. Applying Galois cohomology with coefficients in K we get

$$0 \to \mathbb{F}_p \to k \to k \to Hom(G, \mathbb{F}_p) \to H^1(G,K) = 0.$$

It follows that any continuous homomorphism $G \to \mathbb{F}_p$ is given by $g \cdot a - a$, where a comes from solving the equation $x^p - x - b = 0$. This tells us

that a finite $\mathbb{Z}/p\mathbb{Z}$-extension K is of the form $k[x]/(x^p - x - b)$ for some $b \in k$. Indeed, we see that the minimal polynomial of a over k is given by $(x-a)(x-a-1)\cdots(x-a-p+1)$.

Now suppose k has characteristic zero and contains the n^{th} roots of unity, K a finite abelian extension of k. As before, we get an exact sequence

$$0 \to \mu_n \to K^* \to K^* \to 0,$$

where the third map is given by raising to the n^{th} power. Applying Galois cohomology and Hilbert's Theorem 90, it follows that every element of $\mathrm{Hom}(G, \mu_n)$ is of the form $g \cdot a/a$, where a comes from solving $x^n - b = 0$. This again tells us that finite abelian extensions are given by finite composita of extensions given by adjoining n^{th} roots of elements (n can vary.)

There is an interesting application of Kummer theory to the theory of algebraic curves. Since $\mathbb{C}$ contains all roots of unity, it follows that any abelian cover of a Riemann surface X is given by a compositum of branched cyclic covers.

4.1.3. *Descent.* We summarize a general method that is used to understand when certain objects defined over a field k become isomorphic in a suitable sense when the field is extended to a larger field K. Let V/k be a vector space, and let x be a (p,q)-tensor. We say that $(V,x) \cong (V',x')$ (that is, k-isomorphic,) if there exists a k-linear map $f : V \to V'$ sending x to x'. We extend scalars on V by taking $V_K = V \otimes_k K$. Now, let (V,x) be fixed. Let $E(K/k)$ be the set of k-isomorphism classes of pairs that are K-isomorphic to (V,x). Let A_K denote the group of K-automorphisms of (V_K, x_K). A_K has a noncommutative G-module structure as follows: we have an action on V_K by $g \cdot (v \otimes \lambda) = v \otimes g(\lambda)$. Then, if f is a K-linear map, we write $g \cdot f = g \circ f \circ g^{-1}$.

Now, if $(V',x') \in E(K/k)$ and f witnesses this fact, then

$$p_g = f^{-1} \circ g \cdot f$$

is an element of A_K and in fact represents a 1-cocycle. Changing f changes p_g by a coboundary, so that we obtain a map

$$\theta : E(K/k) \to H^1(G, A_K).$$

Proposition 4.4. *The map θ above is a bijection.*

Proof. [12], X.2.4. □

Descent will allow us to reconcile two definitions of the Brauer group below. It also gives a quick proof of Hilbert's Theorem 90, using the fact that there is only one vector space of dimension n over a field k, up to k-linear isomorphism.

4.1.4. *Brauer groups.* Let K/k be a Galois extension with $Gal(K/k) = G$. By abuse of notation we will write $H^q(K/k)$ for $H^q(G, K^*)$.

Lemma 4.5. *The group $H^q(K/k)$ depends functorially on K/k.*

Proof. Let k' be an extention of k and K'/k' a Galois extension with group G'. Suppose furthermore that there is a k-linear map f from K into K'. We will then get a natural map $f^* : H^q(K/k) \to H^q(K'/k')$ as follows:

let $g' \in G'$. By Galois theory there is a unique element $g \in G$ satisfying $f \circ g = g' \circ f$. Thus, we get a natural homomorphism $G' \to G$, whence the result. □

This map is in fact independent of the choice of f. Indeed, if we choose another such f, then we induce a map on H^q given by an inner automorphism. These act by the identity. In particular, if $k = k'$ and $K \cong K'$, there is a canonical isomorphism $H^q(K/k) \to H^q(K'/k')$. If K is the separable closure of k, we have a well defined notion of $H^q(K_{sep}, k)$. In the case $q = 2$, we write $H^2(k)$ and call this the Brauer group of k.

Recall that the Brauer group of k is classically defined to classify central simple algebras over k. One of the many equivalent definitions of a central simple algebra is that it be isomorphic to a matrix algebra over a division algebra whose center is k. Two such algebras are said to be equivalent if the associated division algebras are k-isomorphic. An equivalent definition of a central simple algebra over k is that there is a finite Galois extension K/k such that B_K is isomorphic to a matrix algebra over K.

Elements of the Brauer group are equivalence classes of central simple algebras over k. There is a group structure on this set, given by the tensor product. It is easy to see that the tensor product of two central simple algebras over k is again a central simple algebra over k, and also that the product is well defined on equivalence classes.

Let B_k denote this group for a field k. If K/k is an extension, we get a map $B_k \to B_K$, and let $B(K/k)$ denote the kernel. It follows from the definition of equivalence that B_k is the union of the $B(K/k)$ as K ranges through finite Galois extensions of k. It suffices to construct isomorphisms $B(K/k) \to H^2(K/k)$ that are compatible with the maps induced by the inclusions $K \to K'$.

Applying descent (where the tensor is of the form $(1, 2)$ that expresses the law of composition,) we obtain that there is a canonical bijection between $B(K/k)$ and $H^1(G, PGL_n(K))$, using the fact that every automorphism of the algebra $M_n(K)$ is inner. From the exact sequence

$$1 \to K^* \to GL_n(K) \to PGL_n(K) \to 1$$

we can extend the exact sequence for nonabelian cohomology to the H^2 term. In particular, if $1 \mapsto A \mapsto B \mapsto C \mapsto 1$ is an exact sequence of nonabelian G-modules, we get an exact sequence of pointed sets as in the long exact sequence for cohomology through the term $H^1(G, C)$. If A is contained in the center of B, we get a map $\Delta : H^1(G, C) \to H^2(G, A)$ that extends the exact sequence. The proof that then $B(K/k) \cong H^2(K/k)$ follows easily from the facts above and can be found in X.5.9 in [12].

We will obtain specific examples of nontrivial Brauer groups below.

4.2. **Local class field theory.** The goal of this subsection is to understand the work that goes into the following result:

Theorem 4.6 (Local class field theory)**.** *Let K be a local field. Then there is a canonical isomorphism $f : \widehat{K^*} \to Gal(K^{ab}/K)$, where $\widehat{K^*}$ denotes the completion of K^* with respect to the norm topology.*

4.2.1. *Brauer groups of local fields.*

Lemma 4.7. *Let K be a local field. Then $H^2(K_{nr}) = 0$, where K_{nr} denotes the unique (up to isomorphism) maximal unramified extension of K.*

Proof. [12], X.7. □

Corollary 4.8. *The Brauer group of K may be identified with $H^2(K_{nr}/K)$.*

Lemma 4.9. *Let L/K be a finite unramified extension and suppose that $G = Gal(L/K)$. There is a split exact sequence*

$$0 \to H^q(\overline{L}/\overline{K}) \to H^q(L/K) \to H^q(G, Z) \to 0$$

for any $q \geq 1$.

Proof. [12], XII.3.4. □

By taking limits, we obtain

$$0 \to H^q(\overline{K}) \to H^q(K_{nr}/K) \to H^q(G, Z) \to 0.$$

Specializing to the case where $q = 2$, we get that the first two groups are Brauer groups. We compute some of the cohomology of G now: note that we have the following exact sequence:

$$0 \to \mathbb{Z} \to \mathbb{Q} \to \mathbb{Q}/\mathbb{Z} \to 0.$$

We have that $\mathbb{Q}$ is cohomologically trivial, so that we have $\mathrm{Hom}(G, \mathbb{Q}/\mathbb{Z}) \cong H^2(G, \mathbb{Z})$. $\mathrm{Hom}(G, \mathbb{Q}/\mathbb{Z})$ is often called $X(G)$, the character group of G and is the Pontryagin dual of G^{ab} (we take the homomorphisms to be continuous.) In the case $G = \widehat{\mathbb{Z}}$, $X(G)$ is identified with $\mathbb{Q}/\mathbb{Z}$. It follows that the Brauer group of a local field is isomorphic to $\mathbb{Q}/\mathbb{Z}$.

4.2.2. *Proving local class field theory.* The basic strategy for establishing the isomorphism $\widehat{K^*} \cong Gal(K^{ab}/K)$ is roughly as follows: we use the theorem of Nakayama-Tate to establish a reciprocity isomorphism between Galois groups of finite abelian extensions and norm subgroups of Galois modules. Passing to the limit, we get the desired result. In this subsection we will tacitly assume all field extensions to be abelian.

If $H < G$ is a subgroup of finite index and A is any G module, then we can define the norm homomorphism as follows, as is done for the corestriction homomorphism in group cohomology. Indeed, let s_i denote a set of coset representatives for G/H. Then we let

$$N_{G/H}(a) = \sum_i s_i \cdot a.$$

In general this is not well-defined, but it is easy to check that this is well-defined as a map from $A^G \to A^H$. For our purposes, A will be a topological G-module for for some Galois group G of some very large extension of a field K. Let $K \subset F \subset L$ be a sequence finite Galois extensions with groups $G_L > G_F$. We denote the corresponding norm homomorphism by $N_{L/F}$. A subgroup of $A_F = A^{G_F}$ is called a norm subgroup if it is the image of a norm homomorphism. To make the notions of norm groups, norm topologies and reciprocity isomorphisms precise, we need the concept of a class formation.

To define a formation, we need to begin with a group G and a family of finite index subgroups, $\{G_i\}_{i\in X}$. This family must be closed under finite intersections, upward closed (i.e. if $H = G_i$ and $H' > H$, then $H = G_j$ for some $j \in X$.) Finally, the family is closed under the conjugation action of G. These conditions are satisfied if G is the Galois group of a Galois field extension and the family is taken to be the Galois groups of all finite subextensions. In the context of formations, we consider only topological G-modules, in the sense that if A is a G-module, then the stabilizer of every element of A is an element of the family. The formation itself consists of G, the family of subgroups, and a topological G-module A. In this context, we write $A_E = H^0(G(F/E), A)$. The meaning of this definition is clear in the case that G is actually a Galois group. Following Serre, elements of X are called fields, and if $G_E > G_F$ in the formation then we say F/E is a Galois extension of fields.

We can define the Tate cohomology groups and we have well-defined notions of inflation, restriction and corestriction.

A class formation consists of a formation and an invariant homomorphism, denoted

$$\mathrm{inv}_E : H^2(F/E) \to \mathbb{Q}/\mathbb{Z}$$

for each Galois extension F/E that satisfying $H^1(F/E) = 0$. Furthermore, inv_E must be injective, map $H^2(F/E)$ onto the unique subgroup of $\mathbb{Q}/\mathbb{Z}$ of order equal to $[F : E]$, and for any extension E'/E, we must have

$$\mathrm{inv}_{E'} \circ Res_{E/E'} = [E' : E] \cdot \mathrm{inv}_E \,.$$

It is not clear a priori that the second cohomology groups should be cyclic, but this follows from the definition of Tate cohomology groups and the Nakayama-Tate theorem.

The invariant behaves nicely under corestriction. Indeed, $\mathrm{inv}_E \circ Cor_{E'/E} = \mathrm{inv}_{E'}$. This follows from the behavior of the invariant under the restriction map and the fact that if $[G : H] = n$, then composing corestriction and restriction is just multiplication by n.

The invariant homomorphism has an explicit definition in the case of a local field K. Let K_{nr} be its maximal unramified extension, and let G denote the Galois group $Gal(K_{nr}/K) = Gal(k_{nr}/k)$, where k denotes the residue field of K.

Recall that we have the following exact sequence in a local field:

$$0 \to B(k) \to B(K) \to X(G) \to 0.$$

Recall also that the Brauer group of a finite field vanishes. Indeed, the groups $H^1(G, k^*)$ and $H^2(G, k^*)$ have the same order since the Herbrand quotient is 1, and the first group vanishes by Hilbert's theorem 90. The last term is identified with $\mathbb{Q}/\mathbb{Z}$, so that we have a map $B(K) \to \mathbb{Q}/\mathbb{Z}$. It is actually an isomorphism, and it is called inv_K. Let α be the canonical isomorphism of $H^2(K_{nr}/K)$ and B_K, and let β be a map $H^2(G, K_{nr}^*) \to H^2(G, \mathbb{Z})$ induced by the valuation map. Let $\delta : H^2(G, \mathbb{Z}) \to H^1(G, \mathbb{Q}/\mathbb{Z})$ be the coboundary induced by $0 \to \mathbb{Z} \to \mathbb{Q} \to \mathbb{Q}/\mathbb{Z} \to 0$. Finally, let $\gamma : H^1(G, \mathbb{Q}/\mathbb{Z}) \to \mathbb{Q}/\mathbb{Z}$ be the evaluation map. Then,

$$\mathrm{inv}_K = \gamma \circ \delta^{-1} \circ \beta \circ \alpha^{-1}.$$

It is not obvious that the valuation map induces an isomorphism. We have an exact sequence of abelian groups

$$0 \to U_K \to K^* \to \mathbb{Z} \to 0$$

for K a local field. The first nonzero term is the group of units and the map $K^* \to \mathbb{Z}$ is the valuation map. Let L/K be a Galois extension with group G, U_L^n be the subgroup of U_l consisting of elements x such that $v(1-x) \geq n$. The claim follows from the following lemma:

Lemma 4.10. *For all $q \geq 1$, we have $H^q(G, U_L^1) = 0$.*

Proof. [12], XII.3.2, XII.3.3. □

The essential point in the proof is that as G-modules, U_L^n/U_L^{n+1} are isomorphic to $\overline{L}$, the additive group of the residue field of L. From the exact sequence

$$0 \to U_L^1 \to U_L \to \overline{L}^* \to 0$$

we obtain that $H^q(G, U_L) \cong H^q(G, \overline{L}^*)$. That β is an isomorphism is now just Hilbert's Theorem 90.

The fundamental property of inv_K is contained in the following result:

Proposition 4.11. *Let L/K be a degree n Galois extension. Then*

$$\mathrm{inv}_L \circ Res_{K/L} = n \cdot \mathrm{inv}_K .$$

Proof. [12], XIII.3.7. □

The class formation we consider for local class field theory is the following: we fix a local field K and a separable closure K_{sep}. X will be the set of finite subextensions of K_{sep} and G will be the Galois group $Gal(K_{sep}/K)$. The invariant homomorphism inv_E will be as defined above. From Hilbert's Theorem 90 and the previous proposition, we see that all the axioms for a class formation are satisfied. If F/E is a Galois extension with group $G_{F/E}$, $E, F \in X$, there exists a unique element

$$u_{F/E} \in H^2(F/E) \text{ satisfying } \mathrm{inv}_E(u_{F/E}) = 1/n.$$

This element is called the fundamental class of the extension. The Nakayama-Tate theorem shows that the cup product with this fundamental class gives an isomorphism

$$\widehat{H}^n(G_{F/E}, \mathbb{Z}) \to \widehat{H}^{n+2}(G_{F/E}, F^*).$$

Specializing to the case where $n = -2$, we get a reciprocity isomorphism

$$\theta_{F/E} : G_{F/E}^{ab} \to E^*/NF^*,$$

where N denotes the norm. In literature, the inverse of $\theta_{F/E}$ is called the reciprocity isomorphism.

To finally establish what we call local class field theory, we have the following:

Proposition 4.12. *For a subgroup of E^* to be a norm subgroup, it is necessary and sufficient for it to be finite index and closed.*

Proof. We need the result of [12], XI.5.2. It is precisely for this result that the norm topology becomes relevant. Three axioms must be verified:

(1) For every extension F/E, where E is a finite extension of K, the map $N_{F/E} : F^* \to E^*$ is proper.
(2) For every prime number p, there is a field E_p with the property that if $E_p \subset E$, then $x \mapsto x^p$ viewed as a map on E^* has a compact kernel and its image contains the group of universal norms. This last object is the intersection of all norm groups.
(3) There exists a compact subgroup U_E of E^* such that every closed subgroup of finite index of E^* that contains U_E is a norm group.

For the class formation considered in local class field theory, these three axioms are verified as follows: Every compact subset of E is contained in a finite number of translates of the group of units in E and $U_F = N_{F/E}^{-1}(U_E)$, verifying the first axiom.

For the second axiom, suppose $p \neq char(K)$. We take E_p to be field obtained by adjoining the p^{th} roots of unity. If $p = char(K)$ then the p^{th} power map has no kernel.

For the last axiom, we let U_E be the group of units in E. Subgroups of finite index of E^* that contain U_E are inverses under discrete valuations of nontrivial subgroups of $\mathbb{Z}$. We then appeal to [12], proposition XIII.5.13. □

4.2.3. *Relationship with classical Artin reciprocity.* We first recall the construction of the Artin symbol. Let L/K be a Galois extension, A a Dedekind domain with fraction field K and B the integral closure of A in L. Let P be a prime ideal of B lying over a prime ideal p of A. Suppose that the extension is unramified at P and that A/p has order q. The decomposition group at P can be identified with the Galois group of $\overline{L}/\overline{K}$, the corresponding extension of residue fields. This group is cyclic, as it is the Galois group of a finite extension of finite fields. The Frobenius element $x \mapsto x^q$ is a generator of this group, and its order if f_P, and it is denoted $(P, L/K)$. An elementary property of this element is that if $g \in Gal(L/K)$, $(g \cdot P, L/K) = g \cdot (P, L/K) \cdot g^{-1}$. If L/K is an abelian extension then $(P, L/K)$ depends only on the prime over which P lies, so we have a well-defined Artin symbol $(p, L/K)$. By linearity one defines $(a, L/K)$ for any ideal $a \subset A$ that does not contain a ramified prime.

Now, let K be a local field and L a Galois extension with group G. For $a \in K^*$, we will write $(a, L/K)$ for the image of a under the composition $a \mapsto \overline{a} \in K^*/NL^* = \widehat{H}(G, L^*)$ followed by $\omega = \theta_{L/K}^{-1}$. It is possible to understand $(a, L/K)$ using characters.

Let χ be a degree 1 character of G, so that $\chi \in \mathrm{Hom}(G, \mathbb{Q}/\mathbb{Z})$, and let $\delta\chi \in H^2(G, \mathbb{Z})$ be the image of χ under the coboundary $\delta : H^1(G, \mathbb{Q}/\mathbb{Z}) \to H^2(G, \mathbb{Z})$.

Proposition 4.13. *$\chi(a, L/K) = \mathrm{inv}_K(\overline{a} \cdot \delta\chi)$, where on the right hand side, the multiplication is the cup product.*

Proof. [9], 2.3.1. □

We can thus obtain a connection between the Artin symbol and the local reciprocity map:

Proposition 4.14. *Let L/K be an unramified extension of fields of degree n. Let $F \in G_{l/K}$ denote the Frobenius element, $a \in K^*$ and $v(a)$ its valuation in L. Then $(a, L/K) = F^{v(a)}$.*

Proof. [9], 2.5.2. □

The Artin symbol can sometimes be computed explicitly. The actual proofs can be given via Lubin-Tate theory. For the moment, consider $\mathbb{Q}_p$. The maximal abelian extension K of $\mathbb{Q}_p$ is generated by all roots of unity. It can be viewed as a compositum of two linearly disjoint subfields: $\mathbb{Q}_{nr}$, generated by roots of unity that are relatively prime to p, and $\mathbb{Q}_{p^\infty}$, the subfield generated by p-power roots. By general theory, the Galois group $Gal(\mathbb{Q}_{nr}/\mathbb{Q}_p) \cong \widehat{\mathbb{Z}}$. It turns out that the group of p^{th} roots of unity has an automorphism group isomorphic to the units in $\mathbb{Z}_p$ (cf. [9].)

Proposition 4.15. *If $a = p^n \cdot u \in \mathbb{Q}_p$, then $(a, K/\mathbb{Q}_p) = \sigma_a$ induced the n^{th} power of the Frobenius automorphism on $\mathbb{Q}_{nr}$ and induces the automorphism given by u^{-1} on $\mathbb{Q}_{p^\infty}$, under the identification above.*

Proof. [9], 3.1.2. □

For the general case, let K be a local field with π a uniformizing element. The maximal abelian extension L/K can be decomposed as the compositum of two subfields, $L = K_\pi K_{nr}$ in such a way that elements $a = \pi^n \cdot u$ correspond Galois automorphisms of these subfields, much in the same way as in the case of $\mathbb{Q}_p$.

These fields can be understood using formal group laws. These are defined as follows: let A be a commutative ring (always with identity,) and let $F \in A[[X, Y]]$. F is called a commutative formal group law if $F(X, F(Y, Z)) = F(F(X, Y), Z)$, $F(0, Y) = Y$, $F(X, 0) = X$, there exists a unique $G(X)$ such that $F(X, G(X)) = 0$, $F(X, Y) = F(Y, X)$, and $F(X, Y) \equiv X + Y \pmod{\deg 2}$. For our purposes we consider the case when $A = O_K$ for K a local field. Let $m_K \subset O_K$ be the maximal ideal. Two elements of m_K can be composed according to a commutative formal group law F, and this sum converges and gives rise to a group structure (cf. [9], 3.2.) This group will be called $F(m_K)$. For L/K a finite extension, one can similarly define $F(m_L)$, and in the general case one passes to the direct limit of the finite cases. Serre notes that the finite order elements of $F(m_{K_{sep}})$ are a torsion group on which the Galois group $Gal(K_{sep}/K)$ acts, and that the Galois module structure is poorly understood. This problem appears analogous to the fundamental problem in arithmetic topology (cf. [4].)

Let K be as above and let $q = |k|$. Denote by F_π the set of formal power series f satisfying $f(X) \equiv \pi X \pmod{\deg 2}$ and $f(X) \equiv X^q \pmod{\pi}$. The proofs of the following statements are in [9], 3.3 and 3.4.

Proposition 4.16. *If $f \in F_\pi$, then there is a unique formal group law F_f for which f is a abelian group endomorphism. Furthermore, for any $a \in O_K$, there is a unique $[a]_f \in O_K[[X]]$ such that $[a]_f$ commutes with f and is congruent to $aX \pmod{\deg 2}$. Then, $[a]_f$ will be an endomorphism of the group defined by F_f. The map $a \mapsto [a]_f$ is an injective homomorphism $O_K \to End(F_f)$. Finally, for any $f, g \in F_\pi$, the resulting group laws are isomorphic.*

Now let K_{sep}/K be a separable closure of K and F_f as above. Let $M_f = F_f(m_{K_{sep}})$ and let E_f be the torsion submodule of M_f. Then, the field K_π mentioned above is defined to be $K(E_f)$. Now, if $u \in K^*$ is a unit, then $[u]_f$ acts on the torsion submodule of M_f. Write $a = \pi^n \cdot u \in K^*$. Then $a \mapsto (a, K^{ab}/K)$ is given by the action by $[u^{-1}]_f$ on K_π/K and the Frobenius on K_{nr}/K (recall that K_{nr} is obtained by a correspondence between unramified extensions of K and separable extensions of k.)

The claim that the maximal abelian extension of K is in fact equal to the compositum of K_π and K_{nr} is a highly nontrivial statement. A proof can be found in [8] or in [9].

4.2.4. *Conductors and the Artin representation.* Let L/K be a finite extension with $\theta_{L/K} : K^* \to Gal(L/K)$ the associated reciprocity map. There is a smallest number n such that $\theta_{L/K}(U_K^n) = 0$, called the conductor of L/K and denoted $f(L/K)$. Let φ be the associated Herbrand function.

Proposition 4.17. *Let n be the largest integer such that the ramification group G_n is nontrivial. Then $f(L/K) = \varphi(n) + 1$.*

Proof. This follows from the following result, whose proof can be found in [9], section 4: if L/K is an abelian extension with group G, then the local reciprocity map θ maps U_K^y onto G^y for all $y \geq 0$. □

Let L/K be an arbitrary Galois extension with group G, and let $\chi : G \to \mathbb{C}^*$ be a one-dimensional character of G. Let L^χ be the fixed field of $ker(\chi)$. This field is evidently a cyclic extension of K, and its conductor is denoted $f(\chi)$, called the conductor of χ.

Proposition 4.18. *If $\{G_i\}$ denote the ramification subgroups of G and if $g_i = |G_i|$, then*

$$\sum_{i=1}^{\infty} \frac{g_i}{g_0}(1 - \frac{1}{g_i}\sum_{g \in G_i} \chi(g)).$$

Proof. Note that

$$(\chi, u_i^*) = (\chi(1) - \frac{1}{G_i}\sum_{g \in G_i} \chi(g)),$$

where the u_i are the augmentation characters of G_i. The claim now follows from proposition 2.24. □

Finally, let $K \subset F \subset L$ be a tower of Galois extensions, $G = Gal(L/K$ and $H = Gal(L/F)$.

Proposition 4.19. *If χ is a character of H and χ^* is the induced character on G, then*

$$f(\chi^*) = v_K(d_{F/K})\chi(1) + f_{F/K}f(\chi),$$

where $d_{F/K}$ is the discriminant and $f_{F/K}$ is the residue index.

Proof. [12], VI.2. □

4.3. **Global class field theory.**

4.3.1. *The Kronecker-Weber theorem and the Hilbert class field.* The following result can be viewed as the first instance of global class field theory.

Theorem 4.20 (Kronecker-Weber)**.** *Let $K/\mathbb{Q}$ be a finite abelian extension. Then K is contained in a cyclotomic extension of $\mathbb{Q}$.*

For a local field K, the statement $K^{ab} = K_\pi K_{nr}$ is sometimes called the local Kronecker-Weber theorem (cf. [8] or [9].) A corollary is that every finite abelian extension of $\mathbb{Q}_p$ sits inside of a cyclotomic extension ([8], corollary 4.12.)

We follow [8] to give a proof of the Kronecker-Weber theorem.

Lemma 4.21. *If K is a finite Galois extension of $\mathbb{Q}$ with group G. Then G is generated by the inertia groups of ramified primes in the extension.*

Proof. Let $H \leq G$ be a subgroup generated by these inertia groups and let L be the fixed field of H. General theory shows that the fixed field for any inertia group of a prime ideal is unramified at that prime. It follows that L is unramified. Minkowski's discriminant bound shows that a finite unramified extension of $\mathbb{Q}$ is $\mathbb{Q}$ itself. □

Proof of the Kronecker-Weber theorem. Suppose $K/\mathbb{Q}$ is a finite abelian extension. Let p be a prime number and P a prime lying over p. We can localize at P to look at the finite abelian extension $K_P/\mathbb{Q}_p$. By the local Kronecker-Weber theorem applied to $\mathbb{Q}_p$, we have that $K_P \subset \mathbb{Q}_p(u, v)$, where $u \in \mathbb{Q}_{nr}$ and $v \in \mathbb{Q}_{p^\infty}$, as above. So, we may assume v is a p^s root of unity, and the transitivity of the Galois group action on primes lying over p shows that s is independent of P.

Let L be the cyclotomic extension of $\mathbb{Q}$ generated by the p^{s_p} roots of unity for primes ramified in K, and denote by F the compositum of L and K. Galois theory shows that F is a finite abelian extension of $\mathbb{Q}$. It suffices to prove the result for F, so we may assume $L \subset K$. We have

$$[K : \mathbb{Q}] \geq [L : \mathbb{Q}] = \prod_p \varphi(p^{s_p}),$$

where the product is taken over ramified primes and φ is the totient function, since a prime q is ramified in $\mathbb{Q}(\zeta_m)$ if and only if $q|m$.

On the other hand, inertia groups can be computed locally, so it follows that the inertia group I_p of a prime p has order $\leq \varphi(p^{s_p})$. By the lemma, using the fact that G is abelian,

$$|G| \leq \prod_p |I_p| \leq \prod_p \varphi(p^{s_p}).$$

It follows that $[K : \mathbb{Q}] = [L : \mathbb{Q}]$, so that $L = K$. □

Now let K be a given number field. The field L in the following result is called the Hilbert class field.

Theorem 4.22. *There exists a finite Galois extension L of K such that L is an unramified, abelian extension of K and any other unramified abelian extension of K is contained in L.*

Proof. [2], theorem 8.10. □

Note that by Minkowski's discriminant bound, $L = \mathbb{Q}$ when $K = \mathbb{Q}$. Recall that if L/K is a Galois extension and $p \subset O_K$ is an unramified prime, then we can uniquely define the Frobenius element and hence the Artin symbol. In the case where L in an unramified extension, we have an Artin symbol defined for all ideals in O_K.

Theorem 4.23 (Artin reciprocity for the Hilbert class field)**.** *If L/K is the Hilbert class field, then the Artin map*

$$(L/K, \cdot) : I_K \to Gal(L/K)$$

is surjective, and is an isomorphism upon passage to the class group of K.

Proof. [2], section 8. □

Corollary 4.24 (Class field theory for unramified abelian extensions)**.** *The Artin map is natural in the following sense: let M/K be an unramified abelian extension. Then there is a unique subgroup $H < C_K$ such that*

$$(L/K, \cdot) : C_K/H \to Gal(M/K)$$

is an isomorphism. Furthermore, there is a bijective correspondence between unramified abelian extensions of K and subgroups of C_K.

4.3.2. *The general theory.* Throughout the rest of this section, K will mean a number field unless otherwise noted. Most of the results contained herein also hold for function fields over a finite field. In a number field K, a prime is an equivalence class of nontrivial valuations. These valuations can be either discrete or archimedean. They are sometimes called finite primes and infinite primes, respectively. Finite primes can be identified with prime ideals in the ring of integers O_K. Infinite primes come in real and complex varieties. They can be identified with embeddings of K in $\mathbb{R}$ and pairs of conjugate embeddings of K in $\mathbb{C}$, respectively.

Let K be fixed, O_K the ring of integers and U_K the units in that ring. We denote by I the group of fractional ideals in K. If S is a finite set of primes, we write I^S for the subgroup generated by prime ideals not contained in S, so that I^S can be viewed as a free abelian group on prime ideals not contained in S. Similarly we define $K^S = \{a \in K^* | (a) \in I^S\}$. We can relate K^S and I^S to the standard ideal class group C_K via the following exact sequence:

$$0 \to U_K \to K^S \to I^S \to C_K \to 0.$$

The only point to be checked is the surjectivity of the last map. The point is that for any finite prime p in S, we can choose $c_p \in p/p^2$, and for any sequence of nonnegative integers $\{n_p\}_{p \in S}$, we can find an algebraic integer a satisfying

$$a \equiv c_p^{n_p} \pmod{p}.$$

This last step requires the Chinese remainder theorem.

We also have the notion of a modulus of K, which is a function m from the set of primes in K to nonnegative integers. A modulus is zero for almost every prime, assigns zero to every complex prime, and assigns either zero or one to each real prime. Note that the modulus defined here is exactly

analogous to the modulus for function fields over an algebraic curve (cf. [11].) We can write

$$m = \prod_p p^{m(p)}.$$

The support of a modulus is denoted $S(m)$.

Moduli also give rise to the concept of the Ray class group C_m (cf. [8].) Fixing a modulus m, we let $K_{m,1}$ be the set of units a in K that satisfy $\mathrm{ord}_p(a-1) \geq m(p)$ for all finite primes dividing m, and a_p is positive for all real primes dividing m. We map $K_{m,1}$ to I^{S_m} by associating an element the principal ideal it generates. We call the image $i(K_{m,1})$. C_m is defined as $I^{S(m)}/i(K_{m,1})$.

Let L/K be an abelian extension and let m be a modulus divisible by all primes in K that ramify in L. If p is a prime not dividing m, then the Artin symbol $(L/K, p)$ is defined. We can thus define the Artin map

$$(L/K, \cdot) : I^{S(m)} \to Gal(L/K).$$

Theorem 4.25 (Class field theory for number fields, cf. [2], theorem 8.2)**.** *Let L/K be an abelian extension, and let m be a modulus divisible by all primes of K that ramify in L. Then, the Artin map is surjective. If the exponents of finite primes dividing m are sufficiently large, then $Gal(L/K) \cong C_m$ under the Artin map.*

In particular, a number field with trivial class group has no unramified abelian extensions. Unfortunately, there is no unique modulus for which $Gal(L/K) \cong C_m$. We do have the following (cf. [2], theorem 8.5:)

Proposition 4.26. *If L/K is an abelian extension, there is a modulus $f = f(L/K)$ such that a prime of K divides f if and only if it ramifies in L, and $C_m \cong Gal(L/K)$ if and only if $f|m$.*

The modulus of the previous proposition is called the conductor of the extension L/K. In general, if L/K s a finite extension of number fields, $G = Gal(L/K)$ is the Galois group and χ is any one-dimensional character of G, we define the conductor $f(\chi)$ analogously to the local case. Let P/p be a pair of primes, $P \subset L$ lying over $p \subset K$, and let D_p be the corresponding decomposition group. We can restrict χ to D_p, and we call the resulting local conductor $f(\chi, p)$. Note that it vanishes when p is unramified. We define the global conductor $f(\chi)$ by:

$$f(\chi) = \prod_p p^{f(\chi,p)}.$$

We have an analogy to proposition 4.19:

Proposition 4.27 ([9], proposition 4.4.5)**.** *Let $K \subset F \subset L$ be a tower of extensions, $H = Gal(L/F)$. If χ is a character of H, let χ^* be the induced character of G. Then,*

$$f(\chi^*) = d_{F/K}^{\chi(1)} N_{F/K} f(\chi).$$

Returning to Artin reciprocity,

Proposition 4.28. *Let $M, L/K$ be two abelian extensions. Let $\Phi_{M,m}$ and $\Phi_{L,m}$ denote the respective Artin maps. Then $L \subset M$ if and only if there exists a modulus m, divisible by all the primes in K that ramify in L or M such that $i(K_{m,1}) \subset ker(\Phi_{M,m}) \subset ker(\Phi_{L,m})$.*

We can use this result to provide a second proof of the Kronecker-Weber theorem. If L/K is an abelian extension, m is a modulus for which the Artin map Φ_m is defined, and $m|n$, then $i(K_{m,1}) \subset ker(\Phi_m)$ implies $i(K_{n,1}) \subset ker(\Phi_n)$.

Second proof of the Kronecker-Weber theorem. If $L/\mathbb{Q}$ is an abelian extension, let m be a modulus that gives the Artin reciprocity isomorphism. By the above observation, we can assume $m = n\infty$, where n is a sufficiently high power of the product of all finite primes that ramify in L and ∞ is the unique infinite prime of $\mathbb{Q}$.

We can explicitly describe the Artin map for this modulus:

$$\Phi_m : I_{\mathbb{Q}}(m) \to Gal(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^*$$

is given by

$$\frac{a}{b}\mathbb{Z} \mapsto [ab^{-1}] \in (\mathbb{Z}/n\mathbb{Z})^*,$$

with both a and b relatively prime to n. It is clear that the kernel of this map is precisely $i(\mathbb{Q}_{m,1})$. So, we have

$$\mathbb{Q}_{m,1} = ker(\Phi_{\mathbb{Q}(\zeta_n)/\mathbb{Q},m}) \subset ker(\Phi_{L/\mathbb{Q}}).$$

It follows that $L \subset \mathbb{Q}(\zeta_n)$. □

We also consider L-series in order to get more information about the Artin map. If m is an integer, a homomorphism $\chi : (\mathbb{Z}/m\mathbb{Z})^* \to S^1 \subset \mathbb{C}^*$ is called a Dirichlet character. This can be extended to all of $\mathbb{Z}$ by zero if $\gcd(m, n) \neq 0$. The Dirichlet L-series is defined to be

$$L(s, \chi) = \sum_{n>0} \chi(n)/n^s = \prod_{\gcd(p,m)=1} \frac{1}{1 - \chi(p)p^{-s}}.$$

Note that $L(\chi_0, s)$ is the classical Riemann zeta function, and it extends to a meromorphic function on the half plane $Re(s) > 0$ and is given by

$$\zeta(s) = \frac{1}{s-1} + \phi(s),$$

where ϕ is holomorphic on the half plane. Applying a logarithm, we obtain

$$\sum \frac{1}{p^s} \sim \log \frac{1}{1-s}$$

as $s \to 1$ from the right on the positive real axis. The analytic density d of a set of primes T is defined by

$$\sum_{p \in T} \frac{1}{p^s} \sim d \log \frac{1}{1-s}$$

as $s \to 1$ as above. In a general number field, the Dirichlet density of T is

$$\lim_{s \to 1^+} \frac{\sum_{p \in S} N(p)^{-s}}{-\log(s-1)}.$$

Let

$$f_\chi(s) = \sum_{\gcd(p,m)=1} \chi(p)/p^s.$$

A result in [10] shows that if $\gcd(p, a) = 1$, then

$$\sum_{p \equiv a \pmod m} 1/p^s = \frac{1}{\varphi(m)} \sum_\chi \chi(a)^{-1} f_\chi(s),$$

where the sum on the right is taken over all Dirichlet characters $\pmod m$. Using the fact that if $\chi \neq \chi_0$ implies $f_\chi(s)$ remains bounded near $s = 1$ (cf. [10],) we see that the Dirichlet density of primes congruent to $a \pmod m$ is $1/\varphi(m)$. It follows that the set of primes splitting in the cyclotomic field $\mathbb{Q}(\zeta_m)$ has Dirichlet density $1/\varphi(m)$. There is a more general result for number fields, known as the Tchebotarev Density Theorem:

Proposition 4.29. *Let L/K be Galois and let σ denote a conjugacy class in $Gal(L/K)$. Let S be the set of primes in K that are unramified in L and whose Artin symbol lies in σ (recall that the Galois group acts transitively on primes P in L lying over ones in L and for an unramified prime p in K, the Artin symbols of primes lying over p are all conjugate.) The Dirichlet density of S is*

$$\frac{|\sigma|}{[L : K]}.$$

This implies that the Artin map for a finite extension has infinite fibers.

The results of class field theory can be restated in a different language, i.e. that of idèles. A good reference for this approach is [15]. We sketch this approach here. Let p be a prime of K. We can complete K with respect to this prime to get a field K_p. The idèle group I_K of K is a subset of the product $\prod_p K_p^*$ that consists of those elements whose entries lie in the group of units U_{K_p} for all but finitely many p. Replacing U_{K_p} by O_{K_p} in the definition of I_K gives the ring of adèles, A_K. For example, the idèle group $I_\mathbb{Q}$ is isomorphic to $\mathbb{Q}^* \times \mathbb{R}_+^* \times \prod_p U_p$. Indeed, given a tuple $x = (x_\infty, x_2, x_3, x_5, \ldots)$, we can write

$$x = a(t, u_2, u_3, u_5, \ldots),$$

where $t > 0$ and

$$a = sgn(x_\infty) \prod_p p^{v_p(x)}.$$

There is a canonical map $K^* \to I_K$, where an element $a \in K^*$ is taken to its image in the completion at each prime. For every prime p of K, there is a map $i_p : K^* \to I_K$. The image $i_p(a)$ is the element whose p^{th} entry is a and all other entries are 1. There is a map $j_p : I_K \to K^*$ that is just projection at the p^{th} coordinate.

It turns out that I_K is a locally compact group, and that the image of K^* under the canonical map is discrete. The quotient C_K is called the idèle class group. Note that this construction is exactly the same as the Jacobian for an algebraic curve: it has the same universal property (cf. [15], proposition 4.1.) The example above shows that the idèle class group $C_\mathbb{Q}$ is $\mathbb{R}_+^* \times \prod_p U_p$.

The Artin reciprocity theorem can be restated in this language as follows:

Theorem 4.30. *Let L/K be an abelian extension. Then there is an Artin map*

$$\Phi_{L/K} : C_K \to Gal(L/K)$$

that is surjective and continuous. The subgroups of finite index in C_K are precisely norm subgroups, i.e. images of norm maps $N_{L/K} : C_L \to C_K$ for finite extensions L/K.

In view of the example above, we have that $\prod_p U_p$ is a Galois group of some algebraic extension of $\mathbb{Q}$. It is in fact the Galois group of the maximal cyclotomic extension of $\mathbb{Q}$.

4.3.3. *Galois cohomology of idèles.* If L/K is an arbitrary finite Galois extension with Galois group G, we obtain A_L from A_K by extension of scalars, i.e. $A_L = A_K \otimes_K L$. There is a canonical G-module structure on A_L and I_L given by $g \mapsto 1 \otimes g$. We get another action of G on I_L however: recall that elements $g \in G$ induce isomorphisms $g_v : L_v \to L_{g\cdot v}$. Thus, if $x = (x_v) \in I_L$, we write $g \cdot x = ((g \cdot x)_{g\cdot v})$. In this way we get $i_{g\cdot v} \circ g_v = g \circ i_v$ and $g_v \circ j_v = j_{g\cdot v} \circ g$. The image of L_v^* in I_L under i_v is not G-invariant. In fact, the smallest G-invariant subgroup containing $i_v(L_v^*)$ is $\prod_{v/w} L_v^*$, where this product is taken over primes lying over w.

Proposition 4.31. *Let v_0 be a fixed prime over w. For any r, there are natural isomorphisms*

$$H^r(G, \prod_{v/w} L_v^*) \to H^r(G_{v_0}, L_{v_0}^*)$$

and

$$H^r(G, \prod_{v/w} U_v^*) \to H^r(G_{v_0}, U_{v_0}^*).$$

These assertions are valid when regular cohomology is replaced by Tate cohomology.

Proof. This follows from Shapiro's lemma: let G be a group, H a subgroup, and B an H-module. Let $B^* = \mathrm{Hom}_{\mathbb{Z}[H]}(\mathbb{Z}[G], B)$. B^* is a G-module via the action $s\varphi(g) = \varphi(gs)$. Let $\theta : B^* \to B$ be given by $\theta(\varphi) = \varphi(1)$. Then we get an associated homomorphism $H^q(G, B^*) \to H^q(H, B)$. This is in fact an isomorphism. See [15], proposition 7.2. □

The next five results can be found, with proof, in [15], sections 7, 8 and 9.

Proposition 4.32. *$I_K = I_L^G$, the group of G-invariant idèles of L. Furthermore,*

$$\widehat{H}^r(G, I_L) \cong \bigoplus_v \widehat{H}^r(G^v, (L^v)^*),$$

where the direct sum is taken over all primes in K.

Corollary 4.33. *$H^1(G, I_L) = 0$ and*

$$H^2(G, I_L) = \bigoplus_v (\frac{1}{n_v}\mathbb{Z}/\mathbb{Z}),$$

where $n_v = [L^v : K_v]$.

The first statement is Hilbert's Theorem 90, and the second follows from the axioms for inv_K.

Proposition 4.34. *$C_K \cong C_L^G$, where the action on C_L comes from passing to the quotient.*

Proposition 4.35. *If L/K is a cyclic extension of degree n, then the Herbrand quotient $h(G, C_L) = n$.*

Proposition 4.36. *Let L/K be a Galois extension of degree n with group G, then $|\widehat{H}^0(G, C_L)|$ and $|\widehat{H}^2(G, C_L)|$ divide n, and $\widehat{H}^1(G, C_L) = 0$.*

This last result has a nice interpretation in terms of central simple algebras. Indeed, let L/K be any finite Galois extension. $H^1(G, C_L) = 0$ so that from the exact sequence

$$0 \to L^* \to I_L \to C_L \to 0$$

we get another short exact sequence

$$0 \to H^2(G, L^*) \to H^2(G, I_L).$$

On the other hand,

$$H^2(G, I_L) \cong \bigoplus_v H^2(G^v, (L^v)^*),$$

by proposition 4.32. It turns out that the image of the injection consists of elements, the sum of whose local invariants is zero. It follows that:

Proposition 4.37. *S central simple algebra over K splits over K if and only if it splits locally everywhere.*

This is called the Brauer-Hasse-Noether theorem.

The local invariants of a global field deserve a more precise treatment. For ease of notation we will write $H^2(L/K)$ for $H^2(G, L^*)$ and $H^2(L^v/K_v)$ for $H^2(G^v, (L^v)^*)$. Let $\alpha \in \bigoplus_v H^2(L^v/K_v)$. The local invariants of α are denoted $\text{inv}_v(\alpha) := \text{inv}_v(j_v(\alpha))$. The local invariants share many of the same functorial properties as invariants in the case of local fields, and they are generally verified by reducing to the local case.

Let $K \subset L \subset F$ be a tower of finite Galois extensions. Let $G' = Gal(F/K)$, $H = Gal(L/K)$, and $G = G'/H = Gal(F/L)$. If $\alpha \in H^2(G, I_L)$, then $inf(\alpha) \in H^2(G', I_F)$. By the properties of the invariant in the local case, we have $\text{inv}_v(inf(\alpha)) = \text{inv}_v(\alpha)$. It follows that the Brauer group of a global field can be treated locally by taking local invariants.

Now let $\alpha \in H^2(G', I_F)$. Let w/v be a valuation on L lying over one on K, and consider the restriction map $Res : H^2(G', I_F) \to H^2(H, I_F)$. Then, $\text{inv}_w \circ Res = n_{w/v} \text{inv}_v$, where $n_{w/v} = [L_w : K_v]$.

For the corestriction $Cor : H^2(H, I_F) \to H^2(G', I_F)$, we have

$$\text{inv}_v \circ Cor = \sum_{w/v} \text{inv}_w,$$

where the sum is taken over all primes of L lying over v.

Corollary 4.38. *Let $\alpha \in Br(K)$ and let $K \subset L \subset K_s$, the lattermost being the separable closure of K. Then for the associated restriction map, $Res(\alpha) = 0$ if and only if $[L_w : K_v] \text{inv}_v(a)$ for every w lying over v.*

Recall that we can denote local Artin maps $\theta_v : K_v^* \to G^v$. We can can define a map $\theta : I_K \to G$ via

$$\theta(x) = \prod_v \theta_v(x)_v.$$

This is well-defined, since $v(x_v) = 0$ whenever $x_v \in U_v$ and $\theta_v(x_v) = F_{L^v/K_v}(v)^{v(x_v)}$ whenever v is unramified. It follows that $\theta_v(x_v) = 1$ for almost all v. This map is called the global Artin map and gives the global Artin reciprocity theorem.

5. Arithmetic topology

Let L be a link in S^3. One can consider coverings of S^3 that are branched over L. The point of arithmetic topology, according to [4], is to understand the Galois module structure of the p-homology of a p-fold cyclic branched cover using p-adic higher linking matrices.

5.1. **Basic constructions.** A link L in S^3 bounds a Seifert surface. If two embedded, nontrivially linked circles in S^3 bound disjoint Seifert surfaces, then they are called a boundary link. The proof that any link bounds a Seifert surface can be done the same way as for a knot. Let X_L denote the complement of a regular neighborhood of L. We can also construct n-fold branched cyclic coverings of S^3 in the same way as for a knot.

To construct the universal abelian cover of a knot complement X_K (whose fundamental group will be $[\pi_1(X_K), \pi_1(X_K)]$,) we proceed as follows: pick a Seifert surface S bounded by K, let $S_0 \subset S$ be its interior, and let N be a regular neighborhood of S_0, so that that $N \cong S_0 \times (-1, 1)$. We denote by N_+ and N_- the subsets $S_0 \times (0, 1)$ and $S_0 \times (-1, 0)$. Let Y_K denote the complement of S in S^3. Take a copy of Y_K for every integer and index them appropriately. N_+ and N_- sit inside of Y_K in a natural way. Glue copies of N between successive copies of Y_K by identifying N_+ with its copy inside of $(Y_K)_i$ and N_- with its copy in $(Y_K)_{i-1}$. The resulting space $\tilde{X}_K$ is a regular cyclic cover of X_K with deck transformation group $\mathbb{Z}$. Since $\pi_1(X_K)^{ab} \cong \mathbb{Z}$, we obtain $\pi_1(\tilde{X}_K) \cong [\pi_1(X_K), \pi_1(X_K)]$. We construct n-fold cyclic coverings of X_K by taking the quotient under the action of $n\mathbb{Z}$. The torsion invariants of K are defined to be the torsion components of the homology of these coverings as n varies. There is always an infinite cyclic summand in the $\mathbb{Z}$-homologies of these spaces, and it is generated by a loop that goes around all the copies of Y_K and N.

Note that all these covers have nonempty boundaries. Filling the boundaries in with solid tori gives rise to the n-fold branched cyclic coverings of S^3, whose branching loci are precisely K.

5.2. **The MKR dictionary.** The summary presented here is essentially taken from [14]. The MKR dictionary was proposed by Kapranov and Reznikov and is based on the work of Mazur in [7].

(1) Closed, orientable, connected 3-manifolds correspond to schemes $Spec\, O_K$ for number fields K.
(2) Links correspond to ideals in O_K and knots correspond to prime ideals.

(3) An algebraic integer corresponds to an embedded surface, and the operation $a \mapsto (a)$ corresponds to taking the boundary of an embedded surface. Closed embedded surfaces correspond to units in O_K.
(4) C_K corresponds to the torsion component of first integral homology. The free component of $H_1(M, \mathbb{Z})$ corresponds to the group of units in O_K after removing the torsion.
(5) Finite extensions of number fields correspond to finite branched coverings.
(6) S^3 is supposed to correspond to $\mathbb{Q}$. Notice that S^3 has no nontrivial unbranched covers, and similarly $\mathbb{Q}$ has no nontrivial unramified extensions.
(7) A Galois extension L/K with Galois group G induces a morphism $Spec\, O_L \to (Spec\, O_L)/G = Spec\, O_K$.
(8) Let $q = p^n$. Consider the cyclotomic extension $\mathbb{Q}(\zeta_q)$. It is ramified only at p. These correspond to cyclic branched covers of knots in S^3. The union of these as q ranges over all powers of p should correspond to the universal abelian cover of $S^3 \setminus K$.

There is no hope for this dictionary to arise from any bijection between homeomorphism classes of appropriate 3-manifolds and number fields. Indeed, the only connected, closed, simply connected 3-manifold is the 3-sphere, but there are number fields with no unramified extensions other than $\mathbb{Q}$: any quadratic extension of $\mathbb{Q}$ with trivial class group, for example.

By analogy to the number field case, we define the decomposition group of a knot. In particular, let $\pi : M \to M/G$ be a branched covering whose branching set is a link L. Note the analogy to number fields: any closed orientable 3-manifold is a branched cover of S^3. If $K \subset L$ is a knot, we denote by D_K the subgroup of G that fixes K. If K' is the image of K under π, we see that the group of deck transformations $Gal(K'/K)$ is cyclic by covering space theory. We get an exact sequence

$$1 \to I_K \to D_K \to Gal(K/K') \to 1,$$

where I_K denotes the kernel of the covering map $\pi|_K : K \to K'$. We will call this group the inertia group of the knot K, and its order is e_K. By analogy to the number field case, we call the order of $Gal(K/K') = f_K$. By Galois theory in the number field case, the Galois group $Gal(O_L/P/O_K/p)$ is cyclic as well, where P is a prime ideal in O_L lying over p.

Recall the splitting theory for prime ideals of O_K in O_L for a Galois extension L/K. Now, if $K' \subset M/G$ is a knot over which the branched cover π is branched, then $\pi^{-1}(K')$ is a link L. Furthermore, it is obvious that components of L are transitively permuted by G. By elementary theory of group actions it follows that e_K and f_K are independent of the choice of component $K \subset L$.

A prime P in O_L is split if $e_P = f_P = 1$ and inert if $f_P = |G|$. We have completely analogous notions for knots. Henceforth, by a knot in M, we will mean a knot whose image under the covering map is also a knot, and whose image is contained in or disjoint from the branching locus.

Proposition 5.1 ([14]. theorem 2.3)**.** *Let L/K be a Galois extension with group G and let $\pi : M \to M/G'$ be a branched cover of 3-manifolds.*

1. *There are only finitely many ramified knots in O_L, and only finitely many ramified knots in M.*
2. *There are infinitely many split primes in O_L and infinitely many split knots in M.*
3. *If G, G' are cyclic then there are infinitely many inert primes in O_L and infinitely many inert knots in M.*
4. *If G, G' are not cyclic then there are no inert primes nor inert knots.*
5. *If G, G' are cyclic of prime order then each prime and each knot is either spit, ramified or inert.*

Proof. We will give proofs of the number theoretic statements and then the topological statements.

1. This follows from the ramification criterion for prime ideals.

   Now, if G' fixes a knot K pointwise, then it must land in the branch locus under the covering. The branching locus is a codimension 2 submanifold, and hence has finitely many components. Since G' is a finite group, π is proper and hence π^{-1}(branching locus) is a compact submanifold of M.
2. A prime P is split if and only if the associated decomposition group is trivial. This will happen if and only if it is unramified and its Artin symbol is trivial. The claim then follows from the Tchebotarev density theorem.

   Let K sit inside of the regular set M^{reg} of M, i.e. the open submanifold of M on which G' acts freely (note that by an easy general position argument, M^{reg} is connected. Indeed, if M^n is any manifold and N is any codimension 2 submanifold, then $M - N$ is always a connected submanifold of M.) The diversity of knots that can be found in a neighborhood of any point in M^{reg} is as complex as $\pi_0(Emb(S^1 \to S^3))$, and all of these knots are split.
3. For any Artin symbol, the Tcheboratev density theorem gives infinitely many unramified primes with that symbol. Take the preimage of a generator of G. Then $D_P = G$ for all such primes.

   It is easy to produce inert knots: indeed, pick an orbit of a point $x \in M^{reg}$, connect two points via a sufficiently nice path in M^{reg}, and apply the G'-action. Some choice is involved in the path: we can locally introduce knotting so that the resulting closed path is knotted. Note that this fails for noncyclic group actions unless we introduce branched submanifolds.
4. Evidently an inert prime must have a cyclic decomposition group which is equal to the Galois group.

   If $K \subset M$ is any knot then the only free finite group actions on K are cyclic.
5. If $|G| = p$ a prime, then one of e, f, g must be equal to p, where these integers are ramification degrees, residue degrees the number of primes lying over the fixed prime in O_K.

   The same argument works for knots.

□

If a finite group G acts properly discontinuously on a manifold M then the projection $\pi : M \to M/G$ induces a map π_* on homology. This is the analogue of the norm in number fields. The analogue of the inclusion $O_K \to O_L$ is the transfer map $H_1(M/G, \mathbb{Z}) \to H_1(M, \mathbb{Z})$ given by adding up lifts of singular chains. The operations on number fields pass to fractional ideals and to the class group.

Several more results concerning the MKR dictionary can be found in [14], but we will not record them here.

References

[1] Arnaud Beauville. *Complex algebraic surfaces*, volume 34 of *London Mathematical Society Student Texts*. Cambridge University Press, Cambridge, second edition, 1996. Translated from the 1978 French original by R. Barlow, with assistance from N. I. Shepherd-Barron and M. Reid.

[2] David A. Cox. *Primes of the form $x^2 + ny^2$*. A Wiley-Interscience Publication. John Wiley & Sons Inc., New York, 1989. Fermat, class field theory and complex multiplication.

[3] A. Fröhlich and M. J. Taylor. *Algebraic number theory*, volume 27 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, 1993.

[4] Jonathan Hillman, Daniel Matei, and Masanori Morishita. Pro-p link groups and p-homology groups. In *Primes and knots*, volume 416 of *Contemp. Math.*, pages 121–136. Amer. Math. Soc., Providence, RI, 2006.

[5] Serge Lang. *Abelian varieties*. Interscience Tracts in Pure and Applied Mathematics. No. 7. Interscience Publishers, Inc., New York, 1959.

[6] Serge Lang. Units and class groups in number theory and algebraic geometry. *Bull. Amer. Math. Soc. (N.S.)*, 6(3):253–316, 1982.

[7] Barry Mazur. Notes on étale cohomology of number fields. *Ann. Sci. École Norm. Sup. (4)*, 6:521–552 (1974), 1973.

[8] J.S. Milne. Class field theory (v4.00), 2008. Available at www.jmilne.org/math/.

[9] J.-P. Serre. Local class field theory. In *Algebraic Number Theory (Proc. Instructional Conf., Brighton, 1965)*, pages 128–161. Thompson, Washington, D.C., 1967.

[10] Jean-Pierre Serre. *Cours d'arithmétique*, volume 2 of *Collection SUP: "Le Mathématicien"*. Presses Universitaires de France, Paris, 1970.

[11] Jean-Pierre Serre. *Groupes algébriques et corps de classes*. Hermann, Paris, 1975. Deuxième édition, Publication de l'Institut de Mathématique de l'Université de Nancago, No. VII, Actualités Scientifiques et Industrielles, No. 1264.

[12] Jean-Pierre Serre. *Local fields*, volume 67 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1979. Translated from the French by Marvin Jay Greenberg.

[13] Sug Woo Shin. Symmetric powers, 2006. Available at http://www.math.harvard.edu/ kass/files/SymPowers.pdf.

[14] Adam S. Sikora. Analogies between group actions on 3-manifolds and number fields. *Comment. Math. Helv.*, 78(4):832–844, 2003.

[15] J. T. Tate. Global class field theory. In *Algebraic Number Theory (Proc. Instructional Conf., Brighton, 1965)*, pages 162–203. Thompson, Washington, D.C., 1967.

[16] André Weil. *Variétés abéliennes et courbes algébriques*. Actualités Sci. Ind., no. 1064 = Publ. Inst. Math. Univ. Strasbourg 8 (1946). Hermann & Cie., Paris, 1948.

(Thomas Koberda) Harvard University, 1 Oxford St., Cambridge, MA 02138
E-mail address: koberda@math.harvard.edu