NOTES ON GLOBAL CLASS FIELD THEORY

AKSHAY VENKATESH

Abstract. I give a proof of the existence and uniqueness theorems of unramified class field theory that largely follows the original arguments of Hilbert and Fürtwangler.

Contents

1. The target theorem

Let k be a number field, by which we mean a subfield of the complex numbers which has finite degree over the rational number field. We will prove the following statement, using largely the methods originally developed by Hilbert [1] and Fürtwangler [2].

> *Theorem:* There's an order-reversing bijection between
> - subgroups of the ideal class group c of k, and
> - everywhere unramified (including infinite places) abelian K/k
>
> characterized by the following property: $c_0 \leqslant c$ corresponds to K_0/k when the prime ideals of k that *split* in K_0/k coincide, up to a density zero set, with the prime ideals whose ideal class lies in c_0.

The proof is given in §2 – §8. The appendices sketch various paths from these to a more modern statement: Appendix A discusses the ramified case, Appendix B examines how to remove the zero density set and the related issue of reciprocity, and Appendix C formulates a more modern approach to index computations using Haar measure.

1.1. The origin of this paper.

This is an expansion of notes for some of my talks in the Spring 2024 number theory learning seminar at Princeton/IAS. The purpose of the seminar was to study original papers of Weber, Hilbert and Fürtwangler on class field theory. These

papers exploit the tension between two phenomena controlling split primes in an cyclic extension K/k: [1]

(i) Many primes must split by counting arguments: otherwise, K would have too few ideals of bounded norm.
(ii) Not too many primes split – they would (indirectly) give too many Galois-fixed ideal classes of K and contradict genus theory.

This key word "indirectly" is described in more detail in §3. The core of the whole proof is §7; read that even if you skip everything else.

The simplicity and beauty of the resulting proof strategy, and in particular its genesis in genus theory, seems to been lost in many modern approaches. Some of the intermediate results, of which (30) is probably the most complicated, may not seem "simple and beautiful." The point is that the *technique* in proving these results is simple and easy to remember, and the result is whatever the technique gives.

At the level of details, notable is the use of *auxiliary primes*, both in the arguments of Hilbert and Fürtwangler (see §7.3). The use of such primes has been important in many 20th century arguments; their original use is, in fact, similar in spirit to their much later use in *nonabelian* class field theory. Another interesting feature of the original arguments which prefigures later developments, although only minimally emphasized here (see §4.3), is the study of the ℓ-part of the class group of a cyclic ℓ-extension as a Galois module.

This paper is an attempt to give proofs in a modern language but preserving this original spirit, at least as it feels to me; it also contains an attempt, in the Appendix, to bridge the gap between the original language and the idelic one. But it is *not*

- ... an accurate exposition of the historical arguments; it is, rather, a free rewriting. I have freely used modern devices and terminology when I felt it would assist the reader in forming a mental image of the argument. But I do hope that, after reading the proofs here, the reader will be in a good position to read and appreciate the original texts.
- ... the shortest or smoothest version of the proof. I have deliberately tried to give each argument in a simple form before it appears in its more general version; and I have deliberately retained some of the intermediate scaffolding that was used in the original development of the argument.

For the proof proper I assume material at the level of a serious course in algebraic number theory, in particular, the decomposition theory of primes in a Galois extension, some basic theory of ζ-functions, the unit theorem, Kummer theory, Hilbert's theorem 90, and a modest familarity with exact sequences and diagram chasing – but no group cohomology, nor local fields. In §C I will additionally assume more: fluency with local fields, ideles, adeles, and Haar measure on locally compact groups.

1.2. **Experiencing proofs of class field theory.** The theorems of class field theory are often considered to be among the most beautiful and central results of arithmetic. Yet I have never met a number theorist who has any enthusiasm for the proofs. Perhaps they slogged through them once and suppressed the memory, or skimmed them, or skipped them altogether (as I was advised to do as a graduate student).

[1] These might be termed "analytic" and "algebraic," but I think this is misleading. For example, the bound on Galois-fixed ideal classes relies essentially on Dirichlet's unit theorem, which comes down to counting arguments that certainly share something in common with (i).

The proofs of class field theory were enthusiastically and repeatedly revised from their original form until, at least, the 1960s; Hazewinkel writes around 1990 that the subject of class field theory"has gone through many "revolutions," generalizations, and changes of point of view; some 7 in my personal count..." However, if I compare the experience of studying relatively modern expositions – for example, arguments presented by Lang [3], Tate [4] or Weil [5] – to the experience of reading Hilbert, Fürtwangler, and Takagi [1, 2, 6], I would say that this enormous effort has brought little improvement in the actual comprehensibility of the proof. This puzzling state of affairs is worthy of a much deeper study; for now, just two points:

First, the modern proofs are all-or-nothing. We either get the full and general statement of class field theory, or none of it. The historical arguments are, unsurprisingly, much closer to special cases which can be understood in isolation (e.g. the case of trivial c, which we treat in §4). The importance of such minimal examples in constructing mental models cannot be underestimated.

Secondly, comparing the arguments, one is struck immediately by the enormous increase in the use of abstraction and what might be called "machinery" in modern versions – in the statements, the intermediate definitions, and the actual proofs. By contrast, Hilbert does not even use the abstract concept of a quotient, let alone any number of more sophisticated concepts; rather, his proofs, and those of Takagi, certainly involve a significant amount of what might be called explicit computation.

These computations appearing in the original argument are not easy but they are neither unmotivated nor unedifying; they are, I would say, well adapted to their native mathematical terrain. In part, they were replaced by "industrial" concepts and techniques, forged for the purpose of creating a unified and standardized mathematics.[2] The new ideas were, by design, applicable across multiple mathematical fields, and for this very reason, when specialized to our present context, capture less arithmetical nuance.

1.3. **Notation.**

- k denotes a number field, and we denote by r_∞ the number of archimedean places of k, i.e. the number of embedding $k \hookrightarrow \mathbf{C}$ up to complex conjugation.
- ℓ is a prime.
- By default an "ideal" of k means a nonzero fractional ideal.
- K/k will always denote a finite abelian extension; if K/k is cyclic, we denote by σ a generator for the Galois group of K/k and often write $m = [K : k]$. We usually denote objects associated to K with capital letters and objects associated to k with lower case letters. In particular lower case letters c, u denote the class group and unit group of k, and upper case letters C, U the same for K; similarly, c' denotes the class group of a field k'.
- A prime ideal of k is *split* if it factorizes in K as $\mathfrak{p}_1 \dots \mathfrak{p}_m$ where $m = [K : k]$. It is *inert* if it is unramified and remains prime in K.
- We say K/k is *unramified* if it is unramified at both finite and infinite places. We similarly say it is"unramified outside S" for a set S of places; if S consists of finite places, this is understood to imply that K/k is unramified at archimedean places.
- We use N for the norm from K to k. We apply this to different objects: the class group norm $N : C \to c$, the field norm $N : K \to k$, etc. Sometimes we also use N

[2]See, for example, Bourbaki [7].

for the "absolute" norm, e.g. for an ideal; where there is a risk of confusion we write N_k^K for the norm for K to k and N for the absolute norm.

- If G is an abelian group with an action of the finite order automorphism σ, then G^σ denotes the σ-fixed elements and $G^{1-\sigma}$ the image of $1-\sigma$ (sorry, these notations clash...)
- We denote with a superscripted bar the relative group:
$$\bar{C} = C/c, \bar{U} = U/u.$$
- c_0 denotes a subgroup of c
- For any abelian group A and integer m, A/m means the quotient of A by mth powers and $A[m]$ means the m-torsion.
- When we write the symbol $\#$ it means that one should replace all groups by their order. Thus e.g. $\#\frac{c}{C}$ means $\frac{\#c}{\#C}$, although the quotient c/C does not make sense.
- We will repeatedly use the fact that, for $f : A \to A$ an endomorphism of a finite abelian group,

$$\#\ker(f) = \#\mathrm{coker}(f), \tag{1}$$

just as the corank and nullity of a square matrix coincide.

1.4. **Acknowledgements.** I would like to thank all the participants of the seminar, most particularly Marco Sangiovanni Vincentelli, Kenz Kallal, Fernando Trejos and Sean Howe for their excellent presentations of, respectively, Weber's work on elliptic functions, Weber's analysis of abelian extension of $\mathbf{Q}$, Hilbert's *Zahlbericht*, and Hilbert's analysis of relative quadratic extensions.

I would also like to give deep thanks to Brian Conrad for numerous and *very* helpful comments.

2. The notion of a class field

The first step in proving the theorem is to observe an elementary link between splitting and the norm on ideal class groups:

> if $\mathfrak{p}$ is a prime of k splitting in K, its ideal class is a norm of an ideal class from K.

Indeed, $\mathfrak{p}$ is the norm from K to k of any prime lying above it. A class field will be one for which this is almost sharp, i.e. for which the general inclusion

$$\text{split primes} \subset \text{primes whose ideal class is a norm} \tag{2}$$

is an equality up to density zero. By computing densities, we will see in §2.3 that (2) turns into the following inequality: for any K/k (abelian, as always) the index of such norms, inside all ideal classes c for k, is at most the degree of the field extension:

$$[c : NC] \leq [K : k]. \tag{3}$$

We will adopt this as our "official" definition of class field: K/k is a *class field* if equality holds in (3). We will show below that this implies that (2) is an equality up to density zero; the converse is also true, but we do not use it.

This is an outstanding definition: the concept of class field is very rigid, and many proofs will write themselves with it in mind, even though it does not appear in the statement of the target theorem.

We outline the proof of (3) verbally. To simplify notation suppose K/k is unramified. The norm of a prime of K is always a power of a prime $\mathfrak{p}$ in k, and the exponent is 1 if and only if $\mathfrak{p}$ is split. Therefore, for any integral nonzero ideal I of K, the factorization of $N_k^K I$ into primes looks like:

(4) $N_k^K(I) =$ primes whose class belong to $NC \times$ primes occurring with multiplicity ≥ 2.

We now count such ideals I in two different ways. Firstly, by the geometry of numbers, the number of (nonzero, integral) ideals I of K of absolute norm $\leq X$ grows linearly in X. On the other hand, we can also count the number of possibilities for $N_k^K(I)$ and then count the number of ideals I with given norm to k. Were NC very small, the restricted factorization pattern (4) forces the second count to be too small, contradicting the geometry of numbers. [3]

It is easiest to formalize this argument with ζ-functions, but it is important to emphasize that the argument does not require any complex analysis; the *only* essential input is the geometry of numbers, via linear growth of ideals of bounded norm. To me, the argument seems on the same level as the argument used to prove the unit theorem, which might be put verbally as "there are more elements of $k^\times$ than fractional ideals, so some elements must generate the unit ideal."

2.1. **Abelian extensions are characterized by splitting primes.** Let K/k be abelian[4]; then

$$\text{density of primes of } k \text{ that split in } K/k = \frac{1}{[K:k]}. \tag{5}$$

Here and throughout we understand density in the sense of Dirichlet. For example, the density of a set M of integers is 0.3 exactly when $\sum_{m \in M} m^{-s} = 0.3 \log(s-1)^{-1} +$ bounded as $s \to 1^+$; the density of a set of ideals is the density of its (multi-)set of norms.

Proof. Write $\zeta_K(s)$ for the Dedekind ζ-function; we will use the fact that $\zeta_K(s) \sim \frac{A}{s-1}$ as $s \to 1^+$ for some nonzero A. The formula

$$\sum_{\mathfrak{P}} (N\mathfrak{P})^{-s} + \underbrace{\sum_{m \geq 2} \frac{(N\mathfrak{P})^{-ms}}{m}}_{\text{bounded as } s \to 1^+} = \log \zeta_K(s), \tag{6}$$

where the sums are taken over prime ideals $\mathfrak{P}$ of K, shows that the Dirichlet density of the multiset $N\mathfrak{P}$ equals 1. Since the absolute norms of $\mathfrak{P}$ and $N_k^K \mathfrak{P}$ coincide, this multiset consists of absolute norms of prime ideals of k that split in K, each with multiplicity $[K:k]$, together with a set that consists of prime powers p^m with $m \geq 2$, each with multiplicity at most $[K:\mathbf{Q}]$; the latter are readily seen to have density zero, whence (5). □

From this we see that an abelian extension K of a fixed number field k is *characterized* by its set of splitting primes, considered up to density zero sets; indeed, if K_1, K_2 had the same set of splitting primes, then so too would the compositum $K_1 K_2$, and so its degree must coincide with that of K_1 and K_2.

[3] As an exercise, prove that there are primes congruent to 1 modulo 4 by thinking about the number of Gaussian integers of norm $\leq X$.

[4] All we use in the argument is that it is Galois.

2.2. **Class group ℓ-functions.** For $c_0 \leqslant c$ a subgroup, we have the inequality

$$\text{(upper) density of primes of } k \text{ whose class lies in } c_0 \leqslant \frac{1}{[c : c_0]}. \tag{7}$$

"Upper" means that we take a limit supremum rather than a limit. The inequality reflects the same issue as Dirichlet's theorem: it is easier to prove that there are primes $\equiv 3$ modulo 4 than to prove there are primes $\equiv 1$ modulo 4. [5]

Proof. Write as usual $L(s,\chi) = \sum_I \frac{\chi(I)}{NI^\sigma}$ for χ a character $c \to \mathbf{C}^\times$; the sum is taken over nonzero integral ideals, where NI is the absolute norm. Summing the analogue of (6) over characters χ of c/c_o we get

$$\sum_{\mathfrak{p}\in c_0} N\mathfrak{p}^{-s} + \underbrace{\sum_{m\geq 2, \mathfrak{p}^m \in c_0} \frac{(N\mathfrak{p})^{-ms}}{m}}_{\text{bounded as } s\to 1^+} = \frac{1}{[c:c_0]} \sum_\chi \log L(s,\chi_i),$$

where the sum is over primes $\mathfrak{p}$ of k. For $\chi = 1$ we have $L(s,\chi) = \zeta_k(s)$ whose logarithm behaves like $\log \frac{1}{s-1}$ as $s \to 1^+$ up to a bounded error. For $\chi \neq 1$, what we know from the theory of class group L-functions (which requires the same inputs as for ζ_k above, nothing more) is that $|L(s,\chi)|$ remains bounded as $s \to 1^+$ (although it might approach zero, or not have a limit), and from this we deduce (7). □

2.3. **Class fields.** From this we deduce that the promised inequality:

> (*) The index $[c : NC]$ of the corresponding map $N : C \to c$ on ideal class groups is at most $[K : k]$, and if equality holds then the split primes agree (up to a zero density set) with those whose ideal class lies in NC.

Indeed, we already noted that ideal classes of split primes belong to NC. The split primes have density $\frac{1}{[K:k]}$, and those whose ideal class belong to NC have upper density at most $\frac{1}{[c:NC]}$. So $\frac{1}{[K:k]} \leq \frac{1}{[c:NC]}$ and so $[c : NC] \leq [K : k]$. We say that an abelian extension K/k is **a class field** if equality holds here, equivalently

$$[c : NC] \geq [K : k].$$

If equality holds then we find that the "upper density" of (7) is actually a density, and that the sets of split primes and primes whose ideal class belongs to NC differ by a set of density zero. The reverse implication is also valid – if these sets differ by a set of density zero, then $[c : NC] = [K : k]$. This follows from a more precise version of our discussion, where we add in some complex analysis, but we will not use it.

2.4. **Basic properties of class fields.** By §2.1, a class field K/k is uniquely characterized by the norm subgroup $NC \leqslant c$; we denote a class field with $NC = c_0$ by $K(c_0)$ if it exists.

For example: Suppose that K/k is a class field; then for any intermediate field $k \subset k' \subset K$, both K/k' and k'/k are class fields. Indeed, the norm of the class group from K to k' has index at most $[K : k']$. Taking norms to k, the inclusion $N_k^K C \subset N_k^{k'} c'$ must also have index at most $[K : k']$, and this shows that $N_k^{k'} c'$ has index at least $[k' : k]$ inside c .

[5] With a little complex analysis, it is easy to prove that equality holds if c/c_0 has odd order. But we do not need this.

3. The basic strategy

To reformulate our theorem, we must prove that

> *class fields exist for every $c_0 \leqslant c$ and give exactly the unramified abelian extensions of k.*

Class fields are very rigid, as we already saw. The difficulty then is making them at all; the difficulty in constructing a class field is *to control NC from above*, for analysis bounds it from below. How are we going to do this?

The "basic strategy" is as follows. Suppose K/k is cyclic, with σ generating the Galois group.

> *Basic strategy:* To control NC from above, it is enough show that $C^{1-\sigma}$ is large (because N is automatically trivial on it). And to show that $C^{1-\sigma}$ is large, it is enough show that C^σ is small (because $C/C^\sigma \simeq C^{1-\sigma}$).

In quantitative form, this argument shows that $\#C^\sigma \geq \#NC$; and the only way in which it fails to be tight is if $C^{1-\sigma}$ is strictly smaller than the kernel of N.

The input to this strategy is control on C^σ from above. The control of σ-fixed elements is the subject of genus theory, which in turn originates in Gauss' study of quadratic forms. Roughly speaking, we will analyze C^σ and several variants just by unwinding the definition in a direct way, as in e.g. the discussion before (25); and the shape of the answer is always:

$$\frac{\#c' \times \prod \text{ramification indices}}{[K:k]} = \#(C^\sigma)' \times \text{index of norms in } u'. \tag{8}$$

Here $c', (C^\sigma)', u'$ are variants on c, C^σ, u that vary from instance to instance. The ultimate form of this we use is (30), but we give a few precursors (15), (20), (26) all of which have the same pattern. The reader should bear in mind that the *technique* to prove these results is simple, even if the results do not look so. It is reasonable that c should be related to C^σ (there is a map $c \to C^\sigma$) and it is reasonable that ramification indices should show up (ramified primes tend to generate σ-fixed classes). The less intuitive parts of the formula are the unit norm index and the factor $[K:k]$, and they both *depress* $\#(C^\sigma)'$.

Note that (8) implies that $\#(C^\sigma)' \leq \frac{\#c'}{[K:k]}$ so long as the index of norms in u' exceeds the ramification index. So (8) shifts the burden of proving that K is a class field from showing that not too many *ideal classes* are norms, to showing that not too many *elements* are norms – a more concrete proposition which can be accomplished by imposing local conditions.

A technically smoother approach is Chevalley's idelic argument. We replace C with the larger group C of idèle classes, where it is almost trivial to understand C^σ. The strategy then applies very easily, see §C. In a literal sense, the above reasoning does not apply either to C because it is not a finite group but it can be readily adapted by using volume in place of size.

4. Warm-up: trivial c, or, why Hilbert proved Theorem 90

In Satz 94 of his *Zahlbericht*, Hilbert proves that *if c is trivial, then k has no unramified abelian extensions*. This is a special case of what we want to prove, and is not strictly required for the proof; but it contains many valuable ideas that inspire the general argument, so we give it separately.

It is enough to show that, if there exists K/k a cyclic unramified ℓ-extension, then c is nontrivial. We assume K/k is cyclic and unramified throughout this section; recall that "unramified" includes archimedean primes by convention.

I have followed the presentation in the Zahlbericht, except in using modern notions of rings and modules in the proof of §4.3.

4.1. **Satz 94.** The key idea is to produce not just classes in c, but classes in the kernel of $c \to C$. In other words, we must find an ideal i of k such that its extension i_K to K is principal, say, $i_K = (Y)$ for some $Y \in K^\times$; then

$$(Y)^\sigma = (Y)$$

as i_K was extended from k. Therefore, $(Y)(Y^\sigma)^{-1}$ is the unit ideal, so $Y^{1-\sigma}$ is a unit of K, clearly of norm 1. We can reverse this process, by Hilbert's Theorem 90, which he introduced precisely for this purpose: any unit Θ of K of norm 1 arises as $\Theta = Y^{1-\sigma}$ for some $Y \in K^\times$, and in this case the ideal (Y) is necessarily extended from k. Indeed by inspection of factorization

$$\text{every } \sigma\text{-fixed ideal is extended from } k. \tag{9}$$

because K/k is unramified. Moreover, (Y) is the extension of a principal ideal if and only if this unit Θ is "the $(1-\sigma)$th power of a unit of K" (i.e. the image of such a unit under $1-\sigma$.) Therefore, to show that the kernel of $c \to C$ is nontrivial, it is sufficient to exhibit a *single* unit of K that has norm 1 but is not a $(1-\sigma)$th power; said differently, we must show that *Hilbert 90 fails for units*:

there are units in K of norm 1 not equal to $W^{1-\sigma}$ for another unit W of K.

Actually, our discussion so far exhibits an isomorphism

$$\ker(c \to C) \simeq \frac{\text{norm 1 units of } U}{U^{1-\sigma}}. \tag{10}$$

We will prove in the following subsections that the right side of (10) is nontrivial, *assuming* that $\zeta_\ell \notin k$; note this excludes $\ell = 2$. It is quite easy to remove this condition on roots of unity, but allowing $[K:k]$ to be composite requires a different technique, see §5.

4.2. **Reduction to the relative unit group.** Note that U is a module under $\mathbf{Z}[\sigma]$ and the *relative unit group*

$$\bar{U} = U/u$$

is too; the norm $N : U \to u$ induces a norm $\bar{N} : \bar{U} \to u/\ell$. We will first reduce to a similar question for $\bar{U}$, which will be, as we will see, easier.

The map $U \to \bar{U}$ induces

$$\frac{\text{norm 1 units of } U}{\{\theta^{1-\sigma} : \theta \in U\}} \to \frac{\text{norm 1 elements of } \bar{U}}{\bar{U}^{1-\sigma}}. \tag{11}$$

This map is evidently surjective, and our assumption that $\zeta_\ell \notin k$ forces it also to be injective. On the other hand, the norm 1 elements of $\bar{U}$ comprise the kernel of $\bar{N}$, so their index within $\bar{U}$ is just the size of the image of $\bar{N}$. That size equals

$$\frac{\#(u/\ell)}{[u/\ell : N\bar{U}]} = \frac{\#(u/\ell)}{[u : NU]}.$$

Thus, both sides of (11) have size

$$\frac{[\bar{U} : \bar{U}^{1-\sigma}]}{\#\text{image } \bar{N}} = \frac{[\bar{U} : \bar{U}^{1-\sigma}][u : NU]}{\#(u/\ell)} \tag{12}$$

Now, the unit theorem, and our assumption $\zeta_\ell \notin k$, means that the size of u/ℓ equals $\ell^{\mathsf{r}_\infty - 1}$. (Recall r_∞ is the number of archimedean places.) So to show that Hilbert 90 fails for U, it is enough to show that $[\bar{U} : \bar{U}^{1-\sigma}]$ is strictly larger; and we will in fact show

$$[\bar{U} : \bar{U}^{1-\sigma}] \stackrel{?}{=} \ell^{\mathsf{r}_\infty}. \tag{13}$$

4.3. **Structure of relative units.** The point of passing to $\bar{U}$ is that studying the action of σ on $\bar{U}$ is easier than the same question for U, because $\bar{U}$ is killed by the "norm"

$$1 + \sigma + \cdots + \sigma^{\ell-1} \in \mathbf{Z}[\sigma] \tag{14}$$

so it is a module under the very nicely-behaved quotient ring $\mathfrak{o} = \mathbf{Z}[\sigma]/(1 + \sigma + \cdots + \sigma^{\ell-1})$. The map $\sigma \mapsto e^{2\pi i/\ell}$ identifies $\mathfrak{o}$ with the cyclotomic integer ring for $\mathbf{Q}(\zeta_\ell)$. It is, in particular, a Dedekind domain, and within $\mathfrak{o}$ the element $1 - \sigma$ generates the unique prime ideal $\mathfrak{l}$ above ℓ; that prime has index ℓ in $\mathfrak{o}$. By the structure theorem for finitely generated modules over Dedekind domains, $\bar{U} = U/u$ is a sum of modules of the following type:

$$\bar{U} \simeq \mathfrak{a}_1 \oplus \ldots \mathfrak{a}_r \oplus \mathfrak{o}/\mathfrak{b}_1 \oplus \cdots \oplus \mathfrak{o}/\mathfrak{b}_s$$

where $\mathfrak{a}_i$ and $\mathfrak{b}_j$ are nonzero ideals of $\mathfrak{o}$. (We can get away with less here: only the localization at ℓ matters and so we can even work with the principal ideal domain $\mathfrak{o}_{(\ell)}$ and use just the similar statement for modules over a PID; or, in different words, we can always find a subgroup $\bar{U}' \subset \bar{U}$ of prime-to-ℓ index which behaves very nicely under $\mathbf{Z}[\sigma]$. We will take up this idea again in §5.1.)

It is easy to compute the number r of ideals $\mathfrak{a}$ above: each $\mathfrak{a}_i$ is a free abelian group of rank $\ell - 1$. But u has rank $\mathsf{r}_\infty - 1$, by the unit theorem, and U has rank $[K : k]\mathsf{r}_\infty = \ell \cdot \mathsf{r}_\infty$, because K/k is unramified at archimedean places, so $\overline{U} = U/u$ has rank $(\ell - 1)\mathsf{r}_\infty$ and we deduce that

$$r = \mathsf{r}_\infty.$$

Now our assumption $\zeta_\ell \notin k$ implies that $\bar{U}$ is free of ℓ-torsion; indeed, if $Y \in U$ outside u has the property that $Y^\ell \in k$, then K, being Galois over k, would contain a nontrivial ℓth root of unity ζ_ℓ, but $[k(\zeta_\ell) : k]$ is prime to ℓ and not 1, by assumption. Therefore each $\mathfrak{b}_j$ appearing above is prime to $\mathfrak{l}$. When we take the quotient $\bar{U}/\bar{U}^{1-\sigma}$ we then get

$$\bar{U}/\bar{U}^{1-\sigma} = \bigoplus_{i=1}^{r} \mathfrak{a}_i/\mathfrak{a}_i\mathfrak{l} \simeq \bigoplus_{i=1}^{r} \mathfrak{o}/\mathfrak{l} \simeq \mathbf{F}_\ell^r.$$

Therefore $\#\bar{U}/\bar{U}^{1-\sigma} = \ell^r = \ell^{\mathsf{r}_\infty}$ and combining with (12) concludes the proof. The above argument *also* works if $\zeta_\ell \in k$, but then there are additional terms at several points which end up cancelling. This is a very nice exercise. □

In fact, we have shown (combing (10) with the above computations) that

$$\frac{(\#\ker(c \to C))}{\ell} = [u : NU], \tag{15}$$

i.e. "the fewer units which are norms, the more ideal classes capitulate." This is our first very simple formula of the type (8), but with no terms related to ramification or to C^σ.

5. Some mild generalizations of §4

We are going to give a (fairly mild) generalization of the previous section. Namely, we will prove a formula (20) that generalizes (15) to the case of composite degree and allows ramification. The reader might like to skip this section on a first pass and simply accept the results as slight improvements of §4; in particular, the results of §5.1 here *will not be used* for the key existence statement of §7.

The original approach of Takagi to composite degree was based on a reduction to prime index by an inductive argument. The argument that follows, however, is substantively due to Chevalley and Herbrand; the idea of using finite index subgroups of U whose structure as a Galois module is simple is already in the Zahlbericht. For other approaches see the comments in §5.1.1.

5.1. **Unit computations.** Recall that our previous reasoning relied essentially on the failure of Hilbert 90 for units. We must first generalize this to the composite degree case. What we will prove is

For K/k a cyclic extension, unramified at archimedean places,

$$\frac{[\text{norm 1 units of } U : U^{1-\sigma}]}{[u : NU]} = [K : k]. \tag{16}$$

In the previous section, we proved this in the case when $[K : k]$ is the odd prime ℓ and $\zeta_\ell \notin k$; this follows from combining (11), (12) and (13). Our previous argument was based on the fact that we could understand U/u explicitly as a $\mathbf{Z}[\sigma]$-module, because $\mathbf{Z}[\sigma]/(1 + \sigma + \cdots + \sigma^{\ell-1})$ was a cyclotomic ring. This doesn't happen in the composite degree case. But we *can* always find a finite index subgroup $U' \leqslant U$ whose behavior as a $\mathbf{Z}[\sigma]$-module is very simple, and for which we can compute explicitly. This is enough because:

> *Claim:* The validity of equality (16) for U is equivalent to its validity for any finite index subgroup $U' \leqslant U$ stable by σ, where we understand u to be replaced by $u' := (U')^\sigma = u \cap U$.

This insensitivity is plausible if one look at the proof in §4.3.

Proof. Let $a = [U^{1-\sigma} : U'^{1-\sigma}]$ and $b = [U^{N=1} : (U')^{N=1}]$. We claim that numerator and denominator of (16) change, upon passage from U to U', by the factor a/b. This is immediate for the numerator. That is so for the denominator follows from the pair of equalities

$$[NU : NU'] = \frac{[U : U']}{b} \text{ and } [u : u'] = \frac{[U : U']}{a}. \tag{17}$$

Both are proved the same way. The first equality expresses how the image of the norm changes as we pass from U to U': the numerator arises because the source of N shrinks, and the denominator because the kernel of N shrinks. The second (in the form $a = \frac{[U:U']}{[u:u']}$) is the same reasoning replacing the role of N by $1 - \sigma$. □

We prove now (16). Write $[K : k] = m$ and r_∞ for the number of archimedean places of k; then, as first proved by Herbrand,

> There are units $u_1, \ldots, u_{\mathsf{r}_\infty}$ in U such that the $\mathsf{r}_\infty \cdot m$ elements $\{\sigma^i u_j\}$, where $1 \leq j \leq \mathsf{r}_\infty$ and $1 \leq i \leq m$, are multiplicatively independent subject only to a single relation.

Indeed a "generic" choice of $u_1, \dots, u_{\mathsf{r}_\infty}$ have the desired property. To prove this, we recall that the unit theorem shows that a finite index subgroup of U is isomorphic to a lattice Λ inside

$$\{(x_1, \dots, x_{\mathsf{r}_\infty m} \in \mathbf{R}^{\mathsf{r}_\infty m} : \sum x_i = 0\} \tag{18}$$

where the σ-action on U cyclically permutes the x_i in orbits of size m. In what follows, then, we regard u_i as belonging to Λ, and in particular to $\mathbf{R}^{\mathsf{r}_\infty m}$. Our assertion is then that we can find $u_1, \dots, u_{\mathsf{r}\infty} \in \Lambda$ such that the vectors $\sigma^i u_j$ $(0 \le i \le m-1)$ when considered as forming a $\mathsf{r}_\infty m \times \mathsf{r}_\infty m$ array, give a matrix of rank $\mathsf{r}_\infty m - 1$. It is enough to find such u_i inside $\mathbf{Q}.L$ (because then we can rescale them to lie in Λ) and then, by density, it is enough to find u_i inside the $\mathbf{R}$-span of Λ. But that is just the real vector space (18) and we leave this easy piece of linear algebra to the reader.

We will take U' be then the multiplicative span of these units, i.e.

$$U' = \{\prod_{i,j} (\sigma^i u_j)^{a_{ij}} : a_{ij} \in \mathbf{Z}\}. \tag{19}$$

We now just compute by hand: The single relation between $\sigma^i u_j$ necessarily has the form $\prod_{i,j} (\sigma^i u_j)^{m_j} = 1$ the exponents depending only on j and not on i - for otherwise, one would obtain additional relations by applying σ. Thus the a_{ij} in (19) are well defined up to the translation $a_{ij} \leftarrow a_{ij} + m_j$. Elements of U' of norm 1 amount to all expressions (19) where $\sum_i a_{ij} = \lambda m_j$ for some $\lambda \in \mathbf{Z}$ and all j; modifying $a_{ij} \leftarrow a_{ij} + m_j$ modifies λ by m. Now considering the class of λ modulo m defines an isomorphism

$$\text{norm one classes in } U' \text{ modulo } (1-\sigma)\text{th powers} \simeq \mathbf{Z}/m\mathbf{Z}.$$

(for this we just check that if $\sum_i a_{ij} = 0$ then (19) is a $(1-\sigma)$th power.)

On the other hand U'^{σ} amounts to all combinations $\prod_{i,j} (\sigma^i u_j)^{a_{ij}}$ where a_{ij} does not depend on i (why?) This element is then the norm of $\prod_j u_j^{a_{0j}}$, so $(U')^\sigma = NU'$.

So, replacing U by U', the numerator of (16) is m, and its denominator is trivial; the ratio is m as desired.

5.1.1. *Other proofs.* Here is a more intuitive, but uglier to write, argument: Note that (16) looks a lot like the discussion in §3: it asserts that the discrepancy between U^σ and NU is almost the same as the discrepancy between $\ker(N)$ and $U^{1-\sigma}$, except now there is an extra factor $[K : k]$. So it is reasonable to try to prove (16) following the *basic strategy* of §3. This can indeed be done; but because the unit group is infinite, we need to replace size by "the number of units in a large ball." We leave the reader to implement this. A cleaner-to-write version of the same strategy will be given in §C.4.5 based on the following idea: Rather than measure the size of a lattice by counting the number of points in a large ball, we can instead compute its covolume.

5.2. **Consequences for the class group; prohibition of even slightly ramified extensions.** By the same reasoning as the last section, we now get a general version of (15) for any cyclic extension of degree $[K : k] = m$, permitted to ramified at finite primes with ramification indices $e_1, e_2, \dots$ (but still unramified at archimedean places):

$$\frac{\#\ker(c \to C) \prod e_i}{m} = \#X \cdot [u : NU] \tag{20}$$

where X is the subgroup of the *relative class group* $\bar{C} = C/c$ spanned by the various σ-fixed classes $\widetilde{\wp}_1, \dots, \widetilde{\wp}_s$ arising from ramified primes; here the $\wp_i$ are all primes of k that ramify, and

$$\widetilde{\wp} := \text{product of prime ideals of } K \text{ dividing } \wp. \tag{21}$$

Formula (20) again has the general type of (8) – note that X is in fact σ-fixed.

Proof. Repeat the same steps as the previous section but replace (9) by the assertion that any σ-fixed ideal is extended from k, modulo a class in X. More formally, the map (10) is now only injective; the obstruction to surjectivity is the failure of (9), and instead we note that a σ-fixed ideal is extended from k if and only if its valuation at primes above $\wp_i$ are divisible by e_i. This gives an exact sequence:

$$0 \to \ker(c \to C) \xrightarrow{\alpha} U^1/U^{1-\sigma} \xrightarrow{\beta} \prod \mathbf{Z}/e_i \xrightarrow{\gamma} X \to 0. \tag{22}$$

where the first map α is as in (10), the map β takes $u \in U^1$, writes $u = x^{1-\sigma}$ and assigns to it the valuation of x at any prime above $\wp_i$ (all these valuations are equal), and the map $\gamma : \prod(\mathbf{Z}/e_i) \to X$ sends a_i modulo e_i to $\widetilde{\wp}_i^{a_i}$. The only point that has not already been discussed is that the kernel of γ coincides with the image of β: if (a_i) lies in that kernel, then $\prod \widetilde{\wp}_i^{a_i}$ is the product of a principal ideal (Y) and an ideal extended from k; then $Y^{1-\sigma}$ is a unit and maps to (a_i) under β.

Computing orders in (22) and using (16) gives (20). □

Observe (20) shows that triviality of c rules out not only unramified extensions but *also* certain ramified extensions. To see how, suppose e.g. that K/k has ramification index e at a single prime $\mathfrak{p}$ and is unramified elsewhere, where we suppose that the absolute norm $N\mathfrak{p} \equiv 1$ modulo e.[6] The norm of any element in U is an eth power modulo $\mathfrak{p}$ (why?) Therefore, if the reduction map

$$u \to k(\mathfrak{p})^\times \text{ modulo } e\text{th powers} \tag{23}$$

is surjective, it follows that NU must have index at least e inside u; the right side of (20) is then $\geq e$. We conclude that K cannot actually ramify in this way if (23) is surjective. We will redeploy this argument in a crucial way later.

6. Unramified cyclic extensions are class fields

We prove that unramified cyclic extensions are class fields. In effect, we just proved this in the case when c is trivial; but we will also give the proof in the *second* simplest case in §6.1 – when c is cyclic of order ℓ; the general case is not much harder.

6.1. Second simplest nontrivial case: when c and $[K : k]$ has order ℓ.

Suppose that c has order ℓ and K/k is an unramified cyclic ℓ-extension. We will show K is a class field, which here simply means that NC is trivial.

We follow the basic strategy (§3). If we could show that C^σ were trivial, then $1-\sigma : C \to C$ is injective and so also surjective; but since the class group norm N kills any $(1-\sigma)$th power, it would follow that N is trivial, as desired.

Take then I an ideal of K whose class is σ-fixed; thus $I^{1-\sigma} = (\theta)$ for some $\theta \in K^\times$; note that $(N\theta)$ generates the trivial ideal of k, so is a unit, and $N\theta$ is determined by the ideal

[6] This is in fact automatic if $\mathfrak{p}$ is relatively prime to the index $[K : k]$; this uses a little more theory about ramification. We will not however use this in what follows.

class of I up to norms of units. In the reverse direction, given a unit $x \in u$ which is a norm, say $x = N\theta$, then the ideal (θ) of K has trivial norm and therefore

$$(\theta) = J^{1-\sigma} \text{ for some fractional ideal } J \text{ of } K, \tag{24}$$

an analogue of Hilbert's theorem 90 for ideals, elementary to check by looking at prime factorization. This J is specified up to σ-fixed ideals, which are all extensions from k by (9) (using unramifiedness of K/k at all finite places); so the rule sending x to the class of J defines an isomorphism

$$\frac{\text{units of } k \text{ that are norms from } K}{\text{units of } k \text{ that are norms from } U} \to \frac{C^\sigma}{\text{image of } c \text{ in } C} \tag{25}$$

But (10) shows that the order of $\ker(c \to C)$ equals $\ell \cdot [u : NU]$ and, since the order of c was exactly ℓ, this forces both $NU = u$ and that the image of c in C is trivial. Substituting these conclusions into (25), we deduce that C^σ is trivial. Done! □

6.2. **Unramified cyclic extensions are class fields; the ambiguous class number formula.** In general, taking K/k cyclic and unramified at archimdean places, we can proceed as above; but now the σ-fixed ideals are extensions from k *together with* the classes of $\widetilde{\wp}_i$ for $\wp_i$ ramified. Therefore, repeating the above reasoning, the left hand side $\frac{u \cap NK^\times}{u \cap NU}$ of (25) is now isomorphic to the quotient of C^σ both by the image of c and all the $\widetilde{\wp}_i$. The quotient of C^σ by the image of c has size $\#\frac{C^\sigma}{c}\ker(c \to C)$, and the further quotient by the $\widetilde{\wp}_i$ has size $\#\frac{C^\sigma \cdot \ker(c \to C)}{c \cdot X}$, where as before X is the subgroup of $\bar{C}$ spanned by the $\widetilde{\wp}_i$.

Multiplying the resulting modification of (25) by (20), and cancelling common terms gives the *ambiguous class number formula*:[7]

$$\frac{\#c \cdot \prod e_i}{m} = \#C^\sigma \cdot [u : u \cap NK^\times] \tag{26}$$

where $m = [K : k]$ (cf. (8)). This shows, in the everywhere unramified case, that $\#C^\sigma$ is at most $\frac{1}{m}\#c$; but then, as above, $[c : NC] \geq m$. So every unramified cyclic K/k is a class field; done! [8]

6.3. **The *relative* ambiguous class number.** The argument above is not yet sharp enough to prove existence. For that, we need (as in §5.2) to handle some potential ramification, and here (26) proves inadequate. Now, Takagi's approach to this involves class groups with modulus, see §A; but Fürtwangler's method is more direct, using, instead, a *relative* class group.

Our argument did not take advantage of the fact that the norm $N : C \to c$ contains in its image mth powers. Using that, it is enough to bound the size of the image of the norm modulo m, which factors through $\bar{C} = C/c$:

$$\bar{N} : \bar{C} \to c/m \tag{27}$$

Now as usual $\bar{N}$ is trivial on $(1-\sigma)\bar{C}$, and this has size at most $[\bar{C} : \bar{C}^\sigma]$; so if we can show that $\bar{C}^\sigma$ has size at most $\frac{1}{m}\#(c/m)$ we will again certify that K/k is a class field. By doing

[7] The name goes back to Hilbert's terminology "ambig" for S-fixed ideals and ideal classes. See Lemmermeyer's exposition [8] for another proof of this formula.

[8] Moreover, we find the interesting consequence that every unit in k is a norm (not necessarily of a unit) from K.

this, we will achieve a sharper version of the previous results. So we now turn to analyzing $\bar{C}^\sigma$ instead of C^σ.

Let K/k be a cyclic extension of degree m, which we assume unramified at archimedean places. To express the relevant formula, define groups $\nu \supset \nu_{\mathrm{norm}}, \nu_{\mathrm{unit}}$

$$\nu = \text{classes in } k^\times/(k^\times)^m \text{ whose valuation is everywhere 0 mod } m, \tag{28}$$

$\nu_{\mathrm{norm}} =$ subset represented by norms from $K^\times$,$\nu_{\mathrm{unit}} =$ subset represented by units in k.

We might think of ν, ν_{norm} as variants of "units" and "units that are norms" – a unit is an element whose valuation is everywhere 0, and now we impose that condition only modulo m. In fact, there is a short exact sequence

$$0 \to u/m \to \nu \to c[m] \to 0, \tag{29}$$

arising from the fact that any m-torsion ideal class I uniquely determines a class in ν modulo the image of units, namely, any generator for I^m. Notice, in particular, that ν is finite.

6.3.1. *The formula and its consequence.* In this situation, we claim that

$$\frac{\#c[m]\prod e_i}{m} = \#\bar{C}^\sigma \cdot [\nu : \nu_{\mathrm{norm}}] \tag{30}$$

(cf. (8)). In particular, K/k cyclic and unramified at archimedean places is a class field *if*

$$[\nu : \nu_{\mathrm{norm}}] \geq \prod e_i \tag{31}$$

Proof. It is easier to get here directly from (20) rather than go through (26). To get from (20) to (30), we must compute the difference between X (= span of the $\widetilde{\wp}_i$) and $\bar{C}^\sigma$ (= all invariant classes). The difference expressed by the following short exact sequence generalizing (25):

$$0 \to \ker(c \to C) \xrightarrow{\delta} \frac{\nu_{\mathrm{norm}}}{NU} \to \frac{(\bar{C})^\sigma}{X} \to 0 \tag{32}$$

First we define δ. An ideal i in k whose class is trivial in K has the property that its extension i_K is of the form (Y), where $Y \in K^\times$ is determined by the ideal class of i up to units of K and $k^\times$. The class of NY lies inside ν_{norm} and is well defined up to $NU \cdot (k^\times)^m$. Thus δ assigns (the class of) NY to (the class of) i; we leave the reader to check injectivity.

To motivate how to define the second map in (32), take an ideal J representing a class in $\bar{C}^\sigma/X$. Then $J^{1-\sigma}$ has the form θi_K for some $\theta \in K^\times$ and i an ideal of k; we write i_K for the extension of i to K, to avoid any confusion. The class of J in $\bar{C}^\sigma/X$ is determined by $J^{1-\sigma}$. Then $(N\theta) = i^{-m}$ so that $N\theta$ defines a class of ν_{norm}. Reversing this reasoning gives the second map of (32): given $\theta \in K^\times$ such that $N\theta \in \nu_{\mathrm{norm}}$ we may write $(N\theta) = i^{-m}$ for some k-ideal i, the norm of the ideal $\theta \cdot i_K$ equals (1), and so $(\theta) \cdot i_K = J^{1-\sigma}$; this J is uniquely specified up to extensions of ideals from k times various $\widetilde{\wp}_i$, and changing the choice of θ with a given norm in ν_{norm} modifies J through principal ideals. Finally, the class of J is trivial in $\bar{C}/X$ if and only if $(\theta) \cdot i_K = (Z)^{1-\sigma}$ for some $Z \in K^\times$. But then $i_K = (Z^{1-\sigma}\theta^{-1})$, and so $\delta(i)^{-1}$ equals the class of $N\theta$, proving exactness at the middle.

We now put together the the formula (20) for the size of X, and the sequence (32) that expresses the difference between X and $(\bar{C})^\sigma$, to prove (30). Indeed the order of $[\nu_{\mathrm{norm}} : NU]$

is, by (32), the product of the order of $\ker(c \to C)$, and the order of $\frac{(\bar{C})^\sigma}{X}$; we multiply this by the equality $\#m^{-1}\ker(c \to C) = \#X \cdot \frac{[u:NU]}{\prod e_i}$ of (20) to get

$$m^{-1}[\nu_{\text{norm}} : NU] = \#(\bar{C})^\sigma \frac{[u : NU]}{\prod e_i},$$

Note that the short exact sequence $u/m \to \nu \to c[m]$ permits us to rewrite

$$[\nu_{\text{norm}} : NU] = \frac{[u : NU] \cdot \#c[m]}{[\nu : \nu_{\text{norm}}]},$$

and substituting this into the prior equation yields (30) upon rearrangement. □

7. Proof of existence for cyclic ℓ-extensions when $\zeta_\ell \in k$

We now come to what I regard as the core of the whole matter: the existence of a class field for $c_0 \leqslant c$ when $\zeta_\ell \in k$ and c/c_0 has order ℓ.

Our presentation broadly follows Fürtwangler [2], in particular, the essential ideas of using the *relative* class group and using *auxiliary primes*. Both ideas are in fact deployed in Hilbert's paper [1] on relative quadratic extensions, although the relative class group, for Hilbert, plays a rather minor role. Takagi's treatment, when specialized to the unramified case, also uses auxiliary primes, but as noted avoids the use of the relative class group, working instead with class groups with modulus.

7.1. **Why existence is hard.** It is important to understand why this is difficult. Cyclic ℓ-extensions K/k, have, by "Kummer theory", the form $k(x^{1/\ell})$ for $x \in k^\times$, where x only matters modulo ℓth powers.[9]

For $k(x^{1/\ell})/k$ to be unramified the valuation of x must be divisible at ℓ for every prime, i.e. x defines a class in the $\mathbf{F}_\ell$-vector space ν defined in (28) (taking $m = \ell$). However, unramifiedness is a yet stronger condition at primes dividing ℓ; it imposes constraints whose number exceed, in general, the dimension of ν. From this point of view it is a miracle that unramified extensions exist.

For example take $k = \mathbf{Q}(\sqrt{-5})$, with ring of integers $\mathfrak{o} = \mathbf{Z}[\sqrt{-5}]$, and class number 2. It must have an unramified quadratic extension, necessarily of the form $k(\sqrt{x})$; if x is prime-to-2, the condition that this be unramified at 2 will amount to imposing two *two* linear constraints on the reduction

$$\bar{x} \in \frac{(\mathfrak{o}/8\mathfrak{o})^\times}{\text{squares}} \simeq \mathbf{F}_2^3.$$

Now, ν is two-dimensional here, represented by the set $\{\pm 1, \pm 2\}$. That k admits an unramified extension, then, arises from the *a priori* surprising fact that the two linear constraints mentioned above become linearly dependent when pulled back to ν.

The key point of the argument may be expressed as

> seek to construct *class fields* not *unramified extensions*.

We saw in the previous section that unramified cyclic extensions are class fields; but – just as we saw in the case of c trivial – the same argument gives information in the ramified case too, so long as (31) holds – in words, if ramification is accompanied by a failure of all elements of ν to be norms.

[9] To say it explicitly we simply construct x as the ℓth power of any nonvanishing Lagrange resolvent $\sum_{i=0}^{\ell-1}(\sigma\zeta)^i\alpha$ for $\alpha \in K$.

In what follows, we will first (§7.2) study more carefully the constraints imposed by being unramified at primes above ℓ. We will then, in §7.3, introduce a specific type of ramification that forces (31), generalizing what we sketched in §5.2 in the unramified case. Allowing such ramification reduces the number of constraints in the above argument exactly to the point that such extensions always exist (§7.4); the rigidity of the notion of class field then miraculously shows, after the fact, that the resulting extensions are unramified.

7.2. **Ramification above ℓ.** Let us examine the condition that $k(x^{1/\ell})$ be unramified at a prime divisor λ of ℓ, where x is prime to λ. In what follows, "valuation" means 'valuation at λ," i.e. the highest power of λ dividing a given element. It will be denoted by v_λ.

Let e, f be the (absolute) ramification index and residue field index of λ and let

$$e_0 = \frac{e}{\ell - 1}; N = e_0\ell + 1.$$

Equivalently, e_0 is the valuation of $1 - \zeta$ at λ, or equivalently the ramification index of λ in the extension $k/\mathbf{Q}(\zeta_\ell)$.

We prove the following three assertions which say that $k(x^{1/\ell})$ can be forced to be unramified at λ by imposing ef constraints modulo ℓ.

(a) The quotient $\overline{G_\lambda}$ of $G_\lambda := (\mathfrak{o}/\lambda^N)^\times$ by ℓth powers has order ℓ^{ef+1}.
(b) The map $\lambda^{N-1}/\lambda^N \to \overline{G_\lambda}$ sending y to $1 + y$ has image of order ℓ.
(c) If $x \in k^\times$ is prime to λ, and its reduction $\bar{x} \in \overline{G_\lambda}$ is nontrivial and belongs to the image described in (b), then $k(x^{1/\ell})$ is unramified at λ.

Actually, all we need from (b) and (c) is that k admits *some* unramified-above-ℓ extension. A modern argument for (b) and (c) might start by producing an unramified extension of the completion k_λ of k at λ, writing it as $k_\lambda(y^{1/\ell})$, and then approximating y by an element $x \in k^\times$; a modern argument for (a) using Haar measure can be found in §C.1.

Proof. For (a): as usual (see (1)) this quotient has the same size as the number of ℓ-torsion elements in G_λ. We claim that this ℓ-torsion are just those classes congruent to some (necessarily unique) power of ζ modulo λ^{N-e}, from where elementary counting gives (a). To prove the claim, observe the factorization

$$t^\ell - 1 = \prod (t - \zeta^i).$$

Let x be an integer of k representing an ℓ-torsion class in G_λ, let m be the largest valuation of any $x - \zeta^i$, and suppose it is achieved when $i = i_0$. Then the valuation of $x^\ell - 1 = \prod (x - \zeta^i)$ is, on the one hand, at most $\ell \cdot m$, and so $m \geq \frac{N}{\ell} > e_0$. But, on the other hand, the valuation of $\zeta^i - \zeta^j$ for $i \neq j$ is precisely equal to e_0, so the valuation of $x - \zeta^i$ for $i \neq i_0$ is also equal to e_0, and so

$$m + (\ell - 1)e_0 \geqslant N,$$

which gives $m \geqslant N - e$.

Now we pass to (b). If, for some $y \in \lambda^{N-1} = \lambda^{\ell e_0}$, the element $1 + y$ is an ℓth power inside G_λ, some pleasant moments spent with the binomial formula shows that it must actually be of the form $(1 + y')^\ell$ with $y' \in \lambda^{e_0}$, and more specifically it lies in the image of the composite map

$$\frac{\lambda^{e_0}}{\lambda^{e_0+1}} \longrightarrow \frac{\lambda^{N-1}}{\lambda^N} \overset{t \mapsto 1+t}{\hookrightarrow} (\mathfrak{o}/\lambda^N)^\times,$$

where the first map is $z \mapsto \ell z + z^\ell$. The first and second groups above are $\mathfrak{o}/\lambda$-vector spaces of dimension 1, and with respect to the basis $(1-\zeta)$ for the first group and $\ell(1-\zeta)$ for the second, the first map becomes $v \mapsto v - v^\ell$. This map, on any finite field of characteristic ℓ, always has kernel the prime field, so its image always has index of size ℓ. This proves (b).

Finally, to prove (c), note that x is congruent to 1 modulo λ^{N-1}, i.e. modulo $\lambda^{\ell \cdot e_0}$. We claim that

$$x' := \frac{x^{1/\ell} - 1}{1-\zeta}$$

is in fact an element of $k(x^{1/\ell})$ that is integral at all primes above λ. To see this, we compute, again with the binomial formula, that $x^{1/\ell}$ is congruent to 1 modulo λ^{e_0}, but the valuation of $1-\zeta$ at λ is also equal to e_0.

We may therefore choose a prime-to-λ element $\eta \in \mathfrak{o}$ such that $x'' := \eta x'$ is actually an algebraic integer. Now we just observe that the conjugates of x'' over k are pairwise distinct modulo any prime above λ: their differences have the form $\eta x^{1/\ell} \frac{\zeta^a - \zeta^b}{1-\zeta}$. It follows from this that the discriminant over $\mathfrak{o}$ of the k'-order $\mathfrak{o}[x'']$ is not divisible by any prime above λ, as required. □

7.3. **Auxiliary primes.** Here is our tool to control the image of the norm (cf. discussion around (23)):

> *Fact:* if K/k is a cyclic ℓ-extension and $\mathfrak{p}$ is a ramified prime, then the norm of any prime-to-$\mathfrak{p}$ integer of K must in fact be an ℓth power modulo $\mathfrak{p}$.

Motivated by this, let us say that a set of primes P, none of which lie above ℓ, is *auxiliary* if the map

$$\nu \longrightarrow \prod_{\mathfrak{p} \in P} k(\mathfrak{p})^\times / \ell \simeq (\mathbf{Z}/\ell)^P \tag{33}$$

arising from reduction modulo $\mathfrak{p}$ is an isomorphism. Here ν is as in (28), and we wrote $k(\mathfrak{p})$ for the residue field; its order is divisible by ℓ since $\mathfrak{p}$ doesn't divide ℓ and $\zeta_\ell \in k$. Also note that the reduction of an element of ν mod $\mathfrak{p}$ makes sense modulo ℓth powers, just by choosing a representative that is a unit at $\mathfrak{p}$. Clearly a set of auxiliary primes has size equal to the dimension q of ν as a $\mathbf{Z}/\ell$-vector space.

(i) auxiliary sets of primes P exist, and can be chosen disjoint to any given finite set of primes, and
(ii) A cyclic degree-ℓ extension unramified outside P is then a class field.

Assertion (ii) follows from the sufficiency criterion (31) to be a class field: if K/k ramifies at precisely the auxiliary primes $\mathfrak{p}_1, \dots, \mathfrak{p}_t$ then the map $\nu \to (\mathbf{Z}/\ell)^t$ from reducing modulo these primes is trivial on ν_{norm} but also surjective, so $[\nu : \nu_{\text{norm}}] \geq \ell^t$.

For (i) fix a basis $\varepsilon_1, \dots, \varepsilon_q$ for ν over $\mathbf{F}_\ell$, and skillfully apply (5) to various subfields of $k(\varepsilon_1^{1/\ell}, \dots, \varepsilon_q^{1/\ell})$: first take $\mathfrak{p}_1$ nonsplit in $k_1 := k(\varepsilon_1^{1/\ell})$, then take $\mathfrak{p}_2$ below any degree one prime of k_1 that is nonsplit in $k_1(\varepsilon_2^{1/\ell})$, and so on. These will have the property that, for $i \leq j$

$$\varepsilon_i \text{ is not an } \ell\text{th power mod } \mathfrak{p}_j \iff i = j. \tag{34}$$

which means the map (33) is represented by an upper triangular matrix with nonzero diagonal entries, and so has nonzero determinant.

7.4. **Proof of existence of an unramified class field when $\zeta_\ell \in k$, for c_0 of index ℓ.** Fix an auxiliary set of primes P. We will construct many cyclic ℓ-extensions K/k unramified outside of P. We carry out the proof for ℓ odd, which forces k totally imaginary, and then indicate the modifications when $\ell = 2$.

Let h be the rank of $c[\ell]$. From (29) we deduce that the rank of ν equals $h + \mathsf{r}_\infty$, so that the size of P also equals $h+\mathsf{r}_\infty$. Then, by the unit theorem, the group $[P]$ of P-units modulo ℓth powers is a $\mathbf{F}_l$-vector space of rank $h + 2\mathsf{r}_\infty = h + [k : \mathbf{Q}]$. (The free part of this group has rank $h + 2\mathsf{r}_\infty - 1$, but the ℓth roots of unity contribute an extra $+1$.)

The desired extensions will be taken to be of the form $K = k(x^{1/\ell})$ for x a P-unit; these are automatically ramified only at primes in P or over ℓ. It follows from §7.2 that, for λ dividing ℓ, the condition of being unramified at λ can be guaranteed by enforcing $e_\lambda f_\lambda$ linear constraints on the class of a nontrivial $x \in [P]$. These constraints arise by imposing that the image of x under the natural map $[P] \to \overline{G}_\lambda$ (notation of §7.2) lies within the one-dimensional $\mathbf{F}_\ell$-subspace specified in (b) of §7.2.

Being unramified at *all* primes above ℓ is ensured by a system of

$$\sum_{\lambda|\ell} e_\lambda f_\lambda = [k : \mathbf{Q}]$$

constraints on a class $x \in [P]$. The subspace satisfying all these constraints is thereby h'-dimensional, where $h' \geq h$, and this gives rise to exactly M different cyclic extensions $K_1, \ldots, K_M$ unramified outside P, where $M = \frac{\ell^{h'}-1}{\ell-1}$ is the number of lines inside an h'-dimensional vector space over $\mathbf{Z}/\ell$. Each such K_i is automatically a class field, as we have seen, and so corresponds to an index-ℓ subgroup of norms inside c, and since these subgroups are all distinct we see that see that $h' \leq h$, so $h' = h$ and moreover the map

$$K_i \mapsto \text{subgroup of } c \text{ of norms of ideal classes from } K_i$$

is a bijection onto the set of index-ℓ subgroups of c. In particular, for any $c_0 \leqslant c$ we have produced a class field attached to c_0 and unramified outside P; choosing a disjoint P shows that $K(c_0)$ is unramified; done (!!)

7.5. **Modifications for $\ell = 2$.** We leave the reader to check the details, but the numerology is modified as follows. Let r be the number of real places; the rank of P-units is now $h + 2\mathsf{r}_\infty = h + [k : \mathbf{Q}] + r$; however, in addition to the $[k : \mathbf{Q}]$ constraints arising from primes $v|2$ exactly as in the above argument, we have a further r constraints arising from the necessity of x being totally positive, so that $k(\sqrt{x})$ is also unramified at the archimdean places.

8. Mopping up; conclusion of the proof

We conclude the proof of the target theorem. The hard work is done; the arguments are now quite routine, building general abelian extensions from cyclic ones using the remarkable rigidity of the concept of class field.

8.1. **Proof of existence of unramified class fields for general k, when c_0 has index ℓ, by "descent."** This has already been proved when k contains ζ_ℓ; so we can suppose ℓ is odd. Let $k' = k(\zeta_\ell)$, so k'/k is cyclic of degree less than ℓ, and consider a subgroup $c_0 \leqslant c$ of index ℓ. Let $c_0' \leqslant c'$ be its preimage under the norm map from k' to k. This norm map is surjective on ℓ-primary parts, because its pre-composition with the inclusion $c \to c'$ equals

multiplication by $[k' : k]$, which is prime to ℓ. In particular, c'_0 also has index ℓ inside c'. By what we have already proved, there is a class field K'/k' for c'_0.

Now, K' is Galois over k, because it is uniquely specified by c'_0, and c'_0 is invariant by the Galois group of k'/k (since the norm $c' \to c$ is invariant by that Galois group). One might worry that K'/k is not abelian; but we show its Galois group is *cyclic*, by exhibiting a prime $\mathfrak{p}$ of k that remains inert in K'; the Frobenius element $\left(\frac{K'/k}{\mathfrak{p}}\right)$ for such $\mathfrak{p}$ then generates $\mathrm{Gal}(K'/k)$.

Choose $\mathfrak{p}$ in such a way that:

(a) its Frobenius class generates $\mathrm{Gal}(k'/k)$ and
(b) its ideal class doesn't lie in c_0.

This is possible: by §2.2, the complement to (b) has upper density *at most* ℓ^{-1}, but that is less than the density of primes satisfying (a) (by §2.1, it is $\geq \frac{1}{[k':k]}$). But the first property means that $\mathfrak{p}$ remains inert in k', and the second means that the unique prime ideal $\mathfrak{p}'$ above $\mathfrak{p}$ doesn't lie inside c'_0; if it did, its norm $\mathfrak{p}^{[k':k]}$ lies in c_0, and so also $\mathfrak{p} \in c_0$ since $[k' : k]$ is prime to $\ell = [c : c_0]$, contradicting (b). Thus, since split primes must always have ideal class that is a norm (see (2)), $\mathfrak{p}'$ remains inert in K'.

The cyclic extension K'/k of degree $\ell \cdot [k' : k]$ therefore admits a unique cyclic subextension K/k of degree ℓ over k. This K/k is unramified: It is automatically unramified at archimedean places, for ℓ is odd; and the ramification index of any prime in K/k divides ℓ, but it also divides the ramification index of the same prime in K'/k, which itself is a divisor of $\ell - 1$. Therefore, K/k is a class field, by what we proved in §6.2.

To show that K/k is the class field attached to c_0, it is enough to show that c_0 is contained in the image of the norm map from the class group of K to the class group of k. That image automatically contains all the prime-to-ℓ torsion in c, because the composite $c \to C \to c$ is multiplication by ℓ. It also contains the image of the norm $C' \to c$ associated to K'/k; this contains, in particular, the image of c'_0 by the norm, which, as already noted, includes all ℓ-power torsion in c_0. Thus the ideal class norm from K to k contains c_0 in its image, as required.

8.2. **Existence of unramified class fields for general k and c/c_0 cyclic.** By induction, let us show the existence of unramified cyclic class fields for all number fields k and for all c/c_0 cyclic of size ℓ^n, when we have proved the same assertion with n replaced by any smaller number. We have already dealt with $n = 1$, so let us suppose $n \geq 2$. Then, for such c_0, there are unique subgroups c_1, c_2

$$c_0 \overset{\ell}{\subset} c_1 \subset c_2 \overset{\ell}{\subset} c$$

where the superscripts denote indices. Let $k' = k(c_1)$ be the class field degree ℓ^{n-1} attached to c_1. Its class group surjects by the norm onto c_1; so the preimage of c_0 thereby defines an index ℓ subgroup $c'_0 \leqslant c'$, to which is again attached a class field K'/k' of degree ℓ; this K' has degree ℓ^n over k, and it is Galois by the same argument as in §8.1. Also K' is unramified over k, for K'/k' and k'/k are both unramified. The norm of the class group of K' equals exactly c_0. Finally, K'/k is actually cyclic by a variant of the argument of §8.1, as we now explain:

If $\mathfrak{p}$ is a prime of k whose ideal class lies outside c_2 then it is necessarily inert in k'. Indeed, it is inert in the class field for c_2, and so the Frobenius class $\left(\frac{k(c_2)/k}{\mathfrak{p}}\right)$ is nontrivial. But $k(c_2)$ is the unique $\mathbf{Z}/\ell$-subextension of k'/k, by the Example of §2.3, and so we also see that

$\left(\frac{k'/k}{\mathfrak{p}}\right)$ generates the cyclic Galois group $\mathrm{Gal}(k'/k)$. Therefore, the unique prime ideal $\mathfrak{p}'$ of k' above $\mathfrak{p}$ has norm equal to $\mathfrak{p}^{[c:c_1]}$ which does not lie inside c_0; so $\mathfrak{p}'$ does not lie inside c_0' and thus remains inert in K' ((2) again). Therefore $\mathfrak{p}$ is inert inside K', and so K'/k is cyclic.

8.3. **Existence of unramified class fields, no restrictions.** For general c_0, we just choose a direct product decomposition of c/c_0:

$$c/c_0 \simeq \prod(\mathbf{Z}/d_i)$$

where each d_i is a prime power. Let $c_1, \dots, c_r$ be subgroups of c correspond to the kernels of the various projections to the factors, and let $K(c_i)$ be the associated class fields. Then the abelian extension

$$K = K(c_1) \dots K(c_r)$$

of k is a class field. Indeed, norms of ideal classes from K are certainly norms from each $K(c_i)$, so the subgroup of norms is contained in $\bigcap c_i = c_0$, and thus for this K we have $[c : NC] \geq [c : c_0]$. But the degree $[K : k]$ is at most the product of the degrees of the $K(c_i)$, which is precisely $[c : c_0]$; equality must hold everywhere, and K is the class field for c_0.

8.4. **Every unramified abelian extension is a class field.** In the converse direction, if K^*/k is unramified abelian, we write its Galois group

$$\mathrm{Gal}(K^*/k) \simeq \prod(\mathbf{Z}/d_i)$$

as a product of cyclic groups of prime power order d_i, and fix a corresponding decomposition of the field $K^* = K_1 \dots K_r$ where K_i/k is cyclic of degree d_i. Each K_i/k is a class field, by what we have already proved in §6.2, attached to some $c_i \leqslant c$; let c' be their intersection. Its index $[c : c']$ is at most $\prod[c : c_i]$.

The class field K' attached to c' contains each K_i, because $c' \leqslant c_i$, and so it contains K^*. But then

$$[K' : k] \geq [K^* : k] = \prod d_i = \prod [c : c_i] \geq [c : c'] = [K' : k]$$

and so equality holds everywhere; and $K' = K^*$ is the class field for c^*.

Appendix A. Takagi's treatment of the ramified case

We are not going to give a full treatment of the ramified case here, primarily because formulating the *statement* would take us too far afield of our main goal. However, its *proof* requires very little beyond what we have already done. To emphasize this, we explain how to extend the crucial equality $[c : NC] = [K : k]$ to the ramified case, and give an example to see how it is used.

We hope that, after reading this section, the motivated reader who is familiar with the statement of ramified class field theory (that is, existence and uniqueness) will be able to fill in the remaining details.

A.1. **Generalized class groups attached to K/k.** Let K/k be a cyclic degree m extension, possibly ramified, of discriminant $\mathfrak{d}$. The norm map $N : C \to c$ actually lifts to a bigger target than c, because, if α is an integer of K, its norm satisfies certain extra congruence constraints; we already exploited this in our earlier proofs.

To formalize this, let $\mathfrak{D} = \mathfrak{d}^N$ be a large enough power of $\mathfrak{d}$.[10] We say that a prime-to-$\mathfrak{d}$ integer $\alpha \in \mathfrak{o}_K$ is a *local norm* if:

- there is a prime-to-$\mathfrak{d}$ integer Y of K such that $\alpha \equiv NY$ modulo $\mathfrak{D}$;
- α is a norm at each archimedean place; that is to say, α is positive at each real place of k above which all places of K are complex.

Let $\tilde{c}_{(K)}$ be the following generalized class group for k:

$$\tilde{c}_{(K)} = \frac{\text{prime-to-}\mathfrak{d}\text{ fractional ideals in } k}{\text{subgroup generated by all } (\alpha) \text{ for } \alpha \text{ a local norm}}.$$

The natural map $\tilde{c}_{(K)} \to c$ is surjective. This $\tilde{c}_{(K)}$ is a "generalized class group" *for* k; the subscript K reminds us that the notion of local norm depends on K. Thus, for example, if we take $K = \mathbf{Q}(i)$ and $k = \mathbf{Q}$, the group $\tilde{c}_{(K)}$ is

$$\frac{\text{prime-to-2 fractional ideals of } \mathbf{Q}}{\text{subgroup generated by } (m) \text{ with } m \equiv 1 \ (4) \text{ and positive}}$$

which is a group of order 2; a fractional ideal (x) represents a nontrivial class exactly when $x \equiv 3$ modulo 4.

Then one readily verifies that the norm $C \to c$ lifts to a norm $C \to \tilde{c}_{(K)}$. Following Takagi, we will prove the following crucial index equality:

$$\text{the index of } NC \text{ in } \tilde{c}_{(K)} \text{ is precisely } m. \tag{35}$$

The analytical argument of §2 generalizes almost verbatim to show that $[\tilde{c}_{(K)} : NC] \leq m$. So it sufficies to show the reverse inequality.

A.2. **Proof that $[\tilde{c}_K : NC] \geq m$.** For simplicity, we suppose that K/k is unramified at ∞, leaving the easy modifications to the reader. We abridge $\tilde{c}_{(K)}$ to $\tilde{c}$ since there is no possibility of confusion. We proceed as usual: NC is at most the size of C^σ, and the ambiguous class number formula (26) shows that this equals $\frac{\#c \cdot \prod e_i}{m} \frac{1}{[u : u \cap NK^\times]}$. So it is enough to show that this is at most $\frac{\#\tilde{c}}{m}$, or equivalently

$$\#\frac{\tilde{c}}{c} \geq \frac{\prod e_i}{[u : u \cap NK^\times]}. \tag{36}$$

We now need the purely local computation about the congruence behavior of norms:

Local norm index: The quotient Q of $(\mathfrak{o}/\mathfrak{D})^\times$ by norms has order $\prod e_i$.

Here "norms" means the subgroup generated by local norms, or, what is the same, the image of the norm from $(\mathfrak{o}_K/\mathfrak{D})^\times \to (\mathfrak{o}/\mathfrak{D})^\times$ restricted to invertible elements.

This computation of the local norm index might be considered part of local class field theory. Takagi's proof is an entirely elementary computation which we will not reproduce;

[10] The definitions that follow will not depend on N so long as it is chosen large enough; it suffices to take it so large that every element congruent to 1 modulo $\mathfrak{d}^N$ is in fact an mth power modulo $\mathfrak{d}^{N'}$ whenever $N' > N$.

however we will give a proof using Haar measures in §C.4.2 of the Appendix. Assuming it, we conclude the proof of (35). We easily see that

$$\ker(\tilde{c} \to c) \simeq \frac{Q}{\text{image of units in } Q}. \tag{37}$$

We claim that the image of u inside Q has size at most $[u : u \cap NK^\times]$; and then (36) will follow. For this it is enough to show that the reduction map $u \to Q$ is trivial on $u \cap NK^\times$. This is not quite trivial because Q is obtained by only killing the norms of prime-to-$\mathfrak{D}$ elements, so we must see that any element of $u \cap NK^\times$ arises thus. Suppose then that $Y \in K^\times$ has unit norm $N(Y) \in u$. Now, as in (24), the ideal (Y) has the form $J^{1-\sigma}$ for some fractional ideal J; choose an element $Z \in K^\times$ such that $(Z)J$ is prime-to-$\mathfrak{d}$. Then $YZ^{1-\sigma}$ also has norm $N(Y)$ but is now integral at $\mathfrak{D}$ because it generates the ideal $((Z).J)^{1-\sigma}$. Thus $N(Y)$ is the norm of a prime-to-$\mathfrak{D}$ element of K, as desired.

A.3. **Existence and uniqueness: ramified case.** With (35) in hand, *our entire proof from §7 and §8 now goes through.* It establishes, now, a bijective correspondence between finite abelian extensions K/k and finite index subgroups of a generalized class group c, which can be taken to be the inverse limit of all class groups with modulus, or, alternately, the idele class group of k.

We simply see how to redo the existence proof in the unramified case that we gave in §7. We leave to the reader the task of generalizing this to the ramified case; once this is done, the argument of §8 goes over to the general case.

We suppose that ℓ is odd and $\zeta_\ell \in k$. We choose a set of auxiliary primes P as before and construct, using the same argument as before, at least $\frac{\ell^h-1}{\ell-1}$ fields K/k ramified only in P (and automatically unramified at ∞). We claim that for all these K the map

$$\tilde{c}_{(K)}/\ell \to c/\ell \tag{38}$$

is an isomorphism. Once this is so, the norm of C inside $\tilde{c}_{(K)}/\ell$, which has index ℓ by (35), is in fact pulled back from a subgroup of c/ℓ of index ℓ, and then the same counting arguments as before put the various K in bijection with index ℓ subgroups of c.

To verify (38), it is enough to show that the map is injective. So, choose a class a prime-to-$\mathfrak{d}$ ideal J that represents a class in the kernel of $\tilde{c}_{(K)} \to c/\ell$. This means that there exists $y \in k^\times$ such that

$$J.(y) = \text{ the } \ell\text{th power of an ideal,}$$

and we easily see that we may suppose that y is also prime to $\mathfrak{d}$. But – by the definition of a set of auxiliary primes, see (33) – there exists another $z \in k^\times$ such that

$$(z) = \text{ the } \ell\text{th power of an ideal, and } \frac{z}{y} \equiv \text{an } \ell\text{th power, modulo } \mathfrak{D}.$$

Then z/y modulo $\mathfrak{D}$ is a local norm from K, and then J and $J.(y/z)$ represent the same class inside $\tilde{c}_{(K)}$. However, by choice of z, $J.(y/z)$ is an ℓth power of another ideal. That shows that J is an ℓth power within $\tilde{c}_{(K)}$ as desired. This concludes the proof that (38) is injective, and so it is an isomorphism as claimed.

Appendix B. That zero density set, and the reciprocity law

We will see how to remove the zero density set of exceptions in the target theorem in a special case (following Takagi's technique) and then, with this as motivation, go on to discuss

Artin reciprocity (§B.2). As in Appendix §A, we do not give complete statements, let alone complete proofs - just examples. Again, hopefully, the motivated reader who is familiar with the statement of reciprocity will be able to fill in the proof for themselves after reading this.

B.1. **Eliminating the zero density set by means of auxiliary fields.** Suppose that we know the target theorem is valid for k, with class group $c \simeq (\mathbf{Z}/\ell)^2$. Let c_0 be the subgroup $(\star, 0)$ and c_1 be the subgroup $(0, \star)$ with associated class fields K_0 and K_1.

Let $\mathfrak{p}$ be a prime ideal of k. We already have seen that, if $\mathfrak{p}$ splits in K_0, then the ideal class of $\mathfrak{p}$ belongs to c_0. We will prove the converse under the auxiliary condition that the class of $\mathfrak{p}$ *does not belong to to* c_1.

The field generated by K_0, K_1 is the class field attached to the trivial subgroup of c, and it has Galois group $(\mathbf{Z}/\ell)^2$. Suppose $\mathfrak{p}$ does not split in K_0. By assumption it does not split in K_1, and so its Frobenius element in $K_0 \cdot K_1$ then has the form $(a, b) \in (\mathbf{Z}/\ell)^2$ with a, b both nonzero. The fixed field for this element gives the unique degree ℓ subextension H of $K_0 \cdot K_1$ in which $\mathfrak{p}$ splits. Then the ideal class $[\mathfrak{p}]$ of $\mathfrak{p}$ belongs to the associated subgroup $c_H \leqslant c$, which is distinct from c_0, c_1. If $[\mathfrak{p}] \in c_0$, then it would belong to $c_0 \cap c_H$ and thus be trivial, contradicting the assumption that $[\mathfrak{p}] \notin c_1$. Therefore $[\mathfrak{p}] \notin c_0$, as required.

There are two lessons we can draw from this argument:

(a) we can eliminate the zero density set for K_0/k by means of an *auxiliary* class field K_1 with suitable properties.
(b) To study a given $\mathbf{Z}/\ell$-extension, it is useful to enlarge it to a $(\mathbf{Z}/\ell)^2$-extension.

An auxiliary field as in (a) can be manufactured in great generality once one has access to ramified class field theory. To put it differently: of course, the class group of k need not be of the form $(\mathbf{Z}/\ell)^2$, but the generalized class groups that control ramified extensions have many quotients of the form $(\mathbf{Z}/\ell)^2$, which is all we need.

And we will apply the principle of (b) in a more powerful way in the next subsection.

B.2. **Reciprocity by means of auxiliary fields.** In later presentations, Artin's reciprocity law acquired a much more central role. But the target theorem is much closer than one might think to reciprocity in Artin's sense. Let us illustrate why the target theorem gives a"reciprocity law up to scalars" so long as the Galois group of K/k is complicated enough.

Suppose, then, that we know the theorem for k, and we have an unramified Galois extension K/k with Galois group $G = (\mathbf{Z}/\ell)^m$. It corresponds to some $c_0 \leqslant c$, and the main theorem asserts that we have an inclusion-preserving bijection between subgroups of c/c_0 and of G. But such bijections are not easy to come by if m is large! Indeed, the *fundamental theorem of projective geometry*, appled over the field $\mathbf{Z}/\ell$, says that, if $m \geq 3$, any such bijection is induced by an *isomorphism*

$$\varphi : c/c_0 \simeq G$$

itself unique up to scalars.[11] So we get, "for free" – by which we mean, without using specifics of number theory – an upgrade from a bijection between subgroups, to an isomorphism of groups. Moreover, the splitting properties of class fields yields

$$\varphi\,(\text{ideal class of } \mathfrak{p}) = a(\mathfrak{p}) \left(\frac{K/k}{\mathfrak{p}}\right) \tag{39}$$

[11]More precisely, the fundamental theorem of projective geometry implies this if one knows *a priori* that c/c_0 is isomorphic to G. That fact actually comes out in the proof of the target theorem, but it can also be deduced from the fact that there is an inclusion-preserving bijection of subgroups.

for some scalar $a(\mathfrak{p}) \in \mathbf{F}_\ell$, possibly dependent on $\mathfrak{p}$. Indeed, a quotient of the Galois group kills the Frobenius element if and only if $\mathfrak{p}$ splits in the associated extension, which forces the class of $\mathfrak{p}$ to be trivial in the associated quotient of c; thus any subgroup containing the Frobenius element also contains the left side. This implies (39).

Artin's reciprocity law is precisely the additional assertion that the scalar $a(\mathfrak{p})$ is independent of $\mathfrak{p}$. Thus, at least in the case above, the existence and uniqueness theorem can be seen as a "reciprocity law up to scalars." Given the statement of *ramified* class field theory, it is easy to enlarge an arbitrary K/k by composition with an auxiliary cyclotomic E/k to a larger $\widetilde{K} = K \cdot E$ for which some version of the above argument applies (cf. §A) , and pin down the scalar ambiguity simply by checking it by hand in $\mathrm{Gal}(E/k)$.

For the reader familiar with the statements of ramified class field theory who is interested in implementing this sketch in full, a suitable generalization of the fundamental theorem of projective geometry is the following statement, due to Baer [9, (3), page 4]: if G has the form

$$(\mathbf{Z}/\ell^a)^3 \times \text{a group killed by } \ell^a$$

for $a \geq 2$, then any automorphism of the subgroup lattice of G comes from an automorphism of G; the same is true for any product of such groups. The resulting argument is functionally equivalent to Artin's original proof, but using Baer's results separates the purely algebraic argument from the arithmetic part.

Appendix C. Index computations via Haar measure

To conclude, I will explain an approach to index computations that, on the one hand, uses some of the modern abstract language (local fields, idèles), but proceeds in a way that is quite parallel to the concrete arguments we have presented. This technique is a more analytic manifestation of the same ideas that find algebraic expression through the theory of the Herbrand quotient.

One can then give a proof of the uniqueness and existence theorems (in the ramified case) along the lines of the present paper by, first of all, replacing c by the idèle class group, and then substituting the present section §C for §4, 5 and 6.

The starting point is that any locally compact topological group admits a Haar measure, unique up to scaling.[12] The basic strategy of §3 can thereby be adapted to settings when C is replaced by various locally compact groups G, using "volume" (Haar measure) for "size." By applying this technique to various choices of G we will recover in a smooth way several results of the main text. This includes, in particular, the lower bound on the norm index for the idèle class group which we discussed in §A.

The resulting proof is in a certain sense a genuine simplification of the one we gave before, because the complexities of the computations with units in §5.1 and the computations with the class group in §6.3 exactly cancel each other. This point is worth emphasizing, since frequently idèles and adèles in number theory serve solely as a linguistic device to abridge computations that can equivalently be done at any fixed finite "modulus."

C.1. **Stretching.** To warm up in using Haar measures for index computations, let us reprove (a) of §7.2, in the following form: For E a local field, the index of ℓth powers of local units

[12]Note that for all the groups we consider are built from finite groups and the real line, and the existence and uniqueness of Haar measure can be checked by hand, or even by mind.

$(\mathfrak{o}_E^\times)^\ell$ inside the local units $\mathfrak{o}_E^\times$ equals

$$|\ell|_E^{-1} \cdot w, \tag{40}$$

where w is the number of ℓth roots of unity in E. Here, $|\ell|_E$ is the normalized absolute value, that is, the amount by which $x \mapsto \ell x$ scales Haar measure on the *additive group* $(E, +)$.

Our proof of (40) will be informal, and we leave to the reader the task of rewriting it in more formal terms. Firstly, the multiplicative and additive groups are locally isomorphic, by means of the exponential map. This shows that $x \mapsto x^\ell$ *locally* "stretches" measure on $\mathfrak{o}_E^\times$ by the same factor $|\ell|_E$. On the other hand, the map $x \mapsto x^\ell$ is not injective in general; its fibers all have size w. Therefore, the volume of ℓth powers of units equals the volume of all units, multiplied by $|\ell|_E/w$. This implies (40).

C.2. **The basic strategy.** Now let G be a locally compact abelian group, and let σ be a continuous endomorphism of G satisfying $\sigma^m = 1$, for some integer m; the norm will now be the map $N : G \to G^\sigma$ defined by $N = 1 + S + \cdots + \sigma^{m-1}$. What we want to argue is that, by analogy with the finite case:

$$\mathrm{vol}(NG) \times \mathrm{vol}(\ker N) \stackrel{??}{=} \mathrm{vol}(G) \stackrel{??}{=} \mathrm{vol}(G^\sigma) \times \mathrm{vol}(G^{1-\sigma}) \tag{41}$$

for suitable notions of "volume." The problem here is that, unlike the case of finite groups, the notion of Haar measure here is only defined up to scaling, and we have to discuss how to pin down the scalar.

To investigate this, we must examine how Haar measure interacts with quotients. Consider

$$\pi : G \to \bar{G}$$

a surjective homomorphism of locally compact groups, with kernel H. We assume that π is an open map; then it induces a homeomorphism of G/H with $\bar{G}$, and this is automatic for $G, \bar{G}$ compact. Then a choice of Haar measure on any two of $H, G, \bar{G}$ determines a Haar measure on the other one, characterized by the compatibility rule

$$\int_{\bar{G}} \int_H f(\widetilde{g}h) dg \cdot dh = \int f(g) dg \tag{42}$$

for any $f \in C_c(G)$; here $\widetilde{g}$ is any preimage under π of an element $g \in \bar{G}$, or, more pedantically, we take $g \mapsto \widetilde{g}$ a measurable section of the projection $G \to \bar{G}$. This equality follows readily from the uniqueness of Haar measure: both sides define a translation-invariant functional on continuous functions of compact support.

We shall impose the following topological conditions on the situation, which we call condition (O):

$$N \text{ is an open map } G \to G^\sigma \text{ and } 1 - \sigma \text{ is an open map } G \to \ker(N). \tag{43}$$

Assume this is so. We fix Haar measures on $G^\sigma, G^{1-\sigma}$. Since $NG \subset G^\sigma$ is open, we get an induced Haar measure on it; since $\ker(N)$ contains $G^{1-\sigma}$ as an open subgroup, we get an induced Haar measure on it too. Now, applying (42) to the surjective homomorphism $1 - \sigma : G \to G^{1-\sigma}$ we get a measure μ_σ on G "compatible" with the chosen measures on $G^\sigma, G^{1-\sigma}$; similarly, applying (42) to $N : G \to NG$ we get a measure μ_N on G "compatible" with the chosen measures on $\ker(N), NG$. But these two measures need not coincide; by uniqueness of Haar measure up to scalar they differ by some positive scalar $\nu(G, \sigma)$:

$$\mu_\sigma = \nu(G, \sigma)\mu_N.$$

Note that $\nu(G,\sigma)$ does not depend on the choice of Haar measures. Note also that (O) was needed to make sense of $\nu(G,\sigma)$, and whenever we write $\nu(G,\sigma)$, we understand that (O) is valid.

Once we understand the constant $\nu(G,\sigma)$ we can proceed just as we do for finite groups. Note that, in the compact case, $[G^\sigma : NG]$ is automatically finite, and is equal to the ratio of Haar measures $\frac{\mathrm{vol}(G^\sigma)}{\mathrm{vol}(NG)}$ when they are normalized as above, as we see simply by choosing coset representatives and using invariance of the measure. The same remarks apply to $[\ker(N) : G^{1-\sigma}]$. Thus we find that for G compact

$$[G^\sigma : NG] = \nu(G,\sigma) \cdot [\ker(N) : G^{1-\sigma}], \tag{44}$$

To prove this, we just apply Fubini's theorem (42) to the constant function 1_G, which shows that (41) holds just as for finite groups, but with a factor of $\nu(G,\sigma)$ on the left.

C.3. **Evaluating $\nu(G,\sigma)$ by use of a local model.** Both (O) and the computation of $\nu(G,\sigma)$ will be handled in a similar way to the analysis after (40) – they are both *local* questions. Suppose, then, that there is a"local model" (G',σ') for (G,σ), that is, there exists a homomorphism

$$\varphi : G' \to G$$

which intertwines σ' and σ, and induces an isomorphism of a neighbourhood of the identity in G' with a neighbourhood of the identity in G. We will abridge this latter property by saying that φ is a "local isomorphism." We will prove that if the topological property (O) is true for one of (G,σ) and (G',σ'), it is also true for the other, and in that case,

$$\nu(G',\sigma') = \nu(G,\sigma). \tag{45}$$

Indeed, everything can be expressed just in terms of what happens in a small neighbourhood of the identity. To write out a proof is an uninspiring exercise in point-set topology, and we postpone it to §C.5.

A particularly important local model for us is the "shift": Take H a locally compact abelian group, and $G = H^m$ and σ to be the cyclic shift. Then $G^\sigma = NG$ is the diagonal copy of H, where $\ker(N) = G^{1-\sigma} \simeq G^{m-1}$ by means of projection to the first $m-1$ factors. Then (O) holds and a straightforward application of Fubini's theorem shows that

$$\nu(H^m, \text{cyclic shift}) = 1. \tag{46}$$

C.4. **Applications.**

C.4.1. Since most of our applications are to noncompact groups, we first formulate a variant of (44) that applies to our cases of interest. Suppose that G satisfies (O) and G admits a σ-invariant homomorphism to $\mathbf{R}^\times_{>0}$ with compact kernel; then we shall show that

$$[G^\sigma : NG] = m \cdot \nu(G,\sigma) \cdot [\ker(N) : G^{1-\sigma}]. \tag{47}$$

Note that this is almost the same formula as in the compact case but with an extra factor of m.

Proof. There are multiple ways to proceed. One is to replace G by a compact quotient group and apply (44) to it. [13] Let us proceed in a more analytical way.

[13]Choose $x \in G$ whose image in $\mathbf{R}_{>0}$ is larger than 1, and put $y = Nx$, so y is σ-invariant. Form the quotient $\bar{G} = G/y^{\mathbf{Z}}$ of G by the discrete subgroup generated by y. We leave further details to the reader.

Consider the set of g with $1 \leqslant |g| < X$; call its characteristic function f and its volume $\mathrm{vol}_X(G)$. Similarly define $\mathrm{vol}_X(G^\sigma)$ and $\mathrm{vol}_X(NG)$. We apply (42) to f, both with $H = G^\sigma$ and $H = \ker(N)$. We get the following version of (41):

$$\nu(G,\sigma)\mathrm{vol}_{X^m}(NG)\mathrm{vol}(\ker N) = \mathrm{vol}(G^{1-\sigma})\mathrm{vol}_X(G^\sigma).$$

Now (47) follows from this and the following observations:

- $\mathrm{vol}_{X^m}(NG) \sim m\mathrm{vol}_X(NG)$ as $X \to \infty$. This is easily deduced from (42); it is exactly true when the norm surjects onto the positive reals, but only asymptotically if its image is discrete.
- $\frac{\mathrm{vol}_X(G^\sigma)}{\mathrm{vol}_X(NG)} = [G^\sigma : NG]$; this follows again by choosing coset representatives and using invariance of Haar measure.

□

C.4.2. *Local fields.* Let us take $G = E^\times$, where E/F is a degree m cyclic extension of nonarchimedean characteristic zero local fields. Let σ generate the Galois group of E/F.

By the normal basis theorem, we may choose $x \in \mathfrak{o}_E$, the ring of integers of E, such that $x_i = \sigma^i x$ give a F-basis for E. Then consider the $\mathfrak{o}_F$-span W of the x_i, which, with addition as the group operation, defines a locally compact topological group. Clearly (W,σ) is isomorphic to $(\mathfrak{o}_F^m, \mathrm{shift})$. Also the exponential map $x \mapsto \exp(ax)$ for small a defines a local isomorphism $(W,\sigma) \to (G,\sigma)$. Therefore we have a local isomorphism from the "shift" to (G,σ), so $\nu(G,\sigma) = 1$ by §C.3. Then (47) shows

$$[F^\times : NE^\times] = m \cdot [\ker(N) : (E^\times)^{1-\sigma}] = m,$$

where we used Hilbert's Satz 90. This is the norm index computation from local class field theory. Now, the valuations of elements of norms from $E^\times$ are precisely those divisible by $\frac{m}{e}$, where e is the ramification index, so we get also

$$[\mathfrak{o}_F^\times : N\mathfrak{o}_E^\times] = e,$$

a statement that was used in §A. In particular, if $e = 1$, that is, if E/F is unramified, then

(48) the norm $\mathfrak{o}_E^\times \to \mathfrak{o}_F^\times$ is surjective with kernel the $(1-\sigma)$th powers.

C.4.3. *Idele class group.* Now we take G to be the idele class group $\mathbf{A}_K^\times/K^\times$, where K/k is a degree m cyclic extension of number fields. By Hilbert's Satz 90, $G^\sigma = \mathbf{A}_k^\times/k^\times$ is the idele class group for k.

For each v a place *of* k, put $K_v = K \otimes_k k_v = \prod_{w|v} K_w$, and let $K_v^\times = \prod_{w|v} K_w^\times$ be the units. Let

$$G'_v = \begin{cases} \mathfrak{o}_{K,v}^\times = \prod_{w|v} \mathfrak{o}_w^\times, & v \text{ finite}, \\ K_v^\times, & v \text{ infinite} \end{cases}.$$

Now we can write $\mathbf{A}_K^\times = \prod'_v K_v^\times$, where the product is over places v *of* k, and the restricted product is taken with respect to the subgroups G'_v. We consider the subgroup

$$G' = \prod_v G'_v,$$

endowed with the product topology (note that almost every factor is compact). It is a closed subgroup of $\mathbf{A}_K^\times$. It is σ stable and the projection defines a local isomorphism $G' \to \mathbf{A}_K^\times/K^\times$. Also (O) holds for (G',σ'): this follows from the fact that it holds for each G'_v *and* that, for almost all v, the norm N maps G'_v onto $(G'_v)^\sigma$ with kernel $(G'_v)^{1-\sigma}$; this follows from (48).

We now readily verify that

$$\nu(G', \sigma) = \prod_v \nu(G'_v, \sigma).$$

But also $\nu(G'_v, \sigma) = 1$ for all v, and so in fact $\nu(G', \sigma) = 1$. To check this, proceed as in the argument of §C.4.2: for any v, choosing $a \in k_v$ with $|a|$ suitably small, the map $x \mapsto \exp(ax)$ defines a local isomorphism from $(K_v, +)$ or $(\mathfrak{o}_{K,v}, +)$ to G'_v, thus showing that (G'_v, σ) is locally isomorphic to a shift. Then the discussion of §C.3 gives $\nu(G'_v, \sigma) = 1$.

Therefore $\nu(G, \sigma)$ is also equal to 1. Now (47) gives, in particular,

$$[\mathbf{A}_k^\times : k^\times N\mathbf{A}_K^\times] = m \cdot \mathsf{H} \geq m. \tag{49}$$

where H is the index of $(1-\sigma)$th powers in $\mathbf{A}_K^\times / K^\times$ inside the kernel of the norm. Coupled with the methods of §2 for the reverse inequality, we get another proof of (35): a cyclic extension is a class field in the idèlic sense. This argument also shows $\mathsf{H} = 1$. [14]

C.4.4. *Comparison with other arguments.* As we commented, this argument has many similarities with the use of the Herbrand quotient. Thus (45) plays the role, here, of the fact that the Herbrand quotient is invariant under maps with finite index kernel and cokernel. Let us compare what we just proved – namely, that the Herbrand quotient of the idele class group $\mathbf{A}_K^\times / K^\times$ equals $[K : k]$ – with the argument in [4] (which goes back to Chevalley's argument [11]), and which contains the following steps:

(a) By knowledge of the unramified case, replace $\mathbf{A}_K^\times / K^\times$ by $\prod_{v \in S} K_v^\times / U$ where S is a large set of places of k, containing all archimedean places, and U is the subgroup of $K^\times$ that are units at all places not above S.
(b) Compute the Herbrand quotient of $\prod_{v \in S} K_v^\times$ to equal $\prod n_v$, where n_v is the degree of any of the field factors of K_v over k_v;
(c) Compute the Herbrand quotient of U to equal $\frac{1}{m} \cdot \prod n_v$, with n_v as above.

The Haar measure argument also uses precise knowledge of what happens in the unramified case. And both arguments also use comparisons, via the exponential map, to the additive group. But the Haar measure argument shows *directly* that the ratio of the answers for (b) and (c) equals m , rather than computing them separately and comparing.

C.4.5. *Application to the unit torus; another proof of* (16). Now take G to be the *unit torus* $\mathbf{T} = (K \otimes \mathbf{R})^\times / U$ of a cyclic extension K/k of number fields, unramified at all archimedean places. Apply our reasoning above to G, with $G' = K \otimes \mathbf{R}$ and the exponential map as the local model, we find

$$[\mathbf{T}^\sigma : N\mathbf{T}] = [K : k] \cdot [\ker(N) : \mathbf{T}^{1-\sigma}].$$

Now, using the following computations which we leave to the valiant reader:[15]

$$\frac{\mathbf{T}^\sigma}{N\mathbf{T}} \simeq \frac{\ker(N : U \to u)}{U^{1-\sigma}} \text{ and } \frac{\ker(N)}{\mathbf{T}^{1-\sigma}} \simeq \frac{u}{NU}. \tag{50}$$

[14] One can show the equivalence of the statement $\mathsf{H} = 1$ and the statement that a cyclic algebra $[L/K, a]$ which is everywhere locally split is globally split. This latter statement, as noted by Zorn [10], can be proved directly by analytic arguments similar in spirit to §2, but more delicate. Again one counts ideals, now in a central simple algebra; however, the leading term alone is not enough to distinguish split from nonsplit algebras. In any case, this analytic argument is a key component of Weil's approach [5].

[15] For example, these are the connecting maps in cohomology of the cyclic group $\langle \sigma \rangle$ with coefficients in the sequence $U \to (K \otimes \mathbf{R})^\times \to \mathbf{T}$.

we arrive at another proof of (16)

$$\frac{[\text{norm 1 units of } U : U^{1-\sigma}]}{[u : NU]} = [K : k].$$

C.5. **Proof of** (45)**: invariance by local isomorphism.** We readily see that a local isomorphism $\varphi : G' \to G$ induces local isomorphisms

$$\ker(N') \to \ker(N) \text{ and } (G')^\sigma \to G^\sigma.$$

Therefore, $N : G \to G^\sigma$ is an open map if and only if $N' : G' \to (G')^\sigma$ is an open map; similarly $1-\sigma : G \to \ker(N)$ is an open map if and only if its G'-analogue is. Assuming that (O) holds for either G or G', both of these will be the case, and therefore if one of $\nu(G,\sigma)$ and $\nu(G',\sigma')$ is defined so is the other. We assume this in what follows.

Now, φ also induces local isomorphisms

$$G'^{1-\sigma'} \to G^{1-\sigma} \text{ and } NG' \to NG,$$

since these are open subgroups of the groups mentioned above.

We next observe that, given two locally isomorphic groups such as G and G', we can choose Haar measures on them compatibly, in the sense that the induced measure on small neighbourhoods of the identity correspond to one another. To do so, we note that a local isomorphism factors into the quotient by a discrete subgroup, and the inclusion of an open subgroup, and check in these two cases separately.

Now fix compatible Haar measures on the locally isomorphic groups $G^\sigma, (G')^\sigma$, as well as on the locally isomorphic groups $G^{1-\sigma}, (G')^{1-\sigma}$. As before, these choices then induce Haar measures μ_σ on G, G'. We claim that these are compatible. By similar reasonings the measures μ_N for G, G' are also compatible and then we get $\nu(G,\sigma) = \nu(G',\sigma')$, as desired.

Let V' be a small open σ-stable neighbourhood of the identity in G' so that φ gives a homeomorphism of V' with its image V. Now choose U' so that $(U')(U')^{-1} \subset V'$ and also $(U')^{1-\sigma} \subset V'$. It follows that:

- φ induces a homeomorphism of $(V')^{1-\sigma}$ with $V^{1-\sigma}$;
- φ induces a homeomorphism of each slice $V' \cap g'(G')^\sigma$ with $V \cap gG^\sigma$, where $g = \varphi(g')$.

Take f' a continuous non-negative function of compact support on V', not identically zero, and put $f' = f \circ \varphi$ as a function on V; extend both by zero to functions on G' and G. Then we readily see that

$$\int_{g \in G^{1-\sigma}} \int_{h \in G^\sigma} f(\tilde{g}h) = \int_{g' \in (G')^{1-\sigma}} \int_{h \in (G')^\sigma} f(\varphi(\tilde{g'})\varphi(h)) = \int_{g',h'} f'(\tilde{g}h).$$

Both sides are strictly positive. The desired statement follows (note that the essential uniqueness of Haar measure allows us to verify it by checking just one case).

References

[1] David Hilbert. Ueber die theorie des relativquadratischen zahlkörpers. *Mathematische Annalen*, pages 1–127, 1899.

[2] Philipp Furtwängler. Allgemeiner existenzbeweis für den klassenkörper eines beliebigen algebraischen zahlkörpers. *Mathematische Annalen*, 63:1–37, 1906.

[3] Serge Lang. *Algebraic number theory*, volume 110 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 1994.

[4] J. W. S. Cassels and A. Fröhlich, editors. *Algebraic number theory*. London Mathematical Society, London, 2010. Papers from the conference held at the University of Sussex, Brighton, September 1–17, 1965, Including a list of errata.
[5] André Weil. *Basic number theory*. Classics in Mathematics. Springer-Verlag, Berlin, 1995. Reprint of the second (1973) edition.
[6] Teiji Takagi. Über eine theorie des relativ-abelschen zahlkörpers. *Journal of the College of Science, Imperial University of Tokyo*, 41:1–133, 1920.
[7] Nicholas Bourbaki. The architecture of mathematics. *Amer. Math. Monthly*, 57:221–232, 1950.
[8] Franz Lemmermeyer. The ambiguous class number formula revisited. *J. Ramanujan Math. Soc.*, 28(4):415–421, 2013.
[9] Reinhold Baer. The Significance of the System of Subgroups for the Structure of the Group. *Amer. J. Math.*, 61(1):1–44, 1939.
[10] Max Zorn. Note zur analytischen hyperkomplexen Zahlentheorie. *Abh. Math. Sem. Univ. Hamburg*, 9(1):197–201, 1933.
[11] C. Chevalley. La théorie du corps de classes. *Ann. of Math. (2)*, 41:394–418, 1940.