23 The idele group, profinite groups, infinite Galois theory

23.1 The idele group

Let K be a global field. Having introduced the ring of adeles $\mathbb{A}_K$ in the previous lecture, it is natural to ask about its unit group. As a group we have

$$\mathbb{A}_K^\times = \{(a_v) \in \mathbb{A}_K : a_v \in K_v^\times \text{ for all } v \in M_K, \text{ and } a_v \in \mathcal{O}_v^\times \text{ for almost all } v \in M_K\},$$

however, as a subspace of $\mathbb{A}_K$, this is not a topological group because the inversion map $a \mapsto a^{-1}$ need not be continuous.

Example 23.1. Consider $K = \mathbb{Q}$ and for each prime p let $x_p = (1, 1, \ldots, 1, 1, p, 1, 1, \ldots) \in \mathbb{A}_\mathbb{Q}$ be the adele with a p in its *pth* component and 1's elsewhere. Every basic open set U about 1 in $\mathbb{A}_\mathbb{Q}$ has the form

$$U = \prod_{v\in S} U_v \times \prod_{V\not\in S} \mathcal{O}_v,$$

with $S \subseteq M_\mathbb{Q}$ finite and $1_v \in U_v$, and it is clear that U contains x_p for all sufficiently large p. It follows that the sequence $x_2, x_3, x_5, \ldots$ converges to 1 in the topology of $\mathbb{A}_\mathbb{Q}$. But notice that U does not contain x_p^{-1} for all sufficiently large p, so the sequence $x_2^{-1}, x_3^{-1}, x_5^{-1}, \ldots$ cannot possibly converge to $1^{-1} = 1$ in $\mathbb{A}_\mathbb{Q}$. Thus the function $x \to x^{-1}$ is not continuous in the subspace topology for $\mathbb{A}_K^\times$.

This problem is not specific to rings of adeles. In general, given a topological ring R, there is no reason to expect its unit group $R^\times \subseteq R$ to be a topological group in the subspace topology unless R happens to be a subring of a topological field (the definition of which requires inversion to be continuous), as is the case for the unit group $\mathcal{O}_K^\times$; this explains why we have not encountered this problem up to now.

There is a standard solution to this problem, which is to give the group $R^\times$ the weakest topology that makes it a topological group. This is done by embedding $R^\times$ in $R \times R$ via the injective group homomorphism

$$\begin{aligned} \phi\colon R^\times &\to R \times R \\ r &\mapsto (r, r^{-1}), \end{aligned}$$

which we may view as an isomorphism $R^\times \simeq \phi(R^\times)$. We then declare this to be an isomorphism of topological groups. This means that the topology on $R^\times$ is determined by the subspace topology on $\phi(R^\times) \subseteq R \times R$; the inversion map $r \mapsto r^{-1}$ is then continuous because it is equal to a restriction of the projection map $R \times R \to R$ onto its second coordinate.

If we now consider this construction in the case of $\mathbb{A}_K^\times$, the topology on $\mathbb{A}_K^\times$ now has a basis of open sets of the form

$$U' = \prod_{v\in S} U_v \times \prod_{v\not\in S} \mathcal{O}_v^\times$$

where $U_v \subseteq K_v^\times$ and $S \subseteq M_K$ is finite. To see this, note that in terms of the embedding $\phi\colon \mathbb{A}_K^\times \to \mathbb{A}_K \times \mathbb{A}_K$ defined above, each $\phi(a) = (a, a^{-1})$ lies in a product $U \times V$ of basic open sets $U, V \subseteq \mathbb{A}_K$, and this forces both a and a^{-1} to lie in $\mathcal{O}_v$, hence in $\mathcal{O}_v^\times$, for almost all v. The open sets U' are precisely the open sets in the restricted product $\prod(K_v^\times, \mathcal{O}_v^\times)$. This leads to the following definition.

Lecture by Andrew Sutherland

Definition 23.2. Let K be a global field. The *idele group* of K is the topological group

$$\mathbb{I}_K := \prod\nolimits_v (K_v^\times, \mathcal{O}_v^\times)$$

with multiplication defined component-wise, which we view as the subgroup $\mathbb{A}_K^\times$ of $\mathbb{A}_K$ endowed with the restricted product topology rather than the subspace topology.

Remark 23.3. In the literature one finds the notations $\mathbb{I}_K$ and $\mathbb{A}_K^\times$ used interchangeably; they both denote the idele group defined above (there is no reason to ever refer to the group $\mathbb{A}_K^\times \subseteq \mathbb{A}_K$ with the subspace topology, other than to note that it is not a topological group).

The canonical embedding $K \hookrightarrow \mathbb{A}_K$ restricts to a canonical embedding of $K^\times$ into $\mathbb{I}_K$, and we have a surjective homomorphism

$$\begin{aligned} \mathbb{I}_K &\to \mathcal{I}_K \\ a &\mapsto \prod \mathfrak{p}^{v_\mathfrak{p}(a)} \end{aligned}$$

where the product ranges over primes of K and $v_\mathfrak{p}(a) := v_\mathfrak{p}(a_v)$, where v is the place of K corresponding to the prime $\mathfrak{p}$. The composition

$$K^\times \hookrightarrow \mathbb{I}_K \twoheadrightarrow \mathcal{I}_K$$

has image $\mathcal{P}_K$, the subgroup of principal fractional ideals, and thus induces a homomorphism of the *idele class group* $C_K := \mathbb{I}_K/K^\times$ onto the ideal class group $\mathrm{Cl}_K = \mathcal{I}_K/\mathcal{P}_K$; we have the following commutative diagram of exact sequences:

$$\begin{tikzcd}
1 \arrow[r] & K^\times \arrow[r] \arrow[d, two heads] & \mathbb{I}_K \arrow[r] \arrow[d, two heads] & C_K \arrow[r] \arrow[d, two heads] & 1 \\
1 \arrow[r] & \mathcal{P}_K \arrow[r] & \mathcal{I}_K \arrow[r] & \mathrm{Cl}_K \arrow[r] & 1
\end{tikzcd}$$

Proposition 23.4. *Let K be a global field. The idele group $\mathbb{I}_K$ is a locally compact group.*

Proof. We need to show that $\mathbb{I}_K$ is compact Hausdorff. Each $K_v^\times$ is Hausdorff, so $\prod_v K_v^\times$ is Hausdorff in the product topology, and this implies that $\prod(K_v^\times, \mathcal{O}_v^\times) \subseteq \prod K_v^\times$ is Hausdorff, since its topology is finer (this only makes it easier to be Hausdorff). For each nonarchimedean place v, the set $\mathcal{O}_v^\times = \{x \in K_v^\times : \|x\|_v = 1\}$ is closed, hence compact (because the local field K_v is Hausdorff); this applies to almost all v, and the $K_v^\times$ are all locally compact, so the restricted product $\prod(K_v^\times, \mathcal{O}_v^\times)$ is locally compact, by Proposition 22.6. □

Proposition 23.5. *Let K be a global field. Then $K^\times$ is a discrete subgroup of $\mathbb{I}_K$.*

Proof. We have $K^\times \hookrightarrow K \times K \subseteq \mathbb{A}_K \times \mathbb{A}_K$. By Theorem 22.12, K is a discrete subset of $\mathbb{A}_K$, and it follows that $K \times K$ is a discrete subset of $\mathbb{A}_K \times \mathbb{A}_K$. The image of $K^\times$ in $\mathbb{A}_K \times \mathbb{A}_K$ lies in $\mathbb{I}_K = \mathbb{A}_K^\times \hookrightarrow \mathbb{A}_K \times \mathbb{A}_K$, hence it is discrete in $\mathbb{A}_K^\times$. □

Remark 23.6. Discrete sets need not be closed, in general, but discrete subgroups of a topological Hausdorff group are (we leave it as an exercise for you to prove this).

We proved last time that K is a discrete cocompact subgroup of $\mathbb{A}_K$, so it is naturally to ask whether $K^\times$ is a cocompact subgroup of $\mathbb{I}_K = \mathbb{A}_K^\times$. The answer is no (at least when K is a number field). An easy way to see this is to note that when K is a number field the unit group $\mathcal{O}_K^\times$ is not cocompact in $K^\times$ because $\operatorname{Log}\mathcal{O}_K^\times$ is not a (full) lattice in $\mathbb{R}^{r+s}$; it lies inside the trace zero hyperplane $\mathbb{R}_0^{r+s}$ (see Proposition 14.7). In order to get a cocompact subgroup we need to restrict $\mathbb{I}_K$ to a subgroup corresponding to the trace zero hyperplane.

We have a continuous homomorphism of topological groups

$$\begin{aligned} \|\ \|\colon \mathbb{I}_K &\to \mathbb{R}_{>0}^\times \\ a &\mapsto \|a\| \end{aligned}$$

where $\|a\| := \prod_v \|a\|_v$. Note that $\|a\| > 0$ for all $a \in \mathbb{I}_K$, because $a_v \in \mathcal{O}_v^\times$ for almost all v, and this means that $\|a\|_v = 1$ for almost all v, so the product $\prod_v \|a\|_v$ is effectively a finite product; it is never 0 because $a_v \in K_v^\times$ for all $v \in M_K$.

Definition 23.7. Let K be a global field. The group of 1-*ideles* is the topological group

$$\mathbb{I}_K^1 := \ker \|\ \| = \{x \in \mathbb{I}_K : \|x\| = 1\},$$

which we note contains $K^\times$, by the product formula (Theorem 12.32).

A useful feature of the group of 1-ideles is that, unlike the group of ideles, its topology is the same as the subspace topology it inherits from $\mathbb{A}_K$.

Lemma 23.8. *The subspace topologies on $\mathbb{I}_K^1 \subseteq \mathbb{I}_K$ and $\mathbb{I}_K^1 \subseteq \mathbb{A}_K$ coincide.*

Proof. Let $U = \prod_{v\in S} U_v \times \prod_{v\notin S} \mathcal{O}_v^\times$ be a basic open set in $\mathbb{I}_K = \prod(K_v^\times, \mathcal{O}_v^\times)$; we assume without loss of generality that S contains all the archimedean places (put $U_v = K_v^\times$ as needed). We then have

$$U \cap \mathbb{I}_K^1 = \prod_{v\in S}(U_v \cap K_v^1) \times \prod_{v\notin S} \mathcal{O}_v^\times,$$

where $K_v^1 := \{x \in K_v^\times : \|x\|_v = 1\}$. If we now define $U' := \prod_{v\in S} U_v \times \prod_{v\notin S} \mathcal{O}_v$, then U' is open in $\mathbb{A}_K$ because each U_v is open in $K_v^\times$ which is open in K_v. We then have $U' \cap \mathbb{I}_K^1 = U \cap \mathbb{I}_K^1$. Thus every open set of $\mathbb{I}_K^1 \subseteq \mathbb{I}_K$ is also open in the subspace topology on $\mathbb{I}_K \subseteq \mathbb{A}_K$; the same argument can be applied in the reverse direction (or just note that that the topology on $\mathbb{I}_K$ is finer than the subspace topology it inherits from $\mathbb{A}_K$). □

Lemma 23.9. *The group of 1-ideles $\mathbb{I}_K^1$ is a closed subset of $\mathbb{A}_K$.*

Proof. Consider any $x \in \mathbb{A}_K$ that is not in $\mathbb{I}_K^1$. We will show that each such x has an open neighborhood U_x disjoint from $\mathbb{I}_K^1$. The union of the U_x is then the open complement of $\mathbb{I}_K^1$.

Case 1: Suppose $\|x\| < 1$. Let S be a finite set containing the archimedean places of K, all v for which $\|x\| > 1$, and such that $\prod_{v\in S}\|x\|_v < 1$ (this is clearly possible given that $\|x\| < 1$ and $\|x\|_v \le 1$ for almost all v). Choose $\epsilon_v > 0$ small enough so that for all y in the open set

$$U_x := \{u \in \mathbb{A}_K : \|u - x\|_v < \epsilon_v \text{ for } v \in S \text{ and } \|u\|_v \le 1 \text{ for } v \notin S\} \subseteq \mathbb{A}_K;$$

we have $\|y\|_v < 1$ (each $v \notin S$ is nonarchimedean, so $\|u\|_v \le 1$ is equivalent to $u_v \in \mathcal{O}_v$), so U_x is basic open set of $\mathbb{A}_K$. Then U_x does not intersect $\mathbb{I}_K^1$.

Case 2: Suppose $\|x\| > 1$. Pick a bound B that is greater than the product of all the $\|x\|_v$ strictly greater than 1. Let S be a finite set that contains all v for which $\|x\|_v > 1$, all archimedean v, and all nonarchimedean v whose residue field has cardinality less than $2B$. This means that for each $v \notin S$ the largest absolute value $\|x\|_v$ strictly less than 1 is smaller than $1/(2B)$. For each $v \in S$ we now choose $\epsilon_v > 0$ so that

$$\|y - x\|_v < \epsilon_v \quad \Longrightarrow \quad 1 < \prod_{v \in S} \|y\|_v < 2B;$$

this is possible, since

$$1 < \|x\| \le \prod_{v \in S} \|x\|_v \le B < 2B.$$

Define U_x as above and consider any $y \in U_x$. Either $\|y\|_v = 1$ for all $v \notin S$, in which case $\|y\| > 1$, or $\|y\|_v < 1$ for some $v \notin S$, in which case $\|y\|_v < 1/(2B)$ for each such v, and $\|y\| < 1$. In either case $\|y\| \neq 1$, so $y \notin \mathbb{I}_K^1$ and therefore U_x does not intersect $\mathbb{I}_K^1$. □

Theorem 23.10. *For any global field K, the group $K^\times$ is a discrete closed subgroup of the abelian group of 1-ideles $\mathbb{I}_K^1$, and the quotient group $\mathbb{I}_K^1/K^\times$ is compact.*

Proof. We know that $K^\times$ is discrete in $\mathbb{I}_K$ (by Proposition 23.5), and it is therefore discrete in the subspace $\mathbb{I}_K^1$, and closed, since $\mathbb{I}_K^1 \subseteq \mathbb{I}_K$ is Hausdorff (a discrete subgroup of a Hausdorff space is always closed). As in the proof of Theorem 22.12, it suffices to construct a compact set $W \subseteq \mathbb{A}_K$ for which $W \cap \mathbb{I}_K^1$ surjects onto $\mathbb{I}_K^1/K^\times$ under the quotient map (here we are using Lemma 23.9: $\mathbb{I}_K^1$ is closed so $W \cap \mathbb{I}_K^1$ is compact).

To construct W we first choose $x \in \mathbb{A}_K$ such that $\|x\| > C$, where C is the Blichfeldt-Minkowski constant in Lemma 22.13, and let

$$W := \{w \in \mathbb{A}_K : \|w\|_v \le \|x\|_v \text{ for all } v \in M_K\}.$$

Now consider any $y \in \mathbb{I}_K^1$. We have $\|y\| = 1$, so $\|\frac{x}{y}\| = \|x\| > C$, and by Lemma 22.13 there is a $z \in K^\times$ for which

$$\|z\|_v \le \|x\|_v = \left\|\frac{x}{y}\right\|_v$$

for all $v \in M_K$. Therefore $zy \in W$. Thus every $y \in \mathbb{I}_K^1$ can be written as ab with $a = z^{-1} \in K^\times$ and $b = zy \in W \cap \mathbb{I}_K^1$. So $W \cap \mathbb{I}_K^1$ contains a complete set of coset representatives for $K^\times$ as desired, and therefore it surjects onto $\mathbb{I}_K^1/K^\times$ under the quotient map $\mathbb{I}_K^1 \to \mathbb{I}_K^1/K^\times$, which is continuous, and therefore $\mathbb{I}_K^1/K^\times$ is compact. □

Remark 23.11. When K is a function field the quotient $\mathbb{I}_K^1/K^\times$ is totally disconnected, in addition to being compact Hausdorff; as we shall see, this makes it a profinite group.

23.2 Profinite groups

In order to state the main theorems of class field theory in our adelic/idelic setup, rather than considering each finite abelian extension L of a global field K individually, we prefer to work in K^{ab}, the compositum of all finite abelian extensions of K. This requires us to understand the infinite Galois group $\text{Gal}(K^{\text{ab}}/K)$, which, like all Galois groups, is a *profinite group*.

Definition 23.12. A *profinite group* is a topological group that is an inverse limit of finite groups with the discrete topology. Given any topological group G, we can construct a profinite group by taking the *profinite completion*

$$\widehat{G} := \varprojlim_{N} G/N \subseteq \prod_{N} G/N$$

where N ranges over finite index open normal subgroups, ordered by containment.[1] If we are given a group G without a specified topology, we make it a topological group by giving it the *profinite topology*. This is the weakest topology that makes every finite quotient discrete and is obtained by taking all cosets of finite-index normal subgroups as a basis.

The profinite completion of G is (by construction) a profinite group, and it comes equipped with a natural homomorphism $\phi\colon G \to \widehat{G}$ that sends each element of G to the sequences of its images ($\overline{G}_N$) in the discrete finite quotients G/N, which we may view as an element of $\prod_N G/N$. The homomorphism ϕ is not necessarily injective; this occurs if and only if the intersection of all finite-index open normal subgroups of G is the trivial group (such a G is said to be *residually finite*), but we always have the following universal property. For every continuous homomorphism $\varphi\colon G \to H$ of topological groups there is a unique continuous homomorphism that makes the following diagram commute

$$\begin{tikzcd}
G \arrow[r, "\phi"] \arrow[dr, "\varphi"'] & \widehat{G} \arrow[d, dashed, "\exists!"] \\
 & H
\end{tikzcd}$$

There is a lot one can say about profinite groups but we shall limit ourselves to a few remarks and statements of the main results we need, deferring the proofs to Problem Set 11; see [3] for a comprehensive treatment of the subject.

Remark 23.13. Taking inverse limits in the category of topological groups is the same thing as taking the inverse limits in the categories of topological spaces and groups independently: the topology is the subspace topology in the product, and the group operation is the group operation in the product (defined component-wise). This might seem obvious, but the same statement does not apply to direct limits, where one must compute the limit in the category of topological groups, otherwise the group operation in the direct limit of the groups is not necessarily continuous under the direct limit topology; see [4].[2]

Remark 23.14. The profinite completion of G as a topological group is not necessarily the same thing as the profinite completion of G as a group (forgetting its topology); this depends on whether the original topology on G contains the profinite topology or not. In particular, a profinite group need not equal to its profinite completion as a group; the group $\operatorname{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ endowed with the Krull topology is an example (see below). Profinite groups that are isomorphic to their profinite completion as groups are said to be *strongly complete*; this is equivalent to requiring every finite index subgroup to be open (see Corollary 23.19 below). It was recently proved that if G is finitely generated as a topological group (meaning it contains a finitely generated dense subgroup), then G is strongly complete [2].

[1] Recall that an inverse system has objects X_i and morphisms $X_i \leftarrow X_j$ for $i \le j$. Here we have objects G/N_i and morphisms $G/N_i \leftarrow G/N_j$ for $i \le j$; we want the indices ordered so that $i \le j$ whenever N_i contains N_j; containment induces a canonical morphism $g + N_i \mapsfrom g + N_j$ on the quotients.

[2] For countable direct systems of locally compact groups this issue does not arise [4, Thm. 2.7].

Remark 23.15. For suitable restricted types of finite groups $\mathcal{C}$ (for example, all finite cyclic groups, or all finite p-groups for some fixed prime p), one can similarly define the notion of a pro-$\mathcal{C}$ group and the pro-$\mathcal{C}$ completion of a group by constraining the finite groups in the inverse system to lie in $\mathcal{C}$. One can also define profinite rings or pro-$\mathcal{C}$ rings.

Example 23.16. Here are a few examples of profinite completions:

1. The profinite completion of any finite group G is isomorphic to G with the discrete topology; the natural map $G \to \widehat{G}$ is an isomorphism.
2. The profinite completion of $\mathbb{Z}$ is $\widehat{\mathbb{Z}} := \varprojlim_n \mathbb{Z}/n\mathbb{Z} = \prod \mathbb{Z}_p$, where the indices n are ordered by divisibility; the natural map $\mathbb{Z} \to \widehat{\mathbb{Z}}$ is injective but not surjective.
3. The profinite completion of $\mathbb{Q}$ is trivial because $\mathbb{Q}$ has no finite index subgroups other than itself. The natural map $\mathbb{Q} \to \widehat{\mathbb{Q}} = \{1\}$ is surjective but not injective.

Lemma 23.17. *Let G be a topological group with profinite completion $\widehat{G}$. The image of G under the natural map $\phi\colon G \to \widehat{G}$ is dense in $\widehat{G}$.*

Proof. See Problem Set 11. □

We now give a topological characterization of profinite groups that can serve as an alternative definition.

Theorem 23.18. *A topological group is profinite if and only if it is totally disconnected and compact Hausdorff.*

Proof. See Problem Set 11. □

Corollary 23.19. *Let G be profinite group. Then G is naturally isomorphic to its profinite completion; in fact*

$$G \simeq \varprojlim G/U,$$

where U ranges over open normal subgroups (ordered by containment).

However, G is isomorphic to its profinite completion as a group (with the profinite topology) if and only if every finite index subgroup of G is open.

Proof. See Problem Set 11 for the first statement. For the second statement, if every finite index subgroup of G is open then every finite-index normal subgroup is open, meaning that the topology on G is finer than the profinite topology, and we get the same profinite completion under both topologies.

Conversely, if G has a finite index subgroup H that is not open, then no subgroup of H is open (since H is the union of the cosets of any of its subgroups); in particular, the intersection of all the conjugates of H, which is a normal subgroup N, is not open in G, nor are any of its subgroups. If the topological group G is isomorphic to its profinite completion $\widehat{G}$ as a group, then by the universal property of the profinite completion the natural map $\phi\colon G \to \widehat{G}$ is an isomorphism, but the image of N under ϕ is an open subgroup of $\widehat{G}$ by construction, which is a contradiction. □

23.3 Infinite Galois theory

The key issue that arises when studying Galois groups of infinite algebraic extensions (as opposed to finite ones) is that the Galois correspondence (the inclusion reversing bijection between subgroups and subextensions) no longer holds. As you proved on Problem Set 5 in the case $\operatorname{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q) \simeq \widehat{\mathbb{Z}} \simeq \prod_p \mathbb{Z}_p$, this happens for a simple reason: there are too many subgroups. For a more extreme example, the absolute Galois group of $\mathbb{Q}$ has uncountably many subgroups of index 2 (all of which are necessarily normal) but $\mathbb{Q}$ has only countably many quadratic extensions, see [1, Aside 7.27].

Thus not all subgroups of an infinite Galois group $\operatorname{Gal}(L/K)$ correspond to subextensions of L/K. We are going to put a topology on $\operatorname{Gal}(L/K)$ that distinguishes those that do.

Lemma 23.20. *Let L/K be a Galois extension with Galois group $G = \operatorname{Gal}(L/K)$, If F/K is a normal subextension of L/K, then $H = \operatorname{Gal}(L/F)$ is a normal subgroup of G with fixed field F, and we have an exact sequence*

$$1 \to \operatorname{Gal}(L/F) \to \operatorname{Gal}(L/K) \to \operatorname{Gal}(F/K) \to 1,$$

where the first map is inclusion and the second map is induced by restriction, and we have

$$G/H \simeq \operatorname{Gal}(F/K).$$

Proof. If F/K is a normal subextension of L/K then the restriction map $\sigma \mapsto \sigma_{|_F}$ defines a homomorphism $\operatorname{Gal}(L/K) \to \operatorname{Gal}(F/K)$ whose kernel is a normal subgroup $H = \operatorname{Gal}(L/F)$. The fixed field of H contains F by definition, and it must be equal to F: if we had $\alpha \in L^H - F$ we could construct an element of H that sends α to a distinct root $\alpha' \neq \alpha$ of its minimal polynomial f over F (this defines an element of $\operatorname{Gal}(E/F)$, where E is the splitting field of f, which can be extended to $\operatorname{Gal}(L/F) = H$ by embedding L in an algebraic closure and applying Theorem 4.11). The restriction map is surjective because any $\sigma \in \operatorname{Gal}(F/K)$ can be extended to $\operatorname{Gal}(L/K)$, by Theorem 4.11, thus the sequence in the lemma is exact, and $G/H \simeq \operatorname{Gal}(F/K)$ follows. □

Unlike the situation for finite Galois extensions, it can happen that a normal subgroup H of $\operatorname{Gal}(L/K)$ with fixed field F is **not** equal to $\operatorname{Gal}(L/F)$; it must be contained in $\operatorname{Gal}(L/F)$, but it could be a proper subgroup. This is exactly what happens for all but a countable number of the uncountably many index 2 subgroups H of $G = \operatorname{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$; the fixed field of H is $\mathbb{Q}$ but $H \subsetneq G$ is not the Galois group of $\overline{\mathbb{Q}}/\mathbb{Q}$, or of any extension of $\mathbb{Q}$ in $\overline{\mathbb{Q}}$. It is thus necessary to distinguish the subgroups of $\operatorname{Gal}(L/K)$ that are actually Galois groups. This is achieved by putting an appropriate topology on the Galois group.

Definition 23.21. Let L/K be a Galois extension with Galois group $G := \operatorname{Gal}(L/K)$. The *Krull topology* on G is defined by taking as a basis all cosets of subgroups $H_F := \operatorname{Gal}(L/F)$, where F ranges over finite normal extensions of K in L.

Under the Krull topology every open normal subgroup necessarily has finite index, but it is typically **not** the case that every normal subgroup of finite index is open. Thus the Krull topology on $\operatorname{Gal}(L/K)$ is strictly coarser than the profinite topology, in general (this holds for $\operatorname{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, for example). However, the topological group we obtain by putting the Krull topology on $\operatorname{Gal}(L/K)$ is a profinite group.

Theorem 23.22. *Let L/K be a Galois extension. Under the Krull topology, the restriction maps induce a natural isomorphism of topological groups*

$$\phi\colon \operatorname{Gal}(L/K) \to \varprojlim \operatorname{Gal}(F/K),$$

where F ranges over finite Galois extensions of K in L. In particular, $\operatorname{Gal}(L/K)$ *is a profinite group whose open normal subgroups are precisely those of the form* $\operatorname{Gal}(L/F)$ *for some finite Galois extension F/K.*

Proof. Every element of L is algebraic over K, hence lies in some finite Galois subextension F/K. Thus each automorphism in $\operatorname{Gal}(L/K)$ is uniquely determined by its restrictions to the F/K, which implies that ϕ is injective. Given an element $(\sigma_F) \in \varprojlim \operatorname{Gal}(F/K)$, we can define an automorphism $\sigma \in \operatorname{Gal}(L/K)$ by simply putting $\sigma(\alpha) = \sigma_F(\alpha)$, where F is the normal closure of $K(\alpha)$ (the fact that this actually gives an automorphism is guaranteed by the inverse system of restriction maps used to define $\varprojlim \operatorname{Gal}(F/K)$). Thus ϕ is surjective.

By Lemma 23.20, if we put $G := \operatorname{Gal}(L/K)$ and $H_F := \operatorname{Gal}(L/F)$, then we can view ϕ as the natural map

$$\phi\colon G \to \varprojlim G/H_F,$$

which is continuous, and we have shown it is a bijection. To prove that ϕ is an isomorphism of topological groups it remains only to show that it is an open map. For this it suffices to show that ϕ maps open subgroups $H \subseteq G$ to open sets of $\varprojlim G/H_F$, since every open set in G is a union of cosets of open subgroups (if $\phi(H)$ is open so is $\phi(\sigma H) = \sigma\phi(H)$, for any $\sigma \in G$, and $\phi(\bigcup U_i) = \bigcup_i \phi(U_i)$ for any family of open sets U_i). If $H = \operatorname{Gal}(L/F)$ then

$$\phi(H) = \{(\sigma_E) : \sigma_E|_{E\cap F} = 1_G|_{E\cap F}\} = \pi_E^{-1}(1_G|_F),$$

where E/K ranges over finite Galois subextensions of L/K and π_E is the projection map from the inverse limit to $\operatorname{Gal}(E/K)$. The set $\{1_G|_F\}$ is open in the discrete group $\operatorname{Gal}(E/F)$, so its inverse image under the continuous map π_E is open.

The last statement follows from Lemma 23.20 and Corollary 23.19. □

Theorem 23.23 (Fundamental theorem of Galois theory)**.** *Let L/K be a Galois extension and let $G := \operatorname{Gal}(L/K)$ be endowed with the Krull topology. The maps $F \mapsto \operatorname{Gal}(L/F)$ and $H \mapsto L^H$ define an inclusion preserving bijection between subextensions F/K of L/K and closed subgroups H of G. Under this correspondence, subextensions of finite degree n correspond to subgroups of finite index n, and normal subextensions F/K correspond to normal subgroups $H \subseteq G$ such that $\operatorname{Gal}(F/K) \simeq G/H$ as topological groups.*

Proof. We first note that every open subgroup of G is closed, since it is the complement of the union of its non-trivial cosets, all of which are open, and closed subgroups of finite index are open by the same argument.

The correspondence between finite Galois subextensions F/K and finite index closed normal subgroups H then follows the previous theorem, and we have $[F:K] = [G:H]$ because $G/H \simeq \operatorname{Gal}(F/K)$, by Lemma 23.20.

If F/K is any finite subextension with normal closure E, then $H = \operatorname{Gal}(L/F)$ contains the normal subgroup $N = \operatorname{Gal}(L/E)$ with finite index. The subgroup N is open and therefore closed, thus H is closed since it is a finite union of cosets of N. The fixed field of H is F (by the same argument as in the proof of Lemma 23.20), thus finite subextensions correspond to closed subgroups of finite index. Conversely, every closed subgroup H of finite index has a fixed field F of finite degree, since the intersection of its conjugates is a normal closed subgroup $N = \operatorname{Gal}(L/E)$ of finite index whose fixed field E contains F and has finite degree. The degrees and indices match because $[G : N] = [G : H][H : N]$ and $[E : K] = [F : K][E : F]$; by the previous argument for finite normal subextensions, $[E : K] = [G : N]$ and $[E : F] = [H : N]$ (for the second equality, replace L/K with L/F and G with H).

Any subextension F/K is the union of its finite subextensions E/K. The intersection of the corresponding closed finite index subgroups $\operatorname{Gal}(L/E)$ is equal to $\operatorname{Gal}(L/F)$, which is therefore closed. Conversely, every closed subgroup H of G is an intersection of basic closed subgroups, all of which have the form $\operatorname{Gal}(L/E)$ for some finite subextension E/K, thus $H = \operatorname{Gal}(L/F)$, where F is the union of the E.

The isomorphism $\operatorname{Gal}(F/K) \simeq G/H$ for normal subextensions/subgroups follows directly from Lemma 23.20. □

Corollary 23.24. *Let L/K be a Galois extension and let H be a subgroup of* $\operatorname{Gal}(L/K)$ *with fixed field F. The closure $\overline{H}$ of H in the Krull topology is* $\operatorname{Gal}(L/F)$*.*

Proof. The Galois group $\operatorname{Gal}(L/F)$ contains H, since it contains every element of $\operatorname{Gal}(L/K)$ that fixes F, and it is closed, by the previous theorem. Thus $\operatorname{Gal}(L/F) \cap \overline{H}$ is a closed group containing H, so $\operatorname{Gal}(L/F) \cap \overline{H} \subseteq \overline{H}$ and therefore $\operatorname{Gal}(L/F) = \overline{H}$. □

We conclude this section with the following theorem due to Waterhouse [5].

Theorem 23.25 (Waterhouse 1973)**.** *Every profinite group G is isomorphic to the Galois group of some Galois extension L/K.*

Proof sketch. Let X be the disjoint union of the finite discrete quotients of G equipped with the G-action induced by multiplication. Now let k be any field and define $L = k(X)$ as a purely transcendental extension of k with indeterminates for each element of X. We can view each $\sigma \in G$ as an automorphism of L that fixes k and sends each $x \in X$ to $\sigma(x)$, and since G acts faithfully on X, we can view G as a subgroup of $\operatorname{Aut}_k(L)$. Now let $K = L^G$. Then L/K is a Galois extension with $G \simeq \operatorname{Gal}(L/K)$, by [5, Thm. 1]. □

Remark 23.26. Although this proof lets us choose any field k we like, we have no way to control K. In particular, it is not known whether every profinite group G is isomorphic to a Galois group over $K = \mathbb{Q}$; indeed, this is not even known for finite G.

References

[1] J.S. Milne, *Fields and Galois theory*, version 4.51, 2015.

[2] Nikolay Nikolov and Dan Segal, *On finitely generated profinite groups I: strong completeness and uniform bounds*, Annals of Mathematics **165** (2007), 171–238.

[3] Luis Ribes and Pavel Zalesskii, *Profinite groups*, second edition, Springer, 2010.

[4] N. Tatsuuma, H. Shimomura, and T. Hirai, *On group topologies and unitary representations of inductive limits of topological groups and the case of the group of diffeomorphisms*, J. Math. Kyoto Univ. **38** (1998), 551–578.

[5] William C. Waterhouse, *Profinite groups are Galois groups*, Proceedings of the American Mathematical Society **42** (1974).