26 The idele group, profinite groups, infinite Galois theory

26.1 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

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

Here $\mathcal{O}_v^\times \coloneqq K_v^\times \cap \mathcal{O}_v$ is the unit group of the valuation ring of K_v when v is nonarchimedean and isomorphic to $\mathbb{R}^\times$ or $\mathbb{C}^\times$ when v is archimedean. As noted in Lecture 25, the definition of $\mathbb{A}_K$ does not actually depend on our choice of $\mathcal{O}_v$ at the finitely many archimedean places of K, but the choice we made ensures that every $\mathcal{O}_v^\times$ is a topological group.

However, as a subspace of $\mathbb{A}_K$, the unit group $\mathbb{A}_K^\times$ is not a topological group. Indeed, the inversion map $a \mapsto a^{-1}$ is not continuous.

Example 26.1. Consider $K = \mathbb{Q}$ and for each prime p let $a(p) = (1, \ldots, 1, p, 1, \ldots) \in \mathbb{A}_\mathbb{Q}$ be the adele with $a(p)_p = p$ and $a(p)_q = 1$ for $q \neq p$. Every basic open set U about 1 in $\mathbb{A}_\mathbb{Q}$ has the form

$$U = \prod_{v \in S} U_v \times \prod_{V \notin S} \mathcal{O}_v,$$

with $S \subseteq M_\mathbb{Q}$ finite and $1_v \in U_v$, and it is clear that U contains $a(p)$ for all sufficiently large p. It follows that $\lim_{p\to\infty} a(p) = 1$ in the topology of $\mathbb{A}_\mathbb{Q}$. But notice that U does not contain $a(p)^{-1}$ for any sufficiently large p, so $\lim_{p\to\infty} a(p)^{-1} \neq 1^{-1}$ in $\mathbb{A}_\mathbb{Q}$. Thus the function $a \to a^{-1}$ is not continuous in the subspace topology for $\mathbb{A}_K^\times$.

This problem is not specific to rings of adeles. For a topological ring R there is in general no reason to expect its unit group $R^\times \subseteq R$ to be a topological group in the subspace topology. One notable exception is when R is 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 before now. But the ring of adeles is not naturally contained in any topological field (note that it is not an integral domain).

There is a standard solution to this problem: 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 map

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

We now declare ϕ to be a homeomorphism; that is, we endow $R^\times$ with the topology matching the subspace topology of $\phi(R^\times) \subset R \times R$. The inversion map $r \mapsto r^{-1}$ is continuous in this topology because it is equal to composition of ϕ with the projection map $R \times R \to R$ onto its second coordinate, both of which are continuous maps.

We now consider this construction in the case of $\mathbb{A}_K^\times$. The implied topology on $\mathbb{A}_K^\times$ has a basis of open sets of the form

$$U' = \prod_{v \in S} U_v \times \prod_{v \notin S} \mathcal{O}_v^\times$$

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.

Definition 26.2. 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. The canonical embedding $K \hookrightarrow \mathbb{A}_K$ restricts to a canonical embedding $K^\times \hookrightarrow \mathbb{I}_K$, and we define the *idele class group* $C_K := \mathbb{I}_K/K^\times$, a topological group.

Remark 26.3. 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. But in this lecture we will temporarily use the notation $\mathbb{A}_K^\times$ to denote the unit group of the ring $\mathbb{A}_K$ in the subspace topology (which is not a topological group).

Example 26.4. Let us again consider the sequence $(a(p))$ defined in Example 26.1. This sequence lies in $\mathbb{A}_\mathbb{Q}^\times$ and converges to $1 \in \mathbb{A}_\mathbb{Q}^\times$ under the subspace topology. But this sequence does not converge to 1 in the topology of $\mathbb{I}_\mathbb{Q}$. Indeed, consider the basic open set $\prod_v \mathcal{O}_v^\times = \prod_p \mathbb{Z}_p^\times \times \mathbb{R}^\times$ of $\mathbb{I}_\mathbb{Q}$. None of the $a(p) = (1, \ldots, 1, p, 1, \ldots)$ lie in this open neighborhood of 1, so the sequence $(a(p))$ cannot converge to 1 in $\mathbb{I}_\mathbb{Q}$ (which means it cannot converge at all: if it converged to $x \neq 1$ in $\mathbb{I}_\mathbb{Q}$ it would converge to $x \neq 1$ in $\mathbb{A}_\mathbb{Q}^\times \subseteq \mathbb{A}_\mathbb{Q}$, which we know is not the case). The counterexample to the continuity of the inversion map $x \mapsto x^{-1}$ in $\mathbb{A}_\mathbb{Q}^\times$ is removed in $\mathbb{I}_\mathbb{Q}$ by adding more open sets to the topology; this makes it easier for maps to be continuous and harder for sequences to converge.

We now define 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 $\mathfrak{p}$ of K and $v_\mathfrak{p}(a) := v_\mathfrak{p}(a_v)$, where v is the equivalence class of the $\mathfrak{p}$-adic absolute value $\| \|_\mathfrak{p}$. The composition

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

has image $\mathcal{P}_K$, the subgroup of principal fractional ideals; we thus have a surjective homomorphism of the idele class group $C_K = \mathcal{I}_K/K^\times$ onto the ideal class group $\mathrm{Cl}_K = \mathcal{I}_K/\mathcal{P}_K$ and a 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 26.5. *Let K be a global field. The idele group $\mathbb{I}_K$ is a locally compact group.*

Proof. It is clear that $\mathbb{I}_K$ is Hausdorff, since its topology is finer than the topology of $\mathbb{A}_K^\times \subseteq \mathbb{A}_K$, which is Hausdorff by Proposition 25.9. For each nonarchimedean place v, the set $\mathcal{O}_v^\times = \{x \in K_v^\times : \|x\|_v = 1\}$ is a closed subset of the compact set $\mathcal{O}_v$, hence compact. This applies to almost all $v \in M_K$, and the $K_v^\times$ are all locally compact, so the restricted product $\prod(K_v^\times, \mathcal{O}_v^\times) = \mathbb{I}_K$ is locally compact, by Proposition 25.6. □

Proposition 26.6. *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 25.12, 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 the image of $\mathbb{A}_K^\times \hookrightarrow \mathbb{A}_K \times \mathbb{A}_K$ and in the discrete image of $K \hookrightarrow \mathbb{A}_K \times \mathbb{A}_K$, and it follows that $K^\times$ is discrete in $\mathbb{A}_K^\times$ and therefore in $\mathbb{I}_K$, since having a finer topology only makes it easier for a set to be discrete. □

We proved last time that K is a discrete cocompact subgroup of $\mathbb{A}_K$, so it is natural to ask whether $K^\times$ is a cocompact in $\mathbb{A}_K^\times$ or $\mathbb{I}_K$. The answer is no, $K^\times$ is not a cocompact subgroup of $\mathbb{I}_K$, thus the idele class group C_K, while locally compact, is not compact.

Recall that for a number field K, the unit group $\mathcal{O}_K^\times$ is not a cocompact subgroup of $K_\mathbb{R}^\times$ because $\operatorname{Log}(\mathcal{O}_K^\times)$ is not a (full) lattice in $\mathbb{R}^{r+s} \simeq \operatorname{Log}(K_\mathbb{R}^\times)$; it lies in the trace zero hyperplane $\mathbb{R}_0^{r+s}$ (see Proposition 15.11). In order to get a cocompact subgroup we need to restrict $\mathbb{I}_K$ to a subgroup that corresponds 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 $\|a\| := \prod_v \|a\|_v$ is the adelic norm defined in the previous lecture. We have $\|a\| > 0$ for $a \in \mathbb{I}_K$, since $a_v \in \mathcal{O}_v^\times$ for almost all v: this implies that $\|a\|_v = 1$ for almost all v and the product $\prod_v \|a\|_v$ is effectively a finite product, and it is nonzero because $a_v \in K_v^\times$ is nonzero for all $v \in M_K$.

Definition 26.7. Let K be a global field. The group of 1-*ideles* is the topological group

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

which we note contains $K^\times$, by the product formula (Theorem 13.21).

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 26.8. *The group of 1-ideles $\mathbb{I}_K^1$ is a closed subset of $\mathbb{A}_K$ and $\mathbb{I}_K$, and the two subspace topologies on $\mathbb{I}_K^1$ coincide.*

Proof. We first show that $\mathbb{I}_K^1$ is closed in $\mathbb{A}_K$, and therefore also in $\mathbb{I}_K$, since it has a finer topology. Consider any $x \in \mathbb{A}_K - \mathbb{I}_K^1$. We will construct an open neighborhood U_x of x that is disjoint from $\mathbb{I}_K^1$. The union of the U_x is then the open complement of the closed set $\mathbb{I}_K^1$. For each $\epsilon > 0$, finite $S \subseteq M_K$, and $x \in \mathbb{A}_K$ we define

$$U_\epsilon(x, S) := \{u \in \mathbb{A}_K : \|u - x\|_v < \epsilon \text{ for } v \in S \text{ and } \|u\|_v \le 1 \text{ for } v \notin S\},$$

which is a basic open set of $\mathbb{A}_K$ (a product of open sets U_v for $v \in S$ and $\mathcal{O}_v$ for $v \notin S$).

The case $\|x\| < 1$. Let S be a finite set containing the archimedean places $v \in M_K$ and all v for which $\|x\|_v > 1$, such that $\prod_{v\in S} \|x\|_v < 1$: such an S exists since $\|x\| < 1$ and $\|x\|_v \le 1$ for almost all v. For all sufficiently small $\epsilon > 0$ the set $U_x := U_\epsilon(x, S)$ is an open neighborhood of x disjoint from $\mathbb{I}_K^1$ because every $y \in U_x$ must satisfy $\|y\| < 1$.

The case $\|x\| > 1$. Let B be twice the product of all the $\|x\|_v$ greater than 1. Let S be the finite set containing the archimedean places $v \in M_K$, all nonarchimedean v with residue field cardinality less than $2B$, and all v for which $\|x\|_v > 1$. For all sufficiently small $\epsilon > 0$ the set $U_x := U_\epsilon(x,S)$ is an open neighborhood of x disjoint from $\mathbb{I}_K^1$ because for every $y \in U_x$, 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 $\|y\|_v < 1/(2B)$ and $\|y\| < 1$.

This proves that $\mathbb{I}_K^1$ is closed in $\mathbb{A}_K$, and therefore also in $\mathbb{I}_K$. To prove that the subspace topologies coincide, it suffices to show that for every $x \in \mathbb{I}_K^1$ and open $U \subseteq \mathbb{I}_K$ containing x there exists open sets $V \subseteq \mathbb{I}_K$ and $W \subseteq \mathbb{A}_K$ such that $x \in V \subseteq U$ and $V \cap \mathbb{I}_K^1 = W \cap \mathbb{I}_K^1$; this implies that every neighborhood basis in the subspace topology of $\mathbb{I}_K^1 \subseteq \mathbb{I}_K$ is a neighborhood basis in the subspace topology of $\mathbb{I}_K^1 \subseteq \mathbb{A}_K$ (the latter is *a priori* coarser than the former).

So consider any $x \in \mathbb{I}_K^1$ and open neighborhood $U \subseteq \mathbb{I}_K$ of x. Then U contains a basic open set

$$V = \{u \in \mathbb{A}_K : \|u - x\|_v < \epsilon \text{ for } v \in S \text{ and } \|u\|_v = 1 \text{ for } v \notin S\},$$

for some $\epsilon > 0$ and finite $S \subseteq M_K$ (take $S = \{v \in M_K : \|x\| \neq 1\}$ and $\epsilon > 0$ small enough). If we now put $W := U_\epsilon(x,S)$ then $x \in V \subseteq U$ and $V \cap \mathbb{I}_K^1 = W \cap \mathbb{I}_K^1$ as desired. □

Theorem 26.9. *For any global field K, the group $K^\times$ is a discrete cocompact subgroup of the group of 1-ideles $\mathbb{I}_K^1$.*

Proof. By Proposition 26.6, $K^\times$ is discrete in $\mathbb{I}_K$, and therefore discrete in the subspace $\mathbb{I}_K^1$.

As in the proof of Theorem 25.12, to prove that $K^\times$ is cocompact in $\mathbb{I}_K^1$ it suffices to exhibit 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 26.8: $\mathbb{I}_K^1$ is closed so $W \cap \mathbb{I}_K^1$ is compact).

To construct W we first choose $a \in \mathbb{A}_K$ such that $\|a\| > B_K$, where B_K is the Blichfeldt-Minkowski constant in Lemma 25.14, and let

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

Now consider any $u \in \mathbb{I}_K^1$. We have $\|u\| = 1$, so $\|\frac{a}{u}\| = \|a\| > B_K$, and by Lemma 25.14 there is a $z \in K^\times$ for which $\|z\|_v \le \left\|\frac{a}{u}\right\|_v$ for all $v \in M_K$. Therefore $zu \in W$. Thus every $u \in \mathbb{I}_K^1$ can be written as $u = z^{-1} \cdot zu$ with $z^{-1} \in K^\times$ and $zu \in W \cap \mathbb{I}_K^1$. Thus $W \cap \mathbb{I}_K^1$ 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 it follows that $\mathbb{I}_K^1/K^\times$ is compact. □

Definition 26.10. For a global field K the compact group $C_K^1 := \mathbb{I}_K^1/K^\times$ is the *norm-1 idele class group.*

Remark 26.11. When K is a function field the norm-1 idele class group C_K^1 is totally disconnected, in addition to being a compact group, and thus a *profinite group.*

26.2 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 $\operatorname{Gal}(K^{\mathrm{ab}}/K)$, which is an example of a *profinite group.*

Definition 26.12. 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 can 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 $g \in G$ to the sequence 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 inverse limits. For every continuous homomorphism $\varphi\colon G \to H$ with H a profinite group, 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 much one can say about profinite groups but we shall limit ourselves to a few remarks and statements of the main results we need, deferring most of the proofs to Problem Set 11. See [4] for a comprehensive treatment of profinite groups.

Remark 26.13. 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 [5].[2]

Remark 26.14. The profinite completion of G as a topological group is not necessarily the same thing as the profinite completion of G as a group if we forget 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 completions as groups are said to be *strongly complete*; this is equivalent to requiring every finite index subgroup to be open (see Corollary 26.19 below). It is known that if G is finitely generated as a topological group (meaning it contains a finitely generated dense subgroup), then G is strongly complete [3]. This applies, for example, to $\operatorname{Gal}(\bar{\mathbb{F}}_q/\mathbb{F}_q)$ for any finite field $\mathbb{F}_q$, since the q-power Frobenius automorphism generates a dense subgroup (it is thus a *topological generator*).

Remark 26.15. 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.

[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 $g + N_i \leftarrow\!\shortmid g + N_j$ on the quotients.

[2] For countable direct systems of locally compact groups this issue does not arise [5, Thm. 2.7].

Example 26.16. 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 26.17. *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 26.18. *A topological group is profinite if and only if it is a totally disconnected compact group.*

Proof. See Problem Set 11. □

Corollary 26.19. *Let G be a 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 (in other words, strongly complete) 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. □

26.3 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) fails spectacularly. As you proved on Problem Set 5 in the case $\mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q) \simeq \widehat{\mathbb{Z}} \simeq \prod_p \mathbb{Z}_p$, 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 [2, 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 26.20. *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, the second map is induced by restriction, and we have

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

This lemma is a list of things we already know to be true for finite Galois extensions, the point is simply to verify that they also hold for infinite Galois extensions; this seems prudent given the aforementioned failure of the Galois correspondence.

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 4.9). The restriction map is surjective because any $\sigma \in \operatorname{Gal}(F/K)$ can be extended to $\operatorname{Gal}(L/K)$, by Theorem 4.9, 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 $\overline{\mathbb{Q}}/\mathbb{Q}$, nor is the the Galois group of $\overline{\mathbb{Q}}/K$ for any subextension $K/\mathbb{Q}$. It is thus necessary to distinguish the subgroups of $\operatorname{Gal}(L/K)$ that are actually Galois groups of a subextension. This is achieved by putting an appropriate topology on the Galois group.

Definition 26.21. Let L/K be a Galois extension with Galois group $G := \operatorname{Gal}(L/K)$. The *Krull topology* on G has the basis consisting of 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 26.22. *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 normal extension F/K.

Proof. Every $\alpha \in L$ is algebraic over K, hence lies in some finite normal subextension F/K (take the normal closure of $K(\alpha)$). Every automorphism in $\operatorname{Gal}(L/K)$ is thus uniquely determined by its restrictions to finite normal 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 26.20, 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 in $\varprojlim G/H_F$, since every open set in G is a union of cosets of open subgroups. If $H = \operatorname{Gal}(L/F)$ then

$$\phi(H) = \{(\sigma_E) : \sigma_{E|_{E\cap F}} = \mathrm{id}_{|_{E\cap F}}\} = \pi_F^{-1}(\mathrm{id}_{|_F}),$$

where E/K ranges over finite normal subextensions of L/K and π_F is the projection map from the inverse limit to $\operatorname{Gal}(F/K)$. The singleton set $\{\mathrm{id}_{|_F}\}$ is open in the discrete group $\operatorname{Gal}(E/F)$, so its inverse image under the continuous projection π_F is open in G.

The last statement follows from Corollary 26.19 and Lemma 26.20. □

Theorem 26.23 (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 reversing 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 26.20.

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 26.20), 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 26.20. □

Corollary 26.24. *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 $\sigma \in \operatorname{Gal}(L/K)$ that fixes F (by definition), and $\operatorname{Gal}(L/F)$ is a closed subgroup of $\operatorname{Gal}(L/K)$ with $L^{\operatorname{Gal}(L/F)} = F$, by Theorem 26.23. We thus have $H \subseteq \overline{H} \subseteq \operatorname{Gal}(L/F)$ with the same fixed field F. The last two groups are closed and therefore equal under the bijection given by Theorem 26.23. □

We conclude this section with the following theorem due to Waterhouse [6].

Theorem 26.25 (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 [6, Thm. 1]. □

Remark 26.26. 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 all finite groups G.

References

[1] Nicolas Bourbaki, *General Topology: Chapters 1-4*, Springer, 1995.

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

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

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

[5] 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.

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

18.785 Number Theory I
Fall 2019