INFINITE GALOIS THEORY (DRAFT, CTNT 2020)

KEITH CONRAD

1. Introduction

Galois theory is about field extensions with “a lot” of automorphisms. Our goal in these lectures is to extend Galois theory from finite extensions to infinite-degree extensions. It turns out that the Galois correspondence for infinite-degree extensions runs into problems: there are mappings in both directions as in the finite case, from intermediate fields to subgroups of the Galois group and *vice versa*, but it is no longer a bijection: there are too many subgroups, so more than one subgroup can have the same fixed field. This was discovered in an example by Dedekind in 1901, who wrote [1, p. 15] that the situation could be fixed by making an infinite Galois group into a “stetige Mannigfaltigkeit” (continuous manifold). Krull [2], in 1928, proposed how to use topology to rescue the Galois correspondence, and this viewpoint is essential in how infinite Galois groups are studied today.

2. Review of finite Galois theory

For an extension of fields L/K, write $\mathrm{Aut}(L/K)$ for the K-automorphisms of L: these are the isomorphisms $L \to L$ that fix each element of K. When L/K is a finite extension,

(1) every $\alpha \in L$ is algebraic over K: $f(\alpha) = 0$ for some nonzero $f(X) \in K[X]$,
(2) the group $\mathrm{Aut}(L/K)$ is finite with size $\leq [L : K]$.

Example 2.1. $\mathrm{Aut}(\mathbf{Q}(i)/\mathbf{Q}) = \{\alpha \mapsto \alpha, \alpha \mapsto \overline{\alpha}\}$.

Example 2.2. $\mathrm{Aut}(\mathbf{Q}(\sqrt[3]{2})/\mathbf{Q})$ is trivial, even though $[\mathbf{Q}(\sqrt[3]{2}) : \mathbf{Q}] = 3$.

Example 2.3. $\mathrm{Aut}(\mathbf{Q}(\sqrt[4]{2})/\mathbf{Q})$ has size 2 even though $[\mathbf{Q}(\sqrt[4]{2}) : \mathbf{Q}] = 4$: the automorphisms send $\sqrt[4]{2}$ to $\pm\sqrt[4]{2}$ and both fix $\sqrt{2}$, so $\mathrm{Aut}(\mathbf{Q}(\sqrt[4]{2})/\mathbf{Q}) = \mathrm{Aut}(\mathbf{Q}(\sqrt[4]{2})/\mathbf{Q}(\sqrt{2}))$.

The following properties turn out to be equivalent for a finite extension L/K:

(1) $|\mathrm{Aut}(L/K)| = [L : K]$,
(2) L is a splitting field over K of a separable polynomial in $K[X]$,
(3) The only elements of L fixed by $\mathrm{Aut}(L/K)$ are the elements of K,
(4) L/K is both separable (every element of L has a separable minimal polynomial over K) and normal (every irreducible polynomial in $K[X]$ that has a root in L splits completely over L).

When these properties hold, L/K is called a *Galois* extension and we write $\mathrm{Aut}(L/K)$ as $\mathrm{Gal}(L/K)$, calling it the *Galois group* of L over K.

Example 2.4. Consider $K = \mathbf{Q}$ and $L = \mathbf{Q}(\sqrt{2}, \sqrt{3})$. We have $[L : \mathbf{Q}] = 4$ and L is the splitting field over $\mathbf{Q}$ of $(X^2-2)(X^2-3)$, which is separable. Therefore L/K is Galois. The Galois group $\mathrm{Gal}(L/\mathbf{Q})$ is isomorphic to $\{\pm 1\} \times \{\pm 1\}$ by associating to each automorphism σ in the Galois group the pair of signs by which it affects the square roots of 2 and the square roots of 3 (in a definite order, to pin down the isomorphism to $\{\pm 1\} \times \{\pm 1\}$.

Example 2.5. (Cyclotomic extensions) Consider $K = \mathbf{Q}$ and $L = \mathbf{Q}(\zeta_m)$ where ζ_m is a root of unity of order m (*e.g.*, $\zeta_m = e^{2\pi i/m}$ in $\mathbf{C}$). Extensions generated by a root of unity are called cyclotomic ("circle-dividing"). All the roots of unity of order m are ζ_m^a where $(a, m) = 1$, so L is a splitting field over $\mathbf{Q}$ of $X^m - 1$, which has distinct roots, so $L/\mathbf{Q}$ is Galois. It turns out that $[L : \mathbf{Q}] = \varphi(m)$, so the roots of unity with order m are all roots of the same minimal polynomial over $\mathbf{Q}$ (called the mth cyclotomic polynomial).

Since a is only determined from ζ_m^a as an integer modulo m, the condition $(a, m) = 1$ when ζ_m^a has order m amounts to saying $a \in (\mathbf{Z}/m\mathbf{Z})^\times$. Therefore $\mathrm{Gal}(\mathbf{Q}(\zeta_m)/\mathbf{Q}) \cong (\mathbf{Z}/m\mathbf{Z})^\times$ by $\sigma \mapsto a(\sigma) \bmod m$ where $\sigma(\zeta_m) = \zeta_m^{a(\sigma)}$. (If one root of unity of order m is sent to a particular power by σ, all other mth roots of unity are sent to the same power.)

Note: Over base fields other than $\mathbf{Q}$, the roots of unity of order m may have smaller degree than $\varphi(m)$, *e.g.*, $\mathbf{R}(\zeta_m) = \mathbf{C}$ when $m \geq 3$, so $[\mathbf{R}(\zeta_m) : \mathbf{R}]$ is 2 when $m \geq 3$.

Example 2.6. Let $K = \mathbf{Q}$ and $L = \mathbf{Q}(\sqrt[4]{2}, i)$. Here $[L : \mathbf{Q}] = 8$ and a $\mathbf{Q}$-automorphism $\sigma \colon L \to L$ is determined by $\sigma(\sqrt[4]{2})$ and $\sigma(i)$. The first value has at most four choices (the four roots of $X^4 - 2$) and the second value has at most two choices (the two roots of $X^2 + 1$). Therefore $|\mathrm{Aut}(L/\mathbf{Q})| \leq 8$. All 8 options work: L is the splitting field over $\mathbf{Q}$ of $X^4 - 2$, which is irreducible and separable over $\mathbf{Q}$. By looking at elements of $\mathrm{Gal}(L/\mathbf{Q})$ by how they permute the four different fourth roots of 2, the 8 permutations of the four roots make $\mathrm{Gal}(L/\mathbf{Q})$ isomorphic to the dihedral group of order 8.

Example 2.7. For an odd prime p, let $L = \mathbf{Q}(\sqrt[p]{2}, \zeta_p)$ where ζ_p is a nontrivial pth root of unity. This is the splitting field over $\mathbf{Q}$ of $X^p - 2$, which is irreducible (and separable, as we're in characteristic 0). The elements σ of $\mathrm{Gal}(L/\mathbf{Q})$ are determined by the values of $\sigma(\zeta_p)$ and $\sigma(\sqrt[p]{2})$:

$$\sigma(\zeta_p) = \zeta_p^{a(\sigma)}, \qquad \sigma(\sqrt[p]{2}) = \zeta_p^{b(\sigma)} \sqrt[p]{2},$$

where $a(\sigma) \in (\mathbf{Z}/p\mathbf{Z})^\times$ and $b(\sigma) \in \mathbf{Z}/p\mathbf{Z}$. Composition of two automorphisms σ and τ in $\mathrm{Gal}(L/\mathbf{Q})$ affects the exponents on ζ_p in the same way that the matrices

$$\begin{pmatrix} a(\sigma) & b(\sigma) \\ 0 & 1 \end{pmatrix}$$

multiply:

$$\sigma(\tau(\zeta_p)) = \sigma(\zeta_p^{a(\tau)}) = \sigma(\zeta_p)^{a(\tau)} = (\zeta_p^{a(\sigma)})^{a(\tau)} = \zeta_p^{a(\sigma)a(\tau)}$$

and

$$\sigma(\tau(\sqrt[p]{2})) = \sigma(\zeta_p^{b(\tau)} \sqrt[p]{2}) = \sigma(\zeta_p)^{b(\tau)} \sigma(\sqrt[p]{2}) = (\zeta_p^{a(\sigma)})^{b(\tau)} \zeta_p^{b(\sigma)} \sqrt[p]{2} = \zeta_p^{a(\sigma)b(\tau)+b(\sigma)} \sqrt[p]{2}.$$

This matches the equation

$$\begin{pmatrix} a(\sigma) & b(\sigma) \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a(\tau) & b(\tau) \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} a(\sigma)a(\tau) & a(\sigma)b(\tau) + b(\sigma) \\ 0 & 1 \end{pmatrix}.$$

Therefore $\mathrm{Gal}(L/\mathbf{Q})$ is isomorphic to the matrix group $\{(\begin{smallmatrix} a & b \\ 0 & 1 \end{smallmatrix}) : a \in (\mathbf{Z}/p\mathbf{Z})^\times, b \in \mathbf{Z}/p\mathbf{Z}\}$.

For a finite Galois extension L/K, the Galois correspondence associates to each subgroup H of $\mathrm{Gal}(L/K)$ the intermediate field $L^H = \{\alpha \in L : \sigma(\alpha) = \alpha \text{ for all } \sigma \in H\}$, where $K \subset L^H \subset L$, and to each intermediate field E the subgroup $\mathrm{Gal}(L/E)$, which fixes E. This is illustrated by the following field diagram.

$$\begin{tikzcd}
L \arrow[r, leftrightarrow] \arrow[d, no head] & \{id.\} \arrow[d, no head] \\
E \arrow[r, leftrightarrow] \arrow[d, no head] & H \arrow[d, no head] \\
K \arrow[r, leftrightarrow] & G
\end{tikzcd}$$

$$H = \mathrm{Gal}(L/E), \quad E = L^H = \{\alpha \in L : \sigma(\alpha) = \alpha \text{ for all } \sigma \in H\}.$$

Theorem 2.8 (Galois). *Let L/K be a finite Galois extension with $G = \mathrm{Gal}(L/K)$. The inclusion-reversing mappings $E \mapsto \mathrm{Gal}(L/E)$ and $H \mapsto L^H$ between the intermediate fields between K and L and the subgroups of G are inverses of each other and satisfy the following properties when E and H correspond ($E = L^H, H = \mathrm{Gal}(L/E)$):*

(a) $|H| = [L : E]$ *and* $[E : K] = [G : H]$,

(b) *two intermediate fields E and E', with corresponding subgroups H and H', are isomorphic over K if and only if H and H' are conjugate subgroups of G; in particular,* $\mathrm{Gal}(L/\sigma(E)) = \sigma \mathrm{Gal}(L/E)\sigma^{-1}$ *for* $\sigma \in G$,

(c) *E/K is Galois if and only if $H \lhd G$, in which case the restriction map $G \to \mathrm{Gal}(E/K)$, where $\sigma \mapsto \sigma|_E$, is surjective with kernel H, so $G/H \cong \mathrm{Gal}(E/K)$.*

In (2.1) we indicate the relations of part a in a diagram, where $E = L^H$ and $H = \mathrm{Gal}(L/E)$ correspond to each other. Because inclusion relations are reversed, the group diagram appears upside-down, with the larger subgroups near the bottom (having a fixed field that is closer to K).

(2.1)
$$\begin{tikzcd}
L \arrow[d, no head] & \{1\} \arrow[d, no head, "{[L:F]}"] \\
E \arrow[d, no head] & H \arrow[d, no head, "{[F:K]}"] \\
K & G
\end{tikzcd}$$

Part (c) of Theorem 2.8 explains why normal field extensions get their name: in the context of a finite Galois extension L/K, where every intermediate field is separable over the base field, the intermediate fields that are normal (equivalently, Galois) over the base are those whose corresponding subgroups in $\mathrm{Gal}(L/K)$ are normal subgroups.

3. Infinite-degree Galois extensions and a problem

We want to relax the condition on field extensions L/K being finite, but keep them algebraic: each element of L should be the root of a nonconstant polynomial in $K[X]$.

Example 3.1. Three algebraic extensions of $\mathbf{Q}$ that are not finite extensions are the composite of all quadratic fields

$$\mathbf{Q}(\sqrt{-1}, \sqrt{2}, \sqrt{3}, \sqrt{5}, \sqrt{7}, \dots),$$

the p-power cyclotomic extension

$$\mathbf{Q}(\zeta_{p^\infty}) = \bigcup_{n \geq 1} \mathbf{Q}(\zeta_{p^n})$$

where $\zeta_{p^n} = e^{2\pi i/p^n}$, and the algebraic closure $\overline{\mathbf{Q}}$.

Even when an algebraic extension L/K has infinite-degree, it has a built-in finiteness: every finite set of elements of L lies in a finite subextension of K. That is, every algebraic extension is a union of finite extensions.

Theorem 3.2. *For an algebraic extension L/K, the following properties are equivalent:*

(1) $L = \bigcup_i L_i$, *with each L_i/K a finite Galois extension,*
(2) L *is the splitting field over K of a set of separable polynomials in $K[X]$,*
(3) $L^{\mathrm{Aut}(L/K)} = K$,
(4) L/K *is both separable (every element of L has a separable minimal polynomial over K) and normal (every irreducible polynomial in $K[X]$ that has a root in L splits completely over L).*

Proof. Exercise 3.2. □

Definition 3.3. We call an algebraic extension L/K *Galois* if it satisfies the conditions in Theorem 3.2.

Example 3.4. All three field extensions of $\mathbf{Q}$ in Example 3.1 are Galois over $\mathbf{Q}$.

Definition 3.5. When L/K is a Galois extension, we set its *Galois group* $\mathrm{Gal}(L/K)$ to be the group of all K-automorphisms of L.

When L/K is an infinite Galois extension, it is often impossible to write down concrete formulas for elements of $\mathrm{Gal}(L/K)$. What we can do is indicate how we want an automorphism to look on a subfield and then know it can be extended (in many ways) to an automorphism in $\mathrm{Gal}(L/K)$ by using Zorn's lemma; see Corollary A.2. For instance, the conjugation automorphism in $\mathrm{Gal}(\mathbf{Q}(\sqrt{2})/\mathbf{Q})$ where $a+b\sqrt{2} \mapsto a-b\sqrt{2}$ can be extended (or "lifted") all the way up to an element of $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$, but it's hopeless to expect any kind of general formula for elements of $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ other than the identity and complex conjugation.

The following two examples are about infinite-degree Galois extensions L/K where all the elements of $\mathrm{Gal}(L/K)$ have concrete descriptions.

Example 3.6. The group $\mathrm{Gal}(\mathbf{Q}(\sqrt{-1}, \sqrt{2}, \sqrt{3}, \sqrt{5}, \sqrt{7}, \dots)/\mathbf{Q})$ is the countable direct product (not direct sum!) of copies of $\{\pm 1\}$, each factor being a choice of sign by which an automorphism affects $\sqrt{-1}$ or $\sqrt{p}$ for a prime p.

Example 3.7. For prime p, since $\mathbf{Q}(\zeta_{p^\infty}) = \bigcup_{n \geq 1} \mathbf{Q}(\zeta_{p^n})$ we can describe an element σ of $\mathrm{Gal}(\mathbf{Q}(\zeta_{p^\infty})/\mathbf{Q})$ by indicating what σ looks like on each field $\mathbf{Q}(\zeta_{p^n})$. By finite Galois theory, $\mathrm{Gal}(\mathbf{Q}(\zeta_{p^n})/\mathbf{Q}) \cong (\mathbf{Z}/p^r\mathbf{Z})^\times$ by $\sigma(\zeta_{p^n}) = \zeta_{p^n}^{a_n}$ for some integer $a_n \bmod p^n$ where $(a_n, p) = 1$.

$$\begin{tikzcd}
\mathbf{Q}(\zeta_{p^\infty}) \\
\vdots \\
\mathbf{Q}(\zeta_{p^3}) \arrow[d, dash] \\
\mathbf{Q}(\zeta_{p^2}) \arrow[d, dash] \\
\mathbf{Q}(\zeta_p)
\end{tikzcd}$$

Each σ gives us a list of numbers $a_n \bmod p^n$ in $(\mathbf{Z}/p^n\mathbf{Z})^\times$, but they are not independent of each other: there is a *compatibility condition* between them: from $\zeta_{p^{n+1}}^p = \zeta_{p^n}$ we have

$$\sigma(\zeta_{p^{n+1}}^p) = \sigma(\zeta_{p^n}) \Longrightarrow \sigma(\zeta_{p^{n+1}})^p = \zeta_{p^n}^{a_n} \Longrightarrow (\zeta_{p^{n+1}}^{a_{n+1}})^p = \zeta_{p^n}^{a_n} \Longrightarrow \zeta_{p^n}^{a_{n+1}} = \zeta_{p^n}^{a_n},$$

so $\boxed{a_{n+1} \equiv a_n \bmod p^n}$. Two examples of this are (i) $a_n = a$ for a common integer a and (ii) $a_n = 1 + p + \cdots + p^{n-1}$.

Conversely, a list of $a_n \bmod p^n \in (\mathbf{Z}/p^n\mathbf{Z})^\times$ for all $n \geq 1$ where $a_{n+1} \equiv a_n \bmod p^n$ for all n leads to an automorphism σ in $\mathrm{Gal}(\mathbf{Q}(\zeta_{p^\infty})/\mathbf{Q})$; see Exercise 3.5.

Finite-degree Galois extensions have finite Galois groups. For infinite-degree Galois extensions, the Galois group is always infinite.

Theorem 3.8. *If L/K is an infinite-degree Galois extension then $\mathrm{Gal}(L/K)$ is an infinite group.*

Proof. We'll prove the contrapositive. If $\mathrm{Gal}(L/K)$ is finite, say of order m, then each $\alpha \in L$ has degree at most m over K, so there is a uniform upper bound on the degrees over K of all elements of L. That implies L/K is finite by [6, Chap. VII, Lemma 4.8]. □

Theorem 3.9. *If L/K is a Galois extension then for each $\alpha \in L$, the roots of its minimal polynomial over K are $\{\sigma(\alpha) : \sigma \in \mathrm{Gal}(L/K)\}$.*

Proof. Since L/K is Galois, there is a finite Galois extension F/K inside L that contains α. By *finite Galois theory* the K-conjugates of α are $\{\varphi(\alpha) : \varphi \in \mathrm{Gal}(F/K)\}$. Corollary A.2 says that for $\varphi \in \mathrm{Gal}(F/K)$, $\varphi(\alpha) = \sigma(\alpha)$ for some $\sigma \in \mathrm{Gal}(L/K)$, so $\{\varphi(\alpha) : \varphi \in \mathrm{Gal}(F/K)\} \subset \{\sigma(\alpha) : \sigma \in \mathrm{Gal}(L/K)\}$. Conversely, for $\sigma \in \mathrm{Gal}(L/K)\}$ and $f(X)$ the minimal polynomial of α over K, the equation $f(\alpha) = 0$ implies $f(\sigma(\alpha)) = 0$ (the coefficients of $f(X)$ are in K and thus are not changed by σ), so $\sigma(\alpha)$ is a K-conjugate of α. □

Watch out: that $\mathrm{Gal}(L/K)$ may be an infinite set does *not* make $\{\sigma(\alpha) : \sigma \in \mathrm{Gal}(L/K)\}$ infinite: that set is always finite since it's the K-conjugates of α; it has enormous repetitions in it. For example if $c \in K$ then $\{\sigma(c) : \sigma \in \mathrm{Gal}(L/K)\} = \{c\}$. An analogue in finite Galois theory is that $\{\sigma(\alpha) : \sigma \in \mathrm{Gal}(L/K)\}$ can have size smaller than $|\mathrm{Gal}(L/K)|$, but in a finite extension there will be some elements (primitive elements) for which $L = K(\alpha)$ and then the number of K-conjugates is $[L : K]$. For infinite Galois extensions that never happens.

We now explain, using Examples 3.6 and 3.7 why there are *too many* subgroups of these Galois groups to have a one-to-one correspondence between subgroups of the Galois group and intermediate fields.

Example 3.10. Let $L = \mathbf{Q}(\sqrt{-1}, \sqrt{2}, \sqrt{3}, \sqrt{5}, \sqrt{7}, \dots)$, so $\mathrm{Gal}(L/\mathbf{Q}) = \prod\{\pm 1\}$, a countable direct product of the group $\{\pm 1\}$. This is an abelian group where each non-identity element has order 2. The group $\mathrm{Gal}(L/\mathbf{Q})$ is uncountable (why?), so $\mathrm{Gal}(L/\mathbf{Q})$ has uncountably many subgroups of order 2. At the same time, L has only countably many subfields of each 2-power degree over $\mathbf{Q}$. Therefore the subfields of L and the subgroups of $\mathrm{Gal}(L/\mathbf{Q})$ do not have the same cardinality.

Example 3.11. In Example 3.7 use $p = 2$: set $L = \mathbf{Q}(\zeta_{2^\infty}) = \bigcup_{r \geq 1} \mathbf{Q}(\zeta_{2^n})$. Then $\mathrm{Gal}(\mathbf{Q}(\zeta_{2^n})/\mathbf{Q}) \cong (\mathbf{Z}/2^n\mathbf{Z})^\times$.

$$\begin{tikzcd}
\mathbf{Q}(\zeta_{2^\infty}) \arrow[r, phantom, "="] & L \\
\vdots & \\
\mathbf{Q}(\zeta_8) \arrow[d, dash] & \\
\mathbf{Q}(\zeta_4) \arrow[r, phantom, "="] \arrow[d, dash] & \mathbf{Q}(i) \\
\mathbf{Q}(\zeta_2) \arrow[r, phantom, "="] & \mathbf{Q}
\end{tikzcd}$$

For odd a in $\mathbf{Z}$, let $\sigma_a \in \mathrm{Gal}(L/\mathbf{Q})$ by $\zeta_{2^n} \mapsto \zeta_{2^n}^a$ for all r. We'll use $a = 5$ and $a = 13$:

$$\sigma_5(\zeta_{2^n}) = \zeta_{2^n}^5, \quad \sigma_{13}(\zeta_{2^n}) = \zeta_{2^n}^{13}.$$

Let $H = \langle \sigma_5 \rangle$ and $H' = \langle \sigma_{13} \rangle$. The cyclic subgroups H and H' in $\mathrm{Gal}(L/\mathbf{Q})$ are not the same: if they were equal then the generator σ_{13} of H' would be one of the generators $\sigma_5^{\pm 1}$ of H, which would mean (when applied to ζ_{2^n})

$$\zeta_{2^n}^{13} = \zeta_{2^n}^{5^{\pm 1}},$$

so $13 \equiv 5^{\pm 1} \bmod 2^n$ for *all* n. Thus $13 = 5^{\pm 1}$, which is incorrect.

Even though $H \neq H'$, let's see that $L^H = L^{H'}$! Set $L_n = \mathbf{Q}(\zeta_{2^n})$. Then

$$\mathrm{Gal}(L_n/\mathbf{Q}) \cong (\mathbf{Z}/2^n\mathbf{Z})^\times \text{ by } \sigma_a(\zeta_{2^n}) = \zeta_{2^n}^a.$$

$$\begin{tikzcd}
\mathbf{Q}(\zeta_{2^n}) \arrow[r, phantom, "="] & L_r \\
\vdots & \\
\mathbf{Q}(\zeta_4) \arrow[r, phantom, "="] \arrow[d, dash] & \mathbf{Q}(i) \\
\mathbf{Q}(\zeta_2) \arrow[r, phantom, "="] & \mathbf{Q}
\end{tikzcd}$$

Since $5, 13 \equiv 1 \bmod 4$, σ_5 and σ_{13} both fix i, so $\mathbf{Q}(i)$ is in both L^H and $L^{H'}$.

For $n \geq 2$, it turns out that $\langle 5 \bmod 2^n \rangle = \langle 13 \bmod 2^n \rangle$ in $(\mathbf{Z}/2^n\mathbf{Z})^\times$ and both subgroups have index 2 (see Exercise 3.8). Since those two subgroups are the same, the subfields of L_n that are fixed by $5 \bmod 2^n$ and by $13 \bmod 2^n$ (as elements of $\mathrm{Gal}(L_n/\mathbf{Q})$, acting as the 5th and 13th power on ζ_{2^n}) are the same and by the *finite* Galois correspondence that common fixed field has degree 2 over $\mathbf{Q}$. Since $\mathbf{Q}(i)$ is known to be fixed and it has degree 2, it is the whole fixed field. Notice this field $\mathbf{Q}(i)$ is independent of n: $L_n^H = \mathbf{Q}(i)$ and $L_n^{H'} = \mathbf{Q}(i)$ for all $n \geq 2$. Every element of L is inside some L_n, so $L^H = \mathbf{Q}(i) = L^{H'}$.

We have met two different subgroups of $\mathrm{Gal}(L/\mathbf{Q})$ with the same fixed field, so the Galois correspondence breaks down. The particular example of this in Example 3.11 was essentially discovered by Dedekind [1] in 1901, although he used odd primes instead of the prime 2 (Exercise 3.9).

To fix the Galois correspondence for infinite-degree Galois extensions, Krull defined a topology on Galois groups so that there is a one-to-one correspondence between intermediate fields and *closed* subgroups of the Galois group. (For a finite Galois extension this topology turns out to be discrete, which is why it's unnecessary to use topology when learning finite Galois theory.) The topology is defined in Section 4. Intuitively, what it means for two automorphisms σ and σ' in $\mathrm{Gal}(L/K)$ to be "close" in this topology is that $\sigma = \sigma'$ on a finite subextension F/K with large degree: the larger the degree, the "closer" the automorphisms because a larger finite extension F/K in L covers more of L.

Exercises.

1. Let $L = \mathbf{Q}(\{\sqrt[p]{2} : p \geq 3 \text{ prime}\})$. Show $\operatorname{Aut}(L/\mathbf{Q})$ is trivial How does the group $\operatorname{Aut}(L/\mathbf{Q})$ change if we include $p = 2$? What if $L = \mathbf{Q}(\{\sqrt[n]{2} : n \geq 3 \text{ odd}\})$?
2. Prove Theorem 3.2.
3. When L/K is Galois and E is an intermediate field between L and K, show L/E is Galois.
4. Work out the calculation of $\operatorname{Gal}(L/\mathbf{Q})$ in Example 3.6.
5. In Example 3.7, show to each list of numbers $a_n \bmod p^n \in (\mathbf{Z}/p^n\mathbf{Z})^\times$ for $n \geq 1$ such that $a_{n+1} \equiv a_n \bmod p^n$ for all r that there is an automorphism $\sigma \in \operatorname{Gal}(\mathbf{Q}(\zeta_{p^\infty})/\mathbf{Q})$ such that $\sigma(\zeta_{p^n}) = \zeta_{p^n}^{a_n}$ for all n.
6. Fill in details in Example 3.10: why does the Galois group in that example have uncountable many subgroups and why does the field L have only countably many subfields?
7. In Example 3.11, show the subgroups H and H' have trivial intersection.
8. For an integer a, if $a \equiv 1 \bmod 4$ and $a \not\equiv 1 \bmod 8$ then prove (i) $a^{2^k} \equiv 1 \bmod 2^{k+2}$ and $a^{2^k} \not\equiv 1 \bmod 2^{k+3}$ for $k \geq 0$ and (ii) the subgroup of $(\mathbf{Z}/2^n\mathbf{Z})^\times$ generated by a can be described as follows:

   $$\langle a \bmod 2^n \rangle = \{x \bmod 2^n : x \equiv 1 \bmod 4\} = \ker((\mathbf{Z}/2^n\mathbf{Z})^\times \to (\mathbf{Z}/4\mathbf{Z})^\times)$$

   for $n \geq 2$, where the map $(\mathbf{Z}/2^n\mathbf{Z})^\times \to (\mathbf{Z}/4\mathbf{Z})^\times$ is reduction, and $\langle a \bmod 2^n \rangle$ has index 2 in $(\mathbf{Z}/2^n\mathbf{Z})^\times$.

   For example, $a = 5$ and $a = 13$ fit the initial hypotheses mod 4 and mod 8, so they generate the same subgroup of $(\mathbf{Z}/2^n\mathbf{Z})^\times$ for all $n \geq 2$, and also for $n = 1$ by a direct check.
9. Let p be an odd prime.

   (a) For an integer a, if $a \equiv 1 \bmod p$ and $a \not\equiv 1 \bmod p^2$ (*e.g.*, $a = 1 + p$ or $a = 1 + (p-1)p$), then prove (i) $a^{p^k} \equiv 1 \bmod p^{k+1}$ and $a^{p^k} \not\equiv 1 \bmod p^{k+2}$ for $k \geq 0$ and (ii) the subgroup of $(\mathbf{Z}/p^n\mathbf{Z})^\times$ generated by a can be described as follows:

   $$\langle a \bmod p^n \rangle = \{x \bmod p^n : x \equiv 1 \bmod p\} = \ker((\mathbf{Z}/p^n\mathbf{Z})^\times \to (\mathbf{Z}/p\mathbf{Z})^\times)$$

   for $n \geq 1$, where the map $(\mathbf{Z}/p^n\mathbf{Z})^\times \to (\mathbf{Z}/p\mathbf{Z})^\times$ is reduction, and $\langle a \bmod p^n \rangle$ has index $p - 1$ in $(\mathbf{Z}/p^n\mathbf{Z})^\times$.

   (b) Use (a) to give an analogue of Example 3.11 in $\operatorname{Gal}(\mathbf{Q}(\zeta_{p^\infty})/\mathbf{Q})$: find two different cyclic subgroups of the Galois group with the same fixed field.

4. The topology on Galois groups

As mentioned at the end of the previous section, the key idea behind the topology that we will put on $\operatorname{Gal}(L/K)$ is to think of two elements of $\operatorname{Gal}(L/K)$ as being close if they are equal on a large finite extension of K inside L. Before we define the topology, let's see that the concept of automorphisms in $\operatorname{Gal}(L/K)$ being equal on a field intermediate between L and K has an algebraic interpretation in terms of lying in a common left coset.

Lemma 4.1. *Let L/K be a Galois extension with $G = \operatorname{Gal}(L/K)$.*

(1) *For $\sigma \in G$ and an intermediate field E between L and K, the coset $\sigma \operatorname{Gal}(L/E)$ is all automorphisms of G that look like σ on E: $\sigma \operatorname{Gal}(L/E) = \{\tau \in G : \tau|_E = \sigma|_E\}$.*

(2) *If F/K is a finite extension inside L then $\operatorname{Gal}(L/F)$ has index $[F : K]$ in $\operatorname{Gal}(L/K)$.*

It makes sense to talk about the "Galois" group $\operatorname{Gal}(L/E)$ because L is genuinely Galois over E: see Exercise 3.3.

Proof. (1) For $\varphi \in \mathrm{Gal}(L/E)$ and $\alpha \in E$, $(\sigma\varphi)(\alpha) = \sigma(\varphi(\alpha)) = \sigma(\alpha)$. Thus $\sigma\varphi = \sigma$ on E. Conversely, suppose $\tau \in G$ satisfies $\tau|_E = \sigma|_E$. Let $\varphi = \sigma^{-1}\tau \in G$, so $\tau = \sigma\varphi$. For $\alpha \in E$, $\tau(\alpha) = \sigma(\alpha)$, so $\sigma^{-1}(\tau(\alpha)) = \alpha$, or $\varphi(\alpha) = \alpha$. Therefore φ fixes all elements of E, so $\varphi \in \mathrm{Gal}(L/E)$ and $\tau = \sigma\varphi \in \sigma\,\mathrm{Gal}(L/E)$.

(2) The index of $\mathrm{Gal}(L/F)$ in $\mathrm{Gal}(L/K)$ is the number of left cosets or the number of right cosets. (It's the same number since inversion gives an intrinsic bijection between left and right cosets: $(gH)^{-1} = H^{-1}g^{-1} = Hg^{-1}$.) We'll use the left coset perspective because of part 1. To say $\sigma\,\mathrm{Gal}(L/F) = \tau\,\mathrm{Gal}(L/F)$ means $\sigma = \tau$ on F: σ and τ define the same field homomorphism $F \to L$ fixing K. Since F/K is a finite separable extension inside the Galois extension L/K, the number of field homomorphisms $F \to L$ that fix K is $[F : K]$. (Concretely this can be explained with the primitive element theorem: $F = K(\alpha)$ for some α. Therefore the number of field homomorphisms $K(\alpha) \to L$ that fix K is the number of K-conjugates of α in L. Since L/K is Galois, the number of K-conjugates of α in L is the degree of the minimal polynomial of α over K, which is $[K(\alpha) : K]$, and that's $[F : K]$.) Therefore the number of left cosets of $\mathrm{Gal}(L/F)$ in $\mathrm{Gal}(L/K)$ is $[F : K]$. □

To help you follow the notation, we will write "E" for an arbitrary intermediate field between L and K ("E" for "extension of K") and we will write "F" for a finite intermediate field extension of K inside L ("F" for "finite").

Definition 4.2. For $\sigma \in \mathrm{Gal}(L/K)$, a *basic open set* around σ or a *basic open neighborhood* of σ is a coset $\sigma\,\mathrm{Gal}(L/F)$ where F/K is a finite extension. A nonempty subset U of $\mathrm{Gal}(L/K)$ is *open* when each element of U is contained in a basic open set inside of U: for each $\sigma \in U$, $\sigma\,\mathrm{Gal}(L/F) \subset U$ for some finite extension F/K inside of L.

To check your understanding of the terminology here, every open set around the identity contains $\mathrm{Gal}(L/F)$ for some finite extension F/K in L. Indeed, open sets are defined to be unions of basic open sets and the basic open sets around the identity are defined to be the subgroups $\mathrm{Gal}(L/F)$.

Equivalently, by Lemma 4.1, a basic open set of σ in $\mathrm{Gal}(L/K)$ is the set of all elements of $\mathrm{Gal}(L/K)$ that look like σ on some finite extension F/K inside L. The intuition here is that a "small" open set around σ is all the automorphisms in $\mathrm{Gal}(L/K)$ that equal σ on a "big" finite extension of K inside L. Note that $F \subset F' \Rightarrow \mathrm{Gal}(L/F') \subset \mathrm{Gal}(L/F)$, so being equal to σ on a bigger subfield corresponds to a smaller open set around σ.

Theorem 4.3. *The open sets in* $\mathrm{Gal}(L/K)$ *as described above, along with the empty set, define a topology on* $\mathrm{Gal}(L/K)$.

Proof. A nonempty open set in $\mathrm{Gal}(L/K)$ is a union of cosets $\sigma_i\,\mathrm{Gal}(L/F_i)$ as σ_i and F_i vary. A union of open sets is a union of a union of such cosets, which is still a union of such cosets, so an arbitrary union of open sets is open (the case of the empty set is trivial).

If $U_1, \dots, U_n$ are finitely many open sets, we want to show $U_1 \cap \cdots \cap U_n$ is open. We can assume the intersection is not empty. Let σ be in the intersection. Since each U_i is open and contains σ, there are finite extensions $F_1, \dots, F_n$ of K in L such that $\sigma\,\mathrm{Gal}(L/F_i) \subset U_i$. The composite field $F := F_1 \cdots F_n$ is a finite extension of K containing each F_i, so $\mathrm{Gal}(L/F) \subset \mathrm{Gal}(L/F_i)$ for $i = 1, \dots, n$. Thus $\sigma\,\mathrm{Gal}(L/F) \subset U_i$ for $i = 1, \dots, n$, so $\sigma\,\mathrm{Gal}(L/F) \subset \bigcap_{i=1}^n U_i$. We showed each element of $\bigcap_{i=1}^n U_i$ is contained in a basic open set inside the intersection, so the intersection is open. □

The topology we have defined on $\mathrm{Gal}(L/K)$ is called its *Krull topology*. Let's see what it means in two earlier examples.

Example 4.4. For $\mathbf{Q}(\sqrt{-1},\sqrt{2},\sqrt{3},\sqrt{5},\sqrt{7},\dots)/\mathbf{Q}$, which has Galois group a countable product of copies of $\{\pm 1\}$, the Krull topology on this product is the product topology where each factor $\{\pm 1\}$ has the discrete topology (Exercise 4.1). Make sure you understand that the product topology on a direct product of infinitely many discrete spaces that are not 1-point sets is not discrete!

Example 4.5. For $\mathbf{Q}(\zeta_{p^\infty})/\mathbf{Q}$, which has for its Galois group the sequences $\{a_n \bmod p^n\}$ in $\prod_{n\geq 1}(\mathbf{Z}/p^n\mathbf{Z})^\times$ with compatibility condition $a_n \equiv a_{n-1} \bmod p^{n-1}$ for $n \geq 2$, two such compatible sequences $\{a_n \bmod p^n\}$ and $\{b_n \bmod p^n\}$ are "close" if the nth terms are equal for a set of early values of n: that is what it means for the automorphisms associated to these two sequences to be the same function on some $\mathbf{Q}(\zeta_{p^n})$. For instance, in $\operatorname{Gal}(\mathbf{Q}(\zeta_{5^\infty})/\mathbf{Q})$, the sequences

$$(2 \bmod 5, 2+3\cdot 5 \bmod 5^2, 2+3\cdot 5+5^2 \bmod 5^3,\dots)$$

and

$$(2 \bmod 5, 2+3\cdot 5 \bmod 5^2, 2+3\cdot 5+4\cdot 5^2 \bmod 5^3,\dots)$$

are equal in the first two components, and the automorphisms they define on $\mathbf{Q}(\zeta_{5^\infty})/\mathbf{Q}$ are equal on $\mathbf{Q}(\zeta_{5^2})$ but not on $\mathbf{Q}(\zeta_{5^3})$.

Every finite extension F/K in L can be enlarged to a finite Galois extension $\widetilde{F}/K$ in L, so every basic open set $\sigma\operatorname{Gal}(L/F)$ contains $\sigma\operatorname{Gal}(L/\widetilde{F})$. Therefore when dealing with a basic open neighborhood of an automorphism σ, by shrinking it we can assume the F defining the basic open neighborhood of σ is Galois over K. This will be used in the next theorem to prove continuity of multiplication and inversion for the Krull topology on $\operatorname{Gal}(L/K)$.

Theorem 4.6. *The topology on* $\operatorname{Gal}(L/K)$ *has the following properties.*

(1) *the operations of multiplication* $\operatorname{Gal}(L/K)\times\operatorname{Gal}(L/K)\to\operatorname{Gal}(L/K)$ *and inversion* $\operatorname{Gal}(L/K)\to\operatorname{Gal}(L/K)$ *are continuous.*

(2) *when* $\operatorname{Gal}(L/K)$ *is finite, the topology is discrete.*

(3) $\operatorname{Gal}(L/K)$ *is Hausdorff.*

The second property explains why topology is irrelevant to finite Galois theory.

Proof. (1) Recall in topology that continuity of a function $f\colon X\to Y$ can be described in two ways: a global way that says the inverse image of each open set in Y is open in X, and a local way (continuity at each point) that says for each x in X and open set V in Y containing $f(x)$, there is an open set U around x in X such that $f(U)\subset V$. When the topology is generated by a basis of open sets (such as the basic open sets in $\operatorname{Gal}(L/K)$, which are analogous to the open balls in a metric space), it suffices to take for V an open set from the basis since all (nonempty) open sets are unions of open sets in the basis. We will check continuity of multiplication and inversion using the pointwise description of continuity.

To show multiplication $m\colon \operatorname{Gal}(L/K)\times\operatorname{Gal}(L/K)\to\operatorname{Gal}(L/K)$ is continuous at a point $(\sigma,\tau)\in\operatorname{Gal}(L/K)\times\operatorname{Gal}(L/K)$, its product is $\sigma\tau$ in $\operatorname{Gal}(L/K)$ so we pick a basic open set $\sigma\tau\operatorname{Gal}(L/F)$ for a finite extension F/K, where by making F larger (but still finite over K) we can suppose F/K is a finite Galois extension. The set $\sigma\operatorname{Gal}(L/F)\times\tau\operatorname{Gal}(L/F)$ is an open set around (σ,τ) in the product $\operatorname{Gal}(L/K)\times\operatorname{Gal}(L/K)$: it is all pairs (f,g) such that $f=\sigma$ on F and $g=\tau$ on F. Then $fg=\sigma\tau$ on F: for $\alpha\in F$, $g(\alpha)=\tau(\alpha)$ and both are still in F (since F/K is Galois!), and thus $f(g(\alpha))=\sigma(\tau(\alpha))$, so $(f\circ g)(\alpha)=(\sigma\circ\tau)(\alpha)$ for all $\alpha\in F$. Thus $m(\sigma\operatorname{Gal}(L/F)\times\tau\operatorname{Gal}(L/F))\subset\sigma\tau\operatorname{Gal}(L/F)$, so multiplication is continuous at (σ,τ). This was proved for all (σ,τ), so multiplication on $\operatorname{Gal}(L/K)$ is continuous.

To show inversion $i\colon \operatorname{Gal}(L/K) \times \operatorname{Gal}(L/K)$ is continuous, pick $\sigma \in \operatorname{Gal}(L/K)$. A basic open set around σ^{-1} in $\operatorname{Gal}(L/K)$ is $\sigma^{-1}\operatorname{Gal}(L/F)$ for some finite extension F/K, and just as in the previous paragraph we can suppose F/K is Galois by passing to a smaller basic open set around σ^{-1}. If $f \in \sigma\operatorname{Gal}(L/F)$ then $f = \sigma$ on F. Since F/K is Galois, f and σ are automorphisms of F and thus their equality on F implies equality of their inverses on F: $f^{-1} = \sigma^{-1}$ on F. That shows $f^{-1} \in \sigma^{-1}\operatorname{Gal}(L/F)$, so inversion is continuous at σ. Since σ was arbitrary in $\operatorname{Gal}(L/K)$, inversion is continuous on $\operatorname{Gal}(L/K)$.

(2) If $\operatorname{Gal}(L/K)$ is finite then L/K is a finite extension by Theorem 3.8, in which case for each $\sigma \in \operatorname{Gal}(L/K)$ the set $\{\sigma\} = \sigma\operatorname{Gal}(L/L)$ is a basic open set around σ in $\operatorname{Gal}(L/K)$.

(3) Let σ and τ be two different elements of $\operatorname{Gal}(L/K)$, so there is an $\alpha \in L$ such that $\sigma(\alpha) \neq \tau(\alpha)$. The number α is contained in a finite extension F of K, such $K(\alpha)$. Then $\sigma|_F \neq \tau|_F$ since σ and τ are different at α, so $\sigma\operatorname{Gal}(L/F) \neq \tau\operatorname{Gal}(L/F)$. Different cosets of a subgroup are disjoint, so $\sigma\operatorname{Gal}(L/F)$ and $\tau\operatorname{Gal}(L/F)$ are disjoint basic open sets around σ and τ. That proves $\operatorname{Gal}(L/K)$ is Hausdorff. □

We are now ready to prove Krull's theorem that the Galois correspondence works for all intermediate fields and closed subgroups of the Galois group.

Theorem 4.7 (Krull)**.** *Let L/K be Galois and set $G = \operatorname{Gal}(L/K)$, equipped with the Krull topology. Associate to each intermediate field E the subgroup $\operatorname{Gal}(L/E)$ of G and associate to each subgroup H of G the intermediate field $L^H = \{\alpha \in L : h(\alpha) = \alpha \text{ for all } h \in H\}$.*

1. *For all E, $\operatorname{Gal}(L/E)$ is a closed subgroup of G.*
2. *For all H, $\operatorname{Gal}(L/L^H)$ is the closure of H in G.*
3. *(Galois correspondence) The mappings $E \mapsto \operatorname{Gal}(L/E)$ and $H \mapsto L^H$ are inclusion-reversing bijections between the intermediate fields in L/K and the closed subgroups of $\operatorname{Gal}(L/K)$, and they are inverses of each other: $L^{\operatorname{Gal}(L/E)} = E$ and $\operatorname{Gal}(L/L^H) = H$ when H is closed.*
4. *For an arbitrary subgroup $H \subset G$, $L^H = L^{\overline{H}}$.*

Although finite Galois theory appears to be a special case of this theorem (with the topology being discrete by Theorem 4.6), in fact our proofs of both (2) and (3) will rely on finite Galois theory. Therefore our approach to Theorem 4.7 is more like a generalization of finite Galois theory to infinite-degree Galois extensions.

Proof. (1): To prove $\operatorname{Gal}(L/E)$ is closed in G, we'll show *its complement is open.* There is nothing to check if $\operatorname{Gal}(L/E) = G$, so suppose there is some $\sigma \in G - \operatorname{Gal}(L/E)$, which means σ is not the identity on E: $\sigma(\alpha) \neq \alpha$ for some $\alpha \in E$.

There is a finite extension F/K inside L containing α. Then $\sigma\operatorname{Gal}(L/F)$ is a basic open set around σ and it is disjoint from $\operatorname{Gal}(L/E)$: everything in $\sigma\operatorname{Gal}(L/F)$ acts on F the same way σ does, which means everything in $\sigma\operatorname{Gal}(L/F)$ moves α, whereas everything in $\operatorname{Gal}(L/E)$ fixes α, since $\alpha \in E$. We have shown each element of G that is not in $\operatorname{Gal}(L/E)$ has a basic open set around it that is disjoint from $\operatorname{Gal}(L/E)$, so the complement of $\operatorname{Gal}(L/E)$ in G is open. Thus $\operatorname{Gal}(L/E)$ is closed. That completes the proof of (1).

(2): We have $H \subset \operatorname{Gal}(L/L^H)$ since each element of H fixes L^H (the elements of H fix the elements of L fixed by H). Let $\overline{H}$ denote the closure of H in $G = \operatorname{Gal}(L/K)$. Since $\operatorname{Gal}(L/L^H)$ is closed by (1), from $H \subset \operatorname{Gal}(L/L^H)$ we get $\overline{H} \subset \operatorname{Gal}(L/L^H)$. To prove this containment is an equality, pick $\sigma \in G - \overline{H}$. We will show $\sigma \notin \operatorname{Gal}(L/L^H)$: σ moves something in L^H.

Since $\sigma \not\in \overline{H}$ and $\overline{H}$ is closed, some basic open set around σ in G is disjoint from $\overline{H}$:

$$\sigma \operatorname{Gal}(L/F) \cap \overline{H} = \emptyset \tag{4.1}$$

for some finite extension F/K in L, and by replacing F with a finite Galois extension of K in L containing F[1] we shrink the basic open set $\sigma \operatorname{Gal}(L/F)$, which preserved the disjointness condition in (4.1) while letting us suppose F/K is Galois.

Claim: For a finite Galois extension F/K in L that fits the condition (4.1), there is an $\alpha \in F$ that is fixed by all of H while being moved by σ.

We'll prove this claim by contradiction. If there's no such α, that means whenever an $\alpha \in F$ satisfies $h(\alpha) = h$ for all $h \in H$, also $\sigma(\alpha) = \alpha$. In other words, $\sigma|_F$ fixes the fixed field of H in F. Writing $H|_F$ for $\{h|_F : h \in H\}$, the fixed field of H in F is $F^{H|_F}$. The automorphism $\sigma|_F$ and group $H|_F$ belong to the finite Galois group $\operatorname{Gal}(F/K)$. By *finite Galois theory*, an automorphism φ in a finite Galois group whose fixed field contains the fixed field of a subgroup M must lie in M: the fixed field of φ is the fixed field of $\langle\varphi\rangle$, and if the fixed field of $\langle\varphi\rangle$ contains the fixed field of M then the Galois correspondence implies $\langle\varphi\rangle$ is contained in M, so $\varphi \in M$. Therefore $\sigma|_F \in H|_F$: there's some $h \in H$ such that $\sigma|_F = h|_F$. That means $h \in \sigma \operatorname{Gal}(L/F)$. But in (4.1), $\sigma \operatorname{Gal}(L/F)$ is disjoint from $\overline{H}$, and thus is disjoint from H, so we have a contradiction and this proves the claim.

By the claim, which is now proved, there is some $\alpha \in F$ such that $\sigma(\alpha) \neq \alpha$ and $h(\alpha) = \alpha$ for all $h \in H$. This means $\alpha \in L^H$ and α is moved by σ, so $\sigma \not\in \operatorname{Gal}(L/L^H)$.

(3): Just as in finite Galois theory, it is easy to see that $E \mapsto \operatorname{Gal}(L/E)$ and $H \mapsto L^H$ reverse inclusions and that $E \subset L^{\operatorname{Gal}(L/E)}$ and $H \subset \operatorname{Gal}(L/L^H)$. For closed H, we have $\operatorname{Gal}(L/L^H) = H$ by (2).

It remains to show the containment $E \subset L^{\operatorname{Gal}(L/E)}$ is an equality. We will show each α in $L - E$ is not in $L^{\operatorname{Gal}(L/E)}$, meaning α is not fixed by $\operatorname{Gal}(L/E)$: if $\alpha \not\in E$ then $\sigma(\alpha) \neq \alpha$ for some $\sigma \in \operatorname{Gal}(L/E)$. This is analogous to what we did in (2) to show the containment $\overline{H} \subset \operatorname{Gal}(L/L^H)$ is equality.

Since L/E is Galois (Exercise 3.3), there is a finite Galois extension of E inside L that contains α, say M. By *finite Galois theory*, since $[E(\alpha) : E] > 1$ there is an E-conjugate β of α inside M with $\beta \neq \alpha$ and $\beta = \varphi(\alpha)$ for some $\varphi \in \operatorname{Gal}(M/E)$. There is a lifting of $\varphi\colon M \to M$ to $\sigma\colon L \to L$ by Corollary A.2 (K there is M here), so $\sigma \in \operatorname{Gal}(L/E)$ and $\beta = \sigma(\alpha)$, so $\sigma(\alpha) \neq \alpha$. This completes the proof of the Galois correspondence.

(4) To prove $L^H = L^{\overline{H}}$ for an arbitrary subgroup H we could use the Galois correspondence: (2) implies $\operatorname{Gal}(L/L^H) = \overline{H}$ and $\operatorname{Gal}(L/L^{\overline{H}}) = \overline{H}$ since $\overline{H}$ is its own closure, so $\operatorname{Gal}(L/L^H) = \operatorname{Gal}(L/L^{\overline{H}})$, so by the Galois correspondence $L^H = L^{\overline{H}}$. We could also argue more directly as follows. Clearly $L^{\overline{H}} \subset L^H$, and to prove $L^H \subset L^{\overline{H}}$ we want to show that if $\alpha \in L$ satisfies $h(\alpha) = \alpha$ for all $h \in H$ then $\sigma(\alpha) = \alpha$ for all $\sigma \in \overline{H}$. For each $\sigma \in \overline{H}$, every basic open set around σ contains an element of H, by the meaning of lying in the closure $\overline{H}$. For an $\alpha \in L^H$, let F be a finite extension of K containing α (*e.g.*, $F = K(\alpha)$) and use the basic open set $\sigma \operatorname{Gal}(L/F)$: this contains some $h \in H$, so $h|_F = \sigma|_F$, which means $\sigma(\alpha) = h(\alpha) = \alpha$. Thus every element of L^H is fixed by $\overline{H}$, so $L^H \subset L^{\overline{H}}$. □

[1] Recall by Theorem 3.2 that one of the equivalent properties of L/K being a Galois extension is that it is a union of finite Galois extensions, so there is a finite Galois extension of K in L containing a primitive element for F/K, which puts F into a finite Galois extension of K in L. Or pass to the splitting field over K in L of the minimal polynomials of a finite set of field generators for F over K: that is a "Galois closure" of F over K, a standard term in finite Galois theory that has nothing to do with the topological term "closure".

Remark 4.8. Notice that there is *no* topology or limit concept being imposed on the fields or on the automorphisms: the fields are just abstract fields and the automorphisms in $\mathrm{Gal}(L/K)$ are just abstract field automorphisms of L fixing all of K. The topology is being put on $\mathrm{Gal}(L/K)$ but does not change its elements in any way. When we showed $L^H \subset L^{\overline{H}}$, there was no "argument by continuity" involving limits is a profound way. The proof just applied the basic notions of general topology to our purely algebraic setting. This is not like what happens with Banach spaces or Hilbert spaces where the notion of linear functional is restricted from abstract linear functionals to continuous linear functionals, and by cutting down the possible linear functionals a nice duality theory is achieved. For infinite Galois theory the possible automorphisms of the field L are not being restricted at all.

The following corollary extends some further aspects of the Galois correspondence from the finite-degree case to the infinite-degree case. Parts of the corollary are purely algebraic as in the finite case, while other parts acquire a topological aspect by involving closures of subgroups.

Corollary 4.9. *Let L/K be a Galois extension and $G = \mathrm{Gal}(L/K)$.*

1. *For two closed subgroups H and H' of G, $L^{H\cap H'} = L^H L^{H'}$ and $L^H \cap L^{H'} = L^{\overline{\langle H,H'\rangle}}$, where $\overline{\langle H,H'\rangle}$ is the closure of the subgroup $\langle H,H'\rangle$ generated by H and H' in G.*
2. *For two intermediate fields E and E', $\mathrm{Gal}(L/EE') = \mathrm{Gal}(L/E) \cap \mathrm{Gal}(L/E')$ and $\mathrm{Gal}(L/E \cap E') = \overline{\langle \mathrm{Gal}(L/E), \mathrm{Gal}(L/E')\rangle}$.*
3. *For $\sigma \in G$ and a subgroup H, $L^{\sigma H \sigma^{-1}} = \sigma(L^H)$.*
4. *For $\sigma \in G$ and an intermediate field E, $\mathrm{Gal}(L/\sigma(E)) = \sigma\,\mathrm{Gal}(L/E)\sigma^{-1}$.*

Proof. (1) By the Galois correspondence, $L^H L^{H'}$ is $L^{H''}$ where $H'' = \mathrm{Gal}(L/(L^H L^{H'}))$. A composite field like $L^H L^{H'}$ is the *smallest field containing both fields*, L^H and $L^{H'}$ in this case. By the inclusion-reversion bijection from the Galois correspondence, the subgroup of G fixing $L^H L^{H'}$ has to be the *largest closed subgroup contained in both subgroups*, which means the largest closed subgroup of the intersection $H \cap H'$. Since H and H' are closed, $H \cap H'$ is closed and thus $H \cap H'$ is the subgroup fixing $L^H L^{H'}$.

The field $L^H \cap L^{H'}$ is the *largest field contained in both fields*, L^H and $L^{H'}$. By the Galois correspondence, the subgroup of G fixing $L^H \cap L^{H'}$ is *smallest closed subgroup containing both subgroups*, which means the smallest closed subgroup containing H and H'. That is $\overline{\langle H,H'\rangle}$.

(2) Write H as $\mathrm{Gal}(L/E)$ and H' as $\mathrm{Gal}(L/E')$, so $E = L^H$ and $E' = L^{H'}$. Now use (1) and the Galois correspondence.

(3) For $\alpha \in L$, we have $(\sigma h \sigma^{-1})(\alpha) = \alpha$ for all $h \in H$ if and only if $h(\sigma^{-1}(\alpha)) = \sigma^{-1}(\alpha)$ for all h, which is the same as $\sigma^{-1}(\alpha) = L^H$, or $\alpha \in \sigma(L^H)$. Thus $L^{\sigma H \sigma^{-1}} = \sigma(L^H)$. Notice this argument involves no topology at all.

(4) This is equivalent to (3) in the same way (2) is equivalent to (1), namely by the Galois correspondence. It can also be proved in a direct way similar to the proof of (3), making no use of topological concepts. Details are left to the reader. □

The following theorem shows how to interpret "open" and "closed" for subgroups of a Galois group. In particular, while finite Galois theory says the subgroups that are normal correspond to intermediate extensions that are Galois over the base field, for infinite Galois theory we have to append the label "open" or "closed" to the subgroups (depending on whether you want Galois extensions of K inside L that are finite or arbitrary).

Theorem 4.10. *Let L/K be a Galois extension.*

1. *The closed subgroups of* $\mathrm{Gal}(L/K)$ *are* $\mathrm{Gal}(L/E)$ *for intermediate field extensions E/K in L.*
2. *The open subgroups of* $\mathrm{Gal}(L/K)$ *are* $\mathrm{Gal}(L/F)$ *for finite extensions F/K in L.*
3. *The closed normal subgroups of* $\mathrm{Gal}(L/K)$ *are* $\mathrm{Gal}(L/E)$ *where E is a Galois extension of K in L. Equivalently, a closed subgroup H of* $\mathrm{Gal}(L/K)$ *is normal if and only if L^H/K is a Galois extension.*
4. *The open normal subgroups of* $\mathrm{Gal}(L/K)$ *are* $\mathrm{Gal}(L/F)$ *where F is a finite Galois extension of K in L. Equivalently, an open subgroup H of* $\mathrm{Gal}(L/K)$ *is normal if and only if L^H/K is a finite Galois extension*

Proof. (1) Theorem 4.7(1) tells us that every $\mathrm{Gal}(L/E)$ is closed. Conversely, if H is a closed subgroup of $\mathrm{Gal}(L/K)$ then the Galois correspondence tells us $H = \mathrm{Gal}(L/E)$ where $E = L^H$ is the subfield of L fixed by H.

(2) If F/K is a finite extension then $\mathrm{Gal}(L/F)$ is open by the definition of basic open sets in the Krull topology. Conversely, if H is an open subgroup of $\mathrm{Gal}(L/K)$ then H contains a basic open set around the identity, so $\mathrm{Gal}(L/F) \subset H$ for some finite extension F/K in L. Writing H as $\mathrm{Gal}(L/E)$ (so really $E = L^H$), the Galois correspondence turns the containment $\mathrm{Gal}(L/F) \subset \mathrm{Gal}(L/E)$ into the reverse containment $E \subset F$. Thus $K \subset E \subset F$, so F/K being finite implies E/K is finite too.

(3) Closed subgroups look like $\mathrm{Gal}(L/E)$ for an intermediate field E between K and L. For this to be a normal subgroup means $\sigma\,\mathrm{Gal}(L/E)\sigma^{-1} = \mathrm{Gal}(L/E)$ for all $\sigma \in \mathrm{Gal}(L/K)$. Just as in finite Galois theory, it is straightforward to show $\sigma\,\mathrm{Gal}(L/E)\sigma^{-1} = \mathrm{Gal}(L/\sigma(E))$, so $\mathrm{Gal}(L/E)$ is a normal subgroup when $\mathrm{Gal}(L/E) = \mathrm{Gal}(L/\sigma(E))$ for all $\sigma \in \mathrm{Gal}(L/K)$. By the Galois correspondence, this equality is the same as $\sigma(E) = E$ for all σ. Thus every element of E has all of its K-conjugates in E (Theorem 3.9), so E/K is a normal field extension. Also E/K is separable since L/K is separable, so E/K is normal and separable, which is one of the equivalent descriptions of being a Galois extension in Theorem 3.2.

The equivalent description of (3) as closed subgroup H being normal if and only if L^H/K is a Galois extension follows from the Galois correspondence by writing an intermediate field (uniquely) as L^H for a closed subgroup H, so $\mathrm{Gal}(L/E) = \mathrm{Gal}(L/L^H) = H$.

(4) Combine (2) and (3). □

In the Krull topology on $\mathrm{Gal}(L/K)$ we had defined the basic open sets around an automorphism σ to be $\sigma\,\mathrm{Gal}(L/F)$ for finite extensions F/K in L, so Theorem 4.10 tells us that we can describe the basic open sets around σ as σH for *open subgroups* H.

Corollary 4.11. *A subgroup of* $\mathrm{Gal}(L/K)$ *in the Krull topology is open if and only if it is closed with finite index.*

Proof. Theorem 4.10(2) tells us an open subgroup of $\mathrm{Gal}(L/K)$ has the form $\mathrm{Gal}(L/F)$ for a finite extension F/K. This is closed by Theorem 4.10(1) because F is an intermediate field, and it has finite index by Lemma 4.1(2). □

For some infinite Galois groups, such as $\mathrm{Gal}(\mathbf{Q}(\zeta_{p^\infty})/\mathbf{Q})$, every subgroup with finite index is open. There are infinite Galois groups in which non-open finite-index subgroups exist, such as in $\mathrm{Gal}(\mathbf{Q}(\sqrt{-1}, \sqrt{2}, \sqrt{3}, \ldots)/\mathbf{Q})$, but every known construction of such subgroups uses Zorn's lemma and thus no "real" examples of non-open finite-index subgroups of an infinite Galois group have ever been written down.

Corollary 4.12. *For a subset S of* $\mathrm{Gal}(L/K)$*, its closure $\overline{S}$ is $\bigcap_H SH$, where H runs over the open subgroups of* $\mathrm{Gal}(L/K)$ *and $SH = \{sh : s \in S, h \in H\}$. We also have $\overline{S} = \bigcap_N SN$ where N runs over the open normal subgroups of* $\mathrm{Gal}(L/K)$*.*

Proof. We have $S \subset SH$ for each open subgroup H, so $S \subset \bigcap_H SH$. We will show the intersection is closed and then that every closed set containing S contains the intersection, so the intersection is the smallest closed subset of $\mathrm{Gal}(L/K)$ containing S, which is precisely how the closure $\overline{S}$ is defined (or at least it's one of the ways the closure of a subset is defined in topology).

By Theorem 4.10, every open subgroup H of $\mathrm{Gal}(L/K)$ is closed with finite index. Therefore each sH for $s \in S$ is closed (multiplication by an element is a homeomorphism, so it sends closed sets to closed sets). Since $SH = \bigcup_{s\in S} sH$ is a union of cosets of H and H has finitely many (left) cosets, SH is a finite union of closed sets and therefore SH is closed. Being closed is preserved under arbitrary intersections, so $\bigcap_H SH$ is closed. .

Now let $S \subset C$ for a closed set C in $\mathrm{Gal}(L/K)$. We will show $\bigcap_H SH \subset C$. Pick $g \in \bigcap_H SH$. To show $g \in C$, suppose $g \notin C$. Then, because $G - C$ is open, a basic open set around g is contained in $G - C$: $gH_0 \subset G - C$ for some open subgroup H_0. By the definition of g we have $g \in SH_0$ too, say $g \in s_0H_0$ for some $s_0 \in S$. Thus gH_0 and s_0H_0 both contain g, which makes these left cosets of H_0 identical. However, s_0H_0 meets S (it contains s_0), which is contained in C, while gH_0 is disjoint from C. That's a contradiction, so $g \in C$.

We mentioned before Theorem 4.6 that every $\mathrm{Gal}(L/F)$ for a finite extension F/K contains some $\mathrm{Gal}(L/\widetilde{F})$ for a finite Galois extension $\widetilde{F}/K$, so each open subgroup H of $\mathrm{Gal}(L/K)$ contains an open normal subgroup N. Therefore in the intersection $\bigcap_H SH$, each SH contains some SN, so $\bigcap_H SH = \bigcap_N SN$, where N runs over the open normal subgroups of $\mathrm{Gal}(L/K)$. □

Example 4.13. For a subgroup H of $\mathrm{Gal}(L/K)$, $\overline{H} = \bigcap_N HN$ where N runs over the open normal subgroups of $\mathrm{Gal}(L/K)$. Since N is normal, the set HN is a subgroup of $\mathrm{Gal}(L/K)$, and if H is open then each HN is open: every element hn of HN is contained in the coset Hn, which is open and in HN. In this case, writing the closure $\overline{H}$ as the intersection of open subgroups HN is analogous in $\mathbf{R}$ to writing a closed interval $[a, b]$ as an intersection of open intervals $(a - \varepsilon, b + \varepsilon)$, except in $\mathbf{R}$ such intervals are not subgroups.

Exercises.

1. When we describe $\mathrm{Gal}(\mathbf{Q}(\sqrt{-1}, \sqrt{2}, \sqrt{3}, \ldots)/\mathbf{Q})$ as a countable direct product of copies of $\{\pm 1\}$, prove that the Krull topology on this group is its product topology where each factor $\{\pm 1\}$ has the discrete topology.
2. When $\mathrm{Gal}(L/K)$ is given the Krull topology, show for each closed normal subgroup N of $\mathrm{Gal}(L/K)$ that its fixed field L^N is a Galois extension of K. Is this still true when N is an arbitrary normal subgroup of $\mathrm{Gal}(L/K)$?
3. Let L/K be a Galois extension. Show the Galois action mapping $\mathrm{Gal}(L/K) \times L \to L$ where $(\sigma, \alpha) \mapsto \sigma(\alpha)$ is continuous, where $\mathrm{Gal}(L/K)$ has the Krull topology, L is considered to be a *discrete* topological space, and $\mathrm{Gal}(L/K) \times L$ has the product topology.

5. Further properties of the Krull topology

Theorem 5.1. *The topology on a Galois group* $\mathrm{Gal}(L/K)$ *is totally disconnected: the only nonempty connected subsets are points.*

Proof. Let C be a nonempty connected subset of $\mathrm{Gal}(L/K)$ and pick $\sigma \in C$. We will show $C = \{\sigma\}$.

Let H be an open subgroup of $\mathrm{Gal}(L/K)$, so σH is an open set containing σ. Since H is an open subgroup, it is also closed (Corollary 4.11). Therefore σH is both open and closed, so the disjoint union $\sigma H \cup (G - \sigma H)$ is a covering of G by two disjoint open sets. Since C is connected and contains σ, like σH does, we get $C \subset \sigma H$. Letting H vary, $C \subset \bigcap_H \sigma H$, where H in the intersection runs over all open normal subgroups of $\mathrm{Gal}(L/K)$. This intersection is $\{\sigma\}$, so $C = \{\sigma\}$. □

When L/K is Galois and E is an intermediate field, L/E is Galois (Exercise 3.3) and the Galois group $\mathrm{Gal}(L/E)$ gets two topologies: its subspace topology from being a subset of $\mathrm{Gal}(L/K)$ and its own Krull topology. It's natural to ask if these topologies agree.

Theorem 5.2. *If L/K is Galois and E is an intermediate field, then the subspace topology on* $\mathrm{Gal}(L/E)$ *as a subset of* $\mathrm{Gal}(L/K)$ *equals the Krull topology on* $\mathrm{Gal}(L/E)$.

Proof. An open subset of $\mathrm{Gal}(L/E)$ for its subspace topology in $\mathrm{Gal}(L/K)$ is $U \cap \mathrm{Gal}(L/E)$ where U is open in $\mathrm{Gal}(L/K)$ for the Krull topology. To show $U \cap \mathrm{Gal}(L/E)$ is open for the Krull topology on $\mathrm{Gal}(L/E)$, we will show each element of $U \cap \mathrm{Gal}(L/E)$ is contained in a basic open set for the Krull topology on $\mathrm{Gal}(L/E)$ that is also in $U \cap \mathrm{Gal}(L/E)$. (If the intersection is empty then it's obviously open for the Krull topology on $\mathrm{Gal}(L/E)$.)

Pick $\sigma \in U \cap \mathrm{Gal}(L/E)$. Since U is open for the Krull topology on $\mathrm{Gal}(L/K)$, U contains

$$\sigma\,\mathrm{Gal}(L/F) = \{\tau \in \mathrm{Gal}(L/K) : \tau = \sigma \text{ on } F\}$$

for some finite extension F/K. The intersection of this basic open set with $\mathrm{Gal}(L/E)$ is

$$\{\tau \in \mathrm{Gal}(L/K) : \tau = \sigma \text{ on } F \text{ and } \tau \text{ fixes } E\} = \{\tau \in \mathrm{Gal}(L/E) : \tau = \sigma \text{ on } F\}.$$

Since σ fixes E, to say a $\tau \in \mathrm{Gal}(L/E)$ satisfies $\tau = \sigma$ on F is the same thing as $\tau = \sigma$ on EF, so

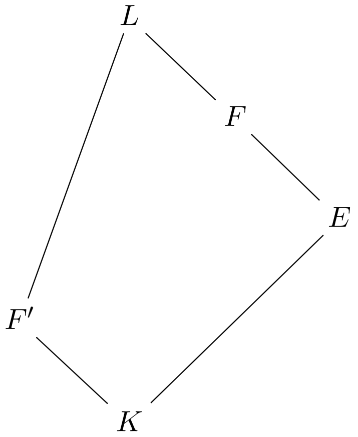
$$\{\tau \in \mathrm{Gal}(L/E) : \tau = \sigma \text{ on } F\} = \{\tau \in \mathrm{Gal}(L/E) : \tau = \sigma \text{ on } EF\} = \sigma\,\mathrm{Gal}(L/EF).$$

Thus

$$\sigma\,\mathrm{Gal}(L/EF) \subset U \cap \mathrm{Gal}(L/E),$$

and EF is a finite extension of E since F is a finite extension of K (a subfield of E). Thus $U \cap \mathrm{Gal}(L/E)$ contains a basic open set for the Krull topology on $\mathrm{Gal}(L/E)$ around each point in it, so this intersection is open for the Krull topology on $\mathrm{Gal}(L/E)$.

Now let V be an open subset of $\mathrm{Gal}(L/E)$ for its Krull topology. To show V is also open for the subspace topology that $\mathrm{Gal}(L/K)$ gives $\mathrm{Gal}(L/E)$, we may assume $V \neq \emptyset$. Pick $\sigma \in V$, so $\sigma\,\mathrm{Gal}(L/F) \subset V$ for some finite extension F/E. (See the field diagram below, with F' to be defined soon.)



Write $F = E(\alpha)$ and set $F' = K(\alpha)$.[2] Then F'/K is a finite extension and

$$\sigma\,\mathrm{Gal}(L/F') = \{\tau \in \mathrm{Gal}(L/E) : \tau|_{F'} = \sigma|_{F'}\} = \{\tau \in \mathrm{Gal}(L/E) : \tau(\alpha) = \sigma(\alpha)\}.$$

This set is $\{\tau \in \mathrm{Gal}(L/K) : \tau(\alpha) = \sigma(\alpha)\} \cap \mathrm{Gal}(L/E) = \sigma\,\mathrm{Gal}(L/K(\alpha)) \cap \mathrm{Gal}(L/E)$, which is an open subset of $\mathrm{Gal}(L/E)$ for its subspace topology in $\mathrm{Gal}(L/K)$. Thus V is open for the subspace topology of $\mathrm{Gal}(L/E)$ being inside $\mathrm{Gal}(L.K)$. □

So far the properties we have established about the Krull topology (group operations are continuous, which subgroups are open or closed, total disconnectedness, *etc.*) have not needed any genuinely hard results from topology. The property of the Krull topology in the next theorem is different, and its method of proof leads to an alternative way of thinking about what the Krull topology means. To set the stage, first we prove a lemma about the relation of $\mathrm{Gal}(L/K)$ and $\mathrm{Gal}(F/K)$ when F is a finite Galois extension of K inside of L.

Lemma 5.3. *If L/K is a Galois extension and F/K is a finite Galois extension inside L, then the restriction mapping* $\mathrm{Gal}(L/F) \to \mathrm{Gal}(F/K)$ *is a continuous homomorphism when we give the finite group* $\mathrm{Gal}(F/K)$ *the discrete topology.*

Proof. First we show restricting the domain of automorphisms from L to F is a homomorphism from $\mathrm{Gal}(L/K)$ to $\mathrm{Gal}(F/K)$. For σ and τ in $\mathrm{Gal}(L/K)$ and $\alpha \in F$,

$$(\sigma\tau)|_F(\alpha) = (\sigma\tau)(\alpha) = \sigma(\tau(\alpha)) = \sigma(\tau|_F(\alpha)) = \sigma|_F(\tau|_F(\alpha)),$$

where we can use the notation for "restrictions to F" on σ and τ because F/K is Galois, so that when $\alpha \in F$ also $\tau(\alpha) \in F$. Thus $(\sigma\tau)|_F = \sigma|_F\tau||_F$ for all σ and τ in $\mathrm{Gal}(L/K)$.

To show the restriction mapping $\mathrm{Gal}(L/K) \to \mathrm{Gal}(F/K)$ is continuous, where the finite group $\mathrm{Gal}(F/K)$ has the discrete topology, amounts to saying the inverse image of every point of $\mathrm{Gal}(F/K)$ is open (since all 1-element subsets of $\mathrm{Gal}(F/K)$ are open). Each $\varphi \in \mathrm{Gal}(F/K)$ has a lifting to an automorphism of L: $\varphi = \sigma|_F$ for some $\sigma \in \mathrm{Gal}(L/K)$ by Corollary A.2 (that uses Zorn's lemma). The inverse image of φ under the restriction from L to F is all the elements of $\mathrm{Gal}(L/K)$ that restrict on F to be φ. Since $\varphi = \sigma|_F$, the inverse image of φ is

$$\{\tau \in \mathrm{Gal}(L/F) : \tau|_F = \varphi\} = \{\tau \in \mathrm{Gal}(L/F) : \tau|_F = \sigma|_F\} = \sigma\,\mathrm{Gal}(L/F),$$

[2] We could replace the single primitive element α for F/E by a finite set of field generators and the argument that follows would be essentially unchanged.

which is (by definition) a basic open set in $\mathrm{Gal}(L/K)$. □

Theorem 5.4. *For a Galois extension L/K, the Krull topology on $\mathrm{Gal}(L/K)$ is compact.*

Proof. We are going to embed $\mathrm{Gal}(L/K)$ as a closed subset of a product of compact spaces having the product topology, so the compactness of $\mathrm{Gal}(L/K)$ will follows from (i) compactness of product spaces using the product topology (Tychonoff's theorem) and (ii) compactness of closed subsets of compact spaces. Mathematically, (i) is a lot harder than (ii).

Since L is covered by finite Galois extensions of K, every $\sigma \in \mathrm{Gal}(L/K)$ is determined by how it looks on the finite Galois extensions of K in L. Therefore we define

$$f\colon \mathrm{Gal}(L/K) \to \prod_F \mathrm{Gal}(F/K) \quad \text{where } \sigma \mapsto (\sigma|_F)_F, \tag{5.1}$$

where the fields F on the right side run over *finite Galois* extensions of K and the F-component of $f(\sigma)$ is simply the restriction of σ to the field F. The product space in (5.1) is both a group and a topological space: each $\mathrm{Gal}(F/K)$ is a group, so the product space is a group using componentwise operations, and each $\mathrm{Gal}(F/K)$ is finite, so we give $\mathrm{Gal}(F/K)$ the discrete topology (what else?) and give the product of these discrete spaces the product topology. (An infinite product of discrete spaces is hardly ever discrete in the product topology, *e.g.*, $\prod_{n\geq 1}\{\pm 1\}$ is not discrete in the product topology when each $\{\pm 1\}$ has the discrete topology.)

We will show the following properties of f:

(1) f is injective,
(2) f is a homomorphism and continuous,
(3) f has a closed image in the product space,
(4) f is an open mapping to its image (f sends open sets in $\mathrm{Gal}(L/K)$ with the Krull topology to open sets in $f(\mathrm{Gal}(L/K))$ equipped with the subspace topology).

(1) The function f is injective since L is covered by finite Galois extensions: if $f(\sigma) = f(\tau)$ then $\sigma|_F = \tau|_F$ for all finite Galois extensions F/K in L. That means $\sigma = \tau$ on all finite Galois extensions of K in L, and since L is a union of such extensions of K, $\sigma = \tau$ on L.

The function f is usually *not* surjective, since general elements of the product space in (5.1) have no connection between their different components, while elements of the product space that are in the image of f have compatibilities between different components: if F and F' are two finite Galois extensions of K in L and $\sigma \in \mathrm{Gal}(L/K)$, then $\sigma|_F$ and $\sigma|_{F'}$ have to be the same on $F \cap F'$: $(\sigma|_F)|_{F\cap F'} = (\sigma|_{F'})_{F\cap F'} = \sigma|_{F\cap F'}$. Therefore the F-component and F'-component of $f(\sigma)$ restrict on $F \cap F'$ to the $(F \cap F')$-component of $f(\sigma)$. For a general term (g_F) in the product space in (5.1), there is no reason $g_F \in \mathrm{Gal}(F/K)$ and $g_{F'} \in \mathrm{Gal}(F'/K)$ need to restrict on $F \cap F'$ to the automorphism $g_{F\cap F'}$ on $F \cap F'$. (In fact, the image of f is precisely those (g_F) where g_F and $g_{F'}$ restrict to $g_{F\cap F'}$ on $F \cap F'$ for all finite Galois extensions F and F' of K in L. See Exercise 5.1.)

(2) Because f is a mapping to a product space, the following basic properties of product spaces will be useful: a function $G \to \prod_i G_i$ from a group to a direct product of groups is a homomorphism if and only if each of its component functions $G \to G_i$ is a homomorphism, and a function $X \to \prod_i X_i$ from a topological space to a product of topological spaces with the product topology is continuous if and only if each of its component functions $X \to X_i$ is a continuous. In the setting of (5.1), the component functions are the restriction maps $\mathrm{Gal}(L/K) \to \mathrm{Gal}(F/K)$. When the finite group $\mathrm{Gal}(F/K)$ has the discrete topology, this restriction map is a continuous homomorphism by Lemma 5.3. Therefore (5.1) is a

continuous homomorphism when the product in (5.1) has the product topology with each component $\operatorname{Gal}(F/K)$ having the discrete topology. (Because f is a homomorphism, we could have proved f is injective by checking its kernel is trivial instead of the argument used in (1) with pairs σ and τ, but the proof with σ and τ is not really any different than a proof with kernels.)

(3) This proof will be similar to the proof in Theorem 4.7(1) that $\operatorname{Gal}(L/E)$ is closed in $\operatorname{Gal}(L/K)$ for each intermediate field E between K and L.

We'll show $f(\operatorname{Gal}(L/K))$ is closed in $\prod_F \operatorname{Gal}(F/K)$ by showing *the complement is open*. Pick (g_F) in $\prod_F \operatorname{Gal}(F/K)$ that is not in the image of f. (If f is surjective, which happens very rarely, namely when L/K is Galois of prime degree, there is no (g_F), but also that means there is nothing to check.) Elements in the image of f satisfy a compatibility among their components: $f(\sigma)$ has its component $\sigma|_F$ and $\sigma|_{F'}$ restrict on $F \cap F'$ to its $(F \cap F')$-component $\sigma|_{F\cap F'}$ for all finite Galois extensions F and F' of K in L. Therefore to say (g_F) is not in the image of f requires that for some F_0 and F_0', g_{F_0} in $\operatorname{Gal}(F_0/K)$ and $g_{F_0'}$ in $\operatorname{Gal}(F_0'/K)$ do not both restrict on $F_0 \cap F_0'$ to $g_{F_0\cap F_0'}$.

Now we define an open set around (g_F) that does not meet the image of f. Set

$$U = \left\{ (h_F) \in \prod_F \operatorname{Gal}(F/K) : h_{F_0} = g_{F_0}, h_{F_0'} = g_{F_0'}, h_{F_0\cap F_0'} = g_{F_0\cap F_0'} \right\},$$

which is all elements of the product space with the same components at F_0, F_0', and $F_0 \cap F_0'$ as (g_F). What U contains are all the elements of the product space with the same incompatibility that (g_F) has at F_0, F_0',and $F_0 \cap F_0'$. This guarantees that U does not intersect the image of f. At the same time, U is open in the product topology on $\prod_F \operatorname{Gal}(F/K)$ since we are imposing a condition in only finitely many components (three components) and the condition in those components defines an open subset of the component because all components have the discrete topology (so all subsets, in particular all 1-element subsets, are open in each component). Thus the complement of $f(\operatorname{Gal}(L/K))$ in $\prod_F \operatorname{Gal}(F/K)$ is open, so $f(\operatorname{Gal}(L/K))$ is closed in $\prod_F \operatorname{Gal}(F/K)$.

(4) Since each open set in $\operatorname{Gal}(L/K)$ is a union of basic open sets, it suffices to show f sends each (nonempty) basic open set in $\operatorname{Gal}(L/K)$ to an open set in $\prod_F \operatorname{Gal}(F/K)$. (Here we use injectivity of f: $f(\bigcup U_i) = \bigcup f(U_i)$ since f is injective.) For $\sigma \in \operatorname{Gal}(L/K)$, every basic open set around σ in $\operatorname{Gal}(L/K)$ contains a basic open set $\sigma \operatorname{Gal}(L/F_0)$ where F_0 is a finite *Galois* extension of K (this just reflects the fact that finite extensions of K in L can be enlarged to finite Galois extensions of K in L), so by shrinking down to such basic open sets we may suppose F_0 is Galois over K. Since $\sigma \operatorname{Gal}(L/F_0) = \{\tau \in \operatorname{Gal}(L/K) : \tau|_{F_0} = \sigma|_{F_0}\}$, $f(\sigma \operatorname{Gal}(L/F_0))$ can be described as a subset of $\prod_F \operatorname{Gal}(F/K)$ in the following way:

$$f(\sigma \operatorname{Gal}(L/F_0)) = f(\operatorname{Gal}(L/K)) \cap \left(\{\sigma|_{F_0}\} \times \prod_{F \neq F_0} \operatorname{Gal}(F/K) \right). \tag{5.2}$$

The right side of (5.2) is all $f(\tau)$ where $\tau \in \operatorname{Gal}(L/K)$ and τ looks like σ on F_0, which is the same as saying $\tau \in \sigma \operatorname{Gal}(L/F_0)$. That explains why the right side equals the left side. If you look at the right side, the product piece is the subset of $\prod_F \operatorname{Gal}(F/K)$ having F_0-component $\sigma|_{F_0}$. That is an open set in the product topology. Intersecting this with $f(\operatorname{Gal}(L/K))$ defines an open set in $f(\operatorname{Gal}(L/K))$ using the subspace topology on $f(\operatorname{Gal}(L/K))$. Therefore $f(\sigma \operatorname{Gal}(L/F_0))$ is open in the subspace topology on $f(\operatorname{Gal}(L/K))$.

By properties (1) and (2),f is isomorphic to its image in $\prod_F \mathrm{Gal}(F/K)$ as a group. By (2), (3), and (4), f is homeomorphic to its image (when it is given the subspace topology) as a topological space. The product $\prod_F \mathrm{Gal}(F/K)$ is compact by Tychonoff's theorem and $f(\mathrm{Gal}(L/K))$ is closed in this product by (3), so $f(\mathrm{Gal}(L/K))$ is compact. Because f is a homeomorphism between $\mathrm{Gal}(L/K)$ and $f(\mathrm{Gal}(L/K))$, $\mathrm{Gal}(L/K)$ is compact in the Krull topology. □

The proof of Theorem 5.4 uses the definition of the Krull topology, but otherwise it uses almost nothing else about topological features of the Krull topology. It gives us a new way to describe the Krull topology: rather than directly defining open sets in $\mathrm{Gal}(L/K)$, map $\mathrm{Gal}(L/K)$ to $\prod_F \mathrm{Gal}(F/K)$ by $\sigma \mapsto (\sigma|_F)_F$, which is injective, and then topologize $\mathrm{Gal}(L/K)$ by giving its image in $\prod_F \mathrm{Gal}(F/K)$ the subspace topology from the product topology, and then pulling back this topology to $\mathrm{Gal}(L/K)$ using its embedding into the product space. Theorem 5.4 tells us this is exactly the Krull topology, but we could have simply (re)define the Krull topology to be the topology resulting from this "pullback from being subspace of product space" point of view.

Many earlier theorems we proved directly with the Krull topology can be seen as consequences of its compactness and the behavior of product spaces in topology and topological groups (see Appendix B). Here are some examples.

1. The group operations on $\mathrm{Gal}(L/K)$ are continuous (Theorem 4.6(1)): each group $\mathrm{Gal}(F/K)$ with the discrete topology is a topological group, a product of topological groups is a topological group when using the product topology, and a subgroup of a topological group is a topological group when using the subspace topology.
2. When L/K is finite, its topology is discrete (Theorem 4.6(2)): $\prod_F \mathrm{Gal}(F/K)$ has finitely many components when L/K is finite, each with the discrete topology, so this finite product has the discrete topology. A subset of a discrete topological space has the discrete topology as its subspace topology.
3. The topology on $\mathrm{Gal}(L/K)$ is Hausdorff (Theorem 4.6(3)): a product of Hausdorff spaces is Hausdorff and a subset of a Hausdorff space is Hausdorff in the subspace topology.
4. A subgroup of $\mathrm{Gal}(L/K)$ is open if and only if it is closed with finite index (Corollary 4.11): in a compact topological group, a subgroup is open if and only if it is closed with finite index (Corollary B.18).
5. The topology on $\mathrm{Gal}(L/K)$ is totally disconnected (Theorem 5.1): each $\mathrm{Gal}(F/K)$ with the discrete topology is totally disconnected, a product of totally disconnected topological spaces is totally disconnected, and a subset of a totally disconnected space is totally disconnected in the subspace topology.

There is something genuinely special about the topology on infinite Galois groups that is not shared by topologies on more familiar groups like $\mathbf{R}$ and S^1: the identity element has a *neighborhood basis of open subgroups*. In $\mathbf{R}$ and S^1, a small neighborhood of the identity no nontrivial subgroups, but in $\mathrm{Gal}(L/K)$ every open set around the identity contains some $\mathrm{Gal}(L/F)$ for a finite extension F/K, which is an open subgroup. We also know, by enlarging F to a finite Galois extension of K, that every open subgroup of $\mathrm{Gal}(L/K)$ contains an open normal subgroup. It turns out this property, as well as the description of closures in Corollary 4.12 and the total disconnectedness in Theorem 5.1, are consequences of a few topological properties of infinite Galois groups and don't need the interpretation of certain subgroups of $\mathrm{Gal}(L/K)$ as Galois groups. The following theorem illustrates this, and assumes you have read a bit about topological groups in Appendix B.

Theorem 5.5. *Let G be a compact Hausdorff topological group in which the identity element has a neighborhood basis of open subgroups.*

1. *For $g \in G$, $\bigcap_H gH = \{g\}$, where the intersection runs over open subgroups of G.*
2. *Every open subgroup of G contains an open normal subgroup of G.*
3. *For each subset S of G, its closure $\overline{S}$ can be described as $\bigcap_H SH$ and as $\bigcap_N SN$, where H runs over open subgroups and N runs over open normal subgroups.*
4. *The topology on G is totally disconnected.*

Note that (1) can be considered as a special case of (3) with $S = \{g\}$: an open subgroup H in a topological group is closed (being the complement of the union of the nontrivial cosets of H, which are all open), so each gH is closed and therefore $\bigcap_H gH$ is closed, so having this equal $\{g\}$ means $\{g\}$ is a closed set. Also, the Hausdorff property of the topological group G implies $\{g\}$ is closed by Theorem B.10, so $\{g\} = \overline{\{g\}}$.

Proof. (1) If $g' \neq g$ in G then there are disjoint open sets U and U' such that $g \in U$ and $g' \in U'$. Then $e \in g^{-1}U$ and $g^{-1}U$ is open. Since e has a neighborhood basis of open subgroups, there is an open subgroup $H_0 \subset g^{-1}U$, so $gH_0 \subset U$. Therefore $g' \notin gH_0$, so $g' \notin \bigcap_H gH$, so the only element in $\bigcap_H gH$ is g.

(2) Let H be an open subgroup of G. Since G is compact, H has finitely many left cosets, say $g_1H, \ldots, g_nH$. Let G act on its left cosets G/H by left multiplication: $\ell_g(g_iH) = gg_iH$ for $i = 1, \ldots, n$. This group action of G on G/H defines a homomorphism $g \mapsto \ell_g$ from G to the symmetric group S_n by keeping track of how ℓ_g permutes the left coset representatives: $\ell_g(g_iH) = g_{\pi(i)}H$ for a permutation π in S_n. Let N be the kernel of this action of G on G/H, so $N \lhd G$. To say $n \in N$ means $ng_iH = g_iH$. In particular, $nH = H$, so $n \in H$: the normal subgroup N is contained in H. Moreover, $ng_iH = g_iH$ is equivalent to $ng_i \in g_iH$, so $n \in g_iHg_i^{-1}$. Thus $N = \bigcap_{i=1}^n g_iHg_i^{-1}$. This is an intersection of finitely many subgroup that are each open (since H is open and G is a topological group, all conjugate subgroups to H are open), so N is open in G. Thus H contains the open normal subgroup N.

(3) In the proof of Corollary 4.12, the only properties we needed about $\mathrm{Gal}(L/K)$ are that its open subgroups are closed with finite index, the identity has a neighborhood basis of open subgroups (so each σ in $\mathrm{Gal}(L/K)$ has a neighborhood basis of cosets σH for open subgroups H), and every open subgroup contains an open normal subgroup. Using (2) and Corollary B.18), these properties are true for the topological groups in the hypothesis of this theorem. Therefore the proof of Corollary 4.12 carries over to all such groups.

(4) In the proof of Theorem 5.1 we needed to know that open subgroups of $\mathrm{Gal}(L/K)$ are closed and that $\bigcap_H \sigma H = \{\sigma\}$ where H runs over the open subgroups of $\mathrm{Gal}(L/K)$. This property is true for all topological groups fitting the hypotheses of this theorem by (1), so the proof of Theorem 5.1 carries over to all such groups.

□

Abstracting the situation further, a set of characterizing topological features of the Krull topology on a Galois group are that it is (i) compact, (ii) Hausdorff, and (iii) totally disconnected. Topological groups with these properties can be built out of finite groups in a similar way to the identification of $\mathrm{Gal}(L/K)$ with a closed subgroup of the product of finite (Galois) groups in (5.1). Such groups are called *profinite groups*, a name introduced by Serre that comes from the longer term "projective limit of finite groups." (The term "inverse limit" is also used as a synonym for "projective limit".) Profinite groups are an important class of compact topological groups that are quite unlike more classical compact groups studied in analysis (orthogonal groups, unitary groups, *etc.*). All Galois groups, with their Krull topology, are profinite groups, and just as all *finite* groups can be shown to arise as a Galois group of some *finite* Galois extension (with no control over the choice of base field!), all profinite groups arise as the Galois group of some Galois extension. Therefore profinite groups are precisely the kinds of topological groups occur as Galois groups.

Exercises.

1. For a Galois extension L/K, show the image of $\mathrm{Gal}(L/K) \to \prod_F \mathrm{Gal}(F/K)$ in (5.1) is all $(g_F) \in \prod_F \mathrm{Gal}(F/K)$ such that $(g_F)_{F\cap F'} = g_{F\cap F'}$ $(g_{F'})_{F\cap F'} = g_{F\cap F'}$ for all finite Galois extensions F and F' of K inside L.
2. Read about topological groups in Appendix B and prove that if $\{G_i\}$ are topological groups their product group $\prod_i G_i$, with componentwise operations, is a topological group using the product topology.

Appendix A. Extending field embeddings

The theorem below about extending field homomorphisms to larger fields is usually proved in the finite-degree case by using induction on the field degree. For infinite-degree extensions, that method o longer works and instead we will rely on Zorn's lemma.

Theorem A.1. *Let L/K be a Galois extension and $\varphi\colon E \to L$ be a K-homomorphism of an intermediate field. There is an extension of φ to a K-automorphism $L \to L$.*

This theorem is purely algebraic and relies on Zorn's lemma (equivalently, the axiom of choice), so it is rather nonconstructive. The extension of φ to L is *very far* from unique.

Proof. We will use Zorn's lemma. Let S be the set of pairs (E', φ') where E' is an intermediate field between E and L and $\varphi'|_E = \varphi$. For instance $(E, \varphi) \in S$, so $S \neq \emptyset$. Since φ fixes all elements of K, so does each φ'.

$$\begin{tikzcd}
L & L \\
E' \arrow[u, dash] \arrow[ur, "\varphi'"] & \\
E \arrow[u, dash] \arrow[uur, "\varphi"'] & \\
K \arrow[u, dash] &
\end{tikzcd}$$

Partially order S by declaring $(E', \varphi') \leq (E'', \varphi'')$ if $E' \subset E''$ and $\varphi''|_{E'} = \varphi'$. For a totally ordered subset $\{(E_i, \varphi_i)\}_{i\in I}$ in S, an upper bound can be produced as follows. Let $\widetilde{E} = \bigcup_{i\in I} E_i$, so $E \subset \widetilde{E} \subset L$. It is left to the reader to check that $\widetilde{E}$ is a field: use the total orderness of the E_i's as subsets of L. To extend φ to a homomorphism $\widetilde{E} \to L$ we'll "patch together" every $\varphi_i\colon E_i \to L$.

Define $\widetilde{\varphi}\colon \widetilde{E} \to L$ by $\widetilde{\varphi}(x) = \varphi_i(x)$ when $x \in E_i$. If x is also in E_j, let's check $\varphi_i(x) = \varphi_j(x)$ so the definition of $\widetilde{\varphi}(x)$ is independent of the choice of E_i containing x. Since our subset of S is totally ordered, either $(E_i, \varphi_i) \leq (E_j, \varphi_j)$ or $(E_j, \varphi_j) \leq (E_i, \varphi_i)$. In the first case, φ_j restricts to φ_i on E_i, so $\varphi_j(x) = \varphi_i(x)$. The argument in the second case is the same. For $x \in E$, we can view x in an arbitrary E_i and we get $\widetilde{\varphi}(x) = \varphi_i(x) = \varphi(x)$ since $\varphi_i|_E = \varphi$ by the definition of S, so $\widetilde{\varphi}|_E = \varphi$. To prove $\widetilde{\varphi}\colon \widetilde{E} \to L$ is a field homomorphism, pick x and y in $\widetilde{E}$. They are each in some E_i and by total ordering they are in a common E_i. Therefore $x + y \in E_i$, so $\widetilde{\varphi}(x + y) = \varphi_i(x + y) = \varphi_i(x) + \varphi_i(y) = \widetilde{\varphi}(x) + \widetilde{\varphi}(y)$, and similarly for multiplication. Also $\widetilde{\varphi}(1) = \varphi(1) = 1$. Thus $(\widetilde{E}, \widetilde{\varphi})$ is in S and is an upper bound on all the (E_i, φ_i)'s.

Now we can apply Zorn's lemma: S has a maximal element (M, σ). That is, M is a field between E and L with a homomorphism $\sigma\colon M \to L$ such that $\sigma|_E = \varphi$ and there is no extension of σ to a homomorphism from a larger intermediate field to L. We want to prove (i) $M = L$, so the original homomorphism φ extends up to L, and (ii) $\sigma\colon L \to L$ is an automorphism of L.

$\underline{M = L}$. We argue by contradiction. Suppose $M \neq L$, so there is an $\alpha \in L$ with $\alpha \notin M$. The fields M and $\sigma(M)$ are isomorphic by σ. We will find a β in L that plays a role "above" $\sigma(M)$ analogous to α "above" M so that $\sigma\colon M \to L$ can be extended to $M(\alpha) \to L$ by using σ on M and sending α to β.

Let $f(X) \in M[X]$ be the minimal polynomial of α over M and let $g(X)$ be the minimal polynomial of α over K, so $f(X) \mid g(X)$ in $M[X]$ and $\deg f = [M(\alpha) : M] > 1$. The field $\sigma(M)$ is K-isomorphic to M by σ, so applying σ to polynomial coefficients makes a ring isomorphism $M[X] \to \sigma(M)[X]$. Therefore the image of $g(X)$, say $g^\sigma(X)$, is irreducible in $\sigma(M)[X]$. (An isomorphism between two UFDs, such as $M[X]$ and $\sigma(M)[X]$, has to map irreducible elements to irreducible elements.)

Since $g(X) \mid f(X)$ in $M[X]$ and the coefficients of $f(X)$ are all in K, which is fixed pointwise by σ, applying σ to coefficients shows $g^\sigma(X) \mid f(X)$ in $(\sigma(M))[X]$. Consider both divisibility relations as taking place in $L[X]$. Since L/K is Galois, and $f(X)$ is irreducible in $K[X]$ with root $\alpha \in L$, $f(X)$ splits completely in $L[X]$. Therefore its factor $g^\sigma(X)$ splits completely in $L[X]$. *That proves $g^\sigma(X)$ has a root in L.* Let β be a root of $g^\sigma(X)$ in L. Evaluating polynomials at α gives a field isomorphism $M[X]/(g(X)) \to M(\alpha)$ and evaluating polynomials at β gives a field isomorphism $(\sigma(M))[X]/(g^\sigma(X)) \cong (\sigma(M))(\beta)$. The ring isomorphism $M[X] \to (\sigma(M))[X]$ by acting σ on coefficients induces an isomorphism $M[X]/(g(X)) \to (\sigma(M))[X]/(g^\sigma(X))$, and putting these field isomorphisms together shows

$$M(\alpha) \cong M[X]/(g(X)) \to \sigma(M)[X]/(g^\sigma(X)) \cong (\sigma(M))(\beta)$$

where the overall isomorphism, say σ', sends M to $\sigma(M)$ by σ an α is mapped to β.

Thus $(M, \sigma) \leq (M(\alpha), \sigma')$ in S, which is impossible by maximality of (M, σ), so $M = L$.

$\underline{\sigma\colon L \to L \text{ is an automorphism of } L}$.

Field homrmophisms are always injective, so we just need to show σ is surjective. Pick $\alpha \in L$. We want to show $\alpha \in \sigma(L)$. We'll consider how σ behaves on the *finite* set of K-conjugates of $\alpha \in L$.

Let $f(X) \in K[X]$ be the minimal polynomial of α over K. Since L/K is Galois and $\alpha \in L$, $f(X)$ splits completely in $L[X]$. When $f(x) = 0$ for an $x \in L$, applying σ to the equation tells us $f(\sigma(x)) = 0$ (the coefficients of $f(X)$ are in K, which is fixed pointwise by σ). Therefore σ sends the finite set of roots of $f(X)$ (the K-conjugates of α) to itself. An injective function from a finite set to itself is surjective, so $\alpha = \sigma(r)$ for some root r of $f(X)$. □

Corollary A.2. *Let L/K be a Galois extension.*

(1) *Every K-isomorphism $\varphi\colon E \to E'$ between two intermediate fields between K and L extends to a K-automorphism $\sigma\colon L \to L$.*
(2) *If E/K is Galois then the restriction homomorphism* $\mathrm{Gal}(L/K) \to \mathrm{Gal}(E/K)$ *where $\sigma \mapsto \sigma|_E$ is surjective.*

Proof. (1) View $\varphi\colon E \to E'$ as a field homomorphism $\varphi\colon E \to L$ with image E'. By Theorem A.1, there is a K-automorphism $\sigma\colon L \to L$ extending φ, meaning $\sigma(x) = \varphi(x)$ for all $x \in E$.

(2) If E/K is Galois inside L/K, then for each $\varphi \in \mathrm{Gal}(E/K)$, part (1) with $E' = E$ tells us there is $\sigma \in \mathrm{Gal}(L/K)$ such that $\sigma = \varphi$ on E, which is another way of saying $\sigma|_E = \varphi$. □

Appendix B. Topological groups

Infinite Galois groups have a topology that makes the group law and inversion continuous (Theorem 4.6(1)). There are many other groups with a topology in which the group law and inversion are continuous, such as $\mathbf{R}^n$ with its usual topology and the general linear and orthogonal matrix groups $\mathrm{GL}_n(\mathbf{R})$ and $\mathrm{O}_n(\mathbf{R})$ with their topologies as subsets of $\mathbf{R}^{n^2}$. In the 19th century mathematicians began to study groups that are also real manifolds, for which the group law and inversion are smooth functions. These are called Lie groups. Infinite Galois groups are not Lie groups[3]. The development of number theory in the first half of the 20th century led to more examples of groups having a notion of continuity on them that are not manifolds (the adeles and ideles of a number field). A unifying concept for groups on which the group operation is continuous (rather than smooth), which includes both arbitrary Galois groups and Lie groups as special cases, is a topological group. In this appendix we review some basic properties of such groups.

Definition B.1. A *topological group* is a group G with a topology on it for which the multiplication operation $G \times G \to G$, where $(x, y) \to xy$, and the inversion operation $G \to G$, where $x \mapsto x^{-1}$ are both continuous.

Example B.2. Under addition, $\mathbf{R}$ and $\mathbf{R}^n$ with their usual (Euclidean) topology are topological groups.

Example B.3. An arbitrary group G equipped with the discrete topology is a topological group. In particular, finite groups are topological groups when they have the discrete topology.

Example B.4. A Galois group with the Krull topology is a topological group.[4]

Remark B.5. We need to include continuity of inversion in the definition of a general topological group. There are examples of groups with a topology for which multiplication is continuous but inversion is not.

[3] An infinite Galois group is totally disconnected with a topology that is not discrete, while a Lie group is totally disconnected only if it has the discrete topology.

[4] In the chapter of Lang's *Real and Functional Analysis* about integration on locally compact groups, his examples of topological groups start off with Lie groups like $\mathbf{C}^\times$ or $\mathrm{SL}_n(\mathbf{R})$ and end with $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ with the Krull topology and the p-adic numbers, after which he writes "If you don't know these last two examples, don't panic; forget about them. They won't be used in this book." If you don't know about $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ with the Krull topology then *do* panic, since understanding that topology is part of the point of these notes.

The key topological feature of a topological group G is its *homogeneity*: the neighborhoods of the identity and the neighborhoods of every other element in G look the same. (This is visually clear when $G = \mathbf{R}^n$.) The reason is that left multiplication by each $g \in G$ is a continuous function $\ell_g \colon G \to G$ with a continuous inverse (namely left multiplication by g^{-1}), so ℓ_g is a homeomorphism that sends the identity element to g. Right multiplication by g is also a homeomorphism of G taking e to g, which need not be the same as left multiplication by g when G is non-abelian. Homogeneity in a topological group often reduces arguments about neighborhoods of arbitrary points to neighborhoods of the identity. The reason is that U is a neighborhood of g if and only if $g^{-1}U$ is a neighborhood of the identity. (More generally, if $\{U_i\}$ is a fundamental system of neighborhoods of the identity in G then for each $g \in G$, $\{gU_i\}$ is a fundamental system of neighborhoods of g.)

To appreciate homogeneity, we use it to prove a theorem on closures and a theorem on continuity of homomorphisms.

Theorem B.6. *Let H be a subgroup of a topological group G. Its closure $\overline{H}$ is a subgroup, and if H is normal in G then $\overline{H}$ is normal in G.*

Proof. This could be proved with a direct use of the definition of closure: $g \in \overline{H}$ when every open subset of G that contains g intersects H. Instead we will give a proof using a property of closures and homogeneity:

- if a subset C is closed, then gC and Cg are closed for each $g \in G$,
- the closure $\overline{A}$ of a subset A is the smallest closed subset containing it: if $A \subset C$ and C is closed then $\overline{A} \subset C$.

To prove $\overline{H}$ is a subgroup we want to show $\overline{H}\,\overline{H} \subset \overline{H}$ and $\overline{H}^{-1} = \overline{H}$.

Since H is a subgroup, $HH \subset H \subset \overline{H}$. Thus for each $h \in H$, $hH \subset \overline{H}$, so $H \subset h^{-1}\overline{H}$. The set $h^{-1}\overline{H}$ is closed since $\overline{H}$ is closed, so $\overline{H} \subset h^{-1}\overline{H}$. Thus $h\overline{H} \subset \overline{H}$ for all $h \in H$, so $H\overline{H} \subset \overline{H}$.

To improve this to $\overline{H}\,\overline{H} \subset \overline{H}$, pick $y \in \overline{H}$ to get $Hy \subset \overline{H}$, so $H \subset \overline{H}y^{-1}$. Since $\overline{H}y^{-1}$ is closed, $\overline{H} \subset \overline{H}y^{-1}$. Thus $\overline{H}y \subset \overline{H}$, and since y was arbitrary in $\overline{H}$ we get $\overline{H}\,\overline{H} \subset \overline{H}$. (Try to reprove that now on your own.)

For inversion, $H \subset \overline{H} \Rightarrow H^{-1} \subset \overline{H}^{-1}$[5] so $H \subset \overline{H}^{-1}$. Since inversion is a homeomorphism, $\overline{H}^{-1}$ is closed, so $\overline{H} \subset \overline{H}^{-1}$. Taking inverses once more gives us $\overline{H}^{-1} \subset \overline{H}$, so $\overline{H}^{-1} = \overline{H}$.

Now suppose $H \lhd G$. To prove $\overline{H} \lhd G$ we want to show $g\overline{H}g^{-1} = \overline{H}$ for *all* $g \in G$, and from basic group theory it suffices to show $g\overline{H}g^{-1} \subset \overline{H}$ for all $g \in G$.

Since $H \lhd G$, $gHg^{-1} = H \subset \overline{H}$, so $H \subset g^{-1}\overline{H}g$. The set $g^{-1}\overline{H}g$ is closed in G since $\overline{H}$ is, so $\overline{H} \subset g^{-1}\overline{H}g$. Thus $g\overline{H}g^{-1} \subset \overline{H}$. Since g is arbitrary in G, $\overline{H} \lhd G$. □

The following theorem shows how topological properties of a homomorphism between topological groups reduces to checking the property at the identity.

Theorem B.7. *Let $f \colon G \to H$ be a homomorphism between topological groups.*

1) *The map f is continuous if and only if f is continuous at the identity in G: for each open set V around the identity in H there's an open set U around the identity in G such that $f(U) \subset V$.*
2) *The map f is open if and only if f is open at the identity in G: for each open set U in G containing the identity, $f(U)$ contains an open set around the identity in H.*

[5] This is not like inequalities: $0 < a < b \Rightarrow 1/b < 1/a$, but $A \subset B \Rightarrow f(A) \subset f(B)$ for functions.

Proof. 1) If f is continuous then it is continuous at the identity in G. Conversely, suppose f is continuous at the identity in G. To prove f is continuous at each $g \in G$, pick an open set V in H around $f(g)$. Then $f(g)^{-1}V$ is an open set around the identity in H, so continuity at the identity implies there's an open set U around the identity in G such that $f(U) \subset f(g)^{-1}V$. Thus $f(gU) = f(g)U \subset V$, so gU is an open set around g in G whose image lies in V.

2) If f is an open map then it is open at the identity in G. To prove the converse, suppose f is open at the identity in G. Pick a nonempty open set U in G and choose $g \in U$. Then $g^{-1}U$ is an open set containing the identity in G, so $f(g^{-1}U) = f(g)^{-1}f(U)$ contains an open set around the identity in H, so using left multiplication by $f(g)$ shows $f(U)$ contains an open set around $f(g)$. Therefore $f(U)$ is open. □

To apply Theorem B.7, it suffices to check the conditions on a fundamental system of neighborhoods around the identity in G. Of course it is crucial in Theorem B.7 that we are working with *homomorphisms*. A random function on a topological group can't have its continuity verified by looking only at its behavior near the identity.

Definition B.8. A function $f\colon G \to H$ between topological groups is called an *isomorphism of topological groups* when f is an isomorphism of groups and a homeomorphism of topological spaces.

Example B.9. The exponential function e^x is an isomorphism between the topological groups $\mathbf{R}$ under addition and $(0, \infty)$ under multiplication.

It's important to keep in mind the difference between an isomorphism of groups and an isomorphism of topological groups. For a function between topological groups to be an isomorphism it has to be an isomorphism both algebraically and topologically: a group isomorphism and a homeomorphism. While a bijective homomorphism between groups is a group isomorphism (that is, the inverse map is automatically a homomorphism), in topology a bijective continuous map need not be a homeomorphism: the inverse map might not be continuous. Equivalently, the original map might not be an open map.

For example, if X is a non-discrete topological space and X_d is the same set as X but it is equipped with the discrete topology, then the identity map $X_d \to X$ is a continuous bijection that is not a homeomorphism. If we write down a continuous homomorphism $G \to H$ of topological groups, prove it is surjective, and call the kernel N, then the induced map $G/N \to H$ is a group isomorphism and it is continuous (using the quotient topology on G/N, of course), but we are not automatically guaranteed that this map is a homeomorphism. In order to prove a continuous group isomorphism is a topological group isomorphism, we need to show the map is open (or equivalently, closed).

Since a continuous bijection from a compact space to a Hausdorff space is closed, when we are dealing with compact Hausdorff topological groups, the subtlety above does not occur: a bijective continuous homomorphism $G \to H$ from a compact topological group to a Hausdorff topological group is a homeomorphism and thus is an isomorphism of topological groups.

Theorem B.10. *Let G be a topological group with identity e.*

(1) *The topology of G is discrete if and only if $\{e\}$ is an open subset.*
(2) *The topology of G is Hausdorff if and only if $\{e\}$ is a closed subset.*

Proof. 1) By definition, a topological space is discrete when all of its subsets are open, which is equivalent to all of its one-element subsets being open.

In particular, if $\{e\}$ is open then $\{g\}$ is open for each $g \in G$ by homogeneity; the converse is obvious.

2) If G is Hausdorff, then every point is a closed subset, so in particular $\{e\}$ is closed. Conversely, if $\{e\}$ is closed then every point in G is closed by the homogeneity of G. To conclude that G is Hausdorff, it suffices to separate e and an arbitrary element $g \neq e$ by disjoint open sets. (Here is why that suffices: given distinct x and y in G, if U and U' are open sets separating e and xy^{-1}, then Uy and $U'x$ are open sets separating y and x.)

First we show that for a neighborhood $\mathcal{N}$ of e in G there is a "symmetric" neighborhood U of e such that $U = U^{-1}$ (U is symmetric) and $UU \subset \mathcal{N}$. Since the multiplication map $m\colon G \times G \to G$ is continuous, there are open sets U_1 and U_2 around e such that $m(U_1 \times U_2) \subset \mathcal{N}$. Let $U' = U_1 \cap U_2$, which is also an open neighborhood of e, so $m(U' \times U') \subset \mathcal{N}$. Set $U = U' \cap U'^{-1}$, so $U = U^{-1}$ and $m(U \times U) = UU \subset U'U' \subset \mathcal{N}$.

Returning to the task of separating e and g by open sets, since $G - \{g\}$ is an open neighborhood of e the previous paragraph tells us there is an open set U containing e such that $U = U^{-1}$ and $UU \subset G - \{g\}$. Then $U \cap gU = \emptyset$: if $u_1 = gu_2$ with u_1 and u_2 in U, then $g = u_1u_2^{-1} \subset UU^{-1} = UU \subset G - \{g\}$, which is a contradiction. Since $e \in U$ and $g \in gU$, the sets U and gU separate e and g by disjoint open sets. □

Corollary B.11. *If $f\colon G \to H$ is a continuous homomorphism of topological groups and H is Hausdorff then $\ker f$ is a closed normal subgroup of G.*

Proof. The kernel of f is the inverse image of the identity in H. The identity is closed in H since H is Hausdorff, so its inverse image under f is closed in G, and that inverse image is $\ker f$. □

When G is a topological group and N is a normal subgroup, the reader should check that the group G/N is a topological group in the quotient topology.

Corollary B.12. *Let G be a topological group and N be a normal subgroup. The group G/N, with the quotient topology, is discrete if and only if N is open in G and G/N is Hausdorff if and only if N is closed in G.*

Proof. The identity element in G/N is the "point" $\overline{N}$ of G/N (the overline in this proof denotes reduction mod N, *not* topological closure) and the inverse image of this point under the quotient map $G \to G/N$ is the subset N of G. From the definition of the quotient topology, $\{\overline{N}\}$ is open in G/N if and only if its inverse image N is an open subset in G, and likewise $\{\overline{N}\}$ is closed in G/N if and only if N is closed in G. Theorem B.10, applied to G/N, completes the proof. □

Remark B.13. If H is an arbitrary subgroup of G, not necessarily normal, then the conclusions of Corollary B.12 remain true for the left coset space G/H using its quotient topology, although we can't prove it by applying Theorem B.10 to G/H since G/H is not generally a group.

Theorem B.14. *In a Hausdorff topological group, every discrete subgroup is closed.*

It is crucial here that we are working with discrete *subgroups*: a discrete subset need not be closed. In the topological group $\mathbf{R}$, the subset $\{1, 1/2, 1/3, 1/4, \dots\}$ is discrete but not closed.

Proof. Let H be a discrete subgroup of a Hausdorff topological group G. To show H is closed, we will show the complement $G - H$ is open. Pick $g \notin H$. We will find an open neighborhood of g in G that is disjoint from H.

By discreteness of H, there is an open subset $\mathcal{N}$ of G such that $\mathcal{N} \cap H = \{e\}$. From the proof of Theorem B.10, there is an open neighborhood U of e such that $U = U^{-1}$ and $UU \subset \mathcal{N}$.

Suppose gU meets H twice: $gu_1 = h_1$ and $gu_2 = h_2$. Then $h_1^{-1}h_2 = u_1^{-1}u_2 \subset H \cap UU \subset H \cap \mathcal{N} = \{e\}$, so $h_1 = h_2$ and $u_1 = u_2$. Thus $gU \cap H$ has size at most 1. If $gU \cap H$ is empty then gU is the desired open neighborhood of g that is disjoint from H. If $gU \cap H$ is not empty then this intersection has size 1. Since G is Hausdorff there is a smaller open set U' in U such that $gU' \cap H$ is empty and we can use gU'. □

It is true more generally that in a Hausdorff topological group every locally compact subgroup is closed [8, p. 8]. (A discrete subgroup is locally compact since all discrete topological spaces are locally compact.)

Corollary B.15. *If N is a discrete normal subgroup of a Hausdorff topological group then G/N is Hausdorff in the quotient topology.*

Proof. Since N is discrete in G and G is Hausdorff, N is closed by Theorem B.14, and therefore G/N is Hausdorff by Corollary B.12. □

Theorem B.16. *In a topological group, every open subgroup is closed and every closed subgroup of finite index is open.*

Proof. Let H be a subgroup of a topological group G. The left H-cosets in G are a disjoint covering of G. If H is open then each gH is open, since gH is homeomorphic to H. Therefore the union of all left H-cosets other than H is open, which implies H is closed (being the complement of an open set). If H is closed then its left cosets are all closed, so if H has finite index in G then the union of the left H-cosets other than H is closed, so H is open. □

Example B.17. In the group $\mathbf{R}^\times$ with its usual topology, the subgroup $\mathbf{R}_{>0}$ is open and closed (with index 2). The subgroup $\{\pm 1\}$ is closed not of finite index and is not open.

Corollary B.18. *In a compact topological group, a subgroup is open if and only if it is closed with finite index.*

Proof. Let G be a compact topological group with subgroup H. If H is open then it is closed by Theorem B.16. The left cosets of H in G are an open covering of G, which has a finite subcovering. This subcovering must be the original one since different cosets are disjoint. Therefore H has finitely many left cosets in G, so $[G : H]$ is finite.

If H is closed with finite index then it is open by Theorem B.16. □

This corollary tells us that in a compact topological group, a subgroup of finite index is open if and only if it is closed. It's natural to ask for an example of a compact topological group that has a subgroup of finite index that is not open (equivalently, not closed). There is no example among compact Lie groups, since in a Lie group (compact or not), every subgroup of finite index is closed. There are examples but the examples all involve Zorn's lemma and thus are totally nonconstructive.

If G is a topological group and N is a normal subgroup then the quotient map $G \to G/N$ is continuous since projection to any quotient topological space is continuous when using the quotient topology. This quotient map also has additional properties:

Theorem B.19. *If G is a topological group and N is a normal subgroup then the quotient map $G \to G/N$ is an open map. If N is compact then $G \to G/N$ is also a closed map.*

Proof. Let U be open in G and $\pi\colon G \to G/N$ be the reduction map. The image $\pi(U)$ is open, by definition, only when $\pi^{-1}(\pi(U)) = \bigcup_{n\in N} Un$ is open in G, and this union is open since each Un is homeomorphic to U and thus is open.

Now let N be compact and C be closed in G. Then $\pi^{-1}(\pi(C)) = \bigcup_{n\in N} Cn = CN$. In a topological group, the product of a closed subset and a compact subset, like CN, is closed. For a proof, see [7, p. 173] or [8, p. 7]. □

In general $G \to G/N$ is not a closed map. Consider $\mathbf{R} \to \mathbf{R}/\mathbf{Z}$ and the discrete subgroup $\sqrt{2}\mathbf{Z}$ in $\mathbf{R}$. It is closed but its image in $\mathbf{R}/\mathbf{Z}$ is dense (it is the multiples of an irrational angle, if we identify $\mathbf{R}/\mathbf{Z}$ with S^1 by $\overline{a} \mapsto e^{2\pi i a}$) and not closed.

There is one simple condition we can impose for a discrete subgroup of G to have a discrete image in G/N.

Theorem B.20. *Let G be a Hausdorff topological group and H be a discrete subgroup. If N is a normal subgroup of G contained in H then H/N is discrete in G/N.*

Proof. The topology on H/N as a subset of G/N is the quotient topology on H/N, which is discrete since H is assumed to have the discrete topology as a subset of G. □

(The reason this proof breaks down when we try applying it to the image of $\sqrt{2}\mathbf{Z}$ in $\mathbf{R}/\mathbf{Z}$ is that we need to write the image as $H/\mathbf{Z}$ where $H \supset \mathbf{Z}$. The only choice for that is $H = \mathbf{Z} + \sqrt{2}\mathbf{Z}$, which is not discrete in $\mathbf{R}$.)

Theorem B.21. *Let G be a Hausdorff topological group and N be a closed normal subgroup. Then G is compact if and only if N and G/N are compact.*

Proof. Since closed subspaces and continuous images of compact spaces are compact, if G is compact then N and G/N are compact.

Conversely, assume N and G/N are compact. Since N is compact, the reduction map $G \to G/N$ has compact fibers (that is, each coset gN is compact) and the reduction map is a closed map by Theorem B.19. A continuous function between topological spaces that is a closed map and has compact fibers is a *proper* map, which means its inverse images of compact sets are compact.[6] For a proof, see the Wikipedia page on proper maps. Since G/N is compact and its full inverse image under the reduction map $G \to G/N$ is G, the group G is compact. □

References

[1] R. Dedekind, "Über die Permutationen des Körpers aller algebraischen Zahlen," Festschrift zur Feier des hundertfnfzighährigen Bestehens der König. Gesell. der Wiss. zu Göttingen Abhandlungen der math.physik. Klasse (1901), 1–17. Online at https://publikationsserver.tu-braunschweig.de/receive/dbbs_mods_00065820

[2] W. Krull, "Galoissche Theorie der unendlichen algebraischen Erweiterungen," Math. Ann. **100** (1928), 687–698. Online at https://eudml.org/doc/159314.

[3] N. Nikolov, D. Segal, "On finitely generated profinite groups. I. Strong completeness and uniform bounds," Ann. of Math. **165** (2007), 171–238.

[4] N. Nikolov, D. Segal, "On finitely generated profinite groups. II. Products in quasisimple groups," Ann. of Math. **165** (2007), 239–273.

[5] S. Lang, *Real and Functional Analysis*, 3rd ed., Springer-Verlag, New York, 1993.

[6] S. Lang, *Undergraduate Algebra*, 2nd ed., Springer-Verlag, 1990.

[7] J. Munkres, *Topology: a First Course*, Prentice Hall, 1974.

[8] D. Ramakrishnan and R. J. Valenza, *Fourier Analysis on Number Fields*, Springer-Verlag, 1999.

[6] The reduction map $\mathbf{R} \to \mathbf{R}/\mathbf{Z}$ is not proper: the inverse image of a point is not compact.