Notes on Etale cohomology: Preliminaries on Galois theory

Chunye Yang

March 30, 2026

This will be the preliminary section following that on field theory. We will discuss mostly Galois groups of finite Galois extensions and give a lot of examples, many of which you are going to find familiar in the main part of the study of etale cohomology.

1 Galois Extensions

As what has been explained in the previous part of the notes on field theory, we will say that an algebraic extension K/k is **Galois** if it's normal and separable. The group of automorphisms of K over k is called the **Galois group** of K/k and is always denoted by $\mathrm{Gal}(K/k)$. If we already have K embedded in an algebraic closure of k, then this group coincides with the group of embeddings of K over k to the algebraic closure. If G is a group of automorphisms (not necessarily all of them) of a field K, then we use K^G to denote the subfield invariant under the group action. Note that this definition of Galois groups makes sense for any field extensions K/k, i.e. is defined to be the group of k-automorphism. The reason we require normal and separable is because this is the case when the Galois groups behaves most nicely.

We will directly state the main result of this section and do the proof later:

Theorem 1.1. Let K/k be a finite Galois extension of k, with the Galois group $\mathrm{Gal}(K/k) = G$. There is a bijection between the set of subfields of E of K containing k and the set of subgroups H of G, given by $E = K^H$. The field E is Galois over k iff H is a normal subgroup in G. If H is indeed normal in G, then the map $\sigma \mapsto \sigma|_E$ induces an isomorphism between the group G/H to $\mathrm{Gal}(E/k)$.

Notice that this theorem is stated for finite Galois extensions. This is the most common situation we will face later in the study of etale cohomology, to avoid distraction, we will only mention what happens for infinite Galois extensions in due time without spending too much time on that in the first few basic sections. There will be an independent section on infinite Galois extensions later.

Theorem 1.2. Let K/k be a Galois extension with Galois group $G = \mathrm{Gal}(K/k)$, then $k = K^G$ and the map that maps intermediate field F to $\mathrm{Gal}(K/F)$ is injective.

Proof. Notice that there is a natural identification of $\mathrm{Gal}(K/F)$ as a subgroup of $\mathrm{Gal}(K/k)$ as if an automorphism fixes F it must fixed k.

Recall that K^G/k is going to be a purely inseparable extension by what we saw in the field theory section (the idea being that any k-embedding of $k(\alpha)$ to the algebraic closure can be extended to an automorphism of K, but α is fixed by all such automorphisms, therefore we know that the embedding must map α to itself, thus is the identity embedding.) However, since K/k is separable, so is K^G/k, therefore we know that K^G/k is both separable and purely inseparable, thus it's k. This proves our first assertion.

Let F be an intermediate field, then we have seen that K/F is again normal separable and normal, thus Galois. Then we know that if we let $H = \mathrm{Gal}(K/F)$, then we know that $K^H = F$. Say F, F' are two different intermediate fields, if the images are the same subgroup H of G, then we know that the fixed field should also be the same, therefore $F = F'$, a contradiction, thus we are done. $\square$

The key observation in the above theorem is that if K/k is separable with $G = \mathrm{Gal}(K/k)$, then $K^G = k$. Here we don't have to assume any finiteness condition on the extension.

Definition 1.3. We will call the subgroup $\mathrm{Gal}(K/F)$ of the intermediate field extension F the group **associated to** the subfield F. We also say that a subgroup $H \subset \mathrm{Gal}(K/k)$ **belongs** to a subfield extension F if $H = \mathrm{Gal}(K/F)$.

Corollary 1.4. If K/k is Galois with Galois group G, then if H, H' are two subgroups of G belonging to subfields F, F', then the subgroup $H \cap H'$ belong to FF'.

Proof. Notice that an automorphism fixing FF' must fix F, F' respectively, therefore for any $\sigma \in \mathrm{Gal}(K/FF')$, it's in $H \cap H'$. Conversely, let $\sigma \in H \cap H'$ it's easy to prove that it also preserves FF'. ☐

Corollary 1.5. Using the same notation as the above corollary, then we know that the fixed field of the smallest subgroup of G containing H, H' is $F \cap F'$.

Proof. Notice that $F \cap F'$ is indeed fixed by the subgroup generated by H, H' therefore the fixed field is at least as large as $F \cap F'$. If there is something not in $F \cap F'$, then we can assume that either it's not in F or it's not in F'. Say it's not in F, then there will be an element in $\mathrm{Gal}(K/F) = H$ that doesn't fix it, therefore this element can not be in the fixed field of the subgroup generated by H, H', similar conclusion holds for F', therefore the fixed field can only be $F' \cap F$. ☐

Corollary 1.6. Still use the same notation, then $F \subset F'$ iff $H' \subset H$.

Proof. If $F \subset F'$, then any automorphism fixing F' must fix F, therefore $H' \subset H$. If $H' \subset H$, then we know that $F = K^H \subset F' = K^{H'}$. ☐

Corollary 1.7. Let E be a finite separable extension of k and let K be the smallest normal extension of k containing E contained in some larger field, then K is finite Galois over k and there are only finitely many intermediate fields between K and k.

Proof. Recall that the smallest normal extension of k containing E is going to be the compositum of $\sigma_i K$ where σ_i are the embeddings of K to the algebraic closure. Notice that each $\sigma_i K$ is separable over k, therefore so is the compositum. Therefore we know that K/k is normal and separable, thus Galois. Moreover, since finiteness is also preserved under finite compositums, we know that K is finite over k as well.

Then recall that any finite separable extension has a primitive element, thus only has a finite number of intermediate extensions. Or you can argue by the fact that K/k is finite Galois then the Galois group only has a finite number of elements, therefore there are only a finite number of subfields of K containing k, thus only a finite number of subfields of E containing k. ☐

The following is a very useful lemma you will also use in the main chapters of the notes. Notice that we have to impose the separability condition in order to invoke the primitive element theorem:

Lemma 1.8. Let K/k be algebraic and **separable**, assume that there is an integer $n \geqslant 1$ such that every $\alpha \in E$ is of degree $\leqslant n$ over k, then $[K : k]$ is a finite number and is at most n.

Proof. There is an element $\alpha \in K$ such that $[k(\alpha) : k]$ is maximal. I claim that $k(\alpha) = K$. To see why, if there is a $\beta \in K$ that is not in $k(\alpha)$, we can consider $k(\alpha, \beta)/k$ which has a strictly larger degree than that of $k(\alpha)/k$. However, recall that $k(\alpha, \beta) = k(\gamma)$ for some $\gamma \in K$, this is a contradiction. ☐

Theorem 1.9. Let K be a field and let G be a finite group of automorphisms of K, of order n. Let $k = K^G$, then K/k is finite Galois with Galois G. Moreover $[K : k] = n$.

Proof. We have already seen the idea of the proof. Let $\alpha \in K$, we want to show that α is separable over $k = K^G$. Recall that G is finite, then we can pick a maximal subset such that: $\sigma_1\alpha, \cdots, \sigma_r\alpha$ are different. Then we saw that:

$$f(x) = \prod_{i=1}^{r}(x - \sigma_i\alpha)$$

is in $k[x]$. This is a separable polynomial, therefore α must be separable over k. Moreover we notice that all the roots of f is in K, therefore K is the splitting field of all such polynomials when α ranges over all elements of K, thus K/k is normal and separable.

Notice that:

$$n = |G| \leqslant |\mathrm{Gal}(K/k)| \leqslant [K : k] \leqslant n$$

Therefore we know that G must be the Galois group. $\square$

Corollary 1.10. Let K/k be a finite Galois extension, then the degree $[K : k]$ is equal to the order of $\mathrm{Gal}(K/k)$.

Proof. Notice that in the case of a finite Galois extension, k is K^G and $G = \mathrm{Gal}(K/k)$ is a finite group, then we know that we can apply the previous theorem and conclude that $[K : k] = |\mathrm{Gal}(K/k)|$. $\square$

Corollary 1.11. Let K be a finite Galois extension of k and let G be it's Galois group, then every subgroup of G belongs to some intermediate subfield.

Proof. Let H be a subgroup of G, since G is finite, then any of it's subgroup must be finite. Then consider the fixed field $F = K^H$. Notice that H/F is again Galois and finite with $F = K^H$. Then we know that the Galois group of F is going to be H by the previous theorem. $\square$

Remark 1.12. Note that in the above proof, the fact that $G = \mathrm{Gal}(K/k)$ is finite is used in an essentially way, i.e. we want all it's subgroups to be finite. Indeed, when K/k is infinite, the corollary is not necessarily true.

In the infinite case, we will give the Galois group G the Krull topology, and it turns out only the subgroups of G that are closed correspond to an intermediate field. We will discuss this later in the section on infinite Galois extension, you will then find that the proof is not that different. In the finite case, you can think of we are giving the Galois group the discrete topology, therefore any subgroup is going to be closed, thus the finite extension case is actually a special case for the infinite extension. For the time being, you only need to keep in mind this conclusion.

By now, we have seen that if K/k is finite Galois, we know that the map $F \mapsto \mathrm{Gal}(K/F)$ is injective. For any $H \subset G$, there is an intermediate F such that $\mathrm{Gal}(K/F) = H$, therefore we get the desired bijection with it's inverse given by $H \mapsto K^H$. This proves the first assertion in the main theorem. Now we begin to discuss the question that when H belongs to F, when H is going to be normal.

We can temporarily drop the assumption that K/k is finite. Let K/k be a Galois extension, and let $\lambda : K \to \lambda K$ be an isomorphism between K and a field called λK. Notice that this isomorphism also induces an isomorphism between k and a subfield of λK. Let's call it λk and we have the following diagram:

$$\begin{tikzcd} K \arrow[r, "\lambda"] & \lambda K \\ k \arrow[u, hook] \arrow[r, "\lambda"'] & \lambda k \arrow[u, hook] \end{tikzcd}$$

We observe that we have an isomorphism of groups:

$$\mathrm{Gal}(K/k) \to \mathrm{Gal}(\lambda K/\lambda k), \qquad \sigma \mapsto \lambda \circ \sigma \circ \lambda^{-1}$$

Therefore we may write $\mathrm{Gal}(\lambda K/\lambda k) = \lambda \mathrm{Gal}(K/k)\lambda^{-1}$. Or we can write $\mathrm{Gal}(\lambda K/\lambda k)^\lambda = \mathrm{Gal}(K/k)$ where the exponential λ means that:

$$\sigma^\lambda = \lambda^{-1} \circ \sigma \circ \lambda$$

In particular, let K/k be an algebraic extension, and let $k \subset F \subset K$ be an intermediate field, we know that if K/k is Galois, then if we consider an embedding $\lambda : F \to K$, which can be extended to an automorphism of K since K/k is normal, therefore we have the diagram:

$$\begin{tikzcd} K \arrow[r, "\lambda"] & K \\ F \arrow[u, hook] \arrow[r, "\lambda"] & \lambda F \arrow[u, hook] \end{tikzcd}$$

Hence:

$$\mathrm{Gal}(K/\lambda F)^{\lambda} = \mathrm{Gal}(K/F)$$

and:

$$\mathrm{Gal}(K/\lambda F) = \lambda \mathrm{Gal}(K/F)\lambda^{-1}$$

Theorem 1.13. Let K be a Galois extension of k with Galois group G. Let F be an intermediate field and let $H = \mathrm{Gal}(K/F)$. Then F is normal over k iff H is normal in G.

Moreover if F is normal over k, then the restriction map $\sigma \mapsto \sigma|_F$ is a homomorphism of G onto $\mathrm{Gal}(F/k)$, whose kernel is H, thus:

$$\mathrm{Gal}(K/k)/H \simeq \mathrm{Gal}(F/k)$$

Proof. First, assume that F/k is normal, then consider the restriction of σ, we know that it's indeed in $\mathrm{Gal}(F/k)$. By definition, we know that the kernel is $\mathrm{Gal}(K/F)$ since by definition the kernel should be those that fixes F. Given any automorphism of F over k, it can be extended to an automorphism of K since K is normal, therefore we know that the morphism is surjective. Therefore H is normal, being the kernel, and G/H is isomorphic to $\mathrm{Gal}(F/k)$.

Conversely, let H be normal, then I will first let you figure out why any embedding λ of F to the algebraic closure containing K maps F to K. Then let the image of λ be λF, then we know that:

$$\mathrm{Gal}(K/\lambda F) = \lambda \mathrm{Gal}(K/F)\lambda^{-1}$$

then since $H = \mathrm{Gal}(K/F)$ is normal, we know that conjugation preserves the subgroup, therefore we have:

$$H = \mathrm{Gal}(K/\lambda F) = \mathrm{Gal}(K/F)$$

Moreover, we know that $\lambda F = K^H = F$, therefore $\lambda F = F$, thus F is normal. $\square$

Remark 1.14. Notice that there is no finiteness condition involved here.

Definition 1.15. A Galois extension K/k is said to be **abelian** (resp. **cyclic**) if it's Galois group G is abelian (resp. cyclic). If we say that K/k is abelian or cyclic, it already implies K/k is Galois.

Proposition 1.16. Let K/k be an abelian (resp. cyclic) extension, if F is an intermediate field $k \subset F \subset K$, then F is automatically Galois over k and is abelian (resp. cyclic).

Proof. This just follows any subgroup of an abelian group is normal and any quotient of an abelian (resp. cyclic) group is abelian (resp. cyclic). $\square$

This finishes the proof of the main theorem in this section. We will then proceed to other interesting topics:

Theorem 1.17. Let K/k be Galois and F/k an arbitrary extension contained in some larger field, then we know that KF/F is Galois and $K/K \cap F$ is also Galois.

Let $H = \mathrm{Gal}(KF/F)$ and $G = \mathrm{Gal}(K/k)$, the we have a group homomorphism:

$$H \to G, \qquad \sigma \mapsto \sigma|_K$$

gives an isomorphism between H and the subgroup $\mathrm{Gal}(K/K \cap F)$ of G. This is illustrated in the following diagram:

$$\begin{tikzcd}
 & KF & \\
K \arrow[ur] & & F \arrow[ul] \\
 & K \cap F \arrow[ul] \arrow[ur] & \\
 & k \arrow[u] &
\end{tikzcd}$$

Proof. First, let σ be an element of H, i.e. an automorphism of KF over F. If we restrict it to K, we know that it's an k-embedding of K to the larger field. Since k is normal over k, then we know that if $\alpha \in K$, let $f(x)$ be the minimal polynomial of α, all of the roots of $f(x)$ is in K, then we know that the embedding maps roots of $f(x)$ to roots of $f(x)$, therefore the image of α is still a root of $f(x)$, therefore is in K. Since K is algebraic over k, this is indeed an isomorphism, therefore we know the restriction is indeed an element in $\mathrm{Gal}(K/k)$. Clearly since restriction commutes with composition, we know that this is a group homomorphism.

Suppose that the restriction of σ is the identity, i.e. it acts trivially on K, then since element in KF are:

$$k_1 f_1 + \cdots + k_r f_r$$

fro $k_i \in K, f_i \in F$, we know that σ also acts trivial on FK. Therefore the kernel is 0, thus injective. Notice that clearly the image fixed $K \cap F$. Then given an element $\alpha \in K$, say fixed by H', then we know that it's also fixed by H, therefore α is actually in F, thus $\alpha \in K \cap F$. If K is finite over k or FK is finite over F, we know that $K \cap K \cap F$ is also Galois and it's Galois group is H' which is the either finite since K/k is finite or is finite since it's isomorphic to the Galois group of KF/F which is finite. Then since $K \cap F$ is the fixed field of H', we know that H' is the Galois group of $K/F \cap F$.

If we don't have the finiteness conditions, notice that we can still conclude that $K \cap F$ is the fixed field of H', but not like the finiteness case, we must prove that H' indeed belongs to a field to conclude that $K \cap F$ maps to H'. To show this, we need the fact that the map $H \to G$ defined by restriction is continuous and the fact that H is a compact group, therefore H' being the image of a compact group is closed, therefore indeed belongs to some field, we are done. □

Corollary 1.18. Let K be a finite Galois extension of k and let F be an arbitrary extension of K. Then we know that the degree $[KF : F]$ divides $[K : k]$.

Proof. Recall that $[KF : F] = |\mathrm{Gal}(KF : F)|$ and $[K : k] = |\mathrm{Gal}(K/k)|$. We know that $\mathrm{Gal}(KF : F)$ is isomorphic to a subgroup of $\mathrm{Gal}(K : k)$. Then since the order of the subgroup always divides the order of the group, we are done. □

Remark 1.19. The assertion of the above corollary is not true if K is not Galois over k. Let's consider $\alpha = \sqrt[3]{2}$, the real cubic root of 2. Let ξ be a cubic root of 1 which is not 1, say $\xi = \frac{-1+\sqrt{-3}}{2}$.

Let $\beta = \alpha\xi$, and let $E = \mathbb{Q}(\beta)$. Notice that β is complex and α is real, then we know $\mathbb{Q}(\beta) \neq \mathbb{Q}(\alpha)$. Then consider the following diagram:

$$\begin{tikzcd}
& \mathbb{Q}(\alpha, \beta) & \\
\mathbb{Q}(\beta) \arrow[ur] & & \mathbb{Q}(\alpha) \arrow[ul] \\
& \mathbb{Q}(\alpha) \cap \mathbb{Q}(\beta) \arrow[ul] \arrow[ur] & \\
& \mathbb{Q} \arrow[u] &
\end{tikzcd}$$

Notice that $\mathbb{Q}(\beta)$ is not normal over $\mathbb{Q}$. To see why, we notice that the minimal polynomial of β is $x^3 - 2$. Then I claim that there is a root of $x^3 - 2$ that is not in $\mathbb{Q}(\beta)$. Recall that the roots of $x^3 - 2$ are $\sqrt[3]{2}, \xi\sqrt[3]{2} = \beta, \xi^2\sqrt[3]{2}$. Then if $\xi^2\sqrt[3]{2}$ is in $\mathbb{Q}(\beta)$, then we know that ξ is in $\mathbb{Q}(\beta)$, therefore we know that:

$$\mathbb{Q}(\beta) = \mathbb{Q}(\beta, \xi) = \mathbb{Q}(\xi, \alpha) = \mathbb{Q}(\sqrt[3]{2}, \sqrt{-3})$$

Notice that this can be divided to a tower:

$$\mathbb{Q} \subset \mathbb{Q}(\sqrt[3]{2}) \subset \mathbb{Q}(\sqrt[3]{2}, \sqrt{-3})$$

Notice that the first degree is 3 and since the minimal polynomial of $\sqrt{-3}$ is $x^2 + 3$, we know that the second degree is 3, therefore the degree is 6, a contradiction to the fact that $\mathbb{Q}(\beta)$ is of degree 3.

Then notice that $\mathbb{Q}(\alpha) \cap \mathbb{Q}(\beta)$ over $\mathbb{Q}$ is of degree that divides 3, thus is either 1 or 3. However since $\mathbb{Q}(\alpha)$ is not equal to $\mathbb{Q}(\beta)$, we know that the degree is 1. Then notice that $\mathbb{Q}(\alpha, \beta) = \mathbb{Q}(\alpha, \sqrt{-3})$, thus of degree 6 over $\mathbb{Q}$, therefore of degree 2 over $\mathbb{Q}(\alpha)$. However, we know that $\mathbb{Q}(\beta)/\mathbb{Q} = 3$.

Theorem 1.20. Let K_1, K_2 be two Galois extensions of k with Galois groups G_1, G_2 respectively. Assume that K_1, K_2 are subfields of some common larger field. Then we know that K_1K_2 is Galois over k, let G be it's Galois group. The map $G \to G_1 \times G_2$ given by restriction:

$$\sigma \mapsto (\sigma|_{K_1}, \sigma|_{K_2})$$

is injective. Moreover if $K_1 \cap K_2 = k$, then it's an isomorphism.

Proof. Obviously this is a group homomorphism and let's assume that σ induce identity on both K_1, K_2, then since elements in K_1K_2 are quotients of the form $x_1y_1 + \cdots + x_ry_r$ for $x_i \in K_1, y_i \in K_2$, we know that σ is also the identity on the compositum, therefore the map is injective.

Now assume $K_1 \cap K_2 = k$, then we know that given $\sigma_1 \in G_1$, there will be an element $\sigma \in \mathrm{Gal}(K_1K_2/K_2)$ such that it's restriction to K_1 is σ_1 from the previous theorem. Notice that such a σ is in $\mathrm{Gal}(K_1K_2/K_2)$, hence we know that $G_1 \times \{e\}$ is contained in the image of $G \to G_1 \times G_2$. Similarly, we can conclude that $\{e\} \times G_2$ is in the image, therefore $G_1 \times G_2$ is in the image, thus surjective. This is illustrated in the following diagram:

$$\begin{tikzcd}
 & K_1K_2 & \\
K_1 \arrow[ur] & & K_2 \arrow[ul] \\
 & K_1 \cap K_2 \arrow[ul] \arrow[ur] & \\
 & k \arrow[u] &
\end{tikzcd}$$

□

Corollary 1.21. If $K_1, \cdots, K_n$ are Galois extensions of a field k, with Galois groups $G_1, \cdots, G_n$. Then if we have $K_{i+1} \cap (K_1 \cdots K_i) = k$ for all $i = 1, \cdots, n-1$, then the Galois group of $K_1 \cdots K_n$ is naturally isomorphic to $G_1 \times \cdots \times G_n$, i.e. through restrictions to K_i.

Proof. Use induction and the above theorem. □

Corollary 1.22. Let K be a finite Galois extension of k with Galois group G. Assume that there is a direct product decomposition $G = G_1 \times \cdots \times G_n$. Let K_i be the fixed field of:

$$G_1 \times \cdots \times \{1\} \times \cdots \times G_n$$

where only the i-th slot is $\{1\}$. Then K_i is Galois over k and $K_{i+1} \cap (K_1 \cdots K_i) = k$ for all i with $K = K_1 \cdots K_n$.

Proof. Recall that the compositum of all K_i belongs to the intersection of all G_i, which is the identity. Then what is the fixed subfield of the identity, we know it's K itself, thus we are done.

Then notice that each factor is normal in G, therefore K_i is going to be normal in K, thus Galois over k, with Galois group $G_1 \times \cdots \times \{1\} \times \cdots \times G_n$ where the i-th slot is $\{e\}$. Recall that the intersection of normal extensions is still normal and it belongs to the smallest subgroup containing all $G_1 \times \cdots \times \{1\} \times \cdots \times G_n$. Then suppose that we consider $K_1 \cap K_2$, we know that the fixed field of the product of their Galois group is going to be $K_1 \cap K_2$. But the product of their Galois group is G, therefore $K_1 \cap K_2 = k$.

Similarly we can argue for $K_3 \cap (K_1K_2)$, we know that the Galois group for K_1K_2 is the intersection which makes the first and second slot e, but we know that the Galois group of K_3 has $G_1 \times G_2$ in the first and second slot, therefore we are done. □

Remark 1.23. In the previous corollary, the reason we assume that the extension is finite is because only by having this algebraic decomposition to direct products, we don't actually know if any of the subgroups are closed or not, therefore we can not use the fundamental theorem to conclude that they are the Galois group of some intermediate fields.

Theorem 1.24. Assume in this theorem, all fields are finite Galois extensions of k contained in a common larger field:

1. If K, L are abelian over k, then so is the composite.
2. If K is abelian over k and E is any extension of k, then KE is abelian over E.
3. If K is abelian over k and $k \subset E \subset K$ is an intermediate field, then E is abelian over k and k is abelian over E.

Proof. To prove 1, notice that the Galois group $\mathrm{Gal}(KL/k)$ is a subgroup of the product $\mathrm{Gal}(K/k) \times \mathrm{Gal}(L/k)$, therefore is abelian.

To prove 2, notice that $\mathrm{Gal}(KE/E)$ is a subgroup of $\mathrm{Gal}(K/k)$, therefore when $\mathrm{Gal}(K/k)$ is abelian, so is $\mathrm{Gal}(KE/E)$.

The last one is trivial thus omitted. □

Definition 1.25. If k is a field, contained in an algebraic closure k^a, then the compositum of all abelian extensions in this algebraic closure is called **maximum abelian extension** of k and is denoted by k^{ab}.

In the section of infinite Galois extensions, we will prove that such an extension is also abelian, thus lives up to the name of maximum abelian extension.

2 Infinite Galois Extension

In this short section, we briefly tie up some loose ends in the previous section related to infinite Galois extensions, especially how Galois correspondence between intermediate fields and subgroups works in the infinite case. Many of the discussions here will find their generalization in the section on group cohomology later. However, you should still read this section if you are not familiar with infinite Galois extensions.

One typical example of infinite Galois extension, which is going to appear as examples in the study of etale cohomology is the following: if k is a field and consider the separable closure k^s in the algebraic closure k^a. By definition k^s/k is separable and it's not hard to prove that k^s/k is also normal, thus is Galois. Then we would like to ask, what is the Galois group $\mathrm{Gal}(k^s/k)$, which is also called the **absolute Galois group** of k. In the end of this section, we will able to define it as an inverse limit using finite Galois extension.

Let's first do some set-up: Let K/k be an Galois extension, possibly infinite. We define the Krull topology on the group $\mathrm{Gal}(K/k) = G$ by defining a base for open sets to consist of sets σH where $\sigma \in G$ and $H = \mathrm{Gal}(K/F)$ for some finite extension F of k contained in K. This is equivalent to define a basis for the identity element, i.e. a basis of e consists of $H = \mathrm{Gal}(K/F)$ for some finite extension F of k contained in K. Then since we want G to be a topological group, then we want multiplication by some element in G to be a homeomorphism of G, therefore the basis at another element σ is transferred from the basis at e to σ by just multiplying by σ.

One immediate question of such a definition is: why we only multiply on the left, not on the right of H? To answer this question:

Proposition 2.1. If we take F/k to be finite and Galois, we obtain another basis for the topology define by σH where $H = \mathrm{Gal}(K/F)$ for finite (not necessarily Galois F over k).

Proof. Notice that every F/k is contained in F', where F'/k is finite and Galois. Then we know that $\mathrm{Gal}(K/F') \subset \mathrm{Gal}(K/F)$, therefore given any element H in the basis defined by finite extension, we can find a finite Galois extension with Galois group H' such that $H' \subset H$. Conversely, we know that every finite Galois extension is finite, therefore we know these two basis are equivalent. □

One we know that we only need to consider finite Galois extensions, we know that H is going to be a normal subgroup of G, therefore there is no difference in differentiating the left multiplication and right multiplication. So from now on, we only consider F/k to be finite Galois.

Now think the set of all finite Galois extensions of K containing k, notice that this is a direct system in the sense of inclusion. Then we know that if $F \subset F'$, we know that $H_{F'} \subset H_F$, therefore we get a canonical morphism:

$$G/H_{F'} \to G/H_F$$

Then we consider the inverse limit:

$$\varprojlim_{F/k} G/H_F \hookrightarrow \prod_{F/k} G/H_F$$

Give the quotient the quotient topology and the direct product the product topology and I claim that it will be compact. To see why, first notice that G/H_F is a finite group for every F/k. Recall that without any of the machinery in this section, we already proved that $G/H_F \simeq \mathrm{Gal}(F/k)$, but since F/k is finite, the Galois group is finite. It's actually to see that the quotient topology on G/H_F is actually the discrete topology, then obviously compact. Then we know from Tychonoff's theorem that the product of any collection of compact topological spaces with the product topology is going to be compact.

Proposition 2.2.

$$\varprojlim_{F/k} G/H_F \hookrightarrow \prod_{F/k} G/H_F$$

makes $\varprojlim_{F/k} G/H_F$ a closed subspace of the product in the subspace topology, therefore the inverse limit is compact as well.

Proof. For each $H' \subset H$, let's call the canonical morphism from $G/H' \to G/H$ $\pi_{H',H}$.

Notice that if for each $H' \subset H$, we define a set:

$$C_{H',H} = \{(x_J)_J : \pi_{H',H}(X_{H'}) = X_H\}$$

Clearly, we know that the inverse limit is the intersection of $C_{H',H}$ when H', H ranges over all pairs $H' \subset H$ where H, H' are Galois groups of F/k and F'/k. Therefore it suffices to show that each $C_{H',H}$ is closed. Now consider the map:

$$\prod_H G/H \to G/H \times G/H$$

where $(X_J) \mapsto (X_H, \pi_{H',H}(X_{H'}))$. Notice that this is continuous where $G/H \times G/H$ is a discrete space, since it's just the projection map. Then we consider the diagonal of $G/H \times G/H$, we know that $C_{H',H}$ is the inverse image of the diagonal of $G/H \times G/H$, therefore is indeed closed. $\square$

I claim that these information is enough for us to show that $\mathrm{Gal}(K/k)$ is compact. The key is the following propositions:

Proposition 2.3. Consider the canonical morphism:

$$G \to \varprojlim_H G/H$$

defined by $G \to G/H$. This is not only an isomorphism of groups, but also a homeomorphism of topological groups.

Proof. Let's first prove that this is an isomorphism of groups. Say $\sigma \in G$ is mapped to the identity, then we know that σ is in H for all F/k, in particular $\sigma \in \mathrm{Gal}(k/k) = \{e\}$, therefore $\sigma = e$.

Consider $\{\sigma_H\}$ in the inverse limit with $\sigma_H \in G/H$. We know that being in the inverse limit means that it has to satisfy some compatibility conditions and you will see this compatibility conditions helps define an element in G. Say $\alpha \in K$, we know that it's contained in some finite Galios F/k, then let $H = \mathrm{Gal}(K/F)$, we define:

$$\sigma\alpha = \sigma_H \alpha$$

Notice that this definition is well defined. First if we pick different representation σ'_H of σ_H we know that $\sigma'_H \circ \sigma_H^{-1} \in H$ therefore we know that the action on α is the identity. Then if we consider another F' finite separable over k which contains α, we know that there is another finite Galois F''/k with F, F' contained in F''. Then we know that the compatibility conditions means that: $\sigma_H, \sigma_{H'}$ both comes from $\sigma_{H''}$, then I will let you check that $\sigma_H \alpha = \sigma_{H''} \alpha = \sigma_{H'} \alpha$, therefore the definition is indeed fine. I will let you check that this is indeed an automorphism of K over k. It's easy to see that σ leaves k fixed, we claim it's an automorphism by observing that $\{\sigma_H^{-1}\}$ is also an element in the inverse limit, which defines the inverse of σ. This shows this is an isomorphism of groups and we know that since this map is defined by the universal property, it's going to be continuous. Therefore, we only need to show it's an open mapping to show it's a homeomorphism.

It suffices to show that it maps basis to opens, i.e. we need to check that σH is mapped to an open in the inverse limit. We can further only check the basis at the identity element. Let H be such a basis open at the identity, I claim that the image in the inverse limit is:

$$\{(x_H) \in \varprojlim G/H : x_H = H\}$$

First, we know that if some element is in the image, then clearly, the H component is H. Therefore the image is contained in the subset we described. Conversely, if we have some element in the subset described above, since the map $G \to \varprojlim_H G/H$ is surjective, there is some $\tau \in G$ such that it's image in the inverse limit has H in the H-component, therefore we know that $\sigma \in H$, thus the subset is contained in the image. Therefore the two are equal, but the subset we described is one of the basic opens of the product space, we are done. $\square$

The above result shows that since G is isomorphic to $\varprojlim_H G/H$ which is compact, we know that G is itself compact.

Proposition 2.4. Every closed subgroup of G of finite index is open.

Proof. Notice that if H in G is of finite index and is closed, we know that the other cosets in G/H rather than H is finite and each of them is homeomorphic to H, thus is also closed. Notice that these cosets are disjoint, therefore H is the complement of the union of other cosets, thus is open. $\square$

The same argument shows that any open subgroup of finite index is closed.

Proposition 2.5. The closed subgroups of $\mathrm{Gal}(K/k)$ are precisely those subgroups which are of the form $\mathrm{Gal}(K/F)$ where F/k is a finite extension.

Proof. Let's first prove that $\mathrm{Gal}(K/F)$ is closed. Recall that if $\alpha \in F$, we know that $\mathrm{Gal}(K/F)$ is the intersection of:

$$C_\alpha = \{\sigma \in G : \sigma(\alpha) = \alpha\}$$

Notice that we can consider $k(\alpha)/k$, which is finite, therefore by definition we know that $C_\alpha = \mathrm{Gal}(K/k(\alpha))$ which is open, then we only need to show it's of finite index. I will let you show it.

Conversely let C be a closed subgroup and let $F = K^C$, we want to show that $\mathrm{Gal}(K/F) = C$. Notice that $\mathrm{Gal}(K/F)$ is closed and F is fixed by it. We know that $C \subset \mathrm{Gal}(K/F)$, so we need to show the reverse inclusion. Let $\sigma \in \mathrm{Gal}(K/F)$ we want to show that $\sigma \in C$, that is every basis of σ meets C. Let E/k be a finite Galois extension of k with $H = \mathrm{Gal}(K/E)$ we want to show that $C \cap \sigma H$ is not empty. Notice that since E/k is Galois finite, we know that EF/F is also finite Galois, then we can consider the restriction map:

$$\mathrm{Gal}(K/F) \to \mathrm{Gal}(EF/F)$$

this makes sense since EF is normal over F.

Notice that since F is the fixed subfield, we know that any element in C restricted to EF is in $\mathrm{Gal}(EF/F)$, then I claim that the restriction is surjective. Notice that the if we consider the field fixed by the image, we notice that it's still F as we know that EF is a subfield of K containing F. Therefore by the finite Galois correspondence the image is all of $\mathrm{Gal}(EF/F)$. Notice that $\sigma \in \mathrm{Gal}(K/F)$, then we know that there is some $c \in C$ such that $\sigma|_{EF} = c|_{EF}$. This implies that $\sigma^{-1}c$ fixes EF, thus fixed E, therefore $\sigma^{-1}c \in \mathrm{Gal}(K/E) = H$, therefore $c \in \sigma H$, we are done. $\square$

Proposition 2.6. Let $C \subset G$ be an arbitrary subgroup of G, then I claim that:

$$\overline{C} = \mathrm{Gal}(K/F)$$

where $F = K^C$.

Proof. Clearly $C \subset \mathrm{Gal}(K/F)$, thus $\overline{C} \subset \mathrm{Gal}(K/F)$ since $\mathrm{Gal}(K/F)$ is closed. Then we need to prove that for any $\sigma \in \mathrm{Gal}(K/F)$, σH for any H associated to a finite Galois extension F, σH intersect with C. This is essentially the same argument as above, thus we are done. $\square$

Remark 2.7. One last piece we used in the proof is that in the following diagram:

$$\begin{tikzcd}
& KF & \\
K \arrow[ur] & & F \arrow[ul] \\
& K \cap F \arrow[ul] \arrow[ur] & \\
& k \arrow[u] &
\end{tikzcd}$$

where K/k is Galois and F/k is arbitrary, the restriction $\mathrm{Gal}(KF/F) \to \mathrm{Gal}(K/k)$ is continuous. We need to show that if E/k is a finite Galois extension of k contained in K, the inverse image of σH where $H = \mathrm{Gal}(K/E)$ is open in $\mathrm{Gal}(KF/F)$.

Notice that the image of the restriction is in $\mathrm{Gal}(K/K \cap F)$, which is a closed subgroup. Therefore we can assume that $K \cap F = k$. Then consider the following diagram:

$$\begin{tikzcd}
& KF & & \\
K \arrow[ur] & & EF \arrow[ul] & \\
& E \arrow[ul] \arrow[ur] & & F \arrow[ul] \\
& & k \arrow[ul] \arrow[ur] &
\end{tikzcd}$$

where E/k is finite Galois and we know that $E \cap F = k$, then we know that the restriction of $\mathrm{Gal}(EF/F) \to \mathrm{Gal}(E/k)$ is bijective using the finiteness of extension.

This implies that the morphism:

$$\mathrm{Gal}(KF/F) \to \mathrm{Gal}(K/k)$$

factors through the isomorphism:

$$\mathrm{Gal}(KF/F)/\mathrm{Gal}(KF/EF) \to \mathrm{Gal}(K/k)/\mathrm{Gal}(K/E)$$

Therefore the inverse image of $\mathrm{Gal}(K/E)$ is exactly $\mathrm{Gal}(KF/EF)$. Recall since the restriction is a group homomorphism and it's continuous at the identity of $\mathrm{Gal}(K/k)$, we know that it's globally continuous and I will let you prove this.

Finally, we tale a little bit about the absolute Galois group, $\mathrm{Gal}(k^s/s)$, by our proposition on the inverse limit, it's the inverse limit:

$$\mathrm{Gal}(k^s/k) \simeq \varinjlim \mathrm{Gal}(F/k)$$

where F are finite Galois extensions of k and the transition maps are given by if $F' \subset F$, then:

$$\mathrm{Gal}(F/k) \to \mathrm{Gal}(F'/k), \qquad \sigma \mapsto \sigma|_{F'}$$

We will use this example in the study of etale cohomology.

3 Examples and Applications

In this section, we will compute some Galois groups as examples, both to be more familiar with the topic and to see some applications. It turns that some example is also useful in the study of etale cohomology so be sure you understand all the examples here.

4 Roots of Unity

5 Linear Independence of Characters

6 Norm and Trace

7 Cyclic Extensions

8 Solvable and Radical Extensions

9 Abelian Kummer Theory

10 The Equation $X^n - a$

11 Algebraic Independence of Homomorphisms

12 The Normal Basis Theorem

References