CAMBRIDGE

Cambridge University Press
978-0-521-88850-9 - Galois Groups and Fundamental Groups
Tamas Szamuely
Excerpt
More information

1

Galois theory of fields

This first chapter is both a concise introduction to Galois theory and a warmup for the more advanced theories to follow. We begin with a brisk but reasonably complete account of the basics, and then move on to discuss Krull's Galois theory for infinite extensions. The highlight of the chapter is Grothendieck's form of Galois theory that expresses the main theorem as a categorical anti-equivalence between finite étale algebras and finite sets equipped with a continuous action of the absolute Galois group. This theorem is a prototype for many statements of similar shape that we shall encounter later.

1.1 Algebraic field extensions

In this section and the next we review some basic facts from the theory of field extensions. As most of the material is well covered in standard textbooks on algebra, we shall omit the proof of a couple of more difficult theorems, referring to the literature instead.

Definition 1.1.1 Let k be a field. An extension $L|k$ is called *algebraic* if every element α of k is a root of some polynomial with coefficients in k. If this polynomial is monic and irreducible over k, it is called the *minimal polynomial* of α.

When L is generated as a k-algebra by the elements $\alpha_1, \ldots, \alpha_m \in L$, we write $L = k(\alpha_1, \ldots, \alpha_m)$. Of course, one may find many different sets of such α_i.

Definition 1.1.2 A field is *algebraically closed* if it has no algebraic extensions other than itself. An *algebraic closure* of k is an algebraic extension $\bar{k}$ that is algebraically closed.

The existence of an algebraic closure can only be proven by means of Zorn's lemma or some other equivalent form of the axiom of choice. We record it in the following proposition, along with some important properties of the algebraic closure.

Proposition 1.1.3 *Let k be a field.*

1. *There exists an algebraic closure $\bar{k}$ of k. It is unique up to (non-unique) isomorphism.*
2. *For an algebraic extension L of k there exists an embedding $L \to \bar{k}$ leaving k elementwise fixed.*
3. *In the previous situation take an algebraic closure $\overline{L}$ of L. Then the embedding $L \to \bar{k}$ can be extended to an isomorphism of $\overline{L}$ onto $\bar{k}$.*

For the proof, see Lang [48], Chapter V, Corollary 2.6 and Theorem 2.8, or van der Waerden [106], §72.

Thus henceforth when speaking of algebraic extensions of k we may (and often shall) assume that they are embedded in a fixed algebraic closure $\bar{k}$.

Facts 1.1.4 A finite extension L of k is algebraic. Its *degree* over k, denoted by $[L : k]$, is its dimension as a k-vector space. If L is generated over k by a single element with minimal polynomial f, then $[L : k]$ is equal to the degree of f. For a tower of finite extensions $M|L|k$ one has the formula $[M : k] = [M : L][L : k]$. All this is proven by easy computation.

Definition 1.1.5 A polynomial $f \in k[x]$ is *separable* if it has no multiple roots (in some algebraic closure of k). An element of an algebraic extension $L|k$ is *separable* over k if its minimal polynomial is separable; the extension $L|k$ itself is called *separable* if all of its elements are separable over k.

Separability is automatic in characteristic 0, because a well-known criterion implies that an *irreducible* polynomial has no multiple roots if and only if its derivative f' is nonzero (see [106], §44). However, the derivative can be zero in characteristic $p > 0$, e.g. for a polynomial $x^p - a$, which is irreducible for $a \in k^\times \setminus k^{\times p}$.

In the case of finite extensions there is the following important characterization of separability.

Lemma 1.1.6 *Let $L|k$ be a finite extension of degree n. Then L has at most n distinct k-algebra homomorphisms to $\bar{k}$, with equality if and only if $L|k$ is separable.*

Proof Choose finitely many elements $\alpha_1, \dots, \alpha_m$ that generate L over k. Assume first $m = 1$, and write f for the minimal polynomial of α_1 over k. A k-homomorphism $L \to \bar{k}$ is determined by the image of α_1, which must be one of the roots of f contained in $\bar{k}$. The number of distinct roots is at most n, with equality if and only if α is separable. From this we obtain by induction on m using the multiplicativity of the degree in a tower of finite field extensions that L has at most n distinct k-algebra homomorphisms to $\bar{k}$, with equality if the α_i are separable. To prove the 'only if' part of the lemma, assume $\alpha \in L$ is not separable over k. Then by the above the number of k-homomorphisms $k(\alpha) \to \bar{k}$ is strictly less than $[k(\alpha) : k]$, and that of $k(\alpha)$-homomorphisms from L to $\bar{k}$ is at most $[L : k(\alpha)]$. Thus there are strictly less than n k-homomorphisms from L to $\bar{k}$. □

The criterion of the lemma immediately implies:

Corollary 1.1.7 *Given a tower $L|M|k$ of finite field extensions, the extension $L|k$ is separable if and only if $L|M$ and $M|k$ are.*

In the course of the proof we have also obtained:

Corollary 1.1.8 *A finite extension $L|k$ is separable if and only if $L = k(\alpha_1, \dots, \alpha_m)$ for some separable elements $\alpha_i \in L$.*

We now show that there is a largest separable subextension inside a fixed algebraic closure $\bar{k}$ of k. For this recall that given two algebraic extensions L, M of k embedded as subfields in $\bar{k}$, their *compositum* LM is the smallest subfield of $\bar{k}$ containing both L and M.

Corollary 1.1.9 *If L, M are finite separable extensions of k, their compositum is separable as well.*

Proof By definition of LM there exist finitely many separable elements $\alpha_1, \dots, \alpha_m$ of L such that $LM = M(\alpha_1, \dots, \alpha_m)$. As the α_i are separable over k, they are separable over M, and so the extension $LM|M$ is separable by the previous corollary. But so is $M|k$ by assumption, and we conclude by Corollary 1.1.7. □

In view of the above two corollaries the compositum of all finite separable subextensions of $\bar{k}$ is a separable extension $k_s|k$ containing each finite separable subextension of $\bar{k}|k$.

Definition 1.1.10 The extension k_s is called the *separable closure* of k in $\bar{k}$.

From now on by 'a separable closure of k' we shall mean its separable closure in some chosen algebraic closure.

The following important property of finite separable extensions is usually referred to as the *theorem of the primitive element*.

Proposition 1.1.11 *A finite separable extension can be generated by a single element.*

For the proof, see Lang [48], Chapter V, Theorem 4.6 or van der Waerden [106], §46.

A field is called *perfect* if all of its finite extensions are separable. By definition, for perfect fields the algebraic and separable closures coincide.

Examples 1.1.12

1. Fields of characteristic 0 and algebraically closed fields are perfect.
2. A typical example of a non-perfect field is a rational function field $\mathbf{F}(t)$ in one variable over a field $\mathbf{F}$ of characteristic p: here adjoining a p-th root ξ of the indeterminate t defines an inseparable extension in view of the decomposition $X^p - t = (X - \xi)^p$.

   This is a special case of a general fact: a field k of characteristic $p > 0$ is perfect if and only if $k^p = k$ ([48], Chapter V, Corollary 6.12 or [106], §45). The criterion is satisfied by a finite field $\mathbf{F}_{p^r}$ as its multiplicative group is cyclic of order $p^r - 1$; hence finite fields are perfect.

1.2 Galois extensions

Now we come to the fundamental definition in Galois theory. Given an extension L of k, denote by $\mathrm{Aut}(L|k)$ the group of field automorphisms of L fixing k elementwise. The elements of L that are fixed by the action of $\mathrm{Aut}(L|k)$ form a field extension of k. In general it may be larger than k.

Definition 1.2.1 An algebraic extension L of k is called a *Galois extension* of k if the elements of L that remain fixed under the action of $\mathrm{Aut}(L|k)$ are *exactly* those of k. In this case $\mathrm{Aut}(L|k)$ is denoted by $\mathrm{Gal}\,(L|k)$, and called the *Galois group* of L over k.

Though the above definition is classical (it goes back to Emil Artin), it may not sound familiar to some readers. We shall now make the link with other definitions. The first step is:

Lemma 1.2.2 *A Galois extension $L|k$ is separable, and the minimal polynomial over k of each $\alpha \in L$ splits into linear factors in L.*

Proof Each element $\alpha \in L$ is a root of the polynomial $f = \prod(x - \sigma(\alpha))$, where σ runs over a system of (left) coset representatives of the stabilizer of α in $G = \mathrm{Gal}\,(L|k)$. The product is indeed finite, because the $\sigma(\alpha)$ must be roots of the the minimal polynomial g of α. In fact, we must have $f = g$. Indeed, both polynomials lie in $k[x]$ and have α as a root, hence each $\sigma(\alpha)$ must be a root of both. Thus f divides g but g is irreducible. Finally, by construction f has no multiple roots, thus α is separable over k. □

The converse also holds. Before proving it, we consider the 'most important' example of a Galois extension.

Example 1.2.3 A separable closure k_s of a field k is always a Galois extension. Indeed, to check that it is Galois we have to show that each element α of k_s not contained in k is moved by an appropriate automorphism in $\mathrm{Aut}(k_s|k)$. For this let $\alpha' \in k_s$ be another root of the minimal polynomial of α, and consider the isomorphism of field extensions $k(\alpha) \xrightarrow{\sim} k(\alpha')$ obtained by sending α to α'. An application of the third part of Proposition 1.1.3 shows that this isomorphism can be extended to an automorphism of the algebraic closure $\bar{k}$. To conclude one only has to remark that each automorphism of $\mathrm{Aut}(\bar{k}|k)$ maps k_s onto itself, since such an automorphism sends an element β of $\bar{k}$ to another root β' of its minimal polynomial; thus if β is separable, then so is β'.

The group $\mathrm{Gal}\,(k_s|k)$ is called the *absolute Galois group* of k.

We can now state and prove the following important characterization of Galois extensions.

Proposition 1.2.4 *Let k be a field, k_s a separable closure and $L \subset k_s$ a subfield containing k. The following properties are equivalent.*

1. *The extension $L|k$ is Galois.*
2. *The minimal polynomial over k of each $\alpha \in L$ splits into linear factors in L.*
3. *Each automorphism $\sigma \in \mathrm{Gal}\,(k_s|k)$ satisfies $\sigma(L) \subset L$.*

Proof The proof of (1) ⇒ (2) was given in Lemma 1.2.2 above. The implication (2) ⇒ (3) follows from the fact that each $\sigma \in \mathrm{Gal}\,(k_s|k)$ must map $\alpha \in L$ to a root of its minimal polynomial. Finally, for (3) ⇒ (1) pick $\alpha \in L \setminus k$. As k_s is Galois over k (Example 1.2.3), we find $\sigma \in \mathrm{Gal}\,(k_s|k)$ with $\sigma(\alpha) \neq \alpha$. By (3), this σ preserves L, so its restriction to L yields an element of $\mathrm{Aut}(L|k)$ which does not fix α. □

Using the proposition it is easy to prove the main results of Galois theory for finite Galois extensions.

Theorem 1.2.5 (Main Theorem of Galois theory for finite extensions) *Let $L|k$ be a finite Galois extension with Galois group G. The maps*

$$M \mapsto H := \mathrm{Aut}(L|M) \quad \text{and} \quad H \mapsto M := L^H$$

yield an inclusion-reversing bijection between subfields $L \supset M \supset k$ and subgroups $H \subset G$. The extension $L|M$ is always Galois. The extension $M|k$ is Galois if and only if H is a normal subgroup of G; in this case we have $\mathrm{Gal}\,(M|k) \cong G/H$.

In the above statement the notation L^H means, as usual, the subfield of L fixed by H elementwise.

Proof Let M be a subfield of L containing k. Fixing a separable closure $k_s|k$ containing L, we see from Proposition 1.2.4 (3) that $L|k$ being Galois automatically implies that $L|M$ is Galois as well. Writing $H = \mathrm{Gal}\,(L|M)$, we therefore have $L^H = M$. Conversely, if $H \subset G$, then L is Galois over L^H by definition, and the Galois group is H. Now only the last statement remains to be proven. If $H \subset G$ is normal, we have a natural action of G/H on $M = L^H$, since the action of $g \in G$ on an element of L^H only depends on its class modulo H. As $L|k$ is Galois, we have $M^{G/H} = L^G = k$, so $M|k$ is Galois with group G/H. Conversely, if $M|k$ is Galois, then each automorphism $\sigma \in G$ preserves M (extend σ to an automorphism of k_s using Proposition 1.1.3 (3), and then apply Proposition 1.2.4 (3)). Restriction to M thus induces a natural homomorphism $G \to \mathrm{Gal}\,(M|k)$ whose kernel is exactly $H = \mathrm{Gal}\,(M|k)$. It follows that H is normal in G. □

Classically Galois extensions arise as *splitting fields* of separable polynomials. Given an irreducible separable polynomial $f \in k[x]$, its splitting field is defined as the finite subextension $L|k$ of $k_s|k$ generated by all roots of f in k_s. This notion depends on the choice of the separable closure k_s.

Lemma 1.2.6 *A finite extension $L|k$ is Galois if and only if it is the splitting field of an irreducible separable polynomial $f \in k[x]$.*

Proof The splitting field of an irreducible separable polynomial is indeed Galois, as it satisfies criterion (3) of Proposition 1.2.4. Conversely, part (2) of the proposition implies that a finite Galois extension $L|k$ is the splitting field of a primitive element generating L over k. □

Corollary 1.2.7 *A finite extension $L|k$ is Galois with group $G = \mathrm{Aut}(L|k)$ if and only if G has order $[L : k]$.*

Proof If $L|k$ is Galois, it is the splitting field of a polynomial by the proposition, so G has order $[L : k]$ by construction. Conversely, for $G = \mathrm{Aut}(L|k)$ the extension $L|L^G$ is Galois by definition, so G has order $[L : L^G]$ by what we have just proven. This forces $L^G = k$. □

Remark 1.2.8 An important observation concerning the splitting field L of a polynomial $f \in k[x]$ is that by definition $\mathrm{Gal}\,(L|k)$ acts on L by permuting the roots of f. Thus if f has degree n, we obtain an injective homomorphism from $\mathrm{Gal}\,(L|k)$ to S_n, the symmetric group on n letters. This implies in particular that $L|k$ has degree at most $n!$. The bound is sharp; see for instance Example 1.2.9 (3) below.

In the remainder of this section we give examples of Galois and non-Galois extensions.

Examples 1.2.9

1. Let $m > 2$ be an integer and ω a primitive m-th root of unity. The extension $\mathbf{Q}(\omega)|\mathbf{Q}$ is Galois, being the splitting field of the minimal polynomial of ω, the m-th *cyclotomic polynomial* Φ_m. Indeed, all other roots of Φ_m are powers of ω, and hence are contained in $\mathbf{Q}(\omega)$. The degree of Φ_m is $\phi(m)$, where ϕ denotes the Euler function. The Galois group is isomorphic to $(\mathbf{Z}/m\mathbf{Z})^\times$, the group of units in the ring $\mathbf{Z}/m\mathbf{Z}$. When m is a prime power, it is known to be cyclic.
2. For an example of infinite degree, let $\mathbf{Q}(\mu)|\mathbf{Q}$ be the extension obtained by adjoining all roots of unity to $\mathbf{Q}$ (in the standard algebraic closure $\overline{\mathbf{Q}}$ contained in $\mathbf{C}$). Every automorphism in $\mathrm{Gal}\,(\overline{\mathbf{Q}}|\mathbf{Q})$ must send $\mathbf{Q}(\mu)$ onto itself, because it must send an m-th root of unity to another m-th root of unity. Thus by criterion (3) of Proposition 1.2.4 we indeed get a Galois extension. We shall determine its Galois group in the next section.

   By the same argument we obtain that for a prime number p the field $\mathbf{Q}(\mu_{p^\infty})$ generated by the p-power roots of unity is Galois over $\mathbf{Q}$.
3. Let k be a field containing a primitive m-th root of unity ω for an integer $m > 1$ invertible in k (this means that the polynomial $x^m - 1$ splits into linear factors over k). Pick an element $a \in k^\times \setminus k^{\times m}$, and let $\sqrt[m]{a}$ be a root of it in an algebraic closure $\bar{k}$. The extension $k(\sqrt[m]{a})|k$ is Galois with group $\mathbf{Z}/m\mathbf{Z}$, generated by the automorphism $\sigma : \sqrt[m]{a} \to \omega\sqrt[m]{a}$. This is because all roots of $x^m - a$ are of the form $\omega^i\sqrt[n]{a}$ for some $0 \leq i \leq m - 1$.
4. When k does not contain a primitive m-th root of unity, we may not get a Galois extension. For instance, take $k = \mathbf{Q}$, $m = 3$ and $a \in \mathbf{Q}^\times \setminus \mathbf{Q}^{\times 3}$. We define $\sqrt[3]{a}$ to be the unique real cube root of a. The extension $\mathbf{Q}(\sqrt[3]{a})|\mathbf{Q}$ is nontrivial because $\sqrt[3]{a} \notin \mathbf{Q}$, but $\mathrm{Aut}(\mathbf{Q}(\sqrt[3]{a})|\mathbf{Q})$ is trivial. Indeed, an automorphism in $\mathrm{Aut}(\mathbf{Q}(\sqrt[3]{a})|\mathbf{Q})$ must send $\sqrt[3]{a}$ to a root of $x^3 - a$ in $\mathbf{Q}(\sqrt[3]{a})$, but $\sqrt[3]{a}$ is the only one, since $\mathbf{Q}(\sqrt[3]{a}) \subset \mathbf{R}$ and the other two roots are complex. Thus the extension $\mathrm{Aut}(\mathbf{Q}(\sqrt[3]{a})|\mathbf{Q})$ is not Galois. The splitting field L of $x^3 - a$ is generated over $\mathbf{Q}$ by $\sqrt[3]{a}$ and a primitive third root of unity ω that has degree 2 over $\mathbf{Q}$, so L has degree 6 over $\mathbf{Q}$.
5. Finally, here is an example of a finite Galois extension in positive characteristic. Let k be of characteristic $p > 0$, and let $a \in k$ be an element so that the polynomial $f = x^p - x - a$ has no roots in k. (As a concrete example, one may take k to be the field $\mathbf{F}_p(t)$ of rational functions with mod p coefficients and $a = t$.) Observe that if α is a root in some extension $L|k$, then the other roots are $\alpha + 1, \alpha + 2, \ldots, \alpha + (p - 1)$, and therefore f splits in distinct linear factors in L. It follows that f is irreducible over k, and that the extension $k(\alpha)|k$ is Galois with group $\mathbf{Z}/p\mathbf{Z}$, a generator sending α to $\alpha + 1$.

Remark 1.2.10 There exist converse statements to Examples 3 and 5 above. The main theorem of *Kummer theory* says that for a field k containing a primitive m-th root of unity every cyclic Galois extension with group $\mathbf{Z}/m\mathbf{Z}$ is generated by an m-th root $\sqrt[m]{a}$ for some $a \in k^\times \setminus k^{\times m}$. This further generalizes to Galois extensions with a finite abelian Galois group of exponent m: they can be generated by several m-th roots.

According to *Artin-Schreier theory,* in characteristic $p > 0$ every cyclic Galois extension with group $\mathbf{Z}/p\mathbf{Z}$ is generated by a root of an 'Artin–Schreier polynomial' $x^p - x - a$ as above. There are generalizations to extensions with a finite abelian Galois group of exponent p, but also to extensions with group $\mathbf{Z}/p^r\mathbf{Z}$; the latter uses the theory of Witt vectors. For details and proofs of the above statements, see e.g. [48], Chapter VI, §8.

Our final example gives an application of the above ideas outside the scope of Galois theory in the narrow sense.

Example 1.2.11 Let k be a field, and $K = k(x_1, \dots, x_n)$ a purely transcendental extension in n indeterminates. Make the symmetric group S_n act on K via permuting the x_i. By definition the extension $K|K^{S_n}$ is Galois with group S_n. It is the splitting field of the polynomial $f = (x - x_1)\dots(x - x_n)$. As f is invariant by the action of S_n, its coefficients lie in K^{S_n}. These coefficients are (up to a sign) the *elementary symmetric polynomials*

$$\begin{aligned}\sigma_1 &= x_1 + x_2 \cdots + x_n,\\ \sigma_2 &= x_1x_2 + x_1x_3 + \cdots + x_{n-1}x_n,\\ &\vdots\\ \sigma_n &= x_1x_2\cdots x_n.\end{aligned}$$

But by definition K is also the splitting field of f over the field $k(\sigma_1, \dots, \sigma_n)$. As $k(\sigma_1, \dots, \sigma_n) \subset K^{S_n}$ and $[K : K^{S_n}] = n!$, Remark 1.2.8 shows that $K^{S_n} = k(\sigma_1, \dots, \sigma_n)$.

With a little commutative algebra one can say more. The x_i, being roots of f, are in fact *integral* over the subring $k[\sigma_1, \dots, \sigma_n] \subset k(\sigma_1, \dots, \sigma_n)$ (see Section 4.1 for basic facts and terminology). Therefore the subring $k[x_1, \dots, x_n]^{S_n} = k[x_1, \dots, x_n] \cap K^{S_n}$ of $k[x_1, \dots, x_n]$ is an integral ring extension of $k[\sigma_1, \dots, \sigma_n]$. But as $K \supset k(\sigma_1, \dots, \sigma_n)$ is a finite extension containing n algebraically independent elements, the σ_i must be algebraically independent over k. Thus $k[\sigma_1, \dots, \sigma_n]$ is isomorphic to a polynomial ring; in particular, it is integrally closed in its fraction field K^{S_n}. It follows that $k[x_1, \dots, x_n]^{S_n} = k[\sigma_1, \dots, \sigma_n]$. This is the *main theorem of symmetric polynomials*: every symmetric polynomial in n variables over k is a polynomial in the σ_i. For more traditional proofs, see [48], Chapter IV, Theorem 6.1 or [106], §33.

Remark 1.2.12 The above example also shows that each finite group G occurs as the Galois group of some Galois extension. Indeed, we may embed G in a symmetric group S_n for suitable n and then consider its action on the transcendental extension $K|k$ of the above example. The extension $K|K^G$ will then do. However, we shall see in the next section that the analogous statement is false for most infinite G.

1.3 Infinite Galois extensions

We now address the problem of extending the main theorem of Galois theory to infinite Galois extensions. The main difficulty is that for an infinite extension it will no longer be true that all subgroups of the Galois group arise as the subgroup fixing some subextension $M|k$. The first example of a subgroup that does not correspond to some subextension was found by Dedekind, who, according to Wolfgang Krull, already had the feeling that *'die Galoissche Gruppe gewissermaßen eine stetige Mannigfaltigkeit bilde'*. It was Krull who then cleared up the question in his classic paper [47]; we now describe a modern version of his theory.

Let $K|k$ be a possibly infinite Galois extension. The first step is the observation that K is a union of finite *Galois* extensions of k. More precisely:

Lemma 1.3.1 *Each finite subextension of $K|k$ can be embedded in a Galois subextension.*

Proof By the theorem of the primitive element (Proposition 1.1.11), each finite subextension is of the form $k(\alpha)$ with an appropriate element α. We may embed $k(\alpha)$ into the splitting field of the minimal polynomial of α which is Galois over k. □

This fact has a crucial consequence for the Galois group $\mathrm{Gal}\,(K|k)$, namely that it is determined by its finite quotients. We shall prove this in Proposition 1.3.5 below, in a more precise form. To motivate its formulation, consider a tower of finite Galois subextensions $M|L|k$ contained in an infinite Galois extension $K|k$. The main theorem of Galois theory provides us with a canonical surjection $\phi_{ML} : \mathrm{Gal}\,(M|k) \twoheadrightarrow \mathrm{Gal}\,(L|k)$. Moreover, if $N|k$ is yet another finite Galois extension containing M, we have $\phi_{NL} = \phi_{ML} \circ \phi_{NM}$. Thus one expects that if we somehow 'pass to the limit in M', then $\mathrm{Gal}\,(L|k)$ will actually become a quotient of the infinite Galois group $\mathrm{Gal}\,(K|k)$ itself. This is achieved by the following construction.

Cambridge University Press
978-0-521-88850-9 - Galois Groups and Fundamental Groups
Tamas Szamuely
Excerpt
More information

Construction 1.3.2 A *(filtered) inverse system* of groups $(G_\alpha, \phi_{\alpha\beta})$ consists of:

- a partially ordered set $(\Lambda, \leq)$ which is directed in the sense that for all $(\alpha, \beta) \in \Lambda$ there is some $\gamma \in \Lambda$ with $\alpha \leq \gamma, \beta \leq \gamma$;
- for each $\alpha \in \Lambda$ a group G_α;
- for each $\alpha \leq \beta$ a homomorphism $\phi_{\alpha\beta} : G_\beta \to G_\alpha$ such that we have equalities $\phi_{\alpha\gamma} = \phi_{\alpha\beta} \circ \phi_{\beta\gamma}$ for $\alpha \leq \beta \leq \gamma$.

The *inverse limit* of the system is defined as the subgroup of the direct product $\prod_{\alpha\in\Lambda} G_\alpha$ consisting of sequences (g_α) such that $\phi_{\alpha\beta}(g_\beta) = g_\alpha$ for all $\alpha \leq \beta$. It is denoted by $\varprojlim G_\alpha$; we shall not specify the inverse system in the notation when it is clear from the context. Also, we shall often loosely say that $\varprojlim G_\alpha$ is the inverse limit of the groups G_α, without special reference to the inverse system.

Plainly, this notion is not specific to the category of groups and one can define the inverse limit of sets, rings, modules, even of topological spaces in an analogous way.

We now come to the key definition.

Definition 1.3.3 A *profinite group* is defined to be an inverse limit of a system of finite groups. For a prime number p, a *pro-p group* is an inverse limit of finite p-groups.

Examples 1.3.4

1. A finite group is profinite; indeed, it is the inverse limit of the system $(G_\alpha, \phi_{\alpha\beta})$ for any directed index set Λ, with $G_\alpha = G$ and $\phi_{\alpha\beta} = \mathrm{id}_G$.
2. Given a group G, the set of its finite quotients can be turned into an inverse system as follows. Let Λ be the index set formed by the normal subgroups of finite index partially ordered by the following relation: $U_\alpha \leq U_\beta \Leftrightarrow U_\alpha \supset U_\beta$. For each pair $U_\alpha \leq U_\beta$ of normal subgroups we have a quotient map $\phi_{\alpha\beta} : G/U_\beta \to G/U_\alpha$. The inverse limit of this system is called the *profinite completion* of G, customarily denoted by $\widehat{G}$. There is a canonical homomorphism $G \to \widehat{G}$.
3. Take $G = \mathbf{Z}$ in the previous example. Then Λ is just the set $\mathbf{Z}_{>0}$, since each subgroup of finite index is generated by some positive integer m. The partial order is induced by the divisibility relation: $m|n$ iff $m\mathbf{Z} \supset n\mathbf{Z}$. The completion $\widehat{\mathbf{Z}}$ is usually called *zed hat* (or *zee hat* in the US). In fact, $\widehat{\mathbf{Z}}$ is also a ring, with multiplication induced by that of the $\mathbf{Z}/m\mathbf{Z}$.
4. In the previous example, taking only powers of some prime p in place of m we get a subsystem of the inverse system considered there; it is more convenient to index it by the exponent of p. With this convention the