Springer Monographs in Mathematics

Jean-Pierre Serre

Galois Cohomology

伽罗瓦上同调

Springer

世界图书出版公司
www.wpcbj.com.cn

Jean-Pierre Serre

Galois Cohomology

Translated from the French by Patrick Ion

Springer

图书在版编目（CIP）数据

伽罗瓦上同调 = Galois Cohomology：英文/(法)塞尔(Serre,J. P.)著. —影印本. —北京：世界图书出版公司北京公司，2013. 10
ISBN 978 - 7 - 5100 - 7027 - 3

Ⅰ. ①G… Ⅱ. ①塞… Ⅲ. ①上同调—英文 Ⅳ. ①O189. 22

中国版本图书馆 CIP 数据核字（2013）第 249313 号

书　　名：	Galois Cohomology
作　　者：	Jean - Pierre Serre
中 译 名：	伽罗瓦上同调
责任编辑：	高蓉　刘慧
出 版 者：	世界图书出版公司北京公司
印 刷 者：	三河市国英印务有限公司
发　　行：	世界图书出版公司北京公司（北京朝内大街 137 号 100010）
联系电话：	010 - 64021602，010 - 64015659
电子信箱：	kjb@ wpcbj. com. cn
开　　本：	24 开
印　　张：	10
版　　次：	2014 年 3 月
版权登记：	图字：01 - 2013 - 5939
书　　号：	978 - 7 - 5100 - 7027 - 3　　**定　　价：** 49. 00 元

Foreword

This volume is an English translation of "Cohomologie Galoisienne". The original edition (Springer LN5, 1964) was based on the notes, written with the help of Michel Raynaud, of a course I gave at the Collège de France in 1962–1963. In the present edition there are numerous additions and one suppression: Verdier's text on the duality of profinite groups. The most important addition is the photographic reproduction of R. Steinberg's "Regular elements of semisimple algebraic groups", Publ. Math. I.H.E.S., 1965. I am very grateful to him, and to I.H.E.S., for having authorized this reproduction.

Other additions include:

- A proof of the Golod-Shafarevich inequality (Chap. I, App. 2).
- The "résumé de cours" of my 1991–1992 lectures at the Collège de France on Galois cohomology of $k(T)$ (Chap. II, App.).
- The "résumé de cours" of my 1990–1991 lectures at the Collège de France on Galois cohomology of semisimple groups, and its relation with abelian cohomology, especially in dimension 3 (Chap. III, App. 2).

The bibliography has been extended, open questions have been updated (as far as possible) and several exercises have been added.

In order to facilitate references, the numbering of propositions, lemmas and theorems has been kept as in the original 1964 text.

Jean-Pierre Serre
Harvard, Fall 1996

Table of Contents

Chapter I

Cohomology of profinite groups

§1. Profinite groups

1.1 Definition

A topological group which is the projective limit of finite groups, each given the discrete topology, is called a *profinite group*. Such a group is compact and totally disconnected.

Conversely:

Proposition 0. *A compact totally disconnected topological group is profinite.*

Let G be such a group. Since G is totally disconnected and locally compact, the open subgroups of G form a base of neighbourhoods of 1, cf. e.g. Bourbaki TG III, §4, n°6. Such a subgroup U has finite index in G since G is compact; hence its conjugates gUg^{-1} ($g \in G$) are finite in number and their intersection V is both normal and open in G. Such V's are thus a base of neighbourhoods of 1; the map $G \to \varprojlim G/V$ is injective, continuous, and its image is dense; a compactness argument then shows that it is an isomorphism. Hence G is profinite.

The profinite groups form a category (the morphisms being continuous homomorphisms) in which infinite products and projective limits exist.

Examples.

1) Let L/K be a Galois extension of commutative fields. The Galois group $\mathrm{Gal}(L/K)$ of this extension is, by construction, the projective limit of the Galois groups $\mathrm{Gal}(L_i/K)$ of the finite Galois extensions L_i/K which are contained in L/K; thus it is a profinite group.

2) A compact analytic group over the p-adic field $\mathbf{Q}_p$ is profinite, when viewed as a topological group. In particular, $\mathbf{SL}_n(\mathbf{Z}_p), \mathbf{Sp}_{2n}(\mathbf{Z}_p), \ldots$ are profinite groups.

3) Let G be a discrete topological group, and let $\hat{G}$ be the projective limit of the finite quotients of G. The group $\hat{G}$ is called the profinite group *associated to* G; it is the separated completion of G for the topology defined by the subgroups of G which are of finite index; the kernel of $G \to \hat{G}$ is the intersection of all subgroups of finite index in G.

4) If M is a torsion abelian group, its dual $M^* = \mathrm{Hom}(M, \mathbf{Q}/\mathbf{Z})$, given the topology of pointwise convergence, is a commutative profinite group. Thus one obtains the anti-equivalence (Pontryagin duality):

$$\text{torsion abelian groups} \iff \text{commutative profinite groups}$$

Exercises.

1) Show that a torsion-free commutative profinite group is isomorphic to a product (in general, an infinite one) of the groups $\mathbf{Z}_p$. [Use Pontryagin duality to reduce this to the theorem which says that every divisible abelian group is a direct sum of groups isomorphic to $\mathbf{Q}$ or to some $\mathbf{Q}_p/\mathbf{Z}_p$, cf. Bourbaki A VII.53, Exerc. 3.]

2) Let $G = \mathbf{SL}_n(\mathbf{Z})$, and let f be the canonical homomorphism

$$\hat{G} \longrightarrow \prod_p \mathbf{SL}_n(\mathbf{Z}_p).$$

(a) Show that f is surjective.

(b) Show the equivalence of the following two properties:

(b_1) f is an isomorphism;

(b_2) Each subgroup of finite index in $\mathbf{SL}_n(\mathbf{Z})$ is a congruence subgroup.

[These properties are known to be true for $n \neq 2$ and false for $n = 2$.]

1.2 Subgroups

Every closed subgroup H of a profinite group G is profinite. Moreover, the homogeneous space G/H is compact and totally disconnected.

Proposition 1. *If H and K are two closed subgroups of the profinite group G, with $H \supset K$, there exists a continuous section $s : G/H \to G/K$.*

(By "section" one means a map $s : G/H \to G/K$ whose composition with the projection $G/K \to G/H$ is the identity.)

We use two lemmas:

Lemma 1. *Let G be a compact group G, and let (S_i) be a decreasing filtration of G by closed subgroups. Let $S = \bigcap S_i$. The canonical map*

$$G/S \longrightarrow \varprojlim G/S_i$$

is a homeomorphism.

Indeed, this map is injective, and its image is dense; since the source space is compact, the lemma follows. (One could also invoke Bourbaki, TG III.59, cor. 3 to prop. 1.)

Lemma 2. *Proposition 1 holds if H/K is finite. If, moreover, H and K are normal in G, the extension*

$$1 \longrightarrow H/K \longrightarrow G/K \longrightarrow G/H \longrightarrow 1$$

splits (cf. §3.4) *over an open subgroup of G/H.*

Let U be an open normal subgroup of G such that $U \cap H \subset K$. The restriction of the projection $G/K \to G/H$ to the image of U is injective (and is a homomorphism whenever H and K are normal). Its inverse map is therefore a section over the image of U (which is open); one extends it to a section over the whole of G/H by translation.

Let us now prove prop. 1. One may assume $K = 1$. Let X be the set of pairs (S, s), where S is a closed subgroup of H and s is a continuous section $G/H \to G/S$. One gives X an ordering by saying that $(S, s) \geq (S', s')$ if $S \subset S'$ and if s' is the composition of s and $G/S \to G/S'$. If (S_i, s_i) is a totally ordered family of elements of X, and if $S = \bigcap S_i$, one has $G/S = \varprojlim G/S_i$ by Lemma 1; the s_i thus define a continuous section $s : G/H \to G/S$; one has $(S, s) \in X$. This shows that X is an inductively ordered set. By Zorn's Lemma, X contains a maximal element (S, s). Let us show that $S = 1$, which will complete the proof. If S were distinct from 1, then there would exist an open subgroup U of G such that $S \cap U \neq S$. Applying Lemma 2 to the triplet $(G, S, S \cap U)$, one would get a continuous section $G/S \to G/(S \cap U)$, and composing this with $s : G/H \to G/S$, would give a continuous section $G/H \to G/(S \cap U)$, in contradiction to the fact that (S, s) is maximal.

Exercises.

1) Let G be a profinite group acting continuously on a totally disconnected compact space X. Assume that G acts freely, i.e., that the stabilizer of each element of X is equal to 1. Show that there is a continuous section $X/G \to X$. [same proof as for prop. 1.]

2) Let H be a closed subgroup of a profinite group G. Show that there exists a closed subgroup G' of G such that $G = H \cdot G'$, which is minimal for this property.

1.3 Indices

A *supernatural number* is a formal product $\prod p^{n_p}$, where p runs over the set of prime numbers, and where n_p is an integer ≥ 0 or $+\infty$. One defines the product in the obvious way, and also the gcd and lcm of any family of supernatural numbers.

Let G be a profinite group, and let H be a closed subgroup of G. The *index* $(G : H)$ of H in G is defined as the lcm of the indices $(G/U : H/(H \cap U))$, where U runs over the set of open normal subgroups of G. It is also the lcm of the indices $(G : V)$ for open V containing H.

Proposition 2. (i) *If $K \subset H \subset G$ are profinite groups, one has*

$$(G : K) = (G : H) \cdot (H : K) .$$

(ii) *If (H_i) is a decreasing filtration of closed subgroups of G, and if $H = \bigcap H_i$, one has $(G : H) = \operatorname{lcm} (G : H_i)$.*

(iii) *In order that H be open in G, it is necessary and sufficient that $(G : H)$ be a natural number* (i.e., an element of $\mathbf{N}$).

Let us show (i): if U is an open normal subgroup of G, set $G_U = G/U$, $H_U = H/(H \cap U)$, $K_U = K/(K \cap U)$. One has $G_U \supset H_U \supset K_U$, from which

$$(G_U : K_U) = (G_U : H_U) \cdot (H_U : K_U) .$$

By definition, $\mathrm{lcm}(G_U : K_U) = (G : K)$ and $\mathrm{lcm}(G_U : H_U) = (G : H)$. On the other hand, the $H \cap U$ are cofinal with the set of normal open subgroups of H; it follows that $\mathrm{lcm}(H_U : K_U) = (H : K)$, and from this follows (i).

The other two assertions (ii) and (iii) are obvious.

Note that, in particular, one may speak of the *order* $(G : 1)$ of a profinite group G.

Exercises.

1) Let G be a profinite group, and let n be an integer $\neq 0$. Show the equivalence of the following properties:

(a) n is prime to the order of G.

(b) The map $x \mapsto x^n$ of G to G is surjective.

(b') The map $x \mapsto x^n$ of G to G is bijective.

2) Let G be a profinite group. Show the equivalence of the three following properties:

(a) The topology of G is metrisable.

(b) One has $G = \varprojlim G_n$, where the G_n $(n \geq 1)$ are finite and the homomorphisms $G_{n+1} \to G_n$ are surjective.

(c) The set of open subgroups of G is denumerable.

Show that these properties imply:

(d) There exists a denumerable dense subset of G.

Construct an example where (d) holds, but not (a), (b) or (c) [take for G the bidual of a vector space over $\mathbf{F}_p$ with denumerably infinite dimension].

3) Let H be a closed subgroup of a profinite group G. Assume $H \neq G$. Show that there exists $x \in G$ so that no conjugate of x belongs to H [reduce to the case where G is finite].

4) Let g be an element of a profinite group G, and let $C_g = \overline{\langle g \rangle}$ be the smallest closed subgroup of G containing g. Let $\prod p^{n_p}$ be the order of C_g, and let I be the set of p such that $n_p = \infty$. Show that:

$$C_g \simeq \prod_{p \in I} \mathbf{Z}_p \times \prod_{p \notin I} \mathbf{Z}/p^{n_p}\mathbf{Z}.$$

1.4 Pro-p-groups and Sylow p-subgroups

Let p be a prime number. A profinite group H is called a pro-p-group if it is a projective limit of p-groups, or, which amounts to the same thing, if its order is a power of p (finite or infinite, of course). If G is a profinite group, a subgroup H of G is called a Sylow p-subgroup of G if it is a pro-p-group and if $(G : H)$ is prime to p.

Proposition 3. *Every profinite group G has Sylow p-subgroups, and these are conjugate.*

One uses the following lemma (Bourbaki, TG I.64, prop. 8):

Lemma 3. *A projective limit of non-empty finite sets is not empty.*

Let X be the family of open normal subgroups of G. If $U \in X$, let $P(U)$ be the set of Sylow p-subgroups in the finite group G/U. By applying Lemma 3 to the projective system of all $P(U)$, one obtains a coherent family H_U of Sylow p-subgroups in G/U, and one can easily see that $H = \varprojlim H_U$ is a Sylow p-subgroup in G, whence the first part of the proposition. In the same way, if H and H' are two Sylow p-subgroups in G, let $Q(U)$ be the set of $x \in G/U$ which conjugate the image of H into that of H'; by applying Lemma 3 to the $Q(U)$, one sees that $\varprojlim Q(U) \neq \emptyset$, whence there exists an $x \in G$ such that $xHx^{-1} = H'$.

One may show by the same sort of arguments:

Proposition 4. (a) *Every pro-p-subgroup is contained in a Sylow p-subgroup of G.*

(b) *If $G \to G'$ is a surjective morphism, then the image of a Sylow p-subgroup of G is a Sylow p-subgroup of G'.*

Examples.

1) The group $\widehat{\mathbf{Z}}$ has the group $\mathbf{Z}_p$ of p-adic integers as a Sylow p-subgroup.

2) If G is a compact p-adic analytic group, the Sylow p-subgroups of G are open (this follows from the well-known local structure of these groups). The order of G is thus the product of an ordinary integer by a power of p.

3) Let G be discrete group. The projective limit of the quotients of G which are p-groups is a pro-p-group, denoted by $\widehat{G}_p$, which is called the *p-completion* of G; it is the largest quotient of $\widehat{G}$ which is a pro-p-group.

Exercise.

Let G be a discrete group such that $G^{\mathrm{ab}} = G/(G,G)$ is isomorphic to $\mathbf{Z}$ (for example the fundamental group of the complement of a knot in $\mathbf{R}^3$). Show that the p-completion of G is isomorphic to $\mathbf{Z}_p$.

1.5 Pro-p-groups

Let I be a set, and let $L(I)$ be the free discrete group generated by the elements x_i indexed by I. Let X be the family of normal subgroups M of $L(I)$ such that:

a) $L(I)/M$ is a finite p-group,
b) M contains almost all the x_i (i.e., all but a finite number).

Set $F(I) = \varprojlim L(I)/M$. The group $F(I)$ is a pro-p-group which one calls the *free pro-p-group* generated by the x_i. The adjective "free" is justified by the following result:

Proposition 5. *If G is a pro-p-group, the morphisms of $F(I)$ into G are in bijective correspondence with the families $(g_i)_{i\in I}$ of elements of G which tend to zero along the filter made up of the complements of finite subsets.*
[When I is finite, the condition $\lim g_i = 1$ should be dropped; anyway, then the complements of finite subsets don't form a filter ...]

More precisely, one associates to the morphism $f : F(I) \to G(I)$ the family $(g_i) = (f(x_i))$. The fact that the correspondence obtained in this way is bijective is clear.

Remark.
Along with $F(I)$ one may define the group $F_s(I)$ which is the projective limit of the $L(I)/M$ for those M just satisfying a). This is the p-completion of $L(I)$; the morphisms of $F_s(I)$ into a pro-p-group are in one-to-one correspondence with *arbitrary* families $(g_i)_{i\in I}$ of elements of G. We shall see in §4.2 that $F_s(I)$ is *free*, i.e., isomorphic to $F(J)$ for a suitable J.

When $I = [1, n]$ one writes $F(n)$ instead of $F(I)$; the group $F(n)$ is the *free pro-p-group of rank n*. One has $F(0) = \{1\}$, and $F(1)$ is isomorphic to the additive group $\mathbf{Z}_p$. Here is an explicit description of the group $F(n)$:

Let $A(n)$ be the algebra of associative (but not necessarily commutative) formal series in n unknowns $t_1, \ldots, t_n$, with coefficients in $\mathbf{Z}_p$ (this is what Lazard calls the "Magnus algebra"). [The reader who does not like "not necessarily commutative" formal power series may define $A(n)$ as the completion of the tensor algebra of the $\mathbf{Z}_p$-module $(\mathbf{Z}_p)^n$.] With the topology of coefficient-wise convergence, $A(n)$ is a compact topological ring. Let U be the multiplicative group of the elements in A with constant term 1. One may easily verify that it is a pro-p-group. Since U contains the elements $1 + t_i$ prop. 5 shows that there exists a morphism, $\theta : F(n) \to U$, which maps x_i to the element $1 + t_i$ for every i.

Proposition 6. (Lazard) *The morphism $\theta : F(n) \to U$ is injective.*

[One may hence identify $F(n)$ with the closed subgroup of U generated by the $1 + t_i$.]

One can prove a stronger result. To formulate it, define the $\mathbf{Z}_p$-*algebra* of a pro-p-group G as the projective limit of the algebras of finite quotients of G, with coeffients in $\mathbf{Z}_p$; this algebra will be denoted $\mathbf{Z}_p[[G]]$. One has:

Proposition 7. *There is a continuous isomorphism α from $\mathbf{Z}_p[[F(n)]]$ onto $A(n)$ which maps x_i to $1 + t_i$.*

The existence of the morphism $\alpha : \mathbf{Z}_p[[F(n)]] \to A(n)$ is easy to see. On the other hand, let I be the augmentation ideal of $\mathbf{Z}_p[[F(n)]]$; the elementary properties of p-groups show that the powers of I tend to 0. Since the $x_i - 1$ belong to I, one deduces that there is a continuous homomorphism

$$\beta : A(n) \longrightarrow \mathbf{Z}_p[[F(n)]]$$

which maps t_i onto $x_i - 1$. One then has to check $\alpha \circ \beta = 1$ and $\beta \circ \alpha = 1$, which is obvious.

Remarks.

1) When $n = 1$, prop. 7 shows that the $\mathbf{Z}_p$-algebra of the group $\Gamma = \mathbf{Z}_p$ is isomorphic to the algebra $\mathbf{Z}_p[[T]]$, which is a regular local ring of dimension 2. This can be used to recover the Iwasawa theory of "Γ-modules" (cf. [143], and also Bourbaki AC VII, §4).

2) In Lazard's thesis [101] one finds a detailed study of $F(n)$ based on prop. 6 and 7. For example, if one filters $A(n)$ by powers of the augmentation ideal I, the filtration induced on $F(n)$ is that of the descending central series, and the associated graded algebra is the free Lie $\mathbf{Z}_p$-algebra generated by the classes T_i corresponding to the t_i. The filtration defined by the powers of (p, I) is also interesting.