Preface

These notes are based on a course given by Prof. J. Neukirch at Queen's University during the academic year 1968–69. I want to express my deep thanks to him for providing me with the opportunity of working on these beautiful questions.

In the first four chapters we have attemted to give a rather detailed introduction to the theory of profinite groups and their cohomology. With a few exceptions, e.g. some examples of §8 of Ch. I, the presentation is essentially self-contained. We simply assume that the reader is familiar with some of the basic notions of Algebra and Topology, and some terminology from Homological Algebra.

In Chapter V we present some applications of the cohomological technique to the study of field extensions. Here we have used several results whose proofs are outside the scope of these notes.

We should like to express our gratitude to Prof. N. Sankaran for many useful conversations, and to Mr. A. Simis for his careful job in proofreadings. We also thank Mrs. E. M. Wight for her patience and skill in typing these notes.

Contents

p. 1

CHAPTER I
PROFINITE GROUPS

§1. Infinite Galois extensions.

Let K be a field and N a Galois extension of K (i.e. algebraic, normal and separable). Let

$$G = G_{N|K} = \{\sigma \in \mathrm{Aut}(N) |\ \sigma|_K = \mathrm{id}_K\}$$

be the Galois group of this extension. Denote by $\{N : K\}$ and $\{G : 1\}$ the lattices of intermediate fields L, $K \subseteq L \subseteq N$, and subgroups $H \subseteq G$, respectively.

The main theorem of Galois theory for finite extensions can be stated then as follows.

THEOREM 1.1: *Let $N|K$ be a finite Galois extension. Then*

(i) $[N : K] = \#G_{N|K}$;

(ii) *The maps*

$$\{N : K\} \underset{\Psi}{\overset{\Phi}{\rightleftarrows}} \{G : 1\}$$

defined by

$$\Phi(L) = \{\sigma \in G_{N|K} |\ \sigma|_L = \mathrm{id}_L\} = G_{N|L},$$

$$\Psi(H) = \{x \in N |\ Hx = x\},$$

p. 2

$$(K \subseteq L \subseteq N;\ H \subseteq G),$$

are inverse lattice anti-isomorphisms;

(iii) *If $L \in \{N : K\}$ and $\Phi(L) = G_{N|L}$, then L is normal over K iff $G_{N|L}$ is a normal subgroup of G, in which case $G_{L|K} \approx G_{N|K}/G_{N|L}$.*

Let us assume now that the Galois extension $N|K$ is not necessarily finite. The maps Φ and Ψ can still be defined as above and it is clear that they are lattice anti-homomorphisms. Moreover one has the following

PROPOSITION 1.2: $\Psi \circ \Phi = \mathrm{id}_{\{N:K\}}$.

Proof: If $K \subseteq L \subseteq N$ one certainly has

$$\Psi(\Phi(L)) = \Psi(G_{N|L}) = \{x \in N |\ G_{N|L}x = x\} \supset L.$$

p. 3 On the other hand, if $x \in N$ and $G_{N|L}x = x$, then x is the only conjugate of x, i.e. $x \in L$. ∎

COROLLARY 1.3: *Φ is injective and Ψ is surjective.*

However in the general case Φ and Ψ are not anti-isomorphisms; in other words in the infinite case it could happen that different subgroups of $G_{N|K}$ have the same fixed field, as the following example shows.

Example: Let $K = \mathbb{F}_p$ be the finite field with p elements. Let $\ell \neq 2$ be a prime number, and consider the sequence

$$K = K_0 \subset K_0 \subset \cdots,$$

where K_i is the unique extension of K of degree $[K_i : K] = \ell^i$. Let

$$N = \bigcup_{i=1}^{\infty} K_i;$$

then

$$K_i = \{x \in N |\ x^{p^{\ell^i}} - x = 0\}.$$

p. 4 Let $G = G_{N|K}$. Consider the Frobenius K-automorphism $\varphi: N \longrightarrow N$ defined by

$$\varphi(x) = x^p.$$

Set

$$H = \{\varphi^n |\ n \in \mathbb{Z}\}.$$

We shall prove that (a) H and G have the same fixed field, i.e. $\Psi(G) = \Psi(H)$, and (b) $H \neq G$, establishing that Ψ is not injective.

For (a): It suffices to show that $\Psi(H) = K$. Let $x \in N$ with $Hx = x$; then $\varphi(x) = x$; so $x^p = x$; hence $x \in K$.

For (b): We construct a K-automorphism σ of N, which is not in H, in the following way. For each $i = 1, 2, \ldots$, let $k_i = 1 + \ell + \cdots + \ell^{i-1}$, and consider the K-automorphisms φ^{k_i} of N. Since

$$\varphi^{k_{i+1}}|_{K_i} = \varphi^{k_i}|_{K_i},$$

we can defined a K-automorphism

p. 5
$$\sigma\colon N \longrightarrow N$$

by setting

$$\sigma(x) = \varphi^{k_i}(x), \qquad \text{when } x \in K_i.$$

Now, if $\sigma \in H$, say $\sigma = \varphi^n$ we would have for each $i = 1, 2, \ldots,$

$$\sigma|_{K_i} = \varphi^n|_{K_i} = \varphi^{k_i}|_{K_i},$$

and hence

$$n \equiv k_i \pmod{\ell^i}$$

for each i, since $G_{K_i|K}$ is the cyclic group generated by $\varphi|_{K_i}$. Multiplying this by $(\ell-1)$ we would obtain $(\ell-1)n \equiv 1 \pmod{\ell^i}$, for each i, which is impossible if $\ell \neq 2$.

Remark: The key idea in the above example is the following: as we will see later (see ex. (4) on p. 26) the Galois group $G_N = G_{N|\mathbb{F}_p}$ is isomorphic to the additive group $\mathbb{Z}_\ell$ of the ℓ-adic integers. The Frobenius automorphism φ corresponds to $1 \in \mathbb{Z}_\ell$, so that the
p. 6 group H is carried onto $\mathbb{Z} \subseteq \mathbb{Z}_\ell$. The elements of G which are not in H correspond to the ℓ-adic integers which are not in $\mathbb{Z}$ (for instance, in our case $\sigma = 1+\ell+\ell^2+\ell^3+\cdots$).

Although the above example shows that Theorem 1.1 does not hold for infinite Galois extension, it suggest a way of modifying the theorem so that it will in fact be valid even in those cases. The map σ of the example is in a sense approximated by the maps φ^{k_i}, since it coincides with φ^{k_i} on the subextension K_i which becomes larger and larger with increasing i, and $N = \bigcup_{i=1}^{\infty} K_i$. This leads to the idea of defining a topology in G so that in fact $\sigma = \lim \varphi^{k_i}$. Then σ would be in the closure of H and once could hope that $G = \mathrm{cl}(H)$, suggesting a correspondence of the intermediate fields of $N|K$ and the closed subgroups of G. In fact this is the case as we will see.

Definition 1.4: Let $N|K$ be a Galois extension and $G = G_{N|K}$. The set

$$\underline{S} = \{G_{N|L} |\ L|K \text{ finite, normal extension, } L \in \{N : K\}\}$$

p. 7 determines a basis of open neighborhoods of $1 \in G$. The topology defined by $\underline{S}$ is called the *Krull topology* of G.

Remarks: 1) If $N|K$ is a finite Galois extension, the the Krull topology of $G_{N|K}$ is the discrete topology.

2) Let $\tau, \sigma \in G_{N|K}$. Then $\tau \in \sigma G_{N|L} \Leftrightarrow \sigma^{-1}\tau \in G_{N|L} \Leftrightarrow \sigma|_L = \tau|_L$, i.e., two elements of $G_{N|K}$ "are near" if they coincide on a large field L.

PROPOSITION 1.5: *Let $N|K$ be a Galois extension and let $G = G_{N|K}$. Then G endowed with the Krull topology is a*

(i) *Hausdorff,*

(ii) *compact,*

(iii) *totally disconnected*

topological group

Proof: For (i): Let $\underline{F}_n$ denote the set of all finite, normal subextension $L|K$ of $N|K$. We have

$$\bigcap_{U \in \underline{S}} U = \bigcap_{L|K \in \underline{F}_n} G_{N|L} = 1,$$

since

$$N = \bigcup_{L|K \in \underline{F}_n} L.$$

p. 8

Then, $\sigma, \tau \in G$, $\sigma \neq \tau \Rightarrow \sigma^{-1}\tau \neq 1 \Rightarrow \exists U_0 \in \underline{S}$ such that $\sigma^{-1}\tau \notin U_0 \Rightarrow \tau \notin \sigma U_0 \Rightarrow \tau U_0 \cap \sigma U_0 = \emptyset$.

For (ii): Consider the homomorphism

$$h: G \longrightarrow \prod_{L|K \in \underline{F}_n} G_{L|K} = P,$$

defined by

$$h(\sigma) = \prod_{L|K \in \underline{F}_n} \sigma|_L.$$

(Notice that P is compact since every $G_{L|K}$ is a discrete finite group.)

We shall show that h is an injective continuous mapping, that $h(G)$ is closed in P and that h is an open map into $h(G)$. This will prove that G is a homeomorphic to the compact space $h(G)$.

Let $\sigma \in G$ with $h(\sigma) = 1$; then $\sigma|_L = 1$, since $N = \bigcup_{L|K \in \underline{F}_n} L$. Thus h is injective.

To see that h is continuous consider the composition

p. 9
$$G \longrightarrow P \xrightarrow{g_{L|K}} G_{L|K}$$

where $g_{L|K}$ is the canonical projection. It suffices to show that each $g_{L|K}h$ is continuous; but this is clear since

$$(g_{L|K}h)^{-1}(\{1\}) = G_{N|L} \in \underline{S}.$$

To prove that $h(G)$ is closed consider the sets $M_{L_1|L_2} = \{\prod \sigma_L \in P |\ \sigma_{L_1}|_{L_2} = \sigma_{L_2}\}$ defined for each pair $L_1|K, L_2|K \in \underline{F}_n$ with $N \supseteq L_1 \supseteq L_2 \supseteq K$. Notice that $M_{L_1|L_2}$ is closed in P since it is a finite union of closed subsets, namely, if $G_{L_2|K} = \{f_1, f_2, \ldots, f_r\}$ and S_i is the set of extensions of f_i to L_1, then

$$M_{L_1|L_2} = \bigcup_{i=1}^{r} \Big(\prod_{\substack{L \neq L_1, L_2 \\ L|K \in \underline{F}_n}} G_{L|K} \times S_i \times \{f_i\} \Big).$$

On the other hand

$$h(G) \subseteq \bigcap_{L_1 \supseteq L_2} M_{L_1|L_2};$$

and if

p. 10
$$\prod_{L|K \in \underline{F}_n} \sigma_L \in \bigcap_{L_1 \supseteq L_2} M_{L_1|L_2}$$

we can define a K-automorphism $\sigma\colon N \longrightarrow N$ by $\sigma(x) = \sigma_L(x)$ if $x \in L$; so that $h(\sigma) = \prod_{L|K \in \underline{F}_n} \sigma_L$. I.e.,

$$h(G) = \bigcap_{L_1 \supseteq L_2} M_{L_1|L_2},$$

and hence $h(G)$ is closed.

Finally h is open into $h(G)$, since if $L|K \in \underline{F}_n$,

$$h(G_{N|L}) = h(G) \cap \Big(\prod_{\substack{L' \neq L \\ L'|K \in \underline{F}_n}} G_{L'|K} \times \{1\} \Big)$$

which is open in $h(G)$.

For (iii): It is enough to prove that the connected component H of 1 is $\{1\}$. For each $U \in \underline{S}$ let $U_H = U \cap H$; then $U_H \neq \emptyset$ and it is open in H.

Let

$$V_H = \bigcup_{\substack{x \in H \\ x \notin U_H}} xU_H;$$

then V_H is open in H, $U_H \cap V_H = \emptyset$ and $H = U_H \cup V_H$. Hence $V_H = \emptyset$; i.e., $U \cap H = H$ for each $U \in \underline{S}$. Therefore

$$H \subseteq \bigcap_{U \in \underline{S}} U = \{1\},$$

p. 11

so $H = \{1\}$. ∎

PROPOSITION 1.6: *Let $N|K$ be a Galois extension. The open subgroups of $G = G_{N|K}$ are just the groups $G_{N|L}$, where $L|K$ is a finite subextension of $N|K$. The closed subgroups are precisely the intersections of open subgroups.*

Proof: Let $L|K$ be a finite subextension of $N|K$. Choose a finite normal extension $\tilde{L}$ of K such that $N \supseteq \tilde{L} \supseteq L \supseteq K$. Then

$$G_{N|\tilde{L}} \subseteq G_{N|L} \subseteq G;$$

so

$$G_{N|L} = \bigcup_{\sigma \in G_{N|L}} \sigma G_{N|\tilde{L}};$$

i.e., $G_{N|L}$ is the union of open sets and thus open. Conversely, let H be an open subgroup of G; then $\exists$ a finite normal extension $\tilde{L}$ with

p. 12

$$G_{N|\tilde{L}} \subseteq H \subseteq G.$$

Consider the epimorphism

$$G \longrightarrow G_{\tilde{L}|K}$$

defined by restriction. Its kernel is $G_{N|\tilde{L}}$. The image of H under this map must be of the form $G_{\tilde{L}|L}$, for some field L with $\tilde{L} \supseteq L \supseteq K$, since $G_{\tilde{L}|K}$ is the Galois group of a finite Galois extension. Thus

$$H = \{\sigma \in G |\ \sigma|_L = \mathrm{id}_L\} = G_{N|L}.$$

Since open subgroups are closed so is their intersection. Conversely, suppose H is a closed subgroup of G; clearly

$$H \subseteq \bigcap_{U \in \underline{S}} H \cdot U.$$

On the other hand, let $\sigma \in \bigcap_{U \in \underline{S}} H \cdot U$; then $U \in \underline{S} \Rightarrow \sigma U \cap H \neq \emptyset$; so every neighborhood of σ hits H; hence $\sigma \in H$. Thus H is the intersection of the open subgroups $H \cdot U$, $U \in \underline{S}$. ∎

p. 13 We are now in a position to generalize Theorem 1.1 to infinite Galois extensions.

THEOREM 1.7 (Krull): *Let $N|K$ be a (finite or infinite) Galois extension and let $G = G_{N|K}$. Let $\{N : K\}$ be the lattice of intermediate fields $N \supseteq L \supseteq K$, and let $\{G : 1\}$ be the lattice of closed subgroups of G. If $L \in \{N : K\}$ define*

$$\Phi(L) = \{\sigma \in G |\ \sigma|_L = \mathrm{id}_L\} = G_{N|L}.$$

Then Φ is a lattice anti-isomorphism of $\{N : K\}$ to $\{G : 1\}$. Moreover $L \in \{N : K\}$ is a normal extension of K iff $\Phi(L)$ is a normal subgroup of G; and if this is the case $G_{L|K} \approx G/\Phi(L)$.

Proof: Since $\Phi(L) = G_{N|L}$ is compact (Prop. 1.5), it is closed in G; so Φ is in fact a map into $\{G : 1\}$. Define

$$\Psi\colon \{G : 1\} \longrightarrow \{N : K\}$$

by

$$\Psi(H) = \{x \in N |\ Hx = x\}.$$

p. 14 Clearly Proposition 1.2 is still valid and we have $\Psi \circ \Phi = \mathrm{id}_{\{N:K\}}$. Now we prove that $\Phi \circ \Psi = \mathrm{id}_{\{G:1\}}$. If $L|K$ is finite,

$$\Phi(\Psi(G_{N|L})) = \Phi(\Psi(\Phi(L))) = G_{N|L}.$$

If $H \in \{G : 1\}$, then, by Proposition 1.6,

$$H = \bigcap G_{N|L},$$

the intersection running through a collection of extensions $N|L$ with $L|K$ finite. Then

$$\Phi(\Psi(H)) = \Phi(\Psi(\bigcap G_{N|L})) =$$
$$\Phi(\bigcup \Psi(G_{N|L})) = \bigcap \Phi(\Psi(G_{N|L})) =$$
$$\bigcap G_{N|L} = H.$$

Assume that L is a normal extension of K, and let $H = \Phi(L)$. Then $\sigma L = L$, $\forall \sigma \in G$; but since $\sigma L = \Psi(\sigma H \sigma^{-1})$, this is equivalent to saying that $\sigma H \sigma^{-1} = H$, $\forall \sigma$, i.e., that H is normal in G. Conversely, suppose that H is an invariant subgroup of G, and let $\Psi(H) = L$. So $\sigma L = L$, $\forall \sigma \in G$, i.e., L is the fixed field of the group of
p. 15 restrictions of the $\sigma \in G$ to L. Thus $L|K$ is Galois and hence normal ([B_2] §10, Prop. 1). Finally, since every K-automorphism of L can be extended to a K-automorphism of N (cf. [B_2] §6, Prop. 7), the homomorphism

$$G \longrightarrow G_{L|K},$$

given by restriction, is onto. The kernel of this homomorphism is $\Phi(L)$; thus $G_{L|K} \approx G/\Phi(L)$. ∎

p. 16 §**2. Profinite groups.**

The groups which occur as Galois groups of field extensions belong to a class of topological groups, the so-called profinite groups. They can be defined in the following abstract way:

Definition 2.1: A *profinite group* is a Hausdorff, compact, totally disconnected topological group.

By Proposition 1.5 every Galois group with the Krull topology is a profinite group. It may be mentioned that, conversely, every profinite group is representable as a Galois group of some field extension.

THEOREM 2.2: *The profinite groups are precisely the projective limits of projective systems (over directed sets) of finite groups.*

In the proof of this theorem we will need the following lemmas.

p. 17 LEMMA 2.3: *Let X be a compact, Hausdorff space. Let $x \in X$ and let $\{U_q |\ q \in Q\}$ be the family of all compact open sets containing x. Then*

$$A = \bigcap_{q \in Q} U_q$$

is connected.

Proof: Assume $A = U \cup V$, $U \cap V = \emptyset$ with both U and V closed. Since X is normal $\exists$ open sets U', V' such that $U' \supseteq U$, $V' \supseteq V$ and $U' \cap V' = \emptyset$. So

$$[X \setminus (U' \cup V')] \cap A = \emptyset.$$

Since $X \setminus (U' \cup V')$ is compact $\exists$ a finite subfamily $Q' \subseteq Q$ such that

$$[X \setminus (U' \cup V')] \cap (\bigcap_{q \in Q'} U_q) = \emptyset.$$

Let $b = \bigcap_{q \in Q'} U_q$. Then B is open and compact, $x \in B$ and $B = (B \cap U') \cup (B \cap V')$. Say $x \in B \cap U'$. Since $B \cap U'$ is open and compact

$$A \subseteq B \cap U' \subseteq U'.$$

p. 18 Hence $A \cap V \subseteq A \cap V' = \emptyset$. Thus $V = \emptyset$. ∎

LEMMA 2.4: *Let G be a compact, Hausdorff, totally disconnected topological group. Then every neighborhood of 1 contains an open normal subgroup. Moreover this subgroup has finite index in G.*

Proof: By the above lemma $\{1\} = \bigcap_{q \in Q} U_q$ where $\{U_q |\ q \in Q\}$ is the family of all compact open neighborhoods of 1. Let U be an open neighborhood of 1. Then $G \setminus U$ is compact and

$$(G \setminus U) \cap (\bigcap_{q \in Q} U_q) = \emptyset.$$

Hence $\exists$ a finite subset $Q' \subseteq Q$ such that

$$(G \setminus U) \cap (\bigcap_{q \in Q'} U_q) = \emptyset.$$

Let $A = \bigcap_{q\in Q} U_q$. Then A is compact open neighborhood of 1 and $A \subseteq U$.

Let $F = (G \setminus U) \cap A^2$. Since A is compact, so is A^2; hence F is closed. Let V be

p. 19 a symmetric open neighborhood of 1 such that

$$AV \cap F = \emptyset \qquad \text{and} \qquad V \subseteq A.$$

Therefore, since $AV \subseteq A^2$, one has $AV \cap (G \setminus A) = \emptyset$, i.e. $AV \subseteq A$. Hence

$$AV^n \subseteq A, \quad \forall n.$$

Hence $K = \bigcup_n V^n \subseteq A$ is an open subgroup contained in A. Since G is compact K has only a finite number of cosets in G, say, $G = \bigcup_{i=1}^r x_i K$. Let

$$H = \bigcap_{x\in G} xKx^{-1} = \bigcap_{i=1}^{r} x_i K x_i^{-1}.$$

It is clear that H is the desired open normal subgroup of finite index. ∎

LEMMA 2.5: *Let $\{X_i, h_{ij}\}$ be a projective system of topological spaces. Let X be a topological space and $h_i\colon X \longrightarrow X_i$ a set of compatible surjective maps. Then either $\varprojlim X_i$ is empty or the induced mapping*

$$h\colon X \longrightarrow \varprojlim X_i$$

p. 20 *sends X onto a dense subset of $\varprojlim X_i$.*

Proof: Consider a basic open set

$$V = (\varprojlim X_i) \cap \Big(\prod_{i\neq i_1,\ldots,i_n} X_1 \times U_1 \times \cdots \times U_n \Big)$$

of $\varprojlim X_i$, where U_j is a non-empty open subset of X_{i_j}. Let $i_0 > i_j$ $(j = 1, \ldots, n)$, and $\prod_i x_i = x \in V$; then $h_{i_0 i_j} x_{i_0} = x_{i_j}$ $(j = 1, \ldots, n)$. Choose $y \in X$ such that $h_{i_0} y = x_{i_0}$. Then $hy \in V$. ∎

Proof of Theorem 2.2: Let

$$G = \varprojlim_L G_L$$

where $\{G_L\}$ is a projective system of finite, discrete groups. Then

$$G \subseteq \prod_L G_L,$$

and the topology in G is induced by that of $\prod_L G_L$. Since each G_L is a Hausdorff,
p. 21 totally disconnected group, so is $\prod_L G_L$ (cf. [B3], §11, Prop. 10), and hence G. On the other hand G is closed in $\prod_L G_L$ (cf. [B3], §8. Cor. 2 to Prop. 7), and therefore compact. Thus G is profinite.

Conversely, suppose G is profinite. Consider the family

$$\underline{S} = \{U |\, U \text{ open, normal subgroup of } G\}.$$

By Lemma 2.4 $\underline{S}$ is a basis of open neighborhoods of $1 \in G$. For each pair $U, V \in \underline{S}$ with $U \subseteq V$, consider the natural map

$$\varphi_{U,V} : G/U \longrightarrow G/V.$$

It is plain that

$$\{G/U, \varphi_{U,V} |\, U, V \in \underline{S}\}$$

is a projective system of groups. Hence the compatible family of homomorphism

$$\varphi_U : G \longrightarrow G/U, \quad U \in \underline{S}.$$

defines a map

$$\varphi : G \longrightarrow \varprojlim_{\underline{S}} G/U \subseteq \prod_{\underline{S}} G/U.$$

p. 22

We will show that φ is a topological isomorphism:

(1) φ is injective: $\sigma \in G$, $\varphi(\sigma) = 1 \Rightarrow \sigma \in U$, $\forall U \in \underline{S} \Rightarrow \sigma \in \bigcap_{\underline{S}} U = \{1\}$.

(2) φ is continuous: it suffices to show that the composition

$$G \xrightarrow{\varphi} \varprojlim_{\underline{S}} G/U \subseteq \prod_{\underline{S}} G/U \xrightarrow{p_U} G/U$$

is continuous for each $U \in \underline{S}$. This is clear since

$$(p_u \varphi)^{-1}\{1\} = U$$

is open in G. (Notice that $\{1\}$ is a basis of open neighborhoods of 1 in G/U, for each $U \in \underline{S}$.)

(3) φ is surjective: by Lemma 2.5 $\varphi(G)$ is dense in $\varprojlim_{\underline{S}} G/U$; hence $\varphi(G) = \varprojlim_{\underline{S}} G/U$ since $\varphi(G)$ is closed.

p. 23 Since G is compact, (1), (2) and (3) imply that φ is a topological isomorphism. ∎

The above theorem gives a new way of looking at profinite groups. In fact profinite groups appear in most concrete situations as projective limits of finite groups. However we have preferred not to use this as a definition since a profinite group may be the limit of different projective systems.

PROPOSITION 2.6: *Let $G = \varprojlim_{I} G_i$ be a profinite group ($\{G_i |\ i \in I\}$ is a projective system of discrete finite groups). Then*

$$\underline{S} = \{\mathrm{Ker}(G \longrightarrow G_i) |\ i \in I\}$$

is a basis of open neighborhoods of $1 \in G$.

Proof: Since each G_i is finite $\{1\}$ is a basis of open neighborhoods of $1 \in G_i$. Hence
p. 24 the neighborhoods of $1 \in G$ of the form

$$\prod_{i \neq i_1, \ldots, i_n} G_i \times \{1\}_{i_1} \times \cdots \times \{1\}_{i_n} \cap G = \bigcap_{j = i_1, \ldots, i_n} \ker(G \longrightarrow G_j) \qquad (1)$$

form a basis of open neighborhoods of $1 \in G$. Let $i_0 > i_1, \ldots, i_n$; then

$$\ker(G \longrightarrow G_{i_0}) \subseteq \bigcap_{j = i_1, \ldots, i_n} \ker(G \longrightarrow G_j).$$

Thus $\underline{S}$ is a a basis of open neighborhoods of 1. ∎

Examples of profinite groups.: (1) Every Galois group $G_{N|K}$ of a Galois extension of fields $N|K$ is a profinite group. In fact $G_{N|K} = \varprojlim G_{N|K}/G_{N|L} = \varprojlim G_{L|K}$, where $L|K$ runs through the finite normal subextensions of $N|K$.

(2) The Prüfer group

$$\hat{\mathbb{Z}} = \varprojlim_m \mathbb{Z}/m\mathbb{Z},$$

p. 25 (if $m, n \in \mathbb{Z}$ define $m > n$,iff $n|m$; then $\mathbb{Z}/m\mathbb{Z} \longrightarrow \mathbb{Z}/n\mathbb{Z}$ is the natural projection), and moreover

$$\mathfrak{o} = \varprojlim_{\mathfrak{a}} \mathfrak{o}/\mathfrak{a},$$

where $\mathfrak{o}$ is the ring of algebraic integers of an algebraic number field and $\mathfrak{a}$ runs through the ideals of $\mathfrak{o}$, are profinite groups.

Notice that if $\mathbb{F}_p$ denotes the field with p elements and $\bar{\mathbb{F}}_p$ its algebraic closure, we have

$$G_{\mathbb{F}_p} = G_{\bar{\mathbb{F}}_p|\mathbb{F}_p} = \varprojlim G_{K_m|\mathbb{F}_p} \approx \varprojlim_m \mathbb{Z}/m\mathbb{Z} = \hat{\mathbb{Z}}$$

($[K_m : \mathbb{F}_p] = m$) where the isomorphism is induced by the natural isomorphisms of projective systems

$$\{G_{K_m|\mathbb{F}_p} |\ [K_m : \mathbb{F}_p] = m\} \longrightarrow \{\mathbb{Z}/m\mathbb{Z} |\ m \in \mathbb{Z}\}$$

given by

$$\varphi|_{K_m} \mapsto 1 + m\mathbb{Z}.$$

($\varphi: \bar{\mathbb{F}}_p \longrightarrow \bar{\mathbb{F}}_p$ is the Frobenius automorphism $\varphi x = x^p$.)

p. 26 (3) The multiplicative group U of the $\mathfrak{p}$-adic units of a $\mathfrak{p}$-adic number field is a profinite group. In fact one has

$$U \supseteq U^1 \supseteq U^2 \supseteq U^3 \supseteq \cdots$$
$$U^i = 1 + \mathfrak{p}^i,$$
$$U = \varprojlim_i U/U^i.$$

(4) The additive group of the $\mathfrak{p}$-adic integers

$$\mathbb{Z}_p = \varprojlim_n \mathbb{Z}/p^n\mathbb{Z}$$

(p is a prime number; if $n, m \in \mathbb{N}$ and $m \leq n$, define $\mathbb{Z}/p^n\mathbb{Z} \longrightarrow \mathbb{Z}/p^m\mathbb{Z}$ to be the natural projection), is a profinite group. More generally, the additive group of the ring of integers of a $\mathfrak{p}$-adic number field

$$\mathfrak{O}_\mathfrak{p} = \varprojlim_n \mathfrak{O}/\mathfrak{p}^n$$

($\mathfrak{O}$ denotes the ring of integers of an algebraic number field and $\mathfrak{p}$ a prime ideal), is a profinite group.

p. 27 An example of a Galois extension whose Galois group is $\mathbb{Z}_\ell$ can be constructed as follows. Let p and ℓ be prime numbers. Let $K = \mathbb{F}_p$ be the field with p elements, and let $N|K$ be defined as in the example on page 3. Then

$$G_{N|K} = \varprojlim_i G_{K_i|K} \approx \varprojlim_i \mathbb{Z}/\ell^i\mathbb{Z} = \mathbb{Z}_\ell,$$

(the isomorphism is induced, as in example (2), by isomorphisms $G_{K_i|K} \longrightarrow \mathbb{Z}/\ell^i\mathbb{Z}$ given by $\varphi|_{K_i} \mapsto 1 + \ell^i\mathbb{Z}$).

(5) Let A be and abelian torsion group considered as a discrete topological group. Its Pontrjagin dual

$$\chi(A) = \mathrm{Hom}(A, \mathbb{Q}/\mathbb{Z})$$

is a profinite group. For, one has

$$A = \varinjlim A_i,$$

where A_i runs through the finite subgroups of A, and therefore

$$\chi(A) = \varprojlim \chi(A_i)$$

with $\chi(A_i)$ finite.

p. 28 For instance $\chi(\mathbb{Q}/\mathbb{Z}) = \hat{\mathbb{Z}}$.

(6) Let $L|K$ be a normal extension of algebraic number fields. Then

$$N = \bigcup_{L|K} L$$

where $N \supseteq L \supseteq K$, $L|K$ finite, normal. To every L associate its ideal class group $\mathrm{CL}(L)$, and to every pair L, L' with $N \supseteq L' \supseteq L \supseteq K$ the norm map $\mathrm{N}_{L'|K}\colon \mathrm{CL}(L') \longrightarrow \mathrm{CL}(L)$. Then

$$I(N) = \varprojlim \mathrm{CL}(L)$$

is a profinite group. The group $G_{N|K}$ operates on $I(N)$ making it into a module, the Iwasawa module.

(7) Let G be any group, $\underline{S}$ the system of its normal subgroups of finite index. The profinite group $\hat{G}$ is defined by

$$\hat{G} = \varprojlim_{U \in \underline{S}} G/U$$

and it is called the profinite completion of G.

p. 29 §**3. Properties of profinite groups.**

PROPOSITION 3.1: *A closed subgroup H of a profinite group G is profinite. In fact if $G = \varprojlim_{\underline{S}} G/U$, with $\underline{S} =$ {open, normal subgroups of G}, then*

$$H \approx \varprojlim_{\underline{S}} HU/U \approx \varprojlim_{\underline{S}} H/H \cap U.$$

PROPOSITION 3.2: *A quotient group G/H of a profinite group G by a closed normal subgroup H, is profinite. In fact if $\underline{S} =$ {open, normal subgroups of G}, then*

$$G/H \approx \varprojlim_{\underline{S}} G/HU.$$

The above propositions follow easily from Lemma 2.5.

PROPOSITION 3.3: *If each G_i, $i \in I$ is a profinite group, so is $G = \prod_I G_i$.*

Proof: This is clear since G is Hausdorff, compact and totally disconnected. ∎

p. 30 COROLLARY 3.4: *If $\{G_i|\ , i \in I\}$ is a projective system of profinite groups, then*

$$G = \varprojlim_{I} G_i$$

is profinite.

Proof: By Cor. 2 to Prop. 7 in §8 of [B3], G is a closed subgroup of $\prod_I G_i$. Hence the result follows from Prop. 3.3. ∎

Example:

$$\hat{\mathbb{Z}} \approx \prod_p \mathbb{Z}_p$$

where p runs through the set of prime numbers (cf. example (2) and (4)). To see this consider the natural projection

$$\alpha_p^m \colon \mathbb{Z}_p \longrightarrow \mathbb{Z}/p^{m_p}\mathbb{Z},$$

p. 31 defined for each prime p and each natural number $m = \prod_p p^{m_p}$. Then

$$\alpha^m = \prod_p \alpha_p^m \colon \prod_p \mathbb{Z}_p \longrightarrow \prod_p \mathbb{Z}/p^{m_p}\mathbb{Z} \approx \mathbb{Z}/m\mathbb{Z}$$

is onto. So the maps α^m, $m \in \mathbb{Z}$ induce a continuous surjection

$$\alpha \colon \prod_p \mathbb{Z}_p \longrightarrow \hat{\mathbb{Z}} = \varprojlim_m \mathbb{Z}/m\mathbb{Z}$$

according to Lemma 2.5. On the other hand $(\prod x_p) \in \prod \mathbb{Z}_p$, with

$$\alpha(\prod x_p) = 0 \Rightarrow \alpha^m(\prod x_p) = 0,\ \forall m \Rightarrow \alpha_p^m(x_p) = 0,\ \forall p, m \Rightarrow x_p = 0,\ \forall p \Rightarrow x = 0.$$

I.e., α is injective. This suffices to show that α is a topological isomorphism since $\prod_p \mathbb{Z}_p$ is compact.

PROPOSITION 3.5: *Let $K \subseteq H \subseteq G$ be profinite groups. Then there exists a continuous section*

$$\sigma \colon G/H \longrightarrow G/K,$$

i.e., a continuous map σ of topological spaces of the left cosets such that if

$$\pi \colon G/K \longrightarrow G/H$$

p. 32 *is the canonical projection then $\pi\sigma$ is the identity.*

Proof: We divide the proof into two cases.

1) Assume that K has finite index in H. Then K is open in H, and therefore there exists an open normal subgroup U of G with $U \cap H \subseteq K$. Let $x_1, x_2, \ldots, x_n$ be representatives of the distinct cosets of UH in G. Then G/H is the disjoint union of the spaces x_iUH/H, $i = 1, 2, \ldots, n$. We will prove that the maps

$$\pi_i \colon x_iUK \longrightarrow x_iUH/H$$

$i = 1, 2, \ldots, n$, defined as restrictions of π, are homeomorphisms. Then it will follow that $\sigma = \bigcup_{i=1}^{n} \pi_i^{-1}$ will be the desired section. It is plain that π_i is a continuous surjection. On the other hand if $\pi_i(x_iu_1) = \pi_i(x_iu_2)$, $(u_1, u_2 \in U)$, then $x_iu_1u_2^{-1}x_i^{-1} \in H$. But since U is normal, $x_iu_1u_2^{-1}x_i^{-1} \in U$, and hence $x_iu_1u_2^{-1}x_i^{-1} \in H \cap U \subseteq K$. Thus x_iu_1 and x_iu_2 represent the same element in x_iUK, i.e., π is injective. Since x_iUK is
p. 33 compact, π must be a homeomorphism.

2) General case. Let $\underline{T}$ be the set of pairs (T, t) where T is a closed subgroup of H with $K \subseteq T \subseteq H$, and $t \colon G/H \longrightarrow G/T$ is a continuous section. Define a partial order in $\underline{T}$ by $(T, t) \geq (T', t') \Leftrightarrow T \subseteq T'$ and the diagram

$$\begin{array}{ccc} G/H & \xrightarrow{\ t\ } & G/T \\ & \searrow^{t'} & \downarrow p \\ & & G/T' \end{array}$$

commutes, where p is the canonical projection. Then $\underline{T}$ is inductively ordered. For assume $\{(T_\alpha, t_\alpha) |\ \alpha \in A\}$ is a totally ordered subset of $\underline{T}$, and let $T = \bigcap_{\alpha \in A} T_\alpha$. The projections $G/T \longrightarrow G/T_\alpha$ induce a surjective, continuous map (Lemma 2.5, and the fact that G/T is compact)

$$\varphi \colon G/T \longrightarrow \varprojlim_{\alpha} G/T_\alpha,$$

which is also injective, for

$$x, y \in G, \quad \varphi x = \varphi y \Rightarrow xT_\alpha = yT_\alpha, \quad \forall \alpha \in A \Rightarrow$$
$$x^{-1}y \in T_\alpha, \quad \forall \alpha \in A \Rightarrow x^{-1}y \in \bigcap_{\alpha} T_\alpha = T.$$

p. 34

Therefore φ is a homeomorphism, since G/T is compact. The sections t_α define a continuous map

$$t\colon G/H \longrightarrow G/T$$

which is easily seen to be a section. Moreover, we obviously have $(T,t) \geq (T_\alpha, t_\alpha)$, $\forall \alpha \in A$. Hence $\underline{T}$ is inductive. By Zorn's lemma there is a maximal element in $\underline{T}$, say $(\bar{T}, \bar{t})$. Then

$$K \subseteq \bar{T} \subseteq H \subseteq G.$$

We will show that $\bar{T}$ is contained in every open subgroup U containing K. This will imply $\bar{T} = K$. Consider an open subgroup $G \supseteq U \supseteq K$. Let $S = \bar{T} \cap U$; Then $S \subseteq \bar{T}$ and $(\bar{T} : S) < \infty$. Hence by part 1), there is a section

$$t'\colon G/\bar{T} \longrightarrow G/S,$$

p. 35 and clearly $(S, t' \circ \bar{t}) \in \underline{T}$ with $(S, t' \circ \bar{t}) \geq (\bar{T}, \bar{t})$. So $S = \bar{T}$, and thus $\bar{T} \subseteq U$. ∎

PROPOSITION 3.6: $\varprojlim$ *is an exact functor from the category of projective systems, over a (directed) indexing set I, of profinite groups to the category of profinite groups.*

Proof: Let

$$1 \longrightarrow \{H_i, \varphi_{ij}\} \xrightarrow{\{f_i\}} \{G_i, \psi_{ij}\} \xrightarrow{\{g_i\}} \{K_i, \eta_{ij}\} \longrightarrow 1$$

be an exact sequence of projective system (over I) of profinite groups. We will show that the corresponding sequence

$$1 \longrightarrow \varprojlim H_i \xrightarrow{f} \varprojlim G_i \xrightarrow{g} \varprojlim K_i \longrightarrow 1$$

is exact. All except the ontoness of g is easy to verify. Let $x = \langle x_i \rangle \in \varprojlim K_i$. Then, for each i , the set $X_i = g_i^{-1}(x_i)$ is compact. Moreover if $i < j$, $\psi_{ij} X_j \subseteq X_i$, i.e., $\{X_i, \psi_{ij}\}$ p. 36 is a projective system of non-empty compact sets. Hence $\varprojlim X_i \neq \emptyset$ (cf. [B3], §9, Prop. 8). Clearly, if $y \in \varprojlim X_i$ then $g(y) = x$. ∎

§4. Supernatural numbers.

For finite field extensions and finite groups we have the notions of degree and order respectively. In considering infinite field extensions $L|K$ of infinite profinite groups G it is convenient to have also a notion of degree and order, but to introduce ∞ or a cardinal number as degree or order respectively in those cases, would be useless since this would add nothing new to the internal description of the extension or the group. If $L|K$ contains a finite subextension of degree n or if G has a closed subgroup of index n, we would like to say that n "divides" the degree of $L|K$ or the order of G respectively.
p. 37 This leads to the notion of supernatural numbers, which we shall use as degrees of infinite field extensions, and as orders of profinite groups and discrete torsion groups.

Definition 4.1: A *supernatural number* is a formal product

$$n = \prod_p p^{n(p)}$$

where p runs through the set of all primes, and where each $n(p)$ is a non-negative integer or $+\infty$. If $m = \prod_p p^{m(p)}$ and for each p $0 \leq m(p) \leq n(p)$, we say that m divides n, and write $m \mid n$.

Definition 4.2: Let $n_i = \prod p^{n(p,i)}$, $i \in I$ be a family of supernatural numbers. Then we define

(i) $\prod n_i = \prod_p p^{n(p)}$, where $n(p) = \sum_i n(p,i)$,
(ii) g.c.d.$\{n_i\} = \prod_p p^{n(p)}$, where $n(p) = \min_i\{n(p,i)\}$,
(iii) l.c.m.$\{n_i\} = \prod_p p^{n(p)}$, where $n(p) = \max_i\{n(p,i)\}$.

p. 38 *Definition 4.3:* Let G be a profinite group and H a closed subgroup. Then the index $(G:H)$ of H in G is defined by $(G:H) = \text{l.c.m.}\{(G/U : HU/U)\} = \text{l.c.m.}\{(G:HU)\}$, and the order $\#G$ of G by $\#G = (G:1)$, where U runs over all open normal subgroups of G.

Remark: $(G:H) = \text{l.c.m.}\{(G:U)|\ U \text{ open subgroup containing } H\}$.

Examples:

(1) $\#\mathbb{Z}_p = p^\infty$;

(2) $\#\hat{\mathbb{Z}} = \prod_p p^\infty$;

(3) $\#(\prod_p(\mathbb{Z}/p\mathbb{Z})) = \prod_p p$.

PROPOSITION 4.4: *(a) Let $K \subseteq H \subseteq G$ be profinite groups. Then*

$$(G : K) = (G : H)(H : K);$$

(b) If $\{H_i |\ i \in I\}$ is a family filtered from below of closed subgroups of G and $H = \bigcap_{i\in I} H_i$, then one has

p. 39
$$(G : H) = \text{l.c.m.}_i\{(G : H_i)\};$$

(c) Let $\{G_i, \varphi_{ij} |\ i, j \in I\}$ be a surjective projective system of profinite groups (i.e. each φ_{ij} is surjective), and $G = \varprojlim_I G_i$. Then

$$\#G = \text{l.c.m.}_i\{\#G_i\};$$

(d) $\#(\prod_i G_i) = \prod_i \#G_i$;

(e) $(G : H)$ is a natural number $\Leftrightarrow$ H is open in G.

Proof: <u>For (a)</u>: Let

$$\underline{S} = \{U |\ U \text{ open normal subgroup of } G\}.$$

Then

$$H \cap \underline{S} = \{H \cap U |\ U \in \underline{S}\}$$

is a basis in H of open, normal subgroups. Hence

$$\begin{aligned}(H : K) &= \text{l.c.m.}\{(H/H \cap U : K(H \cap U)/H \cap U) |\ U \in \underline{S}\} \\ &= \text{l.c.m.}\{(HU/U : KU/U) |\ U \in \underline{S}\}.\end{aligned}$$

Now, for each $U \in \underline{S}$ we have

p. 40
$$(G/U : KU/U) = (G/U : HU/U)(HU/U : KU/U). \tag{1}$$

Let p be a prime. If $p^\infty \mid (G : K)$ it follows from (1) that either $p^\infty \mid (G : H)$ or $p^\infty \mid (H : K)$. If $p^\infty \nmid (G : K)$, let n_1, n_2 and n_3 be the exponent (finite) of p in $(G : K)$,

$(G : H)$ and $(H : K)$ respectively. Then there exist open subgroups $U_i \quad (i = 1, 2, 3)$ of G such that $p^{n_i} \mid (G/U_i : KU_i/U_i) \quad (i = 1, 2, 3)$. Take $U = \bigcap_{i=1}^{3} U_i$. Then it is clear that p^{n_i} divides (and p^{n_i+1} does not divide) $(G/U : KU/U) \quad (i = 1, 2, 3)$, since $(G/U_i : KU_i/U_i) = (G : KU_i)$ divides $(G : KU) = (G/U : KU/U) \quad (i = 1, 2, 3)$. Then from (1) we obtain $n_1 = n_2 + n_3$ as desired.

For (b): Let U be an open subgroup of G with $U \supseteq H$. Put $H_i' = H_i \cap (G \smallsetminus U)$; then $\bigcap_{i \in I} H_i' = \emptyset$; and since G is compact and each H_i' closed there is a finite subset F of I with $\bigcap_{i \in F} H_i' = \emptyset$, i.e. $\bigcap_{i \in F} H_i \subseteq U$. But since $\{H_i |\ i \in I\}$ is filtered from below it follows that $U \supseteq H_{i_0}$ for some $i_0 \in I$.

For each $i \in I$ let $\{U_{ij}\}_j$ be the set of all open subgroups containing H_i. Then

$$\underline{S}_H = \{U |\ U \text{ open } \supseteq H\} = \{U_{ij}\}_{i,j}.$$

p. 41 Hence

$$\begin{aligned}(G : H) &= \underset{U \in \underline{S}_H}{\text{l.c.m.}}\{(G : U)\} = \underset{i,j}{\text{l.c.m.}}\{(G : U_{ij})\} = \underset{i}{\text{l.c.m.}}\{\underset{j}{\text{l.c.m.}}\{(G : U_{ij})\}\} \\ &= \underset{i}{\text{l.c.m.}}\{(G : H_i)\}.\end{aligned}$$

For (c): Notice first that each projection $G \longrightarrow G_i$ is onto since each G_i is compact and the system is surjective (cf. [B3], §9, Prop. 8, 1°). For each open normal subgroup U of G_i let $N_U = G \cap (\prod_{j \neq i} G_j \times U)$. Then the set of all N_U forms a basis of open normal subgroups of G; hence

$$\begin{aligned}\#G &= \text{l.c.m.}\{\#(G/N_U) |\ U \text{ open, normal subgroup of some } G_i\} \\ &= \text{l.c.m.}\{\#(G_i/U) |\ i \in I, U \text{ open, normal subgroup of } G\} \\ &= \text{l.c.m.}\{\#G_i |\ i \in I\}.\end{aligned}$$

For (d): Consider the set

$$\underline{F} = \{F \subseteq I |\ F \text{ finite}\}$$

p. 42 ordered by inclusion. Then $\{\prod_{i \in F} G_i |\ F \in \underline{F}\}$ is a projective system in an obvious way, and one easily sees that

$$\prod_{i \in I} G_i = \varprojlim_{\underline{F}} (\prod_{F} G_i).$$

Hence, using part (c) we get

$$\#(\prod_{i\in I} G_i) = \text{l.c.m.}_F\{\#(\prod_{i\in F} G_i)\} = \prod_{i\in I} \#G_i.$$

For (e): Suppose $(G:H) = n < \infty$. Let U be an open subgroup of G containing H such that

$$(G:U) = \max\{(G:V)|\ V \text{ open subgroup containing } H\}.$$

Then U is contained in every open subgroup V that contains H (for if V is an open subgroup of G with $V \supseteq H$ but $V \not\supseteq U$ then $V \cap U \supseteq H$ but $U \not\supseteq V \cap U$, contradicting the definition of U). Now, H is the intersection of the open subgroups containing it. Thus $U = H$. ∎

Definition 4.5: Let $N|K$ be any algebraic field extension. Define

p. 43
$$[N:K] = \text{l.c.m.}\{[L:K]|\ N \supseteq L \supseteq K, \quad L|K \text{ finite}\}.$$

PROPOSITION 4.6: *Let $N|K$ be a Galois extension. Let H be a closed subgroup of $G = G_{N|K}$ and L the fixed field of H. Then*

$$[L:K] = (G:H).$$

Proof: Notice that if $(G:H) < \infty$ then the number of distinct K-isomorphisms of L into N is precisely $(G:H)$. Then, when $(G:H)$ is finite the result is a consequence of §8, Prop. 8 in [B2]. The general case follows now from the bijective correspondence in Theorem 1.7 and the definitions of $(G:H)$ and $[L:K]$. ∎

PROPOSITION 4.7: *Let $N|K$ be a Galois extension of fields.*

(a) Let $N \supseteq L \supseteq K$. Then

$$[N:K] = [N:L][L:K];$$

p. 44
(b) Let $\{L_i|\ i \in I\}$ be a family filtered from above of subextensions $L_i|K$ of $N|K$ with $N = \varinjlim L_i$. Then

$$[N:K] = \text{l.c.m.}\{[L_i:K]|\ \ i \in I\};$$

(c) If $N|K$ is finite then $[N : K]$ is the usual degree.

Proof: (a) and (b) are consequences of the above Proposition, Th. 1.7 and Prop. 4.4. (c) is trivial. ∎

Definition 4.8: Let A be an abelian torsion group. Then

$$\#A = \text{l.c.m.}\{\#A_i |\ A_i \text{ finite subgroup of } A\}.$$

Examples:

(1) $\#(\mathbb{Q}/\mathbb{Z}) = \prod_p p^\infty$;

(2) $\#(\mathbb{Q}_p/\mathbb{Z}_p) = p^\infty$.

PROPOSITION 4.9: *Let A be an abelian torsion group. Then*

p. 45
$$\#\chi(A) = \#A,$$

where $\chi(A) = \text{Hom}(A, \mathbb{Q}/\mathbb{Z})$, the Pontrjagin dual.

Proof: $\#\chi(A) = \#(\varprojlim A_i) = \text{l.c.m.}\,\#A_i = \#A$, where A_i runs through all finite subgroups of A (see Prop. 4.4, (c)). ∎

p. 46 §**5. The Sylow theorems.**

A large part of the definitions, statements and results of the theory of finite groups can be carried into the theory of profinite groups. Having introduced the supernatural numbers, this is especially true for those notions and results concerning order and indices. Thus, for instance the theory of p-groups and p-Sylow groups has its exact analog for profinite groups. To show this is the aim of this paragraph.

Definition 5.1: Let p be a prime number. A profinite group is called a *pro-p-group* if its order is a power of p, i.e., if it is a projective limit of finite p-groups. A closed subgroup H of a profinite group G is called a *p-Sylow* group of G if H is a pro-p-group and p does not divide $(G : H)$.

Example:

$$\mathbb{Z}_p = \varprojlim_n \mathbb{Z}/p^n\mathbb{Z}$$

is a pro-p-group.

p. 47 PROPOSITION 5.2 (The Sylow theorems.): *Let G be a profinite group. Then*

(a) For every prime p there exists a p-Sylow subgroup of G.

(b) Any two p-Sylow subgroups of G are conjugate.

(c) Every pro-p-subgroup of G is contained in a p-Sylow group of G.

(d) If $h\colon G_1 \longrightarrow G_2$ is a continuous surjective homomorphism of profinite groups then the image of a p-Sylow group is a p-Sylow group.

(e) $\#G = \prod_p \#G_p$, where G_p is a p-Sylow group of G.

Proof: For (a): Let $\underline{S}$ be the set of all open normal U of G, and let $P(U)$ denote the set of all p-Sylow subgroups H_U of G/U. (Notice that if $p \nmid \#(G/U)$, then $P(U) = \{1\}$). If $U \subseteq U'$ are in $\underline{S}$, then natural epimorphism $G/U \longrightarrow G/U'$ induces a map $P(U) \longrightarrow P(U')$ making $\{P(U)|\ U \in \underline{S}\}$ into a projective system of finite non-empty sets. Hence

$$\varprojlim_{\underline{S}} P(U) \neq \emptyset$$

p. 48 (cf. [B3], §9, Prop. 8, 2°). Let $\langle H_U \rangle \in \varprojlim P(U)$. Then $\langle H_U \rangle$ is a projective surjective system of p-Sylow groups. Let

$$H = \varprojlim_{\underline{S}} H_U.$$

Certainly H is a pro-p-group. On the other hand from the commutative diagram

$$\begin{array}{ccccccccc}
 & & 1 & & 1 & & 1. & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
1 & \longrightarrow & H \cap U & \longrightarrow & H = \varprojlim_{\underline{S}} H_U & \longrightarrow & H_U & \longrightarrow & 1 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
1 & \longrightarrow & U & \longrightarrow & G = \varprojlim_{\underline{S}} G/U & \longrightarrow & G/U & \longrightarrow & 1
\end{array}$$

with exact rows (cf. [B3], §9, Prop. 8, 1°) and columns, one one gets that $H \subseteq G$ and that

$$(G : H) = \underset{U}{\text{l.c.m.}}(G/U : UH/U) = \underset{U}{\text{l.c.m.}}(G/U : H/U \cap H) = \underset{U}{\text{l.c.m.}}(G/U : H_U)$$

which is prime to p since each $(G/U : H_U)$ is prime to p.

p. 49 For (b): Let H, H' be p-Sylow groups of G. Then for every $U \in \underline{S}$, $H_U = HU/U$ and $H'_U = H'U/U$ are p-Sylow groups of G/U. Set

$$Q(U) = \{\sigma_U \in G/U |\ \sigma_U H_U \sigma_U^{-1} = H'_U\}.$$

If $U, V \in \underline{S}$ with $U \subseteq V$, the homomorphism $G/U \longrightarrow G/V$ induces a map $Q(U) \longrightarrow Q(V)$ making $\{Q(U) |\ U \in \underline{S}\}$ into a projective system of finite non-empty sets. Hence $\varprojlim Q(U) \neq \emptyset$. Thus we may choose

$$\sigma = \langle \sigma_U \rangle \in \varprojlim G/U = G, \qquad \sigma_U \in Q(U).$$

Clearly $\sigma H \sigma^{-1} = H'$, since $\sigma_U H_U \sigma_U^{-1} = H'_U$ for every $U \in \underline{S}$.

For (c): Let H be a pro-p-subgroup of G. Then $H_U = HU/U$ is a p-subgroup of G/U for every $U \in \underline{S}$. Let $P(U)$ be as in (a), and

$$R(U) = \{H'_U \in P(U) |\ H'_U \supseteq H_U\}.$$

As in (a), $\{R(U) |\ U \in \underline{S}\}$ is a projective system of non-empty finite sets. Let $\langle H'_U \rangle \in \varprojlim R(U)$, and define

$$H' = \varprojlim H'_U.$$

p. 50 It is plain that H' is a p-Sylow group of G containing H.

For (d): Let H be a p-Sylow group of G_1. For each open normal subgroup U of G_2, h induces an epimorphism $G_1/h^{-1}(U) \longrightarrow G_2/U$ mapping $H \cdot h^{-1}(U)/h^{-1}(U)$ onto $h(H) \cdot U/U$. Thus the result.

For (e): This follows immediately from

$$\#G = (G : G_p)(\#G_p)$$

see Prop. 4.4(a)). ∎

APPLICATION. Let k be a field, k_s its algebraic separable closure, and $G_k = G_{k_s|k}$.

PROPOSITION 5.3: *Let*

$$\#G_k = \prod_p p^{n(p)}$$

p. 51 *Then*

$p \neq 2 \Rightarrow n(p) = 0, \infty$;

$p = 2 \Rightarrow n(p) = 0, 1, \infty$.

This theorem is in fact an immediate generalization of the following theorem of Artin-Schreier: *"Let k be a field, $\bar{k}$ its algebraic closure and $[\bar{k} : k] < \infty$. Then either $\bar{k} = k$ or $\bar{k} = k(\sqrt{-1})$".* (Cf. [J], p. 316.)

Proof of theorem 5.3: Let H be a p-Sylow group of G_k and k' the fixed field of H. Then $H = G_{k'}$, and so

$$p^{n(p)} = \#H = \#G_{k'} = [k_s : k']$$

(see Prop. 4.6). Suppose $0 < n(p) < \infty$; then $k_s \neq k'$, and $[k_s : k'] < \infty$.Then we must have $k'(\sqrt{-1}) = k_s$, for let σ be a $k'(\sqrt{-1})$-automorphism of k_s; let $\bar{\sigma}$ be its (unique) extension to $\bar{k}$, and k_1 the fixed field of $\bar{\sigma}$. Clearly if $x_1, x_2, \ldots, x_t$ are k_1-linearly independent elements of $\bar{k}$ and char $(k) = p$, there is some e such that $x_1^{p^e}, x_2^{p^e}, \ldots, x_t^{p^e}$

p. 52 are $k'(\sqrt{-1})$-linearly independent elements of k_s; therefore $[\bar{k} : k_1] < \infty$. So by Artin-Schreier theorem $k_1 = \bar{k}$. Thus $k'(\sqrt{-1}) = k_s$, i.e., $[k_s : k'] = 2$ and hence $p = 2$ and $n(p) = 1$. ∎

PROPOSITION 5.4: *Let G be an abelian profinite group, and for each prime p let G_p denote its p-Sylow group. Then*

$$G = \prod_p G_p.$$

Proof: For each open normal subgroup U of G, let U_p denote the p-Sylow subgroup of G/U. Since G/U is finite, $G/U = \prod_p U_p$. On the other hand $\{U_p |\ U$ open, normal subgroup of $G\}$ is a projective system in a natural way and $\varprojlim_U U_p = G_p$ (see proof of Prop. 5.2(a)). Hence

$$G = \varprojlim_U G/U = \varprojlim_U \prod_p U_p = \prod_p \varprojlim_U U_p = \prod_p G_p$$

(cf. [B1], §6, Prop. 3). ∎

p. 53 The concept of pro-p-group has a natural and useful generalization as follows.

Definition 5.5: Let $\underline{C}$ be a class of finite groups. A profinite group G is a *pro-$\underline{C}$-group* if $G/U \in \underline{C}$ for every open normal subgroup U of G.

Besides the case when $\underline{C}$ consists of all p-groups other interesting examples of $\underline{C}$ are (i) all finite groups; (ii) solvable groups; (iii) abelian groups; (iv) nilpotent groups; (v) cyclic groups.

Let us consider now a class $\underline{C}$ of finite groups satisfying the conditions

(1) $H \subseteq G$ and $G \in \underline{C} \Rightarrow H \in \underline{C}$;

(2) H normal subgroup of $G \in \underline{C} \Rightarrow G/H \in \underline{C}$;

(3) $H, K \in \underline{C} \Rightarrow H \times K \in \underline{C}$.

Let G be a profinite group and put

$$\underline{G}(\underline{C}) = \{U |\ U \text{ open, normal subgroup of } G, \text{ with } G/U \in \underline{C}\}.$$

Note that $U_1, U_2 \in \underline{G}(\underline{C}) \Rightarrow U_1 \cap U_2 \in \underline{G}(\underline{C})$, for $G/U_1 \cap U_2$ is isomorphic to a subgroup of $G/U_1 \times G/U_2 \in \underline{C}$. Let

$$N = \bigcap_{U \in \underline{G}(\underline{C})} U,$$

p. 54 and set

$$G(\underline{C}) = G/N = \varprojlim_{U \in \underline{G}(\underline{C})} G/U.$$

The group $G(\underline{C})$ is a pro-$\underline{C}$-group for assume V/N is an open normal subgroup of G/N with V open and normal in G; then (Prop. 2.6) there is some open normal subgroup U of G such that $U \in \underline{G}(\underline{C})$ and $U \subseteq V$; so

$$G/N/V/N \approx G/V \approx G/U/V/U$$

is an epimorphic image of G/U, and therefore G/V is in $\underline{C}$. The group $G(\underline{C})$ is called the *maximal pro-$\underline{C}$ quotient group* of G, and plays an important role in Galois theory.

Namely, given a field k, denote by $k(\underline{C})$ the compositum of all Galois extensions of k whose Galois group is in $\underline{C}$. Then

$$G_k(\underline{C}) \approx G_{k(\underline{C})|k} \approx G_k/G_{k(\underline{C})}$$

and

$$G_{k(\underline{C})} = \bigcap_{L|k} G_L,$$

p. 55 where $G_{L|k} \in \underline{C}$. ($G_k = G_{k_s|k}$, where k_s is the separable closure of k.)

Remark: Consider the canonical epimorphism $\pi: G \longrightarrow G(\underline{C})$. The pair $(G(\underline{C}), \pi)$ is uniquely characterized by the following universal property: given a continuous homomorphism $\varphi: G \longrightarrow H$, where H is a pro-$\underline{C}$-group, there exists a unique continuous homomorphism $\psi: G(\underline{C}) \longrightarrow H$ such that $\psi \circ \pi = \varphi$.

p. 56 §**6. Classification of pro-cyclic groups.**

As in the finite case, pro-cyclic groups have very simple structure and can be classified by their orders.

LEMMA 6.1: *A finite pro-cyclic group is cyclic.*

Proof: Obvious. ∎

PROPOSITION 6.2: *Let p be a prime number. Then for every power p^n there exists a unique pro-cyclic group G of order p^n. Namely, if $n < \infty$, $G = \mathbb{Z}/p^n\mathbb{Z}$, and if $n = \infty$, $G = \mathbb{Z}_p$.*

Proof: If $n < \infty$, G is finite cyclic of order p^n; so $G = \mathbb{Z}/p^n\mathbb{Z}$. Supppose $n = \infty$. Let U, U' be open subgroups of G of the same index in G. Then $U/U \cap U'$ and $U'/U \cap U'$ are subgroups of the finite cyclic group $G/U \cap U'$ of the same order; hence $U = U'$. For each i let U_i be the open subgroup of G of index p^i. Then

$$G = \varprojlim_i G/U_i \approx \varprojlim_i \mathbb{Z}/p^i\mathbb{Z} = \mathbb{Z}_p.$$

p. 57

∎

PROPOSITION 6.3: *Let p be a prime. For every power p^n there exists a unique closed subgroup H of $G = \mathbb{Z}_p$ of index p^n. Moreover if $n < \infty$ then $H \approx \mathbb{Z}_p$, and if $n = \infty$ then $H \approx 1$.*

Proof: Let U_i be the open subgroup of index p^i $(i = 1, 2, \ldots)$. Then

$$G \supseteq U_1 \supseteq U_2 \supseteq \cdots .$$

Let H be a closed subgroup of $\mathbb{Z}_p$ of index $p^n < \infty$. Since

$$p^n = (G : H) = \underset{i}{\text{l.c.m.}}\{(G : U_i H)\},$$

we must have $U_i H \supseteq U_n, \ \forall i$. But $H = \bigcap_i U_i H$; so $H \supseteq U_n$; therefore $p^n = (G : U_n) = (G : H)(H : U_n) = p^n(H : U_n)$, implies that $(H : U_n) = 1$, i.e., $H = U_n$ since U_n is
p. 58 open. It is obvious that in this case $\#H = p^\infty$, i.e, $H \approx \mathbb{Z}_p$ by Prop. 6.2. Now assume $n = \infty$. Then, given i $\exists j$ with $U_j H \subseteq U_i$; so

$$1 = \bigcap_i U_i H = H.$$

∎

COROLLARY 6.4: *Every pro-cyclic group of order p^n appears uniquely as a quotient group of $\mathbb{Z}_p$.*

THEOREM 6.4: (i) *For every supernatural number $n = \prod_p p^{n(p)}$ there exists a unique pro-cyclic group of order n;*

(ii) *For each $n = \prod_p p^{n(p)}$ there exists a unique closed subgroup H of $\hat{\mathbb{Z}} = \varprojlim_m \mathbb{Z}/m\mathbb{Z}$ (the Prüfer group) of index n. Moreover*

$$H \approx \prod_{p \in S} \mathbb{Z}_p,$$

where $S = \{p |\ n(p) \neq \infty\}$;

(iii) *Every pro-cyclic group is uniquely obtained as a quotient group of $\hat{\mathbb{Z}}$.*

p. 59 *Proof:* For (i): Let G_p be the unique pro-cyclic group of order $p^{n(p)}$ (see Prop. 6.2). Clearly

$$G = \prod_p G_p$$

has order n. To see that G is pro-cyclic, consider a basic open normal subgroup

$$U = \prod_{p \neq p_1, \ldots, p_r} G_p \times U_{p_1} \times \cdots \times U_{p_r}$$

of G where U_{p_i} is an open normal subgroup of G_{p_i}; then

$$G/U \approx \prod_{i=1}^{r} G_{p_i}/U_{p_i},$$

which is a finite cyclic group since each G_{p_i}/U_{p_i} is cyclic and $i \neq j \Rightarrow p_i \neq p_j$. Finally, the uniqueness follows from Prop. 5.4.

For (ii): First notice that the p-Sylow group of $\hat{\mathbb{Z}}$ is $\mathbb{Z}_p = \varprojlim_n \mathbb{Z}/p^n\mathbb{Z}$; so, by (i) $\hat{\mathbb{Z}} = \prod_p \mathbb{Z}_p$. For each p let H_p be the unique closed subgroup of $\mathbb{Z}_p$ of index $p^{n(p)}$ (Prop. 6.3). Then $H = \prod_p H_p$ is the desired subgroup of $\hat{\mathbb{Z}}$.

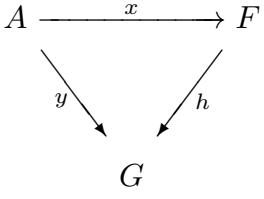
p. 60 For (iii): This is immediate from (i) and (ii). ∎

§7. Free profinite groups

From now on $\underline{C}$ will denote a class of finite groups which is closed under the operations of taking subgroups, quotient groups and finite direct products (see p. 53). It is evident that then the corresponding category of pro-$\underline{C}$-groups is again closed under those operations.

Definition 7.1: Let A be a set and G a pro-$\underline{C}$-group. We say that a map $x: A \longrightarrow G$ is *convergent to* 1 if every open normal subgroup of G contains a.e. (almost every, i.e. all but finite number) x_α, $\alpha \in A$.

p. 61 *Definition 7.2:* A *free pro-$\underline{C}$-group* on a set A is a pro-$\underline{C}$-group F together with a map $x: A \longrightarrow F$ convergent to 1, satisfying the following universal property: if $y: A \longrightarrow G$ is any map convergent to 1 of A into a pro-$\underline{C}$-group, then there exists a unique continuous homomorphism $h: F \longrightarrow G$ such that the diagram



commutes.

The x_α's generate a dense subgroup of F and are said to be a (topological) system of generators of F.

PROPOSITION 7.3: *For every set A there exists a unique free pro-$\underline{C}$-group on the set A. It is denoted by $F_A(\underline{C})$. [If $\underline{C}$ consists of all finite groups we write F_A instead of $F_A(\underline{C})$; if A is a finite set with n elements we write $F_n(\underline{C})$ instead of $F_A(\underline{C})$ and call n the rank of $F_n(\underline{C})$.]*

p. 62 *Proof:* If $x\colon A \longrightarrow F$ and $x'\colon A \longrightarrow F'$ are free groups generated by A, let $h\colon F \longrightarrow F'$ and $h'\colon F' \longrightarrow F$ be the unique continuous homomorphisms such that $hx = x'$ and $h'x' = x$. Then we must have $h' \circ h = \mathrm{id}_F$ and $h \circ h' = \mathrm{id}_{F'}$. Thus F and F' are isomorphic, and hence $F_A(\underline{C})$ is unique.

We shall construct $F_A(\underline{C})$ in the following manner. Let $x^0\colon A \longrightarrow F$ be the discrete free group generated by A and denote by $\underline{S}$ the system of all normal subgroups N of F such that

(1) $F/N \in \underline{C}$, and

(2) N contains a.e. x_α^0.

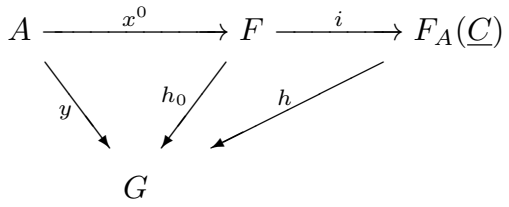
Then $\underline{S}$ is a basis of neighborhoods of 1 in F. For if $N_1, N_2 \in \underline{S}$ then $N_1 \cap N_2$ is clearly normal satisfying condition (2), and since $F/N_1 \cap N_2$ is isomorphic to a subgroup of $F/N_1 \times F/N_2$ we see that $N_1 \cap N_2$ satisfies also condition (1). Hence $\underline{S}$ defines a topology in F.

Set

$$F_A(\underline{C}) = \varprojlim_{\underline{S}} F/N.$$

p. 63 The compatible family $F \longrightarrow F/N$ of continuous homomorphisms defines a continuous homomorphism $i\colon F \longrightarrow F_A(\underline{C})$. By Lemma 2.5 $i(F)$ is dense in $F_A(\underline{C})$. Take $x = i \circ x^0$. Clearly x is convergent to 1. The group $F_A(\underline{C})$ is a pro-$\underline{C}$-group because if U is an open normal subgroup of $F_A(\underline{C})$, let $U' = \ker F_A(\underline{C}) \longrightarrow F/N$ for some N so that $U \supseteq U'$; then $F_A(\underline{C})/U$ is a homomorphic image of $F_A(\underline{C})/U' \approx F/N$ and hence $F_A(\underline{C})/U \in \underline{C}$. Finally $F_A(\underline{C})$ is free, for suppose G is a pro-$\underline{C}$-group and let $y\colon A \longrightarrow G$ be convergent

to 1. Let $h_0: F \longrightarrow G$ be the unique homomorphism such that $h_0 \circ x^0 = y$.



The map h_0 is continuous since, if U is open and normal in G and $N = h_0^{-1}(U)$, the natural map

$$F/N \longrightarrow G/U$$

is injective; so $G/U \in \underline{C}$ implies $F/N \in \underline{C}$. Moreover $y_\alpha \in U \Rightarrow x_\alpha^0 \in N$; hence a.e. x_α^0 is in N.

p. 64 For each open normal subgroup U of G consider the continuous homomorphisms

$$F_A(\underline{C}) \longrightarrow F/h^{-1}(U) \longrightarrow G/U.$$

This compatible family of maps defines a continuous homomorphism

$$h: F_A(\underline{C}) \longrightarrow \varprojlim G/U = G.$$

Clearly $h \circ i = h_0$. Hence $h \circ x = h \circ i \circ x^0 = h_0 \circ x^0 = y$. Finally, if $h': F_A(\underline{C}) \longrightarrow G$ is a continuous homomorphism satisfying $h' \circ x = y$, put $h_0' = h' \circ i$; then $h' \circ x^0 = y$, so $h_0' = h_o$, i.e., $h \circ i = h' \circ i$. Since $i(F)$ is dense in $F_A(\underline{C})$ we have $h = h'$. ∎

Examples:

(1) The free profinite group of rank 1 is $\hat{\mathbb{Z}} = \varprojlim_m \mathbb{Z}/m\mathbb{Z}$.

(2) The free pro-p-group of rank 1 is $\mathbb{Z}_p = \varprojlim_n \mathbb{Z}/p^n\mathbb{Z}$.

p. 65 (3) Let $\underline{C}$ be a class of finite groups satisfying the conditions of p. 53, and let

$$n = \text{l.c.m.}\{\#G |\ G \in \underline{C}\}.$$

Then the free pro-$\underline{C}$-group of rank 1 F, is the unique pro-cyclic group of order n. For, F is clearly pro-cyclic and of order n (see Prop. 4.4(c)).

(4) Suppose $\underline{C} \subseteq \underline{C}'$ are classes of finite groups satisfying the conditions of p. 53. Let A be any set. Then the free pro-$\underline{C}$-group $F_A(\underline{C})$ is just the maximal pro- $\underline{C}$-quotient of $F_A(\underline{C}')$. (This follows easily from the remark on p. 55.)

Let $B \subseteq A$ be sets, and $\underline{C}$ a class of finite groups satisfying the conditions of p. 53. Let $x\colon B \longrightarrow F_B(\underline{C})$ and $y\colon A \longrightarrow F_A(\underline{C})$ be the free pro-$\underline{C}$-groups on B and A respectively.

Define continuous homomorphisms i, π

$$\begin{array}{ccc} F_B(\underline{C}) & \underset{\pi}{\overset{i}{\rightleftarrows}} & F_A(\underline{C}) \\ x\uparrow & & \uparrow y \\ B & & A \end{array}$$

p. 66 to be the liftings of $B \longrightarrow F_A(\underline{C})$ given by $\alpha \mapsto y_\alpha$, and of $A \longrightarrow F_B(\underline{C})$ given by $\alpha \mapsto x_\alpha$ if $\alpha \in B$ and $\alpha \longrightarrow 1$ if $\alpha \in A \smallsetminus B$. Clearly $x = \pi \circ i \circ x$; hence $\pi \circ i =$ identity. Thus i is injective and π is surjective.

PROPOSITION 7.4: *Let $B \subseteq A, i, \pi$ be as above. Then there exists a canonical split extension*

$$1 \longrightarrow K \longrightarrow F_A(\underline{C}) \xrightarrow{\pi} F_B(\underline{C}) \longrightarrow 1$$

where K is the smallest closed normal subgroup of $F_A(\underline{C})$ containing $F_{A \smallsetminus B}(\underline{C})$.

Proof: We have already shown that the extension splits. Certainly $K \supseteq F_{A \smallsetminus B}(\underline{C})$ (we identify $F_{A \smallsetminus B}(\underline{C})$ and $F_B(\underline{C})$ with their canonical images in $F_A(\underline{C})$). Then if N is the intersection of all closed normal subgroups of $F_A(\underline{C})$ containing $F_{A \smallsetminus B}(\underline{C})$ we have $N \subseteq K$. Notice that both $K \cdot F_B(\underline{C})$ and $N \cdot F_B(\underline{C})$ are compact subgroups of $F_A(\underline{C})$ containing A, and therefore

$$K \cdot F_B(\underline{C}) = N \cdot F_B(\underline{C}) = F_A(\underline{C}).$$

On the other hand

p. 67 $$K \cap F_B(\underline{C}) = N \cap F_B(\underline{C}) = 1.$$

Thus $K = N$. ∎

Given a set A consider the projective system consisting of objects $F_S(\underline{C})$ for all finite $S \subseteqq A$, and consider maps

$$\pi^S_{S'}: F_S(\underline{C}) \longrightarrow F_{S'}(\underline{C})$$

defined for $S \supseteq S'$ as the canonical surjections described above. Then the continuous epimorphisms

$$\pi_S: F_A(\underline{C}) \longrightarrow F_S(\underline{C})$$

define a continuous homomorphism

$$\pi: F_A(\underline{C}) \longrightarrow \varprojlim F_S(\underline{C}).$$

PROPOSITION 7.5: *The map π is an isomorphism of pro-$\underline{C}$-groups.*

p. 68 *Proof:* Since $F_A(\underline{C})$ is compact it suffices to show that π is injective and surjective. By Lemma 2.5 it is surjective. Let

$$K = \ker \pi.$$

Then

$$K = \bigcap \ker(\pi_S)$$

(S runs through all finite subsets of A.) We shall show that K is contained in every open normal subgroup of $F_A(\underline{C})$; this will imply $K = 1$. Let U be one such subgroup; choose a finite set $S \subseteq A$ so that $x_\alpha \in U$ for every $\alpha \in A \smallsetminus S$. Then, by Prop. 7.4 $\ker \pi_S \subseteq U$. Thus $K \subseteq U$. ∎

PROPOSITION 7.6: *A surjective continuous endomorphism $f: G \longrightarrow G$ of finitely generated profinite group G is an isomorphism. [A topological group G is said to be (topologically) generated by $\{x_\alpha\}_{\alpha \in A}$ if the $\{x_\alpha\}_{\alpha \in A}$ generate a dense subgroup of G.]*

p. 69 *Proof:* Since G is compact it will suffice to show that $\ker f = 1$, i.e. that $\ker f$ is contained in every open normal subgroup. Denote by $\underline{S}_n$ the set of open normal subgroups of index n in G. Then $\underline{S}_n$ is finite, for there exist finitely many nonisomorphic

groups of order n and finitely many homomorphisms of G into each of those groups since G is finitely generated. Define

$$h: \underline{S}_n \longrightarrow \underline{S}_n$$

by $h(U) = f^{-1}(U)$. Then h is clearly injective and therefore bijective.

Let U be an open normal subgroup of G; then $U = f^{-1}(V)$ for some open normal subgroup V of G. Hence $U = f^{-1}(V) \supseteq \ker f$. ∎

COROLLARY 7.7: *If G_1 and G_2 are (topologically) isomorphic finitely generated profinite groups, then every surjective continuous homomorphism $G_1 \longrightarrow G_2$ is an isomorphism.*

p. 70 **§8. The Galois group of $\overline{\mathbb{C}(t)}/\mathbb{C}(t)$.**

As an application to Galois theory we shall prove now the following result due to Douady [D2].

THEOREM 8.1: *Let $K = \mathbb{C}(t)$ where $\mathbb{C}$ is the field of complex numbers and t an indeterminate. Let $\bar{K}$ be an algebraic closure of K. Then $G_K = G_{\bar{K}|K}$ is the free profinite group on the set $\mathbb{C}$.*

Proof: Let A be the set of all rank 1 valuations of $\mathbb{C}(t)$. Then there exists a 1-1 correspondence between A and the set $\mathbb{C}$. For each finite subset S of A let $K_S|K$ be the maximal normal extension of K unramified at the elements of $A \setminus S$. Let $G_S = G_{K_S|K}$. Clearly if $S \supseteq S'$ then $K_S \supseteq K_{S'}$ and the restriction map $\kappa^S_{S'}: G_S \longrightarrow G_{S'}$ is a surjective continuous homomorphism. Then

$$\{G_S, \kappa^S_{S'} |\ S \supseteq S' \text{ finite subsets of } A\}$$

p. 71 is a projective system and the set of compatible continuous epimorphisms $G_K \longrightarrow G_S$, defines a continuous epimorphism (cf. Lemma 2.5)

$$\varphi: G_K \longrightarrow \varprojlim G_S,$$

which is also 1-1 since

$$\bar{K} = \bigcup K_S$$

(S runs through all finite subsets of A). This implies that φ is a homeomorphism since G_K is compact.

Let us consider now the free profinite group F_A. By Prop. 7.5 $F_A = \varprojlim_S F_S$ (finite $S \subset A$). Hence to prove the theorem it will suffice to show that there exists an isomorphism

$$\{F_S\} \xrightarrow{i} \{G_S\}$$

of projective systems of profinite groups, i.e., a collection of isomorphisms of profinite groups $i_S: F_S \longrightarrow G_S$ such that for any pair $S \supseteq S'$ of finite subsets of A, the diagram

$$\begin{array}{ccc} F_S & \longrightarrow & G_S \\ {\scriptstyle \pi^S_{S'}}\downarrow & & \downarrow{\scriptstyle \kappa^S_{S'}} \\ F_{S'} & \longrightarrow & G_{S'} \end{array}$$

p. 72

commutes.

To see this we will use the following proposition whose proof will be given later.

PROPOSITON 8.2: *For every finite set $S \subset A$ there exists an isomorphisms of profinite groups $j_S: F_S \longrightarrow G_S$ such that if $S \supseteq S'$ then there exists an isomorphisms of profinite groups $k_{S'}: F_{S'} \longrightarrow G_{S'}$ making the diagram*

$$\begin{array}{ccc} F_S & \xrightarrow{j_S} & G_S \\ {\scriptstyle \pi^S_{S'}}\downarrow & & \downarrow{\scriptstyle \kappa^S_{S'}} \\ F_{S'} & \xrightarrow{k_{S'}} & G_{S'} \end{array}$$

commutative.

To continue with the proof of the theorem, for each finite $S \subseteq A$ let J_S be the set
p. 73 of isomorphisms j_S mentioned in Prop. 8.2. Then $J_S \neq \emptyset$. Moreover if $S \supseteq S'$ there exists a mappings $J_S \longrightarrow J_{S'}$ given by $j_S \longrightarrow k_{S'}$ making $\{J_S|$ finite $S \subseteq A\}$ into a projective system of sets. We intend to show that $\varprojlim_S J_S \neq \emptyset$. For this it suffices to endow each J_S with a compact topology so that the maps $J_S \longrightarrow J_{S'}$ are continuous. Notice first that by Cor. 7.7 the isomorphisms $F_S \longrightarrow G_S$ are in 1-1 correspondence

with the systems $\{g_1, g_2, \ldots, g_n\}$ of elements of G_S which generate G_S (topologically) where $n = \#S$. Then consider the subset

$$X_S \subseteq G_S^n = \overbrace{G_S \times \cdots \times G_S}^{n}$$

consisting of all $(g_\alpha)_{\alpha \in S}$ such that

(i) the g_α's generate G_S, and

(ii) $\kappa_{S'}^S(g_\alpha) = 1$ for $\alpha \in S \smallsetminus S'$, $S' \subseteq S'$.

We claim that X_S is closed. First notice that $(g_\alpha)_{\alpha \in S}$ generate G_S if and only if for every open normal subgroup V of G_S the images of the g_α's in G_S/V generate G_S/V. Let $\bar{X}_S$ be the subset of G_S^n satisfying condition (i); then if $\bar{X}_{SV}$ is the image of $\bar{X}_S$ in $(G_S/V)^n$ one has $\bar{X}_S = \varprojlim_V \bar{X}_{SV}$, and therefore $\bar{X}_S$ is closed. It is obvious that the
p. 74 subset of $\bar{X}_S$ satisfying condition (ii) is closed, i.e., X_S is closed and thus compact.

Given $(g_\alpha)_{\alpha \in S}$ consider the isomorphism of profinite groups $j_S \colon F_S \longrightarrow G_S$ given by $j_S(\alpha) = g_\alpha$, $\alpha \in S$. Then if $S' \subseteq S'$, define $k_{S'} \colon F_{S'} \longrightarrow G_{S'}$ by $k_{S'}(\alpha) = \kappa_{S'}^S(g_\alpha)$, $\alpha \in S'$. Then

$$\begin{array}{ccc} F_S & \xrightarrow{\quad j_S \quad} & G_S \\ {\scriptstyle \pi_{S'}^S}\downarrow & & \downarrow{\scriptstyle \kappa_{S'}^S} \\ F_{S'} & \xrightarrow{\quad k_{S'} \quad} & G_{S'} \end{array}$$

commutes, and by Cor. 7.7 $k_{S'}$ is an isomorphism. Hence $j_S \in J_S$. It is plain that there is a 1-1 correspondence

$$X_S \longleftrightarrow J_S.$$

Moreover, if $S \supseteq S'$ then

$$\begin{array}{ccc} X_S & \longleftrightarrow & J_S \\ \downarrow & & \downarrow \\ X_{S'} & \longleftrightarrow & J_{S'} \end{array}$$

p. 75 commutes, where the map

$$X_S \longrightarrow X_{S'},$$

which is given by $(g_\alpha)_{\alpha \in S} \mapsto (\kappa_{S'}^S g_\alpha)_{\alpha \in S'}$ is continuous since $\kappa_{S'}^S$ is continuous. Thus we can define a compact topology in J_S so that the maps $J_S \longrightarrow J_{S'}$, $S \supseteq S'$ are

continuous. This shows that $\varprojlim_S J_S \neq \emptyset$ (cf. [B3], §9, Prop. 8). Let $\langle i_s \rangle \in \varprojlim_S J_S$. Then $i = \{i_S\}$ is an isomorphism of the projective systems

$$\{F_S\} \qquad \text{and} \qquad \{G_S\}$$

as desired. ∎

Proof of Proposition 8.2 (Sketch): Here we use a few facts about the Riemann surface of a field that can be found in [Ch2], p. 133ff., and [Sp] chps. 4 and 10. If $L|K$ is a finite field extension, where $K = \mathbb{C}(x)$ the Riemann surface of L, $R(L)$, consists of all rank 1 valuations of L. A topology is defined on $R(L)$ in the following manner:
p. 76 for each $x \in L$ consider a function $x\colon R(L) \longrightarrow \mathbb{C}$ given by $x(v) =$ image of x in the residue class field of v; the topology on $R(L)$ is the weakest with respect to which all the maps x become continuous. Then $R(L)$ is a 2-dimensional, connected, compact, analytic manifold. In particular, $R(K)$ is the Riemann sphere. The function field of all meromorphic functions on $R(L)$ is precisely L.

Let S be a finite subset of $\mathbb{C} \equiv A$ as before; then $K_S = \bigcup_{L|K} L$, where $L|K$ is a finite extension unramified at $\mathbb{C} \setminus S$. So if $L|K$ is finite with $K \subseteq L \subseteq K_S$, then $R(L)$ is a finite sheeted covering of $R(K)$ with no branch points on $R(K) \setminus (S \cup \{\infty\})$, where the projection $p\colon R(L) \longrightarrow R(K)$ is the restriction map. So, if $R_S(L) = R(L) \setminus$ points above $S \cup \{\infty\}$, we have that

$$p\colon R_S(L) \longrightarrow R_S(K)$$

is a finite covering with no branch points.

Let $\tau(R_S(L))$ be the group of covering transformations, i.e., the group of all homeomorphisms

$$\tau\colon R_S(L) \longrightarrow R_S(L)$$

p. 77 such that $p(P) = p(\tau P)$, $P \in R_S(L)$. Then, for every finite, normal extension $L|K$ with $K \subseteq L \subseteq K_S$, one has $\tau(R_S(L)) \approx G_{L|K}$. For if $\sigma \in G_{L|K}$, define $\tau_\sigma \in \tau(R_S(L))$ by $\tau_\sigma(P) = P \circ \sigma$; clearly the homomorphism $\sigma \mapsto \tau_\sigma$ is injective. It is also surjective,

for given τ, set $\sigma(x(P)) = x(\tau(P))$, where we are identifying each $x \in L$ with its corresponding meromorphic function; then $\sigma \in G_{L|K}$ and $\tau_\sigma = \tau$.

Fix a point z_0 in $R_S(K)$, and let $P_0 \in R_S(L)$ be above z_0. Consider the fundamental group

$$\Pi_S(L) = \Pi_1(R_S(L), P_0).$$

Then $\Pi_S(K)$ is isomorphic, in a non-canonical way, to the free group generated by S. For each finite subset S of A choose one isomorphism $\Pi_S(K) \approx F_S$. Moreover for each finite normal extension $L|K$ we get an exact sequence

$$1 \longrightarrow \Pi_S(L) \longrightarrow \Pi_S(K) \xrightarrow{t} \tau(R_S(L)) \;\approx\; G_{L|K} \longrightarrow 1$$

where the map t can be described in the following manner: given a loop π in $R_S(K)$
p. 78 starting and ending at z_0 lift it to a curve in $R_S(L)$ starting at P_0, and suppose that the end point of this curve is P_1; then define $t(\pi)$ to be the unique covering transformation τ with the property $\tau(P_0) = P_1$. Now, if $N \supseteq L \supseteq K$ are finite normal extensions of K contained in K_S, we obtain a commutative diagram

$$\begin{array}{ccccccccccc} 1 & \longrightarrow & \Pi_S(L) & \longrightarrow & \Pi_S(K) & \longrightarrow & \tau(R_S(L)) & \approx & G_{L|K} & \longrightarrow & 1 \\ & & \uparrow & & \| & & \uparrow & & \uparrow & & \\ 1 & \longrightarrow & \Pi_S(N) & \longrightarrow & \Pi_S(K) & \longrightarrow & \tau(R_S(N)) & \approx & G_{N|K} & \longrightarrow & 1 \end{array}$$

where the vertical maps are the obvious ones. Therefore the projective systems

$$\{\Pi_S(K)/\Pi_S(L)|\ L|K \text{ finite}, K \subseteq L \subseteq K_S\}$$

and

$$\{G_{L|K}|\ L|K \text{ finite}, K \subseteq L \subseteq K_S\}$$

are isomorphic. By definition, $G_S = \varprojlim G_{L|K}$. On the other hand, $\varprojlim(\Pi_S(K)/\Pi_S(L))$ $= \hat{F}_S$ (the free profinite group on S). To see this it suffices to show that for every normal subgroup H of $\Pi_S(K)$ of finite index there is a finite normal extension $L|K$,
p. 79 $K_S \supseteq L \supseteq K$, such that the canonical image of $\Pi_S(L) \longrightarrow \Pi_S(K)$ is precisely H (see the construction of F_S in Prop. 7.3). But this follows from Riemann's existence theorem; namely, consider the covering R of $R(K)$ corresponding to H by the existence

theorem, and let L be the field of meromorphic functions of R. Then L is the desired finite normal field extension of K.

Thus we have obtained an isomorphism

$$j_S: F_S \longrightarrow G_S$$

for each finite set S of A. Moreover if $S' \subseteq S$, then the chosen isomorphism between $\Pi_S(K)$ and F_S induces an isomorphism between $\Pi_{S'}(K)$ and $F_{S'}$. Now, by the process indicated above we obtain an isomorphism $k_{S'}: F_{S'} \longrightarrow G_{S'}$, and it is then clear that the diagram

$$\begin{array}{ccc} F_S & \xrightarrow{\quad j_S \quad} & G_S \\ {\scriptstyle \pi^S_{S'}}\downarrow & & \downarrow{\scriptstyle \kappa^S_{S'}} \\ F_{S'} & \xrightarrow{\quad k_{S'} \quad} & G_{S'} \end{array}$$

p. 80 commutes.

Remark: Theorem 8.1 is still valid if $K = F(t)$ where F is any field of characteristic zero. Cf. [D2].

§9. The embedding problem.

Let K be a field and let H be a profinite group. One may pose then the following question: is there a Galois extension $N|K$ with $G_{N|K} \approx H$? Or, more generally, assume $L|K$ is a Galois extension of fields with $G_{L|K} = H'$; let $j: H \longrightarrow H'$ be an epimorphism of profinite groups. Then one may ask: is there a Galois extension $N|K$ such that $\sigma: H \xrightarrow{\approx} G_{N|K}$ and the diagram

$$\begin{array}{ccc} H & \xrightarrow{\quad j \quad} & H' \\ {\scriptstyle \approx}\downarrow{\scriptstyle \sigma} & & \| \\ G_{N|K} & \xrightarrow{\quad r \quad} & G_{L|K} \end{array}$$

p. 81

commutes where r is the natural restriction map?

Given a field K let K_s denote its separable algebraic closure, and set $G_K = G_{K_S|K}$. The existence of a Galois extension $T|K$ with Galois group $G_{T|K} = S$ is equivalent to

the existence of an epimorphism of profinite groups $\varphi: G_K \longrightarrow S$, as one easily verifies. Hence the above question can be reformulated in the following terms: given a field K, a Galois extension $L|K$ and an epimorphism $j: H \longrightarrow G_{L|K}$, is there an epimorphism $\psi: G_K \longrightarrow H$ such that the diagram

$$\begin{array}{ccc} & & G_K \\ & \overset{\psi}{\swarrow} & \big\downarrow \varphi \\ H & \xrightarrow{\ j\ } & G_{L|K} \end{array}$$

commutes, where φ is the natural restriction?

All these considerations lead to the following purely group-theoretical definitions.

p. 82 *Definition 9.1:* Let $\underline{C}$ be a class of finite groups satisfying the conditions of p. 53. Let G be a profinite group. A *$\underline{C}$-embedding problem* for G is a diagram

$$\begin{array}{ccccccccc} & & & & & & G & & \\ & & & & & & \big\downarrow \varphi & & \\ 1 & \longrightarrow & H'' & \longrightarrow & H & \xrightarrow[j]{} & H' & \longrightarrow & 1 \\ & & & & & & \big\downarrow & & \\ & & & & & & 1 & & \end{array}$$

where H, H', H'' are pro-$\underline{C}$-groups and where the row and the column are exact sequences of continuous homomorphisms. We say that this problem is *solvable* if there exists a continuous surjective homomorphism $\psi: G \longrightarrow H$ such that $j \circ \psi = \varphi$. We say that this problem is *weakly solvable* if there exists a continuous homomorphism $\psi: G \longrightarrow H$ such that $j \circ \psi = \varphi$. If $\underline{C}$ consists of all finite groups we write *"embedding problem"* instead of "$\underline{C}$-embedding problem". It is usually a difficult task to determine in which circumstances an embedding problem is solvable. Especially when the ground field K is an algebraic number field one is far away from knowing which embedding problems have a solution. Perhaps the most general result in this direction is the following theorem of Shafarevich ([Sh]) which we mention without proof.

p. 83 THEOREM 9.2: *Let $G = G_{\bar{K}|K}$ where K is an algebraic number field and $\bar{K}$ its algebraic closure. Then the embedding problem*

$$\begin{array}{ccccccccc} & & & & & & G & & \\ & & & & & & \downarrow & & \\ 1 & \longrightarrow & H'' & \longrightarrow & H & \longrightarrow & H' & \longrightarrow & 1 \\ & & & & & & \downarrow & & \\ & & & & & & 1 & & \end{array}$$

where H, H', H'' are finite groups, is solvable if H'' is nilpotent and the short exact sequence splits.

Example: As one of the many instances of an embedding problem which has no solution, consider the following. Let $\mathbb{Q}$ be the ground field and let $L = \mathbb{Q}(i)$. Then $G_{L|\mathbb{Q}} = \mathbb{Z}_2$. We claim that the embedding problem

$$\begin{array}{ccccccccc} & & & & & & G_{\bar{\mathbb{Q}}/\mathbb{Q}} & & \\ & & & & & & \downarrow & & \\ 1 & \longrightarrow & \mathbb{Z}_2 & \longrightarrow & \mathbb{Z}_4 & \longrightarrow & \mathbb{Z}_2 = G_{L|\mathbb{Q}} & \longrightarrow & 1 \end{array}$$

has no solution. For, suppose $N|L$ is a Galois extension with $G_{N|\mathbb{Q}} \approx \mathbb{Z}_4$. We may
p. 84 assume that $N \subseteq \mathbb{C}$. Then $\mathbb{C} = N(\mathbb{R})$ and $2 = [\mathbb{C} : \mathbb{R}] = [N : N \cap \mathbb{R}]$ (cf. [B2], §10, Th. 1), i.e., $N \cap \mathbb{R} = \mathbb{Q}(i)$, which is certainly impossible.

THEOREM 9.3 ((Iwasawa, [I])): *Let G be a pro-$\underline{C}$-group satisfying the first axiom of countability. Then the following are equivalent:*

(i) *G is a free pro-$\underline{C}$-group on a countable set;*

(ii) *Every $\underline{C}$-embedding problem for G*

$$\begin{array}{ccccccccc} & & & & & & G & & \\ & & & & & & \downarrow & & \\ 1 & \longrightarrow & H'' & \longrightarrow & H & \longrightarrow & H' & \longrightarrow & 1 \\ & & & & & & \downarrow & & \\ & & & & & & 1 & & \end{array}$$

where H, H', H'' are in $\underline{C}$ is solvable.

In the proof of this result we will use the following

LEMMA 9.4: *Let G be a profinite group. The following are equivalent*

(i) *G satisfies the first axiom of countability;*

(ii) *G can be generated by a countable set A converging to 1 (i.e., if U is an open neighborhood of 1, then it contains a.e. element of A).*

p. 85 *Proof:* (i) $\Rightarrow$ (ii): Let

$$U_1 \supseteq U_2 \supseteq \cdots \supseteq U_i \supseteq \cdots$$

be a countable basis of open normal subgroups of G. Use induction to choose a set

$$A_i = \{\sigma_1^{(i)}, \sigma_2^{(i)}, \ldots, \sigma_{r_i}^{(i)}\} \subseteq G$$

of generators of G/U_i, so that $A_i \subseteq A_{i+1}$ and $A_{i+1} \smallsetminus A_i \subseteq U_i \quad (i = 1, 2, 3, \ldots)$. Let Γ be the (closed) subgroup of G generated by $A = \bigcup_{i=1}^{\infty} A_i$. Certainly A is countable and convergent to 1. On the other hand $\Gamma = G = \varprojlim_i G/U_i$, for the canonical projection

$$\Gamma \longrightarrow G/U_i, \qquad (i = 1, 2, 3, \ldots)$$

is an epimorphism and therefore Γ is dense in G (see Lemma 2.5).

(ii) $\Rightarrow$ (i): Let G be generated by the set $A = \{\sigma_1, \sigma_2, \sigma_3, \ldots\}$ convergent to 1.
p. 86 Let $\underline{S}$ be the set of all open normal subgroups of G. We shall show that $\underline{S}$ is countable. Let $\underline{S}_k$ denote the set of open normal subgroups of G containing $\sigma_{k+1}, \sigma_{k+2}, \ldots$. Then

$$\underline{S} = \bigcup_{k=1}^{\infty} \underline{S}_k.$$

Let H be the smallest closed normal subgroup containing $\sigma_{k+1}, \sigma_{k+2}, \ldots$. Then

$$U \in \underline{S}_k \quad \Rightarrow \quad U \text{ is open, normal in } G \text{ and } H \subseteq U \subseteq G.$$

Hence there is a 1-1 correspondence between $\underline{S}_k$ and the open, normal subgroups of G/H. Since G/H is generated by $\sigma_1, \sigma_2, \ldots, \sigma_k$, the number of open, normal subgroups

of G/H is countable (each open normal subgroup of G/H is the kernel of some epimorphism of G/H onto some finite group, and G/H being finitely generated there are only a finite number of such epimorphisms for each finite group). Thus each $\underline{S}_k$, and therefore $\underline{S}$, is countable. ∎

Proof of theorem 9.3:

p. 87 (i) ⇒ (ii): Let G be a free pro-$\underline{C}$-group on the set $\{\sigma_1, \sigma_2, \ldots\}$. Consider the embedding problem

$$\begin{array}{ccccccccc} & & & & & & G & & \\ & & & & & & \downarrow{\scriptstyle \varphi} & & \\ 1 & \longrightarrow & H'' & \longrightarrow & H & \xrightarrow[j]{} & H' & \longrightarrow & 1 \\ & & & & & & \downarrow & & \\ & & & & & & 1 & & \end{array}$$

where $H, H', H'' \in \underline{C}$. Then H' is generated by the $\varphi(\sigma_i)$'s, and there exists some k such that $\varphi(\sigma_i) = 1$ for $i > k$, since $\ker \varphi$ is open and normal. Choose $h_i \in H$, $i = 1, 2, \ldots$ satisfying the following conditions:

1) The h_i's generate H,
2) $h_i = 1$ for a.e. i,
3) $j(h_i) = \varphi(\sigma_i)$.

Define $\psi: G \longrightarrow H$ by $\psi(\sigma_i) = h_i$, $i = 1, 2, \ldots$. Clearly ψ is surjective and $j \circ \psi = \varphi$.

(ii) ⇒ (i): Let F be a free pro-$\underline{C}$-group on a countable set. By Lemma 9.4 there is a basis

$$F = F_1 \supseteq F_2 \supseteq \cdots \supseteq F_n \supseteq \cdots$$

of open, normal subgroups of F. Let

$$G = G_1 \supseteq G_2 \supseteq \cdots \supseteq G_n \supseteq \cdots$$

be a basis of open, normal subgroups of G. We shall construct bases of open, normal subgroups

$$F \supseteq F_1' \supseteq F_2' \supseteq \cdots \supseteq F_n' \supseteq \cdots ,$$

$$G \supseteq G_1' \supseteq G_2' \supseteq \cdots \supseteq G_n' \supseteq \cdots$$

of F and G respectively, such that the projective systems

$$\{F/F_i' |\ i = 1, 2, \ldots\} \quad \text{and} \quad \{G/G_i' |\ i = 1, 2, \ldots\}$$

are isomorphic. This will imply

$$F \approx \varprojlim_i F/F_i' \approx \varprojlim_i G/G_i' \approx G.$$

We proceed by induction on i. Let $F_1' = F_1 = F$, $G_1' = G_1 = G$, and assume we have found F_i', G_i' $(i = 1, 2, \ldots, n)$ such that

1) $F_i' \subseteq F_i$, $G_i' \subseteq G_i$ $(i = 1, 2, \ldots, n)$,

2) $F \supseteq F_1' \supseteq F_2' \supseteq \cdots \supseteq F_n'$,
$G \supseteq G_1' \supseteq G_2' \supseteq \cdots \supseteq G_n'$,

p. 89 3)

$$\begin{array}{ccc} F/F_i' & \xrightarrow[\approx]{} & G/G_i' \\ \downarrow & & \downarrow \\ F/F_{i-1}' & \xrightarrow[\approx]{} & G/G_{i-1}' \end{array}$$

commutes $(i = 2, 3, \ldots, n)$.

We will construct F_{n+1}' and G_{n+1}' as follows. Let $\Phi = F_n' \cap F_{n+1}$ and $\Gamma = G_n' \cap G_{n+1}$. Let $\psi: G \longrightarrow F/\Phi$ be a solution to the embedding problem for G

$$\begin{array}{ccccccc} & & & & G & & \\ & & & & \downarrow & & \\ F/\Phi & \longrightarrow & F/F_n' & \xrightarrow[\approx]{} & G/G_n' & \longrightarrow & 1, \\ & & & & \downarrow & & \\ & & & & 1 & & \end{array}$$

and let $\Delta = (\ker \psi) \cap \Gamma$. Then ψ induces a natural epimorphism $G/\Delta \longrightarrow F/\Phi$. Let $\varphi: F \longrightarrow G/\Delta$ be a solution to the embedding problem for F

$$\begin{array}{ccccc} & & F & & \\ & & \downarrow & & \\ G/\Delta & \longrightarrow & F/\Phi & \longrightarrow & 1, \end{array}$$

p. 90 and let $\Lambda = \ker \varphi$. Then $\Lambda \subseteq \Phi$ and therefore φ induces an isomorphism $F/\Lambda \longrightarrow G/\Delta$. Take $F'_{n+1} = \Lambda$ and $G'_{n+1} = \Delta$. Then $F'_{n+1} \subseteq F_{n+1}$, $G'_{n+1} \subseteq G_{n+1}$ and

$$\begin{array}{ccc} F/F'_{n+1} & \xrightarrow[\approx]{} & G/G'_{n+1} \\ \downarrow & & \downarrow \\ F/F'_n & \xrightarrow[\approx]{} & G/G'_n \end{array}$$

commutes, as desired. ∎

p. 91

CHAPTER II

COHOMOLOGY OF PROFINITE GROUPS

§1. Cohomology groups

Definition 1.1: Let G be a profinite group. A *discrete G-module* (or simply a *G-module*, if there is no danger of confusion) consists of a discrete abelian group A on which G operates continuously, i.e., a G-module is an abelian group A together with a continuous map $G \times A \longrightarrow A$, denoted by $(\sigma, a) \mapsto \sigma a$, satisfying the following conditions

(i) $(\sigma\tau)a = \sigma(\tau a)$;

(ii) $\sigma(a+b) = \sigma a + \sigma b$;

(iii) $1a = a$,

for $a, b \in A$ and $\sigma, \tau \in G$, where 1 is the identity of G.

Remark: If G is a finite group then the above definition coincides with the usual definition of G-module.

p. 92 PROPOSITION 1.2: *Let G be a profinite group and A an abelian group. Let $G \times A \longrightarrow A$ be an action of G on A satisfying conditions (i), (ii), (iii) as above. Then, the following are equivalent:*

(1) *$G \times A \longrightarrow A$ is continuous;*

(2) *For each a in A, the stabilizer of a,*

$$U_a = \{\sigma \in G |\ \sigma a = a\}$$

is an open subgroup of G;

(3) *$A = \bigcup_U A^U$, where U runs through the set of all open subgroups of G, and where*

$$A^U = \{a \in A |\ ua = a, \quad u \in U\}.$$

Proof: Trivial.

Examples of G-modules:

1) Let G be any profinite group and A any abelian group. Define an action of G on

p. 93 A by $\sigma a = a,\ \forall a \in A$ and $\forall \sigma \in G$. Then A is a G-module. This action is called the *trivial action* on A, and A a *trivial G-module.*

2) Let $N|K$ be a Galois extension of fields and $G = G_{N|K}$. If $\sigma \in G$ and $x \in N$ define $\sigma x = \sigma(x)$. Under this action the following are examples of G-modules:

a) N^* (the multiplicative group of N);

b) N^+ (the additive group of N);

c) The roots of unity in N (under multiplication).

If A and B are discrete G-modules, by a *G-homomorphism* or a *G-map* $\varphi\colon A \longrightarrow B$ we mean an abelian group homomorphism for which

$$\varphi(\sigma a) = \sigma\varphi(a), \quad \forall \sigma \in G,\ \forall a \in A.$$

The class of discrete G-modules and G-maps constitutes an abelian category that we denote by $\mathrm{Mod}(G)$.

Let G be a profinite group, and denote by G^q the cartesian product of q copies of G. For $A \in \mathrm{Mod}(G)$ and $q \geq 0$ we set

$$C^q(G, A) = \{x\colon G^{q+1} \longrightarrow A |\ x \text{ continuous and}$$

p. 94 $$x(\sigma\sigma_0, \sigma\sigma_1, \ldots, \sigma\sigma_q) = \sigma x(\sigma_0, \sigma_1, \ldots, \sigma_q)\ ; \sigma, \sigma_i \in G\}.$$

$C^q(G, A)$ is an abelian group under the obvious addition, and it is called the *group of homogeneous q-cochains.* For each $q \geq 0$ define a group homomorphism

$$\partial_{q+1}\colon C^q(G, A) \longrightarrow C^{q+1}(G, A)$$

by

$$(\partial_{q+1}x)(\sigma_0, \sigma_1, \ldots, \sigma_{q+1}) = \sum_{i=0}^{q+1}(-1)^i x(\sigma_0, \sigma_1, \ldots, \hat{\sigma}_i, \ldots, \sigma_{q+1})$$

where the symbol $\hat{}$ indicates that the corresponding coordinate has been cancelled. The maps ∂_q are called *coboundary operators.* It is easily seen that $\partial_{q+1} \circ \partial_q = 0,\ q \geq 1$, so that

$$0 \longrightarrow C^0(G, A) \xrightarrow{\partial_1} C^1(G, A) \xrightarrow{\partial_2} \cdots$$

is a cochain complex, that will be denoted by $\big(C(G,A),\partial\big)$. The q-th cohomology group of this complex will be denoted by $H^q(G,A)$, and is called the *q-th cohomology group* of G with coefficients in A. In detail,

$$H^q(G,A) = H^q\big(C(G,A),\partial\big) = Z^q(G,A)/B^q(G,A),$$

p. 95 where $Z^q(G,A) = \ker\partial_{q+1}$ (*group of q-cocycles*) and $B^q(G,A) = \mathrm{Im}\partial_q$ (*group of q-coboundaries*).

An equivalent way of describing the cohomology groups $H^q(G,A)$ could be the following. Define the group $\bar{C}^q(G,A)$ of *non-homogeneous cochains* by

$$\bar{C}^q(G,A) = \{x\colon G^q \longrightarrow A |\ x \text{ continuous}\}.$$

Consider the cochain complex $\big(\bar{C}(G,A),\bar{\partial}\big)$:

$$0 \longrightarrow \bar{C}^0(G,A) \xrightarrow{\bar{\partial}_1} \bar{C}^1(G,A) \xrightarrow{\bar{\partial}_2} \bar{C}^2(G,A) \longrightarrow \cdots$$

where the homomorphism

$$\bar{\partial}_{q+1}\colon \bar{C}^q(G,A) \longrightarrow \bar{C}^{q+1}(G,A)$$

is given by

$$\begin{aligned}(\bar{\partial}_{q+1}x)(\sigma_1,\sigma_2,\ldots,\sigma_{q+1}) =& \sigma_1 x(\sigma_2,\sigma_3,\ldots,\sigma_{q+1}) + \\ & \sum_{i=1}^{q}(-1)^i x(\sigma_1,\sigma_2,\ldots,\sigma_i\sigma_{i+1},\ldots,\sigma_{q+1}) + \\ & (-1)^{q+1}x(\sigma_1,\sigma_2,\ldots,\sigma_q).\end{aligned}$$

p. 96 Then $\big(C^q(G,A),\partial\big)$ and $\big(\bar{C}^q(G,A),\bar{\partial}\big)$ are isomorphic cochain complexes, where a pair of inverse isomorphisms

$$C(G,A) \underset{\psi_q}{\overset{\varphi_q}{\rightleftarrows}} \bar{C}(G,A)$$

is given by

$$\begin{aligned}(\varphi_q x)(\sigma_1,\sigma_2,\ldots,\sigma_q) =& x(1,\sigma_1,\sigma_1\sigma_2,\ \ldots,\ \sigma_1\sigma_2\cdots\sigma_q),\\ (\psi_q y)(\tau_0,\tau_1,\ldots,\tau_q) =& \tau_0 y(\tau_0^{-1}\tau_1,\tau_1^{-1}\tau_2,\ldots,\tau_{q-1}^{-1}\tau_q).\end{aligned}$$

Therefore

$$H^q(G,A) = H^q\big(C(G,A),\partial\big) = H^q\big(\bar{C}(G,A),\bar{\partial}\big) = \bar{Z}^q(G,A)/\bar{B}^q(G,A),$$

where $\bar{Z}^q(G,A) = \ker\bar{\partial}_{q+1}$ and $\bar{B}^q(G,A) = \mathrm{Im}\bar{\partial}_q$.

p. 97 §**2.** $H^q(G,A)$ **in low dimensions**

In low dimensions one can describe the cohomology groups as follows:

$$H^0(G,A) = \{a \in A |\ \sigma a = a,\ \sigma \in G\} = A^G,$$

i.e., the subgroup of elements of A invariant under the action of G.

$$\begin{aligned} H^1(G,A) =& Z^1(G,A)/B^1(G,A), \text{ where} \\ Z^1(G,A) =& \{x\colon G \longrightarrow A |\ x \text{ cont.}, \bar{\partial}_2 x = 0\} = \\ & \{x\colon G \longrightarrow A |\ x \text{ cont.}, x(\sigma\tau) = \sigma x(\tau) + x(\sigma), \sigma, \tau \in G\}. \\ B^1(G,A) =& \{x\colon G \longrightarrow A |\ x = \bar{\partial}_1 a, \text{ some } a \in A\} = \\ & \{x\colon G \longrightarrow A |\ x(\sigma) = \sigma a - a, \text{ some } a \in A\}. \end{aligned}$$

The elements of $Z^1(G,A)$ and $B^1(G,A)$ are called (continuous) *crossed homomorphisms* and *principal crossed homomorphisms* respectively.

p. 98 Notice that if G operates trivially on A, i.e., $\sigma a = a\ \forall \sigma \in G$ and $\forall a \in A$, then $H^1(G,A)$ is precisely the group of all continuous group homomorphisms from G to A.

Finally $H^2(G,A) = \bar{Z}^2(G,A)/\bar{B}^2(G,A)$, where

$$\begin{aligned} \bar{Z}^2(G,A) =& \{x\colon G \times G \longrightarrow A |\ x \text{ cont.}, \bar{\partial}_3 x = 0\} = \\ & \{x\colon G \times G \longrightarrow A |\ x \text{ cont. and } \sigma_1 x(\sigma_2,\sigma_3) + x(\sigma_1,\sigma_2\sigma_3) = \\ & \qquad x(\sigma_1\sigma_2,\sigma_3) + x(\sigma_1,\sigma_2),\ \sigma_1,\sigma_2,\sigma_3 \in G\}. \\ \bar{B}^2(G,A) =& \{x\colon G \times G \longrightarrow A |\ x = \bar{\partial}_2 y, \text{ some cont. } y\colon G \longrightarrow A\} = \\ & \{x\colon G \times G \longrightarrow A |\ x(\sigma_1,\sigma_2) = \sigma_1 y(\sigma_2) - y(\sigma_1\sigma_2) + y((\sigma_1), \\ & \qquad \text{for some cont. } y\colon G \longrightarrow A\}. \end{aligned}$$

The elements of $Z^2(G,A)$ are called (continuous) *factor systems.*

p. 99 §**2.** $H^2(G,A)$ **and extensions of profinite groups**

Consider a short exact sequence

$$1 \longrightarrow A \longrightarrow \hat{G} \longrightarrow G \longrightarrow 1$$

of profinite groups and continuous homomorphisms, with A abelian. Let $u\colon G \longrightarrow \hat{G}$ be a continuous section (see Prop. 3.5, Ch. I). Define $\psi\colon G \times A \longrightarrow A$ by $\psi(\sigma, a) = u_\sigma a u_\sigma^{-1}$. Clearly ψ is continuous. Assume that A is finite; then A has the discrete topology and the map ψ makes A into a G-module.

Given a profinite group G and finite G-module A, by an *extension E of A by G* we mean an exact sequence, with continuous homomorphisms,

$$E\colon \quad 0 \longrightarrow A \longrightarrow \hat{G} \longrightarrow G \longrightarrow 1 \tag{1}$$

where $\hat{G}$ is a profinite group, A and $\hat{G}$ are written additively, and the canonical action of G on A described above is precisely the given action of G on A.

p. 100 If E, E' are two extensions of A by G, we say that they are *congruent* if there exists a continuous homomorphism (necessarily a homeomorphism) $\hat{G} \longrightarrow \hat{G}'$ such that

$$\begin{array}{lccccccc} E\colon & 0 & \longrightarrow & A & \longrightarrow & \hat{G} & \longrightarrow & G \longrightarrow 1 \\ & & & \| & & \downarrow & & \| \\ E'\colon & 0 & \longrightarrow & A & \longrightarrow & \hat{G}' & \longrightarrow & G \longrightarrow 1 \end{array}$$

commutes.

Denote by $\mathcal{E}(G, A)$ the set of congruence classes of extensions of A by G.

THEOREM 3.1: *Given a profinite group G and finite G-module A, there exists a 1-1 correspondence between $\mathcal{E}(G, A)$ and $H^2(G, A)$.*

Proof: Consider the extension (1) of A by G, and let $u\colon G \longrightarrow \hat{G}$ be a continuous section. Then the action of G on A is given by

$$\sigma a = u(\sigma) + a - u(\sigma), \quad a \in A,\ \sigma \in G.$$

p. 101 Since u is a section, if $\sigma_1, \sigma_2 \in G$, then $u(\sigma_1) + u(\sigma_2)$ and $u(\sigma_1\sigma_2)$ belong to the same coset of A in $\hat{G}$. Hence there exists some $x(\sigma_1, \sigma_2) \in A$ such that $u(\sigma_1) + u(\sigma_2) = x(\sigma_1, \sigma_2) + u(\sigma_1\sigma_2)$. It is clear that $x\colon G \times G \longrightarrow A$ is a continuous map. We shall show that it is in fact a continuous factor system. Let $\sigma_1, \sigma_2, \sigma_3 \in G$; then

$$u(\sigma_1) + [u(\sigma_2) + u(\sigma_3)] = u(\sigma_1) + [x(\sigma_2, \sigma_3) + u(\sigma_2\sigma_3)] =$$

$$\sigma_1 x(\sigma_2, \sigma_3) + u(\sigma_1) + u(\sigma_2\sigma_3) = \sigma_1 x(\sigma_2, \sigma_3) + x(\sigma_1, \sigma_2\sigma_3) + u(\sigma_1\sigma_2\sigma_3),$$

and

$$[u(\sigma_1)+u(\sigma_2)]+u(\sigma_3) = [x(\sigma_1,\sigma_2)+u(\sigma_1\sigma_2)]+u(\sigma_3) = x(\sigma_1,\sigma_2)+x(\sigma_1\sigma_2,\sigma_3)+u(\sigma_1\sigma_2\sigma_3);$$

hence

$$\sigma_1 x(\sigma_2,\sigma_3)+x(\sigma_1,\sigma_2\sigma_3) = x(\sigma_1,\sigma_2)+x(\sigma_1\sigma_2,\sigma_3),$$

i.e., $x \in Z^2(G,A)$.

The definition of x depends on the choice of u. However, if $u'\colon G \longrightarrow \hat{G}$ is another
p. 102 section, and $x'\colon G\times G \longrightarrow A$ its corresponding factor system we will show that $x - x' \in \bar{B}^2(G,A)$. For if $\sigma \in G$, there exists $y(\sigma) \in A$ such that

$$u'(\sigma) = y(\sigma)+u(\sigma).$$

It is plain that $y\colon G \longrightarrow A$ is continuous. On the other hand, if $\sigma_1,\sigma_2 \in G$ we have

$$x'(\sigma_1,\sigma_2)+y(\sigma_1\sigma_2)+u(\sigma_1\sigma_2) = x'(\sigma_1,\sigma_2)+u'(\sigma_1\sigma_2) = u'(\sigma_1)+u'(\sigma_2) =$$
$$y(\sigma_1)+u(\sigma_1)+y(\sigma_2)+u(\sigma_2) = y(\sigma_1)+\sigma_1 y(\sigma_2)+u(\sigma_1)+u(\sigma_2) =$$
$$y(\sigma_1)+\sigma_1 y(\sigma_2)+x(\sigma_1,\sigma_2)+u(\sigma_1\sigma_2);$$

hence

$$x'(\sigma_1,\sigma_2)-x(\sigma_1,\sigma_2) = \sigma_1 y(\sigma_2)-y(\sigma_1\sigma_2)+y(\sigma_1) = (\partial_1 y)(\sigma_1,\sigma_2).$$

So, $x - x' \in \bar{B}^2(G,A)$, and therefore x and x' define a unique element of $H^2(G,A)$. In fact this last argument shows that if E and E' are congruent extensions of A by G, they have the same corresponding element in $H^2(G,A)$. Hence we have shown the existence of a well defined map $\mathcal{E}(G,A) \xrightarrow{\Phi} H^2(G,A)$.

p. 103 Conversely, let $x\colon G\times G \longrightarrow A$ be a continuous factor system representing an element of $H^2(G,A)$. We may assume that $x(\sigma,1) = x(1,\sigma) = 0,\ \forall\sigma \in G$. Define a profinite group $\hat{G}$ in the following manner. The elements of $\hat{G}$ are the pairs (a,σ), $a \in A,\ \sigma \in G$. We set

$$(a_1,\sigma_1)+(a_2,\sigma_2) = (a_1+\sigma_1 a_2+x(\sigma_1,\sigma_2),\sigma_1\sigma_2), \quad a_1,a_2 \in A,\ \sigma_1,\sigma_2 \in G.$$

With this definition $\hat{G}$ becomes a group (the associativity follows from x being a factor system) whose zero element is $(0,1)$, and where $-(a,\sigma) = (-\sigma^{-1}a - x(\sigma^{-1},\sigma),\sigma^{-1})$. We endow $\hat{G}$ with the product topology $A \times G$. Then $\hat{G}$ is a profinite group as one easily checks. Moreover

$$E(x): \quad 0 \longrightarrow A \xrightarrow{i} \hat{G} \xrightarrow{j} G \longrightarrow 1,$$

where i and j are the natural injection and projection, is an extension of A by G.

p. 104 The congruence class to which this extension belongs depends only on the element of $H^2(G,A)$ we started with. For, if $x + \partial f$ is another representative of that element ($f: G \longrightarrow A$, continuous and such that $f(1) = 0$) whose corresponding extension is

$$E(x+\partial f): \quad 0 \longrightarrow A \longrightarrow \hat{G}' \longrightarrow G \longrightarrow 1,$$

define a continuous homomorphism $\eta: \hat{G} \longrightarrow \hat{G}'$ by $\eta(a,\sigma) = (a - f(\sigma),\sigma)$, $a \in A$, $\sigma \in G$. Then

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A & \longrightarrow & \hat{G} & \longrightarrow & G & \longrightarrow & 1 \\ & & \| & & \downarrow{\scriptstyle \eta} & & \| & & \\ 0 & \longrightarrow & A & \longrightarrow & \hat{G}' & \longrightarrow & G & \longrightarrow & 1 \end{array}$$

commutes, and therefore $E(x)$ and $E(x+\partial f)$ are congruent. Hence we have obtained a map $\Psi: H^2(G,A) \longrightarrow \mathcal{E}(G,A)$.

One sees without difficulty that $\Phi \circ \Psi = \mathrm{id}$ and $\Psi \circ \Phi = \mathrm{id}$. This ends the proof of the theorem. ∎

p. 105 *Remark:* The above correspondence induces an abelian group structure on the set $\mathcal{E}(G,A)$. It should be noticed that the extension corresponding to the zero of $H^2(G,A)$ is the split extension, i.e., an extension (1) for which there exists a continuous section $G \longrightarrow \hat{G}$ that is a homomorphism. (All split extensions are congruent.)

p. 106 **§4. Behavior of $H^n(G,A)$**

Let $g: G \longrightarrow G'$ be a continuous homomorphism of profinite groups. Let $A \in \mathrm{Mod}(G)$, $A' \in \mathrm{Mod}(G')$, and let $f: A' \longrightarrow A$ be a group homomorphism. We say that g and f

are *compatible* maps if

$$f\big(g(\sigma)a'\big) = \sigma f(a'), \qquad \sigma \in G,\ a' \in A',$$

i.e., if f is a G-map when A' is considered as a G-module by means of the action $\sigma \cdot a' = g(\sigma)a', a' \in A',\ \sigma \in G$.

Example: Let $N \supseteq L \supseteq K$ be Galois extensions of K. Then the natural projection and injection

$$\pi\colon G_{N|K} \longrightarrow G_{L|K} \quad \text{and} \quad i\colon L^* \longrightarrow N^*$$

respectively, are easily seen to be compatible. (See example 2(a) on p. 93.)

A pair of compatible maps g, f as above, induces homomorphisms of the groups of q-cochains $(g, f)\colon \bar{C}^q(G', A') \longrightarrow \bar{C}^q(G, A),\ q \geq 0$, given by

p. 107
$$(g, f)x'\,(\sigma_1, \ldots, \sigma_q) = fx'(g(\sigma_1), \ldots, g(\sigma_q)).$$

In fact (g, f) is a map of cochain complexes, i.e.,

$$\begin{array}{ccc} \bar{C}^q(G', A') & \xrightarrow{\bar{\partial}_{q+1}} & \bar{C}^{q+1}(G', A') \\ \Big\downarrow{\scriptstyle (g,f)} & & \Big\downarrow{\scriptstyle (g,f)} \\ \bar{C}^q(G, A) & \xrightarrow{\bar{\partial}_{q+1}} & \bar{C}^{q+1}(G, A) \end{array}$$

commutes for $q \geq 0$. From this one easily defines homomorphisms

$$(g, f)\colon H^q(G', A') \longrightarrow H^q(G, A)$$

of the cohomology groups. (See [M], p. 40 for a general setting.)

Remark: The maps (g, f), that we have just constructed behave functorially in the following sense. Let $G_i,\ i = 1, 2, 3$ be profinite groups, $A_i \in \mathrm{Mod}(G_i)$, and let

$$G_1 \xrightarrow{g_1} G_2 \xrightarrow{g_2} G_3$$

p. 108 and

$$A_1 \xleftarrow{f_1} A_2 \xleftarrow{f_2} A_3$$

be continuous homomorphisms and abelian group homomorphisms respectively, such that g_1 and f_1, and g_2 and f_2 are compatible. Then g_2g_1 and f_2f_1* are compatible, and

$$(g_2g_1, f_2f_1) = (g_1, f_1) \circ (g_2, f_2).$$

Moreover, if $g_1 : G_1 \longrightarrow G_1$ and $f_1 : A_1 \longrightarrow A_1$ are identity maps so is (g_1, f_1).

In particular, for each q, $H^q(G, -)$ is a functor from the category $\mathrm{Mod}(G)$ to the category $\underline{Ab}$ of abelian groups.

Let I be a directed index set. Let $(G_\alpha, \pi_{\alpha\beta})_I$ be a projective system of profinite groups, and $(A_\alpha, \lambda_{\alpha\beta})_I$ an inductive system of abelian groups, where each A_α is a G_α-module, such that for each pair $\alpha \geq \beta$ in I, the maps

$$\pi_{\alpha\beta} : G_\alpha \longrightarrow G_\beta \qquad \text{and} \qquad \lambda_{\alpha\beta} : A_\beta \longrightarrow A_\alpha$$

p. 109 are compatible. Then for each q, we obtain in a natural way an inductive system

$$\big(H^q(G_\alpha, A_\alpha),\ \bar{\lambda}_{\alpha\beta}\big)_I.$$

Let $G = \varprojlim_I G_\alpha$ and $A = \varinjlim_I A_\alpha$; let $\pi_\alpha : G \longrightarrow G_\alpha$ and $\lambda_\alpha : A_\alpha \longrightarrow A$ be the corresponding canonical homomorphisms. Then A can be considered as a G-module in the following manner. Given $a \in A$ and $\sigma \in G$, let $\alpha \in I$ such that $a_\alpha \in A_\alpha$ and $\lambda_\alpha a_\alpha = a$; define then $\sigma a = \lambda_\alpha[(\pi_\alpha \sigma)a_\alpha]$. This is a well defined continuous action of G on A. Moreover, we have

Proposition 4.1: *For each* $q \geq 0$

$$H^q(G, A) \approx \varinjlim_I H^q(G_\alpha, A_\alpha).$$

Proof: Since $\varinjlim$ is an exact functor in the category of abelian groups one has

$$\varinjlim_I H^q(G_\alpha, A_\alpha) \approx H^q\big(\varinjlim_I \bar{C}^q(G_\alpha, A_\alpha)\big),$$

p. 110

* Error: should be f_1f_2; ditto in the following displayed equation

where the cochain complexes $\bar{C}^q(G_\alpha, A_\alpha)$ form an inductive system by means of the maps *

$$\bar{\lambda}_{\alpha\beta} = (\pi_{\alpha\beta}, \lambda_{\alpha\beta}) \colon \bar{C}^q(G_\alpha, A_\alpha) \longrightarrow \bar{C}^q(G_\beta, A_\beta), \quad \alpha \geq \beta$$

(see p. 106). Hence, to prove our assertion it will suffice to show the existence of isomorphisms

$$\varinjlim_I \bar{C}^q(G_\alpha, A_\alpha) \approx \bar{C}^q(G, A), \quad q \geq 0,$$

commuting with the coboundary maps $\bar{\partial}_q$. For each $\alpha \in I$, define

$$\varphi_\alpha \colon \bar{C}^q(G_\alpha, A_\alpha) \longrightarrow \bar{C}^q(G, A)$$

by $\varphi_\alpha(x_\alpha) = \lambda_\alpha x_\alpha \pi_\alpha$. It is plain that $\alpha \geq \beta \Rightarrow \varphi_\alpha \bar{\lambda}_{\alpha\beta} = \varphi_\beta$; so the maps φ_α induce a homomorphism

$$\varphi \colon \varinjlim_I \bar{C}^q(G_\alpha, A_\alpha) \longrightarrow \bar{C}^q(G, A).$$

p. 111 It is easily seen that φ commutes with the coboundary operators. It remains to be shown that φ is an isomorphism.

φ is injective: Let $x \in \varinjlim_I \bar{C}^q(G_\alpha, A_\alpha)$ be such that $\varphi x = 0$, and let $x_{\alpha_0} \in \bar{C}^q(G_{\alpha_0}, A_{\alpha_0})$ with $\bar{\lambda}_{\alpha_0} x_{\alpha_0} = x$. For $\alpha \geq \alpha_0$ let $x_\alpha = \bar{\lambda}_{\alpha_0\alpha} x_{\alpha_0}$. Then $0 = \varphi x = \lambda_\alpha x_\alpha \pi_\alpha$, $\alpha \geq \alpha_0$. If $\alpha \geq \alpha_0$ define

$$X_\alpha = \{\sigma_\alpha = (\sigma_{\alpha 1}, \ldots, \sigma_{\alpha q}) \in G_\alpha^q |\ x_\alpha(\sigma_\alpha) \neq 0\}.$$

We shall show that for some $\alpha \geq \alpha_0$: $X_\alpha = \emptyset$, i.e., $x_\alpha = 0$; this will imply that $x = 0$, as desired. Since x_α is continuous, G_α^q compact and A_α discrete, x_α takes only a finite number of values; hence X_α is closed and, therefore, compact. On the other

* Error: should be

$$\bar{\lambda}_{\alpha\beta} = (\pi_{\alpha\beta}, \lambda_{\alpha\beta}) \colon \bar{C}^q(G_\beta, A_\beta) \longrightarrow \bar{C}^q(G_\alpha, A_\alpha), \quad \alpha \geq \beta$$

hand $\alpha \geq \beta \geq \alpha_0$ implies $\pi_{\alpha\beta} X_\alpha \subseteq X_\beta$, for if $\sigma_\alpha \in X_\alpha$, $0 \neq x_\alpha(\sigma_\alpha) = \bar{\lambda}_{\alpha\beta} x_\beta(\sigma_\alpha) =$

p. 112 $\lambda_{\alpha\beta} x_\beta \pi_{\alpha\beta}(\sigma_\alpha)$; so $x_\beta \pi_{\alpha\beta}(\sigma_\alpha) \neq 0$; hence $\pi_{\alpha\beta}(\sigma_\alpha) \in X_\beta$. Therefore

$$\{X_\alpha, \pi_{\alpha\beta} |\ \alpha, \beta \geq \alpha_0\}$$

is a projective system of compact spaces. Clearly

$$\sigma = (\sigma_1, \ldots, \sigma_q) \in \varprojlim_{\alpha \geq \alpha_0} X_\alpha \subseteq G^q \Rightarrow (\varphi x)\sigma \neq 0.$$

Hence $\varprojlim_{\alpha \geq \alpha_0} X_\alpha = \emptyset$. Thus $X_\alpha = \emptyset$ for some $\alpha \geq \alpha_0$ ([B3], §9, Prop. 8).

φ is surjective: Let $x\colon G^q \longrightarrow A$ be continuous. We shall prove that there is a continuous map $x_\alpha\colon G_\alpha^q \longrightarrow A$ such that $x = \lambda_\alpha x_\alpha \pi_\alpha$, for some $\alpha \in I$. Notice first that x takes only a finite number of values, say

$$x(G^q) = \{a_1, \ldots, a_n\} \subseteq A.$$

p. 113 Hence $\lambda_\beta A_\beta \supseteq x(G^q)$ for some β. Also, we may choose an open normal subgroup U_1 of G such that x is constant on the cosets of U_1^q in G^q. Since the groups $\pi_\gamma^{-1} U_\gamma$, where U_γ runs through the open normal subgroups of G_γ for all γ, form a basis of open neighborhoods of 1 in G, there exists an open normal subgroup U_α of G_α with $U_1 \supseteq U = \pi_\alpha^{-1} U_\alpha$, for some α. We may assume $\alpha \geq \beta$. Then $x = \bar{x} \circ p$, where $p\colon G^q \longrightarrow G^q/U^q$ is the natural projection, and $\bar{x}\colon G^q/U^q \longrightarrow A$ is defined by $\bar{x}(\sigma U^q) = x\sigma$; moreover π_α induces an injection $\pi'_\alpha\colon G^q/U^q \longrightarrow G_\alpha^q/U_\alpha^q$. Let $\bar{x}_\alpha\colon (G/U_\alpha)^q \longrightarrow A_\alpha$ be any map such that $\lambda_\alpha \bar{x}_\alpha \pi'_\alpha = \bar{x}$. Define $x_\alpha = \bar{x}_\alpha p_\alpha$, where $p_\alpha\colon G_\alpha^q \longrightarrow G_\alpha^q/U_\alpha^q$ is the natural projection. Clearly x_α is continuous and $x = \lambda_\alpha x_\alpha \pi_\alpha$, as desired. ∎

p. 114 Corollary 4.2: *Let G be a profinite group and $A \in \mathrm{Mod}(G)$. Then*

$$H^q(G, A) = \varinjlim H^q(G/U, A^U)$$

where U runs through all open normal subgroups of G.

Proof: $G = \varprojlim G/U$ and $A = \bigcup A^U = \varinjlim A^U$. Notice G/U acts on A^U by $(gU)a = ga$, $g \in G$ and $a \in A^U$. Finally, it is plain that if $U \subseteq V$, $G/U \longrightarrow G/V$ and the inclusion $A^V \longrightarrow A^U$ are compatible maps. ∎

COROLLARY 4.3: *Let G and A be as above. Then*

$$H^q(G, A) = \varinjlim H^q(G, B)$$

where B runs through all finitely generated G-submodules.

p. 115 *Proof:*

$$A = \varinjlim B.$$

∎

Remark: If G is profinite and $A \in \mathrm{Mod}(G)$, then A is finitely generated as a G-module iff it is finitely generated as an abelian group. For, assume $a_1, \ldots, a_n$ are G-generators of A; then for each i

$$Ga_i = (G/U_i)a_i,$$

where

$$U_i = \{\sigma \in G |\ \sigma a_i = a_i\};$$

since U_i is open, G/U_i is finite (as a set) and hence $\bigcup_{i=1}^{n}(G/U_i)a_i$ is a finite set of $\mathbb{Z}$-generators of A.

PROPOSITION 4.4: *For every short exact sequence*

$$0 \longrightarrow A \xrightarrow{i} B \xrightarrow{j} C \longrightarrow 0$$

of G-modules and G-maps, there exists canonical homomorphisms (the " connecting
p. 116 *homomorphism")*

$$\delta = \delta^q \colon H^q(G, C) \longrightarrow H^{q+1}(G, A), \qquad q \geq 0$$

such that the sequences

$$0 \longrightarrow A^G \xrightarrow[i_0]{} B^G \xrightarrow[j_0]{} C^G \xrightarrow[\delta]{} H^1(G, A) \xrightarrow[i_1]{}$$
$$H^1(G, B) \xrightarrow[j_1]{} H^1(G, C) \xrightarrow[\delta]{} H^2(G, A) \xrightarrow[i_2]{} \cdots$$

is exact, where the i_q's and i_q's are induced by i and j respectively.

Proof I.: The existence of this exact sequence is well-known in the case of finite groups (see, e.g., [M]. p. 116 and p. 97). Since $\varinjlim$ is exact, the result follows from Cor. 4.2.

Proof II.: (Sketch): Consider the short exact sequence of cochain complexes induced by i and j:

$$\begin{array}{ccccccc}
 & & 0 & & 0 & & \\
 & & \downarrow & & \downarrow & & \\
\cdots & \longrightarrow & C^q(G,A) & \xrightarrow{\partial} & C^{q+1}(G,A) & \longrightarrow & \cdots \\
 & & \downarrow{\scriptstyle i} & & \downarrow{\scriptstyle i} & & \\
\cdots & \longrightarrow & C^q(G,B) & \xrightarrow{\partial} & C^{q+1}(G,B) & \longrightarrow & \cdots \\
 & & \downarrow{\scriptstyle j} & & \downarrow{\scriptstyle j} & & \\
\cdots & \longrightarrow & C^q(G,C) & \xrightarrow{\partial} & C^{q+1}(G,C) & \longrightarrow & \cdots \\
 & & \downarrow & & \downarrow & & \\
 & & 0 & & 0 & &
\end{array}$$

p. 117

Let $\bar{c}_q \in H^q(G,C)$ and $c_q \in \bar{c}_q$; then $\partial c_q = 0$. Let $b_q \in C^q(G,B)$ with $jb_q = c_q$. Then $0 = \partial j\, b_q = j\, \partial\, b_q$. Hence there exists $a_{q+1} \in C^{q+1}(G,A)$ with $i\, a_{q+1} = \partial b_q$. Clearly $\partial a_{q+1} = 0$. Define

$$\delta \bar{c}_q = \bar{a}_{q+1} \in H^{q+1}(G,A).$$

It is an easy exercise to check that δ is well defined homomorphism and that the long sequence of the theorem is exact. (Cf. [M], page 45.) ∎

p. 118 PROPOSITION 4.5: *Let*

$$\begin{array}{ccccccccc}
0 & \longrightarrow & A & \xrightarrow{i} & B & \xrightarrow{j} & C & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle f} & & \downarrow{\scriptstyle g} & & \downarrow{\scriptstyle h} & & \\
0 & \longrightarrow & A' & \xrightarrow{i'} & B' & \xrightarrow{j'} & C' & \longrightarrow & 0
\end{array}$$

be a commutative diagram of G-modules and G-homomorphisms, with exact rows. This induces a commutative diagram

$$\begin{array}{ccccccccc}
\cdots\longrightarrow & H^q(G,B) & \xrightarrow{j} & H^q(G,C) & \xrightarrow{\delta} & H^{q+1}(G,A) & \xrightarrow{i} & H^{q+1}(G,B) & \longrightarrow\cdots \\
& \downarrow{\scriptstyle \bar{g}} & & \downarrow{\scriptstyle \bar{h}} & & \downarrow{\scriptstyle \bar{f}} & & \downarrow{\scriptstyle \bar{g}} & \\
\cdots\longrightarrow & H^q(G,B') & \xrightarrow{j'} & H^q(G,C') & \xrightarrow{\delta'} & H^{q+1}(G,A') & \xrightarrow{i'} & H^{q+1}(G,B') & \longrightarrow\cdots
\end{array}$$

Proof: This follows immediately from Remark on p. 107 and the definition of δ and δ'. ∎

PROPOSITION 4.6: *Let* $A = \coprod_{i\in I} A_i$, $A_i \in \mathrm{Mod}(G)$ *(direct sum in the category* $\mathrm{Mod}(G)$*). Then*

$$H^q(G,A) \approx \coprod_{i\in I} H^q(G,A_i).$$

p. 119 *Proof:* Define

$$\varphi\colon \coprod_{i\in I} C^q(G,A_i) \longrightarrow C^q(G,A)$$

to be the lifting of the homomorphism

$$\varphi_i\colon C^q(G,A_i) \longrightarrow C^q(G,A)$$

given by

$$\varphi_i(f_i) = \rho_i \circ f_i,$$

where $\rho_i\colon A_i \longrightarrow A$ is the natural injection.

The reader will have no difficulty in checking that φ is an isomorpism which commutes with the maps ∂_q, $q \geq 0$. Thus our result. ∎

p. 120 **§5. Some Homological Algebra**

In this section we introduce some terminology and prove some general homological results. (For more detail the reader may consult, e.g., [G].) The use of this abstract language will allow us to describe in a compact manner the essential features of the cohomology groups $H^q(G,A)$. The main purpose of this section is to prove Theorem 5.10.

Definition 5.1: Let $\underline{A}$ be an abelian category. A *cohomological functor* $H = (H^q)_{q\in\mathbb{Z}}$ on $\underline{A}$ is a sequence of covariant additive functors $H^q\colon \underline{A} \longrightarrow \underline{Ab}$, where $\underline{Ab}$ is the category of abelian groups, which assigns to every short exact sequence $0 \longrightarrow A \longrightarrow B \longrightarrow C \longrightarrow 0$ in $\underline{A}$ and every $n \in \mathbb{Z}$ a connecting homomorphism $\delta = \delta^n\colon H^n(C) \longrightarrow H^{n+1}(A)$ satisfying the following conditions:

a) For every commutative diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A & \longrightarrow & B & \longrightarrow & C & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle f} & & \downarrow{\scriptstyle g} & & \downarrow{\scriptstyle h} & & \\ 0 & \longrightarrow & A' & \longrightarrow & B' & \longrightarrow & C' & \longrightarrow & 0 \end{array}$$

p. 121 in $\underline{A}$ with exact rows, the following diagram commutes for every q

$$\begin{array}{ccc} H^q(C) & \longrightarrow & H^{q+1}(A) \\ \downarrow{\scriptstyle H^q(h)} & & \downarrow{\scriptstyle H^q(f)} \\ H^q(C') & \longrightarrow & H^{q+1}(A') \end{array}$$

b) For each short exact sequence $0 \longrightarrow A \longrightarrow B \longrightarrow C \longrightarrow 0$ in $\underline{A}$, the long sequence

$$\cdots \longrightarrow H^{q-1}(C) \xrightarrow{\delta^{q-1}} H^q(A) \longrightarrow H^q(B) \longrightarrow H^q(C) \xrightarrow{\delta^q} H^{q+1}(A) \longrightarrow \cdots$$

is exact.

Definition 5.2: Let H, F be cohomological functors on $\underline{A}$. A *morphism* $\varphi\colon H \longrightarrow F$ is a family $\varphi^q\colon H^q \longrightarrow F^q$, $q \in \mathbb{Z}$, of morphisms of functors such that, for every short exact sequence $0 \longrightarrow A \longrightarrow B \longrightarrow C \longrightarrow 0$ in $\underline{A}$, the following diagram commutes:

$$\begin{array}{ccc} H^q(C) & \xrightarrow{\delta^q} & H^{q+1}(A) \\ {\scriptstyle \varphi^q(C)}\downarrow & & \downarrow{\scriptstyle \varphi^{q+1}(A)} \\ F^q(C) & \xrightarrow{\delta^q} & F^{q+1}(A), \qquad q \in \mathbb{Z}. \end{array}$$

p. 122 Corollary 5.3: *Let G be a profinite group and $A \in \mathrm{Mod}(G)$. Then*

$$H(G,-) = \{H^q(G,-)\}_{q\in\mathbb{Z}}$$

where $H^q(G,-) = 0$ if $q < 0$, is a cohomological functor on $\mathrm{Mod}(G)$.

Proof: This is the content of Prop. 4.4 and Prop. 4.5. ∎

Definition 5.4: Let H be a cohomological functor on $\underline{A}$. We say that H is *effaceable* at q by a subclass $\underline{M} \subseteq \underline{A}$ if for every $A \in \underline{A}$ there exists a monomorphism

$$\mathcal{E}: A \longrightarrow M_A, \qquad M_A \in \underline{M},$$

with $H^q(M_A) = 0$.

If H is a *positive cohomological functor*, i.e., if $H = 0$ for $q < 0$, we say that H is *effaceable* by $\underline{M}$, if for every $A \in \underline{A}$ there exists a monomorphism

$$\mathcal{E}: A \longrightarrow M_A, \qquad M_A \in \underline{M},$$

p. 123 with $H^q(M_A) = 0$ for $q > 0$.

THEOREM 5.5: *Let H, F be positive cohomological functors on $\underline{A}$. Assume H is effaceable by the class of injectives of $\underline{A}$. Suppose $\varphi^0: H^0 \longrightarrow F^0$ is a morphism of functors. Then there exists a unique morphism $\psi: H \longrightarrow F$ such that $\psi^0 = \varphi^0$.*

Proof: (Sketch)

Let $A \in \underline{A}$ and let $0 \longrightarrow A \longrightarrow M_A \longrightarrow X_A \longrightarrow 0$ be exact in $\underline{A}$ with M_A injective.

Uniqueness of ψ: Suppose $\bar{\psi}: H \longrightarrow F$ is another morphism with $\bar{\psi}^0 = \varphi^0$. Assume $\psi^{q-1} = \bar{\psi}^{q-1}$. Then from the commutativity of

$$\begin{array}{ccccccc}
\cdots \longrightarrow & H^{q-1}(X_A) & \longrightarrow & H^q(A) & \longrightarrow & 0 \\
& \downarrow & & \downarrow{\scriptstyle \psi^q(A)}\ {\scriptstyle \bar{\psi}^q(A)} & & \downarrow \\
\cdots \longrightarrow & F^{q-1}(X_A) & \longrightarrow & F^q(A) & \longrightarrow & F^q(M_A) \longrightarrow \cdots
\end{array}$$

it follows that $\psi^q(A) = \bar{\psi}^q(A), \ \forall A \in \underline{A}$: hence $\psi^q = \bar{\psi}^q$; thus $\psi = \bar{\psi}$ by induction.

p. 124 *Existence of of ψ:* Suppose the existence of morphisms $\psi^i: H^i \longrightarrow F^i$, $i = 0, 1, \ldots, q-1$, has already been shown, and that they commute with the connecting homomorphisms δ. Define $\psi^q(A): H^q(A) \longrightarrow F^q(A)$ to be the unique map making the following diagram commutative

$$\begin{array}{ccccccccc}
\cdots \longrightarrow & H^{q-1}(M_A) & \longrightarrow & H^{q-1}(X_A) & \xrightarrow{\delta} & H^q(A) & \longrightarrow & 0 \\
& \downarrow & & \downarrow{\scriptstyle \psi^{q-1}(X_A)} & & \downarrow{\scriptstyle \psi^q(A)} & & \\
\cdots \longrightarrow & F^{q-1}(M_A) & \longrightarrow & F^{q-1}(X_A) & \xrightarrow[\delta]{} & F^q(A) & \longrightarrow & F^q(M_A) \longrightarrow \cdots
\end{array}$$

Now, it is straightforward to check that ψ^q is a morphism of functors, and that ψ^0, $\psi^1, \ldots, \psi^q$ commute with the δ's. Thus by induction we construct a morphism $\psi: H \longrightarrow F$ with $\psi^0 = \varphi^0$. ∎

COROLLARY 5.6: *Let H, F, E be cohomological functors on $\underline{A}$, with H and F effaceable by (the class of) injectives. Let*

$$H^0 \xrightarrow{\varphi^0} F^0, \quad F^0 \xrightarrow{\psi^0} E^0, \quad H^0 \xrightarrow{\rho^0} E^0$$

p. 125 *be morphisms of functors, and let*

$$H \xrightarrow{\varphi} F, \quad F \xrightarrow{\psi} E, \quad H \xrightarrow{\rho} E$$

be their extensions to morphisms of cohomological functors. Then

$$\rho^0 = \psi^0 \circ \varphi^0 \qquad \Leftrightarrow \qquad \rho = \psi \circ \varphi.$$

COROLLARY 5.7: *Let H, F be effaceable by injectives, cohomological functors on $\underline{A}$. Let*

$$H^0 \xrightarrow{\varphi^0} F^0$$

be a morphism of functors, and

$$H \xrightarrow{\varphi} F$$

its corresponding extension. Then φ is an isomorphism $\Leftrightarrow$ φ^0 is an isomorphism.

PROPOSITION 5.8: *Let G be a profinite group. Then* $\mathrm{Mod}(G)$ *has enough injectives,*
p. 126 *i.e., for every $A \in \mathrm{Mod}(G)$, there exists a monomorphism $A \longrightarrow M_A$ in* $\mathrm{Mod}(G)$ *with M_A injective.*

Proof: Let G_0 be the discrete group underlying G. Let A be a discrete G-module; then obviously $A \in \mathrm{Mod}(G_0)$. It is well known that $\mathrm{Mod}(G_0)$ has enough injectives (see [M], p. 93). Let $0 \longrightarrow A \xrightarrow{\varphi} M$ be an exact sequence in $\mathrm{Mod}(G_0)$ with M injective in $\mathrm{Mod}(G_0)$. Take

$$M_A = \bigcup_U M^U$$

where U runs through all open normal subgroups of G. Clearly $M_A \in \mathrm{Mod}(G)$. Let $a \in A$, and let U be an open normal subgroup of G such that $a \in A^U$. Then $\varphi a \in M^U$. Hence $\varphi A \subseteq M_A$. Finally M_A is injective in $\mathrm{Mod}(G)$ because any diagram

$$\begin{array}{ccccc} 0 & \longrightarrow & B & \xrightarrow{\psi} & C \\ & & \zeta \downarrow & & \\ & & M_A & & \\ & & \downarrow & & \\ & & M & & \end{array}$$

where ψ, ζ are mappings in $\mathrm{Mod}(G)$ with ψ a monomorphism, can be completed to a
p. 127 commutative diagram by a G_0-map $\xi\colon C \longrightarrow M$. But since C is a G-module, $\xi C \subseteq M_A$. ∎

PROPOSITION 5.9: *Let N be a closed normal subgroup of G, and let A be an injective G-module. Then A^N is injective in* $\mathrm{Mod}(G/N)$.

Proof: Trivial. ∎

THEOREM 5.10: *Let G be profinite. Then the cohomological functor $H(G, -)$ is effaceable by the injectives of* $\mathrm{Mod}(G)$.

Proof: Let A be injective in $\mathrm{Mod}(G)$. For every open normal subgroup U of G, A^U is G/U-injective. Hence $H^q(G/U, A^U) = 0$ if $q > 0$ (see [M], p. 92). So $H^q(G, A) = \varinjlim_U H^q(G/U, A^U) = 0$. ∎

p. 128 PROPOSITION 5.11: *Let $N \subseteq G$ be profinite groups. Then $H(N, -)$ is a cohomological functor on* $\mathrm{Mod}(G)$ *which is effaceable by the injectives of* $\mathrm{Mod}(G)$.

Proof: It is obvious that $H(N, -)$ is a cohomological functor on $\mathrm{Mod}(G)$. Suppose A is an injective G-module. We shall show that $H(N, A) = 0$ if $q > 0$. Since

$$H^q(N, A) = \varinjlim_U H^q(NU/U, A^U)$$

(U open normal subgroup of G), and since A^U is G/U-injective, it will suffice to prove the following lemma.

LEMMA 5.12: *If $N \subseteq G$ are discrete groups and Q is an injective G-module, then Q is injective in* $\mathrm{Mod}(N)$.

Proof: Consider a diagram

$$\begin{array}{ccccc} 0 & \longrightarrow & A & \xrightarrow{\varphi} & B \\ & & \downarrow{\scriptstyle \psi} & & \\ & & Q & & \end{array}$$

in $\mathrm{Mod}(N)$, where φ is a monomorphism. We need an N-map $\zeta\colon B \longrightarrow Q$ such that $\zeta\varphi = \psi$.

p. 129 Construct a new diagram

$$\begin{array}{ccccc} 0 & \longrightarrow & \mathbb{Z}G \otimes_{\mathbb{Z}N} A & \xrightarrow{\bar{\varphi}} & \mathbb{Z}G \otimes_{\mathbb{Z}N} B \\ & & \downarrow{\scriptstyle \bar{\psi}} & & \\ & & Q & & \end{array}$$

of G-modules and G-maps, where $\mathbb{Z}G$ is the group ring over the integers (cf. [M], p. 104); $\mathbb{Z}G \otimes_{\mathbb{Z}N} A$ and $\mathbb{Z}G \otimes_{\mathbb{Z}N} B$ are considered as G-modules by means of the action $\sigma(r \otimes a) = \sigma r \otimes a$, $\sigma \in \mathbb{Z}G$, $a \in A$ (or $a \in B$); the G-maps $\bar{\varphi}$ and $\bar{\psi}$ are given by

$$\begin{aligned} \bar{\varphi}(r \otimes a) &= r \otimes \varphi(a), \\ \bar{\psi}(r \otimes a) &= r\psi(a), \qquad r \in \mathbb{Z}G,\ a \in A. \end{aligned}$$

Since $\mathbb{Z}G$ is free as a right N-module, $\bar{\varphi}$ is again a monomorphism. Since Q is G-injective, there exists a G-map $\bar{\zeta}\colon \mathbb{Z}G \otimes_{\mathbb{Z}N} B \longrightarrow Q$ such that $\bar{\zeta}\bar{\varphi} = \bar{\psi}$. Define $\zeta(b) = \bar{\zeta}(1 \otimes b)$. This is easily seen to be the desired N-map. ∎

p. 130 As a first application of the results obtained in this section we prove the following proposition that will be used later.

PROPOSITION 5.13: *Let G be a profinite group, $A \in \mathrm{Mod}(G)$, and $\sigma \in G$. Let $\varphi\colon G \longrightarrow G$ be the inner automorphism given by $\varphi(\tau) = \sigma\tau\sigma^{-1}$*, and $f\colon A \longrightarrow A$ the group*

* *Error: should be $\sigma^{-1}\tau\sigma$*

homomorphism defined by $f(a) = \sigma a$. *Then* φ *and* f *are compatible maps and the homomorphisms induced in the cohomology*

$$(g, f)\colon H^q(G, A) \longrightarrow H^q(G, A)$$

* *are identity maps* ($q = 0, 1, 2, \ldots$).

Proof: From the definitions of (g, f) (§4) one immediately sees that

$$(g, f)\colon H(G, -) \longrightarrow H(G, -)$$

is a morphism of cohomological functors. Hence, by Th. 5.5, it suffices to show that

$$(g, f)\colon H^0(G, -) \longrightarrow H^0(G, -)$$

p. 131 is the identity. But if $a \in H^0(G, A) = A^G$, then $(g, f)(a) = \sigma a = a$. ∎

§6. Special mappings

THE INFLATION.

Let N be a closed normal subgroup of a profinite group G, and let $A \in \mathrm{Mod}(G)$. Then G/N operates continuously on A^N by $(\sigma N)a = \sigma a$, $\sigma \in G$, $a \in A^N$; i.e., $A^N \in \mathrm{Mod}(G/N)$. It is clear that the projection $G \longrightarrow G/N$ and the inclusion $A^N \longrightarrow A$ are compatible maps. Hence (see p. 107) for each q they induce homomorphisms $\mathrm{Inf} = \mathrm{Inf}_G^{G/N}\colon H^q(G/N, A^N) \longrightarrow H^q(G, A)$ that we call *inflations*.

p. 132 More specifically:

$$\mathrm{Inf}\colon H^0(G/N, A^N) \approx A^G \longrightarrow H^0(G, A) \approx A^G$$

is the identity mapping.

Assume $q > 0$, $x \in \bar{x} \in H^q(G/N, A^N)$, i.e., $x\colon (G/N)^q \longrightarrow A^N$ (continuous) is a q-cocycle. Then $\mathrm{Inf}\,\bar{x}$ has one of its representatives a q-cocycle $y\colon G^q \longrightarrow A$ (continuous) given by

$$y(\sigma_1, \sigma_2, \ldots, \sigma_q) = x(\sigma_1 N, \sigma_2 N, \ldots, \sigma_q N).$$

---

* *Error: g should be* φ *throughout the proof.*

PROPOSITION 6.1: *Let N be a normal closed subgroup of a profinite group G. Let $f\colon A \longrightarrow B$ be a G-map. Then f induces a G/N-map $f^N\colon A^N \longrightarrow B^N$, and the diagram*

$$\begin{array}{ccc} H^q(G/N, A^N) & \xrightarrow{(\mathrm{id}\,., f^N)} & H^q(G/N, B^N) \\ \Big\downarrow{\scriptstyle \mathrm{Inf}} & & \Big\downarrow{\scriptstyle \mathrm{Inf}} \\ H^q(G, A) & \xrightarrow{(\mathrm{id}\,., f)} & H^q(G, B) \end{array}$$

p. 133 *commutes, i.e.,* Inf *is a morphism of functors $H^q(G/N, *^N)$ and $H^q(G, *)$ on* Mod(G), *for each $q \in \mathbb{Z}$.*

PROPOSITION 6.2: *If $f\colon G \longrightarrow G_1$ and $g\colon G_1 \longrightarrow G_2$ are surjective continuous homomorphisms of profinite groups, then*

$$\mathrm{Inf}_G^{G_1} \circ \mathrm{Inf}_{G_1}^{G_2} = \mathrm{Inf}_G^{G_2}\,.$$

Proof: These propositions are consequences of Remark on p. 107. ∎

PROPOSITION 6.3: *Let $0 \longrightarrow A \xrightarrow{i} B \xrightarrow{j} C \longrightarrow 0$ be an exact sequence of G-modules, and assume $0 \longrightarrow A^N \xrightarrow{i^N} B^N \xrightarrow{j^N} C^N \longrightarrow 0$ is again exact. Then*

$$\begin{array}{ccc} H^q(G/N, C^N) & \xrightarrow{\delta} & H^{q+1}(G/N, A^N) \\ \Big\downarrow{\scriptstyle \mathrm{Inf}} & & \Big\downarrow{\scriptstyle \mathrm{Inf}} \\ H^q(G, C) & \xrightarrow{\delta} & H^{q+1}(G, A) \end{array}$$

commutes for each q.

Proof: This is an easy exercise in diagram chasing. ∎

p. 134 THE RESTRICTION.

Let S be a closed subgroup of the profinite group G. For each $A \in \mathrm{Mod}(G)$, $A^G \subseteq A^S$. In fact this inclusion defines a morphism

$$H^0(G, -) \longrightarrow H^0(S, -)$$

of functors on Mod(G). By Theorems 5.5 and 5.10, this extends to a sequence of morphisms

$$\mathrm{Res} = \underset{S}{\overset{G}{\mathrm{Res}}}\colon H^q(G, -) \longrightarrow H^q(S, -), \qquad q \geq 0$$

that are called *restrictions*.

In terms of cochains these maps can be described as follows. Let $x \in \bar{x} \in H^q(G, A)$, i.e., let $x\colon G^q \longrightarrow A$ (continuous) be a q-cocycle; then a representative q-cocycle $y\colon S^q \longrightarrow A$ (continuous) of Res $x \in H^q(S, A)$ is given by

$$y(\sigma_1, \sigma_2, \ldots, \sigma_q) = x(\sigma_1, \sigma_2, \ldots, \sigma_q) \in A, \quad \sigma_1, \sigma_2, \ldots, \sigma_q \in S.$$

Notice that if $0 \longrightarrow A \longrightarrow B \longrightarrow C \longrightarrow 0$ is an exact sequence of G-modules, it is still exact when considered as a sequence of S-modules. Therefore, by the definition of Res

p. 135 we obtain a commutative diagram

$$\begin{array}{ccccccccc}
\cdots \longrightarrow & H^{q-1}(G, B) & \xrightarrow{\delta} & H^q(G, A) & \longrightarrow & H^q(G, B) & \longrightarrow & H^q(G, C) & \longrightarrow \cdots \\
& \downarrow \mathrm{Res} & & \downarrow \mathrm{Res} & & \downarrow \mathrm{Res} & & \downarrow \mathrm{Res} & \\
\cdots \longrightarrow & H^{q-1}(S, B) & \xrightarrow{\delta} & H^q(S, A) & \longrightarrow & H^q(S, B) & \longrightarrow & H^q(S, C) & \longrightarrow \cdots
\end{array}$$

with exact rows. (Cf. Theorem 5.5).

Proposition 6.4: *Let $G \supseteq S \supseteq T$ be profinite groups. Then*

$$\operatorname*{Res}_T^S \circ \operatorname*{Res}_S^G = \operatorname*{Res}_T^G .$$

Proof: By Cor. 5.6, it suffices to show this in dimension 0. If $A \in \mathrm{Mod}(G)$, it is plain that

$$(A^G \hookrightarrow A^S \hookrightarrow A^T) = (A^G \hookrightarrow A^T).$$

∎

The corestriction.

Let S be any open subgroup of a profinite group G, and let $A \in \mathrm{Mod}(G)$. Since

p. 136 S is of finite index, we can define a group homomorphism

$$N_{G|S}\colon A^S \longrightarrow A^G$$

by

$$N_{G|S}(a) = \sum \sigma a, \qquad a \in A^S, \text{ and}$$

σ runs through a set of representatives of the left cosets of S in G.

It is easily seen that in fact $N_{G|S}$ is a morphism of $H^0(S,-)$ to $H^0(G,-)$ as functors on $\mathrm{Mod}(G)$. Hence, by Proposition 5.11 and Theorem 5.5, $N_{G|S}$ extends to a unique morphism of cohomological functors

$$\mathrm{Cor} = \mathrm{Cor}_G^S \colon H(S,-) \longrightarrow H(G,-).$$

In particular for every $A \in \mathrm{Mod}(G)$ and every q, we have a natural homomorphism

$$\mathrm{Cor} = \mathrm{Cor}_G^S \colon H^q(S,A) \longrightarrow H^q(G,A)$$

that we call *corestriction*.

PROPOSITION 6.5: *Let G be a profinite group and let $T \subseteq S$ be open subgroups of G. Then*

p. 137
$$\mathrm{Cor}_G^S \circ \mathrm{Cor}_S^T = \mathrm{Cor}_G^T .$$

Proof: By Cor. 5.6, it suffices to verify this result in dimension 0. If $A \in \mathrm{Mod}(G)$

$$N_{G|S}(N_{S|T}a) = \sum_{\tau \in G/S} \tau \Big(\sum_{\sigma \in S/T} \sigma a \Big) = \sum_{\rho \in G/T} \rho a = N_{G|T}a.$$

∎

THEOREM 6.6: *Let S be an open subgroup of a profinite group G. Then*

$$\mathrm{Cor}_G^S \circ \overset{G}{\underset{S}{\mathrm{Res}}} = (G:S) \cdot \mathrm{id},$$

where id *is the identity on $H(G,-)$.*

Proof: Since both $\mathrm{Cor}_G^S \circ \mathrm{Res}_S^G$ and $(G:S)\cdot \mathrm{id}$ are endomorphisms of the cohomological functor $H(G,-)$, it suffices to prove the result on dimension 0 (Cor. 5.6). Let $A \in \mathrm{Mod}(G)$. Then if $a \in A^G$ we have

$$N_{G|S}(a) = \sum_{\sigma \in G/S} \sigma a = (G:S)a$$

as desired. ∎

p. 138 COROLLARY 6.7: *If G is a profinite group and $A \in \mathrm{Mod}(G)$, then $H^q(G, A)$ is a torsion group for $q \geq 1$. Moreover the order of any element $c \in H^q(G, A)$ divides $\#G$.*

Proof: By Corollary 4.2, every element of $H^q(G, A)$ is in the image of $H^q(G/U, A^U)$ for some open normal subgroup U of G. Hence, we may assume that G is finite and prove that $(G : 1)H^q(G, A) = 0$. By the above theorem

$$(G : 1)H^q(G, A) = \mathrm{Cor}_G^1 \circ \mathop{\mathrm{Res}}_1^G H^q(G, A) = 0$$

since obviously $H^q(1, A) = 0$ if $q \geq 1$. ∎

If G is a profinite group, $A \in \mathrm{Mod}(G)$ and p is a prime number, we will denote the p-primary component of the torsion group $H^q(G, A)$, $q \geq 1$, by $H^q(G, A)(p)$. Notice that

$$H^q(G, A) = \coprod_p H^q(G, A)(p).$$

p. 139 COROLLARY 6.8: *Let $N \subseteq G$ be profinite groups, and let p be a prime such that $p \nmid (G : N)$. Then the mapping*

$$\mathrm{Res}\colon H^q(G, A) \longrightarrow H^q(N, A), \qquad q \geq 1$$

is injective when restricted to $H^q(G, A)(p)$. If moreover N is open in G, then the mapping

$$\mathrm{Cor}\colon H^q(N, A) \longrightarrow H^q(G, A)$$

is a surjection of $H^q(N, A)(p)$ onto $H^q(G, A)(p)$.

Proof: It is clear that

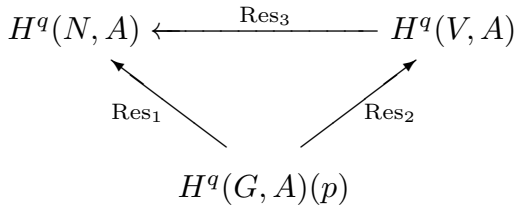
$$N = \bigcap V = \varprojlim V$$

where V runs through the set $\underline{V}$ of all open subgroups containing N. Therefore, by Proposition 4.1,

$$H^q(N, A) = \varinjlim H^q(V, A).$$

Notice that the canonical map $H^q(V,A) \longrightarrow H^q(N,A)$ is precisely the restriction map.

p. 140 For each $V \in \underline{V}$ we have a commutative diagram (see Prop. 6.4).



Suppose $\mathrm{Res}_1(c) = 0$, $c \in H^q(G,A)(p)$. Then there exists some $V \in \underline{V}$ such that $\mathrm{Res}_2(c) = 0$. So, by Theorem 6.6,

$$0 = \mathrm{Cor}_2 \circ \underset{2}{\mathrm{Res}}(c) = (G:V) \cdot c;$$

and hence $c = 0$, since $\big((G:V), p\big) = 1$. Thus Res_1 is injective. Assume now that N is open in G. Again by Theorem 6.6,

$$\mathrm{Cor}_G^N \circ \underset{N}{\overset{G}{\mathrm{Res}}}\colon H^q(G,A)(p) \longrightarrow H^q(G,A)(p)$$

is a multiplication by $(G:N)$. However since $p \nmid (G:N)$, multiplication by $(G:N)$ is an automorphism of $H^q(G,A)(p)$. Thus, the injectivity of Res_N^G on $H^q(G,A)(p)$ implies * the surjectivity of

$$\mathrm{Cor}_G^N\colon H^q(N,A)(p) \longrightarrow H^q(G,A)(p).$$

∎

p. 141 This corollary can be applied in particular to the p-Sylow groups of G. Specifically, we get

COROLLARY 6.9: *Let G be a profinite group, p a prime number and G_p a p-Sylow groups of G. Let $A \in \mathrm{Mod}(G)$. Then*

$$\mathrm{Res}\colon H^q(G,A)(p) \longrightarrow H^q(G_p,A), \qquad q \geq 1.$$

is an injection. If $(G:G_p) < \infty$,

$$\mathrm{Cor}\colon H^q(G_p,A)(p) \longrightarrow H^q(G,A)(p)$$

is a surjection.

---

* Error: instead of 'implies' should be 'and'

COROLLARY 6.10: *Let G, G_p and A be as above. If $H^q(G_p, A) = 0$ for every prime p (and a fixed $q \geq 1$), then $H^q(G, A) = 0$.*

Proof: By Cor. 6.9, $H^q(G, A)(p) = 0$ for each p. Thus

$$H^q(G, A) = \coprod_p H^q(G, A)(p) = 0.$$

∎

p. 142 §**7. Induced modules**

Let $S \subseteq G$ be profinite groups. For $A \in \mathrm{Mod}(S)$ set

$$M_G^S(A) = \{f: G \longrightarrow A |\ f \text{ continuous, } f(\sigma\tau) = \sigma f(\tau), \quad \sigma \in S,\ \tau \in G\}.$$

We define an action of G on $M_G^S(A)$ by

$$(\sigma f)(\tau) = f(\tau\sigma), \qquad \sigma, \tau \in G,\ f \in M_G^S(A).$$

PROPOSITION 7.1: *The action defined above is continuous, i.e., $M_G^S(A) \in \mathrm{Mod}(G)$.*

Proof: Let $f \in M_G^S(A)$ and let $U_f = \{\sigma \in G |\ \sigma f = f\}$. We will show that U_f is open. For each $\sigma \in G$ choose an open normal subgroup U_σ of G such that $\sigma U_\sigma \subseteq f^{-1}(f(\sigma))$. By compactness there exist a finite number of points $\sigma_1\sigma_2, \ldots, \sigma_n$ such that

$$G = \bigcup_{i=1}^n \sigma_i U_{\sigma_i}.$$

p. 143 Put $U = \bigcap_{i=1}^n U_{\sigma_i}$. Then, $\sigma \in G \Rightarrow \sigma U \subseteq f^{-1}(f(\sigma))$. So, $\sigma \in G,\ u \in U \Rightarrow (uf)(\sigma) = f(\sigma u) = f(\sigma)$. Hence $U \subseteq U_f$. Thus U_f is open. ∎

The G-module $M_G^S(A)$ is called an *induced module*. It is easy to see that $M_G^S(A)$ is an additive functor from $\mathrm{Mod}(S)$ to $\mathrm{Mod}(G)$.

PROPOSITION 7.2: *$M_G^S(A)$ is an exact functor.*

Proof: Let

$$0 \longrightarrow A \xrightarrow{i} B \xrightarrow{j} C \longrightarrow 0$$

an exact sequence in Mod(S). A standard reasoning shows that the corresponding sequence

$$0 \longrightarrow M_G^S(A) \xrightarrow{\bar{i}} M_G^S(B) \xrightarrow{\bar{j}} M_G^S(C) \longrightarrow 0$$

is exact at $M_G^S(A)$ and $M_G^S(B)$. We shall prove that $\bar{j}$ is surjective. Let $f \in M_G^S(C)$.
p. 144 Say $f(G) = \{c_1, c_2, \ldots, c_n\} \subseteq C$. Let $b_i \in B$ be such that $jb_i = c_i,\ i = 1, 2, \ldots, n$. For each i consider the open subgroup of S,

$$V_i = \{\tau \in S |\ \tau b_i = b_i\};$$

put $V = \bigcap_{i=1}^n V_i$. Let U_1 be an open normal subgroup of G such that $U_1 \cap S \subseteq V$. Since f is continuous we can find an open normal subgroup U_2 of G such that $u \in U_2,\ \sigma \in G \Rightarrow f(\sigma u) = f(\sigma)$ (see proof of Prop. 7.1). Let $U = U_1 \cap U_2$; then $(G : SU) < \infty$, say $G = \bigcup_{i=1}^t SU\sigma_i$. For each $i = 1, 2, \ldots, t$ let $\bar{b}_i \in \{b_1, b_2, \ldots, b_n\}$ be such that $j\bar{b}_i = f(\sigma_i)$. Define $g: G \longrightarrow B$ by

$$g(\tau u \sigma_i) = \tau \bar{b}_i, \qquad \tau \in S,\ u \in U.$$

Then g is well defined. It is continuous since $u \in U,\ \sigma \in G \Rightarrow g(u\sigma) = g(\sigma)$, so that $U\sigma \subseteq g^{-1}(g(\sigma))$. Finally, g is S-linear since

$$\mu \in S,\ \sigma = \tau\mu\sigma_i \in G \Rightarrow g(\mu\sigma) = g(\mu\tau u\sigma_i) = (\mu\tau)\bar{b}_i = \mu(\tau\bar{b}_i) = \mu g(\sigma), \quad u \in U,\ \tau \in S.$$

Thus $g \in M_G^S(B)$. It is plain that $\bar{j}g = j \circ g = f$. ∎

Given $S \subseteq G$ and $A \in \text{Mod}(S)$, there exists a canonical S-epimorphism

p. 145 $$\pi: M_G^S(A) \longrightarrow A$$

given by

$$\pi(f) = f(1), \qquad f \in M_G^S(A).$$

PROPOSITION 7.3: *$M_G^S(A)$ sends injectives into injectives.*

Proof: Let Q be an injective S-module. Let $i: A \longrightarrow B$ be a monomorphism of G-modules, and let $\varphi: A \longrightarrow M_G^S(Q)$ be a G-map.

$$\begin{array}{ccccc} 0 & \longrightarrow & A & \xrightarrow{\ i\ } & B \\ & & \downarrow{\scriptstyle \varphi} & \swarrow{\scriptstyle \bar{\varphi}} & \downarrow{\scriptstyle \bar{\bar{\varphi}}} \\ & & M_G^S(Q) & \xrightarrow[\ \pi\ ]{} & Q \end{array}$$

Then $\pi \circ \varphi$ is an S-map. Let $\bar{\bar{\varphi}}\colon B \longrightarrow Q$ be an S-map such that $\bar{\bar{\varphi}} \circ i = \pi \circ \varphi$. Define $\bar{\varphi}\colon B \longrightarrow M_G^S(Q)$ by

$$\bar{\varphi}_b(\sigma) = \bar{\bar{\varphi}}(\sigma b), \qquad b \in B,\ \sigma \in G.$$

Then $\bar{\varphi}$ is a G-map into $M_G^S(Q)$ and $\bar{\varphi} \circ i = \varphi$. ∎

THEOREM 7.4 (Lemma of Shapiro): *Let $S \subseteq G$ be profinite groups, and let $A \in \mathrm{Mod}(S)$. Then there exist natural isomorphisms*

$$H^q(G, M_G^S(A)) \approx H^q(S, A), \quad q \geq 0.$$

Proof: Consider the cohomological functors $H^q(S, -)$ and $H^q(G, -) \circ M_G^S$ on $\mathrm{Mod}(S)$. By Prop. 7.3 and Theorem 5.10 they are both effaceable by the injectives of $\mathrm{Mod}(S)$ Hence by Cor. 5.7 it is enough to show the existence of a natural isomorphism in dimension 0. Consider the composition

$$M_G^S(A)^G = H^0(G, M_G^S(A)) \xrightarrow{\mathrm{Res}} M_G^S(A)^S = H^0(S, M_G^S(A)) \xrightarrow{\bar{\pi}} A^S$$

where $\bar{\pi}$ is induced by π (see p. 145). This obviously is an isomorphism of the functors $M_G^S(-)^G$ and Id^S. ∎

COROLLARY 7.5: *Let G be a profinite group, A an abelian group, and $M_G(A) = M_G^1(A)$. Then $H^q(G, M_G(A)) = 0$ if $q > 0$.*

Proof: $H^q(G, M_G(A)) \approx H^q(1, A) = 0,\ \ q > 0.$ ∎

p. 147

CHAPTER III

SPECTRAL SEQUENCES AND CUP PRODUCTS

In this chapter we give a self-contained presentation of the theory of spectral sequences in a fairly general setting. The main objective is to obtain the spectral sequence of Lyndon-Hochschild-Serre (Th. 5.3) that we will use rather frequently in Chapters IV and V. In sections 6 and 7 we study another important tool, the cup product.

§1. Spectral Sequences

In this section R will denote an arbitrary ring.

Definition 1.1: A *bigraded module* E is a family $E = (E^{p,q})$, $p, q \in \mathbb{Z}$, of R-modules. A *differential* d *of* E *of bidegree* $(r, -r+1)$ is a family of R-homomorphisms

p. 148
$$d\colon E^{p,q} \longrightarrow E^{p+r,q-r+1}$$

such that $d \circ d = 0$.

Definition 1.2: A *spectral sequence* consists of a sequence $E = \{E_1, E_2, E_3, \ldots\}$, of bigraded modules $E_r = (E_r^{p,q})$, $p, q \in \mathbb{Z}$, with differentials $d_r\colon E_r \longrightarrow E_r$ of bidegree $(r, -r+1)$, such that

$$E_{r+1}^{p,q} \approx \operatorname{Ker}(d_r\colon E_r^{p,q} \longrightarrow E_r^{p+r,q-r+1})/d_r E_r^{p-r,q+r-1}.$$

The bigraded module E_2 is called the *initial term* of the spectral sequence. The bigraded module E_1 is often omitted.

It is sometimes convenient to think of the modules $E_r^{p,q}$ of a spectral sequence as arranged in layers of points.

(picture missing) !!

p. 149 LEMMA 1.3: *Each* $E_r^{p,q}$ *is a subquotient of* $E_2^{p,q}$*, i.e., there exist submodules* $L \subseteq M$ *of* $E_2^{p,q}$ *such that* $E_r^{p,q} \approx M/L$*. Moreover, for each* $p, q \in \mathbb{Z}$ *there exists a tower of modules*

$$0 = B_2^{p,q} \subseteq B_3^{p,q} \subseteq B_4^{p,q} \subseteq \cdots C_4^{p,q} \subseteq C_3^{p,q} \subseteq C_2^{p,q} = E_2^{p,q}$$

such that $E_r^{p,q} = C_r^{p,q}/B_r^{p,q}$.

Proof: It suffices to prove the second statement. Set $B_2^{p,q} = 0$ and $C_2^{p,q} = E_2^{p,q},\ p, q \in \mathbb{Z}$; then $E_2^{p,q} = C_2^{p,q}/B_2^{p,q}$. Define inductively

$$B_{r+1}^{p,q}/B_r^{p,q} = \mathrm{Im}\left(E_r^{p-r,q+r-1} = C_r^{p-r,q+r-1}/B_r^{p-r,q+r-1} \xrightarrow{d_r} E_r^{p,q} = C_r^{p,q}/B_r^{p,q}\right)$$

$$C_{r+1}^{p,q}/B_r^{p,q} = \mathrm{Ker}\left(E_r^{p,q} = C_r^{p,q}/B_r^{p,q} \xrightarrow{d_r} E_r^{p+r,q-r+1} = C_r^{p+r,q-r+1}/B_r^{p+r,q-r+1}\right);$$

then

$$B_2^{p,q} \subseteq B_r^{p,q} \subseteq C_{r+1}^{p,q} \subseteq C_r^{p,q} \subseteq C_2^{p,q},$$

and

p. 150
$$E_{r+1}^{p,q} \approx C_{r+1}^{p,q}/B_r^{p,q}/B_{r+1}^{p,q}/B_r^{p,q} \approx C_{r+1}^{p,q}/B_{r+1}^{p,q}.$$

∎

Definition 1.4: Let $C_r^{p,q}, B_r^{p,q}$ be as in Lemma 1.3. Define

$$C_\infty^{p,q} = \bigcap_r C_r^{p,q}, \qquad B_\infty^{p,q} = \bigcup_r B_r^{p,q} \qquad \text{and} \qquad E_\infty^{p,q} = C_\infty^{p,q}/B_\infty^{p,q}.$$

The bigraded module $E_\infty = (E_\infty^{p,q}),\ \ p, q \in \mathbb{Z}$, is completely determined by the spectral sequence. We shall think of the terms E_r of the spectral sequence as approximating E_∞.

Definition 1.5: (i) A *filtered module A with filtration F* consists of an R-module A together with a family of submodules F^nA of $A,\ \ n \in \mathbb{Z}$, such that

$$A \supseteq \cdots \supseteq F^nA \supseteq F^{n+1}A \supseteq \cdots\ .$$

p. 151 To each filtered module A we associate a grading in the following manner

$$G^pA = F^pA/F^{p+1}A, \quad p \in \mathbb{Z}.$$

(ii) A *filtered (single) graded* module with filtration F, consists of a family $H = (H^n)\ \ n \in \mathbb{Z}$, of filtered modules H^n.

Definition 1.6: A spectral sequence $E = (E_r)$ is said to *converge* to the filtered graded module $H = (H^n)$ with filtration F if

$$E_\infty^{p,q} \approx G^pH^{p+q} = F^pH^{p+q}/F^{p+1}H^{p+q}$$

We indicate this situation by $E_2^{p,q} \Rightarrow H^n$, or by $E \Rightarrow H$.

§2. Positive spectral sequences

Definition 2.1: A *first quadrant* or *positive* spectral sequence is one with $E_2^{p,q} = 0$ for $p < 0$ or $q < 0$.

p. 152 It is clear that if E is a positive spectral sequence then $E_r^{p,q} = 0$ for $r \geq 2$ and $p < 0$ or $q < 0$.

From now on we will assume that all spectral sequences are positive. If E is a spectral sequence and $E_2^{p,q} \Rightarrow H^n$, where $H = (H^n)$ has filtration F, we will assume that for each $n \in \mathbb{Z}$,

$$\bigcup_p F^p H^n = H^n, \qquad \text{and} \qquad \bigcap_p F^p H^n = 0.$$

Proposition 2.2: *Let E be a positive spectral sequence converging to H. Then*

(1) $E_r^{p,q} = E_\infty^{p,q}$ *if* $r > \max(p, q+1)$,

(2) $H^n = 0$ *if* $n < 0$,

(3) $F^p H^n = 0$ *if* $p > n$,

(4) H^n *if* $p \leq 0$.

Proof: (1) $E_r^{p-r,q+r-1} \xrightarrow{d_r} E_r^{p,q} \xrightarrow{d_r} E_r^{p+r,q-r+1}$. If $r > p$, $E_r^{p-r,q+r-1} = 0$; if p. 153 $r > q+1$, $E_r^{p+r,q-r+1} = 0$, So, $r > \max(p, q+1) \Rightarrow C_r^{p,q} = C_{r+1}^{p,q} = \cdots$, and $B_r^{p,q} = B_{r+1}^{p,q} = \cdots$ (see Lemma 1.3) $\Rightarrow E_r^{p,q} = E_{r+1}^{p,q} = \cdots = E_\infty^{p,q}$.

(2) $p + q = n < 0 \Rightarrow p < 0$ or $q < 0 \Rightarrow F^p H^n / F^{p+1} H^n \approx E_\infty^{p,q} = E_2^{p,q} = 0$, $p \in \mathbb{Z}$, $\Rightarrow F^p H^n = F^{p+1} H^n$, $p \in \mathbb{Z} \Rightarrow F^p H^n = 0$ (since $\bigcap_p F^p H^n = 0$) $\Rightarrow H^n = \bigcup_p F^p H^n = 0$.

(3) Let $p + q = n < 0$. Then $E_\infty^{p,q} \approx F^p H^n / F^{p+1} H^n$. Now,

$$p < 0 \text{ or } q < 0 \Rightarrow E_\infty^{p,q} = 0 \Rightarrow F^p H^n = F^{p+1} H^n.$$

So, $\cdots = F^{-2} H^n = F^{-1} H^n F^0 H^n$ and $F^{n+1} H^n = F^{n+2} H^n = F^{n+2} H^n = \cdots$. Thus $H^n = F^0 H^n$ and $F^{n+1} H^n = 0$. ∎

PROPOSITION 2.3: *For each n there is a sequence*

$$E_\infty^{n,0} \rightarrowtail H^n \twoheadrightarrow E_\infty^{0,n}$$

p. 154 *where i is an injection and j is a surjection. The sequence is exact if $n = 1$.*

Proof: ??Diagram

From the diagram it is clear that

$$E_\infty^{n,0} \xrightarrow{\approx} F^n H^n \rightarrowtail H^n \twoheadrightarrow H^n/F^1 H^n \xrightarrow{\approx} E_\infty^{0,n},$$

and so $E_\infty^{n,0} \overset{i}{\rightarrowtail} H^n \overset{j}{\twoheadrightarrow} E_\infty^{0,n}$. $\mathrm{Im}(i) = F^n H^n \subseteq F^1 H^n = \mathrm{Ker}(j)$, so $ji = 0$. If $n = 1$, $\mathrm{Im}(i) = \mathrm{Ker}(j)$, so the sequence is exact. ∎

The base terms.

The terms of the form $E_r^{p,0}$ are called *base terms*.

p. 155 PROPOSITION 2.4: *There exist epimorphisms*

$$E_2^{p,0} \twoheadrightarrow E_3^{p,0} \twoheadrightarrow \cdots \twoheadrightarrow E_{p+1}^{p,0} \xrightarrow{\approx} E_\infty^{p,0}.$$

Proof: The last arrow is an isomorphism by Prop. 2.2. Since $E_3^{p,0} \approx \mathrm{Ker}\, d_2/\,\mathrm{Im}\, d_2 = E_2^{p,0}/\,\mathrm{Im}\, d_2$, we have a surjection $E_2^{p,0} \twoheadrightarrow E_3^{p,0}$. One obtains the other maps in a similar way. ∎

Definition 2.5: Each of the maps of Proposition 2.4 and the map $E_2^{p,0} \twoheadrightarrow E_\infty^{p,0} \rightarrowtail H^p$ obtained by combining the maps of Proposition 2.3 and 2.4, are called *edge homomorphisms on the base*, and will be denoted by e_B.

The fiber terms.

The terms of the form $E_r^{0,q}$ are called the *fiber terms*.

p. 156 PROPOSITION 2.6: *There exist monomorphisms*

$$E_2^{0,q} \leftarrowtail E_3^{0,q} \leftarrowtail \cdots \leftarrowtail E_{q+2}^{0,q} \xleftarrow{\approx} E_\infty^{0,q}.$$

Proof: The last arrow is an isomorphism by Prop. 2.2. Since $E_3^{0,q} \approx \mathrm{Ker}\, d_2/\,\mathrm{Im}\, d_2 = \mathrm{Ker}\, d_2$, we have an injection $E_3^{0,q} \rightarrowtail E_2^{0,q}$. The other injections are obtained similarly.

∎

Definition 2.7: Each of the maps of the Proposition 2.6 and the map $H^q \twoheadrightarrow E_\infty^{0,q} \rightarrowtail E_2^{0,q}$ obtained by combining the maps of Proposition 2.3 and 2.6, are called *edge homomorphisms on the fiber*, and will be denoted by e_F.

Definition 2.8: For $n \geq 1$, the homomorphism $d_r \colon E_{n+1}^{0,n} \longrightarrow E_{n+1}^{n+1,0}$ is called the *transgression.*

For a fixed $n \geq 1$, we will say that the spectral sequence E satisfies $^*(n)$ if

$$E_2^{p,q} = 0 \text{ when } 1 \leq q \leq n-1 \text{ and } p+q = n$$

$$\text{or when } 1 \leq q \leq n-1 \text{ and } p+q = n+1$$

p. 157 Note that condition $^*(1)$ is vacuous.

PROPOSITION 2.9: *Under the condition* $^*(n)$

(1) *the monomorphism* $e_F \colon E_{n+1}^{0,n} \longrightarrow E_2^{0,n}$ *is an isomorphism;*

(1) *the epimorphism* $e_B \colon E_2^{n+1,0} \longrightarrow E_{n+1}^{n+1,0}$ *is an isomorphism.*

Proof: (1) $E_r^{r,n-r+1} = 0$ if $r \neq n+1$. So $\mathrm{Ker}(d_r \colon E_r^{0,n} \longrightarrow E_r^{r,n-r+1}) = E_r^{0,n}$ if $r \neq n+1$. Therefore $E_2^{0,n} \approx E_3^{0,n} \approx \cdots \approx E_{n+1}^{0,n}$.

(2) $E_r^{n-r+1,r-1} = 0$ if $r \neq n+1$. So $\mathrm{Im}(d_r \colon E_r^{n-r+1,r-1} \longrightarrow E_r^{n+1,0}) = 0$. Therefore, $E_2^{n+1,0} \approx E_3^{n+1,0} \approx \cdots \approx E_{n+1}^{n+1,0}$. ∎

By the above Proposition, we can define a map

$$E_2^{0,n} \xrightarrow{e_F^{-1}} E_{n+1}^{0,n} \xrightarrow{d_r} E_{n+1}^{n+1,0} \xrightarrow{e_B^{-1}} E_2^{n+1,0}$$

p. 158 if condition $^*(n)$ is satisfied. This homomorphism will also be called *transgression* and denoted tr.

THEOREM 2.10: *Let* $E = (E_r^{p,q})$ *be a positive spectral sequence converging to* $H = (H^n)$, *and satisfying condition* $^*(n)$. *Then there exists a five term exact sequence*

$$0 \longrightarrow E_2^{n,0} \xrightarrow{e_B} H^n \xrightarrow{e_F} E_2^{0,n} \xrightarrow{\mathrm{tr}} E_2^{n+1,0} \xrightarrow{e_B} H^{n+1}.$$

Proof: First notice that

$$\mathrm{Ker}(E_r^{p,0} \xrightarrow{e_B} E_{r+1}^{p,0}) = \mathrm{Im}(E_r^{p-r,r-1} \xrightarrow{d_r} E_r^{p,0}) \tag{1}$$

$$\mathrm{Im}(E_{r+1}^{0,q} \xrightarrow{e_F} E_r^{0,q}) = \mathrm{Ker}(E_r^{0,q} \xrightarrow{d_r} E_r^{r,q-r+1}) \tag{2}$$

We now prove the exactness at each point.

I. EXACTNESS AT $E_2^{n,0}$: It is enough to prove that each $E_r^{n,0} \longrightarrow E_{r+1}^{n,0}$ is an injection, $(r = 2, 3, \ldots, n)$. But this follows from (1) since $E^{p-r,r-1} = 0$, $(r = 2, 3, \ldots, n)$.

II. EXACTNESS AT H^n:

p. 159 $$\operatorname{Im} e_B = \operatorname{Im}(E_2^{n,0} \longrightarrow H^n) = \operatorname{Im}(E_\infty^{n,0} \longrightarrow H^n) = F^n H^n;$$

and

$$\operatorname{Ker} e_F = \operatorname{Ker}(H^n \longrightarrow E_2^{0,0}) = \operatorname{Ker}(H^n \longrightarrow E_\infty^{0,0}) = F^1 H^n.$$

But, by condition $^*(n)$,

$$n = p + q,\ 1 \leq p \leq n-1 \Rightarrow 0 = E_\infty^{p,q} = F^p H^n / F^{p+1} H^n \Rightarrow F^p H^n = F^{p+1} H^n.$$

Hence $F^1 H^n = F^n H^n$. Thus $\operatorname{Im} e_B = \operatorname{Ker} e_F$.

III. EXACTNESS AT $E_2^{0,n}$: By Proposition 2.9 and the definition of tr we have

$$\operatorname{Im} e_F = \operatorname{Im}(H^n \longrightarrow E_{n+1}^{0,n}) = \operatorname{Im}(E_{n+2}^{0,n} \longrightarrow E_{n+1}^{0,n})$$

and

$$\operatorname{Ker} tr = \operatorname{Ker}(E_{n+1}^{0,n} \longrightarrow E_{n+1}^{n+1,0}).$$

Thus $\operatorname{Im} e_F = \operatorname{Ker} \mathrm{tr}$.

p. 160 IV. EXACTNESS AT $E_2^{n+1,0}$: Analogously,

$$\operatorname{Im} \mathrm{tr} = \operatorname{Im}(E_{n+1}^{0,n} \longrightarrow E_{n+1}^{n+1,0}),$$

and

$$\operatorname{Ker} e_B = \operatorname{Ker}(E_{n+1}^{n+1,0} \longrightarrow H^{n+1}) = \operatorname{Ker}(E_{n+1}^{n+1,0} \longrightarrow E_{n+1}^{n+1,0}).$$

Thus $\operatorname{Im} \mathrm{tr} = \operatorname{Ker} e_B$. ∎

Remarks: 1) Since condition $^*(1)$ is vacuous, there always exists a five term exact sequence

$$0 \longrightarrow E_2^{1,0} \xrightarrow{e_B} H^1 \xrightarrow{e_F} E_2^{0,1} \xrightarrow{\mathrm{tr}} E_2^{2,0} \xrightarrow{e_B} H^2.$$

2) Condition $^*(n)$ is satisfied if, for instance, $E_2^{p,q} = 0$ for $1 \leq q \leq n-1$.

p. 161 §**3. Spectral sequence of a filtration**

Let

$$X = (X, \partial) = \quad \cdots \longrightarrow X^{n-1} \xrightarrow{\partial} X^n \longrightarrow X^{n+1} \longrightarrow \cdots$$

be a complex of R-modules. We say that X *is filtered* if each X^n has a filtration F compatible with the ∂, i.e., for each p, $\partial F^p X^n \subseteq F^p X^{n+1}$.

Assume that X is a filtered complex.

$$\begin{array}{lll} X^{n-1} & \supseteq \cdots \supseteq & F^p X^{n-1} \quad \supseteq \cdots \\ \downarrow & & \downarrow \\ X^n & \supseteq \cdots \supseteq & F^p X^n \quad \supseteq \cdots \\ \downarrow & & \downarrow \\ X^{n+1} & \supseteq \cdots \supseteq & F^p X^{n+1} \quad \supseteq \cdots \end{array}$$

Let $p + q = n$ and $r \in \mathbb{Z}$. Set

$$Z_r^{p,q} = \{a \in F^p X^n |\ \partial a \in F^{p+r} X^{n+1}\},$$
$$B_r^{p,q} = \partial Z_{r-1}^{p-r+1,q+r-2} = \partial F^{p-r+1} X^{n-1} \cap F^p X^n$$

and

p. 162
$$E_r^{p,q} = Z_r^{p,q}/(B_r^{p,q} + Z_{r-1}^{p+1,q-1}). \tag{1}$$

Since

$$\partial Z_r^{p,q} \subseteq Z_r^{p+r,q-r+1},$$

and

$$\partial(B_r^{p,q} + Z_{r-1}^{p+1,q-1}) = \partial Z_{r-1}^{p+1,q-1} = B_r^{p+r,q-r+1},$$

we have that the map ∂ induces homomorphisms

$$d_r \colon E_r^{p,q} \longrightarrow E_r^{p+r,q-r+1}, \tag{2}$$

with $d_r \circ d_r = 0$.

Moreover, one easily checks that

$$\mathrm{Ker}(E_r^{p,q} \xrightarrow{d_r} E_r^{p+r,q-r+1}) = (Z_{r+1}^{p,q} + Z_{r-1}^{p+1,q-1})/(B_r^{p,q} + Z_{r-1}^{p+1,q-1}),$$

and

p. 163
$$\mathrm{Im}(E_r^{p-r,q+r-1} \xrightarrow{d_r} E_r^{p,q}) = (B_{r+1}^{p,q} + Z_{r-1}^{p+1,q-1})/(B_r^{p,q} + Z_{r-1}^{p+1,q-1}).$$

Hence

$$\operatorname{Ker} d_r / \operatorname{Im} d_r \approx (Z_{r+1}^{p,q} + Z_{r-1}^{p+1,q-1})/(B_{r+1}^{p,q} + Z_{r-1}^{p+1,q-1}) \approx$$
$$Z_{r+1}^{p,q}/(B_{r+1}^{p,q} + Z_{r-1}^{p+1,q-1}) \approx E_{r+1}^{p,q}.$$

Thus we have proved the first part of the following

THEOREM 3.1: *Let (X, ∂) be a filtered complex. Then*

(i) *There exists a spectral sequence E, where $E_r^{p,q}$ is given by (1).*

(ii) *Assume, in addition that the filtration F of (X, ∂) is bounded, i.e., for each n there are integers $s = s(n) < t = t(n)$ with $F^s X^n = X^n$ and $F^t X^n = 0$. Then E converges to the graded module $H(X)$ (the cohomology groups of X) with a suitable filtration.*

p. 164 *Proof:* (ii) Consider the filtration of $H^n(X)$ induced by F, i.e., $F^p\big(H^n(X)\big)$ is the image of $H^n(F^p X)$ under the injection $F^p X \longrightarrow X$. To describe $F^p H^n(X)/F^{p+1} H^n(X)$, write

$$Z_\infty^{p,q} = \{a \in F^p X^n \mid \partial a = 0\}, \qquad \text{and}$$
$$B_\infty^{p,q} = \partial X^{n-1} \cap F^p X^n \qquad (p+q=n).$$

Then,

$$F^p H^n(X) \approx (Z_\infty^{p,q} + \partial X^{n-1})/\partial X^{n-1}.$$

So

$$F^p H^n(X)/F^{p+1} H^n(X) \approx (Z_\infty^{p,q} + \partial X^{n-1})/(Z_\infty^{p+1,q-1} + \partial X^{n-1}) \approx$$
$$Z_\infty^{p,q}/[(Z_\infty^{p+1,q-1} + \partial X^{n-1}) \cap Z_\infty^{p,q}] \approx Z_\infty^{p,q}/(Z_\infty^{p+1,q-1} + B_\infty^{p,q}),$$

by Noether isomorphism theorem.

Since the filtration of (X, ∂) is bounded, it is clear that

$$Z_r^{p,q} \approx Z_\infty^{p,q}$$

and

p. 165
$$B_r^{p,q} \approx B_\infty^{p,q}$$

for r large enough. Hence

$$F^pH^n(X)/F^{p+1}H^n(X) \approx E_r^{p,q}$$

for r large enough.

Finally, it is immediate that the boundedness of the filtration of (X, ∂) implies that $E_r^{p,q} \approx E_\infty^{p,q}$ for r large enough. Thus $E \Rightarrow H(X)$. ∎

§4. The spectral sequence of a double complex

A *double complex* is a family $K = (K^{p,q})$, $p, q \in \mathbb{Z}$ of R-modules together with differentials

$$\partial' \colon K^{p,q} \longrightarrow K^{p+1,q}, \partial'' \colon K^{p,q} \longrightarrow K^{p,q+1},$$

such that $\partial'\partial' = 0$, $\partial''\partial'' = 0$ and $\partial'\partial'' + \partial''\partial' = 0$.

p. 166 (picture missing)

From K we define a complex $(X, \partial) = X = \mathrm{Tot}(K)$, the *total complex* of K, by $X^n = \coprod_{p+q=n} K^{p,q}$ and where $\partial \colon X^n \longrightarrow X^{n+1}$ is $\partial = \partial' + \partial''$. Then (X, ∂) is obviously a complex, for

$$\partial\partial = \partial'\partial' + \partial'\partial'' + \partial''\partial' + \partial''\partial'' = 0.$$

Now we will use the fact that X is defined from a double complex to obtain in a canonical way two filtrations of X.

The *first filtration* $'F$ of X is given by

$$'F^pX^n = \coprod_{\substack{x+y=n \\ x \geq p}} K^{x,y}.$$

p. 167 The *second filtration* $''F$ of X is defined by

$$''F^qX^n = \coprod_{\substack{x+y=n \\ y \geq q}} K^{x,y}.$$

Using these filtrations we can construct corresponding spectral sequences $'E = ('E_r^{p,q})$ and $''E = (''E_r^{p,q})$ called the *first* and *second spectral sequences* of the double

complex K (see §3). Now assume the double complex K is positive, i.e., $K^{p,q} = 0$ if $p < 0$ or $q < 0$. Then both the first and second filtration are bounded. In fact

$$X^n = {}'F^0 X^n \supseteq {}'F^1 X^n \supseteq \cdots \supseteq {}'F^{n+1} X^n = 0$$

and

$$X^n = {}''F^0 X^n \supseteq {}''F^1 X^n \supseteq \cdots \supseteq {}''F^{n+1} X^n = 0.$$

So, according to Theorem 3.1 there exist corresponding spectral sequences ${}'E = ({}'E_r^{p,q})$ and ${}''E = ({}''E_r^{p,q})$ (the first and the second spectral sequences of K) converging both of
p. 168 them to $H(X)$ with the induced filtrations. Now we wish to specify what the $E_1^{p,q}$ and $E_2^{p,q}$ terms of these spectral sequences are. We have

$${}'Z_1^{p,q} = \{a \in {}'F^p X^n |\ \partial a \in {}'F^{p+1} X^{n+1}\} \approx \operatorname{Ker}(K^{p,q} \xrightarrow{\partial''} K^{p,q+1}) \oplus {}'F^{p+1} X^n;$$
$${}'B_1^{p,q} + {}'Z_1^{p+1,q-1} \approx \partial' F^p X^{n-1} + {}'F^{p+1} X^n \approx \operatorname{Im}(K^{p,q-1} \xrightarrow{\partial''} K^{p,q}) \oplus {}'F^{p+1} X^n;$$

hence

$${}'E_1^{p,q} \approx \operatorname{Ker}(K^{p,q} \xrightarrow{\partial''} K^{p,q+1}) / \operatorname{Im}(K^{p,q-1} \xrightarrow{\partial''} K^{p,q}) \approx$$
$$H^q(\cdots K^{p,q-1} \longrightarrow K^{p,q} \longrightarrow K^{p,q+1} \longrightarrow \cdots) \approx H^q(K^{p,\cdot})$$

The mapping $d_1 : {}'E_1^{p,q} \longrightarrow E_1^{p+1,q}$ is induced by ∂', so that

$${}''E_2^{p,q} \approx H^p(H^q(K^{i,\cdot}), \partial') = {}'H^p({}''H^q(K)),$$

p. 169 where ${}''H$ indicates that we are taking the homology of a vertical complex $K^{i,\cdot}$, and ${}'H$ that we are taking the homology of the horizontal complex of homology groups induced by ∂'.

In a similar manner we obtain for the second spectral sequence

$${}''E_1^{p,q} \approx H^q(\cdots K^{q-1,p} \longrightarrow K^{q,p} \longrightarrow K^{q+1,p} \longrightarrow \cdots) \approx H^q(K^{\cdot,p}),$$

and

$${}''E_2^{p,q} \approx H^p(H^q(K^{\cdot,i}), \partial'') = {}''H^p({}'H^q(K)).$$

We collect our results in the following

THEOREM 4.1: *Let $K = (K^{p,q})$ be a positive double complex. Then there is a "first spectral sequence" $'E = ('E_r^{p,q})$ canonically associated to K such that*

i) $'E_2^{p,q} \approx {}'H^p({}''H^q(K))$,

ii) $'E_2^{p,q} \Rightarrow H^n(\operatorname{Tot} K)$;

p. 170 *and there is a "second spectral sequence" $''E = (''E_r^{p,q})$ canonically associated to K such that*

i) $''E_2^{p,q} \approx {}''H^p({}'H^q(K))$,

ii) $''E_2^{p,q} \Rightarrow H^n(\operatorname{Tot} K)$.

§5. The Lyndon-Hochschild-Serre spectral sequence

Now we wish to apply our results on spectral sequences to a concrete case, namely profinite groups.

Let G be a profinite group, N a closed normal subgroup of G and let $A \in \operatorname{Mod}(G)$. We recall that $H^q(G, A)$ is defined as the q-th cohomology group of the chain complex $\big(C(G, A), \partial\big)$ of homogeneous cochains (cf. §1, Ch. II). Now define

$$C_N^q(G, A) = \{x\colon G^{q+1} \longrightarrow A \mid x \text{ continuous}, x(\sigma\sigma_0, \ldots, \sigma\sigma_q) = \sigma x(\sigma_0, \ldots, \sigma_q), \\ \sigma \in N,\ \sigma_0, \ldots, \sigma_q \in G\},$$

and define

$$\partial\colon C_N^q(G, A) \longrightarrow C_N^{q+1}(G, A)$$

by

$$\partial x(\sigma_0, \ldots, \sigma_{q+1}) = \sum_{i=0}^{q+1} (-1)^i x(\sigma_0, \ldots, \hat{\sigma}_i, \ldots, \sigma_{q+1}).$$

p. 171

Then $\partial \circ \partial = 0$, so that $\big(C_N^q(G, A), \partial\big)$ is a complex.

LEMMA 5.1: $H^q(N, A) \approx H^q\big(C_N^q(G, A), \partial\big)$.

Proof: By Theorem 7.4, Ch. II, it suffices to show that there are morphisms of complexes

$$\big(C_N(G, A), \partial\big) \underset{\Psi}{\overset{\Phi}{\rightleftarrows}} \big(C(G, M_G^N(A)), \partial\big)$$

such that $\Phi\circ\Psi$ and $\Psi\circ\Phi$ are identity maps (i.e., that the two complexes are isomorphic). Define

$$(\Phi x)(\sigma_0,\ldots,\sigma_q)(\sigma) = x(\sigma\sigma_0,\ldots,\sigma\sigma_q);$$

$$(\Psi y)(\sigma_0,\ldots,\sigma_q) = y(\sigma_0,\ldots,\sigma_q)(1).$$

Then it is easily checked that Φ, Ψ are inverse isomorphisms. ∎

p. 172 We consider each $C_N^q(G,A)$ as a G/N-module by means of the following action of G/N on $C_N^q(G,A)$. Let

$$\sigma \in G \qquad \text{and} \qquad x \in C_N^q(G,A)$$

then

$$x^\sigma : G^{q+1} \longrightarrow A$$

is defined by

$$x^\sigma(\sigma_0,\ldots,\sigma_q) = \sigma x(\sigma^{-1}\sigma_0,\ldots,\sigma^{-1}\sigma_q).$$

It is easily seen that $x^\sigma \in C_N^q(G,A)$ and that $C_N^q(G,A) \in \mathrm{Mod}(G/N)$ under this action. Moreover since

$$\partial x^\sigma = (\partial x)^\sigma$$

the groups $H_N^q(G,A)$ are also G/N-modules.

Remark: In terms of non-homogeneous cochains the action of G/N on $H^q(N,A)$ is given by

p. 173 $$x^\sigma(\sigma_1,\ldots,\sigma_q) = \sigma x(\sigma^{-1}\sigma_1\sigma,\ldots,\sigma^{-1}\sigma_q\sigma).$$

Now, define a double complex $\big(K^{p,q}, \partial', \partial''\big)$ by

$$K^{p,q} = C^p\big(G/N, C_N^q(G,A)\big)$$

and where

$$\partial' : C^p\big(G/N, C_N^q(G,A)\big) \longrightarrow C^{p+1}\big(G/N, C_N^q(G,A)\big)$$

is induced by

$$\partial : C^p(G/N,-) \longrightarrow C^{p+1}(G/N,-)$$

and

$$\partial'' : C^p\big(G/N, C_N^q(G,A)\big) \longrightarrow C^p\big(G/N, C_N^{q+1}(G,A)\big)$$

is induced by

$$(-1)^p\partial : C_N^q(G,-) \longrightarrow C_N^{q+1}(G,-).$$

p. 174 Clearly $\partial' \circ \partial' = 0$, $\partial'' \circ \partial'' = 0$ and $\partial' \circ \partial' + \partial'' \circ \partial'' = 0$.

LEMMA 5.2: $H^q\big(G/N, C_N^p(G,A)\big) = 0$ *if* $q > 0$.

Proof: Consider $x \in C^q\big(G/N, C_N^p(G,A)\big)$ with $\partial x = 0$. We shall construct $y \in C^{q-1}\big(G/N, C_N^p(G,A)\big)$ with $\partial y = x$. If $\sigma \in G$, denote by $\bar{\sigma}$ its corresponding coset in G/N. Define

$$y(\bar{\sigma}_0, \ldots, \bar{\sigma}_{q-1})(\tau_0, \ldots, \tau_p) = x(\bar{\sigma}_0, \ldots, \bar{\sigma}_{q-1}, \bar{\tau}_0)(\tau_0, \ldots, \tau_p),\ \sigma_i, \tau_j \in G.$$

Since $\partial x = 0$, by expanding $\partial x(\bar{\sigma}_0, \ldots, \bar{\sigma}_q, \bar{\tau}_0)$ one immediately sees that $\partial y = x$. ∎

THEOREM 5.3 (Lyndon-Hochschild-Serre): *Let N be a normal closed subgroup of a profinite group G, and let $A \in \mathrm{Mod}(G)$. Then there exists a spectral sequence $E = (E_r^{p,q})$ such that*

$$E_2^{p,q} \approx H^p\big(G/N, H^q(N,A)\big)$$

p. 175 *and*

$$E_2^{p,q} \Rightarrow H^n(G,A).$$

Proof: We shall show that E is the first spectral sequence of the double complex

$$K^{p,q} = \Big(C^p\big(G/N, C_N^q(G,A)\big), \partial', \partial''\Big).$$

We will make use of the second spectral sequence of this double complex to show that E converges to $H^n(G,A)$.

Using the results in §4 we have

$${}'E_1^{p,q} \approx H^q(K^{p,\cdot}) = H^q\Big(C^p\big(G/N, C_N^{\cdot}(G,A)\big), \partial''\Big).$$

And since $C^p\big(G/N, -\big)$ is an exact functor, we obtain

$${}'E_1^{p,q} \approx C^p\big(G/N, H^q(N,A)\big).$$

From this we get

p. 176
$$'E_2^{p,q} \approx H^p\big(G/N, H^q(N,A)\big).$$

This spectral sequence converges to $H^n(\mathrm{Tot}\, K)$ as we saw in Theorem 4.1. To compute $H^n(\mathrm{Tot}\, K)$, we consider the second spectral sequence of K. We have

$$''E_1^{p,q} \approx H^q(K^{\cdot,p}) = H^q\big(G/N, C_N^p(G,A)\big).$$

By Lemma 5.2, $''E_1^{p,q} = 0$ for $q > 0$. Hence the the second spectral sequence of K collapses, i.e., $''E_r^{p,q} = 0$ for $q > 0$ and $1 \le r \le \infty$. Since

$$''F^p H^n(\mathrm{Tot}\, K)/''F^{p+1} H^n(\mathrm{Tot}\, K) = ''E_\infty^{p,q} = 0$$

if $p + q = n$, $q > 0$, we have

$$''E_\infty^{n,0} \approx ''F^n H^n(\mathrm{Tot}\, K) \approx ''F^{n-1} H^n(\mathrm{Tot}\, K) \approx \cdots \approx H^n(\mathrm{Tot}\, K).$$

On the other hand $''E_2^{n,0} \approx ''E_\infty^{n,0}$. Thus

$$H^n(\mathrm{Tot}\, K) \approx ''E_2^{n,0} \approx H^n\big(H^0(K^{\cdot,i}), \partial''\big) \approx H^n\Big(H^0\big(G/N, C_N^{\cdot}(G,A)\big), \partial''\Big) \approx$$

p. 177
$$H^n\big(C_N^{\cdot}(G,A)^{G/N}, \partial\big) \approx H^n\big(C^{\cdot}(G,A), \partial\big) \approx H^n(G,A).$$

∎

Corollary 5.4: *Let G, N and A be as above. Assume $H^q(N,A) = 0$ for $0 < q < n$. Then we obtain a 5-term exact sequence*

$$0 \longrightarrow H^n(G/N, A^N) \xrightarrow{\mathrm{Inf}} H^n(G,A) \xrightarrow{\mathrm{Res}} H^n(N,A)^{G/N} \xrightarrow{\mathrm{tr}}$$
$$H^{n+1}(G/N, A^N) \xrightarrow{\mathrm{Inf}} H^{n+1}(G,A).$$

Proof: It follows from Theorem 2.10 applied to Lyndon-Hochschild-Serre spectral sequence. ∎

Corollary 5.5: *Let N be a normal closed subgroup of a profinite group G, and $A \in \mathrm{Mod}(G)$. Assume $\big(\#N, (G:N)\big) = 1$. Then, for each $n \ge 1$ there exists a split exact sequence*

$$0 \longrightarrow H^n(G/N, A^N) \longrightarrow H^n(G,A) \longrightarrow H^n(N,A)^{G/N} \longrightarrow 0.$$

p. 178 *Proof:* Let $\#N = h$, $(G : N) = t$. Then by Cor. 6.7, Ch. II, $h\,E_2^{p,q} = t\,E_2^{p,q} = 0$, $p, q > 0$ where $E_2^{p,q}$ is as in Theorem 5.3. But, the condition of Theorem 2.10 being satisfied, we obtain, for each n, an exact sequence as in Cor. 5.4. However in this case each transgression map tr is zero if $n \geq 1$. For clearly $h \cdot \mathrm{Im}(tr) = 0$ since $\mathrm{Im}(tr)$ is the homomorphic image of $H^n(N, A)^{G/N}$, and $t \cdot \mathrm{Im}(tr) = 0$ since $\mathrm{Im}(tr)$ is a subgroup of $H^{n+1}(N, A)^{G/N}$; and so $\mathrm{Im}(tr) = 0$. Thus we obtain a short exact sequence

$$0 \longrightarrow H^n(G/N, A^N) \longrightarrow H^n(G, A) \longrightarrow H^n(N, A)^{G/N} \longrightarrow 0.$$

This sequence splits since $t \cdot H^n(G/N, A^N) = 0$, $h \cdot H^n(G/N, A^N) = 0$ and $(t, h) = 1$. ∎

§6. Cup products

Let G be a profinite group and $A, B \in \mathrm{Mod}(G)$. Consider the tensor product over the
p. 179 integers $A \otimes_{\mathbb{Z}} B$, and define an action of G on $A \otimes_{\mathbb{Z}} B$ by $\sigma(a \otimes b) = \sigma a \otimes \sigma b$. Under this action $A \otimes_{\mathbb{Z}} B$ becomes a discrete G-module, for obviously

$$A \otimes_{\mathbb{Z}} B = \bigcup_U (A \otimes_{\mathbb{Z}} B)^U,$$

where U runs through the set of all open subgroups of G.

For the remainder of this chapter we write $A \otimes B$ instead of $A \otimes_{\mathbb{Z}} B$.

Definition and Theorem 6.1: *Let G be a profinite group. Then there is a unique family of $\mathbb{Z}$-linear maps, called cup-products,*

$$H^p(G, A) \times H^q(G, B) \longrightarrow H^{p+q}(G, A \otimes B),$$

denoted $(a, b) \mapsto a \cup b$, defined for every pair (p, q) of non-negative integers and every pair of discrete G-modules A, B, satisfying the following properties:

p. 180 (i) *These maps are morphisms of functors when we consider both members as covariant bifunctors on (A, B);*

(ii) *For $p = q = 0$, the map*

$$A^G \times B^G \longrightarrow (A \otimes B)^G$$

is given by $(a, b) \mapsto a \otimes b$;

(iii) *Let* $B \in \mathrm{Mod}(G)$. *If*

$$0 \longrightarrow A \longrightarrow A' \longrightarrow A'' \longrightarrow 0$$

is an exact sequence in $\mathrm{Mod}(G)$ *and if*

$$0 \longrightarrow A \otimes B \longrightarrow A' \otimes B \longrightarrow A'' \otimes B \longrightarrow 0$$

is also exact, then the diagram

$$\begin{array}{ccc} H^p(G, A'') \times H^q(G, B) & \xrightarrow{(\delta,1)} & H^{p+1}(G, A) \times H^q(G, B) \\ \downarrow \cup & & \downarrow \cup \\ H^{p+q}(G, A'' \otimes B) & \xrightarrow{\quad\delta\quad} & H^{p+q+1}(G, A \otimes B) \end{array}$$

p. 181

commutes, where δ *denotes the connecting homomorphism corresponding to the above exact sequence; i.e., if* $a'' \in H^p(G, A'')$ *and* $b \in H^q(G, B)$ *then*

$$\delta(a'' \cup b) = \delta a'' \cup b;$$

(iv) *Let* $A \in \mathrm{Mod}(G)$. *If*

$$0 \longrightarrow B \longrightarrow B' \longrightarrow B'' \longrightarrow 0$$

is an exact sequence in $\mathrm{Mod}(G)$ *and if*

$$0 \longrightarrow A \otimes B \longrightarrow A \otimes B' \longrightarrow A \otimes B'' \longrightarrow 0$$

is also exact, then the diagram

$$\begin{array}{ccc} H^p(G, A) \times H^q(G, B'') & \xrightarrow{(1,\delta)} & H^p(G, A) \times H^{q+1}(G, B) \\ \downarrow & & \downarrow \\ H^{p+q}(G, A \otimes B'') & \xrightarrow{\quad(-1)^p\delta\quad} & H^{p+q+1}(G, A \otimes B) \end{array}$$

p. 182

commutes, i.e., if $a \in H^p(G, A)$ *and* $b'' \in H^q(G, B'')$, *then*

$$(-1)^p \delta(a \cup b'') = a \cup \delta b''.$$

Proof: Uniqueness: Let $A \in \mathrm{Mod}(G)$, and consider the exact sequence

$$0 \longrightarrow A \xrightarrow[i]{} M_G(A) \longrightarrow A'' \longrightarrow 0$$

where $M_G(A) = M_G^1(A)$ (see §7, CH. II), and i is the G-homomorphism given by $i(a)\sigma = \sigma a$. This sequence is $\mathbb{Z}$-split, for the map

$$p\colon M_G(A) \longrightarrow A$$

p. 183 defined by $p(x) = x(1)$ is an abelian group homomorphism such that $p\,i =$ identity. Therefore

$$0 \longrightarrow A \otimes_{\mathbb{Z}} B \longrightarrow M_G(A) \otimes_{\mathbb{Z}} B \longrightarrow A'' \otimes_{\mathbb{Z}} B \longrightarrow 0$$

is an exact sequence of G-modules for every $B \in \mathrm{Mod}(G)$. On the other hand, by Cor. 7.5, Ch. II, $H^n(G, M_G(A)) = 0$ if $n \geq 1$. Hence by property (iii) we obtain a commutative diagram with exact upper row

$$\begin{array}{ccccc} H^p(G,A'') \times H^q(G,B) & \xrightarrow{(\delta,1)} & H^{p+1}(G,A) \times H^q(G,B) & \longrightarrow & 0 \\ \downarrow \cup & & \downarrow \cup & & \\ H^{p+q}(G, A'' \otimes B) & \xrightarrow{\quad\delta\quad} & H^{p+q+1}(G, A \otimes B) & & \end{array}$$

for $p, q \geq 0$.

This diagram together with an induction argument shows that

$$H^0(G,A'') \times H^0(G,B) \longrightarrow H^0(G, A'' \otimes B) \tag{1}$$

uniquely determines the maps

$$H^p(G,A) \times H^0(G,B) \longrightarrow H^p(G, A \otimes B). \tag{1}$$

p. 184 Similarly, using property (iv) one sees that the map (1) uniquely determines the maps

$$H^0(G,A) \times H^q(G,B) \longrightarrow H^q(G, A \otimes B).$$

This last fact, the diagram above and an induction argument on p show the uniqueness of the cup-product.

Existence: Here we use the notation of §1, Ch. II. Given $p, q \geq 0$ and $A, B \in \mathrm{Mod}(G)$, we define a mapping

$$\psi_{p,q}\colon C^p(G,A) \times C^q(G,B) \longrightarrow C^{p+q}(G, A \otimes B),$$

by

$$\psi_{p,q}(a,b)(\sigma_0, \ldots, \sigma_{p+q}) = a(\sigma_0, \ldots, \sigma_p) \otimes b(\sigma_p, \ldots, \sigma_{p+q}).$$

It is easy to see that $\psi_{p,q}(a,b) \in C^{p+q}(G, A \otimes B)$, and that each $\psi_{p,q}$ is $\mathbb{Z}$-linear. We show now that each of these mappings induces a map

p. 185
$$\bar{\psi}_{p,q}\colon H^p(G,A) \times H^q(G,B) \longrightarrow H^{p+q}(G, A \otimes B).$$

To see this notice that

$$\partial(a \cup b) = \partial a \cup b + (-1)^p a \cup \partial b$$

for $a \in C^p(G,A)$ and $b \in C^q(G,B)$, and therefore

$$a \in Z^p(G,A),\ b \in Z^q(G,B) \Rightarrow \psi_{p,q}(a,b) \in Z^{p+q}(G, A \otimes B),$$
$$a \in Z^p(G,A),\ b \in B^q(G,B) \Rightarrow \psi_{p,q}(a,b) \in B^{p+q}(G, A \otimes B),$$
$$a \in B^p(G,A),\ b \in Z^q(G,B) \Rightarrow \psi_{p,q}(a,b) \in B^{p+q}(G, A \otimes B),$$

We set $\bar{\psi}_{p,q}(a,b) = \psi_{p,q}(a,b) = a \cup b$, where we let a, b stand both for the classes and representatives of those classes.

Finally we prove that the products $(a,b) \mapsto \bar{\psi}_{p,q}(a,b) = a \cup b$ satisfy the conditions of the theorem. Property (i): Let $f\colon A \longrightarrow A'$ and $g\colon B \longrightarrow B'$ be G-maps. Then the diagram

$$\begin{array}{ccc} H^p(G,A) \times H^q(G,B) & \xrightarrow{\bar{\psi}_{p,q}} & H^{p+q}(G, A \otimes B) \\ \Big\downarrow{\scriptstyle \bar{f} \times \bar{g}} & & \Big\downarrow{\scriptstyle \overline{f \otimes g}} \\ H^p(G,A') \times H^q(G,B') & \xrightarrow{\bar{\psi}_{p,q}} & H^{p+q}(G, A' \otimes B') \end{array}$$

p. 186

commutes, where $\bar{f}, \bar{g}, \overline{f \otimes g}$ are the maps induced on the cohomology groups by $\bar{f}$, $\bar{g}$, $\overline{f \otimes g}$ (see §4, Ch. II). For

$$\big[\bar{\psi}_{p,q} \circ (\bar{f} \times \bar{g})\big](a,b)(\sigma_0, \ldots, \sigma_{p+q}) = \big(\bar{f}(a) \circ \bar{g}(b)\big)(\sigma_0, \ldots, \sigma_{p+q}) =$$
$$f\big[a(\sigma_0, \ldots, \sigma_p)\big] \otimes g\big[b(\sigma_p, \ldots, \sigma_{p,q})\big] = \big[\overline{f \otimes g} \circ \bar{\psi}_{p,q}\big](a,b)(\sigma_0, \ldots, \sigma_{p+q}).$$

Property (ii): This is clear.

Property (iii): Let $B \in \mathrm{Mod}(G)$ and let

$$0 \longrightarrow A \xrightarrow{\alpha} A' \xrightarrow{\beta} A'' \longrightarrow 0$$

be an exact sequence in $\mathrm{Mod}(G)$ such that

p. 187

$$0 \longrightarrow A \otimes B \xrightarrow{\alpha \otimes 1} A' \otimes B \xrightarrow{\beta \otimes 1} A'' \otimes B \longrightarrow 0$$

is again exact.

If $X \in \mathrm{Mod}(G)$ we shall write $C^n(X)$ instead of $C^n(G, X)$. Consider the (non-commutative) diagram with exact rows, which is shown on p. 188.

Recall that if $a'' \in Z^p(G, A'')$ then $\delta a''$ is defined as folows (see Prop. 4.4, Ch. II): let $a \in C^p(A')$ with $\bar{\beta} a' = a''$ and let $a \in C^p(A)$ such that * $\bar{\alpha} a = \partial a'$ (a exists since $\bar{\beta} \partial a' = \partial \bar{\beta} a' = 0$); then $\partial a = 0$; we set $\delta a'' = a$. Assume also that $b \in Z^p(G, B)$; * then we have

$$\overline{\beta \otimes 1}(a' \cup b) = a'' \cup b,$$
$$\overline{\alpha \otimes 1}(a \cup b) = \partial(a' \cup b)$$

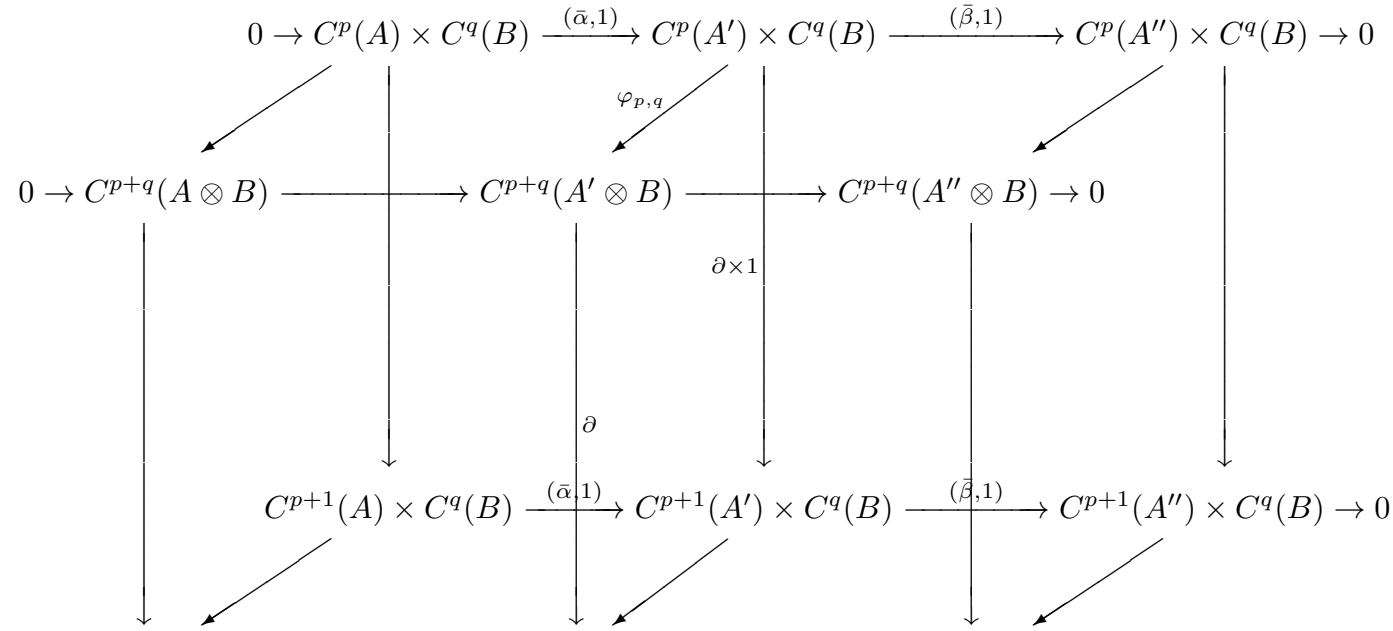
and

$$\partial(a \cup b) = 0.$$

---

* Error: should be $a \in C^{p+1}(A)$
* Error: should be $b \in Z^q(G, B)$

Hence


$0 \to C^p(A) \times C^q(B) \xrightarrow{(\bar{\alpha},1)} C^p(A') \times C^q(B) \xrightarrow{(\bar{\beta},1)} C^p(A'') \times C^q(B) \to 0$
$\varphi_{p,q}$
$0 \to C^{p+q}(A \otimes B) \longrightarrow C^{p+q}(A' \otimes B) \longrightarrow C^{p+q}(A'' \otimes B) \to 0$
$\partial \times 1$
∂
$C^{p+1}(A) \times C^q(B) \xrightarrow{(\bar{\alpha},1)} C^{p+1}(A') \times C^q(B) \xrightarrow{(\bar{\beta},1)} C^{p+1}(A'') \times C^q(B) \to 0$
$0 \to C^{p+q+1}(A \otimes B) \xrightarrow{\overline{\alpha \otimes 1}} C^{p+q+1}(A' \otimes B) \xrightarrow{\overline{\beta \otimes 1}} C^{p+q+1}(A'' \otimes B) \to 0$

p. 188

p. 189 $$\partial(a'' \cup b) = a \cup b = \partial a'' \cup b$$

(notice that a'' and b stand both for cocycles and for the corresponding elements of the cohomology groups.)

Property (iv): This can be verified in a similar manner. ∎

§7. Properties of cup products

PROPOSITION 7.1: *Let G be a profinite group, $A, B \in \mathrm{Mod}(G)$, $a \in H^p(G, A)$ and $b \in H^q(G, B)$. Then*

$$a \cup b = (-1)^{pq} b \cup a,$$

where $A \otimes B$ and $B \otimes A$ are identified in the canonical manner.

p. 190 *Proof:* This is plain if $p = q = 0$. We proceed by induction. Suppose the result holds for $p = p_0$ and $q = q_0$, and assume $a \in H^{p_0+1}(G, A)$ and $b \in H^{q_0}(G, B)$. As in the uniqueness proof of Th. 6.1 we find a commutative diagram with exact upper row

$$\begin{array}{ccccc} H^{p_0}(G, A'') \times H^{q_0}(G, B) & \xrightarrow{(\delta,1)} & H^{p_0+1}(G, A) \times H^{q_0}(G, B) & \longrightarrow & 0 \\ \downarrow \cup & & \downarrow \cup & & \\ H^{p_0+q_0}(G, A'' \otimes B) & \xrightarrow{\delta} & H^{p_0+q_0+1}(G, A \otimes B) & & \end{array}$$

Let $a'' \in H^{p_0}(G, A'')$ be such that $\delta a'' = a$. Hence, using property (iv) of Th. 6.1,

$$a \cup b = \delta(a'' \cup b) = (-1)^{p_0 q_0} \delta(b \cup a'') = (-1)^{p_0 q_0} (-1)^{q_0} b \cup \delta(a'') = (-1)^{(p_0+1)q_0} b \cup a.$$

One proves similarly that if the result holds for $p = p_0$ and $q = q_0$ then it holds for $p = p_0$ and $q = q_0 + 1$. ∎

p. 191 PROPOSITION 7.2: *Let G be a profinite group, $A, B, C \in \mathrm{Mod}(G)$ and $a \in H^p(G, A)$, $b \in H^q(G, B)$, $c \in H^r(G, C)$. Then*

$$(a \cup b) \cup c = a \cup (b \cup c)$$

modulo the identification of $(A \otimes B) \otimes C$ *and* $A \otimes (B \otimes C)$.

Proof: This follows immediately from the definition of the cup product by means of cochains (see proof of "existence" in Th. 6.1). ∎

We now turn to the study of the relationship between cup products and the maps Res, Cor and Inf (see §6 Ch. II).

PROPOSITION 7.3: *Let* $H \subset G$ *be profinite groups,* $A, B \in \mathrm{Mod}(G)$ *and* $a \in H^p(G, A)$, $b \in H^q(G, B)$. *Then*

$$\mathrm{Res}(a \cup b) = \mathrm{Res}(a) \cup \mathrm{Res}(b),$$

p. 192 *where* Res *is the restriction map.*

Proof: This follows immediately from the definition of Res in terms of cochains (cf. §6 Ch. II). ∎

PROPOSITION 7.4: *Let* H *be a closed normal subgroup of a profinite group* G. *Let* $A, B \in \mathrm{Mod}(G)$, $a \in H^p(G/H, A^H)$, $b \in H^q(G/H, B^H)$. *Then*

$$\mathrm{Inf}(a \cup b) = \mathrm{Inf}(a) \cup \mathrm{Inf}(b),$$

where Inf *is the inflation map.*

Proof: This follows from the definition of Inf in terms of cochains (cf. §6 Ch. II). ∎

PROPOSITION 7.5: *Let* G *be a profinite group and* H *an open subgroup of* G. *Let* $a \in H^p(G, A)$ *and* $b \in H^q(G, B)$, *where* $A, B \in \mathrm{Mod}(G)$. *Then*

p. 193 $$\mathrm{Cor}\left(a \cup \mathrm{Res}(b)\right) = \mathrm{Cor}(a) \cup b,$$

where Cor *and* Res *are the corestriction and restriction maps respectively.*

Proof: Assume first that $p = q = 0$. Then $a \in A^H$ and $b \in B^G$. Let $\sigma_1, \sigma_2, \ldots, \sigma_t$ be a set of representatives of the left cosets of H in G. Then (see §6 Ch. II)

$$\mathrm{Cor}\left(a \cup \mathrm{Res}(b)\right) = \sum_{i=1}^{t} \sigma_i(a \cup b) = \sum_{i=1}^{t} \sigma_i a \otimes \sigma_i b = \sum_{i=1}^{t} \sigma_i a \otimes b = \Big(\sum_{i=1}^{t} \sigma_i a\Big) \cup b = \mathrm{Cor}(a) \cup b.$$

We proceed now by induction. Assume the formula holds true for $p = p_0$ and $q = q_0$. Let $a \in H^{p_0+1}(G, A)$ and $b \in H^{q_0}(G, B)$. Consider the $\mathbb{Z}$-split exact sequence

$$0 \longrightarrow A \longrightarrow M_H(A) \longrightarrow A'' \longrightarrow 0$$

p. 194 (see proof of uniqueness in Th. 6.1). Since $H^n\big(H, M_H(A)\big) = 0$ if $n \geq 1$ there is $a'' \in H^{p_0}(H, A)$ with $\delta a'' = a$, where δ is the connecting homomorphism corresponding to the above short exact sequence. Since

$$0 \longrightarrow A \otimes B \longrightarrow M_H(A) \otimes B \longrightarrow A'' \otimes B \longrightarrow 0$$

is also exact, we can apply property (iii) of Th. 6.1. Hence, taking into account that Res and Cor commute with δ (cf. §6 Ch. II), we have by the induction hypothesis

$$\mathrm{Cor}\,\big(a \cup \mathrm{Res}(b)\big) = \mathrm{Cor}\,\big(\delta a'' \cup \mathrm{Res}(b)\big) = \mathrm{Cor}\,\big(\delta(a'' \cup \mathrm{Res}(b))\big) = \delta\ \mathrm{Cor}\,\big(a'' \cup \mathrm{Res}(b)\big) =$$
$$\delta\big(\,\mathrm{Cor}(a'') \cup b\big) = \delta\,\mathrm{Cor}(a'') \cup b = \mathrm{Cor}(\delta a'') \cup b = \mathrm{Cor}(a) \cup b.$$

One proves similarly using property (iv) of Th. 6.1 that if the formula holds for
p. 195 $p = p_0$ and $q = q_0$ it also holds for $p = p_0$ and $q = q_0 + 1$. Thus, by induction, the formula is valid for all $p, q \geq 0$. ∎

Corollary 7.6: *Under the hypothesis of Proposition 7.5 we have*

$$\mathrm{Cor}\,\big(\,\mathrm{Res}(b) \cup a\big) = b \cup \mathrm{Cor}(a).$$

Proof:

$$\mathrm{Cor}\,\big(\,\mathrm{Res}(b) \cup a\big) = \mathrm{Cor}\,\big((-1)^{pq} a \cup \mathrm{Res}(b)\big) = (-1)^{pq}\,\mathrm{Cor}(a) \cup b = b \cup \mathrm{Cor}(a).$$

∎

p. 196

CHAPTER IV

APPLICATIONS

§1. Cohomological dimension

If G is a profinite group, $\mathrm{Mod}_t(G)$ denotes the full subcategory of $\mathrm{Mod}(G)$ consisting of the torsion modules (torsion as abelian groups).

Definition 1.1: Let G be a profinite group, p a prime number and n a natural number. We say that the *cohomological p-dimension* $\mathrm{cd}_p(G)$ (respectively the *strict cohomological p-dimension* $\mathrm{scd}_p(G)$) is n if n is the smallest number such that

$$H^q(G,A)(p) = 0 \quad \text{for all } q > n \text{ and } A \in \mathrm{Mod}_t(G)$$
$$(\text{resp. all } q > n \text{ and } A \in \mathrm{Mod}(G)).$$

If no such an n exists we say that $\mathrm{cd}_p(G) = \infty$, (resp. $\mathrm{scd}_p(G) = \infty$).

p. 197 PROPOSITION 1.2: *The following are equivalent*

(i) $\mathrm{cd}_p(G) \leq n$, *(resp.* $\mathrm{scd}_p(G) \leq n$*)*,

(ii) $H^q(G,A)(p) = 0$ *for all* $q > n$ *and* $A \in \mathrm{Mod}_t(G)$
(resp. $H^q(G,A)(p) = 0$ *for all* $q > n$ *and* $A \in \mathrm{Mod}(G)$*).*

Proof: Trivial. ∎

Definition 1.3: Let G be a profinite group. Set

$$\mathrm{cd}(G) = \sup_p \mathrm{cd}_p(G),$$

(respectively,

$$\mathrm{scd}(G) = \sup_p \mathrm{scd}_p(G)).$$

PROPOSITION 1.4: *Let G be a profinite group and p a prime. Then*

$$\mathrm{cd}_p(G) \leq \mathrm{scd}_p(G) \leq \mathrm{cd}_p(G) + 1.$$

p. 198 *Proof:* The first inequality is clear. For the second we may suppose that $\mathrm{cd}_p(G) < \infty$. Let $n = \mathrm{cd}_p(G) + 1$. Assume $A \in \mathrm{Mod}(G)$ and let $p\colon A \longrightarrow A$ be multiplication by p. Consider the short exact sequences

$$0 \longrightarrow A_p \longrightarrow A \xrightarrow{p} pA \longrightarrow 0,$$

$$0 \longrightarrow pA \longrightarrow A \longrightarrow A/pA \longrightarrow 0.$$

Then A_p and A/pA are torsion; so if $q > n - 1$

$$H^q(G, A_p) = H^q(G, A/pA) = 0.$$

Therefore from the long exact sequences

$$\cdots \longrightarrow H^q(G, A_p) \longrightarrow H^q(G, A) \xrightarrow{\varphi} H^q(G, pA) \longrightarrow \cdots,$$

$$\cdots \longrightarrow H^{q-1}(G, A/pA) \longrightarrow H^q(G, pA) \xrightarrow{\psi} H^q(G, A) \longrightarrow \cdots,$$

one obtains that the maps φ and ψ are injections if $q > n$. Hence their composition

$$\psi\varphi\colon H^q(G, A) \longrightarrow H^q(G, A)$$

p. 199 is again an injection. On the other hand it is clear that $\psi\varphi$ is multiplication by p. Thus

$$H^q(G, A)(p) = 0, \quad \text{if} \quad q > n.$$

The second inequality follows now from Proposition 1.2. ∎

Example:

Consider the group $G = \widehat{\mathbb{Z}}$. As we will see later (Cor. 3.3) for every p, $\mathrm{cd}_p(G) = 1$. On the other hand let G act trivially on $\mathbb{Q}$. Then $H^n(G, \mathbb{Q}) = 0$ if $n \geq 1$, for, by Cor. 6.7, Ch. II, $H^n(G, \mathbb{Q})$ is a torsion group for each $n \geq 1$ and clearly multiplication by any non-zero integer m is an automorphism of $H^n(G, \mathbb{Q})$ (since multiplication by m is an automorphism of $\mathbb{Q}$). So from the exact sequence

$$0 \longrightarrow \mathbb{Z} \longrightarrow \mathbb{Q} \longrightarrow \mathbb{Q}/\mathbb{Z} \longrightarrow 0$$

p. 200 we obtain isomorphisms

$$H^{n+1}(G, \mathbb{Z}) \approx H^n(G, \mathbb{Q}/\mathbb{Z}), \quad n \geq 1.$$

In particular $H^2(G,\mathbb{Z}) \approx H^1(G,\mathbb{Q}/\mathbb{Z}) = \mathrm{Hom}_c(G,\mathbb{Q}/\mathbb{Z}) = \mathbb{Q}/\mathbb{Z}$.

Thus $\mathrm{scd}_p(G) = 2$.

If $A \in \mathrm{Mod}_t(G)$ and p is a prime number, denote by $A(p)$ the p-primary part of A, i.e., those elements of A of order p^n for some n. If $A = A(p)$ we say that A is p-primary. Our next proposition simplifies the problem of finding the cohomological p-dimension of a group.

PROPOSITION 1.5: *The following are equivalent:*

(i) $\mathrm{cd}_p(G) \leq n$,

(ii) $H^q(G,A) = 0$ *for all* $q > n$ *and all* p*-primary* $A \in \mathrm{Mod}_t(G)$,

(iii) $H^{n+1}(G,A) = 0$ *for all simple,* p*-primary* G*-modules* A.

p. 201 *Proof:* The implications (i) $\Rightarrow$ (i) $\Rightarrow$ (iii) are trivial.

(ii) $\Rightarrow$ (i): Let $A \in \mathrm{Mod}_t(G)$. Then

$$A = \coprod_p A(p)$$

So (see Prop. 4.6, Ch. II)

$$H^q(G,A) = \coprod_p H^q\big(G, A(p)\big).$$

Hence

$$H^q(G,A)(p) \approx H^q\big(G, A(p)\big).$$

Thus, if $q > n$ we have

$$H^q(G,A)(p) = 0.$$

(iii) $\Rightarrow$ (ii): First we show, by induction on the order of A, that $H^{n+1}(G,A) = 0$ for all finite p-primary G-modules. If $A = 0$ it is obviously true. If $A \neq 0$, assume true for

p. 202 those modules of order less than $\#A$. Let A_1 be a simple G-module contained in A. Consider the exact sequence

$$0 \longrightarrow A_1 \longrightarrow A \longrightarrow A/A_1 \longrightarrow 0$$

and its corresponding long exact sequence

$$\cdots \longrightarrow H^{n+1}(G, A_1) \longrightarrow H^{n+1}(G, A) \longrightarrow H^{n+1}(G, A/A_1) \longrightarrow \cdots$$

Since $H^{n+1}(G, A_1) = H^{n+1}(G, A/A_1) = 0$, one has $H^{n+1}(G, A) = 0$.

Now we prove that $H^{n+1}(G, A) = 0$ for all p-primary $A \in \mathrm{Mod}_t(G)$. If A_1 is a finitely generated G-submodule of A it is also finitely generated as an abelian group (see p. 115), and hence A_1 is finite since it is p-primary. Now

$$A \approx \varinjlim A_i$$

p. 203 where A_i runs through all the finitely generated (i.e., finite) modules of A. So,

$$H^{n+1}(G, A) \approx \varinjlim H^{n+1}(G, A_i) = 0.$$

Finally, let A be a p-primary, torsion G-module and let $q \geq n$. Consider the induced module $M_G^1(A) = M_G(A)$ and the exact sequence

$$0 \longrightarrow A \xrightarrow{i} M_G(A) \longrightarrow A_1 \longrightarrow 0$$

where $i(a)\sigma = \sigma a$, $a \in A$, $\sigma \in G$; $A_1 = M_G(A)/i(A)$.

From the corresponding long exact sequence

$$\cdots \longrightarrow H^q(G, A_1) \xrightarrow{\delta} H^{q+1}(G, A) \longrightarrow H^{q+1}(G, M_G(A)) \longrightarrow \cdots$$

and the fact that $H^t(G, M_G(A)) = 0$ if $t > 0$ (see Cor. 7.5, Ch. II) we deduce

$$H^q(G, A_1) \approx H^{q+1}(G, A)$$

for $q \geq n + 1$. By an induction argument on q we have

$$H^q(G, A) = 0, \quad \text{if} \quad q > n.$$

∎

§2. Cohomological dimension of subgroups

p. 204

PROPOSITION 2.1: *Let $H \subseteq G$ be profinite groups, and p a prime. Then*

(a) $\mathrm{cd}_p(H) \leq \mathrm{cd}_p(G)$,

(b) $\mathrm{scd}_p(H) \leq \mathrm{scd}_p(G)$.

Moreover, equality holds in either of the following cases

(1) $p \nmid (G : H)$,

(2) *H is open in G and* $\mathrm{cd}_p(G) < \infty$.

Proof: We will give proofs for the case of cohomological dimension, the case of strict cohomological dimension being analogous.

For (a). Let $A \in \mathrm{Mod}_t(H)$ and let $q > \mathrm{cd}_p(G)$. Using Shapiro's Lemma we get

$$H^q(H, A)(p) \approx H^q\big(G, M_G^H(A)\big)(p) = 0,$$

p. 205 as desired.

For (1). Let $n \geq 1$ be such that there exists $A \in \mathrm{Mod}_t(G)$ with $H^n(G, A)(p) \neq 0$. By Cor. 6.8, Ch. II,

$$\text{Res: } H^q(G, A)(p) \longrightarrow H^q(H, A)(p)$$

is an injection if $q \geq 1$, since $p \nmid (G : H)$. Therefore

$$H^n(H, A)(p) \neq 0.$$

Hence $\mathrm{cd}_p(H) \geq \mathrm{cd}_p(G)$. By part (a) we obtain equality.

For (2). Let $\mathrm{cd}_p(G) = n$. Then there exists $A \in \mathrm{Mod}_t(G)$ with $H^n(G, A)(p) \neq 0$. Set $A^* = M_G^H(A)$ and define G-homomorphisms

$$A^* \underset{i}{\overset{\pi}{\rightleftarrows}} A$$

p. 206 by

$$\pi a^* = \sum \sigma_i^{-1} a^*(\sigma_i),$$

and

$$(ia)(\tau\sigma_i) = \begin{cases} \tau a & \text{if } \sigma_i = 1 \\ 0 & \text{if } \sigma_i \neq 1 \ , \end{cases}$$

where the $\{\sigma_i\}$ form a set of representations of the left cosets of H in G. Then $\pi \circ i = id_A$. So π is surjective. Let $A_1 = \text{Ker } \pi$. Consider the exact sequence

$$0 \longrightarrow A_1 \longrightarrow A^* \xrightarrow{\pi} A \longrightarrow 0.$$

From the corresponding long exact sequence in cohomology we obtain that

$$H^n(G, A^*)(p) \xrightarrow{\overline{\pi}} H^n(G, A)(p) \xrightarrow{\delta} H^{n+1}(G, A_1)(p)$$

p. 207 is exact. Since $H^{n+1}(G, A_1)(p) = 0$, $\overline{\pi}$ is surjective. Hence, since $H^n(G, A) \neq 0$,

$$H^n(G, A^*)(p) \neq 0.$$

So by Shapiro's Lemma,

$$H^n(H, A) \neq 0.$$

Thus $\text{cd}_p(H) \geq n$. Equality follows then from part (a). ∎

Remark: The condition $\text{cd}_p(G) < \infty$ in part (2) above is necessary, for as we will see later (Th. 8.8, Ch. V) if

$$G = G_{\mathbb{Q}} \quad \text{and} \quad H = G_{\mathbb{Q}(i)}$$

then

$$\text{cd}_2(G) = \infty \quad \text{and} \quad \text{cd}_2(H) = 2.$$

COROLLARY 2.2: *Let G_p be a p-Sylow group of G. Then*

$$\text{cd}_p(G) = \text{cd}_p(G_p) = \text{cd}(G_p),$$

p. 208
$$\text{scd}_p(G) = \text{scd}_p(G_p) = \text{scd}(G_p).$$

COROLLARY 2.3: $\text{cd}_p(G) = 0 \Longleftrightarrow p \nmid \#G$.

Proof: By Cor. 2.2, $\text{cd}_p(G) = 0 \Longleftrightarrow \text{cd}(G_p) = 0$. On the other hand $p \nmid \#G \Longleftrightarrow G_p = 1$. Hence we have to show that

$$\text{cd}(G_p) = 0 \Longleftrightarrow G_p = 1 \ .$$

Certainly $H^q(1, A) = 0$ if $q \geq 1$. Conversely, assume $\mathrm{cd}(G_p) = 0$. Consider $\mathbb{Z}/p\mathbb{Z}$ as a trivial G_p-module, i.e., $\sigma \in G_p$, $a \in \mathbb{Z}/p\mathbb{Z} \Rightarrow \sigma a = a$. Then (cf. Ch. II, §2)

$$0 = H^1(G_p, \mathbb{Z}/p\mathbb{Z}) \approx \mathrm{Hom}_c(G_p, \mathbb{Z}/p\mathbb{Z})$$

(continuous homomorphisms). However, if $G_p \neq 1$ there exist non-trivial continuous homomorphisms of G_p to $\mathbb{Z}/p\mathbb{Z}$ (take U open and normal in G_p; then G_p/U is a finite p-group, which admits a non-trivial homomorphism into $\mathbb{Z}/p\mathbb{Z}$ since, by a Sylow theorem, it contains a normal subgroup of index p). Therefore $G_p = 1$. ∎

p. 209 COROLLARY 2.4: *If* $\mathrm{cd}_p(G) \neq 0, \infty$ *then* p^∞ *divides* $\#G$.

Proof: By Cor. 2.2, $\mathrm{cd}_p(G) \neq 0, \infty \Longleftrightarrow \mathrm{cd}_p(G_p) \neq 0, \infty$. On the other hand $\mathrm{cd}_p(G_p) \neq 0, \infty$ implies G_p is infinite, for if G_p is finite the subgroup $\{1\}$ is open and by Prop. 2.1

$$0 = \mathrm{cd}_p(\{1\}) = \mathrm{cd}_p(G_p).$$

Finally since G_p is infinite $\#G_p = p^\infty$ and so $p^\infty \mid \#G$. ∎

COROLLARY 2.5: *If* G *is finite and* p *divides* $\#G$, *then* $\mathrm{cd}_p(G) = \infty$.

PROPOSITION 2.6: *Let* N *be a normal closed subgroup of a profinite group* G, *and let* p *be a prime. Then*

$$\mathrm{cd}_p(G) \leq \mathrm{cd}_p(N) + \mathrm{cd}_p(G/N).$$

p. 210 *Proof:* Consider the Lyndon-Hochschild-Serre spectral sequence

$$E_2^{i,j} = H^i\big(G/N, H^j(N, A)\big) \Longrightarrow H^n(G, A).$$

Let $m > \mathrm{cd}_p(N) + \mathrm{cd}_p(G/N)$. We shall show that $H^n(G, A)(p) = 0$ if $A \in \mathrm{Mod}_t(G)$. Set $i + j = m$, $i, j \geq 0$. Then $j > \mathrm{cd}_p(N)$ or $i > \mathrm{cd}_p(G/N)$. So

$$E_2^{i,j}(p) = 0, \quad \text{if} \quad i + j = m.$$

Therefore

$$E_\infty^{i,j}(p) = 0, \quad i + j = m.$$

Thus

$$H^m(G, A)(p) = 0.$$

∎

p. 211

§3. Groups G with $\mathrm{cd}_p(G) \leq 1$

Let G be a profinite group. Recall that an embedding problem for G is a diagram of profinite groups and continuous homomorphisms

$$\begin{array}{ccccccccc} & & & & & & G & & \\ & & & & & & \downarrow{\scriptstyle \gamma} & & \\ 1 & \longrightarrow & P & \longrightarrow & E & \xrightarrow{\varphi} & W & \longrightarrow & 1 \\ & & & & & & \downarrow & & \\ & & & & & & 1 & & \end{array}$$

with exact row and column. We denote such a problem by $I(G)$. We say that $I(G)$ is *weakly solvable* if there exists a continuous homomorphism $\eta\colon G \longrightarrow E$ such that $\varphi\eta = \gamma$.

We recall that a finite elementary abelian p-group A is one for which $pA = 0$.

PROPOSITION 3.1: *Let G be a profinite group and p a prime number. The following statements are equivalent:*

(i) $\mathrm{cd}_p(G) \leq 1$;

(ii) *$I(G)$ is weakly solvable if E is finite and P is a finite elementary abelian p-group;*

p. 212 *(ii)′* *Every extension*

$$1 \longrightarrow P \longrightarrow E \longrightarrow G \longrightarrow 1,$$

where P is a finite elementary abelian p-group, splits;

(iii) *$I(G)$ is weakly solvable if P is a pro-p-group;*

(iii)′ *Every extension*

$$1 \longrightarrow P \longrightarrow E \longrightarrow G \longrightarrow 1,$$

where P is any pro-p-group, splits.

Proof: We shall prove the implications in the following order

$$\text{(i)} \longrightarrow \text{(ii)} \longrightarrow \text{(iii)} \longrightarrow \text{(iii)}' \longrightarrow \text{(ii)}' \longrightarrow \text{(i)}.$$

(i) $\longrightarrow$ (ii): Let $x\colon W^2 \longrightarrow P$ be a representative in $H^2(W,P)$ corresponding to the extension

$$1 \longrightarrow P \longrightarrow E \xrightarrow[\varphi]{} W \longrightarrow 1,$$

(see Ch. II, §§2,3). To x we associate a cocycle $y\colon G^2 \longrightarrow P$ by defining

$$y(\sigma,\tau) = x\big(\gamma(\sigma),\gamma(\tau)\big).$$

p. 213 (I.e., $y = \operatorname{Inf} x$; see Ch. II, §6). Recall that the action of G in P is induced by γ:

$$\text{if } a \in P \text{ and } \sigma \in G, \text{ then } \sigma \cdot a = \gamma(\sigma)a.$$

To y there corresponds an extension

$$1 \longrightarrow P \longrightarrow \overline{E} \xrightarrow[\overline{\varphi}]{} W \longrightarrow 1,$$

which must split, since by hypothesis $H^2(G,P)(p) = 0$; say $\psi\colon G \longrightarrow \overline{E}$ is a continuous homomorphism with $\overline{\varphi} \cdot \psi = id_G$. We identify E and $\overline{E}$ with the cartesian products $P \times W$ and $P \times G$, respectively (see Ch. II, §3, p. 103). Define

$$f\colon \overline{E} \longrightarrow E$$

by $f(a,\sigma) = (a,\gamma(\sigma))$, $a \in P$, $\sigma \in G$. One easily checks that f is a continuous homomorphism (see Ch. II, §3 for the definition of operation in E and $\overline{E}$, and their topologies) making the diagram

$$\begin{array}{ccccccccc}
1 & \longrightarrow & P & \longrightarrow & \overline{E} & \underset{\overline{\varphi}}{\overset{\pi}{\rightleftarrows}} & G & \longrightarrow & 1 \\
 & & \| & & \downarrow{\scriptstyle f} & & \downarrow{\scriptstyle \gamma} & & \\
1 & \longrightarrow & P & \longrightarrow & E & \xrightarrow[\varphi]{} & W & \longrightarrow & 1
\end{array}$$

commutative.

p. 214 Define $\eta: G \longrightarrow E$ by $\eta = f \cdot \psi$. Then

$$\varphi\eta = \gamma$$

as desired.

(ii) $\longrightarrow$ (iii): First we show that $I(G)$ is solvable if P is any finite p-group. Let P' be a subgroup of P of index p, and let

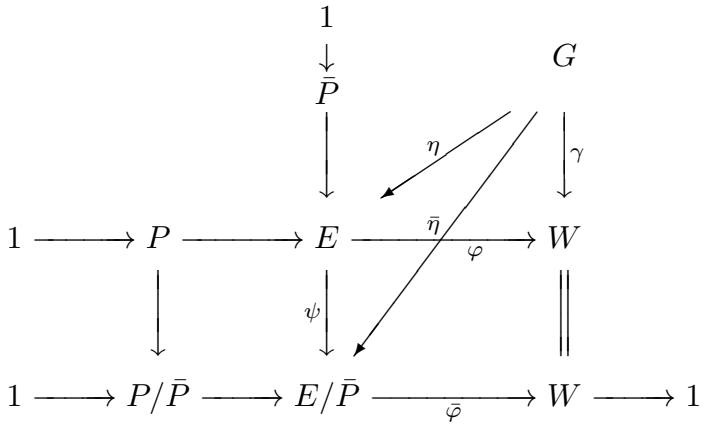
$$\overline{P} = \bigcap_{\sigma \in E} \sigma P' \sigma^{-1}.$$

Then the canonical map

$$P/\overline{P} \longrightarrow \prod_{\sigma \in E} P/\sigma P' \sigma^{-1}$$

is injective, so that $P/\overline{P}$ is p-primary abelian.

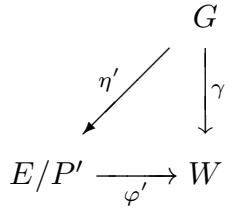
By (ii) there exists a map $\overline{\eta}: G \longrightarrow E/\overline{P}$ with $\overline{\varphi} \cdot \overline{\eta} = \gamma$.



p. 215 Then, again by (ii) and induction on the order of P, there exists $\eta: G \longrightarrow E$ such that $\psi \cdot \eta = \overline{\eta}$. Hence

$$\varphi \cdot \eta = \overline{\varphi} \cdot \psi \cdot \eta = \overline{\varphi} \cdot \overline{\eta} = \gamma \ .$$

We consider now the general case where P is any pro-p-group. Let the set $\underline{P}$ consist of the pairs (P', η') where P' is a closed normal subgroup of E contained in P, and $\eta': G \longrightarrow E/P'$ is a continuous homomorphism such that



commutes. Set $(P', \eta') < (P'', \eta'')$ when $P' \supseteq P''$ and

$$\begin{array}{ccc} & & G \\ & {\scriptstyle\eta'}\swarrow & \downarrow{\scriptstyle\eta''} \\ E/P' & \longrightarrow & E/P'' \end{array}$$

commutes. Then $\underline{P}$ is inductively ordered, for if $(P'_\lambda, \eta'_\lambda)$ is totally ordered, then put $P' = \bigcap_\lambda P'_\lambda$ and $\eta' = \varprojlim_\lambda \eta'_\lambda : G \longrightarrow E/P' = \varprojlim_\lambda E/P'_\lambda$. Then

p. 216

$$\begin{array}{ccccccccc} & & & & & & G & & \\ & & & & & {\scriptstyle\eta'}\swarrow & \downarrow & & \\ 1 & \longrightarrow & P/P' & \longrightarrow & E/P' & \underset{\varphi'}{\longrightarrow} & W & \longrightarrow & 1 \end{array}$$

commutes.

Let $(\overline{P}, \overline{\eta})$ be a maximal element of $\underline{P}$. We shall show that $\overline{P} = 1$. Suppose $\overline{P} \neq 1$; then there exists an open normal subgroup $\overline{\overline{P}}$ of $\overline{P}$ which is normal in E, such that $\overline{\overline{P}} \neq \overline{P}$ (if $\overline{P} \neq 1$, it contains a proper open subgroup $\overline{P} \cap U$ where U is open in E; then U contains an open normal subgroup $\overline{\overline{U}}$ of E; put $\overline{\overline{P}} = P \cap \overline{\overline{U}}$).

Since $\overline{P}/\overline{\overline{P}}$ is finite, by the first part, there exists a map $\overline{\overline{\eta}} : G \longrightarrow E/\overline{\overline{P}}$ such that

$$(G \longrightarrow E/\overline{\overline{P}} \longrightarrow E/\overline{P}) = (G \longrightarrow E/\overline{P}).$$

Then $(G \longrightarrow E/\overline{\overline{P}} \longrightarrow W) = (G \longrightarrow W)$, which contradicts the maximality of $(\overline{P}, \overline{\eta})$. Thus $\overline{P} = 1$.

(iii) $\longrightarrow$ (iii)$'$ and (iii)$'$ $\longrightarrow$ (ii)$'$ are trivial implications.

(ii)$'$ $\longrightarrow$ (i): By (ii)$'$, $H^2(G, P) = 0$ for P elementary abelian p-group. Now, every

p. 217

simple, p-primary G-module is elementary abelian (for if P is simple, let P' consist of the elements of P of order p; then $P = P'$). Hence the result follows from Prop. 1.5. ∎

Corollary 3.2: *Let $G \neq 1$ be a free pro-p-group. Then*

$$\mathrm{cd}_p(G) = \mathrm{cd}(G) = 1.$$

Proof: Since $G \neq 1$, $\mathrm{cd}(G) \geq 1$. We shall prove that (iii)$'$ of the proposition above holds. Let G be free on the set A, and $x\colon A \longrightarrow G$ the canonical mapping. Given an exact sequence

$$1 \longrightarrow P \longrightarrow E \xrightarrow{\varphi} G \longrightarrow 1,$$

where P is a pro-p-group, let $s\colon G \longrightarrow E$ be a continuous section with $s(1) = 1$. Then $y = s \cdot x$ converges to 1. Since P and G are pro-p-groups so is E. Hence there is a continuous homomorphism $\psi\colon G \longrightarrow E$ with $\psi \cdot x = y = s \cdot x$. Thus $\varphi \cdot \psi =$ identity. This verifies (iii)$'$, and so $\mathrm{cd}(G) \leq 1$. ∎

p. 218 COROLLARY 3.3: *Let $G \neq 1$ be a free profinite group. Then for every prime p, $\mathrm{cd}_p(G) = 1$.*

Proof: Similar to the proof of Cor. 3.2. ∎

§4. Cohomology of pro-p-groups

PROPOSITION 4.1: *If G is a pro-p-group, every simple p-primary G-module A is isomorphic to $\mathbb{Z}/p\mathbb{Z}$ (where the abelian group $\mathbb{Z}/p\mathbb{Z}$ is considered as a G-module on which G operates trivially, i.e., $\sigma n = n$, $\sigma \in G$, $n \in \mathbb{Z}/p\mathbb{Z}$).*

Proof: Let $0 \neq a \in A$, and let $U = \{\sigma \in G |\ \sigma a = a\}$. Then U is open, and since A is
p. 219 simple U operates trivially on A. Hence A is a G/U-module, and as such still simple. So, we may assume that G is finite. Then, since A is simple and p-primary A is finite. Consider the decomposition

$$A = \bigcup_{i=1}^{r} K_i$$

of A into G-orbits. Clearly

$$\#A = \sum_{i=1}^{r} \#K_i$$

and

$$\#K_i \mid \#G.$$

Assume $0 \in K_1$. Then $\#K_1 = 1$. The group G must operate trivially on A, for otherwise

$$A^G = \{a \in A |\ \sigma a = a\} = 0,$$

since A is simple; and hence $\#K_i \neq 1$ if $i \neq 1$, so that each $\#K_i$ is a multiple of p if $i \neq 1$, i.e.,

$$\#A \equiv 1 \qquad (\text{mod } p),$$

which contradicts the fact that A is p-primary. Finally, since $\mathbb{Z}/p\mathbb{Z}$ is the only simple
p. 220 p-primary abelian group, we have $A \approx \mathbb{Z}/p\mathbb{Z}$. ∎

COROLLARY 4.2: *Let G be a pro-p-group. Then*

$$\text{cd}(G) \leq n \Longleftrightarrow H^{n+1}(G, \mathbb{Z}/p\mathbb{Z}) = 0.$$

Proof: It follows from Prop. 1.5. ∎

COROLLARY 4.3: *If G is a pro-p-group and $\text{cd}(G) = n$ then $H^n(G, A) \neq 0$ for every finite, p-primary G-module $A \neq 0$.*

Proof: Let A be a finite p-primary G-module. By Prop. 4.1 there exists some submodule K of A such that $A/K \approx \mathbb{Z}/p\mathbb{Z}$. Consider the exact sequence

$$0 \longrightarrow K \longrightarrow A \xrightarrow{\varphi} \mathbb{Z}/p\mathbb{Z} \longrightarrow 0$$

of G-modules. The corresponding long exact sequence in cohomology

p. 221 $$\cdots \longrightarrow H^n(G, A) \xrightarrow{\overline{\varphi}} H^n(G, \mathbb{Z}/p\mathbb{Z}) \longrightarrow H^{n+1}(G, K) = 0$$

shows that $\overline{\varphi}$ is onto. So, since $H^n(G, \mathbb{Z}/p\mathbb{Z}) \neq 0$ we have $H^n(G, A) \neq 0$. ∎

PROPOSITION 4.4: *Let G be a profinite group and let N be a closed normal subgroup of G. Assume that $\text{cd}_p(G/N) = m$ and $\text{cd}_p(N) = n$ are finite. Then*

$$\text{cd}_p(G) = \text{cd}_p(G/N) + \text{cd}_p(N)$$

in either of the following cases

(i) N is a pro-p-group and $H^n(N, \mathbb{Z}/p\mathbb{Z})$ is finite;

(ii) N is in the center of G.

In the proof of this proposition we shall use the following

LEMMA 4.5: *Let G be profinite and N normal and closed in G. Assume* $\mathrm{cd}_p(G/N) = m$ *and* $\mathrm{cd}_p(N) = n$ *are finite. Then, for every prime p*

p. 222 $$H^{n+m}(G, A)(p) \approx H^m\big(G/N, H^n(N, A)\big)(p).$$

Proof: Consider the Lyndon-Hochschild-Serre (L-H-S) spectral sequence

$$E_2^{i,j} = H^i\big(G/N, H^j(N, A)\big) \Rightarrow H^n(G, A).$$

If $i > m$, then $E_2^{i,j}(p) = 0$, and if $i < m$ and $i+j = m+n$, then $j > n$, and so $E_2^{i,j}(p) = 0$. Hence $E_\infty^{i,j}(p) = 0$ if $i + j = m + n$, $i \neq m$. Thus the filtration of $H^{m+n}(G, A)$ is trivial and

$$H^{m+n}(G, A) \approx E_\infty^{m,n}.$$

Finally one easily sees that

$$E_2^{m,n} \approx E_\infty^{m,n}.$$

∎

Proof of proposition: Let $(G/N)'$ be a p-Sylow group of G/N, and let G'= preimage in G of $(G/N)'$. Then

$$G'/N \approx (G/N)',$$

p. 223 and therefore

$$\mathrm{cd}_p(G'/N) = \mathrm{cd}_p(G/N)' = \mathrm{cd}_p(G/N) = m.$$

By propositions 2.1 and 2.6,

$$\mathrm{cd}_p(G') \leq \mathrm{cd}_p(G) \leq m + n.$$

So, it will suffice to prove that

$$\mathrm{cd}_p(G') = m + n.$$

Hence we may assume that G/N is a pro-p-group.

Case (i). By Lemma 4.5 and Cor. 4.3

$$H^{n+m}(G, \mathbb{Z}/p\mathbb{Z}) \approx H^m\big(G/N, H^n(N, \mathbb{Z}/p\mathbb{Z})\big) \neq 0$$

since $H^n(N, \mathbb{Z}/p\mathbb{Z})$ is p-primary and finite by hypothesis.

Case (ii). Since N is in the center of G and the action of G on $\mathbb{Z}/p\mathbb{Z}$ is trivial, the
p. 224 group G/N acts trivially on $H^n(N, \mathbb{Z}/p\mathbb{Z})$ (see Remark on p. 172). Since N is abelian it is the direct sum of its Sylow subgroups $N(p)$. By Cor. 4.3 $H^n\big(N(p), \mathbb{Z}/p\mathbb{Z}\big) \neq 0$. From this one easily sees, by working with the cochains, that $H^n\big(N(p), \mathbb{Z}/p\mathbb{Z}\big)$ is a direct summand of $H^n(N, \mathbb{Z}/p\mathbb{Z})$, and so $H^n(N, \mathbb{Z}/p\mathbb{Z}) \neq 0$. Hence $H^n(N, \mathbb{Z}/p\mathbb{Z})$, as a vector space over $\mathbb{Z}/p\mathbb{Z}$ and therefore as a G/N-module, is isomorphic to a direct sum $\coprod_I(\mathbb{Z}/p\mathbb{Z})$ where $I \neq \emptyset$. Thus we have

$$H^{n+m}(G, \mathbb{Z}/p\mathbb{Z}) \approx \coprod_I H^m(G/N, \mathbb{Z}/p\mathbb{Z}) \neq 0.$$

∎

§5. The Euler-Poincaré characteristic

Let G be a pro-p-group. We denote by $H^q(G)$ the $\mathbb{Z}/p\mathbb{Z}$-vector space $H^q(G, \mathbb{Z}/p\mathbb{Z})$. Set

$$b_q(G) = \dim H^q(G) = \dim_{\mathbb{Z}/p\mathbb{Z}} H^q(G).$$

p. 225 These are called the *Betti numbers* of G. Assume $b_q(G) = 0$ for a.e. q, and $b_q(G) < \infty$ for all q. Then define the *Euler-Poincaré characteristic* $\chi(G)$ of G by

$$\chi(G) = \sum_q (-1)^q b_q(G).$$

LEMMA 5.1: *Let G be a pro-p-group, and assume $\chi(G)$ exists. Let A be a G-module such that $pA = 0$, $\dim A = a < \infty$ and $\dim H^q(G, A) = n_q(A) < \infty$ (as $\mathbb{Z}/p\mathbb{Z}$-vector spaces). Let*

$$\chi(G, A) = \sum_q (-1)^q n_q(A).$$

Then $\chi(G, A)$ exists and

$$\chi(G, A) = a\chi(G).$$

Proof: e use induction on a. If $a = 1$, then $A \approx \mathbb{Z}/p\mathbb{Z}$. So $\chi(G, A) = \chi(G)$. Assume the result holds if $\dim(A) < a$, and suppose $\dim(A) = a > 1$. Let A_1 be a G-submodule of A with $\dim A_1 = a - 1$ (see Prop. 4.1). Then from

p. 226

$$0 \longrightarrow A_1 \longrightarrow A \longrightarrow \mathbb{Z}/p\mathbb{Z} \longrightarrow 0,$$

one obtains the exact sequence

$$\begin{aligned} 0 \longrightarrow & H^0(G, A_1) \longrightarrow H^0(G, A) \longrightarrow H^0(G, \mathbb{Z}/p\mathbb{Z}) \longrightarrow \\ & H^1(G, A_1) \longrightarrow H^1(G, A) \longrightarrow H^1(G, \mathbb{Z}/p\mathbb{Z}) \longrightarrow \cdots \end{aligned}$$

But by hypothesis $H^n(G, A_1) = 0$ and $H^n(G, \mathbb{Z}/p\mathbb{Z}) = 0$ for n large enough, and therefore the above long exact sequence ends. Hence

$$n_0(A_1) - n_0(A) + n_0(\mathbb{Z}/p\mathbb{Z}) - n_1(A_1) + n_1(A) - n_1(\mathbb{Z}/p\mathbb{Z}) + \cdots = 0.$$

So

$$\sum_q (-1)^q n_q(A_1) - \sum_q (-1)^q n_q(A) + \sum_q (-1)^q n_q(\mathbb{Z}/p\mathbb{Z}) = 0$$

i.e.,

$$\chi(G, A_1) - \chi(G, A) + \chi(G) = 0 \ .$$

Thus

$$\chi(G, A) = \chi(G, A_1) + \chi(G) = \chi(G) + (a - 1)\chi(G) = a\chi(G).$$

∎

p. 227 PROPOSITION 5.2: *Let H be an open subgroup of a pro-p-group G. Assume $\chi(G)$ exists. Then $\chi(H)$ exists and*

$$\chi(H) = (G : H)\chi(G).$$

Proof: By Shapiro's Lemma

$$H^q(H, \mathbb{Z}/p\mathbb{Z}) \approx H^q\big(G, M_H^G(\mathbb{Z}/p\mathbb{Z})\big).$$

Then, $\chi\big(G, M_H^G(\mathbb{Z}/p\mathbb{Z})\big)$ exists by Lemma 5.1, and

$$\chi(H) = \chi\big(G, M_H^G(\mathbb{Z}/p\mathbb{Z})\big) = \dim M_H^G(\mathbb{Z}/p\mathbb{Z}) \cdot \chi(G).$$

But

$$\begin{aligned} M_H^G(\mathbb{Z}/p\mathbb{Z}) &= \{x\colon G \longrightarrow \mathbb{Z}/p\mathbb{Z} |\ x \text{ continuous},\ x(\sigma\tau) = \sigma x(\tau) = x(\tau),\ \sigma \in H,\ \tau \in G\} \\ &\approx \{x\colon G/H \longrightarrow \mathbb{Z}/p\mathbb{Z}\} = (\mathbb{Z}/p\mathbb{Z})^{(G:H)}\ ; \end{aligned}$$

so $\dim M_H^G(\mathbb{Z}/p\mathbb{Z}) = (G : H)$. ∎

p. 228 PROPOSITION 5.3: *Let N be a normal closed subgroup of a pro-p-group G. Assume $\chi(N)$ and $\chi(G/N)$ exist. Then $\chi(G)$ exists and*

$$\chi(G) = \chi(N) \cdot \chi(G/N).$$

Proof: Consider the Lyndon-Hochschild-Serre spectral sequence

$$E_2^{i,j} = H^i\big(G/N, H^j(N, \mathbb{Z}/p\mathbb{Z})\big) \Rightarrow H^q(G, \mathbb{Z}/p\mathbb{Z})\ .$$

Notice that by our assumptions and Lemma 5.1, each $E_2^{i,j}$ is finite and $E_2^{i,j} = 0$ for large i or j.

Since $H^q(G, \mathbb{Z}/p\mathbb{Z})$ has a filtration whose corresponding quotients are the $E_\infty^{i,j}$, $i + j = q$, one has

$$\chi(G) = \sum_q (-1)^q \dim H^q(G, \mathbb{Z}/p\mathbb{Z}) = \sum_q (-1)^q \sum_{i+j=q} \dim E_\infty^{i,j} = \sum_{i,j} (-1)^{i+j} \dim E_\infty^{i,j}.$$

If $A = \{A^{i,j}\}$ is a bigraded vector space with each $A^{i,j}$ finite dimensional, and $A^{i,j} = 0$ for large i or j, we write

$$\chi(A) = \sum_{i,j} (-1)^{i+j} \dim A^{i,j}.$$

p. 229

Now we show that in the case of the Lyndon-Hochschild-Serre spectral sequence $\chi(E_2) = \chi(E_\infty)$. For this we use the following notation

$$\begin{aligned} B_r^{i,j} &= d_r E_r^{i-r,j+r-1} \subseteq E_r^{i,j} \\ Z_r^{i,j} &= \ker(d_r\colon E_r^{i,j} \longrightarrow E_r^{i+r,j-r+1}). \end{aligned}$$

Then we obtain canonical short exact sequences (see Ch. III, Def. 1.2)

$$0 \longrightarrow B_r^{i,j} \longrightarrow Z_r^{i,j} \longrightarrow E_{r+1}^{i,j} \longrightarrow 0$$
$$0 \longrightarrow Z_r^{i,j} \longrightarrow E_r^{i,j} \longrightarrow B_r^{i+r,j-r+1} \longrightarrow 0\ .$$

From them we deduce

$$\chi(E_{r+1}) = \chi(Z_r) - \chi(B_r), \qquad \text{and} \qquad -\chi(B_r) = \chi(E_r) - \chi(Z_r).$$

Hence, $\chi(E_{r+1}) = \chi(E_r)$, and so $\chi(E_2) = \chi(E_\infty)$.

p. 230 Finally,

$$\begin{aligned}\chi(G) =& \chi(E_\infty) = \chi(E_2) = \\ &\sum_j (-1)^j \left(\sum_i (-1)^i \dim E_2^{i,j} \right) = \\ &\sum_j (-1)^j \left(\sum_i (-1)^i \dim H^i\big(G/N, H^j(N, \mathbb{Z}/p\mathbb{Z})\big) \right) = \\ &\sum_j (-1)^j \chi\big(G/N, H^j(N, \mathbb{Z}/p\mathbb{Z})\big) = \\ &\sum_j (-1)^j \dim H^j(N, \mathbb{Z}/p\mathbb{Z}) \cdot \chi(G/N) = \chi(N) \cdot \chi(G/N).\end{aligned}$$

∎

Remark. Propositions 5.2 and 5.3 suggest the following definition. Assume G is a pro-p-group, and let H be an open subgroup of G for which $\chi(H)$ exists. Then define

$$\chi(G) = \frac{1}{(G:H)} \chi(H).$$

Then one can prove that this definition is independent of the choice of H.

p. 231 **§6. Generators and relations**

Let G_1, G_2 be pro-p-groups. A continuous homomorphism $f\colon G_1 \longrightarrow G_2$ induces a homomorphism

$$H^1(f)\colon H^1(G_2) = \mathrm{Hom}_c(G_2, \mathbb{Z}/p\mathbb{Z}) \longrightarrow H^1(G_1) = \mathrm{Hom}_c(G_1, \mathbb{Z}/p\mathbb{Z}),$$

given by

$$\chi \mapsto \chi \cdot f,$$

where $\mathrm{Hom}_c(G, \mathbb{Z}/p\mathbb{Z})$ denotes continuous homomorphisms.

LEMMA 6.1: *f surjective $\Leftrightarrow$ $H^1(f)$ injective.*

Proof: $\Rightarrow$: Trivial

$\Leftarrow$: Assume that $H^1(f)$ is injective and that $f(G_1) \neq G_2$. Choose an open normal subgroup U of G_2 such that $f(G_1)U \neq G_2$, and put $P_2 = G_2/U$. Let P_1 be the canonical image of $f(G_1)$ on P_2; then $P_1 \neq P_2$. Let N be a normal subgroup of index p of P_2 with $N \supseteq P_1$ (cf. [H], p. 44). Then the homomorphism

p. 232

$$\chi\colon G_2 \longrightarrow P_2 \longrightarrow P_2/N = \mathbb{Z}/p\mathbb{Z}$$

is non-trivial. However $H^1(f)\chi = \chi \cdot f = 0$. A contradiction. ∎

If C is a pro-p-group let

$$G^* = \cap N$$

where N runs through the set of open normal subgroups of G of index p. G/G^* is clearly compact, and from the natural injection

$$G/G^* \longrightarrow \pi G/N$$

one sees that G/G^* is abelian, annihilated by p. Moreover, let G_0 be the closure of the subgroup of G generated by the commutator of G and the elements of the form σ^p, $\sigma \in G$. Then $G^* = G_0$. For assume $\sigma \in G^* \backslash G_0$; let U be open normal in G such that $\sigma U \cap G_0 U = \emptyset$; then $(G/U)/(G_0U/U)$ is elementary p-primary, i.e., of the form $\oplus\mathbb{Z}/p\mathbb{Z}$; hence there is a continuous homomorphism $\varphi\colon G \longrightarrow \mathbb{Z}/p\mathbb{Z}$ with $\varphi(\sigma) \neq 0$; thus $\sigma \notin G^*$; a contradiction.

p. 233 PROPOSITION 6.2: *$H^1(G)$ and G/G^* are (Pontrjagin) dual.*

Proof:

$$\mathrm{Hom}_c(G/G^*, \mathbb{R}/\mathbb{Z}) \approx \mathrm{Hom}_c(G/G^*, \mathbb{Z}/p\mathbb{Z}) \approx \mathrm{Hom}_c(G, \mathbb{Z}/p\mathbb{Z}) = H^1(G).$$

∎

Now we can extend Lemma 6.1 to the following

PROPOSITION 6.3: *Let $f: G_1 \longrightarrow G_2$ be a continuous homomorphism of pro-p-groups. Then the following are equivalent statements*

(i) *f is surjective,*

(ii) *$H^1(f): H^1(G_2) \longrightarrow H^1(G_1)$ is injective,*

(iii) *$f^*: G_1/G_1^* \longrightarrow G_2/G_2^*$ is surjective.*

Example. Let $G = F_I(p)$ (the free pro-p-group on the set I). Then

$$H^1(G) = \mathrm{Hom}_c(G, \mathbb{Z}/p\mathbb{Z}) \approx \{x: I \longrightarrow \mathbb{Z}/p\mathbb{Z} |\ x(i) = 0,\ \text{a.e. } i \in I\} \approx \coprod_I \mathbb{Z}/p\mathbb{Z}.$$

Hence, by Prop. 6.2, $G/G^* \approx \prod_I \mathbb{Z}/p\mathbb{Z}$.

p. 234

LEMMA 6.4: *Let G be a pro-p-group, I a set, and*

$$\theta: H^1(G) \longrightarrow H^1\big(F_I(p)\big) = \coprod_I \mathbb{Z}/p\mathbb{Z}$$

a homomorphism. Then

(i) *there exists a continuous homomorphism*

$$f: F_I(p) \longrightarrow G$$

such that $H^1(f) = \theta$,

(ii) *f is surjective $\Leftrightarrow$ θ injective,*

(iii) *θ is bijective and $\mathrm{cd}(G) \leq 1 \Rightarrow f$ is bijective.*

Proof:

(i) θ induces $\theta^*: F_I(p)/F_I(p)^* \longrightarrow G/G^*$, from which we obtain a map

$$\overline{\theta}: F_I(p) \longrightarrow G/G^*.$$

p. 235 Since $\mathrm{cd}(F_I(p)) \leq 1$, by Prop. 3.1, there exists a continuous homomorphism $f\colon F_I(p) \longrightarrow G$ such that

$$\begin{array}{ccccccccc} & & & & & & F_I(p) & & \\ & & & & & \swarrow^{f} & \downarrow{\scriptstyle \bar{\theta}} & & \\ 1 & \longrightarrow & G^* & \longrightarrow & G & \longrightarrow & G/G^* & \longrightarrow & 1 \end{array}$$

commutes. It is plain that $H^1(f) = \theta$.

(ii) This is the content of Lemma 6.1.

(iii) Since $\mathrm{cd}(G) \leq 1$, by Prop. 3.1, there exists a continuous homomorphism $s\colon G \longrightarrow F_I(p)$ such that $f \cdot s = \mathrm{id}_G$

$$1 \longrightarrow K \longrightarrow F_I(p) \underset{s}{\overset{f}{\rightleftarrows}} G \longrightarrow 1.$$

So, $H^1(s) \cdot H^1(f) = \mathrm{id}$. And since $H^1(f) = \theta$ is an isomorphism, so is $H^1(s)$. Therefore s is surjective. Thus f is an isomorphism. ∎

THEOREM 6.5: *Let G be a pro-p-group. Then, the following statements are equivalent*

(i) $\mathrm{cd}(G) \leq 1$

(ii) $H^2(G) = 0$

p. 236 *(iii) G is a free pro-p-group.*

Proof: By Cor. 3.2 and Cor. 4.2 it suffices to show the implication (i) $\longrightarrow$ (iii). Since $H^1(G)$ is a $\mathbb{Z}/p\mathbb{Z}$-vector space we have

$$H^1(G) \approx \coprod_I \mathbb{Z}/p\mathbb{Z}$$

for some index set I. Hence (see example on p. 233),

$$\theta\colon H^1(G) \approx H^1\big(F_I(p)\big).$$

Thus, by Prop. 6.4, $G \approx F_I(p)$. ∎

COROLLARY 6.6: *Every closed subgroup H of a free pro-p-group G is a free pro-p-group.*

Proof: By Prop. 2.1, $\mathrm{cd}(H) \leq \mathrm{cd}(G) \leq 1$. ∎

We recall that if G is a profinite group a subset of G converging to 1 is said to

p. 237 generate G (topologically) if it generates (algebraically) a dense subgroup of G.

Definition 6.7. Let G be a profinite group. We define the *rank* of G as the minimal cardinality of a generating set of G.

THEOREM 6.8: *Let G be a pro-p-group. Then*

$$\operatorname{rank}(G) = \dim H^1(G).$$

Proof: Assume $\dim H^1(G) = \operatorname{card} I$, for some set I. Then there is an isomorphism

$$\theta\colon H^1(G) \longrightarrow H^1\big(F_I(p)\big)$$

(see example on p. 233). Hence by Lemma 6.4, there exists a surjective continuous homomorphism $f\colon F_I(p) \longrightarrow G$. Thus

$$\operatorname{rank}(G) \leq \operatorname{card}(I) = \dim H^1(G)\ .$$

Now, assume $\operatorname{rank}(G) = \operatorname{card}(J)$, for some set J. Then there is a continuous epimor-
p. 238 phism $f\colon F_J(p) \longrightarrow G$. By Lemma 6.4, f induces an injection

$$H^1(G) \longrightarrow H^1\big(F_J(p)\big).$$

Thus,

$$\dim H^1(G) \leq \dim H^1\big(F_I(p)\big) = \operatorname{card}(I) = \operatorname{rank}(G).$$

∎

Definition 6.9. Let F be a profinite group and R a closed normal subgroup of F. We say that a subset $\{\rho_\alpha |\ \alpha \in A\}$ of R converging to 1 is a *set of generators of R as a normal subgroup of F*, if the F-conjugates of the ρ_α generate (algebraically) a dense subgroup of R, i.e., if R is the smallest closed normal subgroup of F containing the ρ_α. We define $\operatorname{rank}_F(R)$ to be the smallest cardinal of a generating set of R as a normal subgroup of F.

PROPOSITION 6.10: *Let F be a pro-p-group and R a closed normal subgroup of F. Then*

$$\operatorname{rank}_F(R) = \dim H^1(R)^F$$

p. 239 *where $H^1(R)^F$ is the fixed submodule of $H^1(R)$ under the action of F as described in the remark on p. 172.*

Proof: First we show that $\operatorname{rank}_F(R) \geq \dim H^1(R)^F$. Assume $\operatorname{rank}_F(R) = \operatorname{card}(A)$, where $\{\rho_\alpha |\ \alpha \in A\}$ is a generating set of R as normal subgroup of F. Define a homomorphism

$$\varphi\colon H^1(R)^F \longrightarrow \coprod_A \mathbb{Z}/p\mathbb{Z}$$

by $\varphi(\chi) = \chi(\rho_\alpha)$. Then φ is injective for suppose $\chi(\rho_\alpha) = 0$ for $\alpha \in A$. Then, if $\sigma \in F$

$$\chi(\sigma\rho_\alpha\sigma^{-1}) = \chi^\sigma(\rho_\alpha) = \chi(\rho_\alpha) = 0.$$

So $\chi = 0$ on a dense subgroup of R. Thus $\chi = 0$.

We now prove that $\operatorname{rank}_F(R) \leq \dim H^1(R)^F$. Observe that since $H^1(R)$ and R/R^* are dual (Prop. 6.2), the dual of $H^1(R)^F$ will be a quotient group $\widetilde{R}$ of R/R^*. On the other hand put

$$H^1(R)^F = \coprod_A \mathbb{Z}/p\mathbb{Z} \cdot \chi_\alpha$$

where $\{\chi_\alpha |\ \alpha \in A\}$ is a basis for $H^1(R)^F$. Then

$$\widetilde{R} \approx \prod_A \mathbb{Z}/p\mathbb{Z}\widetilde{\rho}_\alpha$$

p. 240

where $\chi_\alpha(\widetilde{\rho}_\beta) = \delta_{\alpha\beta}$. Since $\operatorname{cd}\big(F_A(p)\big) \leq 1$, the canonical continuous homomorphism $F_A(p) \longrightarrow \widetilde{R}$ given by $\alpha \mapsto \widetilde{\rho}_\alpha$ can be lifted to $F_A(p) \longrightarrow R$. Let $\rho_\alpha \in R$ be the image of α under this homomorphism. Then $\{\rho_\alpha |\ \alpha \in A\} \subseteq R$ is a set converging to 1. We claim that $\{\rho_\alpha |\ \alpha \in A\}$ is a set of generators of R (as a normal subgroup of F). For, let R' be the smallest closed normal subgroup of F containing the ρ_α. Then $R' \hookrightarrow R$. We shall show that this map is surjective, or equivalently, that its induced map

$$f\colon H^1(R) \longrightarrow H^1(R')$$

is injective. In fact it suffices to show that its restriction

$$\overline{f}\colon H^1(R)^F \longrightarrow H^1(R')^F$$

is injective. ($\overline{f}$ injective $\Rightarrow$ ker f contains no element different from 0 invariant under F $\Rightarrow$ ker $f = 0$, otherwise take a non-zero simple submodule A_1 of ker f; then $A_1 \approx \mathbb{Z}/p\mathbb{Z}$).

p. 241 Let $\chi \in H^1(R)^F$, and assume $\chi(R') = 0$. Then $\chi(\rho_\alpha) = 0$; so $\chi(\widetilde{\rho}_\alpha) = 0\ \forall \alpha \in A$. Hence $\chi(\widetilde{R}) = 0$, i.e., $\chi = 0$. ∎

Let G be a pro-p-group and $\{\sigma_i |\ i \in I\}$ a set of generators of G. Set $F = F_I(p)$ (the free pro-p-group on I). Then there exists a unique continuous homomorphism

$$F \longrightarrow G$$

mapping i onto σ_i. Let R be its kernel. A set of generators of R (as a normal subgroup of F) is called a *set* of *defining relations* corresponding to $\{\sigma_i |\ i \in I\}$.

Assume now that $\text{rank}(G) = \text{card}(I)$ is finite and let F and R be as above. Then, define

$$\text{relation rank}(G) = \text{rank}_F(R).$$

THEOREM 6.11: *Let G be a finitely generated pro-p-group. Then*

$$\text{relation rank}(G) = \dim H^2(G)\ .$$

p. 242 *Proof:* Let $\text{rank}(G) = \text{card}(I)$ and consider the exact sequence described above

$$1 \longrightarrow R \longrightarrow F \longrightarrow G \longrightarrow 1$$

where $F = F_I(p)$. By Cor. 5.4, Ch. III, we obtain a five term exact sequence

$$0 \longrightarrow H^1(G) \longrightarrow H^1(F) \longrightarrow H^1(R)^F \longrightarrow H^2(G) \longrightarrow H^2(F).$$

Since both $H^1(G)$ and $H^1(F)$ are finite dimensional $\mathbb{Z}/p\mathbb{Z}$-vectors spaces of the same dimension (Th. 6.8 and example on p. 233), the monomorphism $H^1(G) \longrightarrow H^1(F)$ must be an isomorphism. Since F is free $H^2(F) = 0$. Hence $H^1(R)^F \approx H^2(G)$. The result follows now from Prop. 6.10. ∎

Now, let G be a finite p-group. Let $n(G) = \dim H^1(G)$ and $r(G) = \dim H^2(G)$. (Hence both $n(G)$ and $r(G)$ are finite.)

PROPOSITION 6.12: *Let G be a finite p-group. Then*

$$r(G) - n(G) = \operatorname{rank} H^3(G, \mathbb{Z})$$

p. 243 *(rank $H^3(G,\mathbb{Z})$ = no. of cyclic summands of $H^3(G,\mathbb{Z})$).*

Proof: Consider the short exact sequence

$$0 \longrightarrow \mathbb{Z} \xrightarrow{p} \mathbb{Z} \longrightarrow \mathbb{Z}/p\mathbb{Z} \longrightarrow 0$$

where p is multiplication by p. From it we obtain a corresponding exact sequence

$$0 \longrightarrow H^1(G) \longrightarrow H^2(G,\mathbb{Z}) \xrightarrow{p} H^2(G,\mathbb{Z}) \longrightarrow H^2(G) \longrightarrow H^3(G,\mathbb{Z})_p \longrightarrow 0,$$

where $H^3(G,\mathbb{Z})_p$ denotes the subgroup of elements of $H^3(G,\mathbb{Z})$ annihilated by p. Since G is finite each $H^i(G,\mathbb{Z})$, $i \geq 1$, is finitely generated torsion, and hence finite (see, e.g., [S2], p. 138). Therefore

$$\dim H^1(G) - \dim H^2(G,\mathbb{Z}) + \dim H^2(G,\mathbb{Z}) - \dim H^2(G) + \dim H^3(G,\mathbb{Z})_p = 0$$

i.e.

$$r(G) - n(G) = \dim H^3(G,\mathbb{Z})_p.$$

On the other hand it is plain that $\dim H^3(G,\mathbb{Z})_p = \operatorname{rank} H^3(G,\mathbb{Z})$, since every cyclic summand of $H^3(G,\mathbb{Z})$ contains exactly p elements of order p. ∎

p. 244

CHAPTER V

GALOIS COHOMOLOGY OF FIELDS

In this chapter we apply the results obtained in the preceding chapters for general profinite groups to the study of certain problems arising in field extension theory.

All valuations considered in this chapter are rank 1 valuations.

Assume $N|K$ is a Galois extension of fields and let $L|K$ be a finite normal subextension of $N|K$. Then one obtains a natural short exact sequence of Galois groups

$$1 \longrightarrow G_{N|L} \longrightarrow G_{N|K} \longrightarrow G_{L|K} \longrightarrow 1.$$

Set $G = G_{N|K}$. Then, by Prop. 1.5 and Th. 2.2 of Ch. I, we have

$$G = \varprojlim_{L|K} G_{L|K} \tag{1}$$

where $L|K$ runs through all finite normal subextensions of $N|K$; and the groups $G_{N|L}$
p. 245 form a basis of open neighborhoods of 1.

Let $A \in \mathrm{Mod}(G)$, and write $A_L = A^{G_{N|L}}$. Then, by the definition of G-module,

$$A = \varinjlim_{L|K} A_L$$

($L|K$ finite normal subextension of $N|K$). So, by Cor. 4.2, Ch. II, we have for $q \geq 0$

$$H^q(G_{N|K}, A) \approx \varinjlim_{L|K} H^q(G_{L|K}, A_L)$$

($L|K$ runs through all normal finite subextensions of $N|K$).

We shall often be interested in $G_K = G_{K_s|K}$, where K_s is the algebraic separable closure of K.

If $N|K$ is a Galois extension and $G = G_{N|K}$, the additive group N^+ and multiplicative group N^* are endowed in a natural way with a G-module structure.

p. 246 §**1. Hilbert's Theorem 90**

PROPOSITION 1.1: *Let $N|K$ be a Galois extension, and $G = G_{N|K}$. Then*

$$H^q(G, N^+) = 0, \quad q \geq 1.$$

Proof: By (1) we may assume $[N : K] < \infty$. Then by the normal basis theorem ([B2], §10, Th. 5) there exists $c \in N$ such that

$$N^+ = \bigoplus_{\sigma \in G} K^+ \sigma c.$$

But this is clearly G-isomorphic with $M_G^1(K^+c)$ (see Cor. 7.5, Ch. II). Thus

$$H^q(G, N^+) = 0, \quad q \geq 1.$$

∎

PROPOSITION 1.2 (Hilbert's Theorem 90): *Let $N|K$ be a Galois extension and $G = G_{N|K}$. Then*

$$H^1(G, N^*) = 1.$$

p. 247 *Proof:* By (1) we may assume $[N : K] < \infty$. Let $\sigma \mapsto a_\sigma$ be a 1-cocycle of G into N^*, i.e.,

$$a_{\sigma\tau} = a_\sigma \cdot \sigma a_\tau$$

(see §2, Ch. II; here we use the multiplicative notation). By the linear independence of automorphism (cf. [B2], §7, Th. 3) there exists $c \in N$ such that

$$0 \neq b = \sum_{\tau \in G} a_\tau \cdot \tau c.$$

Then, for $\sigma \in G$ one has

$$\sigma b = \sum_{\tau \in G} \sigma a_\tau \cdot \sigma\tau c = \sum_{\tau \in G} a_\sigma^{-1} \cdot a_{\sigma\tau} \cdot \sigma\tau c = a_\sigma^{-1} \cdot b.$$

Thus

$$a_\sigma = \frac{\sigma(b^{-1})}{b^{-1}}.$$

I.e. a_σ is a 1-coboundary. ∎

COROLLARY 1.3: *Let $N|K$ be a finite Galois extension with $G = G_{N|K}$ cyclic, say*
p. 248 *$G = (\sigma)$. Let $a \in N^*$. Then*

$$\mathfrak{N}_{N|K}(a) = 1 \Leftrightarrow a = \frac{\sigma b}{b}, \text{ some } b \in N \ .$$

($\mathfrak{N}_{N|K}$ is the norm).

Proof: Let $\#G = n$.

$\Leftarrow$): $\mathfrak{N}_{N|K}(a) = a \cdot \sigma(a) \cdot \sigma^2(a) \cdots \sigma^{n-1}(a) = 1$.

$\Rightarrow$): Consider the map $x\colon G \longrightarrow A$ given by

$$x(\sigma^\ell) = \prod_{i=0}^{\ell-1} \sigma^i a, \quad \ell \geq 1.$$

This is well-defined since $x(\sigma^n) = \mathfrak{N}_{N|K}(a) = 1$. Then

$$x(\sigma^r\sigma^s) = x(\sigma^{r+s}) = \left(\prod_{i=1}^{r-1} \sigma^i a\right)\left(\prod_{i=r}^{r+s} \sigma^i a\right) = x(\sigma^r) \cdot \sigma^r x(\sigma^s).$$

So x is a 1-cocycle, and by Prop. 1.2 a 1-coboundary. I.e. there is a $b \in N$ with

$$x(\sigma^k) = \frac{\sigma^k b}{b} \qquad \text{(all } k\text{)}.$$

p. 249 In particular $a = x(\sigma) = \frac{\sigma b}{b}$. ∎

COROLLARY 1.4: *Let $N \supseteq L \supseteq K$ be Galois extensions of K. Then there is an exact sequence*

$$1 \longrightarrow H^2(G_{L|K}, L^*) \xrightarrow{\text{Inf}} H^2(G_{N|K}, N^*) \xrightarrow{\text{Res}}$$
$$H^2(G_{N|L}, N^*)^{G_{N|L}} \xrightarrow{\text{tr}} H^3(G_{L|K}, L^*) \xrightarrow{\text{Inf}} H^3(G_{N|K}, N^*).$$

Proof: By Prop. 1.2, $H^1(G_{N|K}, N^*) = 0$. Therefore the result follows from Cor. 5.4, Ch. III. ∎

p. 250 §**2. The Brauer group**

In this section we remind the reader of the definition and essential features of the Brauer group. For more details see, e.g., [S2], p. 164.

Let K be a field. A central simple K-algebra is a K-algebra whose center is K and with no non-trivial two-sided ideals. If A and B are finitely dimensional central simple K-algebras, then

$$A \approx M_n(D) \qquad \text{and} \qquad B \approx M_m(D'),$$

where D and D' are division rings with center K (Wedderburn-Artin Th.). We say that A and B are similar ($A \sim B$) if $D \approx D'$. Denote by B_K the set of equivalence classes $[A]$ of finite dimensional central simple algebras. If $[A], [B] \in B_K$ then $[A \otimes_K B] \in B_K$. This operation makes B_K into a group, the *Brauer group of the field* K. The unit element of B_K is

$$[K] = \{M_n(K) |\ n \in \mathbb{N}\}.$$

Also, if $[A] \in B_K$, $[A]^{-1} = [A^{op}]$, where A^{op} represents the opposite ring.

p. 251 Let $K'|K$ be a field extension. Then there is a group homomorphism

$$B_K \longrightarrow B_{K'}$$

given by $A \mapsto A \otimes_K K'$. The kernel of this homomorphism is denoted by $B_{K'|K}$, and consists of those K-algebra classes which "split" over K', i.e. which become full matrix algebras over K'.

In particular one can prove

$$B_K = B_{K_s|K} = \bigcup_{L|K} B_{L|K}$$

where $L|K$ runs through the finite Galois extensions.

THEOREM 2.1: *Let $N|K$ be a Galois extension, and $G = G_{N|K}$. Then*

$$\Phi\colon H^2(G, N^*) \approx B_{N|K}.$$

In particular, $H^2(G_K, K_s^*) \approx B_K$.

Although we shall not attempt to prove this theorem, we will describe the isomorphism Φ, when $[N : K] < \infty$. Let $\bar{x} \in H^2(G, N^*)$. Consider the K-vector space

p. 252

$$A = \bigoplus_{\sigma \in G} N u_\sigma$$

where the u_σ are symbols. Define a multiplication on A by

(i) $u_\sigma \cdot a = a^\sigma \cdot u_\sigma$, $a \in N$;

(ii) $u_\sigma \cdot u_\tau = x(\sigma, \tau) \cdot u_{\sigma\tau}$.

Under this multiplication A is a central simple K-algebra. We define $\Phi(\bar{x}) = A$. Finally we state without proof the following

THEOREM 2.2: *Let $N \supseteq L \supseteq K$ be Galois extensions of K. Then*

$$\begin{array}{ccccccc} 0 & \longrightarrow & H^2(G_{L|K}, L^*) & \xrightarrow{\text{Inf}} & H^2(G_{N|K}, N^*) & \xrightarrow{\text{Res}} & H^2(G_{N|L}, N^*) \\ & & \downarrow{\scriptstyle \Phi} & & \downarrow{\scriptstyle \Phi} & & \downarrow{\scriptstyle \Phi} \\ 0 & \longrightarrow & B_{L|K} & \longrightarrow & B_{N|K} & \longrightarrow & B_{N|L} \end{array}$$

is a commutative diagram, where the rows are exact.

p. 253

§3. Cohomological dimension of Galois groups

Let k be a field and p a prime number. Denote by $k(p)$ the *maximal Galois p-extension* of k, i.e. the union of all finite Galois subextensions $K|k$ of $k_s|k$ of degree p^n for some n, where k_s is the algebraic separable closure of k. Set

$$G_k(p) = G_{k(p)|k}.$$

Clearly $G_k(p)$ is the maximal pro-p-quotient group of G_k, i.e.

$$G_k(p) = G/N$$

where N is the intersection of all closed subgroups of G of index p^n for some n.

In this section we will investigate the cohomological dimension of G_k and $G_k(p)$.

LEMMA 3.1: *Let G be any profinite group and $G(p) = G/N$ its maximal pro-p-quotient*
p. 254 *group, where N is as above. Then, if $\mathrm{cd}_p(N) \leq 1$ one has that*

$$\mathrm{Inf}\colon H^q\big(G(p), \mathbb{Z}/p\mathbb{Z}\big) \longrightarrow H^q(G, \mathbb{Z}/p\mathbb{Z})$$

is an isomorphism for $q \geq 0$.

Proof: This is clear for $q = 0$. Assume $\varphi\colon N \longrightarrow \mathbb{Z}/p\mathbb{Z}$ is a continuous non-trivial homomorphism and let $M = \ker\varphi$. Set

$$M_0 = \bigcap_{\sigma\in G} \sigma M_\sigma^{-1}.$$

Then M_0 is normal in G and of p-power index, since M is of p-power index and the obvious homomorphism

$$N/M_0 \longrightarrow \prod_{\sigma\in G} N/\sigma M\sigma^{-1}$$

is an injection. Hence G/M_0 is a pro-p-group with $M_0 \not\subseteq N$ which contradicts the minimality of N. So

$$H^1(N, \mathbb{Z}/p\mathbb{Z}) = \mathrm{Hom}_c(N, \mathbb{Z}/p\mathbb{Z}) = 0.$$

Therefore by our hypothesis $H^n(N, \mathbb{Z}/p\mathbb{Z}) = 0$ for $n \geq 0$. So by Cor. 5.4, Ch. III there is an exact sequence

p. 255 $$0 \longrightarrow H^q\big(G(p), \mathbb{Z}/p\mathbb{Z}\big) \xrightarrow{\mathrm{Inf}} H^q(G, \mathbb{Z}/p\mathbb{Z}) \longrightarrow H^q(N, \mathbb{Z}/p\mathbb{Z}) = 0$$

corresponding to the group extension

$$1 \longrightarrow N \longrightarrow G \longrightarrow G(p) \longrightarrow 1.$$

Thus Inf is an isomorphism. ∎

COROLLARY 3.2: *Let G be a profinite group and $\mathrm{cd}_p(G) \leq 1$. Then $G(p)$ is a free pro-p-group.*

Proof: Put $G(p) = G/N$ where N is the intersection of all closed subgroups of p-power index. By Prop. 2.1, Ch. IV, $\mathrm{cd}_p(N) \leq \mathrm{cd}_p(G) \leq 1$. So, by the above Lemma, $H^n(G(p), \mathbb{Z}/p\mathbb{Z}) = 0$ if $n \geq 2$. Thus, by Cor. 4.2, Ch. IV, $\mathrm{cd}(G(p)) \leq 1$. The result follows now from Th. 6.5, Ch. IV. ∎

p. 256 THEOREM 3.3: *Let k be a field and $p = \text{char } k$. Then $\text{cd}_p(G_k) \leq 1$.*

Proof: First we shall prove that $H^2(G_k, \mathbb{Z}/p\mathbb{Z}) = 0$. Define a G_k-homomorphism

$$f: k_s^+ \longrightarrow k_s^+$$

by $f(x) = x^p - x$. Then f is surjective for if $a \in k_s^+$, the equation $x^p - x - a = 0$ has solutions in k_s^+ since k_s is separably closed. The kernel of f is the prime field of k, and hence G_k-isomorphic to $\mathbb{Z}/p\mathbb{Z}$. Therefore we obtain an exact sequence of G_k-modules

$$0 \longrightarrow \mathbb{Z}/p\mathbb{Z} \longrightarrow k_s^+ \xrightarrow{f} k_s^+ \longrightarrow 0;$$

and from this we get a corresponding exact sequence

$$0 = H^1(G_k, k_s^+) \longrightarrow H^2(G_k, \mathbb{Z}/p\mathbb{Z}) \longrightarrow H^2(G_k, k_s^+) = 0$$

(see Prop. 1.1). Thus $H^2(G_k, \mathbb{Z}/p\mathbb{Z}) = 0$. Now, if H is any closed subgroup of G_k,
p. 257 there is some intermediate field $k \subseteq k' \subseteq k_s$, with $H = G_{k'}$. So, $H^2(H, \mathbb{Z}/p\mathbb{Z}) = 0$. In particular let H be a p-Sylow group of G_k. Then, by Cor. 2.2 and Cor. 4.2 in Ch. IV,

$$\text{cd}_p(G_k) = \text{cd}(H) \leq 1.$$

∎

COROLLARY 3.4: *Let k be a field of characteristic p. Then $G_k(p)$ is a free pro-p-group of rank $r = \dim_{\mathbb{Z}/p\mathbb{Z}} k/f(k)$.*

Proof: It is an immediate consequence of Th. 3.3 and Cor. 3.2 that $G_k(p)$ is a free pro-p-group. Now consider the exact sequence of G_k-modules

$$0 \longrightarrow \mathbb{Z}/p\mathbb{Z} \longrightarrow k_s^+ \xrightarrow{f} k_s^+ \longrightarrow 0.$$

The corresponding exact sequence in cohomology gives us

$$\begin{array}{ccccccc} H^0(G_k, k_s^+) & \xrightarrow{f} & H^0(G_k, k_s^+) & \longrightarrow & H^1(G_k, \mathbb{Z}/p\mathbb{Z}) & \longrightarrow & 0 \\ \approx\downarrow & & \approx\downarrow & & \approx\downarrow & & \\ k & \longrightarrow & k & \longrightarrow & H^1(G_k(p), \mathbb{Z}/p\mathbb{Z}) & \longrightarrow & 0 \end{array}$$

(see Lemma 3.1 and Prop. 1.1). Thus, by Th. 6.8, Ch. IV,

$$\operatorname{rank}\big(G_k(p)\big) = \dim_{\mathbb{Z}/p\mathbb{Z}} k/f(k).$$

∎

p. 258 COROLLARY 3.5: *Let k be a field of characteristic p. Then a pro-p-group G is a Galois group*

$$G \approx G_{K/k}$$

iff G can be generated by $r = \dim_{\mathbb{Z}/p\mathbb{Z}} k/fk$ elements, where $f\colon k \longrightarrow k$ is given by $f(x) = x^p - x$.

Proof: Assume G can be generated by r elements (i.e. there exists a subset converging to 1 of G of cardinality r which generates algebraically a dense subset of G). Let $G_k(p) = G_k/N$. By Cor. 3.4 $G(p)$ is free pro-p of rank r. Consider an exact sequence

$$1 \longrightarrow H/N \longrightarrow G_k/N \longrightarrow G \longrightarrow 1.$$

Then H is a closed normal subgroup of G_k. Let K be the fixed field of H. Then $G \approx G_{K|k}$. The converse is clear. ∎

We now turn to the case when $p \neq \operatorname{char} k$. We say that an abelian group A is p-divisible if given $a \in A$ there exists $b \in A$ with $pb = 1$.

p. 259 THEOREM 3.6: *Let k be a field, $p \neq \operatorname{char} k$ a prime number and let n be a positive integer. Then the following statements are equivalent:*

(i) $\operatorname{cd}_p(G_k) \leq n$;

(ii) $H^{n+1}(G_k, K_s^*)(p) = 0$ *and* $H^n(G_K, K_s^*)$ *is p-divisible for every algebraic extension $K|k$;*

(iii) same as (ii), for $K|k$ finite separable of degree prime to p.

Proof: The map $K_s^* \xrightarrow{p} K_s^*$ given by $x \mapsto x^p$ is a G_K-epimorphism since for $a \in K_s$, the polynomial $X^p - a$ is separable. The kernel μ_p of this map is isomorphic (as an abelian group) to $\mathbb{Z}/p\mathbb{Z}$. From the exact sequence

$$1 \longrightarrow \mu_p \longrightarrow K_s^* \xrightarrow{p} K_s^* \longrightarrow 1$$

we obtain an exact sequence

$$H^n(G_K, K_s^*) \xrightarrow[(1)]{p} H^n(G_K, K_s^*) \xrightarrow{\delta} H^{n+1}(G_K, \mu_p)$$
$$\xrightarrow{i} H^{n+1}(G_K, K_s^*) \xrightarrow[(2)]{p} H^{n+1}(G_K, K_s^*).$$

p. 260 Then,

$$H^n(G_K, K_s^*)\ p-\text{divisible} \Leftrightarrow \text{ map (1) is surjective } \Leftrightarrow \delta = 0.$$

Also,

$$H^{n+1}(G_K, K_s^*)(p) = 0 \Leftrightarrow \text{ map (2) is injective } \Leftrightarrow i = 0.$$

Thus, condition (ii) of the statement is equivalent to $H^{n+1}(G_K, \mu_p) = 0$, for $K|k$ algebraic. Similarly, condition (iii) is equivalent to $H^{n+1}(G_K, \mu_p) = 0$ for $K|k$ finite, separable with $p \nmid [K : k]$.

Now we proceed to prove the implications.

(i) $\Rightarrow$ (ii): Let $K|k$ be algebraic. Then $K_s = Kk_s$, and $G_{k_s|k_s\cap K} \approx G_{k_sK|K} = G_K$ (cf. [B2], §10, Th. 1). So G_K is isomorphic to a closed subgroup of G_k. Hence (see Prop. 2.1, Ch. IV)

$$\mathrm{cd}_p(G) \leq \mathrm{cd}_p(G_k) \leq n.$$

Thus $H^{n+1}(G_K, \mu_p) = 0$.

(ii) $\Rightarrow$ (iii): This is obvious.

p. 261 (iii) $\Rightarrow$ (i): Let H be a p-Sylow group of G_k. Then $H = G_K$ for some field $k_s \supseteq K \supseteq k$. By Prop. 1.6, Ch. I,

$$H = G_K = \bigcap G_{K_i} \approx \varprojlim G_{K_i}$$

where $K_i|k$ runs through the finite separable extensions with $p \nmid [K_i : k]$, $K \supseteq K_i$. Hence

$$H^{n+1}(G_K, \mu_p) = \varinjlim H^{n+1}(G_{K_i}, \mu_p) = 0.$$

Now, since G_K is a pro-p-group it operates trivially on μ_p (see Prop. 4.1, Ch. IV) i.e.

$$H^{n+1}(G_K, \mathbb{Z}/p\mathbb{Z}) = 0.$$

Thus by Prop. 2.1, Ch. IV and Cor. 4.2, Ch. IV,

$$\mathrm{cd}_p(G_k) = \mathrm{cd}(G_K) \leq n.$$

∎

COROLLARY 3.7: *Let k be a field, and p a prime number with $p \neq \mathrm{char}\ k$. Then the following statements are equivalent*

(i) $\mathrm{cd}_p(G_k) \leq 1$

(ii) $B_K(p) = 0$ *for every algebraic extension* $K|k$.

(iii) $B_K(p) = 0$ *for every finite, separable extension* $K|k$.

p. 262 *Proof:* It follows from Theorem 3.6 and Hilbert's theorem 90. ∎

Remark: If the equivalent conditions of Cor. 3.7 are satisfied, then $G_k(p)$ is a free pro-p-group, by Cor. 3.2. If we assume moreover that $\mu_p \subseteq k$, then

$$\mathrm{rank}\, G_k(p) = \dim k^*/(k^*)^p.$$

For then G_k acts trivially on μ_p, i.e. $\mu_p \approx \mathbb{Z}/p\mathbb{Z}$ as G_k-modules and so from the short exact sequence of G_k-modules

$$0 \longrightarrow \mathbb{Z}/p\mathbb{Z} \longrightarrow k_s^* \xrightarrow{p} k_s^* \longrightarrow 1$$

we deduce an exact sequence of cohomology groups

$$k^* \xrightarrow{p} k^* \longrightarrow H^1(G_k, \mathbb{Z}/p\mathbb{Z}) \longrightarrow H^1(G_k, k_s^*) = 1\ ;$$

so the assertion follows from Th. 6.8, Ch. IV.

COROLLARY 3.8: *Let k be a field. If $B_K = 0$ for $K|k$ finite and separable, then* $\mathrm{cd}(G_k) \leq 1$.

p. 263 *Proof:* It follows from Cor. 3.7 and Th. 3.3. ∎

The converse of this corollary does not hold in general. However if k is perfect we have:

PROPOSITION 3.9: *Let k be a perfect field. If* $\mathrm{cd}(G_k) \leq 1$, *then* $B_K = 0$ *for every finite separable field extension* $K|k$.

Proof: Let $K|k$ be finite and separable. Then $K_s = k_s$ is perfect, and therefore for each prime p there is an exact sequence

$$1 \longrightarrow \mu_p \longrightarrow K_s^* \xrightarrow{p} K_s^* \longrightarrow 1,$$

where p is the map $x \mapsto x^p$. Consider the corresponding exact sequence of cohomology groups

$$\cdots \longrightarrow H^2(G_K, \mu_p) \longrightarrow H^2(G_K, K_s^*) \xrightarrow{p} H^2(G_k, K_s^*) \longrightarrow H^3(G_K, \mu_p) \longrightarrow \cdots ;$$

p. 264 since, for each p, $\mathrm{cd}_p(G_K) \leq \mathrm{cd}_p(G_k) \leq 1$, we deduce that $H^2(G_K, \mu_p) = H^3(G_K, \mu_p) = 1$, and hence

$$H^2(G_K, K_s^*) \approx B_K \xrightarrow{p} B_K$$

is an isomorphism for each prime p. Hence $B_K(p) = 1$. On the other hand, by Cor. 6.7, Ch. II, B_K is torsion. Thus $B_K = 1$, or using the additive notation $B_K = 0$. ∎

PROPOSITION 3.10: *Let k be a field. Then the following statements are equivalent.*

(i) $B_K = 0$ *for every finite separable extension* $K|k$.

(ii) The norm map $\mathfrak{N}_{L|K}: L^* \longrightarrow K^*$ *is surjective for every finite Galois extension* $L|K$, *and every finite separable extension* $K|k$.

Before we prove this proposition we remind the reader of the following result ([S2], p. 152). Given a finite group G and a G-module A consider the Tate cohomology groups defined by

$$\hat{H}^q(G, A) = \begin{cases} H^q(G, A), & q > 0 \\ A^G / N_G A, & q = 0, \end{cases}$$

p. 265 where the map $N_G: A \longrightarrow A$ is given by $N_G a = \sum_{\sigma \in G} \sigma a$. Then

$$\hat{H}^{q_0}(H, A) = \hat{H}^{q_0+1}(H, A) = 0 \text{ for some } q_0 \geq 1 \text{ and for every subgroup } H \text{ of } G$$

implies $\hat{H}^q(G, A) = 0$ for every $q \geq 0$.

Proof of Proposition 3.10: (ii) $\Leftrightarrow 0 = K^*/\mathfrak{N}_{L|K}L^* = \hat{H}^0(G_{L|K}, L^*)$ for every finite Galois extension $L|K$ and every finite separable extension $K|k \Leftrightarrow \hat{H}^0(H, L^*) = 0$ and $H^1(H, L^*) = 0$ for every subgroup $H \subseteq G_{L|K}$, every Galois extension $L|K$ and every finite separable extension $K|k$ (see Prop. 1.2) $\Leftrightarrow H^q(G_{L|K}, L^*) = 0$, for every Galois extension $L|K$ and every finite separable extension $K|k$ (by the result quoted above) $\Leftrightarrow H^2(G_{L|K}, L^*) = 0$ for $L|K$ Galois, and $K|k$ finite separable (by Prop. 1.2 and result quoted above) $\Leftrightarrow$

$$B_K \approx H^2(G_K, K_s^*) \approx \varinjlim_{L|K} H^2(G_{L|K}, L^*) = 0$$

for every $L|K$ Galois, and $K|k$ finite separable, since, by Cor. 1.4, each $H^2(G_{L|K}, L^*)$ is a subgroup of B_K. ∎

p. 266 **§4. The property C_1**

Definition 4.1: Let r be a real number. A field k is called C_r if every homogeneous polynomial $f(X_1, \ldots, X_n) \in k[X_1, \ldots, X_n]$ of degree d with $d^r < n$ has a non-trivial zero $(x_1, \ldots, x_n) \in k^n$.

In this section we investigate the cohomological dimension of C_1 fields.

PROPOSITION 4.2: *If k is C_1 then*

(i) Every algebraic extension of K is C_1;

(ii) $\mathfrak{N}_{L|K}: L^* \longrightarrow K^*$ is surjective for every finite Galois extension $L|K$, where $K|k$ is an algebraic extension.

Proof: (i) Let $k'|k$ be an algebraic extension and let $F(X_1, \ldots, X_n) \in k'[X_1, \ldots, X_n]$ be a homogeneous polynomial of degree $d < n$. Since the coefficients of F are contained in a finite extension of k, we may assume $[k' : k] < \infty$. Say $e_1, \ldots, e_m$ is a basis of $k'|k$. Let X_{ij}, $i = 1, \ldots, m$, $j = 1, \ldots, n$ be indeterminates. Then $[k'(X_{1,1}, \ldots, X_{m,n}) :$
p. 267 $k(X_{11}, \ldots, X_{mn})] = m$ with basis $e_1, \ldots, e_m$ again. Set

$$\bar{X}_j = \sum_{i=1}^{m} X_{ij} e_i, \quad j = 1, \ldots, n.$$

Then $F(\bar{X}_1, \ldots, \bar{X}_n) \in k'(X_{11}, \ldots, X_{mn}]$. So

$$F(X_1, \ldots, X_n)e_i = \sum_{j=1}^{m} f_{ij}e_j, \quad i = 1, \ldots, m,$$

where each f_{ij} is a homogeneous polynomial in $k[X_{11}, \ldots, X_{mn}]$ of degree d. Hence

$$f = \det(f_{ij})$$

is a homogeneous polynomial in $k[X_{11}, \ldots, X_{mn}]$ of degree md in mn variables. Since $K \in C_1$ there is a non-trivial zero of f in k^{mn}. Say $f(\alpha_{11}, \ldots, \alpha_{mn}) = 0$, $0 \neq (\alpha_{11}, \ldots, \alpha_{mn}) \in k^{mn}$. Set

$$\beta_j = \sum_{i=1}^{m} \alpha_{ij}e_i, \quad j = 1, \ldots, n.$$

Then $(\beta_1, \ldots, \beta_n) \neq 0$. Moreover $F(\beta_1, \ldots, \beta_n) = 0$ since the k-linear transformation of k' given by

p. 268

$$a \mapsto F(\beta_1, \ldots, \beta_n)a$$

is singular.

(ii) Let $e_1, \ldots, e_n$ be a basis of L over K. Put $L_1 = L(X_1, \ldots, X_n)$ and $K_1 = K(X_1, \ldots, X_n)$ where $X_1, \ldots, X_n$ are indeterminates. Then $e_1, \ldots, e_n$ is again a basis of the finite Galois extension $L_1|K_1$. Moreover $G = G_{L|K} = G_{L_1|K_1}$. Take

$$X = \sum_{i=1}^{n} X_i e_i.$$

Then $\mathfrak{N}_{L_1|K_1}(X) = \prod_{\sigma \in G} \Big(\sum_{i=1}^{n} X_i \sigma(e_i) \Big)$ is a homogeneous polynomial of degree n with coefficients in K. So, given $a \in K^*$

$$\mathfrak{N}_{L_1|K_1}(X) - aX_{n+1}^n$$

is a homogeneous polynomial of degree n in $n+1$ variables. Hence it has non-trivial zero in K^{n+1}, since K is C_1 by (i). Say

$$0 \neq (b_1, \ldots, b_{n+1}) \in K^{n+1}$$

is such a zero. Clearly $b_{n+1} \neq 0$, for otherwise

p. 269
$$\mathfrak{N}_{L_1|K_1}(b_1e_1 + \cdots + b_ne_n) = 0,$$

and so $b_1e_1 + \cdots + b_ne_n = 0$, i.e., $b_1 = \cdots = b_n = 0$. Thus

$$a = \mathfrak{N}_{L_1|K_1}\left(\frac{b_1e_1 + \cdots + b_ne_n}{b_{n+1}}\right) = \mathfrak{N}_{L|K}\left(\frac{b_1e_1 + \cdots + b_ne_n}{b_{n+1}}\right).$$

∎

COROLLARY 4.3: *If k is C_1 then* $\mathrm{cd}(G_k) \leq 1$.

Proof: This follows from Propositions 4.2 and 3.10 and Cor. 3.8. ∎

Examples: The following are examples of fields k which are C_1 and hence of fields for which $\mathrm{cd}(G_k) \leq 1$.

(1) Finite fields and their algebraic extensions. (Cf. [Ch1]).

p. 270
(2) Algebraic function fields of one variable over an algebraically closed field (Cf. [T]).

(3) A Henselian field K with discrete valuation v such that its residue class field k is algebraically closed, and $\hat{K}$ is separable over K, where $\hat{K}$ is the completion of K under v. (This follows from a theorem of Lang [L1] and the fact that if K is Henselian then K is separably closed in its completion [O].)

In particular if k is algebraically closed, then $k((t))$ is C_1. Also $\mathbb{Q}_p(\zeta|\ \zeta$ is a root of unity) is C_1, where $\mathbb{Q}_p$ is the field of p-adic numbers, [(L1]).

(4) Let K be a Henselian field with discrete valuation and perfect residue class field. Assume that $\hat{K}$ (the completion of K) is separable over K. Then the maximal unramified extension K_{nr} of K is C_1. For, since K_{nr} is Henselian $\hat{K}_{nr} = \hat{K} \otimes_K K_{nr}$ and $\hat{K}|K_{nr}$ is separable ([S2], pp. 41 and 64). On the other hand the residue class field of K_{nr} is k_s ([S2], p. 64); but since k is perfect k_s is algebraically closed. The result is then a consequence of example (3) above.

p. 271 **§5. Cohomological dimension and field extensions**

First we will consider algebraic extensions $k'|k$.

PROPOSITION 5.1: *Let $k'|k$ be an algebraic extension and let p be a prime. Then*

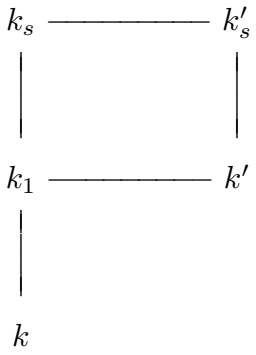
$$\mathrm{cd}_p(G_{k'}) \leq \mathrm{cd}_p(G_k).$$

Moreover one has equality in either of the following cases:

(i) $[k' : k]_s$ *is prime to* p*;*

(ii) $\mathrm{cd}_p(G_k) < \alpha$ *and* $[k' : k]_s < \infty$.

Proof:



Let $k_1 = k' \cap k_s$. Then k' and k_s are linearly disjoint over k_1 and $G_{k_s|k_1} \approx G_{k'}$ ([B2],
p. 272 §10, Th. 1).

So $G_{k'}$ is isomorphic to a closed subgroup of G_k. Moreover

$$(G_k : G_{k'}) = [k' : k]_s.$$

The result follows now from Prop. 2.1, Ch. IV. ∎

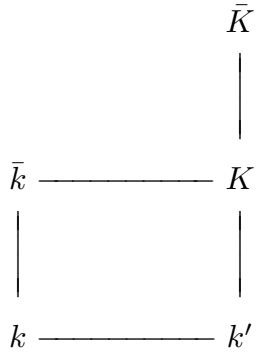
We turn now to the case of transcendental extensions.

PROPOSITION 5.2: *Let k be a field, $k' = k(t)$ where t is an indeterminate, and p a prime. Then*

$$\mathrm{cd}_p(G_{k'}) \leq 1 + \mathrm{cd}_p(G_k).$$

Moreover, equality holds if $\mathrm{cd}_p(G_k) < \infty$ *and* $p \neq \mathrm{char}\ k$.

Proof: Put $K = \bar{k}(t)$.



p. 273 Notice that $G_k \approx G_{\bar{k}|k}$ and $G_{k'} \approx G_{\bar{K}|k'}$. Moreover every $k(t)$-automorphism of K sends $\bar{k}$ onto $\bar{k}$; hence the group of $k(t)$-automorphisms of K is again G_k. Consider the exact sequence

$$1 \longrightarrow G_K \longrightarrow G_{k'} \longrightarrow G_k \longrightarrow 1. \tag{1}$$

By example (2) on p. 269, $\mathrm{cd}_p(G_K) \leq 1$. Thus, by Prop. 2.6, Ch. IV,

$$\mathrm{cd}_p(G_{k'}) \leq \mathrm{cd}_p(G_K) + \mathrm{cd}_p(G_K) \leq 1 + \mathrm{cd}_p(G_k).$$

Assume now that $p \neq \mathrm{char}\ k$ and $\mathrm{cd}_p(G_k) = d < \infty$. To prove equality consider first the case when in addition G_k is a pro-p-group. Let μ_p be the group of p-th roots of unity. To prove equality it will suffice to show that $H^{d+1}(G_{k'}, \mu_p) \neq 1$. To see this consider the spectral sequence of the group extension (1) (cf. Th. 5.3, Ch. III):

$$E_2^{i,j} = H^i\big(G_k, H^j(G_K, \mu_p)\big) \Rightarrow H^n(G_{k'}, \mu_p).$$

Using example (2) on p. 269, it is clear that $E_2^{i,j} = 0$ if $j > 1$ or $i > d$. Hence

p. 274 $$H^{d+1}(G_{k'}, \mu_p) \approx E_\infty^{d,1} \approx E_2^{d,1} = H^d\big(G_k, H^1(G_K, \mu_p)\big).$$

Since $p \neq \mathrm{char}\ k$, the sequence

$$1 \longrightarrow \mu_p \longrightarrow K_s^* \xrightarrow{p} K_s^* \longrightarrow 1$$

is exact; so we obtain a corresponding sequence of cohomology groups

$$\begin{array}{ccccccc} H^0(G_K, K_s^*) & \xrightarrow{p} & H^0(G_K, K_s^*) & \longrightarrow & H^1(G_K, \mu_p) & \longrightarrow 1 \\ \approx\big\downarrow & & \approx\big\downarrow & & & \\ K^* & \xrightarrow{p} & K^* & & & \end{array}$$

(Notice $H^1(G_K, K_s^*) = 1$ by Prop. 1.2). Hence

$$K^*/(K^*)^p \approx H^1(G_K, \mu_p)$$

and this is a G_k-isomorphism. Therefore it is enough to show that

$$H^d\big(G_k, K^*/(K^*)^p\big) \neq 1.$$

Let $v\colon K^* = \bar{k}(t)^* \longrightarrow \mathbb{Z}$ be the valuation given by the element 0 of $\bar{k}$. Then v is an epimorphism which in turn induces an epimorphism of G_k-modules

p. 275
$$\bar{v}\colon K^*/(K^*)^p \longrightarrow \mathbb{Z}/p\mathbb{Z}.$$

Thus we get an exact sequence

$$\cdots \longrightarrow H^d\big(G_k, K^*/(K^*)^p\big) \longrightarrow H^d(G_k, \mathbb{Z}/p\mathbb{Z}) \longrightarrow H^{d+1}(G_k, \ker \bar{v}) = 1.$$

But since G_k is a pro-p-group we have (see Cor. 4.3, Ch. IV)

$$H^d(G_k, \mathbb{Z}/p\mathbb{Z}) \neq 1$$

and hence

$$H^d\big(G_k, K^*/(K^*)^p\big) \neq 1$$

as desired.

Consider now the general case. Let H be a p-Sylow group of G_k. Then $H = G_{k_1}$ for some intermediate field $k \subseteq k_1 \subseteq \bar{k}$, and $\mathrm{cd}_p(G_{k_1}) = \mathrm{cd}_p(G_k)$, by Cor. 2.2, Ch. IV. Hence we have

$$d + 1 = \mathrm{cd}_p(G_{k_1(t)}) \leq \mathrm{cd}_p(G_{k(t)}) \leq d + 1.$$

Thus $\mathrm{cd}_p(G_{k(t)}) = d + 1$. ∎

p. 276 THEOREM 5.3: *Let k be field, $k'|k$ a field extension of transcendence degree N, and p a prime. Then*

$$\mathrm{cd}_p(G_{k'}) \leq N + \mathrm{cd}_p(G_k).$$

Moreover, equality holds if $\mathrm{cd}_p(G_k) < \infty$, $p \neq \mathrm{char}\ k$ *and* k' *is finitely generated over* k.

Proof: Let $t_1, \ldots, t_N$ be indeterminates. Using induction and Prop. 5.2 we have

$$\mathrm{cd}_p\, G_{k(t_1,\ldots,t_N)}) \leq N + \mathrm{cd}_p(G_k).$$

Hence, by Prop. 5.1,

$$\mathrm{cd}_p(G_{k'}) \leq \mathrm{cd}_p(G_{k(t_1,\ldots,t_N)}) \leq N + \mathrm{cd}_p(G_k).$$

Assume that $p \neq \mathrm{char}\ k$, $\mathrm{cd}_p(G_k) < \infty$, and that $k'|k$ is finitely generated. Then using again Propositions 5.1 and 5.2 and an induction argument we obtain

$$\mathrm{cd}_p(G_{k'}) = N + \mathrm{cd}_p(G_k).$$

∎

p. 277 COROLLARY 5.4: *If* $k = k_0(X, Y)$ *where* k_0 *is algebraically closed or if* $k = GF(q)(X)$, *then for every prime* $p \neq \mathrm{char}\ k$ *we have* $\mathrm{cd}_p(G_k) = 2$.

Proof: This follows from Th. 5.3 since $\mathrm{cd}_p(G_{k_0}) = 0$ and $\mathrm{cd}_p(G_{GF(q)}) = 1$ (see ex. (1), p. 269 and Cor. 2.3, Ch. IV). ∎

§6. Henselian fields

We recall that a field K with a non-archimedian valuation $v: K^* \longrightarrow \mathbb{R}$ is called Henselian if there is a unique extension of v to an algebraic closure of K.

THEOREM 6.1: *Let* K *be Henselian with discrete valuation and perfect residue class*
p. 278 *field* k. *Assume* $\hat{K}$ *(the completion of* K*) is separable over* K. *Then for every prime* p

$$\mathrm{cd}_p(G_K) \leq 1 + \mathrm{cd}_p(G_k).$$

Equality holds if $\mathrm{cd}_p(G_k) < \infty$ *and* $p \neq \mathrm{char}\ K$.

Proof: Let $K_{nr}|K$ be the maximal unramified extension of K, i.e.

$$K_{nr} = \varinjlim K_i$$

where K_i runs through the unramified finite algebraic extensions of K. Then $K_{nr}|K$ is a Galois extension and

$$G_{K_{nr}|K} \approx G_{k_s|k} = G_k.$$

(Cf. [S1], p. 63). Hence there is an exact sequence of profinite groups

$$1 \longrightarrow G_{K_{nr}} \longrightarrow G_K \longrightarrow G_k \longrightarrow 1. \tag{1}$$

By example (4) on p. 270, $\mathrm{cd}_p(G_{K_{nr}}) \leq 1$. Hence, by Prop. 2.6, Ch. IV, we have

p. 279
$$\mathrm{cd}_p(G_K) \leq 1 + \mathrm{cd}_p(G_k). \tag{2}$$

Assume now that $\mathrm{cd}_p(G_k) = d < \infty$, and $p \neq \mathrm{char}\ K$. Let μ_p be the G_K-module of p-th roots of unity. To show equality in (2), we will see that

$$H^{d+1}(G_K, \mu_p) \neq 0.$$

Consider the spectral sequence of the extension (1)

$$E_2^{i,j} = H^i\big(G_k, H^j(G_{K_{nr}}, \mu_p)\big) \Rightarrow H^n(G_K, \mu_p),$$

(see Th. 5.3, Ch. III). Clearly $E_\infty^{i,j} = E_2^{i,j} = 0$ if $i > d$ on $j > 1$. Since $H^{d+1}(G_K, \mu_p)$ is filtered by the $E_\infty^{i,j}$'s with $i + j = d + 1$, we obtain

$$H^{d+1}(G_K, \mu_p) \approx E_\infty^{d,1} \approx E_2^{d,1} = H^d\big(G_k, H^1(G_{K_{nr}}, \mu_p)\big).$$

We may assume that G_k is a pro-p-group, for if Γ is a p-Sylow group of G_k, with $\Gamma = G_\ell$, $k \subseteq \ell \subseteq k_s$, and $\Gamma = G_L$, $K \subseteq L \subseteq K_{nr}$; and if

$$\mathrm{cd}_p\, G_L = \mathrm{cd}_p\, G_\ell + 1,$$

then

p. 280
$$\mathrm{cd}_p\, G_K \geq \mathrm{cd}_p\, G_L = \mathrm{cd}_p\, G_\ell + 1 = \mathrm{cd}_p\, G_k + 1$$

and hence $\mathrm{cd}_p\, G_K = \mathrm{cd}_p\, G_k + 1$.

Therefore, assume G_k is pro-p. From the exact sequence

$$1 \longrightarrow u_p \longrightarrow (K_{nr})_s^* \xrightarrow{p} (K_{nr})_s^* \longrightarrow 1$$

we get an exact cohomology sequence

$$\begin{array}{ccccccc} H^0\big(G_{K_{nr}}, (K_{nr})_s^*\big) & \xrightarrow{p} & H^0\big(G_{K_{nr}}, (K_{nr})_s^*\big) & \longrightarrow & H^1(G_{K_{nr}}, \mu_p) & \longrightarrow & 1 \\ \downarrow \approx & & \downarrow \approx & & & & \\ K_{nr}^* & \xrightarrow{\qquad p \qquad} & K_{nr}^* & & & & \end{array}$$

(Notice $H^1(G_{K_{nr}}, (K_{nr})_s^*) = 1$ by Proposition 1.2.)

Thus

$$H^1(G_{K_{nr}}, \mu_p) \approx K_{nr}^*/(K_{nr}^*)^p$$

as G_k-modules.

The valuation $K_{nr} \longrightarrow \mathbb{Z}$ defines an epimorphism

$$K_{nr}^*/(K_{nr}^*)^p \longrightarrow \mathbb{Z}/p\mathbb{Z}.$$

Hence

p. 281
$$H^d(G_k, K_{nr}^*/(K_{nr}^*)^p) \longrightarrow H^d(G_k, \mathbb{Z}/p\mathbb{Z}) \longrightarrow 0$$

is exact. Since G_k is pro-p and $\mathrm{cd}_p\, G_k = d$, $H^d(G_k, \mathbb{Z}/p\mathbb{Z}) \neq 0$ (Corollary 4.2, Ch. IV). Therefore

$$H^{d+1}(G_K, \mu_p) \approx H^d\big(G_k, K_{nr}^*/(K_{nr}^*)^p\big) \neq 0.$$

∎

Remark: The above theorem applies in particular to local fields (i.e. complete under a discrete valuation).

COROLLARY 6.2: *Let K be a p-adic field (i.e. a finite algebraic extension of the field $\mathbb{Q}_p$ of p-adic numbers). Then*

$$\mathrm{cd}(G_K) = 2.$$

Proof: In this case the residue class field k of K is a finite field $GF(q)$ for some q. Since $G_k \approx \widehat{\mathbb{Z}}$ (see ex. (2) on p. 24) and for each prime number t, $\mathrm{cd}_t(\widehat{\mathbb{Z}}) = 1$ (see Cor. 3.3,
p. 282 Ch. IV) we have $\mathrm{cd}_t(G_k) = 1$. The result follows now from Th. 6.1. ∎

§7. Algebraic extensions of $\mathbb{Q}_p$

Let p be a prime number and let $\mathbb{Q}_p$ denote the field of p-adic numbers. First we shall consider finite extensions $K|\mathbb{Q}_p$.

THEOREM 7.1 (The main theorem of local class field theory): *Let $K|\mathbb{Q}_p$ be an algebraic extension with $[K : \mathbb{Q}_p] < \infty$. Then the following axioms are satisfied.*
Axiom 1: $H^1(G_K, \bar{K}^*) = 1$;
Axiom 2: There is an isomorphism

$$\mathrm{inv}_K \colon B_K \longrightarrow \mathbb{Q}/\mathbb{Z}$$

such that whenever $L|K$ is a finite field extension the diagram

$$\begin{array}{ccc} H^2(G_K, \bar{K}^*) \approx B_K & \xrightarrow{\mathrm{inv}_K} & \mathbb{Q}/\mathbb{Z} \\ \Big\downarrow{\scriptstyle \mathrm{Res}} & & \Big\downarrow{\scriptstyle [L:K]} \\ H^2(G_L, \bar{L}^*) \approx B_L & \xrightarrow{\mathrm{inv}_K} & \mathbb{Q}/\mathbb{Z} \end{array}$$

commutes.

Proof: Axiom 1 is Hilbert's theorem 90. To sketch the proof of axiom 2 we shall proceed to describe a sequence of isomorphisms whose composition we will define to be inv_K. Namely,

$$\mathrm{inv}_K \colon B_K \longrightarrow \mathbb{Q}/\mathbb{Z} \quad =$$

$$H^2(G_K, \bar{K}^*) \xrightarrow{\mathrm{Inf}^{-1}} H^2(G_{K_{nr}|K}, K_{nr}^*) \xrightarrow{\bar{v}_K} H^2(G_{K_{nr}|K}, \mathbb{Z})$$
$$\xrightarrow{\kappa} H^2(G_k, \mathbb{Z}) \xrightarrow{\delta^{-1}} H^1(G_k, \mathbb{Q}/\mathbb{Z}) \xrightarrow{\overline{\varphi}_k} \mathbb{Q}/\mathbb{Z}$$

First, consider the homomorphism

$$\mathrm{Res} \colon H^2(G_K, \bar{K}^*) \longrightarrow H^2(G_{K_{nr}}, \bar{K}_{nr}^*).$$

p. 284 Its kernel is $H^2(G_{K_{nr}|K}, K_{nr}^*)$ (see Cor. 5.4, Ch. III). But since K_{nr} is Henselian with algebraically closed residue class field, we have $H^2(G_{K_{nr}}, \bar{K}_{nr}^*) = 0$ (see ex. (3) on p. 270). Hence

$$\mathrm{Inf}^{-1}\colon H^2(G_K, \bar{K}^*) \longrightarrow H^2(G_{K_{nr}|K}, K_{nr}^*)$$

is an isomorphism.

To define the map $\bar{v}_K$, consider the exact sequence

$$1 \longrightarrow U \longrightarrow K_{nr}^* \xrightarrow{v_K} \mathbb{Z} \longrightarrow 0 \tag{1}$$

of $G_{K_{nr}|K}$-modules, where v_K is the discrete valuation of K_{nr} extending that one of K. One can prove that $H^q(G_{K_{nr}|K}, U) = 1$ if $q \geq 1$ (cf. [S2], p. 193). Therefore, we obtain from (1) an exact sequence

$$1 = H^2(G_{K_{nr}|K}, U) \longrightarrow H^2(G_{K_{nr}|K}, K_{nr}^*) \xrightarrow{\bar{v}_K} H^2(G_{K_{nr}|K}, \mathbb{Z}) \longrightarrow H^3(G_{K_{nr}|K}, U) = 1,$$

and therefore $\bar{v}_K$ is an isomorphism.

The isomorphism κ is induced by $G_{K_{nr}|K} \approx C_k$ (cf. [S2], p. 64), where k is the residue class field of (K_{nr}, v_K).

p. 285 The map δ is the connecting homomorphism corresponding to the short exact sequence of trivial G_k-modules

$$0 \longrightarrow \mathbb{Z} \longrightarrow \mathbb{Q} \longrightarrow \mathbb{Q}/\mathbb{Z} \longrightarrow 0.$$

The map δ is an isomorphism since $H^q(G_k, \mathbb{Q}) = 0$ if $q \geq 1$ (each $H^q(G_k, \mathbb{Q})$, $q \geq 1$, is a torsion group by Cor. 6.7, Ch. II, and for each natural number r the isomorphism $r\colon \mathbb{Q} \longrightarrow \mathbb{Q}$ induces an isomorphism $r\colon H^q(G_k, \mathbb{Q}) \longrightarrow H^q(G_k, \mathbb{Q})$).

Finally, the isomorphism $\overline{\varphi}_k$ is given in the following manner. Let $q = \#k$, and let $\varphi\colon \bar{k} \longrightarrow \bar{k}$ be the automorphism $\varphi x = x^q$; then for $\eta \in H^1(G_k, \mathbb{Q}/\mathbb{Z})$ we define

$$\overline{\varphi}_k(\eta) = \eta(\varphi_k).$$

The mapping $\overline{\varphi}_k$ is an isomorphism since φ_k generates G_k (see ex. (2) on p. 24).

Therefore we have shown that inv_K is an isomorphism.

Now, let $L|K$ be a finite field extension, let ℓ and k be their residue class fields, and e and f the ramification index and residue class degree respectively. Then the fact

$$\mathrm{inv}_L \cdot \mathrm{Res} = [L:K] \cdot \mathrm{inv}_K$$

p. 286 follows from the commutativity of the following diagram, which is easily checked.

$$\begin{array}{ccccccc}
B_K & \longrightarrow & H^2(G_{K_{nr}|K}, K_{nr}^*) & \longrightarrow & H^2(G_{K_{nr}|K}, \mathbb{Z}) & \longrightarrow & H^2(G_k, \mathbb{Z}) \longrightarrow \\
\downarrow{\scriptstyle \mathrm{Res}} & & \downarrow{\scriptstyle \mathrm{Res}} & & \downarrow{\scriptstyle e\cdot\mathrm{Res}} & & \downarrow{\scriptstyle e\cdot\mathrm{Res}} \\
B_L & \longrightarrow & H^2(G_{L_{nr}|L}, L_{nr}^*) & \longrightarrow & H^2(G_{L_{nr}|L}, \mathbb{Z}) & \longrightarrow & H^2(G_\ell, \mathbb{Z}) \longrightarrow
\end{array}$$

$$\longrightarrow H^1(G_k, \mathbb{Q}/\mathbb{Z}) \longrightarrow \mathbb{Q}/\mathbb{Z}$$

$$\downarrow{\scriptstyle e\cdot\mathrm{Res}} \qquad \downarrow{\scriptstyle e\cdot f=[L:K]}$$

$$\longrightarrow H^1(G_\ell, \mathbb{Q}/\mathbb{Z}) \longrightarrow \mathbb{Q}/\mathbb{Z}$$

∎

p. 287 The definition of the map inv_K that we have just studied can be extended to the case when $K|\mathbb{Q}_p$ is any algebraic extension not necessarily finite. With this aim in mind we introduce the following rotation. If

$$n = \prod_\ell \ell^{n(\ell)}$$

is a supernatural number, define

$$\frac{1}{n}\mathbb{Z}/\mathbb{Z} = \{x \in \mathbb{Q}/\mathbb{Z} |\ \mathrm{ord}x \mid n\}.$$

Examples:

(1) If $n = \prod_\ell \ell^\infty$, $\frac{1}{n}\mathbb{Z}/\mathbb{Z} = \mathbb{Q}/\mathbb{Z}$.

(2) If $n = \ell^\infty$, $\frac{1}{n}\mathbb{Z}/\mathbb{Z} = \mathbb{Q}/\mathbb{Z}(\ell)$.

Let $K|\mathbb{Q}_p$ be an algebraic extension, and define

$$\bar{n}_K = \prod_{\ell^\infty \nmid [K:\mathbb{Q}_p]} \ell^\infty.$$

THEOREM 7.2: *Let $K|\mathbb{Q}_p$ be an algebraic extension. Then there is an isomorphism*

$$\mathrm{inv}_K\colon B_K \longrightarrow \frac{1}{\bar{n}_K}\mathbb{Z}/\mathbb{Z}\ .$$

p. 288 *Proof:* Write

$$K = \varinjlim_{i\in I} K_i$$

where $\mathbb{Q}_p \subseteq K_i \subseteq K$, $K_i|\mathbb{Q}_p$ is a finite extension for each $i \in I$, and $i < j \Rightarrow K_j \supset K_i$. Then

$$G_K = \varprojlim_{i\in I} G_{K_i}.$$

Therefore (see Prop. 4.1, Ch. II)

$$B_K = H^2(G_K, \overline{\mathbb{Q}}_p^*) \approx \varinjlim_{i\in I} H^2(G_{K_i}, \overline{\mathbb{Q}}_p^*) \approx \varinjlim_{i\in I} B_{K_i}.$$

By Th. 7.1, the map inv is an isomorphism of the directed systems

$$(B_{K_i}, \underset{ij}{\mathrm{Res}}) \quad \text{and} \quad \big((\mathbb{Q}/\mathbb{Z})_i, n_{ij}\big)$$

where each $(\mathbb{Q}/\mathbb{Z})_i$ is a copy of $\mathbb{Q}/\mathbb{Z}$ and $n_{ij}\colon(\mathbb{Q}/\mathbb{Z})_i \longrightarrow (\mathbb{Q}/\mathbb{Z})_j$ is multiplication by $n_{ij} = [K_j : K_i]$ for $j > i$. Thus it induces an isomorphism

$$\mathrm{inv}_K\colon B_K \longrightarrow \varinjlim_{i\in I} (\mathbb{Q}/\mathbb{Z})_i.$$

We shall see that

$$\varinjlim_{i\in I} (\mathbb{Q}/\mathbb{Z})_i = \frac{1}{\bar{n}_K}\mathbb{Z}/\mathbb{Z}.$$

p. 289 Notice that

$$\left(\varinjlim_{i\in I} (\mathbb{Q}/\mathbb{Z})_i\right)(\ell) = \varinjlim_{i\in I} (\mathbb{Q}/\mathbb{Z})_i(\ell).$$

Assume $\ell^\infty \nmid [K : \mathbb{Q}_p]$. Then there exists some i_0 such that $(n_{ij}, \ell) = 1$ if $i \geq i_0$. So if $i \geq i_0$

$$n_{ij}\colon(\mathbb{Q}/\mathbb{Z})_i(\ell) \longrightarrow (\mathbb{Q}/\mathbb{Z})_j(\ell)$$

is an isomorphism, and hence

$$\varinjlim_{i\in I}(\mathbb{Q}/\mathbb{Z})_i(\ell) = (\mathbb{Q}/\mathbb{Z})(\ell) = \frac{1}{\ell^\infty}\mathbb{Z}/\mathbb{Z}.$$

On the other hand suppose $\ell^\infty \mid [K:\mathbb{Q}_p]$. Let $x \in \varinjlim_{i\in I}(\mathbb{Q}/\mathbb{Z})_i(\ell)$ and let $x_i \in (\mathbb{Q}/\mathbb{Z})_i(\ell)$ whose canonical image is x; say $\mathrm{ord}(x_i) = \ell^\beta$. Then there is some $j > i$ such that $\ell^\beta \mid n_{ij}$ (since $\ell^\infty \mid [K:\mathbb{Q}_p]$). Therefore $x_j = n_{ij}x_i = 0$ and so $x = 0$, i.e.

$$\varinjlim_{i\in I}(\mathbb{Q}/\mathbb{Z})_i(\ell) = 0.$$

Thus

$$\varinjlim_{i\in I}(\mathbb{Q}/\mathbb{Z})_i \approx \coprod_\ell \Big(\varinjlim_{i\in\ell}(\mathbb{Q}/\mathbb{Z})_i\Big)(\ell) \approx \coprod_{\ell^\infty\nmid[K:\mathbb{Q}_p]} \frac{1}{p^\infty}\mathbb{Z}/\mathbb{Z} \approx \frac{1}{\bar{n}_K}\mathbb{Z}/\mathbb{Z}.$$

p. 290

∎

Remark: The homomorphism inv_K of Th. 7.2 is "natural", in the sense that it satisfies the following property. Let $\mathbb{Q}_p \subseteq K \subseteq L$ be algebraic extensions, then the following diagram commutes

$$\begin{array}{ccccc} B_K & \xrightarrow{\mathrm{inv}_K} & \frac{1}{\bar{n}_K}\mathbb{Z}/\mathbb{Z} & = & \coprod_{\ell^\infty\nmid[K:\mathbb{Q}_p]} \frac{1}{\ell^\infty}\mathbb{Z}/\mathbb{Z} \\ {\scriptstyle\mathrm{Res}}\downarrow & & {\scriptstyle[L:K]}\downarrow & & \\ B_L & \xrightarrow{\mathrm{inv}_L} & \frac{1}{\bar{n}_L}\mathbb{Z}/\mathbb{Z} & = & \coprod_{\ell^\infty\nmid[L:\mathbb{Q}_p]} \frac{1}{\ell^\infty}\mathbb{Z}/\mathbb{Z} \end{array}$$

where the map $[L:K]$ is "multiplication" by $[L:K]$, i.e., if $[L:K] = \prod_\ell \ell^{\alpha(\ell)}$ and $x \in \frac{1}{\ell^\infty}\mathbb{Z}/\mathbb{Z} \subset \frac{1}{\bar{n}_K}\mathbb{Z}/\mathbb{Z}$ then $[L:K]x = \ell^{\alpha(\ell)}x$ (with the understanding that $\ell^{\alpha(\ell)}x = 0$ if $\alpha(\ell) = \infty$). To see this notice that

$$\mathrm{Res}\colon B_K \longrightarrow B_L$$

is induced by the maps

$$B_{K_i} \xrightarrow{=} B_{K_i} \longrightarrow \varinjlim_{j\in J} B_{L_j} = B_L$$

p. 291 where $\mathbb{Q}_p \subset K_i \subset K$, $\mathbb{Q}_p \subset L_j \subset L$, $[K_i : \mathbb{Q}_p] < \infty$ and $[L_j : \mathbb{Q}_p] < \infty$. (We are assuming $I \subset J$ and $i \in I \Rightarrow K_i = L_i$.) Hence from Th. 7.1 we obtain a commutative diagram

$$\begin{array}{ccc} B_K = \varinjlim_{i\in I} B_{K_i} & \xrightarrow{\text{inv}_K} & \varinjlim_{i\in I} (\mathbb{Q}/\mathbb{Z})_i \\ \Big\downarrow{\scriptstyle \text{Res}} & & \Big\downarrow{\scriptstyle \varphi} \\ B_L = \varinjlim_{j\in J} B_{L_j} & \xrightarrow{\text{inv}_L} & \varinjlim_{j\in J} (\mathbb{Q}/\mathbb{Z})_j \end{array}$$

where φ is induced by

$$(\mathbb{Q}/\mathbb{Z})_i \xrightarrow{=} (\mathbb{Q}/\mathbb{Z})_i \longrightarrow \varinjlim_{j\in J} (\mathbb{Q}/\mathbb{Z})_j.$$

Now it is easily verified that φ is multiplication by $[L : K]$.

COROLLARY 7.3: *Let $K|\mathbb{Q}_p$ be an algebraic extension and let ℓ be a prime. Then $B_K(\ell) = 0 \Leftrightarrow \ell^\infty \mid [K : \mathbb{Q}_p]$.*

p. 292 COROLLARY 7.4: *Let $K|\mathbb{Q}_p$ be an algebraic extension and let ℓ be a prime. Then*

(i) $\text{cd}_\ell(G_K) = 0 \Leftrightarrow \ell \nmid [\bar{K} : K]$;

(ii) $\text{cd}_\ell(G_K) = 1 \Leftrightarrow \ell \mid [\bar{K} : K]$ *and* $\ell^\infty \mid [K : \mathbb{Q}_p]$

(iii) $\text{cd}_\ell(G_K) = 2 \Leftrightarrow \ell^\infty \nmid [K : \mathbb{Q}_p]$.

Proof: (i) This is the content of Cor. 2.3, Ch. IV.

(ii) This is a consequence of Cor. 7.3 and Cor. 3.7.

(iii) If $\text{cd}_\ell(C_K) = 2$, by (i) and (ii) we have $\ell^\infty \nmid [K : \mathbb{Q}_p]$. Conversely, assume $\ell^\infty \nmid [K : \mathbb{Q}_p]$; then, by Cor. 7.3, $B_K(\ell) \neq 0$ and so $\text{cd}_\ell(G_K) \geq 2$ by Th. 3.6. On the other hand, since $G_K = \varprojlim G_{K_\alpha}$ where $K_\alpha|\mathbb{Q}_p$ runs through the set of finite subextensions of $K|\mathbb{Q}_p$, we have

$$H^n(G_K, \bar{K}^*) = \varinjlim H^n(G_{K_\alpha}, \bar{K}^*)$$

(see Th. 4.1, Ch. II); therefore $\text{cd}_\ell(G_K) \leq 2$ by Cor. 6.2. ∎

p. 293 **§8. Algebraic extensions of $\mathbb{Q}$**

Let $K|\mathbb{Q}$ be any algebraic extension (possibly infinite), and let v be a real valuation of K. Then

$$K = \varinjlim_{\alpha} K_\alpha$$

where $K_\alpha|\mathbb{Q}$ runs through the set of all finite sub-extensions of $K|\mathbb{Q}$. Denote by $K_{\alpha v}$ the completion of K_α with respect to the restriction of v to K_α. Set

$$K_v = \varinjlim_{\alpha} K_{\alpha v} \ .$$

It is clear that $K_{\alpha v}$ is either a finite extension of $\mathbb{Q}_p$ (for some fixed p) or of $\mathbb{R}$ depending on whether v is the p-adic valuation or the ordinary absolute value when restricted to $\mathbb{Q}$. Hence K_v is either an algebraic extension of $\mathbb{Q}_p$ or of $\mathbb{R}$. If $\bar{K}$ and $\bar{K}_v$ are algebraic closures of K and K_v respectively, then any K-embedding

$$f\colon \bar{K} \longrightarrow \bar{K}_v$$

induces a homomorphism

p. 294
$$\overline{f}\colon G_{K_v} \longrightarrow G_K$$

which in turn induces a homomorphism

$$\rho_v\colon B_K \longrightarrow B_{K_v}.$$

PROPOSITION 8.1: *ρ_v is independent of the choice of the K-embedding f.*

Proof: Let f, g be two such embeddings. They differ by a K-automorphism of $\bar{K}$, so that $\overline{f}$ and $\bar{g}$ differ by an inner automorphism given by an element of G_K. The result follows now from Prop. 5.13. ∎

Remark: Notice that

$$B_{K_v} = \varinjlim_{\alpha} B_{K_{\alpha v}}$$

and that

$$\rho_v = \varinjlim_{\alpha} \rho_{\alpha v}.$$

p. 295 PROPOSITION 8.2: *The canonical map* $\rho_v: B_K \longrightarrow B_{K_v}$ *is surjective.*

Proof: Assume first that $K|\mathbb{Q}$ is a finite extension. Let K_w denote the completion of K with respect to the valuations w of K. Then B_{K_w} is isomorphic to $\mathbb{Q}/\mathbb{Z}$ by means of inv if w arises from a p-adic valuation of $\mathbb{Q}$ (cf. Th. 7.1); B_{K_w} is isomorphic to the subgroup $\{0, \frac{1}{2}\}$ of $\mathbb{Q}/\mathbb{Z}$ if w arises from the ordinary absolute value on $\mathbb{Q}$ and $K_w = \mathbb{R}$, for

$$B_{\mathbb{R}} = H^2(\mathbb{Z}/2\mathbb{Z}, \mathbb{C}^*) = \mathbb{R}^*/\mathbb{R}_+^* = \mathbb{Z}/2\mathbb{Z}$$

(cf. [M], p. 122); finally $B_{K_w} = 0$ if $K_w = \mathbb{C}$. The maps ρ_w define a homomorphism ρ of B_K into the direct product of the B_{K_w}'s; however, it can be proved that if $x \in B_K$, $\rho_w(x) = 0$ for all but a finite number of w's, so that the homomorphism ρ is in fact into the direct sum of the B_{K_w}'s. Moreover the sequence

$$0 \longrightarrow B_K \xrightarrow{\rho} \coprod_w B_{K_w} \xrightarrow{\sigma} \mathbb{Q}/\mathbb{Z} \longrightarrow 0$$

p. 296 is exact where σ is induced by the maps $B_{K_w} \longrightarrow \mathbb{Q}/\mathbb{Z}$ described above (Hasse's th. , cf. [A-T], p. 64).

Let us go back to the proof that ρ_v is surjective. Let $x_v \in B_{K_v}$. Choose a valuation v' of K and an element $x_{v'} \in B_{K_{v'}}$ such that $\sigma(x) = 0$ where $x \in \coprod_w B_{K_w}$ is defined to have all coordinates zero except coordinates v and v' which are s_v and $x_{v'}$ respectively. Hence by the exactness of the above sequence there is some element $y \in B_K$ with $\rho_v(y) = x_v$.

Assume now that $K|\mathbb{Q}$ is any algebraic extension. Since $\varinjlim$ is an exact functor in the category of abelian groups, by the remark on p. 294 we have that

$$\rho_v = \varinjlim_\alpha \rho_{\alpha v}$$

is surjective. ∎

PROPOSITION 8.3: *Let* $K|\mathbb{Q}$ *be any algebraic extension, possibly infinite. Then the homomorphism*

$$B_K \longrightarrow \prod_v B_{K_v}$$

p. 297 *induced by the maps* $\rho_v : B_K \longrightarrow B_{K_v}$, *where* v *runs through the set of all valuations of* K, *is injective.*

Proof: As before put

$$K = \varinjlim K_\alpha$$

where $K_\alpha|\mathbb{Q}$ runs through all finite subextensions of $K|\mathbb{Q}$. Then

$$K_v = \varinjlim_\alpha K_{\alpha v} \ ,$$
$$B_K = \varinjlim_\alpha B_{K_\alpha} \ ,$$
$$B_{K_v} = \varinjlim_\alpha B_{K_{\alpha v}},$$

and

$$\rho = \varinjlim_\alpha \rho_{\alpha v}.$$

$$\begin{array}{ccc} B_K & \xrightarrow{\rho_v} & B_{K_v} \\ {\scriptstyle \mathrm{Res}_\alpha}\uparrow & & \uparrow{\scriptstyle \mathrm{Res}_{\alpha v}} \\ B_{K_\alpha} & \xrightarrow{\rho_{\alpha v}} & B_{K_{\alpha v}} \end{array}$$

Let $x \in B_K$; put $x_v = \rho_v(x)$. Assume $x_v = 0 \ \forall v$. We shall show that $x = 0$. Choose $\bar{\alpha}$
p. 298 and $x_{\bar{\alpha}}$ such that $x_{\bar{\alpha}} \in B_{K_{\bar{\alpha}}}$ and $\mathrm{Res}_{\bar{\alpha}}(x_{\bar{\alpha}}) = x$. If $\alpha \geq \bar{\alpha}$ we write $x_\alpha = \mathrm{Res}_{\alpha\bar{\alpha}}(x_{\bar{\alpha}})$. For $\alpha \geq \bar{\alpha}$ let V_α be the set of all valuations of K for which $x_{\alpha v} = \rho_{\alpha v}(x_\alpha) \neq 0$. By Hasse's theorem (see proof of Prop. 8.2) each V_α is finite. It is plain that

$$\{V_\alpha |\ \alpha \geq \bar{\alpha}\}$$

form a projective system, where if $\beta \geq \alpha$ the map $V_\beta \longrightarrow V_\alpha$ is given by restriction. On the other hand

$$\varprojlim_\alpha V_\alpha = \emptyset,$$

for otherwise there is some valuation v of K such that $x_{\alpha v} \neq 0$ for all α, and hence $x_v \neq 0$ contradicting our hypothesis. Therefore $V_\alpha = \emptyset$ for some α (cf. [B3], §9, Prop. 8). Thus, by Hasse's th. $x_\alpha = 0$, and so $x = 0$. ∎

COROLLARY 8.4: *Let K be as in Prop. 8.3 and let ℓ be a prime. Then $B_K(\ell) = 0$ iff*
p. 299 *$B_{K_v}(\ell) = 0$ for all valuations v.*

Proof: It follows immediately from Props. 8.3 and 8.4. ∎

COROLLARY 8.5: *Let K and ℓ be as above. Then*

$$B_K(\ell) = 0 \Rightarrow B_L(\ell) = 0$$

for every algebraic extension $L|K$.

Proof: For every valuation v of K $L_v \supseteq K_v$, and so $B_{L_v}(\ell) = 0$ by Cor. 7.3; hence by Cor. 8.4 $B_L(\ell) = 0$. ∎

COROLLARY 8.6: *Let K and ℓ be as above. Then*

$$\mathrm{cd}_\ell(G_K) \leq 1 \Longleftrightarrow B_K(\ell) = 0.$$

Proof: This is a consequence of Cor. 8.5 and Cor. 3.7. ∎

p. 300 We will prove now a lemma that will be used later to describe all possible values of $\mathrm{cd}_\ell(G_K)$ for any algebraic extension $K|\mathbb{Q}$.

LEMMA 8.7: *Let ℓ be a prime and L a finite extension of $\mathbb{Q}$. Then there is a Galois extension $K|L$ such that $G_{K|L} = \mathbb{Z}_\ell$ and $\ell^\infty \mid [K_v : \mathbb{Q}_v]$ for every non-archimedean place v of K.*

Proof: Assume first that $L = \mathbb{Q}$. Given a field H and a natural number n let ζ_n denote a primitive nth-root of 1 and set $H_n = H(\zeta_n)$. Let $\mathbb{Q}(\ell)$ be the field obtained by adjoining to $\mathbb{Q}$ all the ℓ^n-th roots of 1 for all n. Then

$$\mathbb{Q}(\ell) = \varinjlim_n \mathbb{Q}_n.$$

It is well-known that

$$G_{\mathbb{Q}_n|\mathbb{Q}} = \text{group of units of } \mathbb{Z}/\ell^n\mathbb{Z}$$

(cf. [B2], §11, Prop. 2). Hence

$$G_{\mathbb{Q}(\ell)|\mathbb{Q}} = \varprojlim_n G_{\mathbb{Q}_n|\mathbb{Q}}$$

p. 301 is the group of units $U(\mathbb{Z}_\ell)$ of $\mathbb{Z}_\ell$.

Let v be a non-archimedian place. Then

$$\mathbb{Q}(\ell)_v = \varinjlim_n (\mathbb{Q}_n)_v \supseteq \varinjlim_n (\mathbb{Q}_v)_n.$$

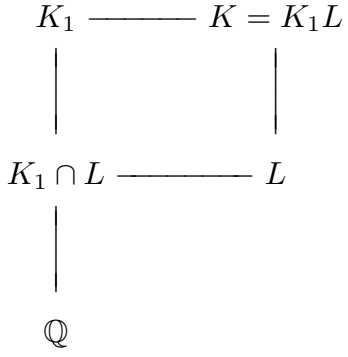
Let p be the prime number defining the valuation v. If $p = \ell$, then

$$\big[(\mathbb{Q}_v)_n : \mathbb{Q}_v\big] = \big[(\mathbb{Q}_p)_n : \mathbb{Q}_p\big] = (\ell - 1)\ell^{n-1}$$

(cf. [S2], p. 85); therefore, by Prop. 4.7, Ch. I, we have $\ell^\infty \mid [\mathbb{Q}(\ell)_v : \mathbb{Q}_v]$. If $p \neq \ell$, then (cf. [S2], p. 85) $r(n) = [(\mathbb{Q}_v)_n : \mathbb{Q}_v]$ is the least positive integer such that $p^{r(n)} \equiv 1 \pmod{\ell^n}$ (hence $r(n) \mid \ell^{n-1}(\ell-1)$), and $[(\mathbb{Q}_v)_n : \mathbb{Q}_v] = [GF(p)_n : GF(p)]$ where $GF(p)$ is the field with p elements (hence $r_n \longrightarrow \infty$ when $n \longrightarrow \infty$); therefore we have again $\ell^\infty | [\mathbb{Q}(\ell)_v : \mathbb{Q}_v]$.

Now, the group $U(\mathbb{Z}_\ell)$ is the direct product of $\mathbb{Z}_\ell$ and a finite group (cf. [S2], p. 220). Hence, since $G_{\mathbb{Q}(\ell)|\mathbb{Q}} = U(\mathbb{Z}_\ell)$ there is a subextension $K|\mathbb{Q}$ of $\mathbb{Q}(\ell)|\mathbb{Q}$ such that $G_{K|\mathbb{Q}} = \mathbb{Z}_\ell$. Moreover, since $[\mathbb{Q}(\ell) : K] < \infty$ we have $\ell^\infty | [K_v : \mathbb{Q}_v]$ for every non-archimedian v.

p. 302 Consider now the general case, that is assume $L|\mathbb{Q}$ is a finite extension. Let $K_1|\mathbb{Q}$ be a Galois extension such that $G_{K_1|\mathbb{Q}} = \mathbb{Z}_\ell$ and $\ell^\infty | [(K_1)_v : \mathbb{Q}_v]$ for every non-archimedian place v.



Set $K = K_1L$. Then $G_{K|L} \approx G_{K_1|K_1\cap L}$ (cf. [B2], §10, Th. 1), and hence $G_{K|L} \approx \mathbb{Z}_\ell$, for $(G_{K_1|\mathbb{Q}} : G_{K_1|K_1\cap L}) = [K_1 \cap L : \mathbb{Q}] < \infty$ (see Prop. 6.3, Ch. I). Finally for every non-archimedian place v of K we have

$$[K_v : \mathbb{Q}_v] = \big[K_v : (K_1)_v\big]\big[(K_1)_v : \mathbb{Q}_v\big],$$

and so $\ell^\infty | [K_v : \mathbb{Q}_v]$. ∎

THEOREM 8.8: *Let K be any algebraic extension of $\mathbb{Q}$, and let ℓ be a prime number. Then*

p. 303 $$\mathrm{cd}_\ell(G_K) = 0, 1, 2, \text{ or } \infty.$$

Specifically we have

(a) $\mathrm{cd}_\ell(G_K) = \infty \Leftrightarrow \ell = 2$ *and K is not totally imaginary;*

(b) Under the assumption that either $\ell \neq 2$ or K is totally imaginary we have

(i) $\mathrm{cd}_\ell(G_K) = 0 \Leftrightarrow \ell \nmid [\bar{K} : K]$

(ii) $\mathrm{cd}_\ell(G_K) = 1 \Leftrightarrow \ell | [\bar{K} : K]$ *and* $\ell^\infty | [K_v : \mathbb{Q}_v]$ *for every non-archimedian place v of K;*

(iii) $\mathrm{cd}_\ell(G_K) = 2 \Leftrightarrow \ell | [\bar{K} : K]$ *and* $\ell^\infty \nmid [K_v : \mathbb{Q}_v]$ *for some non-archimedian place v of K.*

[We recall that K is called totally imaginary if it cannot be embedded into $\mathbb{R}$.]

Proof: (a) If K is not totally imaginary there is a field R, $K \subseteq R \subseteq \bar{K}$ with $[\bar{K} : R] = 2$, namely $R = \mathbb{R} \cap K$. So $G_R \subseteq G_K$ and $\mathrm{cd}_2(G_K) \geq \mathrm{cd}_2(G_R) = \mathrm{cd}_2(\mathbb{Z}/2\mathbb{Z}) = \infty$ by

p. 304 Prop. 2.1, Ch. IV, and Cor. 2.5, Ch. IV.

(b) (i) This follows from Cor. 2.3, Ch. IV.

(b)(ii) Assume first that $\mathrm{cd}_\ell(G_K) = 1$; then by Cor. 8.6, Cor. 8.4 and part (b)(i) and Cor. 7.3 we have $\ell | [\bar{K} : K]$ and $\ell^\infty | [K_v : \mathbb{Q}_v]$ for all non-archimedian v. Conversely, suppose $\ell | [\bar{K} : K]$ and $\ell^\infty | [K_v : \mathbb{Q}_v]$ for every non-archimedian place v; then if v is non-archimedian $B_{K_v}(\ell) = 0$ by Cor. 7.3. If $\ell \neq 2$ and v is archimedian again $B_{K_v}(\ell) = 0$, since B_{K_v} is either $\mathbb{Z}/2\mathbb{Z}$ or 0 (see proof of Prop. 8.2); and if $\ell = 2$ we have assumed K is totally imaginary and so $B_{K_v} = 0$ for every archimedian v ($K_v = \mathbb{C}$). Thus, by Cor. 8.6 and case (b)(i) we have $\mathrm{cd}_\ell(G_K) = 1$.

(b)(iii) If $\mathrm{cd}_\ell(G_K) = 2$ it follows from (b) (i) and (b) (ii) that $\ell | [\bar{K} : K]$ and $\ell^\infty \nmid [K_v : \mathbb{Q}_v]$ for some non-archimedian place v of K. To prove the reverse implication

p. 305 it will suffice to prove that if $\ell \neq 2$ or K is totally imaginary then $\mathrm{cd}_\ell(G_K) \leq 2$. For this we may assume that $[K : \mathbb{Q}] < \infty$, for if $K = \varinjlim K_i$ where K_i runs through the set of finite subextensions $K_i | \mathbb{Q}$ of $K | \mathbb{Q}$, then

$$G_K = \varprojlim G_{K_i}$$

and

$$H^n(G_K, \bar{K}^*) = \varinjlim H^n(G_{K_i}, \bar{K}_i^*)$$

(see Prop. 4.1, Ch. II), and hence $\mathrm{cd}_\ell(G_{K_i}) \leq 2 \Rightarrow \mathrm{cd}_\ell(G_K) \leq 2$ (see Th. 3.6). If $[K : \mathbb{Q}] < \infty$, by Lemma 8.7, there is a Galois extension L of K such that $K_{L|K} = \mathbb{Z}_\ell$ and $\ell^\infty | [L_v : \mathbb{Q}_v]$ for all non-archimedian places v of L. By parts (b) (i) and (b) (ii) we must have $\mathrm{cd}_\ell(G_L) \leq 1$. Finally, from the extension

$$1 \longrightarrow G_L \longrightarrow G_K \longrightarrow G_{L|K} \longrightarrow 1$$

we get

$$\mathrm{cd}_\ell(G_K) \leq \mathrm{cd}_\ell(G_L) + \mathrm{cd}_\ell(G_{L|K}) \leq 2$$

(see Prop. 2.6, Ch. IV). ∎

p. 306 **§9. The abelian subgroups of $G_\mathbb{Q}$ ***

In this section we characterize those algebraic extensions $K|\mathbb{Q}$ over which every algebraic equation has an abelian Galois group, i.e., those algebraic extensions $K|\mathbb{Q}$ for which G_K is abelian. We achieve this by describing the abelian closed subgroups of $G_\mathbb{Q}$. There are two obvious examples of such subgroups:

1) Let $R|\mathbb{Q}$ be real closed, i.e., $[\overline{\mathbb{Q}} : R] = 2$. Then $G_R = \mathbb{Z}/2\mathbb{Z}$.

2) Let $\sigma \in G_\mathbb{Q}$, and let H be the closed subgroup of $G_\mathbb{Q}$ generated by σ. Clearly H is procyclic, and hence abelian.

In fact one has the following result due to W.D. Geyer [Ge].

THEOREM 9.1: *Every abelian closed subgroup of $G_\mathbb{Q}$ is procyclic.*

Proof: Let H be an abelian closed subgroup of $G_\mathbb{Q}$.

Case (1): Assume H contains some torsion element $\sigma \neq 1$. Let H' be the subgroup
p. 307 generated by σ and let R and K be the fixed fields of H' and H respectively. Since $[\overline{\mathbb{Q}} : R] < \infty$, R is real closed and so $\sigma^2 = 1$ (cf. [J], p. 316). Since $R|K$ is a normal extension, for each $\tau \in H$ we must have that τ restricted to R is an automorphism of

R. Hence τ restricted to R is the identity, since R is real closed (cf. [J], p. 273). Thus $\tau \in H'$, i.e. $H = H' = \mathbb{Z}/2\mathbb{Z}$.

Case (2): Suppose H is torsion free. Since H is also compact and totally disconnected we have

$$H = \prod_{p \in S} \mathbb{Z}_p^{e_p}$$

where S is a set of prime numbers, e_p is a cardinal number and $\mathbb{Z}_p$ is the group of p-adic integers (cf., e.g., [H-R], p. 406). Therefore to show that H is pro-cyclic it suffices to show that for each $p \in S$, $e_p = 0, 1$. If this were not the case, then H would contain a closed subgroup of the form $H' = \mathbb{Z}_p \times \mathbb{Z}_p$. We shall prove that this leads to a contradiction. Let K be the fixed field of H'. Clearly K contains the p-th roots of 1,
p. 308 for if η is one such root then $[K(\eta) : K] \leq p - 1$ must be a divisor of p. Assume K contains all p^n-th roots of 1. Then for every non-archimedian place v of K,

$$K_v \supseteq \mathbb{Q}_v(\zeta_{p^n} \mid n \in \mathbb{N}) \supseteq \mathbb{Q}_v$$

where ζ_{p^n} is a primitive p^n-th root of 1. Hence $p^\infty | [K_v : \mathbb{Q}_v]$ for every non-archimedian v. So $\mathrm{cd}_p(H') \leq 1$ by Th. 8.8 (notice K is totally imaginary, for otherwise H would contain a subgroup of order 2 as seen in proof of Th. 8.8 (a)). On the other hand $\mathrm{cd}_p(H) = \mathrm{cd}_p(\mathbb{Z}_p) + \mathrm{cd}_p(\mathbb{Z}_p) = 2$ by Prop. 4.4, Ch. IV. A contradiction.

Assume now that K contains a primitive p^{n-1}-th root of 1 but it does not contain a primitive p^n-th root of 1. Let ζ be primitive p^n-th root of 1, and put $K_1 = K(\zeta)$. Then $K_1|K$ is cyclic of degree p. Since $H' = \mathbb{Z}_p \times \mathbb{Z}_p$ there is some cyclic extension $K_2|K$ of degree p such that $K_1 \neq K_2$ (if U is the open subgroup of $\mathbb{Z}_p$ of index p choose K_2 to be the fixed field of $U \times \mathbb{Z}_p$ or $\mathbb{Z}_p \times U$ so that $K_2 \neq K_1$). Then K_2 is generated over K by the roots of a pure irreducible equation $x^p - a = 0$ (cf. [B2], §11, no. 6).
p. 309 Take $b \in \overline{\mathbb{Q}}$ such that $b^{p^n} - a = 0$. Since $(b^{p^{n-1}})^p - a = 0$ we have $K_2 \subseteq K(b)$, and $K_2 = K(b^{p^{n-1}})$. Let $\sigma \in H'$ be such that $\sigma|_{K_1} =$ identity but $\sigma|_{K_2} \neq$ identity. Set $\zeta = (\sigma b)b^{-1}$; then ζ is a primitive p^n-th root of 1, for $\zeta^{p^{n-1}} = \sigma(b^{p^{n-1}})b^{-p^{n-1}} \neq 1$. Therefore $K_1 \subseteq K(b)$ and $[K(b) : K] = p^n$. Since $K(b)|K$ is normal $\sigma \in G_{K(b)|K_1}$, and so $\sigma^{p^{n-1}} =$ identity on $K(b)$. However

$$\sigma^{p^{n-1}}(b) = \zeta^{p^{n-1}} b \neq b.$$

Contradiction. ∎

Bibliography

p. 310

[A-T] E. Artin and J. Tate, *Class Field Theory,* W. A. Benjamin, N.Y., 1967.

[B1] N. Bourbaki, *Algèbre,* Ch. 2, Hermann, Paris, 1962.

[B2] ———, *Algèbre,* Ch. 5, Hermann, Paris, 1959.

[B3] ———, *Topologie Générale,* Ch. 1, Hermann, Paris, 1962.

[Ch1] C. Chevalley, *Démonstration d'une hypothese de M. Artin,* Abh. Math. Sem. Hansischen Univ. **11** (1935), p. 73.

[Ch2] ———, *Introduction to the Theory of Algebraic Functions of One Variable,* Mathematical Surveys, AMS, 1951.

[D1] A. Douady, *Cohomologie des Groups Compacts Totalement Discontinus,* Seminaire Bourbaki, 1959–60, exposé 189.

[D2] ———, *Determination d'un Groupe de Galois,* C. R. Acad. Sc. Paris, t. **258** (1964), 5305–08.

[G] A. Grothendieck, *Sur quelques points d'algèbre homologique,* Tôhoku Math. J. **9** (1957) 119–221.

[Ge] W.-D. Geyer, *Unendliche algebraische Zahlkörper, über denen jede Gleichung auflösbar von beschränkter Stufe ist,* Queen's University preprint no. 1968-10 (To appear).

[H] M. Hall, Jr., *The Theory of Groups,* Macmillan, N.Y. 1963.

[H-R] E. Hewitt and K. Ross, *Abstract Harmonic Analysis,* Springer Verlag, Berlin, 1963.

[I] K. Iwasawa, *On solvable extensions of algebraic number fields,* Ann. of Math. **58** (1953) 548.

[J] N. Jacobson, *Lectures in Abstract Algebra, III,* Van Nostrand N.Y. 1964.

[L1] S. Lang, *On Quasi-algebraic closure,* Ann. of Math. **55** (1952), 373–390.

[L1] ———, *Rapport sur la Cohomologie des Groupes,* W. A. Benjamin, N.Y. 1966.

p. 311 [M] S. Mac Lane, *Homology,* Springer Verlag, Berlin, 1963.

[N] J. Neukirch, *Klassenkörpertheorie,* Bibliographisches Institut, Mannheim, 1969.

[O] A. Ostrowski, *Untersuchungen zur arithmetischen Theorie der Körper,* Math. Z. **39** (1935) 269–404.

[P] G. Poitou, *Cohomologie Galoisienne des Modules Finis,* Dunod, Paris, 1967.

[S1] J-P. Serre, *Cohomologie Galoisienne,* Lecture Notes in Mathematics no. **5**, Springer Verlag, Berlin, 1965.

[S2] ———, *Corps Locaux,* Act. Sci. Ind. no. **1296**, Paris, 1962.

[Sh] I. R. Shafarevich, *The Imbedding problem for splitting extensions,* Dokl. Akad. Nauk SSSR **120** (1958) 1217–1219 M. R. **21** No. 1301.

[Sp] E. Spanier, *Algebraic Topology,* McGraw-Hill, N.Y. 1966.

[T] C. Tsen, *Divisionalgebren über Funktionenkörper,* Nachrichten Ges. Wiss. Göttingen (1933).