§5. Nonabelian cohomology

In what follows, G denotes a profinite group.

5.1 Definition of H^0 and of H^1

A *G-set* E is a discrete topological space on which G acts continuously; as in the case of G-modules, this amounts to saying that $E = \bigcup E^U$, for U running over the set of open subgroups of G (we denote by E^U the subset of E of elements fixed under U). If $s \in G$ and $x \in E$, the image $s(x)$ of x under s will often be denoted by ${}^s x$ [but never x^s, to avoid the ugly formula $x^{(st)} = (x^t)^s$)]. If E and E' are two G-sets, a *morphism* of E to E' is a map $f : E \to E'$ which commutes with the action of G; if we wish to be explicit about G, we will write "G-morphism". The G-sets form a category.

A *G-group* A is a group in the above-mentioned category; this amounts to saying that it is a G-set, with a group structure invariant under G (i.e. ${}^s(xy) = {}^s x {}^s y$). When A is commutative, one recovers the notion of a *G-module*, used in the previous sections.

If E is a G-set, we put $H^0(G, E) = E^G$, the set of elements of E fixed under G. If E is a G-group, $H^0(G, E)$ is a group.

If A is a G-group, one calls *1-cocycle* (or simply *cocycle*) *of G in A* a map $s \mapsto a_s$ of G to A which is continuous and such that:

$$a_{st} = a_s {}^s a_t \quad (s, t \in G).$$

The set of these cocycles will be denoted $Z^1(G, A)$. Two cocycles a and a' are said to be *cohomologous* if there exists $b \in A$ such that $a'_s = b^{-1} a_s {}^s b$. This is an equivalence relation in $Z^1(G, A)$, and the quotient set is denoted $H^1(G, A)$. This is the "first cohomology set of G in A"; it has a distinguished element (called the "neutral element" even though there is in general no composition law on $H^1(G, A)$): the class of the unit cocycle; we denote it by either 0 or 1. One checks that

$$H^1(G, A) = \varinjlim H^1(G/U, A^U) ,$$

for U running over the set of open normal subgroups of G; moreover, the maps $H^1(G/U, A^U) \to H^1(G, A)$ are injective.

The cohomology sets $H^0(G, A)$ and $H^1(G, A)$ are functorial in A, and coincide with the cohomology groups of dimensions 0 and 1 when A is commutative.

Remarks.

1) One would like also to define $H^2(G,A)$, $H^3(G,A)$, ... I will not attempt to do so; the interested reader may consult Dedecker [38], [39] and Giraud [54].

2) The nonabelian H^1 are *pointed* sets; the notion of an exact sequence therefore makes sense (the image of a map is equal to the inverse image of the neutral element); however, such an exact sequence gives no information about the *equivalence relation* defined by a map; this defect (particularly obvious in [145], p. 131–134), can be remedied thanks to the notion of twisting, to be developed in §5.3.

Exercises.

1) Let A be a G-group, and let $A \cdot G$ be the semidirect product of G by A (defined in such a way that $sas^{-1} = {}^s a$ for $a \in A$ and $s \in G$).

A cocycle $a = (a_s) \in Z^1(G,A)$ defines a continuous lifting

$$f_a : G \longrightarrow A \cdot G$$

by $f_a(s) = a_s \cdot s$, and conversely. Show that the liftings f_a and $f_{a'}$ associated to the cocycles a and a' are conjugate by an element of A if and only if a and a' are cohomologous.

2) Let $G = \widehat{\mathbf{Z}}$; denote by σ the canonical generator of G.

(a) If E is a G-set, σ defines a permutation of E all of whose orbits are finite; conversely, such a permutation defines a G-set structure.

(b) Let A be a G-group. Let (a_s) be a cocycle of G in A, and let $a = a_\sigma$. Show that there exists $n \geq 1$ such that $\sigma^n(a) = a$ and that $a \cdot \sigma(a) \cdots \sigma^{n-1}(a)$ is of finite order. Conversely, every $a \in A$ for which there exists such an n corresponds to one and only one cocycle. If a and a' are two such elements, the corresponding cocycles are cohomologous if and only if there exists $b \in A$ such that $a' = b^{-1} \cdot a \cdot \sigma(b)$.

(c) How does the above need modifying when one replaces $\widehat{\mathbf{Z}}$ by $\mathbf{Z}_p$?

5.2 Principal homogeneous spaces over A – a new definition of $H^1(G,A)$

Let A be a G-group, and let E be a G-set. One says that A *acts on the left* on E (in a manner compatible with the action of G) if it acts on E in the usual sense and if ${}^s(a \cdot x) = {}^s a \cdot {}^s x$ for $a \in A$, $x \in E$ (this amounts to saying that the canonical map of $A \times E$ to E is a G-morphism). This is also written ${}_A E$ as a reminder that A acts on the left (there is an obvious similar notation for right actions).

A *principal homogeneous space* (or *torsor*) over A is a non-empty G-set P, on which A acts on the right (in a manner compatible with G) so as to make of it an "affine space" over A (i.e. for each pair $x, y \in P$, there exists a unique $a \in A$ such that $y = x \cdot a$). The notion of an isomorphism between two such spaces is defined in an obvious way.

Proposition 33. *Let A be a G-group. There is a bijection between the set of classes of principal homogeneous spaces over A and the set $H^1(G, A)$.*

Let $P(A)$ be the first set. One defines a map

$$\lambda : P(A) \longrightarrow H^1(G, A)$$

in the following way:

If $P \in P(A)$, we choose a point $x \in P$. If $s \in G$, one has ${}^s x \in P$, therefore there exists $a_s \in A$ such that ${}^s x = x \cdot a_s$. One checks that $s \mapsto a_s$ is a cocycle. Substituting $x \cdot b$ for x changes this cocycle into $s \mapsto b^{-1} a_s {}^s b$, which is cohomologous to it. One may thus define λ by taking $\lambda(P)$ as the class of a_s.

Vice versa, one defines $\mu : H^1(G, A) \to P(A)$ as follows:

If $a_s \in Z^1(G, A)$, denote by P_a the group A on which G acts by the following "twisted" formula:

$${}^{s\prime}x = a_s \cdot {}^s x \ .$$

If one lets A act on the right on P_a by translations, one obtains a principal homogeneous space. Two cohomologous cocycles give two isomorphic spaces. This defines the map μ, and one checks easily that $\lambda \circ \mu = 1$ and $\mu \circ \lambda = 1$.

Remark.

The principal spaces considered above are *right* principal spaces. One may similarly define the notion of a *left* principal space; we leave to the reader the task of defining a bijection between the two notions.

5.3 Twisting

Let A be a G-group, and let P be a principal homogeneous space over A. Let F be a G-set on which A acts on the left (compatibly with G). On $P \times F$, consider the equivalence relation which identifies an element (p, f) with the elements $(p \cdot a, a^{-1} f)$, $a \in A$. This relation is compatible with the action of G, and the quotient is a G-set, denoted $P \times^A F$, or ${}_P F$. An element of $P \times^A F$ can be written in the form $p \cdot f$, $p \in P$, $f \in F$, and one has $(pa)f = p(af)$, which explains the notation. Remark that, for all $p \in P$, the map $f \mapsto p \cdot f$ is a bijection of F onto ${}_P F$; for this reason, one says that ${}_P F$ is obtained from F *by twisting it using* P.

The twisting process can also be defined from the cocycle point of view. If $(a_s) \in Z^1(G, A)$, denote by ${}_a F$ the set F on which G acts by the formula

$${}^{s\prime} f = a_s \cdot {}^s f \ .$$

One says that ${}_a F$ is obtained *by twisting F using the cocycle a_s*.

The connection between these points of view is easy to make: if $p \in P$, we have seen that p defines a cocycle a_s by the formula ${}^s p = p \cdot a_s$. The map $f \mapsto p \cdot f$ defined above is *an isomorphism of the G-set ${}_a F$ with the G-set ${}_P F$*; indeed one has

$$p \cdot {}^{s\prime} f = p \cdot a_s \cdot {}^s f = {}^s p \cdot {}^s f = {}^s(p \cdot f) \ .$$

This shows in particular that ${}_a F$ *is isomorphic to* ${}_b F$ *if a and b are cohomologous.*

Remark.

Note that there is, in general, no canonical isomorphism between ${}_aF$ and ${}_bF$, and that consequently it is *impossible to identify* these two sets, as one would be tempted to do. In particular, the notation ${}_\alpha F$, with $\alpha \in H^1(G,A)$, is dangerous (even if sometimes convenient...). Of course, the same difficulty occurs in Topology, in the theory of fiber spaces (which we are mimicking).

The twisting operation enjoys a number of elementary properties:

(a) ${}_aF$ is functorial in F (for A-morphisms $F \to F'$).
(b) We have ${}_a(F \times F') = {}_aF \times {}_aF'$.
(c) If a G-group B acts on the right on F (so that it commutes with the action of A), B also acts on ${}_aF$.
(d) If F has a G-group structure invariant under A, the same structure on ${}_aF$ is also a G-group structure.

Examples.

1) Take for F the group A, acting on itself by left translations. Since right translations commute with left translations, property (c) above shows that A acts on the right on ${}_aF$, and one obtains thus a principal homogeneous space over A (namely the space denoted by ${}_aP$ in the previous subsection).

In the notation $P \times {}^AF$, this can be written:

$$P \times {}^AA = P\ ,$$

a cancellation formula analogous to $E \otimes_A A = E$.

2) Again take for F the group A, acting this time by *inner automorphisms.* Since this action preserves the group structure of A, property (d) shows that ${}_aA$ *is a G-group* [one could twist any normal subgroup of A in the same way]. By definition, ${}_aA$ has the same underlying group as A, and the action of G on ${}_aA$ is given by the formula

$$^{s\prime}x = a_s \cdot {}^sx \cdot a_s^{-1} \qquad (s \in G,\ x \in A).$$

Proposition 34. *Let F be a G-set where A acts on the left* (compatibly with G), *and let a be a cocycle of G in A. Then the twisted group ${}_aA$ acts on ${}_aF$, compatibly with G.*

One needs to check that the map $(a,x) \mapsto ax$ of ${}_aA \times {}_aF$ an ${}_aF$ is a G-morphism. This is a simple computation.

Corollary. *If P is a principal homogeneous space over A, the group ${}_PA$ acts on the left on P, and makes P into a principal left-homogeneous space over ${}_PA$.*

The fact that ${}_PA$ acts on P is a special case of prop. 34 (or can be seen directly, if one wishes). It is clear that this makes P into a principal left-homogeneous space over ${}_PA$.

Remark.

If A and A' are two G-groups, one defines the notion of an (A, A')-principal space in an obvious way: it is a principal (left) A-space, and a principal (right) A'-space, with the actions of A and A' commuting. If P is such a space, the above corollary shows that A may be identified with ${}_PA'$. If Q is an (A', A'')-principal space (A'' being some other G-group), the space $P \circ Q = P \times^{A'} Q$ has a canonical structure of an (A', A'')-principal space. In this way one obtains a composition law (not everywhere defined) on the set of "biprincipal" spaces.

Proposition 35. *Let P be a right principal homogeneous space for a G-group A, and let $A' = {}_PA$ be the corresponding group. If one associates to each principal* (right)*-homogeneous space Q over A' the composition $Q \circ P$, one obtains a bijection of $H^1(G, A')$ onto $H^1(G, A)$ that takes the neutral element of $H^1(G, A')$ into the class of P in $H^1(G, A)$.*

[More briefly: if one twists a group A by a cocycle of A itself, one gets a group A' which has the same cohomology as A in dimension 1.]

Define the opposite $\overline{P}$ of P as follows: it is an (A, A')-principal space, identical to P as a G-set, with the group A acting on the left by $a{\cdot}p = p{\cdot}a^{-1}$, and the group A' on the right by $p{\cdot}a' = a'^{-1}{\cdot}p$. By associating with each principal right A-space R the composition $R \circ \overline{P}$, we obtain the inverse map of that given by $Q \mapsto Q \circ P$. The proposition follows.

Proposition 35 bis. *Let $a \in Z^1(G, A)$, and let $A' = {}_aA$. To each cocycle a'_s in A' let us associate $a'_s \cdot a_s$; this gives a cocycle of G in A, whence a bijection*

$$t_a : Z^1(G, A') \longrightarrow Z^1(G, A)\ .$$

By taking quotients, t_a defines a bijection

$$\tau_a : H^1(G, A') \longrightarrow H^1(G, A)$$

mapping the neutral element of $H^1(G, A')$ into the class α of a.

This is essentially a translation of prop. 35 in terms of cocycles. It may also be proved by direct computation.

Remarks.

1) When A is *abelian*, we have $A' = A$ and τ_a is simply the *translation by the class α of a.*

2) Propositions 35 and 35 bis, elementary as they are, are nonetheless useful. As we shall see, they give a method to determine the equivalence relations which occur in various "cohomology exact sequences".

Exercise.

Let A be a G-group. Let $E(A)$ be the set of classes of (A, A)-principal spaces. Show that the composition makes $E(A)$ into a *group*, and that this group acts on $H^1(G, A)$. If A is abelian, $E(A)$ is the semi-direct product of $\mathrm{Aut}(A)$ by the group $H^1(G, A)$. In the general case, show that $E(A)$ contains the quotient of $\mathrm{Aut}(A)$ by the inner automorphisms defined by the elements of A^G. How may one define $E(A)$ using cocycles?

5.4 The cohomology exact sequence associated to a subgroup

Let A and B be two G-groups, and let $u : A \to B$ be a G-homomorphism. This homomorphism defines a map

$$v : H^1(G,A) \longrightarrow H^1(G,B) \ .$$

Let $\alpha \in H^1(G,A)$. We wish to describe the fiber of α for v, that is the set $v^{-1}(v(\alpha))$. Choose a representative cocycle a for α, and let b be its image in B. If one puts $A' = {}_aA$, $B' = {}_bB$, it is clear that u defines a homomorphism

$$u' : A' \longrightarrow B' \ ,$$

hence a map $v' : H^1(G,A') \to H^1(G,B')$.

We also have the following commutative diagram (where the letters τ_a and τ_b denote the bijections defined in 5.3):

$$\begin{array}{ccc} H^1(G,A) & \xrightarrow{v} & H^1(G,B) \\ \tau_a \big\uparrow & & \tau_b \big\uparrow \\ H^1(G,A') & \xrightarrow{v'} & H^1(G,B') \ . \end{array}$$

Since τ_b transforms the neutral element of $H^1(G,B')$ into $v(\alpha)$, we see that τ_a *is a bijection of the kernel of* v' *onto to the fiber* $v^{-1}(v(\alpha))$ *of* α. In other words, twisting allows one to transform each fiber of v into a kernel – and these kernels themselves may occur in exact sequences (cf. [145], *loc. cit.*).

Let us apply this principle to the simplest possible case, that in which A *is a subgroup of* B.

Consider the homogeneous space B/A of *left A-classes* of B; it is a G-set, and $H^0(G,B/A)$ is well-defined. Moreover, if $x \in H^0(G,B/A)$, the inverse image X of x in B is a principal (right-)homogeneous A-space; its class in $H^1(G,A)$ will be denoted by $\delta(x)$. The coboundary thus defined has the following property:

Proposition 36. *The sequence of pointed sets:*

$$1 \to H^0(G,A) \to H^0(G,B) \to H^0(G,B/A) \xrightarrow{\delta} H^1(G,A) \to H^1(G,B)$$

is exact.

It is easy to translate the definition of δ into cocycle terms; if $c \in (B/A)^G$, choose $b \in B$ which projects onto c, and set $a_s = b^{-1}.{}^sb$; this is a cocycle whose class is $\delta(c)$. Its definition shows that it is cohomologous to 0 in B, and that each cocycle of G in A which is cohomologous to 0 in B is of this form. The proposition follows.

Corollary 1. *The kernel of* $H^1(G,A) \to H^1(G,B)$ *may be identified with the quotient space of* $(B/A)^G$ *by the action of the group* B^G.

The identification is made *via* δ; we need to check that $\delta(c) = \delta(c')$ if and only if there exists $b \in B^G$ such that $bc = c'$; this is easy.

Corollary 2. *Let $\alpha \in H^1(G,A)$, and let a be a cocycle representing α. The elements of $H^1(G,A)$ with the same image as α in $H^1(G,B)$ are in one-to-one correspondence with the elements of the quotient of $H^0(G,{}_aB/{}_aA)$ by the action of the group $H^0(G,{}_aB)$.*

This follows from corollary 1 by twisting, as has been explained above.

Corollary 3. *In order that $H^1(G,A)$ be countable* (resp. *finite*, resp. *reduced to one element*), *it is necessary and sufficient that the same be true of its image in $H^1(G,B)$, and of all the quotients $({}_aB/{}_aA)^G/({}_aB)^G$, for $a \in Z^1(G,A)$.*

This follows from corollary 2.

One can also describe the *image* of $H^1(G,A)$ in $H^1(G,B)$ explicitly [just as if $H^1(G,B/A)$ made sense]:

Proposition 37. *Let $\beta \in H^1(G,B)$ and let $b \in Z^1(G,B)$ be a representative for β. In order that β belong to the image of $H^1(G,A)$, it is necessary and sufficient that the space ${}_b(B/A)$, obtained by twisting B/A by b, have a point fixed under G.*

[Combined with cor. 2 to prop. 36, this shows that the set of elements in $H^1(G,A)$ with image β is in one-to-one correspondence with the quotient $H^0(G,{}_b(B/A))/H^0(G,{}_bB)$.]

In order that β belong to the image of $H^1(G,A)$, it is necessary and sufficient that there exist $b \in B$ such that $b^{-1}b_s{}^sb$ belong to A for all $s \in G$. If c denotes the image of b in B/A, this means that $c = b_s \cdot {}^sc$, i.e. that $c \in H^0(G,{}_b(B/A))$, QED.

Remark.

Prop. 37 is an analogue of the classical theorem of Ehresmann: in order that the structural group A of a principal fiber bundle may be reduced to a given subgroup B, it is necessary and sufficient that the associated fiber space with fiber A/B have a section.

5.5 Cohomology exact sequence associated to a normal subgroup

Assume A normal in B, and set $C = B/A$; here, C is a G-group.

Proposition 38. *The sequence of pointed sets:*

$$0 \longrightarrow A^G \longrightarrow B^G \longrightarrow C^G \xrightarrow{\delta} H^1(G,A) \longrightarrow H^1(G,B) \longrightarrow H^1(G,C)$$

is exact.

The verification is immediate (cf. [145], p. 133).

The fibers of the map $H^1(G,A) \to H^1(G,B)$ were described in §5.4. However, the fact that A is normal in B simplifies that description. Note first:

The group C^G acts naturally (on the right) on $H^1(G,A)$. Indeed, let $c \in C^G$, and let $X(c)$ be its inverse image in B; the G-set $X(c)$ has, in a natural way, the structure of a principal (A,A)-space; if P is principal for A, the product $P \circ X(c)$ is also principal for A; it is the transform of P by c. [Translation into cocycle terms: lift c to $b \in B$; then ${}^sb = b \cdot x_s$, with $x_s \in A$; to each cocycle a_s of G in A, one associates the cocycle $b^{-1}a_s b\, x_s = b^{-1}a_s{}^sb$; its cohomology class is the image under c of that of (a_s).]

Proposition 39. (i) *If $c \in C^G$, then $\delta(c) = 1{\cdot}c$, where 1 represents the neutral element of $H^1(G,A)$.*

(ii) *Two elements of $H^1(G,A)$ have the same image in $H^1(G,B)$ if and only if they are in the same C^G-orbit.*

(iii) *Let $a \in Z^1(G,A)$, let α be its image in $H^1(G,A)$, and let $c \in C^G$. For $\alpha \cdot c = \alpha$, it is necessary and sufficient that c belong to the image of the homomorphism $H^0(G,{}_aB) \to H^0(G,C)$.*

[We denote by ${}_aB$ the group obtained by twisting B with the cocycle a — with A acting on B by inner automorphisms.]

The equation $\delta(c) = 1{\cdot}c$ is a consequence of the definition of δ. On the other hand, if two cocycles a_s and a'_s of A are cohomologous in B, there exists $b \in B$ such that $a'_s = b^{-1}a_s{}^sb$; if c is the image of b in C, one has ${}^sc = c$, whence $c \in C^G$, and it is clear that c maps the class of a_s into that of a'_s. The converse is trivial, which proves (ii). Finally, if $b \in B$ is a lift of c, and if $\alpha \cdot c = \alpha$, there exists $x \in A$ such that $a_s = x^{-1}b^{-1}a_s{}^sb\,{}^sx$; this can also be written $bx = a_s{}^s(bx)a_s^{-1}$, i.e. $bx \in H^0(G,{}_aB)$. Hence (iii).

Corollary 1. *The kernel of $H^1(G,B) \to H^1(G,C)$ may be identified with the quotient of $H^1(G,A)$ by the action of the group C^G.*

This is clear.

Corollary 2. *Let $\beta \in H^1(G,B)$, and let b be a cocycle representing β. The elements of $H^1(G,B)$ with the same image as β in $H^1(G,C)$ correspond bijectively with the elements of the quotient of $H^1(G,{}_bA)$ by the action of the group $H^0(G,{}_bC)$.*

[The group B acts on itself by inner automorphisms, and leaves A stable; this allows the *twisting* of the exact sequence $1 \to A \to B \to C \to 1$ by the cocycle b.]

This follows from cor. 1 by twisting, as was explained in the previous section.

Remark.

Proposition 35 shows that $H^1(G,{}_bB)$ may be identified with $H^1(G,B)$, and similarly $H^1(G,{}_bC)$ may be identified with $H^1(G,C)$. In contrast, $H^1(G,{}_bA)$ *bears, in general, no relation to* $H^1(G,A)$.

Corollary 3. *In order that $H^1(G,B)$ be countable* (resp. *finite,* resp. *reduced to a single element*), *it is necessary and sufficient that the same be true for its image in $H^1(G,C)$, and for all the quotients $H^1(G,{}_bA)/({}_bC)^G$, for $b \in Z^1(G,B)$.*

This follows from cor. 2.

Exercise.

Show that, if one associates to each $c \in C^G$ the class of the principal (A,A)-space $X(c)$, one obtains a homomorphism of C^G into the group $E(A)$ defined in the exercise in §5.3.

5.6 The case of an abelian normal subgroup

Assume A is abelian and normal in B. Keep the notation of the preceding section. Write $H^1(G,A)$ additively, since it is now an abelian group. If $\alpha \in H^1(G,A)$, and $c \in C^G$, denote by α^c the image of α by c, defined as above. Let us make this operation more explicit.

To this end, we note that the obvious homomorphism $C^G \to \mathrm{Aut}(A)$ makes C^G act (on the left) on the group $H^1(G,A)$; the image of α by c (for this new action) will be denoted $c \cdot \alpha$.

Proposition 40. *We have $\alpha^c = c^{-1} \cdot \alpha + \delta(c)$ for $\alpha \in H^1(G,A)$ and $c \in C^G$.*

This is a simple computation: if we lift c to $b \in B$, we have ${}^sb = b{\cdot}x_s$, and the class of x_s is $\delta(c)$. On the other hand, if a_s is a cocycle in the class α, we can take as a representative of α^c the cocycle $b^{-1}a_s{}^sb$, and to represent $c^{-1}{\cdot}\alpha$ the cocycle $b^{-1}a_sb$. We have $b^{-1}a_s{}^sb = b^{-1}a_sb \cdot x_s$, from which the formula follows.

Corollary 1. *We have $\delta(c'c) = \delta(c) + c^{-1} \cdot \delta(c')$.*

Write $\alpha^{c'c} = (\alpha^{c'})^c$. Expanding this gives the formula we want.

Corollary 2. *If A is in the center of B, $\delta : C^G \to H^1(G,A)$ is a homomorphism, and $\alpha^c = \alpha + \delta(c)$.*

This is obvious.

Now we shall make use of the group $H^2(G,A)$. *A priori*, one would like to define a coboundary: $H^1(G,C) \to H^2(G,A)$. In this form, this is not possible unless A is contained in the center of B (cf. §5.7). However, one does have a partial result, namely the following:

Let $c \in Z^1(G,C)$ be a cocycle for G in C. Since A is abelian, C *acts on* A, and the twisted group ${}_cA$ is well defined. We shall associate to c a cohomology class $\Delta(c) \in H^2(G,{}_cA)$. To do this, we lift c_s to a continuous map $s \mapsto b_s$ of G into B, and we define:

$$a_{s,t} = b_s{}^sb_tb_{st}^{-1} .$$

This 2-cochain is a *cocycle* with values in ${}_cA$. Indeed, if we take into account the way G acts on ${}_cA$, we see that this amounts to the identity:

$$a_{s,t}^{-1} \cdot b_s{}^s a_{t,u} b_s^{-1} \cdot a_{s,tu} \cdot a_{st,u}^{-1} = 1 \ , \quad (s,t,u \in G),$$

i.e.

$$b_{st}{}^s b_t^{-1} b_s^{-1} \cdot b_s{}^s b_t{}^{st} b_u{}^s b_{tu}^{-1} b_s^{-1} \cdot b_s{}^s b_{tu} b_{stu}^{-1} \cdot b_{stu}{}^{st} b_u^{-1} b_{st}^{-1} = 1 \ ,$$

which is true (all the terms cancel out).

On the other hand, if we replace the lift b_s by the lift $a'_s b_s$, the cocycle $a_{s,t}$ is replaced by the cocycle $a'_{s,t} \cdot a_{s,t}$, with

$$a'_{s,t} = (\delta a')_{s,t} = a'_s \cdot b_s{}^s a'_t b_s^{-1} \cdot a'^{-1}_{st} \ ;$$

this can be checked by a similar (and simpler) computation. Thus, the equivalence class of the cocycle $a_{s,t}$ is well defined; we denote it $\Delta(c)$.

Proposition 41. *In order that the cohomology class of c belongs to the image of $H^1(G,B)$ in $H^1(G,C)$, it is necessary and sufficient that $\Delta(c)$ vanish.*

This is clearly necessary. Conversely, if $\Delta(c) = 0$, the above shows that we may choose b_s so that $b_s{}^s b_t b_{st}^{-1} = 1$, and b_s is a cocycle for G in B with image equal to c. Whence the proposition.

Corollary. *If $H^2(G, {}_cA) = 0$ for all $c \in Z^1(G,C)$, the map*

$$H^1(G,B) \longrightarrow H^1(G,C)$$

is surjective.

Exercises.

1) Rederive prop. 40 using the exercise in §5.5 and the fact that $E(A)$ is the semi-direct product of $\mathrm{Aut}(A)$ with $H^1(G,A)$.

2) Let c and $c' \in Z^1(G,C)$ be two cohomologous cocycles. Compare $\Delta(c)$ and $\Delta(c')$.

5.7 The case of a central subgroup

We assume now that A is *contained in the center* of B. If $a = (a_s)$ is a cocycle for G in A, and $b = (b_s)$ is a cocycle for G in B, it is easy to see that $a \cdot b = (a_s \cdot b_s)$ is a cocycle for G in B. Moreover, the class of $a \cdot b$ depends only on the classes of a and of b. Hence the abelian group $H^1(G,A)$ *acts on the set* $H^1(G,B)$.

Proposition 42. *Two elements of $H^1(G,B)$ have the same image in $H^1(G,C)$ if and only if they are in the same $H^1(G,A)$-orbit.*

The proof is immediate.

Now let $c \in Z^1(G,C)$. Since C acts trivially on A, the twisted group ${}_cA$ used in §5.6 may be identified with A, and the element $\Delta(c)$ belongs to $H^2(G,A)$. An easy computation (cf. [145], p. 132) shows that $\Delta(c) = \Delta(c')$ if c and c' are cohomologous. This defines a map $\Delta : H^1(G,C) \to H^2(G,A)$. Putting together prop. 38 and 41, we obtain:

Proposition 43. *The sequence*

$$1 \longrightarrow A^G \longrightarrow B^G \longrightarrow C^G$$

$$\xrightarrow{\delta} H^1(G,A) \longrightarrow H^1(G,B) \longrightarrow H^1(G,C) \xrightarrow{\Delta} H^2(G,A)$$

is exact.

As usual, this sequence only gives us information about the kernel of $H^1(G,C) \to H^2(G,A)$, and not on the corresponding equivalence relation. To obtain that, we must twist the groups under consideration. More precisely, observe that C acts on B by automorphisms and that these automorphisms are trivial on A. If $c = (c_s)$ is a cocycle for G in C, we may twist the exact sequence $1 \to A \to B \to C \to 1$ with c, and we obtain the new exact sequence

$$1 \longrightarrow A \longrightarrow {}_cB \longrightarrow {}_cC \longrightarrow 1\ .$$

This gives a new coboundary operator $\Delta_c : H^1(G,{}_cC) \to H^2(G,A)$. Since we also have a canonical bijection $\tau_c : H^1(G,{}_cC) \to H^1(G,C)$, we can use it to compare Δ and Δ_c. The result is the following:

Proposition 44. *We have $\Delta \circ \tau_c(\gamma') = \Delta_c(\gamma') + \Delta(\gamma)$, where $\gamma \in H^1(G,C)$ denotes the equivalence class of c, and γ' belongs to $H^1(G,{}_cC)$.*

Let c'_s be a cocycle representing γ'. Choose as above a cochain b_s (resp. b'_s) in B (resp. in ${}_cB$) as a lift of c_s (resp. c'_s). We may represent $\Delta(\gamma)$ by the cocycle

$$a_{s,t} = b_s{}^s b_t b_{st}^{-1}\ ,$$

and $\Delta_c(\gamma')$ by the cocycle

$$a'_{s,t} = b'_s \cdot b_s{}^s b'_t b_s^{-1} \cdot b'^{-1}_{st}\ .$$

On the other hand $\tau_c(\gamma')$ can be represented by $c'_s c_s$, which we may lift to $b'_s b_s$. Thus we may represent $\Delta \circ \tau_c(\gamma')$ by the cocycle

$$a''_{s,t} = b'_s b_s \cdot {}^s b'_t{}^s b_t \cdot b_{st}^{-1} b'^{-1}_{st}\ .$$

Since $a_{s,t}$ is in the center of B, we may write:

$$a'_{s,t} \cdot a_{s,t} = b'_s b_s{}^s b'_t b_s^{-1} a_{s,t} b'^{-1}_{st}\ .$$

Replacing $a_{s,t}$ by its value and simplifying, we see that we find $a''_{s,t}$; the proposition follows.

Corollary. *The elements of $H^1(G,C)$ having the same image as γ under Δ correspond bijectively with the elements of the quotient of $H^1(G,{}_cB)$ by the action of $H^1(G,A)$.*

Indeed, the bijection τ_c^{-1} transforms these elements into those of the kernel of

$$\Delta_c : H^1(G,{}_cC) \longrightarrow H^2(G,A) ,$$

and prop. 42 and 43 show that this kernel may be identified with the quotient of $H^1(G,{}_cB)$ by the action of $H^1(G,A)$.

Remarks.

1) Here again it is, in general, false that $H^1(G,{}_cB)$ is in bijective correspondence with $H^1(G,B)$.

2) We leave to the reader the task of stating the criteria for denumerability, finiteness, etc., which follow from the corollary.

Exercise.

Since C^G acts on B by inner automorphisms, it also acts on $H^1(G,B)$. Let us denote this action by

$$(c,\beta) \mapsto c*\beta \quad (c \in C^G,\ \beta \in H^1(G,B)).$$

Show that:

$$c*\beta = \delta(c)^{-1}\cdot\beta ,$$

where $\delta(c)$ is the image of c in $H^1(G,A)$, cf. §5.4, and where the product $\delta(c)^{-1}\cdot\beta$ is relative to the action of $H^1(G,A)$ on $H^1(G,B)$.

5.8 Complements

We leave to the reader the task of treating the following topics:

a) Group extensions

Let H be a closed normal subgroup in G, and let A be a G-group. The group G/H acts on A^H, which means that $H^1(G/H,A^H)$ is well-defined. On the other hand, if $(a_h) \in Z^1(H,A)$ and $s \in G$, we can define the transform $s(a)$ of the cocycle $a=(a_h)$ by the formula:

$$s(a)_h = s(a_{s^{-1}hs}) .$$

By passing to the quotient, the group G acts on $H^1(H,A)$, and one checks that H acts trivially. Thus *G/H acts on $H^1(H,A)$*, just as in the abelian case. We have the exact sequence:

$$1 \longrightarrow H^1(G/H,A^H) \longrightarrow H^1(G,A) \longrightarrow H^1(H,A)^{G/H} ,$$

and the map $H^1(G/H,A^H) \to H^1(G,A)$ is injective.

b) Induction

Let H be a closed subgroup of G, and let A be an H-group. Let $A^* = M_G^H(A)$ be the group of continuous maps $a^* : G \to A$ such that $a^*({}^h x) = {}^h a^*(x)$ for $h \in H$ and $x \in G$. We let G act on A^* by the formula $({}^g a^*)(x) = a^*(xg)$. We obtain in this way a G-group A^* and one has canonical bijections

$$H^0(G, A^*) = H^0(H, A) \qquad \text{and} \qquad H^1(G, A^*) = H^1(H, A) \ .$$

5.9 A property of groups with cohomological dimension ≤ 1

The following result could have been given in §3.4:

Proposition 45. *Let I be a set of prime numbers, and assume that $\mathrm{cd}_p(G) \leq 1$ for every $p \in I$. Then the group G has the lifting property for the extensions $1 \to P \to E \to W \to 1$, where the order of E is finite, and the order of P is only divisible by prime numbers belonging to I.*

We use induction on the order of P, the case $\mathrm{Card}(P) = 1$ being trivial. Assume therefore $\mathrm{Card}(P) > 1$, and let p be a prime divisor of $\mathrm{Card}(P)$. By hypothesis, we have $p \in I$. Let R be a Sylow p-subgroup in P. There are two cases:

a) R is normal in P. Then it is the only Sylow p-subgroup in P, and it is normal in E. We have the extensions:

$$1 \longrightarrow R \longrightarrow E \longrightarrow E/R \longrightarrow 1$$

$$1 \longrightarrow P/R \longrightarrow E/R \longrightarrow W \longrightarrow 1 \ .$$

Since $\mathrm{Card}(P/R) < \mathrm{Card}(P)$, the induction hypothesis shows that the given homomorphism $f : G \to W$ lifts to $g : G \to E/R$. On the other hand, since R is a p-group, prop. 16 in §3.4 shows that g lifts to $h : G \to E$. We have thus lifted f.

b) R is not normal in P. Let E' be the normalizer of R in E, and let P' be the normalizer of R in P. We have $P' = E' \cap P$. Also, the image of E' in W is equal to all of W. Indeed, if $x \in E$, it is clear that $x\,R\,x^{-1}$ is a Sylow p-subgroup of P, and the conjugacy of Sylow subgroups implies the existence of $y \in Pv$ such that $x\,R x^{-1} = y\,R\,y^{-1}$. Thus we have $y^{-1}x \in E'$, which shows that $E = P \cdot E'$, from which our assertion follows. We thus get the extension:

$$1 \longrightarrow P' \longrightarrow E' \longrightarrow W \longrightarrow 1 \ .$$

Since $\mathrm{Card}(P') < \mathrm{Card}(P)$, the induction hypothesis shows that the morphism $f : G \to W$ lifts to $h : G \to E'$, and because E' is a subgroup of E, this finishes the proof.

Corollary 1. *Every extension of G by a profinite group P whose order is not divisible by the primes belonging to I splits.*

The case where P is finite follows directly from the proposition and from lemma 2 in §1.2. The general case is handled by "Zornification", as in §3.4 (see also exerc. 3).

Remark.
The above corollary gives the fact that a group extension of a finite group A by a finite group B splits when the orders of A and of B are prime to each other (cf. Zassenhaus, [189], Chap. IV, §7).

A profinite group G is said to be *projective* (in the category of profinite groups) if it has the lifting property for every extension; this amounts to saying that, for any surjective morphism $f : G' \to G$, where G' is profinite, there exists a morphism $r : G \to G'$ such that $f \circ r = 1$.

Corollary 2. *If G is a profinite group, the following properties are equivalent:*
(i) *G is projective.*
(ii) $\mathrm{cd}(G) \leq 1$.
(iii) *For any prime number p, the Sylow p-subgroups of G are free pro-p-groups.*

The equivalence (ii) $\Leftrightarrow$ (iii) has already been proved. The implication (i) $\Rightarrow$ (ii) is clear (cf. prop. 16). The implication (ii) $\Rightarrow$ (i) follows from cor. 1, applied to the case where I is the set of all prime numbers.

Examples of projective groups: (a) the completion of a free (discrete) group in the topology induced by subgroups of finite index; (b) a direct product $\prod_p F_p$, where each F_p is a free pro-p-group.

Proposition 46. *With the same hypotheses as in prop. 45, let*

$$1 \longrightarrow A \longrightarrow B \longrightarrow C \longrightarrow 1$$

be an exact sequence of G-groups. Assume that A is finite, and that each prime divisor of the order of A belongs to I. The canonical map $H^1(G,B) \to H^1(G,C)$ is surjective.

Let (c_s) be a cocycle for G with values in C. If π denotes the homomorphism $B \to C$, let E be the set of pairs (b, s), with $b \in B$, $s \in G$, such that $\pi(b) = c_s$. We put on E the following composition law (cf. exerc. 1 in §5.1):

$$(b, s) \cdot (b', s') = (b \cdot {}^s b', ss') \ .$$

The fact that $c_{ss'} = c_s \cdot {}^s c_{s'}$ shows that $\pi(b \cdot {}^s b') = c_{ss'}$, which means that the above definition is legitimate. One checks that E, with this composition law and the topology induced by that of the product $B \times G$, is a compact group. The obvious morphisms $A \to E$ and $E \to G$, make of E *an extension of G by A*. By cor..1 to prop. 45, this extension splits. Therefore there exists a continuous section $s \mapsto e_s$ which is a morphism of G into E. If we write $e_s \in E$ in the form (b_s, s), the fact that $s \mapsto e_s$ is a morphism shows that b_s is a cocycle for G in B which is a lift of the given cocycle c_s. The proposition follows.

Corollary. *Let $1 \to A \to B \to C \to 1$ be an exact sequence of G-groups. If A is finite, and if* $\mathrm{cd}(G) \leq 1$, *the canonical map $H^1(G, B) \to H^1(G, C)$ is surjective.*

This is the special case where I is the set of all prime numbers.

Exercises.

1) Let $1 \to A \to B \to C \to 1$ be an exact sequence of G-groups, with A a finite abelian group. The method used in the proof of prop. 46 associates to each $c \in Z^1(G, C)$ an extension E_c of G by A. Show that the action of G on A resulting from this extension is that of ${}_cA$, and that the image of E_c in $H^2(G, {}_cA)$ is the element $\Delta(c)$ defined in §5.6.

2) Let A be a finite G-group, with order prime to the order of G. Show that $H^1(G, A) = 0$. [Reduce to the finite case, where the result is known: it is a consequence of the Feit-Thompson theorem which says that groups of odd order are solvable.]

3) Let $1 \to P \to E \to G \to 1$ be an extension of profinite groups, where G and P satisfy the hypotheses of cor. 1 to prop. 45. Let E' be a closed subgroup of E which projects onto G, and which is minimal for this property (cf. §1.2, exerc. 2); let $P' = P \cap E'$. Show that $P' = 1$. [Otherwise, there would exist an open subgroup P'' of P', normal in E', with $P'' \neq P'$. Applying prop. 45 to the extension $1 \to P'/P'' \to E'/P'' \to G \to 1$, one would get a lifting of G into E'/P'', and therefore a closed subgroup E'' of E', projecting onto G, such that $E'' \cap P' = P''$; this would contradict the minimality of E'.] Deduce from this another proof of cor. 1 to prop. 45.

4) (a) Let P be a profinite group. Show the equivalence of the following properties:

(i) P is a projective limit of finite nilpotent groups.

(ii) P is a direct product of pro-p-groups.

(iii) For any prime p, P has only one Sylow p-subgroup.

Such a group is called *pronilpotent.*

(b) Let $f : G \to P$ be a surjective morphism of profinite groups. Assume that P is pronilpotent. Show that there exists a pronilpotent subgroup P' of G such that $f(P') = P$. [Write P as a quotient of a product $F = \prod_p F_p$, where the F_p are free pro-p-groups, and lift $F \to G$ to $F \to G$ by cor. 2 of prop. 45.]

When P and G are finite groups, one recovers a known result, (cf. Huppert [74], III.3.10.)

5) Show that a closed subgroup of a projective group is projective.