ELEMENTARY GENERALIZATIONS OF HILBERT'S THEOREM 90

Ian G. Connell

(received May 7, 1965)

Introduction. Let K, k be fields and $K|k$ a finite galois extension with galois group G. The multiplicative group K^* of K is a G-module, that is, a module over the integral group ring ZG, the module action of an element $\sigma \epsilon G$ being its effect as an automorphism. It is shown in [2, p. 158] that the first cohomology group vanishes†:

$$(1) \qquad H^1(G, K^*) = 0 .$$

When G is cyclic, $H^1(G, K^*)$ can be calculated in another way so that comparison with (1) gives Hilbert's

THEOREM 90. If G is cyclic with generator σ and x is an element of K^* of norm 1 (i.e., $N_{K|k}\, x = 1$) then there exists $y \epsilon K^*$ such that $x = \frac{\sigma y}{y}$.

Here we extend this method to non-cyclic groups giving, for example, a 'theorem 90' for abelian extensions. To each finite group G, or more accurately, to each presentation of G, there is attached a 'theorem 90' which tends to become more intricate as G does.

I wish to thank the referee for drawing my attention to the paper of Gruenberg [1]. The proof of our main proposition would be shortened by quoting results from [1], but we decided not to do so since the present proof is self-contained and entirely elementary.

† See the next section for the definition of H^1.

Canad. Math. Bull. vol. 8, no. 6, 1965

Explicit calculation of H^1. Let G be an arbitrary group and A a G-module† written additively. (When $A = K^*$ we will have to switch to multiplicative notation.) A cocycle is a function $f : G \to A$ satisfying

$$(2) \qquad f(\sigma\tau) = \sigma f(\tau) + f(\sigma) \qquad \forall\, \sigma, \tau \in G;$$

the cocycles under pointwise addition form an abelian group, denoted $Z(G, A)$. If there exists an $a \in A$ such that

$$(3) \qquad f(\sigma) = \sigma a - a \qquad \forall\, \sigma \in G$$

then f is a coboundary. The coboundaries form a subgroup $B(G,A)$ and the quotient group

$$H^1(G,A) = Z(G,A)/B(G,A)$$

is called the first cohomology group (of G with coefficients in A).

It follows immediately from (2) that

$$(4) \qquad f(1) = 0, \quad f(\sigma^{-1}) = -\sigma^{-1} f(\sigma).$$

Let G be given by generators $\sigma_1, \ldots, \sigma_m$ and relations $R_1 = R_2 = \ldots = 1$, and put $f(\sigma_i) = a_i$. By repeated application of (2), f is uniquely determined by the a_i so that $f \rightsquigarrow (a_1, \ldots, a_m)$ gives rise to the abelian group monomorphism $\theta : Z(G,A) \to A^m = A \times A \times \ldots \times A$ (direct product with m factors), with the obvious interpretation when m is infinite. We wish to characterize the elements of $\mathrm{Im}\,\theta$ by means of the relations $R_i = 1$.

Every element in the free group F generated by the symbols σ_i is uniquely expressible in the form $x_1 \ldots x_r$ where each x_j is a σ_i or a σ_i^{-1} and no σ_i occurs next to

† All modules are assumed to be unitary.

https://doi.org/10.4153/CMB-1965-055-2 Published online by Cambridge University Press

σ_i^{-1}, so no cancellation can take place. As a technical convenience we assume that each R_i is such a reduced word; this is no real restriction. By a consequence of the R_i we mean an element in the normal subgroup of F generated by the R_i.

If f is a cocycle, the relation $R_i = x_1 \ldots x_r = 1$ in G gives rise, by (2) and (4), to the following relation in A:

$$(5) \qquad R_i^* = 0 = x_1 \ldots x_{r-1} f(x_r) + x_1 \ldots x_{r-2} f(x_{r-1}) + \ldots + f(x_1)$$

where † $$f(x_j) = \begin{cases} a_i & \text{if } x_j = \sigma_i \\ -\sigma_i^{-1} a_i & \text{if } x_j = \sigma_i^{-1} . \end{cases}$$

We will show that conversely an element $(a_1, \ldots, a_m) \in A^m$ satisfying all the relations (5) corresponds to a cocycle.

LEMMA. If $a_1, \ldots, a_m$ satisfy all the relations $R_i^* = 0$ then they satisfy $R^* = 0$ where R is any consequence of the R_i.

---

† Note that the relation $R_i^* = 0$ obtained does not depend upon the bracketing of the x_j. For example $x_1(x_2x_3) = 1$ and $(x_1x_2)x_3 = 1$ give rise respectively to

$$0 = x_1\{x_2 f(x_3) + f(x_2)\} + f(x_1)$$

and

$$0 = x_1x_2 f(x_3) + \{x_1 f(x_2) + f(x_1)\} ,$$

which are the same.

https://doi.org/10.4153/CMB-1965-055-2 Published online by Cambridge University Press

Proof: R is a word in the R_i, their inverses and their conjugates. Thus if the a_j satisfy $R_1^* = 0$ and $R_2^* = 0$ it suffices to verify that they satisfy $R^* = 0$ in the following four cases:

(i) $R = R_1^{-1}$

(ii) $R = R_1 R_2$

(iii) $R = \sigma_i^{-1} R_1 \sigma_i$

(iv) $R = \sigma_i R_1 \sigma_i^{-1}$.

The verifications are of a straightforward computational nature so we only indicate a few details. Let $R_1 = x_1 \ldots x_r$, $R_2 = y_1 \ldots y_s$.

(i) Multiplying

$$0 = R_1^* = x_1 \ldots x_{r-1} f(x_r) + \ldots + f(x_1)$$

by $-x_r^{-1} \ldots x_1^{-1}$ we obtain $R^* = 0$.

(ii) Let $R_1 R_2 = x_1 \ldots x_{r-t} y_{1+t} \ldots y_s$. (We must allow for cancellation since this is how multiplication is defined in F.) Thus

$$y_1 = x_r^{-1}, \ldots, y_t = x_{r-t+1}^{-1} .$$

We have

$$0 = R_1^* = x_1 \ldots x_{r-1} f(x_r) + \ldots + f(x_1)$$

$$= R_2^* = y_1 \ldots y_{s-1} f(y_s) + \ldots + f(y_1) ;$$

https://doi.org/10.4153/CMB-1965-055-2 Published online by Cambridge University Press

adding the first to $x_1 \dots x_r$ times the second, rearranging and cancelling (according to the definition of $f(\sigma_i^{-1})$ in (5)) we obtain $(R_1 R_2)^* = 0$.

In (iii) and (iv) one deals with the various cases when σ_i or σ_i^{-1} does or does not cancel x_1 or x_r.

Now let $a_1, \dots$ satisfy the relations $R_i^* = 0$ (and therefore any consequence $R^* = 0$). Any element $\sigma \in G$ can be written as a word, usually in several ways, in the σ_i: $\sigma = x_1 \dots x_r$, $x_j = \sigma_i$ or σ_i^{-1} for some i. We define

$$f(\sigma) = x_1 \dots x_{r-1} f(x_r) + \dots + f(x_1)$$

where $f(\sigma_i) = a_i$ and $f(\sigma_i^{-1}) = -\sigma_i^{-1} a_i$. To complete the discussion we must show that

(a) $f(\sigma)$ does not depend on how σ is written in terms of the generators, and

(b) $f(\sigma\tau) = \sigma f(\tau) + f(\sigma) \qquad \forall \sigma, \tau \in G$.

(a) If also $\sigma = y_1 \dots y_s$ we have the relation (allowing for cancellation)

$$R = x_1 \dots x_{r-t} y_{s-t}^{-1} \dots y_1^{-1} = 1$$

which, by the lemma, we may suppose to be already in the list $R_i = 1$ since this imposes no new conditions on the a_i. Now

$$0 = R^* = x_1 \dots y_2^{-1} f(y_1^{-1}) + \dots + f(x_1)$$

and this, properly juggled, gives the required equation $f(x_1 \dots x_r) = f(y_1 \dots y_s)$.

(b) follows by calculation (made simple by (a): one need no longer worry about cancellation since $f(\sigma)$ does not depend on how σ is written in terms of the generators).

If f is a coboundary then $\exists c \in A$ such that $f(\sigma) = (\sigma - 1)c \ \forall \sigma$ and therefore $a_i = (\sigma_i - 1)c$. Conversely if $\exists c$ such that $a_i = (\sigma_i - 1)c \ \ \forall i$ then $f(\sigma_i^{-1}) = -\sigma_i^{-1} a_i = (\sigma_i^{-1} - 1)c$ and by induction on the length of the word one easily verifies that $f(\sigma) = (\sigma - 1)c \ \ \forall \sigma \in G$. We have the

PROPOSITION. Let the group G be given by generators $\sigma_1, \ldots, \sigma_m$ and relations $R_1 = \ldots = 1$ and let A be a G-module. Then $Z(G, A)$ is the subgroup of the direct product† A^m consisting of those $(a_1, \ldots, a_m)$ satisfying the relations $R_1^* = \ldots = 0$, as described in (5). $B(G, A)$ consists of those $(a_1, \ldots, a_m)$ for which there exists a $c \in A$ such that $a_i = (\sigma_i - 1)c$ for all i.

As a simple illustration of the use of this proposition, let G act trivially¶ on A; then $(0, \ldots, 0)$ is the only element in $B(G, A)$, and $H^1(G, A)$ consists of those $(a_i, \ldots) \in A^m$ satisfying the relations $R_i^* = 0$.

First, if G is free with generators $\sigma_1, \ldots, \sigma_m$ there are no relations imposed on the a_i so $H^1(G, A) = A^m$.

Secondly let G be finitely generated abelian, say $G = G_1 \times \ldots \times G_m$ where G_i is cyclic with generator σ_i and has order n_i for $1 \leq i \leq r$ and infinite order for $r + 1 \leq i \leq m$. The relations are $\sigma_i^{n_i} = 1 \ \ (1 \leq i \leq r)$ and $\sigma_i \sigma_j \sigma_i^{-1} \sigma_j^{-1} = 1$

---

† m may be infinite.

¶ So by (2), $H^1(G, A) = \text{Hom group } (G, A)$.

$(1 \leq i < j \leq m)$. Only the first set of relations impose restrictions and we have

$$H^1(G, \mathring{A}) = A_1 \times \ldots \times A_r \times A^{m-r}$$

where $A_i = \{ a \in A : n_i a = 0 \}$.

Theorem 90 for non-cyclic extensions. We assume without proof the result already quoted that $H^1(G, K^*) = 0$, i.e., every cocycle is a coboundary. If $\sigma \in G$ let K_σ denote the fixed field of the subgroup generated by σ. A typical relation in the definition of the finite group G is $\sigma^n = 1$ where $\sigma = \sigma_{i_1} \sigma_{i_2} \ldots \sigma_{i_r}$ is a product of generators; the corresponding relation (5) is, in multiplicative notation,

$$\sigma^{n-1} a \cdot \sigma^{n-2} a \ldots \sigma a \cdot a = 1 ,$$

where $a = f(\sigma) = (\sigma_{i_1} \ldots \sigma_{i_{r-1}} a_{i_r}) \ldots (\sigma_{i_1} a_{i_2}) a_{i_1}$, which can be put in the convenient form

$$N_{K|K_\sigma} a = 1 .$$

Of course if $n = 1$ this means that $a = 1$. For example, the relations $\sigma_1^n = 1$, $(\sigma_1 \sigma_2)^n = 1$ and $\sigma_1 \sigma_2 \sigma_1^{-1} \sigma_2^{-1} = 1$ give rise to

$$N_{K|K_{\sigma_1}} a_1 = 1 , \quad N_{K|K_{\sigma_1 \sigma_2}} (\sigma_1 a_2 \cdot a_1) = 1$$

and $\dfrac{\sigma_1 a_2}{a_2} = \dfrac{\sigma_2 a_1}{a_1}$, respectively.

We conclude with some explicit examples (omitting the simple details of the proofs).

Theorem 90 for abelian extensions. Let $G = G_1 \times \ldots \times G_m$ where G_i is cyclic of order n_i with generator σ_i, so G is described by generators $\sigma_1, \ldots, \sigma_m$ and relations $\sigma_i^{n_i} = \sigma_i \sigma_j \sigma_i^{-1} \sigma_j^{-1} = 1$. If $a_1, \ldots, a_m \in K^*$ are such that

(6) $$N_{K|K_{\sigma_i}} a_i = 1 ,$$

and

(7) $$\frac{\sigma_i a_j}{a_j} = \frac{\sigma_j a_i}{a_i} ,$$

then there exists a $c \in K^*$ such that

$$a_i = \frac{\sigma_i c}{c} , \qquad i = 1, \ldots, m .$$

Note that a single c works for all the a_i. When $m = 1$ the compatibility conditions (7) evaporate and we have the original theorem 90.

It will be observed that different presentations of G give rise to different variants of theorem 90. Thus for the cyclic group of order 6 we have the original theorem and also the theorem which arises from writing this group as the direct product of cyclic groups of orders 2 and 3.

Theorem 90 for the dihedral groups. (G is given by generators σ, τ and relations $\sigma^p = \tau^2 = (\sigma\tau)^2 = 1$.) If $a, b \in K^*$ are such that

$$N_{K|K_\sigma} a = N_{K|K_\tau} b = N_{K|K_{\sigma\tau}} (a \cdot \sigma b) = 1$$

then there exists a $c \in K^*$ such that

https://doi.org/10.4153/CMB-1965-055-2 Published online by Cambridge University Press

$$a = \frac{\sigma c}{c}, \qquad b = \frac{\tau c}{c}.$$

Theorem 90 for the symmetric group S_3. (S_3 is given by generators σ, τ and relations $\sigma^2 = \tau^2 = (\sigma\tau)^3 = 1$.) If $a, b \in K^*$ are such that

$$N_{K|K_\sigma} a = N_{K|K_\tau} b = N_{K|K_{\sigma\tau}} \frac{a}{b} = 1$$

then $\exists\, c \in K^*$ such that

$$a = \frac{\sigma c}{c}, \qquad b = \frac{\tau c}{c}.$$

REFERENCES

1. K. W. Gruenberg, Resolutions by Relations, London Math. Soc. J., vol. 35 (1960), pp. 481-494.

2. J. P. Serre, Corps Locaux, Paris, 1962.

McGill University

https://doi.org/10.4153/CMB-1965-055-2 Published online by Cambridge University Press