ON ASSOCIATIVE COMPOSITIONS IN FINITE NILPOTENT GROUPS

NAGAYOSI IWAHORI and AKIRA HATTORI

Let

(1) $$f(X, Y) = X^{m_1} Y^{n_1} \ldots X^{m_r} Y^{n_r}$$

be a word in two variables X, Y, i.e. an element in the free group F_2 on two generators X, Y. Let us say that f defines an associative composition for a group G if for arbitrary elements a, b, c in G we have

(2) $$(a \circ b) \circ c = a \circ (b \circ c)$$

where $a \circ b$ is defined by

(3) $$a \circ b = f(a, b).$$

Now Mr. M. Kuranishi raised the following problem: when f defines an associative composition for every group G?

We shall solve this problem in this note (Proposition 1), and determine moreover associative compositions holding for all finite nilpotent groups using a theorem of Prof. K. Iwasawa[1] (Proposition 2). This result will be refined by Proposition 3.

PROPOSITION 1. *In order that $f(X, Y)$ define an associative composition for a free group F_2 on two generators, it is necessary and sufficient that f is one of the following five types:*

(4) $$1, X, Y, XY, YX.$$

Proof. An element $t \neq 1$ of a free group generated by x and y can be expressed uniquely in the form $z_1^{e_1} \ldots z_k^{e_k}$, where every z_i is either x or y, where $z_i \neq z_{i+1}$ and where e's are non-vanishing integers. k is called the length of t, and is denoted by $l(t)$ (set $l(1) = 0$). Then one will easily verify

(5) $$l(t^f) \geqq l(t), \qquad (f \neq 0),$$

Received March 17, 1954.

https://doi.org/10.1017/S0027763000018134 Published online by Cambridge University Press

for any word t.

Now, let (3) be an associative composition in F_2, defined by f in (1) such that $n_1 \neq 0, \ldots, m_r \neq 0$. From the associativity

$$(a \circ e) \circ e = a \circ (e \circ e), \qquad (a \neq e),$$

we deduce at once that

$$\sum m_i = 1 \quad \text{or} \quad = 0;$$

similarly we have

$$\sum n_i = 1 \quad \text{or} \quad = 0.$$

Now, we may assume $m_1 \neq 0$, since a new composition $a * b = b \circ a$ is associative at the same time as $a \circ b$, and then we have only to prove $r = 1$. Suppose $r \geqq 2$, and compare two expressions

$$(a \circ b) \circ c = (a \circ b)^{m_1} c^{n_1} \ldots,$$

$$a \circ (b \circ c) = \begin{cases} a^{m_1} b^{m_1} c^{n_1} \ldots, & \text{if} \quad n_1 > 0, \\ a^{m_1} c^{-n_r} b^{-m_r} c^{-n_{r-1}} \ldots, & \text{if} \quad n_1 < 0, \end{cases}$$

for $a, b, c \in F$. If we take a, b, c satisfying no non-trivial relation among themselves (e.g. x^2, xy, y^2 if F_2 is generated by x and y), it follows that the length of $(a \circ b)^{m_1}$, as an element of the free group generated by a and b, is at most 2. But this is the case only if the length of $a \circ b$ itself is at most 2 by (5), contradicting the assumption $r \geqq 2$. Hence we must have $r = 1$. q.e.d

Proposition 2. *If $f(X, Y)$ defines an associative composition for every finite nilpotent group generated by two elements, then $f(X, Y)$ is one of the following five types:*

$$1, X, Y, XY, YX.$$

Proof. Let F_2 be a free group on two generators x, y. By a theorem of K. Iwasawa[1] the intersection of all normal subgroups N in F_2 such that F_2/N is a finite nilpotent group coincides with the identity group:

(6) $$\bigcap N = \{1\}.$$

Now, since $f(X, Y) = X \circ Y$ defines an associative composition for F_2/N, we

[1] K. Iwasawa, Einige Sätze über freie Gruppen, Proc. Imp. Acad. Japan, **19** (1943), pp. 272–274.

have for every element z_1, z_2, z_3 in F_2

$$(z_1 \circ z_2) \circ z_3 \equiv z_1 \circ (z_2 \circ z_3) \pmod{N}$$

Hence we have by (6)

$$(z_1 \circ z_2) \circ z_3 = z_1 \circ (z_2 \circ z_3).$$

Thus the proposition follows from Proposition 1.

Now we can refine Proposition 2 as follows:

PROPOSITION 3. *Let $p > 0$ be a given prime integer. If $f(X, Y)$ defines an associative composition for every finite p-group generated by two elements, then, $f(X, Y)$ is one of the following five types*

$$1,\ X,\ Y,\ XY,\ YX.$$

Proof. It is sufficient to show that the intersection of all normal subgroups M in F (a free group on two generators) such that F/M is a finite p-group coincides with the identity group:

(7) $$\bigcap M = \{1\}.$$

This fact can be proved quite similarly as in K. Iwasawa[1] and we shall show only the corresponding lemma and theorem.

Let G be an arbitrary finitely generated group and

$$G = Z_1 \supset Z_2 \supset \ldots$$

be the descending central series of G, i.e. Z_{i+1} be the subgroup of G generated by $(g, z_i) = gz_ig^{-1}z_i^{-1}$ $(g \in G,\ z_i \in Z_i)$:

$$Z_{i+1} = (G, Z_i) \qquad (i = 1, 2, \ldots)$$

Then, as is seen easily,[2] Z_i/Z_{i+1} is a finitely generated abelian group and the torsion of Z_i/Z_{i+1} (i.e. the subgroup formed by all elements in Z_i/Z_{i+1} which are of finite order) is a finite group.

Now let us call a finitely generated group G to be *of p-type* if every torsion of Z_i/Z_{i+1} is a finite p-group. $(i = 1, 2, \ldots)$

Then an analogy of "Satz 1" in K. Iwasawa[1] is given by

2) Note that Z_i/Z_{i+1} is a central subgroup of G/Z_{i+1}. Then for every a, b in G, c, d in Z_{i-1} we have $(ab, cd) \equiv (a, c) \cdot (a, d) \cdot (b, c) \cdot (b, d)$ (mod. Z_{i+1}) (cf. H. Zassenhaus, Lehrbuch der Gruppentheorie, S. 57). The assertion is then completed by induction on i.

THEOREM. *Let G be a finitely generated nilpotent group of p-type. Then the intersection of all normal subgroups M in G such that G/M is a finite p-group coincides with the identity group:*

$$\bigcap M = \{1\}.$$

This theoren can be proved quite similarly as in K. Iwasawa, l. c. using the following lemma which is a direct corollary of his "Hilfssatz."

LEMMA. *Let G be an arbitrary group and let N be a normal subgroup with finitely many generators $a_1, \ldots, a_r$ such that (G, N) is a central, finite subgroup in G of order $l = p^\nu$. Then the subgroup M of G generated by finitely many elements $a_1^l, \ldots, a_r^l$ and (G, N) is a central subgroup of G and the factor group N/M is a finite p-group.*

Now in order to prove (7) it is sufficient to show that $F/F^{(n)}$ is a group of p-type, where $F = F^{(1)}$, $F^{(i+1)} = (F, F^{(i)})$ $(i = 1, 2, \ldots)$. However, as is well-known, $F^{(i)}/F^{(i+1)}$ is a free abelian group[3] (with finitely many generators). Hence $F/F^{(n)}$ is of p-type $(n = 1, 2, \ldots)$. Thus Proposition 3 is proved.

[3] Cf. E. Witt, Treue Darstellung Liescher Ringe, Crelle 177, (1937).