COMPOSITIO MATHEMATICA

PAUL M. WEICHSEL

On Engel-like congruences

Compositio Mathematica, tome 29, nº 1 (1974), p. 67-73

<http://www.numdam.org/item?id=CM_1974__29_1_67_0>

COMPOSITIO MATHEMATICA, Vol. 29, Fasc. 1, 1974, pag. 67–73
Noordhoff International Publishing
Printed in the Netherlands

ON ENGEL-LIKE CONGRUENCES

Paul M. Weichsel

1. Introduction

In this note we investigate the commutator-subgroup structure of groups that satisfy congruences and laws that are similar to Engel laws. We begin with the necessary notation. If G is a group and α a positive integer, then $(G)^{\alpha}$ is the subgroup generated by $\{g^{\alpha}|g \in G\}$. A *left-normed commutator* $(x_1, \cdots, x_n)$ of weight n on $x_1, \cdots, x_n$ is defined inductively for $n \geqq 2$ by $(x_1, x_2) = x_1^{-1}x_2^{-1}x_1x_2$ and $(x_1, \cdots, x_n) = ((x_1, \cdots, x_{n-1}), x_n)$. The rth term of the *lower central series* of a group G, denoted by G_r is the subgroup of G generated by commutators of the form $(x_1, \cdots, x_r)$, all $x_i \in G$, $G_1 = G$. The terms of the derived series are defined by $G^{(0)} = G$, $G^{(1)} = G_2$ and $G^{(l)} = (G^{(l-1)})_2$. A group G is called *metabelian* if $G^{(2)} = 1$. If $A_1, \cdots, A_s$ are normal subgroups of G, $s \geqq 2$, then $(A_1, \cdots, A_s)$ is the subgroup of G generated by $\{(a_1, \cdots, a_s)|a_i \in A_i,\ i = 1, \cdots, s\}$. If $w = (x_{\alpha_1}, \cdots, x_{\alpha_r})$ with $x_{\alpha_i} \in \{x_1, \cdots, x_{\alpha}\}$, then $w(G)$ is the subgroup generated by $\{(g_{\alpha_1}, \cdots, g_{\alpha_r})|g_{\alpha_i} \in G, i = 1, \cdots, r\}$ (α_i may be equal to α_j for some pairs i, j, $i \neq j$). If G is a group, then $\operatorname{var} G$ is the variety generated by G, i.e., the intersection of all varieties containing G.

DEFINITION: Let $w(x_1, \cdots, x_n)$ be a left-normed commutator of weight d on $x_1, \cdots, x_n$. The group G is said to satisfy the *w-congruence* if $w(g_1, \cdots, g_n) \in G_{d+1}$ for all $g_i \in G$, $i = 1, \cdots, n$. G is said to satisfy the *strong w-congruence* if $w(g_1, \cdots, g_n) \in A_{d+1}$, with A the subgroup generated by $\{g_1, \cdots, g_n\}$ for each set $\{g_1, \cdots, g_n\}$ and corresponding subgroup A. w is said to be a law of G if $w(G) = 1$. An important example of a w-*congruence* is the *Engel congruence*: $w = (x, y, y, \cdots, y)$.

The main theorem of this note (2.5) shows that in a group which satisfies a w-congruence the descending central series and the derived series are linked in a special way. Two consequences are derived. The first (3.3) states that a p-group G satisfying a strong w-congruence, w of weight $d < p$ is nilpotent of class at most $(d-1)^{l-1}$ if it is solvable of derived length at most l. The second (4.1) characterizes those finite p-groups of class $c < p$, satisfying the c-weight Engel law.

The proof of the main theorem depends on the observation that a result of Gupta and Newman [1. Theorem] on metabelian groups can be modified to apply to a much larger class of groups.

2. The main theorem

We begin by quoting a weakened version of the theorem of Gupta and Newman.

PROPOSITION: *Let w be a left-normed commutator of weight d. If G is metabelian and $w(G) = 1$, then*

$(G_{d+1})^{\alpha} = 1$ *with α an integer whose prime divisors are less than d, and*

$(G_d/G_{d+1})^{\beta} = 1$ *with β an integer whose prime divisors are less than $d+1$.*

The proof of this theorem depends on a number of properties of commutators in metabelian groups. They are:

(i) $(b, a_1, \cdots, a_t) = (b, a_{\sigma 1}, \cdots, a_{\sigma t})$ for $b \in G_2$, $a_1, \cdots, a_t \in G$ and σ an arbitrary permutation on the set $\{1, \cdots, t\}$.

(ii) $(b^i, a) = (b, a)^i$ for every integer i, whenever $b \in G_2$, and $a \in G$.

On the other hand, once the weight of w is given, then the only commutators which actually occur in the proof are those of weight d or greater. Thus if the weight of w is d, and G is any group, then the theorem will hold for the group $\bar{G} = G/\bigcup_{r,s}(G_r, G_s)$, $r+s = d$ and $r, s \geqq 2$.

We first verify that properties (i) and (ii) hold in the group $\bar{G}$.

2.1 LEMMA: *If G is any group and $i, j \geqq 2$, than*

$$(G_i, G_j, \underbrace{G, \cdots, G}_{k}) \subseteq \bigcup_{r,s} (G_r, G_s),$$

$r+s = i+j+k$, and $r, s \geqq 2$.

PROOF: Induction on k. If $k = 1$, then the lemma follows from the 3-subgroup-lemma of P. Hall, [3. Theorem 3.4.7], since

$$(G_i, G_j, G) \subseteq (G_j, G, G_i)(G, G_i, G_j) = (G_{j+1}, G_i)(G_{i+1}, G_j).$$

We now recall that if $A, B, C \Delta G$, then

$$(AB, C) \subseteq (A, C)(B, C).$$

Hence $(\bigcup_{r,s}(G_r, G_s), G) \subseteq \bigcup_{r,s}(G_r, G_s, G) \subseteq \bigcup_{u,v}(G_u, G_v)$ with $r+s=n$, $r, s \geqq 2$ and $u+v = n+1$, $u, v \geqq 2$, and the lemma follows by induction.

2.2 LEMMA: *Let $a \in G_d$, $d \geqq 2$ and $b, c \in G$. Then $(a, b, c) \in (a, c, b)(G_d, G_2)$.*

PROOF: The proof is identical to the usual one for metabelian groups.

2.3 LEMMA: *Let $a_i \in G$, $i = 1, \cdots, n$ and $b \in G_m$, $m \geqq 2$. Then* $(b, a_1, a_2, a_3, \cdots, a_n) \in (b, a_2, a_1, a_3, \cdots, a_n) \bigcup_{r,s}(G_r, G_s)$, $r+s = n+m$, $r, s \geqq 2$.

PROOF

Case I. Let $n = 2$. Then $(b, a_1, a_2) \in (b, a_2, a_1)(G_m, G_2)$ by (2.2).

Case II. Let $n > 2$ and induct on n. Thus assume the lemma for n and consider $(b, a_1, a_2, a_3, \cdots, a_{n+1})$. By induction $(b, a_1, a_2, a_3, \cdots, a_n) = (b, a_2, a_1, a_3, \cdots, a_n)c$, with $c \in \bigcup_{r,s}(G_r, G_s)$, $r+s = n+m$, $r, s \geqq 2$. Hence $(b, a_1, a_2, a_3, \cdots, a_{n+1}) = ((b, a_2, a_1, a_3, \cdots, a_n)c, a_{n+1}) = (b, a_2, a_3, \cdots, a_n, a_{n+1})ef$, with $e \in (G_{n+m+1}, G_2)$ and $f \in (G_{n+m}, G_2)$, both subgroups of $\bigcup_{r,s}(G_r, G_s)$, $r+s = n+m+1$, $r, s \geqq 2$. This completes the proof.

It now follows easily that property (i) holds in the group

$$\bar{G} = G/\bigcup_{r,s}(G_r, G_s), \qquad r+s = n, \qquad r, s \geqq 2$$

for commutators of total weight greater than or equal to n.

2.4 LEMMA: *Let $b \in G_t$ and $a \in G$. Then for all integers i,*

$$(b^i, a) \in (b, a)^i \bigcup_{r,s}(G_r, G_s), \qquad r+s = 2t+1, \qquad r, s \geqq 2.$$

PROOF: If $i = -1$, then $(b^{-1}, a) \in (b, a)^{-1}(G_r, G_s)$, for $r+s = 2t+1$. We now induct on i for $i \geqq 1$. If $i = 1$, the result is trivial. If $(b^n, a) \in (b, a)^n \bigcup_{r,s}(G_r, G_s)$, $r+s = 2t+1$, $r, s \geqq 2$, then $(b^{n+1}, a) = (b^n, a)(b^n, a, b) \times (b, a)$ and so $(b^{n+1}, a) \in (b, a)^n (b, a) \bigcup_{r,s}(G_r, G_s) = (b, a)^{n+1} \bigcup_{r,s}(G_r, G_s)$, $r+s = 2t+1$, $r, s \geqq 2$.

We will now state the main theorem in two different forms.

2.5 THEOREM: *Let w be a left-normed commutator of weight d and G a group satisfying the w-congruence. Then*

$$(G_d)^\alpha \subseteq \bigcup_{r,s}(G_r, G_s)G_{d+1},$$

with $r+s = d$, $r, s \geqq 2$ and α an integer whose prime divisors are less than $d+1$. Furthermore, if $(G_d)^q = G_d$, for every prime $q < d+1$, then

$$G_d = \bigcup_{r,s}(G_r, G_s)G_t \qquad r, s \text{ as above}$$

and t every integer greater than or equal to $d+1$.

PROOF: *Let* $\bar{G} = G/\bigcup_{r,s}(G_r, G_s)$, $r+s = d$, $r, s \geqq 2$. Then commutators of weight d in $\bar{G}$ satisfy conditions (i) and (ii) needed in the proof of the Gupta-Newman Theorem. Now let $\bar{\bar{G}} = \bar{G}/w(\bar{G})$ and since $w(\bar{\bar{G}}) = 1$, we conclude that $(\bar{\bar{G}}_d)^\alpha = 1$ with α as described in the hypothesis. That is, $(G_d)^\alpha \subseteq \bigcup_{r,s}(G_r, G_s)G_{d+1}$, $r+s = d$, $r, s \geqq 2$.

Now if $(G_d)^q = G_d$ for every prime $q < d+1$ we get

$$G_d = \bigcup_{r,s} (G_r, G_s)G_{d+1}$$

since $\bigcup_{r,s}(G_r, G_s)G_{d+1} \subseteq G_d$. But this relation remains true if d is replaced by $d+1$ since

$$G_{d+1} = (G_d, G) = (\bigcup_{r,s} (G_r, G_s)G_{d+1}, G) \subseteq \bigcup_{r,s} (G_r, G_s, G)G_{d+2} \subseteq$$
$$\bigcup_{a,b} (G_a, G_b)G_{d+2} \subseteq G_{d+1}, \qquad r+s = d, \quad a+b = d+a, \quad r, s, a, b \geqq 2.$$

Thus

$$G_{d+1} = \bigcup_{a,b} (G_a, G_b)G_{d+2}, \qquad a+b = d+1, \quad a, b \geqq 2.$$

Hence

$$G_d = \bigcup_{r,s} (G_r, G_s) \bigcup_{a,b} (G_a, G_b)G_{d+2} = \bigcup_{r,s} (G_r, G_s)G_{d+2},$$

$r+s = d$, $a+b = d+1$, $r, s, a, b \geqq 2$, and the conclusion follows by induction.

2.6 Theorem: *Let w be a left-normed commutator of weight d and G a group satisfying $w(G) = 1$. Then $(G_d)^\alpha \subseteq \bigcup_{r,s}(G_r, G_s)$, $r+s = d$, $r, s \geqq 2$ and α an integer whose prime divisors are less than $d+1$.*

Furthermore if $(G_d)^q = G_d$, for every prime $q < d+1$, then

$$G_d = \bigcup_{r,s} (G_r, G_s), \qquad r+s = d, \quad r, s \geqq 2.$$

Proof: Since $w(G) = 1$, $w(\bar{G}) = 1$ with $\bar{G} = G/\bigcup_{r,s}(G_r, G_s)$ $r+s = d$, $r, s \geqq 2$. Now applying the conclusions of the Gupta-Newman theorem we get that $(\bar{G}_{d+1})^\gamma = 1$ and $(\bar{G}_d/\bar{G}_{d+1})^\beta = 1$ with β, γ integers whose prime divisors are less than $d+1$. Therefore $(G_{d+1})^\gamma \subseteq \bigcup(G_r, G_s)$, $r+s = d$, $r, s \geqq 2$, and $(\bar{G}_d)^\beta \subseteq \bar{G}_{d+1}$. Thus $(G_d)^{\beta\gamma} \subseteq (G_{d+1})^\gamma \subseteq \bigcup_{r,s}(G_r, G_s)$, $r+s = d$, $r, s \geqq 2$ and $\beta\gamma$ satisfies the requirements of α in the theorem.

Now if $(G_d)^q = (G_d)$ for all primes $q < d+1$, we get $G_d = \bigcup_{r,s}(G_r, G_s)$, $r+s = d$, $r, s \geqq 2$.

3. p-groups satisfying a small congruence

We say that a p-group G satisfies a small congruence if $w(G) \subseteq G_{d+1}$ with w a left-normed commutator of weight $d < p$. In this section we will show that a p-group satisfying a small strong congruence is nilpotent if it is solvable and derive a bound on its nilpotency class in terms of its derived length.

3.1. LEMMA: *Let G be a group in which the relation $G_d = \bigcup_{r,s}(G_r, G_s)$, $r+s = d$, $r, s \geqq 2$ holds for some fixed $d \geqq 4$. Then*

$$G_{r(d-1)+1} = \bigcup_{a_i} (G_{a_1}, \cdots, G_{a_{r+1}}), \qquad \sum_{i=1}^{r+1} a_i = r(d-1)+1,$$

$a_i \geqq 2$ all i.

PROOF: Induction on r. If $r = 1$, the conclusion is the hypothesis. Suppose that

$$G_{r(d-1)+1} = \bigcup_{a_i} (G_{a_1}, \cdots, G_{a_{r+1}}), \qquad \sum_{i=1}^{r+1} a_i = r(d-1)+1,$$

$a_i \geqq 2$ all i. Then

$$G_{(r+1)(d-1)+1} = (G_{r(d-1)+1}, \underbrace{G, \cdots, G}_{d-1}) = (\bigcup_{a_i} (G_{a_1}, \cdots, G_{a_{r+1}}),$$

$$\underbrace{G, \cdots, G}_{d-1}) \subseteq \bigcup_{b_i} (G_{b_1}, \cdots, G_{b_{r+1}}) \subseteq G_{(r+1)(d-1)+1},$$

$$\sum_{i=1}^{r+1} a_i = r(d-1)+1, \qquad \sum_{i=1}^{r+1} b_i = \sum_{i=1}^{r+1} a_i + (d-1),$$

$a_i, b_i \geqq 2$ all i by 2.1. Hence we have $G_{(r+1)(d-1)+1} = \bigcup_{b_i}(G_{b_1}, \cdots, G_{b_{r+1}})$ and the lemma follows by induction.

3.2 LEMMA: *Let G be a group in which the relation $H_d = \bigcup_{r,s}(H_r, H_s)$, $r+s = d$, $r, s \geqq 2$, d a fixed integer, $d \geqq 4$ holds for all subgroups H of G. Then*

$$H_{(d-1)^l+1} \subseteq H^{(l+1)}.$$

PROOF: If $l = 1$, then $(d-1)^l+1 = d$ and by hypothesis

$$H_d = \bigcup_{r,s} (H_r, H_s) \subseteq H^{(2)}, \qquad r+s = d, \quad r, s \geqq 2.$$

Now suppose that $H_{(d-1)^l+1} \subseteq H^{(l+1)}$. Then by replacing H by H', we get $(H')_{(d-1)^l+1} \subseteq H^{(l+2)}$. But according to 3.1

$$H_{(d-1)^{(l+1)}+1} = H_{(d-1)^l(d-1)+1} = \bigcup_{a_\iota} (H_{a_1}, \cdots, H_{a_{(d-1)^l+1}}) \subseteq$$
$$\subseteq (H')_{(d-1)^l+1} \subseteq H^{(l+2)}$$

since $a_j \geqq 2$ and $H_{a_j} \subseteq H'$. Hence $H_{(d-1)^{l+1}+1} \subseteq H^{(l+2)}$ which proves the lemma.

3.3 THEOREM: *Let w be a left-normed commutator of weight d, and let G be a p-group with $d < p$. If G satisfies the strong w-congruence and G is solvable of derived length l, then G is nilpotent of class at most $(d-1)^{l-1}$.*

PROOF: We may assume without loss of generality that G is finitely generated and therefore finite. Thus G is nilpotent and we must derive a bound for the nilpotency of G independent of the number of its generators. Since $d < p$ and G is a p-group it follows from 2.5 that every subgroup H of G satisfies

$$H_d = \bigcup_{r,s} (H_r, H_s), \qquad r+s = d, \qquad r, s \geqq 2.$$

Thus by 3.2, $G_{(d-1)^l+1} \subseteq G^{(l+1)}$, and since G is solvable of length l, H is nilpotent of class at most $(d-1)^{l-1}$. This completes the proof.

REMARK: The version of the Gupta-Newman theorem that we have used is a relatively crude version of the original. In particular, the prime divisor properties of the integers α and β are determined not only by the weight of the commutator w but by the multiplicities of the variables which occur in w. In fact, if we know that w involves at least 3 variables, then the bound $d < p$ in the theorem above can be improved to $d \leqq p$. A particularly interesting case of this occurs when G is solvable of derived length l and has exponent p. For then G satisfies the strong $(p-1)$-Engel congruence and Gupta has shown [2. Theorem 7.18] that G is nilpotent of class at most $(p-1)^{l-1} + \cdots + (p-1) + 1$.

If on the other hand G is a solvable-of-length-l p-group satisfying the strong w-congruence with w of weight p and involving at least 3 variables, then the class of G is at most $(p-1)^{l-1}$.

4. Nilpotent p-groups

In this section we will characterize those nilpotent p-groups of class $c < p$ which satisfy the Engel law of weight c.

4.1 THEOREM: *Let G be a nilpotent p-group of class $c < p$ and let*

$$w = (x, \underbrace{y, \cdots, y}_{c-1}).$$

Then G satisfies the law $w = 1$ if and only if $H_c = \bigcup_{r,s} (H_r, H_s)$, $r+s = c$, $r, s \geqq 2$ for all groups $H \in \operatorname{var} G$.

PROOF: Suppose $w(G) = 1$ with

$$w = (x, \underbrace{y, \cdots, y}_{c-1}).$$

Then by 2.6) $G_c = \bigcup_{r,s}(G_r, G_s)$, $r+s = c$, $r, s \geqq 2$.

Thus since G satisfies the law $w = 1$, every group $H \in \operatorname{var} G$ satisfies it and the theorem follows in one direction.

Now suppose that $H_c = \bigcup_{r,s}(H_r, H_s)$, $r+s \geqq c, r, s \geqq 2$ for all $H \in \operatorname{var} G$. It follows that this relation holds for the relatively free groups in $\operatorname{var} G$. Thus every group in $\operatorname{var} G$ satisfies a law: $(x_1, \cdots, x_c) = \prod d_j^{\gamma_j}$ with each d_j an element of (F_r, F_s), F the relatively free group generated by $\{x_1, \cdots, x_c, \cdots\}$. Furthermore we may assume that each factor on the right involves each of the variables $x_1, \cdots, x_c$. Now we set $x = x_1$ and $y = x_2 = \cdots = x_c$ on both sides of the equation. Thus

$$(*) \qquad w = (x, \underbrace{y, \cdots, y}_{c-1}) = \prod_j d_j^{\gamma_j}$$

We now utilize a standard argument based on the facts that each commutator of weight c is a bilinear form and that each non-trivial factor on the right involves at least 2 occurrences of x. Let l be a primitive root of p and replace x by x^l in (*). Then we get

$$w^l = \prod d_j^{\gamma_j l^{r(j)}}$$

where d_j has $r(j)$ occurrences of x. Then raising both sides of (*) to the power $-l$ and multiplying we get

$$(**) \qquad 1 = \prod d_j^{\gamma_j (l^{r(j)} - l)}.$$

We continue this process with (**) thereby eliminating those factors of (**) containing the minimum number of occurrences of x. In this way we eventually get a law of the form

$$1 = (\prod d_j^{\gamma_j})^m$$

in which each factor contains the same number of occurrences of x and y, and with m an integer relatively prime to p. Now working backwards we can conclude that

$$w = (x, \underbrace{y, \cdots, y}_{c-1}) = 1.$$

Thus G satisfies the law $w = 1$.

REFERENCES

[1] N. D. Gupta and M. F. Newman: On metabelian groups. *J. Australian Math. Soc. VI* (1966) 362–368.

[2] D. J. S. Robinson: *Finiteness Conditions and Generalized Soluble Groups, Part 2.* Springer, Berlin, Heidelberg, New York 1972.

[3] W. R. Scott: *Group Theory.* Prentice-Hall, Engelwood Cliffs, N. J. (1964).

(Oblatum 16–XI–1973)

University of Illinois
at Urbana-Champaign