NOTES ON A PAPER BY SANOV. II

RUTH REBEKKA STRUIK

1. **Introduction.** In this paper another proof is given of some results obtained by Sanov (see [3]).

Let $F=\{u, v\}$ be a free group generated by u and v. Let

$$(x, y) = x^{-1}y^{-1}xy$$

for $x, y \in F$. If S, T are subgroups of F, let

$$(S, T) = \{(s, t) \mid s \in S, t \in T\}.$$

Let

$$F(k) = \{x^k \mid x \in F\}; \qquad F_1 = F; \qquad F_k = (F_{k-1}, F).$$

Let $(u, v, 0)=u$, $(u, v, 1)=(u, v)$, $(u, v, n)=((u, v, n-1), v)$. Then Sanov [3] proved that

$$(1.1) \qquad (u, v, \alpha p^\alpha - 1)^{p^{\beta-\alpha}} \in F(p^\beta)F_{\alpha p^\alpha+1}, \qquad \beta, \alpha = 1, 2, \cdots$$

where p is a prime.

In this paper, (1.1) is proved for the cases $\alpha=1, 2$; β arbitrary. A slight generalization of these results is also proved. Sanov's proof involved an investigation of ideals in a Lie Ring. In this paper, Hall's Collection Process will be used. The method also yields other formulas, e.g.

$$(1.2) \qquad (u, v, p^2 - 1)^{p^{\beta-1}} \in F_{2p^2-p}F(p^\beta),$$

$$(1.3) \qquad (u, v, p^{\alpha+1} - 1)^{p^{\beta-1}} \in F_{2p^{\alpha+1}-p^\alpha}F(p^\beta), \qquad \alpha = 1, 2, \cdots$$

and can be used to produce numerous formulas of a similar nature. The author hopes that some of these formulas and/or the method may be of use in solving other group-theoretic problems. The author was unable to use the method to prove (1.1) for $\alpha=3$.

Note that for $\alpha=\beta=1$, (1.1) becomes

$$(1.4) \qquad (u, v, p - 1) \in F(p)F_{p+1}.$$

(1.4) plays an important role in the theory of the Restricted Burnside Problem.

2. **Preliminary results.** Throughout this paper, p will stand for a prime, and α, β for non-negative integers.

Presented to the Society, September 1, 1960; received by the editors August 22, 1960.

By elementary arguments, the following two lemmas and corollary can be proved:

LEMMA 2.1.

$$C_{p^\beta,p^\alpha} = p^{\beta-\alpha}(1 + sp) \tag{2.1}$$

where s is a positive integer. ($C_{n,r}$ *as usual, is the number of combinations of n things taken r at a time.*)

LEMMA 2.2. $p^{\beta-\alpha} \mid C_{p^\beta,s}$ *if* $p^\alpha \leqq s < p^{\alpha+1}$ *where s is a positive integer.*

($a \mid b$ as usual, means a divides b.)

COROLLARY 2.2. *If* $s \not\equiv 0 \pmod{p}$, *and* $p^\alpha < s < p^{\alpha+1}$, *then* $p^{\beta-\alpha+1} \mid C_{p^\beta,s}$.

LEMMA 2.3. *Let x_i, x, $i=1, 2, \cdots, n$ be $n+1$ elements of a group. Then*

$$(\prod x_i, x) = \prod (x_i, x) U \tag{2.2}$$

where U is a product of commutators, each of which contains at least 2 of the x_i and at least one x.

PROOF. Use induction on n and the well-known formula

$$\begin{aligned}(x_1x_2, x) &= (x_1, x)((x_1, x), x_2)(x_2, x)\\ &= (x_1, x)(x_2, x)((x_1, x), x_2)(((x_1, x), x_2), (x_2, x)).\end{aligned}$$

(See e.g. (10.2.1.2) in [1, p. 150].)

LEMMA 2.4 (HALL COLLECTION FORMULA). *Let u, v be any elements of a nilpotent group F. Let p be a prime, α any positive integer. Then*

$$(vu)^{p^\alpha} = v^{p^\alpha} u^{p^\alpha} \prod v_i^{f_i} \tag{2.3}$$

where v_i is a basic commutator in u and v (see [1, p. 178]), *and*

$$f_i = a_1C_{p^\alpha,1} + a_2C_{p^\alpha,2} + \cdots + a_{j(i)}C_{p^\alpha,j(i)} \tag{2.4}$$

where $a_1, a_2, \cdots, a_{j(i)}$ are non-negative integers and if $v_i \in F_{s_i}$, then $j(i) \leqq s_i$. In particular, if

$$v_i = (u, v, n) \tag{2.5}$$

then

$$f_i = C_{p^\alpha,n+1}. \tag{2.6}$$

PROOF. See [1, pp. 178–182, 326].

LEMMA 2.5. *Let $a, b \in F$, F a nilpotent group. Let r, s be positive integers. Then*

$$(2.7) \qquad (b^s, a^r) = (b, a)^{rs} \prod x_i^{C_{r,\lambda} C_{s,\mu}}$$

where the x_i are basic commutators in b and a. If x_i contains m_i a's and n_i b's, then $\lambda \leqq m_i$ and $\mu \leqq n_i$. (The exponent of x_i will in general be of the form

$$\sum n_{\lambda\mu} C_{r,\lambda} C_{s,\mu}, \ n_{\lambda\mu} \textit{ non-negative integers.})$$

PROOF. The proof is essentially the same as that given for (2.3) (this paper) [**1**, pp. 178–182]. Details are given in [**5**].

COROLLARY 2.5. *Let b, a be as in Lemma* 2.5.

$$(2.8) \qquad (b^{p^\alpha}, a) = (b, a)^{p^\alpha} \prod x_i^{C_{p^\alpha, s_{ij}}}$$

where if x_i is a commutator with m_i b's then $s_{ij} \leqq m_i$. Each x_i contains at least 2 b's.

DEFINITION. (u, v, n) for $n \geqq 1$ is a *regular* commutator in u and v. If u_1 and u_2 are regular commutators, so is (u_1, u_2).

COMMENT. $((u, v), (u, v, v))$ is a regular commutator which is not a basic commutator.

LEMMA 2.6. *Let F be a nilpotent group. Let w be a regular commutator in u and v. Let $w \in F_s$, $kp \leqq s < (k+1)p$. Then either w contains $(k+1)$ u's or*

$$(2.9) \qquad w^{p^{\beta-1}} = \prod v_i^{p^{\beta-1}} \prod w_i^{p^{\beta-2}} \cdots \prod x_i^{p^{\beta-t}} \cdots \pmod{F(p^\beta)}$$

where

v_i, w_i, x_i are regular commutators;

$v_i \in F_s$ and contains at least $(k+1)$ u's;

$w_i \in F_{s+(p^2-p)}$ and contains at least as many u's as w does;

$x_i \in F_{s+(p^t-p)}$ and contains at least as many u's as w does.

It may be that the $v_i^{p^{\beta-1}}$, $w_i^{p^{\beta-2}}$, $\cdots$, $x_i^{p^{\beta-t}}$ $\cdots$ are scattered among each other.

PROOF. Applying Lemmas 2.1, 2.2, Corollary 2.2 to Lemma 2.4 and to equation (2.3), one obtains

$$(2.10) \qquad \begin{aligned} &(u, v, p-1)^{p^{\beta-1}} \\ &\qquad = \prod v_i^{p^{\beta-1}} \prod w_i^{p^{\beta-2}} \cdots \prod x_i^{p^{\beta-t}} \cdots \pmod{F(p^\beta)} \end{aligned}$$

where v_i, w_i, x_i are regular commutators; $v_i \in F_p$ and contains at least $2u$'s unless it is of the form $(u, v, np-1)$ $n>1$; $w_i \in F_{p^2}$, $x_i \in F_{p^t}$.

Replace u by $(u, v, (n-1)p)$ on each side of (2.10). This gives

$$(2.11) \qquad (u, v, np-1)^{p^{\beta-1}} = \prod y_i^{p^{\beta-1}} \prod z_i^{p^{\beta-2}} \cdots \prod u_i^{p^{\beta-t}} \cdots \pmod{F(p^\beta)}$$

where $y_i \in F_{np}$ and contains $2u$'s unless it is of the form

$$(u, v, mp-1) \;\; m > n; \;\; z_i \in F_{p^2+np}, \;\; u_i \in F_{p^t+np};$$

y_i, z_i, u_i are regular commutators and may be scattered among each other. Replace the right hand side of (2.11) wherever $(u, v, np-1)^{p^{\beta-1}}$ appears on the right hand side of (2.10). Repeat as often as needed until Lemma 2.6 is proved for $s=p$ and $k=1$. This gives

$$(2.12) \qquad (u, v, p-1)^{p^{\beta-1}} = \prod v_i^{p^{\beta-1}} \prod w_i^{p^{\beta-2}} \cdots \prod x_i^{p^{\beta-t}} \cdots \pmod{F(p^\beta)}$$

where

v_i, w_i, x_i are regular commutators in u and v;
$v_i \in F_p$ and contains at least 2 u's;
$w_i \in F_{p^2}$, $x_i \in F_{p^t}$.

Note that the v_i, w_i, x_i of (2.12) are different from those of (2.10). Using the same letters to designate different commutators will be done frequently in the subsequent argument to maintain uniformity of notation.

Replace u by (u, v, n) on both sides of (2.12). This proves (2.9) for $k=1$, $s=p, p+1, \cdots, 2p-1$. Assume true for $s<r$. Then if $w \in F_r$, $kp \leqq r \leqq (k+1)p$ and does not contain $(k+1)$ u's, then one of its components is (u, v, n), $n \geqq p-1$. Then if $w=(b, a)$, where a, b are regular commutators, and b contains (u, v, n),

$$(2.13) \qquad (b, a)^{p^{\beta-1}} = (b^{p^{\beta-1}}, a) \prod y_i^{C_{p^{\beta-1}, s_{ij}}} \pmod{F(p^\beta)}$$

where (2.8) has been used with α replaced by $\beta-1$, y_i regular commutators. Using induction (on $(b^{p^{\beta-1}}, a)$), Lemma 2.3 and Corollary 2.5 repeatedly, one can eventually put $w^{p^{\beta-1}}$ into the desired form.

COMMENT. If we replace u by (u, v, n) on both sides of (2.12) we obtain

$$(2.14) \qquad (u, v, p-1+n)^{p^{\beta-1}} = \prod v_i^{p^{\beta-1}} \prod w_i^{p^{\beta-2}} \cdots \prod x_i^{p^{\beta-t}} \cdots \pmod{F(p^\beta)}$$

where v_i, w_i, x_i, are regular commutators (but not the same v_i, w_i, x_i as in (2.12)), $v_i \in F_{p+2n}$ and contains at least two u's, $w_i \in F_{p^2+n}$, $x_i \in F_{p^t+n}$.

Let $p+2n=p^2+n$, then $n=p^2-p$. This gives

$$(2.15)\quad (u, v, p^2 - 1)^{p^{\beta-1}} = \prod w_i^{p^{\beta-2}} \cdots \prod x_i^{p^{\beta-t}} \cdots \pmod{F(p^\beta)}$$

where w_i, x_i are regular commutators, $w_i \in F_{2p^2-p}$, $x_i \in F_{p^t+p^2-p}$ which proves (1.2) and is a slight generalization of (1.2).

3. Theorems.

THEOREM 3.1.

$$(3.1)\qquad (u, v, p - 1)^{p^{\beta-1}} \in F(p^\beta)F_{p+1}.$$

PROOF. The proof for the case $\beta = 1$ given in [1, p. 327] goes through, mutatis mutandis, replacing p^β by p. Equation (2.10) of this paper plays the role of (18.4.9) in [1, p. 327].

If one uses (2.12), the above proof for (3.1), the fact that any commutator can be written as a product of basic (or regular commutators), and Lemma 2.4, and the device used in going from (2.10) to (2.12), one obtains,

$$(3.2)\qquad \begin{aligned}&(u, v, p - 1)^{p^{\beta-1}}\\ &\quad = \prod v_i^{p^{\beta-1}} \prod w_i^{p^{\beta-2}} \cdots \prod x_i^{p^{\beta-t}} \cdots \pmod{F(p^\beta)}\end{aligned}$$

where $v_i \in F_{p+1}$ and contains at least 2 u's, $w_i \in F_{p^2}$, $x_i \in F_{p^t}$; v_i, w_i, x_i regular commutators. (The v_i, w_i, x_i may be scattered among each other.)

(3.2) is a slight generalization of (3.1).

THEOREM 3.2.

$$(3.3)\qquad (u, v\ \ 2p^2 - 1)^{p^{\beta-2}} \in F(p^\beta)F_{2p^2+1}.$$

PROOF. From Lemma 2.4, and using Lemmas 2.1, 2.2 and Corollary 2.2, one obtains

$$(3.4)\qquad \begin{aligned}&(u, v, p^2 - 1)^{p^{\beta-2}}\\ &\quad = \prod v_i^{p^{\beta-1}} \prod w_i^{p^{\beta-2}} \cdots \prod x_i^{p^{\beta-t}} \cdots \pmod{F(p^\beta)}\end{aligned}$$

where v_i, w_i, x_i are regular commutators, $v_i \in F_p$, $x_i \in F_{p^t}$, $w_i \in F_{p^2}$, and if $w_i \notin F_{p^2+1}$ it contains at least 2 u's; v_i contains at least 2 u's unless it is of the form $(u, v, np - 1)$, $n \geqq 1$. Replace u by $(u, v, p^2 - p)$ on both sides of (3.4):

$$(3.5)\qquad \begin{aligned}&(u, v, 2p^2 - p - 1)^{p^{\beta-2}}\\ &\quad = \prod v_i^{p^{\beta-1}} \prod w_i^{p^{\beta-2}} \cdots \prod x_i^{p^{\beta-t}} \cdots \pmod{F(p^\beta)}\end{aligned}$$

v_i, w_i, x_i are regular commutators, $v_i \in F_{p^2}$, $w_i \in F_{2p^2-p}$; if $w_i \notin F_{2p^2-p+1}$ it contains at least 2 u's, $x_i \in F_{p^t+(p^2-p)}$.

Using Lemma 2.4 with $\alpha=\beta+1$, one obtains

$$(3.6)\qquad (u, v, p^2 - 1)^{p^{\beta-1}} = \prod v_i^{p^{\beta-1}} \prod w_i^{p^{\beta-2}} \cdots \pmod{F(p^\beta)}$$

where v_i, w_i are basic commutators, $v_i \in F_{p^2}$ and if $v_i \neq (u, v, p^2 - np - 1)$, it contains at least 2 u's, $w_i \in F_{p^3}$. Use the same device that obtained (2.12) from (2.10): this means that one can assume in (3.6) that all v_i contain at least two u's. Replace u by (u, v, n) on both sides of (3.6):

$$(3.7)\qquad (u, v, p^2 - 1 + n)^{p^{\beta-1}} = \prod v_i^{p^{\beta-1}} \prod w_i^{p^{\beta-2}} \cdots \pmod{F(p^\beta)}$$

where $v_i \in F_{p^2+2n}$, $w_i \in F_{p^3+n}$; v_i, w_i are regular commutators and may be scattered among each other.

Put the right hand side of (3.7) wherever $(u, v, p^2-1+n)^{p^{\beta-1}}$ appears on the right hand side of (3.5). This means one can assume that all v_i contain at least two u's. Now apply Lemma 2.6 with $k=p$. This means one can assume each v_i contains at least $(p+1)$ u's. Replace u by (u, v, p) on both sides of (3.5). This gives

$$(3.8)\qquad (u, v, 2p^2 - 1)^{p^{\beta-2}} = \prod w_i^{p^{\beta-2}} \cdots \prod x_i^{p^{\beta-t}} \cdots \pmod{F(p^\beta)},$$

where w_i, x_i are regular commutators, $w_i \in F_{2p^2+1}$, $x_i \in F_{p^t+p^2}$. This is sufficient to prove (3.3). Note that by using the same device used in going from (2.10) to (2.12), one can assume that each w_i of (3.8) contains at least two u's. (3.8) is a slight generalization of Theorem 3.2.

Starting with (3.6) and using the same device used in going from (2.12) to (2.14) to (2.15), one obtains

$$(3.9)\qquad \begin{aligned} &(u, v, p^3 - 1)^{p^{\beta-1}} \\ &\qquad = \prod v_i^{p^{\beta-2}} \prod w_i^{p^{\beta-3}} \cdots \prod x_i^{p^{\beta-t}} \cdots \pmod{F(p^\beta)} \end{aligned}$$

where v_i, w_i, x_i are regular commutators (which may be scattered among each other), $v_i \in F_{2p^3-p^2}$, $w_i \in F_{p^4+(p^3-p^2)}$, $x_i \in F_{p^t+(p^3-p^2)}$ which gives (1.3), for $\alpha=2$. (1.3) can be proved similarly.

Bibliography

1. M. Hall, Jr., *The theory of groups*, New York, Macmillan, 1959.
2. O. Ore, *Number theory and its history*, New York, McGraw-Hill, 1948.
3. I. N. Sanov, *On a certain system of relations in periodic groups with period a power of a prime number*, Izv. Akad. Nauk SSSR. Ser. Mat. vol. 15 (1951) pp. 477–502.
4. R. R. Struik, *Notes on a paper by Sanov*, Proc. Amer. Math. Soc. vol. 8 (1957) pp. 638–641.
5. ———, *On nilpotent products of cyclic groups*. II, Canad. J. Math., to appear.

University of British Columbia