

A NOTE ON A THEOREM BY WITT¹

ROBERT M. THRALL

1. Introduction. Let F denote the free group with n generators and let F^c be the c th member of the lower central series² of F . Witt³ has shown that $Q^c = F^c/F^{c+1}$ is a free abelian group with $\psi_c(n) = (1/c)\sum \mu(c/d)n^d$ generators (the summation is over all divisors d of c and μ is the Möbius μ -function).

The set of k th powers in F generates a normal subgroup H_k . Let $F_k = F/H_k$ and $G_{k,c} = F_k/F_k^{c+1}$. We shall call F_k the *free k -group* and $G_{k,c}$ the *free k -group of class c* . It is a consequence of Witt's result that F_k^c/F_k^{c+1} , the central of $G_{k,c}$, is abelian and has at most $\psi_c(n)$ generators. In this note we show that if p is a prime greater than c , and $q = p^\alpha$, then the central of $G_{q,c}$ is of order q^N where $N = \psi_c(n)$. If the prime divisors of k are all greater than c , an analogous result holds for the central of $G_{k,c}$ as a consequence of Burnside's theorem that a nilpotent group is the direct product of its Sylow subgroups.

Let M_c denote the space of tensors of rank c over the $GF[p]$. A homomorphic mapping of M_c upon the central of $G_{p,c}$ is set up and enables one to apply the theory of decompositions of tensor space under the full linear group mod p , to determine all characteristic subgroups of $G_{p,c}$ which lie in its central. This theory is applied to determine all the characteristic subgroups of $G_{p,c}$ for $c < 5$ and a multiplication table is constructed for $G_{p,3}$.

2. Commutator calculus.⁴ Let s_1, s_2, \dots be operators in any group G and set $s_{12} = (s_1, s_2) = s_1^{-1}s_2^{-1}s_1s_2$ and $s_{12\dots k} = (s_{12}\dots s_{k-1}, s_k)$. $s_{12\dots k}$ is called a *simple commutator of weight k* in the components s_1, \dots, s_k . The group G^k generated by the simple commutators of weight k for all choices of s_1, \dots, s_k in G is called the k th member of the *lower central series* of G . If $s \in G^k$ but $s \notin G^{k+1}$, then s is said to have *weight k* in G .

For all s_1, s_2, s_3 in G we have

$$(1) \quad (s_1s_2, s_3) = s_{13}s_{132}s_{23}, \quad (s_1, s_2s_3) = s_{13}s_{12}s_{123}.$$

Let the weight of s_i be α_i and set $\alpha = \alpha_1 + \dots + \alpha_k + 1$. The following relations are then true:

¹ Presented to the Society, April 13, 1940.

² For definition see §2 below or [4, p. 49].

³ [7, p. 153].

⁴ The relations in this section are either taken directly from Hall, Magnus, or Witt or are immediate consequences of their theorems. See [4, 6 and 7].

$$(2) \quad s_{123\dots k}s_{213\dots k} \equiv I \pmod{G^\alpha},$$

$$(3) \quad s_{123\dots k}s_{231\dots k}s_{312\dots k} \equiv I \pmod{G^\alpha},$$

$$(4) \quad (s_1^{a_1}, s_2^{a_2}, \dots, s_k^{a_k}) \equiv (s_{12\dots k})^{a_1 a_2 \dots a_k} \pmod{G^\alpha}.$$

If now $\alpha - 1 = km$, $m = \text{minimum } (\alpha_1, \dots, \alpha_k)$ and $\rho_\beta = \prod_{\delta=1}^{\delta=n} s_\delta^{\alpha_\beta \delta}$, $\beta = 1, \dots, k$, it follows that

$$(5) \quad \rho_{12\dots k} \equiv \prod_{\beta=1}^n (s_{\beta_1\dots\beta_k})^{a_{\beta_1} \dots a_{\beta_k}} \pmod{G^\alpha}.$$

3. The groups F_q . Let F be the free group generated by s_1, \dots, s_n , and denote by \overline{H}_k the smallest normal subgroup containing the k th powers of all simple commutators of s_1, \dots, s_n .

LEMMA I. *Let $q = p^\alpha$, p any prime. Then $s^q \in \overline{H}_q \cup F^p$ for any element $s \in F$.*

PROOF BY INDUCTION. The lemma is trivial for s of weight greater than $p - 1$. Suppose the lemma true for all weight greater than c and let s be of weight c . By the definition of weight, s can be written in the form $s = t_1 \dots t_m v_0$ where v_0 has weight greater than c and the t_i are of weight c and are all simple commutators in s_1, \dots, s_n . Then by the fundamental expansion formula⁵ for $(PQ \dots)^x$ we have

$$s^q = t_1^q \dots t_m^q v_0^q v_1^q \dots v_j^q w$$

where $w \in F^p$ and the v_β are all of weight greater than c . By definition $t_\beta^q \in \overline{H}_q$ and by our induction hypothesis $v_\beta^q \in \overline{H}_q \cup F^p$ and so $s^q \in \overline{H}_q \cup F^p$.

COROLLARY I. *Let s have weight c , for $c < p$. Then $s^q \in \overline{H}_q \cup F^{c+1}$.*

Set $H_{q,c} = H_q \cap F^c$ and $\overline{H}_{q,c} = \overline{H}_q \cap F^c$. Then we have

COROLLARY II. *For $c < p$, $H_{q,c} \cup F^{c+1} = \overline{H}_{q,c} \cup F^{c+1}$.*

LEMMA II. $F_q^c / F_q^{c+1} \simeq F^c / (F^{c+1} \cup H_{q,c})$.

We note first that applying the second homomorphism theorem⁶ to Hall's formula⁷ $F_q^c = (F^c \cup H_q) / H_q$ we obtain the result $F_q^c = F^c / H_{q,c}$ (for all c). Now

⁵ See [4, formula 3.51] or [6, p. 111].

⁶ See [2, p. 32].

⁷ See [4, formula 2.491] or [2, p. 119].

$$\begin{aligned}
 F^c / (F^{c+1} \cup H_{q,c}) &\simeq (F^c / H_{q,c}) / ([F^{c+1} \cup H_{q,c}] / H_{q,c}) \\
 &\simeq F_q^c / (F^{c+1} / [H_{q,c} \cap F^{c+1}]) = F_q^c / F_q^{c+1},
 \end{aligned}$$

since $H_{q,c} \cap F^{c+1} = H_{q,c+1}$.

Set $Q_q^c = F_q^c / F_q^{c+1}$.

THEOREM I. For $c < p$, Q_q^c is abelian of order q^N , $N = \psi_c(n)$.

DEFINITION. t_1, \dots, t_k is said to be a basis for $F^c \bmod F^{c+1}$, if any operator t of weight c can be written uniquely in the form $t = \prod t_i^{d_i} \theta$ where $\theta \in F^{c+1}$.

Evidently such a basis exists, and by Witt's theorem⁸ $k = N$; and we may choose the t_i as simple commutators in the generators s_1, \dots, s_n . Let ρ_i be the image in Q_q^c of t_i . Then since the t_i are a basis for $F^c \bmod F^{c+1}$, any operator $\rho \in Q$ can be written in the form $\rho = \prod \rho_i^{d_i}$ where $0 \leq d_i < q$. Hence the order of Q_q^c is at most q^N for any c . If the order of Q_q^c is less than q^N there exists a relation $\prod \rho_i^{d_i} = I$ where, say, $d_j \neq 0$.

If now $p > c$, this relation together with Corollary II and Lemma II imply that $\prod t_i^{d_i} \in H_{q,c} \cup F^{c+1}$, or $\prod t_i^{d_i} \equiv \prod t_i^{q e_i} \bmod F^{c+1}$. Since the t_i are a basis for $F^c \bmod F^{c+1}$ this requires $d_i - q e_i = 0, i = 1, \dots, N$, which contradicts the assumption that d_j and, therefore, $d_j - q e_j$ is not divisible by q . Hence there can be no relation between the ρ_i and the theorem is proved.

COROLLARY III. For $p > c$, $G_{q,c}^j$ is of order q^m ,

$$m = \psi_j(n) + \dots + \psi_c(n), \quad j = 1, \dots, c.$$

4. Characteristic subgroups of $G = G_{p,c}$. A large variety of characteristic subgroups of G can be obtained from the lower central series by sequences of joins, intersections, and commutations. In G the upper and lower central series are identical; in particular, the central C ($= C_{p,c}$) of G is G^p . The central quotient group of G is $G_{p,c-1}$, and any characteristic subgroup H of G is mapped into a characteristic subgroup $H' = H \cup C / C$ in $G_{p,c-1}$.

We say that K is a *minimal characteristic subgroup* (m.c.s.) of G if no proper subgroup of K is characteristic in G . For $G = G_{p,c}$, every m.c.s. lies in the central. Indeed any normal subgroup of G must contain commutators of weight c and therefore must have an intersection not equal to I with C . We turn now to the determination of all characteristic subgroups of G which lie in C .

⁸ See [7, Theorems 3 and 4, pp. 152-153].

Let \bar{A} be any automorphism of G , and H any characteristic subgroup of G . \bar{A} induces an automorphism $\bar{A}(H)$ on G/H and an automorphism $\bar{A}[H]$ on H . If in particular H is G^2 , the commutator subgroup of G , then G/H is the abelian group of order p^n and type $1, 1, 1, \dots$. Let the generators of G be s_1, \dots, s_n , and let t_i be the image in G/G^2 of s_i . Then $\bar{A}(H)$ takes the form $t_i \rightarrow t'_i$ where

$$t'_i = \prod t_j^{a_{ij}}, \quad a_{ij} \in GF[p], \quad |a_{ij}| \neq 0.$$

Hence \bar{A} itself must be of the form $s_i \rightarrow s'_i$ where

$$s'_i = \prod s_j^{a_{ij}} r_i, \quad r_i \in G^2.$$

To calculate $\bar{A}[C]$ we apply (5) with $k=c$. Since $G^{c+1} = I$, (5) is now an equality and shows that $\bar{A}[C]$ is independent of the r_i . Indeed if we set $A = (a_{ij})$ we see that the formal commutators $s_{i_1} \dots s_{i_c}$ transform like tensors of rank c , that is, according to $A \times A \times \dots \times A$ (Kronecker direct product with c factors).

Denote by M_c the whole space of tensors of rank c . It has dimension n^c . The group $A_c = \{A \times A \times \dots \times A\}$ (c factors) is homomorphic to the group $\{A\}$ of linear transformations, and hence M_c is a representation space for $\{A\}$. Brauer⁹ has proved the following theorem concerning the decompositions of this representation:

THEOREM II. *If K is a field of characteristic $p \neq 0$, the representation A_c is completely reducible for $c < p$, and it splits into irreducible parts in exactly the same way as in the case of characteristic zero.*

The mapping $x_{i_1} \dots x_{i_c} \rightarrow s_{i_1} \dots s_{i_c}$ (where of course products in C are replaced by sums in M_c) establishes a homomorphic mapping of M_c upon C and this mapping is preserved under the group A_c , that is, C is also a representation space for the group A_c . Let \bar{C} denote C written additively. Then $\bar{C} = M_c - W_c$, where W_c contains all tensors whose image in C is identity. We call W_c the *space of commutator relations*, W_c is evidently an invariant subspace of M_c under the tensor group and by Theorem I it has dimension $n^c - \psi_c(n)$ if $p > c$. Because of the complete reducibility of the representation A_c we can write $M_c = W_c + P_c$ where P_c is likewise an invariant subspace of M_c , and furthermore the decomposition into irreducibly invariant subspaces of P_c under A_c will be the same as that of C under the group of automorphisms of G . (P_c is not uniquely determined by W_c but its decompositions are.) Let R_1, \dots, R_t be irreducibly invariant sub-

⁹ See [3, p. 867].

spaces of M_c whose direct sum is P_c , and let T_1, \dots, T_t be the corresponding subgroups of C . Then the following theorem expresses the above arguments in group theoretic terms:

THEOREM III. *Any minimal characteristic subgroup is isomorphic to one of T_1, \dots, T_t and any characteristic subgroup K of G which lies in the central is the direct product of the minimal characteristic subgroups which it contains. ($p > c$ is assumed throughout.)*

The number of characteristic subgroups in G is clearly independent of the number n of generators provided that $n \geq c$. Hence to obtain all characteristic subgroups of the set of groups $G_{p,c}$ with $p > c$ we need only consider those with $n = c$.

5. The groups $G_{p,3}$ and $G_{p,4}$. In this section we shall make use of the decomposition into irreducibly invariant subspaces of the tensor spaces M_3 and M_4 . These can be readily obtained by a direct computation based upon the decomposition theorems of M_c in general.¹⁰ We suppose $n = 3$ in M_3 and $n = 4$ in M_4 .

$M_3 = \sum_1 + \sum_{2,1} + \sum_{2,2} + \sum_3$ in which the summands have dimensions 10, 8, 8 and 1 respectively. $W_3 = \sum_1 + \sum_{2,1} + \sum_3$ and hence $G_{p,3}$ has just one m.c.s., its central.

$$M_4 = \sum_1 + \sum_{2,1} + \sum_{2,2} + \sum_{2,3} + \sum_{3,1} + \sum_{3,2} \\ + \sum_{4,1} + \sum_{4,2} + \sum_{4,3} + \sum_5$$

in which the summands have dimensions 35, 45, 45, 45, 20, 20, 15, 15, 15, and 1 respectively. $W_4 = \sum_1 + \sum_{2,1} + \sum_{2,2} + \sum_{3,1} + \sum_{3,2} + \sum_{4,1} + \sum_{4,2} + \sum_5$ and hence $G_{p,4}$ has two m.c.s., one of which is its second derived group. Let us denote these by D and E .

$G_{p,1}$ has no proper characteristic subgroups and the only proper characteristic subgroup of $G_{p,2}$ is its central $G_{p,2}^2$.

THEOREM IV. *The only characteristic subgroups of $G_{p,3}$ are the members of its lower central series.*

Let H be characteristic in $G_{p,3}$. Then if $H \neq I$ or C , by Theorem III $H \supset C$. $H' = H/C$ must then be $G_{p,2}$ or its central. In the first case $H = G_{p,3}$ and in the second case $H = G_{p,3}^2$.

THEOREM V. *The only characteristic subgroups of $G_{p,4}$ are D , E and the members of the lower central series.*

It is easy to see that if a characteristic subgroup $H \supset C$ then H is in

¹⁰ See for instance [1, Theorem 4.4D, p. 129].

the lower central series. To complete the proof we show then that if $H \triangleright C$, $H = D$ or E . Since $H \triangleright C$, either $H' = I$; in which case $H \subset C$ and therefore $H = D$ or E ; or $H' \supset G_{p,3}^3$ (by Theorem IV). It remains now only to show that $H' \supset G_{p,3}^3$ implies $H \supset C$. If now $H' \supset G_{p,3}^3$, then $H \cup C \supset G_{p,4}^3$ and hence for the commutator s_{123} of weight 3 we have a factorization $s_{123} = hd$ where $h \in H$ and $d \in C$ (and so d has weight not less than 4). Since H is normal $(h, s_4) = (s_{123} \cdot d^{-1}, s_4) = s_{1234} \in H$. But the conjugates of s_{1234} generate C so that $H \supset C$ contrary to hypothesis, and the theorem is proved.

For the sake of completeness we give a multiplication table for $G_{p,3}$. Applying the formulas of §2 and Theorem I we have for any operator s of $G_{p,3}$ a unique expression in the form

$$s = s^A = \prod s_i^{a_i} \prod_{i < j} s_{ij}^{a_{ij}} \prod_{i \neq j} s_{iji}^{a_{ijj}} \prod_{i < j < k} s_{ijk}^{a_{ijk}} s_{jki}^{a_{jki}} .$$

If now $s^C = s^A s^B$, then applying the readily verified formula $(s_1^\alpha, s_2^\beta) = s_{12}^{\alpha\beta} s_{121}^{\beta C_{\alpha,2}} s_{122}^{\alpha C_{\beta,2}}$ we obtain¹¹ ($i < j < k$)

$$\begin{aligned} c_i &= a_i + b_i, & c_{ij} &= a_{ij} + b_{ij} - b_i a_j, \\ c_{iji} &= a_{iji} + b_{iji} - b_i C_{aj,2} + b_j a_{ij} - b_i b_j a_j, \\ (6) \quad c_{jii} &= a_{jii} + b_{jii} + a_j C_{bj,2} - b_i a_{ij}, \\ c_{ijk} &= a_{ijk} + b_{ijk} + b_j a_{ik} + b_k a_{ij} - b_i a_j a_k - b_i b_j a_k - b_i b_k a_j, \\ c_{jki} &= a_{jki} + b_{jki} + b_i a_{jk} + b_j a_{ik} - b_i b_j a_k. \end{aligned}$$

BIBLIOGRAPHY

1. H. Weyl, *The Classical Groups*, Princeton University Press, 1939.
2. H. Zassenhaus, *Lehrbuch der Gruppentheorie*, Hamburger Mathematische Einzelschriften, vol. 21, 1937.
3. R. Brauer, *Algebras connected with semi-simple groups*, Annals of Mathematics, vol. 38 (1937), pp. 857-872.
4. P. Hall, *Groups of prime power order*, Proceedings of the London Mathematical Society, vol. 36 (1934), pp. 29-95.
5. Levi and van der Waerden, *Über eine besondere Klasse von Gruppen*, Abhandlungen aus dem mathematischen Seminar der Hamburgischen Universität, vol. 9 (1933), pp. 154-158.
6. W. Magnus, *Über Beziehungen zwischen höheren Kommutatoren*, Journal für die reine und angewandte Mathematik, vol. 177 (1937), pp. 105-115.
7. E. Witt, *Treue Darstellung Liescher Ringe*, Journal für die reine und angewandte Mathematik, vol. 177 (1937), pp. 152-160.

UNIVERSITY OF MICHIGAN

¹¹ For $p=3$, $s_{iji} = s_{jii} = I$ and $s_{ijk} = s_{jki}$ so that (6) reduces to formula 9 of Levi and van der Waerden [5, p. 156].