PAPERS

PUBLISHED IN THE

PROCEEDINGS OF THE LONDON MATHEMATICAL SOCIETY

# ON SUB-GROUPS OF A FINITE ABELIAN GROUP

*By* HAROLD HILTON.

[Received October 7th, 1906.—Read November 8th, 1906.]

1. Let $H$ be a sub-group of order $p^r$ in a finite Abelian group $G$ whose order is $p^a$ ($p$ prime). Let $t_1$ of the invariants of $H$ be 1, $t_2$ be 2, ..., $t_m$ be $m$. Let $u_1$ of the invariants of $G$ be 1, $u_2$ be 2, ..., $u_m$ be $m$. The quantities $t_1, t_2, t_3, \ldots, u_1, u_2, u_3, \ldots$ are zeros or positive integers ($u_m > 0$).

Then $\qquad a = u_1+2u_2+3u_3+\ldots, \qquad r = t_1+2t_2+3t_3+\ldots;$

let $\qquad u = u_1+u_2+u_3+\ldots, \qquad t = t_1+t_2+t_3+\ldots.$

We first find the number ($X$) of ways in which a base $[g_1, g_2, g_3, \ldots]$ can be chosen for a sub-group of $G$ of the same type as $H$.

Let $[h_1, h_2, h_3, \ldots]$ be a base of $G$. Then $G$ contains $(p^{u_m}-1)p^{a-u_m}$ elements of order $p^m$; namely, $h_1^{\beta_1} h_2^{\beta_2} h_3^{\beta_3} \ldots$, where at least one of $\beta_1, \beta_2, \ldots, \beta_{u_m}$ is prime to $p$.* Therefore $g_1$ can be chosen in $(p^{u_m}-1)p^{a-u_m}$ ways.

When $g_1$ is chosen $[g_1, h_2, h_3, \ldots]$ may be taken as a base of $G$. Then $G$ contains $(p-1)p^{a-u_m}$ elements of order $p^m$ whose $p^{m-1}$-th powers are in $\{g_1\}$; namely, $g_1^{\beta_1} h_2^{\beta_2} h_3^{\beta_3} \ldots$, where $\beta_2, \beta_3, \ldots, \beta_{u_m}$ are multiples of $p$, $\beta_1$ is prime to $p$, and $\beta_{u_m+1}, \beta_{u_m+2}, \ldots$ are any integers. Therefore $G$ contains

$$[(p^{u_m}-1)-(p-1)]p^{a-u_m} = (p^{u_m-1}-1)p^{1+a-u_m}$$

* See Netto's *Algebra*, Vol. II., p. 246.

elements of order $p^m$ whose $p^{m-1}$-th powers are not in $\{g_1\}$; *i.e.*, $g_2$ may be chosen in $(p^{u_m}-1)\,p^{1+a-u_m}$ ways when $g_1$ is given.

Again, when $g_1$ and $g_2$ are chosen $[g_1, g_2, h_3, h_4, \ldots]$ may be taken as a base of $G$. Then $G$ contains $(p^2-1)\,p^{a-u_m}$ elements of order $p^m$ whose $p^{m-1}$-th powers are in $\{g_1, g_2\}$; namely, $g_1^{\beta_1} g_2^{\beta_2} h_3^{\beta_3} h_4^{\beta_4} \ldots$, where $\beta_3, \beta_4, \ldots, \beta_{u_m}$ are multiples of $p$, $\beta_1$ or $\beta_2$ is prime to $p$, and $\beta_{u_m+1}, \beta_{u_m+2}, \ldots$ are any integers. Therefore $G$ contains

$$[(p^{u_m}-1)-(p^2-1)]\,p^{a-u_m} = (p^{u_m-2}-1)\,p^{2+a-u_m}$$

elements of order $p^m$ whose $p^{m-1}$-th powers are not in $\{g_1, g_2\}$; *i.e.*, $g_3$ may be chosen in $(p^{u_m-2}-1)\,p^{2+a-u_m}$ ways when $g_1$ and $g_2$ are given.

This reasoning may be continued to show that the first $t_m$ generators of the base may be chosen in $\dfrac{f(u_m)}{f(u_m-t_m)}\,p^{t_m(a-u_m)+\frac{1}{2}t_m(t_m-1)}$ ways; where $f(k)$ denotes $(p^k-1)(p^{k-1}-1)\ldots(p^2-1)(p-1)$ and $f(0)=1$.

Now, when $[h_1, h_2, h_3, \ldots]$ is a base of $G$ every element of order $p^{m-1}$ in $G$ is contained in the group whose base is

$$[h_1^p, h_2^p, \ldots, h_{u_m}^p, h_{u_m+1}, h_{u_m+2}, \ldots],$$

and conversely. Hence, by reasoning precisely similar to that used above, $G$ contains $(p^{u_m+u_{m-1}}-1)\,p^{a-u_{m-1}-2u_m}$ elements of order $p^{m-1}$, and the $p^{m-2}$-th powers of $(p^{t_m}-1)\,p^{a-u_{m-1}-2u_m}$ of these elements are in $\{g_1, g_2, \ldots, g_{t_m}\}$. Hence, as before, $g_{t_m+1}$ can be chosen in

$$(p^{u_m+u_{m-1}-t_m}-1)\,p^{t_m+a-u_{m-1}-2u_m}$$

ways when $g_1, g_2, \ldots, g_{t_m}$ are given.

Proceeding as before, we see that $g_{t_m+2}$ can be chosen in

$$(p^{u_m+u_{m-1}-t_m-1}-1)\,p^{1+t_m+a-u_{m-1}-2u_m}$$

ways when $g_1, g_2, \ldots, g_{t_m+1}$ are given. Thus we show that the first $t_m+t_{m-1}$ generators of the base may be chosen in

$$\frac{f(u_m)}{f(u_m-t_m)}\,\frac{f(u_m+u_{m-1}-t_m)}{f(u_m+u_{m-1}-t_m-t_{m-1})}$$
$$\times\,p^{t_m(a-u_m)+t_{m-1}(a-u_{m-1}-2u_m)+\frac{1}{2}[t_1(t_1-1)+t_2(t_2-1)]+t_m t_{m-1}}$$

ways.

Proceeding in this way, we get

$$X = \frac{f(u_m)}{f(u_m-t_m)}\,\frac{f(u_m+u_{m-1}-t_m)}{f(u_m+u_{m-1}-t_m-t_{m-1})}$$
$$\times\,\frac{f(u_m+u_{m-1}+u_{m-2}-t_m-t_{m-1})}{f(u_m+u_{m-1}+u_{m-2}-t_m-t_{m-1}-t_{m-2})}\ \ldots\ p^c$$

$$[c = \tfrac{1}{2}t(t-1)+u_1(t-t_1)+u_2(2t-t_2-2t_1)+u_3(3t-t_3-2t_2-3t_1)+\ldots].$$

To find the number ($Y$) of distinct bases of any sub-group of $G$ of the same type as $H$ we put $u_1 = t_1$, $u_2 = t_2$, $u_3 = t_3$, ... in $X$. The total number ($N$) of sub-groups of $G$ of the same type as $H$ is then

$$\frac{X}{Y} = \frac{f(u_m)}{f(t_m)\,f(u_m-t_m)}\,\frac{f(u_m+u_{m-1}-t_m)}{f(t_{m-1})\,f(u_m+u_{m-1}-t_m-t_{m-1})}$$
$$\times\frac{f(u_m+u_{m-1}+u_{m-2}-t_m-t_{m-1})}{f(t_{m-2})\,f(u_m+u_{m-1}+u_{m-2}-t_m-t_{m-1}-t_{m-2})}\,\dots\,p^d$$

$$[d = (u_1-t_1)(t-t_1)+(u_2-t_2)(2t-t_2-2t_1)+(u_3-t_3)(3t-t_3-2t_2-3t_1)+\dots].$$

The above reasoning shows that the necessary and sufficient conditions for the existence of sub-groups such as $H$ are

$$u_m+u_{m-1}+\dots+u_{m-q+1} \geqslant t_m+t_{m-1}+\dots+t_{m-q+1} \quad (q = 1, 2, \dots, m);$$

*i.e.*, the $k$-th invariant of $H$ is not greater than the $k$-th invariant of $G$ ($k = 1, 2, 3, \dots$).*

2. To find the total number ($M$) of sub-groups of order $p^r$ in $G$, we have only to find every set of values of $t_1$, $t_2$, $t_3$, ... satisfying the relations

$$u_m+u_{m-1}+\dots+u_{m-q+1} \geqslant t_m+t_{m-1}+\dots+t_{m-q+1}$$

and $$r = t_1+2t_2+3t_3+\dots.$$

Then $M$ is the sum of the corresponding values of $N$. A general formula giving $M$ for every value of $r$ would probably be somewhat complicated. We can, however, find the simple expression $\frac{f(u+r-1)}{f(r)\,f(u-1)}$ for $M$ when $r \leqslant$ the smallest invariant of $G$. In this case

$$u_m = u, \qquad u_{m-1} = u_{m-2} = u_{m-3} = \dots = 0$$

for every sub-group considered, while

$$N = \frac{f(u)}{f(u-t)\,f(t_1)\,f(t_2)\dots}\,p^d$$

$$[d = u(r-t)-rt+t_1^2+(t_2+2t_1)\,t_2+(t_3+2t_2+3t_1)\,t_3+\dots].$$

We have to prove $$\frac{f(u+r-1)}{f(r)\,f(u-1)} = \Sigma(N),$$

the sum being taken for all positive integral or zero values of $t_1$, $t_2$, $t_3$, ...

---

* In the notation of Burnside's *Theory of Groups*, § 47, $n_t \leqslant m_t$. Since the above was written Prof. Burnside has informed me that this corrected form of his result was communicated to him by Prof. E. H. Moore, of Chicago, in 1899.

such that $$t = t_1+t_2+t_3+\ldots \leqslant u, \qquad t_1+2t_2+3t_3+\ldots = r.$$

This is obviously true when $u = 1$. We assume it true for all values of $u$ less than the one considered, and use induction to prove the theorem true in general.

Now $\dfrac{f(u+r-1)}{f(r)f(u-1)}$

$$= \text{the coefficient of } x^r \text{ in } p^{-\frac{1}{2}r(r+1)}(1+px)(1+p^2x)\ldots(1+p^{u+r-1}x),$$

*i.e.*, in

$$p^{-\frac{1}{2}r(r+1)}(1+px)(1+p^2x)\ldots(1+p^u x)(1+p\,.\,p^u x)(1+p^2\,.\,p^u x)\ldots(1+p^{r-1}\,.\,p^u x)$$

$$= p^{-\frac{1}{2}r(r+1)}\sum_t p^{\frac{1}{2}t(t+1)}\frac{f(u)}{f(t)\,f(u-t)}\,p^{(r-t)u+\frac{1}{2}(r-t)(r-t+1)}\frac{f(r-1)}{f(r-t)\,f(t-1)}.$$

But, by our assumption,

$$\frac{f(r-1)}{f(r-t)\,f(t-1)} = \sum \frac{f(t)}{f(t-\tau)\,f(\tau_1)\,f(\tau_2)\ldots}\,p^e$$

$$[e = t(r-t-\tau)-(r-t)\,\tau+\tau_1^2+(\tau_2+2\tau_1)\,\tau_2+(\tau_3+2\tau_2+3\tau_1)\,\tau_3+\ldots]$$

for all integral values of $\tau_1, \tau_2, \tau_3, \ldots$ such that

$$\tau = \tau_1+\tau_2+\tau_3+\ldots \leqslant t, \qquad \tau_1+2\tau_2+3\tau_3+\ldots = r-t.$$

But, if we put $t-\tau = t_1$, $\tau_1 = t_2$, $\tau_2 = t_3$, $\tau_3 = t_4$, ..., we have

$$t = t_1+t_2+t_3+\ldots, \qquad t_1+2t_2+3t_3+\ldots = r.$$

Hence $$\frac{f(u+r-1)}{f(r)\,f(u-1)} = \sum \frac{f(u)}{f(u-t)\,f(t_1)\,f(t_2)\ldots}\,p^f$$

$$[f = e+(r-t)\,u+\tfrac{1}{2}\,\{t(t+1)+(r-t)(r-t+1)-r(r+1)\}]$$

for all values of $t_1, t_2, t_3, \ldots$ such that

$$t = t_1+t_2+t_3+\ldots \leqslant u, \qquad t_1+2t_2+3t_3+\ldots = r.$$

We readily verify $f = d$, which completes the proof.

3. We may illustrate the result of § 1 by finding an expression for the number of normal (self-conjugate) sub-groups of index $p^2$ in any group $G$. Let $H_1, H_2, H_3, \ldots$ be these normal sub-groups, and let $D$ be their greatest common sub-group. Since $G/H_1, G/H_2, G/H_3, \ldots$ are Abelian (being of order $p^2$), the commutant of $G$ is contained in $H_1, H_2, H_3, \ldots$, and is therefore contained in $D$. Hence $\Gamma \equiv G/D$ is Abelian. Moreover, the $p^2$-th power of every element of $G$ is in $H_1, H_2, H_3, \ldots$, and is therefore in $D$. Hence the $p^2$-th power of every

element of $\Gamma = 1$. It follows that $\Gamma$ is an Abelian group of the type $(2, 2, 2, \ldots, 1, 1, 1, \ldots)$ [$y$ 2's and $z$ 1's] whose order is a power of $p$.* The number of normal sub-groups of index $p^2$ in $G$ is the same as the number of sub-groups of index $p^2$ in $\Gamma$.

Now, by § 1, $\Gamma$ contains (i.) $\dfrac{f(z)}{f(2)\,f(z-2)}\,p^{2y}$ sub-groups with $y$ invariants 2 and $z-2$ invariants 1; (ii.) $\dfrac{f(y)}{f(2)\,f(y-2)}$ with $y-2$ invariants 2 and $z+2$ invariants 1; (iii.) $\dfrac{f(y)\,f(z+1)}{f(1)\,f(1)\,f(y-1)\,f(z)}\,p^{y-1}$ with $y-1$ invariants 2 and $z$ invariants 1. The factor-group of $\Gamma$ with respect to $\dfrac{f(y)}{f(y-1)\,f(1)}\,p^{y+z-1}$ of the sub-groups (iii.) is cyclic; the factor-group of $\Gamma$ with respect to the remaining $\dfrac{f(y+z)}{f(2)\,f(y+z-2)}$ sub-groups of index $p^2$ is non-cyclic. This is readily proved directly or by considering the reciprocal sub-groups.†

Hence the factor-group of $G$ with respect to $\dfrac{f(y)}{f(y-1)\,f(1)}\,p^{y+z-1}$ normal sub-groups of index $p^2$ is cyclic, and the factor-group with respect to the remaining $\dfrac{f(y+z)}{f(2)\,f(y+z-2)}$ normal sub-groups of index $p^2$ is non-cyclic.

The total number of normal sub-groups of index $p^2$ in $G$ is therefore $\dfrac{(p^{y+z}-1)(p^{y+z-1}-1)}{(p^2-1)(p-1)}+\dfrac{p^y-1}{p-1}\,p^{y+z-1}$, where $y$ and $z$ are zero or positive integers. As an example we may take the group

$$a^{p^{a-1}} = b^p = 1, \qquad ab = ba^{1+p^{a-2}},$$

for which $y = z = 1$.

---

* See M. Bauer, *Nouv. Ann. Math.* [3], Vol. XIX. (1900), p. 508.

† Weber's *Algebra*, Vol. II., p. 56.