A CLASS OF FROBENIUS GROUPS

DANIEL GORENSTEIN

1. Introduction. If a group contains two subgroups A and B such that every element of the group is either in A or can be represented *uniquely* in the form aba', a, a' in A, $b \neq 1$ in B, we shall call the group an *independent* ABA*-group*. In this paper we shall investigate the structure of independent ABA-groups of finite order.

A simple example of such a group is the group G of one-dimensional affine transformations over a finite field K. In fact, if we denote by a the transformation $x' = \omega x$, where ω is a primitive element of K, and by b the transformation $x' = -x + 1$, it is easy to see that G is an independent ABA-group with respect to the cyclic subgroups A, B generated by a and b respectively.

Since G admits a faithful representation on m letters (m = number of elements in K) as a transitive permutation group in which no permutation other than the identity leaves two letters fixed, and in which there is at least one permutation leaving exactly one letter fixed, G is an example of a Frobenius group. In Theorem 1 we shall show that this property is characteristic of independent ABA-groups.

In a Frobenius group on m letters, the set of elements whose order divides m forms a normal subgroup, called the *regular subgroup*. In our example, the regular subgroup M of G consists of the set of translations, and hence is an Abelian group of order $m = p^n$ and of type $(p, p, \ldots, p)$. Our main object will be to give a proof (Theorem 5) that the regular subgroup of an independent ABA-group is always an Abelian group of type $(p, p, \ldots, p)$. We shall call such an Abelian group an *elementary* Abelian group. Throughout the paper all groups will be assumed to be of finite order.

2. Independent ABA-groups as Frobenius groups.

THEOREM 1. *If G is an independent ABA-group, then G is a Frobenius group. If A has order h, B has order k, and the regular subgroup M of G has order m, then $m = h(k-1)+1$.*

Proof. Consider $A \cap xAx^{-1}$ for x in G, and suppose that for some x this intersection contains an element $a \neq 1$. If x is not in A, then by definition of

---

Received November 20, 1957.

A part of this research was done at the 1957 Summer Mathematical Conference at Bowdoin College, under contract to the Electronics Research Directorate, Air Force Cambridge Research Center, Air Research and Development Command, contract number AF 19(604)–2226. A very special case of these results was treated in a joint report of that conference by J. L. Zemmer and the present author.

G, $x = a'ba''$, a', a'' in A, $b \neq 1$ in B; and consequently $(a'ba'')a_1(a'ba'')^{-1} = a$ for some a_1 in A. It follows that $b\bar{a}_1 = \bar{a}b$, where $\bar{a}_1 = a''a_1a''^{-1}$ and $\bar{a} = a'^{-1}aa'$, which contradicts the fact that G is an independent ABA-group.

Hence $A \cap xAx^{-1} \neq 1$ implies x is in A; thus the normalizer of A in G is A itself and the intersection of A with any of its conjugates consists only of the identity element of G. It is well known that these conditions imply that G is a Frobenius group, and furthermore, if M is the regular subgroup of G, that $G = AM$ **(5**, 144**)**.

Thus the order of G is hm. On the other hand, as an independent ABA-group, the order of G is easily computed to be $h^2(k - 1) + h$, whence the equality $m = h(k - 1) + 1$ follows at once.

3. A class of Frobenius groups. Let $G = AM$ be a Frobenius group, its regular subgroup M having order m, and A of order h. Since the automorphism of M induced by conjugation by an element of $A(\neq 1)$ leaves only the identity element of M fixed, it follows that $h|m - 1$, and hence the quantity $k = 1 + (m - 1)/h$ is an integer. In an independent ABA-group this integer k is, by Theorem 1, the order of the subgroup B, and hence k divides the order hm of G.

In this section we shall completely determine the structure of the regular subgroup of a Frobenius group in which the integer k has this additional property.

THEOREM 2. *Let $G = AM$ be a Frobenius group, M its regular subgroup, of order m, A of order h, and set $1 + (m - 1)/h = k$. Then if $k|hm$, M is either a p-group or the direct product of two elementary Abelian groups.*

Proof. Suppose $p|m$, and let S_p be a p-Sylow subgroup of M. If N_p denotes the normalizer of S_p in G, then N_p is itself a Frobenius group, and in fact $N_p = A'N_p'$ where A' is of order h and N_p' is the normalizer of S_p in M **(3**, Lemma 2.5**)**. Thus N_p' is left invariant by the automorphisms of M induced by A'. Since S_p is a characteristic subgroup of N_p', it also is left invariant by these automorphisms. On the other hand, any two subgroups of order h in G are known to be conjugate, so that $A' = xAx^{-1}$ for some x in G. It follows that the p-Sylow subgroup $x^{-1} S_p x$ is left invariant by the automorphisms of M induced by A.

The set of elements H_p of order dividing p which are in the centre of this p-Sylow subgroup themselves form a subgroup of M which is left invariant by A. It is still possible that some proper subgroup of H_p is invariant under the automorphisms induced by A. Let T_p be a minimal such subgroup; T_p is an elementary Abelian group of order p^n, $n \geqslant 1$. Moreover,

3.1 $$h|p^n - 1$$

and *a fortiori* $(h, p) = 1$. Since $T_p \subset M$, we must also have

3.2 $$p^n|m.$$

By definition of k, we also have the equality

3.3 $$m = h(k - 1) + 1.$$

Using 3.1 and 3.2, it follows easily from this relation that

3.4 $$k = \frac{p^n - 1}{h} + 1 + \lambda p^n$$

for some integer $\lambda \geqslant 0$, and hence that

3.5 $$m = p^n(1 + \lambda h).$$

Since $k|hm$, we can write $k = k_1k_2$ where $k_1|h$ and $k_2|m$; and hence using 3.3,

3.6 $$k_1|h, \quad k_2|h - 1.$$

Thus $k = k_1k_2 \leqslant h(h - 1) \leqslant hp^n$, and consequently

3.7 $$\lambda < h.$$

Suppose now that M is not a p-group and hence that there is a prime $q \neq p$ dividing m. As above, M contains a minimal elementary Abelian subgroup T_q of order q^r, $r \geqslant 1$, which is invariant under A. Thus

3.8 $$h|q^r - 1,$$

and as $q^r|m$,

3.9 $$q^r|1 + \lambda h.$$

It follows from 3.8 that $q^r = 1 + \mu h$ for some $\mu \geqslant 1$, whence $1 + \lambda h = \gamma(1 + \mu h)$ for some $\gamma \geqslant 1$, by 3.9. Thus $\gamma \equiv 1 \pmod h$; and hence the assumption $\gamma > 1$ implies $\gamma > h$, whence $1 + \lambda h > 1 + h^2$, contrary to the fact that $\lambda < h$. Hence $\gamma = 1$, $\mu = \lambda$, $q^r = 1 + \lambda h$, and we conclude that

3.10 $$m = p^nq^r.$$

It follows now from Burnside's well-known theorem that M is solvable, and hence by a theorem of Feit **(3)** and Higman **(4)**, M is in fact nilpotent. Thus M is the direct product of the elementary Abelian groups T_p and T_q, and the theorem is proved.

COROLLARY. *Under the hypothesis of Theorem* 2, *G is solvable if A is solvable.*

Proof. $G/M = A$, and, by the theorem, M is solvable.

The structure of M can, however, be determined much more explicitly:

THEOREM 3. *Under the hypothesis of Theorem* 2, *the regular subgroup M of G is either*

I. *An elementary Abelian group,*

II. *An abelian group of order* 16 *and of type* (4, 4), *with* $h = 3$,

https://doi.org/10.4153/CJM-1959-004-5 Published online by Cambridge University Press

III. *The direct product of two elementary Abelian groups whose orders* p^n *and* q^r *are connected by the equalities*

$$2 + p^{\frac{1}{2}n} = q^r = h + 1.$$

Proof. We preserve the notation of Theorem 2.

Case 1. M is a p-group. If $m = p^t$, we must have $t \geqslant n$, since $T_p \subset M$. If $t = n$, $M = T_p$ and there is nothing to prove. Hence we may assume $t > n$.

For suitable integers μ and s, we have

3.11 $$h = 1 + \mu p^s,$$

where $(\mu, p) = 1$ and $s < n$. Since $h|p^t - 1$ and $h|p^n - 1$, $h|p^{t-n} - 1$, and hence

3.12 $$\mu p^s < p^{t-n}.$$

Furthermore, by definition of k, we have

$$k = \frac{p^t - 1}{1 + \mu p^s} + 1 = p^s \frac{p^{t-s} + \mu}{h},$$

whence

3.13 $$k_1 = \frac{p^{t-s} + \mu}{h}, \qquad k_2 = p^s.$$

It follows at once that

3.14 $$(p^{t-s} + \mu)|(p^n - 1)^2.$$

Now $(p^n - 1)^2 = p^{2n-(t-s)}(p^{t-s} + \mu) - (2p^n + \mu p^{2n-(t-s)} - 1)$, and consequently

3.15 $$(p^{t-s} + \mu)|2p^n + \mu p^{2n-(t-s)} - 1.$$

Thus

3.16 $$\mu p^{2n-(t-s)} \geqslant p^{t-s} - 2p^n + \mu + 1.$$

But now, using 3.12 we have $t - s > n$; combining this inequality with the right-hand side of 3.16, yields

3.17 $$\mu p^{2n-(t-s)} \geqslant p^{t-s-1}$$

except when $p = 2$ and $n = t - s - 1$.

Leaving this exceptional case aside for the moment, we see that 3.17 implies $\mu p^s \geqslant p^{2t-2n-s-1} \geqslant p^{t-n}$ since $t - s - n - 1 \geqslant 0$, and this contradicts 3.12.

We have thus proved that either $t = n$ or $p = 2$ and $t = n + s + 1$. Since $h|p^{t-n} - 1$, we have in the latter case $(1 + \mu 2^s)|2^{s+1} - 1$, whence $\mu = 1$, $s = 1$, $h = 3$. But now 3.6 becomes $\frac{1}{3}(2^{n+1} + 1)|3$, and hence $n = 2$, $t = 4$. Thus M is a group of order 16, while T_2 is of order 4.

Since $h = 3$, M must admit an automorphism of order 3 leaving no elements other than the identity fixed. It can be shown that a group of order 16 having such an automorphism is either an elementary Abelian group or an Abelian group of type (4, 4).

We have therefore proved that if M has prime-power order, then it is in fact an elementary Abelian group, with the single exception stated in II.

Case 2. M is not a p-group. Then by Theorem 2, M is the direct product of elementary Abelian groups M_p of order p^n and M_q of order q^r. This time we write

3.18 $$h = 1 + \mu p^s q^t, \qquad (\mu, pq) = 1,$$

and as above

3.19 $$\mu p^s q^t < p^n, \qquad \mu p^s q^t < q^r.$$

From the definition of k, we also have

(3.20) $$k_1 = \frac{p^{n-s}q^{r-t} + \mu}{h}, \qquad k_2 = p^s q^t.$$

Furthermore, $(p^{n-s}q^{r-t} + \mu) | (p^n - 1)(q^r - 1)$, and hence, as in Case 1,

3.21 $$\mu p^s q^t \geqslant p^{n-s}q^{t-t} - p^n - q^r + \mu + 1.$$

We shall suppose, for definiteness, that $p^n > q^r$, and hence that

$$\mu p^s q^t > p^n \left[\frac{q^{r-t}}{p^s} - 2 \right].$$

In view of 3.19, the quantity in the brackets is less than 1, whence

3.22 $$q^r < 3p^s q^t.$$

Using 3.19 again, it follows that $\mu \leqslant 2$. However, 3.19 can be strengthened considerably; in fact, it is clear that $2\mu p^s q^t < q^r$ unless $h = q^r - 1$, and $3\mu p^s q^t < q^r$ unless $h = q^r - 1$ or $2h = q^r - 1$. It follows therefore from 3.22 that

3.23 $$\nu(1 + \mu p^s q^t) = q^r - 1,$$

where $\nu = 1$ or 2 if $\mu = 1$, and $\nu = 1$ if $\mu = 2$.

We deduce by inspection that 3.23 has the following five solutions only:

3.24
$$\begin{array}{ll}
\text{(a) } t = 0, \mu = 1, q \neq 2, & \nu = 1 \\
\text{(b) } t = 0, \mu = 2, q = 2, & \nu = 1 \\
\text{(c) } t = 0, \mu = 1, q \neq 3, & \nu = 2 \\
\text{(d) } t = 1, \mu = 1, q = 2, & \nu = 1 \\
\text{(e) } t = 1, \mu = 1, q = 3, & \nu = 2.
\end{array}$$

In particular, it follows from this that

3.25 $$h = 1 + \alpha p^s,$$

where $1 \leqslant \alpha \leqslant 3$.

Since $h|p^n - 1$, we have $p^n - 1 = \gamma(1 + \alpha p^s)$, $\gamma \geqslant 1$, and hence $\gamma = -1 + \beta p^s$, $\beta \geqslant 1$. Upon substitution for γ, we obtain

3.26 $$\beta\alpha p^{2s} = p^n + (\alpha - \beta)p^s.$$

Since $\alpha \leqslant 3$, the assumption $n < 2s$ implies $\beta = 0$, which is impossible. Thus $n \geqslant 2s$.

Consider next the case $n = 2s$. The only solution of 3.26 is then easily seen to be $\alpha = 1$, $\beta = 1$. This implies that we are either in Case 3.24 (a) or 3.24 (c). However, Case 3.24 (c) with $n = 2s$ yields $q^r = 3 + 2p^s$, and hence

$$k_1 = \frac{p^s(3 + 2p^s) + 1}{1 + p^s} = 2p^s + 1.$$

This is impossible since $k_1|h$ and $h = 1 + p^s$.

In Case 3.24(a), on the other hand, we obtain the solution $h = 1 + p^s = q^r - 1$, $k_1 = 1 + p^s$, $k_2 = p^s$, which accounts for the third alternative of the theorem.

We may therefore assume throughout the remainder of the proof that $n > 2s$. Consider first the cases in which $t = 0$. We use 3.23 to replace q^r in 3.21, obtaining

3.27 $$(\nu\mu + \mu)p^s \geqslant (\nu\mu - 1)p^n + (1 + \nu)p^{n-s} + \mu - \nu.$$

In each of the three cases in which $t = 0$ this inequality implies that $n \leqslant 2s$, contradicting our present assumption that $n > 2s$.

Similarly in Case 3.24(d), 3.21 reduces to

3.28 $$4p^s \geqslant p^{n-s}.$$

Either $n \leqslant 2s$ or, since $q = 2$, $p = 3$ and $n = 2s + 1$. But this would require $1 + 2.3^s|3^{2s+1} - 1$, which is impossible.

Finally in Case 3.24(e), 3.21 reduces to

3.29 $$9p^s \geqslant p^n + p^{n-s} - 1.$$

Since $q = 3$, it follows that $n \leqslant 2s$ except when $p = 5$, $s = 0$, $n = 1$ or $p = 2$, $n \leqslant 2s + 2$. In the first case, $p^n = 5$, $q^r = 9$, contrary to our assumption $p^n > q^r$. The second case requires either $1 + 3.2^s|2^{2s+1} - 1$ or $1 + 3.2^s|2^{2s+2} - 1$, the only solution of which is easily checked to be $s = 1$. But then $2h = 14$, which is not of the form $3^r - 1$. This completes the proof.

COROLLARY. *If M is an elementary Abelian group, A is a maximal subgroup of G, except when the order of M is* 16 *and the order of A is* 3.

Proof. In Case 1 of the proof of the theorem, we actually showed that $M = T_p$, except when $p = 2$, T_p is of order 4, and M is of order 16. Since by construction no proper subgroup of T_p is left invariant by A, the equality $M = T_p$ clearly implies that A is a maximal subgroup of G.

4. Independent ABA-groups in which A is of even order. The following theorem gives the complete structure of independent ABA-groups in which A has even order. Its proof does not depend upon Theorems 2 and 3, but only on the fact that such a group is a Frobenius group. This theorem will be used in the next section in the proof of our main result (Theorem 5).

THEOREM 4. *Let G be an independent ABA-group in which the order h of A is even, and let m be the order of the regular subgroup M of G. Then $h = m - 1$, M is an elementary Abelian group, A is isomorphic to the multiplicative group of a nearfield K, and G is isomorphic to the one-dimensional affine group over K.*

Proof. Since h is even, A contains an element a^* of order 2. Let $\sigma_{a^*}(t) = a^{*-1}ta^*$ for all t in M. Then σ_{a^*} is an automorphism of M or order 2 leaving only the identity element fixed. But a group having such an automorphism can easily be shown to be Abelian. (**1**, p. 90).

It follows therefore that

$$\sigma_{a^*}(t\sigma_{a^*}(t)) = \sigma_{a^*}(t)\sigma_{a^*}^2(t) = \sigma_{a^*}(t)t = t\sigma_{a^*}(t).$$

Thus $t\sigma_{a^*}(t)$ is left fixed by σ_{a^*}, and hence equals 1. We conclude that

4.1 $$a^*t^{-1} = ta^*$$

for all t in M.

Now let $b \in B$, $b \neq 1$. Since $G = AM$, we can write $b = at$, $a \in A$, $t \in M$. If $a = 1$, b is in M, and then 4.1 implies $a^*b^{-1} = ba^*$, contradicting the independence of G.

Thus $a \neq 1$. Suppose, if possible, that $a \neq a^*$. Let a have order d, and put $\sigma_a(t) = a^{-1}ta$. Then

$$b^{d-1} = (at)^{d-1} = a^{d-1}[\sigma_a^{d-2}(t) \ldots\ldots \sigma_a(t)t] = a^{d-1}t',$$

where t', in M, denotes the quantity in brackets. Since M is Abelian, $\sigma_a^{d-1}(t)t'$ is left fixed by σ_a, and hence $\sigma_a^{d-1}(t)t' = 1$. Thus

4.2 $$b^{d-1} = a^{d-1}[\sigma_a^{d-1}(t)]^{-1}.$$

But now it follows from 4.1 that

4.3 $$b^{d-1}a^* = a^{d-1}a^*\sigma_a^{d-1}(t).$$

On the other hand, $ba^{-1} = (at)a^{d-1} = \sigma_a^{d-1}(t)$, and consequently

4.4 $$b^{d-1}a^* = a^{d-1}a^*ba^{-1}.$$

Since $a^* \neq a$, this contradicts the independence of G.

We conclude then that every element of B distinct from the identity is of the form a^*t with t in M. If B contained two such elements $b_1 = a^*t_1$ and $b_2 = a^*t_2$, it would follow that $b = b_1b_2 = t_1^{-1}t_2$ were in $M \in B$, and we have already shown that this leads to a contradiction.

It follows therefore that B has order 2, and hence that $m = h(k-1) + 1 = h + 1$, thus establishing the first conclusion of the theorem.

But the structure of a Frobenius group of order $(m-1)m$, where m is the order of its regular subgroup M, is well-known (compare **2**, chapters VI, X, XIII): M is an elementary Abelian group, G is isomorphic to the one-dimensional affine group over a near field K of order m, and under this isomorphism, the subgroup A of G is mapped onto the multiplicative group of K.

5. The Structure of independent ABA**-groups.** We are now in a position to establish our main result:

THEOREM 5. *The regular subgroup M of an independent ABA-group G is an elementary Abelian group. Moreover, A is a maximal subgroup of G.*

Proof. By Theorem 3, M is either an elementary Abelian group, an Abelian group of type $(4, 4)$ with $h = 3$, or the direct product of two elementary Abelian groups M_p, M_q of orders p^n, q^r satisfying the relations: $h + 1 = 2 + p^{\frac{1}{2}n} = q^r$.

That no independent ABA-group of the third type exists may be seen as follows: since $p \neq q$, we must have $p \neq 2$, and hence h is even. But then Theorem 4 implies $h = m - 1 = p^n q^r - 1$, contrary to the fact that $h = q^r - 1$.

On the other hand, by the corollary of Theorem 3, if M is an elementary Abelian group, A is a maximal subgroup of G except when M has order 16 and $h = 3$. Thus the theorem will be completely proved if we show that no independent ABA-group exists in which $h = 3$ and M is either an elementary Abelian group or an Abelian group of type $(4, 4)$.

From the relation $h(k-1) + 1 = m$ with $h = 3, m = 16$, we conclude that k = order of $B = 6$. Since G is a Frobenius group, every element is either in M or conjugate to an element of A. Thus the elements of G are of orders 1, 2, 3 or 4; and hence B is not cyclic. Consequently B is generated by elements b_1, b_2 of orders 2, 3 respectively satisfying the relation

5.1 $$b_1 b_2 b_1^{-1} = b_2^{-1}.$$

Since b_1 is of order 2, it is in M. On the other hand, $b_2 = a^{\epsilon} t$, where t is in M, and $\epsilon = \pm 1$. Thus $b_1 a^{\epsilon} t\, b_1^{-1} = (a^{\epsilon} t)^{-1}$. Since M is normal in G, it follows at once that $a^{2\epsilon}$ is in M, contrary to the fact that $A \cap M = 1$.

From Theorem 5 we can now deduce the following structure theorem for independent ABA-groups:

THEOREM 6. *Let G be an independent ABA-group with A of order h and the regular subgroup M of G of order m. Then:*

I. *If $h = m - 1$, A is isomorphic to the multiplicatie group of a nearfield K, and G is isomorphic to the one-dimensional affine group over K. Conversely, the one-dimensional affine group over any finite nearfield is an independent ABA-group satisfying these conditions.*

II. *If $h < m - 1$, A is a metacyclic group of odd order whose generators a_1, a_2 satisfy the relations*

$$a_1^{h_1} = a_2^{h_2} = 1, a_2 a_1 a_2^{-1} = a_1^r, r^{h_2} \equiv 1 \pmod{h_1}, \quad \textit{and} \quad ((r-1)h_2, h_1) = 1.$$

In particular, if A is cyclic, G is isomorphic to a subgroup of the one-dimensional affine group over a finite field.

Proof. The proof of I has been given in the last paragraph of Theorem 4.

Conversely, the one-dimensional affine group over a finite nearfield K is easily seen to be an independent ABA-group when A is defined to be the set of transformations $x' = ax$, $a \in K$, $a \neq 0$, and B is the subgroup of order 2 generated by the transformation $x' = -x + 1$.

If $h < m - 1$, A is of odd order by Theorem 4. Since A is isomorphic to a group of automorphisms of M, each of which, except the identity, leaves only the identity element of M fixed, it follows that the Sylow subgroups of A are all cyclic (**1**; **2**; **7**). But then it follows that A is a metacyclic group satisfying the conditions listed in II (**6**, 145).

Finally if A is cyclic, we denote by σ_a the automorphism of M induced by a generator a of A. For convenience, we also regard M as an n-dimensional vector space over the integers modulo p. Since A is maximal in G, no subspace of M is left invariant by A, and hence the elements $t, \sigma_a(t), \ldots, \sigma_a^{n-1}(t)$ are linearly independent over the integers mod p for every $t \neq 0$ in M. For each choice of the integers $c_0, c_1, \ldots, c_{n-1} \pmod{p}$, not all $0 \pmod{p}$, it follows that the mapping

$$t \to \sum_{i=0}^{n-1} c_i \sigma_a^i(t) \tag{5.2}$$

is an automorphism of M leaving only the identity element fixed. In this way we obtain a group of automorphisms A^* of M of order $p^n - 1$, which clearly contains A. It is easy to see that A^* is also cyclic. Hence the Frobenius group $G^* = A^*M$ of order $(p^n - 1)p^n$ is isomorphic to the one-dimensional affine group over $GF(p^n)$. Since $G \subset G^*$, the last statement of the theorem now follows.

References

1. W. Burnside, *Theory of groups of finite order* (New York, 1955).

2. R. D. Carmichael, *Groups of finite order* (Boston, 1937).

3. W. Feit, *On the structure of Frobenius groups*, Can. J. Math., *9* (1957), 587–595.

4. G. Higman, *Groups and rings having automorphisms without non-trivial fixed elements*, J. Lond. Math. Soc., *30* (1957), 321–334.

5. A. Speiser, *Die Theorie der Gruppen von endlicher ordnung*, (Berlin, 1923).

6. H. Zassenhaus, *The Theory of Groups* (New York, 1949).

7. ———, *Ueber Endliche Fastkörper*, Abh. Math. Sem. Hamburg Univ., *11* (1935), 187–220.

Clark University
and Cornell University