Chin. Ann. of Math.
7B (3) 1986

ON GROUPS OF ODD ORDER AND RANK$\leqslant 2$

FAN YUN (樊 恽)*

Abstract

The least common multiple of dimensions of chief factors of a finite solvable group is called the rank of the group.

The groups of odd order with trivial Fratttini subgroups, all of whose subgroups but itself have ranks$\leqslant 2$, are completely determined (Theorem A).

For an odd number n, a necessary and sufficient condition for the groups of order n all to be of rank$\leqslant 2$ is obtained (Theorem B).

All groups and modules in this paper are finite. Terminologies and notations are usual (see [1]), except other explanations.

§ 1. The Main Results

We denote by F_p the Galois field of order p for an odd prime p, i. e. $F_p=GF(p)$. Given a non-square elemet δ in F_p and a root j of the equation $\xi^2=\delta$, we have $F_p(j)=GF(p^2)$.

We call the least commom multiple of dimensions of chief factors of a solvable group G the rank of G and denote it by $r(G)$ (see [2], p. 712).

We appoint that p, r, q are distinct odd primers, $C=\begin{pmatrix} 0 & 1 & & \\ & \ddots & \ddots & \\ \vdots & & \ddots & 1 \\ 0 & & & \ddots \\ 1 & \cdots & & 0 \end{pmatrix}$ is a cyclic matrix and I is the identity matrix.

Our main results are the following Theorem A and Theorem B.

Theorem A. *A group G of odd order with $\Phi(G)=1$ is of rank>2 but all of its proper subgroups are of rank$\leqslant 2$, if and only if G is isomorphic to a semi-direct product $V\rtimes H$ with V being an elementtary Abelian p-group and $H\leqslant GL(V/F_p)$, and H is one of the following nine types, written as three forms according to generators of H:*

Manuscript received July 6, 1983. Revised September 24, 1984.

* Department of Mathematics, Wuhan University, Wuhan, Hubei, China.

(i) $H=\left\langle\begin{pmatrix} 0 & 1 & & \\ \vdots & & \ddots & \\ & & & 1 \\ \alpha_k & \cdots & & \alpha_1 \end{pmatrix}\right\rangle$, $\alpha_1, \cdots, \alpha_k$ *are such that* $\xi^k-\alpha_1\xi^{k-1}-\cdots-\alpha_k$ *is an irreducible factor of* ξ^q-1 *in* $F_p[\xi]$ (hence $\exp(p)=k \pmod q$) *and* $k>2$.

(ii) $H=\left\langle\begin{pmatrix} 0 & 1 & & \\ & 0 & \ddots & \\ & & \ddots & 1 \\ \lambda & & & 0 \end{pmatrix}_{q\times q}, \begin{pmatrix} \varepsilon^{a_1} & & & \\ & \varepsilon^{a_2} & & \\ & & \ddots & \\ & & & \varepsilon^{a_q} \end{pmatrix}_{q\times q}\right\rangle$.

a) $\varepsilon=1$, λ *has order* q^{b-1} $(b>1)$ *in* F_p, $q^{b-1}\|q-1$ (*i.e.* $q^{b-1}|p-1$ *but* $q^b\nmid p-1$).

b) λ *has order* $q^{b-1}(b\geqslant 1)$ *in* F_p *and* $q^b|p-1$, ε *has order* q^a $(a\geqslant 1)$ *in* F_p (hence $q^a|p-1$), $a_i=1+(i-1)kq^{a-1}$ $(1\leqslant k\leqslant q-1)$.

c) λ *has order* $q^{b-1}(b\geqslant 1)$ *in* F_p *and* $q^a|p-1$, ε *has order* r *in* F_p (hence $r|p-1$), $(a_1, \cdots, a_q)$ *is a solution in* F_r *of the linear equation* $(C-tI)\begin{pmatrix} \xi_1 \\ \vdots \\ \xi_q \end{pmatrix}=0$ *with* $a_1=1$, t *being such that* $\xi-t$ *is a factor of* ξ^q-1 *in* $F_r[\xi]$ (hence $q|r-1$) *and* $t\neq 1$.

d) λ *and* ε *are the same as above,* $(a_1, \cdots, a_q)$ *is a solution in* F_r *of the equation* $(C^2-sC-tI)\begin{pmatrix} \xi_1 \\ \vdots \\ \xi_q \end{pmatrix}=0$ *with* $a_1=1$, *and* s, t *being such that* $\xi^2-s\xi-t$ *is an irreducible factor of* ξ^q-1 *in* $F_r[\xi]$ (*hence* $q|r+1$).

(iii) $H=\left\langle\begin{pmatrix} 0 & I & & \\ & 0 & \ddots & \\ & & \ddots & I \\ \Lambda & & & 0 \end{pmatrix}_{2q\times 2q}, \begin{pmatrix} M^{a_1} & & & \\ & M^{a_2} & & \\ & & \ddots & \\ & & & M^{a_q} \end{pmatrix}_{2q\times 2q}\right\rangle$

with I, Λ, M *being of size* 2×2.

a) $M=I$, $\Lambda=\begin{pmatrix} \lambda & \delta\mu \\ \mu & \lambda \end{pmatrix}$ *with* $\lambda+\mu j$ *having order* $q^{b-1}(b>1)$ *in* $F_p(j)$, $q\|p+1$.

b) $\Lambda=\begin{pmatrix} \lambda & \delta\mu \\ \mu & \lambda \end{pmatrix}$ *with* $\lambda+\mu j$ *having order* q^{b-1} $(b\geqslant 1)$ *in* $F_p(j)$ *and* $q^b|p+1$, $M=\begin{pmatrix} \alpha & \delta\beta \\ \beta & \alpha \end{pmatrix}$ *with* $\alpha+\beta j$ *having order* q^a $(a\geqslant 1)$ *in* $F_p(j)$ (*hence* $q^a|p+1$), μ and β are not zero, $a_i=1+(i-1)kq^{a-1}(1\leqslant k\leqslant q-1)$.

c) $\Lambda=\begin{pmatrix} \lambda & \delta\mu \\ \mu & \lambda \end{pmatrix}$ *with* $\lambda+\mu j$ *having order* q^{b-1} $(b\geqslant 1)$ *in* $F_p(j)$ *and* $q^b|p^2-1$, $M=\begin{pmatrix} \alpha & \delta\beta \\ \beta & \alpha \end{pmatrix}$ *with* $\alpha+\beta j$ *having order* r *in* $F_p(j)$ (*hence* $r|p^2-1$), *at least one of* μ *and* β *is not zero,* $(a_1, \cdots, a_q)$ *is the same as* (ii, c).

d) *A and M are the same as above, $(a_1, \cdots, a_q)$ is the same as* (ii, d).

Remark. Among the above types, (i) with $k>1$ instead of $k>2$, (ii, a), (ii, b), (ii, c) are exactly the all minimal non-supersolvable groups with trivial Frattini subgroups, provided the restriction in Theorem A that $|G|=$odd is eliminated (compare with [3, 4]). In fact, the condition that $|G|=$odd is not used in the discussions of these four types in this paper.

Theorem B. *Let $n=p_1^{a_1}, \cdots, p_t^{a_t}$ with p_i being distinct odd primes, and a_i being positive integers. Then $r(G)\leqslant 2$ for all groups of order n if and only if the following three conditions hold:*

1) *If $a_k\geqslant 2$, then $\left(p_i, \prod_{s=1}^{a_k}(p_k^s-1)\right)=(p_i, p_k^2-1)$, $1\leqslant i\leqslant t$.*

2) *If $p_i\leqslant a_k<2p_i$ and $p_i|p_k-1$, then $a_i\leqslant 2$, $p_i^{a_i}|p_k-1$, and there is no p_m such that $p_i|p_m^l-1$ ($l=1$ or 2 according to $a_m=1$ or >1) and $p_m|p_k-1$ both hold.*

3) *If $2p_i\leqslant a_k$ and $p_i|p_k^2-1$, then $a_i\leqslant 2$, $p_i^{a_i}|p_k^2-1$, and there is no p_m such that $p_i|p_m^l-1$ ($l=1$ or 2 according to $a_m=1$ or >1) and $p_m|p_k^2-1$ both hold.*

One can trace an analogy between theorem B and the result of [5], when he compares the two.

§ 2. Preliminaries and Lemmas

we begin with an observation of the following facts ([2] p. 712).

The class of all groups of odd order and rank$\leqslant 2$ is a local formation $\mathscr{F}$ defined by $\mathscr{F}(p)$ with

(i) $\mathscr{F}(2)=\phi$,

(ii) $\mathscr{F}(p)=\{A\,|\,A$ is abelian, $\exp(A)\,|\,p^2-1\}$ for $p>2$.

Because the divisors of p^2-1 are all less than p when p is odd, it is easy to see that each group in $\mathscr{F}$ has sylow-tower in the natural order ([2] p. 698).

For briefness, we use the symbol $\partial\mathscr{X}$ to denote the class of those groups, all of whose subgroups but itself belong to $\mathscr{X}$, where $\mathscr{X}$ is an arbitrary class of groups.

We shall preserve all notations mentioned up to now throughtout.

Lemma 1. *A group G of odd order with $\Phi(G)=1$ belongs to $\partial\mathscr{F}$ if and only if $G=V\leftthreetimes H$, V is an elemntary Abelian p-group for some odd prime p, $H\in\partial\mathscr{F}(p)\cap\mathscr{F}$, and H acts irreducibly faithfully on V.*

Proof By a result of [6], $G\in\partial\mathscr{F}$ if and only if $G=V\leftthreetimes H$, V is an elementary Abelian p-group, $H\in\partial(\mathscr{P}(p)\cdot\mathscr{F}(p))\cap\mathscr{F}$ and H acts faithfully irreducibly on V, where $\mathscr{P}(p)\cdot\mathscr{F}(p)$ is the class of all extensions of p-groups by groups in $\mathscr{F}(p)$.

Obviously, it is sufficient to show $p\nmid|H|$.

Suppose $p||H|$. Notice that the prime divisors of $|H|$ different from p are all

less than p for they divide p^2-1 and $p>2$, H possesses a non-trivial normal p subgroup because $H\in\mathscr{F}$ and the groups of $\mathscr{F}$ have sylow-towers in the natural order. On the other hand, by a basic fact of representation theory of groups $O_p(H)$ acts trivially on any irreducible F_pH-module. This contradicts the fact that H acts irreducibly faithfully on the F_pH-module V.

Lemma 2. *In $GL(n, F_p)$ a q-element x is irreducible* (i. e. $\langle x\rangle$ *is irreducible*) *if and only if $|x|\,|p^n-1$ but $|x|\nmid p^k-1$ for $0<k<n$.*

Proof Set $|x|=m=q^a$. x is irreducible if and only if its characteristic polynomial $f(\xi)$ is irreducible in $F_p[\xi]$. Since the order of x is m which is a power of prime q, at least one of the roots of $f(\xi)$, say ω, is a primitive m' th root of unity. Now x is irreducible if and only if $F_p(\omega)$ is of order p^n, i. e. $F_p(\omega)=GF(p^n)$; the latter is equivalent to $m|p^n-1$ but $m\nmid p^k-1$ for any $0<k<n$, because the multiplicative group of $GF(p^n)$ is a cyclic group of order p^n-1.

Remark. Another version of this lemma is to say that if the exponent of p mod m is n, then the degrees of irreducible factors of the m' th cyclotomic polynomial in $F_p[\xi]$ are all equal to n. In the later we shall, in fact, determine such factors under special conditions.

Lemma 3. *Let A be an Abelian group, $\exp(A)=e$, F a field, ($|A|$, char F) = 1. If F contains the e'th primitive root of unity, then F is a splitting field for A.*

Proof It is sufficient to show that any irreducible FA-module has dimension 1 over F. Obviously the assertion is true when $A=\langle x\rangle$ is cyclic because $\xi^{|x|}-1$ can be written as the product of factors of degree 1 in $F_p[\xi]$. In genersl case, the images of any irreducible representations of A are always cyclic, which are reduced to the above case.

Remark This lemma is, in fact, well known as a result of linear algebra, e. g. see [7] p. 490.

Lemma 4. *Let an Abelian p'-group $A\leqslant GL(V/F_p)$ be irreducible.*

(i) *If $\exp(A)\,|\,p-1$, then $\dim_{F_p}V=1$.*

(ii) *If $\exp(A)\,|\,p^2-1$ but $\exp(A)\nmid p-1$, p is odd, then $\dim_{F_p}V=2$ an there is a basis of V such that*

$$x=\begin{pmatrix}\alpha & \delta\beta\\ \beta & \alpha\end{pmatrix}$$

with $\alpha+\beta j$ having order $|x|$ in $F_p(j)$ for every $x\in A$, and $\beta\neq 0$ for at least one $x\in A$.

Proof (i) See Lemma 3.

(ii) $\exp(A)\,|\,p^2-1$ implies that the irreducible A-subspaces of $V\otimes F_p(j)$ are all of dimension 1 over $F_p(j)$ by Lemma 3. Let $\langle u+vj\rangle$ (u, $v\in V$) be such an A subspace of $V\otimes F_p(j)$. Considering any $x\in A$ acts on $\langle u+vj\rangle$, we have

$$(u+vj)x=(\alpha+\beta j)(u+vj)=(\alpha u+\delta\beta v)+(\beta u+\alpha v)j,$$

where $\alpha+\beta j$ is just the characteristic root of x restricted on $\langle u+vj\rangle$. It follows that

$$ux=\alpha u+\delta\beta v,$$
$$vx=\beta u+\alpha v.$$

Hence the subspace of V generated by $\{u, v\}$ is invariant under A. So $\{u, v\}$ generates V. On the other hand, $\dim_{F_p}V>1$ becasse $\exp(A)\nmid p-1$. Thus $\{u, v\}$ is a basis of V, under which x can be written as

$$x=\begin{pmatrix}\alpha & \delta\beta\\ \beta & \alpha\end{pmatrix}.$$

By the way, it is easy to see that $V\otimes F_p(j)=\langle u+vj\rangle\oplus\langle u-vj\rangle$. Furthermore, if the characteristic root of x on $\langle u+vj\rangle$ is $\alpha+\beta j$, then the characteristic root of x on $\langle u-vj\rangle$ is $\alpha-\beta j$.

The last conclusion is easy. If $\beta=0$ for every $x\in A$, then $V=\langle u\rangle\oplus\langle v\rangle$ and $\langle u\rangle$, $\langle v\rangle$ are both A-invariant, which is impossible.

Lemma 5. *Let x be an irreducible transformation of order q^b in $GL(V/F_p)$.*

(i) *If $q^{b-1}\|p-1$, $b>1$, then $\dim_{F_p}V=q$ and $x=\begin{pmatrix}0 & 1 & & \\ & \ddots & \ddots & \\ & & 0 & 1\\ \lambda & & & 0\end{pmatrix}$ with λ having order q^{b-1} in F_p.*

(ii) *If $q^{b-1}\|p+1$, $b>1$, then $\dim_{F_p}V=2q$ and $x=\begin{pmatrix}0 & I & & \\ & \ddots & \ddots & \\ & & 0 & I\\ \Lambda & & & 0\end{pmatrix}$, $\Lambda=\begin{pmatrix}\lambda & \delta\mu\\ \mu & \lambda\end{pmatrix}$ with $\lambda+\mu j$ having order q^{b-1} in $F_p(j)$.*

Conversely, in the both cases x is an irreducible element of order q^b.

Proof The treats of the two cases are similar. We only prove (ii).

First of all we show that the exponent of p mod q^b is equal to $2q$. $q^{b-1}\|p+1$ implies $p+1=\beta q^{b-1}$ with $(\beta, q)=1$, i. e. $p=\beta q^{b-1}-1$. Now $p^r\equiv1\pmod{q^b}\Leftrightarrow(\beta q^{b-1}-1)^r\equiv1\pmod{q^b}$. Suppose r is odd, then the latter becomes $r\beta q^{b-1}\equiv2\pmod{q^b}$. But this implies $q|2$, which contradicis the fact that q is odd. Thus r must be even. Assume $r=2s$. Then $(\beta q^{b-1}-1)^{2s}\equiv1\pmod{q^b}$ is equivalent to $2sq^{b-1}\equiv0\pmod{q^b}$, so $s\equiv0\pmod{q}$.

Now Lemma 2 shows that $\dim_{F_p}V=2q$. Given a subspace W of V irreducible for x^q, since $|x^q|=q^{b-1}$ and $q^{b-1}|p+1$, W/F_p has dimension 2 by Lemma 4. Moreover, $x^q|_W=\begin{pmatrix}\lambda & \delta\mu\\ \mu & \lambda\end{pmatrix}=:\Lambda$ $(\mu\neq0)$ with respect to a suitable basis of W. Clearly $W+Wx+\cdots+Wx^{q-1}$ is an invariant subspace of V for x. So

$$V=W+Wx+\cdots+Wx^{q-1}.$$

Because dim $V=2q$ and dim $W=2$, the right-hand side of the above equality must be a direct sum. We conclude

$$V=W\oplus Wx\oplus\cdots\oplus Wx^{q-1}.$$

Therefore under a suitable basis of V

$$x=\begin{pmatrix} 0 & I & & \\ & \ddots & \ddots & \\ & & 0 & I \\ \Lambda & & & 0 \end{pmatrix}.$$

Conversely assume $q^{b-1}\|p+1$, $x=\begin{pmatrix} 0 & I & & \\ & \ddots & \ddots & \\ & & 0 & I \\ \Lambda & & & 0 \end{pmatrix}$, $\Lambda=\begin{pmatrix} \lambda & \delta\mu \\ \mu & \lambda \end{pmatrix}$ with $\lambda+\mu j$ having order q^{b-1} in $F_p(j)$. Since the characteristic roots of Λ are $\lambda\pm\mu j$, the order of Λ is also equal to q^{b-1}. Hence $|x|=q^b$. In the first paragraph of this proof it has been seen that the exponent of p mod q^b is $2q$. So x is irreducible by Lemma 2, completing proof.

Lemma 6. *Let N be an Abelian normal subgroup of a non-Abelian group $H\leqslant GL(V/F_p)$, $|H:N|=q$, $H=N\cdot\langle x\rangle$ for a q-element x, $\exp(N)\,|\,p^2-1$. Then the F_pH-module V is irreducible if and only if*

$$V=W\oplus Wx\oplus\cdots\oplus Wx^{b-1},$$

where W is an irreducible F_pN-module and Wx^{i_1} is not F_pN-isomorphic to Wx^{i_2} for $i_1\neq i_2$.

Proof Assume F_pH-module V is irreducible. Write V as the direct sum of N-Wedderburn components (Cliford's theorem, [1], p. 70)

$$V=W_1\oplus W_2\oplus\cdots\oplus W_s,$$

the x acts transitively on W_1, $\cdots$, W_s. Since $x^q\in N$, x^q fixes each W_i. Thus $s=1$ or q. We claim that $s\neq 1$. Suppose $s=1$. Then V is a direct sum of isomorphic irreducible F_pN-modules $V_i(i=1,\cdots,n)$.

$$V=V_1\oplus\cdots\oplus V_n.$$

Either $\exp(N)\,|\,p-1$ or $\exp(N)\nmid p-1$. If $\exp(N)\,|\,p-1$, $\dim_{F_p} V_i=1$ by Lemma 4. Hence each element of N is a scalar transformation. Thus x commuts with each element of N, which contradicts the fact that H is non-Abelian.

In the case of $\exp(N)\nmid p-1$, we extend the F_p to $F_p(j)$ and consider $V\otimes F_p(j)=:\bar{V}$. Reacall $\exp(N)\,|\,p^2-1$, $\bar{V}_i=V_i\otimes F_p(j)$ are of dimension 2 over $F_p(j)$ and $\bar{V}_1=U_{11}\oplus U_{12}$, $U_{11}=\langle u+vj\rangle$, $U_{12}=\langle u-vj\rangle$, using the notations in Lemma 4. It is clear that $U_{12}\not\simeq U_{12}$ as N-modules (see the proof of Lemma 4). Since $\bar{V}_i\simeq\bar{V}_1$ $(i=2,\cdots,n)$, $\bar{V}_i=U_{i1}\oplus U_{i2}$ with $U_{i1}\simeq U_{11}$, $U_{i2}\simeq U_{12}$ as $F_p(j)N$-modules. Thus we obtain the N-wedderburn factorization

$$\widetilde{V}=(U_{11}\oplus\cdots\oplus U_{n1})\oplus(U_{12}\oplus\cdots\oplus U_{n2})=:U_1\oplus U_2.$$

The actions of elements of N on $U_i(i=1, 2)$ are all scalar multiplications. Now we view $\widetilde{V}$ as an $F_p(j)H$–module and write it as a direct sum of irreducible submodules, noting V is complete reducible as an H–module for $(|H|, p)=1$. Let U be a summand of the direct sum. Then as an N–module $U=(U\cap U_1)\oplus(U\cap U_2)$. If $U\cap U_i$ $(i=1, 2)$ are both non–trivial, x would interchange them for U is H–irreducible. Hence $2||x|$, which contradicts the fact that $q\neq 2$. So one of the $U\cap U_i$ $(i=1, 2)$ is trival for every summand U. Then x commuts with elements of N on every U. Consequently $H=N\langle x\rangle$ is Abelian, which is also a contradiction.

Up to now we can assert $s=q$, so it is obvious that

$$V=W\oplus Wx\oplus\cdots\oplus Wx^{q-1}.$$

Next it is easy to prove that W is N–irreducible. In the contrary case there is $0\neq W_1<W$, where W_1 is N–invariant. Then $0\neq W_1\oplus W_1x\oplus\cdots\oplus W_1x^{q-1}<V$ and $W_1\oplus\cdots\oplus W_1x^{q-1}$ is H–invariant, which is impossible.

Conversely let V be such as the assertion of the lemma and V_1 an F_pH–submodule with $0\neq V_1\leqslant V$. As an N–module

$$V_1=V_1\cap W\oplus\cdots\oplus V_1\cap Wx^{q-1}.$$

Clearly at least one of the direct summands of V_1, say $V_1\cap W$, is non–trivial. Then $V_1\cap W=W$. Using the action of x, we see that $V_1=V$ at once, completing the proof.

Remark. For the latter use we translate this lemma into matrix forms. If we choose a basis $\{w_1, \cdots, w_k\}$ of w, then $\{w_1x^i, \cdots, w_kx^i\}$ is a basis of Wx^i and the collection of them is just a basis of V. Hence x is written as

$$x=\begin{pmatrix} 0 & I & & \\ & \ddots & \ddots & \\ & & 0 & I \\ A & & & 0 \end{pmatrix}.$$

In addition, each element y of N is written as a diagonal block form

$$y=\begin{pmatrix} M_1 & & \\ & \ddots & \\ & & M_q \end{pmatrix},$$

where Mi is the matrix of y resticted on Wx^{i-1}. If $\exp(N)\,|\,p^2-1$ but $\exp(N)\nmid p-1$, and $|y|=q^b$, then Mi $(i=1, \cdots, q)$ can be written as powers of one and the same matrix $M=\begin{pmatrix} \alpha & \delta\beta \\ \beta & \alpha \end{pmatrix}$ with $\alpha+\beta j$ having order q^b in $F_p(j)$ (see Lemma 4); moreover, because the W in the factorization $V=W\oplus Wx\oplus\cdots\oplus Wx^{q-1}$ can be, in practice, arbitrary one of the N–Wedderburn components of V, in a suitable order of the basis of V mentioned above

$$y=\begin{pmatrix} M^{a_1} & & & \\ & M^{a_2} & & \\ & & \ddots & \\ & & & M^{a_q} \end{pmatrix} \quad \text{with} \quad a_1=1.$$

Lemma 7. *Let H, N be the same as in Lemma 6. Assume*

$$V=W\oplus Wx\oplus\cdots\oplus Wx^{q-1}$$

with W being an irreducible F_pN-module and $Wx^q=W$. Then H is irreducible if and only if there are two of Wx^i $(i=0, \cdots, q-1)$ which are not F_pN-isomorphic mutually.

Proof The "only if" part is obvious by Lemma 6.

Assume there are two of Wx^i's which are not F_pN-isomorphic mutually. Then there are at least two N-Wedderburn components of V each of which is constructed by means of collecting those members of Wx^i's isomorphic to each other. Since x permuts transitively the Wx^i's, x also permuts transitively the N-Wedderburn components of V. On the other hand, x^q fixes each Wx^i, and then x^q also fixes each N-Wedderburn components of V. Hence the number of N-Wedderburn components is equal to 1 or q. But the previous argument implies that the number must be only equal to q, and consequently each Wx^i is an N-Wedderburn component.

That is $Wx^{i_1}\not\cong Wx^{i_2}$ as F_pN-modules for $i_1\neq i_2$. Thus H is irreducible by Lemma 6.

§ 3. The Proof of Theorem A

Let G be a group of odd order with $\Phi(G)=1$. Lemma 1 shows that $G\in\partial\mathfrak{F}$ if and only if $G=V\rtimes H$, V is an elementary Abelian p-group for some odd prime p, $H\in\partial\mathfrak{F}(p)\cap\mathfrak{F}$ and H acts faithfully irreducibly on V. Hence we view $H\leqslant GL(V/F_p)$, where V is regarded as a vector space over F_p. The proof of Theorem A is reduced to the determination of all irreducible linear groups H over F_p which lie in $\partial\mathfrak{F}(p)\cap\mathfrak{F}$.

By the structures of the groups of $\partial\mathfrak{F}(p)$ and of $\mathfrak{F}$, H must be one of the three types.

(1) H is an Abelian q-group for some odd prime q;

(2) H is a non-Abelian q-group for some odd prime $q|p^2-1$;

(3) H is non-Abelian, $|H|=q^br^c$.

We proceed with the three cases respectively.

(1) H is an Abelian q-group.

Firstly it is immediate that H is cyclic. Suppose the contrary. Then $\langle h\rangle\in\mathfrak{F}(p)$ for any $h\in H$. So $h^{p^2-1}=1$, consequently $H\in\mathfrak{F}(p)$, which is impossible.

Let $H=\langle x\rangle$, $|x|=q^b$. We see that $q^b\nmid p^2-1$ but $q^{b-1}|p^2-1$. In other word, $q^{b-1}\|p^2-1$. With this information we, at once, come to the following conclusions.

If $b=1$, H may be and only may be (i) of Theorem A.

If $b>1$, $q^{b-1}|p-1$, (ii. a) and only (ii. a) of Theorem A are required by Lemma 5, (i).

If $b>1$, $q^{b-1}|p+1$, Lemma 5, (ii) reduces H to (iii. a) of Theorem A.

(2) H is a non-Abelian q-group.

A well-known result (see [8]) shows that H is generated by two elements x, y with $|x|=q^b$, $|y|=q^a$ and $[x, y]$ is an element of $Z(H)$ and of order q. Furthermore, q^a and q^b both divide p^2-1 as $H\in\partial\mathscr{F}(p)$. Conversely if H is as mentioned above, then H is minimal non-Abelian also by [8]. In addition, H is regular by [2] p. 322. Hence $(h_1h_2)^{p^k}=h_1^{p^k}h_2^{p^k}$ for any h_1, $h_2\in H$. It follows that $\exp(H)=\max\{p^a, p^b\}$, consequently $\exp(H)\,|p^2-1$. Hence $H\in\partial\mathscr{F}(p)\cap\mathscr{F}$.

On the other hand, choosing a maximal subgroup N of H containing y, by Lemma 6 and Lemma 4 we immediately write x and y as follows: If $q|p-1$, then

$$x=\begin{pmatrix} 0 & 1 & & \\ & 0 & \ddots & \\ & & & 1 \\ \lambda & & & 0 \end{pmatrix}_{q\times q},\quad y=\begin{pmatrix} \varepsilon^{a_1} & & & \\ & \varepsilon^{a_2} & & \\ & & \ddots & \\ & & & \varepsilon^{a_q} \end{pmatrix}_{q\times q},$$

λ and ε are just the same as (ii. b) of Theorem A. If $q|p+1$, then

$$x=\begin{pmatrix} 0 & I & & \\ & 0 & \ddots & \\ & & & I \\ \Lambda & & & 0 \end{pmatrix}_{2q\times 2q},\quad y=\begin{pmatrix} M^{a_1} & & & \\ & M^{a_2} & & \\ & & \ddots & \\ & & & M^{a_q} \end{pmatrix}_{2q\times 2q},$$

Λ and M are just the same as (iii. b) mentioned in Theorem A.

It only remains to determine $a_1, \cdots, a_q$. We deal with the two cases simultaneously, but write it in the form of the latter case.

Notice that $M=\begin{pmatrix} \alpha & \delta\beta \\ \beta & \alpha \end{pmatrix}$ is of order q^a and $a_1=1$ (see the remark following Lemma 6).

By a simple calculation

$$[x, y]=x^{-1}y^{-1}xy=\begin{pmatrix} M^{a_1-a_q} & & & \\ & M^{a_2-a_{q_1}} & & \\ & & \ddots & \\ & & & M^{a_q-a_{q-1}} \end{pmatrix}.$$

Since $[x, y]$ commuts with x, another straightforward calculation shows

$$c:\equiv a_1-a_q\equiv a_2-a_1\equiv\cdots\equiv a_q-a_{q-1}\ (\mathrm{mod}\ q^a).$$

Since $|[x, y]|=q$, we obtain another equation

$$cq\equiv 0(\mathrm{mod}\ q^a).$$

The latter equation shows $c\equiv 0 (\mathrm{mod}\ q^{a-1})$, so $c=kq^{a-1}$ $(k=1, \cdots, q-1)$. Then the former equation gives the values of a_i,

$$a_1=1,\ a_2=1+kq^{a-1},\ \cdots,\ a_q=1+(q-1)kq^{a-1}.$$

Clearly $a_{i_1}\not\equiv a_{i_2}$ (mod q^a) for $i_1\neq i_2$.

Now we have to deal with the irreducibility of H. The characteristic roots of M are $\alpha\pm\beta j$ $(\beta\neq 0)$ which are all of order q^a in $F_p(j)$. So $(\alpha+\beta j)^{a_1}\neq(\alpha+\beta j)^{a_i}$ $(1\neq i)$. Hence there is at most one of M^{a_i} $(i=2, \cdots, q)$ whose characteristic roots are coincident with that of M. Thus there is at most one of Wx^i $(i=1, \cdots, q-1)$ mentioned in Lemma 7 which is F_pN-isomorphic to W. Noting $q=$odd, there are two of $Wx^i (i=0, \cdots, q-1)$ which are not F_pN-isomorphic to each other. So H is irreducible by Lemma 7.

Summarizing the above, we achieve (ii. b) and (iii. b) of Theorem A.

(3) $|H|=q^br^c$.

In this case $H=RQ$, $Q\in Syl_q(H)$, $R\in Syl_r(H)$, $R\trianglelefteqslant H$ and R is an elementary Abelian r-group, $Q=\langle x\rangle$ is a cyclic group which acts irreducibly on R; consequently $R=\langle y^{\langle x\rangle}\rangle$ for any $1\neq y\in R$. So $H=\langle x, y\rangle$. All the information follows from well-known results on minimal non-Abelian groups. Moreover, since $H\in \partial\mathscr{F}(p)$, $\exp(H)\,|\,p^2-1$. In addition, $H\in\mathscr{F}$. Thus $c=1$ or 2. Conversely the group H determined above belongs obviously to $\partial\mathscr{F}(p)\cap\mathscr{F}$.

Let $N=R\cdot\langle x^q\rangle$. Then $H=N\cdot\langle x\rangle$. We use Lemma 6 in writting x, y and use Lemma 7 in discussing the irreducibility of H.

If $\exp(N)\,|\,p-1$, then

$$x=\begin{pmatrix} 0 & 1 & & \\ & 0 & \ddots & \\ & & \ddots & 1 \\ \lambda & & & 0 \end{pmatrix}_{q\times q},\quad y=\begin{pmatrix} \varepsilon^{a_1} & & & \\ & \varepsilon^{a_2} & & \\ & & \ddots & \\ & & & \varepsilon^{a_q} \end{pmatrix}_{q\times q},$$

λ and ε are the same as (ii, c) of Theorem A.

If $\exp(N)\,|\,p+I$, then

$$x=\begin{pmatrix} 0 & I & & \\ & 0 & \ddots & \\ & & \ddots & I \\ \Lambda & & & 0 \end{pmatrix}_{2q\times 2q},\quad y=\begin{pmatrix} M^{a_1} & & & \\ & M^{a_2} & & \\ & & \ddots & \\ & & & M^{a_q} \end{pmatrix}_{2q\times 2q},$$

Λ and M are just the same as (iii, c) of Theorem A. It is necessary to explain that the reason that at least one of μ and β is not zero is the irreducibility of N-module W in Lemma 6 (see Lemma 4).

It remains only to determine $(a_1, \cdots, a_q)$ like the argurment in case (2) we treat the two types simultaneously and always assume $a_1=1$. But we shall proceed with two cases according to $c=1$ or $c=2$.

Firstly assume $|H|=q^br$. Consequently $q|r-1$. Suppose $xyx^{-1}=y^t$ with $(t, r)=1$, its matrix form is

$$\begin{pmatrix} M^{a_2} & & & \\ & M^{a_3} & & \\ & & \ddots & \\ & & & M^{a_q} \\ & & & & M^{a_1} \end{pmatrix} = \begin{pmatrix} M^{ta_1} & & & \\ & M^{ta_2} & & \\ & & \ddots & \\ & & & M^{ta_q} \\ & & & & M^{ta_q} \end{pmatrix},$$

i. e.

$$\begin{pmatrix} a_2 \\ a_3 \\ \vdots \\ a_1 \end{pmatrix} = t \begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_q \end{pmatrix}, \quad (\text{in } F_r).$$

By use of the cyclic matrix C this formula is rephrased as follows

$$(C-tI)\begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_q \end{pmatrix} = 0 \quad (\text{in } F_r).$$

Hence $(a_1, \cdots, a_q)$ is a solution in F_r of the following linear equation

$$(C-tI)\begin{pmatrix} \xi_1 \\ \vdots \\ \xi_q \end{pmatrix} = 0 \quad (\text{in } F_r).$$

Because $\det(C-tI)=(-1)^q(t^q-1)$, the above equation has non-trivial solution if and only if t is a root of ξ^q-1 (the roots of this polynomial are all in F_r for $q|r-1$). But $t=1$ can not be chosen, because in this case $a_1=a_2=\cdots=a_q$ and $W, \cdots, Wx^{q-1}$ mentioned in Lemma 6 are all isomorphic N-modules, which is not required by Lemma 6. In addition, the above equation has only one solution with $a_1=1$ because the q roots of ξ^q-1 are distinct pairwisely and consequently $C-tI$ has rank $q-1$. In fact, the solution is as follows:

$$a_1=1, \ a_2=t, \ \cdots, \ a_q=t^{q-1}.$$

Thus $a_{i_1} \not\equiv a_{i_2} \pmod r \ (i_1 \neq i_2)$. So H is irreducible by the same argument as in the case (2).

The above discussion reduces H to (ii. c) and (iii. c) of Theorem A. Next let $|H|=q^br^2$, consequently $q|r+1$. Now $R=\langle y, y^a\rangle$ is a 2-dimensional space over F_r. This holds if and only if $y^{a^2}=y^t(y^a)^s$ for some $t, s, \in F_r$, i. e.

$$\begin{pmatrix} M^{a_3} & & & \\ & M^{a_4} & & \\ & & \ddots & \\ & & & M^{a_q} \\ & & & & M^{a_1} \\ & & & & & M^{a_2} \end{pmatrix} = \begin{pmatrix} M^{ta_1+sa_2} & & & \\ & M^{ta_2+sa_3} & & \\ & & \ddots & \\ & & & M^{ta_{q-2}+sa_{q-1}} \\ & & & & M^{ta_{q-1}+sa_q} \\ & & & & & M^{tsa_q+sa_1} \end{pmatrix}.$$

Similarly to the previous it can be written as the linear equation form

$$(C^2-sC-tI)\begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_q \end{pmatrix}=0 \quad (\text{in } F_r).$$

In order to explain this formula and to determine s and t such that H is irreducible, we fransform C in diagonal form, noting $q|r+1$ and the characteristic polynomial of C is ξ^q-1, this can be perfomed in $GF(r^2)$. With these observations it is easy to see that $\det(C^2-sC-tI)=0$ if and only if $\xi^2-s\xi-t$ is an irreducible factor of ξ^q-1 in $F_r[\xi]$. This is exactly consistent with the requiement that x acts irreducibly on R because the characteristic polynomial of x on R is exactly $\xi^2-s\xi-t$. On the other hand, Lemma 2 shows that the irreducible factors of ξ^q-1 in $F_r[\xi]$ are all of degree 2, except for $\xi-1$. Furthermore, by the same observations the rank of $C^2-sC-tI$ is $q-2$ when s, t are chosen as above, so the equation

$$(*) \qquad (C^2-sC-tI)\begin{pmatrix} \xi_1 \\ \vdots \\ \xi_q \end{pmatrix}=0 \quad (\text{in } F_r)$$

has many solutions with $a_1=1$. But we shall show that for any solution of (*) with $a_1=1$ we get the one and the same linear group H which is always irreducible. Hence, in practice, we can choose arbitrary one solution $(a_1, \cdots, a_q)$ of (*) with $a_1=1$.

Let $(a_1, \cdots, a_q)$ be a non-trivial solution of (*). Clearly $C\begin{pmatrix} a_1 \\ \vdots \\ a_q \end{pmatrix}$ is also a solution of (*). Further we claim that the two solutions are linearly independent. In the contrary case, $C\begin{pmatrix} a_1 \\ \vdots \\ a_q \end{pmatrix}=d\begin{pmatrix} a_1 \\ \vdots \\ a_q \end{pmatrix}$ for some $d\in F_r$. Hence $\det(C-dI)=0$. So $\xi-d$ is a factor of ξ^q-1 in $F_r[\xi]$. But we have seen that the factors of ξ^q-1 and of degree 1 is only the $\xi-1$. Thus $(a_1, \cdots, a_q)$ belongs not only to the charactenistic subspace of $\xi-1$, but also to the characteristic subspace of $\xi^2-s\xi-t$. This is impossible because the two subspaces have the trivial intersection.

Assume $H=\langle x, y\rangle=R\cdot\langle x\rangle$ is the group determined by means of $(a_1, \cdots, a_q)$. Notice that $R=\langle y^{\langle x\rangle}\rangle$, $y^x=\operatorname{diag}(M^{z_1}, \cdots, M^{z_q})$, where $\begin{pmatrix} b_1 \\ \vdots \\ b_q \end{pmatrix}=C\begin{pmatrix} a_1 \\ \vdots \\ a_q \end{pmatrix}$, and each element z of R is a combination of y and y^x. Hence $z=\operatorname{diag}(M^{z_1}, \cdots, M^{z_q})$ and $(z_1, \cdots, z_q)$ is a combination of $(a_1, \cdots, a_q)$ and $(b_1, \cdots, b_q)$. Now if we set $z\mapsto(z_1, \cdots, z_q)$,

it is easy to see that R is, in fact, isomorphic to the 2-dimensional subspace of $(F_r)^q$ which consists of all solutions of (*). So we conclude that H is uniquely determind by the irreducible factor $\xi^2-s\xi-t$.

We turn to the irreducibility of H now. Recall $x^k y(x^k)^{-1}=\mathrm{diag}(M^{c_1}, \cdots, M^{c_q})$, where $\begin{pmatrix} c_1 \\ \vdots \\ b_q \end{pmatrix}=O^k\begin{pmatrix} a_1 \\ \vdots \\ a_q \end{pmatrix}$. As first step we show that for any $1\leqslant i_1\neq i_2\leqslant q$ there is k such that $c_{i_1}\neq c_{i_2}$. We prove this by contradiction. Lossing no generality, assume $i_1=1$, $i_2=i+1$. Suppose $c_1=c_{i+1}$ for any k. A simple computation shows $c_1=a_{1+k}$, $c_{i+1}=a_{1+i+k}$, where the subscripts $1+k$, $1+i+k$ are all modulo q. So $a_{1+k}=a_{1+i+k}$ for all k. Putting $k=0, i, 2i, \cdots$, we obtain $a_1=a_{i+1}=a_{2i+1}=a_{3i+1}=\cdots$. Since $(i, q)=1$, there always is l satisfying $l_{i+1}\equiv n \pmod q$. Consequently $a_1=a_n$ for any n, i. e. $a_1=a_2=\cdots=a_q$, which is impossible by the previous argument.

If a_i are all distinct pairwisely, then the irreducibility of H has been proved in the case that $c=1$.

Assume a_i are not all distinct. Lossing no generality, assum $a_1=a_2=1$, i. e. $y=\begin{pmatrix} M & & \\ & M & \\ & & \ddots \end{pmatrix}$. Further assume $y'=x^k y x^{-k}=\begin{pmatrix} M^{c_1} & & \\ & M^{c_2} & \\ & & \ddots \end{pmatrix}$ with $c_1\neq c_2 \pmod r$ by the first step. It is enough for the proof of irreducibility of H by Lemma 7 to show that $W\neq Wx$ (the symbols in Lemma 6 and Lemma 7) as F_pN-modules. Suppose this is not true, then there is $T\in GL(2, F_p)$ such that $T^{-1}MT=M$ and $T^{-1}M^{c_1}T=M^{c_2}$. We extend F_p to $F_p(j)$ and transform M into diagonal form. For convenience, we do not change the symbols, so

$$M=\begin{pmatrix} \alpha+\beta j & \\ & \alpha-\beta j \end{pmatrix}.$$

Because $T^{-1}MT=M$ and $\alpha+\beta j\neq\alpha-\beta j$ (in the case that $\beta=0$) the irreducibility of H is trivial since at least two of $M^{a_i}(i=1, \cdots, q)$ possess characteristic. roots different from each other), T is also a diagonal matrix. Then

$$M^{c_1}=\begin{pmatrix} (\alpha+\beta j)^{c_1} & \\ & (\alpha-\beta j)^{c_1} \end{pmatrix},$$

$$M^{c_2}=\begin{pmatrix} (\alpha+\beta j)^{c_2} & \\ & (\alpha-\beta j)^{c_2} \end{pmatrix},$$

$$M^{c_1}=T^{-1}M^{c_1}T=M^{c_2}.$$

These equalities imply $(\alpha+\beta j)^{c_1}=(\alpha+\beta j)^{c_2}$, which is impossible because $\alpha+\beta j$ is of order r and $c_1\neq c_2 \pmod r$.

Now we obtain (ii. d) and (iii. d) of Theorem A.

The proof of Theorem A is complete.

§ 4. The Proof of Theorem B

The necessity of conditions (1), (2), (3).

First of all we show an obvious fact: if there is a group of order m which has rank>2, then there is a group of order mk for any $k\geqslant 1$ which has rank>2.

Suppose (1) does not hold. Then there are p_i, p_k such that $\left(p_i, \prod_{s=1}^{a_k} p_k^s - 1\right) \neq (p_i, p_k^2-1)$. Hence there exists h with $3\leqslant h\leqslant a_k$ such that $p_i | p_k^h-1$ but $p_i \nmid p_k^s-1$ for any $0<s<h$. Thus (i) of Theorem A gives a group G with $|G| = p_i p_k^h$ and $r(G)=h \geqslant 3$ (see Lemma 2 and the remark following it).

Suppose $p_i \leqslant a_k < 2p_i$ and $p_i | p_k-1$. Firstly we show that it is necessary that $p_i^{a_i} | p_k-1$. If this is not true, then there is h such that $p_i^h \| p_k-1$, $1\leqslant h<a_i$, so (ii. a) of Theorem A gives a group G, $|G| = p_i^{h+1} p_k^{p_i}$, $r(G)=p_i>2$. Next if $a_i>2$, we consider (ii. b) of Theorem A. Take ε to be a p_i^l th primitive root of unity in F_{p_k}(remark $p_i | p_k-1$) and $\lambda=1$. Then $G=V \rtimes H$, $|G| = p_i^3 p_k^{p_i}$, and $r(G)=p_i>2$. This fact shows that it is necessary that $a_i\leqslant 2$. Now assume there is also p_m such that $p_i | p_m^l-1$ ($l=1$ or 2 according to $a_m=1$ or>1) and $p_m | p_k-1$ both hold. Then either $p_i | p_m-1$ or $p_i | p_m+1$ (hence $a_m\geqslant 2$). If $p_i | p_m-1$, we consider (ii, c) of Theorem A and put $p_i=q$, $p_m=r$ $p_k=p$, $\lambda=1$. Then we obtain a group $G=V \rtimes H$, $|G| = p_i p_m p_k^{p_i}$, $r(G)=p_i>2$. If $p_i | p_m+1$, noting $a_m\geqslant 2$, we turn to (ii. d) of Theorem A and put $p_i=q$, $p_m=r$, $p_k=p$, $\lambda=1$. Then we have $G=V \rtimes H$, $|G| = p_i p_m p_k^{p_i}$, $r(G)=1$. c. m of p_i and 2.

Summarizing the above discussion, we assert that the condition (2) is necessary.

It is easy to see that the proof of necessity of condition (3) is similar to the above. In other words, if some one of (3) does not hold, one can find counterexamples in (iii) of Theorem A, except some cases, for example, $p_i | p_k-1$ and $p_m | p_k-1$, which fall into the condition (2) in fact.

The sufficiency of conditions (1), (2), (3).

It is a simple fact that if n satisfies conditions (1), (2), (3) of Theorem B, so does any divisor of n.

If the sufficiency of Theorem B is not true, let G be a minimal counterexample.

Firstly $\Phi(G)=1$. If $\Phi(G)\neq 1$, then $r(G/\Phi(G))\leqslant 2$, so $r(G)\leqslant 2$ because $\mathscr{F}$ is local and consequently saturated (see [2] p. 697). This is impossible.

Now G must be one of the list of Theorem A. After examining the orders of groups listed in Theorem A one by one, we find the following:

The orders of groups of (i) of Theorem A violate the condition (1).

The orders of groups of (ii. a) of Theorem A violate the one of (2): if $p_i \leqslant a_k < 2p_i$, $p_i | p_k-1$, then $p_i^{a_i} | p_k-1$.

The orders of (ii. b) of Theorem A violate the one of condition (2): if

$p_i \leqslant a_k < 2p_i$, $p_i | p_k - 1$, then $a_i \leqslant 2$. In order to clear this contradiction, we show that the group H in (ii. b) is a non-Abelian q-group. So $|H| \geqslant q^3$, whence $q^3 p^q \| |G|$.

The orders of (ii. c) and (ii. d) of Theorem A do not satisfy the one of condition (2): if $p_i \leqslant a_k < 2p_i$, $p_i | p_k - 1$, then there is no p_m such that $p_i | p_m^l - 1$ ($l=1$ or 2 according to $a_m = 1$ or >1) and $p_m | p_k - 1$ both hold. This assertion is deduced from the following fact. In (ii. c) and (ii. d), $H = R \rtimes Q$, $Q = \langle x \rangle$, $|x| = q^b$, x acts non-trivially and irreducibly on R, $|R| = r^c$, $c=1$ or 2. Thus $q | r-1$ (if $c=1$) or $q | r+1$ (if $c=2$), while $r | p-1$ in both the cases.

Similarly the orders of groups of (iii) of Theorem A violate the condition (3) of Theorem B.

Now we conclude that there is no minimal conuterexample to the sufficiency of Theorem B. So the sufficiency of Theorem B is proved.

References

[1] Gorenstein, D., Finite Groups, Now York, Second edition, 1980.

[2] Huppert, B., Endliche Gruppen, I, springer, 1967.

[3] Chen ZhongMu, Inner and outer supersolvable groups, *Acta Math. Sinca*, **27**: 5 (1984), 694—703.

[4] Nagrebetski, B. T (Нагребецкий, В. Т), On finite minimal non-supersolvable groups, in «Finite Groups», Minsk Nauki i texn., 1975, 104—108 (Russion).

[5] Zhang YuanDa and Fan Yun, On supersolability of groups of order n, *J. Math.*, (PRC, Wuhan) **1**: 1 (1981) 86—95.

[6] Fan Yun, On the $\mathscr{F}$-stability and the $\mathscr{F}$-criticality, *Acta Math. Sinica*, **29**: 1 (1986), 117—126.

[7] Zhang Yuanda, The Principle of Linear Algebra, Shanghai, 1980.

[8] Chen ZhongMu, Inner Σ-groups, *Acta Math. Sinica*, **24**: 3 (1981), 331—336.