16. On the structure of infinite M -groups.

By

Kenkiti IWASAWA.

(Received February 21st, 1942.)

§1. Introduction.

In a previous publication⁽¹⁾, I have studied the structure of finite M -groups. The purpose of the present paper is to extend the results of that paper to the case of infinite groups.

A group $\mathfrak{G}$ is called M -group when the lattice $L(\mathfrak{G})$ formed by all subgroups of $\mathfrak{G}$ is a modular lattice⁽²⁾: it holds namely for arbitrary subgroups $\mathfrak{A}$, $\mathfrak{B}$, $\mathfrak{C}$ with $\mathfrak{A} \subseteq \mathfrak{C}$, of $\mathfrak{G}$ the modularity equation

$$(1) \quad \mathfrak{A} \vee (\mathfrak{B} \wedge \mathfrak{C}) = (\mathfrak{A} \vee \mathfrak{B}) \wedge \mathfrak{C}.$$

In this case, if we make each subgroup $\mathfrak{X}$ lying between $\mathfrak{A} \vee \mathfrak{B}$ and $\mathfrak{B}$ correspond to the subgroup $\mathfrak{X} \wedge \mathfrak{A}$, and each subgroup $\mathfrak{Y}$ lying between $\mathfrak{A}$ and $\mathfrak{A} \wedge \mathfrak{B}$ to the subgroup $\mathfrak{Y} \vee \mathfrak{B}$, we have a lattice isomorphism between quotient lattices $\mathfrak{A} \vee \mathfrak{B} / \mathfrak{B}$ and $\mathfrak{A} / \mathfrak{A} \wedge \mathfrak{B}$:

$$(2) \quad \mathfrak{A} \vee \mathfrak{B} / \mathfrak{B} \cong \mathfrak{A} / \mathfrak{A} \wedge \mathfrak{B}.$$

It follows then, that the length of any principal chain which connects two subgroups of $\mathfrak{G}$ is always equal to each other⁽³⁾. A group is called "group of finite length", when all its principal chains which connect the whole group with the identity, have always the same and finite length. For example any finite M -group is a group of finite length. But it is not yet decided whether a group of finite length is finite or not. This is a special case of the unproved assumption, that a group is finite when its subgroups satisfy the both chain conditions⁽⁴⁾,

The structure of a finite M -group is given by the following theorems⁽⁵⁾:

(1) K. Iwasawa. Über die endlichen Gruppen und die Verbände ihrer Untergruppen, Journal of the faculty of science, Tokyo Imperial University, I, vol. IV, part 3. (1941)—referred to as G.V.

(2) See G. V. p. 171.

(3) For the general lattice theory see G. Birkhoff, Lattice theory (1940).

(4) This assumption is indeed valid for those groups which can be isomorphically represented with matrices on some commutative field. Cf. I. Schur, Sitzungsber. Preuss. Acad. Wiss. 1911, p. 619—627.

(5) See G. V. Satz 2, 3, 18.

1. A p -group ($p > 2$) $\mathfrak{P}$ is an M -group if and only if it has the following structure:

- (i) $\mathfrak{P}$ contains an abelian normal subgroup $\mathfrak{A}$,
- (ii) $\mathfrak{P}/\mathfrak{A}$ is cyclical,
- (iii) for a suitable generator T of $\mathfrak{P}/\mathfrak{A}$ we have for any element A of $\mathfrak{A}$

$$(3) \quad TAT^{-1} = A^{1+p^s},$$

where s means an integer which is uniquely determined by $\mathfrak{P}$ and $\mathfrak{A}$, and is independent of A .

2. A 2-group is an M -group, if and only if it has either the same structure as in 1 with an additional condition $s \geq 2$, or it is a Hamiltonian 2-group, i.e. it is the direct product of a quaternion-group and an abelian group of type $(2, 2, \dots, 2)$.

3. Let p, q be two different prime numbers, $p > q$. A group $\mathfrak{G}$ of order $p^\alpha q^\beta$, which is not the direct product of their Sylowgroups, is an M -group if and only if it has the following structure:

- (i) A p -Sylowgroup $\mathfrak{P}$ is normal in $\mathfrak{G}$ and is an abelian group of type $(p, p, \dots, p)$.
- (ii) A q -Sylowgroup $\mathfrak{Q}$ is cyclic; $\mathfrak{G} = \langle \mathfrak{Q} \rangle$.
- (iii) For an arbitrary element P of $\mathfrak{P}$ it holds

$$(4) \quad QPQ^{-1} = P^r$$

where r is a definite integer which depends only on the group $\mathfrak{G}$ and satisfies following conditions

$$(5) \quad r \not\equiv 1 \pmod{p}, \quad r^q \equiv 1 \pmod{p}.$$

4. A finite group $\mathfrak{G}$ is an M -group if and only if it is the direct product of groups of mutually prime orders which have structures mentioned above in 1-3.

Now let $\mathfrak{G}$ be an arbitrary M -group and A and B its elements of finite orders. We prove first that AB is also of finite order. Let $\mathfrak{A} = \langle A \rangle$, $\mathfrak{B} = \langle B \rangle$. From (2) it follows easily that $\mathfrak{A} \cup \mathfrak{B}$ is of finite length; consequently it contains no element of infinite order, because an element C of infinite order would give rise to an infinite sequence of subgroups $\{C\}, \{C^2\}, \{C^3\}, \dots$. As an element of $\mathfrak{A} \cup \mathfrak{B}$ AB is of finite order. Thus we obtain the following

Theorem 1. In an M -group $\mathfrak{G}$, elements of finite orders form together a characteristic subgroup $\mathfrak{C}$ of $\mathfrak{G}$. $\mathfrak{G}/\mathfrak{C}$ is then an M -group whose all elements except the identity are of infinite orders.

In the following we treat two cases separately, $\mathfrak{G} = \mathfrak{C}$, and $\mathfrak{G} \neq \mathfrak{C}$.

In §2 we study the case $\mathfrak{G} = \mathfrak{C}$. On that occasion we must employ the assumption mentioned above, i.e. that a group of finite length is finite. Therefore the theorems which are to be obtained in §2 are available only for those groups whose subgroups of finite length have finite orders, for example locally finite groups, quasi-Hamiltonian groups etc. But if that assumption could have been proved anyhow, then our results would give the structure of general M -groups whose all elements are of finite orders.

In §3, we determine the structure of an M -group which has at least one element of infinite order. It is to be noted that in this case $\mathfrak{G} \neq \mathfrak{C}$, we can carry out our investigation without any assumption. This may deserve some interest. In fact we prove a special case of the above assumption and by help of this lemma we can avoid the relating difficulties after some delicate considerations.

§2. M -groups without element of infinite order.

1. In this paragraph we always consider such an M -group $\mathfrak{G}$ that its elements are all of finite orders and its subgroups of finite length are finite. We have then at once.

Lemma 1. If $\mathfrak{A}$ and $\mathfrak{B}$ are finite subgroups of $\mathfrak{G}$, then $\mathfrak{A} \cup \mathfrak{B}$ is also finite. Finite subgroups of $\mathfrak{G}$ thus form a sublattice of $L(\mathfrak{G})$.

Proof. From (2) it follows easily that $\mathfrak{A} \cup \mathfrak{B}$ is of finite length, and so is finite by the assumption⁽⁶⁾.

Now let p be any prime number. We assume first that any element of p -power order is commutative with all elements which have orders prime to p . Let A, B be any element of order p^a, p^b respectively. According to Lemma 1 $\langle A, B \rangle$ is a finite group and by the assumption its p -Sylowgroup is normal. While A, B are contained in this p -Sylowgroup, $\langle A, B \rangle$ itself is a p -group and AB has also a p -power order. All elements of p -power orders form therefore a characteristic subgroup of $\mathfrak{G}$: the p -component $\mathfrak{P}$ of $\mathfrak{G}$.

We assume next that an element P of order p^m is not commutative with an element Q of different prime power order q^n . As before it is easy to see that $\langle P, Q \rangle$ is a finite group of type 3 in §1. We may suppose for instance, exchanging P and Q if necessary, that a p -Sylowgroup $\mathfrak{P}_0$ is an abelian normal subgroup of type $(p, p, \dots, p)$, and a q -Sylowgroup is cyclic. Now let P' be another element of p -power

⁽⁶⁾ The converse is also true; that is to say, this lemma is equivalent with the assumption mentioned above.

order. $\{P, P', Q\}$ is also a group of type 3 in §1. It follows therefore

$$PP' = P'P, \quad P^p = P'^p = 1,$$

that is, all elements of $\mathfrak{G}$ of p -power orders form an abelian characteristic subgroup $\mathfrak{P}$, any of whose elements satisfy the relation

$$(6) \quad X^p = 1.$$

Then it is easy to see that for an arbitrary element P_0 of $\mathfrak{P}$ it holds

$$(7) \quad QP_0Q^{-1} = P_0^r, \quad r \not\equiv 1, \text{ mod. } p, \quad r^q \equiv 1, \text{ mod. } p.$$

If we take another Q' of q -power order then $\{P, Q, Q'\}$ is also of type 3 in §1. We denote the normal p -Sylowgroup of this group by $\mathfrak{P}_1$ and a cyclic q -Sylowgroup by $\mathfrak{Q}_1 = \{Q^*\}$. It follows then

$$(8) \quad Q^*P_1Q^{*-1} = P_1^{r_1}, \quad r_1 \not\equiv 1, \text{ mod. } p, \quad r_1^q \equiv 1, \text{ mod. } p,$$

for all P_1 in $\mathfrak{P}_1$.

If we have

$$Q^{*u} \equiv Q \quad \text{mod. } \mathfrak{P}_1,$$

it follows that

$$P^{r_1^u} = Q^{*u}PQ^{*-u} = QPQ^{-1} = P^r,$$

consequently (cf. (7), (8))

$$r_1^u \equiv r, \text{ mod. } p, \quad u \not\equiv 0, \text{ mod. } q.$$

Q generates therefore also a q -Sylowgroup and it is

$$\{P, Q, Q'\} = \{\mathfrak{P}_1, Q\}.$$

Any element of q -power order is thus contained in the subgroup $\{\mathfrak{P}, Q\}$. $\{\mathfrak{P}, Q\}$ is therefore a characteristic subgroup of $\mathfrak{G}$. From above considerations we obtain the following theorem which corresponds to 4 in §1.

Theorem 2. An M -group $\mathfrak{G}$ which satisfies the assumption stated at the beginning of this paragraph is the direct product of following groups:

- (α) The M -group in which any element has an order which is a power of a fixed prime number.
- (β) The group $\{\mathfrak{P}, Q\}$, where $\mathfrak{P}$ is an abelian group whose elements satisfy the relation

$$X^p = 1,$$

and Q is an element of q -power order. p, q means then two different prime numbers. Between Q and an arbitrary element P of $\mathfrak{P}$ it holds

$$QPQ^{-1} = P^r, \quad r \not\equiv 1, \text{ mod. } p, \quad r^q \equiv 1, \text{ mod. } p,$$

where r is an integer depending only upon $\{\mathfrak{P}, Q\}$.

The orders of elements contained in different direct factors must be prime to each other.

Conversely any group, which has the structure mentioned above, is an M -group which satisfies our assumption.

The last part of the theorem is easily seen from 3, 4 in §1.

2. According to Theorem 2 it suffices to investigate only such M -groups any of whose elements has an order which is a power of a fixed prime number.

We first consider a 2-group $\mathfrak{G}$ which contains a quaternion-group $\mathfrak{Q}$. Let A, B be any two elements of the group and put $\mathfrak{G}_1 = \{\mathfrak{Q}, A, B\}$. According to 2 in §1, $\mathfrak{G}_1$ is a Hamiltonian 2-group and it holds

$$BAB^{-1} = A^a, \quad ABA^{-1} = B^b.$$

The whole group $\mathfrak{G}$ is therefore also Hamiltonian and is the direct product of $\mathfrak{Q}$ and an abelian group of exponent 2. Conversely any such group is obviously an M -group.

Now let $\mathfrak{G}$ be a modular p -group which is neither abelian nor Hamiltonian. By the assumption $\mathfrak{G}$ contains a finite non-abelian subgroup $\mathfrak{G}_1$. We consider any finite subgroup $\mathfrak{G}_2$ of $\mathfrak{G}$ containing $\mathfrak{G}_1$.

The structure of $\mathfrak{G}_2$ is given by (i), (ii), (iii) in 1 of §1. We will write

$$(9) \quad \mathfrak{G}_2 = \{\mathfrak{A}_2, T, s\},$$

if $\mathfrak{G}_2$ has an abelian normal subgroup $\mathfrak{A}_2$ and

$$\mathfrak{G}_2/\mathfrak{A}_2 = \{T\}, \quad TAT^{-1} = A^{1+p^s} \quad \text{for all } A \text{ in } \mathfrak{A}_2.$$

The expression (9) may not be unique for $\mathfrak{G}_2$, that is to say, it may be also written in the form

$$\mathfrak{G}_2 = \{\mathfrak{A}_2^*, T^*, s^*\}$$

with some other $\mathfrak{A}_2^*, T^*, s^*$. But, as $\mathfrak{G}_2$ is not abelian the maximum of these $s, s^*, \dots$ is surely determined by $\mathfrak{G}_2$ and we denote it by $s(\mathfrak{G}_2)$.

Now let s_0 be the minimum of all $s(\mathfrak{G}_2)$ when $\mathfrak{G}_2$ goes round over all finite subgroups of $\mathfrak{G}$ containing $\mathfrak{G}_1$. We choose such $\mathfrak{G}_3$, that

$$\mathfrak{G}_3 = \{\mathfrak{A}_3, T_3, s_3\}, \quad s_3 = s(\mathfrak{G}_3) = s_0.$$

Take any finite subgroup $\mathbb{G}_4$ containing $\mathbb{G}_3$, and let

$$\mathbb{G}_4 = \{\mathcal{U}_4, T_4, s_4\}, \quad s_4 = s(\mathbb{G}_4).$$

If we put

$$\mathbb{G}_3 \cap \mathcal{U}_4 = \mathcal{U}_3^*, \quad \mathbb{G}_3 \cup \mathcal{U}_4 = \mathbb{G}_4^*, \quad [\mathbb{G}_4 : \mathbb{G}_4^*] = p^u,$$

we have then

$$\mathbb{G}_4^* / \mathcal{U}_4 \cong \mathbb{G}_3 / \mathcal{U}_3^*, \quad \mathbb{G}_3 = \{\mathcal{U}_3^*, T_3^*, s_4 + u\}.$$

From

$$s_4 + u \leq s_3, \quad s_3 = s_0 \leq s_4$$

it follows

$$s_3 = s_4 = s_0, \quad u = 0,$$

that is to say,

$$s(\mathbb{G}_4) = s_0, \quad \mathbb{G}_3 \cup \mathcal{U}_4 = \mathbb{G}_4, \quad \mathbb{G}_4 / \mathcal{U}_4 \cong \mathbb{G}_3 / \mathcal{U}_3^*,$$

$$\mathbb{G}_4 = \{\mathcal{U}_4, T_3^*, s_0\}.$$

If the order of T_3^* is p^l , we have for any element A_4 of $\mathcal{U}_4$

$$A_4 = T_3^{*p^l} A_4 T_3^{*-p^l} = A_4^{(1+p^{s_0})p^l}.$$

The order of A_4 is therefore at most p^{s_0+l} , and the orders of elements of $\mathbb{G}_4$ also do not exceed p^{s_0+l} ⁽⁷⁾. But the number p^{s_0+l} depends only on $\mathbb{G}_3$, and $\mathbb{G}_4$ could be arbitrarily chosen. The orders of elements of $\mathbb{G}$ are therefore bounded.

Now let $\mathbb{G}_4$ be, as before, any finite subgroup containing $\mathbb{G}_3$. We suppose that $\mathbb{G}_4$ can be expressed in two different ways:

$$\begin{aligned} \mathbb{G}_4 &= \{\mathcal{U}_4, T_4, s_0\} \\ &= \{\mathcal{U}_4^*, T_4^*, s_0\}. \end{aligned}$$

It is then easy to see, that the commutator group $\mathbb{G}'_4$ of $\mathbb{G}_4$ is given by

$$\mathbb{G}'_4 = \mathcal{U}_4^{p^{s_0}} = \mathcal{U}_4^{*p^{s_0}},$$

where $\mathcal{U}_4^{p^{s_0}}$ or $\mathcal{U}_4^{*p^{s_0}}$ is the group generated by all p^{s_0} -power of elements of $\mathcal{U}_4$ or $\mathcal{U}_4^*$. The maximum of orders of elements of $\mathcal{U}_4$ and $\mathcal{U}_4^*$ is therefore equal to each other and is uniquely determined by $\mathbb{G}_4$. We denote this by $o(\mathbb{G}_4)$. Let p^k be the maximum of $o(\mathbb{G}_4)$, for all $\mathbb{G}_4$ containing $\mathbb{G}_3$. This is surely determined, as the orders of elements of $\mathbb{G}$ are bounded. For some fixed $\mathbb{G}_5 \geq \mathbb{G}_3$, we have then $o(\mathbb{G}_5) = p^k$.

(7) See G. V. Hilfssatz 18.

Now let

$$(10) \quad \mathfrak{A}_5^{(1)}, \mathfrak{A}_5^{(2)}, \dots, \mathfrak{A}_5^{(r)}$$

be all the abelian normal subgroups of $\mathfrak{G}_5$, such that

$$\mathfrak{G}_5 = \{\mathfrak{A}_5^{(i)}, T_5^{(i)}, s_0\}, \quad i = 1, 2, \dots, r.$$

We prove, that if we choose suitable $\mathfrak{A}_5^{(i_0)}$, we can find for any $\mathfrak{G}_6 \supseteq \mathfrak{G}_5$ an abelian normal subgroup $\mathfrak{A}_6$, such that

$$\mathfrak{A}_6 \supseteq \mathfrak{A}_5^{(i_0)}, \quad \mathfrak{G}_6 = \{\mathfrak{A}_6, T_6, s_0\}.$$

Suppose by the contrary that there exists no such $\mathfrak{A}_5^{(i_0)}$ in (10). Then we can find for any $\mathfrak{A}_5^{(i)}$ a finite subgroup $\mathfrak{G}_6^{(i)}$, which has no abelian normal subgroup $\mathfrak{A}_6^{(i)}$ with conditions

$$\mathfrak{G}_6^{(i)} = \{\mathfrak{A}_5^{(i)}, T_6^{(i)}, s_0\}, \quad \mathfrak{A}_6^{(i)} \supseteq \mathfrak{A}_5^{(i)}.$$

Put

$$\mathfrak{G}_6^* = \mathfrak{G}_6^{(1)} \cup \mathfrak{G}_6^{(2)} \cup \dots \cup \mathfrak{G}_6^{(r)}, \quad \mathfrak{G}_6^* = \{\mathfrak{A}_6^*, T_6^*, s_0\}, \quad \mathfrak{A}_6^* = \mathfrak{A}_5^* \cap \mathfrak{G}_6^*.$$

It follows then

$$\mathfrak{G}_5 = \{\mathfrak{A}_5^*, T_5^*, s_0\},$$

and $\mathfrak{A}_5^*$ is therefore one of $\mathfrak{A}_5^{(i)}$ in (10): $\mathfrak{A}_5^* = \mathfrak{A}_5^{(i_0)}$. Now $\mathfrak{G}_6^{(i_0)}$ can be written in the form

$$\mathfrak{G}_6^{(i_0)} = \{\mathfrak{A}_6^{(i_0)}, T_6^{(i_0)}, s_0\},$$

with

$$\mathfrak{A}_6^{(i_0)} = \mathfrak{A}_5^* \cap \mathfrak{G}_6^{(i_0)} \supseteq \mathfrak{A}_5^* \cap \mathfrak{G}_5 = \mathfrak{A}_5^{(i_0)},$$

which contradicts our assumption.

We have thus found a finite subgroup $\mathfrak{G}_5 = \mathfrak{G}^*$ with following properties:

(α) $\mathfrak{G}^*$ is expressed in the form

$$\mathfrak{G}^* = \{\mathfrak{A}^*, T, s_0\}.$$

(β) Any finite subgroup $\mathfrak{G}_6$, which contains $\mathfrak{G}^*$, can be expressed in the form

$$\mathfrak{G}_6 = \{\mathfrak{A}_6, T_6, s_0\}, \quad \mathfrak{A}_6 \supseteq \mathfrak{A}^*, \quad \mathfrak{G}_6 = \mathfrak{A}_6 \cup \mathfrak{G}^*$$

(γ) $o(\mathfrak{G}^*) = p^k = \text{Max. } o(\mathfrak{G}_4).$

As $\mathfrak{G}_6 = \mathfrak{A}_6 \cup \mathfrak{G}^* = \{\mathfrak{A}_6, T\}$ we can put moreover in (β) $T_6 = T$.

Now let $\mathfrak{G}_7, \mathfrak{G}_8$ be any finite subgroups such that

$$\begin{aligned}\mathfrak{G}_8 &\supseteq \mathfrak{G}_7 \supseteq \mathfrak{G}^*, \\ \mathfrak{G}_7 &= \{\mathfrak{U}_7, T, s_0\}, \quad \mathfrak{U}_7 \supseteq \mathfrak{U}^* \\ \mathfrak{G}_8 &= \{\mathfrak{U}_8, T, s_0\}, \quad \mathfrak{U}_8 \supseteq \mathfrak{U}^*.\end{aligned}$$

Put

$$\mathfrak{U}_7 \cup \mathfrak{U}_8 = \{\mathfrak{U}_8, T^{p^u}\}, \quad T^{p^u} = A_7 A_8, \quad A_7 \in \mathfrak{U}_7, \quad A_8 \in \mathfrak{U}_8.$$

Take an element A_0 of order p^k from $\mathfrak{U}^*$. As $\mathfrak{U}^*$ is contained in $\mathfrak{U}_7 \cap \mathfrak{U}_8$, we have

$$A_0^{(1+p^{s_0})p^u} = T^{p^u} A_0 T^{-p^u} = A_7 A_8 A_0 A_8^{-1} A_7^{-1} = A_0,$$

and consequently

$$(11) \quad s_0 + u \geq k.$$

As the order of any element $\mathfrak{U}_8$ is at most p^k by the assumption, it is easy to see from (11) that T^{p^u} is commutative with any element contained in $\mathfrak{U}_8$. $\mathfrak{U}_7 \cup \mathfrak{U}_8$ is therefore an abelian group and we can write

$$\mathfrak{G}_8 = \{\mathfrak{U}_7 \cup \mathfrak{U}_8, T, s_0\}.$$

If we take $\mathfrak{G}_7 = \mathfrak{G}_8$, above consideration shows that there is unique maximal abelian normal subgroup $\mathfrak{U}_8$ such that

$$\mathfrak{G}_8 = \{\mathfrak{U}_8^*, T, s_0\}, \quad \mathfrak{U}_8^* \supseteq \mathfrak{U}^*.$$

In the following if any $\mathfrak{G}_9 \supseteq \mathfrak{G}^*$ is expressed in the form

$$\mathfrak{G}_9 = \{\mathfrak{U}_9, T, s_0\},$$

we take then always as $\mathfrak{U}_9$ the maximal abelian normal subgroup containing $\mathfrak{U}^*$.

For any finite subgroups $\mathfrak{G}_9, \mathfrak{G}_{10}$ with

$$\begin{aligned}\mathfrak{G}_{10} &\supseteq \mathfrak{G}_9 \supseteq \mathfrak{G}^*, \\ \mathfrak{G}_9 &= \{\mathfrak{U}_9, T, s_0\}, \quad \mathfrak{G}_{10} = \{\mathfrak{U}_{10}, T, s_0\},\end{aligned}$$

it is then easy to see from above consideration, that

$$(12) \quad \mathfrak{U}_9 = \mathfrak{G}_9 \cap \mathfrak{U}_{10}.$$

Now for arbitrary elements X, Y in $\mathfrak{G}$, put

$$\mathbb{G}_X = \{\mathbb{G}^*, X\} = \{\mathfrak{A}_X, T, s_0\}$$

$$\mathbb{G}_Y = \{\mathbb{G}^*, Y\} = \{\mathfrak{A}_Y, T, s_0\}$$

$$\mathbb{G}_{X,Y} = \{\mathbb{G}^*, X, Y\} = \{\mathfrak{A}_{X,Y}, T, s_0\}.$$

It follows from (12) that

$$\mathfrak{A}_X = \mathfrak{A}_{X,Y} \cap \mathbb{G}_X, \quad \mathfrak{A}_Y = \mathfrak{A}_{X,Y} \cap \mathbb{G}_Y.$$

As $\mathfrak{A}_{X,Y}$ is abelian, elements of $\mathfrak{A}_X$ and $\mathfrak{A}_Y$ are commutative with one another. The group

$$\mathfrak{A} = \bigcup_{X \in \mathbb{G}} \mathfrak{A}_X$$

is accordingly an abelian group, and for any element A in $\mathfrak{A}$ we have

$$TAT^{-1} = A^{1+p^{s_0}}.$$

It is also clear that

$$\mathbb{G} = \{\mathfrak{A}, T\}.$$

We have thus proved the first half of the following theorem, which is an extension of results 1, 2 of §1 in the case of infinite groups.

Theorem 3. A non-abelian p -group⁽⁸⁾ $\mathbb{G}$, whose subgroups of finite length are all finite, is an M -group, if and only if it has the following structure.

(a) $p > 2$.

- (i) $\mathbb{G}$ contains an abelian normal subgroup $\mathfrak{A}$. The order of elements of $\mathfrak{A}$ is bounded.
- (ii) $\mathbb{G}/\mathfrak{A}$ is a cyclical group of order p^m .
- (iii) For a suitable generator T of $\mathbb{G}/\mathfrak{A}$ we have for any element A in $\mathfrak{A}$

$$TAT^{-1} = A^{1+p^s},$$

where s means an integer which is uniquely determined by $\mathbb{G}$ and $\mathfrak{A}$ and satisfies the inequality

$$s + m \geq n,$$

if the maximum of the order of elements in $\mathfrak{A}$ is p^n .

- (iv) $T^m = T_0$ is an element of $\mathfrak{A}$ and it holds

$$T_0^{p^s} = 1.$$

(8) A group is called p -group generally when the orders of its elements are all p -powers.

(β) $p = 2$.

$\mathfrak{G}$ is either a Hamiltonian group, or a group which has the same structure as mentioned in (α) with an additional condition $s \geq 2$.

Corollary. A modular p -group, whose subgroups of finite length are finite, is either abelian or meta-abelian.

Proof. We have only to prove the second half. It is easy to see that in any group $\mathfrak{G}$, which has the structure mentioned above, subgroups of finite length are all finite. Let A, B be any element of $\mathfrak{G}$. The finite group $\{A, B\}$ is then of type 1 (or 2) in §1. There exists consequently such integers x, y that

$$BA = A^x B^y.$$

$\mathfrak{G}$ is therefore quasi-Hamiltonian⁽⁹⁾, accordingly modular a fortiori.

In a quasi-Hamiltonian group any subgroup of finite length is, as readily to be seen, finite. If we remark therefore that a finite quasi-Hamiltonian group is the direct product of their Sylowgroups and the groups given in Theorem 3 are all quasi-Hamiltonian, we have immediately the following

Theorem 4. A group, whose elements have all finite orders, is quasi-Hamiltonian, if and only if it is the direct product of an abelian group and such groups, which have the structure stated in Theorem 3, where the orders of elements of different direct factors are prime to each other. A quasi-Hamiltonian group is therefore always either abelian or meta-abelian.

§ 3. M -groups which contain elements of infinite orders.

1. We now determine the structure of M -groups, which contain elements of infinite orders. This time we can carry out our investigation without any assumption.

Lemma 2. Let A, B be any two elements of an M -group $\mathfrak{G}$, of which A has an infinite order. If $\{A\} \cap \{B\} = 1$, then

$$(13) \quad \{A, B\}, \{A^2, B\}, \{A^3, B\}, \dots, \{A^n, B\}, \dots, \{B\}$$

are different from one another and exhaust all subgroups of $\mathfrak{G}$ which lie between $\{A, B\}$ and $\{B\}$.

(9) A group $\mathfrak{G}$ is called "quasi-Hamiltonian", if for any subgroups $\mathfrak{A}, \mathfrak{B}$ we have

$$\mathfrak{A}\mathfrak{B} = \mathfrak{B}\mathfrak{A} = \mathfrak{A} \cup \mathfrak{B}.$$

For the relation between an M -group and a quasi-Hamiltonian group see G. V. § 3.

Proof. Put $\mathfrak{A} = \{A\}$, $\mathfrak{B} = \{B\}$ and apply (2). As $\{A\} \cap \{B\} = 1$ and the subgroups of $\{A\}$ are given by

$$\{A\}, \{A^2\}, \{A^3\}, \dots, \{A^n\}, \dots, \{1\},$$

we can immediately obtain the lemma.

By help of this we prove the following

Lemma 3. Let A be any element of infinite order and B any element of finite order of an M -group $\mathfrak{G}$. It holds then in taking suitably an integer r

$$(14) \quad ABA^{-1} = B^r, \quad (r, m) = 1,$$

where m is the order of B .

Proof. The group $\{B, ABA^{-1}\}$ lies between $\{A, B\}$ and $\{B\}$ and is therefore one of the subgroups (13). But as it is generated by elements of finite orders, it contains no element of infinite order (cf. Theorem 1). It must be then $\{B, ABA^{-1}\} = \{B\}$ and we can readily obtain (14).

Lemma 4. Let A, B be any two elements of an M -group $\mathfrak{G}$, of which A has an infinite order. If it holds for suitable integers α, β

$$(15) \quad BA^\alpha B^{-1} = A^\beta,$$

then it must be $\alpha = \beta$ and A^α commutes with B .

Proof. If $\{A\} \cap \{B\} = \{A^\gamma\} \neq 1$, then it follows from (15)

$$A^{\alpha\gamma} = BA^{\alpha\gamma}B^{-1} = A^{\beta\gamma}$$

whence $\alpha\gamma = \beta\gamma$, $\alpha = \beta$. Let $\{A\} \cap \{B\} = 1$. It is

$$\{A^\alpha, B\} = \{A^\beta, B\}$$

and from Lemma 2 we conclude $\alpha = \pm\beta$. Assume $\alpha = -\beta$. From Lemma 3 it follows easily that B has an infinite order. The group $\{A^\alpha, B\}/\{A^{4\alpha}, B^2\}$ is then a dihedral group, which is not modular. This contradicts to our assumption that $\mathfrak{G}$ is an M -group. It must be therefore $\alpha = \beta$ and $A^\alpha B = BA^\alpha$.

We now study the structure of M -groups which contain elements of infinite orders.

Theorem 5. Let $\mathfrak{G}$ be an M -group which contains elements of infinite orders. The group $\mathfrak{G}$, which consists of all elements of finite orders of $\mathfrak{G}$, is then an abelian group.

Proof. Let Z be an element of infinite order and A, B be any two elements of $\mathfrak{G}$. AZ is then also of infinite order: otherwise the order of Z would be finite (cf. Theorem 1). If we denote the order of B by m , it is then from Lemma 3

$$ZBZ^{-1} = B^r, \quad (AZ)B(AZ)^{-1} = B^{r'}, \quad (rr', m) = 1.$$

Consequently

$$(16) \quad AB^rA^{-1} = B^{r'}.$$

This shows that $\mathfrak{G}$ is either abelian or Hamiltonean. If $\mathfrak{G}$ is Hamiltonean it contains a quaternion group $\mathfrak{Q}$. By Lemma 3 Z gives an automorphism of finite order in $\mathfrak{Q}$:

$$Z\mathfrak{Q}Z^{-1} = \mathfrak{Q}.$$

A suitable power Z_0 of Z is therefore commutative with every element of $\mathfrak{Q}$. $\{Z_0, \mathfrak{Q}\}/\{Z_0^4\}$ is then a 2-group which is not modular (cf. 2 in §1). We thus come to a contradiction and $\mathfrak{G}$ must be abelian.

2. We consider next $\mathfrak{G}/\mathfrak{G}$, that is to say, such M -groups, which contain no element of finite order except the identity. We first prove a lemma, which is a special case of the assumption stated in §§1, 2.

Lemma 5. An M -group which is generated by two elements of order 2 is a finite group.

Proof. Let $\mathfrak{G} = \{A, B\}$, $A^2 = B^2 = 1$. As any element of $\mathfrak{G}$ has a finite order according to Theorem 1, put

$$C = AB, \quad C^m = 1.$$

It is then $\mathfrak{G} = \{A, C\}$ and

$$A^{-1}CA = C^{-1}.$$

The order of $\mathfrak{G}$ is therefore at most $2m$.

The structure of $\mathfrak{G}/\mathfrak{G}$ is then given by the following theorem.

Theorem 6. An M -group which contains no element of finite order except the identity is abelian.

The proof is rather complicated. We divide it into two parts, the latter of which is available for any M -group.

Lemma 6. Let A and B be elements of an M -group which contains no element of finite order except the identity. If $\{A\} \cap \{B\} \neq 1$, then the subgroup $\{A, B\}$ is cyclical.

Lemma 7. Let A and B be elements of infinite orders of an M -group. If $\{A\} \cap \{B\} = 1$, then A and B are commutative with one another ;

$$AB = BA.$$

Proof of Lemma 6. Clearly it is sufficient to prove that $\{A, B\}$ is abelian.

Let

$$\{A\} \cap \{B\} = \{Z\}, \quad A^a = Z$$

and suppose $A \neq BAB^{-1}$. As

$$A^a = (BAB^{-1})^a, \quad \{A\} \cap \{BAB^{-1}\} \neq 1,$$

we put

$$\{A\} \cap \{BAB^{-1}\} = \{C\}, \quad C = A^a = BA^a B^{-1}.$$

From Lemma 4 we have $a = a'$. Therefore if we denote $A_1 = A$, $A_2 = BAB^{-1}$, it holds

$$A_1^a = A_2^a = C, \quad \{A_1\} \cap \{A_2\} = \{C\}.$$

As the M -group $\{A_1, A_2\}/\{C\}$ is generated by two elements of finite orders, it contains no element of infinite order. There is consequently such $\gamma (\neq 0)$, that

$$(A_1 A_2^{-1})^\gamma = C^\gamma.$$

Let

$$\mathfrak{A} = \{(A_1 C^\gamma)\}, \quad \mathfrak{B} = \{(A_2 C^\gamma)\}, \quad \mathfrak{C} = \{A_1\}.$$

It is then $\mathfrak{A} \not\subseteq \mathfrak{C}$ and from $\mathfrak{B} \cap \mathfrak{C} \subseteq \{A_1\} \cap \{A_2\} = \{C\}$ we can readily see that $\mathfrak{B} \cap \mathfrak{C} = \{(A_2 C^\gamma)^a\} = \{C^{1+a\gamma}\}$. As $(A_1 C^\gamma)^a = C^{1+a\gamma}$ it is also $\mathfrak{B} \cap \mathfrak{A} = \{C^{1+a\gamma}\}$. Now $\mathfrak{A} \cup \mathfrak{B}$ contains $(A_1 C^\gamma)(A_2 C^\gamma)^{-1} = A_1 A_2^{-1}$, therefore $\mathfrak{A} \cup \mathfrak{B} = \{A_1 C^\gamma, A_2 C^\gamma, C^\gamma\} = \{A_1, A_2\} = \mathfrak{B} \cup \mathfrak{C}$. We have thus

$$\mathfrak{A} \subseteq \mathfrak{C}, \quad \mathfrak{A} \cap \mathfrak{B} = \mathfrak{C} \cap \mathfrak{B}, \quad \mathfrak{A} \cup \mathfrak{B} = \mathfrak{C} \cup \mathfrak{B}.$$

From (1) we conclude $\mathfrak{A} = \mathfrak{C}$, but this is clearly a contradiction.

Remark that γ is not zero as $A_1 A_2^{-1}$ is of infinite order. We used here essentially the assumption that the group has no element of finite order except the identity.

Proof of Lemma 7. We put $\mathfrak{G} = \{A, B\}$ and prove that $\mathfrak{G}$ is abelian. For that purpose we must first prove the following

Lemma 8. Let $\mathfrak{G} = \{A, B\}$ be an M -group as above defined. If $\mathfrak{G}$ has an abelian normal subgroup $\mathfrak{A}$ with a finite index, then $\mathfrak{G}$ itself is abelian.

Proof. We remark first that $\mathfrak{G}$ contains no element of finite order except the identity: for if $Z \neq 1$ is any of such elements we have

$$\{A, Z\} = \{A, B^m\},$$

and there exist infinitely many subgroups between $\{A, Z\}$ and $\{A\}$ (cf. Lemma 2). But this contradicts to the lattice isomorphism

$$\{A, Z\}/\{A\} \cong \{Z\}/\{A\} \cap \{Z\}.$$

Now according to the assumption there is suitable integers α, β such that

$$A^\alpha, B^\beta \in \mathfrak{A}, \quad A^\alpha B^\beta = B^\beta A^\alpha.$$

Hence we have $\{A\} \cap \{B^\beta A B^{-\beta}\} \neq 1$. If $A \neq B^\beta A B^{-\beta}$, then we come to a contradiction as in the proof of Lemma 6. We must have therefore

$$A = B^\beta A B^{-\beta} \quad \text{or} \quad B^\beta = A^{-1} B^\beta A.$$

From $\{B\} \cap \{A^{-1} B A\} \neq 1$ we have again similarly

$$B = A^{-1} B A \quad \text{or} \quad A B = B A.$$

We now prove Lemma 7. Denote

$$\mathfrak{G} = \{A, B\}, \quad \mathfrak{G}_1 = \{A B A^{-1}, B\}, \quad \mathfrak{G}_2 = \{A, B^2\}, \quad \mathfrak{G}_3 = \{A B^2 A^{-1}, B^2\}.$$

By Lemma 2 we have

$$(17) \quad \mathfrak{G}_1 = \{A^\alpha, B\} \quad \text{or} \quad \mathfrak{G}_1 = \{B\}.$$

As $A B A^{-1}$ is contained in $\mathfrak{G}_1$, A is a normaliser of $\mathfrak{G}_1$ and $\mathfrak{G}_1$ is accordingly normal in $\mathfrak{G}$. In the same way we can see that $\mathfrak{G}_3$ is normal in $\mathfrak{G}_2$. From $\mathfrak{G}_3 = \{(A B) B^2 (A B)^{-1}, B^2\}$ it is also normal in $\{A B, B^2\}$, consequently in $\mathfrak{G} = \{A, A B, B^2\}$. As $\mathfrak{G}_1/\mathfrak{G}_3$ is generated by two elements of order 2 it is a finite group according to Lemma 5.

We first assume that $\mathfrak{G}/\mathfrak{G}_3$ is infinite. $\mathfrak{G}/\mathfrak{G}_1$ is then also infinite and from (17) we have $\mathfrak{G}_1 = \{B\}$: otherwise $\mathfrak{G}/\mathfrak{G}_1$ would be of order α . It follows $A B A^{-1} = B^\beta$ and by Lemma 4 $A B = B A$, that is to say, $\mathfrak{G}$ is abelian. Next let $\mathfrak{G}/\mathfrak{G}_3$ be finite. As $\mathfrak{G}_3 \subseteq \mathfrak{G}_2$ and $\mathfrak{G} \neq \mathfrak{G}_2$ (cf. Lemma 2), $\mathfrak{G}/\mathfrak{G}_3$ is not the identical group. As any finite M -group is meta-abelian (cf. §1) we see from this that the commutator group $\mathfrak{G}'$ of $\mathfrak{G}$ does not coincide with $\mathfrak{G}$: $\mathfrak{G} \neq \mathfrak{G}'$. If $\mathfrak{G}' \subseteq \{A\}$ and $\mathfrak{G}' \subseteq \{B\}$ it follows then from $\{A\} \cap \{B\} = 1$ that $\mathfrak{G}' = 1$ and that $\mathfrak{G}$ is abelian. We assume therefore for instance $\mathfrak{G}' \not\subseteq \{A\}$. From $\{A\} \neq \{A\} \cup \mathfrak{G}'$ we have then by Lemma 2

$$\{A\} \cup \mathfrak{G}' = \{A, B^v\}, \quad v \neq 0.$$

As $\{A\} \cup \mathfrak{G}'/\mathfrak{G}'$ is a cyclic group generated by $\bar{A}$, there exists suitable u such that

$$A^u \equiv B^v \pmod{\mathfrak{G}'}$$

$B_1 = A^u B^{-v}$ is then contained in $\mathfrak{G}'$ and $\{A\} \cup \mathfrak{G}' = \{A, B^v\} = \{A, B_1\}$. If $\{A\} \cap \{B_1\} \neq 1$, then it follows from Lemma 6 that $\{A\} \cup \mathfrak{G}'$ is abelian (cf. the above remark), and as $\mathfrak{G}/\{A\} \cup \mathfrak{G}'$ is finite, $\mathfrak{G}$ is also abelian according to Lemma 8.

Let therefore be

$$\{A\} \cap \{B_1\} = 1.$$

As $\mathfrak{G}'$ is a subgroup of $\{A, B_1\}$ and contains $\{B_1\}$ it is

$$\mathfrak{G}' = \{A^n, B_1\} \quad \text{or} \quad \mathfrak{G}' = \{B_1\}$$

according to Lemma 2.

Assume first $\mathfrak{G}' = \{B_1\}$. By Lemma 4 it is easy to see that B_1 is contained in the center of $\mathfrak{G}$ and that $\{A\} \cup \mathfrak{G}'$ is abelian. $\mathfrak{G}$ itself is then an abelian group according to Lemma 8. We assume therefore

$$\mathfrak{G}' = \{A^n, B\}.$$

$\mathfrak{G}/\mathfrak{G}'$ is then a finite group. In this case $\mathfrak{G}'$ is not abelian: otherwise $\mathfrak{G}$ would be abelian and $\mathfrak{G}' = 1$ according to Lemma 8.

Now $\mathfrak{G}'$ have the same structure as $\mathfrak{G}$. If we denote the commutator group of $\mathfrak{G}'$ by $\mathfrak{G}''$, $\mathfrak{G}'/\mathfrak{G}''$ is also finite, but not the identical group. $\mathfrak{G}''/\mathfrak{G}'''$ is again finite, where $\mathfrak{G}'''$ is the commutator group of $\mathfrak{G}''$. $\mathfrak{G}/\mathfrak{G}'''$ is then also a finite M -group. But according to §1, 1-4 any finite M -group is meta-abelian: we have thus met a contradiction. $\mathfrak{G}$ must be consequently abelian in any case.

Theorem 6 is now clear from these two lemmas.

Let $\mathfrak{G}$ be any M -group, which contains elements of infinite orders, and $\mathfrak{E}$ be the normal subgroup of $\mathfrak{G}$ which consists of all elements of finite order in $\mathfrak{G}$. By Theorem 5, 6 $\mathfrak{E}$ and $\mathfrak{G}/\mathfrak{E}$ are both abelian groups. It remains therefore only to investigate how $\mathfrak{E}$ is extended by an abelian group which contains no element of finite order except the identity.

Suppose first that the rank of $\mathfrak{G}/\mathfrak{E}$ is at least 2. Then there exists in $\mathfrak{G}$ two elements A, B of infinite orders such that

$$(18) \quad \{A\} \cap \{B\} = 1, \quad AB = BA.$$

Let C be any element of infinite order in $\mathfrak{G}$. It is then by (18)

$$\{A\} \cap \{C\} = 1 \quad \text{or} \quad \{B\} \cap \{C\} = 1.$$

Suppose for instance

$$(19) \quad \{A\} \cap \{C\} = 1, \quad AC = CA.$$

Let D be another element of infinite order. If $\{C\} \cap \{D\} = 1$, we have

$$CD = DC.$$

If $\{C\} \cap \{D\} \neq 1$, it follows then from (19) $\{AD\} \cap \{C\} = 1$ and $(AD)C = C(AD)$. We have again by (19)

$$(20) \quad CD = DC.$$

Elements of infinite orders are therefore commutative with one another. Now let E be any element of finite order. Then AE is of infinite order (cf. Theorem 1) and from (20) we obtain

$$(AE)C = C(AE)$$

that is,

$$(21) \quad EC = CE.$$

By (20), (21) and Theorem 5 we see that $\mathfrak{G}$ is abelian.

Theorem 7. Let $\mathfrak{G}$ be any M -group and $\mathfrak{E}$ be the normal subgroup of $\mathfrak{G}$ which consists of all elements of finite orders in $\mathfrak{G}$. If the abelian group $\mathfrak{G}/\mathfrak{E}$ has a rank ≥ 2 , then $\mathfrak{G}$ itself is abelian.

It is sufficient therefore to observe the case that the rank of $\mathfrak{G}/\mathfrak{E}$ is 1. Suppose first that $\mathfrak{G}/\mathfrak{E}$ is an infinite cyclic group: $\mathfrak{G}/\mathfrak{E} = \{\bar{Z}\}$.

Let $\mathfrak{P}$ be the p -component of $\mathfrak{E}$, that is to say, the subgroup of $\mathfrak{E}$ which consists of all elements of p -power order in $\mathfrak{E}$. We denote further by $\mathfrak{P}_k (k = 0, 1, 2, \dots)$ the subgroup of $\mathfrak{P}$ which consists of elements satisfying the relation

$$X^{p^k} = 1.$$

We prove that for any element in $\mathfrak{P}_n$ we have

$$(22) \quad ZAZ^{-1} = A^{r_n},$$

where r_n is uniquely determined mod. p^n by $\mathfrak{P}_n$. This is clear for $n=0$. We prove therefore by induction, assuming (22) for $n=k$. Take any element B of order p^{k+1} . From Lemma 3

$$ZBZ^{-1} = B^r.$$

According to

$$B^p \in \mathfrak{P}_k, \quad ZB^pZ^{-1} = (B^p)^r = (B^p)^{r_k},$$

it is then

$$(23) \quad r \equiv r_k \pmod{p^k}.$$

Hence for an arbitrary element U of $\{B, \mathfrak{P}_k\}$ we have

$$ZUZ^{-1} = U^r.$$

Let C be another element of order p^{k+1} . If $\{B\} \cap \{C\} \neq 1$, then C is contained in $\{B, \mathfrak{P}_k\}$ and we have

$$ZCZ^{-1} = C^r.$$

Let

$$\{B\} \cap \{C\} = 1, \quad ZCZ^{-1} = C^{r'}, \quad Z(BC)Z^{-1} = (BC)^{r''},$$

then

$$B^{r''} C^{r''} = B^r C^{r'}, \quad r'' \equiv r' \equiv r \pmod{p^{k+1}},$$

that is to say,

$$ZCZ^{-1} = C^r.$$

For any element V of $\mathfrak{P}_{k+1}$ we have thus

$$ZVZ^{-1} = V^{r_{k+1}}$$

with $r_{k+1} = r$.

Now for an element A of order p it holds especially

$$ZAZ^{-1} = A^{r_1}.$$

If $r_1 \not\equiv 1 \pmod{p}$ then by taking a suitable power Z_1 of Z we have

$$Z_1 A Z_1^{-1} = A^t, \quad t \not\equiv 1 \pmod{p}, \quad t^q \equiv 1 \pmod{p},$$

where q is a prime number different from p .

But in this case we can easily find by simple calculation that the group $\{Z_1, A\}/Z_1^{pq}$ of order p^2q is not an M -group (cf. 3 in §1). This is a contradiction and it must be

$$r_1 \equiv 1 \pmod{p}.$$

In a similar way we find also that

$$r_1 \equiv 1 \pmod{4}$$

for $p = 2$.

Now if it holds $\mathfrak{P} = \mathfrak{P}_k$ for a suitable k we put $\alpha = \alpha(p) = r_k$. But if $\mathfrak{P} \neq \mathfrak{P}_k$ for any k , put

$$\alpha = \alpha(p) = \lim_{k \rightarrow \infty} r_k$$

as the sequence $\{r_k\}$ is always convergent in p -adic sense according to $r_k \equiv r_{k+1} \pmod{p^k}$ (cf. (23)). In either case it is then

$$(24) \quad Z X Z^{-1} = X^{\alpha(p)}$$

for an element X in $\mathfrak{P}$. (Even in the case, where $\alpha(p)$ is a p -adic number the meaning of above equation will be clear.) We come to the conclusion: there exists for any component, say p -component, $\mathfrak{P}$ of $\mathfrak{G}$ a p -adic number $\alpha(p)$ such that

$$Z X Z^{-1} = X^{\alpha(p)}, \quad \alpha(p) \equiv 1 \pmod{p} \quad (\alpha(2) \equiv 1 \pmod{4} \text{ for } p = 2)$$

for any element X of $\mathfrak{P}$.

We prove next that any group $\mathfrak{G} = \{\mathfrak{G}, Z\}$ given by above relation is always an M -group. For that purpose it is sufficient to prove that for arbitrary A, B of $\mathfrak{G}$ there are suitable integers x, y such that

$$(25) \quad AB = B^x A^y.$$

If A or B is contained in $\mathfrak{G}$ this is almost clear. We suppose therefore

$$A = A_1 Z^u, \quad B = B_1 Z^v, \quad A_1, B_1 \in \mathfrak{G}, \quad u, v \neq 0.$$

The group $\mathfrak{H} = \{Z, A_1, B_1\}$ is an infinite cyclic extension of the finite abelian group $\mathfrak{G}_1 = \{A_1, B_1\}$. If we denote by $\mathfrak{P}_i$ a p_i -Sylowgroup of $\mathfrak{G}_1$ ($i = 1, 2, \dots, s$) we have

$$(26) \quad Z A_i Z^{-1} = A_i^{r_i}, \quad r_i \equiv 1 \pmod{p_i} \quad (r_i \equiv 1 \pmod{4} \text{ for } p_i = 2),$$

for any A_i of $\mathfrak{P}_i$ according to (24).

The order of automorphism given by Z in $\mathfrak{P}_i$ is consequently a power of p_i , say $p_i^{n_i}$. $Z_0 = Z^{p_1^{n_1} \cdots p_s^{n_s}}$ is then commutative with all elements of $\mathfrak{G}_1$ and $\{\mathfrak{G}_1, Z_0\}$ is the centraliser of $\mathfrak{G}_1$ in $\mathfrak{H}$. Suppose $\{A\} \cap \{Z\} = \{Z^\mu\}$, $\{B\} \cap \{Z\} = \{Z^\nu\}$. $Z^{\mu\nu}$ is then commutative with A, B , accordingly with A_1, B_1 .

It follows

$$Z^{\mu\nu} \in \{\mathfrak{G}_1, Z_0\}, \quad Z^{\mu\nu} \in \{Z_0\},$$

$$\mu\nu = p_1^{m_1} \cdots p_s^{m_s} k, \quad (k, p_i) = 1, \quad m_i \geq n_i \quad (i = 1, 2, \dots, s).$$

If we put $\bar{\mathfrak{H}} = \mathfrak{H}/\{Z^{\mu\nu}\}$, it is easy to see that $\bar{\mathfrak{H}}$ is the direct product of its Sylowgroups:

$$\bar{\mathfrak{H}} = \{\bar{\mathfrak{P}}_1, \bar{Z}^{p_2^{m_2} \cdots p_s^{m_s} k}\} \times \{\bar{\mathfrak{P}}_2, \bar{Z}^{p_1^{m_1} p_3^{m_3} \cdots p_s^{m_s} k}\} \times \cdots,$$

and these direct factors have the structure stated in §1, 1 (or 2) according to (26). As the nilpotent M -group $\bar{\mathfrak{G}}$ is quasi-Hamiltonian⁽¹⁰⁾ there are suitable integers x_1, y_1 such that

$$\bar{A}\bar{B} = \bar{B}^{x_1}\bar{A}^{y_1},$$

that is,

$$AB \equiv B^{x_1}A^{y_1} \pmod{\{Z^{\mu\nu}\}},$$

$$AB = B^{x_1}A^{y_1}Z^{h\mu\nu}.$$

If $Z^{\mu\nu} = A^l$, then

$$AB = B^{x_1}A^{y+hl} = B^x A^y, \quad x = x_1, \quad y = y_1 + hl.$$

We have thus proved the following theorem.

Theorem 8. Let $\mathfrak{G}$ be an M -group and $\mathfrak{C}$ be the normal subgroup of $\mathfrak{G}$ which consists of all elements of finite order in $\mathfrak{G}$. If $\mathfrak{G}/\mathfrak{C}$ is an infinite cyclic group then $\mathfrak{G}$ has the following structure:

Let Z be a representative of the co-set which generates $\mathfrak{G}/\mathfrak{C}$ and $\mathfrak{P}$ be any component, say p -component, of $\mathfrak{C}$. It holds then for any A of $\mathfrak{P}$

$$(27) \quad ZAZ^{-1} = A^{a(p)}, \quad a(p) \equiv 1 \pmod{p} \quad (a(2) \equiv 1 \pmod{4} \text{ for } p = 2)$$

where $a(p)$ is a p -adic number which is uniquely determined mod. p^n by $\mathfrak{P}$ and Z if the maximum of order of elements in $\mathfrak{P}$ is p^n (evtl. $n = \infty$). Conversely if we extend an arbitrary abelian group $\mathfrak{C}$ which contains only elements of finite orders by an infinite cyclic group $\{Z\}$ with the relation (27) then we obtain a quasi-Hamiltonian group which is then of course an M -group.

We assume next that $\mathfrak{G}/\mathfrak{C}$ is a general abelian group of rank 1. In this case we can find such normal series of $\mathfrak{G}$

$$(28) \quad \mathfrak{C} < \mathfrak{G}_1 < \mathfrak{G}_2 < \dots < \mathfrak{G},$$

that $\mathfrak{G}_1/\mathfrak{C}$ is an infinite cyclic group and $\mathfrak{G}_{i+1}/\mathfrak{G}_i$ ($i = 1, 2, \dots$) is a cyclic group of a prime order; $[\mathfrak{G}_{i+1} : \mathfrak{G}_i] = p_i$ ($i = 1, 2, \dots$). Now any $\mathfrak{G}_i$ has the structure given in Theorem 8. We put therefore

$$(29) \quad \mathfrak{G}_i/\mathfrak{C} = \{\bar{Z}_i\}, \quad Z_i A Z_i^{-1} = A^{a_i(p)}$$

$$a_i(p) \equiv 1 \pmod{p} \quad (a_i(p) \equiv 1 \pmod{4} \text{ for } p = 2),$$

for any A of the p -component $\mathfrak{P}$ of $\mathfrak{C}$. $a_i(p)$ is uniquely determined mod. p^n if the maximum of order of elements in $\mathfrak{P}$ is p^n (evtl. $n = \infty$). Between two successive $\mathfrak{G}_i, \mathfrak{G}_{i+1}$ it holds

(10) See G. V. Satz 7.

$$(30) \quad a_{i+1}(p)^{p^i} \equiv a_i(p) \pmod{p^n}.$$

$$(31) \quad Z_{i+1}^{p^i} = Z_i E_i$$

$$(32) \quad Z_{i+1} Z_i Z_{i+1}^{-1} = Z_i E_i^{1-p^{i+1}} \quad (Z_{i+1} E_i Z_{i+1}^{-1} = E_i^{p^{i+1}}),$$

where E_i are elements of $\mathfrak{G}$.

Conversely if we extend an abelian group $\mathfrak{G}$ according to (28)–(32) successively, then the whole group $\mathfrak{G}$ thus obtained is quasi-Hamiltonian, because any two elements A, B of $\mathfrak{G}$ are contained in some $\mathfrak{G}_i$ and they satisfy consequently the relation (25). We have therefore

Theorem 9. Let $\mathfrak{G}$ be an M -group and $\mathfrak{E}$ be the normal subgroup of $\mathfrak{G}$ which consists of all elements of finite orders in $\mathfrak{G}$. If $\mathfrak{G}/\mathfrak{E}$ is an abelian group of rank 1 then $\mathfrak{G}$ is generated with $\mathfrak{E}$ and with elements $Z_1, Z_2, \dots$ of infinite orders by the relations (28)–(32).

Conversely any group of such structure is quasi-Hamiltonian, and therefore modular.

We have further

Theorem 10. For groups which contain elements of infinite orders the notions “modular” and “quasi-Hamiltonian” are equivalent.

The structure of an M -group which contains elements of infinite orders is thus thoroughly determined.

Mathematical Institute,
Tokyo Imperial University.