On primitive permutation groups.

By NOBORU ITÔ in Nagoya (Japan).

1. Let G be a (not necessarily finite) group. Let U be a subgroup of G such that the largest normal subgroup $\underline{U}$ of G contained in U is equal to the identity subgroup. Then G is faithfully represented as a group of permutations of the left (or right) residue classes by U in G. In these circumstances we call a pair $\{G, U\}$ *a permutation group.*

A permutation group $\{G, U\}$ is called *primitive,* when U is a maximal subgroup of G, and further $\{G, U\}$ is called *simply transitive,* when there exists no element g of G such that $G = U + UgU$. A permutation group, which is not simply transitive, is called *doubly transitive.*

A doubly transitive permutation group $\{G, U\}$ is primitive. In fact, let U be not maximal in G and let T be a proper subgroup of G containing U properly. Then T and TgT cannot be disjoint with each other and therefore $T = TgT$. This shows that $T = G$, which is a contradiction.

Let $\{G, U\}$ be doubly transitive: $G = U + UgU$. Put $V = U \cap gUg^{-1}$. Then *the pair $\{U, V\}$ is a permutation group.* In fact, let $\underline{V}$ be the largest normal subgroup of U contained in V. Now any element of G not contained in U has the form $u_1 g u_2$, where u_1 and u_2 are elements of U. Therefore since $u_1 g u_2 U u_2^{-1} g^{-1} u_1^{-1} = u_1 g U g^{-1} u_1^{-1}$, any conjugate subgroup $\neq U$ of U is of the form $ugUg^{-1}u^{-1}$. Therefore $\underline{V}$ is contained in any conjugate subgroup of U and consequently $\underline{V} \subseteq \underline{U} = 1$.

Let $\{G, U\}$ be a permutation group and let A be a subgroup of G such that $G = UA$. Then we call *A a transitive subgroup.* If A is abelian, then necessarily $A \cap U = 1$. In fact, since $G = UA$, any conjugate subgroup of U is of the form aUa^{-1}, where a is an element of A. And since A is abelian, $A \cap U$ is contained in the intersection $\underline{U}$ of all the conjugate subgroups of U. Therefore $A \cap U \subseteq \underline{U} = 1$.

Remark. Let $\{G, U\}$ be a primitive permutation group. Then we omit the case $U = 1$ from our considerations. In that case G is of prime order. Now if A is of order 2, then U is normal in G, and therefore $U = \underline{U} = 1$.

2. From now on we assume that *the order of G is finite.* Now the structure of primitive permutation groups is very complicated, because most primitive permutation groups are insoluble and we know less, at present, of the structure of such groups. Such a complicacy does not diminish even if we restrict our considerations to such primitive permutation groups that contain abelian transitive subgroups. Let $\{G, U\}$ be a primitive permutation group with an abelian transitive subgroup A. Now, in 1900, BURNSIDE [1] proved the following celebrated theorem: If A is of prime order, then either G is metacyclic or $\{G, U\}$ is doubly transitive. This result has been generalized by BURNSIDE, SCHUR and WIELANDT. The best is due to WIELANDT [1]: If at least one Sylow subgroup $\neq 1$ of A is cyclic and A is not of prime order, then $\{G, U\}$ is doubly transitive. Further KOCHENDÖRFFER [1] and D. MANNING [1] obtained (at about the same time and by quite different methods) the following result: If A is of type (p^a, p^b), where p is a prime and a and b are distinct natural numbers, then $\{G, U\}$ is doubly transitive. Now the results of these authors show: If there exists a primitive permutation group $\{G, U\}$ containing an abelian transitive subgroup A of a suitable type, then such a $\{G, U\}$ must be necessarily doubly transitive. Therefore the following question may be natural: To what type of an abelian group A', does there exist a primitive permutation group $\{G, U\}$ containing an abelian transitive subgroup A isomorphic to A'? In this direction RITT [1] proved the following theorem: If A' is cyclic of not prime order and if there exists a soluble primitive permutation group $\{G, U\}$ containing an abelian transitive subgroup A isomorphic to A', then A' must be of order 4. Further in this case actually there exists one and only one permutation group of this kind, that is, the symmetric group $\mathfrak{S}_4 = \{G, U\}$ of degree 4, where, for instance, $U = \{(123), (12)\}$ and $A = \{(1234)\}$.

The present paper is a contribution in the same direction. Thereby the result of RITT is not assumed but proved as a special case of our results. Now in our considerations the solubility of the group G is not assumed. (In fact, if we assume solubility, the contents may be vacant in essential except the result of RITT.) But to avoid the occurence of incomputably deep difficulties we assume, a priori, the following condition on G:

(S) *G contains an abelian normal subgroup $N \neq 1$.*

Now since U is maximal in G and since $\underline{U} = 1$, we have $G = U \cdot N$. Therefore, as we remarked above, we have $U \cap N = 1$. These two equalities show us that N is the only one abelian normal subgroup $\neq 1$ of G. In fact, we have two equalities $G = UM$ and $U \cap M = 1$ for every abelian normal subgroup $M (\neq 1)$ of G. Then every abelian normal subgroup $\neq 1$ of G is minimal. To see this, let M and M' be two abelian normal subgroups $\neq 1$ of G such that M contains M' properly. Then we have from the first equality the following factorization of M: $M = M \cap U \cdot M'$. Then since $M \neq M'$, $M \cap U \neq 1$. This contradicts the second equality. Now if there exist two distinct abelian minimal normal subgroups of G, then their join, as the direct product of them, is not a minimal one. This is a contradiction. In particular, N is of type $(p, \ldots, p)$, where p is a prime. Let A be any abelian transitive subgroup of $\{G, U\}$. Then $G = UA$ and $U \cap A = 1$. Therefore the orders of N and A are the same.

3. Let A' be an abelian group of order p^n and of type $(p, \ldots, p) \neq (2)$. We verify the existence of primitive permutation groups with abelian transitive subgroups isomorphic to A'. This may be done without much difficulty. In fact, let U be an irreducible matric group with coefficients in the prime field of characteristic p and let A be its representation module. Let G be the splitting extension of A by U in the sense of Schreier. (This can be constructed as a subgroup of the holomorph of A.) Then the permutation group $\{G, U\}$ is a required one. In fact, $\underline{U} = 1$, because an element of $\underline{U}$ must be commutative with all the elements of A and therefore it must be a unit matrix, and further U is maximal in G, because, otherwise, U must be reducible.

Example 1. U may be the general linear group $GL(n, p)$.

Example 2. We can choose U as a soluble group. In fact, $GL(n, p)$ contains an irreducible cyclic subgroup $Z = \{X\}$ of order $p^n - 1$. To see this let us consider a generator X of the multiplicative group of the finite field of p^n elements. Since the finite field of p^n elements may be considered as the n-dimensional vector space over the prime field, X satisfies an irreducible equation of degree n over the prime field: $X^n - c_1 X^{n-1} - \cdots - c_n = 0$, where c's are elements of the prime field. Then the matrix $X = \begin{pmatrix} c_1, c_2, \ldots, c_{n-1}, c_n \\ E \qquad\qquad 0 \end{pmatrix}$, where E is the unit matrix of degree $n-1$ and 0 is the null matrix of type $(n-1, 1)$, is of order $p^n - 1$ and of degree n. Further all the characteristic roots of X are algebraically conjugate, because of the irreducibility of the equation. Now if $Z = \{X\}$ is reducible, then some power of $X \neq 1$ possesses the characteristic value 1. Therefore $Z = \{X\}$ must be irreducible.

4. Let A' be an abelian group which is not of type $(p, \ldots, p)$. Then, as it can be understood from the result of RITT cited above, we have not always a primitive permutation group satisfying the condition (S) with an abelian transitive subgroup isomorphic to A'.

Now let $\{G, U\}$ be a primitive permutation group with an abelian transitive subgroup A isomorphic to A'. Then G admits the following factorization: $G = UA$ and $U \cap A = 1$. Further by the assumption (S) G also admits the following factorization: $G = UN$ and $U \cap N = 1$, where N is the only one abelian normal subgroup of G. Put $P = AN$. Then P admits the factorizations $P = U_p A$, $U_p \cap A = 1$ where U_p is an abelian p-subgroup of U and also, since $U \cap N = 1$ and A and N are of the same order, $P = U_p N$, $U_p \cap N = 1$. Clearly the centralizers of A and N in P coincide with A and

N themselves respectively. Now a p-group with such a factorization cannot be too simple in its structure. In fact, we prove the following

Lemma 1. *Let P be a p-group and let P admit the following factorizations: $P = NA$ and $P = UA$, $U \cap A = 1$ and $P = UN$, $U \cap N = 1$, where A is abelian, not of type $(p, \dots, p)$, N is abelian of type $(p, \dots, p)$, normal and coincides with its own centralizer, and U is abelian. Then we have*

(i) *P is irregular in the sense of Hall,*

(ii) *Let p^w be the order of the subgroup of A consisting of all the elements of A with order not greater than p. Then $w \geqq p-1$.*

Remark. Under this condition the centralizer of A necessarily coincides with A. In fact, otherwise, since $P = AU$, there exists an element $u_0 (\neq 1)$ such that u_0 is commutative with every element of A. Now since $N \subseteqq AU$, every element of N can be written in the form of a product au, where a and u belong to A and U respectively. Therefore, since U is abelian, u_0 is commutative with every element of N.

Proof. We prove these assertions by an induction argument with respect to the order of P.

(i) Let Z_1 and Z_2 be the centre and the second centre of P. Put $U_2 = U \cap Z_2$. Let us consider the subgroup $U_2 Z_1$. Naturally $U_2 Z_1$ is normal in P. Let us consider the factor group $P/U_2 Z_1$ and its factorizations: $P/U_2 Z_1 = U \cdot U_2 Z_1/U_2 Z_1 \cdot N \cdot U_2 Z_1/U_2 Z_1$ and $P/U_2 Z_1 = U \cdot U_2 Z_1/U_2 Z_1 \cdot A U_2 Z_1/U_2 Z_1$. We show that $P/U_2 Z_1$ satisfies the same conditions as P except the fact that $A U_2 Z_1/U_2 Z_1$ is not of type $(p, \dots, p)$. First it is clear that $U \cdot U_2 Z_1 = U Z_1$, $N \cdot U_2 Z_1 = U_2 N$, $A \cdot U_2 Z_1 = U_2 A$ and therefore $U U_2 Z_1 \cap N U_2 Z_1 = U_2 Z_1$, $A U_2 Z_1 \cap U U_2 Z_1 = U_2 Z_1$. Secondly if $N \cdot U_2 Z_1/U_2 Z_1$ is distinct from its own centralizer, then there exists an element x of $U - U_2$ such that $[x, N] \subseteqq U_2 Z_1$. Since N is normal, $[x, N] \subseteqq N$ and therefore $[x, N] \subseteqq U_2 Z_1 \cap N = Z_1$ and further since U is abelian, we see that x belongs to Z_2. Thus x belongs to U_2, which is a contradiction.

Now if $A U_2 Z_1/U_2 Z_1$ is not of type $(p, \dots, p)$, then, by the induction hypothesis, we see that $P/U_2 Z_1$ is irregular in the sense of Hall. Then, a fortiori, by the definition of regularity of Hall, P is irregular in the sense of Hall, too. So we may assume that $A U_2 Z_1/U_2 Z_1$ is of type $(p, \dots, p)$. Now, since $A \cap U_2 Z_1 = Z_1$, by the second isomorphism theorem, $A U_2 Z_1/U_2 Z_1 \cong A/Z_1$. Further, since $A \cap N = Z_1$, $U \cong A/Z_1$. Therefore U is of type $(p, \dots, p)$. Hence P can be generated by elements of order p. Therefore if P is regular in the sense of Hall, then, by a theorem of Hall, P must be of exponent p, that is, all the elements of P except 1 are of order p, which contradicts the assumption on A. Thus P must be irregular in the sense of Hall [Hall, 1].

(ii) Let us assume $w < p-1$. Then we want to derive a contradiction from this assumption. Now, let C be a central subgroup of order p. We shall denote the subgroup of P which consists of the centre of P/C by $Z_1(P \div C)$ and let $Z_1(P \div C)/C$ be the centre of P/C. Put $U_1 = U \cap Z_1(P \div C)$. Naturally U_1C is normal in P. Let us consider the factor group P/U_1C and its factorizations: $P/U_1C = UC/U_1C \cdot NU_1/U_1C = UC/U_1C \cdot AU_1/U_1C$. We show that $UC \cap NU_1 = U_1C$, $UC \cap AU_1 = U_1C$ and the centralizer of NU_1/U_1C coincides with NU_1/U_1C. Since $P = NU = AU$, $N \cap U = 1$, $A \cap U = 1$, the former is evident. If the centralizer of NU_1/U_1C is distinct from NU_1/U_1C, then since $P = NU$, $N \cap U = 1$, there exists an element x of $U - U_1$ such that $[x, N] \subseteq U_1C$, which implies, since N is normal, $[x, N] \subseteq U_1C \cap N = C$. Since U is abelian, x belongs to $Z_1(P \div C)$ and therefore to $Z_1(P \div C) \cap U = U_1$. This is a contradiction. If AU_1/U_1C is not of type $(p, \ldots, p)$, then by induction hypothesis, we see that the order of the subgroup of $AU_1/U_1C \cong A/C$ consisting of all the elements of order not greater than p is not smaller than p^{p-1}. Then, a fortiori, by the fundamental theorem of abelian groups, the same holds for A itself, which is a contradiction. So we may assume that in the opposite case $AU_1/U_1C \cong A/C$ is of type $(p, \ldots, p)$. Therefore since $U \cong A/A \cap N$ and $A \cap N = Z_1 \supset C$, we see that U is of type $(p, \ldots, p)$. Further A is of order not greater than p^{p-1} and of type $(p^2, p, \ldots, p)$. Let a be an element of A with order p^2. Let us consider the subgroup $\{a\}N$ and put $\{a\}N = V \cdot N$, where V is a subgroup of U. Since a^p is contained in $C \subseteq N$, the order of $\{a\}N$ is at most p^p. Thus, by a theorem of Hall, $\{a\}N$ is regular in the sense of Hall. On the other hand, $V \cdot N$ can be generated by elements of order p. Then, by a theorem of Hall, all the elements of $V \cdot N$ are of order at most p (HALL [1]). This contradicts the fact that the order of a is p^2. Hence the order of the subgroup of A consisting of all the elements of A with order at most p is not smaller than p^{p-1}.

Remark. The proof of (i) holds also good, if we replace Z_1 in that proof by C as in this proof.

Now we can generalize the second part of the preceding lemma as follows.

Lemma 2. *In the same notations as in the preceding lemma, if* $w < \dfrac{p^m - 1}{m}$ *then* p^{m+1} *cannot occur as an invariant number of the abelian group* A. (The case $m = 1$ coincides with the second part of the preceding lemma. Therefore, in the following, we assume $m \geqq 2$.)

Proof. (1) Let $P(n, p)$ be a p-Sylow subgroup of the n-dimensional general linear group over the prime field of characteristic p. Further let us assume $n \leqq p^m$. Then we show that the order of any element of $P(n, p)$ is not greater than p^m. In fact, as is well known (SCHREIER [1]) $P(n, p)$ is isomorphic to the matric group consisting of all the matrices of degree n and of the form $\begin{pmatrix} 1 & a_{12} & \cdots & a_{1n} \\ & \ddots & \ddots & \vdots \\ & & \ddots & a_{n-1\,n} \\ & & & 1 \end{pmatrix}$. Let X be any matrix of such a form. Put $X=E+Y$, where E is the unit matrix of degree n. Then $X^{p^e}=E+Y^{p^e}$ for $e=1,2,\ldots$. Further clearly

$$Y^r=\begin{pmatrix} \overbrace{0\cdots 0}^{r} & & * \\ & \ddots & \ddots \\ & & \ddots & 0 \\ & & & \vdots \\ & & & 0 \end{pmatrix}.$$

Therefore if $n\leqq p^m$, then $Y^{p^m}=0$. This proves $X^{p^m}=E$.

(2) Let V_n be an n-dimensional vector space over the prime field of characteristic p. We may consider $P(n,p)$ as an automorphism group of V_n. Let P_n be the extension of V_n by $P(n,p)$ as a subgroup of the holomorph of V_n. Assume $n<p^m$. Then we show that the order of any element of P_n is not greater than p^m. In fact, let $x=\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$ be any vector of V_n. Then any element of P_n can be represented as a product (in P_n) Xx for some $X\in P(n,p)$ and some $x\in V_n$, where $XxX^{-1}=X\circ x$. ($\circ$ denotes the ordinary matrix multiplication.) We want to show $(Xx)^{p^m}=1$. Now $(Xx)^{p^m}=$ $=XxX^{-1}\cdot X^2xX^{-2}\ldots X^{p^m-1}xX^{-(p^m-1)}\cdot X^{p^m}xX^{-p^m}$, since $X^{p^m}=1$. Therefore to show $(Xx)^{p^m}=1$ we have only to prove that $(E+X+\cdots+X^{p^m-1})\circ x=0$, where 0 is the null vector. Now $E+X+\cdots+X^{p^m-1}=0$, where 0 is the null matrix of degree n. In fact, put $X=E+Y$. Then

$$\begin{aligned} E+X+\cdots+X^{p^m-1}&=E+(E+Y)+\cdots+(E+Y)^r+\cdots+(E+Y)^{p^m-1}= \\ &=p^mE+\left\{\binom{1}{1}+\cdots+\binom{r}{1}+\cdots+\binom{p^m-1}{1}\right\}Y+ \\ &\quad+\left\{\binom{2}{2}+\cdots+\binom{r}{2}+\cdots+\binom{p^m-1}{2}\right\}Y^2+ \\ &\quad+\cdots+\binom{p^m-1}{p^m-1}Y^{p^m-1}. \end{aligned}$$

Here since $m>1$ $\binom{i}{i}+\cdots+\binom{r}{i}+\cdots+\binom{p^m-1}{i}=\binom{p^m}{i+1}\equiv 0 \pmod p$ for $i<p^m-1$. Further by assumption $Y^{p^m-1}=0$. This proves $E+X+\cdots$ $\cdots+X^{p^m-1}=0$. Therefore $(Xx)^{p^m}=1$, as we required.

(3) Now we repeat in the same notations the proof (by induction on the order of the group) of the second part of the preceding lemma. We assume that p^{m+1} occurs as an invariant number of the type of A. If p^{m+1} occurs also as an invariant number of the type of $AU_1/U_1C \cong A/C$, then, by induction hypothesis, the order of the subgroup of A/C consisting of all the elements of order not greater than p is not smaller than $\frac{p^m-1}{m}$. Then, a fortiori, by the fundamental theorem of abelian groups, the same holds for A itself, which contradicts the assumption $w < \frac{p^m-1}{m}$. So we may assume that p^{m+1} does not occur as an invariant number of the type of A/C. Then, since $w < \frac{p^m-1}{m}$, A/C is a subgroup of an abelian group of order $p^{m\left(\frac{p^m-1}{m}-1\right)}$ and of type $(p^m, \ldots, p^m)$ and, therefore, the order of A is at most equal to $p^{m\left(\frac{p^m-1}{m}-1\right)+1} = p^{p^m-m}$. The same holds for N. Now the group P can be considered as a subgroup of P_n for $n \leqq p^m - m$. Therefore any element of P possesses the order at most equal to p^m, as we saw in (2). This contradiction proves our assertion completely.

Remark. The bound $\frac{p^m-1}{m}$ may not be the best possible one. But, at any rate, the result of Ritt cited above is a special case of our lemmas.

5. In this section we construct an example of a primitive permutation group $\{G, U\}$ with an abelian transitive subgroup A not of type $(p, \ldots, p)$. In fact, we choose the p-dimensional general linear group $GL(p, p)$ over the prime field of characteristic p as a U, the p-dimensional vector space V_p over the prime field of characteristic p as an N and the splitting Schreier extension of N by U as a subgroup of the holomorph of N as a G. Naturally since U is irreducible for N and clearly U does not contain a normal subgroup $\neq 1$ of G, $\{G, U\}$ actually defines a primitive permutation group. Therefore we have only to verify the existence of an abelian transitive subgroup A not of type $(p, \ldots, p)$. To do this, first put $B_r = E + \sum_{i+r-1<j} e_{ij}$ for $r = 1, 2, \ldots, p-1$, where E is the unit matrix of degree p and e_{ij}'s are the matrix units:

$$e_{ij} = \begin{array}{c} \\ i \\ \\ \end{array}\!\!\begin{array}{c} \quad j \\ \left(\begin{array}{ccc} & \vdots & \\ \cdots & 1 & \cdots \\ & \vdots & \end{array}\right) \end{array} \qquad (i, j = 1, \ldots, p).$$

First we prove that $\{B_1, B_2, \ldots, B_{p-1}\}$ is abelian of order p^{p-1} and of type $(p, \ldots, p)$. In fact, put $B_r = E + W_r$. Then $B_r B_s = E + W_r + W_s +$

$$+W_rW_s,\quad \text{where}\quad W_rW_s=\begin{array}{c} \overset{r+s+1}{} \\ \begin{pmatrix} & & 1 & 2 & \cdots & \cdot \\ & & & \ddots & & \vdots \\ & & & & \ddots & 2 \\ \mathbf{0} & & & & & 1 \end{pmatrix}\end{array}.$$ Since the matrix W_rW_s is symmetric for r and s, we have $W_rW_s=W_sW_r$. Therefore $B_rB_s=B_sB_r$. Further $B_r^p=E+W_r^p$. Since clearly $W_r^p=0$, $B_r^p=E$. Last let us assume $B_1^{e_1}\dots B_{p-1}^{e_{p-1}}=E$, where $0\leqq e_i<p$ $(i=1,\dots,p-1)$. Then $(E+W_1)^{e_1}\dots$ $\dots(E+W_{p-1})^{e_{p-1}}=E$ and therefore, $(E+e_1W_1+\cdots)\cdots(E+e_{p-1}W_{p-1}+\cdots)=E$. Now the coefficient of e_{12} in $(E+e_1W_1+\cdots)\cdots(E+e_{p-1}W_{p-1}+\cdots)$ is equal to e_1. Therefore $e_1=0$. Thus $B_2^{e_2}\dots B_{p-1}^{e_{p-1}}=E$. Therefore $(E+e_2W_2+\cdots)\cdots$ $\cdots(E+e_{p-1}W_{p-1}+\cdots)=E$. Now the coefficient of e_{13} in $(E+e_2W_2+\cdots)\cdots$ $\cdots(E+e_{p-1}W_{p-1}+\cdots)$ is equal to e_2. Therefore $e_2=0$. Similarly $e_3=\cdots=e_{p-1}=0$. Thus $B_1,\dots,B_{p-1}$ are linearly independent.

Secondly put $x_r=\begin{pmatrix}0\\ \vdots\\ 0\\ 1\\ 0\\ \vdots\\ 0\end{pmatrix}\begin{matrix}\\ \\ \\ r\\ \\ \\ \\ \end{matrix}$ for $r=1,2,\dots,p$, and put $A_r=x_rB_r$ (this is a product in G!) for $r=1,2,\dots,p-1$. We prove that $\{A_1,A_2,\dots,A_{p-1}\}$ is abelian of order p^p and of type $(p^2,p,\dots,p)$. Now the equation $A_rA_s=A_sA_r$ is equivalent to the equation $x_r+B_r\circ x_s=x_s+B_s\circ x_r$, where $\circ$ denotes the ordinary matrix multiplication. Further the equation $x_r+B_r\circ x_s=x_s+B_s\circ x_r$ is equivalent to the equation $W_r\circ x_s=W_s\circ x_r$. Therefore we show $W_r\circ x_s=W_s\circ x_r$. Now if $s+r>p$, then $W_r\circ x_s=0$. If $s+r+i=p$, where i is a non-negative integer, then $W_r\circ x_s=e_1+\cdots+e_{i+1}$. By symmetry, we have $W_r\circ x_s=W_s\circ x_r$. Now similarly as in the second step of the proof of Lemma 2, we have $A_2^p=\cdots=A_{p-1}^p=E$. Further $A_1^p=(x_1B_1)^p=x_1B_1x_1B_1\cdots$ $\cdots x_1B_1=B_1^{-p}x_1B_1^p\cdot B_1^{-(p-1)}x_1B_1^{p-1}\cdots B_1^{-2}x_1B_1^2\cdot B_1^{-1}xB_1$. Here $(B_1^{p-1}+\cdots+$ $+B_1+E)\circ x_1=x_p$. Therefore $A_1^p=x_p$. Clearly $A_1,\dots,A_{p-1}$ are linearly independent of each other.

Last we prove that $A\cap U=1$. Now since an element belonging to $A\cap U$ must be commutative with $x_1,\dots,x_p$, it must be the identity. This proves the assertion.

Thus A is transitive and not of type $(p,\dots,p)$.

Remark. Such a construction may be executed for every $n\geqq p$.

6. Before proceeding further, we refer to KOCHENDÖRFFER's method of the construction of simply transitive, primitive permutation groups with abelian transitive subgroups, in a little generalized form. (In this section G may be infinite.)

Let $\{G, U\}$ be a primitive permutation group with an abelian transitive subgroup A. Let $\{G_i, U_i\}$, and A_i $(i=1,2,\ldots,r)$ be the r copies of $\{G, U\}$ and A, where r is a natural number >1. We denote the isomorphism between G and G_i by $g \longleftrightarrow g_i$ $(g \in G,\ g_i \in G_i)$ for each i $(i=1,2,\ldots,r)$. Put $G^* = G_1 \times \cdots \times G_r$ (the direct product of $G_1, G_2, \ldots, G_r$). Let S be the automorphism of G^* such that $g_i^s = g_{i+1}$ $(g_{r+1} = g_1)$. Let G^{**} be the splitting Schreier extension of G^* by S, which can be constructed as a subgroup of the holomorph of G^*. Put $U^{**} = (U_1 \times \cdots \times U_r)\ \{S\}$ and $A^{**} = A_1 \times \cdots \times A_r$. Now we prove that *the pair $\{G^{**}, U^{**}\}$ is a simply transitive, primitive permutation group with an abelian transitive subgroup A^{**}.*

Clearly $G^{**} = U^{**} A^{**}$ and $U^{**} \cap A^{**} = 1$. Assume $\underline{U}^{**} \neq 1$. Transforming an element of $\underline{U}^{**}$ by an element of $U^* = U_1 \times \cdots \times U_r$, we see $\underline{U}^{**} \cap U^* \neq 1$. Therefore $\underline{U}^{**} \cap G^* \neq 1$. Clearly this is a normal subgroup of G^* contained in U^*. Since $\underline{U}^* = 1$, this is a contradiction. Now we prove the maximality of U^{**} in G^{**}. Since $G^{**} = U^{**} A^{**}$, if U^{**} is not maximal in G^{**}, there exists an element $a \neq 1$ of A^{**} such that $G^{**} \neq \{U^{**}, a\}$. Put $a = a_1 \cdots a_r$, where each a_i belongs to A_i $(i=1,2,\ldots,r)$. Then there exists at least one i, say 1, such that $a_i \neq 1$. Therefore we assume $a_1 \neq 1$. We consider the elements $u_1 a u_1^{-1} = u_1 a_1 u_1^{-1} a_2 \cdots a_r$, where u_1 runs over all the elements of U. Since $\{U_1, a_1\} = G_1$, and since $\underline{U}_1 = 1$, there exists an element a_1 such that $u_1 a_1 u_1^{-1} a_1^{-1}$ does not belong to U_1. Then $\{U^{**}, a\}$ contains an element $\neq 1$ of A_1. Therefore $\{U^{**}, a\}$ contains G_1 and coincides with G^{**}. This is a contradiction. Next we prove that $\{G^{**}, U^{**}\}$ is simply transitive. Since $G^{**} = U^{**} A^{**}$, if $\{G^{**}, U^{**}\}$ is doubly transitive, there exists an element $a \neq 1$ of A^{**} such that $G^{**} = U^{**} + U^{**} a U^{**}$. Put $a = a_1 \cdots a_r$, where each a_i belongs to A_i $(i=1,\ldots,r)$. Let $a' \neq 1$ be any element of A^{**}. Put $a' = a_1' \cdots a_r'$, where each a_i' belongs to A_i $(i=1,\ldots,r)$. Let $l(a')$ be the number of i's such that $a_i' \neq 1$ ($l(a')$ is a natural number). Now to prove the inconsistency of the equation $G^{**} = U^{**} + U^{**} a U^{**}$, we have only to show the following: if $U^{**} a U^{**} = U^{**} a' U^{**}$, then $l(a) = l(a')$. Now $U^{**} a U^{**} = U^{**} a' U^{**}$ implies that there exist two elements u and u' of U^{**} such that $ua = a'u'$. Put $u' = u_1 \cdots u_r S^c$, where each u_i' belongs to U_i $(i=1,\ldots,r)$, and put $a' u_1' \cdots u_r' = u_1'' \cdots u_r'' a''$, where each u_i'' belongs to U_i $(i=1,\ldots,r)$ and a'' is an element of A^{**}. Since $M_i A_i = A_i M_i$ and $M_i \cap A_i = 1$ $(i=1,\ldots,r)$, we see immediately that $l(a') = l(a'')$. Put $a'' S^c = S^c a'''$, where a''' is an element of A^{**}. Since S permutes $A_1, A_2, \ldots, A_r$ cyclically, we see immediately that $l(a'') = l(a''')$. Since $U^{**} \cap A^{**} = 1$, we have $a = a'''$. This proves the assertion. Here we refer to the following

Corollary. If there exists a primitive permutation group with an abelian transitive subgroup of type $(p_1^{e_{11}}; \ldots, p_n^{e_{nn'}})$, then there exists a simply transitive, primitive permutation group with an abelian transitive subgroup of type $(\underbrace{p_1^{e_{11}} \cdots p_1^{e_{11}}}_{s}, \ldots, \underbrace{p_n^{e_{nn'}} \cdots p_n^{e_{nn'}}}_{s})$ for every $s > 1$.

7. Now we treat the KOCHENDÖRFFER—D. MANNING case satisfying the condition (S). In consequence of Lemmas 1 and 2 only the following four cases are to be considered as the type of the abelian group A: $(4, 2), (8, 2), (9, 3)$ and $(8, 4)$. In this section we take the first three of these types into our consideration.

Existence. For the type $(9, 3)$ we have already constructed an example of such primitive permutation groups in §5. Now for the types $(4, 2)$ and $(8, 2)$ the same method of construction as in §5 can be applied. Therefore we have only to tabulate the necessaries with the same notations as in §5:

Type $(4, 2)$, $U = GL(3, 2)$, $N = V_3$, $G = GL(3, 2)\, V_3$

$$A = \{A_1, A_2\},\ A_1 = \begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}\begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix},\ A_2 = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}\begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix};\ A_1^2 = A_2\begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}.$$

Type $(8, 2)$. $U = GL(4, 2)$, $N = V_4$, $G = GL(4, 2)\ V_4$

$$A = \{A_1, A_2, A_3\},\quad A_1 = \begin{pmatrix} 1 & 1 & 1 & 1 \\ & 1 & 1 & 1 \\ & & 1 & 1 \\ & & & 1 \end{pmatrix}\begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix},$$

$$A_2 = \begin{pmatrix} 1 & 0 & 1 & 1 \\ & 1 & 0 & 1 \\ & & 1 & 0 \\ & & & 1 \end{pmatrix}\begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix},\quad A_3 = \begin{pmatrix} 1 & 0 & 0 & 1 \\ & 1 & 0 & 0 \\ & & 1 & 0 \\ & & & 1 \end{pmatrix}\begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix};$$

$$A_1^2 = \begin{pmatrix} 1 & 0 & 1 & 0 \\ & 1 & 0 & 1 \\ & & 1 & 0 \\ & & & 1 \end{pmatrix}\begin{pmatrix} 1 \\ 1 \\ 1 \\ 0 \end{pmatrix},\quad A_1^4 = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} = A_2^2,\qquad A_2^3 A_3 = A_1^2.$$

Insolubility. We show that: Let $\{G, U\}$ be a primitive permutation group with an abelian transitive subgroup A of type either $(4, 2)$ or $(8, 2)$ or $(9, 3)$. Then G is insolube. Thereby we do not use the result of KOCHENDÖRFFER and MANNING.

First we supplement the second part of Lemma 1, and Lemma 2 as follows:

Lemma 3. *In the same notations as before, let p^v be the order of the subgroup of U consisting of all the elements of U with order not greater than p. If $v < \dfrac{p^m - 1}{m}$ then p^{m+1} cannot occur as an invariant number of the type of the abelian group A.*

Proof. We repeat in the same notations the proof (by induction on the order of the group) of the second part of Lemma 1. We assume that

p^{m+1} occurs as an invariant number of the type of A. If p^{m+1} occurs as an invariant number of the type of $AU_1/U_1C \cong A/C$ then, by induction hypothesis, the order of the subgroup of $UC/U_1C \cong U/U_1$ consisting of all the elements of order not greater than p is not smaller than $\frac{p^m-1}{m}$. Then a fortiori, by the fundamental theorem of abelian groups, the same holds for U itself, which contradicts the assumption $v < \frac{p^m-1}{m}$. So we may assume that p^{m+1} does not occur as an invariant number of the type of A/C. Then C coincides with the subgroup of A generated by all the p^m-th powers of elements of A. If the centre Z of P is distinct from C, then, since $Z \leqq N$ is of type $(p, \ldots, p)$, Z contains a central subgroup C' of order p different from C. Repeat the same argument by C' in place of C. Then, since p^{m+1} occurs as an invariant number of the type of A/C', we can apply the induction hypothesis and obtain the conceived contradiction. Therefore we may assume that $Z = C$. Now since clearly $U \cong A/Z$ and, by assumption $v < \frac{p^m-1}{m}$, the order of A is at most equal to $p^{m\left(\frac{p^m-1}{m}-1\right)+1} = p^{p^m-m}$. The same holds for N. Now the group P can be considered as a subgroup of P_n for $n \leqq p^m - m$. Therefore any element of P possesses the order at most equal to p^m, as we saw in (2) of the proof of Lemma 2. This contradiction proves our assertion.

Proof of insolubility. First some remarks of general character: (1) Let N be of order p^n. Then we may consider U as a subgroup of $GL(n, p)$. (2) U does not contain a normal p-subgroup $\neq 1$. In fact, let L be a normal p-subgroup of U. Then LN is normal in G. Let N_1 be the centre of LN. If $N_1 \not\subseteqq N$, then U contains a normal subgroup $\neq 1$ of G, which contradicts $\underline{U} = 1$. Therefore $N_1 \subseteqq N$. Since N is minimal normal in G, $N_1 = N$. Then $LN = L \times N$, which implies that L is normal in G, which contradicts $\underline{U} = 1$.

Now we treat each case separately.

Case of type (4, 2). Assume the solubility of U. Then, as it is well known, since $GL(3, 2)$ is simple and not abelian (Dickson [1]), $U \neq GL(3, 2)$. We denote the order of U by (U). At any rate, $(U) | 2^3 \cdot 3 \cdot 7 =$ the order of $GL(3, 2)$. Assume $7 | (U)$ and let U_7 be a 7-Sylow subgroup of U. If U_7 is not normal in U then we see, by Sylow's theorem[1]), $(U) = 2^3 \cdot 7$. Since U does not contain a normal 2-group, U_7 must be normal in U, which is a contradiction. Therefore U_7 is normal in U. Then since $2 | (U)$, we see, by Sylow's theorem, U_7 must be normal in $GL(3, 2)$, which contradicts the simplicity of $GL(3, 2)$. Thus $7 \nmid (U)$, and $(U) | 2^3 \cdot 3$. If $2^2 | (U)$, then U must

[1]) The number of p-Sylow subgroups is congruent to 1 mod p. Cf. H. Zassenhaus, *Lehrbuch der Gruppentheorie* I (Berlin—Leipzig, 1937), p. 100.

contain a normal 2-group $\neq 1$, which is not the case. Thus $(U)=2\cdot 3$. Let U_3 be the 3-Sylow subgroup of U. Since U is irreducible for $V_3=N$, U_3 is completely reducible (cf. FROBENIUS [1]). Therefore since the degree of the representation is 3, U_3 must be irreducible. On the other hand, by SYLOW's theorem, U_3 is not maximal in U_3N. This contradiction proves our assertion.

Case of type (9, 3). Assume the solubility of U. As above, $U \neq GL(3,3)$. At any rate, $(U)|2^5\cdot 3^3\cdot 13=$ the order of $GL(3,3)$. By Lemma 3, $3^2|(U)$. Assume $13|(U)$ and let U_{13} be a 13-Sylow subgroup of U. If U_{13} is not normal in U, then we see, by SYLOW's theorem, $(U)=2^4\cdot 3^2\cdot 13$ or $=3^3\cdot 13$. Since U does not contain a normal 3-subgroup $\neq 1$, the latter case does not occur. In the former case clearly U_{13} is not maximal in U and this implies that U_{13} is normal in U, which is a contradiction. Thus U_{13} must be normal in U. Then, we see, by SYLOW's theorem, U_{13} must be normal in $GL(3,3)$, because $3^2|(U)$. Thus $13 \nmid (U)$, and $(U)|2^5\cdot 3^3$. Let R be the largest normal nilpotent subgroup of U. Then, since U does not contain a normal 3-subgroup, R is a 2-group. If R is reducible for $V_3=N$, then, since R is completely reducible and the degree of the representation is 3, R is of diagonal form. Then the order of R is at most equal to 2^3. Further the subgroup R_+ of R consisting of all the matrices with determinant 1 is of order at most equal to 2^2. Since $3^2|(U)$, this implies that U contains a normal 3-subgroup $\neq 1$, which is a contradiction. Thus R is irreducible for V_3. If R_+ is not of type (2, 2, 2, 2), then, as above, U contains a normal 3-subgroup $\neq 1$, which is a contradiction. But if R_+ is of type (2, 2, 2, 2), then R_+ cannot be irreducible for V_3 (cf. HUPPERT [1]). But if R_+ is reducible for V_3, then the order of R_+ must be at most equal to 2^3. This contradiction proves our assertion.

Case of type (8, 2). Assume the solubility of U. As above, $U \neq GL(4,2)$. At any rate, $(U)|2^6\cdot 3^2\cdot 5\cdot 7=$ the order of $GL(4,2)$. By Lemma 3, $2^3|(U)$. Assume $7|(U)$ and let U_7 be a 7-Sylow subgroup of U. If U_7 is normal in U, then U_7 is completely reducible for $V_4=N$, because of the irreducibility of U (cf. FROBENIUS [1]). Now U_7 cannot be irreducible, which is easily seen by considering $U\cdot N$ and using SYLOW's theorem. Further U_7 cannot be reducible. In fact, otherwise, since it is completely reducible, $U_7\cdot N=U_7\times N$, which is clearly a contradiction. Thus U_7 is not normal in U. Let R be the largest normal nilpotent subgroup of U. Then, since U does not contain a normal 2-subgroup, R is of order prime to 2. Let us consider RU_7. Then we see, by SYLOW's theorem, that $RU_7=R\times U_7$, which is clearly a contradiction. Thus $7\nmid (U)$, and $(U)|2^6\cdot 3^2\cdot 5$. Assume $5|(U)$ and let $U_5=\{u_5\}$ be a 5-Sylow subgroup of U. If U_5 is normal in U, then, since $2^3|(U)$, there exists an element t of order 2 which belongs to the centralizer of U_5. This is a contradiction. In fact, t admits an invariant vector $x\neq 0$ and since U_5 is irreducible, $u_5^i \circ x$ $(i=0,1,2,3,4)$ ($\circ$ denotes the matrix multiplication) generates the whole vector space $V_4=N$. Therefore t must be the identity.

Thus U_5 is not normal in U. Let R be the largest normal nilpotent subgroup of U. Then, as above, we come to the contradiction that $RU_5 = R \times U_5$. Thus $5 \nmid (U)$ and $(U) | 2^6 \cdot 3^2$. Now let us assume that U contains a normal subgroup of order 3. Then we can easily see that U contains a normal 2-subgroup $\neq 1$, which is a contradiction. Let U_3 be a 3-Sylow subgroup of U. Then U_3 is minimal normal in U. Since the order of $GL(2, 3)$ is $2^4 \cdot 3$, if $2^5 | (U)$, then U contains a normal 2-subgroup $\neq 1$. Further a 2-Sylow subgroup of U is isomorphic to a subgroup of a 2-Sylow subgroup of $GL(2, 3)$, which is generated by matrices $\begin{pmatrix} -1 & 1 \\ 0 & 1 \end{pmatrix}$, $\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$, $\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$ and $\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$ with coefficients in the prime field of characteristic 3 (cf. DICKSON [1], p. 86). As it is easily seen, this group does not contain an abelian subgroup of type (4, 2). On the other hand, a 2-Sylow subgroup of U contains an abelian subgroup V of type (4, 2), where $A \cdot N = V \cdot N$ and $V \cap N = 1$. This contradiction proves our assertion.

Remark. The solubility can be formally weakened to the p-solubility in the sense of ČUNIHIN [1].

Double transitivity. Now we give an other proof to our case of KOCHENDÖRFFER—MANNING's theorem.[2]) As above, we treat each case separately. First we remark the following. Let n be an element of N. Let UnU be a double-sided class of G by U. Then all the elements of N belonging to UnU are conjugate to n and conversely.

Case of type (4, 2). By BURNSIDE's theorem, if $7 \nmid (U)$, then U is soluble. Since U is insoluble, $7 | (U)$. Then, since the order of N is 8, by the remark, we see easily that $G = U + UnU$, where n is an element $\neq 1$ of N, and $\{G, U\}$ is doubly transitive (BURNSIDE [2]).

Case of type (9,3). By BURNSIDE's theorem, if $13 \nmid (U)$, then U is soluble. Since U is insoluble, $13 | (U)$. We notice that every element of order 13 does not possess the characteristic value 1. Again by BURNSIDE's theorem, if $2 \nmid (U)$, then U is soluble. Since U is insoluble, $2 | (U)$. We notice that there exists an element of order 2 such that it possesses only one characteristic value 1. In fact, otherwise, by BURNSIDE's theorem, U is soluble. Then, since the order of N is 27, by the remark, we see easily that $G = U + UnU$, where n is any element $\neq 1$ of N, and $\{G, U\}$ is doubly transitive.

Case of type (8,2). Assume $5 | (U)$. Then, since U clearly does not contain a subgroup of index 5 (*in fact, otherwise, U must be of icosahedral type. But* $8 | (U)$), and since the order of N is 16, by the remark, we see easily that $G = U + UnU$, where n is any element $\neq 1$ of N, and $\{G, U\}$

[2]) Here we want to refer to the following interesting problem: Is there a primitive permutation group of MANNING—KOCHENDÖRFFER type not satisfying the condition (S)?

is doubly transitive. Thus we may assume that $5 \nmid (U)$. Now, by BURNSIDE's theorem, if $7 \nmid (U)$, then U is soluble. Since U is insoluble, $7 \mid (U)$. Again, by BURNSIDE's theorem, if $3 \nmid (U)$, then U is soluble. Since U is insoluble, $3 \mid (U)$. If $3^2 \mid (U)$, then U contains an element of order 3 which does not contain a characteristic value 1. Then, since the order of N is 16, by the remark, we see easily that $G = U + UnU$, where n is any element $\neq 1$ of N. But this implies $5 \mid (U)$, which is a contradiction. Therefore $3^2 \nmid (U)$ and $(U) \mid 2^6 . 3 . 7$. Let U_7 be a 7-Sylow subgroup of U. Since U is insoluble, U_7 is non-normal in U. Using SYLOW's theorem, we see either $(U) = 2^6 . 3 . 7$. or $(U) = 2^3 . 3 . 7$. Now if $\{G, U\}$ is simply transitive, then U contains a subgroup of index 7. Let V be such a subgroup. As it can be easily seen, V does not contain a normal subgroup $\neq 1$ of U. Further since U is insoluble, by BURNSIDE's theorem (BURNSIDE, 1) $\{U, V\}$ is doubly transitive. Therefore V contains a subgroup W such that (i) W is of index 6 in V and (ii) W does not contain a normal subgroup $\neq 1$ of V. (cf. § 1). First let us consider the case $(U) = 2^6 . 3 . 7$. Since the order of the symmetric group of degree 6 is $2^4 . 3^2 . 5$, W must contain a normal subgroup $\neq 1$ of V, which is a contradiction. Therefore $(U) = 2^3 . 3 . 7$. By Lemma 3, a 2-Sylow subgroup U_2 of U is abelian of type (4,2). As it can be easily seen, V contains a normal subgroup X of order 4. Clearly $W \cap X \neq 1$ is a normal subgroup of V, which is a contradiction.

8. Now we treat the remaining case where the type of the abelian group A is (8,4). But the fact is that this case does not occur. The present non-existence proof is complicated. We hope that it becomes trivially simple by a new method.

(1) We use the same notations as before. Let us consider $P_5 = P(5,2) V_5$. Then we want to show that P_5 does not contain an abelian subgroup A of type (8,4) such that $P_5 = P(5,2) A$. Put $P = A V_5 = U V_5$, where U is a subgroup of $P(5,2)$. Let $A_1 = \begin{pmatrix} B & C \\ 0 & D \end{pmatrix} \begin{pmatrix} b \\ c \end{pmatrix}$ and $A_2 = \begin{pmatrix} F & G \\ 0 & H \end{pmatrix} \begin{pmatrix} f \\ g \end{pmatrix}$ be the basic elements of A with orders 8 and 4 respectively, where the multiplication is that in P_5, and further

$$B = \begin{pmatrix} 1 & b_{12} \\ 0 & 1 \end{pmatrix}, \quad C = \begin{pmatrix} c_{11} & c_{12} & c_{13} \\ c_{21} & c_{22} & c_{23} \end{pmatrix}, \quad D = \begin{pmatrix} 1 & d_{12} & d_{13} \\ 0 & 1 & d_{23} \\ 0 & 0 & 1 \end{pmatrix}, \quad b = \begin{pmatrix} b_1 \\ b_2 \end{pmatrix},$$

$$c = \begin{pmatrix} c_1 \\ c_2 \\ c_3 \end{pmatrix}, \quad F = \begin{pmatrix} 1 & f_{12} \\ 0 & 1 \end{pmatrix}, \quad G = \begin{pmatrix} g_{11} & g_{12} & g_{13} \\ g_{21} & g_{22} & g_{23} \end{pmatrix}, \quad H = \begin{pmatrix} 1 & h_{12} & h_{13} \\ 0 & 1 & h_{23} \\ 0 & 0 & 1 \end{pmatrix},$$

$$f = \begin{pmatrix} f_1 \\ f_2 \end{pmatrix} \text{ and } g = \begin{pmatrix} g_1 \\ g_2 \\ g_3 \end{pmatrix},$$

and all the coefficients belong to the prime field of characteristic 2, that is, they are equal to 0 or 1. Moreover $\begin{pmatrix} B & C \\ 0 & D \end{pmatrix}$ and $\begin{pmatrix} F & G \\ 0 & H \end{pmatrix}$ belong to $P(5,2)$, and $\begin{pmatrix} b \\ c \end{pmatrix}$ and $\begin{pmatrix} f \\ g \end{pmatrix}$ belong to V_5.

(2) We shall make use of the following equations, where the multiplication except that of the elements of P_5 is the ordinary matrix multiplication:

(A. I) $$A_1^2 = \begin{pmatrix} E & BC+CD \\ 0 & D^2 \end{pmatrix} \begin{pmatrix} (B+E)b+Cc \\ (D+E)c \end{pmatrix} \quad (E \text{ denotes the unit matrix}).$$

(A. II) $$A_2^2 = \begin{pmatrix} E & FG+GH \\ 0 & H^2 \end{pmatrix} \begin{pmatrix} (F+E)f+Gg \\ (H+E)g \end{pmatrix}.$$

(B. I) $$A_1^4 = \begin{pmatrix} E & (BC+CD)(E+D^2) \\ 0 & E \end{pmatrix} \begin{pmatrix} (BC+CD)(D+E)c \\ 0 \end{pmatrix}.$$

(B. II) $$A_2^4 = \begin{pmatrix} E & (FG+GH)(E+H^2) \\ 0 & E \end{pmatrix} \begin{pmatrix} (FG+GH)(E+H)g \\ 0 \end{pmatrix}.$$

(C) The commutability of $\begin{pmatrix} B & C \\ 0 & D \end{pmatrix}$ and $\begin{pmatrix} F & G \\ 0 & H \end{pmatrix}$:

$$BF = FB, \ DH = HD, \ BG + CH = FC + GD.$$

(D) The commutability of A_1 and A_2 under the equation (B):

$$\begin{pmatrix} F & G \\ 0 & H \end{pmatrix}^{-1} \circ \begin{pmatrix} b \\ c \end{pmatrix} + \begin{pmatrix} f \\ g \end{pmatrix} = \begin{pmatrix} B & C \\ 0 & D \end{pmatrix}^{-1} \circ \begin{pmatrix} f \\ g \end{pmatrix} + \begin{pmatrix} b \\ c \end{pmatrix}$$

($\circ$ denotes the ordinary matrix multiplication).

(3) First we want to show that the order of the centre Z of P is equal to 2. In fact, if Z is of order greater than 2, we may assume, by choosing a suitable base of V_5, that $B = F = E$. Assume $D^2 = E$. Then by (B. 1) $A_1^4 = 1$, which is a contradiction. Hence $D^2 \neq E$ and $D^4 = E$. Therefore we may assume, if necessary, replacing A_1 by A_1^3, that $D = \begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}$. Assume $H = E$. Then, by (C), $G = GD$, whence $G = \begin{pmatrix} 0 & 0 & g_{13} \\ 0 & 0 & g_{23} \end{pmatrix}$. Since $A_2^2 \neq 1$ is a central element, $A_2^2 = \begin{pmatrix} Gg \\ 0 \end{pmatrix} = \begin{pmatrix} g_{13} & g_3 \\ g_{23} & g_3 \end{pmatrix} \neq 0$. In particular, $g_3 = 1$. On the other hand, by (D), $g = D^{-1}g$, whence $g_3 = 0$. This contradiction proves $H \neq E$. Since A_2^2 is a central element, $H^2 = E$ and $G(E+H) = 0$. By (C), $DH = HD$, whence $H = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$, and therefore, $g_{11} = g_{21} = 0$. By (C), $G + C \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} =$

$=C+G\begin{pmatrix}1&1&1\\0&1&1\\0&0&1\end{pmatrix}$, whence $g_{12}=c_{11}$ and $g_{22}=c_{11}$. By (D), $Hc+g=D^{-1}g+c$,

whence $g_3=0$, $g_2=c_3=1$. Now $A_1^4=\begin{pmatrix}c_{11}&c_3\\c_{21}&c_3\\0\\0\\0\end{pmatrix}$ and $A_2^2=\begin{pmatrix}g_{12}\\g_{22}\\0\\0\\0\end{pmatrix}$. Hence $A_1^4=A_2^2$ and $Z=\{A_1^4=A_2^2\}$. Then Z must be of order 2. This is a contradiction. Thus Z is of order 2.

(4) Now only the two types of U: (8,2) and (4,4) are allowable. First we prove that the type of U must be equal to (4,4). Assume that U is of type (8,2). Since A_1^4 does not belong to V_5, $\begin{pmatrix}B&C\\0&D\end{pmatrix}$ is of order 8. Therefore D is of order 4, and we may assume $D=\begin{pmatrix}1&1&1\\0&1&1\\0&0&1\end{pmatrix}$. Since A_2^2 is a central element $\neq 1$, $\begin{pmatrix}F&G\\0&H\end{pmatrix}$ is of order 2. By (C), $DH=HD$. Therefore, if necessary, replacing A_2 by $A_1^2A_2$, we may assume $H=E$. Assume $F=\begin{pmatrix}1&1\\0&1\end{pmatrix}$. Then, if necessary, replacing A_1 by A_1A_2, we may assume $B=E$. Then $\begin{pmatrix}B&C\\0&D\end{pmatrix}^4=E$. This contradiction proves $F=E$, and $B=\begin{pmatrix}1&1\\0&1\end{pmatrix}$. By (A. II), $\begin{pmatrix}(F+E)f+Gg\\(H+E)g\end{pmatrix}=$ $=\begin{pmatrix}Gg\\0\end{pmatrix}=\begin{pmatrix}g_{11}g_1+g_{12}g_2+g_{13}g_3\\g_{21}g_1+g_{22}g_2+g_{23}g_3\end{pmatrix}\neq 0$. By (C), $BG=GD$, whence $g_{11}=g_{21}=$ $=g_{22}=0$. By (D), $g=D^{-1}g$, whence $g_2=g_3=0$. Then $\begin{pmatrix}Gg\\0\end{pmatrix}=0$. This is a contradiction. Thus U is of type (4,4).

(5) At any rate, $\begin{pmatrix}B&C\\0&D\end{pmatrix}$ and $\begin{pmatrix}F&G\\0&H\end{pmatrix}$ are of order 4, respectively. Put $F=\begin{pmatrix}1&1\\0&1\end{pmatrix}$. If necessary, replacing A_1 by A_1A_2, we may assume $B=E$. Assume $D^2=E$. Then, by (B. I), $0\neq\begin{pmatrix}C(D+E)^2C\\0\end{pmatrix}=0$. Hence $D^2\neq E$ and $D=E$. If necessary, replacing A_1 by A_1^3, we may assume $D=\begin{pmatrix}1&1&1\\0&1&1\\0&0&1\end{pmatrix}$. If H is of order not greater than 2, if necessary, replacing A_2 by $A_1^2A_2$, we may assume $H=E$. Now by (C), $G+C=FC+GD$, whence $c_{21}=g_{21}=g_{22}=0$. By (A. II), since A_2^2 does not belong to V_5, $(F+E)G\neq 0$, whence either g_{21} or g_{22} or $g_{23}=1$. Hence $g_{23}=1$. Now by (D) $g=D^{-1}g$, whence $g_2=g_3=0$.

Again by (D), $Fb+FGc=CD^{-1}g+b$, whence, in particular, $g_{21}c_1+g_{22}c_2+$ $+g_{23}c_3=c_{21}g_1+(c_{21}+c_{22})g_2+(c_{22}+c_{23})g_3$. Hence $c_3=0$. On the other hand, by (B. I), since A_1^4 is a central element $\neq 1$, $\begin{pmatrix}(BC+CD)(D+E)C\\ 0\end{pmatrix}=\begin{pmatrix}c_{11}\ c_3\\ c_{21}\ c_3\\ 0\\ 0\\ 0\end{pmatrix}$, whence $c_3=1$. This contradiction proves that H is of order 4. If necessary, replacing A_2 by A_2^3, we may assume $H=\begin{pmatrix}1&1&1\\0&1&1\\0&0&1\end{pmatrix}$. Now by (C), $G+C\begin{pmatrix}1&1&1\\0&1&1\\0&0&1\end{pmatrix}=\begin{pmatrix}1&1\\0&1\end{pmatrix}C+G\begin{pmatrix}1&1&1\\0&1&1\\0&0&1\end{pmatrix}$, whence $c_{21}=g_{21}=0$, $c_{22}=g_{22}$, $c_{11}=c_{22}+g_{11}$. By (B. I), since A_1^4 is a central element $\neq 1$, $\begin{pmatrix}(BC+CD)(D+E)c\\ 0\end{pmatrix}=$ $=\begin{pmatrix}c_{11}\ c_3\\ c_{21}\ c_3\\ 0\\ 0\\ 0\end{pmatrix}\neq 0$, whence $c_3=1$ and $c_{11}=1$. By (D), $\begin{pmatrix}1&1&0\\0&1&1\\0&0&1\end{pmatrix}c+g=\begin{pmatrix}1&1&0\\0&1&1\\0&0&1\end{pmatrix}g+c$, whence $g_3=c_3=1$. By (B. II), since $A_2^4=1$, $\begin{pmatrix}(FG+GH)(E+H)g\\ 0\end{pmatrix}=$ $=\begin{pmatrix}g_{21}g_2+(g_{21}+g_{22}+g_{11})g_3\\ g_{21}g_3\\ 0\\ 0\\ 0\end{pmatrix}=0$, whence $g_{11}+g_{22}=0$. Then, $c_{11}=c_{22}+g_{11}=$ $=g_{22}+g_{11}=0$. Thus $c_{11}=1=0$. This is a contradiction. Thus $F=\begin{pmatrix}1&0\\0&1\end{pmatrix}$.

(6) Now assume $B=\begin{pmatrix}1&0\\0&1\end{pmatrix}$. Since the order of A_1 is 8, by (B. II), D is of order 4. If necessary, replacing A_1 by A_1^3, we may assume $D=\begin{pmatrix}1&1&1\\0&1&1\\0&0&1\end{pmatrix}$. Now if H is of order not greater than 2, then, by (C), since $DH=HD$, we may assume, if necessary, replacing A_2 by $A_2A_1^2$, that $H=\begin{pmatrix}1&0&0\\0&1&0\\0&0&1\end{pmatrix}$. By (A. II), $1\neq A_2^2=\begin{pmatrix}Gg\\ 0\end{pmatrix}$ belongs to V_5, which is a contradiction. Thus H must be

of order 4. Therefore, if necessary, replacing A_2 by A_2^3, we may assume $H=\begin{pmatrix}1&1&1\\0&1&1\\0&0&1\end{pmatrix}$. By (C), $G+C\begin{pmatrix}1&1&1\\0&1&1\\0&0&1\end{pmatrix}=C+G\begin{pmatrix}1&1&1\\0&1&1\\0&0&1\end{pmatrix}$, whence $c_{11}=g_{11}$, and $c_{21}=g_{21}$. By (D), $H^{-1}c+g=D^{-1}g+c$, whence $c_3=g_3$. By (B. I),

$$0\neq\begin{pmatrix}(BC+CD)(D+E)C\\0\end{pmatrix}=\begin{pmatrix}c_{11}\ c_3\\c_{21}\ c_3\\0\\0\\0\end{pmatrix},$$ whence $c_3=1$ and either c_{11} or $c_{21}=1$.

By (B. II), $$0=\begin{pmatrix}(FG+GH)(E+H)g\\0\end{pmatrix}=\begin{pmatrix}g_{11}\ g_3\\g_{21}\ g_3\\0\\0\\0\end{pmatrix},$$ whence, since $g_3=c_3=1$,

$g_{11}=g_{21}=0$. Then, since $c_{11}=g_{11}$, $c_{21}=g_{21}$, $c_{11}=0$ and $c_{21}=0$. This contradiction proves $B=\begin{pmatrix}1&1\\0&1\end{pmatrix}$.

(7) Now let us assume that D is of order 4. Then, if necessary, replacing A_1 by A_1^3, we may assume that $D=\begin{pmatrix}1&1&1\\0&1&1\\0&0&1\end{pmatrix}$. Now if H is of order not greater than 2, then, by (C), since $DH=HD$, we may assume if necessary, replacing A_2 by $A_2A_1^2$, that $H=\begin{pmatrix}1&0&0\\0&1&0\\0&0&1\end{pmatrix}$. By (A. II), $1\neq A_2^2=\begin{pmatrix}Gg\\0\end{pmatrix}$ belongs to V_5, which is a contradiction. Thus H must be of order 4. Therefore, if necessary, replacing A_2 by A_2^3, we may assume $H=\begin{pmatrix}1&1&1\\0&1&1\\0&0&1\end{pmatrix}$.

By (C), $\begin{pmatrix}1&1\\0&1\end{pmatrix}G+C\begin{pmatrix}1&1&1\\0&1&1\\0&0&1\end{pmatrix}=C+G\begin{pmatrix}1&1&1\\0&1&1\\0&0&1\end{pmatrix}$, whence $c_{21}=g_{21}=0$, $c_{22}=g_{22}$ and $c_{11}=g_{11}+g_{22}$. By (D), $H^{-1}c+g=D^{-1}g+c$, whence $c_3=g_3$. By (B. I), since $A_1^4\neq1$ is a central element, $$\begin{pmatrix}(BC+CD)(D+E)c\\0\end{pmatrix}=\begin{pmatrix}(c_{11}+c_{22})\,c_3\\0\\0\\0\\0\end{pmatrix}\neq0,$$

whence $c_3=1$ and $c_{11}+c_{22}=1$. By (B. II), since $A_2^4=1$, $\begin{pmatrix}(FG+GH)(E+H)g\\0\end{pmatrix}=$

$$=\begin{vmatrix} g_{11} & g_3 \\ & 0 \\ & 0 \\ & 0 \\ & 0 \end{vmatrix}=0,$$ whence, since $g_3=c_3=1$, $g_{11}=0$. Then $c_{11}=g_{22}=c_{22}$.

Hence $c_{11}+c_{22}=0$. This is a contradiction. Thus D must be of order not greater than 2. If $D=E$, then, by (B. I), $A_1^4=1$. This contradiction proves that the order of D is 2.

(8) Assume that H is of order 4. Then, if necessary, replacing A_2 by A_2^3, we may assume $H=\begin{pmatrix}1&1&1\\0&1&1\\0&0&1\end{pmatrix}$. By (C), $DH=HD$. Therefore $D=\begin{pmatrix}1&0&1\\0&1&0\\0&0&1\end{pmatrix}$.

By (B. I), since $A_1^4\neq 1$ is a central element, $\begin{pmatrix}(BC+CD)\,(D+E)c\\0\end{pmatrix}\neq 0$, whence $c_3=1$. By (D), $H^{-1}c+g=Dg+c$, whence $c_3=0$. This is a contradiction. Thus H must be of order not greater than 2. If $H=E$, then, by (A. II), $1\neq A_2^2=\begin{pmatrix}Gg\\0\end{pmatrix}$ belongs to the centre, which is a contradiction. Thus H is of order 2.

(9) Put, for abbreviation,

$$M_1=\begin{pmatrix}1&0&1\\0&1&0\\0&0&1\end{pmatrix},\quad M_2=\begin{pmatrix}1&0&0\\0&1&1\\0&0&1\end{pmatrix},\quad M_3=\begin{pmatrix}1&1&0\\0&1&0\\0&0&1\end{pmatrix},$$

$$M_4=\begin{pmatrix}1&0&1\\0&1&1\\0&0&1\end{pmatrix},\quad M_5=\begin{pmatrix}1&1&1\\0&1&0\\0&0&1\end{pmatrix}.$$

Since, by (C), $DH=HD$, the following seventeen pairs of $\{D,H\}$ are only to be considered:

(i) $\{M_1,M_1\}$, (ii) $\{M_1,M_2\}$, (iii) $\{M_1,M_3\}$, (iv) $\{M_1,M_4\}$, (v) $\{M_1,M_5\}$, (vi) $\{M_2,M_1\}$, (vii) $\{M_2,M_2\}$, (viii) $\{M_2,M_4\}$, (ix) $\{M_3,M_1\}$, (x) $\{M_3,M_3\}$, (xi) $\{M_3,M_5\}$, (xii) $\{M_4,M_1\}$, (xiii) $\{M_4,M_2\}$, (xiv) $\{M_4,M_4\}$, (xv) $\{M_5,M_1\}$, (xvi) $\{M_5,M_3\}$, (xvii) $\{M_5,M_5\}$.

Now let us assume $c_3=0$. Since A_1^4 is a central element $\neq 1$, by (B. I)

$$0\neq\begin{pmatrix} c_{21} & d_{12} & c_2 \\ & 0 & \\ & 0 & \\ & 0 & \\ & 0 & \end{pmatrix},$$ whence $c_{21}=d_{12}=c_2=1$. By (C), $c_{21}h_{12}=0$. Hence $h_{12}=0$.

There remain only two cases: (ix) and (xv). In these cases $d_{23}=h_{23}=0$. By (C), $c_{21}=h_{13}+c_{22}h_{23}=g_{22}d_{23}$. Hence $h_{13}=0$. This is a contradiction. Thus $c_3=1$.

Now let us assume $d_{23}=0$. By (B. I), $0 \neq \begin{pmatrix} c_{11}\, d_{12}\, c_2 + c_{21}\, d_{13} \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}$, whence $c_{21}=1$. By (C) $c_{21}h_{12}=0$. Hence $h_{12}=0$. There remain the cases (i), (ii). (iv), (ix), and (xv). Now in the cases (i), (ix), (xv), $h_{23}=0$: By (C), $c_{21}h_{13}+c_{22}h_{23}=g_{22}d_{23}$. Hence $h_{13}=0$. This is a contradiction: Further in the cases (ii), (iv), $h_{23}=1$. By (D), $h_{23}c_3=d_{23}g_3$. Hence $d_{23}=1$. This is a contradiction. Thus $d_{23}=1$. There remain the cases (vi), (vii), (viii), (xii), (xiii) and (xiv). In these cases $h_{12}=d_{12}=0$. Therefore, by (D), $h_{13}=d_{13}g_3$. Hence if $h_{13}=1$, then $d_{13}=1$. Thus the cases (vi) and (viii) vanish. Again by (D), $h_{23}c_3=d_{23}g_3$. Hence $h_{23}=g_3$. If $h_{23}=0$, then $g_3=0$ and therefore $h_{13}=0$. This is a contradiction. Thus $h_{23}=g_3=1$ and $h_{13}=d_{13}$. Thus the cases (xii) and (xiii) vanish. Now let us consider the case (vii). Then $h_{13}=d_{13}=0$. By (B. I), $0 \neq \begin{pmatrix} c_{21}\, d_{13}+c_{22} \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}$, whence $c_{22}=1$. By (C), $c_{21}h_{13}+c_{22}h_{23}=g_{22}d_{23}$ and $g_{22}+c_{11}h_{12}=g_{11}d_{12}$. Hence $c_{22}=0$. This is a contradiction. Last let us consider the case (xiv). Then $h_{13}=d_{13}=1$. By (B. I), $0 \neq \begin{pmatrix} c_{21}\, d_{13}+c_{22} \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}$, whence $c_{31}+c_{22}=1$. By (C), $c_{21}h_{13}+c_{22}h_{23}=g_{22}d_{23}$ and $g_{22}+c_{11}h_{12}=g_{11}d_{12}$. Hence $c_{31}+c_{22}=0$. This is a contradiction.

Q. E. D.

Now, in the long run, if a primitive permutation group $\{G, U\}$ of KOCHENDÖRFFER—MANNING type satisfies the condition (S), then G is insoluble. Further if such a $\{G, U\}$ does not satisfy the condition (S), then primarily G is insoluble. Thus we can say that *a primitive permutation group $\{G, U\}$ of Kochendörffer—Manning type is insoluble.*

9. Now the following two questions may be natural: (1) With some exceptionals which happen for $p=2$, any primitive permutation group with an abelian transitive subgroup not of type $(p, \ldots, p)$ is insoluble? (2) If a primitive permutation group has an abelian transitive subgroup, at least one invariant of which occurs only once, then is this primitive permutation group doubly transitive?

The second question can be answered *negatively*. Let us start from the examples $\{G, U\}$; $G=UN=UA$, where $U=GL(p,p)$, $H=V_p$ and A is of type $(p^2, p, \ldots, p)$, which are constructed in § 5. Let $\{G_i, U_i\}$; N_i and

A^i be the r copies of $\{G, U\}$; N and A, where r is a natural number >1. Then we construct the permutation group $\{G^{**}, U^{**}\}$ by KOCHENDÖRFFER's method of construction in § 6. Put $A^{***}=A_1 \times N_2 \times \cdots \times N_r$. We have only to show the transitivity of A^{***}. As in § 3 put $U^*=U_1 \times \cdots \times U_r$ and $G^*=G_1 \times \cdots \times G_r$. Then clearly $A^{***}U^*=G^*$, whence $A^{***}U^{**}=G^{**}$.

For the first problem we have only partial answers. Let $\{G, U\}$; $G=UN=UA$ be a soluble primitive permutation group with an abelian transitive subgroup A not of type $(p, \ldots, p)$. Further let p^n be the order of N and let p be greater than 2.

(1) (cf. § 7) U may be considered as a subgroup of $GL(n, p)$.

(2) (cf. § 7) U does not contain a normal p-subgroup $\neq 1$.

(3) Put $AN=V \cdot N$, where V is a subgroup of U. Then V is an abelian p-subgroup of U. Now U does not contain a subgroup L such that (i) L is irreducible for $N=V_n$ and (ii) the normalizer of L contains V and L is a minimal normal subgroup of LV.

In fact, let U contain such a subgroup L. Then, by (2), the centralizer of L in LV is coincident with L itself. Therefore we can consider L as a faithful irreducible representation module for V. Therefore V is cyclic [cf. HUPPERT]. Since $p>2$, by Lemma 3, this is a contradiction.

Now let us notice that $n \geqq p > 2$. Therefore there exists a prime q such that $p^n \equiv 1 \pmod q$ and $p^m \not\equiv 1 \pmod q$ for any $m<n$ (ZSIGMONDY [1]). Then the order of U cannot be divisible by such a q.

In fact let the order of U be divisible by such a q. First we remark that in these circumstances any subgroup of U whose order is divisible by q is irreducible. By Hall's theorem (HALL [2]) there exists a $\{p, q\}$-Sylow subgroup $U_{\{p,q\}}$ (a Hall subgroup) in U. Since $U_{\{p,q\}}$ is irreducible for N, by (2), $U_{\{p,q\}}$ does not contain a normal p-subgroup $\neq 1$. Let Q be a minimal normal q-subgroup $\neq 1$ of $U_{\{p,q\}}$ and let us consider the subgroup QV. Again let Q_1 be a minimal normal q-subgroup $\neq 1$ of QV and let us consider the subgroup Q_1V. Since Q_1V is irreducible for N, by (2) Q_1V does not contain a normal p-subgroup $\neq 1$. Therefore the centralizer of Q_1 in Q_1V is coincident with Q_1 itself. Therefore we can consider Q_1 as a faithful, irreducible representation module of V. Therefore V is cyclic (cf. HUPPERT [1]). Since $p>2$, by Lemma 3, this is a contradiction.

As a corollary of the above result we see that $\{G, U\}$ is necessarily simply transitive.

In fact, if $\{G, U\}$ is doubly transitive, then the order of U is divisible by p^n-1.

Addendum. Recently Mr. BERTRAM HUPPERT in Tübingen has independently obtained, by interesting methods, similar results as those of the present paper. See his paper „Primitive, auflösbare Permutationsgruppen", *Archiv für Math.*, **6**(1955), 303—310.

Literature.

BURNSIDE, W. [1] On some properties of groups of odd order, *Proc. London Math. Soc.*, **33** (1900), 162—185.

[2] On groups of order $p^\alpha q^\beta$, *Proc. London Math. Soc.*, (2) **1** (1904), 388—392.

ČUNIHIN, S. [1] O Π-svoĭstvah konečnyh grupp, *Mat. Sbornik*, **25** (67) (1949), 321—346.

DICKSON, L. E. [1] *Linear groups* (Leipzig, 1901).

FROBENIUS, G. [1] Über Relationen zwischen den Charakteren einer Gruppe und denen ihrer Untergruppen, *Sitzungsberichte Berlin* (1898), 501—515.

HALL, P. [1] A contribution to the theory of groups of primepower orders, *Proc. London Math. Soc.*, (2) **36** (1933), 29—95.

[2] A note on soluble groups, *Journal London Math. Soc.*, **3** (1928), 98—105.

HUPPERT, B. [1] Normalteiler und maximale Untergruppen endlicher Gruppen, *Math. Zeitschrift*, **60** (1954), 409—434.

KOCHENDÖRFFER, R. [1] Untersuchung über eine Vermutung von W. Burnside, *Schriften Math. Sem. u. Inst. f. angew. Math. Univ. Berlin*, **3** (1937), 155—180.

MANNING, D. [1] On simply transitive groups with transitive Abelian subgroups of the same degree, *Transactions American Math. Soc.*, **40** (1936), 324—342.

RITT, J. F. [1] On algebraic functions which can be expressed in terms of radicals *Transactions American Math. Soc.*, **24** (1922), 27—30.

SCHREIER, O. [1] Über die Erweiterung von Gruppen. II, *Hamburger Abh.*, **4** (1926), 321—346.

WIELANDT, H. [1] Zur Theorie der einfach transitiven Permutationsgruppen, *Math. Zeitschrift*, **40** (1935), 582—587.

ZSIGMONDY, K. [1] Zur Theorie der Potenzreste, *Monatshefte für Math. und Phys.*, **3** (1892), 265—286.

(Received August 28, 1954.)