On a property of a finite group

By Nagayoshi IWAHORI*

§ 0. Introduction.

Let G be a finite group. A set M is called a G-space if G acts on M as a transformation group, i.e. if there is defined a map $G\times M\to M:(g,x)\to g\cdot x$ such that

(i) $1\cdot x=x$ for any $x\in M$. (1 denotes the unit element of G.)

(ii) $a(bx)=(ab)x$ for any $a, b\in G$ and for any $x\in M$.

A subset L of M of the form $\{gx_0 ; g\in G\}$ is called a *G-orbit* in M. Let M be a G-space and $g\in G$. We denote by M_g the subset of M consisting of the elements of M fixed by g:

$$M_g=\{x\in M ; g\cdot x=x\}.$$

Also for a subset S of G, we denote by M_S the set $\bigcap_{g\in S} M_g$. Now let $x\in M$. We denote by G_x the *isotropy subgroup* of the point x i.e.

$$G_x=\{g\in G ; g\cdot x=x\}.$$

Also for a subset N of M, we denote by G_N the subgroup of G defined by $G_N=\bigcap_{x\in N} G_x$. In the following the cardinality of a set A will be denoted by $|A|$.

DEFINITION 1. Let k be a positive integer. A G-space M is called *of type k* if

(I) $|M_g|=k$ for every $g\in G-\{1\}$,

(II) $M_G=\phi$ (ϕ means the empty set).

DEFINITION 2. Let M be a G-space of a finite group G. M is called *pure* if M is the union of the M_g's for all $g\in G-\{1\}$.

Let us observe that if a finite group G admits a G-space M of type k, then G cannot be cyclic. Also, if M is a pure G-space of type k, then M is a finite set and for any point $x\in M$ we have $G_x\neq\{1\}$ and $G_x\neq G$.

Let us observe also the following fact: let M be a G-space of a finite group G and assume that M is of type k. Then M contains a finite subset P which is G-stable and is a pure G-space of type k under the natural action of G. In fact, let P be the union of M_g for $g\in G-\{1\}$. Then $gP=P$ since $gM_a=M_{gag^{-1}}$ for any

* This research was supported by the National Science Foundation under Grant NSF-G 14100.

$a \in G$. Thus P is a G-space under the natural action of G. Now let $g \in G - \{1\}$. Then we have obviously that $P_g = M_g$ for any $g \in G - \{1\}$. Hence P is a pure G-space of type k. It is easily seen that such a subset P of M (i.e. that P is G-stable and that P is a pure G-space of type k under the natural action of G) is unique. We shall call the subset P just defined *the pure part* of the G-space M which is of type k.

Thus, when we consider the existence of a G-space of type k, we may restrict ourselves without any loss of generality to the consideration of the existence of pure G-spaces of type k.

DEFINITION 3. A finite group G is called *of positive type* if G admits a G-space of type k for some positive integer k. A finite group is called *of type 0* if it is not of positive type. When G is of positive type, a positive integer k will be called *a type number* of G if there exists a G-space of type k. We denote by $t(G)$ the least type number of G. When G is of type 0, we put $t(G)=0$.

EXAMPLE 0. 1. The three-dimensional rotation group (special orthogonal group) $SO(3)$ acts in a natural way on the 2-sphere M and we have $|M_g|=2$ for any $g \in SO(3)-\{1\}$. It is easily verified that for any non-cyclic finite subgroup G of $SO(3)$, M is a G-space of type 2.

EXAMPLE 0. 2. Let G be a finite Frobenius group, i.e. we assume that there is a G-space $\mathfrak{M}$ such that

(i) G is transitive on $\mathfrak{M}$,

(ii) $|\mathfrak{M}_g| \leqq 1$ for every $g \in G-\{1\}$,

(iii) $1 < |\mathfrak{M}| < |G|$.

Then $t(G) > 0$.

In fact, let x_0 be a point of $\mathfrak{M}$. Then there is a normal subgroup N of G such that $G = G_{x_0} N$, $G_{x_0} \cap N = \{1\}$. (cf. e.g. [2, p. 242 (35. 1)]). Let $\mathfrak{M}_1, \cdots, \mathfrak{M}_k$ ($k=|G_{x_0}|=[G:N]$) be k copies of $\mathfrak{M}$. Consider the disjoint union $M=\mathfrak{M}_0 \cup \mathfrak{M}_1 \cup \cdots \cdots \cup \mathfrak{M}_k$ where $\mathfrak{M}_0 = G/N$. Since each $\mathfrak{M}_i$ is a G-space, M is also a G-space in a natural way. It is seen easily that M is a pure G-space of type k.

We shall give in § 1 several elementary but useful lemmas. Using the lemmas we shall determine the finite abelian groups of positive type. We shall prove the following

THEOREM I. *A finite abelian group is of positive type if and only if it is not cyclic and is isomorphic with an elementary abelian group (i.e. the additive group of some finite field).*

In § 2, we shall give a criterion for a finite group to be of positive type in terms of group-characters of G, i.e. we shall prove the following

THEOREM II. *A finite group G admits a G-space of type k if and only if there exist subgroups $G_1, \cdots, G_r$ of G (not necessarily distinct) such that*

(a) $G \neq G_i \neq \{1\}$ for $i=1, \cdots, r$.

(b) $1^*_{G_1}+\cdots+1^*_{G_r}=k\cdot 1^*_G+(r-k)\cdot 1^*_{\{1\}}$

where $1^*_{G_i}$ means the character of G induced by the unit character 1_{G_i} *of the subgroup G_i of G,* i.e. $1^*_{G_i}(g)=\dfrac{|G|}{|G_i|}\dfrac{|\mathfrak{K}_g\cap G_i|}{|\mathfrak{K}_g|}$ where $\mathfrak{K}_g=\{aga^{-1};\ a\in G\}$.

Then we get immediately the following

COROLLARY. *Let K be an algebraic number field of finite degree over the rational number field $\mathbf{Q}$ and k a subfield of K. Assume that K/k is a Galois extension with the Galois group G and that G is of positive type. Then there exist subfields $K_1, \cdots, K_r$ of K (not necessarily distinct) and positive integers α, β such that*

(a′) $K\neq K_i\neq k$ for $i=1, \cdots, r$.

(*b′*) $\zeta_{K_1}(s)\zeta_{K_2}(s)\cdots\zeta_{K_r}(s)=\zeta_k(s)^{\alpha}\zeta_K(s)^{\beta}$

where $\zeta_{K_i}(s)$ means the Dedekind zeta-function of K_i.

The subgroups $G_1, \cdots, G_r$ which appear in Theorem II have some remarkable properties. To begin with we give the

DEFINITION 4. A subgroup H of a finite group G is called *special* if $H\neq\{1\}$, $H\neq G$ and if 1^*_H is constant on $C-\{1\}$ for any cyclic subgroup C of G.

Then (see Prop. 2. 5), in Th. II, every G_i is special and every subgroup C with $t(C)=0$ of G is contained in one of the conjugates of the G_i's. In particular, every cyclic subgroup of G is contained in one of the conjugates of the G_i's.

In § 3 we shall determine finite groups G which satisfy $t(G)=2$. We shall prove the following theorem which is an analogue of the classical determination of the groups of regular polyhedra (cf. example 0. 1 above).

THEOREM III. *Let G be a finite group.* Then $t(G)=2$ *if and only if G is one of the following groups*:

(i) $\mathfrak{A}_4$ *(the alternating group on 4 letters)*

(ii) $\mathfrak{S}_4$ *(the symmetric group on 4 letters)*

(iii) $\mathfrak{A}_5$ *(the alternating group on 5 letters)*

(iv) *G is a generalized dihedral group in the following sense: G contains an abelian normal subgroup H of index 2 and an involutive element a such that* $a\notin H$, $aha^{-1}=h^{-1}$ for every $h\in H$, *and that the 2-Sylow subgroup of H is cyclic.*

Finally in § 4, we shall prove the following

THEOREM IV. *The linear fractional groups $LF(2, q)$ $(=PSL(2, F_q)$ are of positive type.*

Using the basic Lemma 1. 2, we shall show the following two theorems.

THEOREM V. *Let $\mathfrak{g}$ be a simple Lie algebra over the complex number field and F_q a finite field with q elements. Let G, G' be the Chevalley groups associated to the pair* ($\mathfrak{g}$, F_q) (cf. [1]). *Let l be the rank of $\mathfrak{g}$. Assume that the following* (i), (ii) *are satisfied:*

(i) $l \geqq 3$ or $\mathfrak{g}=(G_2)$ *(exceptional simple Lie algebra of rank 2),*

(ii) $q>3$ *and* $q-1$ *is not a prime number.*

Then $t(G)=t(G')=0$.

THEOREM VI. *Let $\mathfrak{g}$ be a simple Lie algebra over the complex number field and W the Weyl group of $\mathfrak{g}$.* (cf. [4, Exposé 14]). *Then $t(W)>0$ if and only if $\mathfrak{g}$ is of type*

$$(A_2),\ (A_3),\ (A_4),\ (B_2),\ (G_2)$$

in the classification of E. Cartan.

§ 1. Basic lemmas and the determination of finite abelian groups of positive type.

We begin with the

LEMMA 1. 1. *Let G be a finite group and k a positive integer. Let M be a G-space of type k. Then*

(i) $|M_H|=k$ *for any subgroup* $H(\neq\{1\})$ *of G with* $t(H)=0$.

(ii) *If A, B are subgroups of G with $A\cap B\neq\{1\}$, $t(A)=t(B)=0$, then $M_A=M_B$.*

PROOF. (i) Let $|M_H|=k'$. If $k'<k$, then $M-M_H$ is a H-space of type $k-k'>0$, which is impossible. Hence $k'\geqq k$. On the other hand, if $h\in H-\{1\}$, we have $M_H\subset M_h$, hence $k'\leqq k$ and we have $k=k'$.

(ii) Let $g\in A\cap B-\{1\}$. Then we have seen above that $M_A=M_g=M_B$, Q.E.D.

LEMMA 1. 2. *(Covering Lemma) Let G be a finite group and $A_1, \cdots, A_r$ subgroups of G such that*

(i) $t(A_1)=\cdots=t(A_r)=0$,

(ii) $A_i\cap A_{i+1}\neq\{1\}$ *for* $i=1, \cdots, r-1$,

(iii) $A_1, \cdots, A_r$ *generate* G.

Then $t(G)=0$.

PROOF. Assume that G admits a G-space M of type k for some positive integer k. Then (i) and (ii) imply that

$$M_{A_1}=\cdots=M_{A_r}, \qquad |M_{A_1}|=k.$$

(see Lemma 1. 1). Then (iii) implies that $M_{A_1}\subset M_G$. Hence $M_G\neq\phi$ which is a contradiction, Q.E.D.

EXAMPLE 1. 1. Let G be a generalized quaternion group of order $4n$, i.e. G is generated by a, b together with the defining relations

$$a^2=b^n, \qquad aba^{-1}=b^{-1}.$$

Then $t(G)=0$.

In fact, a generates a cyclic subgroup A of order 4 and b generates a cyclic subgroup B of order $2n$. A and B generate G and $t(A)=t(B)=0$, $A\cap B\ni a^2\neq 1$. Hence $t(G)=0$ by Lemma 2. 1.

LEMMA 1. 3. *Let G be finite group and M a G-space of type $k>0$. Let a and b be elements in $G-\{1\}$ with orders e and f respectively. Assume that*

(i) $ab=ba$, *and*

(ii) $e\neq f$ *or* $e=f\neq$prime.

Then $M_a=M_b$.

PROOF. Assume that $e<f$. Then the intersection of two cyclic subgroups $\{ab\}$ and $\{b\}$ contains the cyclic subgroup $\{b^e\}$ which is not the unit group. Hence $M_{ab}=M_b$ by Lemma 1. 1. But this gives $M_a=M_b$ immediately. Now suppose that $e=f\neq$prime. Let p be a prime divisor of f. Then the intersection of two cyclic subgroups $\{a\}$ and $\{ab^p\}$ is not the unit group. Hence $M_a=M_{ab^p}$; therefore $M_a=M_{b^p}=M_b$, Q.E.D.

PROPOSITION 1. 4. *Let G be a finite group of positive type. Then the center Z of G is the unit group or an elementary abelian group.*

PROOF. Assume that $Z\neq 1$. Then Z is a direct product of the cyclic subgroups $Z_1, \cdots, Z_r$. Let $e_i=|Z_i|$ $(i=1, \cdots, r)$. We may assume that $e_i|e_{i+1}$ $(i=1, \cdots, r-1)$. We have only to show that e_r is a prime number. Let M be a G-space of type $k>0$ and b a generator of Z_r. If e_r is not a prime number then $M_a=M_b$ for every $a\in G-\{1\}$, (see Lemma 1. 3). Then $M_b\subset M_G$. Hence $M_G\neq\phi$ which is impossible, Q.E.D.

EXAMPLE 1. 2. Let F_q be a finite field with $q>2$. Assume that $q-1$ is not a prime. Then $t(GL(n, F_q))=0$ for $n=1, 2, \cdots$.

In fact, the center Z of $GL(n, F_q)$ is isomorphic with the multiplicative group F_q^* which is cyclic of order $q-1$. Hence, if $q-1$ is not a prime, $GL(n, F_q)$ is of type 0 by Prop. 1. 4.

COROLLARY 1. 5. *Let G be a finite nilpotent group of positive type. Then G is a p-group for some prime number p.*

PROOF OF THEOREM I. If G is a finite abelian group of positive type, then G is an elementary abelian group by Prop. 1. 4. Of course G is not cyclic.

Conversely, let G be a non-cyclic finite abelian group isomorphic with the direct product $Z_p\times Z_p\times\cdots\times Z_p$ of several cyclic groups Z_p of prime order p. Let $G_1, \cdots, G_r$ be the totality of all distinct cyclic subgroups of G of order p. Let M be the disjoint union of the G-spaces $G/G_1, \cdots, G/G_r$. Then it is easily verified that M is a pure G-space of type k, where k is the index of G_1 in G. This completes the proof of Theorem I.

§ 2. A criterion for a finite group to be of positive type.

LEMMA 2. 1. *Let G be a finite group and M a finite G-space. Then the number of G-orbits in M (which we shall denote by $|G/M|$) is given by*

$$|G/M| = \frac{1}{|G|} \sum_{g \in G} |M_g|$$

PROOF. Let $M = M_1 \cup \cdots \cup M_r$ be the partition of M into G-orbits. Then $|M_g| = \sum_i |M_g \cap M_i|$. Hence it is enough to show that

$$1 = \frac{1}{|G|} \sum_{g \in G} |M_g \cap M_i|.$$

In other words we have only to prove our lemma when G is transitive on M. Let Γ be the subset of $G \times M$ given by

$$\Gamma = \{(g, x) \in G \times M;\ gx = x\}.$$

For any $g \in G$, the number of $(g, x) \in \Gamma$ equals $|M_g|$. Thus

$$|\Gamma| = \sum_{g \in G} |M_g|.$$

On the other hand, when G is transitive on M, $|G_x|$ is independent on $x \in M$ and is equal to $|G|/|M|$. Now the number of $(g, x) \in \Gamma$ for fixed $x \in M$ is nothing but $|G_x|$. Hence we have

$$|\Gamma| = \sum_{x \in M} |G_x| = |M| \cdot (|G|/|M|) = |G|.$$

Thus we have $|G| = \sum_{g \in G} |M_g|$. Q.E.D.

PROPOSITION 2. 2. *Let G be a finite group and M a pure G-space of type $k > 0$. Let $M = M_1 \cap \cdots \cup M_r$ be the partition of M into G-orbits. Let $x_i \in M_i$ $(i=1, \cdots, r)$* and $G_{x_i} = G_i$ $(i=1, \cdots, r)$. *Then we have*

(i) $k \geqq 2$,

(ii) $2k > r > k$,

(iii) $|M| - k = (r-k)|G|$,

(iv) $k + \sum_{i=1}^{r} \frac{1}{|G_i|} = r + \frac{k}{|G|}$,

(v) $\sum_{i=1}^{r} 1^*_{G_i} = k \cdot 1^*_G + (r-k) \cdot 1^*_{\{1\}}$.

PROOF. By Lemma 2. 1 applied on the pair (G, M) we have $r|G| = |M| + k(|G| - 1)$, which implies (iii) immediately. Now since $|M| = \sum_{i=1}^{r} |M_i|$, $|M_i| = \frac{|G|}{|G_i|}$ $(i=1, \cdots, r)$, we have by (iii) that

$$\sum_{i=1}^{r}\frac{|G|}{|G_i|}-k=(r-k)|G|,$$

which gives (iv) immediately.

M being a pure G-space of type k, we have $2\leqq|G_i|<|G|$ for $i=1, \cdots, r$. Hence we get from (iv) that

$$k+\frac{r}{2}\geqq r+\frac{k}{|G|}>r \quad \text{and} \quad k+\frac{r}{|G|}<r+\frac{k}{|G|}.$$

These inequalities imply (ii) easily.

Now (i) is an immediate consequence of (ii). Finally if we observe that $1^*_{G_i}(g)=|M_i\cap M_g|(g\in G)$, we see that the value of the left hand side of (v) for $g\in G-\{1\}$ is equal to k because $k=|M_g|=\sum_{i=1}^{r}|M_i\cap M_g|$. The right hand side is also equal to k since $1^*_G(g)=1$, $1^*_{\{1\}}(g)=0$. Now for $g=1$, the left hand side of (v) equals

$$\sum_{i=1}^{r}\frac{|G|}{|G_i|}=|M|,$$

while the right hand side equals $k+(r-k)|G|$ which is $|M|$ by (iii). Thus we have obtained (v), Q.E.D.

COROLLARY 2. 3. *Let G be a p-group and M a pure G-space of type k. Then* $k\equiv 0$ (mod. p).

PROOF. Under the notations of Prop. 2. 2, we have $|M|\equiv 0$ (mod. p) since $G\neq G_i$ $(i=1, \cdots, r)$. Hence $k\equiv 0$ (mod. p) by Prop. 2. 2, (iii).

PROOF OF THEOREM II. The first half of Theorem II was shown above in Prop. 2. 2, (v).

Conversely let G be a finite group and assume that there exist subgroups $G_1, \cdots, G_r$ of G satisfying the conditions (a) and (b) of Theorem II. Let M be the disjoint union of the G-spaces $M_i=G/G_i$ $(i=1, \cdots, r)$. Then, since $1^*_{G_i}(g)=|(M_i)_g|$, it is easy to verify that M is a pure G-space of type k.

PROPOSITION 2. 4. *Let G be a finite abelian group which admits a pure G-space M of type k. Then $|G|\leqq k^2$.*

PROOF. For any $g\in G-\{1\}$, M_g is G-stable since G is abelian. Thus M_g is a union of G-orbits in M. Now any G-orbit M_i of M has a non-empty intersection with some M_g, $g\in G-\{1\}$ since M is pure. Hence $M_i\subset M_g$ and we have $|M_i|\leqq k$. Let $M=M_1\cup\cdots\cup M_r$ be the partition of M into G-orbits. Then we get by Prop. 2. 2, (iii) that $(r-k)|G|+k=|M|=\sum_{i=1}^{r}|M_i|\leqq rk$. Hence we have

$$|G|\leqq\frac{k(r-1)}{r-k}=k\left(1+\frac{k-1}{r-k}\right)\leqq k^2,$$

because $1+\dfrac{k(r-1)}{r-k}\leqq k$, Q.E.D.

PROPOSITION 2. 5. *Let G be a finite group and $G_1, \cdots, G_r$ be subgroups such that $G \neq G_i \neq \{1\}$ $(i=1, \cdots, r)$ and $\sum_{i=1}^{r} 1_{G_i}^* = k \cdot 1_G^* + l \cdot 1_{\{1\}}^*$ for some integers k, l. Then every G_i is a special subgroups of G (see* Def. 4). *Moreover, if a subgroup H of G does not admit any H-space of type k, then some G_i contains a subgroup which is conjugate with H in G. In particular, any subgroup H with $t(H)=0$ is contained in one of the conjugates of the $G_1, \cdots, G_r$.*

PROOF. Comparing the value at $g \in G-\{1\}$ of the function $\sum_i 1_{G_i}^* = k \cdot 1_G^* + l \cdot 1_{\{1\}}^*$ we see that $k \geqq 0$. If $k=0$, then $\sum 1_{G_i}^* = l \cdot 1_{\{1\}}^*$ implies that $G_i = \{1\}$ which is impossible. Hence $k>0$. Then, putting $M_i = G/G_i$ $(i=1, \cdots, r)$, $M = M_1 \cup \cdots \cup M_r$ (disjoint union), we see that M is a pure G-space of type k. To show that G_i is special, it is enough to show that $1_{G_i}^*(\sigma) = 1_{G_i}^*(\sigma^j)$ for σ, $\sigma^j \in G-\{1\}$. Now since $1_{G_i}^*(\sigma) = |(M_i)_\sigma|$ and $1_{G_i}^*(\sigma^j) = |(M_i)_{\sigma^j}|$, we have $1_{G_i}^*(\sigma) \leqq 1_{G_i}^*(\sigma^j)$. However $k = \sum_i 1_{G_i}^*(\sigma)$ and $k = \sum_i 1_{G_i}^*(\sigma^j)$ imply that $1_{G_i}^*(\sigma) = 1_{G_i}^*(\sigma^j)$ $(i=1, \cdots, r)$. Hence G_i is special.

Now assume that a subgroup H of G does not admit any H-space of type k. Then M_H is not empty. In fact, $M_H = \phi$ implies that M is also a H-space of type k which is impossible. Thus there exists some integer i with $M_i \cap M_H \neq \phi$. Take a point x in $M_i \cap M_H$. Then the isotropy group G_x is conjugate with G_i in G and H is obviously contained in G_x, Q.E.D.

§ 3. Determination of finite groups with $t(G)=2$.

Now let us prove Theorem III. Let G be a finite group which admits a pure G-space M of type 2. Let $M = M_1 \cup \cdots \cup M_r$ be the partion of M into the G-orbits $M_1, \cdots, M_r$. Then $r=3$ by Prop. 2.2, (ii). Choose points x_i $(i=1, 2, 3)$ and let $G_i = G_{x_i}$. We may assume that $|G_1| \leqq |G_2| \leqq |G_3|$. Then by Prop. 2.2, (ii) we have $2 + \frac{3}{|G_1|} \geqq 3 + \frac{2}{|G|} > 3$. Hence $|G_1| = 2$ and we get

$$\frac{1}{|G_2|} + \frac{1}{|G_3|} = \frac{1}{2} + \frac{2}{|G|}.$$

This implies that $\frac{2}{|G_2|} > \frac{1}{2}$. Hence $|G_2| = 2$ or 3. Suppose that $|G_2| = 2$. Then we have $|G| = 2|G_3|$. Now suppose that $|G_2| = 3$. Then we get

$$\frac{1}{|G_3|} = \frac{1}{6} + \frac{2}{|G|}. \qquad \text{Hence } 6 > |G_3| \geqslant 3.$$

Therefore $|G_3| = 3, 4, 5$. Then $|G| = 12, 24, 60$ respectively. Thus we have obtained for the possible order of G_1, G_2, G_3, G the following table:

G_1	G_2	G_3	G
2	2	n	$2n$
2	3	3	12
2	3	4	24
2	3	5	60

CASE I. $(G_1, G_2, G_3 ; G)=(2, 2, n ; 2n)$.

Since the subgroup G_3 is of index 2 in G, G_3 is a normal subgroup of G. Now any element g $(\neq 1)$ of G_3 has a fixed point in M_3; moreover g fixes every point in M_3 since M_3 consists of two points. Hence we get $M_g=M_3$ for any $g\in G_3-\{1\}$. Thus $G_1\cap G_3=\{1\}$; therefore $G=G_1G_3$ is a semi-direct product. Let a be the generator of G_1. Then for any $g\in G_3$ we have $M_{ga}\cap M_3=\phi$, i.e. $M_{ga}\subset M_1\cup M_2$. Hence ga is conjugate with an element in G_1 or in G_2. Therefore $(ga)^2=1$, i.e. $aga^{-1}=g^{-1}$. Hence G_3 admits an automorphism $g\longrightarrow aga^{-1}=g^{-1}$. Thus G_3 is an abelian group.

Next let us show that the 2-Sylow subgroup of G_3 is cyclic. Consider the subgroup $A=\{g\in G_3 ; g^2=1\}$. Then by what we have shown above A is contained in the center of G. The A-orbit $A(x_1)$ of the point $x_1\in M_1$ consists of $|A|$ points since $A\cap G_1=\{1\}$. Moreover $A(x_1)\subset M_a$ because A is central. Thus we get $|A|\leqq 2$. However this implies immediately that the 2-Sylow subgroup of G_3 is cyclic. Thus we have proved that G is a generalized dihedral group in the sense of Theorem III, (iv).

Conversely let G be a finite group which contains an abelian normal subgroup H of index 2 and an involutive element a such that $a\notin H$, $aha^{-1}=h^{-1}$ for every $h\in H$, and that the 2-Sylow subgroup of H is cyclic. We assume that $H\neq\{1\}$.

Then it is easy to see that every element of $G-H$ is involutive. Also two elements h_1a and h_2a $(h_1, h_2\in H)$ are conjugate in G if and only if $h_1\equiv h_2$ (mod. H^2) where H^2 denotes the subgroup of H defined by $H^2=\{h^2 ; h\in H\}$. Hence if $|H|$ is odd, then $G-H$ forms a single conjugate class of G; if $|H|$ is even, then $G-H$ consists of two conjugate classes of G. Now let b be an element of $G-H$ such that

(i) b is not conjugate with a if $|H|$ is even,

(ii) b is any element in $G-H$ distinct from a if $|H|$ is odd. Let $G_1=\{1, a\}$, $G_2=\{1, b\}$, $G_3=H$. Let us define a G-space M as the disjoint union of the G-spaces G/G_1, G/G_2, G/G_3. We have to show that M is a G-space of type 2. Clearly if $g\in G_3$, then $|M_g|=2$. Now let $g\in G-G_3$. We distinguish two cases according to $|H|$ even or odd.

(i) Suppose that $|H|$ is even. Then g is conjugate to a or b. We may assume that g is conjugate to a. Then g has no fixed points in G/G_2 or in G/G_3. Now for $c\in G$, $gcG_1=cG_1$ is equivalent to $c^{-1}gc=a$. Hence $|M_g|$ is equal to the index $[C_G(a) : G_1]$, where $C_G(a)$ means the centralizer of a in G. Now it is easy to see that $C_G(a)$ is given by

$$C_G(a)=A\cup Aa,$$

where $A=\{h\in H\,;\,h^2=1\}$. Now since $|H|$ is even and the 2-Sylow subgroup of H is cyclic, A is of order 2 and we get $|M_g|=2$.

(ii) Suppose that $|H|$ is odd. Then g is conjugate to a and b. We see that g has exactly one fixed point in G/G_1 and G/G_2 respectively by a similar argument as in the previous case.

CASE II. $(G_1, G_2, G_3\,;\,G)=(2, 3, 3\,;\,12)$

Since G acts on the set M_3 consisting of 4 points, we have a homomorphism $\varphi: G\longrightarrow\mathfrak{S}_4$. If $g\in G$ is in the kernel of φ, then g has at least 4 fixed points; hence $g=1$ and φ is one-to-one. Now $\varphi(G)$ is a subgroup of $\mathfrak{S}_4$ of order 12, hence $\varphi(G)=\mathfrak{A}_4$. Thus G is isomorphic with $\mathfrak{A}_4$.

Conversely let $G=\mathfrak{A}_4$. Then G admits a pure G-space of type 2; namely the classical tetrahedral group in $SO(3)$ acts on the 2-sphere S^2 and S^2 is a $\mathfrak{A}_4$-space of type 2. (cf. Example 0. 1.)

CASE III. $(G_1, G_2, G_3\,;\,G)=(2, 3, 4\,;\,24)$.

In this case G_2 is a 3-Sylow subgroup of G. Let N be the normalizer of G_2 in G. Then as is well-known $[G:N]\equiv 1$ (mod. 3). On the other hand, $[G:N]$ is a divisor of 8. Hence $[G:N]$ is either 1 or 4. Suppose that $[G:N]=1$. Then G_2 is a normal subgroup of G. Then $M_2\subset M_{G_2}$. However this is impossible since $|M_2|=8$, $|M_{G_2}|\leqq 2$.

Thus we get $[G:N]=4$, i.e. N is a subgroup of G of order 6. N is not abelian. (In fact, if N is abelian, then N is cyclic and G contains an element of order 6 which is however impossible.) Hence N is isomorphic with $\mathfrak{S}_3$ and G_2 is the commutator subgroup of N: $[N, N]=G_2$. Since G_2 is not normal in G, N is not normal in G too.

By the action of G on G/N, we get a homomorphism φ from G into $\mathfrak{S}_4$. Let us show that φ is one-to-one. Let A be the kernel of φ. Then A is the largest normal subgroup of G contained in N. But $N(\cong\mathfrak{S}_3)$ cannot contain any normal subgroup of order 2; also $A\neq N$. Hence $|A|=3$ or 1. If $|A|=3$, then $A=G_2$; which is impossible since G_2 is not normal in G. Thus we get $A=\{1\}$ and φ is one-to-one. Now G and $\mathfrak{S}_4$ are of the same order, hence φ is an isomorphism onto.

Conversely $G=\mathfrak{S}_4$ admits a pure G-space of type 2; namely the classical octahedral group.

CASE IV. $(G_1, G_2, G_3\,;\,G)=(2, 3, 5\,;\,60)$.

In this case every element of G is of order 1 or 2 or 3 or 5.

Let a be any element of order 2 in G. Denote by S the centralizer of a in G. Since a is contained in a 2-Sylow subgroup of G which is of order 4, we have $\{1, a\}\neq S$. Now S cannot contain any element of odd order. In fact, if S contains an element g of odd order e, then ag is of order $2e$ which is impossible. Thus we have shown that S is of order 4 and is a 2-Sylow subgroup of G.

Now let us show that if S_1 and S_2 are two distinct 2-Sylow subgroups of G, then $S_1 \cap S_2 = \{1\}$. In fact, if $S_1 \cap S_2$ is of order 2, then the generator a of $S_1 \cap S_2$ centralizes any element in S_1 or in S_2. Hence the centralizer of a contains the set $S_1 S_2$ which consists of $4 \cdot 4/2 = 8$ elements. This is impossible.

Now let S be the centralizer of G_1 in G and N the normalizer of S in G. Let us show that $[G : N] = 5$. In fact, let $S_1, \cdots, S_r$ be the totality of all distinct 2-Sylow subgroups of G. Then the union $\bigcup_{i=1}^{r} (S_i - \{1\})$ is a disjoint one and coincides with the set of all involutive elements in G. Now since any involutive element of G has its fixed points in the set M_1, it must be conjugate with the generator of G_1. Thus any two elements in $\bigcup_{i=1}^{r} (S_i - \{1\})$ are conjugate with each other. We have seen above that the number of elements in the conjugate class consisting of involutive elements is $60/4 = 15$. Thus we get the equality; $3r = 15$; hence $r = 5$ which gives immediately that $[G : N] = 5$.

By the action of G on G/N, we get a homomorphism φ from G into $\mathfrak{S}_5$. To prove that $G \cong \mathfrak{A}_5$, it is enough to show that φ is one-to-one. ($\mathfrak{A}_5$ is the only subgroup of order 60 in $\mathfrak{S}_5$.) Let K be the kernel of φ. K is the largest normal subgroup of G contained in N.

Now N is not abelian. In fact, if N is abelian, N contains an element of order 6 since $|N| = 12$, which is impossible. Thus the commutator subgroup $[N, N]$ is contained in S and different from $\{1\}$. Hence $[N, N]$ is of order 2 or 4. Suppose that $[N, N]$ is of order 2. Let b be the generator of $[N, N]$. Then b is involutive and is in the center of N. Thus the centralizer of b contains at least 12 elements which is impossible. Thus we have shown that $[N, N] = S$.

Now N is not normal in G. In fact, if N is normal in G, then $S = [N, N]$ is also normal in G which contradicts to the fact that $G \neq N$. Therefore K is a proper subgroup of N; hence the order of K is 1 or 2 or 3 or 4 or 6.

Suppose that $|K| = 2$. Then the generator of K is an involutive element whose centralizer is the whole G, which is impossible.

Suppose that $|K| = 3$. Then N is the direct product of K and S. Hence N is abelian, which is impossible.

Suppose that $|K| = 4$. Then N/K is abelian and K contains S. Hence $K = S$ and S is normal in G, which is impossible.

Suppose finally that $|K| = 6$. Then again N/K is abelian and K contains S. But this is impossible since 4 does not divide 6.

Thus we have shown that $K = \{1\}$ and $G \cong \mathfrak{A}_5$.

Conversely $G = \mathfrak{A}_5$ admits a pure G-space of type 2; namely the classical icosahedral group. Thus we have proved Theorem III.

§ 4. Existence of G-spaces of positive type for $LF(2, q)$, Chevalley groups and Weyl groups.

Let F_q be the finite field consisting of q elements. We denote by $SL(2, F_q)$ the group of all 2 by 2 matrices with determinant unity over F_q. The factor group of $SL(2, F_q)$ over its center is denoted by $PSL(2, F_q)$ or by $LF(2, q)$. Let us now consider the question whether the group $G=LF(2, q)$ admits a G-space of type k for some positive integer k.

Now the character table of $LF(2, q)$ is known. (cf. [3, § 6]). We denote by $\tilde{\mathfrak{H}}$ the subgroup of $SL(2, F_q)$ consisting of diagonal matrices; we also denote by $\tilde{\mathfrak{U}}$ the subgroup of $SL(2, F_q)$ consisting of matrices of the form $\begin{pmatrix} 1 & t \\ 0 & 1 \end{pmatrix}$, $t \in F_q$. We denote by $\tilde{R}$ an element (but fixed once for all) of $SL(2, F_q)$ of order $q+1$. ($\tilde{R}$ is similar to a diagonal matrix in $SL(2, F_{q^2})$. $\tilde{\mathfrak{H}}$ is a cyclic group of order $q-1$. We fix once for all a generator $\tilde{Q}$ of $\tilde{\mathfrak{H}}$. Put $\tilde{P}=\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$, $\tilde{P}^*=\begin{pmatrix} 1 & \rho \\ 0 & 1 \end{pmatrix}$ where ρ is a generator of the multiplicative group F_q^* fixed once for all. We denote by $\tilde{\mathfrak{R}}$ the cyclic subgroup of $SL(2, F_q)$ generated by $\tilde{R}$. $\tilde{\mathfrak{H}}\tilde{\mathfrak{U}}$ is a subgroup of $SL(2, F_q)$; we denote this subgroup by $\tilde{B}$.

We denote the images of the canonical homomorphism $SL(2, F_q) \longrightarrow LF(2, q)$ of the elements $\tilde{P}$, $\tilde{P}^*$, $\tilde{Q}$, $\tilde{R}$, or the subgroups $\tilde{\mathfrak{H}}$, $\tilde{\mathfrak{U}}$, $\tilde{\mathfrak{R}}$, $\tilde{B}$ by the corresponding letters P, P^*, Q, R, $\mathfrak{H}$, $\mathfrak{U}$, $\mathfrak{R}$, B respectively.

We distinguish 3 cases according to $q \equiv 1$ (mod. 4), $q \equiv 3$ (mod. 4), or $q \equiv 0$ (mod. 2) to describe the character table.

CASE I. $q \equiv 1$ (mod. 4). Put $q=4n+1$.

There are $2n+3$ conjugate classes represented by the elements:

$$1,\ P,\ P^*,\ Q,\ Q^2,\ \cdots,\ Q^n,\ R,\ R^2,\ \cdots,\ R^n.$$

The $2n+3$ irreducible characters of $LF(2, q)$ are given by

		1	P	P^*	Q^i	R^j
	χ_1	1	1	1	1	1
	χ_q	q	0	0	1	-1
	$\chi_{2n+1}^{(1)}$	$2n+1$	$(1+\sqrt{q})/2$	$(1-\sqrt{q})/2$	$(-1)^i$	0
	$\chi_{2n+1}^{(2)}$	$2n+1$	$(1-\sqrt{q})/2$	$(1+\sqrt{q})/2$	$(-1)^i$	0
$(1 \leq l \leq n-1)$	$\chi_{q+1}^{(l)}$	$q+1$	1	1	$\alpha^{li}+\alpha^{-li}$	0
$(1 \leq m \leq n)$	$\chi_{q-1}^{(m)}$	$q-1$	-1	-1	0	$-(\beta^{mj}+\beta^{-mj})$

where $\alpha=\exp(2\pi i/2n)$, $\beta=\exp(2\pi i/2n+1)$.

From this table and the Frobenius reciprocity, we get the following table for the induced characters of subgroups $\mathfrak{H}$, $\mathfrak{U}$, $\mathfrak{N}$, and B.

$$1^*_{\mathfrak{H}}=\chi_1+3\chi_q+\sum_{i=1}^{2}\chi^{(i)}_{2n+1}+2\sum_{l=1}^{n-1}\chi^{(l)}_{q+1}+2\sum_{m=1}^{n}\chi^{(m)}_{q-1},$$

$$1^*_{\mathfrak{U}}=\chi_1+\chi_q+\sum_{i=1}^{2}\chi^{(i)}_{2n+1}+2\sum_{l=1}^{n-1}\chi^{(l)}_{q+1},$$

$$1^*_{\mathfrak{N}}=\chi_1+\chi_q+\sum_{i=1}^{2}\chi^{(i)}_{2n+1}+2\sum_{l=1}^{n-1}\chi^{(l)}_{q+1}+2\sum_{m=1}^{n}\chi^{(m)}_{q-1},$$

$$1^*_B=\chi_1+\chi_q.$$

Then we can verify easily that $\mathfrak{H}$, B, $\mathfrak{N}$, $\mathfrak{U}$ are special subgroups of $G=LF(2, q)$ and that the values of the class functions $1^*_{\mathfrak{H}}$, 1^*_B, $1^*_{\mathfrak{N}}$, $1^*_{\mathfrak{U}}$ are given as follows:

	1	P	P^*	Q^i	R^j
$1^*_{\mathfrak{H}}$	$q(q+1)$	0	0	2	0
$1^*_{\mathfrak{U}}$	$(q^2-1)/2$	$(q-1)/2$	$(q-1)/2$	0	0
$1^*_{\mathfrak{N}}$	$q(q-1)$	0	0	0	2
1^*_B	$q+1$	1	1	2	0

From this table we get immediately that

$$i\cdot 1^*_{\mathfrak{H}}+(2n-2i)\cdot 1^*_B+(2n-i)\cdot 1^*_{\mathfrak{N}}+1^*_{\mathfrak{U}}=(4n-2i)\cdot 1^*_G+1^*_{\{1\}}$$

$(i=0, 1, \cdots, n)$. In particular $G=LF(2, q)$ admits a G-space of type $2n=\dfrac{q-1}{2}$.

CASE II. $q\equiv 3 \pmod 4$. Put $q=4n+3$.

There are $2n+4$ conjugate classes represented by the elements:

$$1,\ P,\ P^*,\ Q,\ Q^2,\ \cdots,\ Q^n,\ R,\ R^2,\ \cdots,\ R^{n+1}.$$

The $2n+4$ irreducible characters are given by

		1	P	P^*	Q^i	R^j
	χ_1	1	1	1	1	1
	χ_q	q	0	0	1	-1
	$\chi^{(1)}_{2n+1}$	$2n+1$	$\dfrac{-1+\sqrt{q}\,i}{2}$	$\dfrac{-1-\sqrt{q}\,i}{2}$	0	$(-1)^{j+1}$
	$\chi^{(2)}_{2n+1}$	$2n+1$	$\dfrac{-1-\sqrt{q}\,i}{2}$	$\dfrac{-1+\sqrt{q}\,i}{2}$	0	$(-1)^{j+1}$
$(1\leqq l\leqq n)$	$\chi^{(l)}_{q+1}$	$q+1$	1	1	$\alpha^{li}+\alpha^{-li}$	0
$(1\leqq m\leqq n)$	$\chi^{(m)}_{q-1}$	$q-1$	-1	0	0	$-(\beta^{mj}+\beta^{-mj})$

where $\alpha=\exp(2\pi i/2n+1)$, $\beta=\exp(2\pi i/2n+2)$.

The induced characters are given by

$$1_{\mathfrak{H}}^{*}=\chi_1+3\chi_q+\sum_{i=1}^{2}\chi_{2n+1}^{(i)}+2\sum_{l=1}^{n}\chi_{q+1}^{(l)}+2\sum_{m=1}^{n}\chi_{q-1}^{(m)},$$

$$1_{\mathfrak{U}}^{*}=\chi_1+\chi_q+2\sum_{l=1}^{n}\chi_{q+1}^{(l)},$$

$$1_{\mathfrak{N}}^{*}=\chi_1+\chi_q+\sum_{i=1}^{2}\chi_{2n+1}^{(i)}+2\sum_{l=1}^{n}\chi_{q+1}^{(l)}+2\sum_{m=1}^{n}\chi_{q-1}^{(m)},$$

$$1_{B}^{*}=\chi_1+\chi_q.$$

Then we can verify easily that $\mathfrak{H}$, B, $\mathfrak{N}$, $\mathfrak{U}$ are special subgroups of $G=LF(2, q)$ and that the values of the class functions $1_{\mathfrak{H}}^{*}$, 1_{B}^{*}, $1_{\mathfrak{N}}^{*}$, $1_{\mathfrak{U}}^{*}$ are given as follows:

	1	P	P^*	Q^i	R^j
$1_{\mathfrak{H}}^{*}$	$q(q+1)$	0	0	2	0
$1_{\mathfrak{U}}^{*}$	$(q^2-1)/2$	$(q-1)/2$	$(q-1)/2$	0	0
$1_{\mathfrak{N}}^{*}$	$q(q-1)$	0	0	0	2
1_{B}^{*}	$q+1$	1	1	2	0

From this table we get immediately that

$$i\cdot 1_{\mathfrak{H}}^{*}+(2n+1-2i)\cdot 1_{B}^{*}+(2n+1-i)\cdot 1_{\mathfrak{N}}^{*}+1_{\mathfrak{U}}^{*}=(4n+2-2i)\cdot 1_{G}^{*}+1_{(1)}^{*}$$

$(i=0, 1, \cdots, n)$. In particular $G=LF(2, q)$ admits a G-space of type $2n+2=\frac{q+1}{2}$.

CASE III. $q\equiv 0 \pmod{2}$. Put $q=2n+2$.

There are $2n+3$ conjugate classes represented by the elements:

$$1,\ P,\ Q,\ Q^2,\ \cdots,\ Q^n,\ R,\ R^2,\ \cdots,\ R^{n+1}.$$

The $2n+3$ irreducible characters are given by

		1	P	Q^i	R^j
	χ_1	1	1	1	1
	χ_2	q	0	1	-1
$(1\leq l\leq n)$	$\chi_{q+1}^{(l)}$	$q+1$	1	$\alpha^{li}+\alpha^{-li}$	0
$(1\leq m\leq n+1)$	$\chi_{q-1}^{(m)}$	$q-1$	-1	0	$-(\beta^{mj}+\beta^{-mj})$

where $\alpha=\exp(2\pi i/2n+1)$, $\beta=\exp(2\pi i/2n+3)$.

The induced characters are given by

$$1_{\mathfrak{H}}^{*}=\chi_1+2\chi_q+\sum_{l=1}^{n}\chi_{q+1}^{(l)}+\sum_{m=1}^{n+1}\chi_{q-1}^{(m)},$$

$$1_{\mathfrak{U}}^{*}=\chi_1+\chi_q+\sum_{l=1}^{n}\chi_{q+1}^{(l)},$$

$$1_{\mathfrak{R}}^* = \chi_1 + \sum_{l=1}^{n} \chi_{q+1}^{(l)} + \sum_{m=1}^{n+1} \chi_{q-1}^{(m)},$$

$$1_B^* = \chi_1 + \chi_q.$$

Then we can verify easily that $\mathfrak{H}$, B, $\mathfrak{R}$, $\mathfrak{U}$ are special subgroups of $G=LF(2, q)$ and that the values of the class functions $1_{\mathfrak{H}}^*$, 1_B^*, $1_{\mathfrak{R}}^*$, $1_{\mathfrak{U}}^*$ are given as follows:

	1	P	Q^i	R^j
$1_{\mathfrak{H}}^*$	$q(q+1)$	0	2	0
$1_{\mathfrak{U}}^*$	q^2-1	$q-1$	0	0
$1_{\mathfrak{R}}^*$	$q(q-1)$	0	0	2
1_B^*	$q+1$	1	2	0

From this table we get immediately that

$$i\cdot 1_{\mathfrak{H}}^* + (2n+1-2i)\cdot 1_B^* + (2n+1-i)\cdot 1_{\mathfrak{R}}^* + 1_{\mathfrak{U}}^* = (4n+2-2i)\cdot 1_G^* + 1_{\{1\}}^*$$

$(i=0, 1, \cdots, n)$. In particular, $G=LF(2, q)$ admits a G-space of type $2n+2=q$.

Thus we have proved Theorem IV.

Let us now proceed to the proof of Theorem V. Let $\mathfrak{g}$ be a simple Lie algebra over the complex number field and F_q a finite field with q elements. Let G, G' be the Chevalley groups associated to the pair $(\mathfrak{g}, F_q)$ (cf. [1]). We use the notations in [1]. In particular, for any root α of $\mathfrak{g}$, there is associated a homomorphism ϕ_α from $SL(2, F_q)$ into G' (cf. [1, p. 36]). We denote by G_α the image of $SL(2, F_q)$ under ϕ_α. The module generated by roots of $\mathfrak{g}$ is denoted by P_r. Then for any $\chi \in \mathrm{Hom}(P_r, F_q^*)$ (F_q^* is the multiplicative group of the field F_q), there is associated an element $h(\chi)$ of G and $\chi \longrightarrow h(\chi)$ is an injective homomorphism from $\mathrm{Hom}(P_r, F_q^*)$ into G. The image of this injection is denoted by $\mathfrak{H}$ (see [1, p. 36]). The intersection $\mathfrak{H} \cap G'$ is denoted by $\mathfrak{H}'$. Then for any root α and for any $z \in F_q^*$, the element $\chi_{\alpha,z} \in \mathrm{Hom}(P_r, F_q^*)$ defined by $\chi_{\alpha,z}(\beta) = z^{2(\beta,\alpha)/(\alpha,\alpha)}$ $(\beta \in P_r)$ determines an element $h(\chi_{\alpha,z}) \in G'$ (see [1, p. 47]).

Now it is seen easily using the formulas in [1, p. 36] that $G_\alpha\mathfrak{H}'$ is a subgroup of G' and the $G_\alpha\mathfrak{H}'$ generate G' when α ranges over the root system. Moreover, for any two roots α, β we have $G_\alpha\mathfrak{H}' \cap G_\beta\mathfrak{H}' \supset \mathfrak{H}'$. Hence if $q>2$, we have $G_\alpha\mathfrak{H}' \cap G_\beta\mathfrak{H}' \neq \{1\}$. Thus to show that $t(G')=0$, we have only to show that $t(G_\alpha\mathfrak{H}')=0$ for every root α (cf. Lemma 1. 2). Now if the rank l of $\mathfrak{g}$ is at least 3 or $\mathfrak{g}=(G_2)$, then there is a root β orthogonal to α with respect to the Killing form of $\mathfrak{g}$. Let ρ be a generator of the cyclic group F_q^*. Then $\chi_{\beta,\rho}$ is of order $q-1$. In fact, since $l \geqq 3$ or $\mathfrak{g}=(G_2)$, there exists a root γ which satisfies

$$\frac{2(\beta, \gamma)}{(\gamma, \gamma)} = 1.$$

Hence $\chi_{\beta,\rho}(\gamma) = \rho$ is of order $q-1$. On the other hand, it is easy to see that $\chi_{\beta,\rho}^{q-1} = 1$. Hence $\chi_{\beta,\rho}$ is of order $q-1$. Accordingly $h(\chi_{\beta,\rho})$ is also of order $q-1$. Now it is not difficult to see that $h(\chi_{\beta,\rho})$ is in the center of $G_\alpha\mathfrak{H}'$ using the formulas in [1, p. 36]. Thus the center of $G_\alpha\mathfrak{H}'$ is not an elementary abelian group if $q-1$ is not a prime. Hence $t(G_\alpha\mathfrak{H}') = 0$ and we get $t(G') = 0$.

Similarly, considering $G_\alpha\mathfrak{H}$ instead of $G_\alpha\mathfrak{H}'$ we conclude that $t(G) = 0$. Thus we have proved Theorem V.

Next let us prove Theorem VI. Let $\mathfrak{g}$ be a simple Lie algebra over the complex number field and Δ the root system of $\mathfrak{g}$ with respect to a Cartan subalgebra $\mathfrak{h}$ of $\mathfrak{g}$. Let $\Pi = \{\alpha_1, \cdots, \alpha_l\}$ be a fundamental root system of Δ. We denote by w_i the reflection with respect to the hyperplane orthogonal to α_i. Then the Weyl group W of $\mathfrak{g}$ is generated by $w_1, \cdots, w_l$. (cf. [4, Exposé 14]).

Let us divide the proof of Theorem VI into several steps.

LEMMA 4. 1. *Let* $\mathfrak{g} = (A_l)$, $l \geqq 5$ *or* $l = 1$. *Then* $t(W) = 0$.

PROOF. If $\mathfrak{g} = (A_1)$, then W is a cyclic group of order 2. Hence $t(W) = 0$. Suppose now that $l = 5$. Let α_0 be the highest root of Δ with respect to Π and w_0 the associated reflection. Then we can construct a chain of subgroups $A_1, A_2, \cdots, A_{10}$ in Lemma 1. 2 as follows:

$$A_1 = \langle w_1 w_3 w_4 \rangle, \quad A_2 = \langle w_1 w_4 w_5 \rangle, \quad A_3 = \langle w_2 w_4 w_5 \rangle, \quad A_4 = \langle w_2 w_5 w_0 \rangle,$$
$$A_5 = \langle w_3 w_5 w_0 \rangle, \quad A_6 = \langle w_3 w_0 w_1 \rangle, \quad A_7 = \langle w_4 w_0 w_1 \rangle, \quad A_8 = \langle w_4 w_1 w_2 \rangle,$$
$$A_9 = \langle w_5 w_1 w_2 \rangle, \quad A_{10} = \langle w_5 w_2 w_3 \rangle.$$

($\langle \sigma \rangle$ means the cyclic subgroup generated by σ.) Then each A_i is cyclic of order 6, $A_i \cap A_{i+1} \neq \{1\}$ $(i = 1, \cdots, 9)$ since $w_i^2 = 1$, $(w_i w_{i+1})^3 = 1$ (w_6 means w_0) $w_i w_j = w_j w_i$ (if $|i-j| \geqq 2$) for all $0 \leqq i, j \leqq 5$. Moreover the subgroup A generated by $A_1, \cdots, A_{10}$ contains $w_1, \cdots, w_5$. Thus $A = W$ and we have $t(W) = 0$ by Lemma 1. 2. We have proved thus that the symmetric group $\mathfrak{S}_6$ is of type 0.

Let us show that $t(\mathfrak{S}_n) = 0$ for $n \geqq 6$ by the induction on n. In fact $\mathfrak{S}_n$ $(n > 6)$ contains two subgroups A, B such that $A \cong \mathfrak{S}_{n-1}$, $B \cong \mathfrak{S}_{n-1}$, $A \cap B \neq \{1\}$ and that A, B generate $\mathfrak{S}_n$. Then we have $t(A) = t(B) = 0$. Hence $t(\mathfrak{S}_n) = 0$ by Lemma 1. 2, Q.E.D.

LEMMA 4. 2. *Let* $\mathfrak{g} = (B_l)$ *or* (C_l), $l \geqq 3$. *Then* $t(W) = 0$.

PROOF. W is realized as a subgroup DS of $GL(l, C)$ where D is the group of all diagonal matrices δ with $\delta^2 = 1$ and S is the group of all permutation matrices in $GL(l, C)$. Thus $S \cong \mathfrak{S}_l$.

Now let us consider the case where $l=3$. Let A_1, A_2, A_3 be the subgroups of $W=DS$ generated by

$$\begin{pmatrix} 0 & 1 & 0 \\ -1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix} \text{ and } -1 ; \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & -1 & 0 \end{pmatrix} \text{ and } -1 ; \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ -1 & 0 & 0 \end{pmatrix} \text{ and } -1$$

respectively. Then A_i is an abelian group of order 8 and contains an element of order 4. Hence $t(A_i)=0$ by Prop. 1. 4. Obviously we have $A_i \cap A_j \neq \{1\}$ for any $1 \leqq i,\ j \leqq 3$. Moreover let Γ be the subgroup of W generated by A_1, A_2, A_3. It is seen easily that $\Gamma \supset D,\ S$. Hence $\Gamma = W$ and we have $t(W)=0$ by Lemma 1. 2.

The case $l>3$ is proved similarly as in Lemma 4. 1 using the induction on l, Q.E.D.

LEMMA 4. 3. *Let* $\mathfrak{g}=(D_l)$, $l \geqq 4$. *Then* $t(W)=0$.

PROOF. W is realized as a subgroup D^+S of $GL(l,\ C)$ where D^+ is the subgroup of all diagonal matrices δ with $\delta^2=1$, $\det(\delta)=1$ and S is the group of all permutation matrices in $GL(l,\ C)$. Thus $S \cong \mathfrak{S}_l$.

Now let us consider the case where $l=4$. Let A_1, A_2, A_3 be the subgroups of $W=D^+S$ generated by

$$\begin{pmatrix} 0 & 1 & 0 & 0 \\ -1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix} \text{ and } -1 ; \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix} \text{ and } -1 ; \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & -1 & 0 \end{pmatrix} \text{ and } -1$$

respectively. Then A_i is an abelian group of order 8 and contains an element of order 4. Hence $t(A_i)=0$ by Prop. 1. 4. Obviously we have $A_i \cap A_j \neq \{1\}$ for any $1 \leqq i,\ j \leqq 3$. Moreover let Γ be the subgroup of W generated by A_1, A_2, A_3. Then it is easy to see that $\Gamma \supset D^+,\ S$. Hence $\Gamma = W$ and we have $t(W)=0$ by Lemma 1. 2.

The case $l>4$ is proved similarly as in Lemma 4. 1 using the induction on l, Q.E.D.

LEMMA 4. 4. *Let* $\mathfrak{g}=(F_4)$. *Then* $t(W)=0$.

PROOF. From the Dynkin diagram of $\mathfrak{g}$, we see that W contains subgroups A, B such that

(i) A, B are isomorphic to the Weyl group of type (B_3),

(ii) $A \cap B \neq \{1\}$,

(iii) A and B generate W.

Then $t(A)=t(B)=0$ (Lemma 4. 2) and we have $t(W)=0$ by Lemma 1. 2, Q.E.D.

LEMMA 4. 5. *Let* $\mathfrak{g}=(E_l)$, $l=6,\ 7,\ 8$. *Then* $t(W)=0$.

PROOF. Assume that $l=6$. Then from the Dynkin diagram of (E_6), we see that W contains subgroups A, B such that

(i) $A\cong\mathfrak{S}_6$, $B\cong$ the Weyl group of type (D_4),

(ii) $A\cap B\neq\{1\}$,

(iii) A and B generate W.

Then $t(A)=t(B)=0$ by Lemmas 4. 1 and 4. 3. Hence $t(W)=0$ by Lemma 1. 2.

The cases (E_7), (E_8) are also proved similarly, Q.E.D.

LEMMA 4. 6. *Let* $\mathfrak{g}=(A_2)$ *or* (A_3) *or* (A_4) *or* (B_2) *or* (G_2). *Then* $t(W)>0$.

PROOE. Let $\mathfrak{g}=(A_2)$ or (B_2) or (G_2). Then W is isomorphic with a dihedral group of order 6, 8, 12 respectively. Hence $t(W)>0$ by Theorem III.

Let $\mathfrak{g}=(A_3)$. Then $W\cong\mathfrak{S}_4$ Hence $t(W)>0$ by Theorem III.

Finally let $\mathfrak{g}=(A_4)$. Then $W\cong\mathfrak{S}_5$. Thus we have to show that $t(\mathfrak{S}_5)>0$. Let us consider the following cyclic subgroups G_1, G_2, G_3 of $G=\mathfrak{S}_5$.

$$G_1=\langle(1234)\rangle,\qquad G_2=\langle(12345)\rangle,\qquad G_4=\langle(123)(45)\rangle.$$

Then we can verify that (cf. [5, §2])

$$2\cdot 1^*_{G_1}+1^*_{G_2}+2\cdot 1^*_{G_3}=4\cdot 1^*_{G}+1^*_{\{1\}}.$$

Hence $t(\mathfrak{S}_5)>0$ by Theorem II, Q.E.D.

Thus we completed the proof of Theorem VI.

University of Tokyo

References

[1] C. Chevalley, Sur certains groupes simples, Tôhoku Math. J., **7** (1955), 14-66.

[2] C. W. Curtis and I. Reiner, Representation theory of finite groups and associative algebras, New York (1962), Wiley.

[3] I. Schur, Untersuchungen über die Darstellung der endlichen Gruppen durch gebrochene lineare Substitutionen, Crelles Journal, **132** (1907), 85-137.

[4] Séminaire C. Chevalley, Classification des groupes de Lie algébriques, Paris, (1956-58).

[5] Nobuko Iwahori, On some Diophantine inequalities associated with finite groups, Research Reports of Yamawaki Gakuen Junior College, **2** (1964), 72-129.

(Received July 3, 1964)