PACIFIC JOURNAL OF MATHEMATICS
Vol. 45, No. 2, 1973

ON THE NUMBER OF TYPE-k TRANSLATION-INVARIANT GROUPS

J. HILLEL

The concept of a translation-invariant permutation group was introduced in connection with the problem of constructing "algebras of symmetry-classes of tensors". Such a group is of type-k if it has k orbits. In this paper the number of type-k groups is shown to be the same as the number of divisors of $X^k - 1$ over the two-element field.

Let S_∞ be the group of all permutations of finite degree on the set $\{1, 2, 3, \cdots\}$. If σ is the permutation given by $(a_1b_1)(a_2b_2)\cdots(a_tb_t)$, its *translate* $\sigma^{[1]}$ is defined to be the permutation

$$(a_1 + 1 \;\; b_1 + 1)(a_2 + 1 \;\; b_2 + 1)\cdots(a_t + 1 \;\; b_t + 1)\,.$$

The definition of the translate of σ is independent of the decomposition of σ into a product of transpositions. A subgroup H of S_∞ is said to be *translation-invariant* (briefly, H is a $t - i$ group) if whenever σ is in H so is $\sigma^{[1]}$.

The translation-invariant groups were first introduced in [1] in connection with the problem of generalizing the construction of the Tensor, Grassmann and Symmetric algebras by using symmetry-classes of tensors (see [2]). The following was proven in [1]: if H is a non-trivial $t - i$ group (assume H moves 1), then the orbits for the action of H on $\{1, 2, 3, \cdots\}$ are $Z_{i,k} = \{i, i + k, i + 2k, \cdots\}$, $1 \leqq i \leqq k$, for some $k \geqq 1$. The number of orbits is called the *type* of H. Let $S_{i,\infty}$ (resp. $A_{i,\infty}$) be the group of all (resp. even) permutations on the set $Z_{i,k}$, $1 \leqq i \leqq k$, and let $S_\infty(k) = S_{1,\infty}X\cdots XS_{k,\infty}$, $A_\infty(k) = A_{1,\infty}X\cdots A_{k,\infty}$. For each $k \geqq 1$, these are $t - i$ groups and if H is any type-k $t - i$ group, clearly $H < S_\infty(k)$. Moreover, it was proven that a $t - i$ group contains all the even permutations on each of its orbits, i.e.,

THEOREM 1. *If H is a type-k $t - i$ group then $A_\infty(k) < H < S_\infty(k)$.*

In this presentation we are concerned with determining the number of type-k $t - i$ groups for each $k \geqq 1$. In [1] it was proven that:

THEOREM 2. *There are $2^n + 1$ $t - i$ groups of type-2^n, $n \geqq 0$.*

The above theorem was proved by looking at some special features of the lattice of the type-k $t - i$ groups. However, here we will show that the number of type-k $t - i$ groups is the same as the number of factors of the polynomial $X^k - 1$ over the two-element field F_2 and

thus is completely known.

2. Let $k \geqq 1$ be fixed and let $P(k)$ denote the power set on the set $\{1, 2, \cdots, k\}$. Let Δ denote the symmetric-difference of sets, then $\{P(k), \Delta\}$ is an abelian group whose zero element is the empty set ϕ, and every α in $P(k)$ satisfies $\alpha \Delta \alpha = \phi$, i.e., $\{P(k), \Delta\}$ is a k-dimensional vector-space over F_2 and the singleton sets $\{i\}$, $1 \leqq i \leqq k$ form a basis.

Any permutation σ in $S_\infty(k)$ can be written as a product $\sigma_1\sigma_2 \cdots \sigma_k$ where σ_i is a permutation on the orbit $Z_{i,k}$, $1 \leqq i \leqq k$. Define $F(\sigma)$ to be $\{i_1, \cdots, i_t\}$ where $\sigma_{i_1}, \cdots, \sigma_{i_t}$ are those permutations among $\sigma_1, \cdots, \sigma_k$ which have odd parity. The map $F: S_\infty(k) \to P(k)$ satisfies $F(\sigma\tau) = F(\sigma)\Delta F(\tau)$ for every σ and τ in $S_\infty(K)$, i.e., F is a group homomorphism with $\mathrm{Ker}\,(F) = A_\infty(k)$. By Theorem 1, the usual correspondence between subgroups of $S_\infty(k)$ which contain $A_\infty(k)$ and the subgroups of $P(k)$ sets a one-to-one correspondence between the type-k $t - i$ groups and a certain subfamily of subgroups of $P(k)$ (the $t - i$ mod (k) subgroups in [1]).

Consider the basis $C_k = \{\{1\}, \cdots, \{k\}\}$ of the vector-space $P(k)$ and define a multiplication on C_k by $\{i\} \cdot \{j\} = \{(i + j - 1) \bmod (k)\}$ for $1 \leqq i \leqq k$, $1 \leqq j \leqq k$. C_k thus becomes a cyclic group and the multiplication is uniquely extendable to all of $P(k)$, i.e.,

$$\{i_1, \cdots, i_m\} \cdot \{j_1, \cdots, j_n\} = \mathop{\Delta}_{\substack{1 \leqq r \leqq m \\ 1 \leqq s \leqq n}} \{i_r\} \cdot \{j_s\} .$$

This multiplication endows $P(k)$ with a commutative ring structure. In fact, $P(k)$ is the group-ring $F_2(C_k)$. We note that as $\{2\}$ is a generator of the group C_k, it is also a generator (in the algebraic sense) of $P(k)$.

PROPOSITION. *The type-k $t - i$ groups are in one-to-one correspondence with the ideals of the ring $P(k)$.*

Proof. Let I be a nontrivial subgroup of $P(k)$ which corresponds to a $t - i$ group H under the homomorphism F defined above. Suppose $\alpha = \{i_1, \cdots, i_t\}$ is in I, then $F(\sigma) = \alpha$ for some σ in H, i.e., $\sigma = \sigma_1 \cdots \sigma_k$ where σ_i acts on the orbit $Z_{i,k}$ and $\sigma_{i_1}, \cdots, \sigma_{i_t}$ are the permutations of odd parity. Since H is a $t - i$ group, $\tau = \sigma^{[1]}$ is in H and $F(\tau)$ is in I. Writing τ as a product $\tau_1 \cdots \tau_k$ where τ_i acts on $Z_{i,k}$, it is easily seen that $\tau_{i+1} = \sigma_i$, $1 \leqq i < k$ and $\tau_1 = \sigma_k^{[1]}$. Hence $F(\tau) = \{(i_1 + 1) \bmod (k), \cdots, (i_t + 1) \bmod (k)\} = \{i_1, \cdots, i_t\} \cdot \{2\}$, i.e., $\alpha \cdot \{2\}$ is in I whenever α is in I. As $\{2\}$ generates the whole ring, it follows that I is an ideal.

Conversely, if I is an ideal of $P(k)$ it is immediate that $F^{-1}(I)$ is a $t - i$ group.

The group-ring $P(k)$ is isomorphic to $F_2[X]/(X^k - 1)$ hence the ideals in $P(k)$ correspond to the divisors of $X^k - 1$ in $F_2[X]$. Let $k = 2^n r$ where $(2, r) = 1$, then $X^k - 1 = (X^r - 1)^{2^n}$. Now $X^r - 1 = \prod_{d|r} \phi_d(X)$ where $\phi_d(X)$ are the cyclotomic polynomials. Furthermore (see [3], Theorem 7-2-4), $\phi_d(X)$ is a product of the irreducible polynomials $P_1(X) \cdots P_{m_d}(X)$, $m_d = \varphi(d)/f_d$, where φ is the Euler function and f_d is the smallest integer f such that $2^f \equiv \bmod (d)$. Thus, if s_r is the number of irreducible divisors of $X^r - 1$, then $s_r = \sum_{d|r} \varphi(d)/f_d$. Letting $s_1 = 1$, we conclude:

THEOREM 3. *Let $k = 2^n r$ where $(2, r) = 1$, then there are $(2^n + 1)^{s_r}$ translation-invariant groups of type-k.*

REFERENCES

1. J. Hillel, *Algebras of symmetry classes of tensors*, J. Algebra, **23** (1972), 215-227.
2. M. Marcus and H. Minc, *Permutations on symmetry classes*, J. Algebra, **5** (1967), 59-71.
3. E. Weiss, *Algebraic Number Theory*, McGraw-Hill, 1963.

Received November 14, 1971.

SIR GEORGE WILLIAMS UNIVERSITY