Werk

Titel: A Generalization of the Regular Representation of Finite Abelian Group.

Autor: Wells, Charles

Jahr: 1968

PURL: https://resolver.sub.uni-goettingen.de/purl?362162050_0072|log19

Kontakt/Contact

Digizeitschriften e.V.
SUB Göttingen
Platz der Göttinger Sieben 1
37073 Göttingen

info@digizeitschriften.de

Monatshefte für Mathematik 72, 152—156 (1968)

A Generalization of the Regular Representation of Finite Abelian Groups*

Dedicated to

Professor *Leonard Carlitz*

on his sixtieth birthday

By

Charles Wells, Cleveland, Ohio, U. S. A.

(Received November 28, 1966; in revised form May 8, 1967)

1. Introduction

Let A be a finite Abelian group of order $de = m$, written multiplicatively with identity 1_A. Suppose A contains α distinct dth powers $1_A = u_1, \ldots, u_\alpha$, let $a_1, \ldots, a_\alpha$ be arbitrary elements of A, and let $N_\alpha = \{1, 2, \ldots, \alpha\}$. (Note: α is determined explicitly in Section 2.) Then the mapping

$$\phi : x \to a_r x \qquad (x^d = u_r, r = 1, \ldots, \alpha;\ x \in A) \tag{1.1}$$

takes A into A. The collection $H(d)$ of all such mappings ϕ forms a semigroup on composition, for if

$$\psi : x \to b_r x \qquad (x^d = u_r,\ r = 1, \ldots, \alpha;\ x \in A), \tag{1.2}$$

then

$$\phi \circ \psi : x \to b_{\sigma(r)} a_r x \qquad (x^d = u_r,\ r = 1, \ldots, \alpha;\ x \in A) \tag{1.3}$$

where $\sigma : N_\alpha \to N_\alpha$ is determined by

$$(a_r x)^d = u_{\sigma(r)} \qquad (x^d = u_r,\ r = 1, \ldots, \alpha). \tag{1.4}$$

In this paper the set $M(d)$ of all invertible elements of $H(d)$ is investigated. The following theorem is the main result. Let $\alpha\beta = m$ and let $A(d)$ be the subgroup of A of elements a such that $a^d = 1$. $A(d)$ has order β. Let S_α denote the symmetric group on N_α.

* The author wishes to acknowledge the support of National Science Foundation grant GP-5624.

Theorem. $M(d)$ is a group of order $\alpha!\,\beta^{\alpha}$. It is isomorphic to the wreath product of the regular representation of $A(d)$ by S_{α}.

(For elementary facts about the wreath product, see Hall [3; p. 81].)

The groups obtained here are generalizations of groups obtained by Fillmore [2] and the author [7], in which the group A was the multiplicative group of a finite field. $M(d)$ is denoted G_d in [2] and K_d' in [7]. The group $K(d)$ here (Section 5) is called K_d in [7]. $M(d)$ is a splitting extension of $K(d)$ by the symmetric group on α elements.

In both [2] and [7] representations of the elements of the groups as polynomials over the particular field involved were found. Certain additional properties of these polynomials are deduced in Section 6. The polynomials representing elements of $K(d)$ were in fact known first (Dickson [1; p. 61]). We note here that Lausch, Nöbauer and Schweiger ([4] and [5]) investigated groups of permutations of a group represented as "polynomials" over the group.

In this paper composition of mappings reads from left to right.

2. Determination of α and β

For some positive integers $k, m_1, \ldots, m_k$, A is the direct product of k cyclic groups C_{m_i} of order m_i $(i=1, \ldots, k)$. The orders m_i are here not necessarily powers of primes. Let g_i generate C_{m_i} $(i=1, \ldots, k)$, so that every element $a \in A$ may be expressed uniquely as

$$a = \prod_{i=1}^{k} g_i^{t_i} \qquad (1 \leq t_i \leq m_i,\ i = 1, \ldots, k).$$

Then $a^d = \Pi g_i^{t_i d}$. If $b = \Pi g_i^{s_i}$, then $b^d = a^d$ only if for each i, $s_i d \equiv t_i d$ (mod m_i). For fixed t_i this congruence has (d, m_i) incongruent solutions. Therefore, exactly $\beta = \prod_{i=1}^{k} (d, m_i)$ elements have dth power u_r for each $r = 1, \ldots, \alpha$. Evidently, $\alpha = m\beta^{-1}$. (It follows that if $A = C_m$, then $\alpha = e$, $\beta = d$. The converse is not true; for example, if $m_1 = 3$, $m_2 = 6$, $d = 9$.)

3. Some lemmas

We first prove the following:

Lemma 1. If φ is given by (1.1) *and σ by* (1.4), *then φ permutes A if and only if σ permutes N_{α}.*

Proof. Let $x^d = u_r$, $y^d = u_s$, and $a_r x = a_s y$. Then by (1.4) $u_{\sigma(r)} = u_{\sigma(s)}$ so that $\sigma(r) = \sigma(s)$. If σ is a permutation, then $r = s$, so by cancellation $x = y$ and φ is a permutation.

Conversely, suppose $\sigma(r) = \sigma(s)$, $r \neq s$. We first note that for any t, $1 \leq t \leq \alpha$,

$$a_t^{-d}\, u_{\sigma(t)} = u_t. \tag{3.1}$$

Suppose $x^d = u_r$ and set $y = a_s^{-1} a_r x$. Using (3.1) and the fact that $u_r \neq u_s$, it is easy to verify that $a_r \neq a_s$, so that $x \neq y$. However, $y^d = u_s$ by (3.1), so $\varphi(x) = a_s\, y = \varphi(y)$. Hence, φ is not a permutation. This completes the proof.

Lemma 2. $M(d)$ consists exactly of the permutations in $H(d)$.

Proof. Since every element φ of $M(d)$ has an inverse in $H(d)$, φ is necessarily a permutation. Now suppose φ is a permutation in $H(d)$ and is given by (1.1), and σ by (1.4). Then by Lemma 1, $\tau = \sigma^{-1}$ is defined. Define $\psi : x \to b_r x$ $(x^d = u_r)$ where $b_r = a_{\tau(r)}^{-1}$. Then

$$\varphi \circ \psi : x \to a_{\tau(\sigma(r))}^{-1}\, a_r x = x$$

and clearly $\psi \in H(d)$. Hence, every permutation in $H(d)$ has an inverse in $H(d)$, and so is in $M(d)$. This proves the Lemma.

4. Proof of the Theorem

A coset of $A(d)$ is the set of all elements $x \in A$ for which $x^d = u_r$ for some $r \in N_\alpha$. Let $1 = w_1, \ldots, w_\alpha$ be coset representatives of $A(d)$ in A, numbered so that $x \in w_r A(d)$ if and only if $x^d = u_r$. Each $x \in A$ may be written uniquely as $x = z w_r$ for some $z \in A(d)$ and some $r \in N_\alpha$. Let A' be the *set* $A(d) \times N_\alpha$. Let $\beta : A \to A'$ be the bijection $\beta : z w_r \to (z, r)$. This bijection induces a monomorphism θ^* of $H(d)$ into the semigroup of mappings $A' \to A'$ given by

$$\theta^*(\varphi) : \beta(x) \to \beta(\varphi(x)). \tag{4.1}$$

(That θ^* is a monomorphism is a general property of semigroups of mappings.)

Now if φ is given by (1.1), it takes $z w_r$ onto $a_r z w_r$, and since $(a_r z w_r)^d = u_{\sigma(r)}$ (σ given by (1.4)), there is a $z' \in A(d)$ for which $a_r z w_r = z' w_{\sigma(r)}$. Then $a_r\, w_r\, w_{\sigma(r)}{}^{-1} \in A(d)$ and

$$\theta^*(\varphi) : (z, r) \to (a_r\, w_r\, w_{\sigma(r)}{}^{-1}\, z, \sigma(r)). \tag{4.2}$$

From (4.2) and the Lemmas it follows that θ^* induces a homomorphism $\theta : M(d) \to A(d)\ wr\, S_\alpha$. Ker θ consists of those maps φ for which $a_r\, w_r\, w_{\sigma(r)}{}^{-1} = 1$ and $\sigma(r) = r (r \in N_\alpha)$, hence just of the identity. But θ is also surjective. Let $z_1, \ldots, z_\alpha \in A(d)$ and $\sigma \in S_\alpha$; then for

$$a_r = z_r\, w_r^{-1}\, w_{\sigma(r)}\ (r = 1, \ldots, \alpha),$$

let $\phi : x \to a_r x$ $(x^d = u_r, r = 1, \ldots, \alpha)$. It is easy to show that $\theta(\phi) : (z, r) \to (z_r z, \sigma(r))$. This proves that θ is an isomorphism, hence the Theorem.

5. Some corollaries

It is a property of wreath products that $M(d)$ contains a normal subgroup $K(d)$ isomorphic to the direct product of α copies of $A(d)$; furthermore, $M(d)$ is a splitting extension of $K(d)$ by S_α. The natural homomorphism $M(d) \to S_\alpha$ is $\phi \to \sigma$, where ϕ is given by (1.1) and σ by (1.4). Hence, $K(d)$ consists of permutations

$$\phi : x \to a_r x \qquad (x^d = u_r,\ r \in N_\alpha,\ a_r \in A(d)). \tag{5.1}$$

The fact that $K(d)$ is Abelian and isomorphic to the direct product of α copies of $A(d)$ may also be verified by using an elaboration of the methods of [7].

The set of permutations

$$\psi_\sigma : x \to w_r^{-1}\, w_{\sigma(r)}\, x \qquad (x^d = u_r,\ r \in N_\alpha)$$

forms a subgroup $S(d)$ of $M(d)$ isomorphic to S_α. For if $x = zw_r$, then $\psi_\sigma(x) = zw_{\sigma(r)}$, so that $\psi_\tau\, \psi_\sigma(x) = zw_{\tau(\sigma(r))}$ for $\tau, \sigma \in S_\alpha$. In fact, $S(d)$ consists of representatives of the cosets of $K(d)$, for if $\psi_\sigma\, \psi_\tau^{-1} \in K(d)$, then $\sigma = \tau$. This shows explicitly that $M(d)$ is a splitting extension (that is, a semidirect product) of $K(d)$ by S_α. (Cf. [2], Theorem 2 and [7], Theorem 11.)

A monomial representation for $M(d)$ may be given as follows: (See Hall [3], p. 200, and also Ore [6]) If ϕ is given by (1.1), then, in the notation of Section 4, $a_r = z_r\, w_r^{-1}\, w_{\sigma(r)}$ for some $z_r \in A(d)$ $(r = 1, \ldots, \alpha;\ \sigma$ given by (1.4)). Let ϕ correspond to the $\alpha \times \alpha$ matrix (a_{rs}), where

$$a_{rs} = \begin{cases} z_r & (s = \sigma(r)) \\ 0 & \text{otherwise.} \end{cases}$$

It is then easy to verify that the group of such matrices is isomorphic to $M(d)$.

6. Applications to permutation polynomials over fields

Let k denote the finite field of order $q = p^n$ elements, and let $de = q - 1$. Let $A(d)$ be the set of dth roots of unity in k; $A(d)$ is cyclic of order d. Let S_d be the symmetric group on d letters.

Corollary 1. The set of permutation polynomials of the form $xf(x^d)$ $(f(x) \in k[x])$ *forms, on composition* (*mod* $x^q - x$), *a group of order* $e!\, d^e$ *isomorphic to the wreath product of* $A(d)$ *by* S_e. *It contains a normal Abelian subgroup of type* $(d, d, \ldots, d)$ (e *times*) *consisting of all polynomials of the form* $x(f(x^d))^e$ *for which* $f(x)$ *has no nonzero roots in* k.

Proof. Follows from the main Theorem and Theorem 5 of [7].

Corollary 2. For any d *dividing* $q - 1$, *there is a set of polynomials of the form* $xf(x^d)$ *in* $k[x]$ *which form a group on composition* (*mod* $x^q - x$) *isomorphic to the symmetric group on* e *letters, where* $de = q - 1$.

Proof. Follows from the fact that $M(d)$ splits over $K(d)$.

From this we have

Corollary 3. Let G *be a finite group of order* n, *and let* p *be a prime not dividing* n. *Then* G *is represented by a group of permutation polynomials of the form* $xf(x^m)$ *over* $GF(p^{\phi(n)})$, *where* $mn = p^{\phi(n)} - 1$.

Proof. G is isomorphic to a subgroup of S_n. But $n/p^{\varphi(n)} - 1$, so the Corollary follows from Corollary 2.

Acknowledgement. The author wishes to thank the referee for his suggestion that $M(d)$ be presented as a wreath product instead of a semidirect product (which made the paper considerably more compact) and for pointing out the connection with monomial groups.

References

[1] *L. E. Dickson:* Linear Groups with an Exposition of Galois Field Theory. New York: Dover, 1958.

[2] *J. P. Fillmore:* A note on split dilations defined by higher residues. Proc. A. M. S., **18** (1967), 171–174.

[3] *M. Hall, Jr.*, The Theory of Groups. New York: Macmillan, 1959.

[4] *H. Lausch, W. Nöbauer* and *F. Schweiger.* Polynompermutationen auf Gruppen. Mh. Math., **69** (1965), 410–423.

[5] *H. Lausch, W. Nöbauer* and *F. Schweiger.* Polynompermutationen auf Gruppen II. Mh. Math., **70** (1966), 118–126.

[6] *O. Ore:* Theory of monomial groups. Trans. A. M. S., **51** (1942), 15–64.

[7] *C. Wells:* Groups of permutation polynomials. Mh. Math., **71** (1967), 248–262.