doi：103969/j. issn. 0490-6756. 2016. 03. 007

有限交换环上的多项式置换群

潘嘉堃，张起帆
(四川大学数学学院，成都 610064)

摘　要：1999 年，Frisch 描述了 $\mathbf{Z}/p^2\mathbf{Z}$ 上多项式置换群的结构. 2005 年，张找到 $\mathbf{Z}/p^2\mathbf{Z}$ 上多项式函数与 $\mathbf{Z}/p\mathbf{Z}$ 上多项式函数的 3 维向量之间的对应关系. 本文首先证明在任意有限交换环 R 上，多项式置换群同构于 $R[x]$（作为 R 上多项式函数全体构成的 R-代数）的自同构群，然后用张所提出的对应对 Frisch 的描述给出一个新证明.

关键词：Witt 多项式；置换多项式；圈积；半直积.
中图分类号：O156.2　　**文献标识码**：A　　**文章编号**：0490-6756(2016)02-0275-05

Groups of polynomial permutations over finite commutative rings

PAN Jia-Kun, *ZHANG Qi-Fan*
(College of Mathematics, Sichuan University, Chengdu 610064, China)

Abstract: Frisch characterized the structure of the group of polynomial permutations over $\mathbf{Z}/p^2\mathbf{Z}$ in 1999. Zhang found a correspondence between polynomial functions over $\mathbf{Z}/p^2\mathbf{Z}$ and 3-tuples of polynomial functions over $\mathbf{Z}/p\mathbf{Z}$ in 2005. In this paper, we first prove that over any finite commutative ring R, the group of polynomial permutations is isomorphic to the automorphism group of the R-algebra of the polynomial functions. Then we give an easy proof to the characterization of Frisch using the correspondence set proposed by Zhang.

Key words: Witt polynomials; Polynomial Permutations; Wreath product; Semi-direct product.
(2010 MSC 11T06)

1 Introduction

Throughout this paper we fix the following notations:

R: An arbitrary finite commutative ring with multiplicative identity,

$R[X]$: The ring of polynomials with coefficients in R,

id_R : The identity map of R.

For prime number p and positive integer n,

L_n: The ring of the polynomial functions over $\mathbf{Z}/p^n\mathbf{Z}$,

G_n: The subset of L_n consisting of all its permutations.

Given an R-algebra A,

$\mathrm{End}_R(A)$: The endomorphism ring of A,

$\mathrm{Aut}_R(A)$: The automorphism group of A.

For a finite commutative ring R, every polynomial $F \in R[X]$ induces a function $\bar{F}$ from R to R as following:

$$\bar{F}: x \mapsto F(x).$$

We can say the function $F(x)$ or $\bar{F}(x)$ for short.

收稿日期：2015-4-30
基金项目：国家自然科学基金(11171150)
作者简介：潘嘉堃，男，硕士，主要研究方向为数论. E-mail：jpan_math_scu@163.com

Clearly, the function $\overline{X}$ induced by X means id_R, the identity function. We can also use x to represent the identity function. A polynomial is said to be a permutation polynomial over R if it induces a permutation over R, meanwhile, the permutation is said to be a polynomial permutation. All polynomial functions over R, in a well-known way, form a commutative R-algebra. Moreover, for every $F \in R[X]$, the induced function $\overline{F} = F(id_R)$. So the ring formed by all polynomial functions over R is $R[id_R] = R[x]$. We will study the endomorphisms and automorphisms of $R[x]$ and obtain:

Theorem 1.1 The automorphism group $\mathrm{Aut}_R(R[x])$ of $R[x]$ (as an R-algebra) is isomorphic to the polynomial permutation group of R.

Recently, Zhang uses the special case $R = F_q$ of this theorem to obtain some interesting results on permutation polynomials over finite fields.

Polynomial functions (especially permutations) over finite fields is a topic full of wonder and applications[1-10]. However equivalently ideal properties don't belong to the rings $\mathbf{Z}/p^n\mathbf{Z}$ for $n > 1$. Then in order to know as much as possible, one may try to reduce the problem to the case $\mathbf{Z}/p\mathbf{Z}$, in light of which a fundamental conclusion was achieved:

Theorem 1.2[6] Let $F \in \mathbf{Z}[X], n > 1$. $F(x)$ is a permutation over $\mathbf{Z}/p^n\mathbf{Z}$ if and only if $F(x)$ permutes $\mathbf{Z}/p\mathbf{Z}$ and $F'(x)$ is zero-free, $F'(X)$ being the formal derivative of $F(X)$.

All that is needed for its proof is a simple application of Hensel's Lemma. Going back to the notations, we find that G_n in fact makes a group, because it's a submonoid of $\mathbf{Z}/p^n\mathbf{Z}$'s permutation group, which is finite, and basic group theory tells us that it must be a subgroup. For instance, when $n = 1$, $\mathbf{Z}/p^n\mathbf{Z}$ is the finite field F_p, over which all functions are in L_1, hence $G_1 \cong S_p$. What does G_n look like when $n = 2$ Frisch[1] gave an answer (as shown in the remark after Theorem 3.3 of this paper) in 1999, after which an useful connection between L_2 and L_1 was discovered.

Since every element of $\mathbf{Z}/p^n\mathbf{Z}$ can be represented as an n-dimensional Witt vector, i.e., the Witt polynomial W_n naturally gives a one-to-one correspondence between $\mathbf{Z}/p^n\mathbf{Z}$ and $(\mathbf{Z}/p\mathbf{Z})^n$, Zhang[2] accordingly built a mapping φ from L_1^3 to L_2. To be more specific, for any $(v,w,u) \in L_1^3$, $\varphi(v,w,u) = F(x) \in L_2$ with

$$F(X) = pV(X) + W(X) \cdot (X - X^p) + U(X)^p,$$

where V, W, U are any elements in $\mathbf{Z}[X]$ inducing v, w, u respectively.

On the other hand, for any $f \in L_2$ induced by any polynomial F, there are $v, w, u \in L_1$ such that $f = \varphi(v,w,u)$, where u happens to be the image of f under the natural ring homomorphism from L_2 to L_1, namely $F(x)$ over $\mathbf{Z}/p\mathbf{Z}$, and w the image of $F'(x)$ under the same ring homomorphism. v, w, u being called the V, W and U part of f, Nöbauer's theorem can be rewritten as:

$f \in G_2 \Leftrightarrow$ the U part of $f \in G_1$, and the W part of f vanishes nowhere.

Following the idea of Ref. [2], we will give a new proof to Frisch's aforementioned theorem in Ref. [1].

2 Some basic facts

Let's recall concepts of semi-direct products and wreath products of groups. For any group G, by $\mathrm{Aut}(G)$ we mean the automorphism group of G.

Let H and K be groups with a group homomorphism $\theta: K \to \mathrm{Aut}(H)$. We can define an action of group K on H by ${}^k h = \theta(k)(h)$, where $h \in H, k \in K$. Then the set $H \times K$ together with the following operation make a group:

$$\forall\ h_i \in H, k_i \in K, i = 1,2,$$
$$(h_1, k_1) \circ (h_2, k_2) = (h_1 \cdot {}^{k_1} h_2, k_1 \cdot k_2).$$

This group is called the semi-direct product of H and K with respect to θ, and denoted as $\complement_\theta(H, K)$, or $\complement(H, K)$ when θ is clear.

For any group H and set J, the set of all functions from J to H together with the operation:

$$\forall f_1, f_2: J \to H, f_1 \circ f_2(j) = f_1(j) \circ f_2(j), \forall j \in J$$

form a group denoted by H^J.

If there is another group K acting on J, then in the natural way K has a group action on H^J which can be seen clearly from the following commutative diagraph:

$$\begin{tikzcd} J \arrow[r, "k"] \arrow[dr, "{}^k f"'] & J \arrow[d, "f"] \\ & H \end{tikzcd}$$

where $f \in H^J$ and $k \in K$. Then we can construct a new group $\mathcal{C}(H^J, K) := \mathcal{C}(H_J, K)$ named the wreath product of H and K (with respect to J and the group action of K on J).

Now look back to L_2. In the following contents of this paper, for any $a \in \mathbf{Z}/p^2\mathbf{Z}$, its image of the natural ring homomorphism in $\mathbf{Z}/p\mathbf{Z}$ will be written as $[a]_p$. A classical conclusion goes, as can be seen in Ref. [4]:

Lemma 2.1 For any function f over $\mathbf{Z}/p^2\mathbf{Z}$,
$f \in L_2 \Leftrightarrow \forall\ t \in \mathbf{Z}/p\mathbf{Z}, \exists$
$w: \mathbf{Z}/p\mathbf{Z} \to \mathbf{Z}/p^2\mathbf{Z}$, s. t.
$\forall\ x \in \mathbf{Z}/p^2\mathbf{Z}, f(x + tp) =$
$f(x) + tpw([x]_p)$.

In $\mathbf{Z}/p^2\mathbf{Z}$ there are p elements $1^p, 2^p, \ldots, p^p$ satisfying $X^p = X$, known as the Teichimüer elements of $\mathbf{Z}/p^2\mathbf{Z}$. The function $t: \mathbf{Z}/p\mathbf{Z} \to \mathbf{Z}/p^2\mathbf{Z}$, $t(x) = x^p$ is called the Teichimüer lifting which "lifts" any element a in $\mathbf{Z}/p\mathbf{Z}$ to a Teichimüer element $\tilde{a}$ in $\mathbf{Z}/p^2\mathbf{Z}$ with $[\tilde{a}]_p = a$, and we set T_2 to be the set of all Teichimüer elements of $\mathbf{Z}/p^2\mathbf{Z}$. For any $f \in L_2$, we call $w \circ [\cdot]_p$ the derivative of f, where w is the function in the above lemma. It's easy to see that this derivative coincides with the familiar concepts whether we regard them as functions or polynomials, in other words, $w \circ [\cdot]_p = F'(x)$ over $\mathbf{Z}/p\mathbf{Z}$. With the lemma, in order to decide a polynomial function over $\mathbf{Z}/p^2\mathbf{Z}$, we just need to know the values of $w \circ [\cdot]_p$, and the values of $f(x)$ at T_2.

For a field k of characteristic p, there exist a series of Witt rings $W_n(k)$, $n = 1, 2, \cdots$. They are defined by Witt polynomials in a suitable way (see Ref. [10]). In particular, $W_2(F_p) = \mathbf{Z}/p^2\mathbf{Z}$ because the Witt polynomial $W_2 = X_1^p + pX_2$ induces a natural bijection from $(\mathbf{Z}/p\mathbf{Z})^2$ to $\mathbf{Z}/p^2\mathbf{Z}$. With Witt polynomials Zhang([2]) found that:

Lemma 2.2 $\forall f \in L_2, \exists u, v: \mathbf{Z}/p\mathbf{Z} \to \mathbf{Z}/p\mathbf{Z}$, s. t. the following map commutes:

$$\begin{tikzcd} \mathbb{Z}/p^2\mathbb{Z} \arrow[r, "f"] & \mathbb{Z}/p^2\mathbb{Z} \\ \mathbb{Z}/p\mathbb{Z} \arrow[u, "t"] \arrow[r, "{[u,v]}"] & (\mathbb{Z}/p\mathbb{Z})^2 \arrow[u, "w_2"'] \end{tikzcd}$$

With these two lemmas, Zhang showed:

Theorem 2.3[2] There exists a bijection φ between L_1^3 and L_2.

To be more concrete, let

$$\varphi(v, w, u) = pV(x) + W(x) \cdot (X - X^p) + U(x)^p,$$

where U, V, W are polynomials with integer coefficients inducing u, v, w over $\mathbf{Z}/p\mathbf{Z}$ respectively, and Ref. [2] says that φ is invertible. As pointed out in the introduction, $f = \varphi(v, w, u) \in L_2$ is a permutation if and only if $u \in S_p$ and $w \in L_1{}'$, where $L_1{}'$ stands for all polynomial functions over $\mathbf{Z}/p\mathbf{Z}$ that don't equal to zero anywhere. So if we restrict φ within $L_1 \times L_1{}' \times S_p$ and denote the restriction with the same symbol φ, Nöbauer's theorem tells us that φ makes a bijection from $L_1 \times L_1{}' \times S_p$ to G_2.

3 Proof of the main results

Proof to Theorem 1.1 We first characterize the endomorphisms of $R[x]$. An endomorphism of $R[x]$ means a map ψ (from $R[x]$ to $R[x]$) satisfying:

$$\psi(f \circ g) = f \circ \psi(g) \tag{1}$$

where $f, g \in R[x]$.

Of course, ψ is decided by $\psi(id_R)$, and concretely,

$$\psi(f) = f \circ \psi(id_R) \tag{2}$$

Now we claim for any $\alpha \in R[x]$, there exist unique endomorphism ψ of $R[x]$ such that

$$\psi(id_R) = \alpha \tag{3}$$

Clearly, (2) implies the uniqueness. On the other hand, if we can define $\alpha^*: R[x] \longrightarrow R[x]$ by

$$\alpha^*(f) = f \circ \alpha \qquad (4)$$

It is easy to check that α^* is such an endomorphism ψ satisfying (3). So (4) gives all endomorphisms of $R[x]$. Namely, we give a natural bijection from $R[x]$ to $\mathrm{End}_R[x]$

$$\alpha \mapsto \alpha^* \qquad (5)$$

Furthermore, we have

$$(\alpha \circ \beta)^* = \beta^* \circ \alpha^*.$$

This property easily yields

$$\alpha \circ \beta = id_R \Leftrightarrow \beta^* \circ \alpha^* = id_{R[x]}.$$

So

$$\alpha \text{ is isomorphic} \Leftrightarrow \alpha^* \text{ is isomorphic.}$$

Now we get an anti-isomorphism from the polynomial permutation group to the automorphism group of $R[x]$ by(5). At last, define $\alpha_*: R[x] \to R[x]$ by

$$\alpha_*(f) = f \circ \alpha^{-1},$$

we get the group isomorphism we need.

For convenience in what follows we let $H = \mathcal{C}(\mathbf{Z}/p\mathbf{Z},\ \mathbf{Z}/p\mathbf{Z}^{\times})$ and $J = \mathbf{Z}/p\mathbf{Z}$. Here H is a group while J will just be treated as a set.

The discussion in the last section gives us φ, a bijective $L_1 \times L_1' \times S_p - G_2$ correspondence. We want to know whether we can build a new group whose underlying set is $L_1 \times L_1' \times S_p$ with smaller groups. If yes, and if the group is also isomorphic to G_2, then we at least have represented G_2's structure in a simpler manner.

It's obvious that there is a canonical correspondence between $L_1 \times L_1'$ and H^J, i. e.,

$$(v,w) \leftrightarrow \prod_{a \in \mathbb{Z}/p\mathbb{Z}} (v(a), w(a)).$$

Since S_p can naturally give J a group action, we can define an operation for $L_1 \times L_1' \times S_p$ to make it a group which is isomorphic to $\mathcal{C}(H^J, S_p)$, the canonical correspondence between the sets being the isomorphism between the groups. Let's denote this new group as N. Then we're able to compute, for $(v_i, w_i, u_i) \in N$ and $i = 1,2$:

Lemma 3.1

$$(v_1, w_1, u_1) \circ (v_2, w_2, u_2) =$$
$$(v_1 \circ u_2 + (w_1 \circ u_2) \cdot v_2, (w_1 \circ u_2) \cdot w_2, u_1 \circ u_2).$$

With the correspondence, we just need to compute the product of the counterpart of (v_1, w_1, u_1) and (v_2, w_2, u_2) in $\mathcal{C}(H^J, S_p)$, then trace back the result of operation in $L_1 \times L_1' \times S_p$.

Let's go back to Zhang's $L_1^3 - L_2$ correspondence in Ref. [2].

If f_1 and f_2 are in G_2, and the V, W and U parts of f_i are v_i, w_i and u_i respectively for $i = 1,2$, what's the three parts of $f_1 \circ f_2$. Take any F_i, U_i, V_i and W_i each of which induces f_i, u_i, v_i and w_i respectively. It's easy to see that $F_1 \circ F_2$ induces $f_1 \circ f_2$.

On the other hand, since $F_i(x) = pV_i(x) + W_i(x) \cdot (x - x^p) + U_i(x)^p$, we have

$$F_1(F_2(x)) = pV_1(F_2(x)) + W_i(F_2(x)) \cdot (F_2(x) - F_2^p(x)) + U_1(F_2(x))^p,$$

which means

$$\begin{aligned}F_1(F_2(x)) &= pV_1(U_2(x)^p) + W_1(U_2(x)^p) \cdot (pV_2(x) + W_2(x) \cdot (x - x^p)) + U_1(U_2(x)^p)^p \\ &= p(V_1(U_2(x)) + W_1(U_2(x)) \cdot V_2(x)) + W_1(U_2(x)) \cdot W_2(x) \cdot (x - x^p) + U_1(U_2(x))^p.\end{aligned}$$

Because $V_1(U_2(x)) + W_1(U_2(x)) \cdot V_2(x)$, $W_1(U_2(x)) \cdot W_2(x)$ and $U_1(U_2(x))$ induce $v_1 \circ u_2 + (w_1 \circ u_2) \cdot v_2$, $(w_1 \circ u_2) \cdot w_2$ over $\mathbf{Z}/p^2\mathbf{Z}$ and $u_1 \circ u_2$ respectively, according to Theorem 2.3 there is:

Lemma 3.2 The V, W, and U part of $f_1 \circ f_2$ are $v_1 \circ u_2 + (w_1 \circ u_2) \cdot v_2$, $(w_1 \circ u_2) \cdot w_2$ and $u_1 \circ u_2$.

With such preparation we can give a new proof to the following

Theorem 3.3

$$G_2 \cong \mathcal{C}(H^J, S_p)$$

Proof As we find in the last section, consider Zhang's correspondence

$$\varphi: N \to G_2$$
$$(v,w,u) \mapsto pV(x) + W(x) \cdot (x - x^p) + U(x)^p.$$

As is constructed, $\mathcal{C}(H^J, S_p) \cong N$, so we just need to show that φ is an isomorphism from G_2 to N.

Since Zhang's correspondence is bijective, proving that φ is a group homomorphism suffices.

For any (v_1, w_1, u_1) and (v_2, w_2, u_2) in N with $\varphi(v_i, w_1, u_i) = f_i$, $i = 1,2$, Lemma 3.1 calculates $\varphi^{-1}(f_1) \circ \varphi^{-1}(f_2)$, which equals to $\varphi^{-1}(f_1$

$\circ f_2$)，as shown in Lemma 3.1. Then φ^{-1} is a homomorphism, and so is φ. The proof is end.

Remark In Frisch's origin work[1], she managed to prove the theorem in a general case, where R is isomorphic to the second Witt ring $W_2(F_q)$ of any finite field F_q(here $q=p^m$ for some $m\in\mathbf{Z}_+$). In this case she proved that

$$G_2\cong \bigcap(F_q\times F_q^{\times},S_q),$$

where G_2 represents the group of polynomial permutations over R and J is the underlying set of F_q.

Literally we have only proven the case when $m=1$.

Actually, the same method can be applied to the proof in her case analogously, so it's safe to say that we have proved Frisch's group structure theorem of G_2 in another way.

We limit our discussion to the $R=\mathbf{Z}/p^2\mathbf{Z}$ just for convenience.

References:

[1] Frisch S. Polynomial functions on finite commutative rings [M]. Lecture Notes in Pure and Appl Mathematics 205. New York: Dekker, 1999.

[2] Zhang Q. Witt rings and permutation polynomials [J]. Algebra Colloquium 2005, 1: 161.

[3] Frisch S, Krenn D. Sylow p-groups of polynomial permutations on the integers mod p^n [J]. J Number Theory 2013, 133: 4188.

[4] Zhang Q. Polynomial functions and permutation polynomials over some finite commutative rings [J]. J Number Theory, 2004, 105: 192.

[5] Lidl R, Niederreiter H. Finite fields [M]. Encyclopedia of Math and Appl, Vol 20. New York: Addision-Wesley, 1983.

[6] Nöbauer W. Über Permutationspolynome und Permutationsfunktionen für Primizahlpotenzen [J]. Monatsh, 1965, 69(3): 230.

[7] Qin X and Yan L. Notes on permutation polynomials over finite fields [J]. J Sichuan University: Nat Sci Ed(四川大学学报：自然科学版), 2014, 51 (3): 436.

[8] Jiang J. A note on permutation polynomials over $\mathbf{Z}/p^l\mathbf{Z}$ [J]. J Sichuan University: Nat Sci Ed, 2003, 5: 311.

[9] Mullen G, Wan D, Wang S. Value sets of polynomial maps over finite fields [J]. Quar J Math Oxford, 2013, 61(4): 1191.

[10] Serre J. Local fields [M], GTM 67. New York/Berlin: Springer-Verlag, 1979.