PERMUTATION POLYNOMIALS IN ONE INDETERMINATE OVER MODULAR ALGEBRAS

por

Pablo A. Acosta-Solarte[1] & Víctor S. Albis[2]

Resumen

Acosta-Solarte, Pablo A. & Víctor S. Albis: Permutation polynomials in one indeterminate over modular algebras. Rev. Acad. Colomb. Cienc. **30** (117): 541-548, 2006. ISSN 0370-3908.

Resultados conocidos sobre polinomios de permutación con coeficientes en un cuerpo finito se extienden a álgebras de la forma $L_\nu = K[X]/(p(X)^\nu)$, donde K es un cuerpo finito, $p(X) \in K[X]$ un polinomio irreducible, $\nu = 1, 2, \ldots$, y al álgebra de las series potenciales $L[[Z]]$, donde $L = K[X]/(p(X))$. Se estudian también análogos de polinomios de Dickson en este contexto.

Palabras clave: Polinomio de permutación, polinomio de Dickson.

Abstract

Known results on permutation polynomials with coefficients in a finite field are extended to algebras of the form $L_\nu = K[X]/(p(X)^\nu)$, where K is a finite field, $p(X) \in K[X]$ is an irreducible polynomial, $\nu = 1, 2, \ldots$, and to the algebra of power series $L[[Z]]$. Finally, analogous of Dickson polynomials in these algebras are studied.

Key words: Permutation polynomial, Dickson polynomial.

1 Universidad Distrital Francisco José de Caldas, Bogotá, Colombia. E-mail: paacostas@udistrital.edu.co

2 Universidad Nacional de Colombia, Bogotá, Colombia. Email: valbis@accefyn.org.co AMS Classification 2000: 13B25, 13F25, 11T55.

1. Introduction

In the second half of the last century, the main interest in finite fields $K = \mathbb{F}_q$ focused in the study of permutation polynomials over these fields and the application of its results to coding theory. During the same period of time, most of the obtained results were extended mainly to the classical rings $\mathbb{Z}/p^m\mathbb{Z}$ and the Galois rings $GR(p^m, k)$ (see, for example, [11], [12], [13]), permitting thus the construction of new cryptosystems with a variety of interesting properties. In the same spirit, this paper extends some known results about permutation polynomials over finite fields in one indeterminate to analogous permutation polynomials over the algebras $L_\nu = K[X]/(p(X)^\nu)$, where $p(X) \in K[X]$ is irreducible, and $L[[Z]]$. Since the L_ν algebras are not always Galois rings (the exception being the rings $\mathbb{F}_p[X]/(X^\nu)$, it seems to us that apparently we are stepping into a new nice field of research, with eventual applications to coding theory.

The present paper is structured as follows: In the second section we establish the necessary basic definitions and results needed for a better understanding of what follows. In the third section, we define permutation polynomials over L_ν and $L[[Z]]$, and extend to these algebras analogues of well known general results about permutation polynomials over finite fields. In the fourth section we examine closely the analogues of Dickson polynomials in this new setting.

2. Preliminaries

Let K be a field with q elements and let $p(X) \in K[X]$ be a monic and irreducible polynomial of degree d. We know that the quotient $L = K[X]/(p(X))$ is a finite field containing K, thus a finite extension L/K of degree d. Moreover, $L_\nu = K[X]/(p(X)^\nu)$, $\nu > 1$, is an $L-$algebra with $q^{\nu d}$ elements, which we will denote by $\alpha(z_\nu)$. More precisely,

$$L_\nu = \{\alpha(z_\nu) = \alpha_0 + \alpha_1 z_\nu - \ldots - \alpha_{\nu-1} z_\nu^{\nu-1} : \alpha_i \in L, \quad i = 0, 1, \ldots, \nu - 1\},$$

where $z_\nu^j = 0$ if $j \geq \nu$ and for $i = 0, 1, \ldots, \nu - 1$, the elements z_ν^i, form an $L-$basis of L_ν (see [2], [10]).

From now on, in order to simplify the notation, we assume that *L has q elements, so that L_ν will have q^ν elements.*

The following definitions and facts may be found in [2].

If μ and ν are positive integers and $\mu \leq \nu$, the mapping $\pi_{\mu,\nu} : L_\nu \longrightarrow L_\mu$ defined by $\alpha(z_\nu) \longmapsto \alpha(z_\mu)$, is an epimorphism of $L-$algebras, called the *projection* of L_ν onto L_μ. If $f_\nu(t)$ is a polynomial in $L_\nu[t]$ then,

$$\pi_{\mu,\nu}(f_\nu(t)) = f_\mu(t)$$

is the polynomial in $L_\mu[t]$ whose coefficients are the classes modulo $(p(X)^\mu)$ of the coefficients of $f_\nu(t)$.

If $\alpha(z_\nu) \subset L_\nu$ is a zero of $f_\nu(t)$, and $\mu \leq \nu$, we say that $\alpha(z_\nu)$ is a *descendant* of $\alpha(z_\mu)$, or that $\alpha(z_\mu)$ is an *ascendant* of $\alpha(z_\nu)$, if $\pi_{\mu,\nu}(\alpha(z_\nu)) = \alpha(z_\mu)$. In this case we clearly have $f_\mu(\alpha(z_\mu)) = 0$.

A zero $\alpha(z_\mu) \in L_\mu$ of f_μ is said to be *non singular* (or *regular*) if

$$\frac{df_1(\pi_{1,r}(\alpha(z_\mu)))}{dt} \neq 0\,.$$

Otherwise it is said to be *singular*. The following fact is readily seen: *every descendant (ascendant) of a non singular zero is a non singular zero.*

The set of all formal power series $L[[Z]]$

$$\sum_{i=0}^{\infty} \lambda_i Z^i = \lambda_0 + \lambda_1 Z + \lambda_2 Z^2 + \lambda_3 Z^3 + \ldots, \quad \lambda_i \in L,$$

equipped with the usual operations is an $L-$algebra, called *the algebra of formal power series* in one indeterminate over the finite field L. As a ring, $L[[Z]]$ is a discrete local ring with maximal ideal (Z). Actually, $L[[Z]]$ is the *projective limit* of the projective system of $L-$algebras $(L_\nu, (\pi_{\mu,\nu})_{\mu\leq\nu})$ if we define the canonical projections $\pi_\nu : L[[Z]] \longrightarrow L_\nu$ by

$$\lambda(Z) = \sum_{i=0}^{\infty} \lambda_i Z^i \longmapsto \lambda(z_\nu)\,,$$

where

$$\lambda(z_\nu) = \lambda_0 + \lambda_1 z_\nu + \lambda_2 z_\nu^2 + \ldots + \lambda_{\nu-1} z_\nu^{\nu-1}\,.$$

Let us remark *in passim* that each π_ν is an epimorphism of $L-$algebras. Moreover, $L[[Z]]/(Z^\nu) = L_\nu$. This said, if $f(t)$ is a polynomial with coefficients in $L[[Z]]$, its reduction $f_\nu(t)$ modulo (Z^ν) is the polynomial in $L_\nu[t]$ whose coefficients are the classes modulo (Z^ν) of the coefficients of $f(t)$. Clearly, if $\nu \geq \mu$ then $\pi_{\mu,\nu}(f_\nu(t)) = f_\mu(t)$. The above shows that $(L_\nu, \pi_{\mu,\nu})_{\nu\geq\mu}$ is a projective system whose limit is $L[[Z]]$.

Also, it is well known that $\varepsilon(Z) = \sum_{i=0}^{\infty} \varepsilon_i Z^i$ is a unit in $L[[Z]]$ if, and only if, $\varepsilon_0 \neq 0$. Moreover each $\lambda(Z) \neq 0$ may be written as $\lambda(Z) = \varepsilon(Z) Z^{v(\lambda)}$, where $\varepsilon(Z)$ is a unit and $v(\lambda) \geq 0$. Thus, $\lambda(Z)$ is a unit if $v(\lambda) = 0$, and

conversely. The mapping onto $\{0,1,\ldots\}\cup\{\infty\}$ defined by $\lambda(Z)\longmapsto v(\lambda)$ if $\lambda(Z)\neq 0$ and $v(0)=\infty$ is a discrete valuation, which induces a pseudometric on $L[[Z]]$. In this setting,

$$\lim_{k\to\infty}\sum_{i=0}^{k}\lambda_i Z^i=\lambda(Z)\,. \tag{1}$$

Further,

$$\pi_\nu(\lambda(Z))=\left[\varepsilon_0+\varepsilon_1 z_\nu+\cdots+\varepsilon_{\nu-1}z_\nu^{k-1}\right]z_\nu^{v(\lambda)}\,,$$

which equals 0 if $v(\lambda)\geq\nu$, and equals

$$\varepsilon_0+\varepsilon_1 z_\nu+\cdots+\varepsilon_{\nu-1}z_\nu^{v(\lambda)+k-1}$$

if $v(\lambda)<\nu$ and $\nu=k+v(\lambda)$. In particular, $\pi_1(\lambda(Z))=0$ if $\lambda(Z)$ is not a unit. In turn, this implies that if the leading coefficient of the polynomial $f(t)\in L[[Z]][t]$ of degree m is not a unit, then $f_1(t)$ has degree $<m$. To avoid this inconvenience, from now on we suppose that the leading coefficients of all the polynomials $f(t)$ are units.

The following two results may be found in [6, pp. 33, 53]:

Lemma 2.1. *Let $f(t)\in L[[Z]][t]$. Then the equation $f(t)=0$ has a solution in $L[[Z]]$ if, and only if, the equations $f_\nu(t)=0$ have solutions in L_ν for each $\nu\geq 1$.* □

Lemma 2.2. *Let $\alpha(Z)=\alpha_0+\alpha_1 Z+\cdots$ be a unit, and m a positive integer not divisible by p (the characteristic of L). Then α_0 has an $m-th$ root in L if, and only if, there exist $\gamma(Z)\in L[[Z]]$ such that $\gamma(Z)^m=\alpha(Z)$.* □

If $\tau(z_\nu)=\sum_{i=0}^{\nu-1}\tau_i z_\nu^i\in L_\nu$ let us define

$$\widehat{\tau}(z_\nu)=\sum_{i=0}^{\nu-2}\tau_i z_\nu^i\in L_\nu\,.$$

This notation enables us to state the following version of Taylor's formula, proved in [2, Proposition 2.3]:

Lemma 2.3. *If $f(t)$ is a polynomial with coefficients in $L[[Z]]$, then for each $\nu=2,3,\ldots$ we have*

$$f_\nu(\tau(z_\nu))=f_\nu(\widehat{\tau}(z_\nu))+\tau_{\nu-1}f'_\nu(\widehat{\tau}(z_\nu))z_\nu^{\nu-1}. \tag{2}$$

□

If now we write $f'_\nu(\widehat{\tau}(z_\nu))=\sum_{i=0}^{\nu-1}\chi_i z_\nu^i$, we obtain

$$\tau_{\nu-1}z_\nu^{\nu-1}f'_\nu(\widehat{\tau}(z_\nu))=(\tau_{\nu-1}\chi_0)z_\nu^{\nu-1}\,,$$

using that $z_\nu^n=0$ if $n\geq\nu$. Thus (2) becomes

$$f_\nu(\tau(z_\nu))=f_\nu(\widehat{\tau}(z_\nu))+\tau_{\nu-1}\chi_0 z_\nu^{\nu-1}\,. \tag{3}$$

3. Basic results

A polynomial $f(t)$ over $L[[Z]]$ is said to be a *permutation polynomial* if the associated polynomial function

$$\begin{aligned} f: L[[Z]] &\longrightarrow L[[Z]] \\ \alpha(Z) &\longmapsto f(\alpha(Z))\,, \end{aligned}$$

is a bijective function. Similarly, a polynomial $f_\nu(t)\in L_\nu[t]$, for $\nu=1,2,3,\ldots$ is said to be a permutation polynomial if the associated polynomial function from L_ν into L_ν is a bijective function.

The next proposition is crucial in our purpose to extend known results of permutation polynomials over finite fields to permutation polynomials over the algebras L_ν.

Proposition 3.1. *Let $f(t)\in L[[Z]][t]$. Then $f_\nu(t)$ permutes L_ν if, and only if, $f_1(t)$ permutes L and the zero of $f_1(t)$ in L is non singular.*

Proof. If $f_\nu(t)$ permutes L_ν then $f_\mu(t)$ permutes L_μ for all $\mu\leq\nu$. Indeed, if $\alpha(z_\mu)=\alpha_0+\alpha_1 z_\mu+\cdots+\alpha_{\mu-1}z_\mu^{\mu-1}\in L_\mu$, then $\alpha(z_\nu)=\alpha_0+\alpha_1 z_\nu+\cdots+\alpha_{\mu-1}z_\nu^{\mu-1}\in L_\nu$. Since, by hypothesis, $f_\nu(t)$ permutes L_ν there is $\beta(z_\nu)\in L_\nu$ such that $f_\nu(\beta(z_\nu))=\alpha(z_\nu)$. It is now clear that $\pi_{\mu,\nu}(f_\nu(\beta(z_\nu)))=f_\mu(\beta(z_\mu))=\alpha(z_\mu)$, which shows that the polynomial function induced by $f_\mu(t)$ on L_μ is onto and thus a bijection, since each L_μ is finite. In particular $f_1(t)$ permutes L. Now, using (3), we obtain for $\tau_0+\tau_1 z_2\in L_2$

$$f_2(\tau_0+\tau_1 z_2)=f_2(\tau_0)+\tau_1\chi_0 z_2\,,$$

and putting

$$f_2(\tau_0)=\gamma_0+\gamma_1 z_2$$

we obtain

$$f_2(\tau_0+\tau_1 z_2)=\gamma_0+(\gamma_1+\tau_1\chi_0)z_2\,.$$

Thus, for a given $\alpha_0+\alpha_1 z_2$, the equation

$$f_2(\tau_0+\tau_1 z_2)=\alpha_0+\alpha_1 z_2 \tag{4}$$

is solvable if, and only if, $\gamma_0=\alpha_0$ and $\gamma_1+\tau_1\chi_0=\alpha_1$. Since by hypothesis each $f_\nu(t)$ is a permutation polynomial, (4) is always solvable. In particular, if $\alpha_0=0$ then $f_1(\tau_0)=0$ has a unique solution τ_0. Now, if $\chi_0=0$, i.e., $f'_1(\tau_0)=0$, and since

$$\gamma_1+\tau_1\chi_0=\alpha_1\,, \tag{5}$$

this yields $\gamma_1 = \alpha_1$. But then (5) has exactly q solutions, which is no the case since $f_2(t)$ is a permutation polynomial. Therefore τ_0 is non singular.

Conversely, let $f(t) \in L[t]$ and suppose that $f_1(t)$ is a permutation polynomial whose zero is non singular. We show next that $f_2(t)$ permutes the elements of L_2. For this consider a given $\alpha_0 + \alpha_1 z_2 \in L_2$. Since, by hypothesis, $f_1(t)$ is a permutation polynomial, there is a unique $\tau_0 \in L$ such that $f_1(\tau_0) = \alpha_0$. For this τ_0 consider the equation

$$\begin{aligned} f_2(\tau_0 + \tau_1 z_2) &= f_2(\tau_0) + \tau_1 \chi_0 z_2 \\ &= \gamma_0 + (\gamma_1 + \tau_1 \chi_0) z_2 = \alpha_0 + \alpha_1 z_2 , \end{aligned} \tag{6}$$

where $f_2(\tau_0) = \gamma_0 + \gamma_1 z_2$. It is clear that in this situation γ_0 and γ_1 are completely determined by τ_0. From (6) we obtain $\gamma_0 = \alpha_0$ and

$$\alpha_1 = \gamma_1 + \tau_1 \chi_0 . \tag{7}$$

If $\alpha_0 = 0$, then $f_1(\tau_0) = 0$ has a solution and $f_1'(\tau_0) = \chi_0 \neq 0$, because of the hypothesis made on $f_1(t)$. So $\tau_1 = (\alpha_1 - \gamma_1)/\chi_0$, is uniquely determined. If $\alpha_0 \neq 0$ and $\chi_0 \neq 0$, from (7) we again obtain $\tau_1 = (\alpha_1 - \gamma_1)/\chi_0$. And, finally, if $\chi_0 = 0$ we see that $\gamma_1 = \alpha_1$. Consequently, the polynomial function induced by $f_2(t)$ is an onto mapping, and so this polynomial permutes L_2. We now proceed by induction on ν. Let

$$\alpha(z_\nu) = \alpha_0 + \alpha_1 z_\nu + \cdots + \alpha_{\nu-2} z_\nu^{\nu-2} + \alpha_{\nu-1} z_\nu^{\nu-1}$$

be given. Since by hypothesis $f_{\nu-1}(t)$ permutes the elements of $L_{\nu-1}$, the equation

$$f_{\nu-1}(t) = \alpha_0 + \alpha_1 z_{\nu-1} + \cdots + \alpha_{\nu-2} z_{\nu-1}^{\nu-2}$$

has a unique solution

$$\tau_0 + \tau_1 z_{\nu\ 1} + \cdots + \tau_{\nu\ 2} z_{\nu-1}^{\nu-2} .$$

Then Taylor's formula gives

$$\begin{aligned} f_\nu(\tau_0 + \tau_1 z_\nu + \cdots + \tau_{\nu-2} z_\nu^{\nu-2} + \tau_{\nu-1} z_\nu^{\nu-1}) \\ = f_\nu(\widehat{\tau}(z_\nu)) + \tau_{\nu-1} \chi_0 z_\nu^{\nu-1} , \end{aligned} \tag{8}$$

where $\tau_{\nu-1}$ is to be determined. If now we put

$$f_\nu(\widehat{\tau}(z_\nu)) = \gamma_0 + \gamma_1 z_\nu + \cdots + \gamma_{\nu-2} z_\nu^{\nu-2} + \gamma_{\nu-1} z_\nu^{\nu-1} ,$$

formula (8) becomes

$$\begin{aligned} f_\nu(\widehat{\tau}(z_\nu) + \tau_{\nu-1} z_\nu) = \\ \gamma_0 + \gamma_1 z_\nu + \cdots - \gamma_{\nu-2} z_\nu^{\nu\ 2} + (\gamma_{\nu-1} + \tau_{\nu-1}\chi_0) z_\nu^{\nu\ 1} \end{aligned}$$

Now all γ_i, $i = 0, \ldots, \nu - 1$, depend only on the τ_j, $j = 1, \ldots, \nu - 2$, which have been determined beforehand, so all of them are known quantities. Consequently the equation

$$\begin{aligned} f_\nu(\tau_0 + \tau_1 z_\nu + \cdots + \tau_{\nu-1} z_\nu^{\nu-1}) = \\ \alpha_0 + \alpha_1 z_\nu + \cdots - \alpha_{\nu-2} z_\nu^{\nu-2} - \alpha_{\nu-1} z_\nu^{\nu-1} \end{aligned}$$

has a solution if, and only if, $\gamma_i = \alpha_i$ for $i = 1, \ldots, \nu - 2$ and the linear equation in L

$$\tau_{\nu-1}\chi_0 + \gamma_{\nu-1} = \alpha_{\nu-1} \tag{9}$$

has a solution. If $\chi_0 = 0$, we must have $\gamma_{\nu-1} = \alpha_{\nu-1}$, so the equation (9) is solvable. If $\chi_0 \neq 0$, then $\tau_{\nu-1} = (\alpha_{\nu-1} - \gamma_{\nu-1})/\chi_0$, and again (9) is solvable □

Proposition 3.2. *Let $f(t) \in L[[Z]][t]$. Then $f(t)$ permutes $L[[Z]]$ if, and only if, $f_1(t)$ is a permutation polynomial and its zero in L is non singular.*

Proof. Suppose that $f(t)$ is a permutation polynomial. Given $\alpha(z_\nu) = \alpha_0 + \alpha_1 z_\nu + \alpha_2 z_\nu^2 + \ldots + \alpha_{\nu-1} z_\nu^{\nu-1}$, $\nu \geq 1$, then

$$\alpha(Z) = \alpha_0 + \alpha_1 Z + \alpha_2 Z^2 + \cdots + \alpha_{\nu-1} Z^{\nu-1} \in L[[Z]]$$

is such that $\pi_\nu(\alpha(Z)) = \alpha(z_\nu)$. Since $f(t)$ is a permutation polynomial there exists $\tau(Z) \in L[[Z]]$ such that $f(\tau(Z)) = \alpha(Z)$. This implies that, for all ν, the equation $f_\nu(t) = \alpha(z_\nu)$ has the solution $\tau(z_\nu)$, i.e. the polynomial function induced by $f_\nu(t)$ is onto. Since L_ν is finite, this polynomial function is a bijection. By Proposition 3.1, $f_1(t)$ is a permutation polynomial whose zero is non singular.

Conversely, let $f(t) \in L[[Z]][t]$ and suppose that $f_1(t)$ is a permutation polynomial whose zero is non singular, and consider the equation

$$f(t) = \alpha(Z) = \sum_{i=0}^{\infty} \alpha_i Z^i . \tag{10}$$

By Proposition 3.1, each $f_\nu(t)$ is now a permutation polynomial, so the equations ($\nu \geq 1$) $f_\nu(t) = \alpha(z_\nu)$ have all of them unique solutions

$$\tau(z_\nu) = \tau_0 + \tau_1 z_\nu + \cdots + \tau_{\nu-1} z_\nu^{\nu-1}$$

descending from the preceding ones. By Lemma 2.1, (10) has the solution

$$\tau(Z) = \lim_{\nu \to \infty} \left(\tau_0 + \tau_1 Z + \cdots + \tau_{\nu-1} Z^{\nu-1}\right) .$$

On the other hand, if $f(\alpha(Z)) = f(\beta(Z))$ then $f_\nu(\alpha(z_\nu)) = f_\nu(\beta(z_\nu))$, $\nu \geq 1$, but f_ν is a permutation polynomial, then $\alpha(z_\nu) = \beta(z_\nu)$ for all ν, then, $\alpha(Z) = \beta(Z)$ □

Proposition 3.3. [1, Prop. 4.4] *If $\nu \geq 2$, then the polynomial $f_\nu(t) = t^k \in L_\nu[t]$ is a permutation polynomial if, and only if, $k = 1$.*

Proof. Let us see that if $k > 1$, then the number of zeroes of $f_\nu(t) = t^k$ is bigger that 1, so it cannot be a permutation polynomial. Clearly $f(0) = 0$. If we evaluate f_ν at $\lambda(z_\nu) = z_\nu^{\nu-1}$ we obtain $\lambda(z_\nu)^k = z_\nu^{k(\nu-1)}$ which is null if, and only if, $k(\nu-1) \geq \nu$, i.e., if $k \geq \frac{\nu}{\nu-1} > 1$. If this is the case, $f_\nu(t) = t^k$ can not be a permutation polynomial. Conversely, $\lambda(z_\nu)^k \neq 0$ if, and only if, $k(\nu-1) \leq (\nu-1)$, i.e., if $k \leq 1$, or equivalently , if $k = 1$. Finally, it is clear that $f_\nu(t) = t$ is a permutation polynomial. □

Corollary. *$f(t) = t^k \in L[[Z]][t]$ is a permutation polynomial if, and only if, $k = 1$.* □

Let us consider now the polynomial

$$f(t) = t^{p^r} - \alpha(Z)t + \beta(Z) \in L[[Z]][t]\,, \qquad (11)$$

If $\alpha(Z)$ and $\beta(Z)$ are not units, we see that $1-\alpha(Z) \neq 0$, and $\alpha_0 = 0$, $\beta_0 = 0$, so that $f_1(t) = t^{p^r}$. Using the above corollary, $f_1(t)$ is a permutation polynomial if, and only if,

$$f(t) = t(1 - \alpha(Z)) + \beta(Z)\,,$$

which is indeed a permutation polynomial. Next, if $\alpha(Z)$ is a unit and $\beta_0 = 0$, then $f_1(t) = t^{p^r} - \alpha_0 t$ and $\alpha_0 \neq 0$. If $p < p^{r+1} \leq q$, this polynomial is a permutation polynomial if, and only if, α_0 is not a $(p^r-1)^{\text{th}}$ power in L (see, e.g., [1, Proposition 2.6]). But using Lemma 2.2 and the fact that the characteristic p of L does not divide p^r-1, we see that $\alpha(Z)$ is not the $(p^r-1)^{\text{th}}$ power of an element in $L[[Z]]$. Thus we have proved the following

Proposition 3.4. *If $\beta(Z)$ is not a unit, then the polynomial (11) is a permutation polynomial if, and only if, $\alpha(Z)$ is not a unit and $r = 0$, or $\alpha(Z)$ is a unit which is not a $(p^r-1)^{th}$ power $(p < p^{r+1} \leq q)$ of some element of $L[[Z]]$.* □

The previous proposition gives necessary and sufficient conditions to determine when the polynomial $t^{p^r} - \alpha(Z)t \in L[[Z]][t]$ is a permutation polynomial. A sufficient condition to decide if (11) is a permutation polynomial when $\beta(Z)$ is a unit, is stated in the next corollary.

Corollary. *If $t^{p^r} - \alpha(Z)t \subset L[[Z]]$ is a permutation polynomial and $\beta(Z)$ is a unit, then the polynomial (11) is a permutation polynomial .*

Proof. If $t^{p^r} - \alpha(Z)t$ is a permutation polynomial then $t^{p^r} - \alpha_0 t$ is a permutation polynomial and by Proposition 2.4 in [1], $t^{p^r} - \alpha_0 t + \beta_0$ is a permutation polynomial. Moreover it is clear that its zero is non singular. Therefore the polynomial (11), by proposition 3.2, is a permutation polynomial. □

Lemma 3.4. *If $f(t) \in L[[Z]][t]$ is a permutation polynomial and $\gamma(Z) \in L[[Z]]$ is not a unit, then $f(t)+\gamma(Z)$ is a permutation polynomial.* □

In the previous lemma the hypothesis that $\gamma(Z)$ is a not unit is necessary since otherwise we can find permutation polynomials $f(t)$ such that $f(t)+\gamma(Z)$ is not a permutation polynomial. For example, the polynomial $f(t) = t^5 + 2 \in \mathbb{F}_3[[Z]]$ is a permutation polynomial but the polynomial $f(t) + 1 = t^5$ $(\gamma(Z) = 1)$ is not a permutation polynomial (corollary to proposition 3.3).

If $f(t) \in L[[Z]][t]$ is a permutation polynomial, let us consider the polynomial:

$$g(t) - \alpha(Z)f(t + \beta(Z)) + \gamma(Z) \in L[[Z]]\,, \qquad (12)$$

where $\alpha(Z)$ is a unit and $\gamma(Z)$ is not a unit. Since $f(t)$ is a permutation polynomial, $f_1(t)$ is also a permutation polynomial whose zero is non singular. Therefore, by Proposition 2.4 in [1], $g_1(t) = \alpha_0 f_1(t + \beta_0)$ is a permutation polynomial. Now, if $g_1(\tau_0) = 0$, then $\alpha_0 f_1(\tau_0 + \beta_0) = 0$, i.e., $\tau_0 + \beta_0$ is a zero of $f_1(t)$. If $g_1'(\tau_0) = 0$, then $f_1'(\tau_0 + \beta_0) = 0$ but this is a contradiction since $f'(t)$ is a permutation polynomial. Therefore τ_0 is non singular zero of g_1. Then Proposition 3.2 and lemma 3.4 yield that $g(t)$ is a permutation polynomial. Thus we have proved the following

Proposition 3.5. *If $f(t) \in L[[Z]][t]$ is a permutation polynomial, $\alpha(Z)$ is a unit, and $\gamma(Z)$ is not a unit in $L[[Z]]$, then the polynomial (12) is a permutation polynomial.* □

The following proposition generalize results stated in [1] and [8, pp 362, 390].

Proposition 3.6. *Let L/K be an extension of degree m and consider the polynomial*

$$f(t) = \sum_{j=0}^{m-1} \alpha_j(Z)t^{q^j} \in L[[Z]][t]\,,$$

where $\alpha_0(Z) \in L[[Z]]$ is a unit. Then

a) *$f(t)$ is a permutation polynomial if, and only if, 0 is its only zero in $L[[Z]]$.*
b) *If $f(t)$ is a permutation polynomial then $\det(\alpha_{|i-j|}^{q^j}(Z)) \neq 0$. Furthermore if $\det(\alpha_{|i-j|}^{q^j}) \neq 0$ where $i, j = 0, 1, \ldots, m-1$, then $f(t)$ is a permutation polynomial.*

c) *If $f(t) \in K[t]$ then $f(t)$ is a permutation polynomial in $L[[Z]]$ if, and only if,*

$$\left(\sum_{j=0}^{m-1} \alpha_j t^j, t^m - 1\right) = 1.$$

Proof. a) If $f(t)$ is a permutation polynomial and since $f(0) = 0$, it is clear that 0 is its unique zero in $L[[Z]]$. Conversely, suppose that 0 is the only zero of $f(t)$ in $L[[Z]]$. Then $f_1(t)$ has t as a factor. Moreover, since $f_1'(t) = \alpha_0 \neq 0$ all its zeroes will be then non singular. Suppose now that $\tau_0 \neq 0$ is another non singular zero of $f_1(t)$ in L. The proof of the sufficiency in the proposition 3.2 give us an argument to conclude the existence of $\tau(Z) \neq 0$ in $L[[Z]]$ such that $\pi_1(\tau(Z)) = \tau_0$ and $f(\tau(Z)) = 0$, which is a contradiction. Then by proposition 2.5 of [1], $f_1(t)$ is a permutation polynomial and since its unique zero is non singular, so $f(t)$ is a permutation polynomial.

b) If $f(t)$ is a permutation polynomial then $f_1(t)$ is again a permutation polynomial, which amounts to say that $\det(\alpha_{|i-j|}^{q^i}) \neq 0$, $(i, j = 0, 1, \ldots, m)$ because of item (4) in [7]; therefore $\det(\alpha_{|i-j|}^{q^i}(Z)) \neq 0$. Furthermore, if $\det(\alpha_{|i\ \ j|}^{q^i}) \neq 0$ then $f_1(t)$ is permutation polynomial, and again because of item (4) in [7], its zero is non singular. Therefore, $f(t)$ is a permutation polynomial. □

c) If $f(t)$ permutes $L[[Z]]$ then $f_1(t)$ permutes L (and its zero is non singular), then by item (4) in [7] we have the conclusion. Conversely, if

$$\left(\sum_{j=0}^{m-1} \alpha_j t^j, t^m - 1\right) = 1,$$

then, $f_1(t)$ is a permutation polynomial [7]. Moreover, since $f_1'(t) = \alpha_0 \neq 0$ its unique zero $(= 0)$ is non singular, and thus $f(t) \in L[[Z]][t]$ is a permutation polynomial, by proposition 3.2.

Proposition 3.7. *Let q be odd and $f(t) = t^{(q+1)/2} + \alpha(Z)t + \beta(Z) \in L[[Z]][t]$, $\alpha(Z)$ a unit and $\beta(Z)$ not a unit. Then $f(t)$ is a permutation polynomial if, and only if, $\alpha(Z)^2 - 1$ is a square in $L[[Z]]$.*

Proof. If $f(t)$ is a permutation polynomial over $L[[Z]]$ then $f_1(t)$ is a permutation polynomial in L, thus $\alpha_0^2 - 1$ is a square in L ([3, theor. 4.1]), and by lemma 2.2 $\alpha(Z)^2 - 1$ is a square in $L[[Z]]$. Conversely, if $\alpha(Z)^2 - 1$ is a square in $L[[Z]]$ then $\alpha_0^2 - 1$ is a square in L (lemma 2.2), therefore, again by [3, theor. 4.1], $f_1(t)$ is a permutation polynomial, moreover $f_1(0) = 0$. But

$$f_1'(t) = \frac{q+1}{2} t^{(q-1)/2} + \alpha_0,$$

and since $\alpha_0 \neq 0$, zero is a non singular zero of $f_1(t)$. Therefore, proposition 3.2 and lemma 3.4 implies $f(t)$ is a permutation polynomial. □

The previous proposition is a partial analogue of **Wan Daqing**'s theorem 4.1 in [3]. The following proposition includes analogues of results obtained by **Wan Daqing** in [3, Section 2]. We omit the proof since it is straightforward.

Proposition 3.8. *If $1 < k < q$, $\gamma(Z)$ is not a unit and $\alpha(Z) \in L[[Z]]$, then*

1. *If k is not a power of p that satisfies $q \geq (k^2 - 4k + 6)^2$, then $f(t) = t^k + \alpha(Z)t + \gamma(Z) \in L[[Z]]$, is not a permutation polynomial over $L[[Z]]$.*
2. *Let J be an integer such that $1 \leq J \leq q - 2$. If $f(t) = t^k + \alpha(Z)t + \gamma(Z) \in L[[Z]]$, $\alpha(Z)$ a unit, is a permutation polynomial in $L[[Z]]$ then the equation*

$$ki + j \equiv 0 (\mathrm{mod}\ (q-1)), \quad i + j = J,$$
$$\binom{J}{j} \not\equiv 0 (\mathrm{mod}\ p),\ 0 \leq j \leq J$$

has either no solutions (i, j) or at least two solutions of (i, j). □

The following proposition lists permutation polynomials over $L[[Z]]$, of degree at most 5, corresponding to the classical list in [4, § 90].

Proposition 3.9. *Let $\alpha(Z)$, $\beta(Z)$, $\gamma_1(Z)$, $\gamma_2(Z)$, $\gamma_3(Z)$ and $\gamma(Z)$ elements of $L[[Z]]$. If $\gamma_1(Z)$, $\gamma_2(Z)$, $\gamma_3(Z)$, and $\gamma(Z)$ are not units then the following polynomials in $L[[Z]]$ are permutation polynomials:*

a) $t^3 + \gamma_1(Z)t^2 - \alpha(Z)t + \gamma(Z)$, *if* $\alpha(Z) \notin L[[Z]]^2$ *and* $q = 3^n$,
b) $t^4 + \gamma_1(Z)t^2 + \gamma_2(Z)t \pm 3t + \gamma(Z)$, *if* $q = 7$,
c) $t^4 + \gamma_1(Z)t^3 + \alpha(Z)t^2 + \beta(Z)t + \gamma(Z)$, *if $\beta(Z)$ is a unit, the unique zero of its projection in L is $t - 0$ and if* $q = 2^n$,
d) $t^5 - \gamma_1(Z)t^4 + \gamma_2(Z)t^3 + \gamma_3(Z)t^2 - \alpha(Z)t + \gamma(Z)$, *si* $\alpha(Z) \notin L[[Z]]^4$ *and* $q = 5^n$,
e) $t^5 + \gamma_2(Z)t^4 + \gamma_2(Z)t^3 + \gamma_3(Z)t^2 \pm 2^{1/2}t + \gamma(Z)$, *if* $q = 3^2$,

f) $t^5+\gamma_1(Z)t^4+\alpha(Z)t^3\pm t^2+3\alpha(Z)^2t-\gamma(Z)$, *if* $\alpha(Z)\notin L[[Z]]^2$ *and* $q=7$,

g) $t^5+\gamma_1(Z)t^4+\alpha(Z)t^3+\gamma_2(Z)t^2+\frac{\alpha(Z)^2}{5}t+\gamma(Z)$, *if* $\alpha(Z)$ *is a unit and* $q=5m\pm 2$,

h) $t^5+\gamma_1(Z)t^4+\alpha(Z)t^3+\gamma_2(Z)t^2+3\alpha(Z)^2t+\gamma(Z)$, *if* $\alpha(Z)\notin L[[Z]]^2$ *and* $q=13$,

i) $t^5+\gamma_1(Z)t^4-2\alpha(Z)t^3+\gamma_2(Z)t^2+\alpha(Z)^2t+\gamma(Z)$, *if* $\alpha(Z)\notin L[[Z]]^2$ *and* $q=5^n$.

Proof. The projections over L of these polynomials are identical to the polynomials listed by **Dickson** in [4]. The resultant polynomials over L are permutation polynomials which have 0 as their unique zero. Moreover it is easy to see that 0 is a non singular zero for each one of them, so the given polynomials are permutation polynomials in $L[[Z]]$. □

4. Dickson Polynomials

Dickson introduced a particular kind of polynomials over a finite field afterwards coined by **I. Schur** as *Dickson polynomials*. Dickson polynomials have interesting applications in coding theory, the construction of RSA (Reed-Solomon-Aldeman) cryptosystems, and *complete mappings* of finite fields. In 1923 **Schur** conjectured that polynomials over $\mathbb{Z}$ which are permutation polynomials modulo p for infinitely many primes p are precisely compositions of linear and Dickson polynomials. **Michael Fried** in 1970 [5, §1] succeeded in proving this was so. Also, Dickson polynomials have interesting and diverse properties that make them a valuable study topic.

A polynomial in $L[[Z]][t]$ of the type

$$g_k(t,\alpha(Z))=\sum_{j=0}^{\lfloor k/2\rfloor}\frac{k}{k-j}\binom{k-j}{j}(-\alpha(Z))^j t^{k-2j},$$

where $\alpha(Z)\in L[[Z]]$, k is a positive integer and $\lfloor k/2\rfloor$ denotes the integer part of $k/2$, is called a *Dickson polynomial of the second kind with parameter* $\alpha(Z)$ *and degree* k, or simply a *Dickson polynomial*.

In this section we are interested in finding values for $\alpha(Z)$ and/or k, telling us when a Dickson polynomial is a permutation polynomial. For example, if $\alpha(Z)=0$ then $g_k(t,\alpha(Z))=t^k$, and corollary to proposition 3.3 tells us that $g_k(t,0)$ is a permutation polynomial only when $k=1$. If k is even, all exponents of t are even, and clearly g_k is not a permutation polynomial. From now on we suppose that $\alpha(Z)\neq 0$ and that k is odd and we denote by $g_k(t,\alpha_0)$ the projection of $g_k(t,\alpha(Z))$ in $L[t]$.

Proposition 4.1. *If* $g_k(t,\alpha(Z))\in L[[Z]][t]$ *is a Dickson polynomial of the second kind, then* $g_k(t,\alpha(Z))$ *is a permutation polynomial if, and only if,* $(k,p(q^2-1))=1$ *and* $\alpha(Z)$ *is a unit.*

Proof. We suppose that $g_k(t,\alpha(Z))$ is a permutation polynomial. Then $g_k(t,\alpha_0)\in L[t]$ is a permutation polynomial whose zero is non singular. If $g_k(t,\alpha_0)$ is a permutation polynomial and k is odd, by [7, (3)], $(k,q^2-1)=1$. Moreover, since

$$\frac{d\,g_k(0,\alpha_0)}{dt}=k(-\alpha_0)^{\lfloor k/2\rfloor},$$

and $\alpha_0\neq 0$, if $p\mid k$ then the previous equality is zero, i.e, 0 is a singular zero of $g_k(t,\alpha_0)$, which is a contradiction. Therefore, $(k,p(q^2-1))=1$.

We suppose now that $(k,p(q^2-1))=1$, then, $(k,q^2-1)=1$. Again by (3) in [7] we have that $g_k(t,\alpha_0)$ is a permutation polynomial. Since $\alpha_0\neq 0$ then 0, the unique zero of $g_k(t,\alpha_0)$, is regular, since if $k(-\alpha_0)^{\lfloor k/2\rfloor}=0$ then $\alpha_0=0$ or $k=0$. But $\alpha_0\neq 0$ and since $(k,p(q^2-1))=1$, then $p\nmid k$, and therefore $k\neq 0$. Thus $g_k(t,\alpha_0)$ is a permutation polynomial whose zero is non singular. We conclude finally that $g_k(t,\alpha(Z))$ is a permutation polynomial. □

ACKNOWLEDGEMENTS

We wish to express our thanks to **Yuguang Lu** for his help in reading and understanding of [11] and [13].

References

[1] **Albis, V. S.** *Polinomios de permutation. Algunos problemas de interés*, Lecturas Matemáticas **22** (2001), 35–58.

[2] **Albis, V. S. & Chaparro, R.** *On a conjecture of Borevich and Shafarevich*, Rev. Acad. Colomb. Cienc. **21** (1997), 313–319. [MR: 98g:11130].

[3] **Daqing, W.** *Permutation binomials over finite fields*, Acta. Math. Sinica. **10** (1994), 30–35. [MR: 94m:11145].

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

[5] **Fried, M.** *On a conjecture of Schur*, Michigan Math. J. **17** No. 1 (1970), 41–55. [MR: 41# 1688].

[6] **Greenberg, M. J.** *Lectures on Forms in Many Variables*. W. A. Benjamin, New York, 1969.

[7] **Lidl, R. & Mullen, G. L** *When does a polynomial over a finite field permute the elements of the field?*, Amer. Math. Month. **95** (1988), 243–246.

[8] **Lidl, R. & Niederreiter, H.** *Finite Fields*, Encycl. of Math. and its Appl., Addison Wesley Pub. Comp. Reading Mass., 1983. [MR: 86c:11106].

[9] **McDonald, B. R** *Finite Rings with Identity*, Marcel Dekker, New York, 1974.

[10] **Smits, T. H.** *On the group of units of* $GF(q)[X]/(a(X))$. Indag. Math. **44** (1982), 355-358.

[11] **Sun, Q.** *A note on permutation polynomials vectors over* $\mathbb{Z}/m\mathbb{Z}$, Adv. Math. (China) **25** No. 1 (1996), 311–314. [In Chinese] [MR: 98h:11157]

[12] **Zhang, Q.** *On the polynomials in several indeterminates which can be extended to permutation polynomial vector over* $\mathbb{Z}/p^l\mathbb{Z}$, Adv. Math. **22** No. 5 (1993), 456–457.

[13] **Zhang, Q.** *Permutation polynomials in several indeterminates over* $\mathbb{Z}/m\mathbb{Z}$, Chinese Ann. Math. Ser. A. **16** No. 2 (1995), 168–172. [In Chinese] [MR: 96g:11143].

Recibido el 5 de agosto de 2005

Aceptado para su publicación el 19 de julio de 2006