Polynomial functions on a class of finite non-commutative rings

A Ali Abdulkader Al-Maktry [1] Susan F. El-Deken [2], [1]TU Graz University

[2]Helwan University

Ring Theory Seminar University of Graz 25 April 2024

Outline

1. Basics
2. Dual numbers
3. Polynomial functions on $R[\beta_1, \ldots, \beta_k]$
4. Permutation polynomials on $R[\beta_1, \ldots, \beta_k]$
   – The case R is a chain ring
5. The group of pure polynomial permutations
6. The stabilizer group of R

Definition 1

Let R be a non-commutative ring, and $g = \sum_{i=0}^{n} a_i x^i \in R[x]$. Then:

1. The polynomial g induces a function $F\colon R \longrightarrow R$ by right substitution $F(a) = f(a) = \sum_{i=0}^{n} a_i a^i$ for the variable x. We call F a (right)polynomial function on R. If F is a bijection, we call F a polynomial permutation and f is a permutation polynomial.
2. By $[g]_R$, we denote the (right) polynomial function induced by g on R. When the ring is understood, we write $[g]$.
3. If $f \in R[x]$ such that f and g induce the same (right)function on R, i.e. $[g] = [f]$, then we abbreviate this with $g \triangleq f$ on R.
4. We define $\mathcal{F}(R) = \{[g] \mid g \in R[x]\}$, and

$$\mathcal{P}(R) = \{[f] \mid [f] \text{ is a permutation of } R \text{ and } f \in R[x]\}.$$

Remark 2

- *$\mathcal{F}(R)$ is an additive group with respect to pointwise addition "$+$".*

Remark 2

- *$\mathcal{F}(R)$ is an additive group with respect to pointwise addition "+".*
- *$\mathcal{F}(R)$ is a monoid with respect to "$\circ$". Its group of units is $\mathcal{P}(R)$.*

Remark 2

- *$\mathcal{F}(R)$ is an additive group with respect to pointwise addition "+".*
- *$\mathcal{F}(R)$ is a monoid with respect to "$\circ$". Its group of units is $\mathcal{P}(R)$.*
- *We can not endorse $\mathcal{F}(R)$ with pointwise multiplication "$*$".*

Remark 2

- *$\mathcal{F}(R)$ is an additive group with respect to pointwise addition "+".*
- *$\mathcal{F}(R)$ is a monoid with respect to "$\circ$". Its group of units is $\mathcal{P}(R)$.*
- *We can not endorse $\mathcal{F}(R)$ with pointwise multiplication "$*$".*

Remark 2

- *$\mathcal{F}(R)$ is an additive group with respect to pointwise addition "+".*
- *$\mathcal{F}(R)$ is a monoid with respect to "$\circ$". Its group of units is $\mathcal{P}(R)$.*
- *We can not endorse $\mathcal{F}(R)$ with pointwise multiplication "$*$".*

  Because, substitution is not a homomorphism. Indeed, we can find $f, g \in R[x]$ and $r \in R$ such that

$$h(r) \neq f(r)g(r), \text{ where } h = fg,$$

  that is

$$[fg] \neq [f] * [g].$$

Definition 3

Let $f, g \in R[x]$. Let $f(x) = \sum_{j=0}^{n} a_j x^j$. Then

1. $(fg)(x) = \sum_{j=0}^{n} a_j g(x) x^j$;
2. $(fg)(r) = \sum_{j=0}^{n} a_j g(r) r^j$ for every $r \in R$.
3. $f \in R[x]$ is called null polynomial on R if $f(r) = 0$ for every $r \in R$. We write $f \triangleq 0$ on R.
4. We define: $N_R = \{f \in R[x] \mid f \triangleq 0 \text{ on } R\}$.

Corollary 4

Let R be a finite non-commutative ring. Then

1. *N_R is a left ideal of $R[x]$;*
2. *N_R is an ideal of $R[x]$ if and only if N_R is an R-right module.*

Remark 5

- *If every element in R can be written as a sum of units (for example semisimple rings and local rings), then N_R is an ideal [Werner, 2014].*

Corollary 4

Let R be a finite non-commutative ring. Then

1. *N_R is a left ideal of $R[x]$;*
2. *N_R is an ideal of $R[x]$ if and only if N_R is an R-right module.*

Remark 5

- *If every element in R can be written as a sum of units (for example semisimple rings and local rings), then N_R is an ideal [Werner, 2014].*
- *A result of [Stewart, 1972] infers that every element of a finite ring R is a sum of units if only if $R/J(R)$ has no factor ring isomorphic to $\mathbb{F}_2 \times \mathbb{F}_2$.*

Corollary 4

Let R be a finite non-commutative ring. Then

1. *N_R is a left ideal of $R[x]$;*
2. *N_R is an ideal of $R[x]$ if and only if N_R is an R-right module.*

Remark 5

- *If every element in R can be written as a sum of units (for example semisimple rings and local rings), then N_R is an ideal [Werner, 2014].*
- *A result of [Stewart, 1972] infers that every element of a finite ring R is a sum of units if only if $R/J(R)$ has no factor ring isomorphic to $\mathbb{F}_2 \times \mathbb{F}_2$.*
- *When R is the ring of upper triangular (lower) over commutative ring A, N_R is an ideal [Frisch, 2017].*

Proposition 6

Let R be a finite non-commutative ring. Define an operation "$\cdot$" on $\mathcal{F}(R)$ by letting $F \cdot F_1 = [fg]$, where $f, g \in R[x]$ such that $F = [f]$ and $[g] = F_1$. Then "$\cdot$" is well defined if and only if N_R is a two sided ideal; in this case $\mathcal{F}(R)$ is a ring endorsed with multiplication "$\cdot$" and pointwise addition.

Definition 7

Let R be a non-commutative ring and let T be the ideal of the polynomial ring $R[x_1, \ldots, x_k]$ generated by the set $\{x_i x_j \mid i, j \in \{1, \ldots, k\}\}$. We call the quotient ring $R[x_1, \ldots, x_k]/T$ the ring of dual numbers of k variables over R. We write $R[\beta_1, \ldots, \beta_k]$ for $R[x_1, \ldots, x_k]/T$, where β_i denotes $x_i + T$.

Remark 8

- *$R[\beta_1,\ldots,\beta_k]$ is a free R-algebra with basis $\{1,\beta_1,\ldots,\beta_k\}$. We have,*
$$R[\beta_1,\ldots,\beta_k] = \{r_0 + \sum_{i=1}^{k} r_i\,\beta_i \mid r_0, r_i \in R,\ \text{with}\ \beta_i\,\beta_j = 0 \text{ for } 1 \le i,j \le k\}.$$
- *We call the coefficient of 1 the "constant coefficient".*
- *Every polynomial $f \in R[\beta_1,\ldots,\beta_k][x]$ has a unique representation*
$$f = f_0 + \sum_{i=1}^{k} f_i\,\beta_i, \text{ where } f_0, f_1, \ldots, f_k \in R[x].$$
- $(a_0 + \sum_{i=1}^{k} a_i\,\beta_i)(b_0 + \sum_{i=1}^{k} b_i\,\beta_i) = a_0 b_0 + \sum_{i=1}^{k}(a_0 b_i + a_i b_0)\,\beta_i$ *for every* $a_i, b_i \in R$.

Proposition 9

Let R be a non-commutative ring. Then the following statements hold.

1. *For $a_0, \dots, a_k, b_0, \dots, b_k \in R$, we have:*
   $$a_0 + \sum_{i=1}^{k} a_i \beta_i \text{ is a unit in } R[\beta_1, \dots, \beta_k] \text{ if and only if } a_0 \text{ is a unit in } R.$$
2. *$R[\beta_1, \dots, \beta_k]$ is a local ring if and only if R is a local ring.*
3. $J(R[\beta_1, \dots, \beta_k]) = J(R) + \sum_{i=1}^{k} \beta_i R.$
4. $C(R[\beta_1, \dots, \beta_k]) = C(R) + \sum_{i=1}^{k} C(R) \beta_i.$

If R is commutative, then by binomial theorem, for any $f \in R[x]$ and $a, b_i \in R$,

$$f(a + \sum_{i=1}^{k} b_i \beta_i) = f(a) + \sum_{i=1}^{k} f'(a) b_i \beta_i.$$

If R is commutative, then by binomial theorem, for any $f \in R[x]$ and $a, b_i \in R$,

$$f(a + \sum_{i=1}^{k} b_i \beta_i) = f(a) + \sum_{i=1}^{k} f'(a) b_i \beta_i.$$

Definition 10

Let $f = \sum_{j=0}^{n} a_j x^j \in R[x]$. Then we assign to f a unique polynomial $\lambda_f(y, z)$ in the non-commutative variables y and z defined by

$$\lambda_f(y, z) = \sum_{j=1}^{n} \sum_{r=1}^{j} a_j y^{r-1} z y^{j-r}.$$

We call λ_f the assigned polynomial of (to) f.

Fact 11

Let $r, s, w \in R$. Let f and $g \in R[x]$. Then

1. $\lambda_{rf+sg} = \lambda_{rf} + \lambda_{sg}$;
2. $\lambda_{fr+gs} = \lambda_{fr} + \lambda_{gs}$;
3. $\lambda_f = 0$ *if and only if f is constant;*
4. $\lambda_f(0, z) = a_1 z$ *and* $\lambda_f(y, 1) = f'(y)$, *where* $f(x) = \sum_{j=0}^{n} a_j x^j$;
5. $\lambda_f(y, 0) = 0$;
6. $\lambda_f(r, s \pm w) = \lambda_f(r, s) \pm \lambda_f(r, w)$.

From now on let R_k denote $R[\beta_1, \ldots, \beta_k]$.

Lemma 12

Let R be a ring and $a, b_1, \ldots, b_k \in R$.

1. *If $f \in R[x]$ and λ_f is its assigned polynomial then*

$$f(a + \sum_{i=1}^{k} b_i \beta_i) = f(a) + \sum_{i=1}^{k} \lambda_f(a, b_i) \beta_i .$$

2. *If $f = f_0 + \sum_{i=1}^{k} f_i \beta_i$, where $f_0, \ldots, f_k \in R[x]$, then*

$$f(a + \sum_{i=1}^{k} b_i \beta_i) = f_0(a) + \sum_{i=1}^{k} (\lambda_{f_0}(a, b_i) + f_i(a)) \beta_i .$$

Definition 13

Let $f = \sum_{j=0}^{n} a_j x^j \in R[x]$ and $\lambda_f(y, z)$ be its assigned polynomial. Then

1. the assigned λ_f induces (defines) a function $F \colon R \times R \longrightarrow R$

$$F(a, b) = \lambda_f(a, b) = \sum_{j=1}^{n} \sum_{r=1}^{j} a_j a^{r-1} b a^{j-r},$$

   which we denote by $[\lambda_f(y, z)]$;

2. for every $a \in R$ the polynomial $\lambda_f(a, z) = \sum_{j=1}^{n} \sum_{r=1}^{j} a_j a^{r-1} z a^{j-r}$ defines a function $F_a \colon R \longrightarrow R$ by $F_a(b) = \lambda_f(a, b)$, which we denote by $[\lambda_f(a, z)]$.

Definition 14

1. Let $f \in R[x]$ and let λ_f be its assigned polynomial. We call λ_f is null if $\lambda_f(a, b) = 0$ for every $a, b \in R$. We write $[\lambda_f(y, z)] = 0$.
2. We define AN_R as: $AN_R = \{f \in N_R \mid [\lambda_f(y, z)] = 0\}$.
3. We define N'_R as: $N'_R = \{f \in N_R \mid f' \in N_R\}$.

Remark 15

1. *Obviously, AN_R and N'_R are left ideals of $R[x]$ with $AN_R, N'_R \subseteq N_R$.*
2. *Let $f \in AN_R$. Then $[\lambda_f(y, z)] = 0 \Rightarrow \lambda_f(a, 1) = f'(a) = 0$ for every $a \in R$. Hence $f \in N'_R$, and $AN_R \subseteq N'_R \subseteq N_R$.*
3. *When R is commutative: the condition on λ_f in the definition of AN_R is equivalent to $f' \in N_R$. So, $AN_R = N'_R$ over commutative rings.*

Theorem 16

Let N_R and AN_R be as in Definition 14. Then

1. $N_{R_k} = AN_R + \sum_{i=1}^{k} N_R\,\beta_i$;
2. N_{R_k} *is an ideal of* $R_k[x]$ *if and only if* AN_R *and* N_R *are ideals of* $R[x]$.

Corollary 17

Let $f = f_0 + \sum_{i=1}^{k} f_i\,\beta_i$*, where* $f_0, \ldots, f_k \in R[x]$*. Then the following are equivalent*

1. $f \in N_{R_k}$ *(i.e. f is a null polynomial on R_k)*;
2. $f_0, f_i\,\beta_i \in N_{R_k}$ *for* $i = 1, \ldots, k$;
3. $[\lambda_{f_0}(y, z)] = 0$ *and* $f_i \in N_R$ *for* $i = 0, \ldots, k$.

Corollary 18

Let $f = f_0 + \sum_{i=1}^{k} f_i\,\beta_i$ *and* $g = g_0 + \sum_{i=1}^{k} g_i\,\beta_i$*, where* $f_0, \ldots, f_k, g_0, \ldots, g_k \in R[x]$*.*
Then $f \triangleq g$ *on* R_k *if and only if the following conditions hold:*

1. $[\lambda_{f_0}(y, z)] = [\lambda_{g_0}(y, z)]$*;*
2. $[f_i]_R = [g_i]_R$ *for* $i = 0, \ldots, k$*.*

Corollary 18

Let $f = f_0 + \sum_{i=1}^{k} f_i \beta_i$ *and* $g = g_0 + \sum_{i=1}^{k} g_i \beta_i$, *where* $f_0, \ldots, f_k, g_0, \ldots, g_k \in R[x]$.

Then $f \triangleq g$ *on* R_k *if and only if the following conditions hold:*

1. $[\lambda_{f_0}(y, z)] = [\lambda_{g_0}(y, z)]$;
2. $[f_i]_R = [g_i]_R$ *for* $i = 0, \ldots, k$.

Or equivalently:

- $f_0 \equiv g_0 \mod AN_R$;
- $f_i \equiv g_i \mod N_R$ *for* $i = 1, \ldots, k$.

Proposition 19

Let R be a finite non-commutative. The following statements are equivalent

1. *every element of R is a sum of units;*
2. *every element of R_k is a sum of units;*
3. $R/J(R)$ *has no factor ring isomorphic to* $\mathbb{F}_2 \times \mathbb{F}_2$*;*
4. $R_k/J(R_k)$ *has no factor ring isomorphic to* $\mathbb{F}_2 \times \mathbb{F}_2$*.*

Proposition 19

Let R be a finite non-commutative. The following statements are equivalent

1. *every element of R is a sum of units;*
2. *every element of R_k is a sum of units;*
3. *$R/J(R)$ has no factor ring isomorphic to $\mathbb{F}_2 \times \mathbb{F}_2$;*
4. *$R_k/J(R_k)$ has no factor ring isomorphic to $\mathbb{F}_2 \times \mathbb{F}_2$.*

Proof.

By Remark 5, we need only show only (3)$\Leftrightarrow$ (4). By Proposition 9, $J(R_k) = J(R) + \sum_{i=1}^{k} \beta_i R$. Then one easily sees that

$$R_k/J(R_k) = (R + \sum_{i=1}^{k} \beta_i R)/(J(R) + \sum_{i=1}^{k} \beta_i R) \cong R/J(R).$$

$\square$

Corollary 20

Suppose that R (alternatively R_k) satisfies the condition of Proposition 19. Then

1. N_{R_k} *is an ideal of* $R_k[x]$;
2. N_R *and* AN_R *are ideals of* $R[x]$.

Corollary 20

Suppose that R (alternatively R_k) satisfies the condition of Proposition 19. Then

1. N_{R_k} *is an ideal of* $R_k[x]$;
2. N_R *and* AN_R *are ideals of* $R[x]$.

From now on we consider a non-commutative ring R in which N_R and AN_R are ideals of $R[x]$ (equivalently N_{R_k} is an ideal of $R_k[x]$).

Proposition 21

The number of polynomial functions on R_k is given by

$$|\mathcal{F}(R_k)| = \left[R[x]\colon AN_R\right]\left[R[x]\colon N_R\right]^k = [N_R\colon AN_R]|\mathcal{F}(R)|^{k+1}.$$

Proposition 21

The number of polynomial functions on R_k is given by

$$|\mathcal{F}(R_k)| = \left[R[x]\colon AN_R\right]\left[R[x]\colon N_R\right]^k = [N_R\colon AN_R]|\mathcal{F}(R)|^{k+1}.$$

Corollary 22

Let $F \in \mathcal{F}(R)$ be fixed.

$$[N_R\colon AN_R] = |\{[\lambda_f(y,z)] \mid f \in R[x] \text{ such that } [f]_R = F\}|.$$

Theorem 23

Let R be a finite non-commutative ring. Let $f = f_0 + \sum_{i=1}^{k} f_i \beta_i$, *where* $f_0, \ldots, f_k \in R[x]$. *Then the following statements are equivalent:*

1. f *is a permutation polynomial on* R_k;
2. f_0 *is a permutation polynomial on* R_k;
3. f_0 *is a permutation polynomial on R and* $[\lambda_{f_0}(y, z)]$ *is a local permutation on R in* z.

Theorem 23

Let R be a finite non-commutative ring. Let $f = f_0 + \sum_{i=1}^{k} f_i \beta_i$*, where* $f_0, \ldots, f_k \in R[x]$*. Then the following statements are equivalent:*

1. f *is a permutation polynomial on* R_k*;*
2. f_0 *is a permutation polynomial on* R_k*;*
3. f_0 *is a permutation polynomial on R and* $[\lambda_{f_0}(y, z)]$ *is a local permutation on R in* z*.*

Definition 24

A function $G\colon R \times R \longrightarrow R$ a local permutation in the second coordinate, if for every $a \in R$ the function $G_a\colon R \longrightarrow R$, $r \to G(a, r)$, is bijective.

Remark and Question 25

1. *If R is a commutative ring, then the condition on $\lambda_{f_0}(y, z)$ ($f_0 \in R[x]$) in Theorem 23 is equivalent to f_0' maps R to its group of units.*
2. *In the special case R is a local commutative that is not a field, the condition on f_0' is redundant, that is f_0 is a permutation polynomial on R_k if and only if f_0 is a permutation polynomial on R ([Al-Maktry, 2023, Proposition 4.7]).*
3. *The previous point motivates us to ask the following question in the non-commutative case:*

   Let R be a finite non-commutative local rings does the condition on $\lambda_{f_0}(y, z)$ ($f_0 \in R[x]$) in Theorem 23 is redundant?

Corollary 26

Let $f_0, \ldots, f_k \in R[x]$. The following statements are equivalent:

1. $f = f_0 + \sum_{i=1}^{k} f_i\,\beta_i$ *is a permutation polynomial on* R_k*;*
2. $f_0 + f_i\,\beta_i$ *is a permutation polynomial on* $R[\beta_i]$ *for every* $i \in \{1, \ldots, k\}$*;*
3. f_0 *is a permutation polynomial on* $R[\beta_i]$ *for every* $i \in \{1, \ldots, k\}$*.*
4. $f_0 + \sum_{i=1}^{j} f_i\,\beta_i$ *is a permutation polynomial on* R_l *for every* $1 \le j \le k$ *and* $l \ge j$*;*
5. f_0 *is a permutation polynomial on* R_j *for every* $j \ge 1$*.*

Remark 27

For the ring of Matrices of dimension n over a finite local ring R, $M_n(R)$, Brawley proved the following criteria [Brawley, 1976, Theorem 2]:
Let $f \in R[x]$ and let $\bar{f} \in \mathbb{F}_q[x]$ be the image of f in $\mathbb{F}_q[x]$, where $\mathbb{F}_q = R/M$. Then f is a permutation polynomial on $M_n(R)$ if and only if

1. *$\bar{f}$ is a permutation polynomial on $M_n(\mathbb{F}_q)$, and*
2. *the function $[\lambda_{\bar{f}}(y, z)]$ is a local permutation of $M_n(\mathbb{F}_q)$ in z.*

Proposition 28

Let R be a finite non-commutative ring. Let L be the number of pairs of functions (F, H) such that

1. $F\colon R \longrightarrow R$ *is bijective;*
2. $H\colon R \times R \longrightarrow R$ *is a local permutation in the second coordinate;*

occurring as $([f]_R, [\lambda_f(y, z)])$ for some $f \in R[x]$.
Then the number of polynomial permutations on R_k is given by

$$|\mathcal{P}(R_k)| = L \cdot |\mathcal{F}(R)|^k.$$

Finite local rings

- A finite ring R is called a local ring if the set M of all zero-divisors of R is an ideal (two-sided ideal) of R.
- M is the unique maximal ideal of R, and there exists a minimal positive integer N such that $M^N = \{0\}$.
- The characteristic of the ring $Char(R) = p^c$ $(1 \leq c \leq N)$ (p prime).
- $R/M = \mathbb{F}_q$ where $q = p^w$ $(w \geq 1)$.
- If $c = N$, R is commutative (not vice versa).
- If the lattice of left ideals (right ideals) is a chain, R is called a chain.
- In a chain ring: $M^i = t^i R = Rt^i$ for some element $t \in M \setminus M^2$ $(i = 0, 1, \ldots, N)$.

See [Nechaev, 2008]

The case R is a chain ring

Lemma 29

Let R be a finite chain ring and let $f \in R[x]$. The following statements hold

1. *R is semi-commutative;*
2. $f(a+m) = f(a) + \lambda_f(a, m)$ *for every* $a, m \in R$ *with* $m^2 = 0$.

The case R is a chain ring

Lemma 29

Let R be a finite chain ring and let $f \in R[x]$. The following statements hold

1. *R is semi-commutative;*
2. $f(a+m) = f(a) + \lambda_f(a, m)$ *for every* $a, m \in R$ *with* $m^2 = 0$.

From now on, whenever R is a chain ring, we assume $Char(R) = p^c$ with $c > 1$.

The case R is a chain ring

Proposition 30

Let R be a finite-non commutative chain ring, and let $f \in R[x]$ be a permutation polynomial on R. Then the following statements hold

1. $f'(a) \neq 0 \mod M$ *for every* $a \in R$;
2. $[\lambda_f(y, z)]$ *is a local permutation in* z.

The case R is a chain ring

Theorem 31

Let R be a finite chain. Let $f = f_0 + \sum_{i=1}^{k} f_i \beta_i$, where $f_0, \ldots, f_k \in R[x]$. Then the following statements are equivalent:

1. *f is a permutation polynomial on R_k;*
2. *f_0 is a permutation polynomial on R_k;*
3. *f_0 is a permutation polynomial on R.*

Proof.

(1)$\equiv$ (2)$\Rightarrow$ (3) by Theorem 23. (3) $\Rightarrow$ (2) by Proposition 30. $\square$

Definition 32

Let $k \geq 1$. The set $\mathcal{P}_R(R_k) = \{F \in \mathcal{P}(R_k) \mid F = [f]_{R_k} \text{ for some } f \in R[x]\}$ is a subgroup of the group $\mathcal{P}(R_k)$. We call $\mathcal{P}_R(R_k)$ the group of pure polynomial permutations.

Fact 33

Let $k, i \geq 1$. Then $\mathcal{P}_R(R_i) \cong \mathcal{P}_R(R_k)$.

Definition 32

Let $k \geq 1$. The set $\mathcal{P}_R(R_k) = \{F \in \mathcal{P}(R_k) \mid F = [f]_{R_k} \text{ for some } f \in R[x]\}$ is a subgroup of the group $\mathcal{P}(R_k)$. We call $\mathcal{P}_R(R_k)$ the group of pure polynomial permutations.

Fact 33

Let $k, i \geq 1$. Then $\mathcal{P}_R(R_i) \cong \mathcal{P}_R(R_k)$.

Definition 34

The set $\mathcal{P}_x = \{F \in \mathcal{P}(R_k) \mid F = [x + \sum_{i=1}^{k} f_i \beta_i]_{R_k}, \text{ where } f_1, \ldots, f_k \in R[x]\}$ is a subgroup of the group $\mathcal{P}(R_k)$.

Theorem 35

Let $\mathcal{P}(R_k)$ be the group of polynomial permutations on R_k. Then

1. $\mathcal{P}(R_k) = \mathcal{P}_x \rtimes \mathcal{P}_R(R_k)$;
2. $|\mathcal{P}(R_k)| = |\mathcal{P}_R(R_k)||\mathcal{F}(R)|^k$.

Theorem 35

Let $\mathcal{P}(R_k)$ be the group of polynomial permutations on R_k. Then

1. $\mathcal{P}(R_k) = \mathcal{P}_x \rtimes \mathcal{P}_R(R_k)$;
2. $|\mathcal{P}(R_k)| = |\mathcal{P}_R(R_k)||\mathcal{F}(R)|^k$.

Corollary 36

$$|\mathcal{P}_R(R_k)| = |\{([f]_R, [\lambda(y,z)]) \mid f \in R[x], [f]_R \in \mathcal{P}(R) \text{ and } [\lambda(y,z)] \text{ L. P. in } z\}|\,.$$

In particular, when R is a chain ring,

$$|\mathcal{P}_R(R_k)| = |\{([f]_R, [\lambda(y,z)]) \mid f \in R[x], [f]_R \in \mathcal{P}(R)\}|\,.$$

Definition 37

Let $St_k(R) = \{F \in \mathcal{P}(R_k) \mid F(a) = a \text{ for every } a \in R\}$.

Proposition 38

Let R be a finite ring. Then

$$St_k(R) = \{F \in \mathcal{P}(R_k) \mid F \text{ is induced by } x + h(x), h \in N_R\}.$$

Definition 37

Let $St_k(R) = \{F \in \mathcal{P}(R_k) \mid F(a) = a \text{ for every } a \in R\}$.

Proposition 38

Let R be a finite ring. Then

$$St_k(R) = \{F \in \mathcal{P}(R_k) \mid F \text{ is induced by } x + h(x), h \in N_R\}.$$

Theorem 39

Let $k, i \geq 1$. Then $St_k(R) \cong St_i(R)$.

Proposition 40

The stabilizer group $St_k(R)$ is a normal subgroup of the group $\mathcal{P}_R(R_k)$. Furthermore, if every element of $\mathcal{P}(R)$ is the restriction to R of an element of $\mathcal{P}_R(R_k)$, then

$$\mathcal{P}_R(R_k) \big/ St_k(R) \cong \mathcal{P}(R).$$

Proposition 40

The stabilizer group $St_k(R)$ is a normal subgroup of the group $\mathcal{P}_R(R_k)$. Furthermore, if every element of $\mathcal{P}(R)$ is the restriction to R of an element of $\mathcal{P}_R(R_k)$, then

$$\mathcal{P}_R(R_k)/St_k(R) \cong \mathcal{P}(R).$$

Theorem 41

Let R be a chain ring. Then:

1. *each element of $\mathcal{P}(R)$ appears as a restriction on R of some $G \in \mathcal{P}_R(R_k)$;*
2. *$St_k(R)$ is a normal subgroup of $\mathcal{P}_R(R_k)$ and*

$$\mathcal{P}_R(R_k)/St_k(R) \cong \mathcal{P}(R).$$

Let $\Psi : \mathcal{P}_R(R_k) \longrightarrow \mathcal{P}(R)$ be the map defined by $\Psi(F) = [f]_R$, where $F = [f]_{R_k}$.

Corollary 42

The number of polynomial permutations on R_k is given by

$$|\mathcal{P}(R_k)| = |\mathcal{F}(R)|^k \cdot |\Psi(\mathcal{P}_R(R_k))| \cdot |St_k(R)|.$$

In particular, when R is a finite chain ring,

$$|\mathcal{P}(R_k)| = |\mathcal{F}(R)|^k \cdot |\mathcal{P}(R)| \cdot |St_k(R)|.$$

Corollary 43

Let $F \in \Psi(\mathcal{P}_R(R_k)) \subseteq \mathcal{P}(R)$ be fixed. Then

$$|St_k(R)| = \left|\{[\lambda_g(y,z)] \mid g \in R[x], [g]_{R_k} \in \mathcal{P}_R(R_k) \text{ and } [g]_R = F\}\right|.$$

When R is chain ring, we fixed $F \in \mathcal{P}(R)$. Then

$$|St_k(R)| = \left|\{[\lambda_g(y,z)] \mid g \in R[x], \text{ and } [g]_R = F\}\right|.$$

Definition 44

For $n \geq 1$, we define

$$N_R(< n) = \{g \in R[x] \mid g \in N_R \text{ with } \deg g < n\}, \text{ and}$$

$$AN_R(< n) = \{g \in R[x] \mid g \in AN_R \text{ with } \deg g < n\}.$$

Proposition 45

1. $|St_k(R)| = |\{[\lambda_g(y, z)] \mid g \in N_R \textit{ and } [g + x]_{R_k} \in \mathcal{P}_R(R_k)\}|$.
2. *If there exists a monic null polynomial on R_k in $R[x]$ of degree n, then:*
   - $|St_k(R)| = |\{[\lambda_g(y, z)] \mid g \in N_R \textit{ and } [g+x]_{R_k} \in \mathcal{P}_R(R_k) \text{ with } \deg g < n\}|$;
   - $|St_k(R)| \leq [N_R : AN_R] = \frac{|N_R(<n)|}{|AN_R(<n)|}$.

Theorem 46

Let R be a finite chain.

1. $|St_k(R)| = |\{[\lambda_g(y,z)] \mid g \in N_R\}|$.
2. *If there exists a monic null polynomial on R_k in $R[x]$ of degree n, then:*
   - $|St_k(R)| = |\{[\lambda_g(y,z)] \mid g \in N_R \text{ and } \deg g < n\}|$;
   - $|St_k(R)| = [N_R \colon AN_R] = \frac{|N_R(<n)|}{|AN_R(<n)|}$.

[Al-Maktry, 2023] Al-Maktry, A. A. A. (2023).
Polynomial functions over dual numbers of several variables.
J. Algebra Appl., 22(11):Paper No. 2350231.

[Brawley, 1976] Brawley, J. V. (1976).
Polynomials over a ring that permute the matrices over that ring.
J. Algebra, 38(1):93–99.

[Frisch, 2017] Frisch, S. (2017).
Polynomial functions on upper triangular matrix algebras.
Monatsh. Math., 184(2):201–215.

[Nechaev, 2008] Nechaev, A. A. (2008).
Finite rings with applications.

In *Handbook of algebra. Vol. 5*, volume 5 of *Handb. Algebr.*, pages 213–320. Elsevier/North-Holland, Amsterdam.

[Stewart, 1972] Stewart, I. (1972).

Finite rings with a specified group of units.

Math. Z., 126:51–58.

[Werner, 2014] Werner, N. J. (2014).

Polynomials that kill each element of a finite ring.

J. Algebra Appl., 13(3):1350111, 12.