The structures of a monoid of vector-triangular polynomials and its two related groups over finite rings

Amr Ali Al-Maktry,

Rings and Factorizations

Graz July 2023

13 july 2023

Outline

1. Definitions and Notation

2. The construction

3. Some structures results

4. The tame monoid

Definitions

Let R be a (finite) commutative ring with unity and let $n > 1$.

Definitions

Let R be a (finite) commutative ring with unity and let $n > 1$.

- A function $F : R^n \longrightarrow R$ is said to be a ***polynomial function*** (in n variables) on R if there exists a polynomial $f \in R[x_1, \ldots, x_n]$ such that $f(\vec{r}) = F(\vec{r})$ for every $\vec{r} = (r_1, \ldots, r_n) \in R^n$. In this case we say that F is the ***induced function*** of f on R and f represents (induces) F.

Definitions

Let R be a (finite) commutative ring with unity and let $n > 1$.

- A function $F : R^n \longrightarrow R$ is said to be a ***polynomial function*** (in n variables) on R if there exists a polynomial $f \in R[x_1, \ldots, x_n]$ such that $f(\vec{r}) = F(\vec{r})$ for every $\vec{r} = (r_1, \ldots, r_n) \in R^n$. In this case we say that F is the ***induced function*** of f on R and f represents (induces) F.
- If $f(\vec{r})$ is a unit for each $\vec{r}$, f is a ***unit-valued*** polynomial and F is a ***unit-valued*** polynomial function.

Definitions

An n-vector function $\vec{F} : R^n \longrightarrow R^n$ is a vector-polynomial permutation of R^n if and only if:

- $\vec{F}$ permutes the elements of R^n;

Definitions

An n-vector function $\vec{F} : R^n \longrightarrow R^n$ is a vector-polynomial permutation of R^n if and only if:

- $\vec{F}$ permutes the elements of R^n;
- there exists a vector-polynomial $\vec{f} = (f_1, \dots, f_n)$, $f_i \in R[x_1, \dots, x_n]$ such that $\vec{F}(\vec{r}) = \vec{f} = (f_1(\vec{r}), \dots, f_n(\vec{r}))$ for every $\vec{r} \in R^n$.

Definitions

An n-vector function $\vec{F} : R^n \longrightarrow R^n$ is a vector-polynomial permutation of R^n if and only if:

- $\vec{F}$ permutes the elements of R^n;
- there exists a vector-polynomial $\vec{f} = (f_1, \ldots, f_n)$, $f_i \in R[x_1, \ldots, x_n]$ such that $\vec{F}(\vec{r}) = \vec{f} = (f_1(\vec{r}), \ldots, f_n(\vec{r}))$ for every $\vec{r} \in R^n$.

Definitions

An n-vector function $\vec{F} : R^n \longrightarrow R^n$ is a vector-polynomial permutation of R^n if and only if:

- $\vec{F}$ permutes the elements of R^n;
- there exists a vector-polynomial $\vec{f} = (f_1, \ldots, f_n)$, $f_i \in R[x_1, \ldots, x_n]$ such that $\vec{F}(\vec{r}) = \vec{f} = (f_1(\vec{r}), \ldots, f_n(\vec{r}))$ for every $\vec{r} \in R^n$.

In this case:

- $\vec{f}$ is called a vector-permutation polynomial;

Definitions

An n-vector function $\vec{F}: R^n \longrightarrow R^n$ is a vector-polynomial permutation of R^n if and only if:

- $\vec{F}$ permutes the elements of R^n;
- there exists a vector-polynomial $\vec{f} = (f_1, \ldots, f_n)$, $f_i \in R[x_1, \ldots, x_n]$ such that $\vec{F}(\vec{r}) = \vec{f} = (f_1(\vec{r}), \ldots, f_n(\vec{r}))$ for every $\vec{r} \in R^n$.

In this case:

- $\vec{f}$ is called a vector-permutation polynomial;
- f_i is a permutation polynomial ($i = 1, \ldots, n$).

Definitions

A vector-polynomial $\vec{f} = (f_1, \ldots, f_n)$ is invertible with respect to "$\circ$", if there is $\vec{g} = (g_1, \ldots, g_n)$ such that
$\vec{f} \circ \vec{g} = (f_1(g_1, \ldots, g_n), \ldots, f_n(g_1, \ldots, g_n)) = (x_1, \ldots, x_n) = \vec{g} \circ \vec{f}$

If $n = 1$ and $f \in R[x]$, then

- f is a permutation polynomial iff it induces a bijection $F\colon R \longrightarrow R$;

Definitions

A vector-polynomial $\vec{f} = (f_1, \ldots, f_n)$ is invertible with respect to "$\circ$", if there is $\vec{g} = (g_1, \ldots, g_n)$ such that
$\vec{f} \circ \vec{g} = (f_1(g_1, \ldots, g_n), \ldots, f_n(g_1, \ldots, g_n)) = (x_1, \ldots, x_n) = \vec{g} \circ \vec{f}$

If $n = 1$ and $f \in R[x]$, then

- f is a permutation polynomial iff it induces a bijection $F\colon\ R \longrightarrow R$;
- $f = a_0 + a_1 x + \ldots a_n x^n$ is invertible iff a_1 is unit and a_i is nilpotent for $i \geq 2$ [Gilmer, 1968] iff f is an R-automorphism of $R[x]$.

Notation

- $A^\times$ is the group of units of A.
- $\mathcal{F}(R^k)$ is the ring of all polynomial functions (in k variables) on R.
- $\mathcal{P}(R)$ is the group of polynomial permutations on R.
- $R_{[k]}$ is $R[x_1, \ldots, x_k]$.
- $\mathcal{MU}(R_{[k]})$ is the monoid of unit-valued polynomials with "$\cdot$" on the ring $R_{[k]}$.
- q is the cardinality of the residue field of a given finite local ring.
- π_n is the natural epimorphism maps a vector-permutation polynomial $\vec{f}$ in to its induced permutation $\vec{F}$.

The Triangular Monoid $\mathcal{MT}_n$

Theorem 1

Let g_0 be a permutation polynomial on R. Let $f_i, g_i \in R_{[i]}$, such that g_i is a unit-valued polynomial $1 \leq i \leq n-1$. Then

$$\vec{f} = \begin{pmatrix} g_0(x_1) \\ f_1(x_1) + x_2 g_1(x_1) \\ \vdots \\ f_{n-1}(x_1, \ldots, x_{n-1}) + x_n g_{n-1}(x_1, \ldots, x_{n-1}) \end{pmatrix} \tag{1}$$

induces a permutation $\vec{F}$ on R^n. Further, the set of all $\vec{f}$ of the form (1) is a monid with respect to "$\circ$" and its group of units, TR_n, consists of all $\vec{f}$ of the form (1) such that g_0 is an R-automorphism and $g_i \in R_{[i]}^{\times}$ for $i = 1, \ldots, n-1$.

Remarks

- In algebraic geometry, the (classical) triangular group KTR_n defined to be the group of vector-polynomials of the form
$$\vec{f} = (a_1x_1 + b_0, f_1(x_1) + a_2x_2, \ldots, f_{n-1}(x_1, \ldots, x_{n-1}) + a_nx_n), \qquad (2)$$
where $a_1, \ldots, a_n \in R^{\times}$ (E.g. [van den Essen et al., 2007]). We have,
$$KTR_n \subseteq TR_n \subseteq \mathcal{MT}_n.$$
- In (2), if $a_1 = \ldots = a_n = 1$, we get the unitriangular group.
- When R is a D-ring (E.g. [Loper, 1988]), $\mathcal{MU}(R_{[i]}) = R^{\times}$. We have
$$KTR_n = TR_n = \mathcal{MT}_n.$$

The induced group of permutations of $\mathcal{MT}_n$

Theorem 2

Let R be finite local ring. Let $\mathcal{MT}_n$ be the triangular monoid, TR_n its group of units and π_n is the natural epimorphism. Then

1. $\pi_n(\mathcal{MT}_n)$ *is a finite group of permutations of* R^n;
2. $\pi_n(TR_n) = \pi_n(\mathcal{MT}_n)$ *if and only if* $R = \mathbb{F}_2$.

Lemma 3

Let R be a finite local ring which is not a field. Let F be the unit-valued function induced by $g(x) = (x^q - x) + 1$. Then there is no invertible unit-valued polynomial represents F.

Sketch proof of Theorem 2

1. Closed subsets of finite groups are subgroups.

Sketch proof of Theorem 2

1. Closed subsets of finite groups are subgroups.
2. Clearly, $\pi_n(TR_n) \subseteq \pi_n(\mathcal{MT}_n)$.

   Consider, the case $R \neq \mathbb{F}_q$. We have

$$\vec{f} = (x_1, ((x_1^q - x_1) + 1)x_2, x_3, \ldots, x_n) \in \mathcal{MT}_n.$$

   Then, by Lemma 3, $\pi_n(\vec{f}) \in \pi_n(\mathcal{MT}_n) \setminus \pi_n(TR_n)$

Semidirect-product of monoids

Let A and B be monids and $End(B)$ be the monoid of endomorphisms of B with respect to composition. If $\phi\colon A \longrightarrow End(B)$, $a \to \phi_a$, is a homomorphism then the semi-direct product $B \rtimes_\phi A$ (or simply $B \rtimes A$) is the monoid with elements $\{(a, b)\colon a \in A, b \in B\}$ and operation $(a, b)(c, d) = (ac, b\phi_a(d))$ (see E.g. [Nico, 1983])

Semidirect-product of monoids

Lemma 4

Let A, B be monoids. Consider the homomorphism $\phi\colon A \longrightarrow End(B)$ $(a \to \phi_a)$, and let ψ_a be the restriction of ϕ_a on $B^{\times}$ then

1. $\phi_a \in Aut(B)$ *for every* $a \in A^{\times}$*;*
2. $\psi_a \in Aut(B^{\times})$ *for every* $a \in A^{\times}$*.*

Proof of (1): Let $a \in A^{\times}$. Then,

$$\phi_a \circ \phi_{a^{-1}} = \phi(aa^{-1}) = \phi(1_A) = \phi_{1_A} = \phi(1_A) = \phi(a^{-1}a) = \phi_{a^{-1}} \circ \phi_a,$$

Hence $\phi_a \in Aut(B)$.

Semidirect-product of monoids

Proposition 5

Let A and B be monoids and $\phi\colon A \longrightarrow End(B)$ ($a \to \phi_a$, $\phi_a\colon B \longrightarrow B$ is an endomorphism) be a homomorphism. Let $\psi\colon A^\times \longrightarrow Aut(B^\times)$ be the homomorphism defined by $a \to \psi_a$, where ψ_a is the restriction of ϕ_a on $A^\times$, then

$$(B \rtimes_\phi A)^\times = B^\times \rtimes_\psi A^\times .$$

The structure of the triangular mononid $\mathcal{MT}_n$

Proposition 6

Fix $2 \leq k \leq n$. Let $\mathcal{ML}_k^n$ denote the set of vector polynomials of the form $(x_1, \ldots, x_{k-1}, f + x_k u, x_{k+1}, \ldots, x_n)$, where $f, u \in R_{[k-1]}$ and u is a unit-valued polynomial. Then

1. *$\mathcal{ML}_k^n$ is a submonid of the monoid $\mathcal{MT}_n$;*
2. *$\mathcal{MT}_n \cong \mathcal{ML}_n^n \rtimes \mathcal{MT}_{n-1}$.*
3. *$\mathcal{ML}_k^n \cong R_{[k-1]} \rtimes \mathcal{MU}(R_{[k-1]})$;*

The structure of the triangular mononid $\mathcal{MT}_n$

Theorem 7

Let $n > 1$. Then

1. $\mathcal{MT}_n \cong \mathcal{ML}_n^n \rtimes \cdots \rtimes \mathcal{ML}_2^2 \rtimes \mathcal{MP}(R)$;
2. $\mathcal{MT}_n \cong (R_{[n-1]}] \rtimes \mathcal{MU}(R_{[k-1]})) \rtimes \cdots \rtimes (R[x_1] \rtimes \mathcal{MU}(R[x_1])) \rtimes \mathcal{MP}(R)$.

$\mathcal{MT}_1 = \mathcal{MP}(R)$ is the monoid of permutation polynomials.

The structure of the triangular group TR_n

Theorem 8

Let $n > 1$. Then

1. $TR_n \cong \mathcal{L}_n^n \rtimes \cdots \rtimes \mathcal{L}_2^2 \rtimes Aut_R(R[x])$;
2. $TR_n \cong (R_{[n-1]}] \rtimes R^{\times}_{[n-1]}) \rtimes \cdots \rtimes (R[x_1] \rtimes R[x_1]^{\times}) \rtimes Aut_R(R[x])$.

Moreover, TR_n is solvable if and only if $Aut_R(R[x])$ is solvable . In particular, if $R = \mathbb{F}_q$, TR_n is solvable.

- In [Bardakov et al., 2012] a decomposition of the unitriangular group into semi-products of Abelian groups is given.

The structure of the group $\pi_n(\mathcal{MT}_n)$

Theorem 9

Let $n > 1$, R finite and π_n be the natural epimorphism. Then

1. $\pi_n(\mathcal{MT}_n) \cong \pi_n(\mathcal{ML}_n^n) \rtimes \cdots \rtimes \pi_2(\mathcal{ML}_2^2) \rtimes \mathcal{P}(R)$;
2. $\pi_n(\mathcal{MT}_n) \cong (\mathcal{F}(R^{n-1}) \rtimes \mathcal{F}(R^{n-1})^\times) \rtimes \cdots \rtimes (\mathcal{F}(R) \rtimes \mathcal{F}(R)^\times) \rtimes \mathcal{P}(R)$.

The structure of the group $\pi_n(\mathcal{MT}_n)$

Lemma 10 ([Görcsös et al., 2018] Theorem 4.1)

Let R a finite local commutative ring with a residue $\mathbb{F}_q$. Let $\mathcal{P}(R)$ be the group of polynomial permutations. Then

1. $\mathcal{P}(R)$ *is solvable if and only if* $q \leq 4$;
2. $\mathcal{P}(R)$ *is nilpotent if and only if* $q = 2$;
3. $\mathcal{P}(R)$ *is abelian if and only if* $R = \mathbb{F}_2$.

The structure of the group $\pi_n(\mathcal{MT}_n)$

Theorem 11

Let R be a finite local ring and $k \geq 1$. Then

$$\frac{|\mathcal{F}(R^k)^\times|}{|\mathcal{F}(R^k)|} = \frac{(q-1)^{kq}}{q^{kq}}.$$

The structure of the group $\pi_n(\mathcal{MT}_n)$

Theorem 11

Let R be a finite local ring and $k \geq 1$. Then

$$\frac{|\mathcal{F}(R^k)^\times|}{|\mathcal{F}(R^k)|} = \frac{(q-1)^{kq}}{q^{kq}}.$$

Proposition 12

Let R be a finite local ring and $k \geq 1$. Then the group $(\mathcal{F}(R^k), \text{``}+\text{''})$ is a $p-$ group.

The structure of the group $\pi_n(\mathcal{MT}_n)$

Theorem 13

Let R a finite local commutative ring and let $n \geq 1$. Then

1. $\pi_n(\mathcal{MT}_n)$ *is solvable if and only if* $q \leq 4$*;*
2. $\pi_n(\mathcal{MT}_n)$ *is nilpotent if and only if* $q = 2$*;*
3. $\pi_n(\mathcal{MT}_n)$ *is abelian if and only if* $n = 1$ *and* $R = \mathbb{F}_2$ *.*

$$\pi_n(\mathcal{MT}_n) \cong (\mathcal{F}(R^{n-1}) \rtimes \mathcal{F}(R^{n-1})^{\times}) \rtimes \cdots \rtimes (\mathcal{F}(R) \rtimes \mathcal{F}(R)^{\times}) \rtimes \mathcal{P}(R).$$

The tame monoid and a question

- The group of all invertible vector-polynomials generated by the group KTR_n, and by the affine group $Aff_n(R)$ of all invertible linear vector-polynomials is called the tame group.

Definition 14

We call the monoid $< \mathcal{MT}_n, Aff_n(R) >$ the tame monoid, and we call every element a tame vector-permutation polynomial.

- **Questions**
  - Is every vector-permutation polynomial tame?
  - Is every vector-polynomial permutation only tamely represented?

Thank you

[Bardakov et al., 2012] Bardakov, V. G., Neshchadim, M. V., and Sosnovsky, Y. V. (2012).

Groups of triangular automorphisms of a free associative algebra and a polynomial algebra.

J. Algebra, 362:201–220.

[Gilmer, 1968] Gilmer, Jr., R. W. (1968).

R-automorphisms of $R[X]$.

Proc. London Math. Soc. (3), 18:328–336.

[Görcsös et al., 2018] Görcsös, D., Horváth, G., and Mészáros, A. (2018).

Permutation polynomials over finite rings.

Finite Fields Appl., 49:198–211.

[Loper, 1988] Loper, A. (1988).
On rings without a certain divisibility property.
J. Number Theory, 28(2):132–144.

[Nico, 1983] Nico, W. R. (1983).
On the regularity of semidirect products.
J. Algebra, 80(1):29–36.

[van den Essen et al., 2007] van den Essen, A., Vui, H. H., Kraft, H., Russell, P., and Wright, D. (2007).
Polynomial automorphisms and related topics.
Publishing House for Science and Technology, Hanoi.

Lecture notes from the International School and Workshop (ICPA2006) held in Hanoi, October 9–20, 2006.