Turkish Journal of Mathematics

http://journals.tubitak.gov.tr/math/

Research Article

Turk J Math
(2018) 42: 2965 – 2978
© TÜBİTAK
doi:10.3906/mat-1805-84

When is a permutation of the set $\mathbb{Z}^n$ (resp. $\mathbb{Z}_p^n$, p prime) an automorphism of the group $\mathbb{Z}^n$ (resp. $\mathbb{Z}_p^n$)?

Ben-Eben DE KLERK, Johan MEYER*
Department of Mathematics & Applied Mathematics, University of the Free State, Bloemfontein, South Africa

Received: 16.05.2018 • **Accepted/Published Online:** 15.09.2018 • **Final Version:** 27.11.2018

Abstract: For a given positive integer n, the structure, i.e. the number of cycles of various lengths, as well as possible chains, of the automorphisms of the groups $(\mathbb{Z}^n, +)$ and $(\mathbb{Z}_p^n, +)$, p prime, is studied. In other words, necessary and sufficient conditions on a bijection $f : A \to A$, where $|A|$ is countably infinite (alternatively, of order p^n), are determined so that A can be endowed with a binary operation $*$ such that $(A, *)$ is a group isomorphic to $(\mathbb{Z}^n, +)$ (alternatively, $(\mathbb{Z}_p^n, +)$) and such that $f \in \mathrm{Aut}(A)$.

Key words: Automorphism, abelian group

1. Introduction

In a recent study [2], the structural properties of the automorphisms of certain abelian groups, namely cyclic groups, groups of order p^2 (p prime), and groups of the form $\mathbb{Z}^n$, were studied. The case $\mathbb{Z}^n$ was treated with a 'variable' n, i.e. necessary and sufficient properties of a bijection $f : A \to A$ (where A is a countably infinite set) were found such that there exists some n so that A can be endowed with a binary operation $*$ such that $(A, *)$ is an abelian group isomorphic to $(\mathbb{Z}^n, +)$ and such that $f \in \mathrm{Aut}(A)$. In Section 2 of this paper we investigate the same problem for 'fixed' n. For example, it will be characterized when f has the desired properties such that $(A, *)$ is isomorphic to $(\mathbb{Z}^4, +)$ and $f \in \mathrm{Aut}(A)$.

In the last section, we also study the finite case: if A is a set of cardinality p^n, p prime, and $f : A \to A$ is a bijection, exactly when can we turn A into an abelian group isomorphic to $(\mathbb{Z}_p^n, +)$ and such that $f \in \mathrm{Aut}(A)$?

For a given set A, let us agree to say that a bijection $f : A \to A$ has the *auto-property* if it is possible to find a binary operation $*$ on A such that $(A, *)$ is an abelian group and $f \in \mathrm{Aut}(A)$.

If A is finite, such an f gives rise to *cycles*, i.e. (disjoint) finite sequences $a_1, a_2, \ldots, a_m$ from A such that $f(a_i) = a_{i+1}$ for $1 \le i \le m-1$ and $f(a_m) = a_1$. Every element of A belongs to some cycle. The number of elements in a cycle is its *length*, so a fixed point of f is a cycle of length 1. The *cycle structure* of f is a description of how many cycles of each length f has. If f has c_i cycles of length t_i ($1 \le i \le k$), then we say f has the *cycle structure* $\begin{bmatrix} c_1 & c_2 & \cdots & c_k \\ t_1 & t_2 & \cdots & t_k \end{bmatrix}$. It is possible that some c_i could be 0, and these columns can

*Correspondence: meyerjh@ufs.ac.za
2000 *AMS Mathematics Subject Classification:* 20K30

just as well be omitted from the array. It follows that $\sum_{i=1}^{k} c_i t_i = |A|$, and that the identity map has cycle structure $\begin{bmatrix} |A| \\ 1 \end{bmatrix}$.

On the other hand, if A is infinite, then, apart from possible cycles, there is also the possibility of f having *chains*, i.e. infinite sequences $\ldots, a_i, a_{i+1}, a_{i+2}, \ldots$ from A such that $f(a_i) = a_{i+1}$ for all i. The various lengths of the cycles of f, as well as the number of chains (in our case, either zero or infinite, as we will see later), will be referred to simply as the *structure* of f.

2. The automorphisms of $\mathbb{Z}^n$ for a given n

In this section, we fix a natural number n and focus on the additive group $(\mathbb{Z}^n, +)$. Also, throughout the section, A will be a countably infinite set and $f : A \to A$ a bijection. It is evident that if we want to investigate the conditions f has to satisfy to have the auto-property, then it suffices to find the structures of all possible automorphisms on the group $(\mathbb{Z}^n, +)$. It is known that automorphisms of this group are induced by the units of the ring $\mathbb{M}_n(\mathbb{Z})$, i.e. the group $GL(n, \mathbb{Z})$. The group $GL(n, \mathbb{Z})$ will sometimes be seen in the context of being a subgroup of $GL(n, \mathbb{Q})$. Many of our results depend on properties of such matrices.

Recall (from the Cayley–Hamilton theorem) that if F is any field and $M \in \mathbb{M}_n(F)$, then M is a root of its own characteristic polynomial. However, there often exist polynomials over F of smaller degree than that of the characteristic polynomial, also having M as a root. The monic one of smallest degree of these is called the *minimal polynomial* of M and denoted by $\min_F(M)$, or simply $\min(M)$ if there is no confusion.

Lemma 2.1 *For any $M \in GL(n, \mathbb{Z})$, the structure of the automorphism induced by M on $\mathbb{Z}^n$ is the same as that of the automorphism induced by M on $\mathbb{Q}^n$.*

Proof Clearly every cycle (or chain) induced by M on $\mathbb{Z}^n$ occurs identically as a cycle (or chain) in $\mathbb{Q}^n$. Now consider any $v = (v_i) \in \mathbb{Q}^n$. Denote by ℓ the least common multiple of the denominators of the v_i. Then ℓv lies in $\mathbb{Z}^n$, and lies in a cycle if and only v does. □

From Lemma 2.1, we can prove our results over $\mathbb{Q}$, from which they will follow over $\mathbb{Z}$. For the remainder of the section, F will always denote an arbitrary field, unless otherwise specified.

Definition 2.2 *Let $M \in GL(n, F)$ and $v \in F^n$. We define the point annihilator of M at v as $\mathcal{P}_{M,v} = \{f \in F[X] : f(M)v = 0\}$. Similarly, for any $f \in F[X]$, we define the polynomial annihilator of M at f as $\mathcal{S}_{M,f} = \{v \in F^n : f(M)v = 0\}$.*

It is straightforward to check that $\mathcal{P}_{M,v}$ is an ideal of $F[X]$; hence, there exists an $f_{M,v} \in F[X]$, such that $\mathcal{P}_{M,v} = \langle f_{M,v} \rangle$. It is also routine to check that $\mathcal{S}_{M,f}$ is an F-subspace of F^n.

From now on, we will usually omit M from the subscripts in $\mathcal{P}_{M,v}$, $\mathcal{S}_{M,f}$, and $f_{M,v}$, as the matrix M should be clear from the context.

Theorem 2.3 *For $M \in GL(n, F)$ and $f \in F[X]$, if $f \mid \min(M)$ and f is not constant, then $\mathcal{S}_f$ is nontrivial.*

Proof Suppose $\mathcal{S}_f$ is trivial. It follows that the linear transformation $f(M)$ satisfies $f(M)v \neq 0$ for all $v \in F^n \setminus \{0\}$, and is thus injective. By the rank-nullity theorem it follows that $f(M)$ is surjective, and thus invertible. Consider the polynomial $h = \frac{\min(M)}{f}$. It follows that $h(M)v = f(M)^{-1}\min(M)v = 0$ for all $v \in F^n$, contradicting the minimality of $\min(M)$. □

Lemma 2.4 *For $M \in GL(n, F)$ and $f \in F[X]$, if $f \mid \min(M)$, and $h \mid f$, with h neither constant nor equal to a constant multiple of f, then $\mathcal{S}_h$ is a proper subspace of $\mathcal{S}_f$.*

Proof That $\mathcal{S}_h$ is a subspace of S_f is obvious. We just need to show that it is indeed a proper subset.

Suppose that $\mathcal{S}_h = \mathcal{S}_f$, i.e. for any $v \in F^n$, $f(M)v = 0$ implies $h(M)v = 0$. As $h \mid f$, there exists a nonconstant polynomial r such that $f = hr$. For any $v \in F^n$, $\min(M)(M)v = f(M)\frac{\min(M)}{f}(M)v = f(M)\left(\frac{\min(M)}{f}(M)v\right) = 0$, so $h(M)\left(\frac{\min(M)}{f}(M)v\right) = 0$. As $h\frac{\min(M)}{f} = \frac{\min(M)}{r}$, it follows that $\frac{\min(M)}{r}(M)v = 0$ for all $v \in F^n$, contradicting the minimality of $\min(M)$. □

Definition 2.5 *Let $M \in GL(n, F)$. We shall refer to $m \geq 1$ as a relatively pure cycle length of M if the structure of the automorphism induced by M contains nonzero cycles of length m, but no cycles of lengths a and b, both less than m, with the property that $\operatorname{lcm}(a, b) = m$.*

For the remainder of the section, we let $F = \mathbb{Q}$. Keep in mind that all the cyclotomic polynomials Φ_n, $n \geq 1$, are irreducible over $\mathbb{Q}$. We will also make use of a special kind of polynomial introduced in the next lemma.

Lemma 2.6 *For any $m > 1$, let $m = \prod_{i=1}^{k} p_i^{\alpha_i}$ be the prime factorization of m, where we assume that $p_1 > p_2 > \cdots > p_k$. Define, for each $i \in \{1, 2, \ldots, k\}$, the polynomial Q_i by*

$$Q_i(X) = \sum_{j=0}^{p_i - 1} X^{\frac{m \cdot j}{p_i}}.$$

Then the mth cyclotomic polynomial Φ_m divides Q_i for all $i \in \{1, 2, \ldots, k\}$. Moreover, Φ_m is the only monic nonconstant polynomial in $\mathbb{Q}[X]$ that divides all the Q_i.

Proof First we notice that $X^m - 1 = (X^{\frac{m}{p_i}} - 1)Q_i(X)$ for any $i \in \{1, 2, \ldots, k\}$. Let ζ be a primitive mth root of unity. From $(\zeta^{\frac{m}{p_i}} - 1)Q_i(\zeta) = 0$ and $\zeta^{\frac{m}{p_i}} - 1 \neq 0$ it follows that $Q_i(\zeta) = 0$. An immediate consequence is that $X - \zeta$ is a factor of Q_i for all primitive roots ζ of unity, so the mth cyclotomic polynomial Φ_n divides all of the Q_i.

Now suppose that there is another nonconstant polynomial R, which is a factor of all the Q_is, but with a root η that is not a primitive mth root of unity. As all the roots of R must be mth roots of unity, it follows that $\eta = \zeta^l$ for some $l \in \{1, 2, \ldots, m\}$ and such that $\gcd(l, m) \neq 1$. However, then there exists an i such that $\eta^{\frac{m}{p_i}} - 1 = 0$, and as $Q_i(\eta) = 0$, it follows that η is a root of $X^m - 1$ of multiplicity at least two. This is a contradiction, as all roots of $X^m - 1$ have multiplicity 1. □

Theorem 2.7 *Let $M \in GL(n, \mathbb{Q})$ and $m \geq 1$. If the structure induced by M has relatively pure m-cycles, then $\Phi_m \mid \min(M)$.*

Proof First, assume that $m > 1$. All cycles (and their lengths) will be those induced by M.

Let d be a divisor of m. Let T_d be the set of all members of $\mathbb{Q}^n$ contained in cycles of length d. Define

$$K_m = \bigcup_{d|m;d\neq m} T_d.$$

We note that K_m is a $\mathbb{Q}$-subspace of $\mathbb{Q}^n$: for $x, y \in K_m$, the length of the cycle that contains $x+y$ divides the least common multiple of the lengths of the cycles that contain x and y, respectively, but this least common multiple is a proper divisor of m, as m is relatively pure. Hence, $x + y \in K_m$. Moreover, the length of the cycle of qx is the same as the length of the cycle of x, for all nonzero $q \in \mathbb{Q}$, showing (together with the fact that $0 \in K_m$) that $\mathbb{Q}K_m \subseteq K_m$.

Note that we also have $M^k K_m \subseteq K_m$ for any integer k. This is because the cycle lengths of $M^k x$ and x are the same for any $x \in \mathbb{Q}^n$.

Now let $x \in T_m$. Define $\mathcal{Q}_x$ as the set of all polynomials $f \in \mathbb{Q}[X]$ such that $f(M)(x) \in K_m$. Then $\mathcal{Q}_x$ is an ideal of $\mathbb{Q}[X]$: let $f, g \in \mathcal{Q}_x$ and $h \in \mathbb{Q}[X]$. Then

$$(f + g)(M)(x) = f(M)x + g(M)x \in K_m,$$

since K_m is an additive group. Also, $hg(M)(x) = h(M)g(M)(x)$, and as $g(M)(x) \in K_m$, it follows (from the fact that $qM^k K_m \subseteq K_m$ for all $q \in \mathbb{Q}$ and integers k (from above)), that

$$hg(M)(x) \in K_m.$$

In particular, we have that $Q_i(M)(x) \in K_m$, for all Q_i as defined in Lemma 2.6. This is because $M^{m/p_i}(Q_i(M)(x)) = Q_i(M)(x)$ where p_i is the ith prime factor of m, and $\frac{m}{p_i}$ is a proper divisor of m. From Lemma 2.6 it follows that Φ_m is the greatest common divisor of these Q_i, and hence Φ_m is a linear combination of the Q_is, from which it follows that

$$\Phi_m(M)(x) \in K_m.$$

Consequently, $\Phi_m \in \mathcal{Q}_x$. Since Φ_m is the only monic nonconstant polynomial that divides all of the Q_i (by Lemma 2.6), we must have that $\mathcal{Q}_x = \langle \Phi_m \rangle$. (Note that $\mathcal{Q}_x = \mathbb{Q}[X]$ is not possible, since, for example, the identity polynomial $1 \in \mathbb{Q}[X]$ is not in $\mathcal{Q}_x$.) Finally, since $\min(M) \in \mathcal{Q}_x$, we conclude that $\Phi_m \mid \min(M)$.

Now for the case $m = 1$: if the structure induced by M has nonzero 1-cycles, then 1 is an eigenvalue of M, so that $X - 1 = \Phi_1$ is a divisor of $\min(M)$. □

We now focus on the converse of the above theorem.

Theorem 2.8 *Let $M \in GL(n, \mathbb{Q})$ and $m \geq 1$. If $\Phi_m \mid \min(M)$ then the structure induced by M contains nonzero cycles of length m.*

Proof In case $m > 1$, we know from Theorem 2.3 that S_{Φ_m} is nontrivial, so there exists $v \in \mathbb{Q}^n \setminus \{0\}$ such that $\Phi_m(M)v = 0$. As $\Phi_m \mid X^m - 1$, it follows that $(M^m - I)v = 0$, so v lies in a cycle of length dividing m, but as Φ_m does not divide $X^k - 1$ for any $k < m$, it follows that v lies in a cycle of length m. (Note that Φ_m, being irreducible, is a generator for the ideal $\mathcal{P}_v$. Hence, if $X^d - 1$, with $d \mid m$, is an element of $\mathcal{P}_v$, then $\Phi_m \mid X^d - 1$.)

Finally, if $m = 1$, then $X - 1$ divides $\min(M)$ so that 1 is an eigenvalue of M. However, then the structure induced by M contains nonzero cycles of length 1. □

We now turn our attention to chains.

Theorem 2.9 *Let $M \in GL(n, \mathbb{Q})$. If f is an irreducible, noncyclotomic polynomial over $\mathbb{Q}$ and $f \mid \min(M)$, then the structure induced by M has chains.*

Proof Let $v \in \mathcal{S}_f \setminus \{0\}$. Then $\mathcal{P}_v = \langle f \rangle$. If M has no chains, then there exists m such that $M^m v = v$, so $X^m - 1 \in \mathcal{P}_v$, from which it follows that $f \mid X^m - 1$. This is a contradiction, because $X^m - 1 = \prod_{d|m} \Phi_d(X)$. □

Theorem 2.10 *Let $M \in GL(n, \mathbb{Q})$. If $\min(M)$ has no irreducible, noncyclotomic factors, but a cyclotomic factor of multiplicity greater than 1, then the structure induced by M has chains.*

Proof For the sake of contradiction, suppose that M induces cycles only. Then, for any $v \in \mathbb{Q}^n$, there exists an m such that $X^m - 1 \in \mathcal{P}_v$. Thus, there exist $m_1, m_2, \ldots, m_k$ such that $\mathcal{P}_v = \left\langle \prod_{i=1}^k \Phi_{m_i} \right\rangle$.

Suppose $\min(M) = \prod_{i=1}^s \Phi_{w_i}^{\alpha_i}$ for certain natural numbers $w_1, w_2, \ldots, w_s$ and $\alpha_1, \alpha_2, \ldots, \alpha_s$. We now just need to show that $\alpha_i = 1,\ 1 \le i \le s$, but as $\prod_{i=1}^k \Phi_{m_i} \mid \min(M)$, it follows that

$$\prod_{i=1}^k \Phi_{m_i} \,\Bigg|\, \prod_{i=1}^s \Phi_{w_i}.$$

Therefore,

$$\prod_{i=1}^s \Phi_{w_i} \in \mathcal{P}_v, \text{ for all } v \in \mathbb{Q}^n,$$

and thus we have that $\left(\prod_{i=1}^s \Phi_{w_i}\right)(M) = 0$. This proves the result. □

So far, we have demonstrated two sufficient conditions for chains to occur in the structure induced by $M \in GL(n, \mathbb{Q})$. We now proceed to show that it is also necessary for one of these to hold if the structure induced by M has chains.

Theorem 2.11 *Let $M \in GL(n, \mathbb{Q})$. If the structure induced by M has chains then $\min(M)$ either has a noncyclotomic, irreducible factor, or a cyclotomic factor of multiplicity greater than 1.*

Proof Suppose the result does not hold. Then $\min(M) = \prod_{i=1}^k \Phi_{m_i}$ with $m_i \ne m_j$ if $i \ne j$. Then $\min(M) \mid X^{\operatorname{lcm}(m_1, m_2, \ldots, m_k)} - 1$. As $\min(M) \in \mathcal{P}_v$ for all $v \in \mathbb{Q}^n$, it follows that $X^{\operatorname{lcm}(m_1, m_2, \ldots, m_k)} - 1 \in \mathcal{P}_v$, implying that all v lie in cycles of lengths dividing $\operatorname{lcm}(m_1, m_2, \ldots, m_k)$. □

Before we proceed, we need to introduce one more concept. For a bijection $f : S \to S$, where S is an arbitrary nonempty set, let $\mathcal{G} = (V, E)$ be a directed graph with $|V| = |S|$ and $\rho : S \to V$ a bijection. Then $\mathcal{G}$ is called a *structural graph* of f if $(u, v) \in E \Leftrightarrow (\exists a \in S : u = \rho(a) \wedge v = \rho(f(a)))$. ρ is called a *graph projection* of f.

From [1] we have the following general result:

Theorem 2.12 *([1, Theorem 9.13]) If S is a countably infinite set and $f : S \to S$ is bijective, then there exists some $n \in \mathbb{N}$ such that f has the auto-property with underlying group structure $(\mathbb{Z}^n, +)$ if and only if the structural graph of f satisfies all of the following:*

1. *there exists a cycle of length 1, called the zero cycle;*
2. *there are only finitely many distinct cycle lengths;*
3. *if there is more than one cycle of length 1, then there are infinitely many of them;*
4. *if there are any cycles of length $d > 1$, then there are infinitely many cycles of length d;*
5. *if there are chains, then there are infinitely many chains;*
6. *if there are cycles of lengths u and v, then there are cycles of length $\operatorname{lcm}(u, v)$.*

We agree here that if there is exactly one cycle of length one, then this is the (unique) zero cycle, while if there are infinitely many cycles of length one, then any one of them can by chosen and fixed to represent the (unique) zero cycle.

We conclude this section where we focus on a given $n \in \mathbb{N}$:

Theorem 2.13 *Let $n \in \mathbb{N}$ and let $f : S \to S$ be a bijection where S is a countably infinite set. Then f has the auto-property with underlying group $(\mathbb{Z}^n, +)$ if and only if one of the following cases hold (where φ denotes the Euler totient function):*

1. *f satisfies the conditions stated in Theorem 2.12, the structural graph of f contains no chains, and n can be expressed as*

$$n = \sum_{i=1}^{k} \alpha_i \varphi(c_i),$$

where $c_1, c_2, \ldots, c_k$ denotes the complete list of relatively pure cycle lengths of f, and where α_i is a positive integer for every $i \in \{1, 2 \ldots, k\}$.

2. *f satisfies the conditions stated in Theorem 2.12, the structural graph of f contains chains, and*

$$n - \sum_{i=1}^{k} \varphi(c_i) \geq 2,$$

where $c_1, c_2, \ldots, c_k$ denotes the complete list of relatively pure cycle lengths of f.

Proof First, suppose the structural graph of f contains no chains. Then the automorphism

$$\begin{bmatrix} D_{\Phi_{c_1},\alpha_1} & 0 & \cdots & 0 \\ 0 & D_{\Phi_{c_2},\alpha_2} & \cdots & 0 \\ \vdots & \vdots & \ddots & 0 \\ 0 & 0 & 0 & D_{\Phi_{c_k},\alpha_k} \end{bmatrix}$$

where, for each $j \in \{1, \ldots, k\}$, $D_{\Phi_{c_j},\alpha_j}$ is the matrix consisting of α_j copies of the companion matrix $C_{\Phi_{c_j}}$ of the cyclotomic polynomial Φ_{c_j} along its diagonal, will induce the same structural graph as f.

If n does not have the form stated in (1), i.e. n cannot be written as $\sum_{i=1}^{k} \alpha_i \varphi(c_i)$, then the characteristic polynomial of any matrix $M \in GL(n, \mathbb{Q})$ (which is of degree n) cannot have irreducible factors only of the form Φ_{c_i}, and thus has an irreducible factor that is either a cyclotomic polynomial Φ_d with $d \notin \{c_1, c_2, \ldots, c_k\}$ or a noncyclotomic (irreducible) polynomial. As the characteristic polynomial and the minimal polynomial of a matrix share the same roots (i.e. the eigenvalues), this irreducible factor would be a factor of the minimal polynomial as well, and will, by Theorems 2.8 and 2.9, induce cycles of length d, or chains. Either way, we cannot obtain the desired structural graph. If the minimal polynomial of M has any cyclotomic polynomial occurring more than once as a factor, the induced structural graph will contain chains by Theorem 2.10.

In the event that the structural graph of f has chains, we consider any matrix M of the form

$$M = \begin{bmatrix} C_{\Phi_{c_1}} & 0 & \cdots & 0 & 0 \\ 0 & C_{\Phi_{c_2}} & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & 0 & 0 \\ 0 & 0 & 0 & C_{\Phi_{c_k}} & 0 \\ 0 & 0 & 0 & 0 & X_{s,t} \end{bmatrix}$$

where $X_{s,t}$ is a square matrix consisting of s copies of the companion matrix of $x^2 + 2$ and t copies of the companion matrix of $x^3 + 2$ along its diagonal. Here, s and t are nonnegative integers (with at least one of them strictly positive) such that $2s + 3t = n - \sum_{i=1}^{k} \varphi(c_i)$. The structural graph induced by M is clearly the same as that of f. Note that $X_{s,t}$ can be made to be a square matrix of any size greater than 1×1, and will produce only chains in the induced structural graph (both irreducible factors in the minimal polynomial of $X_{s,t}$ being noncyclotomic). It would also not be possible to get chains using a 1×1 matrix as the only possible 1×1 matrix that we could use and keep that M an automorphism is the identity, which will produce cycles of length one rather than chains. Moreover, any representation of f will require all of the cyclotomic companion matrices along the diagonal listed in order to produce the desired structural graphs. □

Example 2.14 *Let S be a countably infinite set and $f : S \to S$ be a bijection.*

1. *If the structural graph of f has exactly one cycle of length 1, has no chains, and has infinitely many cycles of length 6 (and nothing else), then, for odd n, S cannot be endowed with a binary operation $*$ so as to create a group $(S, *)$ isomorphic to $(\mathbb{Z}^n, +)$ and such that $f \in \mathrm{Aut}(S)$. This is because $\varphi(6) = 2$, and no multiple of it equals n. However, for any even n, a binary operation $*$ on S can be found so that $(S, *)$ is a group isomorphic to $(\mathbb{Z}^n, +)$ and such that $f \in \mathrm{Aut}(S)$. Simply take $\alpha_1 = \frac{n}{2}$ in Theorem 2.13 (1).*

2. *If the structural graph of f has infinitely many cycles of length 1 and infinitely many chains (and nothing else), then S cannot be endowed with a binary operation $*$ so as to create a group $(S, *)$ isomorphic to $(\mathbb{Z}^2, +)$ and such that $f \in \mathrm{Aut}(S)$. This is because, in this case, $n - \sum_{i=1}^{1} \varphi(1) = 2 - 1 < 2$. However, for each $n \geq 3$, a binary operation $*$ on S can be found so that $(S, *)$ is a group isomorphic to $(\mathbb{Z}^n, +)$ and with $f \in \mathrm{Aut}(S)$.*

3. The automorphisms of $\mathbb{Z}_p^n$

We now turn our attention to the automorphisms of groups of the form $(\mathbb{Z}_p^n, +)$, for prime p. Before we study the rational canonical form of arbitrary invertible $n \times n$ matrices over $\mathbb{Z}_p$ to solve the general case, we begin by considering those matrices in $GL(n, \mathbb{Z}_p)$ for which the minimal and characteristic polynomials coincide. Note that these are exactly the matrices M for which the rational canonical form is similar to a companion matrix of a polynomial of degree n.

Consider such a matrix C_f, where $f = \prod_{i=1}^k f_i^{\alpha_i}$, with each f_i irreducible over $\mathbb{Z}_p$. Then consider the matrix

$$D_f = \begin{bmatrix} C_{f_1^{\alpha_1}} & 0 & 0 & \cdots & 0 \\ 0 & C_{f_2^{\alpha_2}} & 0 & \cdots & 0 \\ 0 & 0 & C_{f_3^{\alpha_3}} & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & C_{f_k^{\alpha_k}} \end{bmatrix}$$

with companion matrices $C_{f_i^{\alpha_i}}$ all along the diagonal. Since the $f_i^{\alpha_i}$s are relatively prime, $\min(D_f) = f$ and it follows that C_f is the rational canonical form of D_f, so C_f and D_f are similar matrices, implying that the structures induced by them are identical. The usefulness of this representation is that the effect on the cycle structure attributed by each companion matrix along the diagonal can easily be isolated.

We now appeal to a few results on polynomials [3, pp. 84–87], where, in all these results, it is assumed that F is a finite field:

Lemma 3.1 *([3, Lemma 3.1]) Let $f \in F[X]$ of degree m with $|F| = q$ and $f(0) \neq 0$. There exists a positive integer $e \leq q^m - 1$ such that $f \mid x^e - 1$.*

Definition 3.2 *([3, Definition 3.2]) Given a polynomial $f \in F[X]$ with $f(0) \neq 0$, the least e such that $f \mid x^e - 1$ is called the order of f, denoted by $\operatorname{ord}(f)$.*

Theorem 3.3 *([3, Theorem 3.3]) Denote the finite field with q elements by F_q. Let $f \in F_q[X]$ be irreducible of degree m and $f(0) \neq 0$. Then $\operatorname{ord}(f)$ is equal to the order of any root of f in the multiplicative group $F_{q^m}^*$.*

Corollary 3.4 *([3, Corollary 3.4]) If $f \in F[X]$ is an irreducible polynomial of degree m, then $\operatorname{ord}(f)$ divides $q^m - 1$.*

Theorem 3.5 *([3, Theorem 3.5]) The number of monic irreducible polynomials in $F[x]$ of degree m and order e is equal to:*

1. *$\frac{\phi(e)}{m}$ if $e \geq 2$ and m is the multiplicative order of q modulo e.*
2. *2 if $m = e = 1$.*
3. *0 otherwise.*

In particular, the degree of an irreducible polynomial in $F[x]$ of order e must be equal to the multiplicative order of q modulo e.

Lemma 3.6 *([3, Lemma 3.6]) Let c be any positive integer, and let $f \in F[x]$ with $f(0) \neq 0$. Then f divides $x^c - 1$ if and only if* $\operatorname{ord}(f) \mid c$.

Theorem 3.7 *([3, Theorem 3.8]) Let $g \in F[x]$ be irreducible with $g(0) \neq 0$ and $\operatorname{ord}(g) = e$. Let $f = g^b$ with b a positive integer. Let t be the smallest integer with $p^t \geq b$, with p the characteristic of F. Then $\operatorname{ord}(f) = ep^t$.*

Theorem 3.8 *([3, Theorem 3.9]) Let $g_1, g_2, \ldots, g_k$ be pairwise relatively prime nonzero polynomials over F. Let $f = g_1 g_2 \cdots g_k$. Then $\operatorname{ord}(f) = \operatorname{lcm}(\operatorname{ord}(g_1), \operatorname{ord}(g_2), \ldots, \operatorname{ord}(g_k))$.*

We now summarize these results in one theorem:

Theorem 3.9 *([3, Theorem 3.11]) Let F be a finite field of characteristic p, and let $f \in F[X]$ be a polynomial of positive degree and $f(0) \neq 0$. Let $f = a f_1^{b_1} f_2^{b_2} \cdots f_k^{b_k}$, where $a \in F, b_i \in \mathbb{N}$ and f_i are distinct monic irreducible polynomials over F, be the canonical factorization of f in $F[x]$. Then $\operatorname{ord}(f) = ep^t$ where $e = \operatorname{lcm}(\operatorname{ord}(f_1), \operatorname{ord}(f_2), \ldots, \operatorname{ord}(f_k))$ and t is the smallest integer with $p^t \geq \max(b_1, b_2, \ldots, b_k)$.*

Corollary 3.10 *If f is an irreducible polynomial in $F[X]$ with $\deg(f) = m$, then $\operatorname{ord}(f) \mid p^s - 1$ if and only if $m \mid s$.*

Proof Immediate consequence of Lemma 3.6. □

We now have all of the results on polynomials that we will need for the rest of this section.

For any finite field F, we consider an automorphism of F^n for which the characteristic polynomial, as well as the minimal polynomial, is $f = f_1^{\alpha}$. As $\deg(f) = n$, it follows that $\deg(f_1) = \frac{n}{\alpha}$. Denote the order of f_1 by e.

Consider furthermore the subspaces $\mathcal{S}_{f_1^i}, i \in \{1, 2, \ldots, \alpha\}$ of F^n. We know that $\mathcal{S}_{f_1^{i+1}}$ properly contains $\mathcal{S}_{f_1^i}$, $1 \leq i \leq \alpha - 1$, and that $\mathcal{S}_{f_1}$ is nontrivial.

Lemma 3.11 *Each nonzero member of $\mathcal{S}_{f_1}$ lies in a cycle of length e.*

Proof Let $y \in \mathcal{S}_{f_1} \setminus \{0\}$. Then clearly $X^{\operatorname{ord}(f_1)} - 1 \in \mathcal{P}_y$, from which it follows that the cycle length of y divides $\operatorname{ord}(f_1)$. If s is the least positive integer such that $(X^s - 1)(M)y = 0$, then $X^s - 1 \in \mathcal{P}_y$. As $f_1 \in \mathcal{P}_y$, and f_1 is irreducible, it follows that $f_1 | X^s - 1$, so $e \mid s$, and we have $s = e$. Consequently, each $y \in \mathcal{S}_{f_1} \setminus \{0\}$ lies in a cycle of length e. □

Lemma 3.12 *If $y \in \mathcal{S}_{f_1^{i+1}} \setminus \mathcal{S}_{f_1^i}$ for some $i \in \{1, 2, \ldots, \alpha - 1\}$, then y lies in a cycle of length* $\operatorname{ord}(f_1^{i+1})$.

Proof For any such y, $f_1^{i+1} \in \mathcal{P}_y$, while $f_1^i \notin \mathcal{P}_y$. Consequently, $\mathcal{P}_y$ is generated by f_1^{i+1}. Suppose $X^s - 1 \in \mathcal{P}_y$ for some $s \in \mathbb{N}$. Then, as f_1^{i+1} is a divisor of $X^s - 1$, it follows that $\operatorname{ord}(f_1^{i+1}) \mid s$. However, $X^{\operatorname{ord}(f_1^{i+1})} - 1 \in \mathcal{P}_y$, and it follows that y lies in a cycle of length $\operatorname{ord}(f_1^{i+1})$. □

Lemma 3.13 *For each $i \in \{1, 2, \ldots, \alpha\}$, $|\mathcal{S}_{f_1^i}| = (p^m)^i$, with $m = \deg(f_1)$.*

Proof For each $i \in \{1, 2, \dots, \alpha\}$, let $|\mathcal{S}_{f_1^i}| = p^{t_i}$. From Corollary 3.10, $t_1 = m\delta_1$ for some integer δ_1. By Lemma 3.12, $p^{t_{i+1}} = p^{t_i} + c_{i+1} \cdot \mathrm{ord}(f_1^{i+1})$, with c_{i+1} the number of cycles in $\mathcal{S}_{f_1^{i+1}} \setminus \mathcal{S}_{f_1^i}$. As $e = \mathrm{ord}(f_1)$ divides $\mathrm{ord}(f_1^{i+1})$, we have $p^{t_{i+1}} \equiv p^{t_i} \pmod{e}$. Consequently, $p^{t_{i+1}-t_i} \equiv 1 \pmod{e}$, so that m divides $t_{i+1} - t_i$. We can thus conclude that $t_{i+1} = t_i + m\delta_{i+1}$, for some integer δ_{i+1}. However, $m\alpha = n = m(\delta_1 + \delta_2 + \cdots + \delta_\alpha)$ and as $\mathcal{S}_{f_1^{i+1}}$ strictly contains $\mathcal{S}_{f_1^i}$, each $\delta_i \geq 1$, so $m(\delta_1 + \delta_2 + \cdots + \delta_\alpha) \geq m\alpha$. Since equality holds, $\delta_i = 1$ for each i, from which the result follows. □

We summarize our work in the following theorem:

Theorem 3.14 *Let M be the matrix representation of an automorphism of $\mathbb{Z}_p^n$, with the characteristic polynomial of M equal to $\min(M) = f^\alpha$, for an irreducible polynomial $f \in \mathbb{Z}_p[X]$ of degree m. Then the cycle structure of the automorphism induced by M is*

$$\begin{bmatrix} 1 & \frac{p^m-1}{\mathrm{ord}(f)} & \frac{p^m(p^m-1)}{\mathrm{ord}(f^2)} & \frac{p^{2m}(p^m-1)}{\mathrm{ord}(f^3)} & \cdots & \frac{p^{m(\alpha-1)}(p^m-1)}{\mathrm{ord}(f^\alpha)} \\ 1 & \mathrm{ord}(f) & \mathrm{ord}(f^2) & \mathrm{ord}(f^3) & \cdots & \mathrm{ord}(f^\alpha) \end{bmatrix}$$

with $\alpha = \frac{n}{m}$.

As any square matrix over a field has a rational canonical form, which has companion matrices along the diagonal, and all companion matrices are similar to a matrix with companion matrices of factors of the corresponding polynomial, it follows that every matrix is similar to a matrix of the form

$$\begin{bmatrix} C_{f_1^{\alpha_1}} & 0 & 0 & \cdots & 0 \\ 0 & C_{f_2^{\alpha_2}} & 0 & \cdots & 0 \\ 0 & 0 & C_{f_3^{\alpha_3}} & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & C_{f_k^{\alpha_k}} \end{bmatrix}$$

with each $C_{f_i^{\alpha_i}}$ a companion matrix (they are not necessarily distinct). The important observation is that this form allows for the $C_{f_i^{\alpha_i}}$s along the diagonal to act on disjoint (nonzero) subspaces of $\mathbb{Z}_p^n$ independently.

To shed some light on this, it is perhaps appropriate to look at an example.

Example 3.15 *Consider the automorphism of $\mathbb{Z}_3^3$ induced by*

$$M = \begin{bmatrix} C_{(x+1)^2} & 0 \\ 0 & C_{x-1} \end{bmatrix} = \begin{bmatrix} 0 & 1 & 0 \\ 2 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}.$$

Let $\left\{ e_1 = \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix}, e_2 = \begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix}, e_3 = \begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix} \right\}$ be the natural basis for $\mathbb{Z}_3^3$. The cycle structure induced by M on the subspace $V_1 = \langle e_1, e_2 \rangle$ is, according to Theorem 3.14, given by $\begin{bmatrix} 1 & 1 & 1 \\ 1 & 2 & 6 \end{bmatrix}$. Similarly, the cycle structure induced by M on $V_2 = \langle e_3 \rangle$ is given by $\begin{bmatrix} 1 & 2 \\ 1 & 1 \end{bmatrix} = \begin{bmatrix} 3 \\ 1 \end{bmatrix}$. All members of $\mathbb{Z}_3^3$ can be expressed (uniquely) as linear *combinations of members of the subspaces mentioned above, say* $v = v_1 + v_2, v_i \in V_i$*. Furthermore, if the cycle length of* v_i *is* c_i*, then* v *lies within a cycle of length* $\operatorname{lcm}(c_1, c_2)$*. By pairing off the members of the annihilator spaces with one another in this way, we find* $\frac{2\times 2}{2} = 2$ *cycles of length* 2*, and* $\frac{2\times 6}{6} = 2$ *cycles of length* 6*. Consequently, we find that the cycle structure induced by* M *on* $\mathbb{Z}_3^3$ *is* $\begin{bmatrix} 1+2 & 1+2 & 1+2 \\ 1 & 2 & 6 \end{bmatrix} = \begin{bmatrix} 3 & 3 & 3 \\ 1 & 2 & 6 \end{bmatrix}$.

As a more elaborate example, we proceed to determine all the cycle structures that are induced by automorphisms on $\mathbb{Z}_p^3$ (where, again, $\{e_1, e_2, e_3\}$ denotes the natural basis):

Case 1: $\min(M) = l_1 l_2 l_3$, where the l_i are distinct linear polynomials. M is similar to the matrix $\begin{bmatrix} C_{l_1} & 0 & 0 \\ 0 & C_{l_2} & 0 \\ 0 & 0 & C_{l_3} \end{bmatrix}$.

Lemma 3.13 gives $|\mathcal{S}_{l_i}| = p$. Let the order of l_i be d_i. Then it follows that there are $\frac{p-1}{d_i}$ cycles of length d_i in $\mathcal{S}_{l_i}$. By accounting for all other members of $\mathbb{Z}_p^3$, as linear combinations of the members of $\mathcal{S}_{l_i}$, we get $\frac{(p-1)^2}{\operatorname{lcm}(d_i,d_j)}$ cycles of length $\operatorname{lcm}(d_i, d_j)$ and $\frac{(p-1)^3}{\operatorname{lcm}(d_1,d_2,d_3)}$ cycles of length $\operatorname{lcm}(d_1, d_2, d_3)$. As a result, the cyclic structure induced by a matrix with minimal polynomial the product of three distinct linear factors has the form $\begin{bmatrix} 1 & \frac{p-1}{d_1} & \frac{p-1}{d_2} & \frac{p-1}{d_3} & \frac{(p-1)^2}{\operatorname{lcm}(d_1,d_2)} & \frac{(p-1)^2}{\operatorname{lcm}(d_1,d_3)} & \frac{(p-1)^2}{\operatorname{lcm}(d_2,d_3)} & \frac{(p-1)^3}{\operatorname{lcm}(d_1,d_2,d_3)} \\ 1 & d_1 & d_2 & d_3 & \operatorname{lcm}(d_1,d_2) & \operatorname{lcm}(d_1,d_3) & \operatorname{lcm}(d_2,d_3) & \operatorname{lcm}(d_1,d_2,d_3) \end{bmatrix}$, where the d_i are any (not necessarily distinct) divisors of $p-1$.

Case 2: $\min(M) = l_1^2 l_2$, where the l_i are two distinct linear polynomials. M is similar to the matrix $\begin{bmatrix} C_{l_1^2} & 0 \\ 0 & C_{l_2} \end{bmatrix}$. The cycle structure induced by M on the subspace $\langle e_1, e_2 \rangle$ of $\mathbb{Z}_p^3$ is given by $\begin{bmatrix} 1 & \frac{p-1}{\operatorname{ord}(l_1)} & \frac{p(p-1)}{\operatorname{ord}(l_1^2)} \\ 1 & \operatorname{ord}(l_1) & \operatorname{ord}(l_1^2) \end{bmatrix} = \begin{bmatrix} 1 & \frac{p-1}{d_1} & \frac{p-1}{d_1} \\ 1 & d_1 & pd_1 \end{bmatrix}$ and the cycle structure induced by M on the subspace $\langle e_3 \rangle$ is $\begin{bmatrix} 1 & \frac{p-1}{\operatorname{ord}(l_2)} \\ 1 & \operatorname{ord}(l_2) \end{bmatrix} = \begin{bmatrix} 1 & \frac{p-1}{d_2} \\ 1 & d_2 \end{bmatrix}$. The remaining members of $\mathbb{Z}_p^3$ occur in $\frac{(p-1)^2}{\operatorname{lcm}(d_1,d_2)}$ cycles of length $\operatorname{lcm}(d_1, d_2)$ and $\frac{p(p-1)^2}{p\cdot\operatorname{lcm}(d_1,d_2)}$ cycles of length $p \cdot \operatorname{lcm}(d_1, d_2)$. Summarizing case 2, we get the cycle structure $\begin{bmatrix} 1 & \frac{p-1}{d_1} & \frac{p-1}{d_1} & \frac{p-1}{d_2} & \frac{(p-1)^2}{\operatorname{lcm}(d_1,d_2)} & \frac{(p-1)^2}{\operatorname{lcm}(d_1,d_2)} \\ 1 & d_1 & pd_1 & d_2 & \operatorname{lcm}(d_1,d_2) & p\cdot\operatorname{lcm}(d_1,d_2) \end{bmatrix}$, where the d_i are arbitrary divisors of $p-1$.

Case 3: $\min(M) = l_1^3$, with l_1 a linear polynomial. M is thus similar to the matrix $C_{l_1^3}$. The cycle structure of this matrix is already described by Theorem 3.14, namely $\begin{bmatrix} 1 & \frac{p-1}{\operatorname{ord}(l_1)} & \frac{p(p-1)}{\operatorname{ord}(l_1^2)} & \frac{p^2(p-1)}{\operatorname{ord}(l_1^3)} \\ 1 & \operatorname{ord}(l_1) & \operatorname{ord}(l_1^2) & \operatorname{ord}(l_1^3) \end{bmatrix}$. By Theorem 3.7 the order of l_1^2 is pd_1 and that of l_1^3 is $p^2 d_1$ if $p = 2$ and pd_1 otherwise. Hence, we get that the cycle structure induced by M is given by $\begin{bmatrix} 2 & 1 & 1 \\ 1 & 2 & 4 \end{bmatrix}$ if $p = 2$ and $\begin{bmatrix} 1 & \frac{p-1}{d_1} & \frac{p^2-1}{d_1} \\ 1 & d_1 & pd_1 \end{bmatrix}$ with d_1 any divisor of $p-1$ otherwise.

Case 4: $\min(M) = lq$ with l, q irreducible linear and quadratic polynomials, respectively. In this case, M is similar to a matrix of the form $\begin{bmatrix} C_q & 0 \\ 0 & C_l \end{bmatrix}$. Denote the orders of q and l by d_1 and d_2, respectively. From

Theorem 3.5, d_1 can be any divisor of p^2-1 that is not a divisor of $p-1$ and d_2 can be any divisor of $p-1$. The cycle structure induced by M on the subspace $\langle e_1, e_2\rangle$ of $\mathbb{Z}_p^3$ is then given by $\begin{bmatrix} 1 & \frac{p^2-1}{d_1} \\ 1 & d_1 \end{bmatrix}$. The cyclic structure induced by M on the subspace $\langle e_3\rangle$ is $\begin{bmatrix} 1 & \frac{p-1}{d_2} \\ 1 & d_2 \end{bmatrix}$. The remaining members of $\mathbb{Z}_p^3$ lie within $\frac{(p^2-1)(p-1)}{\operatorname{lcm}(d_1,d_2)}$ cycles of length $\operatorname{lcm}(d_1, d_2)$ each. We conclude that cycle structure in this case is given by $\begin{bmatrix} 1 & \frac{p^2-1}{d_1} & \frac{p-1}{d_2} & \frac{(p^2-1)(p-1)}{\operatorname{lcm}(d_1,d_2)} \\ 1 & d_1 & d_2 & \operatorname{lcm}(d_1,d_2) \end{bmatrix}$ with d_1 any divisor of p^2-1 that does not divide $p-1$, and d_2 any divisor of $p-1$.

Case 5: $\min(M) = c$, with c any irreducible cubic polynomial. Let the order of c be d. By Theorem 3.5, d can be any divisor of p^3-1 that does not divide p^2-1. M is then similar to C_c, and the cycle structure is given by $\begin{bmatrix} 1 & \frac{p^3-1}{d} \\ 1 & d \end{bmatrix}$ for any d that divides p^3-1 but not p^2-1.

Case 6: $\min(M) = l_1 l_2$, with the l_i two distinct linear polynomials. As usual, denote the order of l_i by d_i, which can be any divisor of $p-1$. Without loss of generality, M is similar to $\begin{bmatrix} C_{l_1} & 0 & 0 \\ 0 & C_{l_1} & 0 \\ 0 & 0 & C_{l_2} \end{bmatrix}$. The cycle structure that M induces on the subspace $\langle e_1\rangle$, as well as on the subspace $\langle e_2\rangle$, is $\begin{bmatrix} 1 & \frac{p-1}{d_1} \\ 1 & d_1 \end{bmatrix}$. Once again, the structure induced by M on the subspace $\langle e_3\rangle$ is $\begin{bmatrix} 1 & \frac{p-1}{d_2} \\ 1 & d_2 \end{bmatrix}$. The remaining members of $\mathbb{Z}_p^3$ occur in $\frac{(p-1)^2}{d_1}$ cycles of length d_1 and $2\frac{(p-1)^2}{\operatorname{lcm}(d_1,d_2)} + \frac{(p-1)^3}{\operatorname{lcm}(d_1,d_2)} = \frac{(p+1)(p-1)^2}{\operatorname{lcm}(d_1,d_2)}$ cycles of length $lcm(d_1, d_2)$. The conclusion is that we get the following cycle structure: $\begin{bmatrix} 1 & \frac{p^2-1}{d_1} & \frac{p-1}{d_2} & \frac{(p+1)(p-1)^2}{\operatorname{lcm}(d_1,d_2)} \\ 1 & d_1 & d_2 & \operatorname{lcm}(d_1,d_2) \end{bmatrix}$ with the d_i arbitrary divisors of $p-1$.

Case 7: $\min(M) = q$ with q an irreducible quadratic. The rational canonical form of any 3×3 matrix that has a companion matrix of a quadratic along its diagonal also has a linear factor that divides the quadratic. However, for this case, the quadratic needs to be irreducible, and hence have no linear factors, implying that this case cannot occur.

Case 8: $\min(M) = l^2$, with l a linear polynomial of order d. By Theorem 3.5, d can be any divisor of $p-1$ and M is similar to the matrix $\begin{bmatrix} C_{l^2} & 0 \\ 0 & C_l \end{bmatrix}$. By Theorem 3.14, the cycle structure induced by M on the subspace $\langle e_1, e_2\rangle$ is $\begin{bmatrix} 1 & \frac{p-1}{d} & \frac{p-1}{d} \\ 1 & d & pd \end{bmatrix}$ and the cyclic structure induced by M on the subspace $\langle e_3\rangle$ is given by $\begin{bmatrix} 1 & \frac{p-1}{d} \\ 1 & d \end{bmatrix}$. The remaining members of $\mathbb{Z}_p^3$ lie within $\frac{(p-1)^2}{d}$ cycles of length d each and $\frac{p(p-1)^2}{pd}$ cycles of length pd each. This results in the following cyclic cycle structure in the case: $\begin{bmatrix} 1 & \frac{p^2-1}{d} & \frac{p(p-1)}{d} \\ 1 & d & pd \end{bmatrix}$ for any d that divides $p-1$.

Case 9: $\min(M) = l$ with l a linear polynomial. Let the degree of l be d, which, by Theorem 3.14, can once again be any divisor of $p-1$. M is similar to a matrix of the form $\begin{bmatrix} C_l & 0 & 0 \\ 0 & C_l & 0 \\ 0 & 0 & C_l \end{bmatrix}$. In this case, all nonzero members of $\mathbb{Z}_p^3$ occur in cycles of length d, giving the cycle structure $\begin{bmatrix} 1 & \frac{p^3-1}{d} \\ 1 & d \end{bmatrix}$ for any d that divides $p-1$.

After listing all the cases, we see that some of the cycle structures that arise from different cases might indeed overlap. For example, the cycle structure found in Case 9 is also found as a special case of a structure found in Case 1, with $d_1 = d_2 = d_3$. Clearing up the overlaps, we can give this result in a more compact form as the following theorem:

Theorem 3.16 *Let $|A| = p^3$ where p is prime, and let $f : A \to A$ be a bijection. Then f has the auto-property with underlying group $(\mathbb{Z}_p^3, +)$ if and only if f has one of the following cycle structures:*

1. $\begin{bmatrix} 1 & \frac{p-1}{d_1} & \frac{p-1}{d_2} & \frac{p-1}{d_3} & \frac{(p-1)^2}{\mathrm{lcm}(d_1,d_2)} & \frac{(p-1)^2}{\mathrm{lcm}(d_1,d_3)} & \frac{(p-1)^2}{\mathrm{lcm}(d_2,d_3)} & \frac{(p-1)^3}{\mathrm{lcm}(d_1,d_2,d_3)} \\ 1 & d_1 & d_2 & d_3 & \mathrm{lcm}(d_1,d_2) & \mathrm{lcm}(d_1,d_3) & \mathrm{lcm}(d_2,d_3) & \mathrm{lcm}(d_1,d_2,d_3) \end{bmatrix}$ *where each d_i is an arbitrary divisor of $p-1$.*

2. $\begin{bmatrix} 1 & \frac{p-1}{d_1} & \frac{p-1}{d_1} & \frac{p-1}{d_2} & \frac{(p-1)^2}{\mathrm{lcm}(d_1,d_2)} & \frac{(p-1)^2}{\mathrm{lcm}(d_1,d_2)} \\ 1 & d_1 & pd_1 & d_2 & \mathrm{lcm}(d_1,d_2) & p \cdot \mathrm{lcm}(d_1,d_2) \end{bmatrix}$ *where each d_i is an arbitrary divisor of $p-1$.*

3. $\begin{bmatrix} 2 & 1 & 1 \\ 1 & 2 & 4 \end{bmatrix}$ *if $p = 2$, or* $\begin{bmatrix} 1 & \frac{p-1}{d_1} & \frac{p^2-1}{d_1} \\ 1 & d_1 & pd_1 \end{bmatrix}$ *with d_1 any divisor of $p-1$ otherwise.*

4. $\begin{bmatrix} 1 & \frac{p^2-1}{d_1} & \frac{p-1}{d_2} & \frac{(p^2-1)(p-1)}{\mathrm{lcm}(d_1,d_2)} \\ 1 & d_1 & d_2 & \mathrm{lcm}(d_1,d_2) \end{bmatrix}$ *with d_1 any divisor of p^2-1 and d_2 any divisor of $p-1$.*

5. $\begin{bmatrix} 1 & \frac{p^3-1}{d} \\ 1 & d \end{bmatrix}$ *for any d that divides p^3-1 but not p^2-1.*

6. $\begin{bmatrix} 1 & \frac{p^2-1}{d} & \frac{p(p-1)}{d} \\ 1 & d & pd \end{bmatrix}$ *for any divisor d of $p-1$.*

It is now clear (at least in principle) that when $|A| = p^n$ for any $n \geq 3$, a similar strategy/algorithm can be followed to find necessary and sufficient conditions on a bijection $f : A \to A$ to have the auto-property with underlying group $(\mathbb{Z}_p^n, +)$.

4. Conclusion

Given that a bijection $f : A \to A$ has the correct structure in order to bear the auto-property, it remains to show how to turn A into the appropriate abelian group with $f \in \mathrm{Aut}(A)$.

Let $\mathcal{G}$ be the structural graph of f. Now, if there exists a group automorphism $h : G \to G$ for some abelian group G such that $\mathcal{G}$ and the structural graph of h are isomorphic (as graphs), then one easily sees that A can be endowed with an abelian group structure such that f is a group automorphism.

In particular, let ρ_f and ρ_h be graph projections of f and h, respectively, and let ψ be a graph isomorphism from the codomain of ρ_f to the codomain of ρ_h. Define $\eta : A \to G$ by $\eta = \rho_h^{-1}\psi\rho_f$. Then it is routine to check that $(A, *)$ is an abelian group, where $\alpha * \beta = \eta^{-1}(\eta(\alpha) \cdot_G \eta(\beta))$ for all $\alpha, \beta \in A$. The identity is $1_A = \eta^{-1}(1_G)$. Furthermore, $(A, *) \cong G$ and it is also routine to check that $f \in \mathrm{Aut}(A)$.

Acknowledgment

The second author would like to thank the National Research Foundation of South Africa for financial assistance.

References

[1] De Klerk BE. A structural approach to the endomorphisms of certain abelian groups. PhD, University of the Free State, Bloemfontein, South Africa, 2017.

[2] De Klerk BE, Meyer JH, Szigeti J, van Wyk L. Functions realising as abelian group automorphisms. Comm Algebra 2018; 46: 467-479.

[3] Lidl R, Niederreiter H. Finite Fields. 2nd ed. Cambridge, UK: Cambridge University Press, 2008.