FINITE MODULES OVER $\mathbb{Z}[t, t^{-1}]$

XIANG-DONG HOU

Abstract. Let $\Lambda = \mathbb{Z}[t, t^{-1}]$ be the ring of Laurent polynomials over $\mathbb{Z}$. We classify all $\Lambda$-modules $M$ with $|M| = p^n$, where $p$ is a prime and $n \leq 4$. Consequently, we have a classification of Alexander quandles of order $p^n$ for $n \leq 4$.

1. Introduction

Let $\Lambda = \mathbb{Z}[t, t^{-1}]$ be the ring of Laurent polynomials over $\mathbb{Z}$, which is also the group ring over $\mathbb{Z}$ of the infinite cyclic group. Each $\Lambda$-module is uniquely determined by a pair $(M, \alpha)$, where $M$ is an abelian group and $\alpha \in \text{Aut}_{\mathbb{Z}}(M)$. The resulting $\Lambda$-module, denoted by $M\alpha$, is $M$ with a scalar multiplication defined by $tx = \alpha(x)$, $x \in M$. If two $\Lambda$-modules $M\alpha$ and $N\beta$ are isomorphic, where $\alpha \in \text{Aut}_{\mathbb{Z}}(M)$ and $\beta \in \text{Aut}_{\mathbb{Z}}(N)$, then $M \cong N$ as abelian groups. Moreover, for $\alpha, \beta \in \text{Aut}_{\mathbb{Z}}(M)$, $M\alpha \cong M\beta$ if and only if $\alpha$ and $\beta$ are conjugate in $\text{Aut}_{\mathbb{Z}}(M)$. Thus, to classify $\Lambda$-modules with an underlying abelian group $M$ is to determine the conjugacy classes of $\text{Aut}_{\mathbb{Z}}(M)$.

Our interest in finite $\Lambda$-modules comes from topology. In knot theory, a quandle is defined to be a set of $Q$ equipped with a binary operation $*$ such that for all $x, y, z \in Q$,

(i) $x * x = x$,
(ii) $(x * y)$ is a permutation of $Q$,
(iii) $(x * y) * z = (x * z) * (y * z)$.

Finite quandles are used to color knots; the number of colorings of a knot $K$ by a finite quandle $Q$ is an invariant of $K$ which allows us to distinguish inequivalent knots effectively \cite{1, 2}.

An Alexander quandle is a $\Lambda$-module $M$ with a quandle operation defined by $x * y = tx + (1-t)y$, $x, y \in M$. The following theorem is of fundamental importance.

Theorem 1.1 (\cite{8}). Two finite Alexander quandles $M$ and $N$ are isomorphic if and only if $|M| = |N|$ and the $\Lambda$-modules $(1-t)M$ and $(1-t)N$ are isomorphic.

Therefore, the classification of finite Alexander quandles is essentially the classification of finite $\Lambda$-modules.

The classification of finite $\Lambda$-modules can be reduced to that of $\Lambda$-modules of order $p^n$, where $p$ is a prime; see section 2. The same is true for the classification of finite Alexander quandles; see section 4. Finite Alexander quandles have been classified for orders up to 15 in \cite{8} and for order 16 in [6, 7]. Also known is the classification of connected Alexander quandles of order $p^2$ \cite{3, 8}. (A finite Alexander quandle is called connected if $1-t \in \text{Aut}_{\mathbb{Z}}(M)$.) The purpose of the present paper

2000 Mathematics Subject Classification. 16S34, 20K01, 57M27.

Key words and phrases. Alexander quandle, finite module, knot, group ring.
is to classify all Λ-modules and Alexander quandles of order $p^n$, $n \leq 4$. The details of the classification are given in Table 1 in the appendix. For a snapshot, there are $5p^4 - 2p^3 - 2p - 1$ nonisomorphic Λ-modules of order $p^4$ and there are $5p^4 - 6p^3 + p^2 - 6p - 1$ nonisomorphic Alexander quandles of order $p^4$.

In section 2, we show that every finite Λ-module has a unique decomposition where each direct summand $M$ has the following properties:

(i) $|M| = p^n$ for some prime $p$ and integer $n > 0$.

(ii) When treating $t$ as an element of $\text{End}_{\mathbb{Z}_p}(M/pM)$, the minimal polynomial of $t$ is a power of some irreducible $f \in \mathbb{Z}_p[X]$.

In section 3, we classify such Λ-modules $M$ of order $p^n$ with $n \leq 4$. In section 4, we derive the classification of Alexander quandles of order $p^n$, $n \leq 4$, from the results of section 3. For this purpose, we prove the following fact which is of interest in its own right: Given a finite Λ-module $N$ and an integer $l > 0$, a necessary and sufficient condition for the existence of a Λ-module $M \supset N$ such that $(1 - t)M = N$ and $|M/N| = l$ is $|N/(1 - t)N| \mid l$.

In our notation, the letter $t$ is reserved for the element $t \in \Lambda = \mathbb{Z}[t, t^{-1}]$. The group of units of a ring $R$ is denoted by $R^\times$; the set of all $m \times n$ matrices over $R$ is denoted by $M_{m \times n}(R)$.

### 2. Decomposition of Finite Λ-Modules

Let $M$ be a finite Λ-module. For each prime $p$, let

$$M_p = \{x \in M : p^n x = 0 \text{ for some } n \geq 0\}.$$ 

It is quite obvious that

$$(2.1) \quad M = \bigoplus_p M_p.$$ 

Moreover, two finite Λ-modules $M$ and $N$ are isomorphic if and only if $M_p \cong N_p$ for all primes $p$.

**Theorem 2.1.** Let $M$ be a finite Λ-module with $|M| = p^n$. For each irreducible $f \in \mathbb{Z}_p[X]$, let $\overline{f} \in \mathbb{Z}[X]$ be a lift of $f$ and define

$$(2.2) \quad M_f = \{x \in M : \overline{f}(t)^m x = 0 \text{ for some } m \geq 0\}.$$ 

Then

$$(2.3) \quad M = \bigoplus_f M_f,$$ 

where $f$ runs over all irreducible polynomials in $\mathbb{Z}_p[X]$. Moreover, if $N$ is another finite Λ-module whose order is a power of $p$, then $M \cong N$ if and only if $M_f \cong N_f$ for all irreducible $f \in \mathbb{Z}_p[X]$.

**Note.** $M_f$ depends only on $f$ but not on $\overline{f}$. Also, $M_f = 0$ unless $f$ divides the minimal polynomial of $t$ (viewed as an element of $\text{End}_{\mathbb{Z}_p}(M/pM)$).

**Proof of Theorem 2.1.** Let the minimal polynomial of $t$ ($\in \text{End}_{\mathbb{Z}_p}(M/pM)$) be $f_1^{e_1} \cdots f_k^{e_k}$, where $f_1, \ldots, f_k \in \mathbb{Z}_p[X]$ are distinct irreducibles and $e_1, \ldots, e_k$ are positive integers. We claim that

$$(2.4) \quad M = \bigoplus_{1 \leq i \leq k} M_{f_i}.$$
We first show that $\sum_{1 \leq i \leq k} M_{f_i}$ is a direct sum. Assume that $x \in M_{f_i} \cap (\sum_{1 \leq j \leq k, j \neq i} M_{f_j})$. Then there exists $m > 0$ such that $\overline{f_i}(t)^m x = 0$ and $\left(\prod_{1 \leq j \leq k, j \neq i} \overline{f_j}(t)^m\right) x = 0$. Since $\text{gcd}(f_i, \prod_{1 \leq j \leq k, j \neq i} f_j) = 1$, there exist $u, v \in \mathbb{Z}_p[X]$ such that

$$u f_i^m + v \left( \prod_{1 \leq j \leq k, j \neq i} f_j \right)^m = 1.$$ 

Let $\overline{u}, \overline{v} \in \mathbb{Z}[X]$ be arbitrary lifts of $u, v$, respectively. Then

$$\overline{u} \overline{f_i}^m + \overline{v} \left( \prod_{1 \leq j \leq k, j \neq i} \overline{f_j} \right)^m \equiv 1 \pmod{p}.$$ 

Therefore

$$\overline{u} \overline{f_i^m} + \overline{v} \left( \prod_{1 \leq j \leq k, j \neq i} \overline{f_j} \right)^m \in \text{Aut}_\mathbb{Z}(M).$$

Since

$$\left[ \overline{u} \overline{f_i^m} + \overline{v} \left( \prod_{1 \leq j \leq k, j \neq i} \overline{f_j} \right)^m \right] x = 0,$$

we have $x = 0$.

Now we prove that $M = \sum_{1 \leq i \leq k} M_{f_i}$. There exist $u_1, \ldots, u_k \in \mathbb{Z}_p[X]$ such that

$$\sum_{1 \leq i \leq k} u_i \left( \prod_{1 \leq j \leq k, j \neq i} f_j^{e_j} \right)^n = 1.$$ 

Let $\overline{u_i} \in \mathbb{Z}[X]$ be a lift of $u_i$ and let $F_i = \prod_{1 \leq j \leq k, j \neq i} \overline{f_j^{e_j}}$. Then

$$\sum_{1 \leq i \leq k} \overline{u_i} F_i^n \equiv 1 \pmod{p}.$$ 

Thus $\sum_{1 \leq i \leq k} \overline{u_i} F_i(t)^n \in \text{Aut}_\mathbb{Z}(M)$. It follows that

(2.5) \hfill M = \sum_{1 \leq i \leq k} F_i(t)^n M.$$ 

Since $(\prod_{1 \leq j \leq k} \overline{f_j^{e_j}}) M \subset pM$, we have

$$\overline{f_i(t)^{e_i}} F_i(t)^n M = \left( \prod_{1 \leq j \leq k} \overline{f_j(t)^{e_j}} \right)^n M \subset p^n M = 0.$$ 

Thus $F_i(t)^n M \subset M_{f_i}$. Then it follows from (2.5) that $M = \sum_{1 \leq i \leq k} M_{f_i}$.

2° Let $N$ be another finite $\Lambda$-module whose order is a power of $p$. If there is a $\Lambda$-module isomorphism $\phi : M \to N$, then for each irreducible $f \in \mathbb{Z}_p[X]$, $\phi|_{M_f} : M_f \to N_f$ is an isomorphism. Conversely, if $M_f \cong N_f$ for all irreducible $f \in \mathbb{Z}_p[X]$, then by (2.3), $M \cong N$. \qed
3. Classification of \( \Lambda \)-Modules of Order \( p^n, n \leq 4 \)

3.1. The automorphism group of a finite abelian group.

Let \( p \) be a prime and let \( m \geq n > 0 \) be integers. Elements of \( \mathbb{Z}_{p^m} \) can be viewed as elements of \( \mathbb{Z}_{p^n} \) via the homomorphism

\[
\begin{align*}
\mathbb{Z}_{p^m} & \rightarrow \mathbb{Z}_{p^n} \\
a + p^m \mathbb{Z} & \mapsto a + p^n \mathbb{Z}, \quad a \in \mathbb{Z}.
\end{align*}
\]

Likewise, elements of \( p^{m-n} \mathbb{Z}_{p^n} \) can be viewed as elements of \( \mathbb{Z}_{p^m} \) via the embedding

\[
p^{m-n}(a + p^n \mathbb{Z}) \rightarrow p^{m-n} a + p^m \mathbb{Z}, \quad a \in \mathbb{Z}.
\]

We shall adopt these conventions hereafter. Let \( M = \mathbb{Z}_{p^{n_1}} \times \cdots \times \mathbb{Z}_{p^{n_k}} \), where \( n_i > 0 \) and \( e_1 > \cdots > e_k > 0 \). Elements of \( \text{End}_{\mathbb{Z}}(M) \) are of the form

\[
\sigma_A : M \rightarrow M
\]

\[
\begin{bmatrix}
x_1 \\
\vdots \\
x_k
\end{bmatrix} \mapsto
\begin{bmatrix}
x_1 \\
\vdots \\
x_k
\end{bmatrix}, \quad x_i \in \mathbb{Z}_{p^{n_i}}^{n_i},
\]

where

\[
A = \begin{bmatrix}
A_{11} & p^{e_1-e_2} A_{12} & \cdots & p^{e_1-e_k} A_{1k} \\
A_{21} & A_{22} & \cdots & p^{e_2-e_1} A_{2k} \\
\vdots & \vdots & \ddots & \vdots \\
A_{k1} & A_{k2} & \cdots & A_{kk}
\end{bmatrix},
\]

and \( A_{ij} \in \text{M}_{n_i \times n_j}(\mathbb{Z}_{p^{n_i}}) \). Let \( \mathfrak{M}(M) \) denote the set of all matrices of the form (3.1). Then

\[
\mathfrak{M}(M) \rightarrow \text{End}_{\mathbb{Z}}(M)
\]

\[
A \mapsto \sigma_A
\]

is a ring isomorphism. Let \( \text{GL}(M) \) denote the group of units of \( \mathfrak{M}(M) \). Of course \( \text{GL}(M) \cong \text{Aut}_{\mathbb{Z}}(M) \) under the above isomorphism. It is known \([\text{II, 9}]\) (and also easy to prove) that

\[
\text{GL}(M) = \{ A : A \text{ is of the form (3.1) with } A_{ii} \in \text{GL}(n_i, \mathbb{Z}_{p^{n_i}}), 1 \leq i \leq k \}.
\]

The modulo \( p \) reduction from \( \text{GL}(M) \) to \( \text{GL}(n_1 + \cdots + n_k, \mathbb{Z}_p) \) is denoted by \( ( ) \). For each (monic) irreducible \( f \in \mathbb{Z}_p[X] \) with \( f \neq X \), define

\[
\text{GL}(M)_f = \{ A \in \text{GL}(M) : \text{the minimal polynomial of } A_{ii} \in \text{GL}(n_1 + \cdots + n_k, \mathbb{Z}_p) \text{ is a power of } f \}.
\]

If \( \lambda^{(i)} = (\lambda_{i1}, \lambda_{i2}, \ldots) \) is a partition of the integer \( n_i/\deg f, 1 \leq i \leq k \), we define

\[
\text{GL}(M)^{\lambda^{(i)}, \ldots, \lambda^{(k)}}_f = \{ A \text{ as in (3.1)} : \text{the elementary divisors of } A_{ii} \text{ are } f^{\lambda_{i1}}, f^{\lambda_{i2}}, \ldots, 1 \leq i \leq k \}.
\]

In this setting, our goal is to determine the \( \text{GL}(M) \)-conjugacy classes in \( \text{GL}(M)_f \). We will proceed according to the structure of \( (M,+ \).
3.2. \((M, +) = \mathbb{Z}_p^e\).
In this case we must have \(f = X - a, a \in \mathbb{Z}_p^\times\). The conjugacy classes in \(\text{GL}(M)_f\) are represented by
\[
[b], \quad b \in \mathbb{Z}_p^e, \quad b \equiv a \mod p.
\]

3.3. \((M, +) = \mathbb{Z}_p^n\).
In this case we must have \(\deg f \mid n\). The conjugacy classes in \(\text{GL}(M)_f\) are represented by the rational canonical forms in \(\text{GL}(n, \mathbb{Z}_p)\) with elementary divisors \(f^{\lambda_1}, f^{\lambda_2}, \ldots\), where \(\lambda_1 \geq \lambda_2 \geq \cdots > 0\) is a partition of \(n/\deg f\).

3.4. \((M, +) = \mathbb{Z}_p^e \times \mathbb{Z}_p, e > 1\).
In this case, \(\deg f = 1\).

**Theorem 3.1.** Assume \((M, +) = \mathbb{Z}_p^e \times \mathbb{Z}_p, e > 1,\) and \(f = X - a, a \in \mathbb{Z}_p^\times\). The conjugacy classes in \(\text{GL}(M)_f\) are represented by the following matrices:

1. \[
\begin{bmatrix}
 b & 0 \\
 b & b
\end{bmatrix} + \begin{bmatrix}
p^{-1} \alpha & 0 \\
0 & 0
\end{bmatrix}, \quad 0 < b < p^{-1}, \quad b \equiv a \mod p, \quad \alpha \in \mathbb{Z}_p.
\]
2. \[
\begin{bmatrix}
 b & 0 \\
 b & b
\end{bmatrix} + \begin{bmatrix}
0 & 0 \\
1 & 0
\end{bmatrix}, \quad 0 < b < p^{-1}, \quad b \equiv a \mod p.
\]
3. \[
\begin{bmatrix}
 b & 0 \\
 b & b
\end{bmatrix} + \begin{bmatrix}
p^{-1} & 0 \\
0 & 0
\end{bmatrix}, \quad 0 < b < p^{-1}, \quad b \equiv a \mod p, \quad \gamma \in \mathbb{Z}_p.
\]

**Proof.** Elements of \(\text{GL}(M)_f\) are of the form
\[
A(b, \alpha, \beta, \gamma) := \begin{bmatrix}
 b & 0 \\
 0 & b
\end{bmatrix} + \begin{bmatrix}
p^{-1} \alpha & p^{-1} \beta \\
\gamma & 0
\end{bmatrix},
\]
where \(0 < b < p^{-1}, \quad b \equiv a \mod p, \quad \alpha, \beta, \gamma \in \mathbb{Z}_p\). Let \(A(b, \alpha, \beta, \gamma), A(b', \alpha', \beta', \gamma') \in \text{GL}(M)_f\) and
\[
P = \begin{bmatrix}
x & p^{-1}y \\
0 & w
\end{bmatrix} \in \text{GL}(M), \quad x \in \mathbb{Z}_p^\times, \quad w \in \mathbb{Z}_p^\times, \quad y, z \in \mathbb{Z}_p.
\]
The equation \(PA(b, \alpha, \beta, \gamma) = A(b, \alpha', \beta', \gamma')P\) is equivalent to
\[
\begin{bmatrix}
p^{-1}(xa + y\gamma) & p^{-1}x\beta \\
w\gamma & 0
\end{bmatrix} = \begin{bmatrix}
p^{-1}(\alpha' x + \beta' z) & p^{-1}\beta' w \\
\gamma' x & 0
\end{bmatrix}.
\]
The above equation can be written as a matrix equation over \(\mathbb{Z}_p\):
\[
\begin{bmatrix}
x \alpha + y\gamma & x\beta \\
w\gamma & 0
\end{bmatrix} = \begin{bmatrix}
\alpha' x + \beta' z & \beta' w \\
\gamma' x & 0
\end{bmatrix},
\]
equivalently,
\[
\begin{bmatrix}
x & y \\
0 & w
\end{bmatrix} \begin{bmatrix}
\beta & \alpha \\
0 & \gamma
\end{bmatrix} = \begin{bmatrix}
\beta' & \alpha' \\
0 & \gamma'
\end{bmatrix} \begin{bmatrix}
w & z \\
0 & x
\end{bmatrix}.
\]
So, \(A(b, \alpha, \beta, \gamma)\) and \(A(b', \alpha', \beta', \gamma')\) are conjugate if and only if there exist \(x, y \in \mathbb{Z}_p^\times\) and \(y, z \in \mathbb{Z}_p\) such that
\[
(3.2) \quad \begin{bmatrix}
x & y \\
0 & w
\end{bmatrix} \begin{bmatrix}
\beta & \alpha \\
0 & \gamma
\end{bmatrix} \begin{bmatrix}
w^{-1} & z \\
0 & x^{-1}
\end{bmatrix} = \begin{bmatrix}
\beta' & \alpha' \\
0 & \gamma'
\end{bmatrix}.
\]
Let \(\mathcal{M} = \{ \begin{bmatrix} \beta & \alpha \\ 0 & \gamma \end{bmatrix} : \alpha, \beta, \gamma \in \mathbb{Z}_p \} \). For \(A = \begin{bmatrix} \beta & \alpha \\ 0 & \gamma \end{bmatrix}, \ A' = \begin{bmatrix} \beta' & \alpha' \\ 0 & \gamma' \end{bmatrix} \in \mathcal{M}, \) say \(A \sim A'\) if \((3.2)\) is satisfied for some \(x, w \in \mathbb{Z}_p^\times\) and \(y, z \in \mathbb{Z}_p\). It is easy to see that the \(\sim\) equivalence classes in \(\mathcal{M}\) are represented by
These matrices correspond to the representatives of the conjugacy classes in \( \text{GL}(M)_f \) stated in the theorem.

3.5. \((M, +) = \mathbb{Z}_p^2\).

In this case, \( \deg f = 1 \) or \( 2 \).

**Theorem 3.2.** Assume \((M, +) = \mathbb{Z}_p^2\).

(i) Let \( f = X - a, \ a \in \mathbb{Z}_p^\times \). Then the conjugacy classes in \( \text{GL}(M)_{(1,1)} \) are represented by the following matrices:

\[
(1.1) \begin{bmatrix} b & \alpha \\ b & \delta \end{bmatrix} + p \begin{bmatrix} \alpha & \delta \\ \gamma & \beta \end{bmatrix}, \quad 0 < b < p, \ b \equiv a \pmod{p}, \ 0 \leq \alpha \leq \delta < p.
\]

\[
(1.2) \begin{bmatrix} b & \alpha \\ b & \delta \end{bmatrix} + p \begin{bmatrix} \alpha & 1 \\ \gamma & \alpha \end{bmatrix}, \quad 0 < b < p, \ b \equiv a \pmod{p}, \ \alpha \in \mathbb{Z}_p.
\]

\[
(1.3) \begin{bmatrix} b & 0 \\ b & 1 \end{bmatrix} + p \begin{bmatrix} 0 & \alpha \\ -b_0 & -b_1 \end{bmatrix}, \quad 0 < b < p, \ b \equiv a \pmod{p}, \ X^2 + b_1X + b_0 \in \mathbb{Z}_p[X] \text{ irreducible}.
\]

(ii) Let \( f = X - a, \ a \in \mathbb{Z}_p^\times \). Then the conjugacy class in \( \text{GL}(M)_{(2)} \) are represented by

\[
\begin{bmatrix} b & 1 \\ 0 & b \end{bmatrix} + p \begin{bmatrix} \alpha & \gamma \\ 0 & 0 \end{bmatrix}, \quad 0 < b < p, \ b \equiv a \pmod{p}, \ \alpha, \gamma \in \mathbb{Z}_p.
\]

(iii) Let \( f = X^2 + a_1X + a_0 \in \mathbb{Z}_p[X] \) be irreducible. Then the conjugacy classes in \( \text{GL}(M)_f \) are represented by

\[
\begin{bmatrix} 0 & 1 \\ -b_0 & b_1 \end{bmatrix} + p \begin{bmatrix} \alpha & \beta \\ 0 & 0 \end{bmatrix}, \quad 0 \leq b_0, b_1 < p, \ b_0 \equiv a_0 \pmod{p}, \ b_1 \equiv a_1 \pmod{p}, \ \alpha, \beta \in \mathbb{Z}_p.
\]

**Proof.** We remind the reader that in the proof, our notation is local in each of the three cases.

(i) Elements of \( \text{GL}(M)_{(1,1)} \) are of the form

\[
A(b, \alpha, \beta, \gamma, \delta) := \begin{bmatrix} b & \alpha \\ b & \beta \end{bmatrix} + p \begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix}, \quad 0 < b < p, \ b \equiv a \pmod{p}, \ \alpha, \beta, \gamma, \delta \in \mathbb{Z}_p.
\]

Clearly, \( A(b, \alpha, \beta, \gamma, \delta) \) and \( A(b', \alpha', \beta', \gamma', \delta') \) are conjugate in \( \text{GL}(M) \) if and only if \( \begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix} \) and \( \begin{bmatrix} \alpha' & \beta' \\ \gamma' & \delta' \end{bmatrix} \) are conjugate in \( M_{2 \times 2}(\mathbb{Z}_p) \). The conjugacy classes in \( M_{2 \times 2}(\mathbb{Z}_p) \) are represented by

\[
(1) \begin{bmatrix} \alpha & \beta \\ \delta & \gamma \end{bmatrix}, \quad 0 \leq \alpha \leq \delta < p,
\]

\[
(2) \begin{bmatrix} \alpha & 1 \\ \alpha & \beta \end{bmatrix}, \quad \alpha \in \mathbb{Z}_p.
\]
Assume that which can be simplified as

\[
A(\alpha, \beta, \gamma, \delta) := \begin{bmatrix} b & 1 \\ 0 & b \end{bmatrix} + p \begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix}, \quad 0 < b < p, \ b \equiv a \pmod{p}, \ \alpha, \beta, \gamma, \delta \in \mathbb{Z}_p.
\]


Then over \( \mathbb{Z}_p \),

\[
\mathcal{P} \begin{bmatrix} b & 1 \\ 0 & b \end{bmatrix} = \begin{bmatrix} b & 1 \\ 0 & b \end{bmatrix} \mathcal{P},
\]

which implies that \( \mathcal{P} = \begin{bmatrix} c & d \\ 0 & c \end{bmatrix}, \ c \in \mathbb{Z}_p^\times, \ d \in \mathbb{Z}_p. \) So

\[
P = \begin{bmatrix} c & d \\ 0 & c \end{bmatrix} + p \begin{bmatrix} x & y \\ z & w \end{bmatrix}, \quad x, y, z, w \in \mathbb{Z}_p.
\]

Now (3.3) becomes

\[
P \begin{bmatrix} c & d \\ 0 & c \end{bmatrix} \begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix} + p \begin{bmatrix} x & y \\ z & w \end{bmatrix} \begin{bmatrix} b & 1 \\ 0 & b \end{bmatrix} = p \begin{bmatrix} \alpha' & \beta' \\ \gamma' & \delta' \end{bmatrix} \begin{bmatrix} c & d \\ 0 & c \end{bmatrix} + p \begin{bmatrix} b & 1 \\ 0 & b \end{bmatrix} \begin{bmatrix} x & y \\ z & w \end{bmatrix}.
\]

Over \( \mathbb{Z}_p \), this becomes

\[
\begin{bmatrix} c & d \\ 0 & c \end{bmatrix} \begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix} + \begin{bmatrix} x & y \\ z & w \end{bmatrix} \begin{bmatrix} b & 1 \\ 0 & b \end{bmatrix} = \begin{bmatrix} \alpha' & \beta' \\ \gamma' & \delta' \end{bmatrix} \begin{bmatrix} c & d \\ 0 & c \end{bmatrix} + \begin{bmatrix} b & 1 \\ 0 & b \end{bmatrix} \begin{bmatrix} x & y \\ z & w \end{bmatrix},
\]

which can be simplified as

\[
\begin{bmatrix} c & d \\ 0 & c \end{bmatrix} \begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix} = \begin{bmatrix} \alpha' & \beta' \\ \gamma' & \delta' \end{bmatrix} \begin{bmatrix} c & d \\ 0 & c \end{bmatrix} + \begin{bmatrix} x & y \\ z & w \end{bmatrix} - \begin{bmatrix} x & y \\ z & w \end{bmatrix}.
\]

Thus, \( A(b, \alpha, \beta, \gamma, \delta) \) and \( A(b', \alpha', \beta', \gamma', \delta') \) are conjugate if and only if there exist \( d, z, w \in \mathbb{Z}_p \) such that

\[
(3.4) \quad \begin{bmatrix} 1 & d \\ 0 & 1 \end{bmatrix} \begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix} \begin{bmatrix} 1 & -d \\ 0 & 1 \end{bmatrix} + \begin{bmatrix} z & w \\ 0 & -z \end{bmatrix} = \begin{bmatrix} \alpha' & \beta' \\ \gamma' & \delta' \end{bmatrix}.
\]

For \( A = \begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix}, \ A' = \begin{bmatrix} \alpha' & \beta' \\ \gamma' & \delta' \end{bmatrix} \in M_{2 \times 2}(\mathbb{Z}_p), \) say \( A \sim A' \) if (3.4) is satisfied for some \( d, z, w \in \mathbb{Z}_p \). It is easy to see that the \( \sim \) equivalence classes in \( M_{2 \times 2}(\mathbb{Z}_p) \) are represented by

\[
\begin{bmatrix} \alpha & 0 \\ \gamma & 0 \end{bmatrix}, \quad \alpha, \beta \in \mathbb{Z}_p,
\]

which correspond to the matrices in (ii).

(iii) Elements of \( \text{GL}(M)_f \) are conjugate to matrices of the form

\[
A(f, \alpha, \beta, \gamma, \delta) := \begin{bmatrix} 0 & 1 \\ -b_0 & -b_1 \end{bmatrix} + p \begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix}, \quad 0 \leq b_0, b_1 < p, \ b_0 \equiv a_0 \pmod{p}, \ b_1 \equiv a_1 \pmod{p}, \ \alpha, \beta, \gamma, \delta \in \mathbb{Z}_p.
\]

Assume that \( P \in \text{GL}(2, \mathbb{Z}_p^\times) \) such that

\[
(3.5) \quad PA(f, \alpha, \beta, \gamma, \delta) = A(f, \alpha', \beta', \gamma', \delta') P.
\]
Then over $\mathbb{Z}_p$, 
\[
P \begin{bmatrix} 0 & 1 \\ -b_0 & -b_1 \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ -b_0 & -b_1 \end{bmatrix} P,
\]
which implies that 
\[
P = uI + v \begin{bmatrix} 0 & 1 \\ -b_0 & -b_1 \end{bmatrix} + p \begin{bmatrix} x & y \\ z & w \end{bmatrix}, \quad 0 \leq u, v < p, \ (u, v) \neq (0, 0), \ x, y, z, w \in \mathbb{Z}_p.
\]
Now (3.5) becomes the following equation over $\mathbb{Z}_p$:
\[
(3.6) \quad \left( uI + v \begin{bmatrix} 0 & 1 \\ -b_0 & -b_1 \end{bmatrix} \right) \begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix} = \begin{bmatrix} \alpha' & \beta' \\ \gamma' & \delta' \end{bmatrix} \left( uI + v \begin{bmatrix} 0 & 1 \\ -b_0 & -b_1 \end{bmatrix} \right)
\]
\[
+ \begin{bmatrix} 0 & 1 \\ -b_0 & -b_1 \end{bmatrix} \begin{bmatrix} x & y \\ z & w \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ -b_0 & -b_1 \end{bmatrix}.
\]
The space $\{ \begin{bmatrix} 0 & 1 \\ -b_0 & -b_1 \end{bmatrix} X - X \begin{bmatrix} 0 & 1 \\ -b_0 & -b_1 \end{bmatrix} : X \in M_{2 \times 2}(\mathbb{Z}_p) \}$ has dimension 2 over $\mathbb{Z}_p$ [5 §4.4] and has a basis 
\[
\begin{bmatrix} 0 & 1 \\ -b_0 & -b_1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} - \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ -b_0 & -b_1 \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ -b_0 & 0 \end{bmatrix},
\]
\[
\begin{bmatrix} 0 & 1 \\ -b_0 & -b_1 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} - \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ -b_0 & -b_1 \end{bmatrix} = \begin{bmatrix} b_0 & b_1 \\ 0 & -b_0 \end{bmatrix}.
\]
So (3.6) can be written as 
\[
(3.7) \quad \left( uI + v \begin{bmatrix} 0 & 1 \\ -b_0 & -b_1 \end{bmatrix} \right) \begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix} = \begin{bmatrix} \alpha' & \beta' \\ \gamma' & \delta' \end{bmatrix} \left( uI + v \begin{bmatrix} 0 & 1 \\ -b_0 & -b_1 \end{bmatrix} \right)
\]
\[
+ \begin{bmatrix} -d & \frac{e}{b_0} - \frac{d^{b_0}}{b_0} \\ c & \frac{d}{b_0} \end{bmatrix}, \quad c, d \in \mathbb{Z}_p.
\]
Thus $A(f, \alpha, \beta, \gamma, \delta)$ and $A(f, \alpha', \beta', \gamma', \delta')$ are conjugate if and only if there exist 
$0 \leq u, v < p, \ (u, v) \neq (0, 0)$, and $c, d \in \mathbb{Z}_p$ such that 
\[
(3.8) \quad \left( uI + v \begin{bmatrix} 0 & 1 \\ -b_0 & -b_1 \end{bmatrix} \right) \left( \begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix} - \begin{bmatrix} -d & \frac{e}{b_0} - \frac{d^{b_0}}{b_0} \\ c & \frac{d}{b_0} \end{bmatrix} \right) \left( uI + v \begin{bmatrix} 0 & 1 \\ -b_0 & -b_1 \end{bmatrix} \right)^{-1} = \begin{bmatrix} \alpha' & \beta' \\ \gamma' & \delta' \end{bmatrix}.
\]
For $A = \begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix}$, $A' = \begin{bmatrix} \alpha' & \beta' \\ \gamma' & \delta' \end{bmatrix} \in M_{2 \times 2}(\mathbb{Z}_p)$, say $A \sim A'$ if (3.8) is satisfied for some $0 \leq u, v < p, \ (u, v) \neq (0, 0)$, and $c, d \in \mathbb{Z}_p$. It remains to show that the $\sim$ equivalence classes in $M_{2 \times 2}(\mathbb{Z}_p)$ are represented by 
\[
\begin{bmatrix} \alpha & \beta \\ 0 & 0 \end{bmatrix}, \quad \alpha, \beta \in \mathbb{Z}_p.
\]
First, choose $u = 1, v = 0, c = -\gamma, d = -\delta$. Then the left side of (3.8) becomes 
\[
\begin{bmatrix} \alpha' & \beta' \\ 0 & 0 \end{bmatrix} \quad \text{for some } \alpha', \beta' \in \mathbb{Z}_p.
\]
Next, assume that (3.8) holds with $\gamma = \delta = \gamma' = \delta' = 0$. We want to show that 
$(\alpha, \beta) = (\alpha', \beta')$. Taking the traces of the two sides of (3.8), we have $\alpha = \alpha'$. Now (3.7) with $\alpha = \alpha'$ and $\gamma = \delta = \gamma' = \delta' = 0$ gives 
\[
\begin{bmatrix} u\alpha & u\beta \\ -v\beta \alpha & -v\beta \beta \end{bmatrix} = \begin{bmatrix} \alpha u - \beta v b_0 & \alpha v - \beta (u - v b_1) \\ 0 & 0 \end{bmatrix} + \begin{bmatrix} -d & \frac{e}{b_0} - \frac{d^{b_0}}{b_0} \\ c & \frac{d}{b_0} \end{bmatrix}.
\]
Taking the traces, we have \( vb_0 \beta = vb_0 \beta' \). If \( v \neq 0 \), then \( \beta = \beta' \). If \( v = 0 \), then \( c = d = 0 \), which implies \( u \beta = u \beta' \). Since \( u \neq 0 \), we also have \( \beta = \beta' \). \( \square \)

3.6. \((M, +) = \mathbb{Z}_p^2 \times \mathbb{Z}_p^2\).
In this case \( \deg f = 1 \).

**Theorem 3.3.** Assume \((M, +) = \mathbb{Z}_p^2 \times \mathbb{Z}_p^2\) and \( f = X - a, a \in \mathbb{Z}_p^\times \).

(i) The conjugacy classes in \( \text{GL}(M)(1)^{(1, 1)} \) are represented by the following matrices:

\[
\begin{align*}
(i.1) \quad & \begin{bmatrix} b & b \\ b & b \end{bmatrix} + \begin{bmatrix} p \alpha & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}, \quad 0 < b < p, \ b \equiv a \ (\text{mod} \ p), \ \alpha \in \mathbb{Z}_p. \\
(i.2) \quad & \begin{bmatrix} b & b \\ b & b \end{bmatrix} + \begin{bmatrix} 0 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}, \quad 0 < b < p, \ b \equiv a \ (\text{mod} \ p). \\
(i.3) \quad & \begin{bmatrix} b & b \\ b & b \end{bmatrix} + \begin{bmatrix} 0 & p & 0 \\ 0 & 0 & 0 \\ \eta & 0 & 0 \end{bmatrix}, \quad 0 < b < p, \ b \equiv a \ (\text{mod} \ p), \ \eta \in \mathbb{Z}_p. \\
(i.4) \quad & \begin{bmatrix} b & b \\ b & b \end{bmatrix} + \begin{bmatrix} 0 & p & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}, \quad 0 < b < p, \ b \equiv a \ (\text{mod} \ p). 
\end{align*}
\]

(ii) The conjugacy classes in \( \text{GL}(M)(1)^{(1, 2)} \) are represented by the following matrices:

\[
\begin{align*}
(ii.1) \quad & \begin{bmatrix} b & b \\ b & b \end{bmatrix} + \begin{bmatrix} p \alpha & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}, \quad 0 < b < p, \ b \equiv a \ (\text{mod} \ p), \ \alpha \in \mathbb{Z}_p. \\
(ii.2) \quad & \begin{bmatrix} b & b \\ b & b \end{bmatrix} + \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 1 & 0 & 0 \end{bmatrix}, \quad 0 < b < p, \ b \equiv a \ (\text{mod} \ p). \\
(ii.3) \quad & \begin{bmatrix} b & b \\ b & b \end{bmatrix} + \begin{bmatrix} 0 & p & 0 \\ 0 & 0 & 0 \\ \eta & 0 & 0 \end{bmatrix}, \quad 0 < b < p, \ b \equiv a \ (\text{mod} \ p), \ \eta \in \mathbb{Z}_p. 
\end{align*}
\]

**Proof.** (i) Elements of \( \text{GL}(M)(1)^{(1, 1)} \) are of the form

\[
A(b, \alpha, \ldots, \eta) := \begin{bmatrix} b & b \\ b & b \end{bmatrix} + \begin{bmatrix} p \alpha & p \beta & p \gamma \\ \delta & 0 & 0 \\ \eta & 0 & 0 \end{bmatrix}, \quad 0 < b < p, \ b \equiv a \ (\text{mod} \ p), \ \alpha, \ldots, \eta \in \mathbb{Z}_p.
\]

Assume that \( P \in \text{GL}(M) \) such that

\[
(3.9) \quad PA(b, \alpha, \ldots, \eta) = A(b, \alpha', \ldots, \eta')P.
\]

Write

\[
P = \begin{bmatrix} x & pY \\ Z & W \end{bmatrix}.
\]
where \( x \in \mathbb{Z}_p^\times, Y \in M_{1 \times 2}(\mathbb{Z}_p), Z \in M_{2 \times 1}(\mathbb{Z}_p), W \in \text{GL}(2, \mathbb{Z}_p) \). Then (3.9) becomes

\[
\begin{bmatrix}
p x \alpha + p Y \begin{bmatrix} \delta \\ \eta \end{bmatrix} \\
w \begin{bmatrix} \delta \\ \eta \end{bmatrix} 
\end{bmatrix} = \begin{bmatrix} p \alpha' x + p \beta', \gamma' z \\
\delta', \eta' \end{bmatrix} x \begin{bmatrix} 0 \\
0 \end{bmatrix}.
\]

Over \( \mathbb{Z}_p \), this becomes

\[
\begin{bmatrix}
x \alpha + Y \begin{bmatrix} \delta \\ \eta \end{bmatrix} \begin{bmatrix} \beta, \gamma \end{bmatrix} \\
w \begin{bmatrix} \delta \\ \eta \end{bmatrix} 
\end{bmatrix} = \begin{bmatrix} \alpha' x + \beta', \gamma' z \\\n\delta', \eta' \end{bmatrix} x \begin{bmatrix} 0 \\
0 \end{bmatrix}.
\]

It is more convenient to write the above equation as

\[
\begin{bmatrix}
x \\
0 \\
w \begin{bmatrix} \delta \\ \eta \end{bmatrix} 
\end{bmatrix} \begin{bmatrix} \beta, \gamma \end{bmatrix} = \begin{bmatrix} \alpha' x + \beta', \gamma' z \\\n\delta', \eta' \end{bmatrix} \begin{bmatrix} x \\
0 \end{bmatrix}.
\]

So, \( A(b, \alpha, \ldots, \eta) \) and \( A(b, \alpha', \ldots, \eta') \) are conjugate if and only if

\[
(3.10)
\begin{bmatrix}
x \\
0 \\
w \begin{bmatrix} \delta \\ \eta \end{bmatrix} 
\end{bmatrix} \begin{bmatrix} \beta, \gamma \end{bmatrix} = \begin{bmatrix} \alpha' x + \beta', \gamma' z \\\n\delta', \eta' \end{bmatrix} \begin{bmatrix} x \\
0 \end{bmatrix}
\]

for some \( x \in \mathbb{Z}_p^\times, W \in \text{GL}(2, \mathbb{Z}_p), Y \in M_{1 \times 2}(\mathbb{Z}_p), Z \in M_{2 \times 1}(\mathbb{Z}_p) \).

Let

\[
\mathcal{M} = \left\{ \begin{bmatrix} \beta, \gamma \\
\alpha \\
\delta \\
\eta \end{bmatrix} : \alpha, \ldots, \eta \in \mathbb{Z}_p \right\}.
\]

For

\[
A = \begin{bmatrix} \beta, \gamma \\
\alpha \\
\delta \\
\eta \end{bmatrix}, \quad A' = \begin{bmatrix} \beta', \gamma' \\
\alpha' \\
\delta' \\
\eta' \end{bmatrix} \in \mathcal{M},
\]

say \( A \sim A' \) if (3.10) is satisfied. It is easy to see that the \( \sim \) equivalence classes in \( \mathcal{M} \) are represented by

1. \[
\begin{bmatrix} 0 \\
\alpha \\
0 \\
0 \end{bmatrix}, \quad \alpha \in \mathbb{Z}_p,
\]

2. \[
\begin{bmatrix} 0 \\
1 \\
0 \\
0 \end{bmatrix},
\]

3. \[
\begin{bmatrix} 1 \\
0 \\
0 \\
\eta \end{bmatrix}, \quad \eta \in \mathbb{Z}_p,
\]

4. \[
\begin{bmatrix} 1 \\
0 \\
1 \\
0 \end{bmatrix}.
\]
These correspond to the matrices in (i.1) – (i.4).

(ii) Elements of $GL(M)^{(1)(1.1)}$ are conjugate for matrices of the form

$$A(b, \alpha, \ldots, \eta) := \begin{bmatrix} b & b & 0 \\ b & 1 & \alpha \\ & & \eta \end{bmatrix} + \begin{bmatrix} p \alpha & p \beta & p \gamma \\ \delta & 0 & 0 \\ \eta & 0 & 0 \end{bmatrix}, \quad 0 < b < p, \ b \equiv a \ (\text{mod} \ p), \ \alpha, \ldots, \eta \in \mathbb{Z}_p.$$ 

Assume that $P \in GL(M)$ such that

$$PA(b, \alpha, \ldots, \eta) = A(b, \alpha', \ldots, \eta') P.$$ 

Write

$$P = \begin{bmatrix} x & pY \\ Z & W \end{bmatrix},$$

where $x \in \mathbb{Z}_p^2$, $Y \in M_{1 \times 2}(\mathbb{Z}_p)$, $Z \in M_{2 \times 1}(\mathbb{Z}_p)$, $W \in GL(2, \mathbb{Z}_p)$. Since $W$ commutes with $\begin{bmatrix} b & 1 \\ 0 & \delta \end{bmatrix}$, we have $W = \begin{bmatrix} c & d \\ 0 & e \end{bmatrix}$. Equation (3.11) is equivalent to

$$\begin{bmatrix} 0 & pY \\ 0 & W \end{bmatrix} = \begin{bmatrix} 0 & \eta \end{bmatrix} + \begin{bmatrix} \alpha' x + p[\beta', \gamma]'Z & [\beta', \gamma]'W \\ Z W \end{bmatrix},$$

which can be written as

$$\begin{bmatrix} x & Y \\ 0 & W \end{bmatrix} \begin{bmatrix} [\beta', \gamma] & \alpha \\ 0 & \delta \end{bmatrix} + \begin{bmatrix} Y & 0 \\ 0 & Z \end{bmatrix} = \begin{bmatrix} [\beta', \gamma]' & \alpha' \end{bmatrix} \begin{bmatrix} W & Z \\ 0 & x \end{bmatrix}.$$ 

So, $A(b, \alpha, \ldots, \eta)$ and $A(b, \alpha', \ldots, \eta')$ are conjugate if and only if

$$\begin{bmatrix} x & Y \\ 0 & W \end{bmatrix} [\beta', \gamma]' \begin{bmatrix} \alpha \\ \delta \end{bmatrix} \begin{bmatrix} W^{-1} & Z \\ 0 & x^{-1} \end{bmatrix} + \begin{bmatrix} Y & 0 \\ 0 & Z \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 0 & W \end{bmatrix} = \begin{bmatrix} [\beta', \gamma]' & \alpha' \end{bmatrix} \begin{bmatrix} 0 & \delta' \\ \eta' & Z \end{bmatrix}$$

for some $x \in \mathbb{Z}_p^*$, $Y \in M_{1 \times 2}(\mathbb{Z}_p)$, $Z \in M_{2 \times 1}(\mathbb{Z}_p)$, $W = \begin{bmatrix} c & d \\ 0 & e \end{bmatrix} \in GL(2, \mathbb{Z}_p)$.

Let

$$\mathcal{M} = \left\{ \begin{bmatrix} [\beta, \gamma] & \alpha \\ 0 & \delta \end{bmatrix} : \alpha, \ldots, \eta \in \mathbb{Z}_p \right\}.$$
For
\[
A = \begin{bmatrix} [\beta, \gamma] & \alpha \\ 0 & \delta \\ \eta \end{bmatrix}, \quad A' = \begin{bmatrix} [\beta', \gamma'] & \alpha' \\ 0 & \delta' \\ \eta' \end{bmatrix} \in \mathcal{M},
\]
say \( A \sim A' \) if (3.12) is satisfied. It remains to determine the representatives of the \( \sim \) equivalence classes in \( \mathcal{M} \).

In (3.12), we may assume \( W = \begin{bmatrix} 1 & \xi \end{bmatrix} \) by replacing \( x, Y, W, Z \) with \( 1c, \xi Y, cW, cZ \), respectively. Let \( Y = \begin{bmatrix} y_1, y_2 \end{bmatrix}, Z = \begin{bmatrix} z_1, z_2 \end{bmatrix} \). Then (3.12) becomes
\[
(3.13)
\begin{bmatrix}
0 
\alpha
0 
\eta
\end{bmatrix}
= \begin{bmatrix}
\beta' 
\gamma' 
\alpha'
\delta' 
\eta'
\end{bmatrix}.
\]

We claim that the \( \sim \) equivalence classes in \( \mathcal{M} \) are represented by

(1) \[ \begin{bmatrix} [0 0] \\
0
0
0
0
\end{bmatrix}, \quad \alpha \in \mathbb{Z}_p, \]

(2) \[ \begin{bmatrix} [0 0] \\
0
0
0
0
\end{bmatrix}, \quad \eta \in \mathbb{Z}_p. \]

The proof of (ii) will be complete when this claim is proved.

First, it is clear that matrices from different families of (1) – (3) are not \( \sim \) equivalent. So it remains to show that every \( A \in \mathcal{M} \) can be brought into one of the “canonical forms” in (1) – (3) through \( \sim \) equivalence, and the entries in the canonical form are uniquely determined by \( A \).

Let
\[
A = \begin{bmatrix} [\beta, \gamma] & \alpha \\ 0 & \delta \\ \eta \end{bmatrix} \in \mathcal{M}.
\]

First assume \( \beta = 0 \) and \( \eta = 0 \). Then
\[
\text{LHS of (3.13)} = \begin{bmatrix} [0 0] \\
0
0
\end{bmatrix} = \begin{bmatrix} [0 0] \\
0
0
\end{bmatrix}
\]
if and only if
\[
(3.14) \quad \begin{cases}
x\gamma + y_1 = 0, \\
\delta x^{-1} + z_2 = 0,
\end{cases}
\]
and
\[
(3.15) \quad \alpha' = \alpha + \gamma \delta.
\]
System (3.14) has a solution \((x, y_1, z_2) = (1, -\gamma, -\delta)\). Equation (3.15) shows that \( \alpha' \) is uniquely determined by \( A \).
Next, assume $\beta = 0$ and $\eta \neq 0$. Then

\[
\text{LHS of (3.13)} = \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}
\]

if and only if

\[
\begin{align*}
\alpha + x\gamma z_2 + y_1 = 0, \\
\delta x^{-1} + d\eta x^{-1} + z_2 &= 0, \\
\eta x^{-1} &= 1.
\end{align*}
\] (3.16)

System (3.16) has a solution $(d, x, y_1, y_2, z_2)$. (Let $d$ be arbitrary. Solve for $x$ from the last equation, $y_1$ from the first equation, $z_2$ from the third equation, and $y_2$ from the second equation.)

Finally, assume $\beta \neq 0$. Then

\[
\text{LHS of (3.13)} = \begin{bmatrix} 1 & 0 \\ 0 & \eta' \end{bmatrix}
\]

if and only if

\[
\begin{align*}
x\beta &= 1, \\
-x\beta d + x\gamma + y_1 &= 0, \\
\alpha + x\beta z_1 + x\gamma z_2 + y_1 + y_2 &= 0, \\
\delta x^{-1} + d\eta x^{-1} + z_2 &= 0,
\end{align*}
\] (3.17)

and

\[
\eta' = \eta \beta.
\] (3.18)

System (3.17) has a solution $(d, x, y_1, y_2, z_1, z_2)$. (Let $y_1$ and $y_2$ be arbitrary. Solve for $x$ from the first equation, $d$ from the second equation, $z_2$ from the last equation, and $z_1$ from the third equation.) Equation (3.18) shows that $\eta'$ is uniquely determined by $A$. \hfill \Box

### 3.7. Classification of $\Lambda$-modules of order $p^n$, $n \leq 4$.

The classification of $\Lambda$-modules of order $p^n$, $n \leq 4$, is obtained by combining the results in 3.2 – 3.6 and using Theorem 2.1. A complete description of the classification is given in Table III in the appendix. From Table III we find that the number of nonisomorphic $\Lambda$-modules of order $p^n$ is

\[
\begin{align*}
1 & \quad \text{if } n = 0, \\
p - 1 & \quad \text{if } n = 1, \\
2p^2 - p - 1 & \quad \text{if } n = 2, \\
3p^3 - 2p^2 - 1 & \quad \text{if } n = 3, \\
5p^4 - 2p^3 - 2p - 1 & \quad \text{if } n = 4.
\end{align*}
\] (3.19)
4. Finite Alexander Quandles

By Theorem 1.1, the classification of finite Alexander quandles $M$ is the same as the classification of finite $\Lambda$-modules of the form $(1 - t)M$. First, the following question has to be answered: Given a finite $\Lambda$-module $N$ and an integer $l > 0$, does there exist a $\Lambda$-module $M \supset N$ such that $(1 - t)M = N$ and $|M/N| = l$? Assume that such an $M$ exists. Since

$$M/(1 - t)M \xrightarrow{1 - t} (1 - t)M/(1 - t)^2M = N/(1 - t)N$$

is an onto $\Lambda$-map, we have $|N/(1 - t)N| \mid l$. We will see in Theorem 4.3 that $|N/(1 - t)N| \mid l$ is also a sufficient condition for the existence of $M$.

**Lemma 4.1.** Let $N \subset M$ be abelian groups and let $\alpha : N \to N$ and $\overline{\alpha} : M \to N$ be $\mathbb{Z}$-maps such that $\overline{\alpha}|_N = \alpha$. If $1 - \alpha \in \text{Aut}(N)$, then $1 - \overline{\alpha} \in \text{Aut}(M)$.

**Proof.** We first show that $1 - \overline{\alpha}$ is 1-1. Let $x \in \ker(1 - \overline{\alpha})$. Then

$$0 = \overline{\alpha}(0) = \overline{\alpha}(x - \overline{\alpha}(x)) = \overline{\alpha}(x) - \alpha(\overline{\alpha}(x)) = (1 - \alpha)(\overline{\alpha}(x)).$$

Since $1 - \alpha \in \text{Aut}(N)$, we have $\overline{\alpha}(x) = 0$. Thus $x = [(1 - \overline{\alpha}) + \overline{\alpha}](x) = 0$.

Now we show that $1 - \overline{\alpha} : M \to M$ is onto. Let $y \in M$. Since $\overline{\alpha}(y) \in N$ and $1 - \alpha \in \text{Aut}(N)$, there exists $x \in N$ such that $(1 - \alpha)(x) = \overline{\alpha}(y)$. Then $y = y - \overline{\alpha}(y) + x - \alpha(x) = (1 - \overline{\alpha})(y + x)$.

**Theorem 4.2.** Let $N$ be a finite abelian group and $\alpha \in \text{End}_\mathbb{Z}(N)$. Then there exist a finite abelian group $M \supset N$ with $|M/N| = |N/\alpha(N)|$ and an onto homomorphism $\overline{\alpha} : M \to N$ such that $\overline{\alpha}|_N = \alpha$.

**Proof.** We may assume that $N$ is a finite abelian $p$-group. If $\alpha(N) = N$, there is nothing to prove. So assume $\alpha(N) \neq N$. Let $|N/\alpha(N)| = p^k$ and $\text{rank } N = r$ (the number of cyclic summands in a decomposition of $N$). We will inductively construct finite abelian $p$-groups $N = M_0 \subset M_1 \subset \cdots \subset M_k$ and $\mathbb{Z}$-maps $\alpha_i : M_i \to N$, $0 \leq i \leq k$, such that $\alpha_0 = \alpha$, $|M_{i+1}/M_i| = |\alpha_{i+1}(M_{i+1})/\alpha_i(M_i)| = p$, rank $M_i = r$, and $\alpha_{i+1}|_{M_i} = \alpha_i$. Then $M = M_k$ and $\overline{\alpha} = \alpha_k$ have the desired property.
Let $0 \leq i < k$ and assume that $M_i$ and $\alpha_i$ have been constructed. We now construct $M_{i+1}$ and $\alpha_{i+1}$.

We claim that the mapping $M_i/pM_i \to \mathbb{N}/p\mathbb{N}$ induced by $\alpha_i$ is not 1-1. Otherwise, since $|M_i/pM_i| = p^r = |\mathbb{N}/p\mathbb{N}|$, the mapping is also onto. Then for each $x \in \mathbb{N}$, there exist $y_0 \in M_i$ and $x_0 \in \mathbb{N}$ such that

$$x = \alpha_i(y_0) + px_0.$$ 

In the same way, $x_0 = \alpha_i(y_1) + px_1$ for some $y_1 \in M_i$ and $x_1 \in \mathbb{N}$. Continuing this way, we can write

$$x = \alpha_i(y_0) + p\alpha_i(y_1) + \cdots + p^{n+1}x_n, \quad y_0, \ldots, y_n \in M_i, \quad x_n \in \mathbb{N}.$$ 

Choose $n$ large enough such that $p^{n+1}x_n = 0$. Then $x = \alpha_i(y_0 + py_1 + \cdots + p^ny_n) \in \alpha_i(M_i)$. So $N = \alpha_i(M_i)$, which is a contradiction since $|\alpha_i(M_i)/\alpha_i(N)| = p^i < p^k = |N/\alpha_i(N)|$.

By the above claim, there exists $a \in M_i \setminus pM_i$ such that $\alpha_i(a) \in p\mathbb{N}$. Write $\alpha_i(a) = pb$ for some $b \in \mathbb{N}$.

**Case 1.** Assume $b \notin \alpha_i(M_i)$. Write $M_i = \mathbb{Z}_{p^{e_1}} \times \cdots \times \mathbb{Z}_{p^{e_r}}$, $e_1 \geq \cdots \geq e_r > 0$. Since $a \in M_i \setminus pM_i$, we may assume $a = (pw, 1, 0)$, where $w \in \mathbb{Z}_{p^{e_1}} \times \cdots \times \mathbb{Z}_{p^{e_{r-1}}}$ for some $0 \leq s < r$. Let $M_{i+1} = A \times \mathbb{Z}_{p^{e_s+1}} \times B$ where $A = \mathbb{Z}_{p^{e_1}} \times \cdots \times \mathbb{Z}_{p^{e_{s-1}}}$, $B = \mathbb{Z}_{p^{e_{s+1}}} \times \cdots \times \mathbb{Z}_{p^{e_r}}$. Define $\mathbb{Z}$-maps

$$\begin{align*}
\iota : M_i &= A \times \mathbb{Z}_{p^{e_s}} \times B & \rightarrow & M_{i+1} &= A \times \mathbb{Z}_{p^{e_s+1}} \times B \\
(x, y, z) &\quad \mapsto & (x, py, z) \\
\alpha_{i+1} : M_{i+1} &= A \times \mathbb{Z}_{p^{e_s+1}} \times B & \rightarrow & \mathbb{N}
\end{align*}$$

Then $\iota$ is 1-1, $\alpha_{i+1} = \alpha_i$, and $|M_{i+1}/M_i| = p = |\alpha_{i+1}(M_{i+1})/\alpha_i(M_i)|$.

**Case 2.** Assume $b \in \alpha_i(M_i)$, say, $b = \alpha_i(c)$, $c \in M_i$. Then $\alpha_i(a) = p\alpha_i(c)$. Let $a_1 = a - pc$. Then $a_1 \in M_i \setminus pM_i$ and $\alpha_i(a_1) = 0$. Choose $b' \in \mathbb{N} \setminus \alpha_i(M_i)$ such that $pb' \in \alpha_i(M_i)$. Write $pb' = \alpha_i(d)$, $d \in M_i$. Choose $\epsilon = 0$ or 1 such that $a' := d + \epsilon a_1 \notin pM_i$. Then $\alpha_i(a') = pb'$. Now we are in Case 1 with $a', b'$ in place of $a, b$, respectively. \qed

**Theorem 4.3.** Let $N$ be a finite $\Lambda$-module with $|N/(1-t)N| = l$. Then there exists a finite $\Lambda$-module $M \supset N$ with $|M/N| = l$ and $(1-t)M = N$.

**Proof.** Let $\alpha = 1-t \in \text{End}_2(N)$. By Theorem 4.2 there exist a finite abelian group $M \supset N$ and an onto $\mathbb{Z}$-map $\overline{\alpha} : M \to N$ such that $\overline{\alpha}|_N = \alpha$ and $|M/N| = |N/\alpha(N)|$. Since $1 - \alpha \in \text{Aut}_2(N)$, by Lemma 4.1 $1 - \overline{\alpha} \in \text{Aut}_2(M)$. Make $M$ into a $\Lambda$-module by defining

$$tx = (1 - \overline{\alpha})(x), \quad x \in M.$$ 

Then $\Lambda N$ is a submodule of $\Lambda M$ and $(1-t)M = \overline{\alpha}(M) = N$. \qed

**Corollary 4.4.** Let $p$ be a prime and $n$ a positive integer. Let $\mathcal{M}_{p^n}$ be a complete set of nonisomorphic $\Lambda$-modules $N$ such that $|N| = p^j$, $|(1-t)N| = p^j$, $2i - j \leq n$. For each $N \in \mathcal{M}_{p^n}$, let $M_N \supset N$ be a $\Lambda$-module with $|M_N| = p^n$ and $(1-t)M_N = N$. (The existence of $M_N$ is $M_N$ is guaranteed by Theorem 4.3) Then $\{ (M_N, *) : N \in \mathcal{M}_{p^n} \}$ is a complete set of nonisomorphic Alexander quandles of order $p^n$. \qed
Proof. Given a $\Lambda$-module $N$ with $|N| = p^i$ and $|(1 - t)N| = p^j$, it follows from Theorem 4.3 that $n \geq 2i - j$ is a necessary and sufficient condition on $n$ for which there exists a $\Lambda$-module $M \supset N$ with $|M| = p^n$ and $(1 - t)M = N$. Now the conclusion in the corollary follows from Theorem 1.1. $\square$

The $\Lambda$-modules in $\mathcal{M}_{p^n}, n \leq 4$, are contained in Table 1; to save space, we will not enumerate these modules separately. From Table 1 we find that the number of nonisomorphic Alexander quandles of order $p^n$ ($n \leq 4$) is

$$\begin{cases} 1 & \text{if } n = 0, \\ p - 1 & \text{if } n = 1, \\ 2p^2 - 2p - 1 & \text{if } n = 2, \\ 3p^3 - 4p^2 + p - 3 & \text{if } n = 3, \\ 5p^4 - 6p^3 + p^2 - 6p - 1 & \text{if } n = 4. \end{cases}$$ (4.1)

The number of nonisomorphic connected Alexander quandles of order $p^n$ ($n \leq 4$), also from Table 1, is

$$\begin{cases} 1 & \text{if } n = 0, \\ p - 2 & \text{if } n = 1, \\ 2p^2 - 3p - 1 & \text{if } n = 2, \\ 3p^3 - 6p^2 + p & \text{if } n = 3, \\ 5p^4 - 9p^3 + p^2 - 2p + 1 & \text{if } n = 4. \end{cases}$$ (4.2)

Remark.

(i) (4.1) agrees with the numbers of nonisomorphic Alexander quandles of order $\leq 15$ in [8].
(ii) (4.2) with $n = 2$ agrees with the results of [3, 8]; (4.2) with $p^n = 2^4$ agrees with the number in [7].
(iii) [7] stated that the number of nonisomorphic Alexander quandles of order 16 is 24. Our result (4.1) with $p^n = 2^4$ is 23. It appears that the two Alexander quandles in [7] with $\text{Im}(\text{Id} - \phi) = \mathbb{Z}_4 \oplus \mathbb{Z}_2$ (notation of [7]) are isomorphic. Professor W. E. Clark computed the numbers of nonisomorphic quandles of order $p^n < 2^8$ using a computer program; his results (with $n \leq 4$) agree with (4.1).

APPENDIX: Table

Table 1. Nonisomorphic $\Lambda$-modules of order $p^n$, $n \leq 4$

| $n = 0$ | $(M, +)$ | matrix of $t$ | $|(1-t)M|$ | number | total |
|---|---|---|---|---|---|
| 0 | [0] | 1 | 1 | 1 |

| $n = 1$ | $(M, +)$ | matrix of $t$ | $|(1-t)M|$ | number | total |
|---|---|---|---|---|---|
| $\mathbb{Z}_p$ | $[b], b \in \mathbb{Z}_p^\times$ | $p^0$ if $b = 1$ | $p^1$ if $b \neq 1$ | 1 | $p - 1$ |
FINITE MODULES OVER $\mathbb{Z}[t,t^{-1}]$

ACKNOWLEDGMENT

I thank Professor W. Edwin Clark for sharing his computational results on the numbers of nonisomorphic Alexander quandles.

REFERENCES

[1] S. Carter, S. Kamada, M. Saito, *Surfaces in 4-Space*, Encyclopaedia of Mathematical Sciences, 142. Low-Dimensional Topology, III. Springer-Verlag, Berlin, 2004.

[2] W. E. Clark, M. Elhamdadi, X. Hou, M. Saito, T. Yeatman *Connected quandles associated with pointed abelian groups*, preprint.

[3] M. Graña, *Indecomposable racks of order $p^2$*, Beiträge Algebra Geom. 45 (2004), 665 - 676.

[4] C. J. Hillar and D. L. Rhea, *Automorphisms of finite abelian groups*, Amer. Math. Monthly 114 (2007), 917 - 923.

[5] R. A. Horn and C. R. Johnson, *Topics in Matrix Analysis*, Cambridge University Press, Cambridge, 1991.

[6] G. Murillo and S. Nelson, *Alexander quandles of order 16*, J. Knot Theory Ramifications 17 (2008), 273 - 278.

[7] G. Murillo and S. Nelson, *Erratum: Alexander quandles of order 16*, J. Knot Theory Ramifications 18 (2009), 727.

[8] S. Nelson, *Classification of finite Alexander quandles*, Topology Proc. 27 (2003), 245 - 258.

[9] A. Ranum, *The group of classes of congruent matrices with application to the group of isomorphisms of any abelian group*, Trans. Amer. Math. Soc. 8 (1907), 71 - 91.

DEPARTMENT OF MATHEMATICS AND STATISTICS, UNIVERSITY OF SOUTH FLORIDA, TAMPA, FL 33620

E-mail address: xhou@usf.edu
| $n = 2$ | (M,+) | matrix of t | $| (1-t)M |$ | number | total |
|---|---|---|---|---|---|
| $\mathbb{Z}_p^2$ | $[b]$, $b \in \mathbb{Z}_p^\times$ | $p^0$ if $b = 1$ | 1 | $p^2 - p$ |
| $\mathbb{Z}_p^2$ | $\begin{bmatrix} b \\ c \end{bmatrix}$, $0 < b \leq c < p$ | $p^0$ if $b = c = 1$ | 1 | $(p)_2$ |
| $\mathbb{Z}_p^2$ | $\begin{bmatrix} b_c \\ 1 \end{bmatrix}$, $b \in \mathbb{Z}_p^\times$ | $p^1$ if $b = 1$ | 1 | $p - 1$ |
| $\mathbb{Z}_p^2$ | $\begin{bmatrix} 0 \\ -b_0 \\ -b_1 \end{bmatrix}$, $X^2 + b_1 X + b_0 \in \mathbb{Z}_p[X]$ irr | $p^2$ | $\frac{1}{2}(p^2 - p)$ | $\frac{1}{2}(p^2 - p)$ |

| $n = 3$ | (M,+) | matrix of t | $| (1-t)M |$ | number | total |
|---|---|---|---|---|---|
| $\mathbb{Z}_p^3$ | $[b]$, $b \in \mathbb{Z}_p^\times$ | $p^0$ if $b = 1$ | 1 | $p^3 - p^2$ |
| | | $p^1$ if $b \neq 1$, $b \equiv 1 (p)$ | $p - 1$ | |
| | | $p^2$ if $b \neq 1$ ($p^2$), $b \equiv 1 (p)$ | $p(p - 1)$ | |
| | | $p^3$ if $b \neq 1$ ($p$) | $p^3(p - 2)$ | |
| $\mathbb{Z}_p^2 \times \mathbb{Z}_p$ | $\begin{bmatrix} b_c \\ c \end{bmatrix}$, $b \in \mathbb{Z}_p^\times$, $c \in \mathbb{Z}_p^\times$ | $p^0$ if $b = 1$, $c = 1$ | 1 | $p(p - 1)^2$ |
| | | $p^1$ if $b \neq 1$, $b \equiv 1 (p)$, $c = 1$ | $2p - 3$ | |
| | | or $b = 1$, $c \neq 1$ | | |
| | | $p^2$ if $b \neq 1$ ($p$), $c = 1$ | | |
| | | or $b \neq 1$, $b \equiv 1 (p)$, $c \neq 1$ | $(p - 2)(2p - 1)$ | |
| | | $p^3$ if $b \neq 1$ ($p$), $c \neq 1$ | $p(p - 2)^2$ | |
Table 1. Nonisomorphic $\Lambda$-modules of order $p^n$, $n \leq 4$ (continued)

| $(M, +)$ | matrix of $t$ | $|(1 - t)M|$ | number | total |
|----------|---------------|--------------|--------|-------|
| $\mathbb{Z}_p \times \mathbb{Z}_p$ | $\begin{bmatrix} b & 0 \\ 1 & b \end{bmatrix}$, $0 < b < p$ | $p^1$ if $b = 1$ | 1 | $p - 1$ |
| | | $p^3$ if $b \neq 1$ | | |
| $\mathbb{Z}_p \times \mathbb{Z}_p$ | $\begin{bmatrix} b & p \\ \gamma & b \end{bmatrix}$, $0 < b < p$, $\gamma \in \mathbb{Z}_p$ | $p^1$ if $b = 1$, $\gamma = 0$ | 1 | $p(p - 1)$ |
| | | $p^2$ if $b = 1$, $\gamma \neq 0$ | $p - 1$ | |
| | | $p^3$ if $b \neq 1$ | | $p(p - 2)$ |
| $\mathbb{Z}_p^3$ | $\begin{bmatrix} b & c & d \end{bmatrix}$, $0 < b \leq c \leq d < p$ | $p^0$ if $b = c = d = 1$ | 1 | $(p+1)/3$ |
| | | $p^1$ if $b = c = 1 < d$ | $p - 2$ | |
| | | $p^2$ if $b = 1 < c$ | $(p-1)/2$ | |
| | | $p^3$ if $b > 1$ | $(p-1)/3$ | |
| $\mathbb{Z}_p^3$ | $\begin{bmatrix} b & 1 & b \\ 1 & c \end{bmatrix}$, $b, c \in \mathbb{Z}_p^\times$ | $p^1$ if $b = c = 1$ | 1 | $(p-1)^2$ |
| | | $p^2$ if $b = 1$, $c \neq 1$ | $2(p-2)$ | |
| | | or $b \neq 1$, $c = 1$ | | |
| | | $p^3$ if $b \neq 1$, $c \neq 1$ | $(p-2)^2$ | |
| $\mathbb{Z}_p^3$ | $\begin{bmatrix} b & 1 & b \\ 1 & b \end{bmatrix}$, $b \in \mathbb{Z}_p^\times$ | $p^1$ if $b = 1$ | 1 | $p - 1$ |
| | | $p^3$ if $b \neq 1$ | $p - 2$ | |
| $\mathbb{Z}_p^3$ | $\begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ -b_0 & -b_1 & -b_2 \end{bmatrix}$, $X^3 + b_2X^2 + b_1X + b_0 \in \mathbb{Z}_p[X]$ irr | $p^3$ | $1/(3)(p^3 - p)$ | $1/(3)(p^3 - p)$ |
| | | | | |
| $\mathbb{Z}_p^3$ | $\begin{bmatrix} 0 & 1 & c \\ -b_0 & -b_1 & c \end{bmatrix}$, $X^2 + b_1X + b_0 \in \mathbb{Z}_p[X]$ irr, $c \in \mathbb{Z}_p^\times$ | $p^2$ if $c = 1$ | $1/(2)(p^2 - p)$ | $1/(2)(p^2 - p)(p - 2)$ |
| | | | $p^3$ if $c \neq 1$ | | |
Table 1. Nonisomorphic $\Lambda$-modules of order $p^n$, $n \leq 4$ (continued)

| $n = 4$ | matrix of $t$ | $(1-t)M$ | number | total |
| --- | --- | --- | --- | --- |
| $(M, +)$ | | | | |
| $\mathbb{Z}_{p^4}$ | $[b], \ b \in \mathbb{Z}_{p^4}^\times$ | $p^0$ if $b = 1$ | 1 | $p^3(p-1)$ |
| | | $p^1$ if $b \neq 1, \ b \equiv 1 (p^r)$ | | |
| | | $p^2$ if $b \neq 1 (p^r), \ b \equiv 1 (p^2)$ | | |
| | | $p^3$ if $b \neq 1 (p^r), \ b \equiv 1 (p)$ | | |
| | | $p^4$ if $b \neq 1 (p)$ | | |
| $\mathbb{Z}_{p^3} \times \mathbb{Z}_p$ | $\left[ \begin{array}{c} b \\ c \end{array} \right], \ b \in \mathbb{Z}_{p^3}^\times, \ c \in \mathbb{Z}_p^\times$ | $p^0$ if $b = 1, \ c = 1$ | 1 | |
| | | $p^1$ if $b \neq 1, \ b \equiv 1 (p^2), \ c = 1$ | | |
| | | or $b = 1, \ c \neq 1$ | | |
| | | $p^2$ if $b \neq 1 (p^2), \ b \equiv 1 (p), \ c = 1$ | | |
| | | or $b \neq 1, \ b \equiv 1 (p^2), \ c \neq 1$ | | |
| | | $p^3$ if $b \equiv 1 (p), \ c = 1$ | | |
| | | or $b \neq 1 (p^2), \ b \equiv 1 (p), \ c \neq 1$ | | |
| | | $p^4$ if $b \neq 1 (p), \ c \neq 1$ | | |
| $\mathbb{Z}_{p^3} \times \mathbb{Z}_p$ | $\left[ \begin{array}{c} b \\ 0 \\ 1 \end{array} \right], \ 0 < b < p^2, \ b \neq 0 (p)$ | $p^1$ if $b = 1$ | 1 | $p(p-1)$ |
| | | $p^2$ if $b \neq 1, \ b \equiv 1 (p)$ | | |
| | | $p^3$ if $b \neq 1 (p)$ | | |
| | | $p^4$ if $b \equiv 1 (p)$ | | |
| $\mathbb{Z}_{p^3} \times \mathbb{Z}_p$ | $\left[ \begin{array}{c} b \\ c \end{array} \right], \ 0 < b < p^2, \ b \neq 0 (p), \ \gamma \in \mathbb{Z}_p$ | $p^0$ if $b = c = 1$ | 1 | $p^2(p-1)$ |
| | | $p^1$ if $b = 1, \ c = 0$ | | |
| | | $p^2$ if $b \neq 1, \ b \equiv 1 (p)$ | | |
| | | or $b = 1, \ c \neq 0$ | | |
| $\mathbb{Z}_{p^2}^2$ | $\left[ \begin{array}{c} b \\ c \end{array} \right], \ 0 < b \leq c < p^2$ | $p^0$ if $b = c = 1$ | 1 | $(p(p-1)+1)(p(p-2)/2)$ |
| | | $p^1$ if $b = 1 < c, \ b \equiv 1 (p)$ | | |
| | | or $b, c \neq 1, \ b, c \equiv 1 (p)$ | | |
| | | $p^2$ if $b = 1, \ c \neq 1 (p)$ | | |
| | | or $b, c \neq 1, \ b, c \equiv 1 (p)$ | | |
| | | $p^3$ if $\{b, c\} = \{b_1, c_1\}, \ b_1 \neq 1 (p), \ c_1 \neq 1, \ c_1 \equiv 1 (p)$ | | |
| | | $p^4$ if $b, c \neq 1 (p)$ | | |
| $\mathbb{Z}_{p^2}^2$ | $\left[ \begin{array}{c} b \\ 0 \\ p \\ b \end{array} \right], \ b \in \mathbb{Z}_{p^2}^\times$ | $p^0$ if $b = 1$ | 1 | $p(p-1)$ |
| | | $p^1$ if $b \neq 1, \ b \equiv 1 (p)$ | | |
| | | $p^2$ if $b \neq 1 (p)$ | | |
Table 1. Nonisomorphic \( \Lambda \)-modules of order \( p^n \), \( n \leq 4 \) (continued)

| \((M,+)\) | matrix of \( t \) | \(|(1-t)M|\) | number | total |
|---------|-----------------|-------------|--------|-------|
| \( \mathbb{Z}_p^2 \) | \[
\begin{bmatrix}
 b & p \\
 -p & -b
\end{bmatrix}, \quad 0 < b < p, \\
X^2 + b_1X + b_0 \in \mathbb{Z}_p[X] \text{ irr}
\] | \( p^2 \) if \( b = 1 \) | \( \frac{1}{2}(p^2 - p) \) | \( \frac{1}{2}p(p-1)^2 \) |
| \( \mathbb{Z}_p^2 \) | \[
\begin{bmatrix}
 b + p\alpha & 1 \\
 p\gamma & b
\end{bmatrix}, \quad 0 < b < p, \alpha,\gamma \in \mathbb{Z}_p
\] | \( p^4 \) if \( b = 1, \gamma = 0 \) | \( p \) | \( p^2(p-1) \) |
| \( \mathbb{Z}_p^2 \) | \[
\begin{bmatrix}
 p\alpha & 1 + p\beta \\
 -p & -b_1
\end{bmatrix}, \quad \alpha,\beta \in \mathbb{Z}_p, \ 0 \leq b_0,b_1 < p \\
X^2 + b_1X + b_0 \in \mathbb{Z}_p[X] \text{ irr}
\] | \( p^4 \) | \( \frac{1}{2}p^2(p^2 - p) \) | \( \frac{1}{2}p^2(p^2 - p) \) |
| \( \mathbb{Z}_p^2 \times \mathbb{Z}_p^2 \) | \[
\begin{bmatrix}
 b & c \\
 c & d
\end{bmatrix}, \quad b \in \mathbb{Z}_p^\times, \ 0 < c \leq d < p
\] | \( p^4 \) if \( b = 1, c = d = 1 \) | 1 | \( \frac{1}{2}p^2(p^2 - p) \) |
| \( \mathbb{Z}_p^2 \times \mathbb{Z}_p^2 \) | \[
\begin{bmatrix}
 b & 0 & 0 \\
 0 & 0 & c
\end{bmatrix}, \quad 0 < b < p, \ c \in \mathbb{Z}_p^\times
\] | \( p^4 \) if \( b = 1, c = 1 \) | 1 | \( (p-1)^2 \) |
| \( \mathbb{Z}_p^2 \times \mathbb{Z}_p^2 \) | \[
\begin{bmatrix}
 b & 0 & 0 \\
 0 & b & 0
\end{bmatrix}, \quad 0 < b < p, \ \eta \in \mathbb{Z}_p
\] | \( p^4 \) if \( b = 1, \eta = 0 \) | 1 | \( p(p-1) \) |
| \( \mathbb{Z}_p^2 \times \mathbb{Z}_p^2 \) | \[
\begin{bmatrix}
 b & 0 & 0 \\
 1 & b & 0
\end{bmatrix}, \quad 0 < b < p
\] | \( p^4 \) if \( b = 1, \eta \neq 1 \) | \( p-2 \) | \( p(p-2) \) |
| \( \mathbb{Z}_p^2 \times \mathbb{Z}_p^2 \) | \[
\begin{bmatrix}
 b & 0 & 0 \\
 1 & b & 0
\end{bmatrix}, \quad 0 < b < p
\] | \( p^2 \) if \( b = 1 \) | 1 | \( p-1 \) |
| \( \mathbb{Z}_p^2 \times \mathbb{Z}_p^2 \) | \[
\begin{bmatrix}
 b & 0 & 0 \\
 1 & b & 0
\end{bmatrix}, \quad 0 < b < p
\] | \( p^4 \) if \( b = 1 \) | 1 | \( p-2 \) |
### Table 1. Nonisomorphic \(\Lambda\)-modules of order \(p^n\), \(n \leq 4\) (continued)

| \((\mathbb{Z}_p^2 \times \mathbb{Z}_p^2, +)\) | matrix of \(t\) | \((1-t)\mathbb{M}\) | number | total |
|--------------------------------|-----------------|-----------------|--------|-------|
| \(\mathbb{Z}_p^2 \times \mathbb{Z}_p^2\) | \[
\begin{bmatrix}
  b & c \\
  c & 1 \\
\end{bmatrix}, \ b \in \mathbb{Z}_p^2, \ c \in \mathbb{Z}_p^2
\] | \(p^2\) if \(b = 1, c = 1\) | 1 | \(p(p-1)^2\) |
| | | \(p^2\) if \(b \neq 1, b \equiv 1 (p), c = 1\) | | |
| | | \(p^2\) if \(b \neq 1, b \equiv 1 (p), c \neq 1\) | | |
| | | \((p-2)(2p-1)\) | | |
| \(\mathbb{Z}_p^2 \times \mathbb{Z}_p^2\) | \[
\begin{bmatrix}
  b & 0 & 0 \\
  0 & b & 1 \\
  1 & 0 & b
\end{bmatrix}, \ 0 < b < p
\] | \(p^2\) if \(b = 1\) | 1 | \(p-1\) |
| | | \(p^4\) if \(b \neq 1\) | | \(p-2\) |
| \(\mathbb{Z}_p^2 \times \mathbb{Z}_p^2\) | \[
\begin{bmatrix}
  b & p & 0 \\
  0 & b & 1 \\
  \eta & 0 & b
\end{bmatrix}, \ 0 < b < p, \ \eta \in \mathbb{Z}_p
\] | \(p^2\) if \(b = 1, \ \eta = 0\) | 1 | \(p(p-1)\) |
| | | \(p^3\) if \(b = 1, \ \eta \neq 0\) | | \(p-1\) |
| | | \(p^4\) if \(b \neq 1\) | | \(p(p-2)\) |
| | | \((p+2)^2\) | | |
| \(\mathbb{Z}_p^4\) | \[
\begin{bmatrix}
  b & c & d \\
  c & d & e
\end{bmatrix}, \ 0 < b \leq c \leq d \leq e < p
\] | \(p^3\) if \(b = c = d = e = 1\) | 1 | \((p+2)^2\) |
| | | \(p^4\) if \(b = c = d = 1 < e\) | | \(p-2\) |
| | | \(p^4\) if \(b = c = 1 < d\) | | \((p+1)^2\) |
| | | \(p^4\) if \(b = 1 < c\) | | \((p+1)^2\) |
| | | \(p^4\) if \(b > 1\) | | \((p+1)^2\) |
| \(\mathbb{Z}_p^4\) | \[
\begin{bmatrix}
  b & 1 & c \\
  b & c & d
\end{bmatrix}, \ b \in \mathbb{Z}_p^4, \ 0 < c \leq d < p
\] | \(p^4\) if \(b = 1, c = d = 1\) | 1 | \((p+2)^2\) |
| | | \(p^4\) if \(b \neq 1, c = d = 1\) | | \((p+2)^2\) |
| | | \(p^4\) if \(b \neq 1, c = 1 < d\) | | \((p+1)^2\) |
| | | \(p^4\) if \(b = 1, c > 1\) | | \((p+1)^2\) |
| | | \(p^4\) if \(b \neq 1, c > 1\) | | \((p+1)^2\) |
| | | \(p^4\) if \(b = c = 1\) | | 1 |
| | | \(p^4\) if \(b = 1 < c\) | | \(p-2\) |
| | | \(p^4\) if \(b > 1\) | | \((p-1)^2\) |
| | | \((p+2)^2\) | | |
| \(\mathbb{Z}_p^4\) | \[
\begin{bmatrix}
  b & 1 & \eta \\
  b & \eta & c
\end{bmatrix}, \ 0 < b \leq c < p
\] | \(p^2\) if \(b = c = 1\) | 1 | \((p+2)^2\) |
| | | \(p^3\) if \(b = 1 < c\) | | \((p+2)^2\) |
| | | \(p^4\) if \(b > 1\) | | \((p-1)^2\) |
Table 1. Nonisomorphic \( \Lambda \)-modules of order \( p^n \), \( n \leq 4 \) (continued)

| \((M,+)\) | matrix of \( t \) | \(|(1-t)M|\) | number | total |
|---|---|---|---|---|
| \( \mathbb{Z}_p^4 \) | \[
\begin{bmatrix}
 b & 1 \\
 b & 1 \\
 b & c
\end{bmatrix}, \ b, c \in \mathbb{Z}_p^\times 
\] | \( p^2 \) if \( b = c = 1 \) | \( p^2 \) if \( b = c = 1 \) | \( 1 \) | \( (p-1)^2 \) |
| \( \mathbb{Z}_p^4 \) | \[
\begin{bmatrix}
 b & 1 \\
 b & 1 \\
 b & 1 \\
 b & 1
\end{bmatrix}, \ b \in \mathbb{Z}_p^\times 
\] | \( p^3 \) if \( b = 1 \) | \( p^4 \) if \( b \neq 1 \) | \( 1 \) | \( p-1 \) |
| \( \mathbb{Z}_p^4 \) | \[
\begin{bmatrix}
 0 & 1 \\
 -b_0 & -b_1 \\
 0 & 1 \\
 -c_0 & -c_1
\end{bmatrix}, \ X^2 + b_1X + b_0, \ X^2 + c_1X + c_0 \in \mathbb{Z}_p[X] \text{ irr} \\
(0, b_0) \leq (c_0, c_1) \text{ (*)} 
\] | \( p^4 \) | \( \frac{1}{4}(p^2 - p) \) | \( \frac{1}{4}(p^2 - p) \) | \( \frac{1}{4}(p^2 - p) \) |
| \( \mathbb{Z}_p^4 \) | \[
\begin{bmatrix}
 0 & 1 & 1 & 0 \\
 -b_0 & -b_1 & 0 & 1 \\
 -b_0 & -b_1 & 0 & 1 \\
 -b_0 & -b_1 & -b_2 & -b_3
\end{bmatrix}, \ X^2 + b_1X + b_0 \in \mathbb{Z}_p[X] \text{ irr} 
\] | \( p^4 \) | \( \frac{1}{4}(p^4 - p^2) \) | \( \frac{1}{4}(p^4 - p^2) \) | \( \frac{1}{4}(p^4 - p^2) \) |

(*) \leq \text{ is a total order in } \mathbb{Z}_p^2
Table 1. Nonisomorphic $\Lambda$-modules of order $p^n$, $n \leq 4$ (continued)

| $(M, +)$ | matrix of $t$ | $|(1-t)M|$ | number | total |
|----------|--------------|-------------|--------|-------|
| $\mathbb{Z}_p \times \mathbb{Z}_p^2$ | $\begin{bmatrix} b & p \\ \gamma & b \\ c \end{bmatrix}$, $0 < b < p$, $\gamma \in \mathbb{Z}_p$, $c \in \mathbb{Z}_p^\times$, $b \neq c$ (p) | $p^2$ if $b = 1$, $\gamma = 0$, $c \neq 1$ | $p - 2$ | $p(p-1)(p-2)$ |
| $\mathbb{Z}_p^4$ | $\begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ -b_0 & -b_1 & -b_2 \\ c \end{bmatrix}$, $X^3 + b_2X^2 + b_1X + b_0 \in \mathbb{Z}_p[X]$ irr, $c \in \mathbb{Z}_p^\times$ | $p^3$ if $c = 1$ | $\frac{1}{3}(p^3 - p)$ | $\frac{1}{3}(p^3 - p)(p - 1)$ |
| $\mathbb{Z}_p^2 \times \mathbb{Z}_p^2$ | $\begin{bmatrix} b \\ 0 & 1 \\ -c_0 & -c_1 \end{bmatrix}$, $b \in \mathbb{Z}_p^\times$, $X^2 + c_1X + c_0 \in \mathbb{Z}_p[X]$ irr | $p^2$ if $b = 1$ | $\frac{1}{2}(p^2 - p)$ | $\frac{1}{2}(p^2 - p)(p - 1)$ |
| $\mathbb{Z}_p^2$ | $\begin{bmatrix} 0 & 1 \\ -b_0 & -b_1 \\ c \\ d \end{bmatrix}$, $X^2 + b_1X + b_0 \in \mathbb{Z}_p[X]$ irr, $0 < c \leq d < p$ | $p^2$ if $c = d = 1$ | $\frac{1}{2}(p^2 - p)$ | $\frac{1}{2}(p^2 - p)(p - 1)$ |
| $\mathbb{Z}_p^2$ | $\begin{bmatrix} b & 1 \\ 0 & b \\ -c_0 & -c_1 \end{bmatrix}$, $b \in \mathbb{Z}_p^\times$, $X^2 + c_1X + c_0 \in \mathbb{Z}_p[X]$ irr | $p^3$ if $b = 1$ | $\frac{1}{2}(p^2 - p)$ | $\frac{1}{2}(p^2 - p)(p - 1)$ |
| $\mathbb{Z}_p^4$ | $\begin{bmatrix} 0 & 1 \\ -b_0 & -b_1 \\ -c_0 & -c_1 \end{bmatrix}$, $X^2 + b_1X + b_0 \in \mathbb{Z}_p[X]$ irr, $0 < c \leq d < p$ | $p^4$ if $c > d$ | $\frac{1}{2}(p^2 - p)(p - 1)^2$ | |