ELSEVIER

Available online at www.sciencedirect.com

SCIENCE DIRECT®

Journal of Algebra 276 (2004) 638–662

JOURNAL OF Algebra

www.elsevier.com/locate/jalgebra

Lattices invariant under the affine general linear group

Kanat Abdukhalikov [1]

Department of Mathematics, University of Dortmund, 44221 Dortmund, Germany

Received 23 May 2003

Available online 15 August 2003

Communicated by Eva Bayer-Fluckiger

Abstract

Integral lattices invariant under the affine group $AGL_m(p^t)$ in its natural permutation module Λ of dimension $n = mt$ are studied. A complete description of such lattices is given. As a consequence we have results on automorphism groups of affine invariant codes over fields and finite residue rings $\mathbb{Z}/p^k\mathbb{Z}$.

Keywords: Lattices; Automorphism groups; Cyclic codes

1. Introduction

Let $\mathbb{F}_{p^n}$ be a finite field of p^n elements, and V be its additive group. For $n = mt$ we consider the affine general linear group $G_m = AGL_m(p^t) = V \cdot GL_m(p^t)$ of V considered as a vector space over the subfield $\mathbb{F}_{p^t} \subseteq \mathbb{F}_{p^n}$ of p^t elements. The group G_m defines a doubly transitive action on V. Define a lattice Λ as the group ring $\mathbb{Z}[V]$ with the standard scalar product. The group G_m acts naturally on Λ by permuting the basis vectors. Our goal is to describe sublattices in Λ invariant under the group G_m.

An important example is that the Barnes–Wall lattices can be very simply realized by this construction (see Section 5).

Any invariant sublattice $\Lambda' \subseteq \Lambda$ of full rank contains $l\Lambda$ for some integer l (one can take $l = \det(\Lambda')$). If $l = p_1^{k_1} \cdots p_r^{k_r}$ is the representation as a product of integer prime numbers,

E-mail address: kanat.abdukhalikov@math.uni-dortmund.de.

[1] On leave from: Institute of Mathematics, Pushkin Str. 125, 480100 Almaty, Kazakhstan.

0021-8693/$ – see front matter
doi:10.1016/S0021-8693(03)00496-4

our problem is reduced to studying G_m-submodules in $\Lambda/p_i^{k_i}\Lambda$. The case $p_i \neq p$ can be described very easily, so one needs to classify invariant submodules in $\Lambda/p^k\Lambda$ for all k. This shows that we need to classify invariant submodules in $\mathbb{Z}_p \otimes_{\mathbb{Z}} \Lambda$ over the ring of p-adic integers $\mathbb{Z}_p$.

We consider the group ring $\mathbb{Z}_p[V]$ in the form

$$A = \left\{ \sum_{v \in V} a_v X^v \;\middle|\; a_v \in \mathbb{Z}_p \right\}.$$

The natural action of the group $G_m = AGL_m(p^t)$ on A is defined as follows:

$$\hat{u}\left(X^v\right) = X^{u+v}, \quad u \in V,$$
$$\hat{g}\left(X^v\right) = X^{gv}, \quad g \in GL_m\left(p^t\right),$$

where we consider V as an m-dimensional vector space over $\mathbb{F}_{p^t}$. Thus the problem of describing the G_m-invariant $\mathbb{Z}_p$-submodules in A is equivalent to the problem of describing the $GL_m(p^t)$-invariant ideals of the ring A.

The very first step is the study of invariant submodules in A/pA over the field $\mathbb{F}_p = \mathbb{Z}_p/p\mathbb{Z}_p$. This situation is studied in coding theory [11,14,15,17]. An extended cyclic code of length p^n (i.e., invariant under $GL_1(p^n)$) is called affine invariant if it is invariant under the group V. They were characterized by Kasami, Lin and Peterson [17]. Later Charpin reproved this result in terms of group algebras [14]. Furthermore, Berger and Charpin proved [11] that the permutation group $Per(C)$ of any affine invariant code is either the symmetric group $Sym(p^n)$, or alternating group $Alt(p^n)$, or satisfies the condition $AGL_m(p^t) \subseteq Per(C) \subseteq A\Gamma L_m(p^t)$ for some m, where $A\Gamma L_m(p^t) = AGL_m(p^t) \cdot Gal(\mathbb{F}_{p^t}/\mathbb{F}_p)$ is the semiaffine general linear group. Moreover, Berger [12] showed that the automorphism group of an affine invariant code C over a field F can be easily constructed from the permutation group. Actually $Aut(C) \cong F^* \times Per(C)$. Therefore, determination of $AGL_m(p^t)$-invariant codes settles the question to calculate the automorphism groups of affine invariant codes. This result due to Delsarte [15]. He gave a necessary and sufficient condition (in terms of defining sets) for affine invariant codes to be invariant under $GL_m(p^t)$. Recently Berger and Charpin [11] found another condition equivalent to those of Delsarte. In Section 3 we give new detailed description of $AGL_m(p^t)$-invariant codes and we use these results in [4,7] to get very simple description of defining sets of such codes.

The algebraic structure of modules over $\mathbb{F}_{p^t}GL_m(p^t)$ is studied in [9]. We need more detailed investigation which is done in Section 3. Permutation modules and lattices for related groups are considered also in [3,19,20].

The description of $\mathbb{Z}_p$-submodules in A gives the description of invariant submodules in A/p^kA over the ring $\mathbb{Z}_p/p^k\mathbb{Z}_p \cong \mathbb{Z}/p^k\mathbb{Z}$. There is growing interest in codes over $\mathbb{Z}/p^k\mathbb{Z}$. In particular, there has been much interest in $\mathbb{Z}/4\mathbb{Z}$ codes as they have been shown to be a systematic way of constructing very good binary codes. For example, the famous Kerdock and Preparata codes are non-linear binary codes that contain more codewords than any comparable linear codes presently known. Recently it was shown [16] that the Kerdock

and Preparata codes can be very simply constructed as binary images under a certain map, called the Gray map, of linear codes over $\mathbb{Z}/4\mathbb{Z}$. This fact stimulated investigations of linear codes over $\mathbb{Z}/4\mathbb{Z}$. The Kerdock and Preparata codes, considered as codes (modules) over $\mathbb{Z}/4\mathbb{Z}$, are analogs of classical Reed–Muller codes: they have dimension (rank) p^n and they are invariant under the affine group G_1.

The description of invariant lattices is given in Section 4, Theorems 4.4, 4.9. The particular cases $m = 1$ and $m = n$ were considered in [5,6] in detail, see also Section 3.4. Similar constructions of lattices were studied in [1,2,13,18]. The results of the Section 4 are used in [4,7] to describe G_m-invariant codes over rings $\mathbb{Z}/p^k\mathbb{Z}$.

2. Preliminaries

The overall strategy of the paper is to replace the prime field $\mathbb{F}_p$ by a splitting field $\mathbb{F}_{p^t}$ of $GL_m(p^t)$, and then get the results over $\mathbb{F}_p$ by Galois descent. Similarly let R_p denote the ring of integers in the unramified extension of the field $\mathbb{Q}_p$ of p-adic numbers with property $R_p/pR_p \cong \mathbb{F}_{p^t}$. So we define

$$\mathcal{A} = \left\{ \sum_{v \in V} a_v X^v \;\middle|\; a_v \in R_p \right\}$$

as R_p-module. The group G_m acts on $\mathcal{A}$.

The Frobenius map σ on $\mathbb{F}_{p^t} \cong R_p/pR_p$ can be extended uniquely to an automorphism of R_p. Then we have

$$A = \{ a \in \mathcal{A} \mid \hat{\sigma}(a) = a \},$$

where the action of σ on $\mathcal{A}$ is defined by

$$\hat{\sigma}\Big(\sum a_v X^v \Big) = \sum \sigma(a_v) X^v.$$

The connection between G_m-invariant R_p-lattices in $\mathcal{A}$ and $\mathbb{Z}_p$-lattices in A will be explained in Lemma 4.8.

3. Submodules over a field

In this section we consider the vector space

$$\mathcal{F} = \left\{ \sum_{v \in V} a_v X^v \;\middle|\; a_v \in \mathbb{F}_q \right\}$$

over the field $\mathbb{F}_q$ of $q = p^t$ elements. Our goal is to describe $\mathbb{F}_q$-subspaces in $\mathcal{F}$ invariant under the group $G_m = AGL_m(q)$. There are two interpretations of elements of $\mathcal{F}$, as functions from V to $\mathbb{F}_q$ and as elements of the group algebra. As a function, an element $\sum a_v X^v$ is the one that assigns a_v to the element v of V. In Sections 3.1 and 3.3 we

describe the structure of $\mathcal{F}$ as functions and as a group algebra respectively. We will see that the function realization is more suitable to study the invariance under the linear group $GL_m(q)$, and the group algebra realization is more appropriate to study the invariance under the group V of affine shifts.

3.1. The structure of the space $\mathcal{F}$ of functions over the affine group

Consider the polynomial functions

$$x_0^{i_0}\cdots x_{m-1}^{i_{m-1}} = \sum_{\alpha_0,\ldots,\alpha_{m-1}\in\mathbb{F}_q} \alpha_0^{i_0}\cdots\alpha_{m-1}^{i_{m-1}} X^{\alpha_0 e_0+\cdots+\alpha_{m-1}e_{m-1}}.$$

Since $\alpha^q=\alpha$ for $\alpha\in\mathbb{F}_q$, the polynomial functions can be reduced modulo $x_s^q - x_s$. The monomials $x_0^{i_0}\cdots x_{m-1}^{i_{m-1}}$, $0\leqslant i_s\leqslant q-1$, $s=0,1,\ldots,m-1$, form a basis of the vector space $\mathcal{F}$ over $\mathbb{F}_q$. In this subsection we are going to describe G_m-invariant subspaces in terms of these basis monomials.

We define the modules

$$\mathcal{M}(\lambda_0,\ldots,\lambda_{t-1}) = \big\langle x_0^{i_{00}+i_{01}p+\cdots+i_{0,t-1}p^{t-1}}\cdots x_{m-1}^{i_{m-1,0}+i_{m-1,1}p+\cdots+i_{m-1,t-1}p^{t-1}} \\ \big|\ i_{0j}+i_{1j}+\cdots+i_{m-1,j}\leqslant\lambda_j,\ j=0,1,\ldots,t-1\big\rangle,$$

where $0\leqslant\lambda_j\leqslant m(p-1)$, $0\leqslant i_{sj}\leqslant m(p-1)$. Note that, in general, the monomials in this definition may not be the basis monomials (but we can reduce them to basis ones). It is easy to see that

$$\mathcal{M}\big(m(p-1),\ldots,m(p-1)\big)=\mathcal{F},$$

$$\mathcal{M}(0,\ldots,0)=\langle 1\rangle,$$

$$\mathcal{M}(\lambda_0,\ldots,\lambda_{t-1})\supseteq\mathcal{M}(\lambda_0,\ldots,\lambda_j-1,\ldots,\lambda_{t-1}).$$

Further, if $i_{sj}>p-1$ for some s, j, then $i_{s0}+\cdots+i_{sj}p^j+\cdots+i_{s,t-1}p^{t-1}=i_{s0}+\cdots+(i_{sj}-p)p^j+(i_{s,j+1}+1)p^{j+1}\cdots+i_{s,t-1}p^{t-1}$, so

$$\mathcal{M}(\lambda_0,\ldots,\lambda_{t-1})\supseteq\mathcal{M}(\lambda_0,\ldots,\lambda_j-p,\lambda_{j+1}+1,\ldots,\lambda_{t-1}).$$

Theorem 3.1. *The module $\mathcal{M}(\lambda_0,\ldots,\lambda_{t-1})$ is invariant under the group G_m. Furthermore, any G_m-invariant submodule in $\mathcal{F}$ is equal to a sum of several modules $\mathcal{M}(\lambda_0,\ldots,\lambda_{t-1})$.*

Proof. For any integers $j\geqslant 0$ and s, d such that $0\leqslant s,d\leqslant m-1$, define linear transformations δ_s^j and $\varepsilon_{s,d}^j$ from $\mathcal{F}$ to itself by giving them as follows on the basis of monomials:

$$\delta_s^j\big(x_0^{i_0}\cdots x_{m-1}^{i_{m-1}}\big)=\binom{i_s}{j}x_0^{i_0}\cdots x_s^{i_s-j}\cdots x_{m-1}^{i_{m-1}}, \tag{1}$$

$$\varepsilon_{s,d}^{j}\left(x_0^{i_0}\cdots x_{m-1}^{i_{m-1}}\right)=\binom{i_s}{j}x_0^{i_0}\cdots x_s^{i_s-j}\cdots x_d^{i_d+j}\cdots x_{m-1}^{i_{m-1}}. \tag{2}$$

We recall that $\binom{i_s}{j}=0$ for $i_s<j$. The following lemma is taken from [8] (it also follows from [9]).

Lemma 3.2. *Let $\mathcal{M}$ be a subspace of $\mathcal{F}$. Then $\mathcal{M}$ is invariant under G_m if and only if*

(1) *$\mathcal{M}$ is invariant under the transformations δ_s^j and $\varepsilon_{s,d}^j$ for $s\neq d$ and $0\leqslant s,d\leqslant m-1$ and $0\leqslant j\leqslant q-1$, and*
(2) *$\mathcal{M}$ is spanned by monomials.*

In particular, the lemma says that if a module $\mathcal{M}$ is invariant under G_m,

$$x_0^{i_{00}+i_{01}p+\cdots+i_{0,t-1}p^{t-1}}x_1^{i_{10}+i_{11}p+\cdots+i_{1,t-1}p^{t-1}}\cdots x_{m-1}^{i_{m-1,0}+i_{m-1,1}p+\cdots+i_{m-1,t-1}p^{t-1}}\in\mathcal{M},$$

where $0\leqslant i_{ab}\leqslant p-1$, $0\leqslant a\leqslant m-1$, $0\leqslant b\leqslant t-1$, and $i_{sj}>0$ for some s and j, then

$$x_0^{i_{00}+\cdots+i_{0,t-1}p^{t-1}}\cdots x_s^{i_{s0}+\cdots+(i_{sj}-1)p^j+\cdots+i_{s,t-1}p^{t-1}}\cdots x_{m-1}^{i_{m-1,0}+\cdots+i_{m-1,t-1}p^{t-1}}\in\mathcal{M},$$

$$x_0^{i_{00}+\cdots}\cdots x_s^{i_{s0}+\cdots+(i_{sj}-1)p^j+\cdots+i_{s,t-1}p^{t-1}}\cdots x_d^{i_{d0}+\cdots+(i_{dj}+1)p^j+\cdots+i_{d,t-1}p^{t-1}}\cdots x_{m-1}^{i_{m-1,0}+\cdots}\in\mathcal{M}.$$

Suppose a G_m-invariant module $\mathcal{M}$ contains the monomial

$$x_0^{i_{00}+\cdots+i_{0,t-1}p^{t-1}}x_1^{i_{10}+\cdots+i_{1,t-1}p^{t-1}}\cdots x_{m-1}^{i_{m-1,0}+\cdots+i_{m-1,t-1}p^{t-1}}$$

such that

$$i_{00}+i_{10}+\cdots+i_{m-1,0}=\lambda_0,\ \ldots,\ i_{0,t-1}+i_{1,t-1}+\cdots+i_{m-1,t-1}=\lambda_{t-1},$$

where $0\leqslant i_{sd}\leqslant p-1$. Then by Lemma 3.2 we have $\mathcal{M}\supseteq\mathcal{M}(\lambda_0,\ldots,\lambda_{t-1})$. □

Here is one important particular case.

Example 1. If $\mathcal{M}$ is the ρth order generalized Reed–Muller code then

$$\mathcal{M}=\left\langle x_0^{i_0}\cdots x_{m-1}^{i_{m-1}}\mid i_0+\cdots+i_{m-1}\leqslant\rho\right\rangle=\sum_{\lambda_0+\cdots+\lambda_{t-1}p^{t-1}\leqslant\rho}\mathcal{M}(\lambda_0,\ldots,\lambda_{t-1}).$$

Let $\overline{S}=\bigoplus_{\lambda=0}^{m(p-1)}\overline{S}^{\lambda}$ denote the truncated polynomial ring

$$S\left(V^*\right)/\left(V^{*(p)}\right)\cong\mathbb{F}_q[x_0,\ldots,x_{m-1}]/\left(x_i^p\right)_{i=0}^{m-1}$$

and $\overline{S}^{(p^j)}$ denote the same ring but with the variables x_i replaced by their p^jth powers. The module $\overline{S}^{(p^j)}$ is isomorphic to the jth Frobenius twist of $\overline{S}$. Furthermore, the modules

$$S(\lambda_0,\ldots,\lambda_{t-1}) = \bigotimes_{j=0}^{t-1} \left(\overline{S}^{\lambda_j}\right)^{(p^j)}$$

are simple modules over $GL_m(q)$ and over $SL_m(q)$, by Steinberg's tensor product theorem.

Theorem 3.3. *The following statements hold*:

(i) *The module $\mathcal{M}(\lambda_0,\ldots,\lambda_{t-1})$ has a unique maximal submodule*

$$\sum_{j=0}^{t-1} \mathcal{M}(\lambda_0,\ldots,\lambda_j-1,\ldots,\lambda_{t-1}) + \sum_{j=0}^{t-1} \mathcal{M}(\lambda_0,\ldots,\lambda_j-p,\lambda_{j+1}+1,\ldots,\lambda_{t-1}),$$

where the indices j are considered modulo t and it is assumed $\mathcal{M}(\ldots,-1,\ldots)=0$, $\mathcal{M}(\ldots,m(p-1)+1,\lambda_{j+2},\ldots)=\mathcal{M}(\ldots,(m-1)(p-1),\lambda_{j+2}+1,\ldots)$.

(ii) *The module $\mathcal{M}(\lambda_0,\ldots,\lambda_{t-1})$ is indecomposable as G_m-module with the head isomorphic to $S(\lambda_0,\ldots,\lambda_{t-1})$.*

Proof. (i) Any monomial f from $\mathcal{M}(\lambda_0,\ldots,\lambda_{t-1})$ is either a monomial

$$a x_0^{i_{00}+\cdots+i_{0,t-1}p^{t-1}} x_1^{i_{10}+\cdots+i_{1,t-1}p^{t-1}} \cdots x_{m-1}^{i_{m-1,0}+\cdots+i_{m-1,t-1}p^{t-1}} \tag{3}$$

with the property that

$$i_{00}+i_{10}+\cdots+i_{m-1,0}=\lambda_0,\ \ldots,\ i_{0,t-1}+i_{1,t-1}+\cdots+i_{m-1,t-1}=\lambda_{t-1},$$

where $0\leqslant i_{sd}\leqslant p-1$, or an element of one of the modules

$$\mathcal{M}(\lambda_0,\ldots,\lambda_j-1,\ldots,\lambda_{t-1}) \quad \text{and} \quad \mathcal{M}(\lambda_0,\ldots,\lambda_j-p,\lambda_{j+1}+1,\ldots,\lambda_{t-1})$$

(in fact, these elements are obtained from the element (3) using transformations (1), (2)). In the former case f generates $\mathcal{M}(\lambda_0,\ldots,\lambda_{t-1})$, in the latter case f belongs to the required (maximal) module.

(ii) This is clear. □

Therefore, in order to determine whether $\mathcal{M}(\mu_0,\ldots,\mu_{t-1})\subseteq\mathcal{M}(\lambda_0,\ldots,\lambda_{t-1})$, one has to check the conditions $\mathcal{M}(\mu_0,\ldots,\mu_{t-1})\subseteq\mathcal{M}(\lambda_0,\ldots,\lambda_j-1,\ldots,\lambda_{t-1})$, $0\leqslant j\leqslant t-1$, and $\mathcal{M}(\mu_0,\ldots,\mu_{t-1})\subseteq\mathcal{M}(\lambda_0,\ldots,\lambda_j-p,\lambda_{j+1}+1,\ldots,\lambda_{t-1})$, $0\leqslant j\leqslant t-1$. And so on.

3.2. The structure of $\mathcal{F}$ over the linear group

The module $\mathcal{F}$ can be decomposed as a direct sum of $GL_m(q)$-submodules:

$$\mathcal{F} = \bigoplus_{k=0}^{q-1} \mathcal{F}^k,$$

$$\mathcal{F}^k = \left\{ f : V \to \mathbb{F}_q \mid f(\beta\alpha_0, \ldots, \beta\alpha_{m-1}) = \beta^k f(\alpha_0, \ldots, \alpha_{m-1}),\ \beta \in \mathbb{F}_q \right\}.$$

In particular,

$$\mathcal{F}^k = \left\langle x_0^{i_0} \cdots x_{m-1}^{i_{m-1}} \mid i_0 + \cdots + i_{m-1} \equiv k \pmod{q-1},\ i_0 + \cdots + i_{m-1} > 0 \right\rangle$$

for $k > 0$ and

$$\mathcal{F}^0 = \left\langle x_0^0 \cdots x_{m-1}^0 \right\rangle = \langle 1 \rangle.$$

For k, $0 \leqslant k \leqslant q-1$, let $k = k_0 + k_1 p + \cdots + k_{t-1} p^{t-1}$ be its p-adic expression, $0 \leqslant k_i \leqslant p-1$. For $k > 0$ let $\mathcal{H}[k]$ denote the set of all t-tuples $(r_0, \ldots, r_{t-1})$ of integers satisfying

(1) $0 \leqslant r_j \leqslant m-1$;
(2) $0 \leqslant k_j + p r_{j+1} - r_j \leqslant m(p-1)$.

(Subscripts mod t.) Moreover, let $\mathcal{H}[0]$ consist of one t-tuple $(0, \ldots, 0)$.

Define

$$\mathcal{M}[k](\bar{r}) = \mathcal{M}[k_0, \ldots, k_{t-1}](r_0, \ldots, r_{t-1}) = \mathcal{F}^k \cap \mathcal{M}(\ldots, k_j + p r_{j+1} - r_j, \ldots).$$

Suppose

$$f = x_0^{i_{00} + \cdots + i_{0,t-1} p^{t-1}} \cdots x_{m-1}^{i_{m-1,0} + \cdots + i_{m-1,t-1} p^{t-1}},$$
$$i_{0j} + i_{1j} + \cdots + i_{m-1,j} = k_j + p r_{j+1} - r_j$$

for all $j = 0, 1, \ldots, t-1$. If $0 \leqslant i_{sd} \leqslant p-1$ for all s, d, then $f \in \mathcal{M}[k](\bar{r})$. Further, if $i_{sd} > p-1$ for some s, d, then $f \in \mathcal{M}[k](r_0, \ldots, r_d - 1, \ldots, r_{t-1}) \subseteq \mathcal{M}[k](\bar{r})$.

Note that

$$\mathcal{F}^k = \mathcal{M}[k](m-1, \ldots, m-1).$$

Let us consider $\mathcal{H}[k]$ for $k = q-1$. It is easy to see that if $(r_0, \ldots, r_{t-1}) \in \mathcal{H}[q-1]$ and $r_j = m-1$ for some j then $(r_0, \ldots, r_{t-1}) = (m-1, \ldots, m-1)$. Moreover, introducing

$$\mathcal{W} = \left\langle 1 - \left(1 - x_0^{q-1}\right) \cdots \left(1 - x_{m-1}^{q-1}\right) \right\rangle_{\mathbb{F}_q} = \left\langle \sum_{v \neq 0} X^v \right\rangle_{\mathbb{F}_q}$$

we see that

$$\mathcal{F}^{q-1} = \mathcal{W} \oplus \mathcal{M}[q-1](m-2,\dots,m-2)$$

as a direct sum of $GL_m(q)$-submodules. Therefore, we have the following decomposition into a direct sum of $GL_m(q)$-submodules:

$$\mathcal{F} = \mathcal{W} \oplus \mathcal{M}[q-1](m-2,\dots,m-2) \bigoplus_{k=0}^{q-2} \mathcal{F}^k. \tag{4}$$

All summands (and composition factors) are nonisomorphic except for $\mathcal{W} \cong \mathcal{F}^0$.

There is a natural partial ordering in $\mathcal{H}[k]$: $(r_1,\dots,r_{t-1}) \leqslant (r'_1,\dots,r'_{t-1})$ if and only if $r_j \leqslant r'_j$ for all j. There is a similar natural partial ordering for t-tuples $(k_0,\dots,k_{t-1})$, where $k = k_0 + k_1 p + \cdots + k_{t-1}p^{t-1}$, $0 \leqslant k_i \leqslant p-1$, is the p-adic expression of k, $0 \leqslant k \leqslant q-1$.

The next theorem follows from results of [9], the definitions of $\mathcal{M}(\bar{\lambda})$ and $\mathcal{M}[k](\bar{r})$, Lemma 3.2 and Theorem 3.3.

Theorem 3.4. *The following statements hold*:

(i) *For $k \neq q-1$ any indecomposable $GL_m(q)$-module in $\mathcal{F}^k$ is equal to some module $\mathcal{M}[k](\bar{r})$.*
(ii) *For $k = q-1$ any indecomposable $GL_m(q)$-module in $\mathcal{M}[k](m-2,\dots,m-2)$ is equal to some module $\mathcal{M}[k](\bar{r})$, $\bar{r} \neq (m-1,\dots,m-1)$.*
(iii) *Any $GL_m(q)$-submodule in $\mathcal{F}^k$ is equal to a sum of several modules $\mathcal{M}[k](\bar{r})$, and possibly $\mathcal{W}$.*
(iv) *$\mathcal{M}[k](\bar{r}) \subseteq \mathcal{M}[k](\bar{r}')$ if $\bar{r} \leqslant \bar{r}'$.*
(v) *The submodule $\mathcal{M}[k](\bar{r})$ is indecomposable as $GL_m(q)$-module with the head isomorphic to $S(k_0 + r_1 p - r_0,\dots,k_{t-1} + r_0 p - r_{t-1})$.*
(vi) *If $\bar{r} \in \mathcal{H}(k)$ then $G_m\mathcal{M}[k](\bar{r}) = \mathcal{M}(k_0 + r_1 p - r_0,\dots,k_{t-1} + r_0 p - r_{t-1})$.*
(vii) *The module $\mathcal{M}(\lambda_0,\dots,\lambda_{t-1}) \neq \mathcal{M}(0,\dots,0)$ is equal to $G_m\mathcal{M}[k](\bar{r})$, where $k > 0$, $k \equiv \lambda_0 + \cdots + \lambda_{t-1}p^{t-1} \pmod{q-1}$, $k = k_0 + k_1 p + \cdots + k_{t-1}p^{t-1}$, $0 \leqslant k_i \leqslant p-1$, and*

$$r_j = \frac{1}{q-1}\left(\sum_{i=0}^{t-1} \lambda_{j+i}\, p^i - \sum_{i=0}^{t-1} k_{j+i}\, p^i\right).$$

3.3. The structure of the group algebra $\mathcal{F}$ over the affine group

In this subsection we give another formulation of results from Section 3.1 using the fact that elements of $\mathcal{F}$ can be considered as elements of a group algebra.

Let $\mathcal{F}^{(j)}$ be the ideal in the ring $\mathcal{F}$ generated by elements $(1-X^{v_1})\cdots(1-X^{v_j})$, $v_i \in V$. We have an G_m-invariant filtration:

$$\mathcal{F} = \mathcal{F}^{(0)} \supset \mathcal{F}^{(1)} \supset \mathcal{F}^{(2)} \supset \cdots \supset \{0\}.$$

Note that $\mathcal{F}^{(1)}$ is the unique maximal ideal of the algebra $\mathcal{F}$. For $0 \leqslant s \leqslant m-1$, $0 \leqslant d \leqslant t-1$ we introduce elements

$$Y_{sd} = \sum_{\alpha \in \mathbb{F}_q^*} \alpha^{-p^d} X^{\alpha e_s}, \quad q > 2;$$

$$Y_{sd} = Y_s = X^{e_s} - 1, \quad q = 2.$$

Lemma 3.5. *The following properties hold*:

(i) $Y_{sd} \in \mathcal{F}^{(1)}$;
(ii) *The elements* $\prod_{s=0}^{m-1}\prod_{d=0}^{t-1} Y_{sd}^{i_{sd}}$, $0 \leqslant i_{sd} \leqslant p-1$, *form an* $\mathbb{F}_q$*-basis of the module* $\mathcal{F}$;
(iii) $(Y_{sd})^p = 0$;
(iv) *The subspace* $\mathbb{F}_q \prod_{s=0}^{m-1}\prod_{d=0}^{t-1} Y_{sd}^{i_{sd}}$ *is invariant under the diagonal subgroup of* $GL_m(q)$ *and* $\operatorname{diag}(\alpha_1,\ldots,\alpha_m)(Y_{sd}) = \alpha_s^{p^d} Y_{sd}$;
(v) $\hat{g}(Y_{sd}) \equiv \sum_{i=0}^{m-1} g_{is}^{p^d} Y_{id} \pmod{\mathcal{F}^{(2)}}$ *for* $g = (g_{ij}) \in GL_m(q)$;
(vi) $\hat{\sigma}^i(Y_{sd}) = Y_{s,d+i}$ (*second subscript* mod t);
(vii) *If* $q > 2$ *then* $\mathbb{F}_q \prod_{s=0}^{m-1}\prod_{d=0}^{t-1} Y_{sd}^{i_{sd}} = \mathbb{F}_q \prod_{s=0}^{m-1} x_s^{(p-1-i_{s0})+\cdots+(p-1-i_{s,t-1})p^{t-1}}$ *for* $(\ldots,i_{sd},\ldots) \neq (0,\ldots,0)$, *and* $\prod_{s=0}^{m-1}\prod_{d=0}^{t-1} Y_{sd}^{0} = X^0 = \prod_{s=0}^{m-1}(1-x_s^{q-1})$.

We will prove this lemma later. The advantage of the basis $\{\prod_{s=0}^{m-1}\prod_{d=0}^{t-1} Y_{sd}^{i_{sd}}\}$ is that, it is more suitable to study ideals in $\mathcal{F}$. A submodule $\mathcal{M} \subseteq \mathcal{F}$ is an ideal if and only if it is invariant under multiplications by the elements Y_{sd}. Note that the product $\prod_{s=0}^{m-1}\prod_{d=0}^{t-1} Y_{sd}^{i_{sd}}$ is considered as product in the *group algebra* $\mathcal{F}$. In particular, the element Y_{sd}, considered as a function, is equal to $x_s^{q-1-p^d}$ for $q > 2$. However, $Y_{sd}\cdot Y_{sd} = Y_{sd}^2 \neq x_s^{q-1-2p^d}$.

We define the modules

$$\mathcal{R}(\lambda_0,\ldots,\lambda_{t-1}) = \Bigg\langle Y_{00}^{i_{00}} Y_{01}^{i_{01}} \cdots Y_{0,t-1}^{i_{0,t-1}} \cdots Y_{m-1,0}^{i_{m-1,0}} Y_{m-1,1}^{i_{m-1,1}} \cdots Y_{m-1,t-1}^{i_{m-1,t-1}} \Bigg| \prod_{s=0}^{m-1} x_s^{(p-1-i_{s0})+\cdots+(p-1-i_{s,t-1})p^{t-1}} \in \mathcal{M}\big(m(p-1)-\lambda_0,\ldots,m(p-1)-\lambda_{t-1}\big)\Bigg\rangle,$$

where $0 \leqslant \lambda_j \leqslant m(p-1)$, $0 \leqslant i_{sj} \leqslant p-1$. In the other way, it can be defined inductively: if

$$\mathcal{R}'(\lambda_0,\dots,\lambda_{t-1}) = \big\langle Y_{00}^{i_{00}} Y_{01}^{i_{01}} \cdots Y_{0,t-1}^{i_{0,t-1}} \cdots Y_{m-1,0}^{i_{m-1,0}} Y_{m-1,1}^{i_{m-1,1}} \cdots Y_{m-1,t-1}^{i_{m-1,t-1}} \\ \big| \ i_{0j} + i_{1j} + \cdots + i_{m-1,j} \geqslant \lambda_j, \ j = 0,1,\dots,t-1\big\rangle,$$

then

$$\mathcal{R}(\lambda_0,\dots,\lambda_{t-1}) = \mathcal{R}'(\lambda_0,\dots,\lambda_{t-1}) + \sum_{j=0}^{t-1} \mathcal{R}(\dots,\lambda_j + p, \lambda_{j+1} - 1,\dots).$$

In particular,

$$\mathcal{R}(0,\dots,0) = \mathcal{F}, \qquad \mathcal{R}\big(m(p-1),\dots,m(p-1)\big) = \left\langle \sum_{v\in V} X^v \right\rangle,$$

and one has

$$\mathcal{R}(\lambda_0,\dots,\lambda_{t-1}) \supseteq \mathcal{R}(\dots,\lambda_{j-1},\lambda_j+1,\lambda_{j+1},\dots) \quad \big(\lambda_j < m(p-1)\big),$$

$$\mathcal{R}(\lambda_0,\dots,\lambda_{t-1}) \supseteq \mathcal{R}(\dots,\lambda_j+p,\lambda_{j+1}-1,\dots) \quad (\lambda_{j+1} > 0).$$

We define $GL_m(q)$-modules $\widehat{\mathcal{F}}$, $\widehat{\mathcal{F}}^k$, $\widehat{\mathcal{M}}(\bar{\lambda})$, $\widehat{\mathcal{W}}$, where they are respectively equal to $\mathcal{F}$, $\mathcal{F}^k$, $\mathcal{M}(\bar{\lambda})$, $\mathcal{W}$ as the sets and the action given by

$$g \circ f(x) = f\big({}^t g x\big).$$

Similar to the modules $\overline{S}$ and $S(\lambda_0,\dots,\lambda_{t-1})$ from the previous section, we define modules

$$\widetilde{S} = S(V)\big/\big(V^{(p)}\big), \qquad \widehat{S}(\lambda_0,\dots,\lambda_{t-1}) = \bigotimes_{j=0}^{t-1} \big(\widetilde{S}^{\lambda_j}\big)^{(p^j)},$$

taking V in place of V^*. It is clear that the submodule $\widehat{\mathcal{M}}(\lambda_0,\dots,\lambda_{t-1})$ is indecomposable as G_m-module with the head isomorphic to $\widehat{S}(\lambda_0,\dots,\lambda_{t-1})$.

Since the module $\mathcal{R}(m(p-1),\dots,m(p-1))$ is of dimension 1, one can define $GL_m(q)$-invariant pairings

$$\mathcal{F}\times\mathcal{F} \to \mathbb{F}_q, \qquad \widehat{\mathcal{F}}\times\widehat{\mathcal{F}} \to \mathbb{F}_q,$$

thus there are the following isomorphisms of $GL_m(p^t)$-modules:

$$\widehat{S}\big(m(p-1)-\lambda_0,\dots,m(p-1)-\lambda_{t-1}\big)^* \cong \widehat{S}(\lambda_0,\dots,\lambda_{t-1}) \cong S(\lambda_0,\dots,\lambda_{t-1})^* \\ \cong S\big(m(p-1)-\lambda_0,\dots,m(p-1)-\lambda_{t-1}\big).$$

Theorem 3.6. *The following assertions hold*:

(i) *The submodule* $\mathcal{R}(\lambda_0,\dots,\lambda_{t-1})$ *is indecomposable as* G_m*-module with the head isomorphic to* $\widehat{S}(\lambda_0,\dots,\lambda_{t-1}) \cong S(m(p-1)-\lambda_0,\dots,m(p-1)-\lambda_{t-1})$.
(ii) *For any* G_m*-invariant submodule* $\mathcal{M}\subseteq\mathcal{F}$ *one has* $\mathcal{M}=\mathcal{R}(\lambda_0,\dots,\lambda_{t-1})$ *if and only if* $\mathcal{M}=\mathcal{M}(m(p-1)-\lambda_0,\dots,m(p-1)-\lambda_{t-1})$.
(iii) *Any* G_m*-invariant submodule in* $\mathcal{F}$ *is a sum of several modules* $\mathcal{R}(\lambda_0,\dots,\lambda_{t-1})$.
(iv) *For any* G_m*-invariant submodule* $\mathcal{M}\subseteq\mathcal{F}$ *one has* $\mathcal{R}=\sum_{\bar{\lambda}\in D}\mathcal{M}(\bar{\lambda})$ *if and only if* $\mathcal{M}=\sum_{\bar{\lambda}\in D}\mathcal{M}(m(p-1)-\lambda_0,\dots,m(p-1)-\lambda_{t-1})$.
(v) *For any* G_m*-invariant submodule* $\mathcal{M}\in\mathcal{F}$ *one has*

$$\mathcal{M}=\left\{Y_{00}^{i_{00}}\cdots Y_{0,t-1}^{i_{0,t-1}}\cdots Y_{m-1,0}^{i_{m-1,0}}\cdots Y_{m-1,t-1}^{i_{m-1,t-1}} \;\middle|\; (i_{sj})\in E,\ 0\leqslant i_{sj}\leqslant p-1\right\}$$

if and only if

$$\mathcal{M}=\left\{\prod_{s=0}^{m-1} x_s^{(p-1-i_{s0})+\cdots+(p-1-i_{s,t-1})p^{t-1}} \;\middle|\; (i_{sj})\in E,\ 0\leqslant i_{sj}\leqslant p-1\right\}.$$

Proof. It follows from Lemma 3.5. □

Example 2. For the ideal $\mathcal{F}^{(j)}$ in the ring $\mathcal{F}$ one has

$$\mathcal{F}^{(j)}=\sum_{\lambda_0+\lambda_1+\cdots+\lambda_{t-1}\geqslant j}\mathcal{R}(\lambda_0,\dots,\lambda_{t-1})=\sum_{\lambda_0+\lambda_1+\cdots+\lambda_{t-1}\leqslant tm(p-1)-j}\mathcal{M}(\lambda_0,\dots,\lambda_{t-1}).$$

The next statement are taken from [5].

Lemma 3.7. *The following assertions are true*:

(i) $(1-X^{\alpha})+(1-X^{\beta})\equiv(1-X^{\alpha+\beta}) \pmod{\mathcal{F}^{(2)}}$.
(ii) $(1-X^{\alpha})^p=0$.
(iii) *If* $\{v_1,\dots,v_n\}$ *is a basis of* V *over* $\mathbb{F}_p$*, then the elements*

$$\left(1-X^{v_1}\right)^{k_1}\cdots\left(1-X^{v_n}\right)^{k_n},\quad 0\leqslant k_i\leqslant p-1,$$

form a basis of $\mathcal{F}$ *over* $\mathbb{F}_q$.

Proof of Lemma 3.5. For $q=2$ the statements are obvious. Let $q>2$ and consider the space

$$\mathcal{B}_s=\left\langle X^{\alpha e_s}\mid\alpha\in\mathbb{F}_q\right\rangle_{\mathbb{F}_q}.$$

In [5] it was proved that elements $\prod_{d=0}^{t-1} Y_{sd}^{i_{sd}}$, $0 \leqslant i_{sd} \leqslant p-1$, form a basis of $\mathcal{B}_s$ with required properties (i), (iii), (iv), (vi). Property (ii) follows from the fact $\mathcal{F} = \mathcal{B}_0 \cdot \mathcal{B}_1 \cdots \mathcal{B}_{m-1}$. Property (vii) follows from (iv) and the fact [5, Proposition 9(x)]

$$\prod_{d=0}^{t-1} Y_{sd}^{p-1} = (-1)^{t-1} \sum_{\alpha \in \mathbb{F}_q} X^{\alpha e_s}.$$

It remains for us to prove the property (v). Let $g(e_s) = \sum_i g_{is} e_i$. Then

$$\begin{aligned}
\hat{g}(Y_{sd}) &= \sum_{\alpha \neq 0} \alpha^{-p^d} X^{\alpha \sum_i g_{is} e_i} = \sum_{\alpha \neq 0} \alpha^{-p^d} \left(X^{\alpha \sum_i g_{is} e_i} - 1 \right) \\
&\equiv \sum_{\alpha \neq 0} \alpha^{-p^d} \left(\sum_i \left(X^{\alpha g_{is} e_i} - 1 \right) \right) \equiv \sum_i \sum_{\alpha \neq 0} \alpha^{-p^d} X^{\alpha g_{is} e_i} \\
&= \sum_i g_{is}^{p^d} \sum_{\alpha \neq 0} \alpha^{-p^d} X^{\alpha e_i} = \sum_i g_{is}^{p^d} Y_{id} \pmod{\mathcal{F}^{(2)}}.
\end{aligned}$$

Here we have used the property $(X^v - 1) + (X^u - 1) \equiv (X^{v+u} - 1) \pmod{\mathcal{F}^{(2)}}$ (see Lemma 3.7). □

3.4. Some special cases

In this subsection we consider two important extremal cases $m = 1$ and $m = n$. They were considered in [5,6] in detail. Now we get those results as consequences of the present considerations.

Let $m = 1$. Then $G_m = AGL_1(p^n)$. In the coding theory codes in $\mathcal{F}$ invariant under the group G_1 are called affine invariant [8,14]. They are extended cyclic codes. Any G_1-invariant module $\mathcal{M}$ can be represented as a sum of several modules $\mathcal{M}(\lambda_0, \ldots, \lambda_{n-1})$, where $0 \leqslant \lambda_j \leqslant p-1$. Therefore, for some D we have

$$\mathcal{M} = \bigoplus_{\bar{k} \in D} \langle x_0^{k_0 + k_1 p + \cdots + k_{n-1} p^{n-1}} \rangle,$$

such that $(k_0, \ldots, k_{n-1}) \in D$, $k_i > 0$, implies $(k_0, \ldots, k_i - 1, \ldots, k_{n-1}) \in D$.

In terms of the group algebra realization, any G_1-invariant module $\mathcal{M}$ can be represented as

$$\mathcal{M} = \bigoplus_{\bar{k} \in D'} \langle Y_{00}^{k_0} Y_{01}^{k_1} \cdots Y_{0,n-1}^{k_{n-1}} \rangle,$$

such that $(k_0, \ldots, k_{n-1}) \in D'$, $k_i < p-1$, implies $(k_0, \ldots, k_i + 1, \ldots, k_{n-1}) \in D'$.

Now let $m = n$. Then $t = 1$ and $G_m = AGL_n(p)$. We have that any G_n-invariant module $\mathcal{M}$ can be represented as a sum of several modules $\mathcal{M}(\lambda_0)$, therefore

$$\mathcal{M} = \mathcal{M}(\lambda) = \left\langle x_0^{i_0} \cdots x_{n-1}^{i_{n-1}} \;\middle|\; i_0 + \cdots + i_{n-1} \leqslant \lambda \right\rangle$$

for some λ, which means that $\mathcal{M}$ is a generalized Reed–Muller code.

In terms of the group algebra realization, any G_n-invariant module $\mathcal{M}$ can be represented as $\mathcal{M} = \mathcal{R}(k)$ for some k.

We have proved the following

Theorem 3.8 [6,8]. *A code $\mathcal{M}$ is invariant under $G_n = AGL_n(p)$ if and only if $\mathcal{M}$ is a generalized Reed–Muller code.*

3.5. Submodules over a prime field

In this subsection we are going to determine the G_m-invariant $\mathbb{F}_p$-submodules in the module

$$\overline{A} = \left\{ \sum_{v \in V} a_v X^v \;\middle|\; a_v \in \mathbb{F}_p \right\}.$$

The following well known lemma (see also [5]) allows us to describe invariant submodules over a prime field.

Lemma 3.9. *Let $U = \sum_{i=1}^{n} F g_i$ be a vector space over a finite field F with a basis $\{g_1, \ldots, g_n\}$ and let a group H act on the module U. Let a finite field K be an extension of F and $\tau : K \to K$ be a generator of the Galois group $Gal(K/F)$. Let $\mathcal{U} = \sum_{i=1}^{n} K g_i \supset U$ be a vector space over the field K with the same basis and the actions of H and $Gal(K, F)$ are extended to $\mathcal{U}$ in the natural way. Then the map*

$$\mu : \mathcal{C} \mapsto \mathcal{C} \cap U$$

defines a bijective correspondence between the set of K-subspaces of $\mathcal{U}$ that are invariant under H and τ, and the set of F-subspaces in U that are invariant under H.

Define

$$M(\lambda_0, \ldots, \lambda_{t-1}) = \overline{A} \cap \sum_{i=0}^{t-1} \hat{\sigma}\left(\mathcal{M}(\lambda_0, \ldots, \lambda_{t-1})\right).$$

Introducing the map $Tr : \mathcal{F} \to \overline{A}$ by

$$Tr(f) = f + f^p + \cdots + f^{p^{t-1}},$$

we see that

$$M(\lambda_0,\dots,\lambda_{t-1}) = Tr\big(\mathcal{M}(\lambda_0,\dots,\lambda_{t-1})\big) = \big\{Tr(f) \mid f \in \mathcal{M}(\lambda_0,\dots,\lambda_{t-1})\big\},$$

$$M(\lambda_0,\dots,\lambda_{t-1}) = M(\lambda_{t-1},\lambda_0,\dots,\lambda_{t-2}).$$

Now from Lemma 3.9 and Theorem 3.1 we obtain the following result.

Theorem 3.10. *Any G_m-invariant submodule in $\overline{A}$ is equal to a sum of several modules $M(\lambda_0,\dots,\lambda_{t-1})$.*

4. Submodules over R_p and $\mathbb{Z}_p$

In this section we will give a description of the G_m-invariant R_p-lattices in $\mathcal{A}$ and $\mathbb{Z}_p$-lattices in A. We are going to lift the invariant ideals of $\mathcal{F}$ into $\mathcal{A}$, describe all G_m-invariant lattices in $\mathcal{A}$, and then write them in terms of functions. Finally, Galois descent completes our investigation.

4.1. The structure of the group ring $\mathcal{A}$

In this subsection we study the structure of $\mathcal{A}$ with the help of a special basis, which is a lifting of the basis from Lemma 3.5. First we introduce some notations.

The group $R_p^* = R_p \setminus pR_p$ of invertible elements of the ring R_p has a unique subgroup isomorphic to $\mathbb{F}_q^*$. This subgroup is called the group of multiplicative representatives and is the set of all solutions of the equation $x^{q-1} = 1$. Also it is the set of all invertible elements in R_p of finite order. The Teichmüller representative $\tilde{\alpha} \in R_p$ of an element $\alpha \in \mathbb{F}_q$ is defined as follows: it is 0 if $\alpha = 0$, and it is $(q-1)$st root of unity in R_p whose residue class (modulo p) is α if $\alpha \neq 0$.

Let $\mathcal{A}^{(j)}$ be the ideal in the ring $\mathcal{A}$ generated by elements $(1-X^{v_1})\cdots(1-X^{v_j})$, $v_i \in V$. The next lemma gives a construction of our special basis (compare with Lemma 3.5).

Lemma 4.1. *There exist elements $Z_{sd} \in \mathcal{A}$, $0 \leqslant s \leqslant m-1$, $0 \leqslant d \leqslant t-1$ with the following properties*:

(i) $Z_{sd} \in \mathcal{A}^{(1)}$ *and* $Z_{sd} \equiv Y_{sd} \pmod{\mathcal{A}^{(2)}}$;
(ii) *The elements* $\prod_{s=0}^{m-1}\prod_{d=0}^{t-1} Z_{sd}^{i_{sd}}$, $0 \leqslant i_{sd} \leqslant p-1$, *form an R_p-basis of the module $\mathcal{A}$*;
(iii) $(Z_{sd})^p = -pZ_{s,d+1}$ (*second subscript* mod t);
(iv) *The subspace* $R_p\prod_{s=0}^{m-1}\prod_{d=0}^{t-1} Z_{sd}^{i_{sd}}$ *is invariant under the diagonal subgroup of $GL_m(q)$ and* $\operatorname{diag}(\alpha_1,\dots,\alpha_m)(Z_{sd}) = \tilde{\alpha}_s{}^{p^d} Z_{sd}$;
(v) $\hat{g}(Z_{sd}) \equiv \sum_{i=0}^{m-1} \tilde{g}_{is}^{p^d} Z_{id} \pmod{\mathcal{A}^{(2)}}$ *for* $g = (g_{ij}) \in GL_m(q)$;
(vi) $\hat{\sigma}^i(Z_{sd}) = Z_{s,d+i}$ (*second subscript* mod t);

Proof. Consider space

$$\mathcal{B}_s = \langle X^{\alpha e_s} \mid \alpha \in \mathbb{F}_q \rangle_{R_p}.$$

For $q = 2$ we take $Z_{sd} = Y_{sd} = X^{e_s} - 1$. It was proved in [5] that for $q > 2$ there exist elements Z_{sd}, such that the elements $\prod_{d=0}^{t-1} Z_{sd}^{i_{sd}}$, $0 \leqslant i_{sd} \leqslant p-1$, form a basis of $\mathcal{B}_s$ with required properties (i), (iii), (iv), (vi). Property (ii) follows from the fact $\mathcal{A} = \mathcal{B}_0 \cdot \mathcal{B}_1 \cdots \mathcal{B}_{m-1}$. It remains for us to prove only the property (v). It follows from Lemma 3.5(v). □

We recall that a module $\mathcal{L} \subseteq \mathcal{A}$ is invariant under the group V if and only if $\mathcal{L}$ is an ideal in $\mathcal{A}$. Therefore, by the previous lemma, $\mathcal{L}$ is invariant under V if and only if it is invariant under multiplications by all elements Z_{sd}.

We define a module

$$\mathcal{A}^0 = \left\{ \sum_{v \in V} a_v X^v \;\middle|\; a_v \in R_p,\ \sum_{v \in V} a_v = 0 \right\} = \mathcal{A}^{(1)}$$

and introduce an element

$$w = \sum_{v \in V} X^v - p^n X^0.$$

Let K be the extension field of degree t of the p-adic numbers such that $K \supset R_p$. The G_m-module $K\mathcal{A}$ decomposes as the direct sum of the trivial module K and the module $K\mathcal{A}^0$. So we start with the description of invariant lattices in $\mathcal{A}^0$.

Lemma 4.2. *Let $\mathcal{L}$ be a G_m-invariant sublattice in $\mathcal{A}^0$ and $\mathcal{L} \not\subseteq p\mathcal{A}^0$. Then $\mathcal{L} \ni w$ and $\mathcal{L} \supset p^n\mathcal{A}^0$. In particular, there are only finitely many similarity classes of the G_m-invariant sublattices in $\mathcal{A}^0$.*

Proof. For $v \in V$ let $I_v \subseteq R_p$ be the ideal of all a_v occuring in the decompositions $a = \sum a_v X^v$ of vectors $a \in \mathcal{L}$. Then I_v does not depend on v. If $I_v = p^r R_p$, $r > 1$, then $\mathcal{L} \subset p^r\mathcal{A}^0$, which is a contradiction. Hence $I_v = R_p$. Therefore, there is an element $a = \sum a_v X^v \in \mathcal{L}$ with $a_0 = 1$. Note that $\sum a_v = 0$.

Now let H be a subgroup in $GL_m(q)$ acting cyclically on nonzero vectors of V. We have

$$\sum_{g \in H} ga = a_0(p^n - 1)X^0 + \left(\sum_{v \neq 0} a_v\right)\left(\sum_{v \neq 0} X^v\right) = a_0(p^n - 1)X^0 - a_0\left(\sum_{v \neq 0} X^v\right)$$

$$= a_0 p^n X^0 - a_0\left(\sum X^v\right) = p^n X^0 - \sum X^v = -w \in \mathcal{L}.$$

Therefore, $p^n X^u - \sum X^v \in \mathcal{L}$ for any $u \in V$ and $p^n(X^0 - X^u) \in \mathcal{L}$. So $\mathcal{L} \supset p^n\mathcal{A}^0$. □

We define ideals

$$\mathcal{L}(\lambda_0,\dots,\lambda_{t-1}) = \big\langle Z_{00}^{i_{00}} Z_{01}^{i_{01}} \cdots Z_{0,t-1}^{i_{0,t-1}} \cdots Z_{m-1,0}^{i_{m-1,0}} Z_{m-1,1}^{i_{m-1,1}} \cdots Z_{m-1,t-1}^{i_{m-1,t-1}} \\ \big| \, i_{0j} + i_{1j} + \cdots + i_{m-1,j} \geqslant \mu_j, \ j = 0,1,\dots,t-1; \ \mathcal{R}(\bar{\mu}) \subseteq \mathcal{R}(\bar{\lambda}) \big\rangle.$$

In the other way, it can be defined inductively: if

$$\mathcal{L}'(\lambda_0,\dots,\lambda_{t-1}) = \big\langle Z_{00}^{i_{00}} Z_{01}^{i_{01}} \cdots Z_{0,t-1}^{i_{0,t-1}} \cdots Z_{m-1,0}^{i_{m-1,0}} Z_{m-1,1}^{i_{m-1,1}} \cdots Z_{m-1,t-1}^{i_{m-1,t-1}} \\ \big| \, i_{0j} + i_{1j} + \cdots + i_{m-1,j} \geqslant \lambda_j, \ j = 0,1,\dots,t-1 \big\rangle,$$

then

$$\mathcal{L}(\lambda_0,\dots,\lambda_{t-1}) = \mathcal{L}'(\lambda_0,\dots,\lambda_{t-1}) + \sum_{i=0}^{t-1} \mathcal{L}(\dots,\lambda_i + p, \lambda_{i+1} - 1, \dots).$$

In particular,

$$\mathcal{L}(0,\dots,0) = \mathcal{A}.$$

Note that

$$\hat{\sigma}\big(\mathcal{L}(\lambda_0,\dots,\lambda_{t-1})\big) = \mathcal{L}(\lambda_{t-1},\lambda_0,\dots,\lambda_{t-2}).$$

The modules $\mathcal{L}(\bar{\lambda})$ can be considered as lifts and analogs of the modules $\mathcal{R}(\bar{\lambda})$. It is clear that

$$\mathcal{L}\big(\bar{\lambda}\big) \supseteq \sum_{j=0}^{t-1} \mathcal{L}(\lambda_0,\dots,\lambda_j + 1,\dots,\lambda_{t-1}) + \sum_{j=0}^{t-1} \mathcal{L}(\lambda_0,\dots,\lambda_j + p, \lambda_{j+1} - 1,\dots,\lambda_{t-1}).$$

If $i_{sj} > p-1$ then $Z_{sj}^{i_{sj}} = -pZ_{sj}^{i_{sj}-p} Z_{s,j+1}^{1}$ by Lemma 4.1(iii), thus

$$\mathcal{L}\big(\bar{\lambda}\big) \supseteq p\mathcal{L}(\lambda_0,\dots,\lambda_j - p, \lambda_{j+1} + 1, \dots),$$

where we assume

$$\mathcal{L}\big(\lambda_0,\dots,m(p-1)+1,\lambda_{j+2},\dots\big) = p\mathcal{L}\big(\lambda_0,\dots,m(p-1)+1-p,\lambda_{j+2}+1,\dots\big).$$

In particular, in case $\bar{\lambda} = (m(p-1),\dots,m(p-1))$ we have

$$\begin{aligned}\mathcal{L}(\bar{\lambda}) &\supseteq p\mathcal{L}\big(m(p-1)-p, m(p-1)+1, m(p-1)\ldots, m(p-1)\big)\\ &= p^2\mathcal{L}\big(m(p-1)-p, m(p-1)+1-p, m(p-1)+1\ldots, m(p-1)\big)\\ &= \cdots\\ &= p^t\mathcal{L}\big((m-1)(p-1),\ldots,(m-1)(p-1)\big).\end{aligned}$$

Lemma 4.3. *The module $\mathcal{L}(\bar{\lambda})$ is invariant under G_m.*

Proof. It is clear that $\mathcal{L}(\bar{\lambda})$ is invariant under V. Let us prove its invariance under elements $g \in GL_m(q)$. Consider the variable $Z_{0,t-1}$ (another variables can be considered similarly). The element $a = g(Z_{0,t-1})$ has the property $\mathrm{diag}(\alpha,\ldots,\alpha)(a) = \tilde{\alpha}^{p^{t-1}}a$, thus $g(Z_{0,t-1})$ is a linear combination of elements $Z_{s,t-1}$, $Z_{s_1,t-2}Z_{s_2,t-2}\cdots Z_{s_p,t-2}$, $Z_{s_1,t-3}\cdots Z_{s_{bp},t-3}Z_{t_1,t-2}\cdots Z_{t_{p-b},t-2}$, and so on. It is sufficient to prove that, for any monomial $f \in \mathcal{L}(\bar{\lambda})$, by substituting one variable $Z_{0,p-1}$ in the monomial f by elements $Z_{s,t-1}$, $Z_{s_1,t-2}Z_{s_2,t-2}\cdots Z_{s_p,t-2}$, $Z_{s_1,t-3}\cdots Z_{s_{bp},t-3}Z_{t_1,t-2}\cdots Z_{t_{p-b},t-2}$, …, we will get again an element from the module $\mathcal{L}(\bar{\lambda})$. All these substitutions can be obtained as combination of the following elementary substitutions: $Z_{0,t-1} \to Z_{s,t-1}$, $Z_{s,t-1} \to Z_{s_1,t-2}\cdots Z_{s_p,t-2}$, $Z_{s,t-2} \to Z_{s_1,t-3}\cdots Z_{s_p,t-3}$, and so on. It is easy to see that under these elementary substitutions we will get again monomial from $\mathcal{L}(\bar{\lambda})$. □

We introduce some types of lattices.

- Lattices of type I:

$$\mathcal{L} = \sum p^{l(\lambda_0,\ldots,\lambda_{t-1})}\mathcal{L}(\lambda_0,\ldots,\lambda_{t-1}),$$

  that is, $\mathcal{L}$ is a sum of several lattices $p^l\mathcal{L}(\lambda_0,\ldots,\lambda_{t-1})$.
- Lattices of type II:

$$\mathcal{L} = R_p w + p^s\mathcal{L}^0 + p^n\mathcal{A}^0,$$

  where $\mathcal{L}^0$ is of type I, $1 \leqslant s \leqslant n$.
  Now we set

$$\mathcal{L}^{r,l,b} = R_p\big(w + p^r bX^0\big) + R_p p^l w + R_p p^{r+l}X^0 + p^{\min(n,r)}\mathcal{A}^0,$$

  where $1 \leqslant l \leqslant \min(n,r)$, $b \in R_p^*$, and either $r \neq n$ or $b \not\equiv 1 \pmod{p^l}$. Note that $\mathcal{L}^{r,l,b} = \mathcal{L}^{r,l,c}$ if and only if $b \equiv c \pmod{p^l}$.
- Lattices of type III:

$$\mathcal{L} = \mathcal{L}^0 + p^r\mathcal{A},$$

  where $\mathcal{L}^0$ is a lattice of type I, $r \geqslant 0$.

- Lattices of type IV:

$$\mathcal{L} = \mathcal{L}^{r,l,b} + p^s \mathcal{L}^0,$$

  where $\mathcal{L}^0$ is a lattice of type I, $l \leqslant s \leqslant \min(n, r)$.
- Lattices of type V:

$$\mathcal{L} = \left\langle \sum_{v \in V} X^v \right\rangle + p^s \mathcal{L}^0 + p^{n+l} \mathcal{A},$$

  where $\mathcal{L}^0$ is a lattice of type I, $1 \leqslant l \leqslant s$.

The next theorem gives a description of invariant lattices.

Theorem 4.4. *The following assertions hold*:

(i) *Any G_m-invariant lattice $\mathcal{L}$ in $\mathcal{A}^0$, $\mathcal{L} \not\subseteq p\mathcal{A}^0$, is equal to a lattice of type* I *or* II.
(ii) *Any G_m-invariant full lattice $\mathcal{L}$ in $\mathcal{A}$, $\mathcal{L} \not\subseteq p\mathcal{A}$, is equal to a lattice of type* III, IV *or* V.

We need a couple of lemmas to prove this theorem. First we introduce some modules. Let $\mathcal{L} = \mathcal{L}(\lambda_0, \ldots, \lambda_{t-1})$ and define

$$\mathcal{L}_i = p\mathcal{L}(\lambda_0, \ldots, \lambda_i - p, \lambda_{i+1} + 1, \ldots)$$

if $\lambda_i \geqslant p$, and $\mathcal{L}_i = 0$ otherwise. Recall that $\mathcal{L}_i \subset \mathcal{L}$. Define

$$\widetilde{\mathcal{L}} = \sum_{j=0}^{t-1} \mathcal{L}(\lambda_0, \ldots, \lambda_j + 1, \ldots, \lambda_{t-1}) + \sum_{j=0}^{t-1} \mathcal{L}(\ldots, \lambda_j + p, \lambda_{j+1} - 1, \ldots).$$

Composition factors of $(\mathcal{L} + p^2\mathcal{A})/(\widetilde{\mathcal{L}} + p^2\mathcal{A})$ are $\widehat{S}(\lambda_0, \ldots, \lambda_{t-1})$ (it comes from the head of $\mathcal{L}$) and $\widehat{S}(\lambda_0, \ldots, \lambda_i - p, \lambda_{i+1} + 1, \ldots, \lambda_{t-1})$, $i = 0, \ldots, t-1$ (they come from the heads of $\mathcal{L}_i$). Therefore, there is a module extension of $\widehat{S}(\lambda_0, \ldots, \lambda_{t-1})$ by $\widehat{S}(\lambda_0, \ldots, \lambda_i - p, \lambda_{i+1} + 1, \ldots, \lambda_{t-1})$, and we want to show that it does not split. To this end, we introduce

$$\mathcal{L}^i = \widetilde{\mathcal{L}} + \sum_{j \neq i} \mathcal{L}_j + p^2\mathcal{A},$$

$$\overline{\mathcal{L}} = \left(\mathcal{L} + \mathcal{L}^i\right)/\mathcal{L}^i, \qquad \overline{\mathcal{L}}_i = \left(\mathcal{L}_i + \mathcal{L}^i\right)/\mathcal{L}^i.$$

Note that

$$\left(\mathcal{L} + p^2\mathcal{A}\right)/\left(\widetilde{\mathcal{L}} + \sum \mathcal{L}_i + p^2\mathcal{A}\right) \cong \widehat{S}(\lambda_0, \ldots, \lambda_{t-1}),$$

$$\overline{\mathcal{L}}_i \cong \widehat{S}(\lambda_0, \ldots, \lambda_i - p, \lambda_{i+1} + 1, \ldots, \lambda_{t-1}).$$

Lemma 4.5. *Let* $\mathcal{L} = \mathcal{L}(\lambda_0, \ldots, \lambda_{t-1})$.

(i) *If* $\lambda_i \geqslant p$, $\lambda_{i+1} < m(p-1)$ *then the sequence*

$$0 \to \overline{\mathcal{L}}_i \to \overline{\mathcal{L}} \to \big(\mathcal{L} + p^2\mathcal{A}\big)\Big/\Big(\widetilde{\mathcal{L}} + \sum \mathcal{L}_i + p^2\mathcal{A}\Big) \to 0$$

of $GL_m(q)$*-modules, which can be written as*

$$0 \to \widehat{S}(\lambda_0, \ldots, \lambda_i - p, \lambda_{i+1} + 1, \ldots, \lambda_{t-1}) \to \overline{\mathcal{L}} \to \widehat{S}(\lambda_0, \ldots, \lambda_{t-1}) \to 0,$$

does not split.

(ii) *If* $\bar{\lambda} = (m(p-1), \ldots, m(p-1))$ *then*

$$\mathcal{L}/\widetilde{\mathcal{L}} = \langle \bar{w} \rangle \oplus \big(q\mathcal{L}\big((m-1)(p-1), \ldots, (m-1)(p-1)\big) + \widetilde{\mathcal{L}}\big)/\widetilde{\mathcal{L}},$$

where $\bar{w}$ *is a image of* w *in* $\mathcal{L}/\widetilde{\mathcal{L}}$.

Proof. The case $q = 2$ was actually proved in [6], so we let $q > 2$.

(i) Without loss of generality we can assume $i = 0$. We have to prove that $R_p G_m(a) \supseteq \overline{\mathcal{L}}$ for any element $a \in \overline{\mathcal{L}}$, $a \notin \overline{\mathcal{L}}_0$. Write $\lambda_j = l_j(p-1) + d_j$, $1 \leqslant d_j \leqslant p-1$ for all j. Since $\widehat{S}(\bar{\lambda})$ is irreducible as $GL_m(q)$-module, we can assume that

$$a = b + b' + \mathcal{L}^0,$$

$$b = \big(Z_{00}^{p-1} \cdots Z_{l_0-1,0}^{p-1} Z_{l_0,0}^{d_0}\big) \cdots \big(Z_{0,t-1}^{p-1} \cdots Z_{l_{t-1}-1,t-1}^{p-1} Z_{l_{t-1},t-1}^{d_{t-1}}\big),$$

$$b' = p \sum_J \alpha_J Z^J,$$

where Z^J denotes a monomial in Z_{rs}. Let T be the diagonal subgroup of $GL_m(q)$. Since every $GL_m(q)$-module is a direct sum of its T-isotypic components, we may assume that a is T-stable. Let us study when two elements $b = \prod_{r,s} Z_{rs}^{i_{rs}}$ and $c = p\prod_{r,s} Z_{rs}^{j_{rs}}$ belong to one isotypic component of T. In this case we have

$$\sum_s i_{rs} p^s - \sum_s j_{rs} p^s \equiv 0 \pmod{p^t - 1}$$

for all r, therefore we have

$$b = Z' \prod_{r \in I_1} (Z_{r,0} \cdots Z_{r,t-1})^{p-1}, \qquad c = pZ' \prod_{r \in I_2} (Z_{r,0} \cdots Z_{r,t-1})^{p-1},$$

where $I_1 \cap I_2 = \emptyset$, and

$$\sum_r i_{rs} - \sum_r j_{rs} = |I_1|(p-1) - |I_2|(p-1) = \big(|I_1| - |I_2|\big)(p-1)$$

for all s. On the other hand, we have

$$\begin{aligned} i_{00} + i_{10} + \cdots + i_{m-1,0} &= \lambda_0, \\ &\vdots \\ i_{0,t-1} + i_{1,t-1} + \cdots + i_{m-1,t-1} &= \lambda_{t-1}, \end{aligned}$$

and

$$\begin{aligned} j_{00} + j_{10} + \cdots + j_{m-1,0} &= \lambda_0 - p, \\ j_{01} + j_{11} + \cdots + j_{m-1,1} &= \lambda_1 + 1, \\ &\vdots \\ j_{0,t-1} + j_{1,t-1} + \cdots + j_{m-1,t-1} &= \lambda_{t-1}. \end{aligned}$$

Such element c does not exist unless $t = 1$. But the case $t = 1$ was considered in [6]. Therefore $a = b + \mathcal{L}^0$.

Now consider an element $g \in GL_m(q)$ defined by

$$\hat{g}(Z_{l_0,d}) \equiv Z_{l_0-1,d} + Z_{l_0,d} \pmod{\mathcal{A}^{(2)}},$$

$$\hat{g}(Z_{sd}) \equiv Z_{sd} \pmod{\mathcal{A}^{(2)}},\ s \neq l_0$$

(we recall that $\lambda_0 = l_0(p-1) + d_0$). Writing

$$b = Z'\left(Z_{l_0-1,0}^{i_{l_0-1,0}} \cdots Z_{l_0-1,t-1}^{i_{l_0-1,t-1}}\right)\left(Z_{l_0,0}^{i_{l_0,0}} \cdots Z_{l_0,t-1}^{i_{l_0,t-1}}\right),$$

where $i_{l_0,0} = d_0$, $i_{l_0-1,0} = p-1$, Z' contains no variables $Z_{l_0-1,d}$ and $Z_{l_0,d}$, we see that

$$\begin{aligned} \hat{g}(b) \equiv Z'\left(Z_{l_0-1,0}^{i_{l_0-1,0}} \cdots Z_{l_0-1,t-1}^{i_{l_0-1,t-1}}\right)&(Z_{l_0-1,0} + Z_{l_0,0})^{i_{l_0,0}} \\ &\cdots (Z_{l_0-1,t-1} + Z_{l_0,t-1})^{i_{l_0,t-1}} \pmod{\mathcal{L}^0}. \end{aligned}$$

Hence $\hat{g}(b) - b + \mathcal{L}^0$ is a nonzero element in $\overline{\mathcal{L}}_0$, which generates $\overline{\mathcal{L}}_0$.

(ii) From [5, Proposition 9(x)] we know that

$$Z_{s,0}^{p-1} Z_{s,1}^{p-1} \cdots Z_{s,t-1}^{p-1} = (-1)^{t-1}\left(\sum_{\alpha \in \mathbb{F}_q} X^{\alpha e_s} - qX^0\right). \tag{5}$$

Therefore

$$\prod_{s=0}^{m-1}\prod_{d=0}^{t-1} Z_{sd}^{p-1} = (-1)^{m(t-1)} w - q(-1)^{(m-1)(t-1)} \sum_{j=0}^{m-1}\prod_{s\neq j}\prod_{d=0}^{t-1} Z_{sd}^{p-1} + q^2(\ldots).$$

On the other hand, $w \in \mathcal{L}$ by Lemma 4.2. The element $q\sum_{j=0}^{m-1}\prod_{s\neq j}\prod_{d=0}^{t-1} Z_{sd}^{p-1}$ generates $q\mathcal{L}((m-1)(p-1),\dots,(m-1)(p-1))$ modulo $\widetilde{\mathcal{L}}$. □

Remark. It might be noticed that the previous lemma is similar to Theorem 6.1 from [9]. Moreover, it can be proved that the $GL_m(q)$-module $\mathcal{L}(\bar{\lambda})/\widetilde{\mathcal{L}}(\bar{\lambda})$ is isomorphic to the (unique) indecomposable module in $\widehat{\mathcal{F}}^k$ with the head $\widehat{S}(\bar{\lambda})$ for

$$\bar{\lambda} \neq \big(m(p-1),\dots,m(p-1)\big)$$

(where $k \equiv \sum \lambda_i p^i \pmod{q-1}$), and is isomorphic to

$$\widehat{\mathcal{F}}^{q-1} = \widehat{\mathcal{W}} \oplus \widehat{\mathcal{M}}[q-1](m-2,\dots,m-2)$$

for $\bar{\lambda} = ((m(p-1),\dots,m(p-1))$.

Lemma 4.6. *Let a be a monomial in Z_{sd}, $a \in \mathcal{L} = \mathcal{L}(\bar{\lambda})$, $a \notin \widetilde{\mathcal{L}} + \sum \mathcal{L}_i$. Then a generates $\mathcal{L}(\bar{\lambda})$ over R_pG_m.*

Proof. Denote

$$\mathcal{L}^{+r}\big(\bar{\lambda}\big) = \sum_{r_0+\cdots+r_{t-1}=r} \mathcal{L}(\lambda_0+r_0,\dots,\lambda_{t-1}+r_{t-1}) = \mathcal{A}^{(r)}\cdot\mathcal{L}\big(\bar{\lambda}\big).$$

Lemma 4.5 and Theorem 3.4 imply that a generates all elements of $\mathcal{L}(\bar{\lambda})$ modulo $\mathcal{L}^{+1}(\bar{\lambda})$. Multiplying a by Z_{sd} and applying Lemma 4.5 again, we see that a generates $\mathcal{L}(\bar{\lambda})$ modulo $\mathcal{L}^{+2}(\bar{\lambda})$, and so on. But there exists a number r such that $\mathcal{L}^{+r}(\bar{\lambda}) \subseteq p^n\mathcal{A}^0 \subseteq R_pG_ma$. □

Proof of Theorem 4.4. (i) By induction. Let $\mathcal{L}$ be a G_m-submodule in $\mathcal{A}^0$. If $\mathcal{L} \supseteq p\mathcal{A}^0$ then the statement follows from Theorem 3.6.

Suppose now $\mathcal{L} \supseteq p^s\mathcal{A}^0$. Theorem 3.6 implies that $(\mathcal{L}+p\mathcal{A}^0)/p\mathcal{A}^0$ is equal to a sum of several modules $\mathcal{R}(\bar{\lambda})$. First we assume that

$$\big(\mathcal{L}+p\mathcal{A}^0\big)/p\mathcal{A}^0 \ncong \widehat{S}\big(m(p-1),\dots,m(p-1)\big).$$

Let $a = b + c \in \mathcal{L}$, $b \in \mathcal{L}(\bar{\lambda})$, $b \notin \mathcal{A}^0\mathcal{L}(\bar{\lambda})$, $b \notin p\mathcal{A}^0$, $c \notin \mathcal{L}(\bar{\lambda})$. Consider modules

$$\mathcal{L}_0 = \mathcal{L}\big(\bar{\lambda}\big) \cap p\mathcal{A} + \sum_j \mathcal{L}(\lambda_0,\dots,\lambda_j+1,\dots,\lambda_{t-1}) + \sum_j \mathcal{L}(\dots,\lambda_j+p,\lambda_{j+1}-1,\dots),$$

$$\mathcal{L}' = (R_pG_mb + R_pG_mc + \mathcal{L}_0)/\mathcal{L}_0.$$

It is clear that there is only one submodule in $\mathcal{L}'$ isomorphic to $\widehat{S}(\bar{\lambda})$ and it is a direct summand in $\mathcal{L}'$. Therefore $b \in \mathcal{L}$.

Continuing such reasoning we see that $\mathcal{L}$ is a sum of several modules $\mathcal{L}(\bar{\lambda})$ and (possibly) a module $p\mathcal{L}_1$, $\mathcal{L}_1 \supseteq p^{s-1}\mathcal{A}^0$. Induction finishes the proof.

If $(\mathcal{L}+p\mathcal{A}^0)/p\mathcal{A}^0 \cong \widehat{S}(m(p-1),\dots,m(p-1))$ then we can write $\mathcal{L}=\langle w\rangle + p^d\mathcal{L}_1$ for some module $\mathcal{L}_1$, $d>0$.

(ii) Let $\mathcal{L}\not\subseteq\mathcal{A}^0$. The difference of this case from the previous is that the $GL_m(q)$-module $\mathcal{A}/p\mathcal{A}\cong\mathcal{F}$ contains two isomorphic factors.

If $\mathcal{L}+p\mathcal{A}/p\mathcal{A}\ncong\widehat{S}(m(p-1),\dots,m(p-1))$ then $\mathcal{L}'=\mathcal{A}^0\mathcal{L}=\sum_{i,j}Z_{ij}\mathcal{L}$ is an invariant submodule in $\mathcal{A}^0$. Therefore $w\in\mathcal{L}'$ (see Lemma 4.2) and $\mathcal{L}$ is of type III.

If $\mathcal{L}+p\mathcal{A}/p\mathcal{A}\cong\widehat{S}(m(p-1),\dots,m(p-1))$ then $w+p^rbX^0\in\mathcal{L}$ for some r and b (note that $\langle w\rangle$ and $\langle X^0\rangle$ are isomorphic as $GL_m(q)$-modules). If $r=n$, $b=1$ then $w+p^rbX^0=\sum X^v$. The last element is invariant under G_m, so we have that $\mathcal{L}$ is of type V. Suppose now that $\mathcal{L}$ is not of type V. Then $\mathcal{L}$ is of type IV, and l is determined as the minimal number such that $p^lw\in\mathcal{L}$. Furthermore, $l\leqslant n$ and $l\leqslant r$, since $w+p^rbX^0\in\mathcal{L}$ follows $\mathcal{L}\supseteq p^r\mathcal{A}^0$. Also we have $l\leqslant s$ since $\mathcal{L}\supseteq p^s\mathcal{L}^0$, $\mathcal{L}^0$ is of type I. □

The next theorem is very important because of its coding theory consequences. We identify $p^{d-1}\mathcal{A}/p^d\mathcal{A}$ with $\mathcal{F}$ by dividing by p^{d-1}.

Theorem 4.7. *Let $\mathcal{L}$ be an R_p-submodule in $\mathcal{A}^0$, $\mathcal{M}_d=(\mathcal{L}\cap p^{d-1}\mathcal{A}+p^d\mathcal{A})/p^d\mathcal{A}$. Then $\mathcal{L}$ is invariant under G_m if and only if the following conditions hold*:

(i) *For all $d>0$, $\mathcal{M}_d$ is equal to a sum of several modules $\mathcal{M}(\lambda_0,\dots,\lambda_{t-1})$.*
(ii) *For all $d>0$, the condition $\mathcal{M}(\lambda_0,\dots,\lambda_{t-1})\subseteq\mathcal{M}_d$, $\lambda_j<(m-1)(p-1)$, $\lambda_{j+1}>0$ implies $\mathcal{M}(\dots,\lambda_j+p,\lambda_{j+1}-1,\dots)\subseteq\mathcal{M}_{d+1}$.*
(iii) *For all $d>0$, the condition $\mathcal{M}(\lambda_0,\dots,\lambda_{t-1})\subseteq\mathcal{M}_d$, $\lambda_j=\lambda_{j+1}=\cdots=\lambda_{j+a-1}=0$, $\lambda_{j+a}>0$, $a>0$ implies $\mathcal{M}(\dots,\lambda_{j-1},p-1,\dots,p-1,\lambda_{j+a}-1,\dots)\subseteq\mathcal{M}_{d+a}$.*

Proof. The statement of the theorem is a consequence of Theorems 4.4 and 3.6. If $p^d\mathcal{L}(\mu_0,\dots,\mu_{t-1})\subseteq\mathcal{L}$, $\mu_j\geqslant p$, $\mu_{j+1}<m(p-1)$ then

$$p^{d+1}\mathcal{L}(\dots,\mu_j-p,\mu_{j+1}+1,\dots)\subseteq\mathcal{L},$$

which reflects condition (ii). If $\mu_j\geqslant p$, $\mu_{j+1}=\cdots=\mu_{j+a-1}=m(p-1)$, $\mu_{j+a}<m(p-1)$ then

$$\begin{aligned}&p^{d+1}\mathcal{L}(\dots,\mu_j-p,\mu_{j+1}+1,\dots)\\&\quad=p^{d+2}\mathcal{L}(\dots,\mu_j-p,\mu_{j+1}+1-p,\mu_{j+2}+1,\dots)\\&\quad=\cdots=p^{d+a}\mathcal{L}\big(\dots,\mu_j-p,(m-1)(p-1),\dots,(m-1)(p-1),\mu_{j+a}+1,\dots\big),\end{aligned}$$

so

$$p^{d+a}\mathcal{L}\big(\dots,\mu_j-p,(m-1)(p-1),\dots,(m-1)(p-1),\mu_{j+a}+1,\dots\big)\subseteq\mathcal{L}.$$

But this inclusion can be obtained by several consecutive considerations:

$$\begin{aligned}\mathcal{L} &\supseteq p^{d+1}\mathcal{L}\big(\ldots, m(p-1), m(p-1)-p, \mu_{j+a}+1, \ldots\big)\\ &\supseteq p^{d+2}\mathcal{L}\big(\ldots, m(p-1)-p, (m-1)(p-1), \mu_{j+a}+1, \ldots\big)\\ &\ \ \vdots\\ &\supseteq p^{d+a}\mathcal{L}\big(\ldots, \mu_j-p, (m-1)(p-1), \ldots, (m-1)(p-1), \mu_{j+a}+1, \ldots\big).\end{aligned}$$

Finally, if $p^d\mathcal{L}(\mu_0, \ldots, \mu_{t-1}) \subseteq \mathcal{L}$, $\mu_j = \cdots = \mu_{j+a-1} = m(p-1)$, $\mu_{j+a} < m(p-1)$ then, applying multiplications by Z_{sj}, we see that

$$\begin{aligned}\mathcal{L} &\supseteq p^{d}\mathcal{L}\big(\ldots, \mu_{j-1}, m(p-1)+1, m(p-1), \ldots, \mu_{j+a}, \ldots\big)\\ &\supseteq p^{d+1}\mathcal{L}\big(\ldots, \mu_{j-1}, (m-1)(p-1), m(p-1)+1, \ldots, \mu_{j+a}, \ldots\big)\\ &\ \ \vdots\\ &\supseteq p^{d+a}\mathcal{L}\big(\ldots, \mu_{j-1}, (m-1)(p-1), \ldots, (m-1)(p-1), \mu_{j+a}+1, \ldots\big),\end{aligned}$$

which reflects condition (iii). □

4.2. Lattices over $\mathbb{Z}_p$

The next lemma, which follows from Lemma 3.9 by Nakayama's lemma, explains the connection between lattices in $\mathcal{A}$ and A (see also [5]).

Lemma 4.8. *Let U be a free $\mathbb{Z}_p$-module with basis $\{g_1, \ldots, g_n\}$ and let a group H act on the module U. Let $\mathcal{U} = \sum_{i=1}^{n} R_p g_i \supseteq U$ be a free module over the ring R_p with the same basis and the action of H is extended to $\mathcal{U}$ in the natural way. Then the map*

$$\mu : \mathcal{L} \mapsto \mathcal{L} \cap U$$

defines a bijective correspondence between the set of R_p-submodules of $\mathcal{U}$ that are invariant under H and σ, and the set of $\mathbb{Z}_p$-submodules in U that are invariant under H.

Define

$$L(\bar{\lambda}) = A \cap \sum_{i=0}^{t-1} \hat{\sigma}\big(\mathcal{L}(\bar{\lambda})\big), \quad A^0 = A \cap \mathcal{A}^0,$$

and we call a lattice $L \subseteq A$ of type X if $\mathcal{L} \subseteq \mathcal{A}$ is a lattice of type X and

$$L = A \cap \sum_{i=0}^{t-1} \hat{\sigma}(\mathcal{L}).$$

Lemma 4.8 and Theorems 4.4, 4.7 imply the following theorems.

Theorem 4.9. *The following assertions hold*:

(i) *Any G_m-invariant lattice L in A^0, $L \not\subseteq pA^0$, is equal to a lattice of type* I *or* II.
(ii) *Any G_m-invariant full lattice L in A, $L \not\subseteq pA$, is equal to a lattice of type* III, IV *or* V.

Now we identify $p^{d-1}A/p^dA$ with $\overline{A}$ by dividing by p^{d-1}.

Theorem 4.10. *Let L be a $\mathbb{Z}_p$-submodule in A^0, $M_d = (L \cap p^{d-1}A + p^dA)/p^dA$. Then L is invariant under G_m if and only if the following conditions hold*:

(1) *For all $d > 0$, M_d is equal to a sum of several modules $M(\lambda_0, \ldots, \lambda_{t-1})$.*
(2) *For all $d > 0$, the condition $M(\lambda_0, \ldots, \lambda_{t-1}) \subseteq M_d$, $\lambda_j < (m-1)(p-1)$, $\lambda_{j+1} > 0$ implies $M(\ldots, \lambda_j + p, \lambda_{j+1} - 1, \ldots) \subseteq M_{d+1}$.*
(3) *For all $d > 0$, the condition $M(\lambda_0, \ldots, \lambda_{t-1}) \subseteq M_d$, $\lambda_j = \lambda_{j+1} = \cdots = \lambda_{j+a-1} = 0$, $\lambda_{j+a} > 0$, $a > 0$, implies $M(\ldots, \lambda_{j-1}, p-1, \ldots, p-1, \lambda_{j+a} - 1, \ldots) \subseteq M_{d+a}$.*

5. Barnes–Wall lattices

This section gives a construction for the Barnes–Wall lattices. Let $p = 2$, $t = 1$, $m = n$. Then $G_m = AGL_n(2)$. Let $\Lambda^{(j)}$ be the ideal in the ring $\Lambda = \{\sum_{v \in V} a_v X^v \mid a_v \in \mathbb{Z}\}$ generated by elements $(1 - X^{v_1}) \cdots (1 - X^{v_j})$, $v_i \in V$. Let

$$\Gamma_1 = \Lambda^{(n)} + 2\Lambda^{(n-2)} + 2^2\Lambda^{(n-4)} + 2^3\Lambda^{(n-6)} + \cdots + 2^{[(n+1)/2]}\Lambda^{(0)},$$
$$\Gamma_2 = \Lambda^{(n-1)} + 2\Lambda^{(n-3)} + 2^2\Lambda^{(n-5)} + 2^3\Lambda^{(n-7)} + \cdots + 2^{[n/2]}\Lambda^{(0)}.$$

These lattices are similar to the Barnes–Wall lattices [10], since the codes

$$C_i = \left(\Gamma_j \cap p^i\Lambda + p^{i+1}\Lambda\right)/p^{i+1}\Lambda$$

form a nested sequence of binary Reed–Muller codes of length 2^n. In fact,

$$\frac{1}{2^{[(n+1)/2]/2}}\Gamma_1 \quad \text{and} \quad \frac{1}{2^{[(n-1)/2]/2}}\Gamma_2$$

are isometric to the Barnes–Wall lattices. They are unimodular for odd n and modular of level 2 for even n. The minimal norm of the Barnes–Wall lattice of rank 2^n is equal to $2^{[n/2]}$. It is clear that lattices Γ_1 and Γ_2 are invariant under G_m. Recall that the automorphism group of the Barnes–Wall lattice is isomorphic to $2_+^{1+2n}\Omega_{2n}^+(2)$.

Acknowledgments

I thank anonymous referee for his useful suggestions. This research results were attained with the assistance of the Alexander von Humboldt Foundation. I am very grateful to my host professor R. Scharlau for stimulating conversations and generous hospitality.

References

[1] K.S. Abdukhalikov, Invariant integral lattices in Lie algebras of type A_{p^m-1}, Mat. Sb. 184 (4) (1993) 61–104; English translation in: Russian Acad. Sci. Sb. Mat. 78 (4) (1994) 447–478.

[2] K.S. Abdukhalikov, Integral lattices associated with a finite affine group, Mat. Sb. 185 (12) (1994) 3–18 (in Russian); English translation in: Russian Acad. Sci. Sb. Mat. 83 (2) (1995) 431–443.

[3] K.S. Abdukhalikov, Doubly transitive groups and lattices, J. Math. Sci. 93 (6) (1999) 809–823.

[4] K.S. Abdukhalikov, Defining sets of cyclic codes invariant under the affine group, in: D. Augot et al. (Eds.), WCC 2001 International Workshop on Coding and Cryptography, Paris, France, January 8–12, 2001, in: Electron. Notes Discrete Math., vol. 6, Elsevier, Amsterdam, 2001.

[5] K.S. Abdukhalikov, Affine invariant and cyclic codes over p-adic numbers and finite rings, Des. Codes Cryptogr. 23 (3) (2001) 343–370.

[6] K.S. Abdukhalikov, Codes over p-adic numbers and finite rings invariant under the full affine group, Finite Fields Appl. 7 (4) (2001) 449–467.

[7] K.S. Abdukhalikov, Defining sets of extended cyclic codes invariant under the affine group, submitted for publication.

[8] E.F. Assmus, J.D. Key, Polynomial codes and finite geometries, in: V.S. Pless, W.C. Huffman (Eds.), Handbook of Coding Theory, vol. 2, Elsevier, 1998, pp. 1269–1343, Chapter 16.

[9] M. Bardoe, P. Sin, The permutation modules for $GL(n+1,\mathbb{F}_q)$ acting on $\mathbb{P}^n(\mathbb{F}_q)$ and $\mathbb{F}_q^{n+1}$, J. London Math. Soc. (2) 61 (1) (2000) 58–80.

[10] E.S. Barnes, N.J.A. Sloane, New lattice packings of spheres, Canadian J. Math. 35 (1983) 117–130.

[11] T. Berger, P. Charpin, The permutation group of affine-invariant extended cyclic codes, IEEE Trans. Inform. Theory 42 (6) (1996) 2194–2209.

[12] T.P. Berger, Automorphism groups and permutation groups of affine-invariant codes, in: Finite Fields and Applications, Proceedings of the 3rd International Conference, Glasgow, UK, July 11–14, 1995, in: London Math. Soc. Lecture Note Ser., vol. 233, Cambridge University Press, Cambridge, 1996, pp. 31–45.

[13] A.I. Bondal, A.I. Kostrikin, P.H. Tiep, Invariant lattices, the Leech lattice and its even unimodular analogs in the algebras A_{p-1}, Mat. Sb. 130 (172) (1986) 435–464; English translation in: Math. USSR Sb. 58 (1987).

[14] P. Charpin, Codes cycliques étendus invariants sous le groupe affine, Thèse de Doctorat d'État, Université Paris VII, 1987.

[15] P. Delsarte, On cyclic codes that are invariant under the general linear group, IEEE Trans. Inform. Theory 16 (1970) 760–769.

[16] R. Hammons, P.V. Kumar, A.R. Calderbank, N.J.A. Sloane, P. Solé, The Z_4-linearity of Kerdock, Preparata, Goethals, and related codes, IEEE Trans. Inform. Theory 40 (2) (1994) 301–319.

[17] T. Kasami, S. Lin, W.W. Peterson, Some results on cyclic codes which are invariant under the affine group and their applications, Inform. and Control 11 (1967) 475–496.

[18] A.I. Kostrikin, P.H. Tiep, Orthogonal Decompositions and Integral Lattices, de Gruyter, Berlin, 1994.

[19] N.S.N. Sastry, P. Sin, On the double transitive permutation representations of $\mathrm{Sp}(2n,\mathbb{F}_p)$, J. Algebra 257 (2002) 509–527.

[20] P. Sin, The permutation representations of $\mathrm{Sp}(2m,\mathbb{F}_p)$ acting on the vectors of its standard module, J. Algebra 241 (2001) 578–591.