On free elementary $\mathbb{Z}_p C_p$ -lattices

GABRIELE NEBE

Abstract. We show that all elementary lattices that are free $\mathbb{Z}_p C_p$ -modules admit an orthogonal decomposition into a sum of a free unimodular and a p -modular $\mathbb{Z}_p C_p$ -lattice.

Mathematics Subject Classification. 11H56, 11E08.

Keywords. Quadratic forms over local rings, Automorphism groups of lattices, Free modules, Jordan decomposition, Smith normal form.

1. Introduction. Let $R := \mathbb{Z}_p C_p$ denote the group ring of the cyclic group of order p over the localisation of $\mathbb{Z}$ at the prime p . The present paper considers free R -lattices $L \cong R^a$. The main observation in this situation is Theorem 2.2: Given two free R -modules M and L with $pM \subseteq L \subseteq M$, there is an R -basis $(g_1, \dots, g_a)$ of M and $0 \leq t \leq a$ such that $(g_1, \dots, g_t, pg_{t+1}, \dots, pg_a)$ is an R -basis of L . So these lattices do admit a compatible basis. Applying this observation to Hermitian R -lattices shows that free elementary Hermitian R -lattices admit an invariant splitting (see Theorem 4.1) as the orthogonal sum of a free unimodular lattice and a free p -modular lattice.

The results of this note have been used in the thesis [1] to study extremal lattices admitting an automorphism of order p in the case that p divides the level of the lattice.

2. Existence of compatible bases. For a prime p , we denote by

$$\mathbb{Z}_p := \left\{ \frac{a}{b} \in \mathbb{Q} \mid p \text{ does not divide } b \right\}$$

the localisation of $\mathbb{Z}$ at the prime p . The following arguments also apply accordingly to the completion of this discrete valuation ring. Let $R := \mathbb{Z}_p C_p$ denote the group ring of the cyclic group $C_p = \langle \sigma \rangle$ of order p . Then $e_1 := \frac{1}{p}(1 + \sigma + \dots + \sigma^{p-1}) \in \mathbb{Q} C_p$ and $e_\zeta := 1 - e_1$ are the primitive idempotents in the group algebra $\mathbb{Q} C_p$ with $\mathbb{Q} C_p = \mathbb{Q} C_p e_1 \oplus \mathbb{Q} C_p e_\zeta \cong \mathbb{Q} \oplus \mathbb{Q}[\zeta_p]$, where ζ_p is

a primitive p -th root of unity. The ring $T := \mathbb{Z}_p[\zeta_p]$ is a discrete valuation ring in the p -th cyclotomic field $\mathbb{Q}[\zeta_p]$ with prime element $\pi := (1 - \zeta_p)$ and hence

$$Re_1 \oplus Re_\zeta \cong \mathbb{Z}_p \oplus \mathbb{Z}_p[\zeta_p] =: S \oplus T$$

is the unique maximal $\mathbb{Z}_p$ -order in $\mathbb{Q}C_p$.

Remark 2.1. With the notation above, $T/(\pi) \cong \mathbb{Z}_p/(p) \cong \mathbb{F}_p$ and via this natural ring epimorphism,

$$R = \{(x, y) \in \mathbb{Z}_p \oplus \mathbb{Z}_p[\zeta_p] \mid x + p\mathbb{Z}_p = y + \pi\mathbb{Z}_p[\zeta_p]\}.$$

R is generated as $\mathbb{Z}_p$ -algebra by $1 = (1, 1)$ and $1 - \sigma = (0, \pi)$. Moreover $Re_1 \cap R = pRe_1 = pS$ and $Re_\zeta \cap R = \pi Re_\zeta = \pi T$ and the radical $J(R) := pS \oplus \pi T$ of R is the unique maximal ideal of the local ring R .

By [6], the indecomposable R -lattices are the free R -module R , the trivial R -lattice $\mathbb{Z}_p = Re_1 = S$, and the lattice $\mathbb{Z}_p[\zeta_p] = Re_\zeta = T$ in the rational irreducible faithful representation of C_p . The theorem by Krull-Remak-Schmidt-Azumaya [2, Chapter 1, Section 11] ensures that any finitely generated R -lattice L is a direct sum of indecomposable R -lattices

$$L \cong R^a \oplus T^b \oplus S^c.$$

In this note, we focus on the case of free R -lattices. Though R is not a principal ideal domain, for certain sublattices of free R -lattices, there do exist compatible bases:

Theorem 2.2. *Let $M \cong R^a$ be a free R -lattice of rank a . Assume that L is a free R -lattice with $pM \subseteq L \subseteq M$. Then there is an R -basis $(g_1, \dots, g_a)$ of $M = Rg_1 \oplus \dots \oplus Rg_a$ and $0 \leq t \leq a$ such that*

$$L = Rg_1 \oplus \dots \oplus Rg_t \oplus pRg_{t+1} \oplus \dots \oplus pRg_a.$$

Proof. Let $\tilde{S} := Me_1$ and $\tilde{T} := Me_\zeta$. Now $M \cong R^a$ is a free R -lattice, so, as in Remark 2.1, M is a sublattice of $\tilde{S} \oplus \tilde{T}$ of index p^a , $\tilde{S} \cap M = p\tilde{S}$, and $\tilde{T} \cap M = \pi\tilde{T}$. The Jacobson radical is $J(M) = J(R)M = p\tilde{S} \oplus \pi\tilde{T}$ and of index p^a in M . We proceed by induction on a .

If $a = 1$, then $M = R$, $\tilde{S} \cong S$, $\tilde{T} \cong T$. As $M/pM \cong \mathbb{F}_p C_p \cong \mathbb{F}_p[x]/(x-1)^p$ is a chain ring, the R -sublattices of M that contain pM form a chain:

$$M \supset p\tilde{S} \oplus \pi\tilde{T} \supset p\tilde{S} \oplus \pi^2\tilde{T} \supset \dots \supset p\tilde{S} \oplus \pi^{p-2}\tilde{T} \supset p\tilde{S} \oplus \pi\tilde{T} \supset pM.$$

The only free R -lattices among these are M and pM .

Now assume that $a > 1$. If $L \not\subseteq J(M)$, then we may choose $g_1 \in L \setminus J(M)$. As $g_1 \notin J(M)$, the R -submodule Rg_1 of M is a free submodule of both modules L and M , so $M = Rg_1 \oplus M'$, $L = Rg_1 \oplus L'$ where M' and $L' = L \cap M'$ are free R -lattices of rank $a - 1$ satisfying the assumption of the theorem and the theorem follows by induction. So we may assume that

$$L \subseteq J(M) = p\tilde{S} \oplus \pi\tilde{T}. \quad (1)$$

The element $e_1 \in \mathbb{Q}C_p$ is a central idempotent in $\text{End}_R(J(M))$ projecting onto $p\tilde{S} = J(M)e_1$. The assumption that $pM \subseteq L \subseteq J(M)$ implies that

$$p\tilde{S} = pMe_1 \subseteq Le_1 \subseteq J(M)e_1 = p\tilde{S}.$$

So $Le_1 = pMe_1 = p\tilde{S}$.

To show that $L = pM$, we first show that $Le_\zeta = pMe_\zeta$.

As $pM \subseteq L$, we clearly have that $pMe_\zeta \subseteq Le_\zeta$.

To see the opposite inclusion, put $K := L \cap Le_\zeta$ to be the kernel of the projection $e_1 : L \rightarrow Le_1$. As L is free, we get, as in Remark 2.1, that $K = \pi Le_\zeta$. Let k be maximal such that $K \subseteq \pi^k \tilde{T}$. Then $k \geq 2$ because $Le_\zeta \subseteq \pi \tilde{T}$ (see equation (1)).

Assume that $k \leq p - 1$. There is $\ell \in L$ such that $y = \ell e_\zeta \notin \pi^k \tilde{T}$. As $pMe_1 = Le_1$, there is $m \in M$ such that $pme_1 = \ell e_1$. Now $pM \subseteq L$, so $pm \in L$ and $\ell - pm \in K = Ke_\zeta$.

We compute $\ell - pm = (\ell - pm)e_\zeta = y - pme_\zeta$.

As $pMe_\zeta = p\tilde{T} = \pi^{p-1}\tilde{T}$ and $y \notin \pi^k \tilde{T}$, the assumption that $k \leq p - 1$ shows that $\ell - pm \notin \pi^k \tilde{T}$, which contradicts the definition of k .

Therefore $k \geq p$ and $Le_\zeta \subseteq pMe_\zeta$.

Now pM and L both have index p^a in $pMe_1 \oplus pMe_\zeta = Le_1 \oplus Le_\zeta$ (again by Remark 2.1 as L and M are free). So the assumption $pM \subseteq L$ implies that $pM = L$. $\square$

Remark 2.3. Let $M \cong T^b \oplus S^c$ and let L be a sublattice of M again isomorphic to $T^b \oplus S^c$. Then $M = Me_\zeta \oplus Me_1$ and $L = Le_\zeta \oplus Le_1$. By the main theorem for modules over principal ideal domains, there is a T -basis $(x_1, \dots, x_b)$ of Me_ζ and a $\mathbb{Z}_p$ -basis $(y_1, \dots, y_c)$ of Me_1 , as well as $0 \leq n_1 \leq \dots \leq n_b$, $0 \leq m_1 \leq \dots \leq m_c$, such that $L = \bigoplus_{i=1}^b \pi^{n_i} T x_i \oplus \bigoplus_{i=1}^c p^{m_i} \mathbb{Z}_p y_i$.

Example 2.4. For general modules M , however, Theorem 2.2 has no appropriate analogue. To see this, consider $M \cong R \oplus S$ and choose a pseudo-basis (x, y) of M such that x generates a free direct summand and y , its complement isomorphic to S . Let L be the R -sublattice generated by pxe_1 and $x(1 - \sigma) + y$. As $x(1 - \sigma) + y$ generates a free R -sublattice of M and $R(pxe_1) \cong S$, we have $L \cong S \oplus R$. For $p > 2$, we compute that $pM \subseteq L \subseteq M$. Then the fact that $|M/L| = p^2$ implies that these two modules do not admit a compatible pseudo-basis.

3. Lattices in rational quadratic spaces. From now on, we consider $\mathbb{Z}_p$ -lattices L in a non-degenerate rational quadratic space (V, B) . The *dual lattice* of L is

$$L^\# := \{x \in V \mid B(x, \ell) \in \mathbb{Z}_p \text{ for all } \ell \in L\}.$$

The lattice L is called *integral* if $L \subseteq L^\#$, and *elementary* if

$$pL^\# \subseteq L \subseteq L^\#.$$

Following O'Meara [5, Section 82 G], we call a lattice L *unimodular* if $L = L^\#$, and *p^j -modular* if $p^j L^\# = L$.

We now assume that σ is an automorphism of L of order p , so σ is an orthogonal mapping of (V, B) with $L\sigma = L$. Then also the dual lattice $L^\#$ is a σ -invariant lattice in V . As the dual basis of a lattice basis of L is a lattice basis of $L^\#$, the symmetric bilinear form B yields an identification between $L^\#$ and the lattice $\text{Hom}_{\mathbb{Z}_p}(L, \mathbb{Z}_p)$ of $\mathbb{Z}_p$ -valued linear forms on L . The σ -invariance of B shows that this is an isomorphism of $\mathbb{Z}_p[\sigma]$ -modules.

Remark 3.1. As a $\mathbb{Z}_p[\sigma]$ -module, we have $L^\# \cong \text{Hom}_{\mathbb{Z}_p}(L, \mathbb{Z}_p)$.

As all indecomposable $\mathbb{Z}_p[\sigma]$ -lattices are isomorphic to their homomorphism lattices, we obtain

Proposition 3.2 ([4, Lemma 5.6]). *If $L \cong R^a \oplus T^b \oplus S^c$ as $\mathbb{Z}_p[\sigma]$ -lattice, then also $L^\# \cong R^a \oplus T^b \oplus S^c$.*

The group ring R comes with a natural involution, the unique $\mathbb{Z}_p$ -linear map $^- : R \rightarrow R$ with $\overline{\sigma^i} = \sigma^{-i}$ for all $0 \leq i \leq p-1$. This involution is the restriction of the involution on the maximal order $S \oplus T$ that is trivial on S and the complex conjugation on T .

Remark 3.3. The $\mathbb{Z}_p$ -lattice R is unimodular with respect to the symmetric bilinear form

$$R \times R \rightarrow \mathbb{Z}_p, (x, y) \mapsto \frac{1}{p} \text{Tr}_{\text{reg}}(x\bar{y})$$

where $\text{Tr}_{\text{reg}} : \mathbb{Q}C_p \rightarrow \mathbb{Q}$ denotes the regular trace of the p -dimensional $\mathbb{Q}$ -algebra $\mathbb{Q}C_p$. We thus obtain a bijection between the set of σ -invariant $\mathbb{Z}_p$ -valued symmetric bilinear forms on the R -lattice L and the R -valued Hermitian forms on L : If $h : L \times L \rightarrow R$ is such a Hermitian form, then $B = \frac{1}{p} \text{Tr}_{\text{reg}} \circ h$ is a symmetric bilinear σ -invariant form on L . As $R = R^\#$, these forms yield the same notion of duality. In particular, the dual lattice $L^\#$ of a free lattice $L = \bigoplus_{i=1}^a Rg_i$ is again free $L^\# = \bigoplus_{i=1}^a Rg_i^*$ with the Hermitian dual basis $(g_1^*, \dots, g_a^*)$ as a lattice basis, giving a constructive argument for Proposition 3.2 for free lattices.

4. Free elementary lattices. In this section, we assume that L is an elementary lattice and σ an automorphism of L of prime order p . Recall that R is the commutative ring $R := \mathbb{Z}_p[\sigma]$, so L is an R -module.

Theorem 4.1. *Let p be a prime and let L be an elementary lattice with an automorphism σ such that $L \cong R^a$ is a free R -module. Then also $L^\# \cong R^a$ and there is an R -basis $(g_1, \dots, g_a)$ of $L^\#$ and $0 \leq t \leq a$ such that $(g_1, \dots, g_t, pg_{t+1}, \dots, pg_a)$ is an R -basis of L . In particular, L is the orthogonal sum of the unimodular free R -lattice $L_0 := Rg_1 \oplus \dots \oplus Rg_t$ and a p -modular free R -lattice $L_1 := L_0^\perp$.*

Proof. Under the assumption, both lattices L and $M := L^\#$ are free R -modules satisfying $pM \subseteq L \subseteq M$. So, by Theorem 2.2, there is a basis $(g_1, \dots, g_a)$ of M such that $(g_1, \dots, g_t, pg_{t+1}, \dots, pg_a)$ is a basis of L . Clearly L is an integral lattice and $L_0 := Rg_1 \oplus \dots \oplus Rg_t$ is a unimodular sublattice of L . By [3, Satz 1.6], unimodular free sublattices split as orthogonal summands, so $L = L_0 \perp L_1$ with $L_1^\# = \frac{1}{p}L_1$, i.e. L_1 is p -modular. $\square$

Note that the assumption that the lattice is elementary is necessary, as the following example shows.

Example 4.2. Let $L = Rg_1 \oplus Rg_2$ be a free lattice of rank 2 with R -valued Hermitian form defined by the Gram matrix

$$\begin{pmatrix} (p, 0) & (0, \pi) \\ (0, \bar{\pi}) & (p, 0) \end{pmatrix}.$$

Here we identify R as a subring of $S \oplus T$, so $(p, 0) = pe_1 = 1 + \sigma + \cdots + \sigma^{p-1}$ and $(0, \pi) = (0, (1 - \zeta_p)) = 1 - \sigma \in R$. Then L is orthogonally indecomposable because Le_ζ is an orthogonally indecomposable T -lattice, but L is not modular. Note that the base change matrix between (g_1, g_2) and the dual basis, an R -basis of $L^\#$, is the inverse of the Gram matrix above, so

$$\begin{pmatrix} (p^{-1}, 0) & (0, -\bar{\pi}^{-1}) \\ (0, -\pi^{-1}) & (p^{-1}, 0) \end{pmatrix}.$$

As $(1, 0) = e_1 \notin R$, this shows that $pL^\# \not\subseteq L$, so L is not an elementary lattice.

Funding Open Access funding enabled and organized by Projekt DEAL.

Open Access. This article is licensed under a Creative Commons Attribution 4.0 International License, which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons licence, and indicate if changes were made. The images or other third party material in this article are included in the article's Creative Commons licence, unless indicated otherwise in a credit line to the material. If material is not included in the article's Creative Commons licence and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder. To view a copy of this licence, visit <http://creativecommons.org/licenses/by/4.0/>.

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

References

- [1] Eisenbarth, S.: Gitter und Codes über Kettenringen. RWTH Aachen University, Thesis (2020)
- [2] Feit, W.: The representation theory of finite groups. North Holland (1982)
- [3] Kneser, M.: Quadratische Formen. Revised and edited in collaboration with Rudolf Scharlau. Springer-Verlag, Berlin (2002)
- [4] Nebe, G.: Automorphisms of modular lattices. J. Appl. Algebra, to appear
- [5] O'Meara, O.T.: Introduction to Quadratic Forms. Springer, Berlin (1973)
- [6] Reiner, I.: Integral representations of cyclic groups of prime order. Proc. Amer. Math. Soc. **8**, 142–146 (1957)

GABRIELE NEBE
Lehrstuhl für Algebra und Zahlentheorie
RWTH Aachen University
52056 Aachen
Germany
e-mail: `nebe@math.rwth-aachen.de`

Received: 26 October 2020

Revised: 8 December 2020

Accepted: 12 January 2021.