On homomorphisms of abelian groups of bounded exponent

Mathé Hertogh

July 7, 2017

Bachelor thesis

Thesis supervisor: Mima Stanojkovski

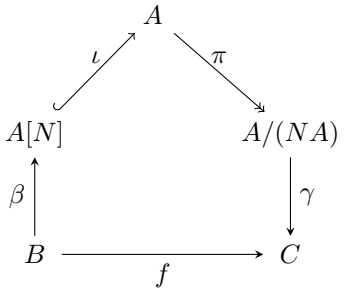
Leiden University
Mathematical Institute

Contents

Introduction

Let N be a positive integer and let A be an abelian group. There are two natural subgroups of A associated to the multiplication by N map in A, namely its kernel, denoted by $A[N]$, and its image, denoted by NA. Let $\iota : A[N] \to A$ be the inclusion map and let $\pi : A \to A/(NA)$ be the canonical projection. Then the map $\pi \circ \iota : A[N] \to A/(NA)$ is a $\mathbb{Z}/N\mathbb{Z}$-module homomorphism. In this thesis we classify homomorphisms of $\mathbb{Z}/N\mathbb{Z}$-modules that arise in this way.

Let $f : B \to C$ be a homomorphism of abelian groups. For each positive integer N, we define an *N-lift of f* to be an abelian group A such that there exist isomorphisms $\beta : B \to A[N]$ and $\gamma : A/(NA) \to C$ making the following diagram commutative.



Here ι is the inclusion map and π is the canonical projection.

Main Problem. For which pairs (N, f), where N is a positive integer and f is a homomorphism of abelian groups, does f have an N-lift?

A necessary condition for a homomorphism $f : B \to C$ of abelian groups to have an N-lift is that both B and C are $\mathbb{Z}/N\mathbb{Z}$-modules.

In Chapter 3 we will reduce the main problem to the case where N is a prime power. Let p be a prime number. For each abelian group A, we define the *p-primary part of A* to be the subgroup $A[p^\infty] = \bigcup_{i \geq 0} A[p^i]$. As a consequence of the definition of p-primary parts, each homomorphism $f : B \to C$ of abelian groups restricts to a homomorphism $f^{[p]} : B[p^\infty] \to C[p^\infty]$.

Theorem A. *Let N be a positive integer and $f : B \to C$ a homomorphism of $\mathbb{Z}/N\mathbb{Z}$-modules. Let $\prod_{i=1}^{t} p_i^{k_i}$ be the prime factorization of N, where the p_i's are distinct. Then there exists an N-lift of f if and only if, for each $i \in \{1, \ldots, t\}$, there exists a $p_i^{k_i}$-lift of $f^{[p_i]}$.*

Theorem A is the same as Theorem 3.1 and we prove it in Chapter 3. Theorem A reduces the main problem to classifying, for each prime number p and each positive integer k, the homomorphisms of $\mathbb{Z}/p^k\mathbb{Z}$-modules that have a p^k-lift. Deciding whether or not a homomorphism of $\mathbb{Z}/p^k\mathbb{Z}$-modules has a p^k-lift becomes easier with the introduction of certain submodules of $\mathbb{Z}/p^k\mathbb{Z}$-modules.

Let p be a prime number, let k be a positive integer and let B be a $\mathbb{Z}/p^k\mathbb{Z}$-module. A *p^k-non-free part of B* is a submodule M of B such that $M + pB = B[p^{k-1}]$ and such that, for each $s \in \mathbb{Z}_{\geq 0}$, one has $p^s B \cap M = p^s M$. In Chapter 4 we explore the properties of these submodules.

Theorem B. *Let p be a prime number, let k be a positive integer and let $f: B \to C$ be a homomorphism of $\mathbb{Z}/p^k\mathbb{Z}$-modules. Then the following statements are equivalent.*

(1) *There exists a p^k-lift of f.*

(2) *For each p^k-non-free part M of B, the map $f|_M : M \to f(M)$ is an isomorphism and $f(M)$ is a p^k-non-free part of C.*

(3) *There exist p^k-non-free parts M_B and M_C of B and C respectively, such that f restricts to an isomorphism $M_B \to M_C$.*

In Chapter 5 we give a constructive proof of Theorem B, which is the same as Theorem 5.1.

1 Preliminaries

Throughout this thesis we will denote all abelian groups additively. The vast majority of the time we will be working with groups. Hence we reserve the word homomorphism to mean group homomorphism. Similarly by an isomorphism we will mean a group isomorphism. Also we use the symbol $\cong$ to mean "isomorphic as groups".

Let A be an abelian group and N a positive integer. Consider the multiplication by N map in A, that is, the map $m_N : A \to A$ defined by $a \mapsto Na$. This map is a homomorphism since A is abelian. For each N, we call the kernel of m_N the *N-torsion of A* and we denote it by $A[N]$. Note that by definition $A[N]$ is a subgroup of A, which consists of precisely those elements of A whose order divides N. Also the image of m_N is a subgroup of A, which we denote by NA.

Lemma 1.1. *Let $(A_i)_{i\in I}$ be a family of abelian groups and N a positive integer. Then*

$$\left(\bigoplus_{i\in I} A_i\right)[N] = \bigoplus_{i\in I} A_i[N].$$

Proof. This is just a simple check of the definitions. □

Lemma 1.2. *Let $(A_i)_{i\in I}$ be a family of abelian groups and N a positive integer. Then*

$$N\left(\bigoplus_{i\in I} A_i\right) = \bigoplus_{i\in I} NA_i.$$

Proof. This is just a verification of the definitions. □

Definition 1.3. Let G be a group. We say that G is *torsion* if all elements of G are of finite order.

Definition 1.4. Let A be an abelian group. The *torsion subgroup of A* is the subgroup consisting of all elements of finite order and it is denoted by A_{tors}.

Note that, in Definition 1.4, the abelianness of A ensures that A_{tors} is indeed a subgroup of A.

Definition 1.5. Let G be a group. The *exponent of* G is the smallest positive integer N such that every element of G is annihilated by N. If such N does not exist, we say that G has infinite exponent.

It is clear from these definitions that any group of finite exponent is also torsion. However, the converse is not true. For example, $\mathbb{Q}/\mathbb{Z}$ is torsion, but has infinite exponent.

Lemma 1.6. *Let m and k be positive integers and let A be an abelian group such that $m^kA = 0$. Let H be a subgroup of A such that $A = H + mA$ and $H \cap mA = 0$. Then $mA = 0$.*

Proof. We claim that, for each positive integer i, one has $mA = m^iA$. We work by induction on i. The case $i = 1$ is clear. Assume now that $i > 1$ and that $m^{i-1}A = mA$. Since $i > 1$ it is clear that $m^iA \subset mA$. We will now show that $mA \subset m^iA$. By the induction hypothesis it suffices to show $m^{i-1}A \subset m^iA$. Let $a \in A$. Then there exist $h \in H$ and $b \in A$ such that $a = h + mb$. Note that we have $m^{i-1}H \subset H \cap mA = 0$, since $i > 1$. Hence $m^{i-1}a = m^{i-1}h + m^ib = m^ib \in m^iA$. Since a was chosen arbitrarily, this shows that $m^{i-1}A \subset m^iA$ and therefore $mA = m^iA$.

This proves the claim. We have proven in particular that $mA = m^kA = 0$. □

Lemma 1.7. *Let m and k be positive integers and let A be an abelian group such that $m^kA = 0$. If H is a subgroup of A such that $A = H + mA$, then $A = H$.*

Proof. Consider A/H and observe that $m(A/H) = (mA + H)/H = A/H$. Now we can apply Lemma 1.6 to A/H and its trivial subgroup $\{H\}$ to get that $0 = m(A/H) = A/H$, and so $A = H$. □

Definition 1.8. Let $(f_i : G_i \to G_i')_{i\in I}$ be a family of group homomorphisms. We define the *direct sum of* $(f_i : G_i \to G_i')_{i\in I}$ to be the homomorphism

$$\bigoplus_{i\in I} f_i : \bigoplus_{i\in I} G_i \to \bigoplus_{i\in I} G_i'$$

defined by

$$(g_i)_{i\in I} \mapsto (f_i(g_i))_{i\in I}.$$

In Definition 1.8, the fact that homomorphisms send the zero-element to the zero-element ensures that, for every element $(g_i)_{i\in I} \in \bigoplus_{i\in I} G_i$, the image $(f_i(g_i))_{i\in I}$ has finitely many non-zero entries and hence is an element of $\bigoplus_{i\in I} G_i'$. Hence $\bigoplus_{i\in I} f_i$ is well-defined. Furthermore, $\bigoplus_{i\in I} f_i$ is a homomorphism since all f_i's are.

Lemma 1.9. *Let $(f_i : G_i \to G_i')_{i\in I}$ be a family of group homomorphisms. The following statements hold.*

(a) *The map* $\bigoplus_{i\in I} f_i$ *is injective if and only if, for each* $i \in I$*, the map* f_i *is injective.*

(b) *The map* $\bigoplus_{i\in I} f_i$ *is surjective if and only if, for each* $i \in I$*, the map* f_i *is surjective.*

(c) *The map* $\bigoplus_{i\in I} f_i$ *is an isomorphism if and only if, for each* $i \in I$*, the map* f_i *is an isomorphism.*

Proof. Equivalences (a) and (b) are straightforward checks of the definitions and (c) is a consequence of those two. □

Lemma 1.10. *Let* $(A_i)_{i\in I}$ *be a family of abelian groups. For each* $i \in I$*, let* B_i *be a subgroup of* A_i*. Then the map*

$$\frac{\bigoplus_{i\in I} A_i}{\bigoplus_{i\in I} B_i} \longrightarrow \bigoplus_{i\in I} A_i/B_i$$

defined by

$$(a_i)_{i\in I} + \bigoplus_{i\in I} B_i \mapsto (a_i + B_i)_{i\in I}$$

is an isomorphism.

Proof. It is readily verified that the map

$$\bigoplus_{i\in I} A_i \to \bigoplus_{i\in I} A_i/B_i$$

defined by

$$(a_i)_{i\in I} \mapsto (a_i + B_i)_{i\in I}$$

is a surjective homomorphism with kernel $\bigoplus_{i\in I} B_i$. From this the lemma follows. □

Definition 1.11. Let A be an abelian group and H a subgroup of A. A *complement of* H *in* A is a subgroup K of A such that $H+K = A$ and $H\cap K = 0$.

Let A be an abelian group, let H be a subgroup of A and let K be a complement of H in A. Note that then also H is a complement of K in A. One checks easily that in this case the map

$$H \oplus K \to A$$

defined by

$$(h, k) \mapsto h + k$$

is an isomorphism. We will usually identify $H\oplus K$ with A using this isomorphism and we simply write $H \oplus K = A$.

Lemma 1.12. *Let* A *be an abelian group and let* B*,* C*, and* D *be subgroups of* A*, such that* $B \subset C$*. Then* $B + (C \cap D) = (B + D) \cap C$*.*

Proof. We have $B + (C \cap D) \subset B + D$ and $B + (C \cap D) \subset B + C \subset C$. Together this gives $B + (C \cap D) \subset (B + D) \cap C$.

For the other inclusion, let $x \in (B + D) \cap C$. Then there exist $b \in B$ and $d \in D$ such that $x = b + d$. Now we have $x \in C$ and $b \in B \subset C$. Hence we get $d = x - b \in C$. So we get $b + d \in B + (C \cap D)$. The choice of x being arbitrary, this proves $(B + D) \cap C \subset B + (C \cap D)$. □

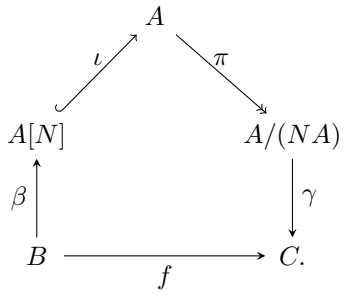
2 Lifts

In this section we will formulate the main problem of this thesis. Let A be an abelian group and N a positive integer. Let $\iota : A[N] \to A$ be the inclusion map and let $\pi : A \to A/(NA)$ be the canonical projection. Both ι and π are homomorphisms and so their composition

$$\pi \circ \iota : A[N] \to A/(NA)$$

is a homomorphism as well. The goal of this thesis will be to classify the homomorphisms that arise in this way. To make this more precise, let us introduce some terminology.

Definition 2.1. Let N be a positive integer and $f : B \to C$ a homomorphism of abelian groups. An *N-lift of f* is an abelian group A such that there exist isomorphisms $\beta : B \to A[N]$ and $\gamma : A/(NA) \to C$ such that $f = \gamma \circ \pi \circ \iota \circ \beta$, where $\iota : A[N] \to A$ is the inclusion map and $\pi : A \to A/(NA)$ the canonical projection.
In other words, the following diagram commutes:



With this terminology we can formulate the main question of this thesis.

Main Problem. *For which pairs (N, f), where N is a positive integer and f is a homomorphism of abelian groups, does f have an N-lift?*

Let N be a positive integer and A an abelian group. Then both $A[N]$ and $A/(NA)$ have exponents dividing N. Now let $f : B \to C$ be a homomorphism of abelian groups such that A is an N-lift of f. Then $B \cong A[N]$ and $C \cong A/(NA)$. As a consequence, both B and C have exponent dividing N. Hence a necessary condition for a homomorphism of abelian groups to have an N-lift is that both its domain and codomain are annihilated by N. For this reason, we will only consider such homomorphisms in the rest of this thesis.

Note that just like being an abelian group is the same as being a $\mathbb{Z}$-module, being an abelian group of exponent dividing N is the same as being a $\mathbb{Z}/N\mathbb{Z}$-module. From now on we will use both terms interchangeably. Moreover, if B and C are $\mathbb{Z}/N\mathbb{Z}$-modules, then a map $f : B \to C$ is a group homomorphism if and only if f is a homomorphism of $\mathbb{Z}/N\mathbb{Z}$-modules.

In important tool for constructing lifts is given by the following proposition.

Proposition 2.2. *Let N be a positive integer and $(f_i : B_i \to C_i)_{i\in I}$ a family of homomorphisms of $\mathbb{Z}/N\mathbb{Z}$-modules. For each $i \in I$, let A_i be an N-lift of f_i. Then $\bigoplus_{i\in I} A_i$ is an N-lift of $\bigoplus_{i\in I} f_i$.*

Proof. Write $A = \bigoplus_{i\in I} A_i$. Let

$$\iota : A[N] \to A$$

be the inclusion of $A[N]$ into A and let

$$\pi : A \to A/(NA)$$

be the canonical projection. Furthermore, let for each $i \in I$

$$\iota_i : A_i[N] \to A_i$$

be the inclusion of the N-torsion of A_i into A and let

$$\pi_i : A_i \to A_i/(NA_i)$$

be the canonical projection.

Note that, by Lemma 1.1, we have $A[N] = \bigoplus_{i\in I} A_i[N]$, and therefore we have $\bigoplus_{i\in I} \iota_i = \iota$. And by Lemma 1.2, we have $A/(NA) = (\bigoplus_{i\in I} A_i)/(\bigoplus_{i\in I} NA_i)$. Let

$$\zeta : \frac{\bigoplus_{i\in I} A_i}{\bigoplus_{i\in I} NA_i} \longrightarrow \bigoplus_{i\in I} A_i/(NA_i)$$

be the isomorphism from Lemma 1.10.

For each $i \in I$, we know that A_i is an N-lift of f_i and so there exist isomorphisms

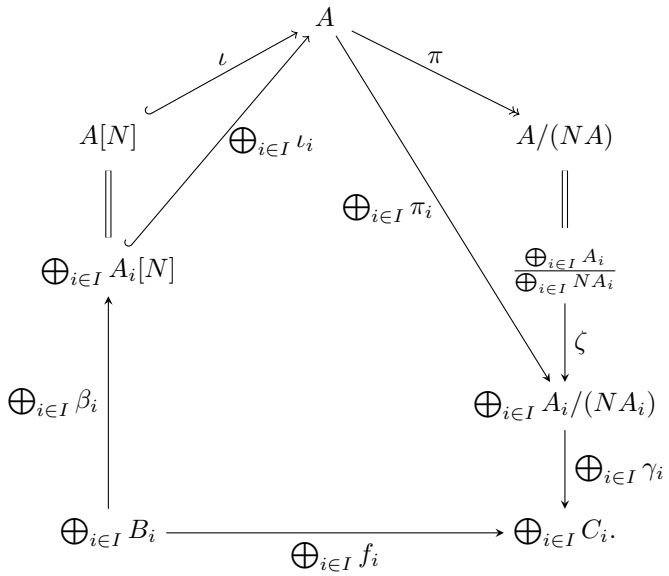
$$\beta_i : B_i \to A_i[N]$$

and

$$\gamma_i : A_i/(NA_i) \to C_i$$

such that $f_i = \gamma_i \circ \pi_i \circ \iota_i \circ \beta_i$. Now, by Lemma 1.9.(c), we have that both $\bigoplus_{i\in I} \beta_i$ and $\bigoplus_{i\in I} \gamma_i$ are isomorphisms as well.

By construction, the following diagram is commutative:



The commutativity of the diagram above together with the fact that $\bigoplus_{i\in I}\beta_i$, $\bigoplus_{i\in I}\gamma_i$, and ζ are isomorphisms, shows that A is an N-lift of $\bigoplus_{i\in I}f_i$. □

Definition 2.3. Let A be an abelian group and let p be a prime number. The *p-primary part of A*, denoted by $A[p^\infty]$, is the subgroup of A consisting of all elements whose order is a power of p.

Note that $A[p^\infty] = \bigcup_{i\geq 0} A[p^i]$, where $A[p^i]$ is the p^i-torsion of A. One checks easily that $A[p^\infty]$ is indeed a subgroup of A.

Proposition 2.4. *Let A be an abelian group. Then the map*

$$\chi_A : \bigoplus_{p \text{ prime}} A[p^\infty] \to A_{tors}$$

defined by

$$(a_p)_{p \text{ prime}} \mapsto \sum_{p \text{ prime}} a_p$$

is an isomorphism.

Proof. See for instance [1, Theorem 8.1] or [2, Theorem 2.1]. □

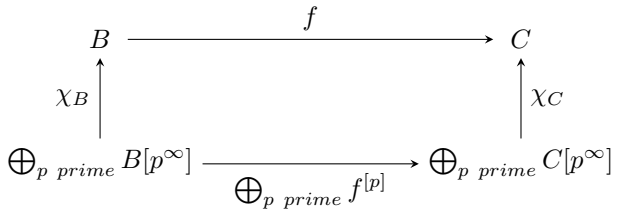
Definition 2.5. Let $f : B \to C$ be a homomorphism of abelian groups and p a prime number. We define the *p-primary part of f* to be the homomorphism

$$f^{[p]} : B[p^\infty] \to C[p^\infty]$$

that sends x to $f(x)$.

The map $f^{[p]}$ is well-defined because, for each $x \in B$, the order of $f(x)$ divides the order of x. Moreover, for all primes p, the map $f^{[p]}$ a homomorphism because f is.

Proposition 2.6. *Let $f : B \to C$ be a homomorphism of torsion abelian groups and let χ_B and χ_C be the isomorphisms defined in Proposition 2.4. Then the diagram*



is commutative.

Proof. This follows directly from the fact that f is a homomorphism and from the definitions of χ_B, χ_C, and $f^{[p]}$. □

Given Proposition 2.6, it seems plausible that we can reduce the main problem to studying pairs (N, f), where N is a prime power. Indeed this is true and it will be the subject of the next chapter.

3 Reduction to prime powers

Recall our main problem: given a positive integer N and a homomorphism f of $\mathbb{Z}/N\mathbb{Z}$-modules, does there exist an N-lift of f? In this chapter we will reduce this problem to the case where N is a prime power. More precisely, this chapter will be devoted to proving the following theorem.

Theorem 3.1. *Let N be a positive integer and $f : B \to C$ a homomorphism of $\mathbb{Z}/N\mathbb{Z}$-modules. Let $\prod_{i=1}^{t} p_i^{k_i}$ be the prime factorization of N, where the p_i's are distinct. Then there exists an N-lift of f if and only if, for each $i \in \{1, \ldots, t\}$, there exists a $p_i^{k_i}$-lift of the p_i-primary part of f.*

Lemma 3.2. *Let m and n be coprime positive integers and let B be a $\mathbb{Z}/m\mathbb{Z}$-module. The multiplication by n map m_n on B*

$$m_n : B \to B$$

defined by

$$b \mapsto nb$$

is an isomorphism.

Proof. Consider the homomorphism

$$\varphi : \mathbb{Z}/m\mathbb{Z} \to \mathrm{End}(B)$$

that defines the $\mathbb{Z}/m\mathbb{Z}$-module structure of B. Let $\overline{n}$ denote the coset of n in $\mathbb{Z}/m\mathbb{Z}$. Then we naturally have $m_n = \varphi(\overline{n})$. Since n is coprime to m, we have $\overline{n} \in (\mathbb{Z}/m\mathbb{Z})^*$. Moreover, φ restricted to $(\mathbb{Z}/m\mathbb{Z})^*$ maps into $\mathrm{End}(B)^* = \mathrm{Aut}(B)$. Hence, $m_n = \varphi(\overline{n}) \in \mathrm{Aut}(B)$. □

Lemma 3.3. *Let A be an abelian group and let m and n be coprime positive integers. Then the map*

$$A/(mnA) \to A/(mA) \oplus A/(nA)$$

defined by

$$a + mnA \mapsto (a + mA, a + nA)$$

is an isomorphism.

Proof. We will show that the map

$$\varphi : A \to A/(mA) \oplus A/(nA)$$

defined by

$$a \mapsto (a + mA, a + nA)$$

is a surjective homomorphism with kernel mnA. The fact that it is a homomorphism is clear from the definition.

Note that $A/(mA)$ is a $\mathbb{Z}/m\mathbb{Z}$-module. Since m and n are coprime, Lemma 3.2 yields that the multiplication by n map m_n on $A/(mA)$ is an isomorphism. By symmetry the multiplication by m map m_m on $A/(nA)$ is also an isomorphism. By surjectivity of m_n there exists $c \in A$ such that $a \equiv nc \mod mA$. By surjectivity of m_m there exists $d \in A$ such that $b \equiv md \mod nA$. Now we have $\varphi(nc + md) = (a + mA, b + nA)$ and hence φ is surjective.

What is left to show is that $\ker(\varphi) = mnA$. The inclusion $mnA \subset \ker(\varphi)$ is clear, so we will only prove that $\ker(\varphi) \subset mnA$. Let $x \in \ker(\varphi)$, so $x \in mA \cap nA$. In particular, $x \in nA$, so there exists $y \in A$ such that $x = ny$. Additionally $x \in mA$, so $m_n(y+mA) = ny+mA = x+mA = mA$. Hence $y+mA \in \ker(m_n)$. Since m_n is injective, we get $y \in mA$. Hence $x = ny \in nmA$. □

Let A be an abelian group and let N be a positive integer. Let $\prod_{i=1}^{t} p_i^{k_i}$ be the prime factorization of N, where the p_i's are distinct. Define the map

$$\psi_N^A : A/(NA) \to \bigoplus_{i=1}^{t} A/(p_i^{k_i} A)$$

by

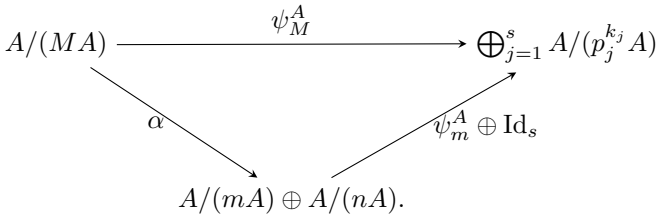
$$a + NA \mapsto (a + p_i^{k_i} A)_{i=1}^{t}.$$

Proposition 3.4. *Let A be an abelian group. For each positive integer N, the map ψ_N^A is an isomorphism.*

Proof. We work by induction on the number t of different prime divisors of N. If $t = 1$ then ψ_N^A is the identity and hence an isomorphism. Now assume that $t > 1$. Let $s \in \{2, \ldots, t\}$ and assume that for every positive integer N' with at most $s - 1$ different prime divisors the map $\psi_{N'}^A$ is an isomorphism. Let M be a positive integer whose prime factorization is $\prod_{j=1}^{s} p_j^{k_j}$, where the p_j's are distinct. We will show that ψ_M^A is also an isomorphism. Set $m = \prod_{j=1}^{s-1} p_j^{k_j}$ and $n = p_s^{k_s}$, so $M = mn$. Note that m and n are coprime. Let

$$\alpha : A/(MA) \to A/(mA) \oplus A/(nA)$$

be the isomorphism from Lemma 3.3. Let Id_s be the identity map on $A/(p_s^{k_s}A)$. By definition of these maps, the following diagram is commutative:



Since m has $s-1$ different prime divisors, the map ψ_m^A is an isomorphism by the induction hypothesis. Hence, by Lemma 1.9.(c), the map $\psi_m^A \oplus \mathrm{Id}_s$ is an isomorphism too. Since α is an isomorphism as well and the diagram is commutative, ψ_M^A is an isomorphism too. □

Lemma 3.5. *Let N be a positive integer and let B be a $\mathbb{Z}/N\mathbb{Z}$-module. Let p a prime number and let k be the largest integer such that p^k divides N. Then $B[p^\infty] = B[p^k]$.*

Proof. Every element of B has order dividing N. The elements of $B[p^\infty]$ are precisely those elements whose order is a power of p. Hence by the maximality of k we have $p^k B[p^\infty] = 0$. □

Proposition 3.6. *Let N be a positive integer, let $f : B \to C$ be a homomorphism of $\mathbb{Z}/N\mathbb{Z}$-modules and let A be an N-lift of f. Let $\prod_{i=1}^{t} p_i^{k_i}$ be the prime factorization of N, where the p_i's are distinct. Then, for each $i \in \{1, \ldots, t\}$, the group A is a $p_i^{k_i}$-lift of the p_i-primary part of f.*

Proof. Let $j \in \{1, \ldots, t\}$. By definition of an N-lift, there exist isomorphisms

$$\beta : B \to A[N]$$

and

$$\gamma : A/(NA) \to C$$

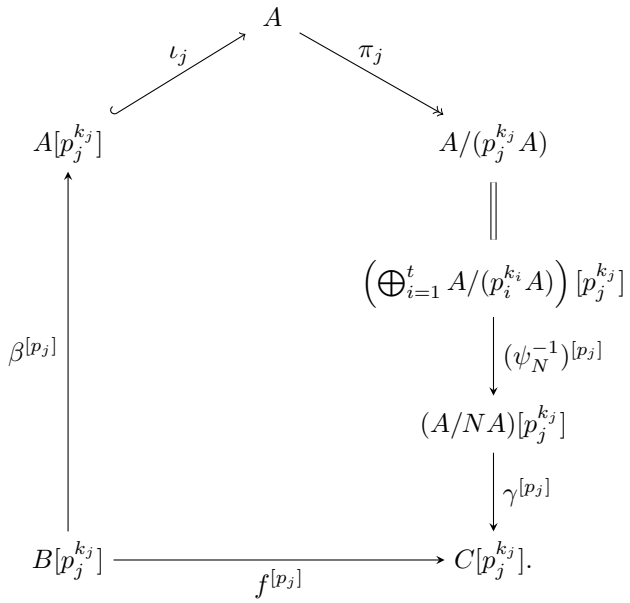
such that $f = \gamma \circ \pi \circ \iota \circ \beta$, where $\iota : A[N] \to A$ is the inclusion map and $\pi : A \to A/(NA)$ is the canonical projection.

By Proposition 3.4, the map

$$\psi_N^A : A/(NA) \to \bigoplus_{i=1}^{t} A/(p_i^{k_i}A)$$

is an isomorphism.

Since B, C, $A[N]$, and $A/(NA)$ are $\mathbb{Z}/N\mathbb{Z}$-modules, by Lemma 3.5, their p_j-primary parts are equal to their $p_j^{k_j}$-torsions. As a consequence of Lemmas 1.1 and 3.2, the p_j-primary part of $\bigoplus_{i=1}^{t} A/(p_i^{k_i}A)$ is $0^{(j-1)} \oplus A/(p_j^{k_j}A) \oplus 0^{(t-j)}$. Let us identify $0^{(j-1)} \oplus A/(p_j^{k_j}A) \oplus 0^{(t-j)}$ with $A/(p_j^{k_j}A)$ in the obvious way. Now we can consider the following diagram:



Here ι_j is the inclusion and π_j is the canonical projection. The diagram is commutative by construction of these maps. Furthermore, from Lemma 1.9.(c) and Proposition 2.6 it follows that the p_j-primary part of an isomorphism is again an isomorphism. Hence $\beta^{[p_j]}$, $\gamma^{[p_j]}$, and $(\psi_N^{-1})^{[p_j]}$ are all isomorphisms and therefore A is a $p_j^{k_j}$-lift of $f^{[p_j]}$. □

Note that Proposition 3.6 proves the implication of Theorem 3.1 from left to right. For the implication from right to left we will need a bit more machinery. Namely, we will use the so-called modules of fractions. Below we will give a construction of them. The construction can be thought of as a generalization of the construction of $\mathbb{Q}$ from $\mathbb{Z}$. It is a very classical construction, so our exposition of it will be very concise. An interested reader can find more details for example in [3, Chapter 3].

Let R be a commutative ring and S a subset of R containing 1 that is closed under multiplication. Furthermore let M be an R-module. Define a relation on $M \times S$ by saying that two pairs (m, s) and (n, t) are equivalent if and only if there exists some $u \in S$ such that $u(tm - sn) = 0$. One can show that this is an equivalence relation. Denote the equivalence class of (m, s) by m/s or $\frac{m}{s}$ and let $S^{-1}M$ be the set of all such equivalence classes. We define addition on $S^{-1}M$ by

$$\frac{m}{s} + \frac{n}{t} = \frac{tm + sn}{st}, \quad \text{for } m/s, n/t \in S^{-1}M,$$

which turns $S^{-1}M$ into an abelian group with zero-element $0/1$.

If we take M to be equal to R, we can also define multiplication on $S^{-1}R$ by

$$\frac{r}{s} \cdot \frac{r'}{s'} = \frac{rr'}{ss'}, \quad \text{for } r/s, r'/s' \in S^{-1}R.$$

The set $S^{-1}R$, equipped with the just-defined addition and multiplication, is a commutative ring called the *ring of fractions of R with respect to S*. The

unity element of $S^{-1}R$ is $1/1$. There is a natural ring homomorphism from R to $S^{-1}R$ that sends r to $r/1$. This map is not in general injective. For an extreme example, take R to be any non-zero ring and S containing 0. Then $S^{-1}R$ is the zero ring.

Let us now go back to the general case where M is any R-module. Then we can define a scalar multiplication $S^{-1}R \times S^{-1}M \to S^{-1}M$ by

$$\frac{r}{s} \cdot \frac{m}{t} = \frac{rm}{st}, \quad \text{for } r/s \in S^{-1}R \text{ and } m/t \in S^{-1}M.$$

Such scalar multiplication gives a $S^{-1}R$-module structure to $S^{-1}M$, which we will refer to as the *module of fractions of M with respect to S*. Via the natural ring homomorphism from R to $S^{-1}R$, we can view $S^{-1}M$ as an R-module. There is a natural R-module homomorphism from M to $S^{-1}M$ that sends m to $m/1$. This map is also not necessarily injective.

For our purposes, the following special case of modules of fractions will be important: let R be a commutative ring and M an R-module. Let $\mathfrak{p}$ be a prime ideal of R and set $S = R \setminus \mathfrak{p}$. Then S contains 1 and is multiplicatively closed. So we can consider the module of fractions of M with respect to S, which we will call the *localization of M at $\mathfrak{p}$* and which we denote by $M_{\mathfrak{p}}$.

We will be working with abelian groups, which are the same as $\mathbb{Z}$-modules. Here we list some properties of their localizations. For p a prime number, we denote the prime ideal $p\mathbb{Z}$ of $\mathbb{Z}$ by (p).

Lemma 3.7. *Let p be prime number and let A be a $\mathbb{Z}$-module. Let N be a positive integer and let k be the largest integer such that p^k divides N. Then $A_{(p)}[N] = A_{(p)}[p^k]$ and $NA_{(p)} = p^k A_{(p)}$.*

Proof. The inclusions $A_{(p)}p[p^k] \subset A_{(p)}p[N]$ and $NA_{(p)}p \subset p^k A_{(p)}p$ are obvious, so we will only show the other two inclusions. Note that there exists a positive integer m such that $N = mp^k$, since p^k divides N. By the maximality of k, we know that p and m are coprime. Hence $1/m$ is an element of $\mathbb{Z}_{(p)}$.

Now we show $A_{(p)}[N] \subset A_{(p)}[p^k]$. Let $a/s \in A_{(p)}[N]$. Then we have $N(a/s) = 0/1$. Note that we also have $m \cdot 1/m = 1/1$. Hence we get

$$p^k \frac{a}{s} = \frac{1}{m} \cdot m \cdot p^k \frac{a}{s} = \frac{1}{m} \cdot N \frac{a}{s} = \frac{1}{m} \cdot \frac{0}{1} = \frac{0}{1}.$$

Hence $a/s \in A_{(p)}[p^k]$.

For the inclusion $p^k A_{(p)} \subset NA_{(p)}$, let $p^k(b/t) \in p^k A_{(p)}$. Then

$$p^k \frac{b}{t} = m \cdot 1/m \cdot p^k \frac{b}{t} = N \frac{b}{tm} \in NA_{(p)}.$$

This concludes the proof. □

Lemma 3.8. *Let p be a prime number, let k be a non-negative integer and let A be a $\mathbb{Z}$-module. Then the natural homomorphism from A to $A_{(p)}$ restricts to an isomorphism between $A[p^k]$ and $A_{(p)}[p^k]$.*

Proof. We will first show that $A_{(p)}[p^k] = (A[p^k])_{(p)}$. The inclusion $(A[p^k])_{(p)} \subset A_{(p)}[p^k]$ is clear, so we will only prove $A_{(p)}[p^k] \subset (A[p^k])_{(p)}$. Let $a/s \in A_{(p)}[p^k]$. Then $p^k a/s = 0/1$, hence there exists some $v \in \mathbb{Z} \setminus (p)$ such that $v(p^k a - 0) = 0$. Hence $p^k va = 0$ and so $va \in A[p^k]$. Now we have $va/1 \in (A[p^k])_{(p)}$ and both $s, v \in \mathbb{Z} \setminus (p)$, and so $a/s = 1/(sv) \cdot va/1 \in (A[p^k])_{(p)}$. Since a/s was chosen arbitrarily, this shows that $A_{(p)}[p^k] \subset (A[p^k])_{(p)}$.

For injectivity, suppose that $a/1 = b/1$ for certain $a, b \in A[p^k]$. Then there exists some $u \in \mathbb{Z} \setminus (p)$ such that $u(a - b) = 0$. Since $A[p^k]$ is a subgroup of A, we also have $a - b \in A[p^k]$. Since u is coprime to p^k and $A[p^k]$ is a $\mathbb{Z}/p^k\mathbb{Z}$-module, we know by Lemma 3.2 that multiplication by u in $A[p^k]$ is an isomorphism. So in particular it is injective and hence $a - b = 0$.

For surjectivity, let $c/s \in A_{(p)}[p^k]$. Then $c/s \in (A[p^k])_{(p)}$. By Lemma 3.2, multiplication by s map m_s in $A[p^k]$ is an isomorphism. Since m_s is surjective and $c \in A[p^k]$, there exists some $d \in A[p^k]$ such that $sd = c$. Then we have $d/1 = sd/s = c/s$. □

Lemma 3.9. *Let p be a prime number, let k be a positive integer and let A be a $\mathbb{Z}$-module. The map*

$$\xi : \ A/p^k A \to A_p/p^k A_p$$

defined by

$$x + p^k A \mapsto x/1 + p^k A_p$$

is an isomorphism.

Proof. Consider the map

$$\xi' : \ A \to A_{(p)}/p^k A_{(p)}$$

defined by

$$x \mapsto x/1 + p^k A_{(p)}.$$

It suffices to show that ξ' is a surjective homomorphism with kernel $p^k A$. As the composition of the natural homomorphism from A to A_p and the canonical projection $A_{(p)} \to A_{(p)}/p^k A_{(p)}$, the map ξ' is clearly a homomorphism.

To show that ξ' is surjective, let $a/s \in A_p$. We will show that there exists some $b \in A$ such that $\xi'(b) = a/s + p^k A_{(p)}$. Since s and p^k are coprime, there exist integers m and n such that $ms + np^k = 1$. Now define $b = ma$. Then

$$\xi'(b) = \frac{ma}{1} + p^k A_{(p)} = \frac{ma}{1} + p^k \cdot \frac{na}{s} + p^k A_{(p)} = \frac{sma + p^k na}{s} + p^k A_{(p)} = \frac{a}{s} + p^k A_{(p)}.$$

The choice of a/s being arbitrary, ξ' is surjective.

Now we will show that the kernel of ξ' equals $p^k A$. The inclusion $p^k A \subset \ker(\xi')$ is clear, so we will only show $\ker(\xi') \subset p^k A$. Let $x \in \ker(\xi')$. Then $x/1 + p^k A_p = p^k A_p$, so there exists $c/t \in A_p$ such that $x/1 = p^k c/t$. It follows that there exists some $u \in \mathbb{Z} \setminus p\mathbb{Z}$ such that $u(tx - p^k c) = 0$. Then we have $utx = p^k uc$ and so $utx \in p^k A$. Note that ut is coprime to p since both u and t are. Let $m_{ut} : A/p^k A \to A/p^k A$ be the multiplication by ut map, which is an isomorphism by Lemma 3.2. Note that $x + p^k A$ is an element of the kernel of m_{ut} since $utx \in p^k A$. Since m_{ut} is injective, we have $x + p^k A \in \ker(m_{ut}) = p^k A$ and so $x \in p^k A$. Hence $\ker(\xi') \subset p^k A$ and so the kernel of ξ' is $p^k A$. □

Proposition 3.10. *Let N be a positive integer, let p be a prime number dividing N and let k be the largest integer such that p^k divides N. Furthermore let $f : B \to C$ a homomorphism of $\mathbb{Z}/p^k\mathbb{Z}$-modules and let A be a p^k-lift of f. Then $A_{(p)}$ is an N-lift of f.*

Proof. Let

$$\iota : A[N] \to A$$

be the inclusion of $A[N]$ into A and let

$$\pi : A \to A/(NA)$$

be the canonical projection . Let moreover

$$\iota_p : A_{(p)}[N] \to A_{(p)}$$

be the inclusion of $A_{(p)}[N]$ into $A_{(p)}$ and let

$$\pi_p : A_{(p)} \to A_{(p)}/(NA_{(p)})$$

be the canonical projection.

Since A is a p^k-lift of N, there exist isomorphisms

$$\beta : B \to A[p^k]$$

and

$$\gamma : A/(p^kA) \to C$$

such that $f = \gamma \circ \pi \circ \iota \circ \beta$.

Let

$$\eta : A \to A_{(p)}$$

be the natural map from A to $A_{(p)}$. Let

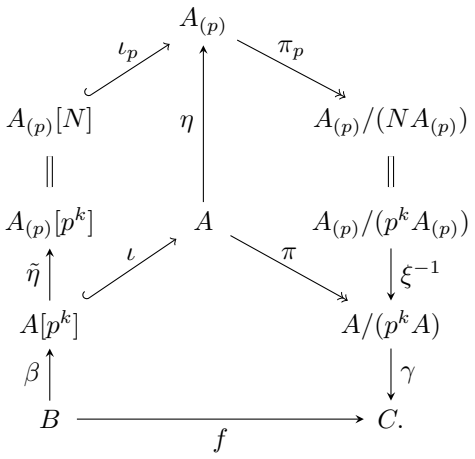
$$\tilde{\eta} : A[p^k] \to A_p[p^k]$$

be the isomorphism from Lemma 3.8. Furthermore let

$$\xi : A/p^kA \to A_{(p)}/p^kA_{(p)}$$

be the isomorphism from Lemma 3.9.

Note that, by Lemma 3.7, we have $A_{(p)}[N] = A_{(p)}[p^k]$ and $NA_{(p)} = p^kA_{(p)}$. Now consider the following diagram:



By definition of these maps, the diagram is commutative. Since β, η, ξ^{-1}, and γ are all isomorphisms, the diagram shows that $A_{(p)}$ is an N-lift of f. □

With this result, we are able to prove Theorem 3.1.

Proof of Theorem 3.1. The implication from left to right is given by Proposition 3.6. What is left to show is the implication for right to left. Suppose that, for each $i \in \{1, \ldots, t\}$, there exists a $p_i^{k_i}$-lift A_i of $f^{[p_i]}$. By Proposition 3.10 we know that, for each $i \in \{1, \ldots, t\}$, the group $(A_i)_{(p_i)}$ is an N-lift of $f^{[p_i]}$. Now we can apply Proposition 2.2 to get that $\bigoplus_{i=1}^t (A_i)_{(p_i)}$ is an N-lift of $\bigoplus_{i=1}^t f^{[p_i]}$. It follows from Proposition 2.6 that $\bigoplus_{i=1}^t (A_i)_{(p_i)}$ is also an N-lift of f. □

4 Free and non-free parts

In Chapter 3 we have reduced the main problem to prime powers. In order to solve the problem for prime powers, we will be working with certain "free" and "non-free" parts of groups whose exponent is a prime power. In this chapter we will define these objects and we will discuss their properties.

Until the end of Chapter 4, let p be a prime number, let k be a positive integer and let B be a $\mathbb{Z}/p^k\mathbb{Z}$-module.

Definition 4.1. A subgroup F of B is a *p^k-free part of B* if $F[p^{k-1}] = pF$ and $F + B[p^{k-1}] = B$.

Definition 4.2. A subgroup M of B is a *p^k-non-free part of B* if $M + pB = B[p^{k-1}]$ and, for each $s \in \mathbb{Z}_{\geq 0}$, one has $p^s B \cap M = p^s M$.

In this chapter we will prove the existence of free and non-free parts of $\mathbb{Z}/p^k\mathbb{Z}$-modules and, among others, we will prove the following main result.

Theorem 4.3. *Let F be a p^k-free and M a p^k-non-free part of B. The collection of complements of F in B is equal to the collection of p^k-non-free parts of B. The collection of complements of M in B equals the collection of p^k-free parts of B.*

Proposition 4.4. *There exist unique cardinals $a_1, a_2, \ldots, a_k$ such that*

$$B \cong \bigoplus_{i=1}^{k} (\mathbb{Z}/p^i\mathbb{Z})^{(a_i)}.$$

Proof. This is the result of the combination of Theorems 11.2 and 11.4 of [2]. □

Proposition 4.5 (Existence of free and non-free parts)**.** *There exist both a p^k-free and a p^k-non-free part of B.*

Proof. By Proposition 4.4 there exist cardinals $a_1, a_2, \ldots, a_k$ and an isomorphism $\varphi : \bigoplus_{i=1}^{k} (\mathbb{Z}/p^i\mathbb{Z})^{(a_i)} \to B$. It is a routine check to show that $\bigoplus_{i=1}^{k-1} \{0\}^{(a_i)} \oplus (\mathbb{Z}/p^k\mathbb{Z})^{(a_k)}$ is a p^k-free part of $\bigoplus_{i=1}^{k} (\mathbb{Z}/p^i\mathbb{Z})^{(a_i)}$ and that $\bigoplus_{i=1}^{k-1} (\mathbb{Z}/p^i\mathbb{Z})^{(a_i)} \oplus \{0\}^{(a_k)}$ is a p^k-non-free part. Since φ is an isomorphism, the images of these subgroups under φ are p^k-free and p^k-non-free parts of B respectively. □

Lemma 4.6. *Suppose that k is at least 2. If F is a p^k-free part of B then pF is a p^{k-1}-free part of pB.*

Proof. We want to show that $(pF)[p^{k-2}] = p(pF)$ and $pF + (pB)[p^{k-2}] = pB$. Note that we have

$$(pB)[p^{k-2}] = \{pb \mid b \in B \text{ and } p^{k-2}pb = 0\} = pB[p^{k-1}].$$

And by the same argument we have $(pF)[p^{k-2}] = pF[p^{k-1}]$. Since F is a p^k-free part of B we have $F[p^{k-1}] = pF$ and $F + B[p^{k-1}] = B$. Hence we get

$$(pF)[p^{k-2}] = pF[p^{k-1}] = p(pF)$$

and

$$pF + (pB)[p^{k-2}] = pF + pB[p^{k-1}] = p(F + B[p^{k-1}]) = pB.$$

This proves the lemma. □

Lemma 4.7. *Suppose k is at least 2. Let M be a p^k-non-free part of B. Then pM is a p^{k-1}-non-free part of pB.*

Proof. First we need to show that $pM + p(pB) = (pB)[p^{k-2}]$. Since M is a p^k-non-free part of B, we have $M + pB = B[p^{k-1}]$ and therefore $pM + p^2B = pB[p^{k-1}]$. Also we have

$$(pB)[p^{k-2}] = \{pb \mid b \in B \text{ and } p^{k-2}pb = 0\} = pB[p^{k-1}]$$

and therefore $pM + p^2B = (pB)[p^{k-2}]$.

Now let $s \in \mathbb{Z}_{\geq 0}$. We will prove that $p^s(pB) \cap pM = p^s(pM)$. The inclusion $p^{s+1}M \subset p^{s+1}B \cap pM$ is clear, so we will only show the other inclusion. Since M is a p^k-non-free part of B, we have $p^{s+1}B \cap M = p^{s+1}M$. Hence we get

$$p^s(pB) \cap pM \subset p^{s+1}B \cap M = p^{s+1}M = p^s(pM).$$

This proves the lemma. □

Proposition 4.8. *Let F be a p^k-free part of B and M a p^k-non-free part of B. Then $F \oplus M = B$.*

Proof. We will first show that $F+M = B$ and then we will prove that $F \cap M = 0$.

Since F is a p^k-free part of B we have $F + B[p^{k-1}] = B$. Since M is a p^k-non-free part of B we have $M + pB = B[p^{k-1}]$. Combining these equations gives us $F + M + pB = B$. Hence, by Lemma 1.7, we have $F + M = B$.

We will show that $F \cap M = 0$ by induction on k. Note that $M \subset B[p^{k-1}]$ since M is a p^k-non-free part of B. Hence if $k = 1$ we have $F \cap M \subset M \subset B[p^{1-1}] = 0$, so indeed $F \cap M = 0$.

Now suppose that $k > 1$. Let $\ell \in \{2, 3, \ldots, k\}$. Assume that for each $p^{\ell-1}$-free part V of $p^{k-\ell+1}B$ and each $p^{\ell-1}$-non-free part P of $p^{k-\ell+1}B$ we have $V \cap P = 0$. We will show that for every p^ℓ-free part W and for every p^ℓ-non-free part Q of $p^{k-\ell}B$ we have $W \cap Q = 0$.

Let W be a p^ℓ-free part of $p^{k-\ell}B$ and let Q be a p^ℓ-non-free part of $p^{k-\ell}B$. By definition of Q we have $Q \subset B[p^{\ell-1}]$ and by definition of W we have $W[p^{\ell-1}] = pW$. Hence $W \cap Q \subset W \cap B[p^{\ell-1}] = W[p^{k-1}] = pW$. Now, by definition of Q, we have $Q \cap pB = pQ$, so $W \cap Q \subset pW \cap Q \subset pB \cap Q = pQ$. So we get $W \cap Q \subset pW \cap pQ$. Now we apply Lemma 4.6 to $p^{k-\ell}B$ to get that pW is a $p^{\ell-1}$-free part of $p^{k-\ell+1}B$. Similarly by Lemma 4.7 we have that pQ is a $p^{\ell-1}$-non-free part of $p^{k-\ell+1}B$. Hence by our induction hypothesis, we have $W \cap Q \subset pW \cap pQ = 0$.

Now by induction we get that $F \cap M = 0$ and so $F \oplus M = B$. □

Corollary 4.9. *Any two p^k-free parts of B are isomorphic and any two p^k-non-free parts of B are isomorphic.*

Proof. Let F and V be two p^k-free parts of B. By Proposition 4.5 there exists a p^k-non-free part M of B. By Proposition 4.8 we have $F \oplus M = B = V \oplus M$. Now we have $F \cong (F \oplus M)/M = (V \oplus M)/M \cong V$. An analogous argument proves the statement for p^k-non-free parts. □

Proposition 4.10 (Structure of free parts)**.** *Let F be a p^k-free part of B. Then F is a free $\mathbb{Z}/p^k\mathbb{Z}$-submodule of B.*

Proof. If $F = 0$ we are done, so suppose $F \neq 0$. As a consequence of Proposition 4.4, there exist non-trivial cyclic subgroups $(F_i)_{i \in I}$ in F such that $F = \bigoplus_{i \in I} F_i$. Now suppose there exists $j \in I$ such that the order of F_j is smaller than p^k. Then all elements of F_j have order dividing p^{k-1}, and so $F_j \subset F[p^{k-1}]$. Since F is a p^k-free part of B, we have $F[p^{k-1}] = pF$. Hence

$$F = F_j + \sum_{i \in I \setminus \{j\}} F_i = pF + \sum_{i \in I \setminus \{j\}} F_i.$$

Now, by Lemma 1.7, we have $F = \sum_{i \in I \setminus \{j\}} F_i$. However, we know that F_j intersects $\sum_{i \in I \setminus \{j\}} F_i$ trivially and therefore $F_j = F_j \cap F = 0$. This contradicts the fact that F_j is non-trivial. Hence, for all $i \in I$, we have F_i is cyclic of order p^k. This proves that F is a free $\mathbb{Z}/p^k\mathbb{Z}$-module. □

Lemma 4.11. *Let F be a free $\mathbb{Z}/p^k\mathbb{Z}$-module and let $i \in \{0, 1, \ldots, k\}$. Then $p^i F = F[p^{k-i}]$.*

Proof. One easily checks that $(\mathbb{Z}/p^k\mathbb{Z})[p^{k-i}] = p^i(\mathbb{Z}/p^k\mathbb{Z})$. Since F is a free $\mathbb{Z}/p^k\mathbb{Z}$-module, F is isomorphic to a direct sum of copies of $\mathbb{Z}/p^k\mathbb{Z}$. Now Lemmas 1.1 and 1.2 ensure that we have $p^i F = F[p^{k-i}]$. □

Lemma 4.12. *Let F be a p^k-free part of B and let E be a free $\mathbb{Z}/p^k\mathbb{Z}$-submodule of B that contains F. Then $E = F$.*

Proof. Since E is a free $\mathbb{Z}/p^k\mathbb{Z}$-module, Lemma 4.11 yields that $E[p^{k-1}] = pE$. Since $E[p^{k-1}] = E \cap B[p^{k-1}]$, this gives $F + pE = F + (E \cap B[p^{k-1}])$. Now, by Lemma 1.12, we get $F + pE = (F + B[p^{k-1}]) \cap E$. Since F is a p^k-free part of B we have $F + B[p^{k+1}] = B$. Hence we get $F + pE = B \cap E = E$. By Lemma 1.7 we thus have $F = E$. □

Lemma 4.13. *Let F be a p^k-free part of B. Then every complement of F in B is a p^k-non-free part of B.*

Proof. Let C be a complement of F in B. First we will show that $C \subset B[p^{k-1}]$. We do this by contradiction. Suppose there exists $c \in C$ such that the order of c is p^k. Then $\langle c \rangle \cap F \subset C \cap F = 0$. Hence $F \oplus \langle c \rangle$ is a free $\mathbb{Z}/p^k\mathbb{Z}$-submodule of B containing F. So, by Lemma 4.12, we have $F = F \oplus \langle c \rangle$. But then $c \in C \cap F = 0$, which contradicts the fact that c has order p^k. Hence such c does not exist and we have $C \subset B[p^{k-1}]$.

Since F is a p^k-free part of B, we have $pF + C = (F \cap B[p^{k-1}]) + C$. Moreover, since $C \subset B[p^{k-1}]$, Lemma 1.12 yields $(F \cap B[p^{k-1}]) + C = (C + F) \cap B[p^{k-1}]$. The fact that C is a complement of F in B gives us that $C + F = B$. Hence we get $pF + C = B \cap B[p^{k-1}] = B[p^{k-1}]$.

What is left to show is that, for each $s \in \mathbb{Z}_{\geq 0}$, we have $C \cap p^s B = p^s C$. Let $s \in \mathbb{Z}_{\geq 0}$. Since C is complement of F in B we have $C \cap p^s B = C \cap (p^s C + p^s F)$. By Lemma 1.12, we have $C \cap (p^s C + p^s F) = (C \cap p^s F) + p^s C$. Now we have $C \cap p^s F \subset C \cap F = 0$, since C is a complement of F in B. Hence we get $C \cap p^s B = p^s C$. This concludes the proof. □

Lemma 4.14. *Let M be a p^k-non-free part of B. Then every complement of M in B is a p^k-free part of B.*

Proof. Let C be a complement of M in B. Since M is a p^k-non-free part of B, we have $C + B[p^{k-1}] = C + M + pB$. We also have $C + M = B$, since C is a complement of M in B. It follows that $C + B[p^{k-1}] = B$.

Now we will show that $C[p^{k-1}] = pC$. Note that $C[p^{k-1}] = C \cap B[p^{k-1}]$. Since M is a p^k-non-free part of B, we have $C \cap B[p^{k-1}] = C \cap (M + pB)$. Since C is a complement of M in B we get $M + pB = M + pM + pC = M + pC$. It follows that $C[p^{k-1}] = C \cap (M + pC)$. Now, by Lemma 1.12, we have $C \cap (M + pC) = (C \cap M) + pC$. And since C is a complement of M in B we have $C \cap M = 0$. Combining these equations gives us $C[p^{k-1}] = pC$. □

Proof of Theorem 4.3. This follows from the composition of Proposition 4.8, Lemma 4.13, and Lemma 4.14. □

5 Solution to the prime power case

In Chapter 3 we reduced the main problem to the case of prime powers, which we will consider in the present chapter. Given some prime power p^k and a $\mathbb{Z}/p^k\mathbb{Z}$-module homomorphism f, does f have a p^k-lift? The theory of free and non-free parts from Chapter 4 helps us answer this question.

Theorem 5.1. *Let p be a prime number, let k be a positive integer and let $f : B \to C$ be a homomorphism of $\mathbb{Z}/p^k\mathbb{Z}$-modules. Then the following statements are equivalent.*

(1) *There exists a p^k-lift of f.*

(2) *For each p^k-non-free part M of B, the map $f|_M : M \to f(M)$ is an isomorphism and $f(M)$ is a p^k-non-free part of C.*

(3) *There exist p^k-non-free parts M_B and M_C of B and C respectively, such that f restricts to an isomorphism $M_B \to M_C$.*

The rest of this chapter will be devoted to proving Theorem 5.1.

Lemma 5.2. *Let p be a prime number, let k be a positive integer and let A be an abelian group. Then*

$$(A/(p^kA))[p^{k-1}] = \frac{A[p^{k-1}] + pA}{p^kA}.$$

Proof. The inclusion from right to left is clear, so we will only prove the other inclusion. Let $x + p^kA \in (A/(p^kA))[p^{k-1}]$. Then $p^{k-1}x \in p^kA$ and hence there exists $a \in A$ such that $p^{k-1}x = p^ka$. Then $p^{k-1}(x - pa) = 0$ and so $x - pa \in A[p^{k-1}]$. From this it follows that $x \in A[p^{k-1}] + pA$ and hence $x + p^kA \in (A[p^{k-1}] + pA)/(p^kA)$. Since $x + p^kA$ was chosen arbitrarily, we have $(A/(p^kA))[p^{k-1}] \subset (A[p^{k-1}] + pA)/(p^kA)$. □

Lemma 5.3. *Let p be a prime number and let k be a positive integer. Let A be an abalian group and let M be a p^k-non-free part of $A[p^k]$. Then, for all $s \in \mathbb{Z}_{\geq 0}$, one has $M \cap p^sA = p^sM$.*

Proof. We will first show that, for each $s \in \{0, \ldots, k\}$, we have $M \cap p^sA = p^sM$. We will work by induction on s. For $s = 0$ we clearly have $M \cap p^0A = p^0M$. Now let $s \in \{1, \ldots, k\}$ and suppose that $M \cap p^{s-1}A = p^{s-1}M$. We will show that $M \cap p^sA = p^sM$. The inclusion $p^sM \subset M \cap p^sA$ is clear, so we will only prove the other inclusion. Let $m \in M \cap p^sA$. Then there exists $a \in A$ such that $p^sa = m$. By the induction hypothesis we have $M \cap p^sA \subset M \cap p^{s-1}A = p^{s-1}M$. Hence there exists $n \in M$ such that $p^{s-1}n = m$. Since M is a p^k-free part of $A[p^k]$, we have $M \subset (A[p^k])[p^{k-1}] = A[p^{k-1}]$. Hence we have

$$p^ka = p^{k-s}(p^sa) = p^{k-s}m = p^{k-s}(p^{s-1}n) = p^{k-1}n = 0.$$

So $a \in A[p^k]$ and therefore we get $m \in M \cap p^sA[p^k]$. Since M is a p^k-non-free part of $A[p^k]$, we have $M \cap p^sA[p^k] = p^sM$. Hence $m \in p^sM$. Since m was chosen arbitrarily this proves that $M \cap p^sA \subset p^sM$ and so $M \cap p^sA = p^sM$.

This concludes the proof in case $s \leq k$. Now let $s \in \mathbb{Z}_{>k}$. Since $M \subset A[p^k]$ we have

$$M \cap p^s A \subset M \cap p^k A = p^k M = 0 = p^s M.$$

The inclusion $p^s M \subset M \cap p^s A$ clearly also holds and therefore $M \cap p^s A = p^s M$. □

Proposition 5.4. *Let p be a prime number and k a positive integer. Let A be an abelian group and let M be a p^k-non-free part of $A[p^k]$. Furthermore, let $\iota : A[p^k] \to A$ be the inclusion and let $\pi : A \to A/(p^k A)$ be the canonical projection. Set $\rho = \pi \circ \iota$. Then the map $\rho|_M$ is an injective homomorphism whose image is a p^k-non-free part of $A/(p^k A)$.*

Proof. First of all, note that $\ker(\rho|_M) = M \cap p^k A$. By Lemma 5.3, we have $M \cap p^k A = p^k M \subset p^k A[p^k] = 0$. This proves the injectivity of $\rho|_M$. So we only have to show that $\rho(M)$ is a p^k-non-free part of $A/(p^k A)$. To ease the notation, define $B = A[p^k]$, $C = A/(p^k A)$ and $Q = \rho(M)$.

First we will show that $Q + pC = C[p^{k-1}]$. By definition of Q and C we have $Q + pC = (M + p^k A + pA)/p^k A$. Since $p^k A \subset pA$ and $pB \subset pA$, we get $Q+pC = (M+pB+pA)/p^k A$. Since M is a p^k-non-free part of B and $B = A[p^k]$, we have $M + pB = B[p^{k-1}] = A[p^{k-1}]$. Hence $Q + pC = (A[p^{k-1}] + pA)/p^k A$, which equals $C[p^{k-1}]$ by Lemma 5.2.

Now we want to show that, for each $s \in \mathbb{Z}_{\geq 0}$, we have $Q \cap p^s C = p^s Q$. Note that, for all $s \in \mathbb{Z}_{\geq k}$, we have $Q \cap p^s C = 0 = p^s Q$, since C is annihilated by p^k. Now let $s \in \{0, \ldots, k-1\}$. We will show that then also $Q \cap p^s C = p^s Q$. By definition of C and Q it suffices to show that $(M + p^k A) \cap p^s A = p^s M + p^k A$. Since $s < k$, we have $p^k A \subset p^s A$. Hence, by Lemma 1.12, we have $(M + p^k A) \cap p^s A = (M \cap p^s A) + p^k A$. Lemma 5.3 gives us that $M \cap p^s A = p^s M$. Hence $(M + p^k A) \cap p^s A = p^s M + p^k A$, and therefore $Q \cap p^s C = p^s Q$.

We conclude that Q is a p^k-non-free part of C. □

5.1 Submodules of free modules

In this section we will prove the following.

Proposition 5.5. *Let p be a prime number and let k be a positive integer. Let F a free $\mathbb{Z}/p^k\mathbb{Z}$-module and let H be a submodule of F. Then there exist disjoint subsets $\mathcal{C}$ and $\mathcal{X}$ in F and, for each $c \in \mathcal{C}$, an integer s_c, such that $\mathcal{C} \cup \mathcal{X}$ is a $\mathbb{Z}/p^k\mathbb{Z}$-basis of F and $\{p^{s_c} c + pH \mid c \in \mathcal{C}\}$ is an $\mathbb{F}_p$-basis of H/pH.*

Throughout Section 5.1 we will work under the assumptions of Proposition 5.5.

For each $i \in \{1, \ldots, k-1\}$ define

$$U_i = H[p^i]/(H[p^{i-1}] + pH[p^{i+1}]).$$

Also define

$$U_k = H/H[p^{k-1}].$$

For all $i \in \{1, \ldots, k\}$ we have that U_i is annihilated by p and hence is an $\mathbb{F}_p$-vector space. For each $i \in \{1, \ldots, k\}$, let $(\overline{b_{ij}})_{j \in J_i}$ be an $\mathbb{F}_p$-basis of U_i.

Here b_{ij} is a representative of the coset $\overline{b_{ij}}$. Note that b_{ij} has order p^i, since $b_{ij} \in H[p^i] \setminus H[p^{i-1}]$. Set

$$\mathcal{B} = \{b_{ij} \mid i \in \{1, \dots, k\}, j \in J_i\}.$$

The notation we just introduced will be respected until the end of Section 5.1.

Note that for some $i \in \{1, \dots, k\}$ we might have $U_i = 0$. In that case, $J_i = \emptyset$, since the only basis of the trivial vector space is the empty set. In the sequel, set empty sums to be equal to zero.

Lemma 5.6. *For each $s \in \{1, \dots, k\}$ we have $H[p^s] = \sum_{i=s}^{k} \sum_{j \in J_i} \langle p^{i-s} b_{ij} \rangle + H[p^{s-1}]$.*

Proof. We will prove this by induction on s. For $s = k$, the statement follows directly from the fact that $(\overline{b_{kj}})_{j \in J_k}$ is a basis of $H/H[p^{k-1}]$. If $k = 1$ then we are done. Else, let $t \in \{2, \dots, k\}$ and assume that $H[p^t] = \sum_{i=t}^{k} \sum_{j \in J_i} \langle p^{i-t} b_{ij} \rangle + H[p^{t-1}]$. Since $(\overline{b_{(t-1)j}})_{j \in J_{t-1}}$ is a basis for U_{t-1} we have

$$H[p^{t-1}] = \sum_{j \in J_{t-1}} \langle b_{(t-1)j} \rangle + H[p^{t-2}] + pH[p^t].$$

Combining this with the induction hypotheses and simplifying the resulting equation gives

$$H[p^{t-1}] = \sum_{i=t-1}^{k} \sum_{j \in J_i} \langle p^{i-(t-1)} b_{ij} \rangle + H[p^{t-2}] + pH[p^{t-1}].$$

Hence, by Lemma 1.7, we get

$$H[p^{t-1}] = \sum_{i=t-1}^{k} \sum_{j \in J_i} \langle p^{i-(t-1)} b_{ij} \rangle + H[p^{t-2}].$$

Since the statement holds for the base case $s = k$, this proves the lemma. □

Lemma 5.7. *For each $s \in \{1, \dots, k\}$ we have $H = \sum_{i=s}^{k} \sum_{j \in J_i} \langle b_{ij} \rangle + H[p^{s-1}]$. Moreover, $\mathcal{B}$ generates H.*

Proof. We prove the lemma by induction on s. For $k = s$ the statement holds by Lemma 5.6. If $k = 1$, we are done. Else, let $t \in \{2, \dots, k\}$ and assume the statement holds for $s = t$, that is, we have

$$H = \sum_{i=t}^{k} \sum_{j \in J_i} \langle b_{ij} \rangle + H[p^{t-1}].$$

By Lemma 5.6 we have

$$H[p^{t-1}] = \sum_{i=t-1}^{k} \sum_{j \in J_i} \langle p^{i-(t-1)} b_{ij} \rangle + H[p^{t-2}].$$

Combining these equations gives us

$$H = \sum_{i=t-1}^{k} \sum_{j \in J_i} \langle b_{ij} \rangle + H[p^{t-2}].$$

Since the statement holds for $s = k$ this proves the statement is true for all $s \in \{1, \ldots, k\}$. The case $s = 1$ gives us that $\mathcal{B}$ generates H. □

Now for each $i \in \{1, \ldots, k\}$ and for each $j \in J_i$ define $v_{ij} = p^{i-1} b_{ij}$. Since each b_{ij} has order p^i, we have $v_{ij} \in H[p] \setminus \{0\}$. Set

$$\mathcal{V} = \{v_{ij} \mid i \in \{1, \ldots, k\}, j \in J_i\}.$$

We will keep these definitions until the end of Section 5.1.

Next we will show that the set $\mathcal{V}$ consists of linearly independent elements over $\mathbb{F}_p$. For each $i \in \{1, \ldots, k\}$ and for each $j \in J_i$ let $\lambda_{ij} \in \mathbb{Z}$. Suppose that $\sum_{i=1}^{k} \sum_{j \in J_i} \lambda_{ij} v_{ij} = 0$.

Lemma 5.8. *Let $s \in \{0, \ldots, k-1\}$. Then for each $i \in \{1, \ldots, s\}$ and for each $j \in J_i$ we have $\lambda_{ij} \equiv 0 \mod p$.*

Proof. We will prove the lemma by induction on s. For $s = 0$ the set $\{1, \ldots, s\}$ is empty, hence the statement of the lemma is true. Now let $t \in \{0, \ldots, k-2\}$ and assume that for each $i \in \{1, \ldots, t\}$ and for each $j \in J_i$ we have $\lambda_{ij} \equiv 0 \mod p$. Then for each $i \in \{1, \ldots, t\}$ and for each $j \in J_i$ we have $\lambda_{ij} v_{ij} = 0$, since $v_{ij} \in F[p]$. So we get $\sum_{i=t+1}^{k} \sum_{j \in J_i} \lambda_{ij} v_{ij} = 0$. Now define

$$x = \sum_{i=t+2}^{k} \sum_{j \in J_i} \lambda_{ij} p^{i-(t+1)} b_{ij} + \sum_{j \in J_{t+1}} \lambda_{(t+1)j} b_{(t+1)j}.$$

Then

$$p^t x = \sum_{i=t+1}^{k} \sum_{j \in J_i} \lambda_{ij} v_{ij} = 0,$$

hence $x \in H[p^t]$. Note that for all $i \in \{t+2, \ldots, k\}$ we have $p^{i-(t+1)} b_{ij} \in p^{i-(t+1)} H[p^i] \subset pH[p^{t+2}]$. Hence $\sum_{i=t+2}^{k} \sum_{j \in J_i} \lambda_{ij} p^{i-(t+1)} b_{ij} \in pH[p^{t+2}]$. So by definition of x we have

$$\sum_{j \in J_{t+1}} \lambda_{(t+1)j} b_{(t+1)j} \equiv x \equiv 0 \mod H[p^t] + pH[p^{t+2}].$$

Since $(\overline{b_{(t+1)j}})_{j \in J_{t+1}}$ is an $\mathbb{F}_p$-basis of U_{t+1} we have, for each $j \in J_i$, that $\lambda_{(t+1)j} \equiv 0 \mod p$. Hence the claim is true for $s = t + 1$.

Since the lemma holds for $s = 0$, this proves the lemma. □

Lemma 5.9. *The elements of $\mathcal{V}$ are linearly independent over $\mathbb{F}_p$ in $F[p]$.*

Proof. We will show that for each $i \in \{1, \ldots, k\}$ and for each $j \in J_i$ we have $\lambda_{ij} \equiv 0 \mod p$. As a consequence of Lemma 5.8 we have $\sum_{j \in J_k} \lambda_{kj} v_{kj} = 0$. It suffices thus to show that for all $j \in J_k$ we have $\lambda_{kj} \equiv 0 \mod p$. We have

$$p^{k-1} \sum_{j \in J_k} \lambda_{kj} b_{kj} = \sum_{j \in J_k} \lambda_{kj} v_{kj} = 0.$$

Hence we have $\sum_{j \in J_k} \lambda_{kj} b_{kj} \in H[p^{k-1}]$. Since $(\overline{b_{kj}})_{j \in J_k}$ is an $\mathbb{F}_p$-basis of $H/H[p^{k-1}]$ this gives that for each $j \in J_i$ we have $\lambda_{ij} \equiv 0 \mod p$. □

Since for each $i \in \{1, \ldots, k\}$ and for each $j \in J_i$ we have $b_{ij} \in H[p^i] \subset F[p^i] = p^{k-i}F$, there exists $c_{ij} \in F$ such that $p^{k-i} c_{ij} = b_{ij}$. Set

$$\mathcal{C} = \{c_{ij} \mid i \in \{1, \ldots, k\}, j \in J_i\}.$$

This notation will be respected until the end of Section 5.1.

Lemma 5.10. *There exists a subset $\mathcal{X}$ of F such that $\mathcal{C} \cap \mathcal{X} = 0$ and $\mathcal{C} \cup \mathcal{X}$ is a $\mathbb{Z}/p^k\mathbb{Z}$-basis of F.*

Proof. As a consequence of Lemma 5.9, we can extend the set $\mathcal{V}$ to an $\mathbb{F}_p$-basis $\mathcal{V} \cup \mathcal{W}$ of $F[p]$, where we choose $\mathcal{W}$ to be such that $\mathcal{V} \cap \mathcal{W} = 0$. Let $m : F \to F$ denote multiplication by p^{k-1} in F. The image of m is $p^{k-1}F$, which by Lemma 4.11 is equal to $F[p]$. The kernel of m is $F[p^{k-1}]$, which is equal to pF by Lemma 4.11. Hence m induces an isomorphism.

$$\overline{m} : F/pF \to F[p].$$

Let $\pi : F \to F/pF$ be the canonical projection. Note that, for each $i \in \{1, \ldots, k\}$ and each $j \in J_i$, we then have

$$\overline{m}(\pi(c_{ij})) = p^{k-1} c_{ij} = p^{i-1}(p^{k-i} c_{ij}) = p^{i-1} b_{ij} = v_{ij}.$$

For each $w \in \mathcal{W}$, let $x_w \in \overline{m}^{-1}(w)$. Set

$$\mathcal{X} = \{x_w \mid w \in \mathcal{W}\}.$$

Note that since $\mathcal{V} \cap \mathcal{W} = 0$, we have $\mathcal{C} \cap \mathcal{X} = 0$. Now $\overline{m}$ is a bijection from $\pi(\mathcal{C} \cup X)$ to $\mathcal{V} \cup \mathcal{W}$. Since $\overline{m}$ is an isomorphism and $\mathcal{V} \cup \mathcal{W}$ is an $\mathbb{F}_p$-basis of $F[p]$, the set $\pi(\mathcal{C} \cup X)$ is an $\mathbb{F}_p$ basis of F/pF. Hence $\mathcal{C} \cup X$ is a $\mathbb{Z}/p^k\mathbb{Z}$-basis of F. □

Lemma 5.11. *The elements of $\{b_{ij} + pH \mid i \in \{1, \ldots, k\}, j \in J_i\}$ are linearly independent over $\mathbb{F}_p$ in H/pH.*

Proof. For each $i \in \{1, \ldots, k\}$ and for each $j \in J_i$, let $\lambda_{ij} \in \mathbb{Z}$. Suppose $\sum_{i=1}^{k} \sum_{j \in J_i} \lambda_{ij} b_{ij} \in pH$. So there exists $h \in H$ such that $\sum_{i=1}^{k} \sum_{j \in J_i} \lambda_{ij} b_{ij} = ph$. Since, by Lemma 5.7, the set $\mathcal{B}$ generates H, there exist $\mu_{ij} \in \mathbb{Z}$ such that $h = \sum_{i=1}^{k} \sum_{j \in J_i} \mu_{ij} b_{ij}$. Using this and the fact that $p^{k-i} c_{ij} = b_{ij}$ we obtain

$$\sum_{i=1}^{k} \sum_{j \in J_i} (\lambda_{ij} - p\mu_{ij}) p^{k-i} c_{ij} = 0.$$

Now let $i \in \{1, \ldots, k\}$ and let $j \in J_i$. From Lemma 5.10 it follows that the elements of $\mathcal{C}$ are linearly independent over $\mathbb{Z}/p^k\mathbb{Z}$ in F. Hence we know that $(\lambda_{ij} - p\mu_{ij})p^{k-i} \equiv 0 \mod p^k$. This gives us $\lambda_{ij} - p\mu_{ij} \equiv 0 \mod p^i$ and so $\lambda_{ij} \equiv 0 \mod p$. □

Proof of Proposition 5.5. By Lemma 5.10, there exists a subset $\mathcal{X}$ of F such that $\mathcal{C} \cap \mathcal{X} = 0$ and $\mathcal{C} \cup \mathcal{X}$ is a $\mathbb{Z}/p^k\mathbb{Z}$-basis of F. From Lemmas 5.7 and 5.11 it follows that $\{b_{ij} + pH \mid i \in \{1, \ldots, k\}, j \in J_i\}$ is an $\mathbb{F}_p$-basis of H/pH. Furthermore, for each $i \in \{1, \ldots, k\}$ and each $j \in J_i$, we have $b_{ij} = p^{i-1}c_{ij}$. This proves the proposition. □

5.2 Construction of lifts

This section will be devoted to proving the following proposition.

Proposition 5.12. *Let p be a prime number, let k be a positive integer and let $f : B \to C$ be a homomorphism of $\mathbb{Z}/p^k\mathbb{Z}$-modules. Let M_B and M_C be p^k-non-free parts of B and C respectively, such that f restricts to an isomorphism $f_{nf} : M_B \to M_C$. Then there exists a p^k-lift of f.*

Lemma 5.13. *Let p be a prime number, let k be a positive integer and let n be a non-zero integer. Let i be the largest integer such that p^i divides n. Let $m_n : \mathbb{Z}/p^k\mathbb{Z} \to \mathbb{Z}/p^k\mathbb{Z}$ be multiplication by n. Then $\mathbb{Z}/p^{k+i}\mathbb{Z}$ is a p^k-lift of m_n.*

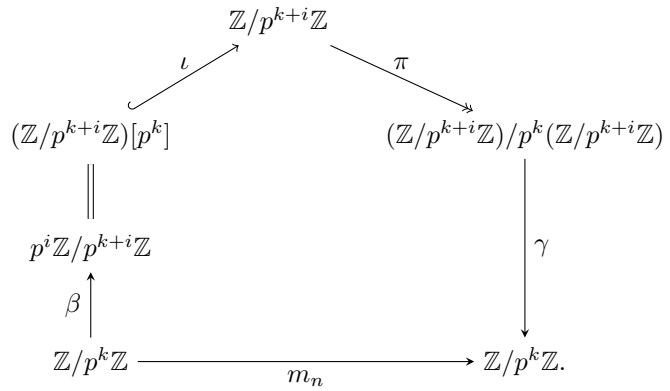
Proof. Define

$$\beta : \mathbb{Z}/p^k\mathbb{Z} \to p^i\mathbb{Z}/p^{k+i}\mathbb{Z}$$

by

$$a + p^k\mathbb{Z} \mapsto na + p^{k+i}\mathbb{Z}$$

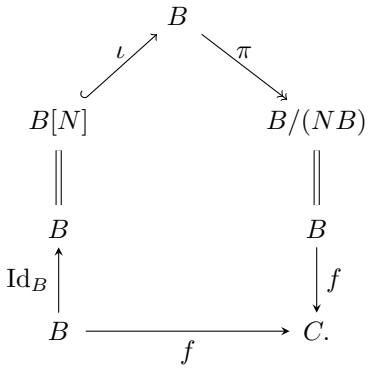
and let γ be the unique ring homomorphism $(\mathbb{Z}/p^{k+i}\mathbb{Z})/p^k(\mathbb{Z}/p^{k+i}\mathbb{Z}) \to \mathbb{Z}/p^k\mathbb{Z}$. The map β is easily shown to be an isomorphism using Lemma 3.2. The map γ is an isomorphism by the isomorphism theorems. Now consider the following diagram.



Here ι is the inclusion and π is the canonical projection. The diagram is commutative and hence $\mathbb{Z}/p^{k+i}\mathbb{Z}$ is a p^k-lift of m_n. □

Lemma 5.14. *Let N be a positive integer and let $f : B \to C$ be an isomorphism of $\mathbb{Z}/N\mathbb{Z}$-modules. Then both B and C are N-lifts of f.*

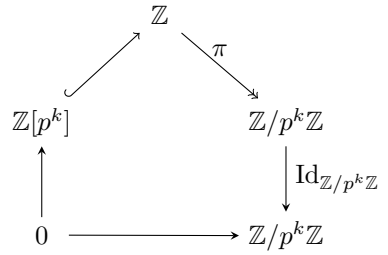
Proof. Since $NB = 0$, we have $B/(NB) = B$. Now consider the diagram below.



Here ι is the inclusion and π is the canonical projection. The diagram is commutative and all maps involved are isomorphisms. Hence B is a N-lift of f. In a similar way one shows that C is also an N-lift of f. □

Lemma 5.15. *Let p be a prime number and let k be a positive integer. The group $\mathbb{Z}$ is a p^k-lift of the homomorphism $0 \to \mathbb{Z}/p^k\mathbb{Z}$.*

Proof. Note that $\mathbb{Z}$ is torsion-free, so $\mathbb{Z}[p^k] = 0$. Let $\pi : \mathbb{Z} \to \mathbb{Z}/p^k\mathbb{Z}$ be the canonical projection. Then the following diagram is commutative.



The diagram shows that $\mathbb{Z}$ is a p^k-lift of the homomorphism $0 \to \mathbb{Z}/p^k\mathbb{Z}$. □

Lemma 5.16. *Let p be a prime number and let k be a positive integer. The group $\mathbb{Q}/\mathbb{Z}$ is a p^k-lift of the homomorphism $\mathbb{Z}/p^k\mathbb{Z} \to 0$.*

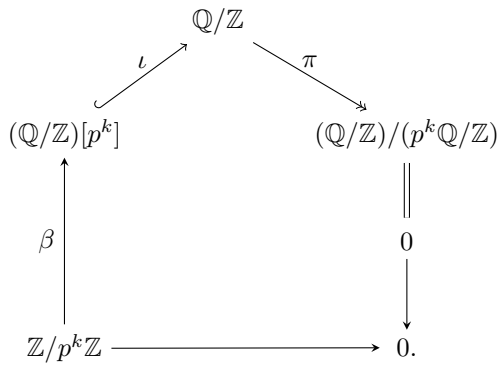
Proof. One easily shows that $(\mathbb{Q}/\mathbb{Z})[p^k] = \{a/p^k \mid a \in \mathbb{Z}\}/\mathbb{Z}$. Now define

$$\beta : \mathbb{Z}/p^k\mathbb{Z} \to (\mathbb{Q}/\mathbb{Z})[p^k]$$

by

$$a + p^k\mathbb{Z} \mapsto a/p^k + \mathbb{Z}.$$

It is a routine check to show that β is an isomorphism. Note that $\mathbb{Q}/\mathbb{Z}$ is divisible, so $p^k(\mathbb{Q}/\mathbb{Z}) = \mathbb{Q}/\mathbb{Z}$. Consider the following diagram.



Here ι is the inclusion map and π is the canonical projection. This diagram is clearly commutative. Moreover, β and the zero-map $0 \to 0$ are both isomorphisms. Hence $\mathbb{Q}/\mathbb{Z}$ is a p^k-lift of the homomorphism $\mathbb{Z}/p^k\mathbb{Z} \to 0$. □

Lemma 5.17. *Let p be a prime number, let k be a positive integer and let $f : B \to C$ be a homomorphism of $\mathbb{Z}/p^k\mathbb{Z}$-modules. Let M_B and M_C be p^k-non-free parts of B and C respectively, such that f restricts to an isomorphism $f_{nf} : M_B \to M_C$. Then, for each p^k-free part F_C of C, there exists a p^k-free part F_B of B and a homomorphism $g : F_B \to F_C$ such that $f = f_{nf} \oplus g$.*

Proof. Let F_C be a p^k-free part of C. We write $F_B = f^{-1}(F_C)$. Since f is a homomorphism and F_C is a subgroup of C, the set F_B is a subgroup of B. We will show that F_B is a complement of M_B.

To show that $M_B \cap F_B = 0$, let $x \in M_B \cap F_B$. Then we have $f(x) \in M_C \cap F_C$. By Theorem 4.3, we have $M_C \cap F_C = 0$. Hence $x \in \ker(f)$. Since $x \in M_B$ and f_{nf} is injective, we get $x = 0$. Since the choice of x was arbitrary, this proves that $M_B \cap F_B = 0$.

Now we will show that $M_B + F_B = B$. Let $b \in B$. By Theorem 4.3, we have $M_C + F_C = C$. Hence there exist $m \in M_C$ and $f \in F_C$ such that $f(b) = m + f$. Since f_{nf} is surjective, there exists $n \in M_B$ such that $f(n) = m$. Now we get $f(b-n) = f(b) - f(n) = f(b) - m = f \in F_C$. Hence $b = n + (b-n) \in M_B + F_B$. The choice of b being arbitrary, this proves $M_B + F_B = B$.

This proves that F_B is a complement of M_B in B. Now we define $g : F_B \to F_C$ by $g(x) = f(x)$. The map g is well-defined by definition of F_B. Now we have $F_B \oplus M_B = B$ and, by Proposition 4.8, we also have $M_C \oplus F_C = C$. Hence we get $f = f_{nf} \oplus g$. Moreover, by Theorem 4.3, the subgroup F_B is a p^k-free part of B. □

Proof of Proposition 5.12. We will write f as a direct sum of homomorphisms that have a p^k-lift, to then apply Proposition 2.2 and get a p^k-lift of f.

Let F_C be a p^k-free part of C, which exists by Proposition 4.5. By Lemma 5.17, there exists a p^k-free part F_B of B and a homomorphism $g : F_B \to F_C$ such that $f = f_{nf} \oplus g$. By Proposition 4.10 we know that F_C is a free $\mathbb{Z}/p^k\mathbb{Z}$-module. The image of g is a submodule of F_C. Hence by Proposition 5.5 there

exist disjoint subsets $(c_j)_{j\in J}$ and $(x_l)_{l\in L}$ in F_C and integers $(s_j)_{j\in J}$ such that $(c_j)_{j\in J} \cup (x_l)_{l\in L}$ is a $\mathbb{Z}/p^k\mathbb{Z}$-basis of F_C and $(p^{s_j}c_j + pIm(g))_{j\in J}$ is an $\mathbb{F}_p$-basis of $Im(g)/pIm(g)$.

For each $j \in J$, let $b_j \in F_B$ be such that $g(b_j) = p^{s_j}c_j$, which exists since $p^{s_j}c_j \in Im(g)$. Let

$$\varphi : F_B/(pF_B + \ker(g)) \to Im(g)/pIm(g)$$

be the isomorphism induces by g. Then, φ maps the set $(b_j + pF_B + \ker(g))_{j\in J}$ to $(p^{s_j}c_j + pIm(g))_{j\in J}$, which is an $\mathbb{F}_p$-basis of $Im(g)/pIm(g)$. Hence $(b_j + pF_B + \ker(g))_{j\in J}$ is an $\mathbb{F}_p$-basis of $F_B/(pF_B + \ker(g))$.

From the linear independence of $(b_j + pF_B + \ker(g))_{j\in J}$ over $\mathbb{F}_p$ it follows that $(b_j+pF_B)_{j\in J}$ are linearly independent over $\mathbb{F}_p$ as well. Now extend $(b_j+pF_B)_{j\in J}$ to an $\mathbb{F}_p$-basis $(b_j+pF_B)_{j\in J}\cup(y_i+pF_B)_{i\in I}$ of F_B/pF_B such that $(y_i)_{i\in I} \subset \ker(g)$. Then $(b_j)_{j\in J} \cup (y_i)_{i\in I}$ is a $\mathbb{Z}/p^k\mathbb{Z}$-basis of F_B.

Since $(y_i)_{i\in I} \subset \ker(g)$, we have $(b_j)_{j\in J} \cap (y_i)_{i\in I} = 0$ and so we can write

$$F_B = \bigoplus_{j\in J} b_j\mathbb{Z}/p^k\mathbb{Z} \oplus \bigoplus_{i\in I} y_i\mathbb{Z}/p^k\mathbb{Z}.$$

Moreover, since we have $(c_j)_{j\in J} \cap (x_l)_{l\in L} = 0$, we can write

$$F_C = \bigoplus_{j\in J} c_j\mathbb{Z}/p^k\mathbb{Z} \oplus \bigoplus_{l\in L} x_l\mathbb{Z}/p^k\mathbb{Z}.$$

Now let $j \in J$. We can restrict g to a map $g_j : b_j\mathbb{Z}/p^k\mathbb{Z} \to c_j\mathbb{Z}/p^k\mathbb{Z}$ since we have $g(b_j) = p^{s_j}c_j$. Let $\beta : b_j\mathbb{Z}/p^k\mathbb{Z} \to \mathbb{Z}/p^k\mathbb{Z}$ be defined by $b_j \mapsto 1$. Moreover, let $\gamma : c_j\mathbb{Z}/p^k\mathbb{Z} \to \mathbb{Z}/p^k\mathbb{Z}$ be defined by $c_j \mapsto 1$. Let furthermore m be multiplication by p^{s_j} in $\mathbb{Z}/p^k\mathbb{Z}$. Consider the diagram

$$\begin{array}{ccc} \mathbb{Z}/p^k\mathbb{Z} & \xrightarrow{\quad m \quad} & \mathbb{Z}/p^k\mathbb{Z} \\ \beta\uparrow & & \uparrow\gamma \\ b_j\mathbb{Z}/p^k\mathbb{Z} & \xrightarrow[g_j]{} & c_j\mathbb{Z}/p^k\mathbb{Z}. \end{array}$$

Here β and γ are readily seen to be isomorphisms and the diagram commutes because $g(b_j) = p^{s_j}c_i$. By Lemma 5.13 we have that $\mathbb{Z}/p^{k+s_i}\mathbb{Z}$ is a p^k-lift of m. Hence $\mathbb{Z}/p^{k+s_j}\mathbb{Z}$ is also a p^k-lift of g_j.

Let $i \in I$. By a similar argument, it follows from Lemma 5.16 that $\mathbb{Q}/\mathbb{Z}$ is a p^k-lift of the homomorphism $u_i : y_i\mathbb{Z}/p^k\mathbb{Z} \to 0$. Note that g and u_i agree on $y_i\mathbb{Z}/p^k\mathbb{Z}$ since $y_i \in \ker(g)$.

Moreover, let $l \in L$ and let v_l be the homomorphism $0 \to x_l\mathbb{Z}/p^k\mathbb{Z}$. As a consequence of Lemma 5.15, we have that $\mathbb{Z}$ is a p^k-lift of v_l.

Since f_{nf} is an isomorphism between p^k-non-free parts, Lemma 5.14 gives us that M_B is a p^k-lift of f_{nf}.

Now we have

$$f = f_{nf} \oplus g = f_{nf} \oplus \bigoplus_{j\in J} g_j \oplus \bigoplus_{i\in I} u_i \oplus \bigoplus_{l\in L} v$$

by definition of these maps. Hence Proposition 2.2 gives us that

$$M_B \oplus \bigoplus_{j \in J} \left(\mathbb{Z}/p^{k+s_j}\mathbb{Z}\right) \oplus \bigoplus_{i \in I} (\mathbb{Q}/\mathbb{Z}) \oplus \bigoplus_{l \in L} \mathbb{Z}$$

is a p^k-lift of f.

Proof of Theorem 5.1. The implication (1) $\Rightarrow$ (2) follows from Proposition 5.4 and the definition of a p^k-lift. The implication (2) $\Rightarrow$ (3) holds, since, by Proposition 4.5, there exists a p^k-non-free part of B. The implication (3) $\Rightarrow$ (1) is given by Proposition 5.12. $\square$

References

[1] S. Lang, *Algebra*, Revised Third Edition, Springer, 2002.

[2] L. Fuchs, *Abelian Groups*, Third Edition, Pergamon Press, 1960.

[3] M. Atiyah and I. MacDonald, *Introduction to Commutative Algebra*, First Indian Edition, Levant Books, 2007.