Finite monoids and actions on group ring units

Perone, M.

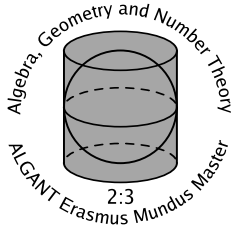
UNIVERSITEIT LEIDEN

Mathematisch Instituut

Finite monoids and actions on group ring units

student: Marco Perone

advisor: Dr. Bart de Smit



Padova, 26 june 2007

Acknowledgements

I would like to thank my supervisor and advisor Dr. B. de Smit for all the support and the attention that he paid to me and to my work during the developing and the writing of this master thesis.

I would like to thank also Prof. Lenstra and Prof. Facchini who agreed to read my thesis and be part of my committee and who suggested interesting comments.

Contents

1 Introduction

Let A be a finite abelian group; the main goal of this thesis is to analyze $\mathbb{Z}[A]^\times$ as a module over a large ring of operators. To do this we do not look at the action of the automorphisms group of A on the group of units, but we consider a large set of operators that has a monoid structure; in this way we have an action that makes the unit group into a module over a monoid ring.

The study of units of a cyclotomic field $\mathbb{Q}(\zeta_n)$, where ζ_n is a primitive n-th root of unity, is an interesting and well-known problem. Since describing the whole group of units turns out not to be easy, the most natural thing to do first is to study a subgroup made by elements with an easy structure; what is usually considered, for n not congruent to 2 modulo 4 is the subgroup of the so-called cyclotomic units, made by units contained in the multiplicative group generated by $\pm\zeta_n$ and elements of the form $1-\zeta_n^a$, for $1 \leq a \leq n-1$. This is a subgroup of full rank in $\mathbb{Z}[\zeta_n]^\times$ and it is possible to explicit a $\mathbb{Z}$-basis of it. Cyclotomic units have also a structure of module over the ring $\mathbb{Z}[G]$, where $G = (\mathbb{Z}/n\mathbb{Z})^\times$ is the Galois group of the cyclotomic field $\mathbb{Q}(\zeta_n)$ over $\mathbb{Q}$, but already when n is not a prime power this structure is not so easy; more details about this can be found in the works of Conrad [5] and Solomon [25].

If C is a finite cyclic group of order n and we consider its associated group ring, we get a ring of the form $\mathbb{Z}[C] \cong \mathbb{Z}[x]/(x^n-1)$, that is contained in the maximal order of the product of number fields $\mathbb{Q}[x]/(x^n-1) \cong \prod_{d|n} \mathbb{Q}(\zeta_d)$, where ζ_d is a primitive d-th root of unity.

In this way we establish a connection between units in a group ring and units in cyclotomic fields. We can try to use this connection in both directions: we can use what is already known about cyclotomic units to deduce information about units in cyclic group rings or, otherwise, try to enlighten the setting of cyclotomic units by explaining the structure of units in a cyclic group ring.

As it is for cyclotomic units, general units in a cyclic group ring are not easy to describe either, so what one needs to do is to restrict to a subgroup made by units, which will be called constructible, that can be expressed by an explicit formula.

One can ask what the gain is by passing to units in group rings instead of working directly with cyclotomic units. What we get is that, for any prime p, we can lift the Frobenius map modulo p to the whole ring, since $\pi_p : x \to x^p$ belongs to the endomorphisms of $\mathbb{Z}[x]/(x^n-1)$. In this way we give to $\mathbb{Z}[x]/(x^n-1)$ the structure of Λ-ring; this notion was introduced by Grothendieck, to give an abstract setting for studying the structure on

Grothendieck groups inherited from exterior power operations. However, it seems that the study of abstract Λ-rings will have something to say about number theory. For this we refer to the paper by Bart de Smit and James Borger, "Galois theory and integral models of Λ-rings" [7].

Adding the morphisms $\pi_p : x \to x^p$, for any prime $p|n$, to the group of automorphisms $(\mathbb{Z}/n\mathbb{Z})^\times$ we obtain an action of the monoid $(\mathbb{Z}/n\mathbb{Z})^\circ$, where the $^\circ$ indicates that we are considering the multiplicative structure of the ring. By doing this we get a finer module structure, which gives a nicer description of the units.

Dealing with actions of the monoid $(\mathbb{Z}/n\mathbb{Z})^\circ$, we are interested in knowing more about $\mathbb{Z}[(\mathbb{Z}/n\mathbb{Z})^\circ]$-modules and therefore, before doing this, we need to know something more about the ring itself. One question that can arise is whether the ring is reduced, i.e. if it does not contain nontrivial nilpotents, and, if this is the case, what its discriminant over $\mathbb{Z}$ is.

At this point it was quite natural to start dealing with a general finite commutative monoid. This is also a reasonable thing to do for the following reason: as $(\mathbb{Z}/n\mathbb{Z})^\times$, that is the Galois group of the cyclotomic extension $\mathbb{Q}(\zeta_n)$ over $\mathbb{Q}$, is the set of invertible elements of the monoid $(\mathbb{Z}/n\mathbb{Z})^\circ$, the ray class group of a number field K is the set of invertible elements of a monoid, called the Deligne-Ribet monoid [6].

We found an easy criterion to decide if the integral monoid ring $\mathbb{Z}[M]$ of a finite commutative monoid M is reduced; if this is the case, we call M itself reduced. The criterion deals just with the elements of the monoid and shows clearly how reduced monoids are a good generalization of finite abelian groups. This comes out to be true in a really surprising way, since there is an equivalence of categories between finite reduced commutative monoids and functors from a finite lattice to finite abelian groups.

Thanks to this equivalence of categories, we are also able to extend duality of abelian groups to reduced monoids. This will turn out to be a nice tool, giving us another easy criterion to decide if a monoid ring is reduced and, if this is not the case, to compute its reduction.

The computation of the discriminant of the monoid ring comes directly from the description of the monoid M as a lattice of finite abelian groups and it is easily seen to be a slight generalization of the finite abelian group case.

Moreover, since $\mathbb{C}[M]$, for M a finite commutative monoid, is an artinian ring, it admits a decomposition into a product of artinian local rings. To underline that the monoid $(\mathbb{Z}/n\mathbb{Z})^\circ$ has some particular property, we compute its components and we deduce that $\mathbb{C}[(\mathbb{Z}/n\mathbb{Z})^\circ]$ is a complete intersection ring.

In the last section, we deal with units in a group ring. If A is a finite abelian group, the units of the ring $\mathbb{Z}[A]$, considered as a $\mathbb{Z}$-module, can be decomposed in the torsion part $\langle -1 \rangle \times A$ times a free abelian group.

If A is a finite abelian group of exponent n, the ring $\mathbb{Z}[A]$ and also the unit group $\mathbb{Z}[A]^\times$ are endowed with an action of the monoid $(\mathbb{Z}/n\mathbb{Z})^\circ$ and therefore they have a structure of $\mathbb{Z}[(\mathbb{Z}/n\mathbb{Z})^\circ]$-modules. As we said above, describing the structure of the whole group turns out not to be easy, so what one tries to do is to construct and understand the structure of subgroups of finite index in the whole group of units.

The first step in this process is to restrict to cyclic subgroups $C \subseteq A$. The second is to restrict to units that have a standard form and can be "constructed" in a easy way. This was done first by Bass, in [2], where he gave a way to construct a set of multiplicative independent units of full rank. Afterwards Hoechsmann and Ritter, in [19], gave a way to build, for p-groups, a set of full rank of multiplicatively independent units, called constructible, in such a way that the index was much smaller than the one obtained by Bass; two years later Hoechsmann improved his construction and extended it to every finite abelian group [10].

What we want to underline is the role that the $\mathbb{Z}[(\mathbb{Z}/n\mathbb{Z})^\circ]$-module structure plays. This was already noticed by Hoechsmann and Ritter in their paper mentioned above, but we try to do it in a more systematic way, changing a little bit the point of view. The main result we obtain in this section is the following: suppose A is cyclic of order n and $(\mathbb{Z}/n\mathbb{Z})^\circ/\langle -1 \rangle$ is cyclic, then the above mentioned group of constructible units is a cyclic $\mathbb{Z}[(\mathbb{Z}/n\mathbb{Z})^\circ]$-submodule of $\mathbb{Z}[A]^\times$.

2 Monoids

2.1 Preliminaries and basic definitions

In this first chapter we deal with finite commutative monoids and their integral monoid rings (from now on we will skip the adjective integral: all monoid rings have to be considered over $\mathbb{Z}$, if there is no further specification). The latter are just a generalization of integral group rings of finite abelian groups, which are all reduced, while monoid rings in general are not; so, we want a criterion that tells us which monoid rings are reduced and which ones are not: this will be the object of the first main theorem.

With the second theorem we describe a way to compute the reduction of a monoid ring, which we will find out to be also a monoid ring, where the monoid lives in the subcategory of the so-called reduced monoids. On this category there is also a duality given by characters and, with this tool, we can find another criterion for $\mathbb{Z}[M]$ to be reduced and we can compute the reduced monoid that gives the reduction of the monoid ring. Furthermore, we will give a description of the category of reduced monoids in terms of lattices of abelian groups; this will also explain the duality we mentioned above in terms of the duality of abelian groups.

Definition 2.1. A *monoid* is a triple $(M, *, e)$, where M is a set, $* : M \times M \to M$ is an associative binary operation with a unit element e.

A *monoid morphism* $f : M \to M'$ between two monoids $(M, *, e)$ and $(M', *', e')$ is a map from M to M' such that

- $f(m_1 * m_2) = f(m_1) *' f(m_2)$ for any two elements m_1, m_2 of M.
- $f(e) = e'$.

A monoid $(M, *, e)$ is said to be *commutative* if $m_1 * m_2 = m_2 * m_1$ for any two elements m_1, m_2 of M.

We say that an element, that will be denoted by 0, of a monoid $(M, *, e)$ is a zero for M if $m * 0 = 0 * m = 0$ for every $m \in M$.

From now on we will drop the star to indicate the product in the monoid $(M, *, e)$, defining $m_1 m_2$ to be $m_1 * m_2$ for every $m_1, m_2 \in M$.

Remark 2.2. If there is another element $e' \in M$ that satisfies the axiom of the unit element e of M, i.e. $e'm = me' = m$ for every $m \in M$, then $e = ee' = e'$. Moreover if an element $m \in M$ admits an inverse, i.e. an element m' such that $mm' = m'm = e$, then this element is unique; indeed if also m'' is an inverse of m, we have that $m' = m'e = m'mm'' = em'' = m''$. We will indicate with $M^\times$ the set of invertible elements of a monoid M.

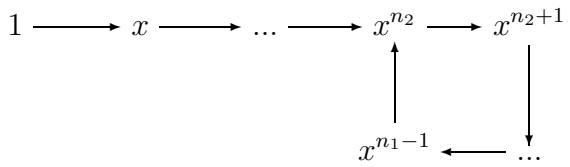
A group is just a monoid such that every element admits an inverse.

From now on we will restrict to commutative monoids, so, also if we forget the adjective, the monoid must be considered commutative.

Example 2.3.

- Given a ring R, considering only its multiplicative structure we obtain a monoid which we will indicate with the symbol R°
- A simple class of monoids is the one made by cyclic monoids, i.e. generated by one element. A cyclic monoid can be infinite, and therefore isomorphic to the monoid coming from the additive structure of natural numbers with the zero included, or it can be finite and in this case it must be of the form $\langle x \mid x^{n_1} = x^{n_2} \rangle$, where $n_1 > n_2$ are distinct non-negative integers; this means that $M = \{1, x, ..., x^{n_1 - 1}\}$ with the multiplication defined by addition of the exponents, where we consider $n_1 = n_2$.

  We can represent a finite cyclic monoid with the following ρ-shaped picture, where the arrows stand for multiplication by x.



Definition 2.4. If R is a commutative ring and M is a monoid we define the *monoid ring* $R[M]$ to be the free R-module with basis M. Then $R[M]$ is naturally a ring with addition defined by addition in the module. Multiplication between two elements $\sum_{l \in M} a_l l$ and $\sum_{m \in M} b_m m$ is defined by $(\sum_{l \in M} a_l l)(\sum_{m \in M} b_m m) = \sum_{l,m \in M} (a_l b_m) lm$, that is extending by linearity the product of the monoid.

Example 2.5. For a finite cyclic monoid $M = \langle x \mid x^{n_1} = x^{n_2} \rangle$, its monoid ring over a given commutative ring R is obviously the polynomial ring $R[x]/(x^{n_1} - x^{n_2})$.

Definition 2.6. An element r of a commutative ring R is said to be *nilpotent* if there exists a positive integer n such that $r^n = 0$.

A commutative ring R is called *reduced* if it has no non-zero nilpotent elements.

A monoid M is called *reduced* if its monoid ring $\mathbb{Z}[M]$ is reduced.

Example 2.7. For a finite cyclic monoid $M = \langle x \mid x^{n_1} = x^{n_2} \rangle$, its integral monoid ring $\mathbb{Z}[x]/(x^{n_1} - x^{n_2})$ is reduced if and only if the smallest between n_1 and n_2 is strictly less than 2. In fact, supposing $n_1 > n_2$, we have the decomposition

$$\mathbb{Z}[x]/(x^{n_1} - x^{n_2}) \cong \mathbb{Z}[x]/(x^{n_2}) \times \mathbb{Z}[x]/(x^{n_1 - n_2} - 1)$$

by the Chinese remainder theorem. The only nilpotent element of the second component of the right hand side is 0, since a group ring is reduced, while $\mathbb{Z}[x]/(x^{n_2})$ has a non trivial nilpotent element if and only if $n_2 \geq 2$.

In the representation with the ρ-shaped diagram, $n_2 < 2$ means that the tail of the ρ has length at most 1.

2.2 Reduced monoid rings

In this section we want to give a criterion to decide whether a monoid ring is already reduced and, if it is not, a way to compute its reduction.

Lemma 2.8. *Let M and M' be finite commutative monoids*

- *if there is a surjective morphism $f : M \to M'$ and M is reduced, then also M' is reduced;*
- *if M and M' are reduced, then also $M \times M'$ is reduced.*

Proof

- First we claim that $\mathbb{Z}[M]$ is reduced if and only if $\mathbb{Q}[M]$ is. Obviously, if $\mathbb{Z}[M]$ has a non trivial nilpotent element, then the same element is a non trivial nilpotent also in $\mathbb{Q}[M]$. For the other implication, take $\sum_{m\in M} a_m m$, with $a_m = b_m/c_m \in \mathbb{Q}$, to be nilpotent; then $(\prod_{m\in M} c_m)\sum_{m\in M} a_m m$ is a nilpotent element of $\mathbb{Z}[M]$.

  Now we want to prove that $\mathbb{C}[M] \cong \mathbb{C} \otimes \mathbb{Q}[M]$ is reduced if and only if $\mathbb{Q}[M]$ is. As above, a non trivial nilpotent in $\mathbb{Q}[M]$ is also a non trivial nilpotent in $\mathbb{C}[M]$. To prove the converse implication, we notice that $\mathbb{Q}[M]$ is an artinian ring and therefore it is a finite direct product of local artinian rings. If $\mathbb{Q}[M]$ is reduced it decomposes in a product of number fields and, tensoring with $\mathbb{C}$, we just get a number of copies of $\mathbb{C}$; therefore $\mathbb{C}[M]$ is reduced.

  Now, supposing $\mathbb{C}[M]$ to be reduced, we have that $\mathbb{C}[M] \cong \mathbb{C} \times ... \times \mathbb{C}$; we consider the map $\mathbb{C}[M] \to \mathbb{C}[M']$ induced by f. Every quotient $\mathbb{C}$-algebra of $\mathbb{C} \times ... \times \mathbb{C}$ is again of the form $\mathbb{C} \times ... \times \mathbb{C}$; this says that $\mathbb{C}[M']$ is also reduced and going back with the implications above we eventually obtain that $\mathbb{Z}[M']$ is reduced.

- We just saw that M reduced is equivalent to $\mathbb{C}[M]$ reduced. It is straightforward to see that the map

$$\begin{array}{ccc} \mathbb{C}[M] \otimes_{\mathbb{C}} \mathbb{C}[M'] & \to & \mathbb{C}[M \times M'] \\ m \otimes m' & \mapsto & (m, m') \end{array}$$

is an isomorphism of $\mathbb{C}$-algebras. From this we can conclude that $M \times M'$ is reduced, since the tensor product of factors of the form $\mathbb{C} \times ... \times \mathbb{C}$ is again of that form.

Theorem 2.9. *Let M be a finite commutative monoid; then the following are equivalent:*

1. *$\mathbb{Z}[M]$ is reduced;*

2. *for every $m \in M$ exists an $n \in \mathbb{N}_{>1}$ such that $m^n = m$.*

Proof Suppose that for every $m \in M$ exists an $n \in \mathbb{N}_{>1}$ such that $m^n = m$; this means that the monoid ring $\mathbb{Z}[\langle m \rangle] \cong \mathbb{Z}[x]/(x^n - x) \cong \mathbb{Z} \times \mathbb{Z}[C_{n-1}]$, where $\langle m \rangle$ is the monoid generated by m and C_{n-1} is the cyclic group with $n-1$ elements, is reduced.

Observing that M is a homomorphic image of the monoid $\prod_{m \in M} \langle m \rangle$, thanks to the previous lemma we can conclude that $\mathbb{Z}[M]$ is reduced.

For the reverse implication, suppose that there exist an $m \in M$ such that $m^n \neq m$ for any integer $n > 1$; since the monoid is finite there must exist two distinct integers n_1 and n_2 bigger or equal than two such that $m^{n_1} = m^{n_2}$. This means that the monoid ring $\mathbb{Z}[M]$ contains as a subring $\mathbb{Z}[\langle m \rangle]$, which by example 2.7 is not reduced, and therefore it is not reduced itself.

Now that we have an easy criterion to compute whether a finite monoid is reduced, we can construct, starting from a general finite monoid M, a quotient monoid that realizes the reduction of the monoid ring $\mathbb{Z}[M]$. First of all, let us make a remark to justify what we are going to do.

Remark 2.10. Let M be a commutative monoid. If m_1 and m_2 are elements in M that have the same eventual powers, i.e. there exists an $\overline{n}$ such that for every $n \geq \overline{n}$, $m_1^n = m_2^n$, then the element $m_1 - m_2$ of the associated monoid ring is nilpotent. In fact we have that $(m_1 - m_2)^{2\overline{n}} = 0$; this comes from the fact that every monomial in the expansion of $(m_1 - m_2)^{2\overline{n}}$ will have the exponent of m_1 or the one of m_2 to be at least $\overline{n}$; therefore all the monomials are equal and summing over all the coefficients of the binomial expansion we will get 0.

Therefore, if we want to avoid nontrival nilpotents just by passing to a quotient monoid, a necessary condition that we have to satisfy is that pairs of elements as in the previous remark need to be identified. This turns out to be enough.

Theorem 2.11. *Let M be a finite commutative monoid. Defining on M the equivalence relation $m_1 \sim m_2$ if m_1 and m_2 have the same eventual powers, then $M/\sim$ is a quotient monoid and $\mathbb{Z}[M/\sim]$ is the reduction of $\mathbb{Z}[M]$.*

Proof First we need to notice that $\sim$ is really an equivalence relation and that $M/\sim$ is still a monoid since the equivalence relation is compatible with the monoid operation. We need to verify that, if $m_1 \sim m_2$ and $m_3 \sim m_4$, then $m_1 m_3 \sim m_2 m_4$; suppose $m_1^n = m_2^n$ for every $n \geq \overline{n}_{12}$ and $m_3^n = m_4^n$ for every $n \geq \overline{n}_{34}$, then we have that $(m_1 m_3)^n = (m_2 m_4)^n$ for every $n \geq max\{\overline{n}_{12}, \overline{n}_{34}\}$.

Since M is a finite monoid, we know that for every $m \in M$ there must exist $n_1, n_2 \in \mathbb{Z}_{\geq 0}$ such that $n_1 > n_2$ and $m^{n_1} = m^{n_2}$. We note that multiplying by $m^{n_1 - n_2}$ acts as the identity on the elements m^i, for $n_2 \leq i < n_1$; therefore, if we choose n' and k such that $n' = 1 + k(n_1 - n_2)$ and $n_2 \leq n' < n_1$, we get that

$$(m^{n'})^{n_2} = m^{n_2}(m^{n_1 - n_2})^{k n_2} = m^{n_2}.$$

We then have that $m \sim m^{n'}$ since multiplication by $m^{n'}$ acts just as multiplication by m on the elements m^i, for $n_2 \leq i < n_1$, and therefore we can take $\overline{n} = n_2$. Now, since the criterion given in the previous theorem is satisfied, we get that $\mathbb{Z}[M/\sim]$ is reduced.

To prove that $\mathbb{Z}[M/\sim]$ is actually the reduction of $\mathbb{Z}[M]$, it is enough to prove that the kernel of the quotient map is nilpotent and this comes directly from the previous remark.

Example 2.12. From what we just proved, we can obtain again that a finite cyclic monoid $M = \langle x \mid x^{n_1} = x^{n_2} \rangle$, where $0 \leq n_2 < n_1$, is reduced if and only if $n_2 \leq 1$. If this is not the case, i.e. $2 \leq n_2$, we can use our last theorem to compute the reduction of the ring: applying the method described there we see that we will identify $x^{n_2 - i}$ with $x^{n_1 - i}$, for $i = 1, ..., n_2 - 1$. The result of this will be the monoid $\langle x \mid x^{n_1 - n_2 + 1} = x \rangle$, whose monoid ring will give us the reduction of the starting one.

Graphically, what we do is just "rolling up" the tail of the ρ around its cycle until the tail has length one.

Example 2.13. Let us consider now the monoid $M = (\mathbb{Z}/n\mathbb{Z})^\circ$. We want to show that its monoid ring is reduced if and only if n is square-free.

If $n = p$ is prime then $(\mathbb{Z}/p\mathbb{Z})^\circ = \mathbb{F}_p^\circ$ is reduced since every element of the monoid satisfy the condition given in theorem 2.9. Suppose now that $n = p_1 \cdot ... \cdot p_k$; then $M = (\mathbb{Z}/n\mathbb{Z})^\circ$ is equal to $\prod_{i=1,...,k} \mathbb{F}_p^\circ$ and therefore, by the second part of lemma 2.8, is reduced. If n is not square-free, then the monoid ring is obviously non reduced. Indeed, let $n = d^2 e$ with $d > 1$; then de is a non trivial nilpotent element.

2.3 Lattices

Proceeding towards the structure theorem for finite commutative reduced monoids, we need to introduce and discuss the concept of lattice. We will

define it in three different ways and prove that the three definitions are equivalent. This will be helpful when we want to pass from one context to another.

Definition 2.14. Let $(S, \leq)$ be a partially ordered set. The greatest lower bound of a subset $S' \subseteq S$ is an element $\overline{s} \in S$ such that $\overline{s} \leq s'$ for every $s' \in S'$ and $s \leq \overline{s}$ for every element $s \in S$ such that $s \leq s'$ for every $s' \in S'$.

It is a *semilattice* if for all elements $s_1, s_2 \in S$, the greatest lower bound of the set $\{s_1, s_2\}$ exists. The greatest lower bound of the set $\{s_1, s_2\}$ is called the *meet* of s_1 and s_2, denoted by $s_1 \wedge s_2$.

A semilattice is *bounded* if it has a greatest element, which will be called *top*.

Definition 2.15. A *algebraic semilattice* is an algebraic structure $(S, \wedge)$ consisting of a set S with the binary operation $\wedge$, called *meet*, such that for all members x, y, and z of S, the following identities hold:

- Associativity: $x \wedge (y \wedge z) = (x \wedge y) \wedge z$;
- Commutativity: $x \wedge y = y \wedge x$;
- Idempotency: $x \wedge x = x$.

An algebraic semilattice $(S, \wedge)$ is *bounded* if S includes the distinguished element 1 such that for all x in S, $x \wedge 1 = x$.

Remark 2.16. Bounded algebraic semilattices are exactly the commutative monoids in which every element is idempotent.

Example 2.17. To give an example of semilattice that will be used later, let M be any commutative monoid; we define $I(M)$ to be the submonoid of M consisting of all its idempotent elements. It is clearly an idempotent commutative monoid and therefore it can be seen as a bounded algebraic semilattice.

As one can suspect, the two definitions given above are equivalent.

Proposition 2.18. *A semilattice $(S, \leq)$ gives rise to a binary operation $\wedge_{\leq}$ such that $(S, \wedge_{\leq})$ is an algebraic semilattice. Conversely, an algebraic semilattice $(S, \wedge)$ gives rise to a binary relation $\leq_{\wedge}$ that partially orders S.*

Moreover, the relation $\leq_{\wedge}$ introduced in this way defines a partial ordering such that $\Lambda = \Lambda_{\leq_{\wedge}}$. Conversely, the order induced by the algebraically defined semilattice $(S, \wedge_{\leq})$ coincides with that induced by $\leq$.

Proof Let $(S, \leq)$ be a semilattice; for every $s_1, s_2 \in S$ let $s_1 \wedge_{\leq} s_2$ be the greatest lower bound of s_1 and s_2. We have that:

- $s_1 \wedge_{\leq} (s_2 \wedge_{\leq} s_3) = (s_1 \wedge_{\leq} s_2) \wedge_{\leq} s_3$ for every s_1, s_2 and s_3 in S, because both terms are equal to the greatest lower bound of the set $\{s_1, s_2, s_3\}$;
- $s_1 \wedge_{\leq} s_2 = s_2 \wedge_{\leq} s_1$ for every s_1 and s_2 in S, because both terms are equal to the greatest lower bound of the set $\{s_1, s_2\}$;
- $s \wedge_{\leq} s = s$ for every $s \in S$, since the greatest lower bound of the set $\{s\}$ is s itself.

This proves that a semilattice gives rise to an algebraic semilattice.

Now let $(S, \wedge)$ be an algebraic semilattice and let us define $x \leq_{\wedge} y \iff x = x \wedge y$. We show that $(S, \leq_{\wedge})$ is a semilattice:

- $x \leq_{\wedge} x$ since $x = x \wedge x$ because of the idempotency of $(S, \wedge)$;
- $x \leq_{\wedge} y$ and $y \leq_{\wedge} x$ implies $x = y$ since the meet operation is commutative;
- $x \leq_{\wedge} y$ and $y \leq_{\wedge} z$ implies $x \leq_{\wedge} z$ since the meet operation is associative;
- for any pair of elements $x, y \in S$, their greatest lower bound is $x \wedge y$ since $x \wedge y = (x \wedge y) \wedge x$ and $x \wedge y = (x \wedge y) \wedge y$; moreover, if $z \in S$ is such that $z \leq_{\wedge} x$ and $z \leq_{\wedge} y$ we get that $z \leq_{\wedge} (x \wedge y)$ since we can deduce $z = z \wedge (x \wedge y)$ from $z = z \wedge x$ and $z = z \wedge y$ using the associativity of the meet operation.

Passing from a semilattice to an algebraic semilattice and from an algebraic semilattice to a semilattice in the way described above are inverse operations. In fact, if we start from a semilattice, we have that $s_1 \leq s_2 \iff s_1 = s_1 \wedge_{\leq} s_2 \iff s_1 \leq_{\wedge_{\leq}} s_2$; conversely, if we start from an algebraic semilattice $(S, \wedge)$, we get that $x \wedge y = x \wedge_{\leq_{\wedge}} y$ since $x \wedge y$ is the greatest lower bound of x and y in the partial order $\leq_{\wedge}$.

Remark 2.19. Obviously, also the boundedness conditions in semilattices and algebraic semilattices are equivalent. In fact, let $(S, \leq)$ be a bounded semilattice with $\overline{s}$ as top; then, for any other element $s \in S$ we have that $s \leq \overline{s} \Rightarrow s \wedge_{\leq} \overline{s} = s$, proving that $(S, \wedge_{\leq})$ is a bounded algebraic semilattice with $1 = \overline{s}$.

Conversely, let $(S, \wedge)$ be a bounded algebraic semilattice containing an element 1 such that $x \wedge 1 = x$ for every $x \in S$; this means exactly that $x \leq_{\wedge} 1$ for every $x \in S$, i.e. $(S, \leq_{\wedge})$ is a bounded semilattice with 1 as top.

At this point we can avoid the use of the adjective algebraic and we will talk only of semilattice, using without difference one of the two definitions given above.

To give a description of the category of bounded semilattices, we need to describe what the morphisms are. Since a bounded semilattice is just an idempotent commutative monoid, the morphisms are the one of the category of monoids; this means that a morphism $f : S \to S'$, between two bounded semilattices $(S, \wedge, 1)$ and $(S', \wedge', 1')$, needs to respect the following axioms:

- $f(x \wedge y) = f(x) \wedge' f(y)$;
- $f(1) = 1'$.

Now we want to interpret everything we said above about semilattices in term of categories. Before stating the result, we need to define a new category.

Definition 2.20. We define *BS category* to be a small category with set of objects S such that:

- for every pair of objects s_1 and s_2 in S, $\sharp\mathrm{Hom}(s_1, s_2) \leq 1$;
- if there exist morphisms $f \in \mathrm{Hom}(s_1, s_2)$ and $g \in \mathrm{Hom}(s_2, s_1)$, then $s_1 = s_2$;
- it admits finite coproducts;
- it has an initial object.

Moreover we define the category of BS categories the category that has as objects the class of BS categories and for morphisms functors between BS categories that respect the coproduct and send the initial object to the initial object.

Proposition 2.21. *There is an equivalence of categories between the category of bounded semilattices and the category of BS categories.*

Proof Given a bounded semilattice $(S, \leq, 1)$ where $\leq$ is the partial order on S with 1 as top, we can interpret it as a BS category taking S as the set of objects and setting $\sharp\mathrm{Hom}(s_1, s_2) = 1$ if and only if $s_2 \leq s_1$; the meet of the semilattice satisfy the property of the coproduct and 1 give rise to an initial object. The antisymmetry of $\leq$ assures that there are no other isomorphisms except the identities.

If we are given a BS category instead, we can order its set of objects by the relation $s_1 \leq s_2 \iff \sharp\mathrm{Hom}(s_2, s_1) = 1$. The meet of two elements will

be their coproduct and the top of the semilattice will be the initial object of the category.

In this setting we see that a morphism of bounded semilattices correspond to a morphism of BS categories and given a functor between two BS categories we can naturally get a morphism between the associated bounded semilattices.

There is almost no need to verify that with these correspondences we have an equivalence of categories, since we are just calling things in two different languages and the dictionary that we gave allows us to pass from one to the other really easily.

Definition 2.22. A *lattice* is a semilattice $(S, \leq)$ such that for every pair of elements s_1 and s_2, the set $\{s_1, s_2\}$ admits a least upper bound, that will be called the *join* of s_1 and s_2 and denoted by $s_1 \vee s_2$. A *bounded lattice* is a bounded semilattice that is a lattice and has a *bottom*, i.e. a smallest element, that will be denoted by 0.

Example 2.23.

- For any set S, the collection of all subsets of S can be ordered via subset inclusion to obtain a lattice bounded by S itself and the null set. Set intersection and union interpret meet and join, respectively.

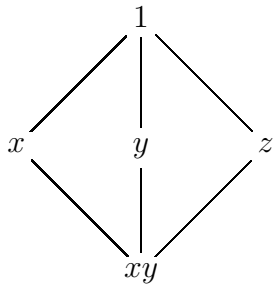
- For any group G, the collection of all subgroups of G can be ordered via inclusion to obtain a lattice bounded by G itself and the trivial group. In this lattice, the join of two subgroups is the subgroup generated by their union, and the meet of two subgroups is their intersection.

- Given a topological space, the collection of its open subsets is a bounded lattice with intersection as meet and union as join, the whole set as top and the empty set as bottom.

Remark 2.24. We want to observe that the lattice made by open sets of a topological space is distributive, i.e. $x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z)$ for every x, y and z elements of the lattice.

Not every lattice has this property; for example, if we consider the finite reduced idempotent commutative monoid $\langle x, y, z \mid x^2 = x, y^2 = y, z^2 = z, xy = xz = yz \rangle$, that is shown as a lattice in the following diagram, we

have that $x \wedge (y \vee z) = x \neq xy = (x \wedge y) \vee (x \wedge z)$



A morphism between two lattices is just a morphism of semilattices that respects the join, too.

Remark 2.25. We need to note that usually the definition of morphism between two bounded lattices requires also that the 0, i.e. the bottom, is preserved. We do not do this since we are considering lattices as particular objects in the category of monoids and so we use the morphisms in this category.

We saw above that an idempotent commutative monoid is a bounded semilattice. Now we want to know which conditions the monoid must satisfy to be a lattice and a bounded lattice.

Remark 2.26. To get a bottom, we need an element $\overline{m}$ such that $\overline{m} \leq m$ for every $m \in M$; this is equivalent of asking for an element $\overline{m}$ such that $\overline{m}m = \overline{m}$, that is a 0 for the monoid.

Therefore if an idempotent commutative monoid M is a lattice, then it is bounded if and only if it has a 0.

Proposition 2.27. *Let M be an idempotent commutative monoid. Then M is a lattice if and only if the set $S(x,y) = \{a \mid x \leq a, y \leq a\}$ has a greatest lower bound for every pair of elements $x, y \in M$.*

Proof If a least upper bound of two elements x and y, which we denote by $x \vee y$, exists, then it belongs to the set $S(x,y)$ and it is the greatest lower bound of $S(x,y)$. In fact $x \leq a$ and $y \leq a$ imply that $x \vee y \leq a$ and if $z \leq a$ for every $a \in S(x,y)$ then $z \leq x \vee y$ since $x \vee y \in S(x,y)$.

Conversely, suppose that the greatest lower bound of the set $S(x,y)$, which we will indicate by $\bigwedge S(x,y)$, exists for every pair x, y of elements in M. Then we can define $x \vee y$ to be $\bigwedge S(x,y)$; in fact:

- $x \leq a$ for every $a \in S(x,y)$ implies that $x \leq \bigwedge S(x,y)$. The same for y;

- $x \leq z$ and $y \leq z$ implies that $\bigwedge S(x,y) \leq z$ since $z \in S(x,y)$.

Remark 2.28. We just want to show that the above condition for M to be a lattice does not imply the existence of a greatest lower bound for any subset S of M. Consider the following partially ordered set. Let $M = \{x^i \mid i \in \mathbb{N}\} \cup \{y^j \mid j \in \mathbb{N}\}$ with the total order generated by the following relations:

- $x^{i_1} \leq x^{i_2} \iff i_1 \geq i_2$;
- $y^{j_1} \leq y^{j_2} \iff j_1 \leq j_2$;
- $y^j \leq x^i$ for any i and j.

We can represent this totally ordered set in the following way:

$$x^0 \geq x^1 \geq x^2 \geq ... \geq x^i \geq ... \geq y^j \geq ... \geq y^2 \geq y^1 \geq y^0$$

Then every pair of elements has a meet and a join, x^0 is the top, y^0 is the bottom, but the subset $\{x^i \mid i \in \mathbb{N}\}$ does not have a greatest lower bound.

If we want to translate the concept of lattice into the language of categories we can just note that, using the dictionary explained above, the axioms of the join translates into the ones of the product and vice versa and the notion of bottom correspond exactly to the one of terminal object.

If moreover we assume that a semilattice is finite, i.e. its defining set is finite, then automatically it admits join, top and bottom and therefore it is in fact a bounded lattice.

Proposition 2.29. *Every finite semilattice is a bounded lattice.*

Proof Let $(S, \leq)$ be a finite semilattice. For every pair x and y of elements of the semilattice the set $S(x,y)$ is finite and therefore, by induction, it admits a greatest lower bound; therefore, by proposition 2.27, S is a lattice. It is bounded since we can take the top and the bottom to be respectively $\bigwedge S$ and $\bigvee S$.

To conclude this section we need to stress a fact that we will use later. We show that in the category of finite lattices we have a duality; this is given by the controvariant functor ^{op} that sends a lattice L to its opposite lattice L^{op} and a morphism of lattices $f : L_1 \to L_2$ to the morphism of lattices

$$\begin{array}{rccc} f^{op}: & L_2^{op} & \to & L_1^{op} \\ & y & \mapsto & \bigwedge_{f(x) \geq y} x \end{array}$$

Proposition 2.30. *The functor ^{op} is an involution.*

The first thing that we need to check is that the functor ^{op} is well defined, and to do this we need to verify that, if $f : L_1 \to L_2$ is a morphism of lattice, then the morphism $f^{op} : L_2^{op} \to L_1^{op}$ defined above is a morphism of lattices, too.

Doing this is equivalent to show that the map $f^* : L_2 \to L_1$, defined as f^{op}, preserves the join and the bottom. For the latter is enough to notice that the image of the 0 of L_2 is the meet of all the elements of L_1 and therefore it is the 0 of L_1.

Suppose now that we have two elements y and y' of L_2 that maps through f^* respectively to $s = \bigwedge\{l \in L_1 \mid f(l \geq y)\}$ and to $t = \bigwedge\{l \in L_1 \mid f(l \geq y')\}$. We can easily observe that $\{l \in L_1 \mid f(l \geq y)\} = \{l \in L_1 \mid l \geq s\}$ and similarly for y' and t. From this we can deduce the implications

$$f(l) \geq y \vee y' \iff f(l) \geq y \text{ and } f(l) \geq y' \iff l \geq s \text{ and } l \geq t \iff l \geq s \vee t.$$

that say that f^* preserves the join.

To prove that our functor is an involution, we need to prove that $\bigwedge\{y \in L_2 \mid \bigwedge\{a \in L_1 \mid f(a) \geq y\} \geq x\} = f(x)$. First we notice that $f(x)$ itself belongs to the set since $\bigwedge\{a \in L_1 \mid f(a) \geq f(x)\} = x$; moreover, there cannot be an element $\leq f(x)$ because this would contradict the condition that defines our set. This proves that applying the functor ^{op} two times we get the identity functor and therefore the functor itself is an involution.

2.4 Structure theorem for finite commutative reduced monoids

One question that can arise when working with monoids is how to construct them; one way to do it is to start with easy monoids, for example cyclic ones or also groups, and enlarge them.

For example, starting with a monoid M, we can add to it a zero, just considering the new monoid $M \dot{\bigcup} \{0\}$, where obviously the operation in M remains the same and $m0 = 0m = 0$ for every $m \in M \dot{\bigcup} \{0\}$.

Similarly, starting with a monoid M, we can add to it a different identity, considering the new monoid $\{1\} \dot{\bigcup} M$, where the operation is defined extending the operation of the monoid M with $1m = m1 = m$ for every $m \in \{1\} \dot{\bigcup} M$. It is clear that in this way the identity of M is no more the identity of the new monoid, since it does not stabilize 1.

We can generalize the constructions given above in the following way: let $(M, \star)$ and $(M', \star')$ be two monoids and $f : M \to M'$ a morphism of monoids. We can obtain a new monoid endowing the set $M \dot{\bigcup} M'$ with the

multiplicative operation that coincide with $\star$ on $M \times M$, with $\star'$ on $M' \times M'$ and is defined by $f(m) \star' m'$ for $(m, m') \in M \times M'$.

This construction can be further generalized to lattices of monoids, and the main result we will obtain in this section is that constructing monoids in this way starting from finite abelian groups allows us to obtain exactly all the finite reduced commutative monoids.

In fact, what we will do is to proceed in the opposite direction; given a finite reduced commutative monoid we will construct a lattice and a family of abelian groups, indexed by the elements of the lattice, from which we can reconstruct the original monoid.

Lemma 2.31. *Let M be a finite commutative monoid; then $I(M) = \{e \in M \mid e^2 = e\}$, the set of idempotents of M, is a bounded lattice.*

Proof As we said in the previous section, $I(M)$ is a bounded semilattice. Since it is finite, by proposition 2.29, it is also a bounded lattice with 1 as top and $\prod_{e \in I(M)} e$ as bottom.

Example 2.32. If $M = \langle x \mid x^{n_1} = x^{n_2} \rangle$, where $0 \leq n_2 < n_1$, is a finite cyclic monoid, then $I(M)$ is equal to $\{1, x^k\}$, where k is the multiple of $n_1 - n_2$ between n_2 and n_1. The order relation is $x^k \leq 1$ since $x^k = 1 \cdot x^k$. If $n_2 = 0$, then $k = 0$ and 1 is the only idempotent.

If M is a reduced monoid we can obtain the submonoid $I(M)$ also as a quotient monoid.

Definition 2.33. Let M a finite commutative monoid; we define the *principal ideal monoid* $\overline{M}$ to be the set $\{mM \mid m \in M\}$ with the operation induced from that of M.

Proposition 2.34. *Let M be a finite reduced commutative monoid. Then the canonical map from $I(M)$ to $\overline{M}$ is an isomorphism.*

Proof What we have to show is just that every fiber of the canonical map $M \to \overline{M}$ contains exactly one idempotent $e \in I(M)$.

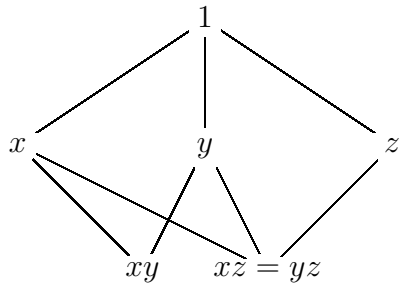
Since M is reduced we know that for every $m \in M$ exists an $n \in \mathbb{N}_{>1}$ such that $m^n = m$; this tells us that m^{n-1} is an idempotent element that belongs to the same fiber of m.

Suppose now that we have two different idempotents e_1 and e_2 in the same fiber; this means that $e_1 = m_1 e_2$ and $e_2 = m_2 e_1$ for some m_1 and m_2 in M. From this we can deduce that $e_1 = m_1 e_2 = m_1 e_2^2 = e_1 e_2 = m_2 e_1^2 = m_2 e_1 = e_2$. Therefore in every fiber of the canonical map $M \to \overline{M}$ we have exactly one idempotent and this means that $\overline{M}$ is isomorphic to the lattice $I(M)$.

Remark 2.35. One can try to consider $\overline{M}$ also for a non reduced monoid M, but it happens that it is not always a lattice.

Consider in fact the monoid $M = \langle x, y, z \mid x^3 = x^2, y^3 = y^2, z^3 = z^2, xz = yz \rangle$; we obtain that both xy and $xz = yz$ are $\leq x$ and y, but an element $\leq x$ and $\leq y$ that is bigger than both xy and $xz = yz$ does not exist. This means that we can not define the meet of x and y and therefore $\overline{M}$ can not be a lattice.

The diagram below depicts the part of the given monoid that describes the impossibility of defining a greatest lower bound of the set $\{x, y\}$



The one pointed out above in proposition 2.34 is not the only property characterizing reduced monoids; if we restrict to them in fact, we also have that every fiber of the canonical map $M \to \overline{M}$ turns out to be a group.

Proposition 2.36. *Let M be a finite reduced commutative monoid, then every fiber of the map $M \to \overline{M}$ is a group.*

Before proving our proposition we need to underline that we cannot expect the fibers to be groups with the same identity as the monoid. Since the fibers are disjoint, only one of them, that turns out to be $M^\times$, will have the identity of the monoid as identity. All the other identities will be provided by the idempotents of M.

Proof We just showed that every fiber can be identified with the only idempotent it contains; therefore we can choose an idempotent e and show that its fiber is a group with e as identity.

- Multiplicativity: $eM = m_1M$ and $eM = m_2M$ imply that $m_1m_2M = e^2M = eM$;
- Identity element: $eM = mM$ implies that $m = e\overline{m}$; from this it follows that $em = e^2\overline{m} = e\overline{m} = m$;
- Inverse: $eM = mM$ implies that $e = mm'$ and this says that em' is the inverse of m.

For finite reduced commutative monoids, we can define the groups coming as fibers just by saying that they are the biggest multiplicative closed subsets that are groups with the idempotents as identity elements; this is done as follows.

Definition 2.37. Let $e \in I(M)$; we define $M_e = \{m \in M \mid m = em\}$ the biggest multiplicative closed subset of M with e as identity element, $N_e = \{m \in M \mid \exists\, m' \in M \text{ such that } mm' = e\}$ and $G_e = M_e \cap N_e$.

Then we have that the fiber of e is equal to G_e. To prove this it is enough to show that $m \in G_e \iff mM = eM$. If $mM = eM$, then $m = e\overline{m} \Rightarrow em = e^2\overline{m} = e\overline{m} = m$ says that $m \in M_e$ and $e = mm'$ tells us that $m \in N_e$, so $m \in G_e$. On the converse, if $m \in G_e$, then $m = em$ and $e = mm'$ mean that $mM = eM$.

Remark 2.38. We can define G_e in the same way for an idempotent e also for a non reduced monoid. Also in this case G_e turns out to be a group and all the G_e's are still disjoint, but they do not cover all the monoid.

Using the methods that we just described we obtain a way to construct the reduction of a finite commutative monoid M as a submonoid.

Proposition 2.39. *Let M be a finite commutative monoid. Then the submonoid M_r consisting of the elements in the groups G_e, where $e \in I(M)$, is isomorphic to the reduced monoid $M/\sim$ that gives the reduction of M, via the canonical morphism $M_r \hookrightarrow M \twoheadrightarrow M/\sim$.*

Proof We need to prove two things:

- every element of M is equivalent to an element of M_r for the relation $\sim$ that defines the reduction of a monoid;
- M_r is reduced.

To prove the first, let $m \in M$; since M is finite, there exist n_1 and n_2 distinct non-negative integers such that $m^{n_1} = m^{n_2}$; this implies that m^k is idempotent, where $n_2 \leq k < n_1$ and $k \equiv 0 \bmod n_1 - n_2$, and that $(m^{k+1})^n = m^n$ for every $n \geq k$, i.e. $m \sim m^{k+1}$, where clearly $m^{k+1} \in G_{m^k}$.

For the second point, let $m \in G_{e_m}$; since G_{e_m} has finite order, then there exists a positive integer k such that $m^k = e_m$; this implies that $m^{k+1} = m$. Therefore the criterion given in theorem 2.9 is satisfied and M_r is reduced.

Corollary 2.40. *Let M be a finite commutative monoid; then, if we consider the canonical map $f : M \to \overline{M}$, we can recover the reduction M_{red} of M just by taking the inverse image through f of the idempotents of $\overline{M}$.*

Proof It is enough to notice that an element of $\overline{M}$ is idempotent if and only if its fiber under the map $M \to \overline{M}$ contains an idempotent. Indeed if $e \in I(M)$, then $(eM)^2 = e^2M = eM$ is idempotent and, conversely, if $(mM)^2 = m^2M = mM$, for $m \in M$, then $m^kM = mM$ for every positive integer k. If we choose $\overline{k}$ to be the multiple of $n_1 - n_2$, where $m^{n_1} = m^{n_2}$, between n_1 and n_2, then $m^{\overline{k}}$ is an idempotent in the same fiber of M.

Therefore the inverse image of the idempotents of $\overline{M}$ is exactly the submonoid of M made by the groups G_e, for $e \in I(M)$.

Corollary 2.41. *The monoid M_r described above is the submonoid of M made by the elements $m \in M$ such that $m^2M = mM$.*

Proof We just proved that $M_r = \coprod_{e \in I(M)} G_e$. We saw also that $G_e = \{m \in M \mid mM = eM\}$ and therefore M_r is made by the elements $m \in M$ such that $mM = eM$ for some idempotent $e \in M$; this is equivalent to say $m^2M = mM$: indeed, if $mM = eM$, then $m^2M = e^2M = eM = mM$; on the other hand, if $m^2M = mM$, then $m^nM = mM$ for every positive n, and we know that some power of m is idempotent since M is finite.

Example 2.42. Let $M = \langle x \mid x^{n_1} = x^{n_2} \rangle$, where $0 \leq n_2 < n_1$, be a finite cyclic monoid. If $n_2 = 0$ then 1 is the only idempotent and M is already a group. If $n_2 > 0$, then there are two idempotents, 1 and x^k, where k is the multiple of $n_1 - n_2$ between n_2 and n_1; then $G_1 = \{1\}$ and G_{x^k} is the cyclic group $\{x^n \mid n_2 \leq n < n_1\}$ generated by x^{k+1}.

The union of the two groups is the whole M if and only if $n_2 < 2$.

Remark 2.43. Let M be a finite commutative monoid and $e, e' \in I(M)$. First we note that $e' \in M_e \iff e \in N_{e'}$. In fact $e' \in M_e$ implies that $e'e = e'$ and this means that $e \in N_{e'}$; on the contrary, if $e \in N_{e'}$, then there exists an $m \in M$ such that $em = e'$, and this implies, using the idempotency of e, that $e' = em = e^2m = ee'$, that is $e' \in M_e$.

These equivalent conditions are also equivalent to say that $e' \leq e$ in the order given considering $I(M)$ as a partial ordered set.

According to proposition 2.21, we can interpret this also in the category theory language: $e' \leq e$ means that we have a unique morphism from e to e'. With this map we associate a group homomorphism $\cdot|_{e'} : G_e \to G_{e'}$ defined by multiplication by e'.

We can summarize what we did above in the following theorem. Before stating this, it is better to give a further definition.

Definition 2.44. A *lattice of abelian groups* is a pair (L, F) where L is a lattice and F is a functor from L, thought as a category, to abelian groups.

A morphism between two lattices of abelian groups $(L, F) \to (L', F')$ is a pair (G, α) where $G : L \to L'$ is a morphism of lattices and α is a natural transformation between the functors F and $F'G$.

Theorem 2.45. *The category of finite reduced commutative monoid is equivalent to the category of finite lattices of finite abelian groups.*

Proof If we are given a finite reduced monoid we can associate to it the lattice of abelian groups $(I(M), G)$, where G is the functor from the finite lattice $I(M)$ to finite abelian groups that sends $e \in I(M)$ to the abelian group G_e and a morphism $e' \leq e$ to the morphism $\cdot|_{e'} : G_e \to G_{e'}$ defined by multiplication by e'.

If we have a finite lattice of finite abelian groups (L, F), where F is a functor that to every element $i \in L$ associates a finite abelian group $F(i)$ and to a morphism $i \leq j$ a morphism $\cdot|_i : F(j) \to F(i)$, we can construct the following finite reduced monoid: let $M = \coprod_{i \in L} F(i)$ and for $m \in F(i)$ and $m' \in F(j)$ we can define their product to be $mm' = m|_{i \wedge j} m'|_{i \wedge j}$ where the product is computed in $F(i \wedge j)$; then M is a monoid with identity the identity of the group corresponding to the initial object of L. It is clearly finite and it is reduced since for every element $m \in F(i)$ we have that $m^{\sharp F(i)+1} = m$ and therefore the criterion of theorem 2.9 is satisfied.

These two maps are one the inverse of the other. Indeed, if we are given a finite lattice of finite abelian groups (L, F) where F is a functor that to every element $i \in L$ associates a finite abelian group $F(i)$ and to a morphism $i \leq j$ a morphism $\cdot|_i : F(j) \to F(i)$, we have that the lattice of the idempotents of the corresponding monoid $M = \coprod_{i \in L} F(i)$ is equal to L and the functor from L to finite abelian groups that we obtain in the way described above is just the starting one.

If we start from a monoid M, we need to check that the operation defined on the monoid $\coprod_{e \in I(M)} G_e$ is the same given on M. Let $m \in G_e$ and $m' \in G_{e'}$; then $m = em$ and $m' = e'm'$ and their product is $mm' = ee'mm'$; we have that the map $\cdot|_{e \wedge e'} : G_e \to G_{e \wedge e'}$ is just multiplication by e' and the map $\cdot|_{e \wedge e'} : G_{e'} \to G_{e \wedge e'}$ is given by multiplication by e. Therefore

$$m|_{e \wedge e'} m'|_{e \wedge e'} = ee'mm' = mm'.$$

To show that there is an equivalence of categories we must show that the behavior is good also at the level of morphisms.

If $f : M_1 \to M_2$ is a morphism of finite reduced commutative monoids then we can obtain a morphism of lattices $\overline{f} : I(M_1) \to I(M_2)$ just by restricting to $I(M_1)$, and f also induces morphisms $f_e : G_e \to G_{\overline{f}(e)}$ by restricting to G_e, giving the data of the required natural transformation.

On the converse, let (L_1, F_1), where F_1 is a functor from the finite bounded lattice L_1 to finite abelian groups sending $i \in L_1$ to $F_1(i)$ and a morphism $i \leq j$ to a morphism $\cdot|_i : F_1(j) \to F_1(i)$, and (L_2, F_2), where F_2 is a functor from the finite bounded lattice L_2 to finite abelian groups sending $i \in L_2$ to $F_2(i)$ and a morphism $i \leq j$ to a morphism $\cdot|_i : F_2(j) \to F_2(i)$, two finite lattices of finite abelian groups. Consider now a morphism of lattices of abelian groups (g, α) where $g : L_1 \to L_2$ is a morphism of lattices and α is a natural transformation between F_1 and $F_2 g$ that gives maps $\alpha_i : F_1(i) \to F_2(g(i))$; we have to show that the map that sends $m \in F(i)$ to $\alpha_i(m)$ is a multiplicative map from $\coprod_{i \in L_1} F_1(i)$ to $\coprod_{i \in L_2} F_2(i)$. Let $m \in F_1(i)$ and $m' \in F_1(j)$; what is to prove is that

$$\alpha_{i \wedge j}(m|_{i \wedge j} m'|_{i \wedge j}) = \alpha_i(m)|_{g(i) \wedge g(j)} \alpha_j(m')|_{g(i) \wedge g(j)}.$$

This is true since $\alpha_{i \wedge j}$ is multiplicative and the commutativity $\alpha_{i \wedge j}(m|_{i \wedge j}) = \alpha_i(m)_{g(i) \wedge g(j)}$ is given by the definition of natural transformation.

To conclude the proof we want to see that also at level of morphism the composition of the two given functors is the identity.

Let $f : M_1 \to M_2$ a morphism of finite reduced commutative monoids. The composition of the two functors will give the map

$$(M_1 \xrightarrow{f} M_2) \to (f_e : G_e \to G_{\overline{f}(e)})_{e \in I(M_1)} \to (\coprod_{e \in I(M_1)} G_e \to \coprod_{e' \in I(M_2)} G_{e'}).$$

The last map will map an element $m \in M$ belonging to the group G_e to the element $f_e(m)$, where f_e is the restriction of f to G_e.

Conversely, if we start with a morphism of lattices of abelian groups as above, and we compose with our two functors, we will get the starting morphism since what we do is just taking the restrictions to the groups $F_1(i)$ after combining them to construct the monoid structure.

The structure theorem for finite reduced commutative monoids gives us also a nice description of the monoid ring of such a monoid.

Proposition 2.46. *Let M be a finite reduced commutative monoid associated to the lattice of abelian groups (L, F). Then the monoid ring $\mathbb{Z}[M]$ is isomorphic to the product of group rings $\prod_{i \in L} \mathbb{Z}[F(i)]$.*

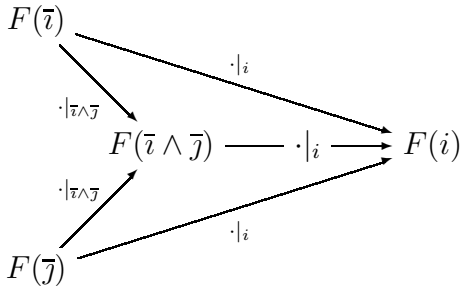
Proof To prove this theorem we want to show that the map

$$\begin{array}{rccc} \varphi : & \mathbb{Z}[M] & \to & \prod_{i \in L} \mathbb{Z}[F(i)] \\ & a & \mapsto & (a_i) \end{array},$$

where $a \in F(\overline{i})$ and $a_i = a|_i$ if $i \leq \overline{i}$, and 0 otherwise, is an isomorphism of rings.

First we want to prove that φ is an homomorphism of rings. Let $a \in F(\overline{i})$ with image $\varphi(a) = (a_i)_{i \in L}$ with $a_i = a|_i$ if $i \leq \overline{i}$ and 0 otherwise, and $b \in F(\overline{j})$ with image $\varphi(b) = (b_i)_{i \in L}$ defined in the same way. We have to show that $(a_i)(b_i) = ((ab)_i) = \varphi(ab)$, where it is clear that $ab \in G_{\overline{i} \wedge \overline{j}}$. We have to prove the equality only in the case $i \leq \overline{i} \wedge \overline{j}$, since otherwise both terms are equal to zero. So we are left to show that $a|_i b|_i = (ab)|_i$ for $i \leq \overline{i} \wedge \overline{j}$.

Our situation is described by the following diagram



we have that

$$\begin{aligned} (ab)|_i &= a|_{\overline{i}\wedge\overline{j}}|_i b|_{\overline{i}\wedge\overline{j}}|_i \\ &= a|_i b|_i \end{aligned}$$

where the first equality is true since $\cdot|_i$ is an morphism of groups and the second because the triangles of the diagram above commute. This shows that φ is an homomorphism of rings.

Now we need to prove that φ is an isomorphism. If we refine the order of the lattice L to a total order, we can represent φ via a matrix of the form

$$\begin{pmatrix} Id & & 0 \\ & \ddots & \\ \star & & Id \end{pmatrix}$$

This is a lower triangular matrix that has all 1 on the diagonal; this means that the map φ is invertible and therefore an isomorphism.

Corollary 2.47. *Let M a finite reduced commutative monoid associated to the lattice of abelian groups (L, F). Then the absolute value of the discriminant of the monoid ring $\mathbb{Z}[M]$ over $\mathbb{Z}$ is equal to $\prod_{i \in L} (\sharp F(i))^{\sharp F(i)}$.*

Proof The proof is made by two not so difficult observations:

- the discriminant of a product is the product of the discriminants ([22], pag.621);

- the absolute value of the discriminant of an integral group ring $\mathbb{Z}[G]$, where G is a finite group of order n, is equal to n^n [4].

2.5 Duality of monoids

In this section we explain how we can extend the usual notion of duality of finite abelian groups to monoids and how to use this notion to give a criterion for being reduced and a way to compute the reduction.

Definition 2.48. Let M be a monoid. A *character* of M is a map of monoids from M to $\mathbb{C}^\circ$.

The collection of the characters of M form a monoid, called the *dual monoid* of M and denoted by $M^\vee = \mathrm{Hom}(M, \mathbb{C}^\circ)$, with as identity the trivial morphism that sends M to 1 and multiplication defined by $f_1 f_2(m) = f_1(m) f_2(m)$.

Remark 2.49. We note that if M is a group, then $M^\vee$ is its dual group.

Remark 2.50. If M is a finite monoid every element of the dual monoid $M^\vee$ maps M to the submonoid of $\mathbb{C}$ given by $\{0\} \cup \mu_\infty$, where with μ_∞ we denote the set of all roots of unity, since every element $m \in M$ satisfies an equation of the form $m^{n_1} = m^{n_2}$, where n_1 and n_2 are distinct non-negative integers.

Lemma 2.51. *If M is a finite commutative monoid, then its dual $M^\vee$ is reduced.*

Proof If we take $f \in M^\vee$, it sends every element $m \in M$ either to 0 or to a root of unity, say of order n_m; let n be the least common multiple of all the n_m. Then we have that $f^{n+1}(m) = f(m)$ for every $m \in M$ and so $f^{n+1} = f$. This implies that the monoid ring $\mathbb{Z}[M^\vee]$ is reduced, thanks to theorem 2.9.

There is a natural homomorphism from M to its double dual $M^{\vee\vee} = \mathrm{Hom}\{M^\vee, \mathbb{C}^\circ\}$ defined by

$$\begin{array}{ccccccc} M & \to & M^{\vee\vee} & & & & \\ m & \mapsto & m^{\vee\vee} : & M^\vee & \to & \mathbb{C}^\circ \\ & & & f & \mapsto & f(m) \end{array}$$

By the previous lemma we have that $M^{\vee\vee}$ is also reduced and so the map $M \to M^{\vee\vee}$ factors through the reduction M_{red} of M.

It is well-known that on the category of finite abelian groups the map described above gives a canonical isomorphism between a group and its double dual. What we want to do now is to show that this is true also on the category of finite reduced monoids.

To do this we will prove that if a finite reduced monoid M is associated to the lattice of abelian groups (L, F) then its dual $M^\vee$ corresponds to the lattice of abelian groups $(L^{op}, ^\vee \circ F)$, where the last $^\vee$ denotes duality in finite abelian groups. Since both duality in finite abelian groups and taking the opposite lattice are involution, we will get that also in reduced monoids it is so.

Before proving this we need three useful lemmas.

Lemma 2.52. *A monoid character of a finite reduced commutative monoid M is, restricted to any group G_e, for $e \in I(M)$, either the 0 morphism or a group character.*

Proof The only difference between a monoid character and a group character is that the first can assume also 0 as a value. Since G_e is finite, for any $g \in G_e$ there exists a positive integer n such that $g^n = e$; therefore, if an element $\overline{g} \in G_e$ is not mapped to 0, then also the identity of G_e is not mapped to zero. Moreover, since any element $g \in G$ is invertible, it must be sent to an element that divides the image of the identity of G_e; therefore the value 0 can not be assumed.

Lemma 2.53. *Let M be a finite reduced commutative monoid. If a monoid character $f : M \to \mathbb{C}^\circ$ does not map to zero the groups G_{e_1} and G_{e_2}, then it does not map to zero also $G_{e_1 e_2}$.*

Proof If $m_1 \in G_{e_1}$ and $m_2 \in G_{e_2}$ are elements of M such that $f(m_1) \neq 0 \neq f(m_2)$, then $m_1 m_2$ is an element in $G_{e_1 e_2}$ that is not mapped to 0.

These two lemmas imply that for any character $f \in M^\vee$ there is a smallest idempotent e_f such that f restricted to G_{e_f} is a group character of the group G_{e_f}.

We will denote the restriction of a character f to the group G_{e_f} simply by the symbol $f|$

Lemma 2.54. *A monoid morphism f from a finite reduced commutative monoid is determined by its restriction $f|$ to the group G_{e_f}.*

Proof By definition of e_f every element in a group $G_{e'}$, where e' is not $\geq e$, is mapped to 0. Since $f|$ is a group morphism, e_f must be mapped to 1 by $f|$; given any other element $m \in G_{e'}$, for $e' \geq e$, we have that $f(m) = f(m)f(e_f) = f(me_f) = f|(me_f)$.

Theorem 2.55. *Let M be a finite reduced commutative monoid associated to the lattice of abelian groups (L, F), where F sends a morphism $i \leq j$ to the morphism $\cdot|_i : F(j) \to F(i)$; then the dual $M^\vee$ of M is the finite reduced commutative monoid associated to the lattice of abelian groups $(L^{op}, ^\vee \circ F)$, where the last $^\vee$ denotes duality of finite abelian groups, that sends the morphism $j \leq i$ to the morphism $\cdot|_i^\vee : F(i)^\vee \to F(j)^\vee$, dual of $\cdot|_i$.*

Proof As a consequence of the above lemmas, we can define the map

$$\begin{array}{rccc} \chi: & M^\vee & \to & N \\ & f & \mapsto & f| \in G_{e_f}^\vee \end{array}$$

where N is the monoid associated to the lattice of abelian groups $(L^{op}, ^\vee \circ F)$. Lemma 2.54 tells us that this map is injective.

For the surjectivity we have that, if $f \in N$ is an element of $G_e^\vee$, then we can define the following element of $M^\vee$

$$\begin{array}{rcl} M & \to & \mathbb{C}^\circ \\ m & \mapsto & \begin{cases} f(em) & \text{if } mM \supseteq eM \\ 0 & \text{otherwise} \end{cases} \end{array}$$

that coincide with f on G_e.

We are left to prove that χ is a morphism of monoids:

- it sends the trivial character to the trivial character of the group $G_{\overline{e}}$, where $\overline{e}$ is the bottom in the lattice $I(M)$, that is the identity in the monoid N;
- for the multiplicativity, consider two characters $g, h \in M^\vee$; we have to show that $\chi(gh)(m) = (\chi(g)\chi(h))(m)$ for any $m \in G_{e_{gh}} = G_{e_g \vee e_h}$. By definition we have that

  $$\chi(gh)(m) = (gh)|(m) = g(m)h(m)$$

  and

  $$(\chi(g)\chi(h))(m) = (g|h|)(m).$$

  By how the product acts in N we have that

  $$\begin{array}{rcl} (g|h|)(m) & = & (g|)|_{e_g}^\vee(m)(h|)|_{e_h}^\vee(m) \\ & = & g|(e_g m)h|(e_h m) \\ & = & g(e_g m)h(e_h m) = g(m)h(m) \end{array}$$

  since the idempotents are mapped to 1.

Corollary 2.56. *If M is a finite reduced commutative monoid, then the map $M \to M^{\vee\vee}$ described above is an isomorphism.*

Proof It is enough to notice that taking the dual is an involution both on lattices and on abelian groups and to use the structure theorem for finite reduced commutative monoids.

Now that we know more about how duality works on finite reduced monoids, we can proceed by explaining the role of $M^{\vee\vee}$ in the reduction of a finite commutative monoid M.

Proposition 2.57. *If M be a finite commutative monoid, then $M^{\vee\vee} \cong M_{red}$.*

Proof What we prove in fact is that the dual map $M_{red}^{\vee} \to M^{\vee}$ of the canonical map $M \to M_{red}$ is an isomorphism; then, dualizing this map, we will get an isomorphism $M^{\vee\vee} \to M_{red}^{\vee\vee} \cong M_{red}$.

Now, let $f \in M_{red}^{\vee}$; if $f \neq 1$, there is an element in M_{red} that is not mapped to 1 by f. Since $M \to M_{red}$ is surjective, there exists an $m' \in M$ that is mapped to m and therefore is not mapped to 1 by the image of f in $M^{\vee}$; this means that $M_{red}^{\vee} \to M^{\vee}$ is injective.

To prove the surjectivity, we need to show that every character of M factors through M_{red}. This is true because two elements of M that have the same image in M_{red} have the same eventual powers and therefore they must have the same image in $\mathbb{C}^{\circ}$.

As a consequence of this proposition, we have another criterion to decide whether a monoid is reduced or not.

Corollary 2.58. *Let M be a finite commutative monoid. Then M is reduced if and only if $\sharp M = \sharp M^{\vee}$.*

Proof First we have to notice that $\sharp M^{\vee} = \sharp M^{\vee\vee}$, since this is true at the level of abelian groups and $M^{\vee}$ is a reduced monoid.

If M is reduced, as we said above, the map that sends $m \in M$ to $m^{\vee\vee} \in M^{\vee\vee}$ is an isomorphism.

If M is not reduced than we saw than $\sharp M_{red} < \sharp M$, since M_{red} is a quotient monoid of M different from M.

To conclude the section we want to give some examples.

Example 2.59. Let $M = \langle x \mid x^{n_1} = x^{n_2} \rangle$ be a finite cyclic monoid; suppose also that $0 < n_2 < n_1$ to avoid the case where M is the cyclic group of order n_1.

To define a character on M we have only to decide where to send x; the choice must be done inside the set of the complex numbers z that satisfies the defining equation for x, i.e. $z^{n_1} - z^{n_2} = z^{n_2}(z^{n_1-n_2} - 1) = 0$. Therefore all the possible characters are the following:

$$g : x \mapsto 0$$

$$f_i : x \mapsto \zeta_{n_1-n_2}^i$$

for $i = 0, ..., n_1 - n_2 - 1$, where $\zeta_{n_1-n_2}$ is a primitive $(n_1 - n_2)$-th root of unity.

Moreover we have $g \cdot f_i = g$ and $f_i \cdot f_j = f_{i+j \bmod n_1-n_2}$. Therefore we can represent the monoid $M^\vee$ with the lattice of abelian groups

$$C_{n_1-n_2} \to C_1$$

where C_n indicates the cyclic group of order n.

By dualizing this diagram, we get that $M^{\vee\vee}$ is associated to the lattice of abelian groups

$$C_1 \to C_{n_1-n_2}$$

that is clearly the monoid $M = \langle x \mid x^{n_1-n_2+1} = x \rangle$.

We have also

$$\begin{array}{rccc} 1^{\vee\vee} : & M^\vee & \to & \mathbb{C}^\circ \\ & f & \mapsto & f(1) = 1 \end{array}$$

where f is any element in $M^\vee$, and

$$\begin{array}{rccc} (x^j)^{\vee\vee} : & M^\vee & \to & \mathbb{C}^\circ \\ & g & \mapsto & g(x^j) = 0 \\ & f_i & \mapsto & f_i(x^j) = \zeta_{n_1-n_2}^{ij} \end{array}$$

Clearly $1^{\vee\vee}(x^j)^{\vee\vee} = (x^j)^{\vee\vee}$ and $(x^{j_1})^{\vee\vee}(x^{j_2})^{\vee\vee} = (x^{j_1+j_2 \bmod n_1-n_2})^{\vee\vee}$, making in this way explicit the isomorphism between M_{red} and $M^{\vee\vee}$.

Example 2.60. We want to compute the dual of the monoid $M = (\mathbb{Z}/4\mathbb{Z})^\circ = \{0, 1, 2, -1\}$ that is not reduced.

The reduction is easily seen to be $M_{red} = \{0, 1, -1\}$ where the quotient map identifies 0 and 2, since $2 - 0$ is nilpotent in the monoid ring $\mathbb{Z}[(\mathbb{Z}/4\mathbb{Z})^\circ]$. Its associated lattice of abelian groups is clearly

$$C_2 \longrightarrow C_1$$

and therefore, dualizing the groups and the lattice, we obtain that $M^\vee$ is

$$C_1 \longrightarrow C_2$$

which is the cyclic monoid $\langle x \mid x = x^3 \rangle$.

To make the things explicit, the non trivial characters of M are

$$\begin{array}{rccc} \chi: & M & \to & \mathbb{C}^\circ \\ & 0,2 & \mapsto & 0 \\ & 1 & \mapsto & 1 \\ & -1 & \mapsto & -1 \end{array}$$

and

$$\begin{array}{rccc} \chi^2: & M & \to & \mathbb{C}^\circ \\ & 0,2 & \mapsto & 0 \\ & 1,-1 & \mapsto & 1 \end{array}$$

3 The monoid $(\mathbb{Z}/n\mathbb{Z})^\circ$

We want to dedicate a whole chapter to this special class of monoids to emphasize their role and to use them as a bridge between the preceding and the following chapter.

We already know from the first chapter, example 2.13, that a monoid of the form $(\mathbb{Z}/n\mathbb{Z})^\circ$ is reduced if and only if n is square-free. Here we want to apply the theory developed above to explicitly describe what the reduction of $(\mathbb{Z}/n\mathbb{Z})^\circ$ is, what its associate lattice $I((\mathbb{Z}/n\mathbb{Z})^\circ)$ is and what the groups G_e are, for $e \in I((\mathbb{Z}/n\mathbb{Z})^\circ)$.

Moreover, we point out another particularity of the monoids $(\mathbb{Z}/n\mathbb{Z})^\circ$: in the decomposition of $\mathbb{C}[(\mathbb{Z}/n\mathbb{Z})^\circ]$ as a direct product of local rings, we obtain only rings of the form $\mathbb{C}[x_1, ..., x_l]/(x_1^{k_1}, ..., x_l^{k_l})$.

3.1 Reduction of the monoid ring $(\mathbb{Z}/n\mathbb{Z})^\circ$

First we observe that the fibers of the map $(\mathbb{Z}/n\mathbb{Z})^\circ \to \overline{(\mathbb{Z}/n\mathbb{Z})^\circ}$ can be identified via an easy criterion.

Lemma 3.1. *Let $M = (\mathbb{Z}/n\mathbb{Z})^\circ$. Then $m_1 M = m_2 M \Leftrightarrow \gcd(m_1, n) = \gcd(m_2, n)$.*

Proof We just need to recall that the ring $\mathbb{Z}/n\mathbb{Z}$ is a principal ideal ring and the greatest common divisor of $m \in \mathbb{Z}/n\mathbb{Z}$ with n is the smallest element of the ideal $mM = (m, n)$ if we choose $\{1, ..., n\}$ as representatives for $\mathbb{Z}/n\mathbb{Z}$ and we order them in the usual way.

To make things easier, we notice that the monoid $(\mathbb{Z}/n\mathbb{Z})^\circ$, where $n = p_1^{\nu_1} \cdot ... \cdot p_k^{\nu_k}$ is the product of the monoids $(\mathbb{Z}/p_i^{\nu_i}\mathbb{Z})^\circ$. Indeed the map

$$\begin{array}{rccc} f: & (\mathbb{Z}/n\mathbb{Z})^\circ & \to & \prod_{i=1,...,k}(\mathbb{Z}/p_i^{\nu_i}\mathbb{Z})^\circ \\ & m & \mapsto & (m \bmod p_i^{\nu_i}) \end{array}$$

is multiplicative and it is a ring isomorphism by the Chinese remainder theorem.

This allows us to deal first with n a prime power, and then deduce results for a general n.

Now we want to give a criterion to describe the idempotents of $M = (\mathbb{Z}/n\mathbb{Z})^\circ$. Before doing this we need a definition.

Definition 3.2. A divisor d of an integer n is called *unitary* if d is coprime with n/d.

Proposition 3.3. *Let $M = (\mathbb{Z}/n\mathbb{Z})^\circ$; then the idempotents of M are the elements that are congruent either to 0 or to 1 with respect to every unitary divisor of n that is a prime power.*

Proof If $n = p^\nu$ is a prime power then the only idempotents of M are 0 and 1 since these two are the only solutions of the congruence $m^2 \equiv m \bmod p^\nu$.

For a general n, we have just to take the product of all the $(\mathbb{Z}/d\mathbb{Z})^\circ$, for d unitary divisor of n, and use the Chinese remainder theorem.

Moreover, we can notice that the Euclidean algorithm gives us an explicit way to find the solutions of the set of congruences and therefore all the idempotents of $(\mathbb{Z}/n\mathbb{Z})^\circ$.

Remark 3.4. From this proposition we get also that the lattice $I(M)$ of idempotents for a monoid $M = (\mathbb{Z}/n\mathbb{Z})^\circ$ is exactly the lattice of unitary divisors of n. This lattice is clearly the k-th hypercube, where k is the number of primes dividing n.

The next step to describe the structure of $M = (\mathbb{Z}/n\mathbb{Z})^\circ$ is to give a description of the abelian groups G_e for $e \in I(M)$.

First we can make a general remark about the cardinality of a fiber of the map $M \to \overline{M}$.

Remark 3.5. We saw above that $m_1 M = m_2 M \Leftrightarrow \gcd(m_1, n) = \gcd(m_2, n)$; this implies that the cardinality of the fiber determined by a divisor d of n is equal to the number of elements in M that have greatest common divisor with n equal to d.

This number is clearly equal to $\varphi(n/d)$ since there is a bijection from $(\mathbb{Z}/(n/d)\mathbb{Z})^\times$ to our fiber given by multiplication by d.

This bijection is not always a morphism of monoids, but, when d is a unitary divisor, we can modify it to be so.

Proposition 3.6. *Let $M = (\mathbb{Z}/n\mathbb{Z})^\circ$ and $e \in I(M)$ an idempotent of M. Then the group G_e is isomorphic to the group $(\mathbb{Z}/(n/\gcd(n,e))\mathbb{Z})^\times$.*

Proof We know that an idempotent $e \in I(M)$ is in the class of a unitary divisor $d = \gcd(n, e)$.

If we modify the map from $(\mathbb{Z}/(n/d)\mathbb{Z})^\times$ to G_e in the previous remark substituting multiplication by d by multiplication by e we still obtain a bijection, but, since e is idempotent, in this case it is also a morphism of groups.

To conclude with the description of G_e, for $e \in I(M)$, we can recall that $(\mathbb{Z}/n\mathbb{Z})^\times$ is cyclic if and only if $n = 1, 2, 4, p^\nu, 2p^\nu$ for p an odd prime and

$\nu > 0$, while for $n = 2^k$, with $k > 2$, $(\mathbb{Z}/n\mathbb{Z})^\times \cong C_2 \oplus C_{2^{k-2}}$; for the other n's it is enough to use the Chinese remainder theorem to deduce the structure of $(\mathbb{Z}/n\mathbb{Z})^\times$.

Remark 3.7. We can observe that all the monoids $(\mathbb{Z}/p^\nu\mathbb{Z})^\circ$, for p an odd prime, are co-cyclic, with this meaning that their dual is cyclic. Indeed the lattice of abelian group associated to $(\mathbb{Z}/p^\nu\mathbb{Z})^\circ$ is

$$C_{\varphi(p^\nu)} \longrightarrow C_1$$

and therefore its dual is

$$C_1 \longrightarrow C_{\varphi(p^\nu)}$$

that is associated to the cyclic monoid $\langle x \mid x^{\varphi(p^\nu)} = x^{\varphi(p^\nu)+1} \rangle$.

3.2 Decomposition in local rings of $\mathbb{C}[(\mathbb{Z}/n\mathbb{Z})^\circ]$

The ring $\mathbb{C}[(\mathbb{Z}/n\mathbb{Z})^\circ]$ is an artinian ring since it is a finite dimensional vector space over a field. We recall that every artinian ring is uniquely, up to isomorphism, a direct product of local artinian rings; for more details we refer to [1].

Lemma 3.8. *The monoid ring $\mathbb{C}[(\mathbb{Z}/n\mathbb{Z})^\circ]$, where $n = p_1^{\nu_1} \cdot \ldots \cdot p_k^{\nu_k}$, is isomorphic to the tensor product of the monoid rings $\mathbb{C}[(\mathbb{Z}/p_i^{\nu_i}\mathbb{Z})^\circ]$, for $i = 1, ..., k$.*

Proof Extending by linearity on each component the inverse of the map f described in the beginning of the previous section, we can construct a multilinear map

$$\begin{array}{ccc} \prod_{i=1,\ldots,k} \mathbb{C}[(\mathbb{Z}/p_i^{\nu_i}\mathbb{Z})^\circ] & \to & \mathbb{C}[\prod_{i=1,\ldots,k}(\mathbb{Z}/p_i^{\nu_i}\mathbb{Z})^\circ] \cong \mathbb{C}[(\mathbb{Z}/n\mathbb{Z})^\circ] \\ (a_i) & \mapsto & f^{-1}((a_i)_{i=1,\ldots,k}) \end{array}$$

that induces an isomorphism between $\bigotimes_{i=1,\ldots,k} \mathbb{C}[(\mathbb{Z}/p_i^{\nu_i}\mathbb{Z})^\circ]$ and $\mathbb{C}[(\mathbb{Z}/n\mathbb{Z})^\circ]$.

Therefore we can restrict to the case where n is a power of a prime p.

Proposition 3.9. *Every local artinian ring in the decomposition of the monoid ring $\mathbb{C}[(\mathbb{Z}/p^\nu\mathbb{Z})^\circ]$ is of the form $\mathbb{C}[x]/(x^k)$ for some positive integer k depending on the component.*

Proof First thing to notice is that we have a surjective monoid morphism

$$\begin{array}{ccc} C_\nu \times (\mathbb{Z}/p^\nu\mathbb{Z})^\times & \to & (\mathbb{Z}/p^\nu\mathbb{Z})^\circ \\ (x^a, b) & \mapsto & p^a b \end{array}$$

where C_ν is the cyclic monoid $\langle x \mid x^{\nu+1} = x^\nu \rangle$. If we consider the monoid ring over the complex numbers of the left-hand side, we see that

$$\mathbb{C}[C_\nu \times (\mathbb{Z}/p^\nu\mathbb{Z})^\times] \cong \mathbb{C}[C_\nu] \otimes \mathbb{C}[(\mathbb{Z}/p^\nu\mathbb{Z})^\times].$$

The two factors of the right-hand side are

$$\mathbb{C}[C_\nu] \cong \mathbb{C} \times \mathbb{C}[x]/(x^\nu)$$

and

$$\mathbb{C}[(\mathbb{Z}/p^\nu\mathbb{Z})^\times] \cong \mathbb{C} \times ... \times \mathbb{C}$$

since a group ring is reduced.

Taking the tensor product of these two, we get that $\mathbb{C}[C_\nu \times (\mathbb{Z}/p^\nu\mathbb{Z})^\times]$ is the product of components of the form $\mathbb{C}[x]/(x^k)$ for some positive integer k depending on the component. The surjection that we pointed out first tells us that $\mathbb{C}[(\mathbb{Z}/p^\nu\mathbb{Z})^\circ]$ is just a quotient of $\mathbb{C}[C_\nu \times (\mathbb{Z}/p^\nu\mathbb{Z})^\times]$ and, since every quotient of $\mathbb{C}[x]/(x^k)$ has the same form, our starting monoid ring must be a product of local rings of this form, too.

Going back to a general n, just taking the tensor product of the complex rings $\mathbb{C}[(\mathbb{Z}/p^\nu\mathbb{Z})^\circ]$ for p^ν unitary divisor of n, we get that every local artinian ring in the decomposition of the monoid ring $\mathbb{C}[(\mathbb{Z}/n\mathbb{Z})^\circ]$ is of the form $\mathbb{C}[x_1, ..., x_l]/(x_1^{k_1}, ..., x_l^{k_l})$.

This implies that the ring $\mathbb{C}[M]$ is a complete intersection ring. For this definition of commutative algebra, and the ones that will follow, we refer to [8].

To see that this is really a restrictive condition on M, we give an example of a monoid whose monoid ring over $\mathbb{C}$ is not a complete intersection.

Example 3.10. Let $M = \{1, 0, x, y\}$ with the relations $x^2 = y^2 = xy = 0$. Some computations give that the decomposition in local rings of $\mathbb{C}[M]$ is

$$\mathbb{C}[M] \cong \mathbb{C} \times \mathbb{C}[x, y]/(x, y)^2.$$

The second component of the right hand side is not a complete intersection since it is a zero dimensional local ring that is not Gorenstein; indeed being Gorenstein is equivalent to having a simple socle, where the latter is the annihilator of the maximal ideal, and the annihilator of the maximal ideal (x, y) is the ideal (x, y) itself, that is not simple.

Remark 3.11. We need to observe that what we proved for $\mathbb{C}$ is no more true if we consider $\mathbb{Z}$ or a finite field. For example, if we consider the monoid

$(\mathbb{Z}/4\mathbb{Z})^\circ$ and we take its monoid ring over the field $\mathbb{F}_2$ of two elements, we obtain that the map

$$\begin{array}{ccc} \mathbb{F}_2[(\mathbb{Z}/4\mathbb{Z})^\circ] & \to & \mathbb{F}_2 \times \mathbb{F}_2[x,y]/(x,y)^2 \\ 0 & \mapsto & (1,0) \\ 1 & \mapsto & (1,1) \\ -1 & \mapsto & (1,y+1) \\ 2 & \mapsto & (1,x) \end{array}$$

is an isomorphism. By a reasoning similar to the one in the previous example we have that the second component of the right-hand side is not Gorenstein and therefore $\mathbb{F}_2[(\mathbb{Z}/4\mathbb{Z})^\circ]$ is not a complete intersection ring.

This implies that also $\mathbb{Z}[(\mathbb{Z}/4\mathbb{Z})^\circ]$ is not a complete intersection ring; if it was, in fact, it would be enough to consider everything modulo 2 to prove that also $\mathbb{F}_2[(\mathbb{Z}/4\mathbb{Z})^\circ]$ is complete intersection.

4 Units in group rings

In this last chapter we want to study units in a group ring $\mathbb{Z}[A]$, where A is a finite abelian group.

First we will describe the structure of the group of units of $\mathbb{Z}[A]$ as an abelian group, identifying its torsion part and computing the rank of the torsion free one. A big goal would be to find a basis for the torsion free part. As it is in cyclotomic fields, this turns out to be really hard and so what one does is try to give a basis of a subgroup of full rank, possibly with a small index in the full group: as in cyclotomic fields there are cyclotomic units, we will deal with constructible units.

Continuing in the parallel between cyclotomic fields and group rings, as cyclotomic units have a structure of $(\mathbb{Z}/n\mathbb{Z})^\times$-module, passing to group rings we get more structure, since we get an action on constructible units of the full monoid $(\mathbb{Z}/n\mathbb{Z})^\circ$ that gives them a cyclic module structure if A is cyclic and H is cyclic, where H is the quotient of the group of automorphisms of A by the involution $\star : x \to x^{-1}$.

Inside a group ring, we can define a more natural generalization of cyclotomic units, considering just units that map to cyclotomic units under every character, obtaining the group of the so-called circular units. The last section of this chapter will deal with the difference between constructible units and circular ones in the case of an abelian p-group, showing the role that the regularity of p plays.

4.1 Units as a $\mathbb{Z}$-module

Definition 4.1. Let A be a finite abelian group. We will denote the group of units of $\mathbb{Z}[A]$ by $U(A)$.

The first thing that we want to do is to describe $U(A)$ as an abelian group, giving its torsion part and the rank of its free part.

Definition 4.2. Consider the ring involution $\star : \mathbb{Z}[A] \to \mathbb{Z}[A]$ which is induced by mapping each element of A to its inverse; a unit $u \in U(A)$ will be called *symmetric* if it is stable under this involution, *anti-symmetric* if $u^\star = u^{-1}$. The subgroups of symmetric and anti-symmetric units will be labeled by $U^+(A)$ and $U^-(A)$, respectively.

At this point we need to remind that, according to Maschke theorem, a group ring over a field is semisimple if and only if the characteristic of the field does not divide the order of the group. Therefore a finite roup ring over $\mathbb{Q}$ or $\mathbb{C}$ is always semisimple.

Moreover, by the Artin-Wedderburn theorem, a semisimple ring is isomorphic to a product of n_i by n_i matrix rings over division rings D_i, for some integers n_i, where both n_i and D_i are uniquely determined up to permutation of the index i. We will call the factors of the product Wedderburn components.

Lemma 4.3. *The torsion subgroup of $U(A)$ is $U^-(A)$, that is also equal to $\langle -1 \rangle \times A$.*

Proof The torsion subgroup of $U(A)$ is contained in $U^-(A)$, because in each Wedderburn component of $\mathbb{Q}[A]$, the elements of finite multiplicative order must satisfy the condition $|w| = w\overline{w} = 1$.

On the other hand we have that $U^-(A) = \ker[v \to vv^\star] \subseteq \langle -1 \rangle \times A$; indeed, if $v = \sum_{z \in A} a_z z \in \mathbb{Z}[A]$, the coefficient of identity in $vv^\star$ is $\sum_z a_z^2 \neq 1$, unless v is equal to z or $-z$ for some $z \in A$.

Since it is clear that $\langle -1 \rangle \times A$ is contained in the torsion part of $U(A)$, all the inclusion must be equalities and therefore the lemma is proved.

Now we can decompose $U(A)$ into its torsion subgroup $U^-(A)$ and a free $\mathbb{Z}$-module.

Definition 4.4. Let $\Delta(A)$ be the augmentation ideal, that is the kernel of the augmentation map $\mathbb{Z}[A] \to \mathbb{Z}$ that sends every element of A to 1. Define $U_i(A) = U(A) \cap (1 + \Delta(A)^i)$, for $i = 1, 2$, the set of units of A that are congruent to 1 modulo the i-th power of the augmentation ideal.

Lemma 4.5. *1. $U(A) = \langle -1 \rangle \times U_1(A)$.*

2. The map

$$e_A : \sum_{z \in A} c_z z \mapsto \prod_{z \in A} z^{c_z}$$

from the additive group of $\mathbb{Z}[A]$ to the multiplicative group $A \subset U_1(A)$, is multiplicative on $U_1(A)$ and yields a split exact sequence

$$1 \to U_2(A) \to U_1(A) \stackrel{e_A}{\to} A \to 1.$$

3. Moreover $U_2(A) \subseteq U^+(A)$.

Proof

1. Trivial, since every unit has augmentation 1 or -1.

2. First we claim that e_A satisfies the congruence $e_A(\delta) \equiv 1 + \delta \bmod \Delta(A)^2$, for $\delta \in \Delta(A)$. It is enough to prove it for $\delta = z - 1$, since if δ contains more terms, we can split it in pairs of them and note that

$$\begin{aligned} e_A(x + y - v - z) &= e_A(x - v)e_A(y - z) \\ &\equiv (1 + x - v)(1 + y - z) \bmod \Delta(A)^2 \\ &\equiv 1 + x + y - v - z \bmod \Delta(A)^2 \end{aligned}$$

We have now that $e_A(z - 1) = z = 1 + (z - 1)$ and therefore the claim is true.

In particular we can deduce that $e_A(\delta) = 1 \iff \delta \in \Delta(A)^2$; the implication from left to right comes directly from the above, the other one from the observation that in the expansion of an element of $\Delta(A)^2$ each term of A appear as many times with sign + and -. This tells us that our sequence is exact.

The multiplicativity of e_A on $U_1(A)$ is established by the fact that $(1 + \delta_1)(1 + \delta_2) = (1 + \delta_1 + \delta_2 + \delta_1\delta_2)$ is mapped to $e_A(\delta_1 + \delta_2) = e_A(\delta_1)e_A(\delta_2)$.

Eventually, the sequence is split since the identity on A is a right inverse of e_A.

3. Note first that $u \in U(A) \Rightarrow v = \frac{u}{u^\star} \in U_1^-(A) = A$ by lemma 4.3. If $u \in U_2(A)$, also $v \in U_2(A)$; since, by point 2, $A \cap U_2(A) = \{1\}$, we have $v = 1 \Rightarrow u = u^\star$.

We can conclude the description of the units of an integral group ring of a finite abelian group A by saying that

$$U(A) = \langle -1 \rangle \times A \times U_2(A),$$

$$U_1(A) = A \times U_2(A),$$

$$U_1^+(A) = A_2 \times U_2(A),$$

where A_2 is the subgroup of A generated by the elements of order 2. This tells us that $U_1^+(A) = U_2(A)$ for every group A of odd order.

Remark 4.6. Given a commutative group G, one has a short exact sequence

$$1 \to G_{tor} \to G \to G/G_{tor} \to 1$$

where G_{tor} denotes the torsion part of G.

The previous lemma says is that if we consider $G = U(A)$ or $U_1(A)$, this exact sequence splits.

Therefore, unlike, for example, in cyclotomic units, to consider the torsion part we just need to restrict to the component $U_2(A)$.

Now we restrict to a cyclic group C. This is a reasonable thing to do mainly because of two reasons:

1. if A is a finite abelian group and we denote by $\dot{U}(A)$ the group of units of $\mathbb{Z}[A]$ modulo torsion, we have that the natural homomorphism

$$\dot{\alpha} : \prod_C \dot{U}(C) \to \dot{U}(A)$$

where the product is direct and C runs over all cyclic subgroups $\neq 1$ of A, is of finite index [2] and, if A is an elementary abelian p-group, for a regular prime p, then $\dot{\alpha}$ is an isomorphism [21].

2. Let $C = C_n = \langle x \rangle$ be the cyclic group of order n. We have

$$\mathbb{Q}[C] = \prod_{d|n} \mathbb{Q}(\zeta^d),$$

where $\zeta = \zeta_n$ is a primitive complex n-th root of unity. Under the above identification, we have the embedding

$$\mathbb{Z}[C] \subset \prod_{d|n} \mathbb{Z}[\zeta^d] = \mathcal{M}_C,$$

where $\mathcal{M}_C$ is the maximal order of the product of number fields $\mathbb{Q}[C]$.

In this way we establish a relation between our cyclic group ring and cyclotomic fields; therefore we can both make use of the theory for the latter and try to deduce something about them starting from the analysis of cyclic group rings.

Remark 4.7. The previous embedding of $\mathbb{Z}[C]$ into $\mathcal{M}_C$ allows us to compute the rank of $U(C)$, that is the r such that $\dot{U}(C) \cong \mathbb{Z}^r$. In fact, denoting by $\mathcal{M}_C^\times$ the group of invertible elements in $\mathcal{M}_C$, by theorem 8.3 in [26] we have

$$rk\, U(C) = rk\, \mathcal{M}_C^\times = \sum_{2<d|n} \left(\frac{\varphi(d)}{2} - 1 \right).$$

4.2 Constructible units

At this point we want to construct a subgroup of the full unit group that consists of units given by an explicit formula. To do this let us start fixing a cyclic group C of order n; we have $\mathbb{Z}[C] \cong \mathbb{Z}[x]/(x^n - 1)$ and we will call $G = \mathrm{Aut}(C) = (\mathbb{Z}/n\mathbb{Z})^\times$ the group of automorphisms of C.

Let ξ be the image of x in the quotient ring $\mathbb{Z}[\xi] = \mathbb{Z}[x]/(1+x+...+x^{n-1})$. We can observe that ξ is not simply a primitive n-th root of 1, but it can specialize to a d-th root for any $1 \neq d|n$. In fact $\mathbb{Q}[\xi]$ is the direct sum of $\mathbb{Q}[\zeta_d]$, for all $1 \neq d|n$ and ζ_d denoting a primitive d-th root of 1; this means that $\mathbb{Q}[\xi]$ is essentially $\mathbb{Q}[C]$ without the component corresponding to the trivial character.

Note that we have a fiber product

$$\begin{array}{ccc} \mathbb{Z}[C] & \longrightarrow & \mathbb{Z} \\ \downarrow & & \downarrow \\ \mathbb{Z}[\xi] & \xrightarrow{\varepsilon} & \mathbb{Z}/n\mathbb{Z} \end{array}$$

where ε maps ξ to 1 and all the other maps are the natural ones. This is a pull-back diagram since, given $a \in \mathbb{Z}$ and $\sum_i a_i \xi^i \in \mathbb{Z}[\xi]$ such that $\sum_i a_i = a + kn$, we can construct the unique ancestral element $\sum_i a_i x^i - k(1+x+...+x^{n-1}) \in \mathbb{Z}[C]$.

For any x generator of C, whereas $x - 1$ is a zero divisor in $\mathbb{Q}[C]$, its image $\xi - 1$ is a unit in $\mathbb{Q}[\xi]$. Hence it makes sense to write $(\xi - 1)^{\sigma-1}$ for any $\sigma \in G$, and more generally $(\xi - 1)^\delta$ for any $\delta \in \Delta(G)$. Since

$$(\xi - 1)^{\sigma-1} = \frac{\xi^c - 1}{\xi - 1} = 1 + \xi + ... + \xi^{c-1},$$

where $c > 0$ is prime to n and $\sigma : x \mapsto x^c$, these elements actually lie in $\mathbb{Z}[\xi]$. Moreover they are units, because $(\xi - 1)^{1-\sigma} = (\xi^\sigma - 1)^{\tau-1}$ with $\tau = \sigma^{-1}$.

In this way we obtain a natural G-homomorphism

$$\begin{array}{rccc} u: & \Delta(G) & \to & U(\xi) \\ & \delta & \mapsto & (\xi - 1)^\delta, \end{array}$$

where $U(\xi)$ denotes the unit group of $\mathbb{Z}[\xi]$.

Lemma 4.8. *The G-map u yields a morphism of short exact sequences*

$$\begin{array}{ccccccccc} 1 & \longrightarrow & \Delta(G)^2 & \longrightarrow & \Delta(G) & \xrightarrow{e_G} & G & \longrightarrow & 1 \\ & & \downarrow & & \downarrow u & & \downarrow & & \\ 1 & \longrightarrow & U_1(C) & \longrightarrow & U(\xi) & \xrightarrow{\varepsilon} & (\mathbb{Z}/n\mathbb{Z})^\times & \longrightarrow & 1 \end{array}$$

where the third vertical line is the identity of $G = (\mathbb{Z}/n\mathbb{Z})^\times$.

Proof During the proof of the second point of lemma 4.5 we saw that $\Delta(G)^2$ equals the kernel of the surjection $\Delta(G) \to G$. By the pull-back property of the previous diagram, an element of $U_1(C)$ is uniquely determined by the pair $1 \in \mathbb{Z}$ and $v = \sum_i a_i \xi^i \in \mathbb{Z}[\xi]$ such that $\sum_i a_i \equiv 1 \bmod n$, that is $v \in ker(\varepsilon)$. This proves exactness.

The commutativity of the left hand square is clear. For the right hand square it is enough to check on a typical generator $\delta = \sigma - 1 \in \Delta(G)$: if $x^\sigma = x^c$ with $c > 0$, we have $u(\delta) = 1 + \xi + ... + \xi^{c-1}$; this goes to $c \in (\mathbb{Z}/n\mathbb{Z})^\times$ under ε, which is the same as $e(\sigma - 1) = \sigma \in G$.

What we are interested in is the image of the restricted map $u : \Delta(G)^2 \to U_1(C)$. However, to avoid torsion, we shall still have to compose it with the canonical projection $e' : U_1(C) \to U_2(C)$ coming from the splitting $U_1(C) = C \times U_2(C)$ given by lemma 4.5.

Before proving the next theorem we need the following lemma; it contains a lot of analytic number theory that we will just use without any further explanation.

Lemma 4.9. *The map* $u : (1 + \star)\Delta(G) \to U(\xi)$ *is injective.*

Proof Let $\delta = \sum_\sigma a_\sigma \sigma \in \Delta(G)$ be such that $a_\sigma = a_{\star\sigma}$ for all $\sigma \in G$. We need to prove that $u(\delta) = 1$ implies $\delta = 0$

For any system $\{b_\tau \mid \tau \in G\}$ of complex numbers, and any character $\chi : G \to \mathbb{C}^\times$ we have

$$\sum_\sigma a_\sigma \chi(\sigma) \sum_\tau b_\tau \chi(\tau^{-1}) = \sum_\rho \chi(\rho^{-1}) \sum_\sigma a_\sigma b_{\rho\sigma}$$

with ρ, σ and τ ranging over G. Put $b_\sigma = \log|\zeta^\sigma - 1|$, where $\zeta \neq 1$ is an n-th root of 1 yet to be chosen. Then $u(\delta) = 1$ implies $\prod_\sigma (\zeta^{\rho\sigma} - 1)^{a_\sigma} = (\xi - 1)^\delta = 1$ where we specialize ξ to be ζ^ρ. Hence, applying logarithm, the right hand side of the previous identity is zero for any choice of ζ.

If $\delta \neq 0$, however, there must be a $\chi \neq 1$ such that $\sum_\sigma a_\sigma \chi(\sigma) \neq 0$ and $\chi(\star) = 1$. But by choosing ζ so as to be primitive with respect to the conductor f_χ, we also get $\sum_\tau \chi(\tau^{-1}) \log|\zeta^\tau - 1| \neq 0$. Indeed this expression equals $-f_\chi L(1, \chi)/\tau(\chi)$, involving L-functions and Gauss sums in the usual notation of analytic number theory (cf. book [26], theorem 4.9).

Theorem 4.10. *The composite map*

$$\Delta(G)^2 \xrightarrow{u} U_1(C) \xrightarrow{e'} U_2(C)$$

induces an injection $w : \Delta(H)^2 \to U_2(C)$, *where* $H = G/\langle\star\rangle$.

Proof To prove that $e' \circ u$ factors over the canonical map $h : \Delta(G)^2 \to \Delta(H)^2$ induced by taking G modulo $\langle\star\rangle$, we must show that u maps $\ker(h) = (\star - 1)\Delta(G)$ into $\ker(e') = C$. This follows from the trivial calculation

$$(\xi - 1)^{\star - 1} = \frac{\xi^{-1} - 1}{\xi - 1} = -\xi^{-1}$$

by which u maps $(\star - 1)$ to a torsion element.

Injectivity of w follows from lemma 4.9, which grants this property to the restriction of u to the H-module $\Delta_\star(G) = (\star + 1)\Delta(G) \subset \Delta(G)$, consisting of all $\delta \in \Delta(G)$ such that $\delta = \star\delta$.

The canonical homomorphism h clearly bijects $\Delta_\star(G)$ onto $2\Delta(H) \subset \Delta(H)$.

If an element $\alpha \in \Delta(H)^2$ lies in the kernel of w, then so does 2α, which corresponds to $h(\delta)$ for suitable $\delta \in \Delta_\star(G)$. Since $w \circ h = e' \circ u$, it follows that $e'(u(\delta)) = 1$ and therefore $u(\delta) \in \ker(e') = C$. This implies $n\delta = 0$ because u is injective on $\Delta_\star(G)$, whence $\delta = 0$ and finally $2\alpha = h(\delta) = 0$. So $\alpha = 0$, proving that w is injective, as claimed.

As next step, we want to give explicit formulas for u and w in terms of the sums $s_i(t) = 1 + t + ... + t^{i-1}$ defined for any $i > 0$. Without risk of confusion, we use the same notation for elements in G and their counterparts in H.

Proposition 4.11. *For every $\sigma, \tau \in G$, let $\alpha = (\sigma - 1)(\tau - 1)$ be a typical generator of $\Delta(G)^2$ with $\sigma : x \to x^c$, and let b, k be positive integers with $bc = 1 + kn$. Then*

$$u(\alpha)(x) = s_b(x^\sigma)s_c(x^\tau) - ks_n(x)$$

and

$$w(\alpha)(x) = x^{-(\tau-1)(c-1)/2}u(\alpha)(x).$$

Proof As given above, $u(\alpha)(x)$ satisfies $u(\alpha)(1) = 1$ and $u(\alpha)(\xi) = (\xi - 1)^\alpha$, since $\alpha = (\sigma^{-1} - 1)\sigma + (\sigma - 1)\tau$. To project this into the torsion free component $U_2(C)$, we must divide it by $e_C(u(\alpha)(x))$. Applying e_C to $s_c(x^\tau)s_b(x^\sigma) = \sum_{i,j} x^{j\tau + i\sigma}$ we get $\prod_{i,j} x^{j\tau+i\sigma}$, with $0 \le i < b$ and $0 \le j < c$, which yields x raised to the power $\tau bc(c-1)/2 + \sigma bc(b-1)/2$. The element $x^{(c-1)/2}$ is always well-defined, since, if c is odd, there is no problem dividing the even number $c - 1$ by 2, and if c is even, n must be odd, and therefore we can take the square root of any element of C. Therefore the exponent of x amounts to $\tau(c-1)/2 + \sigma(b-1)/2$, because $bc = 1 + kn$ can be dropped.

To complete our computation we have to take into account the term $-ks_n(x)$; we get

$$e_C(-ks_n(x)) = x^{-k\frac{n(n-1)}{2}}.$$

Considering that using H we can identify $n-1$ and 1 and remembering that $bc - kn = 1$, we get the desired result.

Remark 4.12. All this could be simplified in case $\sharp C$ is odd. Then $x^{1/2}$ makes sense, and we could replace u by the map $v : \Delta(G) \to U^+(\xi)$ which takes $\delta \in \Delta(G)$ directly into the $\star$-symmetric unit $(\xi^{1/2} - \xi^{-1/2})^\delta$. As in the lemma 4.8, we would get a morphism of short exact sequences

$$\begin{array}{ccccccccc} 1 & \longrightarrow & \Delta(G)^2 & \longrightarrow & \Delta(G) & \xrightarrow{e_G} & G & \longrightarrow & 1 \\ & & \downarrow{\scriptstyle w} & & \downarrow{\scriptstyle v} & & \downarrow & & \\ 1 & \longrightarrow & U_1^+(C) & \longrightarrow & U^+(\xi) & \xrightarrow{\varepsilon} & (\mathbb{Z}/n\mathbb{Z})^\times & \longrightarrow & 1 \end{array}$$

by the same reasoning, because $\varepsilon \circ v = \varepsilon \circ u$. For every $\delta \in \Delta(G)$ we would have $v(\delta)(\xi) = \xi^{-\delta/2} u(\delta)(\xi)$ by definition, and w would be obtainable from v by simple restriction to $\Delta(G)^2$. There would be no need to mention the projection $e' : U_1(C) \to U_2(C)$, which would be identity on U_1^+ anyway.

For $\alpha = (\sigma - 1)(\tau - 1) \in \Delta(G)^2$, and b, c, k as in proposition 4.11, we would have the simpler formula

$$w(\alpha)(x) = v_b(x^\sigma) v_c(x^\tau) - ks_n(x) \quad \text{with} \quad v_c(x) = x^{\frac{1-c}{2}} s_c(x).$$

This fails for even n because $(c-1)/2$ is known only modulo $n/2$ if c is given modulo n.

Definition 4.13. The image $W(C) := w(\Delta(H)^2)$ will be referred to as the group of *well formed units* belonging to C.

For any finite abelian group A, let $Y(A)$ denote the product $\prod_C W(C) \subseteq U_2(A)$, with $C \subseteq A$ ranging over all cyclic subgroups of order > 2; it will be called the group of *constructible units* of A.

Now we want to prove that the product of the $W(C)$ is direct and that has finite index in $U_2(A)$. Before doing that we need to prove the following lemma.

Lemma 4.14. *Let A a finite abelian group. We denote by $U_1(\mathcal{M}_A)$ the units of augmentation 1 of the maximal order $\mathcal{M}_A$ of the ring $\mathbb{Q}[A]$. Then there is an injection of the direct sum*

$$\bigoplus_{C \subseteq A} \Delta_\star(G_C) \to U_1(\mathcal{M}_A),$$

where $C \subseteq A$ runs over all nontrivial cyclic subgroups, and the components $\Delta_\star(G_C) \to U_1(\mathcal{M}_C) \subseteq U_1(\mathcal{M}_A)$ are defined sending δ to $(\psi(x)-1)^\delta$, with $\psi : C \to \mathbb{C}^\times$ running over the nontrivial characters of C.

Proof For every C of order > 2, the rank of $\Delta_\star(G_C)$ is $\frac{1}{2}\sharp G_C - 1$, which equals the free rank of the units in the ring of the $\sharp C$-th roots of unity. By Dirichlet's unit theorem, the left hand term has the same rank as the right hand term taken modulo torsion. Hence the lemma is equivalent to saying that the map in the statement has an image of finite index.

By a theorem of Bass and Milnor [2] the product of the inclusions $U_1(C) \to U_1(A)$, as $C \subseteq A$ runs over all cyclic subgroups, does have finite index. Hence so does the corresponding product of inclusions $U_1(\mathcal{M}_C) \to U_1(\mathcal{M}_A)$. Combining this with Bass's independence theorem [2], that proves the case $A = C$ of this lemma, yields the stated result.

Theorem 4.15. *For any finite abelian group A, the product*

$$Y(A) = \prod_{C \subseteq A} W(C)$$

is direct and has finite index in $U_2(A)$.

Any homomorphism $A \to A'$ of abelian groups maps $Y(A)$ into $Y(A')$ by surjecting each $W(C)$ onto $W(C')$, where C' denotes the image of C.

Proof The explicit formula shows that $w(\alpha)(x)^2 = w(\alpha)(x)w(\alpha)(x^{-1}) = u(\alpha)(x)u(\alpha)(x^{-1}) = u(\alpha + \star\alpha)(x)$. Therefore the square of any constructible unit $y = \prod_C w_C$ is in the image of the injection shown in the previous lemma, and $y = 1$ implies $w_C = 1$ for all C.

The finiteness of the index follows by the same rank computation as was used in the proof of the previous lemma.

For the second statement, let $x' \in C'$ be the image of the generator x of C. Every automorphism $\sigma : x \mapsto x^c$ of C induces an automorphism $\sigma' : x' \mapsto (x')^c$ of C', and in that sense every $\alpha \in \Delta(H)^2$ produces an $\alpha' \in \Delta(H')^2$. Since the correspondence $\alpha \mapsto \alpha'$ is surjective, and since every $w(\alpha)(x)$ maps to $w(\alpha')(x')$, the surjectivity $W(C) \to W(C')$ follows.

We can say more about the group $Y(A)$, if H happens to be cyclic. This is the case, for example, if $\sharp C = p^\nu$ or $\sharp C = 2p^\nu$. The following proposition comes from the fact that the ideals $\Delta(H)$ and $\Delta(H)^2$ are principal if H is cyclic; in fact, if h is a generator of H then $\Delta(H) = (h^i - 1 \mid i = 1, ..., \sharp H) = (h-1)$ and $\Delta(H)^2 = ((h^i-1)(h^j-1) \mid 1 \le i, j \le \sharp H) = ((h-1)^2)$.

Proposition 4.16. *Suppose that H is cyclic and let α be a generator of the ideal $\Delta(H)^2$. Then $Y(A)$ is generated over $\mathbb{Z}$ by the H-set $\{w(\alpha)(z) \mid z \in A\}$, which can be reduced to a $\mathbb{Z}$-basis of $Y(A)$ by omitting one element from each of its H-orbits.*

Proof If h is a generator of H, multiplication by $h-1$ induces isomorphisms

$$\mathbb{Z}[H]/\Sigma(H) \xrightarrow{\sim} \Delta(H) \quad \text{and} \quad \Delta(H) \xrightarrow{\sim} \Delta(H)^2,$$

where $\Sigma(H)$ denotes the ideal generated by the sum over all the elements of H. Mapping 1 to $w(\alpha)(x)$, we therefore have an H-isomorphism of $\mathbb{Z}[H]/\Sigma(H)$ with $W(C)$ by theorem 4.10. Hence the product over the H-orbit $\{w(\alpha)(z) \mid \langle z\rangle = C\}$ is trivial, and a basis of $W(C)$ is obtained from this orbit by throwing out any one of its elements.

By theorem 4.15, the corresponding element $w(\alpha)(z)$ can similarly serve to generate $W(C)$, where $C = \langle z\rangle$ for any $z \in A$. Since every $z \in A$ occurs exactly once as a generator of one of the cyclic subgroups $C \subseteq A$, we thus obtain each of the components of the direct product $Y(A) = \prod_C W(C)$.

Example 4.17. Let C be the cyclic group of order 9; then $G = \{\overline{1}, \overline{2}, \overline{4}, \overline{5}, \overline{7}, \overline{8}\}$ is the cyclic group of order 6, generated by $\overline{2}$ and $H = \{\overline{1}, \overline{2}, \overline{4}\}$ is the cyclic group of order 3. The element $\overline{2}$ is a generator of H and therefore $\Delta(H)^2 = (\overline{2} - \overline{1})^2$.

Let $\alpha = (\overline{2} - \overline{1})^2$. Now we can compute $w(\alpha)(x)$ with the formula given in remark 4.12. We set $\sigma = \tau = \overline{2}$, $c = 2$, $b = 5$ and $k = 1$. We get

$$\begin{aligned} w = w(\alpha)(x) &= v_5(x^2)v_2(x^2) - s_9(x) \\ &= x^{-4}(1 + x^2 + x^4 + x^6 + x^8)x^{-1}(1 + x^2) - (1 + x + ... + x^8) \\ &= -1 + x - x^2 + x^3 + x^6 - x^7 + x^8 \\ &= x^{-3} - x^{-2} + x^{-1} - 1 + x - x^2 + x^3 \end{aligned}$$

Then we know, by the proof of the previous proposition, that $\mathbb{Z}[H]/\Sigma(H) \cong W(C)$, mapping 1 to $w(\alpha)(x)$. Therefore

$$W(C) = \frac{w^{\mathbb{Z}} \cdot w^{\overline{2}\mathbb{Z}} \cdot w^{\overline{4}\mathbb{Z}}}{(w \cdot w^{\overline{2}} \cdot w^{\overline{4}})^{\mathbb{Z}}}$$

Moreover we notice that $w(\alpha)(x^3) = 1$ and this, according to the previous proposition, tells us that $W(C^3) = 1$ and therefore

$$Y(C) = W(C) \times W(C^3) = W(C).$$

The element $w \cdot w^{\overline{2}} \cdot w^{\overline{4}}$ that we needed to quotient out to obtain $W(C)$ above, is just the norm of w; in fact we obtain it taking the product of the conjugate elements of w.

As it is clear from previous proposition, we are sure that this condition is the only one that we need for $W(C)$, since we have to omit only one element from every H-orbit.

Obviously every element of $Y(A)$ must satisfy a norm condition, which is given by the product of all its conjugates in H. In fact these conditions are the only ones that we need.

Theorem 4.18. *Let C be a cyclic group of order n such that H is cyclic. Then $Y(C)$ is a cyclic submodule of $U(C)$ over the monoid ring $\mathbb{Z}[(\mathbb{Z}/n\mathbb{Z})^\circ]$ and its annihilator is given just by the norm conditions.*

Proof By the previous proposition we know that $Y(C)$ is generated over $\mathbb{Z}$ by the set $\{w(\alpha)(x^i) \mid 1 \leq i < n\}$, where x is a generator of C and α is a generator of $\Delta(H)$; this set is equal to $w(\alpha)(x)^{(\mathbb{Z}/n\mathbb{Z})^\circ}$ since every element x^i of the group is in $x^{(\mathbb{Z}/n\mathbb{Z})^\circ}$. This means that $Y(C)$ is a cyclic monoid over the ring $\mathbb{Z}[(\mathbb{Z}/n\mathbb{Z})^\circ]$ generated by the element $w(\alpha)(x)$.

Moreover we know that $Y(C) = \prod_{C'} W(C')$, where C' runs over the cyclic subgroups of C. Since C is cyclic, then every C' is generated by a power of x, and we can obtain all cyclic subgroups considering the elements x^d, where d runs over all the divisors of n.

From the proof of the previous proposition we see also that $W(C) \cong \mathbb{Z}[H]/\Sigma(H)$. This implies that

$$Y(C) \cong \frac{\mathbb{Z}[\frac{(\mathbb{Z}/n\mathbb{Z})^\circ}{\langle\star\rangle}]}{(\frac{\overline{d}(\Sigma(H))}{k_d} \mid d|n)}$$

where $k_d = \varphi(n)/\varphi(n/d)$. This is true since by acting with the $\overline{d}$'s we reach all the others components $W(C')$; for the norm conditions, $\Sigma(H)$ is obviously the one of the component $W(C)$. For another component C', the norm condition is given by the sum over all the elements of $(\mathbb{Z}/n\mathbb{Z})^\circ/\langle\star\rangle$ corresponding to the elements of C'; realizing that there is a surjection from G to $G' = \mathrm{Aut}(C')$, where C' is generated by x^d, such that all the fibers have the same cardinality k_d, we can conclude that the norm condition for C' is $\overline{d}(\Sigma(H))/k_d$.

Since we will need it later, we want to explicit the relation between $W(C)$ and $W(C^p)$ in the case C is a cyclic p-group.

Corollary 4.19. *If C is a cyclic group of order p^ν, then $W(C^p) = W(C)^\pi$, where π is the endomorphism of C that sends x to x^p.*

Proof It is enough to notice that, if C is generated by x, C^p is generated by x^p, that is reached by the morphism $\pi : x \mapsto x^p$.

Example 4.20. Let C be the cyclic group of order 15. Then $G = \mathrm{Aut}(C) = \{\overline{1}, \overline{2}, \overline{4}, \overline{7}, \overline{8}, \overline{11}, \overline{13}, \overline{14}\} \cong C_4 \times C_2$ and $H = \{\overline{1}, \overline{2}, \overline{4}, \overline{7}\} \cong C_4$, generated by $\overline{2}$.

We can compute $w(\alpha)(x)$ according to the formula on remark 4.12. We can choose $\sigma = \tau = \overline{2}$, $c = 2$, $b = 8$ and $k = 1$.

$$\begin{aligned} w = w(\alpha)(x) &= v_8(x^2)v_2(x^2) - s_{15}(x) \\ &= x^8(1 + x^2 + x^4 + x^6 + x^8 + x^{10} + x^{12} + x^{14})x^{-1}(1 + x^2) + \\ &\quad -(1 + x + ... + x^{14}) \\ &= x^{-6} - x^{-5} + x^{-4} - x^{-3} + x^{-2} - x^{-1} + 1 - x + x^2 - x^3 + \\ &\quad +x^4 - x^5 + x^6 \end{aligned}$$

Mapping 1 to w we obtain an isomorphism of $W(C)$ with $\mathbb{Z}[H]/\Sigma(H)$. Thanks to our last theorem we can give to $Y(C)$ a cyclic module structure over the ring $\mathbb{Z}[(\mathbb{Z}/15\mathbb{Z})^\circ]$ as follows

$$\begin{aligned} Y(C) &\cong \frac{\mathbb{Z}[\frac{(\mathbb{Z}/15\mathbb{Z})^\circ}{\langle\star\rangle}]}{(\overline{0}, \Sigma(H), \frac{\Sigma(H)^{\overline{3}}}{2}, \frac{\Sigma(H)^{\overline{5}}}{4})} \\ &\cong \frac{\overline{0}\mathbb{Z} + \overline{1}\mathbb{Z} + \overline{2}\mathbb{Z} + \overline{3}\mathbb{Z} + \overline{4}\mathbb{Z} + \overline{5}\mathbb{Z} + \overline{6}\mathbb{Z} + \overline{7}\mathbb{Z}}{(\overline{0}, \overline{1} + \overline{2} + \overline{4} + \overline{7}, \overline{3} + \overline{6}, \overline{5})} \end{aligned}$$

It is just a matter of computation to verify that w is annihilated by $(\overline{0}, \overline{1} + \overline{2} + \overline{4} + \overline{7}, \overline{3} + \overline{6}, \overline{5})$

4.3 Constructible and circular units

In this section we restrict to abelian p-groups, since in this setting we can go on with our analysis and say much more about units in groups rings. What we want to do is to define a more natural generalization of cyclotomic units in a group ring, looking at the units that map to cyclotomic units under every character, and try to understand what is the difference between this group and the one made by constructible units.

It will turn out that the index between the two groups is always a power of p and in a lot of cases the two groups are equal; we will see that this equality depends on the regularity of the prime p.

What we present here is a summary of what is available in the papers by Hoechsmann [10], [19], [14]. We will use a lot of references to them and to other papers because we want to present the result without proving every single detail.

Let us start with a lemma.

Lemma 4.21. *Let C a cyclic group such that $\sharp C = n = p^\nu > 2$ be a prime power, and ζ denote a primitive n-th root of unity. Consider the maps $\varphi : \xi \mapsto \zeta$ and $\psi : x \mapsto \zeta$ of $U(\xi)$ and $U(C)$, respectively, into $\mathbb{Z}[\zeta]^\times$. Then*

1. *φ yields an injection of the group $\langle\xi\rangle(1-\xi)^{\Delta(G)}$ into $\mathbb{Z}[\zeta]^\times$;*
2. *for $\delta \in \Delta(G)$, we have $(1-\zeta)^\delta \in \psi(U_1(C)) \iff \delta \in \Delta(G)^2$.*

Proof For each $\mu = 1, ..., \nu$ let $\psi_\mu : C \to \mathbb{C}^\times$ be the $p^{\nu-\mu}$-th power of ψ, and F_μ be the ψ_μ-image of $\mathbb{Q}[C]$. It is well-known that $\psi_\mu(x)$ and $1-\psi_\mu(x)$ are the F_ν/F_μ-norms of ζ and $1-\zeta$, respectively [19]. Hence all Wedderburn components of any element of the form $\xi^a(1-\xi)^\delta$ are determined by its ψ-image $\zeta^a(1-\zeta)^\delta$. This is enough for the first point.

For the second one, suppose that we have $(1-\zeta)^\delta \in \psi(U_1(C))$. By the first point, it has in $U(\xi)$ exactly one pre-image, namely $(1-\xi)^\delta$, which must therefore be liftable to an element of $U_1(C)$. This does not mean that we know δ itself, but it does mean that $\varepsilon((1-\xi)^\delta) = 1$, by lemma 4.8. Hence it follows that $e_G(\delta) = 1$ and therefore $\delta \in \Delta(G)^2$. The other implication is also clear from the diagram of lemma 4.8.

Definition 4.22. For any $n > 2$, and any n-th root of unity $\zeta \neq 1$, the cyclotomic units of $\mathbb{Q}(\zeta)^+$ are

$$U^\oplus(\zeta) = \langle\zeta\rangle(1-\zeta)^{\Delta(G)} \cap \mathbb{R}^\times.$$

These are the only elements of $\mathbb{Z}[\zeta]$ which have a hope of turning up as Wedderburn components of constructible units.

If A is abelian of exponent n, i.e. $A^n = \{1\}$, we write $U^\oplus(A)$ for the group of all the units in $U(A)$ which are mapped into the appropriate $U^\oplus(\zeta)$ by every character $\mathbb{Z}[A] \to \mathbb{Z}[\zeta]$. Such units are called *circular*.

It is just a remark to note that all constructible units are automatically circular, i.e. $Y(A) \subseteq U^\oplus(A)$.

Now we want to explain the special role played by $W(C)$, which turns out to be, modulo the subgroup $C_2 \subset C$ generated by elements of order 2, the maximal subgroup of $U_1(C)$ that injects in $U^\oplus(\zeta)$. First a useful lemma:

Lemma 4.23. *If $n = \sharp C = p^\nu$, with $\nu \geq 2$, let $s_1 = 1 + \tau_1 + ... + \tau_1^{p-1} \in \mathbb{Z}[G]$ with $\tau_1 : x \mapsto x^{1+n/p}$. Then $w(\zeta_n^p) = w(\zeta_n)^{s_1}$ for any $w(x) \in C_2 \cdot W(C)$.*

Proof It is well-known that $(\zeta_n - 1)^{s_1} = (\zeta_n^p - 1)$ and that $\zeta_n^{s_1} = \pm\zeta_n^p$, with the minus sign occurring only for $p = 2$ [19]. It follows that $v(\zeta_n)^{s_1} = v(\zeta_n^p)$ for any $v(\zeta_n) = \zeta_n^a(\zeta_n - 1)^\beta$, with $a \in \mathbb{Z}$ and $\beta \in \Delta(G)$, as long as a is even

when $p = 2$. For $\beta = (\sigma - 1)(\tau - 1) \in \Delta(G)^2$, it turns out that $v(\zeta_n)$ is real if and only if $2a \equiv (1 - c)(1 - d) \bmod n$, where $\sigma : x \mapsto x^c$ and $\tau : x \mapsto x^d$. If $p = 2$, this makes $2a$ divisible by 4.

Proposition 4.24. *If $n = \sharp C$ is a prime power and ζ is a primitive n-th root of unity, the map $\psi : x \mapsto \zeta$ induces a bijection*

$$C_2 \cdot W(C) \to \psi(U_1(C)) \cap U^{\oplus}(\zeta).$$

Proof For $w(x) \in C_2 \cdot W(C)$ suppose that $w(\zeta_n) = 1$. Then $w(\zeta_n^p) = 1$ as well, either because all of $W(C^p)$ is trivial or because $w(\zeta_n^p) = w(\zeta_n)^{s_1} = 1$ by the previous lemma. By induction, $w(\zeta_d) = 1$ for all $d|n$, whence the injectivity.

For the surjectivity, consider a $t \in U_1(C)$ such that $\psi(t) \in U^{\oplus}(\zeta)$. Then, by the same reasoning as above, all Wedderburn components of t are real, and hence $t \in U_1^+(C)$. The condition $t \in U_1(C)$ implies that $t/x^k \in U_1(C)$ for any integer k; we can choose the value of k such that $\psi(t/x^k) = (1 - \zeta)^{\delta}$. This, by the second point of lemma 4.21, implies that $\delta \in \Delta(G)^2$; therefore $t \in C \cdot u(\Delta(G)^2)$. Eventually $t \in U_1^+(C) \cap C \cdot u(\Delta(G)^2) = C_2 \cdot W(C)$.

According to the last proposition, $W(C)$ is shown to be, in some sense, maximal; to conclude this section we want to prove a theorem which claims a similar kind of maximality for $Y(A)$ is case A is a p-group for odd regular p. To do this we must go through a series of lemmas and intermediate results. We start from cyclic groups C and then we deduce the result for the p-group A.

First we want to improve theorem 4.15 in the case of a cyclic group.

Proposition 4.25. *The index $[U_1^{\oplus}(C) : Y(C)]$ is a power of p.*

Proof By theorem 4.15 know that the map

$$\lambda : \prod_{\nu=0}^{m-1} W(C^{p^\nu}) \to U_1^{\oplus}(C)$$

is an injection with finite cokernel. We just have to refine the proof to show that the index is a p-power.

By proposition 4.24, the surjection $\varphi : U_1^{\oplus}(C) \to \varphi(U_1(C)) \cap U_1^{\oplus}(\zeta)$ splits: $U_1^{\oplus}(C) = C_2 \cdot W(C) \times \ker\varphi$. Let w be a $\mathbb{Z}[G]$-generator of $W(C)$. The proof will be by induction, with nothing to do if $m = 1$.

By lemma 4.23 we have that the kernel of φ contains the elements of the form $w^{\pi^\nu - s_\nu \pi^{\nu-1}}$, for $\nu = 1, ..., m - 1$; therefore we shall be done if we can

prove that the elements $w^{\pi^\nu - s_\nu \pi^{\nu-1}}$, for $\nu = 1, ..., m-1$, generate over $\mathbb{Z}[G]$ a submodule of p-power index in $\ker\varphi$. For this purpose we introduce the map

$$\kappa : W(C) \times W(C)^\pi \times \cdots W(C)^{\pi^{m-2}} \to \ker\varphi,$$

whose components are $(\pi - s_1), ..., (\pi - s_{m-1})$, where $s_\nu = 1 + \tau_\nu + ... + \tau_\nu^{p-1}$, with $\tau_\nu \in G$ of order p^ν.

At this point we need to refer to the fundamental pull-back diagram of ring maps

$$\begin{array}{ccc} \mathbb{Z}[C] & \xrightarrow{\varphi} & \mathbb{Z}[\zeta] \\ \downarrow{\scriptstyle \pi} & & \downarrow \\ \mathbb{Z}[C^p] & \xrightarrow{\rho} & \dfrac{\mathbb{Z}}{p\mathbb{Z}}[C^p] \end{array}$$

where ρ denotes the reduction of the coefficients modulo p [23].

This shows that π induces an isomorphism $\ker\varphi \to \ker\rho$. We can produce a commutative square

$$\begin{array}{ccc} W(C)^\pi \times \cdots \times W(C)^{\pi^{m-2}} & \xrightarrow{\kappa} & \ker\varphi \\ \downarrow{\scriptstyle \pi} & & \downarrow{\scriptstyle \pi} \\ U_1^\oplus(C^p) & \xrightarrow{\pi - p} & \ker\rho \end{array}$$

whose right vertical arrow is an isomorphism, thus shifting the problem to showing the clockwise composite $\pi\kappa$ is of p-power index. The commutativity of the diagram is due to the fact that $s_\nu \pi = p\pi$, for $\nu = 1, ..., m-1$. This allows us to consider the counter-clockwise composite $\pi(\pi - p)$ instead. To prove that $\pi : U_1^\oplus(C) \to U_1^\oplus(C^p)$ and $\pi - p : U_1^\oplus(C) \to \ker\rho$ have p-power index we will also proceed by induction.

Since $W(C^p) = W(C)^\pi$, the induction hypothesis on λ implies that $[U_1^\oplus(C^p) : W(C)^{\pi\mathbb{Z}[M]}]$, where $M = (\mathbb{Z}/p^\nu\mathbb{Z})^\circ$, is a p-power. For the bottom arrow, let $u \in U_1^\oplus(C)$ with $\rho(u) = 1$. By induction assumption, there exists a $v_1 \in U_1^\oplus(C^p)$ such that $u^{\pi p^k} = v_1^{\pi - p}$ for suitable k. Since π has p-power index, there exists a $v \in U_1^\oplus(C)$ such that $v^\pi = v_1^{p^l}$ for suitable l. Hence $u^{p^{k+l}\pi} = v_1^{p^l(\pi-p)} = v^{\pi(\pi-p)}$, and $(u^{p^{k+l}} v^{p-\pi})^\pi = 1$.

Therefore

$$(u^{p^{k+l}} v^{p-\pi})^{p-\pi} = u^{p^{k+l+1}} v^{p(p-\pi)},$$

i.e. a certain p-power of u is in $U_1^\oplus(C)^{\pi-p}$.

Remark 4.26. It is a classical fact ([26], theorem 8.2) that $[U_1^+(\zeta_\mu) : U_1^\oplus(\zeta_\mu)] = h_\mu^+$, the class number of $\mathbb{Q}(\zeta_\mu + \zeta_\mu^{-1})$. Putting $h^+(m) = h_\mu^+ \cdots h_{\mu^m}^+$, it is clear that $U_1^+(C)^{h^+(m)} \subseteq U_1^\oplus(C)$. Hence $[U_1^+(C) : U_1^\oplus(C)]$ is finite and involves only prime divisors occurring in $h^+(m)$. If h_μ^+ is not divisible by p, the prime p is called *semi-regular*. In that case $h^+(m)$ and hence $[U_1^+(C) : U_1^\oplus(C)]$ is also prime to p. Vandiver's conjecture ([26], remark at page 159), says that this would be true for any prime p. So far it has been verified for p less than 12 million.

Definition 4.27. A prime number p is said to be *regular* if it doesn't divide the class number of the full cyclotomic field $\mathbb{Q}(\zeta_p)$, where ζ_p is a p-th primitive root of unity.

For a prime number p to be regular is definitely a restrictive condition; the first irregular primes are 37, 59, 67, 101, 103, 131, 149. It is relatively easy to show that there are infinitely many irregular primes, but the infinitude of regular primes is still just a conjecture.

Proposition 4.28. *If p is a regular prime, $Y(C) = U_1^\oplus(C)$.*

Proof The main reason for this is a generalization of Kummer's lemma [12], which for regular p says that $u \to u^{\pi-p}$ yields an isomorphism

$$U_1^+(C) \xrightarrow{\sim} \ker\rho,$$

the map ρ now referring to the reduction modulo p on all of $U_1^+(C)$. Shifting our attention from $U_1^\oplus(C)$ to $U_1^+(C)$ is not difficult because, by previous remark, for regular primes, the index $[U_1^+(C) : U_1^\oplus(C)]$ is prime to p.

For any $\mathbb{Z}$-module X, let $\hat{X} = X \otimes \mathbb{Z}_p$. Then we have $\hat{U}_1^\oplus(C) = \hat{U}_1^+(C)$. Since $\mathbb{Z}_p$ is flat over $\mathbb{Z}$, the hat functor is exact. Thus it preserves the isomorphism $\hat{U}_1^+(C) \xrightarrow{\sim} \ker\hat{\rho}$, as well as $\ker\hat{\varphi} \xrightarrow{\sim} \ker\hat{\rho}$. We can now read through the proof of proposition 4.25, putting hats on everything and replacing the words 'p-power index' by 'index 1'. This proves that $\hat{\lambda}$ is an isomorphism, hence that the index of λ is prime to p.

Proposition 4.29. *If $m \geq 2$ and $Y(C) = U_1^\oplus(C)$, then p is regular.*

Proof We have the direct decomposition $U_1^\oplus(C) = C_2 \cdot W(C) \times \ker\varphi$ and $Y(C) = W(C) \times \operatorname{im}\kappa$, where κ is defined in the proof of proposition 4.25. Hence $U^\oplus(C)/Y(C)$ is isomorphic to $\ker\varphi/\operatorname{im}\kappa$. A glance at the second diagram in the proof of proposition 4.25 shows that π induces a surjection of $\ker\varphi/\operatorname{im}\kappa$ onto $\ker\rho/U_1^\oplus(C^p)^{\pi-p}$. Hence $Y(C) = U_1^\oplus(C)$ implies $\ker\rho = U_1^\oplus(C^p)^{\pi-p}$.

Now we have both maps into kerρ in the diagram referred above being isomorphisms. Hence the surjectivity of κ implies that of

$$\pi : W(C) \times \cdots \times W(C)^{\pi^{m-2}} \to U_1^{\oplus}(C^p),$$

i.e. $U^{\oplus}(C^p) = Y(C^p)$.

By recursively applying this fact, we may assume that $m = 2$. Then C^p has order p, and the result on kerρ yields an exact sequence

$$1 \to U_1^{\oplus}(C^p)^p \to U_1^{\oplus}(C^p) \xrightarrow{\rho} U_1^{+}(C^p),$$

i.e. the image $\rho(U_1^{\oplus}(C^p))$ has dimension $(p-3)/2$ in the $\mathbb{F}_p$-module $\overline{U}_1^{+}(C^p)$, where the bar denotes the reduction modulo p. This is precisely equivalent to the non-vanishing of the Bernoulli numbers $B_2, B_4, ..., B_{p-3}$ [23], i.e. to the regularity of p ([3], chapter V, §6.3).

Finally we can deal with a general abelian p-group A of exponent $q = p^{\nu}$. Let $\mathcal{M}_A$ be the maximal order in the rational group algebra $\mathbb{Q}[A]$. We recall that $U_1^{\oplus}(A)$ and $U_1^{\oplus}(\mathcal{M}_A)$ are the symmetric units of augmentation 1 of, respectively, $\mathbb{Z}[A]$ and $\mathcal{M}_A$, such that every Wedderburn component appears as a cyclotomic unit. Between them lies the group $U^1(\mathcal{M}_A)$ of those circular units which are congruent to 1 modulo the ideal $\Delta(A)\mathcal{M}_A$; its Wedderburn components $U^1(\zeta_\mu) \subseteq U_1^{\oplus}(\zeta_\mu)$ consist of units which are congruent to 1 modulo the prime ideal above p in $\mathbb{Z}[\zeta_\mu]$.

Now we want to prove that the cokernel of the natural map

$$\alpha_1 : \prod_C U^1(\mathbb{Q}[C]) \to U^1(\mathbb{Q}[A]),$$

as C runs over all cyclic subgroups of A, is a finite p-group. This is true provided that the functor U^1 satisfies the following condition: for every p-subgroup $\Gamma \subset G = \mathrm{Aut}(A)$, the Γ-fixed submodule $U^1(\mathbb{Q}[\zeta])^{\Gamma}$ is the isomorphic image of $U^1(\mathbb{Q}[\zeta^{\sharp\Gamma}])$ under the natural inclusion [15]. We check this in the following lemma.

Lemma 4.30. *Let $\Gamma \subset G$ be a p-group and put $\eta = \zeta^{\sharp\Gamma}$. Then $u \in U^1(\zeta)$ is fixed under Γ if and only if $u \in U^1(\eta)$.*

Proof The prime ideal above p in $\mathbb{Z}[\eta]$ is the Γ-fixed part of the analogous ideal in $\mathbb{Z}[\zeta]$. Hence the lemma is just saying that $U_1^{\oplus}(\eta) = U_1^{\oplus}(\zeta) \cap \mathbb{Q}[\eta]$, that is a well-known fact [19].

Lemma 4.31. *The cokernel of*

$$\alpha_2 : \prod_C U_1^{\oplus}(C) \to U_1^{\oplus}(A),$$

as C ranges over all cyclic subgroups in A, is a finite p-group, which is trivial if p is regular.

Proof The multiplicative group $E_p(A) = 1 + \Delta_p(A)$, where $\Delta_p(A)$ denotes the kernel of the p-adic augmentation $\mathbb{Z}_p[A] \to \mathbb{Z}_p$, is of finite index in $E_p(\mathcal{M}_A) = 1 + \Delta_p(\mathcal{M}_A)$, where $\Delta_p(\mathcal{M}_A) = \Delta_p(A)\mathcal{M}_A$ is the direct sum of the appropriate prime ideals in the Wedderburn components. Since $E_p(\mathcal{M}_A)$ is a $\mathbb{Z}_p$-module ([27],II.3, proposition 9), this index is a p-power. For $U^1(\mathcal{M}_A) = U_1^{\oplus}(\mathcal{M}_A) \cap E_p(\mathcal{M}_A)$, this implies that $U^1(\mathcal{M}_A)/U_1^{\oplus}(A)$ is a finite p-group. In fact for every $u \in U^1(\mathcal{M}_A)$ a suitable p-power v lies in $E_p(A)$. Thus v has rational coefficients that are integral with respect to p. On the other hand $(\sharp A)v \in \mathbb{Z}[A]$ because $v \in \mathcal{M}_A$ ([24], theorem 41.1) and therefore $v \in \mathbb{Z}[A] \cap U_1^{\oplus}(\mathcal{M}_A) = U_1^{\oplus}(A)$.

Now look at the commutative square

$$\begin{array}{ccc} \prod_C U_1^{\oplus}(C) & \longrightarrow & U_1^{\oplus}(A) \\ \downarrow & & \downarrow \\ \prod_C U^1(\mathcal{M}_C) & \longrightarrow & U^1(\mathcal{M}_A) \end{array}$$

We have just seen that $[U^1(\mathcal{M}_C) : U_1^{\oplus}(C)]$ is a p-power for every cyclic subgroup C. Thanks to the previous lemma, we can conclude that also the bottom horizontal arrow has p-power index.

Since the cokernel in question is a p-group, it is also the cokernel of the map

$$\hat{\alpha}_2 : \prod_C \hat{U}_1^{\oplus}(C) \to \hat{U}_1^{\oplus}(A),$$

where the hat denotes p-adic completion as before. Now, if p is regular, remark 4.26 shows us that $\hat{U}_1^{\oplus}(A) = \hat{U}_1^{+}(A)$, so that $\hat{\alpha}_2$ shows up as the higher horizontal arrow in the diagram

$$\begin{array}{ccc} \prod_C \hat{U}_1^{+}(C) & \longrightarrow & \hat{U}_1^{+}(A) \\ \downarrow & & \downarrow \\ \prod_C \hat{U}_p'(C) & \longrightarrow & \hat{U}_p'(A), \end{array}$$

where $U_p'(A)$ is the group of symmetric units in the p-adic group ring $\mathbb{Z}_p[A]$ with augmentation 1 and G-norm 1. The lower horizontal arrow of this diagram is surjective [13]. The proof is finished by remarking that, for regular p, the vertical arrows are bijective [20].

Corollary 4.32. *The natural map*

$$\lambda_A : \prod_C W(C) \to U_1^{\oplus}(A),$$

with the product direct and C ranging over all cyclic subgroups of A, is an injection of p-power index; it is bijective if p is regular.

Proof We already proved this for cyclic A. Thus, for every $u_C \in U_1^{\oplus}(C)$ a certain p-power is constructible, i.e. in $Y(C)$. By previous lemma, for every $u \in U_1^{\oplus}(A)$ a certain p-power is a product of such u_C, hence a possibly higher p-power will be constructible. These p-powers are trivial in the regular case.

Remark 4.33. We defined the group of constructible units $Y(A)$ to be $\operatorname{im}\lambda_A = \prod_C W(C)$. In particular, if $B \subseteq A$, it follows that

$$Y(A) = Y(B) \times \prod_{C' \not\subseteq B} W(C').$$

This implies that the notion of constructibility does not depend on the ambient group. In other words, a unit $u \in U_1^{\oplus}(B)$ can not be made constructible by going to a larger group, i.e. $Y(A) \cap U_1^{\oplus}(B) = Y(B)$. In fact, if $u \in Y(A) \cap U_1^{\oplus}(B)$, a certain power u^N lies in $Y(B)$. Now, if we factor $u = v \cdot v'$ with $v \in Y(B)$ and $v' \in \prod_{C' \not\subseteq B} W(C')$, the N-th power of v' would be trivial; but there is no torsion, hence $v' = 1$.

We can summarize what we said in the following theorem.

Theorem 4.34. *Let A be an abelian p-group of order $> p$. Then $U_1^{\oplus}(A)$ contains $Y(A)$ as a subgroup of p-power index $c(A)$ and $c(A) = 1$ if and only if p is regular.*

Proof Almost everything follows immediately from what we said above. It remains to be shown that $Y(A) \neq U_1^{\oplus}(A)$ if p is non regular and A is non cyclic, elementary abelian. For this we refer to [17] and [19] and we will just give an example.

Example 4.35. We want to show a non constructible unit, as provided by Hoechsmann in [16]. If A is an abelian group of order p^2, where p is an

irregular prime there is a procedure that gives non constructible units . We do this in the easiest case, choosing $p = 37$ the first irregular prime, and A to be elementary abelian of order p^2.

A non constructible unit in this case is

$$1 + (1 + x^p + ... + x^{p(p-1)}) \sum_{i \in I} c_i (x^i + x^{-i} + x^{6i} + x^{-6i} - 4),$$

where $\langle x \rangle = A$, $I = \{1, 2, 3, 4, 5, 8, 9, 10, 15\}$ and

$$\begin{array}{ll} c_1 = +1826391438413288649 & c_2 = -1021466795253062642 \\ c_3 = +162246643879408744 & c_4 = +706070271863032512 \\ c_5 = -1501545774926023726 & c_8 = +878425477417643782 \\ c_9 = -280909292629400144 & c_{10} = -328201689410415248 \\ c_{15} = +106002969513013355 & \end{array}$$

For the theory about non constructible units we refer to [11] and [16].

To conclude, we want to say briefly what is known more than what we exposed about the index $c(A)$. Hoechsmann himself studied it for cyclic groups of order pq, for p and q distinct primes, in [10] and [18]. One of his students, R. A. Ferguson, devoted his PhD thesis to the study the index $c(A)$ for cyclic group rings for order $p^r q^s$ and was able to find an inductive method to compute it [9].

References

[1] Atiyah, M. F.; Macdonald, I. G. *Introduction to commutative algebra*, Addison-Wesley Publishing Co., Reading, Mass.-London-Don Mills, Ont. (1969)

[2] Bass, H. *The Dirichlet unit theorem, induced characters, and Whitehead groups of finite groups*, Topology 4 (1965) pp. 391-410

[3] Borevič, Z.I.; Shafarevich, I.R. *Number theory*, Academic Press, New York (1966)

[4] Brakenhoff, J. *The representation ring and the center of the group ring*, master thesis (2005) available at www.math.leidenuniv.nl/scripties/Brakenhoff.pdf

[5] Conrad, M.; Replogle, D.R. *Nontrivial Galois module structure of cyclotomic fields*, Math. Comp. 72 (2003), no.242, pp.891-899

[6] Deligne, P.; Ribet, K.A. *Values of abelian L-functions at negative integers over totally real fields*, Invent. Math. 59 (1980), no.3, pp. 227-286

[7] de Smit, B.; Borger J. *Galois theory and integral models of* Λ*-rings*, preprint (2007) available at www.math.leidenuniv.nl/ desmit/prep/gl.pdf

[8] Eisenbud, D. *Commutative algebra with a view toward algebraic geometry*, Springer-Verlag, New York (1995)

[9] Ferguson, R. A. *Units in integral cyclic group rings for order* $l^r p^s$, unpublished (1997)

[10] Hoechsmann, K. *Constructing units in commutative group rings*, Manuscripta math. 75 (1992), no.1, pp. 5-23

[11] Hoechsmann, K. *Exotic units in group rings of rank* p^2, Arch. Math. 58 (1992), pp. 239-247

[12] Hoechsmann, K. *Généralisation d'un lemme de Kummer*, Canad. Math. Bull. 32 (1989), pp. 486-489

[13] Hoechsmann, K. *Norms and traces in p-adic abelian group rings* Arch. Math. 51 (1988), pp. 50-54

[14] Hoechsmann, K. *On the arithmetic of commutative group rings* in Group theory, algebra and number theory (Saarbrücken, 1993), de Gruyter, Berlin (1996), pp. 145-201

[15] Hoechsmann, K. *On the Bass-Milnor index of abelian p-groups*, Contemp. Math. 93 (1989), pp. 179-195

[16] Hoechsmann, K. *Unit bases in small cyclic group rings* in Methods in ring theory (Levico Terme, 1997), Lecture Notes in Pure and Appl. Math. 198, Dekker, New York (1998), pp.121-139

[17] Hoechsmann, K. *Units and class-groups in integral elementary abelian group rings*, J. Pure Appl. Algebra 47 (1987), pp. 253-264

[18] Hoechsmann, K. *Units in integral group rings for order pq*, Can. J. Math. 47 (1995), no.1, pp. 113-131

[19] Hoechsmann, K.; Ritter J. *Constructible units in abelian p-group rings*, Journal of Pure and Applied Algebra 68 (1990), no.3, pp. 325-339

[20] Hoechsmann, K.; Sehgal S.H. *Units in regular abelian p-group rings*, J. Number Theory 30 (1988), pp. 375-381

[21] Hoechsmann, K.; Sehgal S.H. *Units in regular elementary abelian group rings*, Arch. Math. 47 (1986), no.5, pp. 413-417

[22] Jacobson, N. *Basic algebra II*, W. H. Freeman and Co., San Francisco, Calif., (1980)

[23] Kervaire, M.A.; Murthy, M.P. *On the projective class group of cyclic groups of prime power order*, Comment. Math. Helv. 52 (1977), pp. 415-452

[24] Reiner, J. *Maximal orders*, Academic Press, New York (1975)

[25] Solomon, D. *Galois relations for cyclotomic numbers and p-units*, J. Number Theory 46 (1994), no. 2, pp. 158-178

[26] Washington, L.C. *Introduction to cyclotomic fields*, Springer-Verlag, New York (1982)

[27] Weil, A. *Basic number theory*, Springer, New York (1967)