Constructing Units of Integral Group Rings

Renata Rodrigues Marcuz Silva
Joint work with Raul Antonio Ferraz

Instituto de Matemática e estatística - USP

Supported by FAPESP Proc. (2012/20138 – 4)

August 12, 2014

Definition

A **group** is a non empty set G together with a binary operation, denoted by $\cdot$, called multiplication, such that (or $+$, called addition) such that for all $a, g, h \in G$, the following proprieties hold:

Definition

A **group** is a non empty set G together with a binary operation, denoted by $\cdot$, called multiplication, such that (or $+$, called addition) such that for all $a, g, h \in G$, the following proprieties hold:

(i) $(a \cdot g) \cdot h = a \cdot (g \cdot h)$;

Definition

A **group** is a non empty set G together with a binary operation, denoted by $\cdot$, called multiplication, such that (or $+$, called addition) such that for all $a, g, h \in G$, the following proprieties hold:

(i) $(a \cdot g) \cdot h = a \cdot (g \cdot h)$;

(ii) There exists an element, that we we will denoted by $1 \in G$, such that $g \cdot 1 = 1 \cdot g = g$;

Definition

A **group** is a non empty set G together with a binary operation, denoted by $\cdot$, called multiplication, such that (or $+$, called addition) such that for all $a, g, h \in G$, the following proprieties hold:

(i) $(a \cdot g) \cdot h = a \cdot (g \cdot h)$;

(ii) There exists an element, that we we will denoted by $1 \in G$, such that $g \cdot 1 = 1 \cdot g = g$;

(iii) For each element $g \in G$ there exists an element, which we will denoted by $g^{-1} \in G$, such that $g \cdot (g^{-1}) = (g^{-1}) \cdot g = 1$.

Definition

A **group** is a non empty set G together with a binary operation, denoted by $\cdot$, called multiplication, such that (or $+$, called addition) such that for all $a, g, h \in G$, the following proprieties hold:

(i) $(a \cdot g) \cdot h = a \cdot (g \cdot h)$;

(ii) There exists an element, that we we will denoted by $1 \in G$, such that $g \cdot 1 = 1 \cdot g = g$;

(iii) For each element $g \in G$ there exists an element, which we will denoted by $g^{-1} \in G$, such that $g \cdot (g^{-1}) = (g^{-1}) \cdot g = 1$.

Definition

A **group** is a non empty set G together with a binary operation, denoted by $\cdot$, called multiplication, such that (or $+$, called addition) such that for all $a, g, h \in G$, the following proprieties hold:

(i) $(a \cdot g) \cdot h = a \cdot (g \cdot h)$;

(ii) There exists an element, that we we will denoted by $1 \in G$, such that $g \cdot 1 = 1 \cdot g = g$;

(iii) For each element $g \in G$ there exists an element, which we will denoted by $g^{-1} \in G$, such that $g \cdot (g^{-1}) = (g^{-1}) \cdot g = 1$.

If G is a finite group, then the number of elements of G is called **order** of G and it is denoted by $|G|$.

If, in addition, the following propriety is verified

(iv) $g \cdot h = h \cdot g$

for all $g, h \in G$ then the group is said to be **abelian (or commutative)**.

If, in addition, the following propriety is verified

(iv) $g \cdot h = h \cdot g$

for all $g, h \in G$ then the group is said to be **abelian (or commutative)**.

If, in addition, the following propriety is verified

(iv) $g \cdot h = h \cdot g$

for all $g, h \in G$ then the group is said to be **abelian (or commutative)**.

Definition

Let G be a group. A non empty subset H of G is called **subgroup** of G, and we denoted by $H < G$, when with the operation of G, the set H is a group.

If, in addition, the following propriety is verified

(iv) $g \cdot h = h \cdot g$

for all $g, h \in G$ then the group is said to be **abelian (or commutative)**.

Definition

Let G be a group. A non empty subset H of G is called **subgroup** of G, and we denoted by $H < G$, when with the operation of G, the set H is a group.

If, in addition, the following propriety is verified

(iv) $g \cdot h = h \cdot g$

for all $g, h \in G$ then the group is said to be **abelian (or commutative)**.

Definition

Let G be a group. A non empty subset H of G is called **subgroup** of G, and we denoted by $H < G$, when with the operation of G, the set H is a group.

Proposition

Let H be a non empty subset of G. Then $H < G$ if, and only if, the following conditions hold:

If, in addition, the following propriety is verified

(iv) $g \cdot h = h \cdot g$

for all $g, h \in G$ then the group is said to be **abelian (or commutative)**.

Definition

Let G be a group. A non empty subset H of G is called **subgroup** of G, and we denoted by $H < G$, when with the operation of G, the set H is a group.

Proposition

Let H be a non empty subset of G. Then $H < G$ if, and only if, the following conditions hold:

(i) $a \cdot b \in H, \; \forall \; a, b \in H;$

If, in addition, the following propriety is verified

(iv) $g \cdot h = h \cdot g$

for all $g, h \in G$ then the group is said to be **abelian (or commutative)**.

Definition

Let G be a group. A non empty subset H of G is called **subgroup** of G, and we denoted by $H < G$, when with the operation of G, the set H is a group.

Proposition

Let H be a non empty subset of G. Then $H < G$ if, and only if, the following conditions hold:

(i) $a \cdot b \in H, \ \forall \ a, b \in H$;

(ii) $h^{-1} \in H, \ \forall \ h \in H$.

Let g be an element of a group $(G, \cdot)$ and let $n \in \mathbb{Z}$. We define the power if g as:

$$g^n = \begin{cases} \underbrace{g^{-1} \cdot g^{-1} \cdots g^{-1}}_{|n| \text{ times}} & \text{if } n < 0 \\ 1 & \text{if } n = 0 \\ \underbrace{g \cdot g \cdots g}_{n \text{ times}} & \text{if } n > 0 \end{cases}$$

Let g be an element of a group $(G, \cdot)$ and let $n \in \mathbb{Z}$. We define the power if g as:

$$g^n = \begin{cases} \underbrace{g^{-1} \cdot g^{-1} \cdots g^{-1}}_{|n| \text{ times}} & \text{if } n < 0 \\ 1 & \text{if } n = 0 \\ \underbrace{g \cdot g \cdots g}_{n \text{ times}} & \text{if } n > 0 \end{cases}$$

Since $g^n \cdot g^m = g^{n+m}$, we have that the set $\langle g \rangle = \{g^n : n \in \mathbb{Z}\}$ is a subgroup of G, called **cyclic subgroup of G generated by g**.

Let g be an element of a group $(G, \cdot)$ and let $n \in \mathbb{Z}$. We define the power if g as:

$$g^n = \begin{cases} \underbrace{g^{-1} \cdot g^{-1} \cdots g^{-1}}_{|n| \text{ times}} & \text{if } n < 0 \\ 1 & \text{if } n = 0 \\ \underbrace{g \cdot g \cdots g}_{n \text{ times}} & \text{if } n > 0 \end{cases}$$

Since $g^n \cdot g^m = g^{n+m}$, we have that the set $\langle g \rangle = \{g^n : n \in \mathbb{Z}\}$ is a subgroup of G, called **cyclic subgroup of G generated by g**.

If this group $\langle g \rangle$ is finite, then there exists distinct integers numbers n and m such that $g^n = g^m$, and therefore, $g^{m-n} = 1$.

The least positive integer number n such that $g^n = 1$ is said to be **order of g** and it is denoted by $\mathbf{o}(g)$. If $\langle g \rangle$ is not finite we say that g is an element of infinite order.

The least positive integer number n such that $g^n = 1$ is said to be **order of g** and it is denoted by $\mathbf{o}(g)$. If $\langle g \rangle$ is not finite we say that g is an element of infinite order.

Definition

Let G be a group. If there exists an element g in G such that $G = \langle g \rangle$, then we say that G is a **cyclic group** and g is a **generator** of G. Observe that, if G is finite, then $\mathbf{o}(g) = |G|$.

Definition

Let $(G, .)$ and $(H, *)$ be groups. A map

$$\begin{array}{ccc} G & \xrightarrow{f} & H \\ g & \longmapsto & f(g) \end{array}$$

satisfying $f(g_1.g_2) = f(g_1) * f(g_2)$ is called **homomorphism of groups**.

Definition

Let $(G, .)$ and $(H, *)$ be groups. A map

$$\begin{array}{ccc} G & \xrightarrow{f} & H \\ g & \longmapsto & f(g) \end{array}$$

satisfying $f(g_1.g_2) = f(g_1) * f(g_2)$ is called **homomorphism of groups**.

Definition

Let $(G, .)$ and $(H, *)$ be groups. A map

$$\begin{array}{ccc} G & \xrightarrow{f} & H \\ g & \longmapsto & f(g) \end{array}$$

satisfying $f(g_1.g_2) = f(g_1) * f(g_2)$ is called **homomorphism of groups**.

We can easily check that if $f : G \to H$ is a group homomorphism, then $f(1_G) = 1_H$ and $f(g^{-1}) = f(g)^{-1}$.

Definition

Let $(G, .)$ and $(H, *)$ be groups. By $f : G \to H$ denote the group homomorphism. The subset

$$\mathrm{Ker}(f) := \{g \in G : f(g) = 1_H\},$$

is called **kernel of** f.

Definition

Let $(G, .)$ and $(H, *)$ be groups. By $f : G \to H$ denote the group homomorphism. The subset

$$\mathrm{Ker}(f) := \{g \in G : f(g) = 1_H\},$$

is called **kernel of** f.

Definition

Let $(G, .)$ and $(H, *)$ be groups. By $f : G \to H$ denote the group homomorphism. The subset

$$\mathrm{Ker}(f) := \{g \in G : f(g) = 1_H\},$$

is called **kernel of** f.

Definition

Let $(G, .)$ and $(H, *)$ be groups and let $f : G \to H$ be the group homomorphism. The subset
$\mathrm{Im}(f) := \{h \in H :$ exists $g \in G$ such that $f(g) = h\}$,
is called **image of** f.

Proposition

Let $(G, \cdot)$ *and* $(H, *)$ *be groups and let* $f : G \to H$ *be a group homomorphism. Then:*

Proposition

Let $(G, \cdot)$ *and* $(H, *)$ *be groups and let* $f : G \to H$ *be a group homomorphism. Then:*

(i) f *is injector if, and only if,* $Ker(f) = \{1\}$*. In this case,* f *is called* ***monomorphism****;*

Proposition

Let $(G, \cdot)$ and $(H, *)$ be groups and let $f : G \to H$ be a group homomorphism. Then:

(i) *f is injector if, and only if, $Ker(f) = \{1\}$. In this case, f is called* ***monomorphism****;*

(ii) *f is surjective if, and only if, $Im(f) = H$. In this case, f is called a* ***epimorphism****.*

Proposition

Let $(G, \cdot)$ and $(H, *)$ be groups and let $f : G \to H$ be a group homomorphism. Then:

(i) *f is injector if, and only if, $Ker(f) = \{1\}$. In this case, f is called* ***monomorphism****;*

(ii) *f is surjective if, and only if, $Im(f) = H$. In this case, f is called a* ***epimorphism****.*

Proposition

Let $(G, \cdot)$ and $(H, *)$ be groups and let $f : G \to H$ be a group homomorphism. Then:

(i) *f is injector if, and only if, $Ker(f) = \{1\}$. In this case, f is called* ***monomorphism****;*

(ii) *f is surjective if, and only if, $Im(f) = H$. In this case, f is called a* ***epimorphism****.*

If the group homomorphism f is injective and subjective, then f is called **isomorphism**. Besides that, given two groups G and H, if there exists a isomorphism f between then we shall say that G and H are isomorphic and write $G \simeq H$.

Proposition

Let $(G, \cdot)$ and $(H, *)$ be groups and let $f : G \to H$ be a group homomorphism. Then:

(i) *f is injector if, and only if, $Ker(f) = \{1\}$. In this case, f is called* ***monomorphism****;*

(ii) *f is surjective if, and only if, $Im(f) = H$. In this case, f is called a* ***epimorphism****.*

If the group homomorphism f is injective and subjective, then f is called **isomorphism**. Besides that, given two groups G and H, if there exists a isomorphism f between then we shall say that G and H are isomorphic and write $G \simeq H$.

Example

Let $(G, \cdot)$ be a group and take $h \in G$. We define a map $\sigma_h : G \to G$ given by $\sigma_h(g) = h^{-1} \cdot g \cdot h$, $\forall\, g \in G$. σ_h is a group homomorphism, known as **conjugation**.

Definition

A **ring** $(R, +, \cdot)$ is a non empty set R together with two binary operations, that we shall denote by $+$ and $\cdot$ and called addition and multiplication respectively, such that the following proprieties hold:

Definition

A **ring** $(R, +, \cdot)$ is a non empty set R together with two binary operations, that we shall denote by $+$ and $\cdot$ and called addition and multiplication respectively, such that the following proprieties hold:

A_1 $(r+s)+t = r+(s+t), \ \forall\, r, s, t \in R$

Definition

A **ring** $(R, +, \cdot)$ is a non empty set R together with two binary operations, that we shall denote by $+$ and $\cdot$ and called addition and multiplication respectively, such that the following proprieties hold:

- A_1 $(r+s)+t = r+(s+t), \forall\, r, s, t \in R$
- A_2 There exists an element $0 \in R$ such that $0 + r = r = r + 0, \forall\, r \in R$

Definition

A **ring** $(R, +, \cdot)$ is a non empty set R together with two binary operations, that we shall denote by $+$ and $\cdot$ and called addition and multiplication respectively, such that the following proprieties hold:

- A_1 $(r + s) + t = r + (s + t), \ \forall \ r, s, t \in R$
- A_2 There exists an element $0 \in R$ such that $0 + r = r = r + 0, \ \forall \ r \in R$
- A_3 $\forall \ r \in R$, there exists an element $-r \in R$ such that $r + (-r) = 0 = (-r) + r$

Definition

A **ring** $(R, +, \cdot)$ is a non empty set R together with two binary operations, that we shall denote by $+$ and $\cdot$ and called addition and multiplication respectively, such that the following proprieties hold:

- A_1 $(r + s) + t = r + (s + t)$, $\forall\, r, s, t \in R$
- A_2 There exists an element $0 \in R$ such that $0 + r = r = r + 0$, $\forall\, r \in R$
- A_3 $\forall\, r \in R$, there exists an element $-r \in R$ such that $r + (-r) = 0 = (-r) + r$
- A_4 $r + s = s + r$, $\forall\, r, s \in R$

Definition

A **ring** $(R, +, \cdot)$ is a non empty set R together with two binary operations, that we shall denote by $+$ and $\cdot$ and called addition and multiplication respectively, such that the following proprieties hold:

- A_1 $(r + s) + t = r + (s + t)$, $\forall\ r, s, t \in R$
- A_2 There exists an element $0 \in R$ such that $0 + r = r = r + 0$, $\forall\ r \in R$
- A_3 $\forall\ r \in R$, there exists an element $-r \in R$ such that $r + (-r) = 0 = (-r) + r$
- A_4 $r + s = s + r$, $\forall\ r, s \in R$
- M_1 $r \cdot (s \cdot t) = (r \cdot s) \cdot t$, $\forall\ r, s, t \in R$

Definition

A **ring** $(R, +, \cdot)$ is a non empty set R together with two binary operations, that we shall denote by $+$ and $\cdot$ and called addition and multiplication respectively, such that the following proprieties hold:

- A_1 $(r+s)+t = r+(s+t), \ \forall\, r,s,t \in R$
- A_2 There exists an element $0 \in R$ such that $0 + r = r = r + 0, \ \forall\, r \in R$
- A_3 $\forall\, r \in R$, there exists an element $-r \in R$ such that $r + (-r) = 0 = (-r) + r$
- A_4 $r + s = s + r, \ \forall\, r,s \in R$
- M_1 $r \cdot (s \cdot t) = (r \cdot s) \cdot t, \ \forall\, r,s,t \in R$
- D1 $r \cdot (s + t) = r \cdot s + r \cdot t, \ \forall\, r,s,t \in R$

Definition

A **ring** $(R, +, \cdot)$ is a non empty set R together with two binary operations, that we shall denote by $+$ and $\cdot$ and called addition and multiplication respectively, such that the following proprieties hold:

- A_1 $(r+s)+t = r+(s+t)$, $\forall\, r, s, t \in R$
- A_2 There exists an element $0 \in R$ such that $0 + r = r = r + 0$, $\forall\, r \in R$
- A_3 $\forall\, r \in R$, there exists an element $-r \in R$ such that $r + (-r) = 0 = (-r) + r$
- A_4 $r + s = s + r$, $\forall\, r, s \in R$
- M_1 $r \cdot (s \cdot t) = (r \cdot s) \cdot t$, $\forall\, r, s, t \in R$
- D1 $r \cdot (s + t) = r \cdot s + r \cdot t$, $\forall\, r, s, t \in R$
- D2 $(r + s) \cdot t = r \cdot t + s \cdot t$, $\forall\, r, s, t \in R$

If the proprieties of the definition hold and

M2 $\exists\, 1 \in R$ such that $1 \cdot r = r = r \cdot 1$,

then $(R, +, \cdot)$ is called **ring with unity**.

If the proprieties of the definition hold and

M2 $\exists\, 1 \in R$ such that $1 \cdot r = r = r \cdot 1$,

then $(R, +, \cdot)$ is called **ring with unity**.

If the proprieties of the definition hold and

M_2 $\exists\, 1 \in R$ such that $1 \cdot r = r = r \cdot 1$,

then $(R, +, \cdot)$ is called **ring with unity**.

If all previous conditions hold and, in addition,

M_3 $r \cdot s = s \cdot r,\ \forall\, r, s \in R$,

then $(R, +, \cdot)$ is called **commutative ring**. The set $\mathbb{Z}$ together with its usual operations is a commutative ring with unity.

If the proprieties of the definition hold and

M_2 $\exists\, 1 \in R$ such that $1 \cdot r = r = r \cdot 1$,

then $(R, +, \cdot)$ is called **ring with unity**.

If all previous conditions hold and, in addition,

M_3 $r \cdot s = s \cdot r,\ \forall\, r, s \in R$,

then $(R, +, \cdot)$ is called **commutative ring**. The set $\mathbb{Z}$ together with its usual operations is a commutative ring with unity.

If the proprieties of the definition hold and

M$_2$ $\exists\, 1 \in R$ such that $1 \cdot r = r = r \cdot 1$,

then $(R, +, \cdot)$ is called **ring with unity**.

If all previous conditions hold and, in addition,

M$_3$ $r \cdot s = s \cdot r$, $\forall\, r, s \in R$,

then $(R, +, \cdot)$ is called **commutative ring**. The set $\mathbb{Z}$ together with its usual operations is a commutative ring with unity.

Example

Let $n \in \mathbb{N}$. The set of all integers which have the same remainder as a when divided by n is called the congruence class of a modulo n, and is denoted by $\bar{a}$. The set $\mathbb{Z}_n := \{\bar{0}, \bar{1}, \bar{2}, \cdots, \overline{n-1}\}$ with the operations:

is an example of commutative ring with unity, called **ring of integers modulo** m.

If the proprieties of the definition hold and

M$_2$ $\exists\, 1 \in R$ such that $1 \cdot r = r = r \cdot 1$,

then $(R, +, \cdot)$ is called **ring with unity**.

If all previous conditions hold and, in addition,

M$_3$ $r \cdot s = s \cdot r,\ \forall\, r, s \in R$,

then $(R, +, \cdot)$ is called **commutative ring**. The set $\mathbb{Z}$ together with its usual operations is a commutative ring with unity.

Example

Let $n \in \mathbb{N}$. The set of all integers which have the same remainder as a when divided by n is called the congruence class of a modulo n, and is denoted by $\overline{a}$. The set $\mathbb{Z}_n := \{\overline{0}, \overline{1}, \overline{2}, \cdots, \overline{n-1}\}$ with the operations:

- $+ : \overline{a} + \overline{b} = \overline{a+b} \pmod{m}$

is an example of commutative ring with unity, called **ring of integers modulo** m.

If the proprieties of the definition hold and

M_2 $\exists\, 1 \in R$ such that $1 \cdot r = r = r \cdot 1$,

then $(R, +, \cdot)$ is called **ring with unity**.

If all previous conditions hold and, in addition,

M_3 $r \cdot s = s \cdot r, \ \forall\, r, s \in R$,

then $(R, +, \cdot)$ is called **commutative ring**. The set $\mathbb{Z}$ together with its usual operations is a commutative ring with unity.

Example

Let $n \in \mathbb{N}$. The set of all integers which have the same remainder as a when divided by n is called the congruence class of a modulo n, and is denoted by $\bar{a}$. The set $\mathbb{Z}_n := \{\bar{0}, \bar{1}, \bar{2}, \cdots, \overline{n-1}\}$ with the operations:

- $+ : \bar{a} + \bar{b} = \overline{a+b} \pmod{m}$
- $\cdot : \bar{a} \cdot \bar{b} = \overline{a \cdot b} \pmod{m}$

is an example of commutative ring with unity, called **ring of integers modulo** m.

Definition

Let $(R, +_R, \cdot_R)$ and $(S, +_S, \cdot_S)$ be rings. A **ring homomorphism** is a map $f : R \to S$ that satisfies:

for all $r_1, r_2 \in R$.

Definition

Let $(R, +_R, ._R)$ and $(S, +_S, ._S)$ be rings. A **ring homomorphism** is a map $f : R \to S$ that satisfies:

(i) $f(r_1 +_R a_2) := f(r_1) +_S f(r_2)$;

for all $r_1, r_2 \in R$.

Definition

Let $(R, +_R, ._R)$ and $(S, +_S, ._S)$ be rings. A **ring homomorphism** is a map $f : R \to S$ that satisfies:

(i) $f(r_1 +_R a_2) := f(r_1) +_S f(r_2)$;

(ii) $f(r_1 ._R r_2) := f(r_1) ._S f(r_2)$;

for all $r_1, r_2 \in R$.

Definition

Let $(R, +_R, ._R)$ and $(S, +_S, ._S)$ be rings. A **ring homomorphism** is a map $f : R \to S$ that satisfies:

(i) $f(r_1 +_R a_2) := f(r_1) +_S f(r_2)$;

(ii) $f(r_1 ._R r_2) := f(r_1) ._S f(r_2)$;

for all $r_1, r_2 \in R$.

Definition

Let $(R, +_R, ._R)$ and $(S, +_S, ._S)$ be rings. A **ring homomorphism** is a map $f : R \to S$ that satisfies:

(i) $f(r_1 +_R a_2) := f(r_1) +_S f(r_2)$;

(ii) $f(r_1 ._R r_2) := f(r_1) ._S f(r_2)$;

for all $r_1, r_2 \in R$.

Definition

An element r of a ring with unity $(R, +, \cdot)$ is called **invertible** if there exists an element, which we shall denote by $r^{-1} \in R$, and call its **inverse**, such that $r \cdot r^{-1} = r^{-1} \cdot r = 1$.
The set

$$\mathcal{U}(R) = \{ r \in R : r \text{ is invertivel } \}$$

is called the **group of units of** R.

Definition

Let R be a ring with unity and let G be a group. We definite the **group ring**

$$RG := \left\{ \sum_{g \in G} a_g g : a_g \in R \text{ and } a_g = 0 \text{ almost everywhere} \right\}.$$

together with the operations:

Definition

Let R be a ring with unity and let G be a group. We definite the **group ring**

$$RG := \left\{ \sum_{g \in G} a_g g : a_g \in R \text{ and } a_g = 0 \text{ almost everywhere} \right\}.$$

together with the operations:

(i) $+ : \sum_{g \in G} a_g g + \sum_{g \in G} b_g g := \sum_{g \in G} (a_g + b_g) g;$

Definition

Let R be a ring with unity and let G be a group. We definite the **group ring**

$$RG := \left\{ \sum_{g \in G} a_g g : a_g \in R \text{ and } a_g = 0 \text{ almost everywhere} \right\}.$$

together with the operations:

(i) $+ : \sum_{g \in G} a_g g + \sum_{g \in G} b_g g := \sum_{g \in G} (a_g + b_g) g;$

(ii) $\cdot : \left(\sum_{g \in G} a_g g \right) \cdot \left(\sum_{h \in G} b_h h \right) := \left(\sum_{g \in G} \sum_{h \in G} (a_g b_h) gh \right).$

In our case, the ring R will be the $\mathbb{Z}$ and $\mathbb{Z}G$ are called **integral group rings.**

Example

Let $C_5 = \langle g \rangle = \{1, g, g^2, g^3, g^4\}$ be the cyclic group of order 5. We have

$$\mathbb{Z}C_5 = \left\{a_0 + a_1 g + a_2 g^2 + a_3 g^4 + a_4 g^4 : a_i \in \mathbb{Z},\ \forall\, 1 \leq i \leq 4\right\},$$

the group ring $\mathbb{Z}C_5$.

In our case, the ring R will be the $\mathbb{Z}$ and $\mathbb{Z}G$ are called **integral group rings.**

Example

Let $C_5 = \langle g \rangle = \{1, g, g^2, g^3, g^4\}$ be the cyclic group of order 5. We have

$$\mathbb{Z}C_5 = \left\{a_0 + a_1 g + a_2 g^2 + a_3 g^4 + a_4 g^4 : a_i \in \mathbb{Z}, \ \forall\, 1 \leq i \leq 4\right\},$$

the group ring $\mathbb{Z}C_5$.

In our case, the ring R will be the $\mathbb{Z}$ and $\mathbb{Z}G$ are called **integral group rings.**

Example

Let $C_5 = \langle g \rangle = \{1, g, g^2, g^3, g^4\}$ be the cyclic group of order 5. We have

$$\mathbb{Z}C_5 = \left\{a_0 + a_1 g + a_2 g^2 + a_3 g^4 + a_4 g^4 : a_i \in \mathbb{Z}, \ \forall\, 1 \leq i \leq 4\right\},$$

the group ring $\mathbb{Z}C_5$.

Definition

Let R be a ring with unity and let G be a group. Consider its group ring RG. The homomorphism of rings: $\epsilon : RG \to R$ define as

$\epsilon \left(\sum_{g \in G} a_g g \right) := \sum_{g \in G} a_g$ is called the **augmentation mapping** of RG.

Definition

Let RG be a group ring. Consider the map $* : RG \to RG$ define as $\left(\sum_{g\in G} a_g g\right)^* = \sum_{g\in G} a_g g^{-1}$. Such map is called the **classical involution**.

Definition

Let RG be a group ring. Consider the map $* : RG \to RG$ define as $\left(\sum_{g\in G} a_g g\right)^* = \sum_{g\in G} a_g g^{-1}$. Such map is called the **classical involution**.

Definition

Let RG be a group ring. Consider the map $*: RG \to RG$ define as $\left(\sum_{g\in G} a_g g\right)^* = \sum_{g\in G} a_g g^{-1}$. Such map is called the **classical involution**.

We recall that we denote by $\mathcal{U}(R)$ the of units of R. That is

$$\mathcal{U}(R) = \{r \in R : \exists s \in R \text{ such that } r \cdot s = s \cdot r = 1\}.$$

In Particular, given a group G and a ring with unity R, $\mathcal{U}(RG)$ denotes the group of units of the group ring RG.

Definition

The set

$$\mathcal{U}_1(RG) := \{u \in \mathcal{U}(RG) : \epsilon(u) = 1\}$$

is the a subgroup of units augmentation 1 in $\mathcal{U}(RG)$, known as the group of **normalized units**.

Definition

The set

$$\mathcal{U}_1(RG) := \{u \in \mathcal{U}(RG) : \epsilon(u) = 1\}$$

is the a subgroup of units augmentation 1 in $\mathcal{U}(RG)$, known as the group of **normalized units**.

Definition

The set

$$\mathcal{U}_1(RG) := \{u \in \mathcal{U}(RG) : \epsilon(u) = 1\}$$

is the a subgroup of units augmentation 1 in $\mathcal{U}(RG)$, known as the group of **normalized units**.

Let $u \in \mathcal{U}(\mathbb{Z}G)$. Then exists $v \neq 0 \in \mathbb{Z}G$ such that $uv = 1 = vu$. Hence, $\epsilon(uv) = 1$ and, since ϵ is a ring homomorphism $\epsilon(u)\epsilon(v) = 1$. Since $\epsilon(u), \epsilon(v) \in \mathbb{Z}$, $\epsilon(u) = 1$ and $\epsilon(v) = 1$ or $\epsilon(u) = -1$ e $\epsilon(v) = -1$. Therefore, $\mathcal{U}(\mathbb{Z}G) \subseteq \pm\mathcal{U}_1(\mathbb{Z}G)$. We conclude $\mathcal{U}(\mathbb{Z}G) = \pm\mathcal{U}_1(\mathbb{Z}G)$.

Definition

The set $\mathcal{U}_1^*(RG) := \{u \in \mathcal{U}_1(RG) : u^* = u\}$ is called the set of **normalized symmetric units** of RG, where $*$ denotes the classical involution.

Definition

The set $\mathcal{U}_1^*(RG) := \{u \in \mathcal{U}_1(RG) : u^* = u\}$ is called the set of **normalized symmetric units** of RG, where $*$ denotes the classical involution.

Definition

The set $\mathcal{U}_1^*(RG) := \{u \in \mathcal{U}_1(RG) : u^* = u\}$ is called the set of **normalized symmetric units** of RG, where $*$ denotes the classical involution.

Example (Trivial Units)

Let RG be the group ring. An element $rg \in RG$ such that $r \in \mathcal{U}(R)$, has a inverse, given by $r^{-1}g^{-1}$. Elements of this form are called **trivial units** of RG. Therefore the elements $\pm g$ are trivial units of the integral group ring $\mathbb{Z}G$. If F is a field, then elements if the form kg, where $k \neq 0 \in K$ are trivial units.

Example (Unipotent Units)

If $r \in R$ is such that $r^k = 0$ for some positive integer k, then we have that $1 - r, 1 + r \in \mathcal{U}(R)$. The elements $1 \pm r$ are called **unipotent units** of R.

Example (Unipotent Units)

If $r \in R$ is such that $r^k = 0$ for some positive integer k, then we have that $1 - r, 1 + r \in \mathcal{U}(R)$. The elements $1 \pm r$ are called **unipotent units** of R.

Example (Unipotent Units)

If $r \in R$ is such that $r^k = 0$ for some positive integer k, then we have that $1 - r, 1 + r \in \mathcal{U}(R)$. The elements $1 \pm r$ are called **unipotent units** of R.

Example (Bicyclic Units)

Let g be an element of finite order $n > 1$ of the group G, i. e., $g^n = 1$ and let $h \in G$. The element $u_{g,h} = 1 + (g-1)h\widehat{g}$, where $\widehat{g} = 1 + g + g^2 + \ldots + g^{n-1}$ is a unit of RG namely as **bicyclic unit** of the group ring RG.

Example (Bass Cyclic Units)

Let g be an element of finite order n in a group G. A **Bass cyclic unit** is an element of the group ring $\mathbb{Z}G$ of the form:

$$u_i = (1 + g + g^2 + \cdots + g^{i-1})^{\phi(n)} + \left(\frac{1 - i^{\phi(n)}}{n} \right) \widehat{g},$$

where i is an integer such that $1 < i < n$, $\gcd(i, n) = 1$ and ϕ denotes the Euler's totient function.

Example (Bass Cyclic Units)

Let g be an element of finite order n in a group G. A **Bass cyclic unit** is an element of the group ring $\mathbb{Z}G$ of the form:

$$u_i = (1 + g + g^2 + \cdots + g^{i-1})^{\phi(n)} + \left(\frac{1 - i^{\phi(n)}}{n} \right) \widehat{g},$$

where i is an integer such that $1 < i < n$, $\gcd(i, n) = 1$ and ϕ denotes the Euler's totient function.

Example (Bass Cyclic Units)

Let g be an element of finite order n in a group G. A **Bass cyclic unit** is an element of the group ring $\mathbb{Z}G$ of the form:

$$u_i = (1 + g + g^2 + \cdots + g^{i-1})^{\phi(n)} + \left(\frac{1 - i^{\phi(n)}}{n} \right) \widehat{g},$$

where i is an integer such that $1 < i < n$, $\gcd(i, n) = 1$ and ϕ denotes the Euler's totient function.

Example (Hoechsmann's Units)

Let $G = C_n = \langle g \rangle$ be the cyclic group of order n. Then

$$u = \frac{1 + g^j + \cdots + g^{j(i-1)}}{1 + g + \cdots + g^{i-1}},$$

where $\gcd(i, n) = 1$ and $\gcd(j, n) = 1$ is a unit, call **Hoechsmann's unit**.

Definition

Let $G = C_p \cong \langle g \rangle$. For each i such that $1 \leq i \leq \frac{p-3}{2}$ we define:

$$u_i = \left(1 + g^{t} + \ldots + g^{t(r-1)}\right)\left(1 + g^{t^i} + \ldots + g^{t^i(t-1)}\right) - k\widehat{g}$$

where $t \in \mathbb{Z}$ is such that $\overline{t}$ generates $\mathcal{U}(\mathbb{Z}_p)$, r is the least positive integer satisfying $tr \equiv 1 \pmod{p}$ and $k = \dfrac{rt-1}{p}$.

Definition

Let $G = C_p \cong \langle g \rangle$. For each i such that $1 \leq i \leq \frac{p-3}{2}$ we define:

$$u_i = \left(1 + g^{t} + \ldots + g^{t(r-1)}\right)\left(1 + g^{t^i} + \ldots + g^{t^i(t-1)}\right) - k\widehat{g}$$

where $t \in \mathbb{Z}$ is such that $\overline{t}$ generates $\mathcal{U}(\mathbb{Z}_p)$, r is the least positive integer satisfying $tr \equiv 1 \pmod{p}$ and $k = \dfrac{rt-1}{p}$.

Definition

Let $G = C_p \cong \langle g \rangle$. For each i such that $1 \leq i \leq \frac{p-3}{2}$ we define:

$$u_i = \left(1 + g^t + \ldots + g^{t(r-1)}\right)\left(1 + g^{t^i} + \ldots + g^{t^i(t-1)}\right) - k\widehat{g}$$

where $t \in \mathbb{Z}$ is such that $\overline{t}$ generates $\mathcal{U}(\mathbb{Z}_p)$, r is the least positive integer satisfying $tr \equiv 1 \pmod{p}$ and $k = \dfrac{rt-1}{p}$.

Theorem (Ferraz)

If $\left\langle -1, \theta, \mu_2, \cdots, \mu_{\frac{p-3}{2}} \right\rangle$ *generates* $\mathcal{U}(\mathbb{Z}[\theta])$, *then the set* $S := \left\langle u_1, u_2, u_3, \cdots, u_{\frac{p-3}{2}} \right\rangle$ *is a multiplicatively independent subset of* $\mathcal{U}_1(\mathbb{Z}C_p)$ *such that*

$$\mathcal{U}_1(\mathbb{Z}C_p) = \langle g \rangle \times \langle S \rangle .$$

Consider the integral group ring $\mathbb{Z}(C_p \times C_2)$, where $C_p \cong \langle g \rangle$ and $C_2 \cong \langle a \rangle$.

Consider the integral group ring $\mathbb{Z}(C_p \times C_2)$, where $C_p \cong \langle g \rangle$ and $C_2 \cong \langle a \rangle$.

Every element α of $\mathbb{Z}(C_p \times C_2)$ can be written as

$$\alpha = x + ya_n,$$

with $x, y \in \mathbb{Z}C_p$.

Consider the integral group ring $\mathbb{Z}(C_p \times C_2)$, where $C_p \cong \langle g \rangle$ and $C_2 \cong \langle a \rangle$.

Every element α of $\mathbb{Z}(C_p \times C_2)$ can be written as

$$\alpha = x + ya_n,$$

with $x, y \in \mathbb{Z}C_p$.

Therefore

$$u \in \mathcal{U}(\mathbb{Z}(C_p \times C_2)) \Leftrightarrow u = u_1 \left[\left(\frac{1+u_2}{2} \right) + \left(\frac{1-u_2}{2} \right) a \right]$$

where $u_1, u_2 \in \mathcal{U}(\mathbb{Z}C_p)$ and $u_2 \equiv 1 \pmod{\langle 2 \rangle}$.

Consider the integral group ring $\mathbb{Z}(C_p \times C_2)$, where $C_p \cong \langle g \rangle$ and $C_2 \cong \langle a \rangle$.

Every element α of $\mathbb{Z}(C_p \times C_2)$ can be written as

$$\alpha = x + ya_n,$$

with $x, y \in \mathbb{Z}C_p$.

Therefore

$$u \in \mathcal{U}(\mathbb{Z}(C_p \times C_2)) \Leftrightarrow u = u_1 \left[\left(\frac{1+u_2}{2} \right) + \left(\frac{1-u_2}{2} \right) a \right]$$

where $u_1, u_2 \in \mathcal{U}(\mathbb{Z}C_p)$ and $u_2 \equiv 1 \pmod{\langle 2 \rangle}$.

Consider the following ring homomorphism $\phi : \mathbb{Z}C_p \to \mathbb{Z}_2 C_p$ and define $\Phi := \phi|_{\mathcal{U}(\mathbb{Z}(C_p))}$.

Then

$$u \in \mathcal{U}(\mathbb{Z}(C_p \times C_2)) \Leftrightarrow u = u_1 \left[\left(\frac{1 + u_2}{2} \right) + \left(\frac{1 - u_2}{2} \right) a \right]$$

where $u_1, u_2 \in \mathcal{U}(\mathbb{Z}(C_p)$ and $u_2 \in \text{Ker}(\Phi)$.

Then

$$u \in \mathcal{U}(\mathbb{Z}(C_p \times C_2)) \Leftrightarrow u = u_1 \left[\left(\frac{1+u_2}{2} \right) + \left(\frac{1-u_2}{2} \right) a \right]$$

where $u_1, u_2 \in \mathcal{U}(\mathbb{Z}(C_p)$ and $u_2 \in \text{Ker}(\Phi)$.

So in order to find the units of $\mathbb{Z}(C_p \times C_2)$ we must describe the units of $\mathbb{Z}C_p$ and the kernel of Φ.

Then

$$u \in \mathcal{U}(\mathbb{Z}(C_p \times C_2)) \Leftrightarrow u = u_1 \left[\left(\frac{1+u_2}{2} \right) + \left(\frac{1-u_2}{2} \right) a \right]$$

where $u_1, u_2 \in \mathcal{U}(\mathbb{Z}(C_p)$ and $u_2 \in \text{Ker}(\Phi)$.

So in order to find the units of $\mathbb{Z}(C_p \times C_2)$ we must describe the units of $\mathbb{Z}C_p$ and the kernel of Φ.

Let $\rho := \Phi|_{\mathcal{U}_1^*(\mathbb{Z}C_p)}$.

Then

$$u \in \mathcal{U}(\mathbb{Z}(C_p \times C_2)) \Leftrightarrow u = u_1 \left[\left(\frac{1+u_2}{2} \right) + \left(\frac{1-u_2}{2} \right) a \right]$$

where $u_1, u_2 \in \mathcal{U}(\mathbb{Z}(C_p)$ and $u_2 \in \text{Ker}(\Phi)$.

So in order to find the units of $\mathbb{Z}(C_p \times C_2)$ we must describe the units of $\mathbb{Z}C_p$ and the kernel of Φ.

Let $\rho := \Phi|_{\mathcal{U}_1^*(\mathbb{Z}C_p)}$.

Since $\mathcal{U}(\mathbb{Z}C_p) = \langle -1 \rangle \times \mathcal{U}_1(\mathbb{Z}C_p)$ and $-1 \in \text{Ker}(\psi)$ we have $\text{Ker}(\Phi) = \langle -1 \rangle \times \text{Ker}(\Phi|_{\mathcal{U}_1(\mathbb{Z}C_p)})$. Because p is an odd prime number, we obtain $\mathcal{U}_1(\mathbb{Z}C_p) = C_p \times \mathcal{U}_1^*(\mathbb{Z}C_p)$. Thus, we can easily see that $\text{Ker}(\Phi|_{\mathcal{U}(\mathbb{Z}C_p)}) = \langle -1 \rangle \times \text{Ker}(\rho)$.

Suppose that 2 generates $\mathcal{U}(\mathbb{Z}_p)$ or $\overline{2}$ generates $\mathcal{U}(\mathbb{Z}_p)^2$ and $\overline{-1} \notin \mathcal{U}(\mathbb{Z}_p)^2$. Based on the Hoeschmann's units, we build

$$\begin{aligned} w_1 &= u_1 \\ w_i &= g^{\left(\frac{p-1}{2}\right)\cdot t^i} \cdot g^{\left(\frac{p+1}{2}\right)\cdot t^{i-1}} u_i u_{i-1}^{-1} \end{aligned}$$

where t is such that $\mathcal{U}(\mathbb{Z}_p) = \langle t \rangle$ and

$$u_i = \left(1 + g^t + \ldots + g^{t(r-1)}\right)\left(1 + g^{t^i} + \ldots + g^{t^i(t-1)}\right) - k\widehat{g}$$

These w_i are an symmetric normalized unit of $\mathbb{Z}C_p$ such that

$$\mathcal{U}_1(\mathbb{Z}C_p) = \langle g \rangle \times \left\langle w_1, \cdots w_{\frac{p-3}{2}} \right\rangle$$

and the set $\{w_i : 1 \leq i \leq \frac{p-3}{2}\}$ is multiplicatively independent.

Definition

Let θ be the p-th primitive roof of the unity. An odd prime number p is called a **nice prime** if $\left\langle -1, \theta, \mu_2, \cdots, \mu_{\frac{p-3}{2}} \right\rangle$ generates $\mathcal{U}(\mathbb{Z}[\theta])$ where $\mu_i = 1 + \theta + \cdots + \theta^{i-1}$ and

From now on p will be a nice prime.

Definition

Let θ be the p-th primitive roof of the unity. An odd prime number p is called a **nice prime** if $\left\langle -1, \theta, \mu_2, \cdots, \mu_{\frac{p-3}{2}} \right\rangle$ generates $\mathcal{U}(\mathbb{Z}[\theta])$ where $\mu_i = 1 + \theta + \cdots + \theta^{i-1}$ and

(i) $\mathcal{U}(\mathbb{Z}_p) \cong \langle \overline{2} \rangle$

From now on p will be a nice prime.

Definition

Let θ be the p-th primitive roof of the unity. An odd prime number p is called a **nice prime** if $\left\langle -1, \theta, \mu_2, \cdots, \mu_{\frac{p-3}{2}} \right\rangle$ generates $\mathcal{U}(\mathbb{Z}[\theta])$ where $\mu_i = 1 + \theta + \cdots + \theta^{i-1}$ and

(i) $\mathcal{U}(\mathbb{Z}_p) \cong \langle \overline{2} \rangle$

(ii) or $\mathcal{U}(\mathbb{Z}_p)^2 \cong \langle \overline{2} \rangle$ and $-\overline{1} \notin \mathcal{U}(\mathbb{Z}_p)^2$.

From now on p will be a nice prime.

Definition

Let p be an odd prime number. By δ we denote the ring isomorphism

$$\begin{array}{rccc} \delta: & \mathbb{Z}C_p & \rightarrow & \mathbb{Z}C_p \\ & \displaystyle\sum_{i=0}^{p-1} a_i g^i & \longmapsto & \displaystyle\sum_{i=0}^{p-1} a_i g^{2i}. \end{array}$$

Definition

Let p be an odd prime number. By δ we denote the ring isomorphism

$$\begin{array}{rccc} \delta: & \mathbb{Z}C_p & \to & \mathbb{Z}C_p \\ & \displaystyle\sum_{i=0}^{p-1} a_i g^i & \longmapsto & \displaystyle\sum_{i=0}^{p-1} a_i g^{2i}. \end{array}$$

Lemma

Let p be a nice prime. $\delta^{n-1}(w_1) = w_n$.

Lemma

$\rho(w_1)^{2^n} = \widehat{g} + g^{(\frac{p-1}{2})\cdot 2^n}(\overline{1} + g^{2^n}), \ \forall\ n \in \mathbb{N}.$

It follows from this result that $\rho(w_1^{2^n} w_{n-1}^{-1}) = \overline{1}$, i.e., $w_1^{2^n} w_{n-1}^{-1} \in \mathrm{Ker}(\rho),\ 1 \leq n \leq \frac{p-3}{2}$.

By the above Lemma, we deduce that $\mathbf{ord}(\rho(w_1)) \leq 2^{\frac{p-1}{2}} - 1$.

Lemma

$\rho(w_1)^{2^n} = \widehat{g} + g^{(\frac{p-1}{2})\cdot 2^n}(\overline{1} + g^{2^n}), \ \forall \ n \in \mathbb{N}.$

Corollary

$\rho(w_1)^{2^n} = \rho(w_{n+1})$. *In particular,* $Im(\rho) = \langle \rho(w_1) \rangle$.

It follows from this result that $\rho(w_1^{2^n} w_{n-1}^{-1}) = \overline{1}$, i.e., $w_1^{2^n} w_{n-1}^{-1} \in \text{Ker}(\rho), \ 1 \leq n \leq \frac{p-3}{2}$.

By the above Lemma, we deduce that $\textbf{ord}(\rho(w_1)) \leq 2^{\frac{p-1}{2}} - 1$.

Lemma

$\rho(w_1)^{2^n} = \widehat{g} + g^{(\frac{p-1}{2})\cdot 2^n}(\overline{1} + g^{2^n}), \ \forall\ n \in \mathbb{N}.$

Corollary

$\rho(w_1)^{2^n} = \rho(w_{n+1})$. *In particular,* $Im(\rho) = \langle \rho(w_1) \rangle$.

It follows from this result that $\rho(w_1^{2^n} w_{n-1}^{-1}) = \overline{1}$, i.e., $w_1^{2^n} w_{n-1}^{-1} \in \mathrm{Ker}(\rho),\ 1 \leq n \leq \frac{p-3}{2}$.

Lemma

$\rho(w_1)^{2^{\frac{p-1}{2}}-1} = \overline{1}.$

By the above Lemma, we deduce that $\mathbf{ord}(\rho(w_1)) \leq 2^{\frac{p-1}{2}} - 1$.

Lemma

If $\mathbf{ord}(\rho(w_1)) = 2^{\frac{p-1}{2}} - 1$, *then* S_1 *generates the kernel of* ρ, *where*

$$S_1 = \{w_1^2 w_2^{-1}, w_1^4 w_3^{-1}, w_1^8 w_4^{-1}, \cdots, w_i^{2^i} w_{i+1}^{-1}, \cdots, w_1^{2^{\frac{p-3}{2}}} w_{\frac{p-1}{2}}^{-1}\}$$

This set has the very interesting property that each element is taken into its successor via δ.

Lemma

If $\mathbf{ord}(\rho(w_1)) = 2^{\frac{p-1}{2}} - 1$, *then* S_1 *generates the kernel of* ρ, *where*

$$S_1 = \{w_1^2 w_2^{-1}, w_1^4 w_3^{-1}, w_1^8 w_4^{-1}, \cdots, w_i^{2^i} w_{i+1}^{-1}, \cdots, w_1^{2^{\frac{p-3}{2}}} w_{\frac{p-1}{2}}^{-1}\}$$

Corollary

If $\mathbf{ord}(\rho(w_1)) = 2^{\frac{p-1}{2}} - 1$, *then* $Ker(\rho) = \langle S_4 \rangle$, *where*

$$S_4 = \{w_1^2 w_2^{-1}, w_2^2 w_3^{-1}, \cdots, w_i^2 w_{i+1}^{-1}, \cdots, w_{\frac{p-3}{2}}^2 w_{\frac{p-1}{2}}^{-1}\}$$

This set has the very interesting property that each element is taken into its successor via δ.

Theorem

If $\mathbf{ord}(\rho(w_1)) = 2^{\frac{p-1}{2}} - 1$, *then*

$$\mathcal{U}(\mathbb{Z}C_{2p}) = \langle -1 \rangle \times \langle g, a \rangle \times \left\langle \left\{ w_i : 1 \leq i \leq \tfrac{p-3}{2} \right\} \right\rangle \times \left\langle \left\{ u_i(a) : 1 \leq i \leq \tfrac{p-3}{2} \right\} \right\rangle.$$

Furthermore, the set $\left\{ w_1, w_2, \ldots, w_{\frac{p-3}{2}}, u_1(a), u_2(a), \ldots, u_{\frac{p-3}{2}}(a) \right\}$ *is multiplicatively independent.*

Example

Assume that $C_7 \cong \langle g \rangle$ and $C_2 \cong \langle a \rangle$. We want to find $\mathcal{U}(\mathbb{Z}C_{14})$.

We already know that

$$\mathcal{U}_1(\mathbb{Z}C_7) = \langle g \rangle \times \langle w_1, w_2 \rangle$$

where $w_1 = 1 - g + g^2 + g^5 - g^6$ and $w_2 = 1 - g^2 + g^3 + g^4 - g^5$.

Example

Assume that $C_7 \cong \langle g \rangle$ and $C_2 \cong \langle a \rangle$. We want to find $\mathcal{U}(\mathbb{Z}C_{14})$.

We already know that

$$\mathcal{U}_1(\mathbb{Z}C_7) = \langle g \rangle \times \langle w_1, w_2 \rangle$$

where $w_1 = 1 - g + g^2 + g^5 - g^6$ and $w_2 = 1 - g^2 + g^3 + g^4 - g^5$.

Example

Assume that $C_7 \cong \langle g \rangle$ and $C_2 \cong \langle a \rangle$. We want to find $\mathcal{U}(\mathbb{Z}C_{14})$.

We already know that

$$\mathcal{U}_1(\mathbb{Z}C_7) = \langle g \rangle \times \langle w_1, w_2 \rangle$$

where $w_1 = 1 - g + g^2 + g^5 - g^6$ and $w_2 = 1 - g^2 + g^3 + g^4 - g^5$.

Since $2^3 - 1 = 7$ is a prime number, we get that $\mathbf{ord}(\rho(w_1)) = 7$.

Example

Assume that $C_7 \cong \langle g \rangle$ and $C_2 \cong \langle a \rangle$. We want to find $\mathcal{U}(\mathbb{Z}C_{14})$.

We already know that

$$\mathcal{U}_1(\mathbb{Z}C_7) = \langle g \rangle \times \langle w_1, w_2 \rangle$$

where $w_1 = 1 - g + g^2 + g^5 - g^6$ and $w_2 = 1 - g^2 + g^3 + g^4 - g^5$.

Since $2^3 - 1 = 7$ is a prime number, we get that $\mathbf{ord}(\rho(w_1)) = 7$.

$$\beta_1 = \frac{1 - w_1^3 w_2^{-1}}{2} = 4 - 3g + 2g^2 - g^3 - g^4 + 2g^5 - 3g^6$$

$$\beta_2 = \frac{1 - w_1 w_2^2}{2} = 4 - g - 3g^2 + 2g^3 + 2g^4 - 3g^5 - g^6$$

$$u_1(a) = (1-\beta_1) + \beta_1 a = (-3 + 3g - 2g^2 + g^3 + g^4 - 2g^5 + 3g^6) + (4 - 3g + 2g^2 - g^3 - g^4 + 2g^5 - 3g^6)a$$

$$u_2(a) = (1-\beta_2) + \beta_2 a = (-3 + g + 3g^2 - 2g^3 - 2g^4 + 3g^5 + g^6) + (4 - g - 3g^2 + 2g^3 + 2g^4 - 3g^5 - g^6)a$$

$u_1(a) = (1-\beta_1) + \beta_1 a = (-3+3g-2g^2+g^3+g^4-2g^5+3g^6) + (4-3g+2g^2-g^3-g^4+2g^5-3g^6)a$

$u_2(a) = (1-\beta_2) + \beta_2 a = (-3+g+3g^2-2g^3-2g^4+3g^5+g^6) + (4-g-3g^2+2g^3+2g^4-3g^5-g^6)a$

It follows from Theorem 24 that

$$\mathcal{U}(\mathbb{Z}C_{14}) = \langle -1 \rangle \times \langle g, a \rangle \times \langle w_1, w_2 \rangle \times \langle u_1(a), u_2(a) \rangle$$

S. K. Sehgal and C. Polcino-Milies, *An Introduction to Group Rings*, Kluwer Academic Publishers, Netherlands, (2002).

S. K. Sehgal and C. Polcino-Milies, *An Introduction to Group Rings*, Kluwer Academic Publishers, Netherlands, (2002).

R. A. Ferraz, *Units of* $\mathbb{Z}C_p$, Groups, Rings e Group Rings, Contemp. Math. 499, Amer. Math. Soc., Providence, RI, (2009), 107-119.

S. K. Sehgal and C. Polcino-Milies, *An Introduction to Group Rings*, Kluwer Academic Publishers, Netherlands, (2002).

R. A. Ferraz, *Units of* $\mathbb{Z}C_p$, Groups, Rings e Group Rings, Contemp. Math. 499, Amer. Math. Soc., Providence, RI, (2009), 107-119.

R. A. Ferraz and R. Marcuz, *Units of* $\mathbb{Z}(C_p \times C_2)$ *and* $\mathbb{Z}(C_p \times C_2 \times C_2)$, Commun. Algebra, to appear.

S. K. Sehgal and C. Polcino-Milies, *An Introduction to Group Rings*, Kluwer Academic Publishers, Netherlands, (2002).

R. A. Ferraz, *Units of* $\mathbb{Z}C_p$, Groups, Rings e Group Rings, Contemp. Math. 499, Amer. Math. Soc., Providence, RI, (2009), 107-119.

R. A. Ferraz and R. Marcuz, *Units of* $\mathbb{Z}(C_p \times C_2)$ *and* $\mathbb{Z}(C_p \times C_2 \times C_2)$, Commun. Algebra, to appear.

S. K. Sehgal, *Topics in Group Rings*, Marcel Dekker, Inc., New York and Basel, 1978.

- S. K. Sehgal and C. Polcino-Milies, *An Introduction to Group Rings*, Kluwer Academic Publishers, Netherlands, (2002).
- R. A. Ferraz, *Units of* $\mathbb{Z}C_p$, Groups, Rings e Group Rings, Contemp. Math. 499, Amer. Math. Soc., Providence, RI, (2009), 107-119.
- R. A. Ferraz and R. Marcuz, *Units of* $\mathbb{Z}(C_p \times C_2)$ *and* $\mathbb{Z}(C_p \times C_2 \times C_2)$, Commun. Algebra, to appear.
- S. K. Sehgal, *Topics in Group Rings*, Marcel Dekker, Inc., New York and Basel, 1978.
- S. K. Sehgal, *Units in Integral Group Rings*, Logman Scientific & Technical, New York, 1993.