Facultad De Matemáticas
Universidad de Murcia
Trabajo De Fin De Grado

UNIDADES EN ANILLOS DE GRUPO

Autor:
Mariano Serrano Sánchez

Tutor:
Ángel Del Río Mateos

21 de junio de 2013

Mi más sincero agradecimiento a mi tutor Ángel del Río por su apoyo y por el tiempo que me ha dedicado, haciendo posible tanto la elaboración de esta memoria como mi formación como matemático.
También quisiera expresar mi agradecimiento a todos mis familiares y amigos, por su incondicional cariño.

A Cristina.
A mis padres.

Índice general

Resumen. 1
Abstract. 2
Introducción. 6

1. Preliminares. **15**
1.1. Notación general de grupos y anillos. 15
1.2. Grupos Hamiltonianos. 17
1.2.1. Clasificación de los grupos Hamiltonianos. 21
1.3. Anillos semisimples. 24
1.4. Introducción a los anillos de grupo. 25
1.5. Anillos de enteros algebraicos. 27
1.6. Órdenes. 28
1.7. Representaciones y caracteres. 30

2. Unidades en Anillos de Grupo. **33**
2.1. Unidades triviales y unidades unipotentes. 33
2.2. Unidades Bicíclicas. 36
2.3. Unidades Cíclicas de Bass. 38
2.4. Unidades de torsión. 40
2.5. Unidades en $\mathbb{Z}A$, con A un grupo abeliano finito. 41

3. El Teorema de Higman. **47**
3.1. Unidades en $\mathbb{Z}K_8$. 47
3.2. El Teorema de Higman. 50

4. El grupo de unidades de $\mathbb{Z}C_n$. 55

4.1. Unidades en $\mathbb{Z}C_8$. 55

4.2. Unidades en $\mathbb{Z}C_5$. 60

Bibliografía. 65

Índice Alfabético. 67

Resumen.

Este Trabajo de fin de Grado trata sobre el estudio de unidades en anillos de grupo con coeficiente enteros y en la búsqueda de un resultado que nos garantice cuándo el grupo de unidades de un anillo de grupo con coeficientes enteros es finito.

En la primera parte del documento demostramos el Teorema de clasificación de los grupos Hamiltonianos, que fue obtenido por Richard Dedekind en [4]. Además, introducimos el concepto de anillo semisimple, anillo de grupo y orden junto con sus propiedades más relevantes. Posteriormente enunciamos el Teorema de las Unidades de Dirichlet junto con el concepto de unidad ciclotómica. Para terminar esta primera parte, hacemos una breve mención a la teoría de representaciones y caracteres.

La segunda etapa de este documento se centra en el estudio de unidades en anillos de grupo con coeficientes enteros. En un primer lugar estudiamos las unidades triviales y unipotentes, e incluso demostramos bajo qué hipótesis KG, con K un cuerpo, solamente tiene unidades triviales. Después introducimos el concepto de unidad bicíclica y caracterizamos cuando una unidad bicíclica es trivial. Además, justificaremos que todas las unidades bicíclicas no triviales tiene orden infinito. A continuación estudiamos las unidades cíclicas de Bass y demostramos bajo qué condiciones tienen orden infinito. Demostraremos el Teorema de Passman-Bass y deduciremos varios corolarios importantes. Para finalizar el capítulo, describiremos el grupo de unidades de $\mathbb{Z}A$ con A un grupo abeliano finito y daremos estructura al grupo de unidades de aumento uno.

La última etapa del documento se centra en el estudio del Teorema de Higman y en calcular $U(\mathbb{Z}C_n)$ para valores pequeños de $n \in \mathbb{N}$. Para poder abordar su demostración, necesitamos en primer lugar estudiar el grupo de unidades de $\mathbb{Z}K_8$, de hecho, demostramos que todas las unidades de $\mathbb{Z}K_8$ son triviales y además, calcularemos $U(\mathbb{Z}[\zeta_3])$ y $U(\mathbb{Z}[\zeta_4])$. Tras haber logrado demostrar el Teorema de Higman, nos centraremos en la justificación de otro resultado que nos garantizará bajo que hipótesis el grupo de unidades de $\mathbb{Z}G$ es finito. Como consecuencia de este resultado, demostramos que $U(\mathbb{Z}C_n) = \pm C_n$ para $n = 1,\ 2,\ 3,\ 4,\ 6$. Por último, calcularemos $U(\mathbb{Z}C_8)$ y $U(\mathbb{Z}C_5)$.

Abstract.

In this dissertation we study the question of when the group ring $\mathbb{Z}G$ has only trivial torsion units, where G is a finite group. It turns out that the above question is closely related to Hamiltonian groups and related to the most important units of $\mathbb{Z}G$ such as bicyclic units and Bass cyclic units. So, we are going to study Hamiltonian groups and units of group rings in order to be able to use them during the proof of when $\mathbb{Z}G$ has only trivial torsion units.

In the first chapter, we introduce terms and basic properties which are going to be used during this project. After this, we will prove the Theorem of classification of Hamiltonian groups. To prove this theorem we first prove that if G is an abelian finite p-group and $g \in G$ is an element of maximal order, then $\langle g \rangle$ is a direct summand of G. Later, we prove that every Hamiltonian group contains a subgroup isomorphic to the Quaternion group of order 8 which we denote by K_8. We will use these two lemmas to prove that a group G is Hamiltonian if and only if $G = K_8 \times E \times A$ where E is an elementary abelian 2-group and A is an abelian group where all elements have odd order. Theorem 1.5 is known as the classification of Hamiltonian groups and the idea of the proof was taken from the paper [4] which was written by R. Dedekind. This result will be very important during the proof of Higman's Theorem, which we will study in Chapter 3. Later on, we are going to introduce the concept of R-modules and semisimple rings in order to be able to use the Wedderburn-Artin Theorem. It states that a ring R is semisimple if and only if it is a direct sum of matrix algebras over division rings. Next, we introduce the concept of group ring. Let G be a group and R be a ring. By RG we denote the set of all R-linear combinations of elements of G. The operations in R and G induce a natural sum and product in RG which make RG into a ring called the group ring of G with coefficients in R. After this, we introduce the augmentation map and the Universal Property of Group Ring. In addition, semisimple group rings are characterized by Maschke's Theorem 1.7 which states that the group ring RG is semisimple if and only if R is a semisimple ring, G is finite and $|G|$ is invertible in R.

There are two important theorems in the first chapter which we are going to use frequently but we need not to prove because this is not the aim of the dissertation. One of these theorems is the Perlis-Walker's Theorem 1.9 which states that if G is a finite abelian group, of order n, and K is a field such that $char(k) \nmid n$, then $KG \simeq \oplus_{d|n} a_d K(\zeta_d)$ where ζ_d denotes a primitive root of unity of order d, $a_d = \frac{n_d}{[K(\zeta_d) : K]}$ and n_d denotes the number of elements of order d in G. The last theorem is the Dirichlet's Unit Theorem 1.11 which states that if K is a finite extension of $\mathbb{Q}$ then $U(\mathcal{O}_K) = C \times F$ is a finitely generated abelian group where $\mathcal{O}_K$ is the ring of algebraic integers, C is a finite cyclic group and F is torsion free of rank $n_1 + n_2 - 1$ where n_1 denotes the number of real embeddings of K and n_2 denotes the number of pairs of complex embeddings of K which are not real. Later, we introduce the cyclotomic units, the concept of order and we prove their basic properties. Let ζ be a complex root of unity of order $n > 1$ and consider the subring $R = \mathbb{Z}[\zeta]$ of $\mathbb{C}$ generated by ζ. For every positive integer k let $\eta_k(\zeta) = \frac{\zeta^k - 1}{\zeta - 1} = 1 + \zeta + \zeta^2 + \cdots + \zeta^{k-1}$. We prove that $\eta_k(\zeta) \in U(\mathbb{Z}[\zeta])$ and that $\eta_k(\zeta)^{-1} = \eta_l(\zeta^k)$ if $kl \equiv 1 \mod |\zeta|$. The units of this form are called cyclotomic units. The last part of Chapter 1 is dedicated to the introduction of representations and characters.

The principal aim of Chapter 2 is to study the most important units in group rings in order to be able to search for a theorem which characterizes when the unit group of $\mathbb{Z}G$ is finite. We have proved this theorem using Higman's Theorem 3.9 which we will explain in Chapter 3. In addition, we prove in Chapter 2 some basic lemmas which help us during the project.

Only a few ways to build units in the group ring $\mathbb{Z}G$ are known.We are going to use two of them in order to build bicyclic units and Bass cyclic units. First, an element of the form rg where $r \in U(R)$ and $g \in G$, has an inverse $r^{-1}g^{-1}$. The elements of this form are called the trivial units of RG. If $\eta \in R$ is such that $\eta^k = 0$ for some positive integer k, then we have $(1 - \eta)(1 + \eta + \eta^2 + \cdots + \eta^{k-1}) = 1 - \eta^k = 1$. Thus, $1 \pm \eta$ are units of R. They are called unipotent units of R. In the first theorem of Chapter 2, which is Theorem 2.3, we prove that if G is not torsion-free and K is a not trivial field of characteristic $p \geq 0$ then KG has only trivial units if and only if one of the following

conditions hold:

1. $K = \mathbb{Z}_2$ and $G = C_2$ or $G = C_3$.

2. $K = \mathbb{Z}_3$ and $G = C_2$.

The idea of the last proof was taken from the paper [17] which was written by Passman. Moreover, the case of when G is torsion-free is a opened problem yet. Next, bicyclic units were introduced by Ritter and Sehgal in [22]. Let G be a group and let $R = \mathbb{Z}G$ be an integral group ring. If $a \in G$ is an element of finite order $n > 1$ then $(a-1)\hat{a} = 0$, where $\hat{a} = 1 + a + \cdots + a^{n-1}$. Thus, taking any other element $b \in G$, we can construct a unit: $\mu_{a,b} = 1 + (a-1)b\hat{a}$. It is called a bicyclic unit of the group ring $\mathbb{Z}G$. After this, we prove that if $g, h \in G$ with $o(g) = n < \infty$ then $\mu_{g,h}$ is trivial if and only if h normalizes $\langle g \rangle$. Then, we prove that every bicyclic unit $\mu_{g,h} \neq 1$ of $\mathbb{Z}G$ is of infinite order.

Next, we introduce Bass cyclic units. Let G be a group and let $R = \mathbb{Z}G$ be an integral group ring. Let $g \in G$ of order $n < \infty$. Suppose that k is an integer that is coprime with n, therefore we can find another positive integer m such that $k^m \equiv 1 \mod n$. Because of this, we can build a unit: $u_{k,m}(g) = (1+g+g^2+\cdots+g^{k-1})^m + \frac{1-k^m}{n} \cdot \hat{g}$. These units were discovered by Hyman Bass and are called Bass cyclic units. Later, we will prove that if $g \in G$ with order $n < \infty$ and $l \in \mathbb{Z}$ is such that $1 < l < n-1$ and $(l, n) = 1$ then the Bass cyclic unit $u_{l,\phi(n)}(g)$ is of infinite order, where $\phi(n)$ denotes Euler's totient function.

The following units we are going to study are called torsion units and the main theorem which we have proved previously is the Passman-Bass's Theorem 2.10 which states that if $\gamma = \sum_{g \in G} \gamma(g) g \in \mathbb{Z}G$ is a torsion unit and $\gamma(1) \neq 0$ then $\gamma = \pm 1$. This theorem gives us an important Corollary 2.13 which states that if A is an abelian group then all torsion units of $\mathbb{Z}A$ are trivial. This result will be very important during the proof of Higman's Theorem 3.9, which we will study in Chapter 3. In addition, the original proof of the Passman-Bass's theorem used concepts related to idempotent elements but we have changed this proof in order to obtain the result easier by using group representations and characters. This new proof was taken from [24]. The next

theorem we have proved is the classification of the unit group of $\mathbb{Z}A$ in Theorem 2.14, where A is an abelian finite group, showing that $U(\mathbb{Z}A) = \pm A \times F$ where F is a free abelian group of finite rank and this rank was calculated in the paper [23]. Using this theorem, we prove in Theorem 2.18 that the subgroup of units of augmentation 1 in $U(\mathbb{Z}A)$, which we denote by $U_1(\mathbb{Z}A)$, has the next structure: $U_1(\mathbb{Z}A) = A \times U_2(\mathbb{Z}A)$ where $U_2(\mathbb{Z}A) = \{u \in U(\mathbb{Z}A) \ : \ u \equiv 1 \mod (\Delta A)^2\}$ and ΔA denotes the kernel of the augmentation map. During the last part of this chapter, we mention more theorems which were proved in [27]. It implies that if G is a finite group then the unit group of $\mathbb{Z}G$ is a finitely generated group.

Chapter 3 is going to be the most important chapter because it contains the main theorem of this project which is known as the Higman's Theorem 3.9. To prove it we need to study the units of $\mathbb{Z}K_8$ because it turns out that the proof is closely related to the units of $\mathbb{Z}K_8$ and, in fact, we will prove that all the units of $\mathbb{Z}K_8$ are trivial. In addition, before proving the Higman's Theorem, we have shown that $U(\mathbb{Z}[\zeta_3]) = \{\pm 1, \ \pm\zeta_3, \ \pm\zeta_3^2\}$ and that $U(\mathbb{Z}[\zeta_4]) = \{\pm 1, \ \pm i\}$. Later, we will prove Higman's Theorem 3.9 which states that if G is a torsion group, then all units of $\mathbb{Z}G$ are trivial if and only if G is either a group of exponents equal to $1, 2, 3, 4, 6$ or a Hamiltonian 2-group. We will obtain as corollary of Higman's Theorem that if G is a finite group then the unit group of $\mathbb{Z}G$ is finite if and only if G is either an abelian group of exponent equal to $1, 2, 3, 4, 6$ or a Hamiltonian 2-group as before.

The last chapter of this paper is used to calculate the unit group of $\mathbb{Z}C_n$ with small values of n, where C_n denotes the cyclic group of order n. Because of Higman's Theorem we obtain that $U(\mathbb{Z}C_n) = \pm C_n$ for all $n = 1, 2, 3, 4, 6$. After this, we will calculate two unit groups which are $U(\mathbb{Z}C_n)$ for $n = 5, 8$. For that, we first prove $U(\mathbb{Z}[\sqrt{2}]) = \langle -1 \rangle \times \langle 1 + \sqrt{2} \rangle$ and $U(\mathbb{Z}[\zeta_8]) = \langle \zeta_8 \rangle \times \langle 1 + \sqrt{2} \rangle = \langle \zeta_8 \rangle \times \langle \eta_3(\zeta_8) \rangle$. Later or, we prove that $U(\mathbb{Z}C_8) = \pm C_8 \times \langle u_{3,2}(g) \rangle$, where $C_8 = \langle g \rangle$ is the cyclic group of order 8. Then, if p is prime, we prove two previous results such us $U_1(\mathbb{Z}C_p) \simeq U_1(\mathbb{Z}[\zeta_p])$ and $[U(\mathbb{Z}[\zeta_p]) \ : \ U_1(\mathbb{Z}[\zeta_p])] = p - 1$. Using these two results which we have proved in Preposition 4.6, we will obtain the final result of this dissertation which is the Theorem 4.7 and it states that if $C_5 = \langle x \rangle$ then $U(\mathbb{Z}C_5) = \langle -1, \ x, \ u \rangle$ where $u = (x + 1)^2 - \hat{x}$.

Introducción.

El objeto de esta memoria es el estudio de las unidades más importantes del anillo de grupo con coeficientes enteros $\mathbb{Z}G$, con G un grupo finito, y en la búsqueda de un resultado que nos garantice cuando el grupo de unidades $U(\mathbb{Z}G)$ es finito. Este resultado lo vamos a obtener como consecuencia del Teorema de Higman 3.9, por lo tanto, nos centraremos en lograr demostrar este resultado en primer lugar. Además, es importante remarcar que el problema de estudiar $U(\mathbb{Z}G)$ se puede enmarcar en uno mucho más general que consistiría en el estudio del grupo de las unidades de un $\mathbb{Z}$-orden en un álgebra racional semisimple de dimensión finita. Este tipo de órdenes son conocidos con el nombre de órdenes clásicos.

Los ejemplos más conocidos de órdenes clásicos son los anillos de enteros algebraicos de un cuerpo K. La estructura de estos grupos es bien conocida y viene dada por uno de los teoremas más importantes de la Teoría de Números Algebraicos, el Teorema de las Unidades de Dirichlet 1.11. Existen varias generalizaciones de este teorema para órdenes clásicos, entre las que destacamos el resultado de Hey [8] y el de Bass [2]. Sin embargo, estas generalizaciones no son tan satisfactorias como la que nos proporciona el Teorema de las Unidades de Dirichlet ya que no nos dan a conocer de forma precisa la estructura del grupo de unidades. En la publicación de Kleinert [12] se recogen los resultados más importantes relacionados con este tema.

Los órdenes clásicos que resultan de mayor interés en los últimos años son los anillos de grupo con coeficientes enteros. Varios libros se han publicado teniendo como único objetivo el estudio de los anillos de grupo [16, 17, 20, 23] e incluso hay algunos que están destinados solamente al estudio de unidades en anillos de grupo con coeficientes enteros [11, 24]. Nuestro trabajo se encuentra enmarcado dentro de este contexto y tiene como objetivo principal, lograr demostrar qué propiedades tiene que satisfacer el grupo G para que $U(\mathbb{Z}G)$ sea finito.

A continuación, vamos a describir el contexto histórico en el que apareció el concepto de anillo de grupo. En 1837, William Rowan Hamilton escribió la primera teoría formal

sobre los número complejos, definiéndolos como pares ordenados de número reales, exactamente como los conocemos ahora. Como él era consciente de su interpretación como vectores de un espacio plano dos-dimensional, se dio cuenta de que en realidad, había construido un álgebra que le permitía trabajar con vectores en el plano. Después de mucho esfuerzo, descubrió que podía describir un álgebra, no con vectores, pero sí con operadores que actuaran sobre los vectores del espacio, trabajando de esta forma en un álgebra cuatro-dimensional. Por lo tanto, consideró elementos de la forma $\alpha = a + bi + cj + dk$ llamados cuaterniones, donde los coeficientes a, b, c, d eran números reales y a los símbolos i, j, k los llamó unidades fundamentales. La manera de sumar dos cuaterniones era de la forma obvia, siguiendo la siguiente regla:

$$(a + bi + cj + dk) + (a' + b'i + c'j + d'k) = (a + a') + (b + b')i + (c + c')j + (d + d')k$$

Sin embargo, para introducir el producto, tuvo más dificultades. Finalmente, en octubre de 1843 descubrió las leyes fundamentales con las que se rige el producto de los cuaterniones: $i^2 = j^2 = k^2 = ijk = -1$. Estas leyes implican las conocidas formulas:

$$ij = k = -ji$$
$$jk = i = -kj$$
$$ki = j = -ik$$

Este descubrimiento causó gran expectación en el mundo matemático ya que abría la puerta a numerosas posibilidades. De igual forma a los cuaterniones, se definieron los bicuaterniones pero utilizando coeficientes complejos y el sistema hipercomplejo como la generalización de los bicuaterniones.

Los hechos mencionados anteriormente pueden ser considerados como los primeros avances más significativos en la teoría de anillos. En pocos años, muchos otros sistemas fueron descubiertos y apareció la necesidad de poder clasificarlos. La mayor parte de este trabajo se realizó por Benjamin Peirce, ya que introdujo importantes ideas en la teoría de anillos, tales como la noción de elementos idempotentes y nilpotentes. Posteriormente, A. Sudy y G. Scheffers introdujeron los conceptos de álgebras simples y semisimples. Todo este trabajo culminó en el maravilloso Teorema de Wedderburn con el que se describe la estructura de álgebras de dimensión finita sobre un cuerpo

arbitrario, utilizando técnicas relacionadas con la existencia de elementos idempotentes.

La primera definición de grupo abstracto fue dada por A. Cayley en [3]. Es muy interesante mencionar, que en esta publicación fue donde apareció por primera vez el concepto de anillo de grupo. Casi al final de este artículo, Cayley menciona que él considera elementos de un grupo finito como unidades fundamentales de un sistema hipercomplejo. De forma más explícita, dado un grupo finito $G = \{g_1,\ g_2, \ldots,\ g_n\}$, consideró todos los elementos de la forma

$$x_1g_1 + x_2g_2 + \cdots + x_ng_n$$

donde $x_1,\ x_2 \ldots,\ x_n$ son números reales o complejos. Entonces la suma y el producto de dos elementos $\alpha = \sum_{i=1}^{n} x_ig_i$ y $\beta = \sum_{i=1}^{n} y_ig_i$ venían dados por:

$$\alpha + \beta = \sum_{i=1}^{n}(x_i + y_i)g_i$$

$$\alpha\beta = \sum_{i,j}(x_iy_j)(g_ig_j)$$

De hecho, esta es la definición de un anillo de grupo en este caso particular. El trabajo de Cayley pasó desapercibido durante un tiempo pero Theodor Molien volvió a retomarlo en su tesis doctoral dando estructura a la teoría de sistemas hipercomplejos. En el artículo [14] Molien descubrió resultados sobre la teoría de representaciones complejas de grupos finitos, incluyendo la relación de ortogonalidad para caracteres. La conexión entre la teoría de representaciones de grupos y la teoría de álgebras fue reconocida después de la publicación del artículo [15] elaborado por Emmy Noether.

El estudio de los anillos de grupo fue estimulado en gran parte por la famosa lista de problemas de I. Kaplansky's [10]. A los pocos años, se publicó el primer libro enteramente destinado al estudio de los anillos de grupo [18], obra de D. S. Passman. A partir de este momento, se publicaron numerosos artículos relacionados con este tema, entre los que destacamos [1, 5, 6]. En los últimos años se han realizado muchas publicaciones relacionadas con anillos de grupo. Las más interesantes de mencionar son [17, 23].

Pasemos ya a una descripción detallada de los contenidos de esta memoria. El documento se encuentra destinado a estudiar cuándo el grupo de unidades de $\mathbb{Z}G$ solamente tiene unidades triviales, donde G es un grupo de torsión. La respuesta a esta pregunta se encuentra muy relacionada con los grupos Hamiltonianos y con las unidades más importantes de los anillos de grupo, tales como las unidades bicíclicas y las unidades cíclicas de Bass. Por lo tanto, vamos a estudiar los grupos Hamiltonianos y las unidades en anillos de grupo para poder usarlas durante la demostración anteriormente citada.

El Capítulo 1 lo dedicaremos a introducir la notación y las propiedades elementales que utilizaremos a lo largo de la memoria. Destacamos la clasificación de los grupos Hamiltonianos. Para demostrar este resultado, primero demostramos que si G es un p-grupo abeliano finito y $g \in G$ es un elemento de orden máximo, entonces $\langle g \rangle$ es un sumando directo de G. A continuación, demostramos que todo grupo Hamiltoniano contiene un subgrupo isomorfo al grupo de los cuaterniones de orden 8, que lo denotaremos por K_8, Estos dos resultados previos nos serán de gran ayuda para demostrar que todo grupo Hamiltoniano es de la forma $G = K_8 \times E \times A$ donde E es un 2-grupo abeliano elemental y A es un grupo abeliano con todos los elementos de orden impar. Este teorema aparece en la memoria como Teorema 1.5 y es conocido como la clasificación de los grupos Hamiltonianos. Además, la idea de la demostración se extrajo de la publicación [4], la cual fue escrita por R. Dedekind. Este resultado desempeñará un papel fundamental en el trascurso de la demostración del Teorema de Higman que estudiaremos en el capítulo 3. Más adelante, introducimos el concepto de R-módulo y de anillos semisimples con el fin de poder utilizar el Teorema de Wedderburn-Artin 1.6. Introducimos a continuación el concepto de anillo de grupo. Sea G un grupo y sea R un anillo. Vamos a denotar por RG al conjunto de todas las combinaciones R-lineales de elementos de G. Las operaciones en R y en G inducen de forma natural una suma y un producto en RG convirtiendo a RG en un anillo y lo llamaremos el anillo de grupo de G con coeficientes en R. A continuación, introducimos la aplicación aumento y la Propiedad Universal de los Anillos de Grupo. Además, los anillos de grupo semisimples están caracterizados por el Teorema de Maschke 1.7.

Hay dos teoremas muy importantes en el primer capítulo que vamos a utilizar con

mucha frecuencia a lo largo de todo el documento, pero no vamos a demostrarlos porque ese no es el objetivo de esta memoria. El primero de estos teoremas es el Teorema de Perlis-Walker 1.9 y el segundo es el Teorema de las Unidades de Dirichlet 1.11. Los siguientes conceptos que trataremos son el de unidad ciclotómica y el de orden, donde probaremos varios resultados muy útiles para el desarrollo del documento. Sea ζ una raíz compleja de la unidad de orden $n > 1$ y consideramos el subanillo $R = \mathbb{Z}[\zeta]$ de $\mathbb{C}$ generado por ζ. Para todo entero positivo k, consideramos $\eta_k(\zeta) = \frac{\zeta^k - 1}{\zeta - 1} = 1 + \zeta + \zeta^2 + \cdots + \zeta^{k-1}$. Probaremos que $\eta_k(\zeta) \in U(\mathbb{Z}[\zeta])$ y que $\eta_k(\zeta)^{-1} = \eta_l(\zeta^k)$ si $kl \equiv 1 \mod |\zeta|$. A las unidades de esta forma las llamaremos unidades ciclotómicas. La parte final del Capítulo 1 está basada en la introducción a la teoría de representaciones y caracteres.

El segundo capítulo de esta memoria tiene como objetivo realizar un estudio sobre las unidades más importantes en los anillos de grupo con coeficientes enteros que nos facilitará después la búsqueda de un resultado que nos garantice bajo qué condiciones el grupo de unidades del anillo de grupo $\mathbb{Z}G$ es finito. Este resultado se deduce del Teorema de Higman 3.9 que veremos en el capítulo 3. Para llevar a cabo este teorema, necesitamos en primer lugar introducir los diferentes tipos de unidades necesarias para la elaboración de la demostración y también tenemos que probar unos resultados previos que nos ayudarán en futuras demostraciones. Se conocen pocas maneras de construir unidades en $\mathbb{Z}G$, entre las que destacamos la construcción de las unidades bicíclicas y las unidades cíclicas de Bass. En un primer lugar estudiamos las unidades triviales y unipotentes. Un elemento de la forma rg donde $r \in U(R)$ y $g \in G$ tiene como inverso $r^{-1}g^{-1}$. A los elementos de esta forma los llamaremos unidades triviales de RG. Si $\eta \in R$ es tal que $\eta^k = 0$ para algún entero positivo k, entonces se tiene que $(1 - \eta)(1 + \eta + \eta^2 + \cdots + \eta^{k-1}) = 1 - \eta^k = 1$. Por lo tanto, $1 \pm \eta$ son unidades en R y las llamaremos unidades unipotentes de R. En el primer teorema de este capítulo demostramos que KG, con K un cuerpo y G un grupo no libre de torsión, solamente tiene unidades triviales si y solo si se verifican una de las siguiente condiciones:

1. $K = \mathbb{Z}_2$ y $G = C_2$ ó $G = C_3$.

2. $K = \mathbb{Z}_3$ y $G = C_2$.

La idea para elaborar esta demostración fue tomada de la publicación [17] de Passman. Es importante mencionar que el caso en que G sea un grupo libre de torsión aún sigue abierto, es decir, no hay un resultado concreto que lo demuestre. Después realizamos la construcción de las unidades bicíclicas. Estas fueron introducidas por Ritter y Sehgal en [22]. Sea G un grupo y se $\mathbb{Z}G$ un anillo de grupo con coeficientes enteros. Tomamos $a \in G$ con orden $n < \infty$, entonces $(a-1)\hat{a} = 0$, donde $\hat{a} = 1+a+\cdots+a^{n-1}$. Por lo tanto, si tomamos otro elemento $b \in G$, podemos construir una unidad $\mu_{a,b} = 1+(a-1)b\hat{a}$. A las unidades de esta forma las llamaremos unidades bicíclicas. Demostraremos que $\mu_{a,b}$ es una unidad trivial si y solo si b normaliza a $\langle a \rangle$. Y por último, demostraremos que toda unidad bicíclica $\mu_{a,b} \neq 1$ tiene orden infinito. A continuación construimos las unidades cíclicas de Bass y demostramos bajo qué condiciones tienen orden infinito. Supongamos que k es un entero coprimo con n, por lo tanto, podemos encontrar otro entero positivo m tal que $k^m \equiv 1 \mod n$. Como consecuencia de esto, podemos construir una unidad: $u_{k,m}(a) = (1+a+a^2+\cdots+a^{k-1})^m + \frac{1-k^m}{n} \cdot \hat{a}$. Este tipo de unidades fueron descubiertas por Hyman Bass y las llamaremos unidades cíclicas de Bass. Demostraremos que si $l \in \mathbb{Z}$ tal que $1 < l < n-1$ entonces la unidad cíclica de Bass $u_{l,\phi(n)}(a)$ tiene orden infinito, donde $\phi(n)$ denota la función de Euler. Es de destacar que las unidades cíclicas de Bass son una especie de unidades ciclotómicas, pero en un contexto más general. De hecho, Bass demostró en [2] que si G es un grupo abeliano entonces las unidades cíclicas de Bass generan un subgrupo que contiene un subgrupo de índice finito del centro de $U(\mathbb{Z}G)$. Además, se sabe que el grupo generado por las unidades cíclicas de Bass y las unidades bicíclicas genera un subgrupo de índice finito en $U(\mathbb{Z}G)$ en los siguientes casos (véase [21]):

1. G un 2-grupo tal que $\mathbb{Q}G \simeq \oplus_i M_{n_i}(D_i)$ donde D_i son cuerpos y si $n_i = 2$ entonces $D_i \neq \mathbb{Q}$ o una extensión cuadrática imaginaria.

2. G es un grupo finito nilpotente de orden impar.

3. G es el grupo simétrico S_n.

Más aún, Jesper y Leal [9] han extendido estos resultados a clases más amplias de grupos. Las siguiente unidades que estudiaremos son las unidades de torsión, demostrando el Teorema de Passman-Bass 2.10 que nos dice que si $\gamma = \sum_{g \in G} \gamma(g)g \in \mathbb{Z}G$ es una unidad de torsión y $\gamma(1) \neq 0$ entonces se tiene que $\gamma = \pm 1$. Además, deduciremos en el

Corolario 2.13 que si A es un grupo abeliano entonces todas las unidades de torsión de $\mathbb{Z}A$ son triviales. Este resultado desempeñará un papel fundamental en la demostración del Teorema de Higman 3.9 que estudiaremos en el Capítulo 3. Es importante mencionar que la demostración original de Passman-Bass utilizaba conceptos de elementos idempotentes en anillos de grupo, pero hemos utilizado otra demostración alternativa utilizando representaciones y caracteres, ya que de esta forma obteníamos el resultado de forma más directa. La demostración fue obtenida de la publicación [24] de S. K. Sehgal. Posteriormente clasificamos el grupo de unidades de $\mathbb{Z}A$ con A un grupo abeliano finito, demostrando en el Teorema 2.14 que $U(\mathbb{Z}A) = \pm A \times F$, donde F es un grupo abeliano libre de rango finito. El rango de F en el teorema anterior se encuentra calculado de forma explícita en [23]. Incluso daremos estructura a las unidades de aumento uno de $\mathbb{Z}A$ mediante el resultado 2.18 que nos decía lo siguiente: Si A es un grupo abeliano finito entonces $U_1(\mathbb{Z}A) = A \times U_2(\mathbb{Z}A)$ donde $U_2(\mathbb{Z}A) = \{u \in U(\mathbb{Z}A) \ : \ u \equiv 1 \mod (\Delta A)^2\}$. Para terminar este capítulo del documento, hacemos mención a un resultado de [27] que es mucho más general y con el que se determina que si G es un grupo finito, entonces el grupo de unidades de $\mathbb{Z}G$ es un grupo finitamente generado.

El Capítulo 3 es el más importante de la memoria y se encuentra centrado en el estudio del Teorema de Higman 3.9. Para poder abordar la demostración, necesitamos en primer lugar estudiar el grupo de unidades de $\mathbb{Z}K_8$ ya que la demostración del teorema está muy relacionada con las unidades de $\mathbb{Z}K_8$, de hecho, llegamos incluso a demostrar que todas las unidades de $\mathbb{Z}K_8$ son triviales. También nos resultará de gran ayuda calcular $U(\mathbb{Z}[\zeta_3]) = \{\pm 1, \pm\zeta_3, \pm\zeta_3^2\}$ y $U(\mathbb{Z}[\zeta_4]) = \{\pm 1, \pm i\}$. Con todo esto, logramos demostrar el Teorema de Higman 3.9 que nos dice que si G es un grupo de torsión entonces todas las unidades de $\mathbb{Z}G$ son triviales si y solo si se verifica una de las siguientes condiciones:

1. G es un grupo abeliano de exponente igual a $1, 2, 3, 4, 6$.

2. G es un 2-grupo Hamiltoniano.

A continuación de este resultado, nos centraremos en la justificación de otro teorema que nos garantizará bajo que hipótesis el grupo de unidades de $\mathbb{Z}G$ es finito, lo obtendremos como consecuencia del Teorema de Higman. De hecho, demostraremos en el Teorema

3.10 que si G un grupo finito, entonces $U(\mathbb{Z}G)$ es un grupo finito si y solo si todas las unidades de $\mathbb{Z}G$ son triviales.

El último capítulo del documento se encuentra destinado a calcular el grupo de unidades de $\mathbb{Z}C_n$ para valores pequeños de $n \in \mathbb{N}$, donde C_n denota el grupo cíclico de orden n. Como consecuencia del Teorema de Higman, lograremos demostrar que $U(\mathbb{Z}C_n) = \pm C_n$ para $n = 1, 2, 3, 4, 6$. El objetivo de Capítulo 4 consiste en calcular $U(\mathbb{Z}C_8)$ y $U(\mathbb{Z}C_5)$. En un primer lugar, demostraremos que $U(\mathbb{Z}[\sqrt{2}]) = \langle -1 \rangle \times \langle 1+\sqrt{2} \rangle$ y que $U(\mathbb{Z}[\zeta_8]) = \langle \zeta_8 \rangle \times \langle 1 + \sqrt{2} \rangle = \langle \zeta_8 \rangle \times \langle \eta_3(\zeta_8) \rangle$. Estos dos grupos de unidades nos serán de gran ayuda para lograr demostrar en el Teorema 4.5, el cual afirma que $U(\mathbb{Z}C_8) = \pm C_8 \times \langle u_{3,2}(g) \rangle$ donde $C_8 = \langle g \rangle$. Como última etapa de este capítulo, abordamos el cálculo del grupo de unidades de $\mathbb{Z}C_5$. Para poder realizar este calculo, introducimos la notación $U_1(\mathbb{Z}[\zeta_p])$ para referirnos a un tipo especial de unidades de $\mathbb{Z}[\zeta_p]$ con p un número primo, más concretamente, a las unidades $y \in U(\mathbb{Z}[\zeta_p])$ tales que $y \equiv 1 \mod \zeta_p - 1$. Como resultados previos, demostraremos que $U_1(\mathbb{Z}C_p) \simeq U_1(\mathbb{Z}[\zeta_p])$ y que $[U(\mathbb{Z}[\zeta_p]) : U_1(\mathbb{Z}[\zeta_p])] = p - 1$. Finalmente, logramos demostrar en el Teorema 4.7 que si $C_5 = \langle x \rangle$ entonces $U(\mathbb{Z}C_5) = \langle -1, x, u \rangle$, donde $u = (x+1)^2 - \hat{x}$ y en este caso particular $\hat{x} = 1 + x + x^2 + x^3 + x^4$.

Con el fin de elaborar esta memoria correctamente, una buena parte de mi trabajo se encuentra obtenido de la siguiente bibliografía: [4, 17, 20, 22, 24]. Sin embargo, he profundizado más en las técnicas matemáticas empleadas en esta memoria utilizando material de un documento en preparación de Ángel del Río y Eric Jespers. Además, he asistido a los seminarios semanales de álgebra durante todo el curso académico, en los cuales participaban alumnos de doctorado y una amplia variedad de profesores de álgebra, a fin de complementar mi formación. También es importante mencionar, que me ha resultado muy útil la asignatura Álgebra No Conmutativa sobre todo en la fase de asimilación de conceptos relacionados con anillos de grupo. Por último, en la primera semana de junio asistí al congreso de álgebra que se celebró en la Facultad de Matemáticas de la Universidad de Murcia, teniendo como principales objetivos tanto conocer los últimos descubrimientos relacionados con mi trabajo como mi preparación para futuros proyectos.

Capítulo 1

Preliminares.

Vamos a introducir una serie de conceptos, propiedades y resultados que utilizaremos en el desarrollo del documento y que nos resultaran de vital importancia para el estudio de las unidades en anillos de grupo.

1.1. Notación general de grupos y anillos.

Sea R un anillo y sea G un grupo. Definimos el *grupo multiplicativo de las unidades de* R como el siguiente conjunto:

$$U(R) = \{x \in R \ : \ \text{existe algún } y \in R \text{ verificando que } \ xy = yx = 1\}$$

Si $x \in U(R)$ entonces diremos que x *es un elemento invertible o unidad en* R. Supongamos que $f : R \longrightarrow S$ es un homomorfismo de anillos. Entonces es claro que f se restringe a un homomorfismo de grupos $g : U(R) \longrightarrow U(S)$.

Sea $a \in G$ y consideramos n, $m \in \mathbb{Z}$. Definimos las *potencias de* a de la siguiente forma:

$$a^n = \begin{cases} a \cdot a \cdot \underbrace{\cdots}_{n \text{ veces}} \cdot a & \text{si } n > 0 \\ a^{-1} \cdot a^{-1} \cdot \underbrace{\cdots}_{|n| \text{ veces}} \cdot a^{-1} & \text{si } n < 0 \\ 1 & \text{si } n = 0 \end{cases}$$

Como $a^n \cdot a^m = a^{m+n}$ entonces $\langle a \rangle = \left\{a^k \ : \ k \in \mathbb{Z}\right\}$ es un subgrupo de G y lo llamaremos el *subgrupo cíclico de* G *generado por* a. En el caso en que G sea finito, al número de elementos de G lo llamaremos *orden de* G y lo denotaremos por $|G|$. Al menor entero positivo k tal que $a^k = 1$ lo llamaremos *orden de* a y lo vamos a denotar por $o(a)$ ó por $|a|$. Si $\langle a \rangle$ tiene infinitos elementos entonces diremos que a es un *elemento*

de orden infinito. En el caso en que $o(a) = n$, vamos a introducir la notación $\hat{a} = 1 + a + a^2 + \cdots + a^{n-1}$. Diremos que G es un *grupo cíclico*, si existe un elemento $a \in G$ tal que $G = \langle a \rangle$, además, diremos que a *es el generador de* G. Es claro que $o(a) = |\langle a \rangle|$ y que todo grupo cíclico es abeliano. Introducimos la notación $C_n = \langle a \ : \ a^n = 1 \rangle$ para referirnos al *grupo cíclico de orden* $n \in \mathbb{N}$ y C_∞ para referirnos a un *grupo cíclico infinito*. Un elemento $g \in G$ diremos que es un *elemento de torsión* si tiene orden finito y G es un *grupo de torsión* si todo elemento de G es un elemento de torsión. Por lo tanto, el conjunto formado por todos los elementos de torsión de G vendría dado por $\{g \in G \ : \ o(g) < \infty\}$. En el caso en que el único elemento de torsión de G sea el 1 diremos que G es un *grupo libre de torsión*.

Dado un conjunto X, un *grupo libre* en X es una aplicación $j : X \longrightarrow F$, donde F es un grupo, que cumple la siguiente propiedad: para cada aplicación $f : X \longrightarrow G$, con G un grupo, existe un único homomorfismo de grupos $\bar{f} : F \longrightarrow G$ verificando $\bar{f} \circ j = f$.

Sea p un número entero primo. Diremos que G es un *p-grupo* si todo elemento de G tiene orden una potencia de p. Un elemento de G diremos que es un *p-elemento* si su orden es una potencia p. Por lo tanto, si G es un p-grupo entonces todo elemento de G es un p-elemento. Un grupo abeliano se dice que es un *grupo abeliano libre* si es suma directa de grupos cíclicos infinitos. Si el número de sumandos directos es finito, entonces lo llamaremos el *rango* de G. En cualquier otro caso diremos que el grupo es de *rango infinito*. Además, un grupo abeliano diremos que es un *p-grupo abeliano elemental* si todo elemento distinto de la unidad tiene orden p. Definimos el *exponente de* G como el menor entero positivo m tal que $g^m = 1$ para todo $g \in G$, en el caso en que este número exista.

Introducimos la notación $H \leq G$ para referirnos a que H es un subgrupo de G. Se verifica que H es un *subgrupo normal* de G si y solo si para todo $g \in G$ se verifica que $g^{-1}Hg = H$. Además, diremos que $g \in G$ *normaliza a* H si y solo si $g^{-1}Hg \subseteq H$. Es obvio que si A es un grupo abeliano, entonces todo subgrupo de A es normal.

Definimos el *centralizador* de H en G como el subgrupo de G dado por

$$C_G(H) = \{x \in G \ : \ xh = hx \text{ para todo } h \in H\}$$

y vamos a denotar al *centro* de G como $Z(G) = C_G(G)$.

Por otro lado, al *grupo de los cuaterniones de orden 8* lo vamos a denotar de la siguiente forma:

$$K_8 = \langle a, b \ : \ a^4 = 1, \ a^2 = b^2, \ bab^{-1} = a^{-1} \rangle = \left\{1, a, a^2, a^3, b, ab, a^2b, ab^3\right\}$$

Una propiedad muy importante de K_8 es que $Z(K_8) = \langle a^2 \rangle = \{1, a^2\}$.

Sean $x, y \in G$, introducimos la notación x *conjugado por* y como $x^y = y^{-1}xy$.

Sea n un entero positivo y se K un cuerpo cuya característica no divide a n. Sea L la clausura algebraica de K. Definimos el *n-ésimo polinomio ciclotómico en K* como el polinomio mónico irreducible en $K[X]$ que se anula en ζ, donde ζ es una *raíz primitiva n-ésima de la unidad en L.* Además, es bien conocido que viene dado por la expresión:

$$\Phi_n(x) = \prod_{(i,n)=1} (x - \xi^i)$$

En particular, si n es un número primo p entonces se tiene que $\Phi_p(x) = x^{p-1} + x^{p-2} + \cdots + 1$.

Es bien conocido que si F es un cuerpo tal que $|F| = p$ entonces $F \simeq \mathbb{Z}_p$. Denotamos con $\mathbb{Z}_p$ *al cuerpo con p elementos.*

1.2. Grupos Hamiltonianos.

En este apartado vamos a definir los grupos Hamiltonianos y vamos a obtener su clasificación que luego utilizaremos con mucha frecuencia. Para ello introducimos las definiciones y unos lemas previos necesarios para la demostración más importante de esta sección.

En primer lugar, sabemos que K_8 es un grupo no abeliano y verifica que todos sus subgrupos son normales. Esto motiva el concepto de grupo Hamiltoniano. Diremos que un grupo no conmutativo G es un *grupo Hamiltoniano* si todos sus subgrupos son normales.

Definimos el *conmutador* de $x, y \in G$ como $(x, y) = x^{-1}y^{-1}xy \in G$. El conmutador de dos elementos de un grupo G verifica las siguientes propiedades:

Lema 1.1. *Sea G un grupo y sean x, y, $z \in G$. Entonces se verifica lo siguiente:*

1. $(x,y)=1$ *si y solo si* $xy=yx$.

2. $(x,y)^{-1}=(y,x)$.

3. $(xy,z)=(x,z)^y(y,z)=(x,z)((x,z),y)(y,z)$.

4. $(x,yz)=(x,z)(x,y)^z=(x,z)(x,y)((x,y),z)$.

Demostración. $(x,y)=1$ si y solo si $x^{-1}y^{-1}xy=1$ si y solo si $xy=(x^{-1}y^{-1})^{-1}=yx$. Lo que demuestra el primer apartado. El segundo se obtiene por lo siguiente: $(x,y)^{-1}=(x^{-1}y^{-1}xy)^{-1}=y^{-1}x^{-1}yx=(y,x)$.

Veamos la demostración del tercer apartado. Utilizando que $(x,z)^y=y^{-1}(x,z)y=y^{-1}x^{-1}z^{-1}xzy$ entonces deducimos lo siguiente:

$$(x,z)^y(y,z)=y^{-1}x^{-1}z^{-1}xzyy^{-1}z^{-1}yz=y^{-1}x^{-1}z^{-1}xyz=(xy,z)$$

Como $((x,z),y)=(x^{-1}z^{-1}xz,y)=z^{-1}x^{-1}zxy^{-1}x^{-1}z^{-1}xzy$ entonces se tiene que $(x,z)((x,z),y)(y,z)=x^{-1}z^{-1}xzz^{-1}x^{-1}zxy^{-1}x^{-1}z^{-1}xzyy^{-1}z^{-1}yz=y^{-1}x^{-1}z^{-1}xyz=(xy,z)$.

La demostración del apartado 4 es análoga a la del apartado 3, realizando cálculos sencillos la obtenemos de igual manera. □

Lema 1.2. *Sea* $H=\langle x,y\rangle$ *tal que* $(x,y)\in Z(H)$. *Entonces se verifica lo siguiente para* $r\in\mathbb{N}$*:*

1. $(x^r,y)=(x,y)^r=(x,y^r)$.

2. *Si* $r\geq 2$ *entonces* $(xy)^r=x^ry^r(y,x)^{\binom{r}{2}}$

Demostración. Para demostrar el primer apartado procedemos por inducción en $r\in\mathbb{N}$. Para $r=1$ es obvio. Supongamos cierto para $r-1$ con $r>1$ y vamos a demostrarlo para r. Utilizando el apartado 3 del Lema 1.1 y utilizando que $(x,y)\in Z(H)$ obtenemos que $(x^r,y)=(x,y)^{x^{r-1}}(x^{r-1},y)=x^{-(r-1)}(x,y)x^{r-1}(x,y)^{r-1}=(x,y)^r$. El caso $(x,y)^r=(x,y^r)$ es análogo utilizando el Lema 1.1 apartado 4.

Vamos a demostrar el segundo apartado. Procedemos otra vez por inducción en $r\in\mathbb{N}$. Supongamos que $r=2$. Aplicando que $(x,y)\in Z(H)$ tenemos que

$$x^2y^2(y,x)^{\binom{2}{2}}=x^2y^2(y,x)=x^2y(y,x)y=(xy)^2$$

Supongamos cierto $(xy)^n = x^n y^n (y,x)^{\binom{n}{2}}$ y vamos a demostrarlo para $n+1$. Se tiene que $(xy)^{n+1} = (xy)^n(xy) = x^n y^n (y,x)^{\binom{n}{2}}(xy) = x^n y^n xy (y,x)^{\binom{n}{2}}$. Como se verifica que

$$y^n x = xy^n y^{-n} x^{-1} y^n x = xy^n (y^n, x) = xy^n (y,x)^n$$

entonces si sustituimos en la expresión anterior obtenemos lo siguiente:

$$(xy)^{n+1} = x^n xy^n (y,x)^n y(y,x)^{\binom{n}{2}} = x^{n+1} y^{n+1} (y,x)^{\binom{n+1}{2}}$$

□

Lema 1.3. *Sea G un p-grupo abeliano finito y sea $g \in G$ un elemento de orden máximo. Entonces $\langle g \rangle$ es un sumando directo de G.*

Demostración. Tomamos

$$S = \{N \leq G \ : \ N \cap \langle g \rangle = \{1\}\}$$

Como G es un grupo finito entonces existe un subgrupo M de G maximal en S. Si probamos que $G = M\langle g \rangle$ entonces aplicando que $M \cap \langle g \rangle = \{1\}$ tendríamos que $G = M \times \langle g \rangle$. Por lo tanto vamos a demostrar que $G = M\langle g \rangle$.

Procedemos por reducción al absurdo. Supongamos que $G \neq M\langle g \rangle$. Tomamos $x \in G$ tal que $x \notin M\langle g \rangle$ y además vamos a suponer que x tiene orden mínimo entre los que satisfacen esta propiedad. Aplicando la fórmula para el grado de x

$$|x^p| = \frac{|x|}{mcd(p,|x|)} = \frac{|x|}{p}$$

deducimos que $o(x^p) < o(x)$ y como x tenía orden mínimo entonces tenemos que $x^p \in M\langle g \rangle$. Por lo tanto $x^p = yg^l$ con $y \in M$ y $l \in \mathbb{Z}$. Supongamos que $o(g) = p^n$. Entonces como g tiene orden máximo tendríamos que $x^{p^n} = 1$. Luego $1 = x^{p^n} = y^{p^{n-1}} \cdot g^{lp^{n-1}}$ y esto implica que

$$g^{lp^{n-1}} = \left(y^{p^{n-1}}\right)^{-1} \in M \cap \langle g \rangle = \{1\}$$

Por lo que tenemos $1 = g^{lp^{n-1}}$ de donde deducimos que $p|l$. Supongamos que $l = pl_1$. Obsérvese que $\left(xg^{-l_1}\right)^p = x^p g^{-l_1 p} = yg^l g^{-l_1 p} = y \in M$, pero como $x \notin M\langle g \rangle$ entonces tenemos que $xg^{-l_1} \notin M$. Debido a la maximalidad de M en S deducimos que

$\langle xg^{-l_1}\rangle \cap \langle g\rangle \neq 1$. Luego existe un elemento $y' \in M$ y enteros positivos u, k tales que $(xg^{-l_1})^u \cdot y' = g^k \neq 1$ por lo que $(xg^{-l_1})^u \in M\langle g\rangle$.

Vamos a distinguir dos casos. Supongamos en primer lugar que $p|u$ y tomamos $u = p\alpha$. Entonces $(xg^{-l_1})^u = (xg^{-l_1})^{p\alpha} = (x^p g^{-l_1 p})^\alpha = (yg^l g^{-l_1 p})^\alpha = y^\alpha \in M$. Luego $y^\alpha y' = g^k \neq 1$. Entonces $g^k \in M$, de donde obtenemos que $g^k \in M \cap \langle g\rangle = \{1\}$. Contradicción. Supongamos ahora que $p \nmid u$. Entonces existen enteros positivos r, s tales que $1 = rp + su$. Ponemos $x = x^{rp+su} = x^{rp} \cdot x^{su}$. Como $o(x^{rp}) < o(x)$ y $x^p \in M\langle g\rangle$ entonces $x^{rp} \in M\langle g\rangle$. Aplicando además que $x^u \in M\langle g\rangle$ deducimos que $x \in M\langle g\rangle$. Contradicción. □

Lema 1.4. *Sea G un grupo Hamiltoniano. Entonces G contiene un subgrupo isomorfo a K_8.*

Demostración. Sean $x, y \in G$ tales que $(x, y) = c \neq 1$. Utilizando la primera propiedad del Lema 1.1 deducimos que x e y no conmutan. Aplicando que G es un grupo Hamiltoniano obtenemos que $\langle x\rangle$ y $\langle y\rangle$ son subgrupos normales de G. Entonces $c \in \langle x\rangle$ y $c \in \langle y\rangle$. Luego $c \in \langle x\rangle \cap \langle y\rangle$. Por lo tanto existen enteros positivos r y s tales que $c = (x, y) = x^r = y^s$.

Tomamos $H = \langle x, y\rangle = \langle x\rangle\langle y\rangle$. Entonces $c \in Z(H)$. Utilizando la propiedad 1 del Lema 1.2 obtenemos que $c^r = (x, y)^r = (x^r, y) = (c, y) = 1$. Luego deducimos que $o(c) < \infty$. Entonces se tiene que $o(x) < \infty$ y que $o(y) < \infty$. Aplicando que los ordenes de x, y, c son finitos junto con que $c \in Z(H)$ deducimos que $|H| < \infty$. Tomamos $o(x) = m$ y $o(y) = n$. Supongamos que hemos tomado x e y de tal forma que $m + n$ sea lo menor posible. Sea p un número primo que divide a m. Utilizando la fórmula del grado para x^p obtenemos que $o(x^p) = \frac{m}{p}$. Entonces por la elección mínima de $m + n$ deducimos que x^p e y conmutan. Luego $1 = (x^p, y) = (x, y)^p = c^p$, lo que implica que $o(c) = p$. Como acabamos de probar que para cualquier primo p que divida a m se tiene que $o(c) = p$ y además $c = x^r = y^s$ entonces deducimos que $o(x)$ y $o(y)$ son una potencia de p.

Supongamos que $r = kp^{r_1}$ y que $s = lp^{s_1}$ con $mcd(p, k) = mcd(p, l) = 1$. Luego $c = x^{kp^{r_1}} = y^{lp^{s_1}}$. Es bien conocido que podemos encontrar enteros k' y l' tales que $kk' \equiv 1 \mod o(x)$ y $ll' \equiv 1 \mod o(y)$. Denotamos por $x' = x^{l'}$ e $y' = y^{k'}$. Por un lado, utilizando el apartado 1 del Lema 1.2, se verifica que $(x', y') = (x^{l'}, y^{k'}) = (x, y)^{l'k'} = c^{k'l'}$. Por otro lado, como $(x')^{p^{r_1}} = x^{l' p^{r_1}} = (x^{p^{r_1}})^{l'}$ entonces $c^{k'} = (x^{kp^{r_1}})^{k'} = x^{p^{r_1}}$. Por

lo tanto $(x')^{p^{r_1}} = x^{p^{r_1}} = c^{k'l'}$. Luego hemos demostrado que $(x')^{p^{r_1}} = (x', y')$. Llamamos $c' = (x', y')$. Con un razonamiento análogo al anterior obtenemos que $c' = (y')^{p^{s_1}}$. Luego $c' = (x')^{p^{r_1}} = (y')^{p^{s_1}}$. Como $o(c') = p$ entonces $(c')^p = \left((x')^{p^{r_1}}\right)^p = \left((y')^{p^{s_1}}\right)^p = 1$. Por lo tanto $o(x') = p^{r_1+1}$ y $o(y') = p^{s_1+1}$. Podemos suponer para evitar complicación en la notación que $x = x'$ y que $y = y'$. Además sin pérdida de generalidad vamos a suponer que $r_1 \geq s_1$.

Tomamos $y_1 = x^{-p^{r_1-s_1}} \cdot y \in H$. Entonces aplicando el Lema 1.1 junto con que x^p e y conmutan obtenemos que $(x, y_1) = (x, x^{-p^{r_1-s_1}} \cdot y) = (x, y) \cdot (x, x^{-p^{r_1-s_1}})^y = (x, y) = c \neq 1$. Luego x e y_1 no conmutan. Como hemos tomado $m + n$ mínimo entonces se verifica que $o(y_1) \geq o(y) = p^{s_1+1}$, luego $y_1^{p^{s_1}} \neq 1$. Pero por otro lado obtenemos al aplicar el Lema 1.2 apartado 2 lo siguiente:

$$y_1^{p^{s_1}} = \left(x^{-p^{r_1-s_1}} y\right)^{p^{s_1}} = x^{-p^{r_1}} y^{p^{s_1}} (y, x^{-p^{r_1-s_1}})^{\binom{p^{s_1}}{2}} = (x, y)^{p^{r_1-s_1} \cdot \binom{p^{s_1}}{2}} = c^{\frac{p^{r_1} \cdot (p^{s_1}-1)}{2}}$$

Si suponemos que p sea un número primo impar entonces $p^{s_1} - 1$ sería par. Por lo tanto aplicando que $p | \frac{p^{r_1} \cdot (p^{s_1}-1)}{2}$ y que $o(c) = p$ deducimos que $o(c) | \frac{p^{r_1} \cdot (p^{s_1}-1)}{2}$. Luego $y_1^{p^{s_1}} = 1$. Contradicción.

Entonces la única posibilidad sería $p = 2$ y $r_1 = 1$ porque en caso contrario obtendríamos $y_1^{p^{s_1}} = 1$. Como estamos suponiendo que $r_1 \geq s_1$ entonces tenemos que $s_1 = 1$. Luego $o(x) = o(y) = 4$. Esto implica que $x^4 = 1$, $c = x^2 = y^2$ y por lo tanto también implica que $x^{-1} = y^{-1}xy$. Luego $K = \langle x, y \rangle$ es isomorfo a K_8. □

1.2.1. Clasificación de los grupos Hamiltonianos.

En el siguiente teorema se clasifican los grupos Hamiltonianos. Nos resultará de gran ayuda en el trascurso del documento.

Teorema 1.5. *Un grupo G es Hamiltoniano si y solo si $G = K_8 \times E \times A$ donde K_8 es el grupo de los cuaterniones de orden 8, E es un 2-grupo abeliano elemental y A es un grupo abeliano con todos los elementos de orden impar.*

Demostración. Supongamos que $G = K_8 \times E \times A$. Para ver que G es un grupo Hamiltoniano es suficiente con probar que para cada $g \in G$ se verifica que $\langle g \rangle$ es un subgrupo normal de G. Supongamos que $g \in G$. Entonces $g = xab$ con $x \in K_8$, $a \in A$ y $b \in E$. Supongamos además que $a \neq 1$ y que $b \neq 1$.

Si $o(x) = 2$ entonces x es central, luego g es central y por lo tanto $\langle g \rangle$ es normal. Con lo que terminaríamos la demostración. En caso contrario tendríamos que $o(x) = 4$. Entonces la clase de conjugación de x es $C(x) = \{x, x^{-1}\}$ y la clase de conjugación de g es $C(g) = \{g, x^{-1}ab\}$.

Vamos a demostrar que $x^{-1}ab \in \langle g \rangle$. Como $a \in A$ entonces $o(a)$ es impar. Tomamos $s = 2o(a) + 1$. Como $o(a) - 1 > 0$ y $2 \cdot (o(a) - 1) \equiv 0 \mod 4$ entonces se tiene que $s \equiv 3 \mod 4$. Veamos que $g^s = x^{-1}ab$. Por un lado tenemos que como $o(x) = 4$ y como $s \equiv 3 \mod 4$ entonces $x^s = x^{-1}$. Por otro lado tenemos que como $s \equiv 1 \mod o(a)$ entonces $a^s = a$. Finalmente como $o(b)$ es par y s es impar entonces $b^s = b$. Luego hemos conseguido demostrar que $g^s = x^s a^s b^s = x^{-1}ab$. Esto implica que $x^{-1}ab \in \langle g \rangle$. Luego $C(g) \subseteq \langle g \rangle$ y por lo tanto se verifica que $\langle g \rangle$ es un subgrupo normal de G. Con lo que termina esta parte de la demostración.

Veamos ahora la otra implicación. Supongamos que G es un grupo Hamiltoniano, entonces utilizando el Lema 1.2 sabemos que contiene un subgrupo K isomorfo a K_8. Entonces $K = \langle x, y \rangle$ con x e y satisfaciendo $x^4 = 1$, $x^2 = y^2$ y $x^{-1} = yxy^{-1}$.

Vamos a demostrar que $G = KC_G(K)$. Procedemos por reducción al absurdo. Supongamos que existe un $g \in G$ tal que $g \notin KC_G(K)$. Entonces g no conmuta con x o g no conmuta con y . Sin pérdida de generalidad podemos suponer que g no conmuta con y. Como $y^g \in \langle y \rangle$ entonces tenemos que $y^g = y^3 = y^{-1}$. Además se tiene que $ygx = gy^g x = gy^3 x = gxy$. Por tanto gx conmuta con y. Como $gx \notin C_G(K)$ y $K = \langle x, y \rangle$ entonces deducimos que gx no conmuta con x. Luego $x^{gx} = x^{-1}$. Entonces como $x^{gxy} = (x^{gx})^y = (x^{-1})^y = x$ y $y^{gxy} = y^y = y$ obtenemos que $gxy \in C_G(K)$. Como $xy \in K$ entonces deducimos que $g \in KC_G(K)$ en contradicción con la hipótesis.

Veamos ahora que G es un grupo de torsión. Como ya tenemos demostrado que $G = KC_G(K)$, entonces aplicando que los elementos de K y de $C_G(K)$ conmutan junto con que K es un grupo de torsión deducimos que para que G sea de torsión lo único que tenemos que demostrar es que $C_G(K)$ es de torsión. Sea $g \in C_G(K)$. Entonces aplicando el Lema 1.1 apartado 3 obtenemos que $(x, gy) = (x, y) \cdot (x, g)^y$. Como $g \in C_G(K)$ entonces $(x, g) = 1$ y por lo tanto $(x, gy) = (x, y) = x^2 \neq 1$. Como G es Hamiltoniano entonces $\langle x \rangle$ y $\langle gy \rangle$ son subgrupos normales de G. Por lo que $(x, gy) \in \langle x \rangle$ y $(x, gy) \in \langle gy \rangle$, entonces se tiene que $(x, gy) \in \langle x \rangle \cap \langle gy \rangle$. Por lo tanto existen enteros r y s tales que $(x, gy) = x^r = (gy)^s$. Tomamos $H = \langle x, gy \rangle = \langle x \rangle \langle gy \rangle$. Luego se tiene

que $(x, gy) \in Z(H)$. Por lo tanto deducimos que $(x, gy)^r = (x^r, gy) = ((x, gy), gy) = 1$, luego $o((x, gy)) < \infty$ y $o(gy) < \infty$. Entonces $o(g) < \infty$.

Veamos que $C_G(K)$ no contiene elementos de orden 4. Procedemos por reducción al absurdo. Supongamos que existe $g \in C_G(K)$ con orden 4. Por lo demostrado anteriormente sabemos que $(x, gy) = (x, y) = x^2 \neq 1$. Como G es un grupo Hamiltoniano, todos sus subgrupos son normales y todo elemento de orden 2 es central, entonces como g tiene orden 4 deducimos que $o(gy) = 4$. Por lo tanto tenemos que como $(x, gy) \neq 1$ y $o(gy) = 4$ entonces $(gy)^x = (gy)^{-1}$. Además $(gy, x) = (gy)^{-1} \cdot (gy)^x = g^{-2}y^{-2}$. Como $(gy, x) = (y, x) = (x, y)^{-1} = x^2 = y^2$, entonces tenemos que $g^2y^2 = y^2$ y por lo tanto $g^2 = 1$. Contradicción.

A continuación vamos a demostrar que todos lo elementos de orden impar en G son centrales. Procedemos por reducción al absurdo. Supongamos que existe un elemento $a \in G$ tal que $a \notin Z(G)$ y $|a|$ impar. Sea $b \in G$ talque $ab \neq ba$. Consideramos el grupo Hamiltoniano $H = \langle a, b \rangle$. Tomamos la proyección canónica

$$f : H \longrightarrow H/\langle a \rangle$$

Es claro que $ker(f) = \langle a \rangle$ y que $H/\langle a \rangle$ es cíclico, por tanto abeliano. Como H es un grupo Hamiltoniano, utilizando el Lema 1.4 sabemos que H contiene un subgrupo K isomorfo a K_8. Como $K \cap \langle a \rangle = \{1\}$ entonces la restricción de f a K es una aplicación inyectiva. Contradicción porque $H/\langle a \rangle$ es abeliano pero K no.

Como ya hemos demostrado que no hay elementos de orden 4 en $C_G(K)$, entonces si $h \in C_G(K)$ es un 2-elemento, eso implica que es central porque como máximo tiene orden 2. Por lo tanto $C_G(K) \subseteq Z(G)$, $C_G(K)$ es un grupo abeliano y el conjunto de los 2-elementos de $C_G(K)$ es un 2-grupo abeliano elemental. Lo llamaremos B. Consideramos A el subgrupo de G formado por todos los elementos de orden impar en G. Cómo A es central en G entonces $C_G(K) = B \times A$. Como x^2 tiene orden 2 entonces es central y además $x^2 \in B$. Aplicando que x^2 tiene orden máximo en B, podemos utilizar el Lema 1.3 y obtenemos que $B = \langle x^2 \rangle \times E$ donde E es un 2-grupo abeliano elemental.

Aplicando que el único elemento de orden 2 en K_8 es x^2, que $K_8 \cap (E \times A) = \{1\}$ y que $E \times A$ es central tenemos lo siguiente:

$$G = KC_G(K) = K_8(B \times A) = K_8\left(\langle x^2 \rangle \times E \times A\right) = K_8 \times E \times A$$

□

1.3. Anillos semisimples.

Sea R un anillo. Diremos que R es un *anillo de división* si todo elemento no nulo de R es invertible en R.

Un grupo abeliano y aditivo M diremos que es un *R-módulo por la izquierda* si para cada elemento $a \in R$ y para cada $m \in M$ tenemos un producto $am \in M$ tal que se verifican las siguientes propiedades para todo $a, b \in R$ y $m_1, m_2 \in M$: $(a+b)m = am + bm$, $a(m_1 + m_2) = am_1 + am_2$, $a(bm) = (ab)m$ y $1m = m$. Con un proceso similar podemos definir los *R-módulos por la derecha* considerando la multiplicación de elementos de M por elementos de R por el lado derecho. Un subconjunto no vacío $N \subset M$ diremos que es un *R-submódulo* de M si se verifican las dos propiedades siguientes: para todo $x, y \in N$ se tiene que $x + y \in N$, y para todo $r \in R$ y todo $n \in \mathbb{N}$ se tiene que $rn \in N$.

Supongamos que M y N son dos R-módulos por la izquierda. Entonces definimos un *homomorfismo de R-módulos por la izquierda* como una función $f : M \longrightarrow N$ que verifica lo siguiente: para cualquier m, $n \in M$ y cualquier r, $s \in R$ se tiene que $f(rm + sn) = rf(m) + sf(n)$. La definición de homomorfismo de R-módulos por la derecha sería análoga, considerando la multiplicación de elementos de M por elementos de R por el lado derecho.

Diremos que un R-módulo P es *proyectivo* si y solo si para cualquier homomorfismo de R-módulos suprayectivo $f : M \longrightarrow N$ existe un homomorfismo de R-módulos $h : P \longrightarrow M$ tal que $fh = I_P$.

En el caso en que R fuera un anillo conmutativo, un R-módulo A diremos que es una *R-álgegra* si hay una multiplicación definida en A tal que juntando esa multiplicación con la suma de A dotamos a A de estructura de anillo y además se verifica para todo $r \in R$ y para todo $a, b \in A$ la siguiente propiedad: $r \cdot (ab) = (ra) \cdot b = a \cdot (rb)$.

Diremos que un *R-módulo M es semisimple* si todo submódulo de M es un sumando directo de M. Además, *R es semisimple* si visto como R-módulo es semisimple.

Los anillos semisimples están caracterizados por el Teorema de Wedderburn-Artin.

Teorema 1.6. *Teorema de Wedderburn-Artin.*

Un anillo R es semisimple si y solo si es suma directa de álgebras de matrices sobre

anillos de división:

$$R \simeq M_{n_1}(D_1) \oplus M_{n_2}(D_2) \oplus \cdots \oplus M_{n_s}(D_s)$$

1.4. Introducción a los anillos de grupo.

En esta sección vamos a dar unas nociones generales de los anillos de grupo junto con sus propiedades más importantes. Comenzamos con unas nociones básicas.

Sea G un grupo y R un anillo. Denotaremos por RG al conjunto de todas las combinaciones R-lineales de elementos de G. Las operaciones de R y de G inducen de forma natural una suma y un producto en RG, dotando a RG de estructura de anillo, llamado el *anillo de grupo de G con coeficientes en R.*

Vamos a precisar este concepto. Cada elemento a en RG tiene una única expresión de la forma $\sum_{g\in G} a_g g$ donde $a_g \in R$ para todo elemento $g \in G$, y $a_g = 0$ para casi todo elemento $g \in G$. Por lo tanto RG es el anillo cuyo conjunto subyacente es

$$RG = \left\{ \alpha = \sum_{g\in G} a_g g \quad : \quad a_g \in R \ \text{ para todo } g \in G \ \text{ y } \ a_g = 0 \ \text{ para casi todo } g \in G \right\}$$

y la suma y la multiplicación en RG vienen dadas por las siguientes fórmulas:

$$\sum_{g\in G} a_g g + \sum_{g\in G} b_g g = \sum_{g\in G} (a_g + b_g) \cdot g$$

$$\left(\sum_{g\in G} a_g g\right) \cdot \left(\sum_{g\in G} b_g g\right) = \sum_{g,h\in G} a_g b_h gh = \sum_{g\in G} \sum_{h\in G} (a_h b_{h^{-1}g}) \cdot g.$$

Sea $\alpha \in RG$, vamos a denotar por a_g el *coeficiente en R de g*, por lo que $\alpha = \sum_{g\in G} a_g g$. El *soporte* de un elemento $\alpha = \sum_{g\in G} a_g g \ \in RG$ es el conjunto finito $supp(\alpha) = \{g \in G \ : \ a_g \neq 0\}$.

Consideramos R y G como subconjuntos de RG identificando $r \in R$ con $r1_G$ y $g \in G$ con $1_R g$. Denotamos por $i \ : \ G \longrightarrow RG$ y $v \ : \ R \to RG$ las aplicaciones de inclusión de forma que R es un subanillo de RG y G es un subgrupo del grupo de unidades de RG.

Sea A un anillo. Dado un homomorfismo de anillos $f : \ R \longrightarrow A$ y un homomorfismo de grupos $h : \ G \longrightarrow U(A)$ tales que $f(r)h(g) = h(g)f(r)$ para todo $r \in R$ y $g \in G$, es

bien conocido que existe un único homomorfismo de anillos $w: RG \longrightarrow A$ que extiende a f y a h. Ésta propiedad se conoce con el nombre de la *Propiedad Universal de los Anillos de Grupo*.

Denotamos al conjunto de todas las *unidades de torsión de* RG como $TU(RG)$. Definimos la *aplicación de aumento* del anillo de grupo RG como el homomorfismo de anillos $\epsilon: RG \to R$ dado por $\epsilon(\sum_{g\in G} a_g g) = \sum_{g\in G} a_g$ y denotaremos su núcleo como

$$\Delta(G) = ker(\epsilon) = \{\alpha \in RG \text{ tales que } \epsilon(\alpha) = 0\}.$$

Además se verifica que $\{g-1 \ : \ g \in G,\ g \neq 1\}$ es una base de $\Delta(G)$ como R-módulo por la izquierda y por la derecha por lo tanto tenemos que:

$$\Delta(G) = \left\{ \sum_{g\in G-\{1\}} a_g(g-1) \ : \ a_g \in R \right\}$$

A continuación enunciamos la caracterización de los anillos de grupo semisimples y el Teorema de Perlis-Walker.

Teorema 1.7. *Teorema de Maschke.*

Sea R un anillo y sea G un grupo. RG es semisimple si y solo si R es semisimple, G es finito y $|G| \cdot 1_R \in U(R)$.

Corolario 1.8. *Sea K un cuerpo y sea G un grupo finito. Entonces KG es semisimple si y solo si $\mid G \mid < \infty$ y $char(K)$ no divide a $|G|$.*

Demostración. Es consecuencia inmediata del Teorema de Maschke. □

La prueba del siguiente resultado se sale del objetivo de este trabajo y por lo tanto hacemos referencia a [19].

Teorema 1.9. *Teorema de Perlis-Walker.*

Sea G un grupo abeliano finito con orden n y sea K un cuerpo tal que $char(K) \nmid n$. Entonces $KG \simeq \oplus_{d|n} a_d K(\zeta_d)$ donde ζ_d denota una raíz primitiva de la unidad de orden d y $a_d = \frac{n_d}{[K(\zeta_d):K]}$. En esta fórmula, n_d representa el número de elementos de orden d en G.

Corolario 1.10. *Sea G un grupo y consideramos $g \in G$ con $o(g) = n < \infty$. Entonces se verifica que $\mathbb{Q}\langle g\rangle \simeq \oplus_{d|n}\mathbb{Q}(\zeta_d)$ donde ζ_d es una raíz d-ésima primitiva de la unidad en $\mathbb{C}$.*

Demostración. Es consecuencia del Teorema de Perlis-Walker. □

1.5. Anillos de enteros algebraicos.

Esta sección se encuentra destinada a enunciar el Teorema de las Unidades de Dirichlet y a definir las unidades ciclotómicas.

En primer lugar vamos a considerar K una *extensión finita* de $\mathbb{Q}$. Diremos que un elemento $\alpha \in K$ *es algebraico* sobre $\mathbb{Q}$ si existen $a_i \in \mathbb{Q}$ tales que $\alpha^n + a_{n-1}\cdot\alpha^{n-1} + \cdots + a_0 = 0$. Un elemento $\beta \in K$ diremos que es un *entero algebraico* si satisface una ecuación mónica en $\mathbb{Z}[X]$, es decir, si existen $b_i \in \mathbb{Z}$ tales que $\beta^n + b_{n-1}\cdot\beta^{n-1} + \cdots + b_0 = 0$. Además es bien conocido que el conjunto de todos los enteros algebraicos de K forman un anillo que lo denotaremos por $\mathcal{O}_K$ y lo llamaremos el *anillo de los enteros algebraicos de K.*

Procedemos al enunciado del Teorema de las Unidades de Dirichlet, la demostración se sale de lo que buscamos en este documento por lo que hacemos referencia a [7].

Teorema 1.11. *Teorema de las Unidades de Dirichlet.*

Sea K una extensión finita de $\mathbb{Q}$. Sea s el número de inclusiones reales de K y $2t$ el número de inclusiones complejas de K que no están incluidas en los reales. Entonces $U(\mathcal{O}_K) = C \times F$ es un grupo abeliano finitamente generado, donde C es un grupo cíclico finito y F es un grupo abeliano libre de torsión de rango $s + t - 1$.

De acuerdo con el Teorema de las Unidades de Dirichlet 1.11 tenemos que

$$U(\mathcal{O}_K) = C \times F = C \times \langle u_1\rangle \times \langle u_2\rangle \times \cdots \times \langle u_\rho\rangle$$

donde $\{u_1, u_2, \cdots, u_\rho\}$ es un *sistema fundamental de unidades*.

Vamos a introducir el concepto de unidad ciclotómica. Sea ζ una raíz compleja de la unidad de orden $n > 1$ y consideramos el subanillo $R = \mathbb{Z}[\zeta]$ de $\mathbb{C}$ generado por ζ. Para todo entero positivo k tomamos

$$\eta_k(\zeta) = \frac{\zeta^k - 1}{\zeta - 1} = 1 + \zeta + \zeta^2 + \cdots + \zeta^{k-1} \in R.$$

Si además se tiene que k es coprimo con n entonces k tiene un inverso l módulo n, es decir, $kl \equiv 1 \mod n$. En este caso tendríamos que

$$\eta_k(\zeta)^{-1} = \frac{\zeta - 1}{\zeta^k - 1} = \frac{\zeta^{kl} - 1}{\zeta^k - 1} = 1 + \zeta^k + \zeta^{2k} + \cdots + \zeta^{(l-1)k} \in R$$

Por lo tanto $\eta_k(\zeta) \in U(\mathbb{Z}[\zeta])$ y si $kl \equiv 1 \mod n$ entonces $\eta_k(\zeta)^{-1} = \eta_l(\zeta^k)$. Las unidades de la forma $\eta_k(\zeta)$ las llamaremos *unidades ciclotómicas.*

La prueba del siguiente resultado se sale del objetivo de este trabajo por lo que hacemos referencia a [26].

Teorema 1.12. *Sea K una extensión finita de $\mathbb{Q}$. Entonces las unidades ciclotómicas generan un subgrupo de índice finito en $U(\mathcal{O}_K)$.*

1.6. Órdenes.

Vamos a introducir el concepto de orden junto con algún ejemplo ilustrativo y posteriormente demostraremos algunas de sus propiedades más importantes. Se realiza este estudio sobre órdenes porque en futuras demostraciones aparecerá este concepto y necesitaremos aplicarlo sobre todo como herramienta auxiliar en algunas pruebas.

Sea A una $\mathbb{Q}$-álgebra. Un subanillo R de A diremos que es un *orden* en A si R es finitamente generado como $\mathbb{Z}$-módulo y además $\mathbb{Q}R = A$, es decir, A como espacio vectorial sobre $\mathbb{Q}$ está generado por R.

Ejemplo 1.13. Si G es un grupo finito entonces $\mathbb{Z}G$ es un orden en $\mathbb{Q}G$.

Ejemplo 1.14. Si K es una extensión finita sobre $\mathbb{Q}$ entonces $\mathcal{O}_K$ es un orden en K.

Veamos las propiedades más importantes de los órdenes que utilizaremos en el estudio de las unidades en anillos de grupo.

Lema 1.15. *Sean $R_1 \subset R_2$ dos órdenes en una $\mathbb{Q}$-álgebra A. Entonces existe un entero $d \neq 0$ tal que $dR_2 \subset R_1$. Además, el índice de grupos aditivos $[R_1 : dR_2]$ es finito.*

Demostración. Como R_2 es un orden en A entonces R_2 es finitamente generado como $\mathbb{Z}$-módulo. Sea $\{\gamma_1, \gamma_2, \ldots, \gamma_t\}$ un conjunto de generadores de R_2 considerado como $\mathbb{Z}$-módulo. Como R_1 también es un orden en A entonces A visto como espacio vectorial

sobre $\mathbb{Q}$ esta generado por R_1, es decir, $A = \mathbb{Q}R_1$. Entonces existe un número entero $d \neq 0$ tal que $d\gamma_i \in R_1$ para todo $i = 1, 2, \ldots, t$. Por lo tanto tenemos que $dR_2 \subset R_1$.

Veamos que $[R_1 \ : \ dR_2]$ es finito. Como R_2 es un orden en A entonces R_2 es un grupo abeliano aditivo y finitamente generado por lo que utilizando el teorema fundamental de los grupos abelianos sabemos que R_2 es producto de un número finito de subgrupos cíclicos, luego el índice aditivo $[R_2 \ : \ dR_2]$ es finito. Aplicando que $R_1 \subset R_2$ y que $dR_2 \subset R_1$ obtenemos lo siguiente:

$$[R_1 \ : \ dR_2] \leq [R_2 \ : \ dR_2] < \infty$$

□

Lema 1.16. *Sean R_1 y R_2 dos órdenes en una $\mathbb{Q}$-álgebra A tales que $R_1 \subset R_2$. Entonces se tiene que $(U(R_2) \ : \ U(R_1))$ es finito.*

Demostración. Utilizando el Lema 1.15 sabemos que existe un entero d tal que $dR_2 \subset R_1$ y además el índice de grupos aditivos $[R_1 \ : \ dR_2]$ es finito.

Vamos a probar que $(U(R_2) \ : \ U(R_1)) \leq [R_1 \ : \ dR_2]$. Tomamos $x, y \in U(R_2)$ tales que $x + dR_2 = y + dR_2$. Entonces $y^{-1}x + dR_2 = 1 + dR_2$ y por lo tanto $y^{-1}x - 1 \in dR_2 \subset R_1$. Luego $y^{-1}x \in R_1$. Razonando de forma análoga obtenemos que $x^{-1}y \in R_1$. Por lo que $y^{-1}x \in U(R_1)$ con $(y^{-1}x)^{-1} = x^{-1}y$. Como $y^{-1}x \in U(R_1)$ entonces se tiene que $x \in yU(R_1)$.

Con este argumento hemos probado que si dos unidades de R_2 pertenecen a la misma clase aditiva de R_1 módulo dR_2 entonces esas dos unidades también pertenecen a la misma clase multiplicativa de $U(R_2)$ módulo $U(R_1)$. Por lo tanto, si $x_1, \ x_2, \ \ldots, \ x_k$ son elementos de $U(R_2)$ que no son congruentes multiplicativamente módulo $U(R_1)$, entonces no son congruentes aditivamente módulo dR_2. Luego $(U(R_2) \ : \ U(R_1)) \leq [R_1 \ : \ dR_2]$. □

Proposición 1.17. *Sean R_1 y R_2 dos órdenes en una $\mathbb{Q}$-álgebra A tales que $R_1 \subset R_2$. Sea $u \in R_1$. Si u es invertible en R_2 entonces $u^{-1} \in R_1$.*

Demostración. Como por hipótesis tenemos que $u \in R_1$ es invertible en R_2, entonces se tiene que $R_2 = uR_2$. Si consideramos los grupos aditivos asociados a R_1 y a R_2 obtenemos que

$$[R_2 \ : \ uR_1] = [uR_2 \ : \ uR_1].$$

Tomamos $r_1 \in R_1$ y $r_2 \in R_2$. Como $r_2 \equiv r_1 \mod R_1$ si y solo si $ur_2 \equiv ur_1 \mod uR_1$ entonces se tiene que $[uR_2 : uR_1] = [R_2 : R_1]$. Por lo tanto tenemos que $[R_2 : uR_1] = [R_2 : R_1]$. Luego $uR_1 = R_1$. Esto implica que $u^{-1} \in R_1$. □

1.7. Representaciones y caracteres.

Sea F un cuerpo con característica $p \geq 0$ y sea A una F-álgebra. Una *representación* de A es un homomorfismo de F-álgebras $A \longrightarrow M_n(F)$ donde n es un número entero positivo y lo llamaremos el *grado de la representación*. Dos F-representaciones ρ y ρ' de A diremos que son equivalentes si tienen el mismo grado, pongamos n, y además existe $U \in GL_n(F)$ tal que $U\rho(a) = \rho'(a)U$, para todo $a \in A$.

Es bien conocido que existe una correspondencia biyectiva entre clases de equivalencia de representaciones de A y clases de isomorfía de A-módulos por la izquierda de dimensión finita sobre F. Supongamos que M es un A-módulo por la izquierda de dimensión finita sobre F. Entonces la aplicación

$$\begin{array}{rccc} p: & A & \longrightarrow & End_F(M) \\ & a & \mapsto & \rho_a \end{array}$$

dada por $\rho_a(m) = am$ para cada $a \in A$ y $m \in M$, es un homomorfismo de F-álgebras. Para cada F-base B de M y para cada $a \in A$ consideramos $\rho_B(a)$ la matriz asociada a ρ_a respecto de la base B. Entonces ρ_B es una representación de A de grado $dim_F(A)$ y la llamaremos la *representación de A asociada a M respecto de la base B.*

Sea G un grupo. Una *F-representación de G* es un homomorfismo de grupos $\rho : G \longrightarrow GL_n(F)$. Al número entero positivo n lo llamaremos el *grado de la representación*. Dos F-representaciones ρ y ρ' de G diremos que son *equivalentes* si tienen el mismo grado, pongamos n, y además existe una matriz $U \in GL_n(F)$ tal que $U\rho(g) = \rho'(g)U$ para todo $g \in G$. Vamos a establecer a continuación una conexión entre álgebras de grupo y representaciones de grupos. Una F-representación ρ de G de grado n se extiende de forma única a un homomorfismo de F-álgebras $\overline{\rho} : FG \longrightarrow M_n(F)$. Además, si ρ' es otra representación de G entonces se tiene que ρ y ρ' son equivalentes si y solo si $\overline{\rho}$ y $\overline{\rho'}$ son equivalentes. De esta forma deducimos que una F-representación de G y una representación de FG definen la misma noción matemática. En lo sucesivo, denotaremos

a $\overline{\rho}$ simplemente por ρ. Por lo tanto, vamos a identificar clases de equivalencia de F-representaciones de G con clases de isomorfía de FG-módulos de dimensión finita sobre F.

En el caso en que G sea un grupo finito, definimos la *representación regular de G* por la izquierda como la F-representación de FG considerado como FG-módulo por la izquierda. Sea ρ una F-representación de G. Definimos el *carácter asociado a ρ* como la aplicación $\chi : G \longrightarrow F$ dada por $\chi(g) = tr(\rho(g))$, donde $tr(\rho(g))$ representa la *traza* de la matriz $\rho(g)$.

Un F-carácter de G es el carácter asociado a una F-representación de G. En términos de FG-módulos, si M es un FG-módulo entonces el carácter asociado a M es el carácter asociado a su representación respecto de cualquier base elegida. Por lo tanto, el carácter χ asociado a ρ es el mismo que el carácter del FG-módulo M asociado a ρ.

Proposición 1.18. *Sea G un grupo finito y F un cuerpo con característica $p \geq 0$. Sea χ el carácter asociado a la F-representación regular ρ de G. Entonces se verifica que:*

$$\chi\left(\sum_{g\in G} a_g g\right) = |G| a_{1_G}$$

donde $a_g \in F$ para todo $g \in G$.

Demostración. Consideramos G como base de FG. Entonces se tiene lo siguiente: $\chi\left(\sum_{g\in G} a_g g\right) = tr\left(\rho\left(\sum_{g\in G} a_g g\right)\right) = tr\left(\sum_{g\in G} a_g \rho(g)\right) = \sum_{g\in G} a_g tr(\rho(g))$. Luego para cada $h \in G$ se tiene que la columna de $\rho(g)$ asociada a h está formada por ceros excepto en la fila gh que aparecerá un 1. Por lo tanto, si $g = 1_G$ entonces en la diagonal de $\rho(g)$ solamente aparecerán unos mientras que si $g \neq 1_G$ entonces en la diagonal de $\rho(g)$ solamente aparecerán ceros. Esto implica lo siguiente:

$$\chi\left(\sum_{g\in G} a_g g\right) = \sum_{g\in G} a_g tr(\rho(g)) = tr(\rho(1_G)) a_{1_G} = |G| a_{1_G}.$$

□

Capítulo 2

Unidades en Anillos de Grupo.

En este capítulo vamos a realizar un estudio sobre las unidades más importantes en los anillos de grupo que nos facilitará después la búsqueda de un resultado que nos garantice bajo qué condiciones el grupo de unidades del anillo de grupo $\mathbb{Z}G$ es finito. Este resultado se deduce del Teorema de Higman 3.9 que veremos en el capítulo 3. Para llevar a cabo este teorema, necesitamos en primer lugar introducir los diferentes tipos de unidades necesarias para la elaboración de la demostración y también tenemos que demostrar unos resultados previos que nos ayudarán en el transcurso del documento.

Sea R un anillo y sea G un grupo. Consideramos la aplicación aumento de la sección 1.4 denotada por $\epsilon : RG \to R$. Como ϵ es un homomorfismo de anillos entonces se verifica que si $u \in U(RG)$ entonces $\epsilon(u) \in U(R)$. Denotamos por $U_1(RG) = \{u \in U(RG) \ : \ \epsilon(u) = 1\}$ el subgrupo de $U(RG)$ formado por las *unidades de aumento 1*. Diremos que $\gamma \in RG$ es una *unidad de torsión* de RG si $\gamma \in U(RG)$ y además existe un entero positivo n tal que $\gamma^n = 1$.

2.1. Unidades triviales y unidades unipotentes.

En esta sección se definen las unidades triviales y las unidades unipotentes y se demuestra bajo qué condiciones KG, con K un cuerpo, tiene solamente unidades triviales.

Consideramos el anillo de grupo RG. Sea $r \in U(R)$ y sea $g \in G$. Al elemento $rg \in RG$ lo llamaremos una *unidad trivial de* RG. Su inverso es $r^{-1}g^{-1}$.

Ejemplo 2.1. Las unidades triviales de $\mathbb{Z}G$ son los elementos de la forma $\pm g$ con $g \in G$.

Ejemplo 2.2. Las unidades triviales de KG, con K un cuerpo, son los elementos de la forma kg con $k \in K$, $k \neq 0$ y $g \in G$.

Supongamos que $\eta \in R$ tal que $\eta^k = 0$ con $k \in \mathbb{N}$. Entonces tenemos que

$$(1-\eta)\cdot(1+\eta+\eta^2+\cdots++\eta^{k-1}) = 1-\eta^k = 1$$

Por lo tanto $1 \pm \eta$ son unidades de R y las llamaremos *unidades unipotentes*.

Teorema 2.3. *Sean G un grupo finito que no es libre de torsión y K un cuerpo no trivial con característica $p \geq 0$ tal que $p \nmid |G|$. Entonces se verifica lo siguiente: KG solo tiene unidades triviales si y solo si se verifica una de las siguientes condiciones:*

1. $K = \mathbb{Z}_2$ y $G = C_2$ ó $G = C_3$.
2. $K = \mathbb{Z}_3$ y $G = C_2$.

Demostración. Supongamos que $KG = \mathbb{Z}_2C_2 = \{0,\ 1,\ a,\ 1+a\}$. Entonces las únicas unidades de KG son $\{1,\ a\}$. Claramente son triviales. Supongamos ahora que $KG = \mathbb{Z}_2C_3 = \{0,\ 1,\ a,\ a^2,\ 1+a,\ 1+a^2,\ 1+a+a^2,\ a+a^2\}$. Entonces las únicas unidades de KG son $\{1,\ a,\ a^2\}$. Claramente son triviales. Si fuera $KG = \mathbb{Z}_3C_2 = \{0,\ 1,\ 2,\ a,\ 1+a,\ 1+2a,\ 2+a,\ 2+2a,\ 2a\}$, entonces las únicas unidades de KG son $\{1,\ 2,\ a,\ 2a\}$. Claramente son triviales. Esto demuestra la suficiencia del resultado.

Supongamos que KG solamente contiene unidades triviales con el fin de demostrar la otra implicación. En un primer lugar, vamos a demostrar que todos los subgrupos finitos de G son normales. Procedemos por reducción al absurdo. Supongamos que G contiene un subgrupo cíclico finito de orden n, pongamos generado por a, tal que $\langle a\rangle$ no está normalizado por un elemento $b \in G$. Tomamos $\eta = (a-1)\cdot b\cdot \hat{a}$. Si $\eta = 0$ entonces $ab\hat{a} = b\hat{a}$. Luego $b^{-1}ab\hat{a} = \hat{a}$. Entonces se tiene que $b^{-1}ab\langle a\rangle = supp(b^{-1}ab\hat{a}) = supp(\hat{a}) = \langle a\rangle$. En contradicción con que $b^{-1}ab \notin \langle a\rangle$. Luego $\eta \neq 0$. Además, se tiene que $\eta^2 = 0$ porque $\hat{a}(a-1) = 0$. Luego $1+\eta$ es una unidad unipotente en KG. Como $\eta \neq 0$ entonces deducimos que $ab\hat{a} \neq b\hat{a}$. Luego existe un $i \in \{0,\ 1,\ \ldots, n-1\}$ tal que $aba^i \neq ba^j$ para todo $j \in \{0,\ 1,\ \ldots, n-1\}$. Por lo tanto se tiene que $1,\ aba^i \in supp(1+\eta) \neq \{1\}$. Esto implica que $1+\eta$ es una unidad no trivial de KG en contradicción con la hipótesis. Luego todos los subgrupos finitos de G son normales.

Supongamos que H es un subgrupo finito y propio de G tal que $H \neq \{1\}$. Consideramos $\hat{H} = \sum_{h\in H} h$. Es bien conocido que $\hat{H} \in Z(KG)$ y que $\hat{H}^2 = |H| \cdot \hat{H}$. Si $|H|$ fuera múltiplo de p entonces tendríamos que $\hat{H}^2 = 0$. Tomamos $g \in G$ tal que $g \notin H$ y consideramos $\eta = g + \hat{H}$. Entonces η es una unidad en KG porque $(g + \hat{H}) \cdot (g^{-1} \cdot (1 - g^{-1}\hat{H})) = 1$. Además como $supp(\hat{H}) = H$ y $g \notin H$ entonces $1, g \in supp(\eta)$. Luego $|supp(\eta)| \neq 1$. Por lo tanto η no es una unidad trivial en KG. En contradicción con la hipótesis.

Supongamos ahora que $|H|$ no es múltiplo de p. Esto implica que $e = \frac{1}{|H|}\hat{H}$ es un elemento central y además es idempotente porque $e^2 = \left(\frac{\hat{H}}{|H|}\right)^2 = \frac{\hat{H}^2}{|H|^2} = \frac{|H|\hat{H}}{|H|^2} = \frac{\hat{H}}{|H|} = e$. Luego $e + g(1 - e)$ es una unidad de KG porque $(e + g(1 - e)) \cdot (e + g^{-1}(1 - e)) = 1$. Además, como $supp(e) = H$ y $g \notin H$ entonces $1,\ g \in supp(e + g(1 - e))$. Luego $|supp(\eta)| \neq 1$. Por lo tanto, $e+g(1-e)$ es una unidad no trivial en KG. En contradicción con la hipótesis.

Como G no es libre de torsión, entonces necesariamente contiene un subgrupo de orden primo, pero como hemos demostrado que no contiene ningún subgrupo propio finito, entonces deducimos que G es cíclico de orden primo. Pongamos que $G = \langle a\rangle$ con $o(a) = h$, donde h es un número primo. Vamos a distinguir dos casos.

Supongamos que $h = p$. Sea $c \in K$ con $c \neq 1$. Vamos a demostrar que $1+c\hat{G}$ es una unidad no trivial de KG a menos que $h = 2$ y $K = \mathbb{Z}_2$. Sabemos que $1+c\hat{G} = 1+c|G|\frac{\hat{G}}{|G|}$. Llamamos $e = \frac{\hat{G}}{|G|}$. Se tiene que e es idempotente porque $e^2 = \left(\frac{\hat{G}}{|G|}\right)^2 = \frac{\hat{G}^2}{|G|^2} = \frac{|G|\hat{G}}{|G|^2} = \frac{\hat{G}}{|G|} = e$. Por lo tanto tenemos que $1 + c\hat{G} = 1 + c|G|e = (1 - e) + (c|G| - 1)e = 1 \cdot (1 - e) + ae$ donde $a = c|G| - 1$. Veamos que $a \neq 0$. En el caso en que $a = 0$, tendríamos que $c|G| = 1$ y que $c\hat{G} = -e$. Utilizando que e es idempotente obtenemos que $e^2 = (-c\hat{G})^2 = cc\hat{G}^2 = cc|G|\hat{G} = c\hat{G} \neq -c\hat{G} = e$. Contradicción. Por lo tanto se tiene que $(1 \cdot (1 - e) + ae) \cdot ((1 - e) + a^{-1}e) = 1 - e + e = 1$. Luego hemos demostrado que $1 + c\hat{G}$ es una unidad de KG. Además, $1 + c\hat{G}$ es una unidad trivial en KG si y solo si $|G| = 1$ ó $|G| = 2$ y $c = -1$. Por lo tanto, $1 + c\hat{G}$ es una unidad no trivial de KG a menos que $h = 2$ y $K = \mathbb{Z}_2$. Con esto ya tendríamos demostrado que si KG solo contiene unidades triviales y $h = p$ entonces $K = \mathbb{Z}_2$ y $G = C_2$.

Supongamos que $h \neq p$. Usando el Corolario 1.8 obtenemos que $K\langle a\rangle$ es semisimple

y además usando el Teorema 1.9 de Perlis-Walker deducimos que existe un isomorfismo

$$\mu : \ K\langle a\rangle \longrightarrow K \oplus K(\zeta) \oplus K(\theta) \cdots$$

donde $\zeta, \theta, \ldots$ son raíces complejas de la unidad de orden h. Además se tiene que $\mu(a) = (1, \zeta, \theta, \ldots)$. Por lo tanto, si $ka^i \in U(K\langle a\rangle)$ para algún i entonces $\mu(ka^i) = (k, k\zeta^i, k\theta^i, \ldots)$. Supongamos que la descomposición de $K\langle a\rangle$ como suma directa de simples tuviera más de dos sumandos. Consideramos $k = 1$. Entonces tendríamos en $K\langle a\rangle$ una unidad de la forma $(1, \zeta, 1, \ldots)$. Por lo tanto, se tiene para algún i que $\mu(ka^i) = (k, k\zeta^i, k\theta^i, \ldots) = (1, \zeta, 1, \ldots) = (1, \zeta^i, \theta^i, \ldots)$. Luego $\zeta^i = \zeta$ y $\theta^i = 1$. Esto último implica que $h|i$. Luego $\zeta^i = 1$. Contradicción, porque $1 = \zeta^i = \zeta \neq 1$. Por lo tanto se tiene que:

$$K\langle a\rangle \simeq K \oplus K(\zeta)$$

Denotamos por $q = |K|$, $E = K(\zeta)$. Por lo tanto $|E| = q^r$ para algún $r \in \mathbb{N}$. Como K y $K(\zeta)$ son cuerpos y como $K\langle a\rangle \simeq K \oplus K(\zeta)$ entonces deducimos que las unidades de $K\langle a\rangle$ son de la forma (x, y) con $x \in U(K)$ e $y \in U(K(\zeta))$. Por hipótesis tenemos que todas las unidades de $K\langle a\rangle$ son triviales entonces el número de unidades de $K\langle a\rangle$ coincide con el número de unidades triviales, luego $p(q-1) = (q-1)(q^r-1)$. Esto implica que $p = q^r - 1$ y por lo tanto $q^r = p + 1$.

Por otro lado sabemos que el número de elementos de $K\langle a\rangle$ es $q^p = q \cdot q^r = q^{r+1}$ y si sustituimos en la expresión anterior obtenemos que $q^p = q \cdot q^r = q \cdot (p+1)$. Entonces $q^{p-1} = p + 1$. Como q^{p-1} es potencia de un primo entonces $p + 1$ es potencia de un primo. Luego la igualdad $q^{p-1} = p + 1$ solamente puede ocurrir cuando o bien $q = 2$ y $p = 3$ o bien $q = 3$ y $p = 2$, es decir, o $K = F_2$ y $G = C_3$ o $K = F_3$ y $G = C_2$. □

2.2. Unidades Bicíclicas.

Vamos a introducir el concepto de unidad bicíclica en el anillo de grupo con coeficientes enteros $\mathbb{Z}G$. Demostraremos unas propiedades muy útiles para posteriores resultados y justificaremos que toda unidad bicíclica no trivial tiene orden infinito.

Sea R un anillo y sean $x, y, t \in R$. Tomamos $\eta = ytx$. Si $xy = 0$ entonces $\eta^2 = 0$ y por lo tanto $1 + \eta$ es una unidad unipotente de R.

Sea G un grupo y consideramos $R = \mathbb{Z}G$. Tomamos un elemento $a \in G$ de orden finito. Supongamos que $o(a) = n$. Sea $b \in G$. Entonces se tiene que $(a-1)\cdot\hat{a} = 0$. Por lo tanto $((a-1)\cdot b\cdot\hat{a})^2 = 0$. Luego $1+(a-1)\cdot b\cdot\hat{a}$ es una unidad en $\mathbb{Z}G$. Los elementos de la forma $\mu_{a,b} = 1+(a-1)\cdot b\cdot\hat{a}$ se llaman *unidades bicíclicas* de $\mathbb{Z}G$. Además, es claro que si $ab = ba$ entonces $\mu_{a,b} = 1$.

Vamos a demostrar un resultado que nos va a caracterizar cuándo las unidades bicíclicas son triviales.

Proposición 2.4. *Sea G un grupo y sean $g, h \in G$ elementos de G con $o(g) = n < \infty$. Entonces la unidad bicíclica $\mu_{g,h}$ es una unidad trivial en $\mathbb{Z}G$ si y solo si h normaliza a $\langle g\rangle$.*

Demostración. Supongamos por hipótesis que h normaliza a $\langle g\rangle$. Entonces $h^{-1}gh = g^j$ para algún $j \in \mathbb{N}$. Luego $gh = hg^j$. Es claro que $g^j\hat{g} = \hat{g}$. Además, como $gh = hg^j$ entonces $gh\hat{g} = hg^j\hat{g} = h\hat{g}$. Por lo tanto $\mu_{g,h} = 1+(g-1)h\hat{g} = 1+gh\hat{g}-h\hat{g} = 1$.

Supongamos que $\mu_{g,h}$ es una unidad trivial en $\mathbb{Z}G$ entonces existe un $x \in G$ tal que $\mu_{g,h} = \pm x$. Vamos a demostrar que h normaliza a $\langle g\rangle$. Como $x = 1+(1-g)h\hat{g}$ entonces despejando obtenemos lo siguiente:

$$1 + h\cdot(1+g+g^2+\cdots+g^{n-1}) = x + gh(1+g+g^2+\cdots+g^{n-1}) \tag{2.2.1}$$

Como el 1 aparece a la izquierda de la igualdad, entonces aparece a la derecha. Si $1 \neq x$ entonces $1 = ghg^i$ para algún $i \in \{0,\ 1, \ldots, n-1\}$. Luego $h \in \langle g\rangle$ y $gh(1+g+g^2+\cdots+g^{n-1}) = h\cdot(1+g+g^2+\cdots+g^{n-1})$. De donde deducimos que $x = 1$. Por lo tanto $h \in supp(gh(1+g+g^2+\cdots+g^{n-1}))$, luego $h = ghg^i$ para algún $i \in \{0,\ 1, \ldots, n-1\}$. Lo que implica que $g^{-i} = h^{-1}gh$, de donde deducimos que $h^{-1}gh \in \langle g\rangle$. Luego h normaliza a $\langle g\rangle$. □

Corolario 2.5. *Sea G un grupo finito. Entonces el subgrupo de $U(\mathbb{Z}G)$ generado por todas las unidades bicíclicas de $\mathbb{Z}G$ es trivial si y solo si todo subgrupo de G es normal.*

Demostración. Es consecuencia inmediata de la proposición anterior. □

Proposición 2.6. *Toda unidad bicíclica $\mu_{g,h} \neq 1$ de $\mathbb{Z}G$ tiene orden infinito.*

Demostración. Sea $\mu_{g,h} = 1 + (g-1)h\hat{g}$ una unidad bicíclica de $\mathbb{Z}G$ con $\mu_{g,h} \neq 1$. Considero $s \in \mathbb{N}$ con $s \neq 0$. Entonces $\mu_{g,h}^s = (1 + (g-1)h\hat{g})^s = 1 + s \cdot (g-1) \cdot h \cdot \hat{g}$. Por lo tanto deducimos lo siguiente: $\mu_{g,h}^s = 1$ si y solo si $s(g-1)h\hat{g} = 0$ si y solo si $(g-1)h\hat{g} = 0$ si y solo si $\mu_{g,h} = 1$. Esto implica que implica que si $\mu_{g,h} \neq 1$ entonces $\mu_{g,h}$ tiene orden infinito. □

2.3. Unidades Cíclicas de Bass.

En esta sección se introducen las unidades cíclicas de Bass y se demuestra bajo qué condiciones tienen orden infinito.

Consideramos G un grupo y sea $g \in G$ con $o(g) = n < \infty$. Sea $R = \mathbb{Z}G$ un anillo de grupo con coeficientes enteros. Tomamos k un entero coprimo con n tal que $1 \leq k \leq n-1$, luego existe algún entero positivo m tal que $k^m \equiv 1 \mod n$. Entonces definimos una *unidad cíclica de Bass* como un elemento de $\mathbb{Z}G$ de la forma:

$$u_{k,m}(g) = (1 + g + g^2 + \cdots + g^{k-1})^m + \frac{1-k^m}{n} \cdot \hat{g}.$$

Proposición 2.7. *Sea $g \in G$ con $o(g) = n > 1$ y sea k un entero coprimo con n. Consideramos un entero positivo m tal que $k^m \equiv 1 \mod n$. Entonces $u_{k,m}(g)$ es invertible en $\mathbb{Z}G$ con inverso*

$$u_{k,m}(g)^{-1} = (1 + g^k + \cdots + g^{k(l-1)})^m + \frac{1-l^m}{n} \cdot \hat{g}$$

donde $l \in \mathbb{Z}$ tal que $kl \equiv 1 \mod n$.

Demostración. En un primer lugar, observamos que $u_{k,m}(g) = x_k(g)^m + r\hat{g}$ con m un entero elegido tal que $\epsilon(x_k(g)^m) \equiv 1 \mod \epsilon(\hat{g})$ y r es el único entero tal que $\epsilon\left(x_k(g)^m + r\hat{g}\right) = 1$. Si $k \equiv k' \mod n$ entonces se tiene que $x_{k'}(g) = x_k(g) + s\hat{g}$ para algún entero s. Como r es único, entonces tenemos que $u_{k,m}(g) = u_{k',m}(g)$. Luego, si en la expresión de $u_{k,m}(g)$ sustituimos el elemento g por una raíz n-ésima compleja de la unidad ζ, obtenemos que $u_{k,m}(\zeta) = \eta_k(\zeta)^m$. Además, esta expresión tiene sentido porque $n > 1$. Como ya sabemos que $\eta_k(\zeta)^{-1} = \eta_l(\zeta^k)$ para $l \in \mathbb{Z}$ tal que $kl \equiv 1 \mod n$, entonces el candidato lógico para el inverso de $u_{k,m}(g)$ es $u_{l,m}(g^k)$. Vamos a comprobarlo.

$u_{k,m}(g) \cdot u_{l,m}(g^k) = \left(\left(1+g+g^2+\cdots+g^{k-1}\right)\cdot\left(1+g^k+g^{2k}+\cdots+g^{(l-1)k}\right)\right)^m + t\hat{g} = x_{kl}(g)^m + t\hat{g}$, donde t es el único entero tal que $\epsilon\left(x_{kl}(g)^m + t\hat{g}\right) = 1$. Como t es único y además hemos demostrado que para $k \equiv k'$ mód n se tenía que $u_{k,m}(g) = u_{k',m}(g)$, entonces deducimos que $u_{k,m}(g)\cdot u_{l,m}(g^k) = u_{kl,m}(g) = u_{1,m}(g) = 1$. Por lo tanto $u_{k,m}(g)$ es una unidad en $\mathbb{Z}G$ y además si $kl \equiv 1$ mód n se tiene que $u_{k,m}(g)^{-1} = u_{l,m}(g^k)$. □

Sea $n = p_1^{n_1}\cdot p_2^{n_2}\cdot\cdots p_t^{n_t} \in \mathbb{N}$ donde los p_i son números primos distintos. Definimos la *función de Euler* como la función ϕ que toma los siguiente valores:

$$\phi(n) = p_1^{n_1-1}\cdot(p_1-1)\cdot\cdots p_t^{n_t-1}(p_t-1)$$

Además, es bien conocido que la podemos expresar de la siguiente forma:

$$\phi(n) = |\,\{l \in \mathbb{Z} \;:\; 1 \le l \le n, \quad m.c.d(n,l) = 1\}\,|$$

Una propiedad muy importante de la función de Euler es el siguiente teorema.

Teorema 2.8. *Teorema de Euler.*

Si i y n son coprimos entre si entonces $i^{\phi(n)} \equiv 1$ mód n.

Proposición 2.9. *Sea $g \in G$ con $o(g) = n < \infty$. Sea $l \in \mathbb{Z}$ tal que $1 < l < n-1$ y $m.c.d(l,n) = 1$. Entonces la unidad cíclica de Bass $u_{l,\phi(n)}(g)$ tiene orden infinito en $\mathbb{Z}G$.*

Demostración. Sabemos por el Corolario 1.10 que

$$\mathbb{Q}\langle g\rangle \simeq \oplus_{d|n}\mathbb{Q}(\zeta^d)$$

donde ζ es una raíz n-ésima primitiva de la unidad en $\mathbb{C}$. Utilizando la Propiedad Universal de los Anillos de Grupo deducimos que hay un único homomorfismo $f : \mathbb{Q}\langle g\rangle \longrightarrow \mathbb{C}$ tal que $f(g) = \zeta$. Entonces $f(u_{l,\phi(n)}(g)) = (1+\zeta+\zeta^2+\cdots+\zeta^{l-1})^{\phi(n)} + \frac{1-l^{\phi(n)}}{n}\cdot\hat{\zeta}$, donde $\hat{\zeta} = 1+\zeta+\zeta^2+\cdots+\zeta^{n-1}$ es considerado como suma en los complejos. Como ζ es una raíz n-ésima compleja primitiva de la unidad entonces $0 = \zeta^n - 1 = (\zeta-1)\cdot\hat{\zeta}$. Si $\zeta = 1$ entonces $f(u_{l,\phi(n)}(g)) = 1$, luego $u_{l,\phi(n)}(g) = 1$. En el caso en que $\zeta \neq 1$ tenemos que $\hat{\zeta} = 0$. Luego $f(u_{l,\phi(n)}(g)) = (1+\zeta+\zeta^2+\cdots+\zeta^{l-1})^{\phi(n)}$.

Veamos ahora que $f(u_{l,\phi(n)}(g))$ tiene orden infinito. Procedemos por reducción al absurdo. Supongamos que $f(u_{l,\phi(n)}(g))$ tiene orden finito. Entonces $1+\zeta+\zeta^2+\cdots+\zeta^{l-1}$

tiene orden finito. Vamos a demostrar que esta última afirmación es imposible. Sabemos que $\{\pm\zeta^t : 0 \leq t \leq n-1\}$ son todas las raíces primitivas de la unidad en $\mathbb{Q}(\zeta)$ por lo que existe algún entero positivo s tal que $1+\zeta+\zeta^2+\cdots+\zeta^{l-1} = \pm\zeta^s$. Luego $1-\zeta^l = \left(1+\zeta+\zeta^2+\cdots+\zeta^{l-1}\right)\cdot(1-\zeta) = \pm\zeta^s\cdot(1-\zeta)$. Tomando módulos en esta última igualdad tenemos que $|1-\zeta^l| = |\pm\zeta^s|\cdot|1-\zeta|$. Esto implica que $|1-\zeta^l| = |1-\zeta|$.

Como $1, \zeta^l, \zeta$ son vértices de un polígono regular de n lados y además se verifica que $|1-\zeta^l| = |1-\zeta|$ entonces deducimos que $\zeta^l = \zeta$ ó $\zeta^l = \zeta^{-1}$. Contradicción porque ninguno de estos dos casos están permitidos por hipótesis. Luego hemos demostrado que en este caso $1+\zeta+\zeta^2+\cdots+\zeta^{l-1}$ no puede tener orden finito, con lo que obtenemos que $f(u_{l,\phi(n)}(g))$ no puede tener orden finito en contradicción con la hipótesis. Luego $u_{l,\phi(n)}(g)$ tiene orden infinito. □

2.4. Unidades de torsión.

En esta sección vamos a demostrar unos resultados relacionados con unidades de torsión en $\mathbb{Z}G$. En primer lugar, diremos que $\gamma \in \mathbb{Z}G$ es una *unidad central* de $\mathbb{Z}G$ si $\gamma \in U(\mathbb{Z}G)$ y además $\gamma \in Z(\mathbb{Z}G)$. Sea R un anillo conmutativo. Definimos la *aplicación involución* del anillo de grupo RG como la aplicación $\star :\ RG \to RG$ dada por $(\sum_{g\in G} a_g \cdot g)^\star = \sum_{g\in G} a_g \cdot g^{-1}$. Se verifican las siguientes propiedades:

1. $(\alpha+\beta)^\star = \alpha^\star + \beta^\star$
2. $(\alpha\cdot\beta)^\star = \beta^\star\cdot\alpha^\star$
3. $(\alpha^\star)^\star = \alpha$

Teorema 2.10. *Teorema de Passman-Bass.*

Sean G un grupo y $\gamma = \sum_{g\in G}\gamma(g)g \in \mathbb{Z}G$ una unidad de torsión en $\mathbb{Z}G$. Si $\gamma(1) \neq 0$ entonces $\gamma = \pm 1$.

Demostración. Consideramos la representación regular $\rho :\ \mathbb{C}G \longrightarrow M_m(\mathbb{C})$ con $m = |G|$. Como γ tiene orden finito, entonces $\rho(\gamma)$ tiene orden finito y por lo tanto sabemos que es diagonalizable. Luego existe una matriz $U \in M_m(\mathbb{C})$ tal que $U^{-1}\rho(\gamma)U$ es una matriz diagonal y además, los elementos que aparecen en la diagonal son m raíces complejas de la unidad, las denotamos por $\{\zeta_1, \zeta_2, \ldots, \zeta_m\}$. Entonces se tiene que

$tr(\rho(\gamma)) = \zeta_1 + \zeta_2 + \cdots + \zeta_m$, por lo que $|tr(\rho(\gamma))| = |\zeta_1 + \zeta_2 + \cdots + \zeta_m| \leq m$. Utilizando la Proposición 1.18 deducimos que $tr(\rho(\gamma)) = m\gamma(1)$, luego $|tr(\rho(\gamma))| = |m\gamma(1)| \leq m$.

Como por hipótesis teníamos que $\gamma(1) \neq 0$ y además $\gamma(1)$ es un número entero, entonces $|m\gamma(1)| = m$ implica que $\gamma(1) = \pm 1$. De donde deducimos que $|\zeta_1 + \zeta_2 + \cdots + \zeta_m| = m$. Esto implica que $\zeta_1 + \zeta_2 + \cdots + \zeta_m = \pm m$, luego $\zeta_1 = \zeta_2 = \ldots = \zeta_m = \pm 1$. Aplicando que $U^{-1}\rho(\gamma)U$ es una matriz diagonal, cuyos elementos de la diagonal son todos ± 1, deducimos que es central y por lo tanto obtenemos que $\rho(\gamma) = diag(\pm 1, \pm 1, \ldots, \pm 1)$, lo que implica que $\gamma = \pm 1$. □

Corolario 2.11. *Sea G un grupo. Supongamos que $\gamma \in \mathbb{Z}G$ tal que $\gamma\gamma^\star = \gamma^\star\gamma$. Si γ es una unidad de torsión en $\mathbb{Z}G$ entonces existe un $g_0 \in G$ tal que $\gamma = \pm g_0$.*

Demostración. Como γ es una unidad de torsión en $\mathbb{Z}G$, entonces existe un entero positivo n tal que $\gamma^n = 1$. Aplicando que $\gamma\gamma^\star = \gamma^\star\gamma$, que $\gamma^n = 1$ y que $(\gamma^\star)^n = 1$ obtenemos que $(\gamma\gamma^\star)^n = 1$. Además se tiene que $(\gamma\gamma^\star)(1) = \sum_{g\in G} \gamma(g)^2 \neq 0$. Utilizando el Teorema 2.10 de Passman-Bass deducimos que $\gamma\gamma^\star = 1$. Por lo tanto $\sum_{g\in G} \gamma(g)^2 = 1$. Esto implica que solamente puede haber un coeficiente $\gamma(g_0)$ diferente de cero para algún $g_0 \in G$. Luego $\gamma = \pm g_0$. □

Corolario 2.12. *Todas las unidades centrales de orden finito en $\mathbb{Z}G$ son triviales.*

Demostración. Sea γ una unidad central y de orden finito en $\mathbb{Z}G$. Como γ es central entonces $\gamma\gamma^\star = \gamma^\star\gamma$, y como tiene orden finito, aplicando el Corolario 2.11 obtenemos que es una unidad trivial. □

Corolario 2.13. *Si A es un grupo abeliano entonces todas las unidades de torsión de $\mathbb{Z}A$ son triviales.*

Demostración. Sea γ una unidad de torsión de $\mathbb{Z}A$. Como A es un grupo abeliano entonces γ es una unidad central. Aplicando el Corolario 2.12 obtenemos que es una unidad trivial. □

2.5. Unidades en $\mathbb{Z}A$, con A un grupo abeliano finito.

En un primer lugar vamos a clasificar el grupo de unidades de $\mathbb{Z}A$, donde A es un grupo abeliano finito. Posteriormente, daremos estructura al grupo de unidades de aumento 1 de $\mathbb{Z}A$.

Teorema 2.14. *Sea A un grupo abeliano finito. Entonces $U(\mathbb{Z}A) = \pm A \times F$, donde F es un grupo abeliano libre de rango finito.*

Demostración. Como A es un grupo finito, entonces $|A| = n$ para algún $n \in \mathbb{N}$. Utilizando el Teorema 1.9 de Perlis-Walker sabemos que existe un isomorfismo

$$\mu : \mathbb{Q}A \longrightarrow \oplus_{d|n}\mathbb{Q}[\zeta_d]$$

donde ζ_d son raíces complejas de la unidad de orden d, dado por $\mu(\sum_{g\in A} a_g g) = (\sum_{g\in A} a_g\zeta_{d_1}, \sum_{g\in A} a_g\zeta_{d_2}, \sum_{g\in A} a_g\zeta_{d_3}, \ldots, \sum_{g\in A} a_g\zeta_{d_s})$ donde $\{d_1,\ d_2, \ldots, d_s\}$ son los divisores de n. Como $\oplus_{d|n}\mathbb{Z}[\zeta_d] \subseteq \oplus_{d|n}\mathbb{Q}[\zeta_d]$ entonces podemos definir

$$M = \mu^{-1}\left(\oplus_{d|n}\mathbb{Z}\left[\zeta_d\right]\right)$$

Es claro que $\mathbb{Z}A \subset M \subset \mathbb{Q}A$. Además $\mathbb{Z}A$ y M son ordenes en $\mathbb{Q}A$. Aplicando el Teorema de las Unidades de Dirichlet 1.11 deducimos que $U(\mathbb{Z}[\zeta_d])$ es un grupo abeliano finitamente generado para todo d. Por lo tanto $U(M)$ está también finitamente generado, lo que implica que $U(\mathbb{Z}A)$ es un grupo abeliano finitamente generado. Por lo tanto podemos aplicar el teorema fundamental de los grupos abelianos con el que obtenemos que

$$U(\mathbb{Z}A) = TU(\mathbb{Z}A) \times F$$

donde F es un grupo abeliano libre de rango finito. Usando el Corolario 2.13 deducimos que $TU(\mathbb{Z}A) = \pm A$. Luego $U(\mathbb{Z}A) = \pm A \times F$. □

El rango de F en el teorema anterior se encuentra calculado de forma explícita en la publicación [23].

Proposición 2.15. *Sean G un grupo y $u \in U(\mathbb{Z}G)$ tal que $u^\star u = 1$. Entonces $u = \pm g_0$ con $g_0 \in G$.*

Demostración. Supongamos que $u = \sum_{g\in G} u_g \cdot g$ y que $u^\star = \sum_{g\in G} u_g \cdot g^{-1}$. Entonces se tiene que $1 = u^\star \cdot u = \left(\sum_{g\in G} u_g \cdot g^{-1}\right) \cdot \left(\sum_{g\in G} u_g \cdot g\right) = \left(\sum_{g\in G} u_g^2\right) \cdot 1 + \sum_{g\in G-\{1\}} c_g \cdot g$ para algunos $c_g \in \mathbb{Z}$. Por lo tanto $\sum_{g\in G} u_g^2 = 1$. Esto implica que existe un único $g_0 \in G$ tal que $u_{g_0} = \pm 1$ y $u_h = 0$ para todo h distinto de g_0. Luego se tiene que $u = \pm g_0$. □

Proposición 2.16. *Sean G un grupo finito y $g \in G$ con $o(g) = n < \infty$. Entonces se verifica lo siguiente:*

$$\{\gamma \in \mathbb{Z}G \ : \ (g-1)\gamma = 0\} = \hat{g}\mathbb{Z}G$$

Demostración. Vamos a demostrar el doble contenido. Sea $\alpha \in \mathbb{Z}G$. Aplicando que $g \cdot \hat{g} = \hat{g}$ obtenemos lo siguiente:

$$(g-1) \cdot \hat{g}\alpha = g\hat{g}\alpha - \hat{g}\alpha = \hat{g}\alpha - \hat{g}\alpha = 0$$

Luego $\hat{g}\alpha \in \{\gamma \in \mathbb{Z}G \ : \ (g-1)\gamma = 0\}$.

Sea $\gamma = \sum_{h\in G} a_h h \in \mathbb{Z}G$ tal que $(g-1)\gamma = 0$. Entonces $g\sum_{h\in G} a_h h = \sum_{h\in G} a_h h$. Luego $\sum_{h\in G} a_h gh = \sum_{h\in G} a_h h$. Por lo tanto se tiene que $\sum_{h\in G} a_{g^{-1}h} h = \sum_{h\in G} a_h h$, es decir, $a_h = a_{g^{-1}h}$ para todo $h \in G$. Luego $a_h = a_{g^i h}$ para todo $h \in G$ y para todo $i \in \{0, 1, 2, 3, \ldots, n-1\}$. Tomamos $\{h_1, h_2, \ldots, h_s\}$ representantes de las clases laterales de G módulo $\langle g \rangle$ por la izquierda. Por lo tanto tenemos lo siguiente:

$$\begin{aligned} \gamma &= \sum_{g\in G} a_g g = \sum_{i=1}^{s}\sum_{j=0}^{n-1} a_{g^j h_i} g^j h_i = \sum_{i=1}^{s}\sum_{j=0}^{n-1} a_{h_i} g^j h_i = \\ &= \hat{g}\sum_{i=1}^{s} a_{h_i} h_i \in \hat{g}\mathbb{Z}G. \end{aligned}$$

□

Recordemos que la aplicación de aumento del anillo de grupo RG venía dada por el homomorfismo de anillos $\epsilon : \ RG \to R$, donde $\epsilon(\sum_{g\in G} \ a_g \cdot g) = \sum_{g\in G} \ a_g$. Además, su núcleo lo denotábamos por $\Delta(G)$ y venía dado por

$$\Delta(G) = \left\{ \sum_{g\in G-\{1\}} a_g(g-1) \ : \ a_g \in R \right\}.$$

Proposición 2.17. *Sea A un grupo abeliano finito y sea $a \in A$. Si $a - 1 \in (\Delta A)^2$ entonces $a = 1$.*

Demostración. En un primer lugar vamos a suponer que $A = \langle c \rangle$ con $o(c) = n$. Sea $a \in A$ con $a - 1 \in (\Delta A)^2$. Sabemos que $(\Delta A)^2$ es la unión de todas las combinaciones lineales de productos de dos elementos de ΔA. Supongamos que $a = c^i$ para algún

$i \in \{1,\ 2,\ 3, \ldots,\ n-1\}$. Sabemos que para un grupo $G = \langle X \rangle$, donde X es un conjunto de elementos de G, se tiene que ΔG visto como $\mathbb{Z}G$-módulo lo podemos expresar de la siguiente forma: $\Delta G_{\mathbb{Z}G} = \{x-1 \ :\ x \in X\}\,\mathbb{Z}G$. Entonces para el caso particular $A = \langle c \rangle$, tenemos que ΔA visto como $\mathbb{Z}A$-módulo lo podemos expresar de la siguiente forma:

$$\Delta A_{\mathbb{Z}A} = (c-1) \cdot \mathbb{Z}A$$

Aplicando también que $a - 1 \in (\Delta A)^2$ deducimos que $a - 1 = c^i - 1 = (c-1)^2 \cdot \delta$ con $\delta \in \mathbb{Z}A$. Como $c^i - 1 - (c-1)^2 \cdot \delta = 0$ entonces se tiene que

$$(c-1) \cdot \left((1 + c + c^2 + \cdots + c^{i-1}) - (c-1) \cdot \delta\right) = 0$$

Utilizando la Proposición 2.16 deducimos que $(1+c+c^2+\cdots+c^{i-1})-(c-1)\cdot\delta = \hat{c}\cdot\beta$ para algún $\beta \in \mathbb{Z}A$. Tomando la aplicación aumento a ambos lados de la igualdad obtenemos lo siguiente:

$$\epsilon\left((1 + c + c^2 + \cdots + c^{i-1})\right) - \epsilon\left((c-1) \cdot \delta\right) = \epsilon\left(\hat{c} \cdot \beta\right) = \epsilon(\hat{c}) \cdot \epsilon(\beta)$$

Como $(c-1)\delta \in \Delta A$ entonces $\epsilon\left((c-1)\delta\right) = 0$. Utilizando que $\epsilon\left((1 + c + \cdots + c^{i-1})\right) = i$ y que $\epsilon(\hat{c}) = n$ obtenemos que $i = n\epsilon(\beta)$. Por lo tanto deducimos que i es múltiplo de n. Pero como $o(c) = n$ y $a = c^i$ entonces se tiene que $a = 1$.

Veamos ahora el caso general. Por hipótesis teníamos que A es un grupo abeliano finito, entonces es bien conocido que lo podemos expresar como producto finito de grupos cíclicos. Supongamos que $A = \prod_{i=1}^{n} \langle c_i \rangle$. Sea $a \in A$ tal que $a - 1 \in (\Delta A)^2$. Consideramos $p_j : A \longrightarrow \langle c_j \rangle$ la proyección canónica como homomorfismo de grupos. Utilizando la Propiedad Universal de los Anillos de Grupo obtenemos que p_j induce un único homomorfismo de anillos $f_j : \mathbb{Z}A \longrightarrow \mathbb{Z}\langle c_j \rangle$ que extiende a p_j. Además se tiene que $f_j(\Delta A) = \Delta\langle c_j \rangle$ y $f_j\left((\Delta A)^2\right) = (\Delta\langle c_j \rangle)^2$ para todo j. Como $a - 1 \in (\Delta A)^2$ entonces $f_j(a-1) \in (\Delta\langle c_j \rangle)^2$ para todo j. Por lo tanto, como el caso en que A era un grupo cíclico finito ya lo tenemos demostrado, deducimos que $f_j(a) = 1$ para todo j. Como f_j extiende a p_j entonces sobre A coinciden y como por hipótesis teníamos que $a \in A$ entonces $p_j(a) = f_j(a) = 1$ para todo j. Luego $a = 1$. □

Teorema 2.18. *Sea A un grupo abeliano finito. Entonces $U_1(\mathbb{Z}A) = A \times U_2(\mathbb{Z}A)$ donde*

$$U_2(\mathbb{Z}A) = \left\{u \in U(\mathbb{Z}A) \ :\ u \equiv 1 \mod (\Delta A)^2\right\}$$

Además se tiene que $U_2(\mathbb{Z}A) \subset U_\star(A) = \{u \in U(\mathbb{Z}A) \ :\ u^\star = u\}$.

Demostración. Sea $u \in AU_2(\mathbb{Z}A)$. Entonces existe un $x \in U_2(\mathbb{Z}A)$ y un $a \in A$ tales que $u = ax$. Es claro que tanto el aumento de x como el de a valen 1. Por lo tanto $u \in U_1(\mathbb{Z}A)$.

Supongamos ahora que $u \in U_1(\mathbb{Z}A)$. Entonces se tiene que $u = 1 + \sum_{a\in A} z_a \cdot (a-1)$, donde $z_a \in \mathbb{Z}$ para cada $a \in A$. Sean x, $y \in A$. Como $(x-1)\cdot(y-1) \in (\Delta A)^2$ entonces se verifica la siguiente congruencia:

$$(xy-1) = (x-1) + (y-1) + (x-1)\cdot(y-1) \equiv (x-1) + (y-1) \mod (\Delta A)^2$$

Tomando $y = x^{-1}$ en la congruencia anterior obtenemos lo siguiente:

$$-(x-1) \equiv (x^{-1}-1) \mod (\Delta A)^2$$

Vamos a demostrar que $u \equiv 1 + (a_0 - 1) \mod (\Delta A)^2$ para algún $a_0 \in A$. Utilizando que $-(x-1) \equiv (x^{-1}-1) \mod (\Delta A)^2$ tenemos que para ciertos m, $k \in \mathbb{Z}$ se verifica la siguiente congruencia:

$$\sum_{a\in A} z_a \cdot (a-1) = \sum_{i=1}^{m}(a_i - 1) - \sum_{i=1}^{k}(b_i - 1) \equiv \sum_{i=1}^{m}(a_i - 1) + \sum_{i=1}^{k}(b_i^{-1} - 1) \mod (\Delta A)^2$$

donde a_i, $b_i \in A$ para cada i. Juntando ambas sumas obtenemos que para ciertos $c_i \in A$ se tiene lo siguiente: $\sum_{i=1}^{m}(a_i-1) + \sum_{i=1}^{k}(b_i^{-1}-1) = \sum_{i=1}^{m+k}(c_i - 1)$. Llamamos $h = m + k$. Entonces tenemos que $\sum_{i=1}^{h}(c_i-1) - \sum_{i=1}^{h-2}(c_i-1) - (c_{h-1}\cdot c_h - 1) = (c_{h-1}-1) + (c_h - 1) - (c_{h-1}\cdot c_h - 1) = -(c_h-1)(c_{h-1}-1) \in (\Delta A)^2$. Luego $\sum_{i=1}^{h}(c_i-1) \equiv \sum_{i=1}^{h-2}(c_i-1) + (c_{m-1}\cdot c_m - 1) \mod (\Delta A)^2$. Continuando este proceso por inducción deducimos que $\sum_{i=1}^{h}(c_i-1) \equiv \sum_{i=0}^{h-2}(c_{h-2i-1}\cdot c_{h-2i} - 1) \mod (\Delta A)^2$. Por lo tanto, existe un $a_0 \in A$ tal que

$$\sum_{a\in A} z_a \cdot (a-1) \equiv (a_0 - 1) \mod (\Delta A)^2.$$

Luego $u \equiv a_0 \mod (\Delta A)^2$. Esto implica que $ua_0^{-1} \equiv 1 \mod (\Delta A)^2$. Por lo tanto $ua_0^{-1} \in U_2(\mathbb{Z}A)$.

Ya tenemos probado que $U_1(\mathbb{Z}A) = AU_2(\mathbb{Z}A)$. Nos falta justificar que el producto es directo. Sea $a \in A \cap U_2(\mathbb{Z}A)$. Como $a \in U_2(\mathbb{Z}A)$ entonces $a \in U(\mathbb{Z}A)$ y $a \equiv 1$ mód $(\Delta A)^2$, luego se tiene que $a - 1 \in (\Delta A)^2$. Utilizando la Proposición 2.17 deducimos que $a = 1$. Luego $U_1(\mathbb{Z}A) = A \times U_2(\mathbb{Z}A)$.

Vamos a demostrar que $U_2(\mathbb{Z}A) \subset U_\star(A)$. Sea $u \in U_2(\mathbb{Z}A)$. Consideramos $v = u^{-1} \cdot u^\star$. Entonces se tiene lo siguiente:

$$v^{-1} = \left(u^{-1} \cdot u^\star\right)^{-1} = u \cdot (u^\star)^{-1} = v^\star$$

Luego $v^\star v = 1$. Aplicando la Proposición 2.15 deducimos que $v = \pm a \in A$ es una unidad trivial en $\mathbb{Z}A$. Si fuera $v = -a$, entonces tendríamos que el aumento de v sería -1, en contradicción con que $u \in U_2(\mathbb{Z}A)$. Supongamos que $v = a$. Como $u \in U_2(\mathbb{Z}A)$ entonces $a = v \in U_2(\mathbb{Z}A)$. Esto implica que $a \equiv 1 \mod (\Delta A)^2$. Luego $a - 1 \in (\Delta A)^2$. Utilizando la Proposición 2.17 obtenemos que $a = 1$. Luego $1 = v = u^{-1} \cdot u^\star$ implica que $u = u^\star$. Por lo tanto $u \in U_\star(A)$. □

Enunciamos a continuación unos resultados importantes pero sus demostraciones se salen del objetivo de este trabajo por lo que hacemos referencia a otros documentos donde se pueden encontrar. Para el Teorema de Bass-Milnor y el de Bass hacemos referencia a [2], sin embargo, para los Teoremas 2.21 y 2.22 hacemos referencia a [25] y a [27] respectivamente.

Teorema 2.19. *Teorema de Bass-Milnor.*

Sea A un grupo abeliano finito. Entonces se tiene que el índice

$$(U(\mathbb{Z}A) : \langle U(\mathbb{Z}C) : C \text{ es un subgrupo cíclico de } A\rangle)$$

es finito.

Teorema 2.20. *Teorema de Bass.*

Sea C un grupo cíclico finito. Entonces el grupo formado por todas las unidades cíclicas de Bass genera un subgrupo de índice finito en $U(\mathbb{Z}C)$.

Podemos resumir los dos resultado anteriores en el siguiente teorema.

Teorema 2.21. *Sea A un grupo abeliano finito. Entonces el grupo formado por todas las unidades cíclicas de Bass genera un subgrupo de índice finito en $U(\mathbb{Z}A)$.*

Por último, enunciamos el teorema más general de esta sección.

Teorema 2.22. *Sea G un grupo finito. Entonces $U(\mathbb{Z}G)$ es un grupo finitamente generado.*

Capítulo 3

El Teorema de Higman.

Comenzamos el capítulo más importante del documento, destinado al estudio del Teorema de Higman y de un resultado que nos determinará cuando el grupo de unidades de $\mathbb{Z}G$ es finito. Con el fin de poder demostrar estos resultados, necesitamos estudiar en primer lugar las unidades de $\mathbb{Z}K_8$.

3.1. Unidades en $\mathbb{Z}K_8$.

Vamos a demostrar unos lemas previos que utilizaremos posteriormente.

Lema 3.1. *Sea G un grupo de torsión tal que todas las unidades de $\mathbb{Z}G$ son triviales y sea C_2 el grupo cíclico de orden 2. Entonces todas las unidades de $\mathbb{Z}(G \times C_2)$ son triviales.*

Demostración. Supongamos que $C_2 = \langle a \rangle$. Como $\mathbb{Z}(G \times C_2) \simeq (\mathbb{Z}G)\, C_2$ entonces un elemento $u \in \mathbb{Z}(G \times C_2)$ se puede escribir de la forma $u = \alpha + \beta a$ con $\alpha \in \mathbb{Z}G$ y $\beta \in \mathbb{Z}G$. Supongamos que $u \in U(\mathbb{Z}(G \times C_2))$ y que $u^{-1} = \gamma + \delta a$ con $\gamma \in \mathbb{Z}G$ y $\delta \in \mathbb{Z}G$. Entonces tenemos que $1 = u \cdot u^{-1} = (\alpha + \beta a) \cdot (\gamma + \delta a) = (\alpha \cdot \gamma + \beta \cdot \delta) + (\alpha \cdot \delta + \beta \cdot \gamma)\, a$ de donde deducimos que $\alpha \cdot \gamma + \beta \cdot \delta = 1$ y que $\alpha \cdot \delta + \beta \cdot \gamma = 0$. Utilizando estas dos ecuaciones obtenemos lo siguiente:

$$(\alpha + \beta) \cdot (\gamma + \delta) = \alpha \cdot \gamma + \alpha \cdot \delta + \beta \cdot \gamma + \beta \cdot \delta = 1 + 0 = 1$$

$$(\alpha - \beta) \cdot (\gamma - \delta) = \alpha \cdot \gamma - \alpha \cdot \delta - \beta \cdot \gamma + \beta \cdot \delta = 1 - 0 = 1$$

Por lo tanto $\alpha + \beta \in U(\mathbb{Z}G)$ con inverso $(\alpha + \beta)^{-1} = \gamma + \delta$ y $\alpha - \beta \in U(\mathbb{Z}G)$ con inverso $(\alpha - \beta)^{-1} = \gamma - \delta$.

Sabemos por hipótesis que todas las unidades de $\mathbb{Z}G$ son triviales luego $\alpha+\beta$ y $\alpha-\beta$ son unidades triviales en $\mathbb{Z}G$. Por el ejemplo 2.1 sabemos que las unidades triviales de $\mathbb{Z}G$ son de la forma $\pm g$ con $g \in G$. Luego existen $g_1, g_2 \in G$ tales que $\alpha+\beta = \pm g_1$ y $\alpha-\beta = \pm g_2$. Despejando obtenemos que $\alpha = \pm g_1 - \beta$ y $\beta = \alpha \pm g_2$. Estas dos ecuaciones implican que $\alpha = \pm g_1 - \alpha \pm g_2$. Entonces $\alpha = \frac{1}{2}(\pm g_1 \pm g_2)$. Como los coeficientes de α tiene que ser enteros porque $\alpha \in \mathbb{Z}G$ entonces $g_1 = \pm g_2$. Luego tenemos que o bien $\alpha+\beta = \alpha-\beta = \pm g_1$ o bien $\alpha+\beta = -(\alpha-\beta) = \pm g_1$. Vamos a distinguir los dos casos.

Supongamos que $\alpha+\beta = \alpha-\beta = \pm g_1$ entonces $\alpha = \pm g_1$ y $\beta = 0$. Luego u es una unidad trivial en $\mathbb{Z}(G \times C_2)$. Supongamos que $\alpha+\beta = -(\alpha-\beta) = \pm g_1$ entonces $\alpha = 0$ y $\beta = \pm g_1$. Luego u es una unidad trivial en $\mathbb{Z}(G \times C_2)$. □

Consideramos el *álgebra de cuaterniones Hamiltonianos* $\mathbb{H}(\mathbb{R}) = \mathbb{R} \oplus \mathbb{R}i \oplus \mathbb{R}j \oplus \mathbb{R}k$ con $k = ij = -ji$ e $i^2 = j^2 = 1$. Sea $\alpha = x_0 + x_1 i + x_2 j + x_3 k \in \mathbb{H}(\mathbb{R})$. Entonces definimos el *conjugado* de α como el elemento $\overline{\alpha} = x_0 - x_1 i - x_2 j - x_3 k \in \mathbb{H}(\mathbb{R})$. Definimos la *norma* de α como $||\alpha|| = \alpha \cdot \overline{\alpha}$. Es fácil ver que el siguiente subconjunto de $\mathbb{H}(\mathbb{R})$, $\mathcal{H} = \{m_0 + m_1 \cdot i + m_2 \cdot j + m_3 \cdot k \ : \ m_h \in \mathbb{Z} \text{ para todo } h\}$, es un anillo y lo llamaremos el *anillo de los cuaterniones enteros*. Vamos a calcular el grupo de unidades de $\mathcal{H}$.

Lema 3.2. $U(\mathcal{H}) = \{\pm 1, \pm i, \pm j, \pm k\}$.

Demostración. Sea $\alpha = x_0 + x_1 i + x_2 j + x_3 k \in \mathcal{H}$ con $\alpha \neq 0$. Luego $\overline{\alpha} = x_0 - x_1 i - x_2 j - x_3 k$ y $\| \alpha \| = \alpha \cdot \overline{\alpha} = x_0^2 + x_1^2 + x_2^2 + x_3^2$. Supongamos que $\alpha \in U(\mathcal{H})$. Entonces existe $\alpha^{-1} \in \mathcal{H}$ tal que $\alpha \cdot \alpha^{-1} = 1$. Por lo tanto $||\alpha|| \cdot ||\alpha^{-1}|| = ||\alpha\alpha^{-1}|| = 1$ siendo $||\alpha||$ y $||\alpha^{-1}||$ enteros positivos porque $\alpha \neq 0$. Luego $||\alpha|| = 1$, lo que implica que $x_0^2 + x_1^2 + x_2^2 + x_3^2 = 1$. Como los x_j son enteros para cada j entonces la igualdad anterior es cierta solo cuando $x_i = 1$ para algún i con $0 \leq i \leq 3$ y $x_j = 0$ para todo j distinto de i. Por lo tanto deducimos que $U(\mathcal{H}) = \{\pm 1, \pm i, \pm j, \pm k\}$. □

Lema 3.3. $K_8/\langle a^2 \rangle \simeq C_2 \times C_2$.

Demostración. En primer lugar vamos a calcular el orden de $K_8/\langle a^2 \rangle$.

$$|K_8/\langle a^2 \rangle| = \frac{|K_8|}{|\langle a^2 \rangle|} = \frac{8}{|a^2|} = \frac{8}{2} = 4$$

Sabemos que solo hay dos grupos de orden 4, C_4 y $C_2 \times C_2$. Vamos a demostrar que $K_8/\langle a^2\rangle$ no puede ser isomorfo a C_4 porque $K_8/\langle a^2\rangle$ no tiene elementos de orden 4 pero C_4 si tiene un elemento de orden 4, su propio generador. Como $Z(K_8) = \langle a^2\rangle$ y el cociente de un grupo por su centro siempre da un grupo abeliano, deducimos que $K_8/\langle a^2\rangle$ es un grupo abeliano.

Por otro lado, aplicando que además a y b tienen orden 2 en $K_8/\langle a^2\rangle$ entonces obtenemos que ab tiene orden 2 en $K_8/\langle a^2\rangle$. Por lo que $K_8/\langle a^2\rangle$ no tiene elementos de orden 4 y por lo tanto no puede ser isomorfo a C_4. Luego $K_8/\langle a^2\rangle \simeq C_2 \times C_2$. □

Teorema 3.4. *Todas las unidades de $\mathbb{Z}K_8$ son triviales.*

Demostración. Sea $\alpha \in \mathbb{Z}K_8$ entonces se tiene que

$$\alpha = x_0 + x_1a + x_2b + x_3ab + y_0a^2 + y_1a^3 + y_2a^2b + y_3ab^3$$

con x_i e y_i enteros para todo i. Usando el Lema 3.2 sabemos que $U(\mathcal{H}) = \{\pm 1, \pm i, \pm j, \pm k\}$. Definimos el epimorfismo $\phi :\ \mathbb{Z}K_8 \longrightarrow \mathcal{H}$ dado por

$$\phi(\alpha) = (x_0 - y_0) + (x_1 - y_1)i + (x_2 - y_2)j + (x_3 - y_3)k$$

Supongamos que $\alpha \in U(\mathbb{Z}K_8)$ entonces como ϕ es un homomorfismo se tiene que $\phi(\alpha) \in U(\mathcal{H})$. Por lo tanto para algún entero r con $0 \leq r \leq 3$ se tiene que $x_r - y_r = \pm 1$ y $x_s - y_s = 0$ para todo s distinto de r. Utilizando el Lema 3.3 obtenemos que $K_8/\langle a^2\rangle \simeq C_2 \times C_2$. Tomamos la proyección canónica $K_8 \longrightarrow K_8/\langle a^2\rangle$ y consideramos su extensión a $\mathbb{Z}K_8$ como la aplicación

$$\psi :\ \mathbb{Z}K_8 \longrightarrow \mathbb{Z}\left(K_8/\langle a^2\rangle\right)$$

dada por:

$$\psi(\alpha) = (x_0 + y_0) + (x_1 + y_1)\bar{a} + (x_2 + y_2)\bar{b} + (x_3 + y_3)\bar{a}\bar{b}$$

Como $\alpha \in U(\mathbb{Z}K_8)$ entonces:

$$\psi(\alpha) \in U\left(\mathbb{Z}\left(K_8/\langle a^2\rangle\right)\right) \simeq U\left(\mathbb{Z}\left(C_2 \times C_2\right)\right)$$

Utilizando el Lema 3.1 sabemos que todas las unidades de $\mathbb{Z}(C_2 \times C_2)$ son triviales, por lo tanto $\psi(\alpha)$ es una unidad trivial. Luego para algún indice h con $0 \leq h \leq 3$ se tiene

que $x_h + y_h = \pm 1$ y $x_k + y_k = 0$ para todo k distinto de h. Como los x_j son enteros entonces deducimos que $r = h$ y además también se tiene lo siguiente:

O bien $x_r = \pm 1$, $y_r = 0$ y $x_s = y_s = 0$ para todo s distinto de r.

O bien $x_r = 0$, $y_r = \pm 1$ y $x_s = y_s = 0$ para todo s distinto de r.

En ambos casos deducimos que α en una unidad trivial en $\mathbb{Z}K_8$. □

3.2. El Teorema de Higman.

Como consecuencia del Corolario 2.13, sabemos que si G es un grupo abeliano, entonces todas las unidades de torsión de $\mathbb{Z}G$ son triviales. Vamos a buscar un resultado que nos garantice qué hipótesis tiene que satisfacer el grupo G para que $\mathbb{Z}G$ tenga todas sus unidades triviales. Comenzamos con un lema previo.

Lema 3.5. *Sea G un grupo de torsión tal que $U_1(\mathbb{Z}G) = G$. Entonces todo subgrupo de G es normal.*

Demostración. Es suficiente con demostrar que todo subgrupo cíclico de G es normal. Procedemos por reducción al absurdo. Supongamos que $\langle g \rangle$ es un subgrupo cíclico de G que no sea normal. Entonces existe un $h \in G$ que no normaliza a $\langle g \rangle$. Por lo tanto, utilizando la Proposición 2.4 deducimos que la unidad bicíclica $\mu_{g,h}$ no es trivial en $\mathbb{Z}G$. En contradicción con que todas las unidades de $\mathbb{Z}G$ sean triviales. □

Recordemos que el exponente de un grupo G lo definíamos como el menor entero positivo m tal que $g^m = 1$ para todo $g \in G$, en el caso en que este número exista.

Proposición 3.6. *Sea G un grupo de torsión verificando $U_1(\mathbb{Z}G) = G$. Entonces se verifica una de las siguientes afirmaciones:*

1. *G es un grupo abeliano de exponente igual a $1, 2, 3, 4$ ó 6.*

2. *G es un 2-grupo Hamiltoniano.*

Demostración. Utilizando el Lema 3.5 deducimos que todo subgrupo de G es normal, por lo tanto, G puede ser o bien un grupo abeliano o bien un grupo Hamiltoniano.

Supongamos en primer lugar que G es un grupo abeliano. Llamamos n al exponente de G y procedemos por reducción al absurdo. Supongamos que $n \neq 1, 2, 3, 4, 6$. Luego

$n = 5$ ó $n > 6$. Supongamos que $n = 5$. Entonces evaluando la función de Euler tenemos que $\phi(5) = 5^{1-1} \cdot (5-1) = 4 > 2$. En el caso $n > 6$ obtenemos también que $\phi(n) > 2$ porque ya teníamos previamente calculado que $\phi(5) > 2$. Por lo tanto en ambos casos obtenemos que $\phi(n) > 2$ y usando la Proposición 2.9 deducimos que para $g \in G$ con $o(g) = n$ se tiene que $u_{l,\phi(n)}(g)$ es una unidad cíclica de Bass con orden infinito y no trivial en $\mathbb{Z}G$ para $1 < l < n-1$ y $m.c.d(l,n) = 1$. Contradicción con la hipótesis.

Supongamos ahora que G es un grupo Hamiltoniano. Utilizando el Teorema 1.5 sabemos que $G = K_8 \times E \times A$, donde E es un 2-grupo abeliano elemental y A es un grupo abeliano con todos los elementos de orden impar. Procedemos por reducción al absurdo. Supongamos que G no es un 2-grupo. Entonces $A \neq \{1\}$. Además, como todo elemento en A tiene orden impar entonces existe un $x \in A$ con $x \neq 1$ tal que $o(x) = p > 2$ con p impar. Consideramos $g = ax \in G$. Se tiene que $o(g) = o(ax) = o(a) \cdot o(x) = 4p$ porque $o(a) = 4$ en K_8. Por el mismo argumento que hemos utilizado al comienzo de la demostración tenemos que $\phi(4p) > 2$ y usando la Proposición 2.9 deducimos que $\mu_{l,\phi(n)}(g)$ es una unidad cíclica de Bass con orden infinito y no trivial en $\mathbb{Z}G$ para $1 < l < n-1$ y $m.c.d(l,n) = 1$. Contradicción con la hipótesis. □

Lema 3.7. *Si ζ_3 una raíz compleja primitiva de la unidad de orden 3 entonces*

$$U(\mathbb{Z}[\zeta_3]) = \left\{\pm 1,\ \pm\zeta_3,\ \pm\zeta_3^2\right\}.$$

Demostración. Como ζ_3 es una raíz cúbica compleja primitiva de la unidad, entonces el polinomio mínimo asociado a ζ_3 es $\Phi_3(x) = x^2+x+1$. Sea $\alpha \in U(\mathbb{Z}[\zeta_3])$. Supongamos que $\alpha = a + b\zeta_3$ con $a, b \in Z$. Consideramos el homomorfismo suprayectivo $f : \mathbb{Z}[\zeta_3] \longrightarrow \mathbb{Z}[\zeta_3]$ dado por $f(x + y\zeta_3) = x + y\zeta_3^2$. Como $\alpha \in U(\mathbb{Z}[\zeta_3])$ y f es un homomorfismo entonces tenemos que $f(\alpha) \in U(\mathbb{Z}[\zeta_3])$. Llamamos $f(\alpha) = \alpha_1$. Luego $\alpha \cdot \alpha_1 = (a + b\zeta_3) \cdot (a + b\zeta_3^2) = a^2 + ab\zeta_3^2 + ab\zeta_3 + b^2\zeta_3^3 = a^2 + b^2 + ab \cdot (\zeta_3 + \zeta_3^2)$. Como $\Phi_3(\zeta_3) = 0$ entonces $\zeta_3^2 + \zeta_3 + 1 = 0$, lo que implica que $\zeta_3^2 + \zeta_3 = -1$. Por lo tanto, tenemos que $\alpha \cdot \alpha_1 = a^2 + b^2 - ab \in \mathbb{Z}$. Además, $\alpha \cdot \alpha_1 \in U(\mathbb{Z}[\zeta_3])$ porque $\alpha, \alpha_1 \in U(\mathbb{Z}[\zeta_3])$, pero como $\alpha \cdot \alpha_1 \in \mathbb{Z}$ entonces $\alpha \cdot \alpha_1 \in U(\mathbb{Z}) = \{1, -1\}$. Por lo tanto deducimos que $a^2 + b^2 - ab = \pm 1$.

Vamos a suponer que $|a| \geq |b|$ con $a, b \in \mathbb{Z}$. Si por lo contrario fuera $|a| \leq |b|$, procedemos de forma análoga. Distinguimos los siguientes casos. Supongamos que $b \neq 0, 1$. Entonces $a^2 + b^2 > ab \pm 1$. Esta desigualdad es falsa porque $a, b \in \mathbb{Z}$ y si tomamos

$a = 1$ y $b = 2$ no se verifica. Luego llegamos a una contradicción. Supongamos que $b = 0$. Entonces $\alpha = a \in \mathbb{Z}$. Como $\alpha \in U(\mathbb{Z}[\zeta_3])$ deducimos que $\alpha = \pm 1$, de donde obtenemos que $\pm 1 \in U(\mathbb{Z}[\zeta_3])$.

Supongamos que $b = 1$. Entonces $a^2 + 1 = a \pm 1$ por lo que o bien $a^2 = a$ o bien $a^2 - a + 2 = 0$. Vamos a distinguir estos dos subcasos. Si $a^2 - a + 2 = 0$ entonces $a = \frac{1 \pm \sqrt{1-8}}{2}$ no tiene solución entera. Contradicción. Supongamos ahora que $a^2 = a$. Entonces $a^2 - a = 0$, lo cual implica que $a \cdot (a - 1) = 0$. Entonces deducimos que o bien $a = 0$ o bien $a = 1$. Si $a = 0$ entonces $\alpha = b\zeta_3 = \pm\zeta_3$ porque $b = 1$ y $|\alpha| = 1$. Luego $\pm\zeta_3 \in U(\mathbb{Z}[\zeta_3])$. Por otro lado, si $a = 1$ entonces $\alpha = 1 + \zeta_3 = -\zeta_3^2$ porque $\Phi_3(\zeta_3) = 0$. De donde deducimos que $\pm\zeta_3^2 \in U(\mathbb{Z}[\zeta_3])$. Por lo tanto hemos demostrado que $U(\mathbb{Z}[\zeta_3]) = \{\pm 1,\ \pm\zeta_3,\ \pm\zeta_3^2\}$. □

Lema 3.8. *Si ζ_4 una raíz compleja primitiva de la unidad de orden 4 entonces*

$$U(\mathbb{Z}[\zeta_4]) = \{\pm 1,\ \pm i\}\,.$$

Demostración. Sabemos que las raíces cuartas complejas de la unidad son $\{\pm 1, \pm i\}$. Supongamos que $\zeta_4 = i$ entonces $\mathbb{Z}[i] = \{a + bi \ :\ a, b \in \mathbb{Z}\}$. Sea $\alpha \in U(\mathbb{Z}[i])$. Supongamos que $\alpha = a + bi$ con $a, g \in \mathbb{Z}$. Entonces $\| \alpha \| = a^2 + b^2 = 1$ porque α es unidad. Como $a, b \in \mathbb{Z}$ y $a^2 + b^2 = 1$ entonces deducimos que o bien $a = \pm 1$ y $b = 0$, en cuyo caso tendríamos que $\alpha = \pm 1$, o bien $a = 0$ y $b = \pm 1$, en cuyo caso tendríamos que $\alpha = \pm i$. Luego hemos demostrado que $U(\mathbb{Z}[\zeta_4]) = \{\pm 1,\ \pm i\}$. □

Teorema 3.9. *Teorema de Higman.*

Sea G un grupo de torsión. Todas las unidades de $\mathbb{Z}G$ son triviales si y solo si se verifica una de las siguientes condiciones:

1. *G es un grupo abeliano de exponente igual a $1, 2, 3, 4$ ó 6.*

2. *G es un 2-grupo Hamiltoniano.*

Demostración. Si todas las unidades de $\mathbb{Z}G$ son triviales, entonces utilizando la Proposición 3.6 sabemos que se verifica una de las dos condiciones del enunciado. Vamos a demostrar el recíproco. Para ello, supongamos que G es un grupo abeliano finito de exponente igual a $1, 2, 3, 4, 6$. Utilizando el Teorema 1.9 de Perlis-Walker deducimos que existe un isomorfismo $\mu : \mathbb{Q}G \longrightarrow \oplus_{d|n} a_d \mathbb{Q}(\zeta_d)$ donde ζ_d es una raíz compleja primitiva

de la unidad de orden d y $a_d = \frac{n_d}{[\mathbb{Q}(\zeta_d):\mathbb{Q}]}$ donde n_d es el número de elementos de orden d en G. Deducimos que solamente las raíces de la unidad cuyos órdenes coinciden con órdenes de elementos de G aparecen en la descomposición. Como $\oplus_{d|n} a_d\mathbb{Z}[\zeta_d] \subseteq \oplus_{d|n} a_d\mathbb{Q}[\zeta_d]$ entonces podemos definir

$$R = \mu^{-1}\left(\oplus_{d|n} a_d\mathbb{Z}[\zeta_d]\right)$$

Por un lado, es bien conocido que si G es un grupo abeliano finito entonces se puede expresar como producto directo de sus subgrupos cíclicos. Como además el exponente de G es $1, 2, 3, 4$ ó 6, entonces se nos pueden presentar los siguientes casos: $G \simeq C_2 \times \cdots \times C_2$, $G \simeq C_3 \times \cdots \times C_3$, $G \simeq C_4 \times \cdots \times C_4$, $G \simeq C_2 \times \cdots \times C_2 \times C_4 \times \cdots \times C_4$ y $G \simeq C_2 \times \cdots \times C_2 \times C_3 \times \cdots C_3$. Utilizando el Lema 3.1 deducimos que basta solo con considerar los casos $G \simeq C_3 \times \cdots \times C_3$ y $G \simeq C_4 \times \cdots \times C_4$. Utilizando la descomposición que nos facilita el Teorema 1.9 de Perlis-Walker y utilizando el Lema 3.7 y el lema 3.8 sabemos que hay un número finito de unidades en $a_d\mathbb{Z}[\zeta_d]$ para $d = 1, 2, 3, 4$. Entonces tenemos un número finito de unidades en $\oplus_{d|n} a_d\mathbb{Z}[\zeta_d]$. Como μ es un isomorfismo, entonces R tiene un número finito de unidades. Como $U(\mathbb{Z}G) \subseteq U(R)$ entonces deducimos que hay un número finito de unidades en $\mathbb{Z}G$. Al ser G un grupo abeliano, podemos utilizar el Corolario 2.13 y obtenemos que todas las unidades de torsión en $\mathbb{Z}G$ son triviales. Luego todas las unidades de $\mathbb{Z}G$ son triviales.

Por otro lado, supongamos que G es un grupo abeliano no finito y de torsión con exponente igual a $1, 2, 3, 4$ ó 6. Sea $u \in U(\mathbb{Z}G)$. Sabemos que $supp(u)$ es finito. Como G es abeliano entonces se tiene que un conjunto de elementos de torsión de G generan un subgrupo finito. Luego $supp(u)$ genera un subgrupo finito de G. Tomamos $H = \langle supp(u), supp(u^{-1})\rangle$. Como $supp(u) \subseteq H$ entonces $u \in \mathbb{Z}H$. De forma análoga, como $supp(u^{-1}) \subseteq H$ entonces $u^{-1} \in \mathbb{Z}H$. Por lo tanto, deducimos que $u \in U(\mathbb{Z}H)$. Como H es un grupo abeliano finito de exponente $1, 2, 3, 4$ ó 6 entonces utilizando el caso anterior deducimos que u es una unidad trivial en $\mathbb{Z}G$.

Supongamos ahora que G es un 2-grupo Hamiltoniano. Utilizando el Teorema 1.5 sabemos que $G = K_8 \times E \times A$, donde E es un 2-grupo abeliano elemental y A es un grupo abeliano con todos los elementos de orden impar. Como G es 2-grupo entonces $|G| = 2^\alpha$ con $\alpha \in \mathbb{Z}$ y para todo $g \in G$ se tiene que $o(g) = 2^\beta$ para algún $\beta \in \mathbb{Z}$. Aplicando que todo elemento de A tiene orden impar deducimos que $A = \{1\}$. Luego $G = K_8 \times E = K_8 \times C_2 \times \cdots \times C_2 \times \cdots$. Usando el Teorema 3.4 deducimos que todas

las unidades de $\mathbb{Z}K_8$ son triviales y por el Lema 3.1 obtenemos que todas las unidades de $\mathbb{Z}(K_8 \times C_2)$ son triviales. Continuando de esta forma el proceso demostramos que todas las unidades de $\mathbb{Z}G$ son triviales. □

Teorema 3.10. *Sea G un grupo finito. Entonces $U(\mathbb{Z}G)$ es un grupo finito si y solo si se verifica una de las siguientes condiciones:*

1. *G es un grupo abeliano de exponente igual a $1, 2, 3, 4$ ó 6.*

2. *G es un 2-grupo Hamiltoniano.*

Demostración. Como G un grupo finito, en particular, G es un grupo de torsión. Supongamos que se verifica la condición 1 ó la condición 2 del enunciado. Entonces utilizando el Teorema de Higman 3.9 deducimos que todas las unidades de $\mathbb{Z}G$ son triviales. Luego $U(\mathbb{Z}G) = \pm G$. Como G es finito entonces $U(\mathbb{Z}G)$ es un grupo finito. Con lo que demostraríamos esta implicación.

Supongamos ahora que $U(\mathbb{Z}G)$ es un grupo finito. Es claro que para todo $g, h \in G$ se tiene que $\mu_{g,h}$ es una unidad trivial en $\mathbb{Z}G$, porque en caso contrario, utilizando la proposición 2.6 deduciríamos que $\mu_{g,h}$ tiene orden infinito, en contradicción con que $U(\mathbb{Z}G)$ sea un grupo finito. Por lo tanto, aplicando la Proposición 2.4 deducimos que para todo $g, h \in G$ se tiene que h normaliza a $\langle g \rangle$. Esto implica que todo subgrupo cíclico de G es normal por lo que todo subgrupo de G es normal. Entonces o bien G es un grupo abeliano, o bien G es un grupo Hamiltoniano. Distinguimos los dos casos posibles.

Supongamos en primer lugar que G es un grupo abeliano. Utilizando el Corolario 2.13 sabemos que todas las unidades de torsión de $\mathbb{Z}G$ son triviales. Como G es finito, entonces todas las unidades de $\mathbb{Z}G$ son triviales. Aplicamos el Teorema 3.9 de Higman y deducimos que G es un grupo abeliano de exponente $1, 2, 3, 4$ ó 6.

Supongamos ahora en último lugar que G es un grupo Hamiltoniano. Utilizando el Teorema 1.5 obtenemos que $G = K_8 \times E \times A$, donde E es un 2-grupo abeliano elemental y A es un grupo abeliano con todos los elementos de orden impar. Sea $x \in A$ con $o(x) = p$ siendo p un primo positivo impar. Como a tiene orden 4 en K_8 entonces $g = ax \in G$ tiene orden $4p$. Pero $4p \neq 1, 2, 3, 4, 6$ para todo primo positivo impar p. Luego $p = 1$, lo que implica que $A = \{1\}$. Por lo tanto hemos demostrado que $G = K_8 \times E = K_8 \times C_2 \times \cdots \times C_2$. Por lo tanto G es un 2-grupo Hamiltoniano. □

Capítulo 4

El grupo de unidades de $\mathbb{Z}C_n$.

Este capítulo está destinado a calcular el grupo de unidades de $\mathbb{Z}C_n$, para valores de n pequeños. Los casos $n = 5$ y $n = 8$ los estudiaremos de forma separada.

Teorema 4.1. *Si $n = 1,\ 2,\ 3,\ 4,\ 6$ entonces se verifica que $U(\mathbb{Z}C_n) = \pm C_n$.*

Demostración. Como C_n es un grupo abeliano de torsión y con exponente n, entonces utilizando el Teorema de Higman 3.9 deducimos que todos las unidades de $\mathbb{Z}C_n$ son triviales. Por lo tanto se tiene que $U(\mathbb{Z}C_n) = \pm C_n$. □

En las sucesivas secciones, vamos a denotar el *módulo* de un elemento $x \in \mathbb{C}$ por $|x| = x \cdot \bar{x}$.

4.1. Unidades en $\mathbb{Z}C_8$.

El objetivo de esta sección es calcular el grupo de unidades de $\mathbb{Z}C_8$. Para ello necesitamos varios resultados previos.

Lema 4.2. $U(\mathbb{Z}[i]) = \{\pm 1,\ \pm i\}$.

Demostración. Supongamos que $\alpha = a + bi \in U(\mathbb{Z}[i])$. Entonces existe $\alpha^{-1} = \frac{1}{a+bi}$ tal que $\alpha \cdot \alpha^{-1} = 1$. Como $\alpha^{-1} = \frac{1}{a+bi} \cdot \frac{a-bi}{a-bi} = \frac{a}{a^2+b^2} - \frac{b}{a^2+b^2} i$ entonces se tiene que $\alpha^{-1} \in \mathbb{Z}[i]$ si y solo si $\frac{a}{a^2+b^2} \in \mathbb{Z}$ y $\frac{b}{a^2+b^2} \in \mathbb{Z}$. Esto último es cierto si y solo si $a^2+b^2 = \pm 1$. Además, esto solamente puede ocurrir si $a = 0$, en cuyo caso tendríamos que $b = \pm 1$, o cuándo $b = 0$, en cuyo caso tendríamos que $a = \pm 1$. Luego se tiene que $U(\mathbb{Z}[i]) = \{\pm 1,\ \pm i\}$. □

Sea d un número entero libre de cuadrados y distinto de 1. Consideramos la aplicación $N : \mathbb{Q}(\sqrt{d}) \longrightarrow \mathbb{Q}$ dada por $N(a+b\sqrt{d}) = a^2 - db^2$. Es bien conocido que N posee

buenas propiedades algebraicas. Entre ellas, destacamos que $u \in U(\mathbb{Z}[\sqrt{d}])$ si y solo si $N(u) = \pm 1$.

Consideramos también la aplicación $\Phi : \mathbb{Z}[\sqrt{d}] \longrightarrow \mathbb{R} \times \mathbb{R}$ dada por $\Phi(a + b\sqrt{d}) = (a + b\sqrt{d}, a - b\sqrt{d})$. Se verifica que la aplicación Φ es inyectiva y además envía $\mathbb{Z}[\sqrt{d}]$ a un subconjunto discreto de $\mathbb{R} \times \mathbb{R}$. Además, utilizando el párrafo anterior deducimos que toda unidad de $\mathbb{Z}[\sqrt{d}]$ es enviada a una de las hipérbolas $xy = 1$ y $xy = -1$.

Lema 4.3. $U(\mathbb{Z}[\sqrt{2}]) = \langle -1 \rangle \times \langle 1 + \sqrt{2} \rangle$.

Demostración. Tomamos $u = 1 + \sqrt{2}$. Como $N(u) = -1$ entonces $u \in U(\mathbb{Z}[\sqrt{2}])$. Sea $v = a + b\sqrt{2} \in \mathbb{Z}[\sqrt{2}]$ con $a,\ b \in \mathbb{Z}$. Llamamos $K = \{(x, y) \in \mathbb{R} \times \mathbb{R} : |x|,\ |y| \leq u\}$. Supongamos que $\Phi(v) = (a + b\sqrt{2},\ a - b\sqrt{2}) \in K$. Aplicando que $|a - b\sqrt{2}| < 3$ se tiene que $|2a| = |2a + b\sqrt{2} - b\sqrt{2}| \leq |a + b\sqrt{2}| + |a - b\sqrt{2}| \leq 2|u| < 2 \cdot 3$. Luego $|a| \leq |u| < 3$. Además, obtenemos que $|2b\sqrt{2}| \leq |a - a + 2b\sqrt{2}| \leq |a + b\sqrt{2}| + |a - b\sqrt{2}| \leq 2|u| < 2 \cdot 3$, luego $|b| \leq \frac{|u|}{\sqrt{2}} < 2$.

Supongamos además que $v \in U(\mathbb{Z}[\sqrt{2}])$, entonces se tiene que $a^2 - 2b^2 = \pm 1$, o equivalentemente, $\Phi(v)$ es una de las dos hipérbolas $xy = 1$ y $xy = -1$. Por lo tanto obtenemos 6 unidades posibles, $v = \pm 1$, $\pm(1 + \sqrt{2})$ ó $\pm(1 - \sqrt{2})$.

Supongamos que v es una unidad no trivial y arbitraria en $\mathbb{Z}[\sqrt{2}]$. Para obtener el resultado tenemos que probar que $v \in \langle -1,\ u \rangle$. Vamos a asumir que $v > 0$, ya que en el caso de que fuera negativo, remplazaríamos v por $-v$. Además vamos a suponer que $v \geq 1$, ya que si v fuera menor que 1, entonces remplazaríamos v por v^{-1}. Por lo tanto, existe algún entero no negativo k tal que $u^k \leq v < u^{k+1}$. Luego esto implica que $w = vu^{-k}$ es una unidad de $U(\mathbb{Z}[\sqrt{2}]) \cap [1,\ u)$. Entonces $\Phi(w) \in K$ y además w tiene que ser una de las 6 opciones anteriores en el rango $[1,\ u)$, por lo que $w = 1$. Entonces tenemos que $v = u^k$. Luego $U(\mathbb{Z}[\sqrt{2}]) = \langle -1 \rangle \times \langle 1 + \sqrt{2} \rangle$. □

Es importante remarcar que si n es impar entonces $-\zeta_n$ tiene orden $2n$ y $\mathbb{Z}[\zeta_n] = \mathbb{Z}[\zeta_{2n}]$. Claramente se tiene que $U(\mathbb{Z}[\zeta_1]) = U(\mathbb{Z}[\zeta_2]) = U(\mathbb{Z}) = \langle -1 \rangle$ y hemos visto en el Lema 4.2 que $U(\mathbb{Z}[\zeta_4]) = U(\mathbb{Z}[i]) = \langle i \rangle$. Vamos a calcular a continuación $U(\mathbb{Z}[\zeta_8])$.

Lema 4.4. $U(\mathbb{Z}[\zeta_8]) = \langle \zeta_8 \rangle \times \langle 1 + \sqrt{2} \rangle = \langle \zeta_8 \rangle \times \langle \eta_3(\zeta_8) \rangle \simeq C_8 \times C_\infty$, *donde* $\eta_3(\zeta_8) = 1 + \zeta_8 + \zeta_8^2$.

Demostración. Tomamos $\zeta_8 = e^{\frac{\pi i}{4}} = \frac{\sqrt{2}}{2}(1+i)$. Entonces se tiene que $\zeta_8^2 = i$ y además se verifica $(\zeta_8 + \zeta_8^{-1})^2 = \zeta_4 + 2 + \zeta_4^{-1} = i + 2 - i = 2$. Esto implica que $\mathbb{Z}[\sqrt{2}] \subset \mathbb{Z}[\zeta_8]$ porque

$\zeta_8+\zeta_8^{-1}=\pm\sqrt{2}$. Sea $u=1+\sqrt{2}$. Sabemos por el Lema 4.3 que $U(\mathbb{Z}[\sqrt{2}])=\langle -1\rangle\times\langle u\rangle$. Luego $\langle -1\rangle\times\langle u\rangle\subseteq U(\mathbb{Z}[\zeta_8])$. Llamamos $v=\eta_3(\zeta_8)$. Entonces $v=1+\zeta_8+\zeta_8^2=1+\zeta_8+\zeta_4=1+\zeta_8+i$. Aplicando que $\zeta_8=\frac{\sqrt{2}}{2}(1+i)$ obtenemos los siguiente:

$$v=\left(1+\frac{\sqrt{2}}{2}\right)\cdot(1+i)=\frac{\sqrt{2}}{2}\cdot(\sqrt{2}+1)\cdot(1+i)=\zeta_8 u$$

Por lo tanto tenemos que $\langle\zeta_8,u\rangle=\langle\zeta_8,v\rangle$. Tomamos $x\in U(\mathbb{Z}[\zeta_8])$. Como $\zeta_8^4=-1$, entonces existen enteros a, b, c y d tales que $x=a+b\zeta_8+c\zeta_8^2+d\zeta_8^3$. Aplicando que $\zeta_8^2+\zeta_8^{-2}=i-i=0$ y que $\zeta_8+\zeta_8^{-1}=-\zeta_8^3-\zeta_8^{-3}=\sqrt{2}$ obtenemos lo siguiente:

$$\begin{aligned}|x|^2 &= (a+b\zeta_8+c\zeta_8^2+d\zeta_8^3)\cdot(a+b\zeta_8^{-1}+c\zeta_8^{-2}+d\zeta_8^{-3})\\ &= a^2+b^2+c^2+d^2+(ab+bc+cd)\cdot(\zeta_8+\zeta_8^{-1})+(ac+bd)\cdot(\zeta_8^2+\zeta_8^{-2})\\ &\quad +ad(\zeta_8^3+\zeta_8^{-3})\\ &= a^2+b^2+c^2+d^2+(ab+bc+cd-ad)\sqrt{2}\end{aligned}$$

Entonces, la aplicación $x\mapsto|x|^2$ define un homomorfismo de grupos

$$N:\ U(\mathbb{Z}[\zeta_8])\longrightarrow U(\mathbb{Z}[\sqrt{2}])\cap\mathbb{R}^+=\langle u\rangle.$$

Además el núcleo de N es $\langle\zeta_8\rangle$ y $N(u)=u^2$. Como la imagen de N toma valores positivos, es claro que u no puede estar en la imagen de N. Por lo tanto tenemos que la imagen de N es $\langle u^2\rangle\simeq\mathbb{Z}$. Aplicando que $\mathbb{Z}$ es un grupo libre desde el punto de vista aditivo, sabemos que $\mathbb{Z}$ es proyectivo visto como módulo y por lo tanto el homomorfismo N se escinde. Luego $U(\mathbb{Z}[\zeta_8])=\langle\zeta_8\rangle\times\langle w\rangle$ para todo $w\in N^{-1}(u^2)$. Utilizando que u, $v\in N^{-1}(u^2)$ deducimos que $U(\mathbb{Z}[\zeta_8])=\langle\zeta_8\rangle\times\langle 1+\sqrt{2}\rangle$. □

Vamos a realizar un argumento que nos será de gran utilidad en la demostración del siguiente teorema.

Consideramos $C_n=\langle g\rangle$. Para cada divisor d de n, tomamos una raíz d-ésima primitiva de la unidad ζ_d en $\mathbb{C}$ y definimos el homomorfismo de grupos $\rho_d:C_n\longrightarrow U(\mathbb{C})$ dado por $\rho_d(g)=\zeta_d$. Es claro que ρ_d es una representación de C_n y además se puede extender a un homomorfismo suprayectivo de álgebras racionales

$$\rho_d:\ \mathbb{Q}C_n\longrightarrow\mathbb{Q}(\zeta_d).$$

Utilizando el Corolario 1.10 llegamos a la conclusión de que existe un isomorfismo

$$\Phi = \prod_{d|n} \rho_d : \mathbb{Q}C_n \longrightarrow \prod_{d|n} \mathbb{Q}(\zeta_d) \tag{4.1.1}$$

Además, $\Phi(\mathbb{Z}C_n) \subset \prod_{d|n} \mathbb{Z}[\zeta_d]$. Por lo tanto Φ se restringe a un homomorfismo de grupos inyectivo de la siguiente forma:

$$\Phi : U(\mathbb{Z}C_n) \longrightarrow \prod_{d|n} U(\mathbb{Z}[\zeta_d]) \tag{4.1.2}$$

De hecho, si $d \neq 1$ entonces $\rho_d(\hat{g}) = 0$. Por lo tanto tenemos la siguiente relación:

$$\rho_d(u_{k,m}(g)) = \begin{cases} 1 & si\ d = 1 \\ \eta_k(\zeta_d)^m & si\ d \neq 1 \end{cases} \tag{4.1.3}$$

Consideramos G un grupo y N un subgrupo normal de G. Entonces la *aplicación aumento módulo* N es el homomorfismo de anillos

$$\begin{array}{rccc} \epsilon_{N,R} : & RG & \longrightarrow & R(G/N) \\ & \sum_{g\in G} a_g g & \mapsto & \displaystyle\sum_{g\in G} a_g(gN) \end{array}$$

Al núcleo de $\epsilon_{N,R}$ lo llamaremos el *ideal de aumento de* RG *módulo* N. En el caso en que no haya confusión con el anillo R, escribiremos $\epsilon_{N,R}$ como ϵ_N. Obsérvese que $\epsilon_G = \epsilon$ coincide con la aplicación aumento de RG definida en la sección 1.4.

Teorema 4.5. *Sea* $C_8 = \langle g \rangle$ *con* $o(g) = 8$. *Entonces se verifica lo siguiente:*

$$U(\mathbb{Z}C_8) = \pm C_8 \times \langle u_{3,2}(g) \rangle_\infty$$

Demostración. Utilizando 4.2.2 obtenemos lo siguiente:

$$\Phi = \prod_{d|8} \rho_d : \mathbb{Q}C_8 \longrightarrow \prod_{d|8} \mathbb{Q}(\zeta_d).$$

Además se tiene que $\Phi(\mathbb{Z}C_8) \subset \mathbb{Z} \times \mathbb{Z} \times \mathbb{Z}[i] \times \mathbb{Z}[\zeta_8]$ y por lo tanto $U(\mathbb{Z}C_8)$ es isomorfo a un subgrupo de $U(\mathbb{Z}) \times U(\mathbb{Z}) \times U(\mathbb{Z}[i]) \times U(\mathbb{Z}[\zeta_8])$. Llamamos $b = u_{3,2}(g)$ y $v = \eta_3(\zeta_8)$. Por el Lema 4.4 deducimos lo siguiente:

$$U(\mathbb{Z}[\zeta_8]) = \pm\langle \zeta_8 \rangle \times \langle v \rangle.$$

Utilizando la relación 4.3.2 obtenemos que:

$$\Phi(b) = (1,\ \eta_3((-1))^2,\ \eta_3(i)^2,\ \eta_3(\zeta_8)^2) = (1,\ 1,\ -1,\ v^2).$$

Vamos a demostrar que $\rho_8(U(\mathbb{Z}C_8)) = \pm\langle\zeta_8\rangle \times \langle v^2\rangle$. Como $\rho_8(g) = \zeta_8$ entonces es claro que $\rho_8(\pm C_8) = \pm\langle\zeta_8\rangle$. Además, utilizando que $\rho_8(b) = v^2$, obtenemos lo siguiente:

$$\pm\langle\zeta_8\rangle \times \langle v^2\rangle \subseteq \rho_8(U(\mathbb{Z}C_8)) \subseteq U(\mathbb{Z}[\zeta_8]) = \pm\langle\zeta_8\rangle \times \langle v\rangle.$$

Además se tiene que $[\pm\langle\zeta_8\rangle \times \langle v\rangle\ :\ \pm\langle\zeta_8\rangle \times \langle v^2\rangle] = 2$. Luego lo único que tenemos que demostrar es que $\rho_8(U(\mathbb{Z}C_8)) \subsetneq U(\mathbb{Z}[\zeta_8])$. Para ello vamos a probar que $v \notin \rho_8(U(\mathbb{Z}C_8))$. Procedemos por reducción al absurdo. Supongamos que existe $u = \sum_{i=0}^{7} u_i g^i \in U(\mathbb{Z}C_8)$ tal que $\rho_8(u) = v$. Aplicando que $v = \eta_3(\zeta_8) = 1 + \zeta_8 + \zeta_8^2$ obtenemos lo siguiente:

$$1 + \zeta_8 + \zeta_8^2 = \rho_8(u) = \sum_{i=0}^{7} u_i\zeta_8^i = (u_0 - u_4) + (u_1 - u_5)\cdot\zeta_8 + (u_2 - u_6)\cdot\zeta_8^2 + (u_3 - u_7)\cdot\zeta_8^3$$

Como es bien conocido que $\{1,\ \zeta_8,\ \zeta_8^2,\ \zeta_8^3\}$ es una base de $\mathbb{Q}(\zeta_8)$ sobre $\mathbb{Q}$ entonces tenemos que $u_0 - u_4 = u_1 - u_5 = u_2 - u_6 = 1$ y $u_3 - u_7 = 0$. Consideramos la aplicación aumento módulo $\langle g^4\rangle$:

$$\epsilon_{\langle g^4\rangle}\ :\ \mathbb{Z}C_8/\langle g^4\rangle \longrightarrow \mathbb{Z}C_4/\langle g^4\rangle.$$

Entonces se tiene que $\epsilon_{\langle g^4\rangle}(u) = (u_0 + u_4) + (u_1 + u_5)\bar{g} + (u_2 + u_6)\bar{g}^2 + (u_3 - u_7)\bar{g}^3 = (2u_0 - 1) + (2u_1 - 1)\bar{g} + (2u_2 - 1)\bar{g}^2 + 2u_3\bar{g}^3$. Como $u \in U(\mathbb{Z}C_8)$ y $\epsilon_{\langle g^4\rangle}$ es un homomorfismo entonces se tiene que $\epsilon_{\langle g^4\rangle}(u) \in U(\mathbb{Z}C_4)$ módulo $\langle g^4\rangle$. Contradicción porque utilizando el Teorema 4.1 sabemos que $U(\mathbb{Z}C_4) = \pm C_4$ pero $\epsilon_{\langle g^4\rangle}(u) \notin \pm C_4$ módulo $\langle g^4\rangle$. Luego $v \notin \rho_8(U(\mathbb{Z}C_8))$ y esto implica que $\rho_8(U(\mathbb{Z}C_8)) = \pm\langle\zeta_8\rangle \times \langle v^2\rangle$.

Tomamos $u \in U(\mathbb{Z}C_8)$. Entonces $\Phi(u) \in U(\mathbb{Z}) \times U(\mathbb{Z}) \times U(\mathbb{Z}[i]) \times U(\mathbb{Z}[\zeta_8])$, donde $\rho_8(u) = \pm\zeta_8^i v^{2k}$ para ciertos i, k. De forma análoga tendríamos que $\Phi(b^k) \in U(\mathbb{Z}) \times U(\mathbb{Z}) \times U(\mathbb{Z}[i]) \times U(\mathbb{Z}[\zeta_8])$, donde $\rho_8(b^k) = v^{2k}$. Por lo tanto tenemos que $\Phi(ub^{-k}) = (\rho_1(ub^{-k}),\ \rho_2(ub^{-k}),\ \rho_4(ub^{-k}),\ \rho_8(ub^{-k}))$, donde $\rho_8(ub^{-k}) = \pm\zeta_8^i$ claramente tiene orden finito. Luego como $U(\mathbb{Z}) = \{1, -1\}$, $U(\mathbb{Z}[i]) = \langle i\rangle$ y aplicando que $\rho_8(ub^{-k})$ tiene orden finito, deducimos que $\Phi(ub^{-k})$ tiene orden finito. Como Φ es inyectiva, entonces ub^{-k} es una unidad de torsión en $\mathbb{Z}C_8$. Utilizando el Corolario 2.13 deducimos que ub^{-k} es una unidad trivial en $\mathbb{Z}C_8$. Luego todas las unidades triviales de $\mathbb{Z}C_8$ son de la forma ub^{-k} con $u \in U(\mathbb{Z}C_8)$. Por lo tanto se tiene que $U(\mathbb{Z}C_8) = \pm C_8 \times \langle b\rangle_\infty$. □

4.2. Unidades en $\mathbb{Z}C_5$.

Sea p un número primo. Consideramos ζ_p una raíz p-ésima primitiva compleja de la unidad. Definimos el siguiente conjunto:

$$U_1(\mathbb{Z}[\zeta_p]) = \{y \in U(\mathbb{Z}[\zeta_p]) \ : \ y \equiv 1 \mod (\zeta_p - 1)\}.$$

Es fácil ver que $U_1(\mathbb{Z}[\zeta_p])$ es un subgrupo de $U(\mathbb{Z}[\zeta_p])$. Supongamos que $C_p = \langle x \rangle$, con $o(x) = p$. Utilizando el Corolario 1.10 deducimos que existe un isomorfismo

$$\mu : \mathbb{Q}C_p \longrightarrow \mathbb{Q} \oplus \mathbb{Q}[\zeta_p]$$

dado por $\mu(\sum_{i=0}^{p-1} c_i x^i) = (\sum_{i=0}^{p-1} c_i, \sum_{i=0}^{p-1} c_i \zeta_p^i)$. Como $\mathbb{Z} \oplus \mathbb{Z}[\zeta_p] \subseteq \mathbb{Q} \oplus \mathbb{Q}[\zeta_p]$ entonces podemos definir

$$M = \mu^{-1}(\mathbb{Z} \oplus \mathbb{Z}[\zeta_p])$$

Es claro que $\mathbb{Z}C_p \subset M \subset \mathbb{Q}C_p$. Además $\mathbb{Z}C_p$ y M son ordenes en $\mathbb{Q}C_p$. Aplicando el Teorema de las Unidades de Dirichlet 1.11 deducimos que $U(\mathbb{Z}[\zeta_p])$ es un grupo abeliano finitamente generado para todo p. Por lo tanto $U(M)$ está también finitamente generado. Usando ahora el Lema 1.16 obtenemos que el índice $[U(M) \ : \ U(\mathbb{Z}C_p)]$ es finito, lo que implica que $U(\mathbb{Z}C_p)$ es un grupo abeliano finitamente generado.

Proposición 4.6. *Sea $p > 3$ un número primo y sea ζ_p una raíz p-ésima primitiva de la unidad en $\mathbb{C}$. Entonces se verifican las siguientes propiedades:*

1. $\mu(U_1(\mathbb{Z}C_p)) = U(\mathbb{Z}) \oplus U_1(\mathbb{Z}[\zeta_p])$.
2. $[U(\mathbb{Z}[\zeta_p]) \ : \ U_1(\mathbb{Z}[\zeta_p])] = p - 1$.

Demostración. Vamos a justificar el primer apartado de la proposición. Supongamos que $u = \sum_{i=0}^{p-1} c_i x^i \in U_1(\mathbb{Z}C_p)$. Entonces se verifica lo siguiente:

$$\mu(u) = (\sum_{i=0}^{p-1} c_i, \ \sum_{i=0}^{p-1} c_i \zeta_p^i) = (1, \ \sum_{i=0}^{p-1} c_i \zeta_p^i)$$

Llamamos $\alpha = \sum_{i=0}^{p-1} c_i \zeta_p^i$ y $\pi = \zeta_p - 1$. Entonces se verifica la siguiente congruencia:

$$\alpha = \sum_{i=0}^{p-1} c_i(\zeta_p^i - 1) + \sum_{i=0}^{p-1} c_i = 1 + \sum_{i=0}^{p-1} c_i(\zeta_p^i - 1) \equiv 1 \mod \pi$$

Luego $\alpha \in U_1(\mathbb{Z}[\zeta_p])$. Lo que implica que $\mu(u) = (1, \alpha) \in U(\mathbb{Z}) \oplus U_1(\mathbb{Z}[\zeta_p])$.

Tomamos ahora $\beta = \sum_{i=0}^{p-1} b_i \zeta_p^i \in U_1(\mathbb{Z}[\zeta_p])$. Vamos a demostrar que $\sum_{i=0}^{p-1} b_i = 1$. Como $\beta \in U_1(\mathbb{Z}[\zeta_p])$ entonces $\beta \equiv 1 \mod \zeta_p - 1$. Por lo tanto, existe un $c \in \mathbb{Z}[\zeta_p]$ tal que $\beta = 1 + c(\zeta_p - 1)$. Pongamos que $c = \sum_{i=0}^{p-1} c_i \zeta_p^i$. Entonces se tiene que $\beta = 1 + \sum_{i=0}^{p-1} c_i \zeta_p^i (\zeta_p - 1) = 1 + \sum_{i=0}^{p-1} c_i \zeta_p^{i+1} - c_i \zeta_p^i = 1(1 - c_0 + c_{p-1}) + \sum_{i=1}^{p-1} (c_{i-1} - c_i)\zeta_p^i$. Tomamos

$$b_i = \begin{cases} 1 - c_0 + c_{p-1} & \text{si } i = 0 \\ c_{i-1} - c_i & \text{si } i \neq 0 \end{cases}$$

Por lo tanto, se tiene lo siguiente: $\sum_{i=0}^{p-1} b_i = 1 - c_0 + c_{p-1} + c_0 - c_1 + c_1 - c_2 + \cdots + c_{p-2} - c_{p-1} = 1$. Consideramos $u = \sum_{i=0}^{p-1} b_i x^i$. Entonces se tiene que:

$$\mu(u) = (\sum_{i=0}^{p-1} b_i,\ \sum_{i=0}^{p-1} b_i \zeta_p^i) = (1,\ \beta) \in U(\mathbb{Z}) \oplus U_1(\mathbb{Z}[\zeta_p])$$

Por lo tanto, como μ es un isomorfismo de M a $\mathbb{Z} \oplus \mathbb{Z}[\zeta_p]$ tenemos que u es una unidad en M. Además, si aplicamos la Proposición 1.17 deducimos que $u \in U_1(\mathbb{Z}C_p)$. Luego $\mu(U_1(\mathbb{Z}C_p)) = U(\mathbb{Z}) \oplus U_1(\mathbb{Z}[\zeta_p])$.

Veamos ahora el segundo apartado de la proposición. Como $M \simeq \mathbb{Z} \oplus \mathbb{Z}[\zeta_p]$ entonces $U(M) \simeq U(\mathbb{Z}) \oplus U(\mathbb{Z}[\zeta_p])$. Además $U(\mathbb{Z}C_p) \subseteq U(M)$ y $\langle \pm 1 \rangle \times U_1(\mathbb{Z}[\zeta_p]) \subseteq U(\mathbb{Z}) \oplus U(\mathbb{Z}[\zeta_p])$. Consideramos el homomorfismo de anillos $f : \mathbb{Z}[\zeta_p] \longrightarrow \mathbb{Z}[\zeta_p]/\langle \zeta_p - 1 \rangle$ que se restringe de forma canónica a un homomorfismo de grupos $g : U(\mathbb{Z}[\zeta_p]) \longrightarrow U(\mathbb{Z}[\zeta_p]/\langle \zeta_p - 1 \rangle)$. Además se verifica que el núcleo de g es $U_1(\mathbb{Z}[\zeta_p])$. Recordemos que μ venía dada por $\mu(\sum_{i=0}^{p-1} c_i x^i) = (\sum_{i=0}^{p-1} c_i, \sum_{i=0}^{p-1} c_i \zeta_p^i)$. Además se tiene la siguiente congruencia:

$$\sum_{i=0}^{p-1} c_i \zeta_p^i \equiv \sum_{i=0}^{p-1} c_i \mod \zeta_p - 1.$$

Esto implica que cada elemento de $\mathbb{Z}[\zeta_p]/\langle \zeta_p - 1 \rangle$ tiene un representante en $\mathbb{Z}$. Además, aplicando que $x^p - 1 = \prod_{i=0}^{p-1}(x - \zeta_p^i)$ deducimos que $1 + x + x^2 + \cdots + x^{p-1} = \frac{x^p - 1}{x - 1} = \prod_{i=1}^{p-1}(x - \zeta_p^i)$. Tomando $x = 1$ obtenemos que $p = \prod_{i=1}^{p-1}(1 - \zeta_p^i)$. Luego p es múltiplo de $\zeta_p - 1$. Por lo tanto $\mathbb{Z}[\zeta_p]/\langle \zeta_p - 1 \rangle$ tiene exactamente p elementos y cada uno de ellos tiene un representante en $\mathbb{Z}$. Luego $\mathbb{Z}[\zeta_p]/\langle \zeta_p - 1 \rangle \simeq \mathbb{Z}_p$.

Por lo tanto, se tiene que $U(\mathbb{Z}[\zeta_p]/\langle \zeta_p - 1 \rangle)$ está formado exactamente por $p - 1$ unidades, pero como teníamos exactamente $\phi(p) = p - 1$ unidades ciclotómicas en

$U(\mathbb{Z}[\zeta_p])$, entonces deducimos que la imagen de las unidades ciclotómicas recubre toda la imagen de g, por lo que g es suprayectiva. Luego el índice del núcleo de g sobre $U(\mathbb{Z}[\zeta_p])$ coincide con el cardinal de $U(\mathbb{Z}[\zeta_p]/\langle\zeta_p - 1\rangle)$. Esto implica que

$$[U(\mathbb{Z}[\zeta_p]) \ : \ U_1(\mathbb{Z}[\zeta_p])] = p - 1.$$

□

En el siguiente teorema calculamos el grupo de unidades de $\mathbb{Z}C_5$, para ello utilizaremos las propiedades demostradas en la proposición anterior.

Teorema 4.7. *Si* $C_5 = \langle x\rangle$ *con* $o(x) = 5$ *entonces* $U(\mathbb{Z}C_5) = \langle -1,\ x,\ u\rangle$, *donde* $u = (x+1)^2 - \hat{x}$.

Demostración. Sea p un número primo. Consideramos ζ_p una raíz p-ésima primitiva de la unidad en $\mathbb{C}$. Utilizando la Proposición 4.6 obtenemos que $[U(\mathbb{Z}[\zeta_p]) \ : \ U_1(\mathbb{Z}[\zeta_p])] = p-1$. Como las unidades de $\mathbb{Z}C_p$ tienen aumentos ± 1 entonces $[U(\mathbb{Z}C_p) : U_1(\mathbb{Z}C_p)] = 2$.

Consideramos ahora $p = 5$. Utilizando el Teorema de las Unidades de Dirichlet 1.11 deducimos que $U(\mathbb{Z}[\zeta_5]) = C \times F$, donde C es un grupo cíclico finito y F es un grupo libre de torsión de rango $n_1 + n_2 - 1 = 0 + 2 - 1 = 1$. Además, tenemos que $\frac{1-\zeta_5^2}{1-\zeta_5} = 1 + \zeta_5$ es una unidad fundamental de F. La demostración se sale del objetivo de este documento y hacemos referencia a la página 85 de [13]. Luego $F = \langle 1 + \zeta_5\rangle$. De donde obtenemos que $U(\mathbb{Z}[\zeta_5]) = C \times \langle 1 + \zeta_5\rangle$.

Por un lado sabemos que C es un grupo cíclico finito formado por todos los elementos con orden finito de $U(\mathbb{Z}[\zeta_p])$ y por otro lado sabemos que $[\mathbb{Q}(\zeta_5) \ : \ \mathbb{Z}(\zeta_5)] = 4$. Como $-\zeta_5$ tiene orden 10 porque $(-\zeta_5)^5 = -1$, entonces por lo menos habrá 10 elementos en C, que serían las potencias de $-\zeta_5$. Sin embargo, no hay más de 10 elementos en C ya que es bien conocido que las raíces de la unidad de $\mathbb{Q}(\zeta_5)$ vienen dadas por $\langle -1,\ \zeta_5\rangle$. Entonces deducimos que $C = \pm\langle\zeta_5\rangle$. Por lo tanto, hemos demostrado lo siguiente:

$$U(\mathbb{Z}[\zeta_5]) = \pm\langle 1 + \zeta_5\rangle \times \langle\zeta_5\rangle$$

Utilizando el Corolario 1.10 deducimos que existe un isomorfismo

$$\mu : \ \mathbb{Q}C_5 \longrightarrow \mathbb{Q} \oplus \mathbb{Q}[\zeta_5]$$

dado por $\mu(\sum_{i=0}^{4} c_i x^i) = (\sum_{i=0}^{4} c_i, \sum_{i=0}^{4} c_i \zeta_5^i)$. Como $\mathbb{Z} \oplus \mathbb{Z}[\zeta_5] \subseteq \mathbb{Q} \oplus \mathbb{Q}[\zeta_5]$ entonces podemos definir

$$M = \mu^{-1}\left(\mathbb{Z} \oplus \mathbb{Z}[\zeta_5]\right)$$

Por lo que $M \simeq \mathbb{Z} \oplus \mathbb{Z}[\zeta_5]$. Luego es claro que $\mathbb{Z}C_5 \subset M \subset \mathbb{Q}C_5$. Además $\mathbb{Z}C_5$ y M son ordenes en $\mathbb{Q}C_5$. Aplicando el Teorema de las Unidades de Dirichlet 1.11 deducimos que $U(\mathbb{Z}[\zeta_5])$ es un grupo abeliano finitamente generado. Por lo tanto $U(M)$ está también finitamente generado. Usando ahora el Lema 1.16 obtenemos que el índice $[U(M) : U(\mathbb{Z}C_5)]$ es finito, lo que implica que $U(\mathbb{Z}C_5)$ es un grupo abeliano finitamente generado.

Tomamos $u = (x+1)^2 - \hat{x}$. Entonces $\mu(u) = (-1,\ (\zeta_5+1)^2) \in U(\mathbb{Z}) \oplus U(\mathbb{Z}[\zeta_5])$. Como $\mu(u)$ es una unidad en $\mathbb{Z} \oplus \mathbb{Z}[\zeta_5]$, entonces u es una unidad en M. Utilizando la Proposición 1.17 se tiene que $u \in U(\mathbb{Z}\langle x\rangle)$.

Es claro que $\mu(-1),\ \mu(\zeta_5),\ \mu((\zeta_5+1)^2) \in \mu(\langle -1,\ x,\ u\rangle)$ porque $\mu(-1) = (-1,\ 1)$, $\mu(\zeta_5) = (1,\ \zeta_5)$ y $\mu((\zeta_5+1)^2) = (4,\ (\zeta_5+1)^2)$. Luego $\mu(\langle -1,\ \zeta_5,\ (\zeta_5+1)^2\rangle) \subset \mu\left(\langle -1,\ x,\ u\rangle\right)$. Además, se verifica lo siguiente:

$$\frac{U(\mathbb{Z}[\zeta_5])}{\langle -1,\ \zeta_5,\ (\zeta_5+1)^2\rangle} \simeq \frac{\langle -1,\ \zeta_5,\ (1+\zeta_5)\rangle / \langle -1,\ \zeta_5\rangle}{\langle -1,\ \zeta_5,\ (1+\zeta_5)^2\rangle / \langle -1,\ \zeta_5\rangle} = \frac{\langle 1+\zeta_5\rangle}{\langle (1+\zeta_5)^2\rangle}$$

Aplicando que $1+\zeta_5$ tiene orden infinito, deducimos que $[\langle 1+\zeta_5\rangle : \langle (1+\zeta_5)^2\rangle] = 2$ y por lo tanto $[U(\mathbb{Z}[\zeta_5]) : \langle -1,\ \zeta_5,\ (\zeta_5+1)^2\rangle] = 2$. Como además se tiene que $[U(\mathbb{Z}\langle x\rangle) : \langle -1,\ x,\ u\rangle] = 2$, entonces $\mu(\langle -1,\ x,\ u\rangle) = U(\mathbb{Z}) \oplus \langle -1,\ \zeta_5,\ (1+\zeta_5)^2\rangle$.

Vamos a calcular $U_1(\mathbb{Z}[\zeta_5])$. Sabemos que $(1+\zeta_5)^2 \equiv 4 \mod \zeta_5 - 1$ porque $1+2\zeta_5+\zeta_5^2-4 = (\zeta_5-1)\cdot(\zeta_5+3)$. Además se tiene que $\frac{x^5-1}{x-1} = 1+x+x^2+x^3+x^4 = \prod_{i=1}^{4}(x-\zeta_5^i)$. Tomando $x=1$, obtenemos que $\prod_{i=1}^{p-1}(1-\zeta_5^i) = 1+1+1^2+1^3+1^4 = 5$. Luego $1-\zeta_5 | 5$. Por lo tanto, deducimos que $-(1+\zeta_5)^2 \equiv 1 \mod \zeta_5 - 1$. Luego $\langle \zeta_5,\ -(1+\zeta_5)^2\rangle \subseteq U_1(\mathbb{Z}[\zeta_5])$. Entonces se tiene que $[\langle -1,\ \zeta_5,\ (\zeta_5+1)^2\rangle : \langle \zeta_5,\ -(1+\zeta_5)^2\rangle] = 2$. Aplicando que $[U(\mathbb{Z}[\zeta_5]) : U_1(\mathbb{Z}[\zeta_5])] = 4$, $[U(\mathbb{Z}[\zeta_5]) : \langle -1,\ \zeta_5,\ (\zeta_5+1)^2\rangle] = 2$ y $\langle \zeta_5,\ -(1+\zeta_5)^2\rangle \subseteq U_1(\mathbb{Z}[\zeta_5])$ obtenemos lo siguiente:

$$U_1(\mathbb{Z}[\zeta_5]) = \langle \zeta_5,\ -(1+\zeta_5)^2\rangle.$$

Por un lado tenemos que $[U(\mathbb{Z}) \oplus U(\mathbb{Z}[\zeta_5]) : U(\mathbb{Z}) \oplus \langle -1,\ \zeta_5,\ (\zeta_5+1)^2\rangle] = 2$ y $[U(\mathbb{Z}) \oplus \langle -1,\ \zeta_5,\ (\zeta_5+1)^2\rangle : U(\mathbb{Z}) \oplus U_1(\mathbb{Z}[\zeta_5])] = 2$. Por otro lado tenemos que $[U(\mathbb{Z}C_5) : U_1(\mathbb{Z}C_5)] = 2$, $[U(\mathbb{Z}C_5) : \langle -1,\ x,\ u\rangle] = 2$ y $[\langle -1,\ x,\ u\rangle : \langle x,\ -u\rangle] = 2$. Como

$\mu\left(\langle -1,\ x,\ u\rangle\right) = U(\mathbb{Z})\oplus\langle -1, \zeta_5, (\zeta_5+1)^2\rangle$ entonces $\mu\left(\langle x,\ -u\rangle\right) = U(\mathbb{Z})\oplus\langle \zeta_5, -(1+\zeta_5)^2\rangle$. Utilizando la Proposición 4.6 sabemos que $\mu(U_1(\mathbb{Z}C_p)) = U(\mathbb{Z})\oplus U_1(\mathbb{Z}[\zeta_p])$. Luego como μ es inyectiva, deducimos que $U_1(\mathbb{Z}C_5) = \langle x, -u\rangle$. Aplicando que $[U(\mathbb{Z}C_5) : U_1(\mathbb{Z}C_5)] = 2$ junto con que $[\langle -1,\ x,\ u\rangle\ :\ \langle x,\ -u\rangle] = 2$ deducimos que $U(\mathbb{Z}C_5) = \langle -1,\ x,\ u\rangle$. $\square$

Bibliografía

[1] V. A. Artamonov and A. A. Bovdi, Integral group rings: Groups of units and classical K-theory, J. Soviet Math. 57 (1991), 2931-2958. 8

[2] H. Bass, The Dirichlet unit theorem, induced characters and Whitehead gruops of finite gruops, Topology 4 (1966), 391-410. 6, 11, 46

[3] A. Cayley, On the theory of groups as depending on the sumbolic equation $\theta^n = 1$, Phil. Mag. 7 (1854), 40-47. 8

[4] R. Dedekind, Über Gruppen, deren sämtliche teiler normalteiler sind, Math. Ann. 48 (1897), 548-561. 1, 2, 9, 13

[5] K. Dennis, The structure of the unit group of group rings, in Lecture notes in Pure and Applied Math. N 26, Marcel Dekker, New York, 1977. 8

[6] D. Farkas, Group rings: An annotated questionaire, Comm. Algebra 8 (1980), 585-602. 8

[7] H. Hasse, Number Theory, Springer-Verlag, Berlin, 1980. 27

[8] K. Hey, Analytische Zahalentheorie in Systemen hyperkomplexer Zahlen, Tesis Doctoral, Hamburgo, 1929. 6

[9] E. Jesper and G.Leal, Generators of large subgroups of the unit group of integral group rings, Manuscripta Math. 78 (1993), 303-315. 11

[10] I. Kaplansky, Problems in the theory of rings, Nas-NRC Publi. 502, Washington, 1957, pp.1-3. 8

[11] G. Karpilovsky, Units in Group Rings, Longman, Essex, 1989. 6

[12] E. Kleinert, Units in Skew Fields, Birkhäuser Verlag, Basilea 2000. 6

[13] S. Lang, Cyclotomic Fields, Springer, New York, 1978. 62

[14] T. Molien, Über die Invarianten del Linearen Substitutionsgruppen, S'ber Akad. d. Wiss. Berlin (1897), 1152-1156. 8

[15] E. Noether, Hypercomplexe Grössen und -darstellungtheorie, Math. Z. 30 (1929), 641-692. 8

[16] I.B.S. Passi, Group Rings and their Augmentation Ideals, Lecture Notes in Mathematics, 715 Springer, New York 1979. 6

[17] D.S. Passman, The Algebraic Structure of Group Rings, Wiley-Interscience, New York, 1977. 4, 6, 8, 11, 13

[18] D.S. Passman, Infinite Group rings, Marcel Dekker, New York, 1971. 8

[19] S. Perlis and G.Walker, Abelian group algebras of finite order, Trans. Amer. Math. Soc. 68, 1950. 26

[20] C. Polcino and S. K. Sehgal. An Introduction to Group Rings. Kluwer Academic Publishers. London. 2002. 6, 13

[21] J. Ritter and S.K. Sehgal, Construction of units in integral group rings of finite nilpotent groups, Trans. Amer. Math. Soc. 324 (2) 1991 603-6021. 11

[22] J. Ritter and S. K. Sehgal, Generators of Subgroups of $U(\mathbb{Z}G)$, Contemp. Math. 93 (1988), 331-347. 4, 11, 13

[23] S.K. Sehgal, Topics in Group Rings, Marcel Dekker, New York, 1978. 5, 6, 8, 12, 42

[24] S. K. Sehgal, Units of Integral Group Rings, Longman Scientific and Technical Essex, 1993. 4, 6, 12, 13

[25] C.L. Siegel, Discontinuous groups, Ann. Math. 44 (1943) 674-689. 46

[26] L. C. Washimgton, Introduction to Cyclotomic Fields, Springer-Verlag, New York, Heidelberg, Berlin, 1982. 28

[27] H.J. Zassenhaus, On units of orders, J. Algebra 20 (1972), 368-395. 5, 12, 46

Índice alfabético

g normaliza a H, 16
n-ésimo polinomio ciclotómico en K, 17
x conjugado por y, 17
álgebra, 24
álgebra de cuaterniones Hamiltonianos, 48

anillo de división, 24
anillo de enteros algebraicos de K, 27
anillo de grupo, 25
anillo de los cuaterniones enteros, $\mathcal{H}$, 48
anillo semisimple, 24
aplicación aumento módulo N, 58
aplicación de aumento, 26
aplicación involución, 40
aplicaciones de inclusión, 25

carácter asociado a una representación, 31
centralizador, 16
centro de G, 16
coeficiente en R de g, a_g, 25
conjugado de un elemento, 48
conjunto de todos los elementos de torsión de G, 16
conmutador, 17
cuerpo con p elementos, 17

elemento algebraico sobre $\mathbb{Q}$, 27
elemento de orden infinito, 16
elemento de torsión, 16
elemento invertible en R, 15
entero algebraico, 27
exponente de G, 16
extensión finita, 27

función de Euler $\phi(n)$, 39

generador de G, 16
grado de la representación, 30
grupo abeliano libre, 16
grupo cíclico, 16
grupo cíclico de orden n, C_n, 16
grupo cíclico infinito, C_∞, 16
grupo de los cuaterniones de orden 8, K_8, 17
grupo de torsión, 16
grupo Hamiltoniano, 17
grupo libre, 16
grupo libre de torsión, 16
grupo multiplicativo de las unidades de R, $U(R)$, 15

homomorfismo de R-módulos, 24

ideal de aumento de RG módulo N, 58

módulo de $x \in \mathbb{C}$, 55

módulo por la derecha, 24
módulo por la izquierda, 24
módulo proyectivo, 24
módulo semisimple, 24

núcleo de la aplicación aumento, $\triangle(G)$, 26
norma de un elemento, 48
notación $\hat{a}$, 16

orden, 28
orden de G, 15
orden de $a \in G$, 15

p-elemento, 16
p-grupo, 16
p-grupo abeliano elemental, 16
potencias de a, 15
Propiedad Universal de los Anillos de Grupo, 26

raíces primitivas n-ésimas de la unidad, 17
rango, 16
rango infinito, 16
representación de A asociada a M respecto de la base B, 30
representación de un grupo, 30
representación de una F-álgebra., 30
representación regular, 31
representaciones equivalentes, 30

sistema fundamental de unidades, 27
soporte, 25
subgrupo cíclico de G generado por a, $\langle a \rangle$, 15
subgrupo normal, 16
submódulo, 24

Teorema de Bass, 46
Teorema de Bass-Milnor, 46
Teorema de Euler, 39
Teorema de Higman, 52
Teorema de las Unidades de Dirichlet, 27
Teorema de Maschke, 26
Teorema de Passman-Bass, 40
Teorema de Perlis-Walker, 26
Teorema de Wedderburn-Artin, 24
traza, 31

unidad cíclica de Bass, 38
unidad central, 40
unidad de torsión, 33
unidad trivial, 33
unidades bicíclicas, 37
unidades ciclotómicas, 28
unidades de aumento 1, 33
unidades de torsión de RG, $TU(RG)$, 26
unidades unipotentes, 34