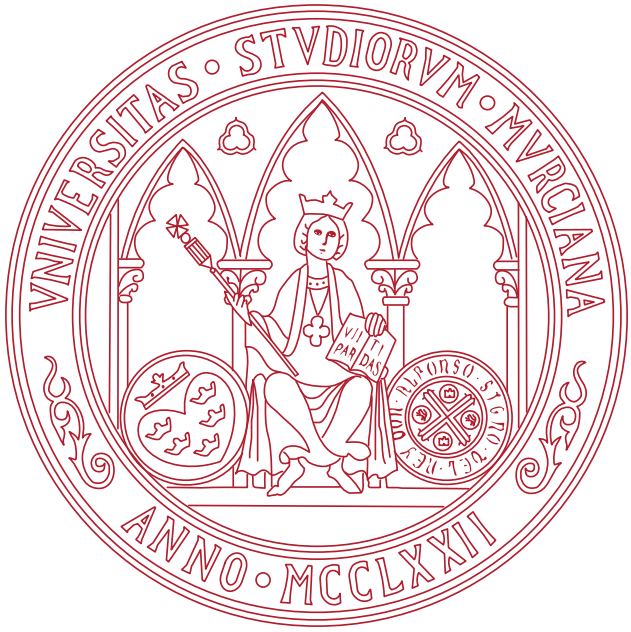


Universidad de Murcia

Trabajo Final de Grado

Grupos CUT

Autor:
Pablo Miralles González
pablo.mirallesg@um.es

Tutor:
Ángel del Río Mateos
adelrio@um.es

16 de junio de 2022

Me gustaría expresar mi agradecimiento a mi tutor Ángel del Río por su atenta ayuda, a mi familia por la educación y el apoyo recibidos y a mis compañeros de carrera por todo lo vivido juntos.

Declaración de originalidad

Pablo Miralles González, autor del Trabajo de Fin de Grado "Grupos CUT", bajo la tutela del profesor Ángel del Río Mateos, declara que el trabajo que presenta es original, en el sentido de que ha puesto el mayor empeño en citar debidamente todas las fuentes utilizadas, y que la obra no infringe el copyright de ninguna persona.

En Murcia, a 16 de junio de 2022

Fdo.: Pablo Miralles González

Índice general

Resumen

El estudio del grupo de unidades del anillo de grupo entero comenzó con el influyente trabajo de Higman en 1940 [Hig40]. Uno de sus resultados más importantes es el siguiente: si G es un grupo abeliano finito, entonces el grupo de unidades de su anillo de grupo entero $\mathcal{U}(\mathbb{Z}[G])$ es de la forma $\pm G \times F$, donde F es un grupo abeliano libre de rango $\frac{n+1+k_2-2c}{2}$, siendo n el orden de G, k_2 el número de subgrupos cíclicos de G de orden 2 y c el número de subgrupos cíclicos de G.

En la situación más general en la que G es un grupo finito no necesariamente abeliano, el centro del grupo de unidades de su anillo de grupo entero $Z(\mathcal{U}(\mathbb{Z}[G]))$ es de la forma $\pm Z(G) \times F$, donde F es de nuevo un grupo abeliano libre, pero cuyo rango es $\frac{c+c_1}{2} - d$, siendo c el número de clases de conjugación de G, c_1 el número de clases de conjugación de G cerradas bajo tomar inversos y d es el número de clases de conjugación de subgrupos cíclicos de G [JR16, Corolario 7.1.13]. En este trabajo abordamos el caso en el que dicho rango es 0. Más concretamente, llamamos unidades triviales del anillo de grupo entero a los elementos de $\pm G$. Un grupo se dice CUT (*Central Units are Trivial*) si todas las unidades centrales de su anillo de grupo entero están en $\pm G$. El propósito principal de este proyecto es la exploración de las caracterizaciones principales de estos grupos, introduciendo la base necesaria para ello.

Los grupos CUT son de interés por diversos motivos, como su relación con ciertas propiedades de punto fijo, su papel en la simplificación a la hora de encontrar generadores de subgrupos de índice finito en el grupo de las unidades del anillo de grupo entero o las múltiples propiedades que presentan. Aunque el trabajo termina en el Capítulo 6 con una recopilación de problemas abiertos sobre grupos CUT, nos centraremos en el estudio y demostración de las caracterizaciones de grupo CUT que enunciamos a continuación (Capítulo 5).

Sea G un grupo finito, entonces las siguientes afirmaciones son equivalentes:

(CUT-1) G es un grupo CUT.

(CUT-2) $Z(\mathcal{U}(\mathbb{Z}[G]))$ es finito.

(CUT-3) Para cada carácter complejo irreducible χ de G, la extensión de $\mathbb{Q}$ generada por la imagen de χ está contenida en un cuerpo cuadrático imaginario.

(CUT-4) Para cada $g \in G$ y $j \in \mathbb{N}$ coprimo con $|G|$ se tiene que g^j es conjugado en G, o bien con g, o bien con g^{-1}.

(CUT-5) G es semi-racional por inversión, esto es, para cada elemento $g \in G$ se tiene que cualquier generador de $\langle g \rangle$ es conjugado, o bien con g, o bien con g^{-1}.

(CUT-6) Para cada elemento g de G, la extensión sobre $\mathbb{Q}$ generada por las imágenes de g por los caracteres complejos irreducibles está contenida en un cuerpo cuadrático imaginario.

El Capítulo 1 incluye una breve introducción a los anillos de grupo generales y a la propiedad CUT. El Capítulo 2 revisa algunos conceptos de Teoría de Galois que se usarán posteriormente.

El Capítulo 3 cubre los conceptos de álgebra, módulo sobre un álgebra, representación de álgebras y orden, así como Teoría de Caracteres. Los resultados de este capítulo serán aplicados a las álgebras $\mathbb{Q}[G]$ y $\mathbb{C}[G]$ y al anillo $\mathbb{Z}[G]$.

El Capítulo 4 concluye la base necesaria para las caracterizaciones demostrando el Teorema de las Unidades de Dirichlet. Este teorema describe el grupo de las unidades del anillo de enteros de extensiones finitas de $\mathbb{Q}$ y se conecta con el grupo de unidades centrales de $\mathbb{Z}[G]$ a través del concepto de orden y la Teoría de Caracteres.

El Capítulo 5 culmina la preparación realizada anteriormente con la demostración de la equivalencia entre las seis condiciones (CUT-1)-(CUT-6). Finalmente, en el Capítulo 6 recopilamos algunos de los problemas abiertos sobre grupos CUT sin entrar en detalles técnicos.

Abstract

The study of the group of units of the integral group ring was started in the seminal work of Higman in 1940 [Hig40]. One of his most important results states that if G is an abelian finite group then the group of units of the integral group ring $\mathcal{U}(\mathbb{Z}[G])$ is of the form $\pm G \times F$, where F is a free abelian group of rank $\frac{n+1+k_2-2c}{2}$, and n is the order of G, k_2 the number of cyclic subgroups of G of order 2 and c the number of cyclic subgroups of G.

If G is a finite group, not necessarily abelian, then the center of the group of units of the integral group ring $Z(\mathcal{U}(\mathbb{Z}[G]))$ is of the form $\pm Z(G) \times F$, where F is again a free abelian group, but its rank is now $\frac{c+c_1}{2} - d$, where c is the number of conjugacy classes of G, c_1 is the number of conjugacy classes of G that are closed under taking inverses and d is the number of conjugacy classes of cyclic subgroups of G [JR16, Corollary 7.1.13]. The case where this rank is 0 is the subject of this project. More precisely, the elements in $\pm G$ are called trivial units of the integral group ring. A group is said to be CUT (Central Units are Trivial) if the central units of its integral group ring are in $\pm G$. The main purpose of this project is to explore the most important characterisations of finite CUT groups, introducing the necessary theory to understand and prove them.

CUT groups are of interest for a variety of reasons. One of the original ones is that, if G is a finite group, then the group of units of its integral group ring has a subgroup of finite index that is generated by the central units of the integral group ring together with some particular units. It is the case for many such groups that the latter generators belong to a very specific class of units known as "bicyclic units". In the case of finite CUT groups, finitely many generators of a large subgroup of units of their integral group ring can be determined without taking into account its central units, as they are all trivial.

Another motive for the interest in finite CUT groups is their relation to certain fixed point properties, such as Kazhdan's property or Serre's property. The understanding of these properties and the study of non-central generators of the large subgroup of $\mathcal{U}(\mathbb{Z}[G])$ previously mentioned are beyond the scope of this project.

Finite CUT groups present many interesting properties, specially in the presence of other hypothesis such as solvability. For example:

- The order of a finite CUT group is always divisible by either 2 or 3.
- The prime spectrum of a finite solvable CUT group is contained in $\{2, 3, 5, 7\}$, this is, the only primes that can divide the order of the group are the ones in the previous set.
- Any quotient group of a CUT group is again CUT.
- An abelian finite group is CUT if and only if its exponent divides 4 or 6.

These and many more peculiar properties are known for CUT groups.

A class of groups strongly related to CUT groups is that of rational groups. A group is rational if its character table only contains rationals, which actually must be integers. A classic example of rational groups is found in the symmetric groups. CUT groups can be seen as a generalisation of this widely studied class.

The CUT property is not a rare phenomenon among groups of small order. For example, CUT groups make up for 85.62% of groups with order less or equal than 512, as opposed to the 0.57% of rational groups.

In the case of finite groups, the CUT property has been characterised in terms of both the character table and the conjugacy classes of the group. This project develops the required theory to fully understand these characterisations, presupposing basic undergraduate knowledge of abstract algebra. These characterisations are stated next.

Let G be a finite group, then the following affirmations are equivalent.

(CUT-1) G is CUT.

(CUT-2) The group of central units of the integral group ring of G is finite.

(CUT-3) For each irreducible complex character χ of G, the extension of $\mathbb{Q}$ generated by the image of χ is contained in a quadratic imaginary field.

(CUT-4) For each $g \in G$ and $j \in \mathbb{Z}$ coprime with $|G|$, g^j is a conjugate in G of either g or g^{-1}.

(CUT-5) G is inverse semi-rational, this is, for each $g \in G$ every generator of $\langle g \rangle$ is a conjugate in G of either g or g^{-1}.

(CUT-6) For each element g of G, the extension of $\mathbb{Q}$ generated by the set of images of g under the irreducible complex characters of G is contained in a quadratic imaginary field.

Chapter 1 provides a very brief introduction about general group rings and the CUT property. Chapter 2 reviews the basics of Galois Theory and introduces the concepts of characteristic polynomial, norm and trace of an element in a field extension.

Chapter 3 covers the topics of algebras, modules over algebras, algebra representations, orders and character theory, needed for the remainder of the project. No previous knowledge of non commutative algebra is required.

In Section 3.1, the structure of the group algebra $F[G]$ for a field F is studied. Maschke's Theorem is of particular importance here. It states that if the characteristic of the field F does not divide the order of a finite group G, then every $F[G]$-module is semisimple, that is, it is the direct sum of simple or irreducible modules. This is precisely the case for $F = \mathbb{Q}$ or $F = \mathbb{C}$. As it turns out, the number of isomorphism classes of simple modules over a semisimple algebra is finite, and therefore under Maschke's conditions $F[G]$ is the finite direct sum of semisimple components, each one of them being the direct sum of isomorphic simple modules. These components are called the Wedderburn components of $F[G]$, and they are also simple algebras, i.e., algebras with no ideals other than 0 and themselves. The expression of $F[G]$ as the direct sum of its Wedderburn components is called its Wedderburn decomposition. The unities of the Wedderburn components of $F[G]$ are the projections of $1_{F[G]}$ along its Wedderburn decomposition, and they are called the primitive central idempotents of $F[G]$. If we denote the set formed by these idempotents by $\mathcal{E}$, the Wedderburn decomposition is typically written as $F[G] = \oplus_{e \in \mathcal{E}} eF[G]$. The section ends by introducing the concept of F-algebra representations, which are algebra homo-

morphisms onto matrix spaces over F. As we will see, algebra representations are just another way of looking at modules of finite dimension over F.

Representations of the group algebra $F[G]$ are equivalent to group representations of G, as there is a one to one correspondance by restriction and linear extension. The traces of group representations afford some special maps from the group onto the field F called characters. Of particular importance is the case of $F = \mathbb{C}$, which is studied extensively in Section 3.2. As it turns out, every complex character is the sum of irreducible characters, which are afforded by algebra representations corresponding to simple modules. Irreducible complex characters are in fact in one to one correspondance with the classes of simple $\mathbb{C}[G]$-modules. For a finite group G the irreducible complex characters are typically presented in the so called *character table*. In this table, each row corresponds to an irreducible character, whereas each column corresponds to a conjugacy class, as characters are constant in each conjugacy class. Basic character theory is enough to prove the equivalence of properties (CUT-1) and (CUT-2), which is done in Chapter 5.

The end of Section 3.2 is dedicated to studying the finite extensions of $\mathbb{Q}$ generated by the image of an irreducible complex character. There is a surjective correspondance between the Wedderburn components of $\mathbb{Q}[G]$ and irreducible complex characters, and we will show that the center of each of these Wedderburn components is isomorphic to the extension generated by the corresponding irreducible $\mathbb{C}$-characters. Thus, the objective will be to connect the central units of $\mathbb{Z}[G]$ with the centers of the Wedderburn components of $\mathbb{Q}[G]$ and to study this relationship through the isomorphic finite extension of $\mathbb{Q}$.

The former is achieved in Section 3.3. This section introduces the concept of order in an algebra. The integral group ring has this structure in $\mathbb{Q}[G]$, and in fact for each primitive central idempotent e of $\mathbb{Q}[G]$ it is true that $e\mathbb{Z}[G]$ is an order in the Wedderburn component $e\mathbb{Q}[G]$. Finally, we will show that the center of an order is still an order in the center of the algebra, resulting in the connection to the center of the Wedderburn components of $\mathbb{Q}[G]$ we were seeking.

At the end of Section 3.3 we decompose the central units of $\mathbb{Z}[G]$ uniquely as sum of central units of the components $e\mathbb{Z}[G]$, where e is a primitive central idempotent of $\mathbb{Q}[G]$. It follows that to show the finitude of the central units of the integral group ring, and therefore property (CUT-3), we just need to prove the finitude of its components.

To summarise, we have that for each primitive central idempotent e of $\mathbb{Q}[G]$, the center $Z(e\mathbb{Z}[G])$ of $e\mathbb{Z}[G]$ is an order in $Z(e\mathbb{Q}[G])$, which is isomorphic to a finite extension of $\mathbb{Q}$. Chapter 4 is dedicated to proving the Dirichlet's Unit Theorem. This theorem studies precisely the rank of the group of units of a particular order in finite extensions of $\mathbb{Q}$, called its ring of algebraic integers. We will show that this group of units is finite if and only if the extension is either $\mathbb{Q}$ or a quadratic imaginary extension of $\mathbb{Q}$. Even though the ring of algebraic integers of the extension is not necessarily isomorphic to $Z(e\mathbb{Z}[G])$, we show at the end of Section 3.3 that the group of units of two orders have a common subgroup of finite index if the algebra is of finite dimension, and thus the finitude of the group of units of $Z(e\mathbb{Z}[G])$ is equivalent to that of the ring of algebraic integers of the extension.

This ends the outline of the proof of the equivalence of the properties (CUT-2) and (CUT-3). Using these characterisations it is not difficult to complete the proof for every condition stated. This is done in the latter half of Chapter 5.

As CUT groups are a very active line of research, we end this project in Chapter 6 by compiling several open problems related to this class of groups. Some problems and properties related to rational groups are discussed as well, due to their ties to CUT groups.

CAPÍTULO 1

Introducción

Este trabajo pretende reunir las caracterizaciones principales de los grupos conocidos con el acrónimo de *CUT* (*central units are trivial*). Para explicar dicha propiedad es necesario definir primero el siguiente concepto.

Definición 1.0.1. Dado un grupo G y un anillo A, se llama *anillo de grupo*, y se denota $A[G]$, al A-módulo libre generado por los elementos de G. Se define como conjunto de la siguiente forma:

$$A[G] = \left\{ \sum_{g \in G} a_g g | a_g \in A, a_g \text{ casi todos nulos} \right\},$$

es decir, como el conjunto de las combinaciones A-lineales "formales" de elementos de G. Este conjunto adquiere estructura de anillo mediante la suma y el producto dados por

$$\left(\sum_{g \in G} a_g g \right) + \left(\sum_{g \in G} b_g g \right) = \sum_{g \in G} (a_g + b_g) g; \qquad \left(\sum_{g \in G} a_g g \right) \left(\sum_{g \in G} b_g g \right) = \sum_{g \in G} \sum_{h \in G} \left(a_h b_{h^{-1}g} \right) g.$$

Podemos identificar un elemento g de G con el elemento $\sum_{h \in G} a_h h$ de $A[G]$ tal que $a_g = 1$ y $a_h = 0$ si h es distinto de g. Los elementos son ahora combinaciones A-lineales de G. Es claro entonces que G es una base de $A[G]$ como A-módulo tanto por la derecha como por la izquierda.

El objeto de estudio del trabajo es $\mathbb{Z}[G]$, llamado anillo de grupo entero. Dado un anillo A cualquiera, denotamos $\mathcal{U}(A)$ al grupo de unidades de A y $Z(A)$ al centro de su grupo multiplicativo. Consideramos el grupo de las unidades centrales de $\mathbb{Z}[G]$, esto es, $\mathcal{U}(Z(\mathbb{Z}[G]))$, el cual coincide con $Z(\mathcal{U}(\mathbb{Z}[G]))$, como veremos posteriormente. Llamamos unidades centrales triviales a los elementos de $\pm Z(G)$, conjunto contenido claramente en $\mathcal{U}(Z(\mathbb{Z}[G]))$. Cuando se da la igualdad se dice que G es CUT.

En el caso de que G sea un grupo finito, la condición de que G sea CUT ha sido caracterizada en términos tanto de sus clases de conjugación como de su tabla de caracteres. Este último concepto se introduce en la Sección 3.2, dedicada a la Teoría de Caracteres. El resultado principal para describir grupos de unidades de ciertos anillos conmutativos es el Teorema de las Unidades de Dirichlet, al que se dedica el Capítulo 4 en su totalidad. La Sección 3.3 relaciona $\mathbb{Z}[G]$ con $\mathbb{Q}[G]$, mientras que la Sección 3.1 reduce el problema descomponiendo $\mathbb{Q}[G]$ en componentes que se pueden conectar mediante Teoría de Caracteres con el Teorema de las Unidades de Dirichlet.

CAPÍTULO 2

Preliminares de extensiones de cuerpos

En este capítulo se incluyen algunos preliminares necesarios sobre extensiones de cuerpos. El esquema seguido es el de la sección 1.2 de [dRío21], con referencias a otros textos publicados en demostraciones omitidas.

2.1. Polinomios simétricos

Fijamos un cuerpo K. Un polinomio $P(X_1, \ldots, X_n) \in K[X_1, \ldots, X_n]$ se dice *simétrico* si es invariante por cualquier permutación de las variables, y se definen los polinomio simétricos elementales $S_1, \ldots, S_n$ como

$$S_i = \sum_{1 \leqslant j_1 < \ldots < j_i \leqslant n} \prod_{k=1}^{i} X_{j_i}.$$

Teorema 2.1.1 (Teorema Fundamental de los Polinomios Simétricos)**.** *Un polinomio es simétrico si y solo si puede expresarse como $P(S_1, \ldots, S_n)$ con $P \in K[X_1, \ldots, X_n]$.*

Demostración. [ACM02, Teorema 1.5.12]. □

2.2. Conjugados de un elemento, polinomio carácterístico y otras funciones

En esta sección F/K es una extensión de cuerpos. Recordemos que dado un elemento α de F, decimos que α es algebraico sobre K si el homomorfismo $K[X] \to F$ de evaluación en α no es inyectivo. En ese caso existe un único polinomio mónico que genera el núcleo de dicho homomorfismo. A ese polinomio se le llama *polinomio mínimo* de α sobre K, y se denota por $Min_K(\alpha)$.

Definición 2.2.1. Un *polinomio* $f \in K[X]$ es *separable* si no tiene raíces múltiples en un cuerpo de descomposición sobre K, y por lo tanto en ninguno.

Un *elemento* $\alpha \in F$ es *separable* sobre K si su polinomio mínimo sobre K, $Min_K(\alpha)$, es separable.

Una *extensión* algebraica F/K se dice *separable* si cada elemento de F es separable sobre K.

Notación 2.2.2. En este trabajo denotamos la característica de un anillo A por $car(A)$.

Proposición 2.2.3. *Si $car(K) = 0$ y $f \in K[X]$ es irreducible entonces f es separable. En particular toda extensión algebraica de cuerpos de característica cero es separable.*

Demostración. [ACM02, Proposición 1.3.7]. □

Supongamos que la extensión F/K es separable. Sea $\alpha \in F$ con $[K(\alpha) : K] = n$ y sea L un cuerpo algebraicamente cerrado que contiene a F, notación que mantendremos hasta el final del capítulo. Entonces para cada homomorfismo de cuerpos σ de K en L existen exactamente n homomorfismos de $K(\alpha)$ en L que extienden a σ, que denotaremos $\{\sigma_1, \ldots, \sigma_n\}$. En este caso, las raíces de $Min_K(\alpha)$ en L son $\alpha_i = \sigma_i(\alpha)$ [ACM02, Proposición 2.3.14], y son todas distintas por la separabilidad de la extensión. Estas raíces se llaman *conjugados* de α. Se verifica además que

$$Min_K(\alpha) = \prod_{i=1}^{n}(X - \alpha_i) = X^n + \sum_{i=1}^{n}(-1)^i S_i(\alpha_1, \ldots, \alpha_n)X^{n-i} \in K[X].$$

En particular, el resultado de aplicar los polinomios simétricos a los α_i está en K. Recordemos que a un homomorfismo cuyo dominio es una extensión de K y tal que su restricción a K coincide con la identidad se le llama *K-homomorfismo*. Aplicando el desarrollo anterior a $\sigma = \mathrm{Id}$, se tiene que existen exactamente n K-homomorfismos de $K(\alpha)$ en L.

Para una extensión separable general F/K con $[F : K] = n$ se puede hacer el mismo razonamiento, ya que $F = K(\alpha)$ para cierto $\alpha \in F$ por el Teorema del Elemento Primitivo [ACM02, Teorema 8.2.4].

Definición 2.2.4. Sean $\sigma_1, \ldots, \sigma_n$ los K-homomorfismos de F en L. Dado un elemento α de F, se define su *polinomio característico* sobre K como

$$\chi_{F/K}(\alpha) = \prod_{i=1}^{n}(X - \sigma_i(\alpha)),$$

y se define la *norma* y la *traza* de α sobre K como

$$N_{F/K}(\alpha) = \prod_{i=1}^{n}\sigma_i(\alpha);\ T_{F/K}(\alpha) = \sum_{i=1}^{n}\sigma_i(\alpha).$$

Proposición 2.2.5. *Sea F/K una extensión separable de grado n. Sea $\alpha \in F$ y supongamos que $m = [K(\alpha) : K]$, $n = [F : K]$ y $\sigma_1, \ldots, \sigma_n$ son los K-homomorfismos de F en L. Entonces:*

1. *m divide a n.*
2. *La lista $\sigma_1(\alpha), \ldots, \sigma_n(\alpha)$ está formada por los conjugados de α sobre K, cada uno repetido $\frac{n}{m}$ veces.*
3. *$\chi_{F/K}(\alpha) = Min_K(\alpha)^{\frac{n}{m}}$, y por lo tanto pertenece a $K[X]$.*
4. *α pertenece a K si y solo si $\sigma_i(\alpha) = \alpha$ para cada i.*
5. *$K(\alpha) = F$ si y solo si $\sigma_i(\alpha) \neq \sigma_j(\alpha)$ para cada $i \neq j$.*
6. *$N_{F/K}(\alpha)$ y $T_{F/K}(\alpha)$ son elementos de K.*

7. *Si α y β son elementos de F entonces $N_{F/K}(\alpha\beta) = N_{F/K}(\alpha)N_{F/K}(\beta)$ y $T_{F/K}(\alpha+\beta) = T_{F/K}(\alpha) + T_{F/K}(\beta)$.*

Demostración. El primer apartado es evidente, ya que $n = km$ si $k = [F : K(\alpha)]$.

Considero $\tau_1, \dots, \tau_m$ los K-homomorfismos de $K(\alpha)$ en L. Cada τ_i tiene k extensiones distintas a un homomorfismo de F en L, y el conjunto de las extensiones de todos los τ_i debe ser $\sigma_1, \dots, \sigma_n$. Fijado cierto τ_i, sus k extensiones a F aplicadas a α resultan en $\tau_i(\alpha)$, y por separabilidad $\tau_i(\alpha) \neq \tau_j(\alpha)$ si $i \neq j$, lo que demuestra la segunda afirmación.

La tercera propiedad se desprende de la segunda, ya que $\chi_{F/K}(\alpha) = \prod_{i=1}^{m}(X - \tau_i(\alpha))^k = Min_K(\alpha)^k$.

Como $\alpha \in K$ si y solo si $[K(\alpha) : K] = 1$ o, equivalentemente, $[F : K(\alpha)] = n$, es claro que la cuarta afirmación se desprende de la segunda. De la misma forma, $K(\alpha) = F$ si y solo si $[F : K(\alpha)] = 1$, lo que demuestra (5).

El apartado (6) es cierto porque $N_{F/K}(\alpha)$ y $T_{F/K}(\alpha)$ son coeficientes de $\chi_{F/K}(\alpha)$, con lo que se deduce de la tercera afirmación. El último apartado es trivial por definición. □

Definición 2.2.6. Sea F/K una extensión separable de grado n. Sea $\alpha \in F$ y supongamos que $m = [K(\alpha) : K]$, $n = [F : K]$ y $\sigma_1, \dots, \sigma_n$ son los K-homomorfismos de F en L. Dados n elementos $\alpha_1, \dots, \alpha_n$ de F, se define su *discriminante* sobre K como

$$\Delta_{F/K}[\alpha_1, \dots, \alpha_n] = det(\sigma_i(\alpha_j))^2.$$

Para un elemento α de F se denota $\Delta_{F/K}(\alpha)$ a $\Delta_{F/K}[1, \alpha, \dots, \alpha^{n-1}]$.

Proposición 2.2.7. *Sea F/K una extensión separable de grado n, y sean $\alpha_1, \dots, \alpha_n$ elementos de F. Entonces:*

1. *$\Delta_{F/K}[\alpha_1, \dots, \alpha_n] = det(T_{F/K}(\alpha_i\alpha_j)) \in K$.*
2. *Si para cada $i = 1, \dots, n$ se tiene $\beta_i = \sum_{j=1}^{n} c_{ij}\alpha_j$ con $c_{ij} \in K$, entonces $\Delta_{F/K}[\alpha_1, \dots, \alpha_n] = \Delta_{F/K}[\beta_1, \dots, \beta_n]det(c_{ij})^2$.*
3. *Si $F = K(\theta)$ y $\theta_1, \dots, \theta_n$ son los conjugados de θ sobre K entonces $\Delta_{F/K}(\theta) = \prod_{1 \leqslant i < j \leqslant n}(\theta_i - \theta_j)^2$.*
4. *$\Delta_{F/K}[\alpha_1, \dots, \alpha_n] \neq 0$ si y solo si $\alpha_1, \dots, \alpha_n$ forman una base de F sobre K. En particular, si $\alpha \in F$ entonces $\Delta_{F/K} \neq 0$ si y solo si $F = K(\alpha)$.*

Demostración. (1) Si $\sigma_1, \dots, \sigma_n$ son los K-homomorfismos de F en L, se tiene

$$\begin{aligned}\Delta[\alpha_1, \dots, \alpha_n] &= det(\sigma_i(\alpha_j))^2 = det(\sigma_i(\alpha_j))det(\sigma_j(\alpha_i)) \\ &= det\left(\sum_{k=1}^{n}\sigma_k(\alpha_i)\sigma_k(\alpha_j)\right) = det\left(\sum_{k=1}^{n}\sigma_k(\alpha_i\alpha_j)\right) \\ &= det(T_{F/K}(\alpha_i\alpha_j)).\end{aligned} \tag{2.1}$$

(2) Es directo por ser $(\sigma_i(\beta_j)) = (\sigma_i(\alpha_j))(c_{ij})$ y el determinante del producto de matrices el producto de sus determinantes.

(3) Si $\theta_i = \sigma_i(\theta)$, entonces

$$\Delta(\theta) = \begin{vmatrix} 1 & 1 & \dots & 1 \\ \theta_1 & \theta_2 & \dots & \theta_n \\ \theta_1^2 & \theta_2^2 & \dots & \theta_n^2 \\ \vdots & \vdots & \ddots & \vdots \\ \theta_1^{n-1} & \theta_2^{n-1} & \dots & \theta_n^{n-1} \end{vmatrix}^2,$$

que es el cuadrado de un determinante de Vandermonde. Es bien conocido que este determinante al cuadrado es igual a $\prod_{i<j}(\theta_i - \theta_j)^2$, y como la extensión es separable los θ_i son distintos dos a dos. Se tiene entonces que $\Delta(\theta) \neq 0$.

(4) Como $\{1, \theta, \dots, \theta^{n-1}\}$ es una base de F sobre K se tiene $\alpha_i = \sum_{i=1}^{n} c_{ij}\theta^{i-1}$ con los $c_{ij} \in K$. Por ser $\Delta(\theta) \neq 0$ y el segundo apartado, $\Delta[\alpha_1, \dots, \alpha_n] \neq 0$ si y solo si $C = (c_{ij})$ es invertible, lo cual equivale a que $\{\alpha_1, \dots, \alpha_n\}$ sea una base de F sobre K. La última afirmación es obvia, pues $F = K(\alpha)$ si y solo si $\{1, \alpha, \dots, \alpha^{n-1}\}$ es base de F sobre K. □

CAPÍTULO 3

Estructuras algebraicas y Teoría de Caracteres

Procedemos en la primera sección al estudio de la estructura de álgebra y de módulo, que podremos aplicar a los anillos de grupo $\mathbb{Q}[G]$ y $\mathbb{C}[G]$. En particular, se obtendrán descomposiciones de dichos anillos en componentes "irreducibles", que podremos conectar con extensiones de cuerpos en $\mathbb{C}$ gracias a la Teoría de Caracteres de la segunda sección. Finalmente estudiaremos la estructura de orden, que será precisamente lo que relaciona el grupo de unidades centrales del anillo de grupo entero con lo estudiado para $\mathbb{Q}[G]$.

Las dos primeras secciones se basan respectivamente en los capítulos 1 y 2 de [Isa94], mientras que la última en la sección 4.6 de [JR16].

3.1. Álgebras, módulos y representaciones

Definición 3.1.1. Sea F un cuerpo. Una *F-álgebra* A es un anillo que tiene además estructura de espacio vectorial sobre F con la misma suma y tal que para cada $c \in F$ y $x, y \in A$ se cumple que $(cx)y = c(xy) = x(cy)$.

Observación 3.1.2. Sean A es una F-álgebra y $F \cdot 1 = \{c1 | c \in F\}$. Entonces $F \cdot 1$ es un subconjunto de A claramente cerrado para el producto por F y para el producto y diferencia de sus elementos, así que es una subálgebra de A, esto es, un subanillo de A que también es una F-álgebra. Es claro que $F \cdot 1$ está contenido en $Z(A)$, pues para cada $c \in F$ y $x \in A$ se verifica $(c1)x = c(1x) = c(x1) = x(c1)$. Es común identificar F con $F \cdot 1$.

Ejemplo 3.1.3. Si L/F es una extensión de cuerpos, entonces L es una F-álgebra de forma natural.

Ejemplo 3.1.4. El anillo de las matrices cuadradas $n \times n$ sobre un cuerpo F es también una F-álgebra.

Ejemplo 3.1.5. Dado un cuerpo F, el anillo de grupo $F[G]$ tiene estructura de F-espacio vectorial, luego es una F-álgebra. En este caso se suele llamar *álgebra de grupo*.

Recordemos que en el caso de que G sea un grupo finito se cumple que $F[G]$ tiene dimensión finita sobre F, de manera que es razonable restringirnos al estudio de este caso. En lo que resta "álgebra" significará "álgebra de dimensión finita".

Definición 3.1.6. Sean A y B dos F-álgebras. Un *homomorfismo de álgebras* o *F-homomorfismo* es una aplicación $\phi : A \to B$ que cumple:

1. $\phi(xy) = \phi(x)\phi(y)$ para cada $x, y \in A$.
2. $\phi(1) = 1$.
3. ϕ es una aplicación F-lineal.

Definición 3.1.7. Dado un anillo A, un *A-módulo por la izquierda* es un grupo abeliano V junto con un producto $\cdot : A \times V \to V$ tal que para cada $x, y \in A$ y $v, w \in V$ se cumple:

(a) $x \cdot (v + w) = xv + xw$;

(b) $(x + y) \cdot v = xv + yv$;

(c) $y \cdot (x \cdot v) = (yx) \cdot v$;

(d) $1_A \cdot v = v$.

Siempre que queramos enfatizar la estructura de A-módulo por la izquierda de V escribiremos ${}_AV$.

De manera análoga se definen los módulos por la derecha, pero siempre trabajaremos con módulos por la izquierda. En adelante "módulo" significará "módulo por la izquierda".

Observación 3.1.8. Si A es una F-álgebra y V es un A-módulo, entonces V es un F-espacio vectorial con el producto dado por

$$(f, v) \mapsto (f1_A) \cdot v$$

para cada f de F y v de V. En este caso también se verifica la siguiente propiedad, identificando F con $F \cdot 1_A$:

(e) $x \cdot (fv) = (xf) \cdot v = (fx) \cdot v = f(x \cdot v)$ para cada $f \in F, x \in A$ y $v \in V$.

En general omitiremos los símbolos del producto e identificaremos F con $F \cdot 1_A$.

Definición 3.1.9. Si V es un A-módulo y W es un subgrupo aditivo de V invariante por el producto con elementos de A, entonces decimos que W es un *A-submódulo* de V. Se denotará por $W \leqslant_A V$, o $W <_A V$ en caso de ser un submódulo propio.

Ejemplo 3.1.10. Sea V un espacio vectorial sobre un cuerpo F. Si A es un subanillo de los endomorfismos F-lineales de V, denotados por $End(V)$, entonces V es un A-módulo con el producto definido por $f \cdot v := f(v)$.

Ejemplo 3.1.11. Si A es la F-álgebra de las matrices $n \times n$ con entradas en F, denotada por $M_n(F)$, entonces el espacio de los vectores columna de dimensión n sobre F es un A-módulo con la multiplicación de matrices por la izquierda.

Definición 3.1.12. Si A es una F-álgebra, entonces A es un A-módulo con el producto por la izquierda, llamado el *A-módulo regular*. De nuevo, para enfatizar esta estructura escribiremos ${}_AA$.

Observación 3.1.13. Los submódulos del A-módulo regular son claramente los ideales por la izquierda de A.

En adelante todos los A-módulos considerados serán sobre una F-álgebra para cierto cuerpo F. Esta suposición no afecta al desarrollo posterior, pues el objetivo es aplicar la Teoría de Módulos al estudio de ${}_{F[G]}F[G]$.

Observación 3.1.14. Si V es un A-módulo y W un submódulo de V, entonces V/W es un A-módulo con el producto definido por $a(v+W) = av + W$.

Definición 3.1.15. Si V y W son A-módulos, entonces un *A-homomorfismo* u *homomorfismo de A-módulos* es una aplicación aditiva $\phi : V \to W$ que cumple $\phi(av) = a\phi(v)$ para cada $a \in A$.

Denotaremos que dos módulos V y W son A-isomorfos con $V \cong_A W$ o, siempre que esté claro por el contexto, $V \cong W$.

Observación 3.1.16. Si $\phi : V \to W$ es un A-homomorfismo, entonces es evidente que $\ker\phi$ e $\operatorname{Im}\phi$ son A-submódulos de V y W respectivamente.

Teorema 3.1.17 (Primer Teorema de Isomorfía)**.** *Sean V y W dos A-módulos, y $\phi : V \to W$ un A-homomorfismo. Entonces*

$$V/\ker\phi \cong \operatorname{Im}\phi.$$

Demostración. Si $K = \ker\phi$, es obvio que $a + K \mapsto \theta(a)$ está bien definido y es un A-isomorfismo. □

Dado un A-módulo V, por las condiciones (a) y (e) de la Definición 3.1.7 y la Observación 3.1.8 cada $x \in A$ define una aplicación F-lineal $x_V : V \to V$ dada por $v \mapsto xv$. Por las condiciones (b), (c), (d) y (e) la aplicación $x \mapsto x_V$ define un homomorfismo de álgebras entre A y $End(V)$ con la composición como producto, cuya imagen denotamos A_V.

Si W es otro A-módulo, denotamos $Hom_A(V,W)$ al conjunto de los A-homomorfismos de V en W. Tiene estructura de F-espacio vectorial con el producto $(c\phi)(v) = c\phi(v)$ y la suma $(\phi + \theta)(v) = \phi(v) + \theta(v)$. $Hom_A(V,V)$ posee también estructura de anillo con la composición como producto, así que $Hom_A(V,V)$ es de hecho una F-álgebra, denotada $E_A(V)$. Por las definiciones es claro que $E_A(V)$ es precisamente el centralizador de A_V en $End(V)$, o sea,

$$E_A(V) = \{f \in End(V) | fg = gf \text{ para cada } g \in A_V\}.$$

Definición 3.1.18. Si V es un *A-módulo* no nulo, decimos que es *irreducible* o *simple* si y solo si sus únicos submódulos son 0 y V.

Lema 3.1.19 (Schur)**.** *Si V y W son A-módulos simples, entonces todo elemento no nulo de $Hom_A(V,W)$ tiene inverso en $Hom_A(W,V)$.*

Demostración. Si ϕ es un elemento no nulo de $Hom_A(V,W)$, entonces $\ker\phi$ es un submódulo propio de V e $\operatorname{Im}(\phi)$ es un submódulo no nulo de W. Por ser V y W simples debe ser $\ker\phi = 0$ e $\operatorname{Im}(\phi) = W$, de forma que ϕ es biyectivo. Es rutinario comprobar que el inverso de un A-isomorfismo también es A-isomorfismo. □

Una consecuencia inmediata es que si V es un A-módulo simple entonces $E_A(V)$ es un álgebra de división, esto es, un álgebra en el que todo elemento no nulo tiene inverso.

Corolario 3.1.20. *Si F es un cuerpo algebraicamente cerrado, A es una F-álgebra y V es un A-módulo simple y de dimensión finita sobre F, entonces $E_A(V) = F \cdot \mathrm{Id}$, es decir, el conjunto de los productos por escalares de F.*

Demostración. Claramente $F \cdot \mathrm{Id} \subseteq E_A(V)$ pues si $f \in F, a \in A$ y $v \in V$ entonces $f_V(av) = f(av) = a(fv) = a(f_V(v))$. Sea $\theta \in E_A(V)$. Entonces θ es una aplicación F-lineal entre espacios de dimensión finita con F algebraicamente cerrado, luego tiene un valor propio λ. Deducimos que $\theta - \lambda\,\mathrm{Id}$ es un elemento no invertible de $E_A(V)$, luego por el lema de Schur es 0, o sea $\theta = \lambda\,\mathrm{Id}$. □

Veremos que si A tiene dimensión finita sobre F entonces los A-módulos simples también, haciendo la hipótesis sobre la dimensión de V superflua en nuestro caso.

Definición 3.1.21. Sea V un A-módulo. Si para cada submódulo W de V existe otro submódulo U de V tal que $V = W \oplus U$, entonces decimos que V es *completamente reducible* o *semisimple*.

Observación 3.1.22. Dado un módulo V, si $V = U \oplus W$ para ciertos submódulos U y W, la aplicación dada por $\theta(u + w) = w$ para cada $u \in U$ y $w \in W$ está bien definida y es un A-homomorfismo con núcleo U e imagen W. La aplicación $v + U \mapsto \theta(v)$ está bien definida también, y es un A-isomorfismo entre V/U y W.

Definición 3.1.23. Un álgebra A es semisimple si su A-módulo regular ${}_AA$ es semisimple.

El siguiente teorema explica el interés por los módulos completamente reducibles, pues se dará dicha condición en nuestro caso de estudio.

Teorema 3.1.24 (Maschke)**.** *Sean G un grupo finito y F un cuerpo cuya característica no divide a $|G|$, entonces cada $F[G]$-módulo es completamente reducible.*

Demostración. Sea V un $F[G]$-módulo y W un submódulo suyo. Consideremos un F-subespacio vectorial U_0 complementario a W, es decir, tal que $V = W \oplus U_0$. Si ϕ la proyección dada por $\phi(w + u) = w$ para cada $w \in W$ y $u \in U_0$, ϕ es una aplicación F-lineal que no tiene por qué ser $F[G]$-homomorfismo. Definimos ahora, usando que $char(F) \nmid |G|$, la siguiente función:

$$\begin{aligned} \theta : V &\longrightarrow w \\ v &\longmapsto \theta(v) = \frac{1}{|G|} \sum_{g \in G} g^{-1}\phi(gv). \end{aligned}$$

Es claro que θ es F-lineal, y si $h \in G$ entonces

$$\theta(hv) = \frac{1}{|G|} \sum_{g \in G} g^{-1}\phi(ghv) = \frac{1}{|G|} \sum_{g \in G} h(gh)^{-1}\phi((gh)v) = h\theta(v),$$

pues gh recorre G si g lo hace. Por F-linealidad lo anterior se cumple con elementos de $F[G]$ y θ es un $F[G]$-homomorfismo.

Dado $w \in W$, como W es $F[G]$-submódulo se tiene que gw pertenece a W para cada $g \in G$. En concreto, $\phi(gw) = gw$ para cada $g \in G$, de donde $\theta(w) = w$. Definiendo entonces el $F[G]$-submódulo $U = \ker\theta$ de V, basta ver que $V = W \oplus U$.

Por definición de ϕ, para cada elemento v de V y g de G se tiene que $\phi(gv)$ está en W, luego $\theta(v)$ también. Se tiene entonces que $\theta(\theta(v)) = \theta(v)$ para cada $v \in V$, y en concreto $\theta(v - \theta(v)) = 0$. Podemos entonces descomponer cada elemento v de V como $v = \theta(v) + (v - \theta(v)) \in W + U$. Finalmente, si $w \in W \cap U$, entonces $w = \theta(w) = 0$. □

Teorema 3.1.25. *Un A-módulo V es completamente reducible si y solo si es suma de submódulos simples.*

Demostración. Supongamos que $V = \sum V_\alpha$ para ciertos submódulos simples V_α, y sea W un submódulo de V. Consideremos la familia Ω de submódulos U de V tales que $U \cap W = 0$, ordenados por la inclusión. Es claro que $0 \in \Omega$ y que la unión de una cadena de elementos de Ω está en Ω. Aplicando el Lema de Zorn obtenemos un elemento maximal U de Ω. Basta ver entonces que $V = W + U$, pues que la suma es directa se da por la definición de U. Si no fuese así, existiría un α con $V_\alpha \nsubseteq W + U$, luego se daría que U está contenido estrictamente en $U + V_\alpha$. Por la irreducibilidad de V_α se cumple que $(W + U) \cap V_\alpha = 0$. Dado entonces un elemento $w = u + v$ de $W \cap (U + V_\alpha)$ con $u \in U$ y $v \in V_\alpha$, se tiene que $v = w - u$ pertenece a $(W + U) \cap V_\alpha = 0$, luego $u = w$ es un elemento de $W \cap U = 0$. Deducimos que $W \cap (U + V_\alpha) = 0$, contradiciendo la maximalidad de U.

Supongamos que V es completamente reducible, y sea S la suma de todos los submódulos simples de V. Entonces S es un submódulo de V. Si S fuese propio podríamos poner $V = S \oplus T$ para cierto submódulo no nulo T de V. Sea ahora Ω la familia de submódulos no nulos U de T con el orden inverso a la inclusión. Como $T \in \Omega$ y la intersección de una cadena de elementos de Ω está en Ω, por el Lema de Zorn existe un elemento maximal U de Ω, es decir, minimal para la inclusión. Pero entonces U es simple, lo que contradice que $S \cap T = 0$. □

Lema 3.1.26. *Si V es un A-módulo y $V = \sum_{\alpha \in I} V_\alpha$ para ciertos submódulos simples V_α, entonces V es suma directa de algunos de los V_α.*

Demostración. Sea Ω la familia de los subconjuntos J de I tales que la suma $\sum_{\alpha \in J} V_\alpha$ es directa, ordenada por la inclusión. Es claro que $\varnothing \in \Omega$. Consideremos una cadena $\{J_i\}$ de elementos de Ω, y su unión J. Si J no estuviese en Ω existirían $j_1, \dots, j_r \in J$ y elementos no nulos $v_{j_1} \in V_{j_1}, \dots, v_{j_r} \in V_{j_r}$ tales que $v_{j_1} + \cdots + v_{j_r} = 0$. Como cada j_k está en J, está en algún J_{i_k}. Si J' es el máximo de los J_{i_k}, entonces todos los j_k están en J', y la suma $\sum_{\alpha \in J'} V_\alpha$ no puede ser directa, contradiciendo que $J' \in \Omega$. Deducimos que J es una cota de la cadena en Ω. Aplicando el Lema de Zorn obtenemos un elemento maximal J de Ω, y definimos $W = \bigoplus_{\alpha \in J} V_\alpha$.

Si W es propio entonces existe α con $V_\alpha \nsubseteq W$, de forma que $\alpha \notin J$. Como V_α es simple se tiene que $V_\alpha \cap W = 0$, y deducimos que $J \cup \{\alpha\}$ es un elemento de Ω que contiene a J estrictamente, lo cual es una contradicción. □

Corolario 3.1.27. *Los módulos completamente reducibles son precisamente las sumas directas de módulos simples.*

Este resultado simplifica el estudio de los módulos completamente reducibles, como es el caso de los módulos sobre $\mathbb{C}[G]$ o $\mathbb{Q}[G]$ por el Teorema de Maschke. Basta entonces estudiar los módulos simples, aunque primero debemos identificarlos.

Definición 3.1.28. Sean V un A-módulo completamente reducible y M un A-módulo simple. Se llama *parte M-homogénea* de V a la suma de todos los submódulos de V isomorfos a M, y se denota $M(V)$.

Lema 3.1.29. *Sea A una F-álgebra, entonces cada A-módulo simple es isomorfo a un módulo cociente de A. Si A es semisimple, entonces cada A-módulo simple es isomorfo a un submódulo de A.*

Demostración. Sean V un A-módulo simple, v un elemento no nulo de V y $\theta : A \to V$ la aplicación dada por $\theta(x) = xv$. Es claro que θ es F-lineal, y si $x, y \in A$ entonces $\theta(xy) = (xy)(v) = x(yv) = x\theta(y)$, con lo que $\theta \in Hom_A(A, V)$. Como $v \in \mathrm{Im}(\theta)$, deducimos que $\mathrm{Im}(\theta)$ es un submódulo no nulo de V, que es simple. Pero este último es simple, luego $V = \mathrm{Im}(\theta)$. Tomando $W = \ker\theta$

tenemos que $V \cong A/W$, por el Primer Teorema de Isomorfía. Si A es semisimple entonces $A = W \oplus U$ para cierto submódulo U de A, de donde $V \cong A/W \cong U$. □

Observación 3.1.30. El último lema permite obtener de A un conjunto de representantes de los A-módulos simples.

Observación 3.1.31. Como estamos trabajando con F-álgebras de dimensión finita, los A-módulos simples tienen dimensión finita sobre F.

Lema 3.1.32. *Sea $V = \oplus_i W_i$ para ciertos A-módulos W_i simples. Dado un A-módulo simple M, entonces:*

1. *$M(V)$ es un $E_A(V)$-submódulo de V.*
2. *$M(V) = \oplus\{W_i | W_i \cong M\}$.*
3. *El número $n_M(V)$ de W_i isomorfos a M es un invariante de V, no depende de la descomposición tomada.*

Demostración. (1) Sea $\theta \in E_A(V)$, se trata de ver que $\theta(M(V)) \subset M(V)$. Como $M(V)$ es suma de los submódulos isomorfos a M, basta demostar que $\theta(W) \subseteq M(V)$ para los submódulos W de V tales que $M \cong W$. Si $\theta(W) = 0$ es evidente. Supongamos que $\theta(W) \neq 0$, entonces θ es inyectivo en W, pues $\ker\theta$ es un submódulo no nulo de W, que es simple. Se deduce que $\theta(W)$ es isomorfo a W, que a su vez lo es a M, luego $\theta(W) \subseteq M(V)$.

(2) Por definición se cumple que $\oplus\{W_i | W_i \cong M\} \subseteq M(V)$. Denotaremos π_i a la proyección sobre W_i, y consideramos un submódulo W de V con $W \cong M$. Si $\pi_j(W) \neq 0$, entonces $\pi_j(W) = W_j$ por argumentos de irreducibilidad, de donde deducimos que $\pi_j(W) \subseteq \oplus\{W_i | W_i \cong M\}$ para cada j. Ahora bien, W está contenido en $\oplus_j \pi_j(W)$, que a su vez lo está en $\oplus\{W_i | W_i \cong M\}$, y por lo tanto $M(V) \subseteq \oplus\{W_i | W_i \cong M\}$.

(3) Por el apartado anterior $\dim M(V) = n_M(V) \cdot \dim M$. Como $\dim M < \infty$, $n_M(V) = \frac{\dim M(V)}{\dim M}$, donde $\dim M(V)$ puede ser infinito. En cualquier caso $n_M(V)$ no depende de la descomposición. □

Es obvio que si $M \cong N$ entonces $M(V) = N(V)$. Por contra, si $M \ncong N$ entonces $M(V) \cap N(V) = 0$ por (3.1.32.(2)). Nos interesa entonces estudiar las clases de A-módulos simples salvo isomorfismo.

Fijado un conjunto de representantes $\mathcal{S}(A)$ de los A-módulos simples, para cualquier A-módulo completamente reducible V se tiene que $V = \bigoplus_{M \in \mathcal{S}(A)} M(V)$.

Teorema 3.1.33 (Wedderburn)**.** *Sea A un álgebra semisimple y M un A-módulo simple. Entonces:*

1. *$M(A)$ es un ideal minimal de A.*
2. *Si W es un A-módulo simple, entonces*

$$M(A)W = \begin{cases} W, & \text{si } W \cong M; \\ 0, & \text{si } W \ncong M. \end{cases}$$

3. *La aplicación por $x \mapsto x_M$ es biyectiva entre $M(A)$ y A_M, donde recordemos que la función x_M viene dada por $m \mapsto xm$.*
4. *$\mathcal{S}(A)$ es finito.*

Demostración. (1) Sea $x \in A$, entonces la aplicación $\theta_x : A \to A$ dada por $y \mapsto yx$ cumple que $\theta_x \in E_A(A)$, y por (3.1.32.(1)) se tiene que $M(A)x = \theta(M(A))$ está contenido en $M(A)$, luego $M(A)$ un ideal por la derecha. Como $M(A)$ es un submódulo de ${}_AA$, deducimos que también es un ideal por la izquierda. La minimalidad se verá tras el apartado (3).

(2) Sea W un A-módulo simple. Supongamos que $M \ncong W$. Ya vimos por (3.1.32.(2)) que $M(A) \cap W(A) = 0$, y como $W(A)$ y $M(A)$ son ideales $M(A)W(A) \subseteq M(A) \cap W(A) = 0$. Por (3.1.29) A tiene un submódulo W_0 isomorfo a W. W_0 está entonces contenido en $W(A)$, de donde se deduce que $M(A)$ anula a W_0. Como W_0 es A-isomorfo a W tienen el mismo anulador en A, y $M(A)$ anula a W. El caso $M \cong W$ es obvio, pues $M(A)W$ es un submódulo de W, y debe ser no nulo, ya que de lo contrario $W = AW$ sería nulo. Como W es simple deducimos que $W = M(A)W$.

(3) Dado un A-módulo simple W, por el apartado anterior $x_W = 0$ si $x \in M(A)$ y $W \ncong M$. De la descomposición $A = \oplus_{N \in \mathcal{S}(A)} N(A)$ se deduce que para cada $y \in A$ con componente x en $M(A)$ se tiene que $y_M = x_M$. La imagen de la aplicación $x \mapsto x_M$ por $M(A)$ es entonces todo A_M, y si $x \in M(A)$ cumple que $x_M = 0$ entonces x anula todo A-módulo simple, y por lo tanto todo módulo completamente reducible. En concreto anula A, de donde $x = x1_A \in xA = 0$, y queda demostrada la inyectividad.

Para la minimalidad de $M(A)$, supongamos que I es un ideal de A contenido estrictamente en $M(A)$. Por (3.1.32.(2)) $M(A)$ es suma directa de módulos W_i simples e isomorfos a M, alguno de ellos debe cumplir $W_j \nsubseteq I$. Como $W_j \cap I$ es un submódulo propio de W_j y este es simple deducimos que $W_j \cap I = 0$. Pero entonces $IW_j = 0$, pues está contenido en $I \cap W_j$ al ser I un ideal y W_j un A-módulo. Deducimos que I anula a W_j, luego debe anular también a M por ser este isomorfo a W_j. Dado un elemento x de I se tiene entonces que $x_M = 0$, y por la inyectividad demostrada antes en $M(A) \supsetneq I$ debe ser $x = 0$, es decir, $I = 0$ y queda demostrada la minimalidad de $M(A)$.

(4) Por la definición de suma directa se cumple que la descomposición de 1_A en $A = \oplus_{M \in \mathcal{S}(A)} M(A)$ solo tiene componentes no nulas para un número finito de simples de $\mathcal{S}(A)$. Si hubiese un módulo simple N de $\mathcal{S}(A)$ tal que la componente de 1_A en $N(A)$ fuese 0, entonces N sería un módulo simple tal que $N = 1_A N = 0$, por el apartado (2), lo cual es una contradicción. Deducimos entonces que $\mathcal{S}(A)$ es finito. □

Sean A un álgebra semisimple, su descomposición $A = \bigoplus_{M \in \mathcal{S}(A)} M(A)$ y la expresión de $1_A = \sum_{M \in \mathcal{S}(A)} e_M$ en la misma. Dado cierto e_M, por ortogonalidad $e_M = e_M \cdot 1_A = e_M^2$, luego e_M es idempotente. De la ortogonalidad se deduce también que si x está en $M(A)$ entonces $x = 1_A x = e_M x$. De hecho, $M(A)$ es un anillo cuyo uno es precisamente e_M. Se tiene por lo tanto que e_M conmuta con los elementos de $M(A)$, y evidentemente también con los de otras componentes, ya que los anula. Deducimos que e_M está en el centro de A.

Definición 3.1.34. Sea A un álgebra semisimple. Consideremos su descomposición $A = \bigoplus_{M \in \mathcal{S}(A)} M(A)$ y la expresión de $1_A = \sum_{M \in \mathcal{S}(A)} e_M$ en la misma. Entonces a los e_M se les llama *idempotentes centrales primitivos* de A.

Observación 3.1.35. Es fácil comprobar que para cada $M \in \mathcal{S}(A)$ se da $M(A) = Ae_M$.

Hemos descompuesto entonces A en la suma directa de los $M(A)$, que son isomorfos a A_M. El siguiente teorema estudia precisamente las álgebras A_M.

Teorema 3.1.36 (Doble centralizador)**.** *Sean A una F-álgebra semisimple y M un A-módulo simple. Entonces si $D = E_A(M)$ se tiene que $E_D(M) = A_M$.*

Demostración. Recordemos que si M es un A-módulo por la izquierda, entonces es un D-módulo por la izquierda con el producto dado por $(f, x) \mapsto f(x)$ para cada $x \in M$ y $f \in D$.

Sea $a_M \in A_M$. Para cada $m \in M$ y $f \in D = E_A(M)$ se tiene que $a_M(f \cdot m) = a_M(f(m)) = af(m) = f(am) = f(a_M(m)) = f \cdot a_M(m)$. Deducimos por lo tanto que a_M está en $E_D(M)$, luego $A_M \subset E_D(M)$.

Para la otra inclusión comenzamos suponiendo que M es un submódulo de A. Pongamos $I = M(A)$, de modo que M está contenido en I. Sea $\theta \in E_D(M)$. Para cada $m \in M$ definimos la aplicación $\alpha_m : M \to M$ dada por $x \mapsto xm$, bien definida por ser M un A-módulo por la izquierda. Si $a \in A$ y $x \in M$, entonces $\alpha_m(ax) = (ax)m = a(xm) = a\alpha_m(x)$, de donde α_m pertenece a $E_A(M) = D$. Dados dos elementos m y n de M, aplicando que M es un D-módulo obtenemos la siguiente ecuación

$$\theta(nm) = \theta(\alpha_m(n)) = \theta(\alpha_m n) = \alpha_m\theta(n) = \alpha_m(\theta(n)) = \theta(n)m. \tag{3.1}$$

Sea ahora un elemento no nulo n de M, y consideramos el idempotente central primitivo e correspondiente a M. Se tiene entonces que AnA es un ideal contenido en I, y por minimalidad de este último se tiene que $I = AnA$. Podemos poner entonces que $e = \sum a_i n b_i$ para ciertos $a_i, b_i \in A$. Para $m \in M$ se verifica

$$m = em = \left(\sum a_i n b_i\right) m = \sum (a_i n)(b_i m).$$

Como $a_i n$ y $b_i m$ son elementos de M por ser este A-módulo, la Ecuación 3.1 implica que para cada $m \in M$ se cumple

$$\theta(m) = \sum \theta((a_i n)(b_i m)) = \sum \theta(a_i n)(b_i m) = \left(\sum \theta(a_i n) b_i\right) m,$$

de donde $\theta = u_M \in A_M$ para $u = \sum \theta(a_i n) b_i$.

Para el caso general, por (3.1.29) existe un submódulo M_0 de A isomorfo a M. Sea f un A-isomorfismo entre M y M_0. Es claro que la aplicación

$$\begin{aligned} G : End(M) &\longrightarrow End(M_0) \\ \phi &\longmapsto G(\phi) = f \circ \phi \circ f^{-1}, \end{aligned}$$

es un isomorfismo de F-espacios vectoriales con inversa dada por $\theta \mapsto f^{-1} \circ \theta \circ f$. Hemos demostrado previamente que $A_M \subseteq E_D(M)$ y que $A_{M_0} = E_{D_0}(M_0)$, donde $D_0 = E_A(M_0)$. Si demostramos que G se restringe a biyecciones $A_M \to A_{M_0}$ y $E_D(M) \to E_{D_0}(M_0)$ tendremos que $A_M = E_D(M)$, por igualdad de dimensiones finitas.

Como f es un A-isomorfismo se cumple que $G(a_M) = a_{M_0}$ para cada $a \in A$, luego la restricción a la primera biyección es evidente. Aplicando esto y que $E_{D_0}(M_0) = A_{M_0}$ se cumple

$$G^{-1}\left[E_{D_0}(M_0)\right] = G^{-1}\left[A_{M_0}\right] = A_M \subseteq E_D(M).$$

Dada ahora una aplicación ϕ en $E_D(M)$, para cada $h \in D_0$ y $m \in M_0$, se tiene:

$$\begin{aligned} G(\phi)(hm) = G(\phi)(h(m)) &= (f \circ \phi \circ f^{-1}) \circ (h \circ f \circ f^{-1})(m) \\ &= f \circ \phi \circ (f^{-1} \circ h \circ f) \circ (f^{-1}(m)) \\ &= f \circ (f^{-1} \circ h \circ f) \circ \phi \circ (f^{-1}(m)) \\ &= (h \circ G(\phi))(m) = hG(\phi)(m), \end{aligned}$$

siendo la tercera igualdad cierta porque ϕ es un D-homomorfismo y $f^{-1} \circ h \circ f$ un elemento de $D = E_A(M)$. Se tiene por lo tanto que $G[E_D(M)] \subset E_{D_0}(M_0)$, como queríamos demostrar. □

Corolario 3.1.37. *Sea A una F-álgebra semisimple para un cuerpo algebraicamente cerrado F, y sea M un A-módulo simple. Entonces:*

(a) $A_M = End(M)$.

(b) $\dim(A_M) = \dim(M(A)) = \dim(M)^2$.

(c) $n_M(A) = \dim(M)$.

Es más, si $\mathcal{S}(A)$ es un conjunto de representantes de A-módulos simples, entonces:

(d) $\dim(A) = \sum_{M \in \mathcal{S}(A)} \dim(M)^2$.

(e) $\dim(Z(A)) = |\mathcal{S}(A)|$.

Demostración. (a) Por (3.1.20) $E_A(M) = F \cdot \mathrm{Id}$, y por lo tanto $A_M = E_{F\cdot \mathrm{Id}}(M) = End(M)$ por (3.1.36).

(b) Por álgebra lineal básica el espacio de los F-endomorfismos de M es F-isomorfo al espacio de las matrices $d \times d$ sobre F, denotado $M_d(F)$, donde $d = \dim(M)$. Deducimos entonces que $\dim(A_M) = \dim(End(M)) = \dim(M_d(F)) = d^2$. Por (3.1.33) se tiene que $M(A) \cong A_M$, lo que demuestra la igualdad restante.

(c) $M(A)$ es suma directa de $n_M(A)$ copias isomorfas a M, de donde $d^2 = \dim(M(A)) = n_M(A)\dim(M) = d \cdot n_M(A)$.

(d) Directo por (b) y la descomposición $A = \oplus_{M \in \mathcal{S}} M(A)$.

(e) Consideramos la cadena de igualdades

$$Z(A_M) = A_M \cap E_A(M) = A_M \cap F \cdot \mathrm{Id} = F \cdot \mathrm{Id},$$

donde la primera es obvia y la segunda es cierta por (3.1.20). Deducimos entonces que la dimensión de $Z(A_M)$ es 1, la cual coincide con la de $Z(M(A))$ por (3.1.33). Es claro que $\oplus_{M \in \mathcal{S}(A)} Z(M(A))$ es un subconjunto de $Z(A)$, pues los elementos de distintas componentes se anulan y por lo tanto conmutan. Observemos que basta comprobar la inclusión contraria, ya que la dimensión de $\oplus_{M \in \mathcal{S}(A)} Z(M(A))$ es igual a $|\mathcal{S}(A)|$. Sea $z \in Z(A)$, y consideremos su descomposición $z = \sum a^M$ con $a^M \in M(A)$. Si $y \in M(A)$, entonces $ya^M = yz = zy = a^M y$, con lo que $a^M \in Z(M(A))$ y $\oplus Z(M(A)) = Z(A)$, como queríamos ver. □

Introducimos ahora el concepto de representación.

Definición 3.1.38. Sea A una F-álgebra. Una *representación* de A es un homomorfismo de álgebras ρ de A en $M_n(F)$ para cierto $n \in \mathbb{N}$, al que llamamos *grado* de ρ. Dos *representaciones* ρ_1 y ρ_2 son *similares* si existe una matriz $n \times n$ no singular P tal que $\rho_1(a) = P^{-1}\rho_2(a)P$ para cada $a \in A$.

Observación 3.1.39. Es fácil comprobar que la similaridad define una relación de equivalencia entre representaciones, y que si P es una matriz $n \times n$ invertible sobre F y ρ es una representación de A entonces $\hat{\rho}(a) := P^{-1}\rho(a)P$ también es una representación.

Si ρ es una representación de A de grado n y V_ρ es el F-espacio de vectores columna de n elementos, entonces el producto $\cdot : A \times V_\rho \to V$ dado por $a \cdot v = \rho(a)v$ le da estructura a V de A-módulo por la izquierda.

Recíprocamente, para un A-módulo V de dimensión finita sobre F y una F-base $\mathcal{B}$ fija de V, para cada $a \in A$ podemos definir $\rho_V(a)$ como la matriz del endomorfismo a_V en la base $\mathcal{B}$, aplicada a vectores columna. No es complejo comprobar que ρ es una representación de A.

Consideremos ahora dos A-módulos V y W de dimensiones m y n sobre F, respectivamente. Fijamos F-bases $\mathcal{B}_V$ y $\mathcal{B}_W$ de V y W, y construimos representaciones ρ_V y ρ_W mediante el proceso anterior. Si $\theta \in Hom_A(V, W)$, entonces θ es F-lineal y podemos considerar la matriz P de θ entre las bases fijadas, aplicada a vectores columna. Dados $a \in A$ y $v \in V$, se cumplen las igualdades

$$\theta(a_V(v)) = \theta(av) = a\theta(v) = a_W(\theta(v))$$

y, tomando coordenadas, deducimos

$$P\rho_V(a)[v]_{\mathcal{B}_V} = \rho_W(a)P[v]_{\mathcal{B}_V},$$

donde $[w]_{\mathcal{B}}$ denota el vector columna de las coordenadas de w en la base $\mathcal{B}$. Como la ecuación anterior es cierta para cada $v \in V$ y $a \in A$, se tiene que $P\rho_V(a) = \rho_W(a)P$ para cada $a \in A$. Si θ es un isomorfismo, entonces P es una matriz cuadrada no singular y la igualdad anterior implica que ρ_V y ρ_W son similares.

Volvemos a la situación inicial, con dos A-módulos V y W de dimensión finita con sendas representaciones ρ_V y ρ_W. Suponemos ahora que ρ_V y ρ_W son similares. Existe entonces una matriz $n \times n$ invertible P tal que $P\rho_V(a) = \rho_W(a)P$ para cada $a \in A$. Definimos $\theta : V \to W$ como la aplicación lineal cuya matriz entre las bases $\mathcal{B}_V$ y $\mathcal{B}_W$ aplicada a vectores columna es P. De la condición $P\rho_V(a) = \rho_W(a)P$ deducimos que $\theta(a_V(v)) = a_W(\theta(v))$ para cada $v \in V$ y $a \in A$, de donde θ es un A-isomorfismo.

Los cuatro últimos párrafos proporcionan una correspondencia inyectiva de las clases de A-módulos de dimensión finita con la relación ser isomorfos a las clases de representaciones con la relación de similitud. La suprayectividad se desprende de que el proceso de inducir una representación a partir de un A-módulo y el contrario definidos anteriormente son de hechos inversos uno del otro. En este aspecto las representaciones no son más que otra forma de ver los módulos.

Una pregunta natural ahora es la correspondencia entre la irreducibilidad de módulos y otro concepto análogo en representaciones. Sea V un A-módulo y W un submódulo propio no nulo, de dimensiones n y m sobre F respectivamente. Puedo tomar una F-base $\mathcal{B}_W$ de W y extenderla a una base $\mathcal{B}_V$ de V, de forma que los últimos m vectores sean los de $\mathcal{B}_W$. Construimos las representaciones ρ_V y ρ_W como antes. Como para cada $a \in V$ y $w \in W$ se cumple que $a_W(w) = a_V(w)$, la matriz $\rho_V(a)$ tiene que ser de la forma

$$\rho_V(a) = \begin{pmatrix} \alpha(a) & 0 \\ \beta(a) & \rho_W(a) \end{pmatrix}, \tag{3.2}$$

donde α es de hecho una representación correspondiente a V/W. El argumento anterior implica que si V no es simple podemos encontrar una descomposición diagonal inferior por bloques de ρ_V como la de la Ecuación 3.2. El recíproco también es cierto: si ρ_V es similar a una representación diagonal inferior por bloques, mediante el cambio de base correspondiente y tomando los últimos vectores de la nueva base se obtiene un subespacio W de V que también es submódulo, ya que $a_V(w) = aw$ estaría en W para cada $a \in A$ y $w \in W$.

Definición 3.1.40. Decimos que una *representación* en la forma de la Ecuación 3.2 está en *forma reducida*, y que una *representación* similar a otra en forma reducida es *reducible*. Una *representación* se dice *irreducible* si no es reducible.

Por el comentario anterior a la definición, la correspondencia vista entre clases de módulos de dimensión finita y de representaciones se restringe a otra entre clases de módulos simples y de representaciones irreducibles. Además, si consideramos $V = U \oplus W$ con U y W submódulos, fijamos una base de V formada por la concatenación de bases de U y W y generamos la representación ρ_V asociada a esta base, entonces

$$\rho_V = \begin{pmatrix} \rho_U(a) & 0 \\ 0 & \rho_W(a) \end{pmatrix},$$

donde ρ_U y ρ_W son representaciones correspondientes a U y W respectivamente. De (3.1.27) deducimos que las representaciones correspondientes a módulos completamente reducibles son similares a representaciones diagonales por bloques, siendo estos bloques representaciones irreducibles.

3.2. Representaciones de grupo y caracteres

Comenzamos esta sección extendiendo el concepto anterior de representación a un grupo.

Definición 3.2.1. Sea F un cuerpo y G un grupo. Una *F-representación de G* es un homomorfismo de grupos $\rho : G \to GL_n(F)$, donde $GL_n(F)$ denota el grupo multiplicativo de las matrices no singulares $n \times n$ sobre F.

Observación 3.2.2. Si ρ es una F-representación de G, esta se extiende por linealidad a una de $F[G]$. Recíprocamente, una representación de $F[G]$ se restringe a una de G, pues para cada $g \in G$ se cumple que $Id = \rho(1) = \rho(gg^{-1}) = \rho(g)\rho(g^{-1})$, de donde deducimos que $\rho(g) \in GL_n(F)$. Es obvio que esta correspondencia es inyectiva fijado el cuerpo F.

Siempre que el cuerpo esté claro extenderé los conceptos de "similar" e "irreducible" a representaciones de grupos a través de la representación de $F[G]$ correspondiente, e incluso denotaré la representación del grupo y la del álgebra de la misma forma.

Las representaciones contienen una gran cantidad de información sobre el grupo, incluso redundante. El concepto de carácter elimina parte de esa información, pero mantiene información suficiente para determinar muchas características del grupo. Este texto se centra en sus aplicaciones a las caracterizaciones de grupos CUT.

Definición 3.2.3. Sea ρ una F-representación de G, entonces el F-carácter proporcionado por ρ es la función

$$\begin{aligned} \chi : G &\longrightarrow F \\ g &\longmapsto \chi(g) = tr(\rho(g)). \end{aligned}$$

Al igual que las representaciones, se pueden ver como funciones en todo $F[G]$ extendiendo por linealidad.

En el caso $F = \mathbb{C}$ escribiremos representación o carácter a secas.

Observación 3.2.4. Pongamos $n = char(F)$. Si n no es 0, entonces la aplicación en G dada por $g \mapsto Id_n$ es una representación del grupo que induce la traza constantemente nula. Sin embargo, si $n = 0$ y ρ es una representación, se cumple que $\chi(1) = tr(\rho(1)) = tr(Id_{gr(\rho)}) = gr(\rho)$.

Definición 3.2.5. Si $char(F) = 0$, llamamos *grado* de χ a $gr(\chi) := \chi(1)$. Si el grado de un carácter es 1 decimos que es lineal.

Lema 3.2.6. *F-representaciones similares de G inducen el mismo carácter, y los caracteres son constantes en cada clase de conjugación del grupo.*

Demostración. Evidente puesto que $tr(P^{-1}AP) = tr(A)$ y $\rho(g^{-1}) = \rho(g)^{-1}$. □

Observación 3.2.7. Si ρ_1 y ρ_2 son representaciones de G entonces $\rho_3 := diag(\rho_1, \rho_2)$ también lo es, e induce el carácter $tr(\rho_3(g)) = tr(\rho_1(g)) + tr(\rho_2(g))$. Deducimos que el conjunto de caracteres es cerrado para la suma.

Definición 3.2.8. Decimos que un *carácter* es *irreducible* si es proporcionado por una representación irreducible.

En adelante estudiaremos el caso $F = \mathbb{C}$, aunque el mismo desarrollo se podría hacer en el caso del *cuerpo de los números algebraicos* $\mathcal{A}_{\mathbb{Q}}$, pues usamos que son cuerpos de característica 0 y algebraicamente cerrados. Considérese la siguiente notación. Por el Teorema de Maschke (3.1.24) $\mathbb{C}[G]$ es semisimple, y por el Teorema de Wedderburn (3.1.33) $\mathcal{S}(\mathbb{C}[G])$ es finito, pongamos $\mathcal{S}(\mathbb{C}[G]) = \{M_1, \ldots, M_k\}$. En cada M_i considero una F-base y la representación ρ_i que induce, junto con sus respectivos caracteres proporcionados χ_i. Como módulos isomorfos inducen representaciones similares y representaciones similares inducen el mismo carácter, el conjunto de todos los caracteres irreducibles es precisamente $\{\chi_1, \ldots, \chi_k\}$, y se denota por $Irr(G)$. Fijamos un grupo finito G en lo que resta de sección, y mantenemos la notación introducida para los módulos, representaciones y caracteres irreducibles de G.

Observación 3.2.9. Como la suma de caracteres es un carácter, $\chi = \sum n_i\chi_i$ es un carácter si los n_i son enteros no negativos. Recíprocamente, dado un carácter χ proporcionado por una representación ρ, entonces ρ es similar a otra en forma diagonal por bloques correspondientes a representaciones irreducibles, de donde χ es suma de los caracteres irreducibles χ_i. Más concretamente, si V es un módulo correspondiente a la representación ρ, entonces se cumple que $\chi = \sum_{i=1}^{k} n_{M_i}(V)\chi_i$.

Por (3.1.37.(d)) sabemos que $\dim(\mathbb{C}[G]) = \sum(\dim M_i)^2$. Como la dimensión de $\mathbb{C}[G]$ es el orden de G y $\dim(M_i) = gr(\rho_i) = \chi_i(1)$, deducimos la fórmula

$$|G| = \sum_{i=1}^{k} \chi_i(1)^2. \tag{3.3}$$

Observación 3.2.10. Por (3.1.37.(e)) $k = |\mathcal{S}(\mathbb{C}[G])| = \dim(Z(\mathbb{C}[G]))$.

Teorema 3.2.11. *Sean $\mathcal{H}_1, \ldots, \mathcal{H}_r$ las clases de conjugación de G, y sea $K_i := \sum_{x\in\mathcal{H}_i} x \in \mathbb{C}[G]$. Entonces $\{K_i\}$ es una base de $Z(\mathbb{C}[G])$, y si $K_iK_j = \sum a_{ijv}K_v$ con $a_{ijv} \in \mathbb{C}$, entonces los a_{ijv} son enteros no negativos.*

Demostración. Dado $g \in G$, observamos que

$$g^{-1}K_ig = \sum_{h\in\mathcal{H}_i} g^{-1}hg = \sum_{h\in\mathcal{H}_i} h = K_i,$$

pues $g^{-1}hg$ recorre $\mathcal{H}_i$ si h lo hace. Se tiene pues que $K_ig = gK_i$ para cada $g \in G$, relación que se extiende a todo $\mathbb{C}[G]$ por linealidad. Deducimos por lo tanto que $K_i \in Z(\mathbb{C}[G])$. Es claro también que los K_i son linealmente independientes, pues son suma de elementos de subconjuntos disjuntos de G. Finalmente, si $z = \sum_{g\in G} a_g g$ es un elemento central de $\mathbb{C}[G]$ y h un elemento de G, comparando los coeficientes de $z = h^{-1}zh = z^h$ se tiene que $a_{g^h} = a_g$ para cada $g \in G$. Deben

coincidir entonces los coeficientes a_g con $g \in \mathcal{H}_i$ para cada i, y si llamamos b_i al valor que toman se cumple que $z = \sum_{i=1}^{r} b_i K_i$.

Por definición de producto en el álgebra de grupo se cumple

$$K_i K_j = \sum_{g \in G} \sum_{(x \in \mathcal{H}_i, y \in \mathcal{H}_j | xy = g)} g = \sum_{g \in G} |\{(x,y) \in \mathcal{H}_i \times \mathcal{H}_j | xy = g\}| g,$$

y como todos los coeficientes son cardinales, son enteros no negativos. Como los $K_i K_j$ son elementos centrales de $\mathbb{C}[G]$ ya hemos visto que los coeficientes son iguales para elementos conjugados, lo que termina de probar la última afirmación. □

Corolario 3.2.12. *El número de clases de similitud de representaciones irreducibles de G es igual al número de clases de conjugación de G.*

Los caracteres irreducibles de un grupo se suelen presentar en forma de tabla, cada fila correspondiendo a un carácter irreducible y cada columna a un representante de la clase de conjugación. En el cuadro 3.1 se puede observar el ejemplo de la tabla del grupo simétrico de 4 elementos.

	1	(1 2)	(1 2)(3 4)	(1 2 3 4)	(1 2 3)
χ_1	1	1	1	1	1
χ_2	1	-1	1	-1	1
χ_3	2	0	2	0	-1
χ_4	3	1	-1	-1	0
χ_5	3	-1	-1	1	0

Cuadro 3.1: Tabla de caracteres del grupo simétrico de 4 elementos.

Corolario 3.2.13. *Un grupo G es abeliano si y solo si cada carácter irreducible es lineal.*

Demostración. Si k es el número de clases de conjugación de G, entonces G es abeliano si y solo si $k = |G|$. Usando que $|G| = \sum_1^k \chi_i(1)^2$ y que cada cada $\chi_i(1)$ es mayor o igual que 1 el resultado es obvio. □

Observación 3.2.14. Consideramos en la descomposición $\mathbb{C}[G] = \oplus_1^k M_i(\mathbb{C}[G])$ la expresión de 1:

$$1 = \sum_1^k e_i \text{ con } e_i \in M_i(\mathbb{C}[G]) \text{ para cada i.}$$

Si $i \neq j$, como $e_j \in M_j(\mathbb{C}[G])$ y este anula a M_i por (3.1.33), deducimos que la aplicación $(e_j)_{M_i}$ es nula, y por lo tanto $\rho_i(e_j) = 0$. Por el contrario, e_i es el uno de la componente $M_i(\mathbb{C}[G])$, y en concreto $(e_i)_{M_i} = Id$, de donde $\rho_i(e_i) = Id$. Esto demuestra no solo que los caracteres χ_i son distintos dos a dos, sino también que son linealmente independientes sobre $\mathbb{C}$. Mantendremos la notación e_i para los idempotentes centrales de $\mathbb{C}[G]$ en el resto de la sección.

Definición 3.2.15. Dado un grupo G y un cuerpo F, una función de clase es una función $G \to F$ constante en las clases de conjugación.

En este trabajo siempre hablaremos de funciones de clase sobre $\mathbb{C}$. Es evidente que los caracteres son funciones de clase.

Observación 3.2.16. Las funciones de clase forman un espacio vectorial de dimensión el número de clases de conjugación, es decir, $k = |Irr(G)|$.

Teorema 3.2.17. *$Irr(G)$ es una base del espacio de funciones de clase. Es más, una función de clase es un carácter si y solo si sus coeficientes en dicha base son enteros no negativos.*

Demostración. La primera afirmación es consecuencia de (3.2.14) y (3.2.16), mientras que la última se prueba en (3.2.9). □

Este espacio es de hecho un espacio de Hilbert, e $Irr(G)$ es una base ortonormal de dicho espacio, como veremos en los siguientes resultados.

Definición 3.2.18. Se denomina carácter regular de un grupo G al carácter proporcionado por la representación generada por el $\mathbb{C}[G]$-módulo regular.

Lema 3.2.19. *Sean ϕ el carácter regular de $\mathbb{C}[G]$ y $g \in G$, entonces*

$$\phi(g) = \begin{cases} 0 & si\ g \neq 1; \\ |G| & si\ g = 1. \end{cases}$$

Demostración. Tomamos como base de $\mathbb{C}[G]$ el propio G, que genera cierta representación ρ. Pongamos $G = \{g_1, g_2, \ldots, g_r\}$ y sea $g \in G$. Si $\rho(g) = (a_{ij})$, entonces para cualquier elemento g_j de G se cumple que $gg_j \in G$, de modo que $a_{ij} = 0$ a no ser que gg_j sea precisamente g_i, en cuyo caso $a_{ij} = 1$. $\phi(g)$ es entonces el número de $g_i \in G$ con $gg_i = g_i$, de lo cual se deduce el resultado trivialmente. □

Lema 3.2.20. *Si ϕ es el carácter regular de $\mathbb{C}[G]$, entonces $\phi = \sum_{i=1}^{k} \chi_i(1)\chi_i$.*

Demostración. Por (3.2.9) tenemos que $\phi = \sum_1^k n_{M_i}(\mathbb{C}[G])\chi_i$, y por (3.1.37) se cumple que $n_{M_i}(\mathbb{C}[G]) = \dim M_i = \chi_i(1)$. □

Teorema 3.2.21. $e_i = \frac{1}{|G|} \sum_{g \in G} \chi_i(1)\chi_i(g^{-1})g$.

Demostración. Pongamos $e_i = \sum_{g \in G} a_g g$ con $a_g \in \mathbb{C}$ y sea ϕ el carácter regular. Aplicando (3.2.19) deducimos que $\phi(e_i g^{-1}) = a_g|G|$. Usando dicha igualdad y (3.2.20) obtenemos

$$a_g|G| = \sum_j \chi_j(1)\chi_j(e_i g^{-1}).$$

Por (3.2.14) se cumple

$$\rho_j(e_i g^{-1}) = \rho_j(e_i)\rho_j(g^{-1}) = \begin{cases} 0 & \text{si } i \neq j; \\ \rho_i(g^{-1}) & \text{si } i = j, \end{cases}$$

y tomando trazas obtenemos que $\chi_j(e_i g^{-1}) = \chi_i(g^{-1})\delta_{ij}$, donde δ_{ij} denota la delta de Kronecker. Deducimos por lo tanto que $a_g|G| = \chi_i(1)\chi_i(g^{-1})$. □

Teorema 3.2.22. *Para cada $h \in G$ se cumple*

$$\frac{1}{|G|} \sum_{g \in G} \chi_i(gh)\chi_j(g^{-1}) = \delta_{ij} \frac{\chi_i(h)}{\chi_j(1)}.$$

Demostración. Consideramos la igualdad $e_i e_j = \delta_{ij} e_i$, en la que aplicamos las expresiones calculadas de los e_i en (3.2.21) e igualamos coeficientes en la base G. Para cierto $h \in G$, los coeficientes de $\delta_{ij} e_i$ y $e_i e_j$ quedan, respectivamente:

$$\frac{\delta_{ij}}{|G|}\chi_i(1)\chi_i(h^{-1}) = \frac{\chi_i(1)\chi_j(1)}{|G|^2}\sum_{g\in G}\chi_i((hg^{-1})^{-1})\chi_j(g^{-1}).$$

Cambiando en la igualdad anterior h por h^{-1} y dividiendo por $\chi_i(1)\cdot\chi_j(1) \neq 0$ se obtiene el enunciado. □

Corolario 3.2.23. $\frac{1}{|G|}\sum_{g\in G}\chi_i(g)\chi_j(g^{-1}) = \delta_{ij}$.

Demostración. Es el caso particular de (3.2.22) para $h = 1$. □

Lema 3.2.24. *Sea ρ una representación de G, y sea $g \in G$ de orden n. Entonces $\rho(g)$ es similar a una matriz diagonal $diag(\varepsilon_1, \ldots, \varepsilon_s)$ tal que $\varepsilon_j^n = 1$ para cada $j = 1, \ldots, s$.*

Demostración. La restricción de ρ al subgrupo $\langle g\rangle$ es una representación del mismo, así que podemos suponer $G = \langle g\rangle$. Por el teorema de Maschke ρ es similar una forma diagonal por bloques de representaciones irreducibles. Estos bloques deben ser de tamaño 1 por (3.2.13), ya que $\langle g\rangle$ es un grupo abeliano. Deducimos que ρ es similar a cierta representación diagonal, y existe una matriz invertible P tal que $P^{-1}\rho(g)P = diag(\varepsilon_1, \ldots, \varepsilon_s)$. Pero la aplicación $\hat{\rho}$ dada por $h \mapsto P^{-1}\rho(h)P$ es también una representación, de donde $Id = \hat{\rho}(g^n) = \hat{\rho}(g)^n = diag(\varepsilon_1^n, \ldots, \varepsilon_r^n)$, como queríamos demostrar. □

Corolario 3.2.25. *Si χ es un carácter, entonces $\chi(g^{-1}) = \overline{\chi(g)}$.*

Demostración. De igual manera que en la demostración anterior tomamos una representación ρ que induce χ tal que $\rho(g) = diag(\varepsilon_1, \ldots, \varepsilon_s)$ y los ε_i son raíces $o(g)$-ésimas de la unidad. En este caso se tiene que

$$\rho(g^{-1}) = \rho(g)^{-1} = diag(\varepsilon_1^{-1}, \ldots, \varepsilon_s^{-1}),$$

y como $\varepsilon_i^{o(g)} = 1$ para cada i deducimos que $|\varepsilon_i| = 1$ y $\varepsilon_i^{-1} = \overline{\varepsilon_i}$. Basta entonces tomar trazas. □

Corolario 3.2.26. *Si χ es un carácter de G, $n = |G|$ y ξ_n es una raíz primitiva n-ésima de la unidad, entonces $\chi(g) \in \mathbb{Z}[\xi_n] \subseteq \mathbb{Q}(\xi_n)$ para cada $g \in G$. En particular, los caracteres de un grupo finito toman valores algebraicos sobre $\mathbb{Q}$.*

Demostración. Tomamos por (3.2.24) una representación ρ que induzca χ tal que $\rho(g) = diag(\varepsilon_1, \ldots, \varepsilon_s)$ y $\varepsilon_j^{o(g)}$ para cada $j = 1, \ldots, s$. Se tiene entonces que cada ε_j es raíz n-ésima de la unidad, ya que $o(g)$ divide a n, y por lo tanto cada ε_j es una potencia de ξ_n. Como $\chi(g) = \varepsilon_1 + \cdots + \varepsilon_s$, ya tenemos que $\chi(g) \in \mathbb{Z}[\xi_n]$. La última afirmación es cierta porque $\mathbb{Q}(\xi_n)$ es una extensión finita sobre $\mathbb{Q}$, y por lo tanto es algebraica. □

Teorema 3.2.27. *La aplicación que a cada par de funciones de clase θ y ψ asigna $\langle\theta, \psi\rangle = \frac{1}{|G|}\sum_{g\in G}\theta(g)\overline{\psi(g)}$ define un producto escalar complejo, con el cual $Irr(G)$ es base ortonormal del espacio de las funciones de clase.*

Demostración. Es rutinario comprobar que se trata de un producto escalar complejo. Ya habíamos demostrado que $Irr(G)$ es una base del espacio de las funciones de clase. La ortonormalidad se deduce de (3.2.23) y de (3.2.25). □

Corolario 3.2.28. *Si χ_1 y χ_2 son caracteres de G, entonces $\langle \chi_1, \chi_2 \rangle = \langle \chi_2, \chi_1 \rangle$ es un entero no negativo, Además, χ_1 es irreducible si y solo si $\langle \chi_1, \chi_1 \rangle = 1$.*

Demostración. Basta usar (3.2.9) y la sesquilinealidad del producto escalar para la primera afirmación. Un carácter es irreducible si y solo si en la descomposición de (3.2.9) un coeficiente igual 1 y el resto nulos, de donde, junto a la sesquilinealidad, deducimos fácilmente la segunda afirmación. □

Corolario 3.2.29. *Los $\mathcal{A}_{\mathbb{Q}}$-caracteres irreducibles son los mismos que los $\mathbb{C}$-caracteres irreducibles. En concreto, todo $\mathbb{C}$-carácter es proporcionado por una $\mathcal{A}_{\mathbb{Q}}$-representación.*

Demostración. Obsérvese que todo el desarrollo sobre $\mathbb{C}$ se puede hacer sobre $\mathcal{A}_{\mathbb{Q}}$, pues solo se usa que el cuerpo es algebraicamente cerrado y que es de característica 0. En concreto, tanto el número de $\mathcal{A}_{\mathbb{Q}}$-caracteres irreducibles como el de $\mathbb{C}$-caracteres irreducibles coinciden con el número de clases de conjugación. Dado un $\mathcal{A}_{\mathbb{Q}}$-carácter irreducible proporcionado por una $\mathcal{A}_{\mathbb{Q}}$-representación ρ, esta se puede ver de forma natural como una $\mathbb{C}$-representación, pues $\mathcal{A}_{\mathbb{Q}}$ es un subconjunto de $\mathbb{C}$. Tenemos entonces que χ es un $\mathbb{C}$-carácter. Además, como el desarrollo del producto escalar es idéntico en ambos cuerpos, se cumple que $\langle \chi, \chi \rangle = 1$ visto sobre $\mathcal{A}_{\mathbb{Q}}$ por (3.2.28). Como el valor del producto escalar depende de los valores que tomen los caracteres y no del cuerpo de llegada, $\langle \chi, \chi \rangle$ también vale 1 sobre $\mathbb{C}$, y de nuevo por (3.2.28) deducimos que χ es $\mathbb{C}$-irreducible. Por lo tanto, $Irr_{\mathcal{A}_{\mathbb{Q}}}(G)$ es un subconjunto de $Irr(G)$ con el mismo cardinal finito, luego son iguales.

La última afirmación es entonces evidente para caracteres irreducibles. Para caracteres generales basta usar (3.2.9) y representaciones diagonales por bloques que sean $\mathcal{A}_{\mathbb{Q}}$-representaciones irreducibles. □

Hasta el momento no se ha hablado de $\mathbb{Q}[G]$. Aunque los $\mathbb{Q}$-caracteres irreducibles no coinciden exactamente con los $\mathbb{C}$-caracteres irreducibles, si guardan cierta relación que no es explorada en este texto. Siguiendo la sección 3.3 de [JR16], descompondremos $\mathbb{Q}[G]$ en componentes simples, al igual que $\mathbb{C}[G]$, y conectaremos los centros de dichas componentes con las extensiones algebraicas generadas sobre $\mathbb{Q}$ por las imágenes de los $\mathbb{C}$-caracteres irreducibles. Podremos estudiar las unidades de ciertos subanillos de estas extensiones gracias al Teorema de las Unidades de Dirichlet, que se verá en el Capítulo 4.

Consideramos una extensión de cuerpos $\mathbb{C}/F$, con lo que $char(F) = 0$. Por el Teorema de Maschke (3.1.24) $F[G]$ es semisimple, y por el Teorema de Wedderburn (3.1.33) $\mathcal{S}(F[G])$ es un conjunto finito, pongamos $\{N_1, \ldots, N_r\}$. En la descomposición $F[G] = \oplus N_i(F[G])$ consideramos la expresión de $1 = f_1 + \ldots + f_r$, con cada $f_i \in N_i(F[G])$, es decir, los f_i son los idempotentes centrales primitivos de $F[G]$.

Observación 3.2.30. Es claro que $F[G]$ es un subanillo de $\mathbb{C}[G]$. Consideremos la igualdad

$$e_1 + \ldots + e_k = 1 = f_1 + \ldots + f_r.. \tag{3.4}$$

Como los f_j son ortogonales, para cada e_i existe un único f_j tal que $e_i f_j$ no es 0. Multiplicando la igualdad de la Ecuación 3.4 por e_i se tiene que $e_i f_j = e_i$. Deducimos que los f_j particionan los

e_i en conjuntos E_j tales que $f_j = \sum_{e \in E_j} e$. Por lo tanto, dado un $\mathbb{C}$-carácter irreducible χ existe un único idempotente central primitivo f de $F[G]$ tal que $\chi(f) \neq 0$.

Notación 3.2.31. Dado $\chi \in Irr(G)$, denotamos:

1. $e_F(\chi)$ al único idempotente central primitivo de $F[G]$ tal que $\chi(e_F(\chi)) \neq 0$.
2. $A_F(\chi) = e_F(\chi)F[G]$ a la componente de $F[G]$ asociada.
3. $F(\chi)$ a la extensión generada por la imagen de χ sobre F, esto es, $F(\chi) = F(\chi(g)|g \in G)$.

Observación 3.2.32. $e_{\mathbb{C}}(\chi_i) = e_i$, y se denotará simplemente por $e(\chi_i)$. Nótese que en este caso la correspondencia de caracteres irreducibles a idempotentes centrales primitivos es inyectiva además de sobreyectiva.

Fijamos en lo que queda de sección un $\mathbb{C}$-caracter irreducible χ, y pasamos a estudiar el caso $F = \mathbb{Q}$. Ya hemos visto que $\mathbb{Q}(\chi)$ es una extensión algebraica, veamos ahora que es además una extensión de Galois abeliana, esto es, una extensión de Galois con grupo de Galois abeliano.

Lema 3.2.33. $\mathbb{Q}(\chi)/\mathbb{Q}$ *es una extensión de Galois abeliana.*

Demostración. Pongamos $n = |G|$, y sea ξ_n una raíz n-ésima primitiva de la unidad. Por (3.2.26) se tiene la cadena de extensiones $\mathbb{Q} \subseteq \mathbb{Q}(\chi) \subseteq \mathbb{Q}(\xi_n)$. La extensión $\mathbb{Q}(\xi_n)/\mathbb{Q}$ es una extensión ciclotómica, y sabemos que tiene grupo de Galois $\mathbb{Z}_n^*$ [ACM02, Corolario 9.2.5], que es abeliano, y por lo tanto todos sus subgrupos son normales. Aplicando entonces el Segundo Teorema Fundamental de la Teoría de Galois [ACM02, Teorema 5.3.6] al cuerpo intermedio $\mathbb{Q}(\chi)$, la extensión $\mathbb{Q}(\chi)/\mathbb{Q}$ es de Galois, y su grupo de Galois es un grupo cociente de $\mathbb{Z}_n^*$, luego también es abeliano. □

Consideramos ahora $\sigma \in Gal(\mathbb{Q}(\chi)/\mathbb{Q})$. Podemos extender este automorfismo a la clausura algebraica $\mathcal{A}_{\mathbb{Q}}$ de $\mathbb{Q}(\chi)$ [ACM02, Corolario 4.1.18], resultando en un isomorfismo $\overline{\sigma} : \mathcal{A}_{\mathbb{Q}} \to \mathcal{A}_{\mathbb{Q}}$. Podemos considerar por (3.2.29) una $\mathcal{A}_{\mathbb{Q}}$-representación ρ que induzca χ , y denotaremos por ρ^σ a la aplicación dada por $g \mapsto (\overline{\sigma}(\rho(g)_{ij}))$, esto es, el resultado de aplicar $\overline{\sigma}$ componente a componente en la representación ρ. Es sencillo comprobar que ρ^σ es también una representación, y se tiene entonces que $\overline{\sigma} \circ \chi = \sigma \circ \chi$ es un carácter, pues es proporcionado por ρ^σ. Denotaremos a $\sigma \circ \chi$ por χ^σ. Consideramos entonces la siguiente cadena de igualdades:

$$\langle \sigma \circ \chi, \sigma \circ \chi \rangle = \frac{1}{|G|} \sum_{g \in G} \sigma \circ \chi(g) \cdot \sigma \circ \chi(g^{-1}) = \sigma \left(\frac{1}{|G|} \sum_{g \in G} \chi(g) \cdot \chi(g^{-1}) \right) = \sigma(1) = 1,$$

donde en la primera igualdad aplicamos (3.2.25), en la tercera que χ es irreducible y en el resto que σ es homomorfismo. Por (3.2.28) deducimos que χ^σ es también un carácter irreducible.

Podemos extender también de forma natural σ a una aplicación en $\mathbb{Q}(\chi)[G]$ que asocia cada $\sum_{g \in G} a_g g$ con $\sum_{g \in G} \sigma(a_g)g$. Aplicando (3.2.21) obtenemos que $e(\chi)$ es un elemento de $\mathbb{Q}(\chi)G$ y que $e(\sigma \circ \chi) = \sigma(e(\chi))$.

Observación 3.2.34. Si σ y τ son $\mathbb{Q}$-automorfismos de $\mathbb{Q}(\chi)$, entonces por (3.2.32) $e(\sigma \circ \chi) = e(\tau \circ \chi)$ si y solo si $\sigma \circ \chi = \tau \circ \chi$, lo cual ocurre si y solo si $\sigma(\chi(g)) = \tau(\chi(g))$ para cada $g \in G$ o, equivalentemente, $\sigma = \tau$.

Teorema 3.2.35. *Sean $\chi \in Irr(G)$ y $G_\chi = Gal(\mathbb{Q}(\chi)/\mathbb{Q})$, entonces*

1. $e_{\mathbb{Q}}(\chi) = tr_{\mathbb{Q}(\chi)/\mathbb{Q}}(e(\chi)) = \sum_{\sigma \in G_\chi} e(\sigma \circ \chi)$:

2. *Si $\psi \in Irr(G)$ entonces $A_{\mathbb{Q}}(\psi) = A_{\mathbb{Q}}(\chi)$ si y solo si $e_{\mathbb{Q}}(\psi) = e_{\mathbb{Q}}(\chi)$, lo cual equivale a que ψ sea igual a $\sigma \circ \chi$ para cierto $\sigma \in G_\chi$.*
3. *Si $E/\mathbb{Q}$ es una extensión de cuerpos y ρ es una E-representación que induce χ, entonces $A_{\mathbb{Q}}(\chi)$ es isomorfo a $\rho(\mathbb{Q}[G])$, que es el $\mathbb{Q}$-espacio generado por $\rho(G)$ en el espacio de las matrices $n \times n$ sobre E, con $n = \chi(1) = gr(\chi) = gr(\rho)$.*
4. *$Z(A_{\mathbb{Q}}(\chi))$ es $\mathbb{Q}$-isomorfo a $\mathbb{Q}(\chi)$.*

Demostración. (1) Sea $e = tr_{\mathbb{Q}(\chi)/\mathbb{Q}}(e(\chi))$. Entonces e es un elemento de $\mathbb{Q}[G]$ por (2.2.5.(6)), y es además suma de idempotentes centrales primitivos de $\mathbb{C}[G]$, distintos dos a dos por (3.2.34). Deducimos que e es un idempotente central de $\mathbb{Q}[G]$. Lo que buscamos demostrar es que $e = e_{\mathbb{Q}(\chi)}$.

Consideremos el producto $e' = e \cdot e_{\mathbb{Q}}(\chi)$. Este elemento está en $\mathbb{Q}[G]$, es idempotente central del mismo y no es nulo, ya que en las descomposición de e y $e_{\mathbb{Q}}(\chi)$ en $\mathbb{C}[G]$ aparece la componente $e(\chi)$. Si e' fuese distinto de e, sería porque en la descomposición de e en $\mathbb{C}[G]$ aparecen idempotentes centrales primitivos que no están en la de $e_{\mathbb{Q}}(\chi)$, y existiría por lo tanto un subconjunto propio I de G_χ que contiene a la identidad de manera que $e' = \sum_{\sigma \in I} e(\sigma \circ \chi)$. Para cada α de G_χ se tendría entonces que $e' = \alpha(e') = \sum_{(\alpha\sigma) \in I} e(\sigma \circ \chi)$, de forma que $I = \{\alpha\sigma | \sigma \in I\}$ y α estaría en I. Esto contradice que I sea subconjunto propio de G_χ.

Recapitulando, tanto e como $e_{\mathbb{Q}}(\chi)$ son suma de idempotentes centrales primitivos de $\mathbb{C}[G]$, y el párrafo anterior demuestra que los sumandos de e son un subconjunto de los de $e_{\mathbb{Q}}(\chi)$. Si e no fuese $e_{\mathbb{Q}}(\chi)$ sería porque sus sumandos idempotentes centrales primitivos de $\mathbb{C}[G]$ son un subconjunto propio de los de $e_{\mathbb{Q}}(\chi)$, y en particular existiría un idempotente central primitivo e_i de $\mathbb{C}[G]$ tal que $e_i e = 0 \neq e_i e_{\mathbb{Q}}(\chi)$. En ese caso se tendría que $e\mathbb{Q}[G]$ es un ideal contenido en $e_{\mathbb{Q}}(\chi)\mathbb{Q}[G]$, este último siendo ideal minimal de $\mathbb{Q}[G]$ por (3.1.33). Debe ser entonces $e\mathbb{Q}[G] = e_{\mathbb{Q}}(\chi)\mathbb{Q}[G]$, y existir $x \in \mathbb{Q}[G]$ tal que $e_{\mathbb{Q}}(\chi) = ex$, de donde llegamos a la contradicción $0 \neq e_i e_{\mathbb{Q}}(\chi) = e_i e x = 0$. Esto termina de demostrar que $e = e_{\mathbb{Q}}(\chi)$, que era lo que queríamos ver.

(2) La primera equivalencia es evidente, mientras que la segunda es una consecuencia directa de (1) y de (3.2.34).

(3) Como $\rho(e_{\mathbb{Q}}(\chi)) = Id$ y ρ se anula en el resto de componentes de Wedderburn de $\mathbb{Q}[G]$, ρ induce un $\mathbb{Q}$-homomorfismo no nulo de $A = A_{\mathbb{Q}}(\chi)$ en la imagen por ρ de todo $\mathbb{Q}[G]$. El núcleo K de la restricción de ρ a $\mathbb{Q}[G]$ es claramente un ideal de $\mathbb{Q}[G]$, luego la intersección de K con A es un ideal de $\mathbb{Q}[G]$ contenido en A. Por (3.1.33.(1)) debe ser $K \cap A = 0$, de donde deducimos que ρ es inyectivo en A.

(4) Tomando E igual a $\mathbb{C}$ o $\mathcal{A}_{\mathbb{Q}}$ sabemos que existen tales representaciones, de las cuales fijamos una. Por (3.1.37.(a)) sabemos que el E-espacio generado por $\rho(G)$, esto es, la imagen por ρ de $E[G]$, es todo el espacio $M_n(E)$. Como $\rho(A)$ es el $\mathbb{Q}$-espacio generado por $\rho(G)$, el centro de $\rho(A)$ está contenido en $Z(M_n(E))$, que es $E\,\mathrm{Id}_n$. Basta ver que $Z(\rho(A)) = \mathbb{Q}(\chi)\,\mathrm{Id}_n$, pues en ese caso el $\mathbb{Q}$-isomorfismo entre $Z(\rho(A))$ y $\mathbb{Q}(\chi)$ es claro.

Consideremos un elemento $\sum_{g \in G} a_g \rho(g)$ de $Z(\rho(A))$, con los a_g racionales. Sea $x \in E$ tal que $x\,\mathrm{Id}_n = \sum_{g \in G} a_g \rho(g)$. Tomando trazas deducimos que $nx = \sum_{g \in G} a_g \chi(g)$, que es un elemento de $\mathbb{Q}(\chi)$. Como n no es 0 se tiene que x también está en $\mathbb{Q}(\chi)$, de donde obtenemos que $Z(\rho(A))$ está contenido en $\mathbb{Q}(\chi)\,\mathrm{Id}_n$.

Sea ahora $g \in G$, y denotemos por g^G a la clase de conjugación de g y por $\widetilde{g}$ a la suma de los elementos de g^G, que es claramente un elemento central de $\mathbb{Q}[G]$. Se tiene entonces que $\rho(\widetilde{g})$ es un elemento central de $\rho(A)$, y como $Z(\rho(A)) \subseteq Z(M_n(E)) = E\,\mathrm{Id}_n$ existe $x \in E$ tal

que $\rho(\widetilde{g}) = x\,\mathrm{Id}_n$. Tomando trazas deducimos que $|g^G|\chi(g) = \chi(1)x$, ya que los caracteres son constantes en clases de conjugación. Despejando el valor de x resulta que

$$\rho(\widetilde{g}) = \frac{|g^G|\chi(g)}{\chi(1)}\,\mathrm{Id}_n,$$

y finalmente

$$\chi(g)\,\mathrm{Id}_n = \frac{\chi(1)}{|g^G|}\rho(\widetilde{g}).$$

Ahora bien, el elemento de la derecha pertenece a $Z(\rho(A))$ ya que $\chi(1)/|g^G|$ es racional. Deducimos de la arbitrariedad de $g \in G$ que $\mathbb{Q}(\chi)\,\mathrm{Id}_n$ está contenido en $Z(\rho(A))$. □

3.3. Órdenes

Introducimos en esta sección la estructura de orden. El desarrollo que se hace a continuación está basado en la sección 4.6 de [JR16]. Consideremos un dominio Noetheriano conmutativo R con cuerpo de fracciones F, y sea además K/F una extensión de cuerpos.

Definición 3.3.1. Si V es un K-espacio vectorial de dimensión $n < \infty$, un *R-retículo* en V es un R-submódulo finitamente generado de V. Diremos que es *pleno* si contiene una K-base de V.

Un caso particular es el de una K-álgebra A de dimensión finita. Podemos definir entonces el siguiente concepto.

Definición 3.3.2. Un *R-orden* en A es un subanillo de A que también es un R-retículo pleno en A.

Nos restringimos ahora al caso $R = \mathbb{Z}$ y $F = K = \mathbb{Q}$, y hablaremos directamente de retículos y órdenes, omitiendo el prefijo "$\mathbb{Z}$-".

El concepto de orden juega un papel importante en los argumentos presentados en este texto. $\mathbb{Z}[G]$ será precisamente un orden en $\mathbb{Q}[G]$, y $e\mathbb{Z}[G]$ lo será en $e\mathbb{Q}[G]$ para cada idempotente central primitivo e de $\mathbb{Q}[G]$. En (3.2.35) estudiamos el centro de las componentes $e\mathbb{Q}[G]$, que son isomorfas a extensiones finitas de $\mathbb{Q}$. El Teorema de las Unidades de Dirichlet estudia las unidades de un orden concreto en este tipo de extensiones, pero veremos que la finitud del grupo de las unidades de un orden implica la de todos los demás.

En adelante A será una $\mathbb{Q}$-álgebra de dimensión finita n y $\mathcal{O}$ un orden en A. Nótese que el producto entre elementos de $\mathbb{Z}$ y de $\mathcal{O}$ procede del producto por escalares de un espacio vectorial, de forma que no hay elementos de torsión. Como $\mathbb{Z}$ es un DIP, se tiene que $\mathcal{O}$ es un $\mathbb{Z}$-módulo finitamente generado libre [Lan02, Teorema 7.43]. Podemos considerar entonces una $\mathbb{Z}$-base $\mathcal{B}$ de $\mathcal{O}$. Como $\mathcal{O}$ es un retículo pleno, dicha base genera una $\mathbb{Q}$-base de A, luego el $\mathbb{Q}$-espacio generado por $\mathcal{B}$ es todo A. Además, los elementos de $\mathcal{B}$ son linealmente independientes sobre $\mathbb{Z}$, luego también lo son sobre $\mathbb{Q}$. Deducimos que $\mathcal{B}$ es también $\mathbb{Q}$-base de A. Esto demuestra el siguiente lema.

Lema 3.3.3. *Sea A una $\mathbb{Q}$-álgebra de dimensión finita y $\mathcal{O}$ un orden en A. Entonces $\mathcal{O}$ es un $\mathbb{Z}$-módulo libre finitamente generado, y toda $\mathbb{Z}$-base suya es también $\mathbb{Q}$-base de A.*

Lema 3.3.4. *Sea V un $\mathbb{Q}$-espacio vectorial de dimensión finita n, y sea L un $\mathbb{Z}$-retículo pleno en V. Si X es un subconjunto finito de V, entonces existe un entero no nulo r tal que rX está contenido en L. Si L' es otro $\mathbb{Z}$-retículo pleno en V, entonces existe un entero no nulo r tal que rL está contenido en L'.*

Demostración. Sea $v_1, \dots, v_n$ una base de V en L. Dado entonces $x \in X$, consideremos sus expresiones en la base fijada, $x = \sum_{i=1}^{n} a_{i,x} v_i$ con $a_{i,x} \in \mathbb{Q}$. Es claro que tomando r como el producto de los denominadores de los $a_{i,x}$ se verifica que rX está contenido en L. La última afirmación se deduce de aplicar la primera a un conjunto generador finito de L'. □

Lema 3.3.5. *1. Si $\mathcal{O}_1$ y $\mathcal{O}_2$ son órdenes en A entonces $\mathcal{O}_1 \cap \mathcal{O}_2$ también.*

2. Si B es subálgebra de A y $\mathcal{O}$ es orden en A, entonces $\mathcal{O} \cap B$ es orden en B. En particular $Z(\mathcal{O})$ es orden en $Z(A)$.

Demostración. (1) La intersección de subanillos es un subanillo, y la de submódulos es un submódulo. Para ver que es pleno, sea $X = \{v_1, \dots, v_n\}$ una base de A, de forma que por (3.3.4) existen enteros no nulos r_1 y r_2 tales que $r_1 X$ está contenido en $\mathcal{O}_1$ y $r_2 X$ en $\mathcal{O}_2$. Deducimos que $r_1 r_2 X$ está contenido en $\mathcal{O}_1 \cap \mathcal{O}_2$, siendo $r_1 r_2 X$ una base de A.

(2) Es claro que $\mathcal{O} \cap B$ es un subanillo de B. Como B es una subálgebra, es cerrado para el producto por $\mathbb{Q}$, así que también lo es para el producto por $\mathbb{Z}$. Se tiene entonces que $\mathcal{O} \cap B$ es un $\mathbb{Z}$-módulo, y es finitamente generado, porque es un submódulo sobre un DIP del módulo finitamente generado $\mathcal{O}$ [Lan02, Corolario 7.2]. Para ver que es un retículo pleno basta tomar una $\mathbb{Q}$-base $X = \{v_1, \dots, v_m\}$ de B, y un entero no nulo r tal que rX esté contenido en $\mathcal{O}$ por (3.3.4). Se deduce entonces que rX es una base de B contenida en $\mathcal{O} \cap B$.

Como $F \cdot 1_A$ es un subconjunto de $Z(A)$, se cumple que $Z(A)$ es una subálgebra de A. Se tiene además que $Z(\mathcal{O})$ es $\mathcal{O} \cap Z(A)$, pues $\mathcal{O}$ contiene una $\mathbb{Q}$-base de A, y si un elemento conmuta con los de una base de A lo hace con todos los elementos de A. Se desprende entonces la segunda afirmación de la primera. □

Consideremos un cuerpo F, una F-álgebra de dimensión finita B y un B-módulo M de dimensión finita sobre F. Recordemos el F-homomorfismo de álgebras entre B y los F-endomorfismos lineales de M dado por $b \mapsto b_M$. Podemos considerar una F-base de M y las matrices de las aplicaciones b_M en dicha base. Tomando polinomios característicos, trazas y determinantes en dichas matrices obtenemos los conceptos de polinomios característicos, trazas y normas de elementos de B sobre un B-módulo y un cuerpo fijos. Estos se desarrollan en la sección 2.3 de [JR16]. Sin embargo, para el último lema de la subsección solo es necesario el uso de unas pocas propiedades de la aplicación norma, de forma que restringiremos el caso de estudio al mínimo necesario.

Consideremos la aplicación $A \to End_{\mathbb{Q}}(A)$ dada por $a \mapsto a_A$, que cumple $a_A(x) = ax$ para cada $x \in A$. Tomemos además una $\mathbb{Z}$-base $\mathcal{B}$ de $\mathcal{O}$, que es $\mathbb{Q}$-base de A por (3.3.3), y denotemos por $M_{\mathcal{B}}(a)$ a la matriz de a_A en dicha base, que es una matriz con coeficientes en $\mathbb{Q}$. Podemos definir las aplicaciones

$$\begin{aligned} Char : A &\longrightarrow \mathbb{Q}[X] \\ a &\longmapsto Char(a) = \det(x\,\mathrm{Id} - M_{\mathcal{B}}(a)) \end{aligned}$$

y

$$\begin{aligned} N : A &\longrightarrow \mathbb{Q} \\ a &\longmapsto N(a) = \det(M_{\mathcal{B}}(a)) = (-1)^n Char(a)(0). \end{aligned}$$

Observación 3.3.6. 1. Como $(ab)_A = a_A \circ b_A$ para cada par de elementos a y b de A, se tiene que $N(ab) = N(a)N(b)$.

2. $(1_A)_A$ es la identidad, luego $N(1_A) = 1$.
3. $\mathrm{Char}(a)(a) = 0$, pues $a\,\mathrm{Id} - a_A = 0$.
4. Si a y b son elementos de $\mathcal{O}$, entonces $a_A(b) = ab$ también. Como $\mathcal{B}$ es un subconjunto de $\mathcal{O}$, para cada $a \in \mathcal{O}$ y $b \in \mathcal{B}$ se cumple que $a_A(b) \in \mathcal{O}$, y $a_A(b)$ se escribe como combinación $\mathbb{Z}$-lineal de los elementos de $\mathcal{B}$. $M_{\mathcal{B}}(a)$ es entonces una matriz entera, y deducimos que $\mathrm{Char}(a) \in \mathbb{Z}[X]$ y $N(a) \in \mathbb{Z}$ para cada $a \in \mathcal{O}$.

Lema 3.3.7. *Sea $\mathcal{O}$ un orden en A y $a \in \mathcal{O}$:*

1. *$N(a)1_A$ es un elemento de $a\mathcal{O} \cap \mathcal{O}a$.*
2. *$a \in \mathcal{U}(\mathcal{O})$ si y solo si $N(a) = \pm 1$.*
3. *Si $\mathcal{O}'$ es otro orden en A y $a \in \mathcal{O} \cap \mathcal{O}'$, entonces $a \in \mathcal{U}(\mathcal{O})$ si y solo si $a \in \mathcal{U}(\mathcal{O}')$.*
4. *En el caso anterior $\mathcal{U}(\mathcal{O} \cap \mathcal{O}')$ tiene índice finito en $\mathcal{U}(\mathcal{O})$. Es más, si r es un entero no nulo tal que $r\mathcal{O} \subseteq \mathcal{O}'$, entonces $[\mathcal{U}(\mathcal{O}) : \mathcal{U}(\mathcal{O} \cap \mathcal{O}')] \leqslant [\mathcal{O} : r\mathcal{O}]$, siendo este último índice finito.*

Demostración. (1) Pongamos $\mathrm{Char}(a) = \sum_{i=0}^{n} r_i X^i$ con cada r_i entero (3.3.6.(4)). Por (3.3.6.(3)) se tiene que $\mathrm{Char}(a)(a) = 0$. Deducimos que

$$\left(\sum_{i=1}^{n} r_i a^{i-1}\right) \cdot a = a \cdot \left(\sum_{i=1}^{n} r_i a^{i-1}\right) = \pm N(a) 1_A,$$

donde $\sum_{i=1}^{n} r_i a^{i-1}$ es un elemento de $\mathcal{O}$.

(2) Si $ab = 1$ para cierto $b \in \mathcal{O}$, entonces $1 = N(ab) = N(a)N(b)$, donde $N(a)$ y $N(b)$ son enteros por (3.3.6.(4)), luego $N(a) = \pm 1$. Si $N(a) = \pm 1$, por el apartado anterior se cumple que $\pm 1_A \in a\mathcal{O} \cap \mathcal{O}a$, de forma que $a \in \mathcal{U}(\mathcal{O})$.

(3) Es consecuencia directa del apartado anterior.

(4) Por (3.3.5) podemos suponer que $\mathcal{O}'$ está contenido en $\mathcal{O}$. Por (3.3.4) existe un entero no nulo r tal que $r\mathcal{O}$ está contenido en $\mathcal{O}'$. Como $\mathcal{O}$ es finitamente generado como $\mathbb{Z}$-módulo, $\mathcal{O}/r\mathcal{O}$ también. Se tiene además que $\mathcal{O}/r\mathcal{O}$ es de torsión, ya que r lo anula. Aplicando que $\mathbb{Z}$ es un DIP, deducimos que $\mathcal{O}/r\mathcal{O}$ se descompone en suma directa de una cantidad finita de $\mathbb{Z}$-módulos de la forma $\mathbb{Z}/m\mathbb{Z}$ para ciertos enteros m [Lan02, Teorema 7.7]. Cada componente $\mathbb{Z}/m\mathbb{Z}$ es finita, luego $\mathcal{O}/r\mathcal{O}$ es finito.

Dados ahora elementos x e y de $\mathcal{U}(\mathcal{O})$ tales que $x - y \in r\mathcal{O}$, entonces $(x-y)y^{-1} = xy^{-1} - 1_A$ pertenece a $r\mathcal{O}$, y por lo tanto a $\mathcal{O}'$. Como 1_A pertenece a $\mathcal{O}'$ por ser este subanillo de A, deducimos que xy^{-1} pertenece a $\mathcal{O}'$. Es claro que xy^{-1} es también un elemento de $\mathcal{U}(\mathcal{O})$, cuya intersección con $\mathcal{O}'$ es $\mathcal{U}(\mathcal{O}')$ por el apartado anterior. Esto demuestra que $[\mathcal{U}(\mathcal{O}) : \mathcal{U}(\mathcal{O}')]$ es menor o igual que $|\mathcal{O}/r\mathcal{O}|$, cuya finitud ya habíamos demostrado. □

Sea ahora G un grupo finito, y consideremos los anillos de grupo $\mathbb{Z}[G]$ y $\mathbb{Q}[G]$. Es claro que $\mathbb{Z}[G]$ es un orden en $\mathbb{Q}[G]$. Fijamos ahora el conjunto $\mathcal{E}$ de los idempotentes centrales primitivos de $\mathbb{Q}[G]$, entonces

$$\mathbb{Z}[G] \subseteq \bigoplus_{e \in \mathcal{E}} e\mathbb{Z}[G] \subseteq \bigoplus_{e \in \mathcal{E}} e\mathbb{Q}[G] = \mathbb{Q}[G],$$

donde cada $e\mathbb{Z}[G]$ es de hecho un orden en $e\mathbb{Q}[G]$.

Lema 3.3.8. $Z\left(\oplus_{e \in \mathcal{E}} e\mathbb{Z}[G]\right) = \oplus_{e \in \mathcal{E}} Z\left(e\mathbb{Z}[G]\right)$.

Demostración. El contenido de derecha a izquierda se deduce de que por ortogonalidad cada $Z(e\mathbb{Z}[G])$ está contenido en $Z(\oplus_{e\in\mathcal{E}} e\mathbb{Z}[G])$. Dado entonces $x = \sum_{e\in\mathcal{E}} x_e \in Z\left(\oplus_{e\in\mathcal{E}} e\mathbb{Z}[G]\right)$ con cada $x_e \in e\mathbb{Z}[G]$, se cumple que para todo $e \in \mathcal{E}$ y cada $y_e \in e\mathbb{Z}[G]$

$$x_e y_e = x y_e = y_e x = y_e x_e,$$

de modo que $x_e \in Z(e\mathbb{Z}[G])$. □

Observemos que $G \subseteq \mathbb{Z}[G]$, y por lo tanto conmutar con los elementos de $\mathbb{Z}[G]$ implica hacerlo con los de $\mathbb{Q}[G]$. Aplicando el lema anterior y que $\mathbb{Z}[G] \subseteq \oplus_{e\in\mathcal{E}} e\mathbb{Z}[G]$ obtenemos

$$Z(\mathbb{Z}[G]) \subseteq Z(\oplus_{e\in\mathcal{E}} e\mathbb{Z}[G]) = \oplus_{e\in\mathcal{E}} Z(e\mathbb{Z}[G]). \tag{3.5}$$

Lema 3.3.9. *$\mathcal{U}(Z(\mathbb{Z}[G]))$ es un subgrupo de índice finito en $\oplus_{e\in\mathcal{E}}\mathcal{U}(Z(e\mathbb{Z}[G]))$.*

Demostración. Por (3.5) tenemos que $\mathcal{U}(Z(\mathbb{Z}[G]))$ es un subgrupo de

$$\mathcal{U}(\oplus_{e\in\mathcal{E}} Z(e\mathbb{Z}[G])) = \oplus_{e\in\mathcal{E}}\mathcal{U}(Z(e\mathbb{Z}[G])).$$

Además, $\mathbb{Z}[G]$ es un orden en $\mathbb{Q}[G]$, y $e\mathbb{Z}[G]$ también lo es en $e\mathbb{Q}[G]$ para cada $e \in \mathcal{E}$. Deducimos de (3.3.5) que $Z(\mathbb{Z}[G])$ es un orden en $Z(\mathbb{Q}[G])$ y que cada $Z(e\mathbb{Z}[G])$ lo es en $Z(e\mathbb{Q}[G]) = eZ(\mathbb{Q}[G])$. Por esto último se tiene que $\oplus_{e\in\mathcal{E}} Z(e\mathbb{Z}[G])$ es un orden en $\oplus_{e\in\mathcal{E}} eZ(\mathbb{Q}[G]) = Z(\mathbb{Q}[G])$. Aplicando entonces (3.3.7.(4)) resulta que $\mathcal{U}(Z(\mathbb{Z}[G]))$ tiene índice finito en $\mathcal{U}(\oplus_{e\in\mathcal{E}} Z(e\mathbb{Z}[G]))$. □

Fijamos ahora $e \in \mathcal{E}$. Ya hemos visto que $Z(e\mathbb{Z}[G])$ es un orden en $Z(e\mathbb{Q}[G])$. Además, sabemos que $Z(e\mathbb{Q}[G])$ es $\mathbb{Q}$-isomorfo a $\mathbb{Q}(\chi)$ para cada $\chi \in Irr(G)$ tal que $\chi(e) \neq 0$ por (3.2.35). Sea $\chi \in Irr(G)$ con $\chi(e) \neq 0$, y consideremos un $\mathbb{Q}$-isomorfismo $f : Z(e\mathbb{Q}[G]) \to \mathbb{Q}(\chi)$.

Podemos considerar un orden R cualquiera en la $\mathbb{Q}$-álgebra $\mathbb{Q}(\chi)$. En ese caso, f se restringe a un isomorfismo de anillos y de $\mathbb{Z}$-módulos entre $\tilde{R} = f^{-1}[R]$ y R. Se tiene entonces que $\tilde{R}$ es un orden en $Z(e\mathbb{Q}[G])$ y que los grupos de unidades de $\tilde{R}$ y de R son isomorfos.

Por (3.3.5) deducimos que $\mathcal{O} = \tilde{R} \cap Z(e\mathbb{Z}[G])$ es un orden en $Z(e\mathbb{Q}[G])$, y por (3.3.7) se cumple que tanto $[\mathcal{U}(\tilde{R}) : \mathcal{U}(\mathcal{O})]$ como $[\mathcal{U}(Z(e\mathbb{Z}[G])) : \mathcal{U}(\mathcal{O})]$ son finitos. Concluimos que $\mathcal{U}(Z(e\mathbb{Z}[G]))$ es finito si y solo si $\mathcal{U}(\mathcal{O})$ es finito, lo cual equivale a que $\mathcal{U}(\tilde{R})$ lo sea. Como $\mathcal{U}(\tilde{R})$ es isomorfo a $\mathcal{U}(R)$, uno es finito si y solo si el otro lo es. Este desarrollo se puede resumir en el siguiente resultado:

Corolario 3.3.10. *Sea G un grupo finito. Entonces $\mathcal{U}(Z(\mathbb{Z}[G]))$ es finito si y solo si $\mathcal{U}(Z(e\mathbb{Z}[G]))$ lo es para cada idempotente central primitivo e de $\mathbb{Q}[G]$. Además, dado un idempotente central primitivo e de $\mathbb{Q}[G]$, entonces $\mathcal{U}(Z(e\mathbb{Z}[G]))$ es finito si y solo si algún (equivalentemente todo) orden en $\mathbb{Q}(\chi)$ es finito para algún (equivalentemente todo) $\chi \in Irr(G)$ tal que $\chi(e) \neq 0$.*

CAPÍTULO 4

Teorema de las Unidades de Dirichlet

El objetivo de este capítulo es demostrar el teorema que lo titula, pasando por el estudio de Teoría de Números Algebraicos, y en concreto de los siguientes objetos.

Definición 4.0.1. Un cuerpo de números es una extensión de cuerpos sobre los racionales de grado finito.

Como $\mathbb{C}$ es una extensión de $\mathbb{Q}$ algebraicamente cerrada, contiene una copia de toda extensión algebraica de los racionales, de forma que podemos suponer todo cuerpo de números subcuerpo de $\mathbb{C}$.

En este trabajo tan solo se incluyen los resultados necesarios de Teoría de Números Algebraicos para demostrar el Teorema de las Unidades de Dirichlet, el lector puede referirse a [Mar18] para profundizar en el tema. La estructura del capítulo está basada en [dRío21].

Todo anillo en este capítulo es conmutativo.

4.1. Anillos de enteros

4.1.1. Elementos enteros sobre un anillo

Considero en esta subsección una extensión de anillos $A \subseteq B$.

Definición 4.1.1. Dado un elemento b de B, decimos que:

- b es *algebraico* sobre A si b es la raíz de un polinomio no constante con coeficientes en A.
- b es *entero* o *entero algebraico* sobre A si es raíz de un polinomio mónico con coeficientes en A.

Por otro lado, decimos que:

- B es *entero* sobre A si todo elemento de B es entero sobre A.
- A es *íntegramente cerrado* en B si todo elemento de B entero sobre A está en A.

Definición 4.1.2. Un *dominio* D es *normal* si es íntegramente cerrado en su cuerpo de fracciones $Q(D)$.

Proposición 4.1.3. *Todo DFU es normal.*

Demostración. Sea D un DFU con cuerpo de fracciones Q. Consideramos un elemento b de Q entero sobre D. Como D es DFU podemos poner $b = r/s$ con r y s coprimos en D. Por ser b entero existen coeficientes $a_i \in D$ con

$$b^n + a_{n-1}b^{n-1} + \cdots + a_0 = 0.$$

Multiplicando por $s^n \neq 0$ obtenemos

$$0 = r^n + a_{n-1}r^{n-1}s + \cdots + a_1 r s^{n-1} + a_0 s^n,$$

de donde $r^n = -s(a_{n-1}r^{n-1} + \cdots + a_0 s^{n-1})$. Pero entonces $s|r^n$ con r y s coprimos, luego s es unidad y b pertenece a D.

□

Definición 4.1.4. El conjunto de elementos de B que son enteros en A se llama *clausura entera de A en B*, y es un subanillo de B que contiene a A [AM18, Corolario 5.3].

4.1.2. Anillos de enteros

Definición 4.1.5. Un *número algebraico* es un número complejo entero sobre $\mathbb{Q}$. Un *entero algebraico* es un número complejo entero sobre $\mathbb{Z}$.

Definición 4.1.6. El *anillo de enteros de un subcuerpo K de $\mathbb{C}$* es la clausura entera de $\mathbb{Z}$ en K y lo denotamos $\mathbb{A}_K$.

Observación 4.1.7. $\mathbb{A}_K = K \cap \mathbb{A}_{\mathbb{C}}$.

El Teorema de las Unidades de Dirichlet estudia precisamente las unidades de los anillos de enteros de un cuerpo de números en función de los $\mathbb{Q}$-homomorfismos de dicho cuerpo en $\mathbb{C}$. En el contexto de cuerpos de números el término "entero" querrá decir entero sobre $\mathbb{Z}$.

Consideramos en lo que resta de sección un cuerpo de números K, y pongamos $n = [K : \mathbb{Q}]$.

Lema 4.1.8. *Si $\alpha \in K$, entonces existe $c \in \mathbb{Z}^+$ tal que $c\alpha$ es entero.*

Demostración. Sea $\alpha \in K$. Como K es una extensión finita α es algebraico sobre $\mathbb{Q}$, pongamos que $\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_0 = 0$ con los α_i racionales. Tomando c el producto de los denominadores con signo positivo de los a_i se tiene que ca_i está en $\mathbb{Z}$ para cada i y c es un entero positivo. Multiplicando por c^n en la primera igualdad

$$(c\alpha)^n + ca_{n-1}(c\alpha)^{n-1} + \cdots + c^n a_0 = 0,$$

de donde $c\alpha$ es entero. □

Lema 4.1.9. *Un número algebraico es un entero algebraico si y solo si su polinomio mínimo sobre $\mathbb{Q}$ está en $\mathbb{Z}[X]$.*

Demostración. La suficiencia es evidente. Sean pues α entero algebraico y $f \in \mathbb{Z}[X]$ mónico con $f(\alpha) = 0$. Como $\mathbb{Z}[X]$ es DFU puedo descomponer f en irreducibles mónicos. Alguno de ellos debe anularse en α, por lo que puedo suponer que f es irreducible en $\mathbb{Z}[X]$. Por ser f mónico es primitivo e irreducible sobre $\mathbb{Q}$, así que es el polinomio mínimo de α sobre $\mathbb{Q}$ y está en $\mathbb{Z}[X]$. □

Este resultado restringe el valor que puede tomar el polinomio característico, la norma y la traza sobre $\mathbb{Q}$ de un elemento entero:

Corolario 4.1.10. *Si K es un cuerpo de números y $\alpha \in \mathbb{A}_K$ entonces $\chi_{K/\mathbb{Q}}(\alpha) \in \mathbb{Z}[X]$ y $N_{K/\mathbb{Q}}(\alpha), T_{K/\mathbb{Q}}(\alpha) \in \mathbb{Z}$.*

Demostración. Es consecuencia de (2.2.5) y (4.1.9). □

4.1.3. Bases enteras

Definición 4.1.11. Una *base entera* de K es una base de $\mathbb{A}_K$ como $\mathbb{Z}$-módulo, esto es, una lista $\alpha_1, \ldots, \alpha_r$ que cumple $\mathbb{A}_K = \mathbb{Z}\alpha_1 \oplus \ldots \oplus \mathbb{Z}\alpha_r$.

De igual manera que antes el discriminante de elementos enteros está en $\mathbb{Z}$, como demostramos a continuación, y sirve de apoyo para demostrar la existencia de bases enteras.

Lema 4.1.12. *Si $\alpha_1, \ldots, \alpha_n \in \mathbb{A}_K$ entonces $\Delta[\alpha_1, \ldots, \alpha_n] \in \mathbb{Z}$.*

Demostración. Consideramos los $\mathbb{Q}$-monomorfismos $\sigma_1, \ldots, \sigma_n$ de K en $\mathbb{C}$. Como $\alpha_1, \ldots, \alpha_n$ pertenecen a $\mathbb{A}_K$ sus conjugados también, pues si $f = Min_{\mathbb{Q}}(\alpha_j)$ entonces f es un polinomio mónico con coeficientes enteros por (4.1.10), y por lo tanto $0 = \sigma_i(0) = \sigma_i(f(\alpha_j)) = f(\sigma_i(\alpha_j))$. Como $\Delta[\alpha_1, \ldots, \alpha_n] = det(\sigma_i(\alpha_j))^2$ es el resultado de sumas y multiplicaciones de elementos de $\mathbb{A}_K$ se tiene que $\Delta[\alpha_1, \ldots, \alpha_n] \in \mathbb{A}_K$. Por (2.2.7), $\Delta[\alpha_1, \ldots, \alpha_n] \in \mathbb{Q}$, así que $\Delta[\alpha_1, \ldots, \alpha_n] \in \mathbb{Q} \cap \mathbb{A}_K = \mathbb{A}_{\mathbb{Q}} = \mathbb{Z}$, siendo esta última igualdad cierta por ser $\mathbb{Z}$ DFU y (4.1.3). □

Teorema 4.1.13. *Todo cuerpo de números K tiene una base entera y el grupo aditivo de su anillo de enteros es libre de rango $[K : \mathbb{Q}]$.*

Demostración. Por (4.1.8), $\mathbb{A}_K$ contiene una base de K sobre $\mathbb{Q}$, y por (4.1.12) y el buen orden de $\mathbb{N}$ podemos tomarla con discriminante mínimo en valor absoluto. Sea $w_1, \ldots, w_n$ una base en estas condiciones, basta ver que es base entera de K.

Supongamos por reducción al absurdo que $w_1, \ldots, w_n$ no es base entera. Como son linealmente independientes deben no ser conjunto generador, luego existe $w \in \mathbb{A}_K \backslash (\mathbb{Z}w_1 + \ldots + \mathbb{Z}w_n)$. Tomamos $a_1, \ldots, a_n \in \mathbb{Q}$ con $w = a_1w_1 + \ldots + a_nw_n$, de forma que no todos los a_i pueden estar en $\mathbb{Z}$. Podemos suponer sin pérdida de generalidad que $a_1 = a + r$ con $a \in \mathbb{Z}$ y $r \in (0, 1)$. Tomamos $\psi_1 = w - aw_1$ y $\psi_i = w_i$ para $i = 2, \ldots, n$. Es claro que $\{\psi_i\}_{i=1}^n$ sigue siendo una $\mathbb{Q}$-base de K formada por elementos de $\mathbb{A}_K$. El determinante de la matriz de cambio de base es

$$\begin{bmatrix} a_1 - a & a_2 & a_3 & \ldots & a_n \\ 0 & 1 & 0 & \ldots & 0 \\ 0 & 0 & 1 & \ldots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \ldots & 1 \end{bmatrix} = a_1 - a = r.$$

Por (2.2.7) se tiene $\Delta[\phi_1, \ldots, \phi_n] = r^2\Delta[w_1, \ldots w_n] < \Delta[w_1, \ldots, w_n]$, que contradice la elección de w_i. □

Observación 4.1.14.
- Es trivial que un grupo cociente de otro finitamente generado también es finitamente generado.

- Los grupos abelianos son $\mathbb{Z}$-módulos y $\mathbb{Z}$ es un DIP. Aplicando resultados de Teoría de Modulos [Lan02, Teorema 7.1] todo $\mathbb{Z}$-submódulo de un $\mathbb{Z}$-módulo libre de rango m es libre de rango menor o igual que m. Esto se aplica en concreto a los anillos de enteros por el teorema anterior.

Antes de demostrar el último teorema de la sección se requiere de un lema técnico sobre grupos que se usará en varias ocasiones.

Lema 4.1.15. *Sean $x_1, \dots, x_m$ una base de un grupo abeliano libre F, $A = (a_{ij})$ una matriz $m \times m$ entera y G el subgrupo generado por $y_1, \dots, y_m$ con $y_i = \sum_{j=1}^{m} a_{ij} x_j$ para $i = 1, \dots, m$. Entonces G tiene rango m si y solo si $det(A) \neq 0$, y en tal caso $[F : G] = |det(A)|$. En concreto, $\{y_1, \dots, y_m\}$ forma una base de F si y solo si $det(A) = \pm 1$.*

Demostración. [dRSdV06, Capítulo 7, problema 30]. □

Observación 4.1.16.

- El grupo aditivo de K es libre de torsión, ya que K es un dominio de característica 0, y cualquier subgrupo finitamente generado será libre.
- Un subconjunto de K es linealmente independiente sobre $\mathbb{Z}$ si y solo si lo es sobre $\mathbb{Q}$.
- Si G es un subgrupo aditivo finitamente generado de K, por la observación anterior tiene rango menor o igual que n, con rango n si y solo si contiene una $\mathbb{Q}$-base de K. En concreto, está generado por n elementos.

Definición 4.1.17. Dado un subgrupo aditivo G de K generado por $\alpha_1, \dots, \alpha_n$, se define su *discriminante*

$$\Delta[G] = \Delta_{K/\mathbb{Q}}[\alpha_1, \dots, \alpha_n].$$

Si G tiene rango menor que n los α_i son linealmente dependientes y su discriminante es 0 por (2.2.7.(4)). En otro caso, los α_i forman una base de G, y si cogemos dos bases distintas la matriz de cambio de base tiene determinante ± 1 por (4.1.15). Aplicando (2.2.7.(2)) ambas bases tienen el mismo discriminante. Se tiene por lo tanto que la definición anterior es correcta, no depende de los generadores tomados.

Definición 4.1.18. Se define el discriminante de K como $\Delta_K := \Delta[\mathbb{A}_K]$.

Por (4.1.13) K tiene una base entera, luego $\Delta_K = \Delta[\mathbb{A}_K] \neq 0$.

Teorema 4.1.19. *Si G es un subgrupo aditivo de índice finito en $\mathbb{A}_K$ entonces*

$$\Delta[G] = [\mathbb{A}_K : G]^2 \Delta_K.$$

Demostración. (4.1.15) y (2.2.7.(2)). □

4.2. Dominios de Dedekind

En esta sección se introducen y estudian los dominios de Dedekind, que son anillos que en general no admiten una teoría de factorización de elementos por no ser DFUs (aunque sí DFs), pero permiten la factorización única de ideales en producto de ideales primos. Entre estos dominios se encuentran los anillos de enteros de cuerpos de números, cuyas unidades queremos estudiar. Estas factorizaciones, junto con la aplicación norma que se puede definir sobre sus ideales introducida en la siguiente sección, sirven de apoyo en la demostración del Teorema de las Unidades de Dirichlet.

Definición 4.2.1. Un *dominio de Dedekind* es un dominio noetheriano normal tal que todos sus ideales primos no nulos son maximales.

Comenzamos recordando la definición de anillo noetheriano y una propiedad básica. Dado un anillo A, denotaremos por $\mathcal{L}(A)$ al retículo de ideales A.

Definición 4.2.2. Un *anillo* se dice *noetheriano* si cumple una de las siguientes propiedades, que son equivalentes [AM18, p. 80]:

1. Todos los ideales de A son finitamente generados.
2. $\mathcal{L}(A)$ verifica la condición de cadena ascendente (CCA): no hay cadenas de ideales estrictamente ascendentes infinitas.
3. $\mathcal{L}(A)$ verifica la condición maximal: toda familia no vacía de ideales posee elementos maximales.

Teorema 4.2.3. *Todo dominio noetheriano es dominio de factorización.*

Demostración. Supongamos por reducción al absurdo que D es un dominio noetheriano pero no es DF. Consideremos S el conjunto de los elementos que no se factorizan en irreducibles, que suponemos no vacío. Definimos la familia de ideales no vacía $\Omega = \{(s) | s \in S\}$. Por ser D noetheriano Ω tiene un elemento maximal $I = (s)$ para cierto s de S. Como s no se factoriza en irreducibles, en concreto no es nulo, invertible ni irreducible. Debe ponerse entonces como el producto de dos elementos a y b de D no asociados de s, de manera que (s) está contenido estrictamente en (a) y en (b). Por maximalidad de (s) los ideales (a) y (b) no están en Ω, luego a y b no están en S y se factorizan en irreducibles. La concatenación de las factorizaciones de a y b resulta en una factorización de s, lo cual es una contradicción. □

Teorema 4.2.4. *El anillo de enteros de un cuerpo de números es noetheriano (y en particular dominio de factorización).*

Demostración. Por (4.1.13) el grupo aditivo de un anillo de enteros D es libre de rango finito. Cualquier ideal de D es en particular subgrupo aditivo de D, luego es libre de rango finito por (4.1.14). Se tiene pues que cualquier ideal de D es finitamente generado como grupo y en consecuencia como ideal. □

Lema 4.2.5. *Sea D el anillo de enteros de un cuerpo de números K.*

1. *Si I es un ideal no nulo de D, entonces D/I es finito.*
2. *Los ideales primos no nulos de D son maximales.*

Demostración. Sea a un elemento no nulo de I, y pongamos $n = N_{K/\mathbb{Q}}(a)$. Por (4.1.10) n es un entero no nulo. Si escribimos $n = ab$ (a priori en $\mathbb{C}$), se tiene:

- $na^{-1} = b$, y como n y a son elementos de K, también lo es b.
- Si G es el conjunto de los $\mathbb{Q}$-homomorfismos de K en $\mathbb{C}$ y σ_1 es la inclusión, entonces $b = \prod_{\sigma \in G \setminus \{\sigma_1\}} \sigma(a)$. Ya vimos que los conjugados de un elemento entero eran enteros, luego b es producto de enteros y por lo tanto entero.

Se tiene entonces que $b \in D$, luego $a|n$ en D y $nD \subseteq aD \subseteq I$. Por los Teoremas de Isomorfía D/I es un anillo cociente de D/nD. Este último es finitamente generado como grupo abeliano

por (4.1.14), y por (4.1.15) $|D/nD| = n^{[K:\mathbb{Q}]} < \infty$. Se tiene por lo tanto que D/nD es finito, con lo que D/I también.

Para la segunda parte, si I es un ideal primo no nulo de D, entonces D/I es un dominio finito y por lo tanto un cuerpo, luego I es maximal. □

Teorema 4.2.6. *Los anillos de enteros de cuerpos de números son dominios de Dedekind.*

Demostración. Los anillos de enteros se definen como clausuras enteras, de forma que son dominios normales. Basta aplicar entonces (4.2.5) y (4.2.4). □

4.2.1. Factorización de ideales

Definición 4.2.7. Sea D un dominio y K su cuerpo de fracciones. Llamamos *ideal fraccional* de D a un D-submódulo no nulo I de K tal que $cI \subseteq D$ para algún $c \in D\backslash\{0\}$.

Observación 4.2.8. Dados dos ideales fraccionales M y N de un dominio D, el producto dado por

$$MN = \left\{ \sum_{i=1}^{k} m_i n_i | m_i \in M, n_i \in N \right\}$$

es claramente ideal fraccional. Este producto es además conmutativo, asociativo y tiene neutro D. Veremos que todo ideal fraccional no nulo tiene un inverso para este producto si D es un dominio de Dedekind. De esa manera tendremos que el conjunto de ideales fraccionales de un dominio de Dedekind es un grupo abeliano multiplicativo.

Observación 4.2.9. Si I es ideal fraccional de un dominio D y $c \in D\backslash\{0\}$ es tal que $cI \subseteq D$, entonces $J = cI$ es claramente un ideal no nulo de D. El recíproco es también cierto, si J es un ideal no nulo de D y $c \in D\backslash\{0\}$ entonces $c^{-1}J$ es ideal fraccional de D.

Suponemos en lo que resta de sección que D es un dominio de Dedekind.

Lema 4.2.10. *Si A es un anillo noetheriano e I es un ideal no nulo de A, entonces existen ideales primos no nulos $P_1, P_2, \ldots, P_r$ cuyo producto está contenido en I.*

Demostración. Supongamos por reducción al absurdo que no es cierto. La familia de ideales que no cumplen la propiedad del enunciado, a la que denotamos Ω, es entonces no vacía. Por ser A noetheriano existe un elemento maximal I de Ω. Como I no puede ser primo existen a y b elementos de $A\backslash I$ tal que ab pertenece a I. Los ideales $I + (a)$ e $I + (b)$ contienen estrictamente a I, luego por la maximalidad de I se tiene que $I + (a)$ e $I + (b)$ contienen productos de primos no nulos. Ahora bien, $(I + (a))(I + (b))$ está contenido en I, lo que contradice que I no contenga productos de primos no nulos. □

Definición 4.2.11. Dado un dominio de Dedekind D y un ideal fraccional I de D, se define su inverso como

$$I^{-1} = \{x \in K | xI \subseteq D\}.$$

Observación 4.2.12. Sea I un ideal fraccional de D.

1. I^{-1} es claramente un D-submódulo de K, y no es nulo ya que existe $c \in D\backslash\{0\}$ tal que $cI \subseteq D$.
2. $cI^{-1} \subseteq D$ para cada $0 \neq c \in I$, con lo que I^{-1} es ideal fraccional.

3. Tomar inversos invierte la inclusión.

Si I está contenido en D, entonces I es un ideal de D y se tiene:

4. $D \subseteq I^{-1}$, luego $I = ID \subseteq II^{-1} \subseteq D$, donde el último contenido es cierto por la definición de I^{-1}.

5. II^{-1} es cerrado para el producto por elementos de D y para sumas, así que es un ideal de D que contiene a I.

Lema 4.2.13. *Si I es un ideal no nulo y propio de D, entonces $D \subsetneq I^{-1}$.*

Demostración. Tomo un ideal maximal P de D que contiene a I, de forma que $D \subseteq P^{-1} \subseteq I^{-1}$ y basta ver que el primer contenido es estricto. Sea $a \in P \backslash \{0\}$ y r un entero positivo mínimo tal que existen ideales primos no nulos $P_1, \ldots, P_r$ de D con $P_1 \cdots P_r \subseteq (a)$. Como P es primo contiene a algún P_i, y debe ser $P_i = P$ por ser los dos maximales, ya que D es dominio de Dedekind. Podemos suponer sin pérdida de generalidad que $i = 1$.

Se tiene entonces que $P_2 \cdots P_r$ no está contenido en (a), pues r era mínimo, así que existe $b \in P_2 \cdots P_r \backslash (a)$. Ahora bien, $bP \subseteq (a)$, con lo que $ba^{-1}P \subseteq D$ y $ba^{-1} \in P^{-1}$. Como $b \notin (a)$, concluimos que $ba^{-1} \in P^{-1} \backslash D$, como queríamos demostrar. □

Lema 4.2.14. *Si I es un ideal no nulo de D y S es un subconjunto de K con $IS \subseteq I$ entonces $S \subseteq D$.*

Demostración. Como D es noetheriano existen $a_1, \ldots, a_n$ tales que $I = (a_1, \ldots, a_n)$. Fijo $x \in S$. Por hipótesis existen $b_{ij} \in D$ de forma que $xa_i = \sum_{j=1}^{n} b_{ij} a_j$ para cada $i = 1, \ldots, n$. Llamando $B = (b_{ij})$ y $a = \begin{pmatrix} a_1 & \ldots & a_n \end{pmatrix}^T$, podemos escribir las igualdades anteriores en la forma matricial $xa = Ba$, de donde $(x \cdot Id - B)a = 0$ con $a \neq 0$ porque I no es nulo. Debe ser entonces $det(x \cdot Id - B) = 0$, esto es, x es raíz de un polinomio mónico con coeficientes en D, luego x es entero sobre D. Como D es normal, x pertenece a D, como queríamos demostrar. □

Lema 4.2.15. *Si I es un ideal no nulo de D entonces $II^{-1} = D$.*

Demostración. Ya observamos que siempre se tiene $II^{-1} \subseteq D$ (4.2.12), y el caso $I = D$ es obvio.

Supongamos que I maximal de D, y denotémoslo P para remarcarlo. Por (4.2.12) se tiene $P \subseteq PP^{-1} \subseteq D$ con PP^{-1} ideal de D, luego $PP^{-1} = P$ o $PP^{-1} = D$. Por (4.2.13), $D \subsetneq P^{-1}$. Si fuese $P = PP^{-1}$ por (4.2.14) se daría $P^{-1} \subseteq D$, lo que sería una contradicción. Debe ser pues $PP^{-1} = D$.

Veamos el caso general con I propio por reducción al absurdo, suponiendo que algún I cumple $II^{-1} \neq D$. Por ser D noetheriano podemos tomar un ideal maximal I entre los que cumplen $II^{-1} \neq D$. Tomo además un ideal maximal P de D que contiene a I. Multiplicando por I en $D \subseteq P^{-1} \subseteq I^{-1}$ se tiene

$$I \subseteq IP^{-1} \subseteq II^{-1} \subseteq D.$$

De nuevo, por (4.2.13) $D \subsetneq P^{-1}$, y no puede ser $IP^{-1} \subseteq I$ por (4.2.14). Se tiene por lo tanto que $I \subsetneq IP^{-1}$. Es fácil ver que IP^{-1} es también ideal de D, luego por la maximalidad de I se tiene que $(IP^{-1})(IP^{-1})^{-1} = D$. Por la definición de I^{-1} se da entonces que $P^{-1}(IP^{-1})^{-1} \subseteq I^{-1}$. Multiplicando por I

$$D = (IP^{-1})(IP^{-1})^{-1} \subseteq II^{-1} \subseteq D.$$

□

Teorema 4.2.16. *Sea D un dominio de Dedekind.*

1. *Los ideales fraccionales de D (no nulos) forman un grupo abeliano, y en particular el producto de ideales fraccionales es cancelativo.*
2. *Cada ideal no nulo se puede escribir de forma única (salvo el orden) como producto de ideales primos.*

Demostración. Para la primera parte solo resta probar que todo ideal fraccional tiene inverso. Sea $I = c^{-1}J$ un ideal fraccional con $0 \neq c \in D$ y J un ideal no nulo de D. Por (4.2.15) tiene inverso I^{-1}, queda ver que es un ideal fraccional. Es claro que I^{-1} es un D-submódulo del cuerpo de fracciones de D. Además, $I^{-1} = cJ^{-1}$, así que si $0 \neq d \in J$ entonces $dJ^{-1} \subseteq D$ y $dI^{-1} \subseteq D$. Esto demuestra que I^{-1} es un ideal fraccional de D.

Veamos ahora la segunda afirmación. Como D es producto de una cantidad vacía de primos basta demostrarlo para ideales propios. Si no fuese cierto, considero I un ideal maximal entre los contraejemplos, ya que D es noetheriano, y P un ideal maximal que contiene a I. Se tiene entonces

$$I \subsetneq IP^{-1} \subseteq PP^{-1} \subseteq D,$$

donde la primera inclusión es estricta, pues en otro caso $D = I^{-1}I = I^{-1}IP^{-1} = DP^{-1} = P^{-1}$, que contradice (4.2.13). Por maximalidad de I se tiene que $IP^{-1} = P_2 \cdots P_r$ con los P_i primos, luego $I = PP_2 \cdots P_r$. Queda ver solo la unicidad de la factorización.

Supongamos que $P_1 \cdots P_r = Q_1 \cdots Q_s$ con cada factor ideal primo de D. Razonamos por inducción sobre r. En el caso $r = 1$ algún $Q_i \subseteq P_1$ por ser P_1 primo, pero como son maximales se tiene que $Q_i = P_1$. Cancelando por el primer apartado s deber ser 1, ya que en el lado izquierdo de la igualdad queda D. Si suponemos ahora $r > 1$ y la hipótesis de inducción para $r - 1$, se tiene

$$Q_1 \cdots Q_s = P_1 \cdots P_r \subseteq P_1.$$

De nuevo por ser P_1 primo contiene algún Q_i, y por maximalidad de ambos deben ser iguales. Podemos entonces cancelar y aplicar la hipótesis de inducción. □

Estamos en disposición de demostrar el siguiente lema, necesario posteriormente.

Lema 4.2.17. *Si I es un ideal de D entonces existe un ideal no nulo J de D con IJ principal.*

Demostración. Es obvio si $I = 0$. En otro caso, sean $a \in I\backslash\{0\}$ y $J = \{b \in D | bI \subseteq Da\}$. J es un ideal no nulo de D, ya que contiene a a, y cumple $IJ \subseteq Da$. Basta ver que $IJ = Da$, lo cual hacemos por reducción al absurdo.

Supongamos que $IJ \neq Da$ y sea $A = \frac{IJ}{a} = \{x \in D : ax \in IJ\}$. A es claramente ideal de D, y es propio, ya que hemos supuesto que $IJ \subsetneq Da$. Por (4.2.13) tenemos que $D \subsetneq A^{-1}$. Sea $b \in A^{-1}\backslash D$, de modo que $bA \subseteq D$ y $bJI = bIJ = bAa \subseteq Da$. Pero entonces $bJ \subseteq J$ (por definición de J), lo que contradice (4.2.14) porque $b \notin D$. □

Es natural investigar la relación de divisibilidad entre ideales. Un ideal I dividirá a otro J si existe un tercero L con $IL = J$, y se denota $I|J$. Por la propiedad cancelativa el único ideal fraccional L que satisface $IL = J$ es $I^{-1}J$, que siempre es cerrado para suma y producto por D, de modo que $I|J$ si y solo si $I^{-1}J \subseteq D$ (en cuyo caso es ideal de D) si y solo si $J \subseteq I$. En resumen, dados dos ideales I y J de D, se cumple que

$$I|J \text{ si y solo si } J \subseteq I.$$

Observación 4.2.18. Dado un dominio de Dedekind D, se tiene:

1. Todo ideal tiene un número finito de divisores, que son los productos de algunos de sus factores primos.
2. Cada elemento está en un número finito de ideales, pues un elemento $d \in D$ está en un ideal I de D si y solo si $aD \subseteq I$ si y solo si $I|aD$, pero aD tiene un número finito de divisores por la observación anterior.

4.3. Norma de ideales

Pasamos ahora a estudiar la aplicación norma que se puede definir para ideales de anillos de enteros. En esta sección K es un cuerpo de números y $R = \mathbb{A}_K$. Llamaremos primo de K a un ideal maximal de R o, equivalentemente, primo y no nulo, ya que R es un dominio de Dedekind.

Definición 4.3.1. Se define la norma de un ideal I de R como $N(I) = [R : I] = |R/I|$.

Nótese que esta norma es un entero positivo por (4.2.5).

Proposición 4.3.2. *Sea Δ_K el discriminante de K e I un ideal de R. Entonces*

$$N(I) = \left|\frac{\Delta[I]}{\Delta_K}\right|^{\frac{1}{2}}.$$

Demostración. Tiene sentido $\Delta[I]$ porque I es subgrupo aditivo de R, y es directo por (4.1.19). □

Observación 4.3.3. Si m es un entero positivo, $n = [K : \mathbb{Q}]$ y $\alpha_1, \ldots, \alpha_n$ es una base entera de K, es claro que $m\alpha_1, \ldots, m\alpha_n$ genera mR. Por (2.2.7.(4)) se tiene que $\Delta[m\alpha_1, \ldots, m\alpha_n] = m^{2n}\Delta_K$, y aplicando (4.3.2) deducimos que $N(mR) = m^n$.

Proposición 4.3.4. *Si I y J son ideales de R, entonces $N(IJ) = N(I)N(J)$.*

Demostración. Comenzamos suponiendo que J es primo, y lo denotamos por P para remarcarlo. Si demostramos $[R : IP] = [R : I][I : IP]$ e $[I : IP] = [R : P]$ se tendrá $N(IP) = [R : IP] = [R : I][R : P] = N(I)N(P)$, que es lo que queremos ver. La primera es consecuencia de los Teoremas de Isomorfía (nótese que trabajamos con conjuntos finitos):

$$R/I \cong \frac{R/IP}{I/IP}.$$

Por (4.2.16), $IP \subsetneq I$. Veamos que no hay ideales entre IP e I. Supongamos que B es un ideal de R que cumple que $IP \subseteq B \subseteq I$. Se tiene entonces

$$P = I^{-1}IP \subseteq I^{-1}B \subseteq I^{-1}I = R$$

y, como P es ideal maximal, $P = I^{-1}B$ o $I^{-1}B = R$, de donde $B = IP$ o $B = I$.

Considero ahora $a \in I \backslash IP$. Por lo que acabamos de ver $I = IP + (a)$. Definimos $\psi : R \to I/IP$ dada por $x \mapsto ax + IP$, que es un homomorfismo de R-módulos que cumple:

- Es suprayectivo, pues su imagen es $\frac{(a)+IP}{IP} = I/IP$.
- Su núcleo contiene a P pero no es R, pues $\psi(1) = a + IP \neq 0 + IP$.

Como $\ker\psi$ es un ideal de R debe ser $\ker\psi = P$, y los Teoremas de Isomorfía para módulos dan que $R/P \cong I/IP$ y $[R : P] = [I : IP]$.

En el caso general, J se factoriza en primos de forma única $J = P_1 \cdots P_r$ por (4.2.16). Basta proceder por inducción sobre r.

□

Proposición 4.3.5. *Dado un ideal no nulo I de R, se tiene:*

1. *$I = R$ si y solo si $N(I) = 1$.*
2. *Si $N(I)$ es primo entonces I es primo.*
3. *$N(I) \in I$ o, equivalentemente , $I|N(I)R$.*
4. *Si I es primo entonces divide a un único pR con $p \in \mathbb{Z}$ primo, en cuyo caso $N(I) = p^f$ para cierto $f \leqslant [K : \mathbb{Q}]$.*
5. *Dado un número entero positivo m, solo un número finito de ideales tiene norma m.*

Demostración. La afirmación (1) es obvia.

(2) Si I se factoriza como $P_1 \cdots P_r$, entonces $N(I) = N(P_1) \cdots N(P_r)$. Debe ser algún $N(P_i)$ igual a $N(I)$, mientras que el resto serán unos, es decir, $P_j = R$ para $j \neq i$ e $I = P_i$, que es primo.

(3) $N(I) = [R : I] = |R/I|$, luego para cada $x \in R$ se tiene $(N(I)x + I) = N(I)(x + I) = 0 + I$ por el Teorema de Lagrange, de donde $N(I)x \in I$. Haciendo $x = 1$ ya lo tenemos.

(4) Consideramos ψ la composición de la inclusión $\mathbb{Z} \to R$ con la proyección $R \to R/I$. ψ tiene entonces núcleo $n\mathbb{Z} = \mathbb{Z} \cap I$ para cierto $n \in \mathbb{Z}$, así que ψ induce un homomorfismo inyectivo $\mathbb{Z}_n \to R/I$. Como I es primo, $\mathbb{Z}_n$ es dominio y n es primo, que pasamos a denotar p. R/I es entonces un $\mathbb{Z}_p$-espacio vectorial y $N(I) = p^f$ para $f = dim_{\mathbb{Z}_p}(R/I)$. Como $p \in I$, se tiene que I divide a pR.

Supongamos que $I|qR$ para cierto $q \in \mathbb{Z}$ primo, que podemos suponer positivo. Entonces $N(I)|N(qR)$, pero $N(qR) = q^{[K:\mathbb{Q}]}$ por (4.3.3), luego $q = p$ y $f \leqslant [K : \mathbb{Q}]$.

(5) Si I tiene norma m, entonces por (3) se tiene que $I|N(I)R = mR$. Basta aplicar que $N(I)R$ tiene un número finito de divisores por (4.2.18). □

4.4. Índice de ramificación y grado residual

En esta sección considero una extensión E/F de cuerpos de números con anillos de enteros S y R respectivamente. El desarrollo posterior tiene como único propósito demostrar que la norma definida en (4.3.1) coincide en valor absoluto para ideales principales con la norma (para extensiones de cuerpos) del elemento que genera el ideal.

Dado un primo Q de E, $P = Q \cap F = Q \cap R$ es un ideal de F. Se observa:

- Si $ab \in P \subseteq Q$ con $a, b \in R$, entonces a o b están en Q y por lo tanto en P. Además, $0 \neq N(Q) \in Q \cap \mathbb{Z} \subseteq P$, de modo que P es primo de F.
- Se tiene además que SP está contenido en $SQ = Q$, con SP claramente ideal de S. En concreto, Q divide a SP.

Definición 4.4.1. Se llama índice de ramificación de Q sobre F, denotado $e(Q/F)$, al exponente de Q en la factorización de SP como producto de ideales primos de E.

Podemos también considerar la composición ψ de la inclusión $R \hookrightarrow S$ con la proyección canónica $S \to S/Q$, cuyo núcleo es $Q \cap R = P$. ψ induce entonces un monomorfismo $R/P \to S/Q$, que permite ver S/Q como R/P-espacio vectorial, dando lugar a la siguiente definición.

Definición 4.4.2. Se define el grado residual o grado de inercia de Q sobre F a

$$f(Q/F) = [S/Q : R/P].$$

Nótese la igualdad

$$N(Q) = |S/Q| = |R/P|^{f(Q/F)} = N(P)^{f(Q/F)} = N(Q \cap F)^{f(Q/F)}. \tag{4.1}$$

Partimos ahora de un primo P de F cualquiera. Es claro que un ideal de S contiene a P si y solo si contiene a SP o, equivalentemente, divide a SP como ideal. Se tiene entonces que los primos de E que contienen a P son los factores primos de SP, y se llaman primos de E sobre P. Estos son además los primos Q de E que cumplen que $Q \cap F = P$. Si los primos de E sobre P son $Q_1, \dots, Q_k$, de las definiciones se desprende que

$$SP = Q_1^{e(Q_1/F)} \cdots Q_k^{e(Q_k/F)}.$$

Definición 4.4.3. Sean P y Q primos de F y E respectivamente. Decimos que:

- Q es ramificado sobre F si $e(Q/F) > 1$.
- P es ramificado en E o P ramifica en E si algún primo de E sobre P es ramificado sobre F.
- P es inerte en E si SP es un ideal primo de S (su descomposición tiene entonces un solo primo de exponente 1).
- P es totalmente ramificado en E si $SP = Q^{[E:F]}$ para cierto maximal Q de S.
- P escinde completamente en E si SP es un producto de $[E : F]$ primos distintos.

Lema 4.4.4. *Si I es un ideal de R entonces $N(SI) = N(I)^{[E:F]}$.*

Demostración. Por (4.3.4) podemos suponer que I es primo, y lo denotaremos por P en adelante. En ese caso S/SP es un R/P-espacio vectorial, y en cuanto demostremos que $dim_{R/P}(S/SP) = [E : F]$ habremos terminado, pues entonces $N(SP) = |S/SP| = |R/P|^{[E:F]} = N(P)^{[E:F]}$. Pongamos $n = [E : F]$.

Comienzo con el caso $F = \mathbb{Q}$, o sea que $R = \mathbb{Z}$. Como P es primo, $P = p\mathbb{Z}$ con p un número primo. Pero entonces $SP = pS$, y por (4.3.3)

$$N(SP) = N(pS) = p^n = [\mathbb{Z} : p\mathbb{Z}]^n = N(p\mathbb{Z})^n = N(P)^{[E:\mathbb{Q}]}.$$

El caso general lo vemos en dos pasos.

En primer lugar veremos que $n \geqslant dim_{R/P}(S/SP)$. Si no fuese así existirían $s_0, \dots, s_n \in S$ con $\overline{s_0}, \dots, \overline{s_n}$ linealmente independientes sobre R/P, donde $\bar{\cdot}$ representa la clase de equivalencia en el espacio cociente que corresponda.

Como los s_i son linealmente dependientes sobre F lo son sobre R por (4.1.8), por lo que existen $r_i \in R$ tales que $\sum_{i=0}^{n} r_i s_i = 0$ y algún r_i no es nulo. Considero $I = \sum_{i=0}^{n} Rr_i \neq 0$. Por (4.2.17) existe un ideal J de R tal que $IJ = Ra$ para algún $a \in R\backslash\{0\}$. Como P es un ideal maximal y por lo tanto propio de R, debe ser $Ra \neq Pa$ por la unicidad de la factorización de ideales.

Existe entonces $b \in J$ tal que $Ib \nsubseteq Pa$, y en concreto $ba^{-1}I \subseteq R$ pero $ba^{-1}I \nsubseteq P$. Se tiene entonces que cada $r_i' = ba^{-1}r_i$ pertenece a R y cierto r_j' no está en P. Como $\sum_{i=0}^{n} r_i' s_i = 0$ deducimos que $\sum_{i=0}^{n} \overline{r_i'}\overline{s_i} = 0$ con $\overline{r_j'} \neq 0$, contradicción.

Finalmente demostramos que de hecho $n = dim_{R/P}(S/SP)$. Pongamos $m = [F : \mathbb{Q}]$ y $P \cap \mathbb{Z} = p\mathbb{Z}$ con $p \in \mathbb{Z}$ primo positivo. Sean $P_1, \dots, P_r$ los primos de F sobre $p\mathbb{Z}$. Podemos suponer $P_1 = P$. Denotamos $e_i' = e(P_i/\mathbb{Q})$, $f_i' = f(P_i/\mathbb{Q})$ y $n_i = dim_{R/P_i}(S/SP_i)$. Nótese que la desigualdad demostrada en primer lugar implica que $n_i \leqslant n$ para cada i. Se tiene entonces

$$p^m \underbrace{=}_{(4.3.3)} N(Rp) = N(P_1^{e_1'} \cdots P_r^{e_r'}) \underbrace{=}_{(4.3.4)} N(P_1)^{e_1'} \cdots N(P_r)^{e_r'} \underbrace{=}_{\text{(Ecuación 4.1)}} p^{e_1'f_1' + \cdots + e_r'f_r'}$$

Deducimos que $m = \sum_{i=1}^{r} e_i' f_i'$. Ahora bien, es fácil ver que $S = SS = RS$, de forma que

$$pS = pRS = \left(\prod_{i=1}^{r} P_i^{e_i'}\right) S = \left(\prod_{i=1}^{r} P_i^{e_i'} S\right) = \prod_{i=1}^{r} (P_i S)^{e_i'}.$$

De manera análoga a la anterior:

$$p^{nm} \underbrace{=}_{(4.3.3)} N(pS) \underbrace{=}_{(4.3.4)} \prod_{i=1}^{r} N(P_i S)^{e_i'} \underbrace{=}_{(*)} \prod_{i=1}^{r} p^{n_i e_i' f_i'} = p^{\sum_1^r n_i e_i' f_i'},$$

donde $(*)$ se obtiene aplicando el caso $F = \mathbb{Q}$, ya que $n_i f_i' = dim_{R/P_i}(S/SP_i) \cdot [R/P_i : \mathbb{Z}/p\mathbb{Z}] = dim_{\mathbb{Z}/p\mathbb{Z}}(S/SP_i)$. Se deduce entonces que $nm = \sum_{i=1}^{r} n_i e_i' f_i' \leqslant n \sum_{i=1}^{r} e_i' f_i' = nm$. Como $n_i \leqslant n$ para cada i debe ser $n_i = n$ para todo i, y en concreto $n_1 = n$, como queríamos demostrar. □

Llegamos ahora al resultado que buscábamos.

Corolario 4.4.5. *Si R es el anillo de enteros de un cuerpo de números F y $a \in R\backslash\{0\}$ entonces $N(Ra) = |N_{F/\mathbb{Q}}(a)|$.*

Demostración. Por el Teorema del Elemento Primitivo [ACM02, Teorema 8.2.4], $F = \mathbb{Q}(\theta)$ para cierto $\theta \in \mathbb{C}$. Consideremos los homomorfismos $\sigma_1, \dots, \sigma_n$ de F en $\mathbb{C}$, con $n = [F : \mathbb{Q}]$. Sea $E = \mathbb{Q}(\sigma_1(\theta), \dots, \sigma_n(\theta))$, que es el cuerpo de descomposición de $Min_{\mathbb{Q}}(\theta)$ sobre $\mathbb{Q}$. Considero además el anillo de enteros S de E, $m = [E : F]$ y $k = N_{F/\mathbb{Q}}(a)$.

Evidentemente los σ_i tienen imagen contenida en E, los podemos ver como monomorfismos de F en E. Se tiene además que $S = \sigma_i(S)$ para cada i, ya que los homomorfismos conservan elementos enteros, de donde $\sigma_i(Sa) = S\sigma_i(a)\ \forall i = 1, \dots, n$. Cada σ_i induce entonces un isomorfismo $S/Sa \to S/S\sigma_i(a)$ dado por $x + Sa \mapsto \sigma_i(x) + S\sigma_i(a)$, y por lo tanto $N(S\sigma_i(a)) = N(Sa)$. Se tiene pues que

$$|k|^{mn} = N(Sk) = N\left(S\prod_{i=1}^{n}\sigma_i(a)\right) = N\left(\prod_{i=1}^{n} S\sigma_i(a)\right) = \prod_{i=1}^{n} N\left(S\sigma_i(a)\right) = N(Sa)^n = N(Ra)^{nm},$$

donde en la última igualdad se usa (4.4.4) y la primera es cierta por (4.3.3). Por lo tanto, $N(Ra) = |k| = |N_{F/\mathbb{Q}}(a)|$. □

4.5. Retículos, representaciones geométricas y Teorema de las Unidades de Dirichlet

Pasamos ahora a la demostración del Teorema de las Unidades de Dirichlet. Comenzamos introduciendo el concepto de retículo de un $\mathbb{R}$-espacio vectorial. El grupo de las unidades de un anillo de enteros tendrá una componente libre, que determinará su finitud, y que tendrá estructura de retículo, de modo que el estudio de estos nos permite calcular su rango. Se tendrá además que este rango depende de los monomorfismos de la extensión en $\mathbb{C}$, en concreto del número de monomorfismos con imagen real y no real. Salvo otra indicación los contenidos se basan en el capítulo 5 de [dRío21].

4.5.1. Retículos

En esta subsección V es un $\mathbb{R}$-espacio vectorial de dimensión n. En este caso existe un isomorfismo $f : V \to \mathbb{R}^n$ que dota a V de topología euclídea dada por $\|v\|_f = \|f(v)\|$. Esta topología no depende de f, pues si $g : V \to \mathbb{R}^n$ es otro isomorfismo, entonces $h = g \circ f^{-1}$ es un isomorfismo $\mathbb{R}^n \to \mathbb{R}^n$, y $x \mapsto \|h(x)\|$ define una norma en $\mathbb{R}^n$. Como todas las normas en $\mathbb{R}^n$ son equivalentes existen constantes c, C reales tales que $c\|x\| \leqslant \|h(x)\| \leqslant C\|x\|$ para todo $x \in \mathbb{R}^n$, y haciendo $x = f(y)$ se tiene que para cada $y \in V$ se da $c\|f(y)\| \leqslant \|g(y)\| \leqslant C\|f(y)\|$. Nótese también que el concepto de fijar isomorfismo equivale a fijar una base en V y asignar a cada elemento el correspondiente en la base canónica de $\mathbb{R}^n$.

Podemos trasladar el concepto de medibilidad de $\mathbb{R}^n$ a V:

Definición 4.5.1. Un subconjunto $X \subseteq V$ es *medible* si la integral de Riemann $\int_{f(X)} 1dx$ existe, y en ese caso a dicha integral se llama *volumen* de X y se denota por $vol(X)$.

Es claro que el concepto de volumen depende de la base de referencia, pero el de medibilidad no. Si $T : V \to V$ es isomorfismo lineal, por el teorema del cambio de variable se da para cada $X \subseteq V$ medible

$$vol(T(X)) = |\det(T)| vol(X), \tag{4.2}$$

y en particular X es medible si y solo si lo es $T(X)$. Aplicando esto a un cambio de base se obtiene la independencia de la medibilidad respecto a la base escogida.

Definición 4.5.2. Un subconjunto $X \subseteq V$ es *discreto* si $X \cap K$ es finito para cada subconjunto compacto K de V.

Observación 4.5.3. Se puede sustituir la condición de que K sea compacto por la de ser acotado, pues un conjunto es compacto si y solo si es cerrado y acotado en V (es bien conocido en $\mathbb{R}^n$, y se argumenta para V fácilmente usando que f es una isometría con la norma $\|\cdot\|_f$). Si suponemos la definición con compactos y A es un subconjunto acotado de V, entonces su clausura es compacta y la intersección de esta con X finita, luego $A \cap X \subseteq \overline{A} \cap X$, siendo este último finito. La otra implicación es obvia.

En esta sección trabajamos con $\mathbb{Z}$-retículos en $\mathbb{R}$-espacios vectoriales. En otras palabras, un retículo L de rango k en un $\mathbb{R}$-espacio vectorial V será un subgrupo aditivo o $\mathbb{Z}$-submódulo de V generado por k elementos linealmente independientes sobre $\mathbb{R}$, en cuyo caso decimos que dichos elementos forman una base de L

Lema 4.5.4. *Si L es un retículo de V, entonces L es pleno si y solo si existe un subconjunto acotado B de V tal que*

$$V = \cup_{x \in L}(x + B).$$

Demostración. Para la condición necesaria basta tomar $B = \{a_1v_1 + \ldots + a_nv_n | 0 \leqslant a_i \leqslant 1\}$ para una base $\{v_i\}_{=1}^n$ de L. Para la condición suficiente, sean W el subespacio vectorial generado por L y $p : V \to W^\perp$ la proyección ortogonal a lo largo de W. Nótese que $\|p(v)\| \leqslant \|v\|$ para cada $v \in V$. Si B cumple la hipótesis entonces $V = W + B$, y $W^\perp = p(B)$. Como B es acotado $W^\perp$ también, luego $W^\perp = 0$ y $V = W$, esto es, L es pleno. □

Proposición 4.5.5. *Un subgrupo aditivo de V es un retículo si y solo si es discreto.*

Demostración. Si L es un retículo de V, puedo suponer sin pérdida de generalidad que es pleno, ya que si lo amplío y las intersecciones con subconjuntos acotados son finitas, las del original también. Sea entonces $\{v_i\}_1^n$ una $\mathbb{R}$-base de V tal que $L = \mathbb{Z}v_1 \oplus \ldots \oplus \mathbb{Z}v_n$, y sea $K \subseteq V$ acotado. Tomamos $R > 0$ con $K \subseteq \{\sum_{i=1}^n a_iv_i | a_i \in [-R, R]\}$. Todo elemento x de $L \cap K$ es entonces de la forma $\sum_{i=1}^n a_iv_i$ con $a_i \in \mathbb{Z} \cap [-R, R]$, luego $L \cap K$ finito.

Supongamos ahora que L es un subconjunto discreto de V, y procedamos por inducción en $n = \dim V$. El caso $n = 0$ es trivial, así que consideramos $n \geqslant 1$ y la hipótesis de inducción en dimensión menor. Podemos además suponer que L contiene una base de V, ya que en otro caso L está contenido en un subespacio propio W de V, y si K es un subconjunto acotado de W también lo es de V, por hipótesis de inducción L sería un retículo en W y por lo tanto en V. Sea entonces $\{v_i\}_1^n$ una base de V sobre $\mathbb{R}$ contenida en L. Tomamos $W = \mathbb{R}v_1 \oplus \ldots \oplus \mathbb{R}v_{n-1}$ y $L_0 = L \cap W$. Es claro que L_0 es discreto en W y que $v_1, \ldots, v_{n-1}$ pertenecen a L_0, de forma que L_0 es retículo pleno de W por hipótesis de inducción. En concreto, $L_0 = \mathbb{Z}w_1 \oplus \ldots \oplus \mathbb{Z}w_{n-1}$ para cierta base $\{w_i\}_1^{n-1}$ de W. Se tiene también que $w_1, \ldots, w_{n-1}, v_n$ es base de V, y considero

$$K = \left\{ \sum_{i=1}^{n-1} a_iw_i + a_nv_n | 0 \leqslant a_1, ..., a_{n-1} < 1; 0 \leqslant a_n \leqslant 1 \right\}.$$

Como K es un subconjunto acotado de V y v_n pertenece a $(K \cap L)\backslash W$, $(K \cap L)\backslash W$ es un conjunto finito y no vacio. Podemos tomar $\varepsilon \geqslant 0$ mínimo tal que algún $x_0 = a_1w_1 + \ldots + a_{n-1}w_{n-1} + \varepsilon v_n$ pertenezca a $(K \cap L)\backslash W$ para ciertos $a_1, \ldots, a_{n-1}$ en $[0, 1)$. Es necesario también que ε sea positivo, pues $x_0 \notin W$. Sea entonces $L_1 = \mathbb{Z}w_1 + \ldots + \mathbb{Z}w_{n-1} + \mathbb{Z}x_0$, que es un retículo de V contenido en L. Basta ver que L está contenido en L_1. Sea $x = b_1w_1 + \ldots + b_{n-1}w_{n-1} + b_nv_n$ un elemento arbitrario de L con los b_i reales. Ponemos $b_n = m_n\varepsilon + c_n$ con $0 \leqslant c_n < \varepsilon$ y $m_n \in \mathbb{Z}$, y también $b_i - m_na_i = m_i + c_i$ con $c_i \in [0, 1)$ y $m_i \in \mathbb{Z}$ para cada $i = 1, \ldots, n-1$. Consideramos el elemento de L_1

$$\begin{aligned} y &= m_1w_1 + \ldots + m_{n-1}w_{n-1} + m_nx_0 \\ &= (m_1 + m_na_1)w_1 + \ldots + (m_{n-1} + m_na_{n-1})w_{n-1} + m_n\varepsilon v_n \\ &= x - (c_1w_1 + \ldots + c_{n-1}w_{n-1} + c_nw_n). \end{aligned}$$

En concreto $x - y = \sum_{i=1}^{n-1} c_i w_i + c_n v_n$ pertenece a $L \cap K$. Como $0 \leqslant c_n < \varepsilon$, si $x - y$ no estuviese en W se tendría que c_n está en $(0, \varepsilon)$ y $x - y$ en $(K \cap L) \backslash W$, contradiciendo la minimalidad de ε. Se tiene entonces que $x - y$ es un elemento de $L \cap W = L_0 \subseteq L_1$, y $x \in L_1$, como queríamos ver. □

Definición 4.5.6. Sean L un retículo pleno de V y $B = \{v_1, \ldots, v_n\}$ una base de L, de manera que B es una $\mathbb{R}$-base de V. Llamamos *poliedro fundamental* o *dominio fundamental* de B a

$$P_B = \left\{ \sum_{i=1}^{n} x_i v_i | 0 \leqslant x_i < 1 \right\}.$$

Observación 4.5.7. $V = \dot{\cup}_{a \in L} a + P_B$.

Lema 4.5.8. *Todos los poliedros fundamentales de un retículo pleno tienen el mismo volumen.*

Demostración. Sean $B_1 = \{v_i\}_1^n$ y $B_2 = \{w_i\}_1^n$ bases de L en V. Sea $f : V \to V$ un isomorfismo lineal que asocia $v_i \mapsto w_i$. Como $\mathbb{Z}v_1 + \ldots + \mathbb{Z}v_n = \mathbb{Z}w_1 + \ldots + \mathbb{Z}w_n$ la matriz A de f sobre B_1 tiene entradas enteras, y su inversa también. Esto implica que $\det(f) = \det(A) = \pm 1$. Es obvio que $f(P_{B_1}) = P_{B_2}$, luego por la Ecuación 4.2 se tiene que $vol(P_{B_2}) = |\det(f)| vol(P_{B_1}) = vol(P_{B_1})$. □

Podemos definir entonces el siguiente concepto.

Definición 4.5.9. Dado un retículo L en V se llama covolumen de L en V a

$$vol(V/L) = \begin{cases} vol(P_B), & \text{si } L \text{ es pleno en } V \text{ y } B \text{ es una base de } L; \\ \infty, & \text{si } L \text{ no es pleno en } V. \end{cases}$$

Lema 4.5.10. *Sea L un retículo pleno en V con base $B = \{v_1, \ldots, v_n\}$. Sean $w_1, \ldots, w_n \in L$ y pongamos $w_i = \sum_{j=1}^{n} a_{ij} v_j$ con los $a_{ij} \in \mathbb{Z}$. Entonces $M = \mathbb{Z}w_1 + \ldots + \mathbb{Z}w_n$ es un retículo en V.*

Es más, M es pleno si y solo si $\det((a_{ij})) \neq 0$ si y solo si M tiene índice finito en L. En ese caso se tiene que

$$[L : M] = |\det((a_{ij}))| = \frac{vol(V/M)}{vol(V/L)}.$$

Demostración. Como M es un subconjunto de L y este es discreto, es claro que M también lo es, luego también es un retículo.

M será pleno si y solo si $V = span\{w_1, \ldots, w_n\}$, lo cual equivale a que $\det((a_{ij}))$ no sea nulo. La segunda equivalencia es consecuencia directa de (4.1.15), al igual que la igualdad $[L : M] = |\det((a_{ij}))|$. Sea f el automorfismo de V que asocia v_i con w_i para cada $i = 1, \ldots, n$, de forma que $f(P_B) = P_{B'}$ para $B' = \{w_1, \ldots, w_n\}$. La matriz de f sobre B es precisamente (a_{ij}), de donde

$$vol(V/M) = vol(P_{B'}) = |\det((a_{ij}))| vol(P_B) = |\det((a_{ij}))| vol(V/L).$$

□

El siguiente teorema es el resultado principal sobre retículos que aplicaremos en la demostración final.

Teorema 4.5.11 (Minkowski)**.** *Sean V un espacio vectorial sobre $\mathbb{R}$ de dimensión n y L un retículo pleno en V. Sea X un subconjunto acotado y medible de V que cumple*

1. $vol(X) > 2^n vol(V/L)$;

2. *si* $x, y \in X$ *entonces* $\frac{x-y}{2} \in X$.

Entonces $X \cap L$ *contiene un elemento no nulo. Si* X *es cerrado se puede sustituir la desigualdad estricta en (1) por una no estricta.*

Demostración. Fijamos $B = \{v_1, \dots, v_n\}$ de L, de forma que $2B = \{2v_1, \dots, 2v_n\}$ es una base de $2L$. Sea P_{2B} el poliedro fundamental de $2B$. Por la primera hipótesis y (4.5.10) se tiene que $vol(P_{2B}) = vol(V/2L) = 2^n vol(V/L) < vol(X)$. Cada elemento de V tiene una única expresión como $x + y$ con $x \in 2L$ e $y \in P_{2B}$, así que podemos considerar la aplicación $f : V \to V$ que a cada elemento x de V le asigna el único $f(x) \in P_{2B}$ con $x - f(x) \in 2L$. Para cada $a \in 2L$ y $x \in a + P_{2B}$ se tiene que $f(x) = x - a$, es decir, f restringida a los conjuntos de la forma $a + P_B$ es una traslación, y como estas conservan el volumen, para cualquier subconjunto medible Y de $a + P_{2B}$ se cumple $vol(f(Y)) = vol(Y)$.

Como X es acotado, existen $a_1, \dots, a_k \in 2L$ tales que $X \subseteq \dot\cup_1^k (a_i + P_{2B})$, luego $X = X \cap \dot\cup_1^k (a_i + P_{2B})$ y por lo tanto

$$vol(P_{2B}) < vol(X) = \sum_1^k vol(X \cap (a_i + P_{2B})) = \sum_1^k vol(f(X \cap (a_i + P_{2B}))).$$

Pero cada $f(X \cap (a_i + P_{2B}))$ está contenido en P_{2B}, luego la desigualdad anterior implica que k es mayor que 1 y que los $f(X \cap (a_i + P_{2B}))$ no son disjuntos dos a dos. Se tiene por lo tanto que f no es inyectiva en X, y puedo tomar elementos distintos x e y de X con $f(x) = f(y)$. Se cumple entonces que $x - y = (x - f(x)) + (f(y) - y)$ es un elemento de $2L$. Por la segunda hipótesis $0 \neq \frac{x-y}{2} \in X \cap L$.

Para la última afirmación, dado $\varepsilon > 1$ se tiene que $vol(\varepsilon X) > vol(X)$, y por lo que hemos demostrado existe $x_\varepsilon \in (\varepsilon X) \cap L$ no nulo. Sea $r > 0$ tal que X está contenido en $B(0, r)$. Como L es discreto $B(0, 2r) \cap L$ es finito, pongamos $B(0, 2r) \cap L = \{0, a_1, \dots, a_k\}$. Supongamos por reducción al absurdo que $X \cap L$ no tiene elementos no nulos. En ese caso a_i no puede pertenecer a X, que es cerrado, luego existe $r_i > 0$ tal que $B(a_i, r_i) \cap X = \varnothing$. Poniendo $\varepsilon_i = 1 + \frac{r_i}{\|a_i\|}$ se tiene que a_i no está en εX para cada $\varepsilon \in (1, \varepsilon_i)$. Basta tomar ε mayor que 1 y menor que 2 y que cada ε_i, en cuyo caso se da $\varepsilon X \cap L \subseteq \{0\}$, que es una contradicción. □

4.5.2. Representación geométrica de números algebraicos

Considero en lo que queda de sección un cuerpo de números K con $[K : \mathbb{Q}] = n$ y anillo de enteros R. Dado un homomorfismo $\sigma : K \to \mathbb{C}$, decimos que es real si $\sigma(K) \subseteq \mathbb{R}$, y en caso contrario que es complejo. La composición de σ con la conjugación define otro homomorfismo $\overline{\sigma} : K \to \mathbb{C}$ dado por $\overline{\sigma}(x) = \overline{\sigma(x)}$. Si σ es complejo su conjugado es distinto, por lo que los n $\mathbb{Q}$-isomorfismos de K en $\mathbb{C}$ vienen divididos en reales y pares de conjugados, digamos r reales y $2s$ complejos, de manera que $n = r + 2s$. En el desarrollo posterior los ordenamos

$$\sigma_1, \dots, \sigma_r, \sigma_{r+1}, \overline{\sigma_{r+1}}, \dots, \sigma_{r+s}, \overline{\sigma_{r+s}},$$

con los primeros r reales y el resto complejos. Denotamos $\mathbb{L}^{r,s}$ a $\mathbb{R}^r \times \mathbb{C}^s$, que es una $\mathbb{R}$-álgebra de dimensión $r + 2s = n$. En dicho espacio se define la siguiente aplicación norma:

$$N(x_1, \dots, x_{r+s}) = x_1 \cdots x_r |x_{r+1}|^2 \cdots |x_{r+s}|^2,$$

claramente real y multiplicativa.

Tomamos la base de referencia $e_1, \dots, e_r, e_{r+1}, ie_{r+1}, \dots, e_{r+s}, ie_{r+s}$, y consideramos la aplicación

$$\begin{aligned} \sigma : K &\longrightarrow \mathbb{L}^{r,s} \\ x &\longmapsto \sigma(x) = (\sigma_1(x), \dots, \sigma_{r+s}(x)), \end{aligned}$$

que es un homomorfismo de $\mathbb{Q}$-álgebras. Es clara la igualdad

$$N(\sigma(x)) = N_{K/\mathbb{Q}}(x). \tag{4.3}$$

Como cada σ_i es inyectivo también lo es σ, así que es un monomorfismo de $\mathbb{Q}$-espacios vectoriales. Por lo tanto, si $\{\alpha_1, \dots, \alpha_n\}$ es una $\mathbb{Q}$-base de K entonces $\sigma(\alpha_1), \dots, \sigma(\alpha_n)$ son $\mathbb{Q}$-linealmente independientes. La matriz de coordenadas de esos vectores sobre la base de referencia debe tener determinante no nulo, con lo que también son $\mathbb{R}$-linealmente independientes. Es claro que $\sigma(R)$ es un retículo de $\mathbb{L}^{r,s}$, y el argumento anterior demuestra que es pleno. Como se enuncia en el siguiente resultado, eso es cierto para todo ideal no nulo de R.

Proposición 4.5.12. *Si I es un ideal no nulo de R entonces $\sigma(I)$ es un retículo pleno de $\mathbb{L}^{r,s}$, y además $vol(\mathbb{L}^{r,s}/\sigma(I)) = \frac{\sqrt{|\Delta_K|}N(I)}{2^s}$.*

Demostración. Los ideales de R son finitamente generados como subgrupos aditivos por (4.1.14), luego $\sigma(I)$ es un retículo para cada ideal I de R. Además, $\sigma : R \to \sigma(R)$ es un isomorfismo de grupos, luego $[\sigma(R) : \sigma(I)] = [R : I] < \infty$ por (4.2.5). Aplicando (4.5.10) se tiene que $\sigma(I)$ es un retículo pleno de $\mathbb{L}^{r,s}$ y $vol(\mathbb{L}^{r,s}/\sigma(I)) = N(I)vol(\mathbb{L}^{r,s}/\sigma(R))$. Basta entonces comprobar la fórmula para $I = R$. Sea $\alpha_1, \dots, \alpha_n$ una base entera de K, y pongamos

$$\sigma(\alpha_i) = (x_{i,1}, \dots, x_{i,r}, y_{i,1} + iz_{i,1}, \dots, y_{i,s} + iz_{i,s})$$

con los $x_{i,k}, y_{i,k}, z_{i,k}$ reales. Considero además para $k = 1, \dots, r$ y $j = 1, \dots, s$

$$X_k = \begin{pmatrix} x_{k,1} \\ \vdots \\ x_{k,n} \end{pmatrix}, Y_j = \begin{pmatrix} y_{j,1} \\ \vdots \\ y_{j,n} \end{pmatrix}, Z_j = \begin{pmatrix} z_{j,1} \\ \vdots \\ z_{j,n} \end{pmatrix}, v_j = Y_j + iZ_j, \overline{v_j} = Y_j - iZ_j.$$

Integrando se comprueba que el volumen del poliedro del retículo generado por la base de referencia es 1, luego por (4.5.10) se cumple que $vol(\mathbb{L}^{r,s}/\sigma(R))$ es el valor absoluto de $D = \det(X_1, \dots, X_r, Y_1, Z_1, \dots, Y_s, Z_s)$. Por otra parte,

$$\begin{aligned} \Delta_K = \Delta[\alpha_1, \dots, a_n] &= \det(X_1, \dots, X_r, v_1, \overline{v_1}, \dots, v_s, \overline{v_s})^2 = \det(X_1, \dots, X_r, v_1, 2Y_1, \dots, v_s, 2Y_s)^2 \\ &= 2^{2s} \det(X_1, \dots, X_r, v_1, Y_1, \dots, v_s, Y_s)^2 = 2^{2s} \det(X_1, \dots, X_r, iZ_1, Y_1, \dots, iZ_s, Y_s)^2 = \pm 2^{2s} D^2, \end{aligned} \tag{4.4}$$

de donde $2^s vol(\mathbb{L}^{r,s}/\sigma(R)) = 2^s|D| = \sqrt{|\Delta(K)|}$. □

4.5.3. Espacio logarítmico

Manteniendo el contexto y notación introducidos en la subsección anterior, denotamos $U^{r,s}$ al grupo de las unidades de $\mathbb{L}^{r,s}$, esto es,

$$U^{r,s} = \{x = (x_1, \dots, x_{r+s}) \in \mathbb{R}^r \times \mathbb{C}^s | x_i \neq 0 \ \forall i = 1, \dots, r+s\}.$$

Definimos también la aplicación

$$\begin{aligned} l : U^{r,s} &\longrightarrow \mathbb{R}^{r+s} \\ x &\longmapsto l(x) = (l_1(x), \dots, l_{r+s}(x)), \end{aligned}$$

con $l_k(x) = \begin{cases} \log|x_k| & \text{si } k \leqslant r; \\ \log|x_k|^2 & \text{si } k > r. \end{cases}$

Por las propiedades del logaritmo $l(xy) = l(x) + l(y)$, i.e. l es un homomorfismo de $U^{r,s}$ al grupo aditivo de $\mathbb{R}^{r+s}$. Se tiene también por la definición de norma que $\log|N(x)| = \sum_{i=1}^{r+s} l_i(x_i)$ para cada $x \in U^{r,s}$. Recordemos además que $\sigma : K \to \mathbb{L}^{r,s}$ era un monomorfismo de $\mathbb{Q}$-álgebras, y por lo tanto se restringe a un monomorfismo de grupos $\sigma : K^* \to U^{r,s}$ que compuesto con l nos da un homomorfismo $K^* \to \mathbb{R}^{r+s}$ al que también denotaremos l. En concreto, para cada $\alpha \in K^*$

$$l(\alpha) = l(\sigma(\alpha)) \text{ y } l_k(\alpha) = l_k(\sigma(\alpha)).$$

Llamamos a $\mathbb{R}^{r+s}$ espacio logarítmico, y a $l : K^* \to \mathbb{R}^{r+s}$ la representación logarítmica de K. Consideramos ahora el anillo de enteros R de K, y denotamos por U al grupo de unidades de R. El objetivo es usar la restricción de l a U para describir la estructura de U.

Lema 4.5.13. *$l(U)$ es un retículo dentro del hiperplano $\pi = \{x \in \mathbb{R}^{r+s} | x_1 + \dots x_{r+s} = 0\}$.*

Demostración. Sea $u \in U$. De la Ecuación 4.3 y de (4.1.10) deducimos que $N(u) \in \mathbb{Z}$, luego $N(u) = \pm 1$. Por lo tanto, $\sum_{i=1}^{r+s} l_i(u) = \log|N(u)| = \log 1 = 0$, esto es, $l(U) \subseteq \pi$. Veamos que $l(U)$ es discreto y por lo tanto un retículo. Sean $C > 0$ y $u \in U$ con $l(u) \in B(0, C)$. Entonces $|l_k(u)| \leqslant \|l(u)\| < C$ para cada k, lo que equivale a que

$$\begin{aligned} |\sigma_k(u)| &< e^C \text{ si } k \leqslant r \\ |\sigma_k(u)|^2 &< e^C \text{ si } k > r. \end{aligned}$$

Se tiene entonces que $\|\sigma(u)\| < e^C\sqrt{r+s}$, con lo que $X = l^{-1}(l(U) \cap B(0, C))$ es un subconjunto acotado de $\sigma(R)$, que es un retículo de $\mathbb{L}^{r,s}$. X es por lo tanto finito, y $l(U) \cap B(0, C)$ también debido a que l es sobreyectiva de X en $l(U) \cap B(0, C)$. □

Lema 4.5.14. *Sea $P \in \mathbb{Z}[X]$ mónico cuyas raíces tienen módulo 1. Entonces cada raíz de P es raíz de la unidad.*

Demostración. Puedo suponer sin pérdida de generalidad que P es irreducible sobre $\mathbb{Q}$ (lo que equivale a serlo sobre $\mathbb{Z}$, por ser mónico), pues $\mathbb{Q}[X]$ es un DFU y las raíces de P se reparten entre los factores irreducibles de P.

Pongamos entonces $P = \prod_{i=1}^{k}(X - \alpha_i)$, donde los α_i son distintos dos a dos por ser $\mathbb{Q}$ de característica 0 y por lo tanto P separable (2.2.3) . Sea además $F = \mathbb{Q}(\alpha_1, \dots, \alpha_k)$ el cuerpo de descomposición de P sobre $\mathbb{Q}$ y R el anillo de enteros de F. Se tiene entonces que $F/\mathbb{Q}$ es una

extensión de Galois [ACM02, Corolario 7.14 + Proposición 8.1.1]. Consideramos los polinomios simétricos elementales en k variables $S_1, \dots, S_k$. Dado $m \in \mathbb{Z}$ positivo, sea $a_i = S_i(\alpha_1^m, \dots, \alpha_k^m)$ para $i = 1, \dots, k$, y sea

$$P_m = \prod_{i=1}^{k}(X - \alpha_i^m) = X^k + \sum_{i=1}^{k}(-1)^i a_i X^i \in F[X].$$

Como cada $\sigma \in Gal(F/\mathbb{Q})$ permuta los α_i y estos son distintos dos a dos, $\hat{\sigma}(P_m) = P_m$ para cada m, donde $\hat{\sigma}$ es la extensión natural de σ a un automorfismo de $F[X]$ que fija X. Cada a_i debe pertenecer a $\mathbb{Q}$ por ser $F/\mathbb{Q}$ de Galois, y cada a_i debe ser también entero, ya que es el resultado de productos y sumas de los α_i, que son enteros. Se tiene por lo tanto que a_i está en $\mathbb{Z}$ para cada i. Como S_i es suma de $\binom{k}{i}$ monomios de coeficiente 1 y cada α_i tiene norma 1, por la desigualdad triangular se cumple que $|a_i| \leqslant \binom{k}{i}$ para cada i. De estos dos argumentos se deduce que los a_i pueden tomar una cantidad finita de valores, y por lo tanto solo hay una cantidad finita de polinomios P_m. Existen entonces enteros distintos m_1 y m_2 con $P_{m_1} = P_{m_2}$, y en concreto con las mismas raíces. Tomamos una permutación ρ de $\{1, \dots, k\}$ tal que $\alpha_i^{m_1} = \alpha_{\rho(i)}^{m_2}$.

Veamos por inducción sobre r que $\alpha_i^{m_1^r} = \alpha_{\rho^r(i)}^{m_2^r}$ para cada i, de forma que como $\rho^r = Id$ para cierto r resulta $\alpha_i^{m_1^r} = \alpha_i^{m_2^r}$, i.e. $\alpha_i^{m_1^r - m_2^r} = 1$ y α_i es raíz de la unidad. El caso $r = 1$ es la última observación del párrafo anterior, y si $r > 1$:

$$\alpha_i^{m_1^r} = \left(\alpha_i^{m_1^{r-1}}\right)^{m_1} = \left(\alpha_{\rho^{r-1}(i)}^{m_2^{r-1}}\right)^{m_1} = \left(\alpha_{\rho^{r-1}(i)}^{m_1}\right)^{m_2^{r-1}} = \left(\alpha_{\rho^r(i)}^{m_2}\right)^{m_2^{r-1}} = \alpha_{\rho^r(i)}^{m_2^r},$$

donde aplicamos la hipótesis de inducción en la segunda y cuarta igualdad. □

Lema 4.5.15. *El núcleo W de $l : U \to \mathbb{R}^{s+t}$ es el conjunto de las raíces de la unidad de K. Además, W es un grupo cíclico finito de orden par.*

Demostración. Si α es una raíz de la unidad en K, se verifica que α pertenece a U y que $l(u) = 0$, pues $|\sigma(u)| = 1$ para todo monomorfismo de K en $\mathbb{C}$. Recíprocamente, si $\alpha \in W$ entonces $|\sigma_i(\alpha)| = 1$ para cada i. Como los $\sigma_i(\alpha)$ son las raíces de $Min_{\mathbb{Q}}(\alpha)$, aplicando (4.5.15) se tiene que todos son raíces de la unidad, y en particular lo es α.

Respecto a la última afirmación, por (4.5.12) $\sigma(R)$ es un retículo en $\mathbb{L}^{r,s}$, luego es discreto. Las componentes de un elemento de $\sigma(W)$ tienen norma 1, de manera que $\sigma(W)$ es un conjunto acotado. Como $\sigma(W)$ está además contenido en $\sigma(R)$, $\sigma(W)$ es finito, y de la inyectividad de σ se deduce que W también lo es. Es bien conocido que todo subgrupo finito del grupo de unidades de un cuerpo es cíclico, y como $-1 \in W$ es de orden 2 el orden de W es par. □

4.5.4. Teorema de las Unidades de Dirichlet

Por el Lema 4.5.15, el núcleo W de $l : U \to \mathbb{R}^{s+t}$ es finito. Además, $l(U)$ es un retículo en π (4.5.13), luego es un grupo abeliano libre de torsión finitamente generado. Como U/W es isomorfo a $l(U)$ y W es finito deducimos que U es también finitamente generado, ya que es el producto directo de un grupo abeliano finito y un grupo abeliano libre de rango $\leqslant r + s - 1 = \dim_{\mathbb{R}}(\pi)$. El Teorema de Dirichlet asegura la igualdad, es decir, que $l(U)$ es un retículo pleno de π.

Para cada $y \in \mathbb{L}^{r,s}$ consideramos la aplicación lineal $\lambda_y : \mathbb{L}^{r,s} \to \mathbb{L}^{r,s}$ dada por $\lambda_y(x) = yx$.

Lema 4.5.16. $\det(\lambda_y) = N(y)$.

Demostración. Si $y = (x_1, \dots, x_r, y_1 + iz_1, \dots, y_s + iz_s)$, entonces la matriz asociada a λ_y en la base de referencia es

$$diag\left(x_1, \dots, x_s, \begin{pmatrix} y_1 & -z_1 \\ z_1 & y_1 \end{pmatrix}, \dots, \begin{pmatrix} y_s & -z_s \\ z_s & y_s \end{pmatrix}\right),$$

con determinante claramente $N(y)$. □

Lema 4.5.17. *Sea M un retículo pleno de $\mathbb{L}^{r,s}$, que tiene dimensión $r+2s$, y sean $c_1, \dots, c_{r+s} > 0$ con*

$$c_1 \dots c_{r+s} \geqslant \left(\frac{4}{\pi}\right)^s vol(\mathbb{L}^{r,s}/M).$$

Entonces existe $x = (x_1, \dots, x_{r+s}) \in M \backslash \{0\}$ tal que

$$\begin{cases} |x_i| \leqslant c_i & si\ i \leqslant r; \\ |x_i|^2 \leqslant c_i & si\ i > r. \end{cases} \tag{4.5}$$

Demostración. Considero el conjunto X de los puntos de $\mathbb{L}^{r,s}$ que satisfacen la Ecuación 4.5. X es claramente compacto y satisface las hipótesis del Teorema de Minkowski (4.5.11) en el caso de un cerrado, la segunda trivialmente y la primera por lo siguiente:

$$\begin{aligned} vol(X) &= \int_{-c_1}^{c_1} dx_1 \dots \int_{-c_r}^{c_r} dx_r \int\int_{y_1^2+z_1^2<c_{r+1}} dy_1 dz_1 \dots \int\int_{y_s^2+z_s^2<c_{r+s}} dy_s dz_s \\ &= 2c_1 \dots 2c_r \cdot \pi c_{r+1} \dots \pi c_{r+s} = 2^r \pi^s c_1 \dots c_{r+s} \geqslant 2^{r+2s} vol(\mathbb{L}^{r+s}/M), \end{aligned}$$

usando en la última desigualdad la hipótesis sobre el producto de los c_i. Basta aplicar entonces el Teorema de Minkowski. □

Proposición 4.5.18. *La imagen $l(U)$ de U por la aplicación logarítmica l es un retículo de dimensión $r+s-1$.*

Demostración. Ya hemos visto que $l(U)$ es retículo del hiperplano π de dimensión $r+s-1$, basta ver que es pleno. Para ello usaré (4.5.4). Considero $S = l^{-1}(\pi) = \{x \in \mathbb{L}^{r,s} | \, |N(x)| = 1\}$. Como l transforma conjuntos acotados en conjuntos acotados, basta encontrar $C \subseteq \mathbb{L}^{r,s}$ acotado con

$$S = \bigcup_{u \in U} \sigma(u) C,$$

pues entonces $\pi = l(l^{-1}(\pi)) = l(S) = \bigcup_{u \in U}(l(u) + l(C))$.

Pongamos $M = \sigma(R)$ y sean $c_1, \dots, c_{r+s} > 0$ reales con

$$Q = c_1 \dots c_{r+s} > \left(\frac{4}{\pi}\right)^s vol(\mathbb{L}^{r,s}/M).$$

Sea además

$$X = \left\{ (x_1, \dots, x_{r+s}) \in \mathbb{L}^{r,s} | \ \begin{matrix} |x_i| \leqslant c_i & \text{si } i \leqslant r; \\ |x_i|^2 \leqslant c_i & \text{si } i > r \end{matrix} \right\}.$$

Por (4.3.5.(5)), solo un número finito de ideales tiene norma menor que Q. Por (4.4.5) existen $\alpha_1, \ldots, \alpha_k \in R\backslash\{0\}$ tales que todo elemento de R con norma en valor absoluto menor o igual que Q es asociado de algún α_i en R. Definimos

$$C = S \cap \left(\bigcup_{i=1}^{k} \sigma(\alpha_i^{-1}) X \right).$$

Como X es acotado también lo es C. Nótese que $l \circ \sigma(U)$ está contenido en π, luego $\sigma(U)$ está contenido en $S = l^{-1}(\pi)$. Se tiene también que C es un subconjunto de S por definición y que S es cerrado para el producto, de modo que $\bigcup_{u \in U} \sigma(u)C$ está contenido en S.

Para la otra inclusión, sea $y \in S$ y considero la aplicación λ_y. Por la Ecuación 4.2, (4.5.16) y teniendo en cuenta que $|N(y)| = 1$, deducimos que $vol(\mathbb{L}^{r,s}/yM) = vol(\mathbb{L}^{r,s}/M)$. Se tiene entonces por (4.5.17) que existe un elemento no nulo x de $X \cap yM$, pongamos $x = y\sigma(\alpha)$ con $0 \neq \alpha \in R$. Entonces $Q > |N(x)| = |N(y)||N(\sigma(\alpha))| = |N_{K/\mathbb{Q}}(\alpha)|$, con lo que $\alpha u = \alpha_i$ para cierto i y algún $u \in U$. Se tiene por lo tanto que $y = x\sigma(\alpha_i^{-1})\sigma(u)$ o, equivalentemente, $x\sigma(\alpha_i^{-1}) = y\sigma(u)^{-1} \in S$, de donde $x\sigma(\alpha_i^{-1}) \in C$ y deducimos que y pertenece a $\sigma(u)C$.

□

Teorema 4.5.19 (Teorema de las Unidades de Dirichlet)**.** *El grupo de las unidades del anillo de enteros de un cuerpo de números K con r monomorfismos reales y $2s$ monomorfismos complejos es isomorfo a*

$$W \times \mathbb{Z}^{r+s-1},$$

donde W es el conjunto de las raíces de la unidad de K, que es un grupo finito cíclico de orden par.

Demostración. La última afirmación sobre W es (4.5.15). Al comienzo de la subsección argumentamos que U es un grupo abeliano finitamente generado, luego $U \cong T(U) \times (U/T(U))$ [Lan02, Teorema 7.3+7.4], donde $T(U)$ es el subgrupo de torsión de U. Como W es finito y consecuentemente de torsión, y U/W es isomorfo a $\mathbb{Z}^{r+s-1}$ por (4.5.18), que es libre de torsión, deducimos que $W = T(U)$. □

Acabamos el capítulo con un corolario, en el que usaremos la siguiente nomenclatura.

Definición 4.5.20. Sea K un subcuerpo de $\mathbb{C}$. Decimos que:

- K es *racional* si $K = \mathbb{Q}$.
- K es *cuadrático* si $[K : \mathbb{Q}] = 2$.
- K es *imaginario* si no está contenido en $\mathbb{R}$.

Corolario 4.5.21. *Sea K un cuerpo de números y R su anillo de enteros. Entonces el grupo de unidades de R es finito si y solo si K está contenido en un cuerpo cuadrático imaginario.*

CAPÍTULO 5

Caracterizaciones de grupos CUT finitos

5.1. Introducción

Llegamos finalmente a las caracterizaciones de grupos CUT finitos. Enunciaremos todas antes de proceder a la demostración una por una, pero es necesario introducir antes varios conceptos.

Sea G es un grupo finito. En la Sección 3.2 definimos la extensión

$$\mathbb{Q}(\chi) = \mathbb{Q}(\chi(g)|g \in G)$$

para un caracter complejo χ. Se puede definir un concepto dual para un elemento g de G [Ten12]:

$$\mathbb{Q}(g) = \mathbb{Q}(\chi(g)|\chi \in Irr(G)).$$

En [Ten12] se introduce también el siguiente concepto.

Definición 5.1.1. Dado un grupo G, se dice que $g \in G$ es *semi-racional* en G si existe $m \in \mathbb{Z}$ tal que cualquier generador de $\langle g \rangle$ es conjugado en G de g o de g^m. Decimos que G es *semi-racional* si todos sus elementos lo son en G.

En [Bäc+21a] encontramos una especialización de esta definición.

Definición 5.1.2. Dado un grupo G, se dice que $g \in G$ es *semi-racional* en G *por inversión* si cualquier generador de $\langle g \rangle$ es conjugado en G de g o de g^{-1}. Decimos que G es *semi-racional por inversión* si todos sus elementos lo son en G.

Es claro que un elemento semi-racional por inversión es en particular semi-racional. Recordemos también que si el orden de un elemento g de G es finito, entonces los generadores de $\langle g \rangle$ son de la forma g^j con j coprimo con $o(g)$.

Estamos ya en disposición de enunciar todas las caracterizaciones.

Teorema 5.1.3. *Sea G un grupo finito, entonces las siguientes afirmaciones son equivalentes:*

(CUT-1) *G es un grupo CUT, esto es, $Z(\mathcal{U}(\mathbb{Z}[G]))$ es igual a $\pm Z(G)$.*

(CUT-2) *$Z(\mathcal{U}(\mathbb{Z}[G]))$ es finito.*

(CUT-3) *$\mathbb{Q}(\chi)$ es racional o cuadrático imaginario para cada $\mathbb{C}$-caracter irreducible de G.*

(CUT-4) *Para cada $g \in G$ y $j \in \mathbb{N}$ coprimo con $|G|$ se tiene que g^j es conjugado en G, o bien con g, o bien con g^{-1}.*

(CUT-5) *G es semi-racional por inversión.*

(CUT-6) *$\mathbb{Q}(g)$ es racional o cuadrático imaginario para cada elemento g de G.*

Demostraremos este teorema paso a paso, y conforme avancemos utilizaremos las condiciones cuya equivalencia esté demostrada indistintamente. Comenzamos viendo la equivalencia de las condiciones (CUT-1) y (CUT-2). Requerimos primero un par de resultados técnicos.

Proposición 5.1.4. *Dado un grupo G, se verifica $\mathcal{U}(Z(\mathbb{Z}[G])) = Z(\mathcal{U}(\mathbb{Z}[G]))$.*

Demostración. Sea $x \in \mathcal{U}(Z(\mathbb{Z}[G]))$. Esto implica que $x \in Z(\mathbb{Z}[G])$ y que existe $x^{-1} \in Z(\mathbb{Z}[G])$. De lo segundo se deduce que $x \in \mathcal{U}(\mathbb{Z}[G])$. Como además x conmuta con los elementos de $\mathbb{Z}[G]$, en concreto conmuta con los de $\mathcal{U}(\mathbb{Z}[G])$, luego $x \in Z(\mathcal{U}(\mathbb{Z}[G]))$.

Dado ahora $x \in Z(\mathcal{U}(\mathbb{Z}[G]))$, se observa:

- $G \subseteq \mathcal{U}(\mathbb{Z}[G])$, luego x conmuta con los elementos de G. Es fácil comprobar que entonces conmuta con todos los elementos de $\mathbb{Z}[G]$, luego $x \in Z(\mathbb{Z}[G])$.
- $x \in \mathcal{U}(\mathbb{Z}[G])$, esto es, existe $x^{-1} \in \mathbb{Z}[G]$. Ya hemos visto que $x\alpha = \alpha x$ para cada $\alpha \in \mathbb{Z}[G]$, multiplicando por x^{-1} por ambos lados se tiene que $x^{-1} \in Z(\mathbb{Z}[G])$.

De las dos observaciones se deduce que $x \in \mathcal{U}(Z(\mathbb{Z}[G]))$. □

Teorema 5.1.5 (Berman-Higman)**.** *[MS02, Lema 7.1.2] Sea G un grupo finito, y sea $\alpha = \sum_{g \in G} a_g g$ una unidad de orden finito en $\mathbb{Z}[G]$ con $a_1 \neq 0$. Entonces $\alpha = a_1 1 = \pm 1$.*

Demostración. Pongamos $n = |G|$ y $\alpha^m = 1$ para cierto $m \in \mathbb{Z}$ positivo. Sea ϕ el carácter regular y ρ una representación de $\mathbb{C}[G]$ que lo induzca. Por (3.2.19) se tiene que $\phi(\alpha) = na_1$.

Puedo considerar la restricción de ρ al subgrupo multiplicativo $\langle \alpha \rangle$, ya que las imágenes de elementos invertibles son invertibles, lo que resulta en una representación de $\langle \alpha \rangle$. Por (3.2.13) $\rho(\alpha)$ es similar a una matriz diagonal $diag(\varepsilon_1, \ldots, \varepsilon_n)$. Multiplicando ρ por matrices invertibles P y P^{-1} adecuadas puedo suponer que $\rho(\alpha)$ es de esa forma. Como $\alpha^m = 1$ se tiene que $diag(\varepsilon_1^m, \ldots, \varepsilon_n^m) = (\rho(\alpha))^m = \rho(\alpha^m) = \mathrm{Id}$, y en concreto $|\varepsilon_i| = 1$ para cada i. Se deduce entonces

$$na_1 = \phi(\alpha) = \sum_{i=1}^{n} \varepsilon_i,$$

y por la desigualdad triangular

$$n|a_1| = |na_1| = \left| \sum_{i=1}^{n} \varepsilon_i \right| \leqslant \sum_{i=1}^{n} |\varepsilon_i| = n.$$

Debe ser $|a_1| = 1$, ya que a_1 es un entero no nulo. Se deduce que $|\sum_{i=1}^{n} \varepsilon_i| = \sum_{i=1}^{n} |\varepsilon_i|$, de donde $\varepsilon_1 = \varepsilon_2 = \ldots = \varepsilon_n$. Llegamos finalmente a la igualdad $na_1 = n\varepsilon_1$, y por lo tanto $\varepsilon_1 = a_1 = \pm 1$. Se concluye entonces que $\rho(\alpha) = \pm \mathrm{Id}$, esto es, la aplicación en $\mathbb{C}[G]$ dada por $x \mapsto x\alpha$ es $\pm \mathrm{Id}$, y de dicha función aplicada a 1 se deduce que $1\alpha = \pm 1$. □

Se tiene entonces la siguiente caracterización.

Corolario 5.1.6. *Si G es un grupo finito, entonces G es CUT si y solo si el grupo de las unidades centrales de $\mathbb{Z}[G]$ es finito.*

Demostración. La condición necesaria es obvia puesto que G es finito. Recíprocamente, si el grupo multiplicativo de las unidades centrales de $\mathbb{Z}[G]$ es finito, todos sus elementos son de orden finito. Si $\alpha = \sum_{g\in G} a_g G$ es una unidad central, en concreto $\alpha \neq 0$ y cierto a_g no es nulo. Consideramos $\beta = \alpha g^{-1}$, que también es una unidad de orden finito porque α es central. Aplicando (5.1.5) se deduce que $\beta = \pm 1 = \alpha g^{-1}$, de donde $\alpha = \pm g$ con $g \in G$. Como α es central, g es un elemento de $Z(G)$. □

Este corolario demuestra la equivalencia de las condiciones (CUT-1) y (CUT-2).

5.2. Caracterización por filas de la tabla de caracteres

La caracterización anterior y el desarrollo de los capítulos previos demuestran la caracterización en términos de las filas de la tabla de caracteres.

Teorema 5.2.1. *[JR16, Corolario 7.1.2] Sea G un grupo finito. Entonces el grupo de las unidades centrales de $\mathbb{Z}[G]$ es finito si y solo si para cada carácter irreducible complejo χ de G existe una extensión cuadrática imaginaria que contiene $\chi(G)$.*

Demostración. Es una consecuencia directa de (5.1.6), (3.3.10) y (4.5.21), ya que un anillo de enteros es un orden en su cuerpo de números. □

Con este teorema queda demostrada la equivalencia de las condiciones (CUT-2) y (CUT-3).

5.3. Caracterización por clases de conjugación

Lema 5.3.1. *Sean G un grupo finito, $n = |G|$, $\chi \in Irr(G)$ y $\sigma \in Gal(\mathbb{Q}(\chi)/\mathbb{Q})$. Supongamos que σ se extiende a un $\mathbb{Q}$-automorfismo $\hat{\sigma}$ de $\mathbb{Q}(\xi)$ para una raíz n-ésima primitiva de la unidad ξ, de forma que $\hat{\sigma}$ viene determinado por la imagen de ξ, que será ξ^j para cierto j coprimo con n. Entonces*

$$\chi^\sigma(g) = \chi(g^j).$$

Demostración. Consideramos ρ una representación que induzca χ. Fijado $g \in G$, por (3.2.24) puedo suponer que $\rho(g)$ es de la forma $diag(\varepsilon_1, \ldots, \varepsilon_s)$ para ciertas raíces n-ésimas de la unidad ε_i. Se tiene entonces que cada ε_i es potencia de ξ, de donde se deduce que $\sigma(\varepsilon_i) = \varepsilon_i^j$ para cada $i = 1, \ldots, s$, y por lo tanto

$$\chi(g^j) = tr(\rho(g^j)) = tr(\rho(g)^j) = \sum_{i=1}^{s} \varepsilon_i^j = \sum_{i=1}^{s} \sigma(\varepsilon_i) = \sigma\left(\sum_{i=1}^{s} \varepsilon_i\right) = \sigma \circ \chi(g) = \chi^\sigma(g).$$

□

Demostramos ahora la primera caracterización en términos de las clases de conjugación de G.

Teorema 5.3.2. *[RS90] Sea G un grupo finito. Entonces el grupo de las unidades centrales de $\mathbb{Z}[G]$ es finito si y solo si para cada $g \in G$ y $j \in \mathbb{N}$ coprimo con $|G|$ se tiene que g^j es conjugado en G de g o de g^{-1}.*

Demostración. Aplicaré (5.2.1). Pongamos $n = |G|$ y ξ raíz n-ésima primitiva de la unidad.

Comenzamos suponiendo la condición suficiente. Sea $\chi \in Irr(G)$ proporcionado por la representación ρ y $\sigma \in Gal(\mathbb{Q}(\chi)/\mathbb{Q})$. Por (3.2.26) y ser $\mathbb{Q}(\xi)$ el cuerpo de descomposición de $X^n - 1$ sobre $\mathbb{Q}(\chi)$, se puede extender σ a un automorfismo $\hat{\sigma}$ de $\mathbb{Q}(\xi)$ [ACM02, Proposición 4.1.6], que debe venir dado por $\xi \mapsto \xi^j$ para cierto j coprimo con n. Por (5.3.1) se cumple que $\chi^\sigma(g) = \chi(g^j)$.

Se tiene entonces para cada elemento g de G que $\chi^\sigma(g)$ es o bien $\chi(g)$, o bien $\chi(g^{-1})$, por hipótesis, donde recordemos que $\chi(g^{-1}) = \overline{\chi(g)}$. Como $\overline{\xi^j} = \overline{\xi}^j$ resulta que la conjugación conmuta con σ y debe cumplirse que $\chi + \overline{\chi} = \chi^\sigma + (\overline{\chi})^\sigma$, donde todos los sumandos son caracteres irreducibles. Como los caracteres irreducibles son linealmente independientes (3.2.14), debe ser o bien $\chi^\sigma = \chi$, o bien $\chi^\sigma = \overline{\chi}$, y por (3.2.34) los únicos elementos de $Gal(\mathbb{Q}(\chi)/\mathbb{Q})$ son la identidad y la conjugación. Se tiene pues que $[\mathbb{Q}(\chi) : \mathbb{Q}] \leqslant 2$, y si es 2 la conjugación es distinta de la identidad, con lo que la extensión es imaginaria. Hemos demostrado por lo tanto (CUT-3).

Supongamos ahora que G es CUT. Consideremos $j \in \mathbb{N}$ coprimo con n. Definimos para cada $g \in G$ la aplicación $T(g) : Irr(G) \to \mathbb{C}$ dada por $\chi \to \chi(g)$. Estas funciones son iguales para elementos conjugados. Pongamos $\mathrm{Rep} : G \to G$ una elección de representantes en las clases de conjugación, de forma que $\mathrm{Rep}(G)$ es un conjunto de representantes, y denotemos $\mathrm{Orb}(g)$ a la clase de conjugación de g. Veamos que los elementos de $\{T(g) | g \in \mathrm{Rep}(G)\}$ son linealmente independientes. Pongamos que

$$\sum_{g \in \mathrm{Rep}(G)} a_g T(g) = 0,$$

con los $a_g \in \mathbb{C}$. Se tiene entonces para cada $\chi \in Irr(G)$ que $\sum_{g \in \mathrm{Rep}(G)} a_g \chi(g) = 0$. Defino la función de clase $\varphi : G \mapsto \mathbb{C}$ dada por $g \mapsto \overline{a_{\mathrm{Rep}(g)}} \frac{|G|}{|\mathrm{Orb}(g)|}$, de forma que $\langle \chi, \varphi \rangle = 0$ para cada $\chi \in Irr(G)$. Como $Irr(G)$ es una base ortonormal del espacio de las funciones de clase, se tiene que $\varphi = 0$, y por lo tanto $a_g = 0$ para cada $g \in Rep(G)$.

Como j es coprimo con n se tiene que $\xi \mapsto \xi^j$ induce un automorfismo de $\mathbb{Q}(\xi)$, que se restringe a otro de $\mathbb{Q}(\chi)$ al que denotaremos σ. Pero σ solo puede ser la identidad o la conjugación por (CUT-3), de forma que para cada elemento g de G, o bien $\chi^\sigma(g) = \chi(g)$, o bien $\chi^\sigma(g) = \chi(g^{-1})$, y por lo tanto $T(g^j) + T(g^{-j}) = T(g) + T(g^{-1})$. De la independencia lineal de las funciones $T(g)$ salvo conjugados se deduce primero que $T(g^j)$ es igual a $T(g)$ o a $T(g^{-1})$, y después que g^j es conjugado de g o de g^{-1}. □

Con este último resultado hemos demostrado ya la equivalencia de las todas las condiciones desde (CUT-1) a (CUT-4).

Observación 5.3.3. El argumento sobre la independencia lineal de las funciones $T(g)$ en concreto implica que dos elementos de G son conjugados si y solo si tienen la misma imagen por todos los caracteres complejos irreducibles.

Demostramos ahora que (CUT-5) es condición necesaria y suficiente de (CUT-4)

Teorema 5.3.4. *[Bäc18, Proposición 2] Sea G un grupo finito. Entonces G es semi-racional por inversión si y solo si para cada $g \in G$ y $j \in \mathbb{N}$ coprimo con $|G|$ se tiene que g^j es conjugado en G, o bien con g, o bien con g^{-1}.*

Demostración. La implicación de izquierda a derecha es evidente. Para el recíproco, sea $g \in G$ y pongamos $n = o(g)$ y $N = |G|$. Podemos descomponer $N = N_1N_2$ de manera que cualquier primo p cumple que $p|n$ si y solo si $p|N_1$. Como n divide a N y es coprimo con N_2, n debe dividir a N_1.

Supongamos entonces que j es un entero coprimo con n, y por lo tanto coprimo con N_1. Por el Teorema Chino de los Restos existe otro entero k tal que $k \equiv j \ (mod\ N_1)$ y $k \equiv 1 \ (mod\ N_2)$. Tenemos entonces que k es coprimo con N_1, ya que j lo es, y también es coprimo con N_2, luego k es coprimo con N. Aplicando la hipótesis sabemos que g^k es conjugado en G de g o de g^{-1}, pero como n divide a N_1 se tiene que $g^j = g^k$.

□

5.4. Caracterización por columnas de la tabla de caracteres

Llegamos a la última caracterización de grupo CUT finito, también en términos de la tabla de caracteres, aunque esta vez de sus columnas.

Lema 5.4.1. *[Ten12, Lema 1] Sean G un grupo finito y g un elemento de G. Entonces g es semi-racional en G si y solo si $\mathbb{Q}(g)$ es racional o cuadrático.*

Demostración. Pongamos $n = o(g)$, y sea ξ una raíz n-ésima primitiva de la unidad. Dado un elemento de $Gal(\mathbb{Q}(\xi)/\mathbb{Q})$, este viene determinado por la imagen de ξ, que será ξ^j para cierto $j \in \mathbb{Z}$ coprimo con n, y dicho elemento de $Gal(\mathbb{Q}(\xi)/\mathbb{Q})$ será denotado por σ_j. De manera análoga usaremos la notación τ_j para el automorfismo de $\langle g \rangle$ que asocia g con g^j para cada j coprimo con n. Podemos definir entonces el isomorfismo de grupos dado por

$$\begin{aligned} \phi : Gal(\mathbb{Q}(\xi)/\mathbb{Q}) &\longrightarrow Aut(\langle g \rangle) \\ \sigma_j &\longmapsto \phi(\sigma_j) = \tau_j. \end{aligned}$$

Realizamos dos observaciones:

1. Si $\chi \in Irr(G)$, entonces $\chi(g) \in \mathbb{Q}(\xi)$ por (3.2.24) y $\sigma_j \circ \chi(g) = \chi(g^j)$ por (5.3.1).
2. Consideremos el normalizador $N_G(\langle g \rangle) = \{h \in G | h \langle g \rangle h^{-1} = \langle g \rangle\}$, que es un subgrupo de G que contiene al centralizador $C_G(g) = \{h \in G | hg = gh\}$. Es fácil ver que $C_G(g)$ es un subgrupo normal de $N_G(\langle g \rangle)$. Considero además la función

$$\begin{aligned} Q : N_G(\langle g \rangle) &\longrightarrow Aut(\langle g \rangle) \\ h &\longmapsto (g \mapsto hgh^{-1}), \end{aligned}$$

que es un homomorfismo de grupos con núcleo $C_G(g)$. Se identifica entonces el grupo cociente $H_g = N_G(\langle g \rangle)/C_G(g)$ con el subgrupo $\mathrm{Im}(Q)$ de $Aut(\langle g \rangle)$, más concretamente

$$H_g \equiv \{f \in Aut(\langle g \rangle) | f \text{ viene dado por } g \mapsto hgh^{-1} \text{ para cierto } h \in N_G(\langle g \rangle)\}.$$

Tenemos entonces que σ_j está en $Gal(\mathbb{Q}(\xi)/\mathbb{Q}(g))$ si y solo si $\chi(g) = \sigma_j(\chi(g))$ para cada caracter irreducible de G. Aplicando la primera observación, la condición anterior equivale a que $\chi(g^j)$ sea igual a $\chi(g)$ para cada caracter irreducible de G, y por (5.3.3) esto ocurre si y solo si g y g^j son conjugados en G, digamos $g^j = hgh^{-1}$ para cierto $h \in N_G(\langle g \rangle)$, lo que equivale a que $\phi(\sigma_j) = \tau_j$ esté en $\mathrm{Im}(Q) \equiv H_g$.

Se restringe entonces ϕ a un isomorfismo de grupos entre $Gal(\mathbb{Q}(\xi)/\mathbb{Q}(g))$ y H_g. El resultado es directo dadas las siguientes observaciones:

- Como $\mathbb{Q}(\xi)$ es de Galois, por el Primer Teorema Fundamental de Galois [ACM02, Teorema 5.2.7]
$$[\mathbb{Q}(g) : \mathbb{Q}] = [Gal(\mathbb{Q}(\xi)/\mathbb{Q}) : Gal(\mathbb{Q}(\xi)/\mathbb{Q}(g))],$$
Además, $\mathbb{Q}(g)$ es racional o cuadrático si y solo si
$$[\mathbb{Q}(g) : \mathbb{Q}] \leqslant 2.$$

- g es semi-racional en G si y solo si existe $m \in \mathbb{Z}$ tal que para cada automorfismo f de $\langle g \rangle$ se tiene que $f(g)$ es conjugado en G de g o de g^m, esto es, todo automorfismo f de $\langle g \rangle$ se viene dado por $g \mapsto hgh^{-1}$ o por $g \mapsto hg^m h^{-1}$ con $h \in N_G(\langle g \rangle)$, lo cual equivale a que
$$[Aut(\langle g \rangle) : H_g] \leqslant 2.$$

□

Observación 5.4.2. Siguiendo en el contexto de la demostración anterior, $\mathbb{Q}(g)$ es racional si y solo si $[\mathbb{Q}(g) : \mathbb{Q}] = 1$ si y solo si $[Aut(\langle g \rangle) : H_g] = 1$ si y solo si cada $f \in Aut(\langle g \rangle)$ viene dado por $g \mapsto hgh^{-1}$ o, equivalentemente, para cada j coprimo con $o(g)$ se cumple que g^j es conjugado de g en G.

Definición 5.4.3. Sea G un grupo y g un elemento de G. Decimos que g es *racional* en G si es conjugado de cualquier generador de $\langle g \rangle$ en G. Decimos que G es *racional* si cada elemento suyo lo es en G.

Observación 5.4.4. Por la Observación 5.4.2 se cumple que G es racional si y solo si todas las entradas de su tabla de caracteres son elementos de $\mathbb{Q}$. Denotaremos por $\mathbb{Q}(G)$ a la extensión de $\mathbb{Q}$ generada por las entradas de la tabla de caracteres de G

Teorema 5.4.5. *[Bäc+21a, Proposición 3.2] Sea G un grupo finito. Entonces G es CUT si y solo si $\mathbb{Q}(g)$ es racional o cuadrático imaginario para cada elemento g de G.*

Demostración. Supongamos que G es CUT y sea $g \in G$, que por (CUT-5) es semi-racional por inversión en G. Por (5.4.1) se tiene que $[\mathbb{Q}(g) : \mathbb{Q}] \leqslant 2$. Si $\mathbb{Q}(g)$ es racional ya lo tenemos, así que supongamos que $[\mathbb{Q}(g) : \mathbb{Q}] = 2$. Existe por lo tanto $\chi \in Irr(G)$ tal que $\chi(g)$ no es racional, luego $\mathbb{Q} \subsetneq \mathbb{Q}(g) \subseteq \mathbb{Q}(\chi)$. Por (CUT-3) $\mathbb{Q}(\chi)$ debe ser cuadrático imaginario, y por igualdad de grados sobre $\mathbb{Q}$ se tiene que $\mathbb{Q}(g) = \mathbb{Q}(\chi)$.

Suponemos ahora la segunda condición y fijamos $g \in G$, que es semi-racional en G por (5.4.1). Existe entonces $m \in \mathbb{Z}$ tal que para cada j entero coprimo con $o(g)$ se cumple que g^j es conjugado de g o de g^m en G. Distinguimos dos casos:

- Si g y g^{-1} son conjugados en G, para cada $\chi \in Irr(G)$ se tiene que $\chi(g) = \chi(g^{-1}) = \overline{\chi(g)}$, esto es, $\chi(g) \in \mathbb{Q}(g) \cap \mathbb{R}$, siendo esta intersección igual a $\mathbb{Q}$ por ser $\mathbb{Q}(g)$ racional o cuadrático imaginario. Deducimos que $\mathbb{Q}(g) = \mathbb{Q}$ y que para cada j coprimo con $o(g)$ se cumple que g^j es conjugado de g en G por (5.4.2).
- Si g y g^{-1} no son conjugados en G deben serlo g^{-1} y g^m, luego podemos elegir $m = -1$.

En ambos casos g es semi-racional en G por inversión, de modo que se cumple (CUT-5). □

CAPÍTULO 6

Problemas abiertos sobre grupos CUT

Los grupos CUT son una línea de investigación en auge. Es por esto que terminamos el trabajo recopilando algunas de las preguntas abiertas en este campo. Las fuentes utilizadas son [Bäc+21a], [Bäc19] y [Bäc+21b].

La clase de los grupos CUT se puede considerar como una extensión de los grupos racionales, que han sido ampliamente estudiados [Kle84]. En consecuencia, es conveniente utilizarlos como modelo a la hora de estudiar los grupos CUT, motivando nuevos problemas y comparando los resultados.

6.1. Sobre el encaje de S-grupos

Definición 6.1.1. Si p es un primo, un *p-grupo* es un grupo finito cuyo orden es una potencia de p. Si S es un conjunto de primos, un *S-grupo* es un grupo finito cuyo orden es producto de potencias de los primos de S.

Definición 6.1.2. Un *grupo G* es *resoluble* si existe una cadena de subgrupos

$$1 = G_0 \subseteq G_1 \subseteq \cdots \subseteq G_k = G$$

tal que G_i es normal en G_{i+1} y G_{i+1}/G_i es abeliano para cada $i = 1, \ldots, k-1$.

Definición 6.1.3. Dado un grupo finito G, denotamos por $\pi(G)$ al *espectro primo* de G, que es el conjunto de todos los divisores primos del orden de G.

Se conoce el siguiente resultado sobre el espectro primo de grupos CUT finitos y resolubles.

Teorema 6.1.4. *[Bäc18, Teorema 1.2] Si G es un grupo CUT finito y resoluble, entonces $\pi(G) \subseteq \{2, 3, 5, 7\}$.*

Bächle y col. [Bäc+21a, Proposición 4.6] demostraron que todo 5-grupo y 7-grupo H puede ser encajado en un grupo CUT finito y resoluble G, es decir, existe un monomorfismo de grupos de H a G. Este resultado y el teorema anterior motivan la siguiente pregunta.

Problema 1. ¿Puede cualquier $\{2, 3, 5, 7\}$-grupo ser encajado en un grupo CUT finito y resoluble?

6.2. Sobre el tamaño de $\mathbb{Q}(G)$

Ya hemos visto que G es racional si y solo si $[\mathbb{Q}(G) : \mathbb{Q}] = 1$. Uno de los problemas abiertos sobre grupos CUT actualmente es si existe una cota uniforme de este grado para todos ellos.

Problema 2. ¿Existe $K > 0$ tal que $[\mathbb{Q}(G) : \mathbb{Q}] \leqslant K$ para cada grupo CUT G?

Se conoce que la respuesta es afirmativa añadiendo otras hipótesis. Por ejemplo, para grupos CUT resolubles es válida la cota $K = 2^5$. Sin embargo, para la clase más general de los grupos semi-racionales sabemos que no es cierto, sirviendo los grupos alternados como contraejemplo.

6.3. Sobre subgrupos de Sylow

Definición 6.3.1. Dado un grupo finito G y un número primo p, un subgrupo H de G es un *p-subgrupo de Sylow* de G si H es un p-grupo y $[G : H]$ es coprimo con p. El conjunto de los p-subgrupos de Sylow de G se denota por $\mathrm{Syl}_p(G)$.

Como los grupos racionales no triviales tienen orden par, los 2-subgrupos de Sylow de un grupo racional tienen cierto interés. Durante mucho tiempo se conjeturó que los 2-subgrupos de Sylow de un grupo racional debían ser también racionales. A pesar de ser demostrado para ciertas clases de grupos, se acabaron encontrado contraejemplos [IN12].

Una situación similar ocurre con los grupos CUT. Se sabe que el orden de todo grupo CUT no trivial es divisible por 2 o por 3. Se han encontrado 2-subgrupos de Sylow de grupos CUT que no son CUT, pero la pregunta sigue abierta para $p = 3$.

Problema 3. Sea G un grupo CUT y $P \in \mathrm{Syl}_3(G)$. ¿Es P un grupo CUT?

Se conoce el siguiente resultado.

Lema 6.3.2. *Sea G un grupo y g un elemento de G de orden potencia de 3. Entonces g es semi-racional por inversión en G si y solo si g es semi-racional por inversión en P para algún $P \in \mathrm{Syl}_3(G)$.*

El lema anterior se puede transformar en el Problema 3 sustituyendo "algún $P \in \mathrm{Syl}_3(G)$" por todos los $P \in \mathrm{Syl}_3(G)$ que contengan a g. Además, sabemos que bajo alguna de las siguientes condiciones la respuesta es afirmativa:

1. P es abeliano,
2. P es un subgrupo normal de G,
3. G es superesoluble,
4. G es un grupo de Frobenius,
5. G es simple o G tiene orden impar.

Definimos a continuación los conceptos nuevos de esta lista.

Definición 6.3.3. Un *grupo G* es *superesoluble* si existe una cadena de subgrupos

$$1 = G_0 \subseteq G_1 \subseteq \cdots \subseteq G_k = G$$

tal que G_i es normal en G y G_{i+1}/G_i es cíclico para cada $i = 1, \ldots, k-1$.

Definición 6.3.4. Un grupo de Frobenius es un grupo de permutaciones actuando sobre un conjunto finito X no vacío que cumple:

1. Dados $x, y \in X$, existe $g \in G$ tal que $g \cdot x = y$.
2. Ningún elemento no trivial de G fija más de un elemento de X.
3. Al menos un elemento no trivial de G fija un elemento de X.

Definición 6.3.5. Un grupo no trivial G es simple si sus únicos subgrupos normales son $\{1\}$ y G.

6.4. Sobre la frecuencia de los grupos CUT

En esta sección denotamos por $c(r)$ al número de grupos CUT de orden r y por $f(r)$ al número de grupos de orden r.

Para tamaños pequeños los grupos CUT son sorprendentemente comunes. Por ejemplo, suponen un 86.62 % de los grupos de orden menor o igual que 512, frente al 0.52 % que suponen los grupos racionales. Se conoce también el siguiente resultado asintótico.

Proposición 6.4.1. *Para $p \in \{2, 3\}$ se cumple*

$$\lim_{n\to\infty} \frac{\ln c(p^n)}{\ln f(p^n)} = 1.$$

En el cuadros 6.1 y 6.2 se muestra la proporción de grupos CUT para grupos cuyo orden es potencia de 2 o potencia de 3, respectivamente. Observamos que en el caso de 2 hay un cambio de tendencia decreciente a creciente en 2^7, mientras que para las potencias de 3 hay decrecimiento a partir de 3^3. Esto motiva el siguiente problema.

Problema 4. ¿Existe un entero m mayor que 2 tal que

$$\frac{c(3^{m+1})/f(3^{m+1})}{c(3^m)/f(3^m)} > 1,$$

es decir, tal que la proporción de grupos CUT vuelva a crecer?

2^2	2^3	2^4	2^5	2^6	2^7	2^8	2^9
100 %	80 %	71.43 %	64.71 %	60.30 %	57.95 %	67.02 %	86.98 %

Cuadro 6.1: Proporción de grupos CUT para grupos de orden potencia de 2 hasta $2^9 = 512$.

3^2	3^3	3^4	3^5	3^6	3^7	3^8
50 %	60 %	26.67 %	20.90 %	19.05 %	6.39 %	5.06 %

Cuadro 6.2: Proporción de grupos CUT para grupos de orden potencia de 3 hasta $3^8 = 6561$.

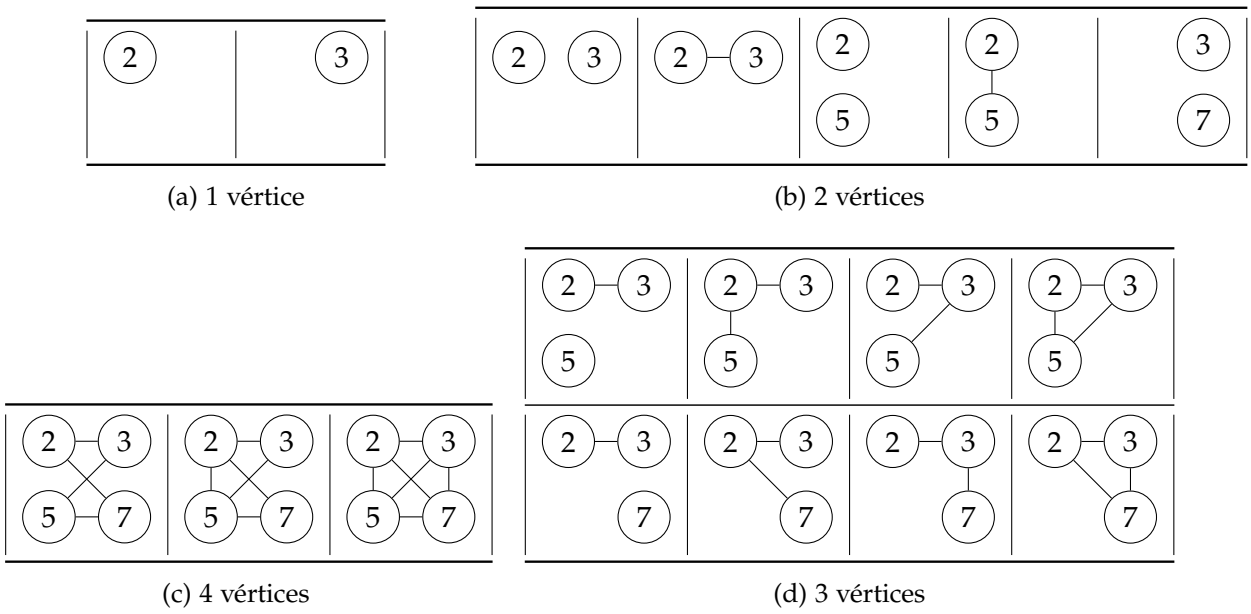
6.5. Sobre el grafo Gruenberg-Kegel

Definición 6.5.1. Sea G un grupo. El *grafo Gruenberg-Kegel* de G, abreviado como el *GK-grafo* de G y denotado por $\Gamma_{GK}(G)$, es el grafo no dirigido y sin ejes paralelos cuyos nodos son los primos

p tales que existe un elemento en G de orden p, y tal que dos nodos p y q están unidos si y solo si existe un elemento en G de orden pq.

Este grafo es de interés porque refleja propiedades curiosas del grupo. En el caso de los grupos CUT finitos y resolubles ya hemos visto que puede tener a lo más 4 nodos. El último problema que nos concierne es el de determinar qué grafos son generados como GK-grafos de un grupo CUT finito y resoluble. En el cuadro 6.3 encontramos grafos para los cuales la respuesta es afirmativa. En el caso de 3 o menos vértices se trata de hecho de una lista exhaustiva, esto es, esos son los únicos grafos que lo cumplen. Para 4 vértices aún quedan algunos por comprobar.

Problema 5. ¿Cuáles de los grafos en el cuadro 6.4 pueden ser generados como GK-grafos de un grupo CUT resoluble?



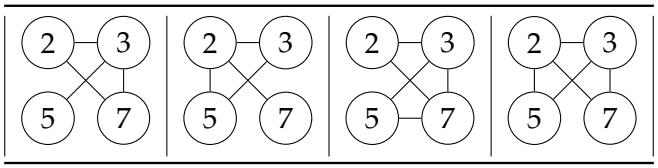
(a) 1 vértice

(b) 2 vértices

(c) 4 vértices

(d) 3 vértices

Cuadro 6.3: Grafos generados como GK-grafos de un grupo CUT resoluble.



Cuadro 6.4: Potenciales GK-grafos de grupos CUT resolubles.

Referencias

[ACM02] José Asensio Mayor, José Caruncho y Juan Martínez Hernández. *Ecuaciones algebraicas*. Murcia: DM, 2002.

[AM18] Michael Francis Atiyah y Ian G. Macdonald. *Introduction to Commutative Algebra*. Addison-Wesley Series in Mathematics. Boca Raton London New York: CRC Press, Taylor & Francis Group, 2018.

[Bäc+21a] Andreas Bächle, Mauricio Caicedo, Eric Jespers y Sugandha Maheshwary. "Global and Local Properties of Finite Groups with Only Finitely Many Central Units in Their Integral Group Ring". *Journal of Group Theory* 24.6, págs. 1163-1188. DOI: 10.1515/jgth-2020-0165.

[Bäc+21b] Andreas Bächle, Ann Kiefer, Sugandha Maheshwary y Ángel del Río. *Gruenberg-Kegel Graphs: Cut Groups, Rational Groups and the Prime Graph Question*. 2021. DOI: 10.48550/ARXIV.2112.08188.

[Bäc18] Andreas Bächle. "Integral Group Rings of Solvable Groups with Trivial Central Units". *Forum Mathematicum* 30.4, págs. 845-855. DOI: 10.1515/forum-2017-0021.

[Bäc19] Andreas Bächle. "ADV Perspectives in Group Theory". *Advances in Group Theory and Applications* 8, págs. 157-160. DOI: 10.32037/agta-2019-015.

[dRío21] Ángel del Río Mateos. "Apuntes de Teoría de Números Algebraicos". Murcia, 20 de dic. de 2021.

[dRSdV06] Ángel del Río Mateos, Juan Jacobo Simón Pinero y Alberto del Valle Robles. *Álgebra básica*. Murcia: DM, 2006.

[Hig40] Graham Higman. "The Units of Group-Rings". *Proceedings of the London Mathematical Society* s2-46.1, págs. 231-248. DOI: 10.1112/plms/s2-46.1.231.

[IN12] I. M. Isaacs y Gabriel Navarro. "Sylow 2-Subgroups of Rational Solvable Groups". *Mathematische Zeitschrift* 272.3-4, págs. 937-945. DOI: 10.1007/s00209-011-0965-9.

[Isa94] I. Martin Isaacs. *Character Theory of Finite Groups*. New York: Dover, 1994.

[JR16] Eric Jespers y Ángel del Río. *Group Ring Groups*. De Gruyter Graduate. Berlin: De Gruyter, 2016.

[Kle84] Dennis Kletzing. *Structure and Representations of Q-groups*. Lecture Notes in Mathematics 1084. Berlin Heidelberg: Springer, 1984.

[Lan02] Serge Lang. *Algebra*. Rev. 3rd ed. Graduate Texts in Mathematics 211. New York: Springer, 2002.

[Mar18] Daniel A. Marcus. *Number Fields*. Col. de Emanuele Sacco. Second edition. Universitext. Cham: Springer, 2018. DOI: 10.1007/978-3-319-90233-3.

[MS02] César Polcino Milies y Sudarshan K Sehgal. *An Introduction to Group Rings*. Dordrecht; Boston: Kluwer Academic Publishers, 2002.

[RS90] Jürgen Ritter y Sudarshan K. Sehgal. "Integral Group Rings with Trivial Central Units". *Proceedings of the American Mathematical Society* 108.2, págs. 327-329. JSTOR: 2048279.

[Ten12] Joan F. Tent. "Quadratic Rational Solvable Groups". *Journal of Algebra* 363, págs. 73-82. DOI: 10.1016/j.jalgebra.2012.04.019.

Índice alfabético