Universidad de Valladolid

FACULTAD DE CIENCIAS

TRABAJO FIN DE GRADO

Grado en Matemáticas

POLINOMIOS Y CUERPOS CICLOTÓMICOS: DISCRIMINANTES Y RAMIFICACIÓN DE NÚMEROS PRIMOS

Autora: Itziar Campo Juarros
Tutor: Antonio Campillo López
Año: 2023

A mis padres, por ser la calma antes, durante y después de la tormenta.
A mi tío y padrino Ricardo, todo lo que soy a día de hoy es por ti.
A mi Ángel.

Índice

Introducción

Los cuerpos y anillos siempre han sido de gran interés en el álgebra y en las matemáticas en general ya que proveen de estructuras sobre las que construir otras estructuras y teorías más complejas. La teoría de números en concreto es una rama de las matemáticas que estudia las propiedades de los anillos de números. De forma general este campo estudia los problemas que surgen con el estudio de los números enteros. Es por eso que el reconocido matemático *Jürgen Neukirch* (Dortmund, 1937 - Regensburgo, 1997), quien dedicó su estudio a este campo, cita lo siguiente: "la teoría de números ocupa entre las disciplinas matemáticas una posición idealizada análoga a aquella que ocupan las matemáticas mismas entre las otras ciencias". El término aritmética era utilizado antiguamente para referirse a esta disciplina de las matemáticas hasta que el estudio de la misma adquirió un carácter mucho más teórico, muy lejos de lo trivial.

Dentro de la teoría de cuerpos cobra gran relevancia el estudio y descripción de las propiedades de los cuerpos de números. Los cuerpos de números son extensiones K del cuerpo de los números racionales $\mathbb{Q}$, tales que el grado de la extensión $[K : \mathbb{Q}]$ es finito. Este tipo de extensiones posee un elemento primitivo (o elemento generador), que hace que el cuerpo de números considerado sea el mínimo que contiene tanto a $\mathbb{Q}$ como al propio elemento. Sin embargo, en la mayoría de casos resulta complicado conocer tal elemento, cuando además se le pide que también genere el anillo de enteros θ_K de K. Es aquí donde aparece el caso a tratar en este trabajo, los cuerpos ciclotómicos.

Los cuerpos ciclotómicos son un ejemplo particular de los cuerpos de números en los que ese elemento primitivo es bien conocido: una raíz primitiva de la unidad z de un orden n conocido. Las raíces primitivas n-ésimas la unidad forman un grupo multiplicativo, cuyas propiedades no resultan para nada triviales pero sí muy interesantes. Este grupo posee una estrecha relación con la conocida *función de Euler* y el grupo de unidades (también multiplicativo) $(\mathbb{Z}/n\mathbb{Z})^*$. Además, una de las inumerables propiedades y particularidades de los cuerpos de números son los ya mencionados anillos de enteros. Los anillos de enteros de cuerpos de números están formados por los elementos de una extensión $K/\mathbb{Q}$ que son raíces de algún polinomio con coeficientes sobre el anillo $\mathbb{Z}$.

Una de las cuestiones más estudiadas en teoría de números siempre ha sido la posible (o no) factorización única de los elementos que constituyen una estructura algebraica. Es por eso que dependiendo de las características que cumplen distintos casos, estos sufren diferentes clasificaciones: dominio de factorización única, dominio de Dedekind. Estrechamente relacionado con este concepto se encuentra el discriminante. Existen dos definiciones de discriminante, en principio completamente desvinculadas: el discriminante de un polinomio y el discriminante de un cuerpo. Sin embargo estas se enlazan y conectan en el caso de los cuerpos ciclotómicos, dando lugar a una definición sin ambigüedad.

Como se ha comentado antes, los cuerpos ciclotómicos poseen la propiedad de que el elemento primitivo que genera la extensión de anillos de enteros es conocido; es decir, si

z es una raíz primitiva n-ésima de la unidad la extensión ciclotómica L_n será igual a la extensión de números generada por z, $\mathbb{Q}(z)$. Es más, para este caso es conocido también el polinomio mónico irreducible asocidado a la raíz primitiva n-ésima z, denominado polinomio ciclotómico n-ésimo. Esto lleva a que el anillo de enteros de esta clase de extensiones sea monógeno, y este generado exactamente por este mismo elemento z, es decir, el anillo de enteros será $\theta_K = \mathbb{Z}[z]$. El interés se encuentra en que existe un teorema que afirma que en el caso de que el anillo de enteros sea de la forma $\theta_K = \mathbb{Z}[z]$ para un cuerpo de números que posee un elemento primitivo z, entonces los discriminantes de ese cuerpo, $\mathscr{D}_K$ y el discriminante del polinomio irreducible que posee al elemento primitivo como raíz, coinciden.

El estudio y desarrollo de estos resultados es el objeto de este trabajo, así como las consecuencias más destacables en teoría de números que esto ha podido acarrear. Además se adjunta una de las muchas pruebas existentes de la Ley de Reciprocidad Cuadrática. Este último resultado es uno de los más importantes de la teoría de números y es por eso que se ha considerado oportuno agregar una prueba de este, que además está relacionada con la sección dedicada a las raíces de la unidad.

1. Conceptos básicos sobre las extensiones de cuerpos

La teoría de cuerpos abarca varios conceptos y resultados importantes. En esta sección se van a introducir una serie de resultados y conceptos, a modo introductorio, que después serán utilizados a lo largo de todo el texto. Estas definiciones y resultados elementales pueden encontrarse en la referencia [[4]].
Uno de los temas centrales es el estudio de las extensiones de cuerpos, que son cuerpos más grandes construidos a partir de cuerpos más pequeños dados. Estas extensiones son fundamentales para comprender las estructuras algebraicas más complejas y tienen aplicaciones en diversos campos de las matemáticas y la física.
Además, la teoría de cuerpos investiga las propiedades de los polinomios sobre cuerpos y la relación entre los cuerpos y sus extensiones. El teorema fundamental de la teoría de cuerpos establece que cualquier polinomio no constante con coeficientes en un cuerpo concreto tiene una raíz en alguna extensión de dicho cuerpo.

1.1. Primeras definiciones

Antes de comenzar con los resultados y teoremas principales de la teoría de las extensiones de cuerpos se van a presentar una serie de definiciones, que pueden encontrarse en la referencia [[[9]]]. Así, existen diferentes tipos de extensiones de cuerpos, dependiendo de las características que tengan en relación a los polinomios con coeficientes sobre ellas:

Definición 1.1. Se dice que una extensión L/K es algebraica si todos los elementos de L son raíces de algún polinomio con coeficientes en K; es decir, si todos los elementos de L son elementos algebraicos sobre K.

Nota. Si $x \in L$ es un elemento algebraico sobre K, el polinomio mónico $p(t)$ de grado mínimo con coeficientes en K que tiene a x como raíz es irreducible y se denomina *polinomio irreducible de* x sobre K.

Observación 1. Si L/K es una extensión finita; es decir, si L es de dimensión finita como espacio vectorial sobre K, entonces L/K es una extensión algebraica.
Dicha dimensión $dim(L) = [L : K]$, se llama grado de la extensión.
Además, si L' es otro cuerpo tal que $K \subset L' \subset L$, entonces $[L : K] = [L : L'] \cdot [L' : K]$

Así mismo se tiene también el concepto contrario.

Definición 1.2. Una extensión L/K se dice que es transcendente si existe algún elemento en L que no es raíz de ningún polinomio no nulo de $K[t]$; o en otras palabras, si existe algún elemento en L que no es algebraico sobre K.

A continuación se definirá un concepto de gran importancia en la teoria de extensiones de cuerpos:

Definición 1.3. Se llama clausura algebraica de un cuerpo K a una extensión algebraica $\bar{K}/K$ tal que $\bar{K}$ es un cuerpo algebraicamente cerrado.

Como se ha visto en clase, un teorema que afirma que existe una clausura algebraica $\bar{K}/K$ y que si $\bar{K}'/K$ es otra clausura algebraica para el mismo cuerpo, entonces existe un isomorfismo de cuerpos $f : \bar{K} \longrightarrow \bar{K}'$ que deja fijos todos los elementos de K.

Por último, se incluye una proposición, cuya consecuencia se utilizará más adelante para determinar el grado de una extensión ciclotómica.

Proposición 1.1. *Sea x un elemento algebraico sobre un cuerpo K y $p(t)$ su polinomio irreducible en $K[t]$. Entonces, la extensión generada por este elemento, $K(x)/K$ es finita y $[K(x) : K]$ es igual al grado de $p(t)$.*

Nota. Recordemos que $p(t)$ es, por definición, el polinomio mónico de $K[t]$ de grado mínimo que tiene a x como raíz. Si L/K es una extensión finita y $x \in L$, entonces se deduce de la proposición 1.1 que el grado del polinomio irreducible de x sobre K es un divisor de $[L : K]$.

1.2. Extensiones separables y extensiones normales.

Ahora se presentarán una serie de resultados relacionados con polinomios con coeficientes en un cuerpo $K[t]$, que pueden encontrarse en este caso también en la bibliografía mencionada antes, es decir [[4]] y [[9]].

Definición 1.4. Sea $p(t)$ un polinomio de grado $m > 0$ con coeficientes en $K[t]$. Se dice que $p(t)$ es separable cuando, dado un cuerpo de descomposición L/K, toda sus raíces son distintas, o equivalentemente, cuando su discriminante $\Delta(p)$ es no nulo.

Otra condición equivalente para que $p(t)$ sea separable es que el máximo común divisor de $p(t)$ y su polinomio derivado $p'(t)$ sea 1, siempre y cuando, además, $p'(t) \neq 0$.
Se introduce también en la definición anterior el concepto de discriminante, el cual cobrará importancia más adelante en este trabajo.

Nota. Para el caso en el que la característica del cuerpo K sea $p > 0$, debe utilizarse la definición determinantal del discriminante $\Delta(p)$, ya que puede darse el caso en el que el grado de $p'(t)$ sea menor que m-1, incluso puede ocurrir que $p'(t)$ sea nulo.

Definición 1.5. Una extensión algebraica L/K se dice que es separable cuando para todo $x \in L$ el polinomio irreducible de x sobre K es un polinomio separable.

Daremos a continuación un resultado de suma importancia dentro de la teoría de extensiones de cuerpos. Este resultado no se probará, ya que es parte del contenido de la asignatura de *Ecuaciones Algebraicas* del grado y no es interesante para el tema que nos concierne, pero se hará uso de él en varias ocasiones.

Teorema 1.1. ***(de las inmersiones)*** *Sea K'/K una extensión finita de grado m, $\bar{K}/K$ una clausura algebraica de K y H el conjunto de los homomorfismos de cuerpos $h : K' \longrightarrow \bar{K}$, que dejan invariantes todos los elementos de K.*
Entonces:

- *H es finito y su cardinal es menor o igual que m, $|H| \leq m$.*
- *El cardinal de $|H|$ es igual a m si y sólo si la extensión K'/K es separable.*

Tras estos resultados sobre separabilidad estamos en condiciones de caracterizar las extensiones de una última forma, necesaria para poder adentrarse en la teoría de Galois y poder describir más tarde las extensiones ciclotómicas con precisión.

Definición 1.6. Sean una extensión finita K'/K y una clausura algebraica $\bar{K}/K'$. Se dice que la extensión K'/K es normal cuando para todo homomorfismo $h : K' \longrightarrow \bar{K}$ que deja invariantes a todos los elementos de K se tiene que $h(K') = K'$.

Esta condición es obviamente equivalente a decir que $h(K') \subset K'$ y $K' \subset h(K')$.

Nota. El comentario anterior resulta de cierta utilidad ya que, por tratarse de cuerpos, para cualquier extensión, los homomorfismos de cuerpos h son inyectivos. Denotemos ahora entonces $L = K'$ y supongamos que L/K es normal. Entonces L es el cuerpo de descomposición de un polinomio $q(t) \in K[t]$ y se tiene que $q(t) = (t-x_1)(t-x_2)...(t-x_n)$ y que $L = K(x_1, ..., x_n)$; es decir, L es el mínimo cuerpo que contiene a K y a las raíces $x_1, x_2, ..., x_n$ de $q(t)$.
Si se aplica ahora el homomorfismo $h : L \longrightarrow \bar{L} = \bar{K}$, se tiene $h(x_j) = x_i$ para todo $j \in 1, ..., n$, y para algún i, que depende de este j. Entonces se tiene que $Im(h) \supset K(x_1, ..., x_n)$ y en consecuencia $Im(h) \supset x_1, ..., x_n$.
Esto implica que $Im(h) = L$.

Con esto puede demostrarse el siguiente resultado, recíproco del anterior.

Proposición 1.2. *Todo cuerpo de descomposición es una extensión normal.*

Observación 2. Todo cuerpo de descomposición es también una extensión finita, ya que sus elementos son todos algebraicos sobre K.

Entonces, si la extensión finita L/K es una extensión normal arbitraria, y se tiene el conjunto de homomorfismos $H = \{h : L \longrightarrow \bar{K} = \bar{L}\}$ y según se ha reflejado en el comentario anterior, $Im(h) = L$. Esto permite identificar H con el conjunto de automorfismos $G = \{g : L \longrightarrow L\}$ que dejan invariantes a todos los elementos de K. Entonces, $G = H$.

Nota. Cada extensión normal puede ser simultáneamente cuerpo de descomposición de varios polinomios diferentes.

Todos estos resultados sobre extensiones permiten establecer un puente entre los polinomios de $K[t]$ y los grupos finitos. A cada polinomio $p(t)$ de $K[t]$ se le asocia el grupo

de automorfismos de la extensión L/K que corresponde al cuerpo de descomposición del polinomio sobre K. En virtud del *teorema de inmersiones*, el grupo asociado es finito. Si además la extensión es separable, cosa que ocurre siempre en cuerpos de característica 0 y ciertas veces si la característica es $p > 0$, el orden del grupo es igual al grado de la extensión $[L : K]$.

Observación 3. Sea L/K una extensión y L' un cuerpo intermedio. Entonces:

- L/K es finita si y sólo si L'/K y L/L' son extensiones finitas. De hecho se tiene que $[L : K] = [L : L'][L' : K]$ (como ya se comentó en la observación 1).
- L/K es separable si y sólo si L'/K y L/L' son ambas separables.
- Sin embargo, si L/K es normal, la extensión intermedia superior L/L' será normal, pero L'/K no tiene por qué serlo.

2. Correspondencia y teorema de Galois

El teorema fundamental de la teoría de Galois establece una correspondencia entre las extensiones de cuerpos y los subgrupos del grupo de Galois asociado a dicha extensión. El teorema fue desarrollado por *Évariste Galois* (Bourg-la-Reine, 1811 - París, 1832) en el siglo XIX y es uno de los resultados fundamentales de la teoría que lleva su nombre.
Esta correspondencia entre los subcuerpos y los subgrupos permite estudiar las propiedades de las extensiones de cuerpos a través de la teoría de grupos. Además, el teorema de Galois proporciona un criterio para determinar si una extensión de cuerpos es "resoluble" o "no resoluble" por radicales, lo que tiene implicaciones importantes en la resolubilidad de ecuaciones polinómicas.

Esta información ha sido tomada de las referencias [[4]] y [[11]].
Se da comienzo a esta sección dando una definición que permite entrar en materia.

Definición 2.1. Una extensión de cuerpos finita L/K se dice que es *de Galois* o *galoisiana* si es normal y separable.
Si L/K es una extension galoisiana, su grupo de automorfismos, $G = Gal(L/K)$ (es decir, el grupo de automorfismos de L que deja invariantes todos los elementos de K), llamado grupo de Galois de la extensión, tiene orden $m = [L : K]$.

Un grupo G puede tener subgrupos S, (es decir, grupos intermedios entre el trivial y G) de los cuales algunos pueden ser subgrupos normales. Un subrgupo S de G se dice normal cuando el cociente G/S está bien definido y es también un grupo. Esto es equivalente a decir que para todo $h \in G$ se tiene que $h^{-1}Sh = S$.
En el caso de los cuerpos ocurre una cosa similar. Una extensión L/K de Galois puede tener subextensiones L'/K, algunas de las cuales pueden ser también de Galois. En realidad, basta que dichas subextensiones sean normales, pues según lo comentado al final de la sección [1.2], si una extensión es separable, todas sus subextensiones lo son.

El teorema de Galois muestra que estos dos casos, que en principio parecerían similares pero no idénticos, relativos a la teoría de grupos y la teoría de cuerpos respectivamente, son realmente dos caras de la misma moneda.

Dentro de este escenario se tiene también la denominada *correspondencia de Galois*, la cual se explica a continuación:

Dada una extensión finita L/K, cuyo grupo de Galois denotamos por $G = Gal(L/K)$, la correspondencia de Galois asocia a cada extensión intermedia L' un subgrupo $S(L') \subset G$ que viene dado por

$$S(L') = \{g \in G \text{ tal que } g(x) = x \text{ para todo } x \text{ en } L'\}$$

De forma recíproca, cada subgrupo $S \subset G$ tiene asociado un cuerpo intermedio dado por

$$F(S) = \{x \in L \text{ tal que } g(x) = x \text{ para todo } g \text{ en } S\}$$

De esta forma podemos enunciar el teorema central de la teoría de Galois. Este teorema es también parte del curso en *Ecuaciones algebraicas*, sin embargo, dado que se considera un resultado central y de gran relevancia para lo que este trabajo pretende abarcar, se presenta a continuación una de las varias demostraciones que existen.

Teorema 2.1. ***(de Galois)*** *Sea L/K una extensión de Galois y G su grupo de Galois. Entonces, la correspondencia de Galois descrita anteriormente,*

$$\{\textit{subcuerpos intermedios entre } L \textit{ y } K\} \longleftrightarrow \{\textit{subgrupos de } G\}$$

es biunívoca e invierte el orden de contención conjuntista. Además se cumple lo siguiente:

1. *F(S(L'))=L', para todo cuerpo intermedio L'.*
2. *S(F(S))=S, para todo subgrupo $S \in G$.*
3. *L'/K es una extensión normal si y sólo si el subgrupo $S(L')$ de G es normal. De ser así, existe un isomorfismo entre el grupo de Galois de L'/K y el grupo cociente $G/S(L')$.*

Demostración. A partir de cómo se ha definido el conjunto $S(L')$, se prueba que este es un subrgupo de G, para cada cuerpo intermedio $L' \subset L$. De forma análoga, pero con la definición de $F(S)$ se deduce que este es un subcuerpo de L, para cada grupo $S \subset G$.
De la misma forma se prueba además que $L' \subset F(S(L'))$ para todo $L' \subset L$, y que $S \subset S(F(S))$ para todo $S \subset G$.

Primero de todo se comenzará probando la primera afirmación del teorema:
Para ello, se tomará un elemento $x \in L$, tal que $x \notin L'$. Este elemento x es raíz de un polinomio irreducible $f(t)$ de $L'[t]$ de grado mayor que 1. Se sabe que la extensión L/L' es separable y normal, por lo tanto $f(t)$ tendrá otra raíz y en L, con $y \neq x$. A partir de esta raíz puede definirse el isomorfismo

$$g' : L'(x) \longrightarrow L'(y), \text{ tal que } g'(x) = y$$

y deja invariantes los elementos de L'.
Observemos que $L/L'(x)$ y $L/L'(y)$ son ambas extensiones normales. Entonces el isomorfismo anterior, g', puede extenderse de forma natural al automorfismo $g : L \longrightarrow L$, que pertenece al grupo $S(L')$.
Del hecho de que $g(x) = y$ se sigue que $x \notin F(S(L'))$ y, por lo tanto, $F(S(L')) \subset L'$. Así se consigue la doble inclusión y $F(S(L')) = L'$.

Probar 2. es algo más complicado y debe realizarse la prueba en tres etapas distintas.

De esta demostración de la primera afirmación se deduce que la correspondencia S es inyectiva. Entonces, al haber sólo una cantidad finita de subgrupos de G, se deduce que sólo existe una cantidad finita de cuerpos intermedios de entre L y K. Esto permite demostrar que para cualquier cuerpo intermedio L', se puede tomar un elemento $x \in L$ tal

que $L = L'(x)$.
Esto se prueba de la siguiente forma: Tomemos $x \in L$ tal que el grado de la extensión $[L'(x) : L']$ sea máximo, y razonemos por reducción al absurdo suponiendo que $L'(x) \neq L$. Entonces, existe un elemento $z \in L$, tal que $z \notin L'(x)$. Se considera ahora todos los cuerpos intermedios de la forma $L'(x + cz)$, cuando c recorre todos los elementos de L'. Como L' es un cuerpo infinito y sólo existe una cantidad finita de cuerpos intermedios, existen dos elementos c, c' distintos tales que $L'(x + cz) = L'(x + c'z) = L''$. Esto implica que ambos elementos x y z pertenecen al cuerpo L'', y por lo tanto

$$[L'' : L'] \geq [L'(x, z) : L'] > [L'(x) : L']$$

Esta última afirmación entra en contradicción con el hecho de que se ha tomado x tal que $[L'(x) : L']$ fuera máximo, y por lo tanto z no puede existir.
Además, si L' es finito, entonces también lo es L, por lo que el grupo de sus unidades, L^*, es cíclico. De aquí se deduce que $L'(x) = L$, como se quería demostrar.

Vamos ahora con la segunda etapa. Se quiere probar que

$$|S| \geq [L : F(S)]$$

para cualquier subrgupo $S \subset G$.
Sea x un elemento de L, que se elige como en el apartado anterior. Entonces, $L = F(S(x))$. Se consideran ahora los dos polinomios siguientes:

1. El polinomio $q(t)$ de $L[t]$, dado como el producto

$$q(t) = \prod_{g \in S} (t - g(x))$$

2. El polinomio irreducible de x $p(t)$ sobre $F(S)$.

Observemos que el grado de $q(t)$ es exactamente $|S|$ y que tiene por raíz el elemento x. Por otro lado, el grado de $p(t)$ es $[L : F(S)]$.
Ahora, como para todo $h \in S$, cuando g recorre S se tiene que el producto $h \cdot g$ recorre S también, se tiene que

$$q(t) = \prod_{h \in S} (t - h(g(x)))$$

De aquí se sigue que $q(t)$ tiene sus coeficientes en el cuerpo $F(S(L'))$, ya que dichos coeficientes satisfacen que $h(c) = c$, para todo $h \in S$.
Como $q(t) \in F(S(L'))[t]$, y tiene a x como ráiz, el grado de $q(t)$ tiene que ser mayor que el grado de $p(t)$. Como el grado de $q(t)$ es $|S|$ y el grado de $p(t)$ es $[L : F(S)]$, se concluye lo que se quería demostrar.

Con todos estos resultados intermedios ya se está en condiciones de probar la segunda afirmación del teorema. Consideremos $S \in G$.
Por un lado, se tiene que

$S(F(S)) = Gal(L/F(S))$, lo que implica que $|S| \leq |S(F(S))| = [L : F(S)]$. Como ya se había probado en la etapa anterior la desigualdad contraria, se da la igualdad.
Por otro lado, $S \subset S(F(S))$. Y de aquí se puede concluir que

$$S = S(F(S))$$

Sólo resta por probar el tercer punto del teorema. Se quiere demostrar que L'/K es normal (y por lo tanto de Galois) si y sólo si su grupo asociado a través de la correspondencia de Galois, $S = S(L')$, es un subgrupo normal de G.

- $\Longrightarrow$) Si L'/K es de Galois, y por lo tanto normal, dado un automorfismo $h \in G$, $h(L') = L'$..
  Como para todo $g \in S(L)$, se cumple que $g(x) = x$, para $x \in L'$, se tendrá también que
  $$(h^{-1}(g(h(x)))) = x$$
  Luego, $h^{-1} \cdot g \cdot h \in S(L')$, para todo $h \in G$ y todo $g \in S(L')$; y en conclusión, $S(L')$ es un subgrupo normal de G.

- $\Longleftarrow$) Sea $S(L')$ es un subgrupo normal. Se consideran $\bar{K}$ clausura algebraica de L, y las inmersiones $h' : L' \longrightarrow \bar{K}$. Estas inmersiones pueden considerarse como restricciones a L' de las inmersiones $h : L \longrightarrow \bar{K}$. Entonces basta ver que dados $h \in G$ y $x \in L'$, entonces $h(x) \in L'$ para concluir que $h'(x) \in L'$; y que en efecto, $h'(L') = L'$.
  Por definición de $S(L')$ basta ver que $g(h(x)) = h(x)$ o lo que es igual, que $(h^{-1}(g(h(x)))) = x$, para todo $g \in S(L')$. Esto es directo del hecho de que $S(L')$ es normal, y entonces $h^{-1}(g(h)) \in S(L')$.

Además, se deduce que si $S(L')$ es un grupo normal y se considera el grupo cociente $G/S(L')$. Si se toman dos automorfismos de G y se considera su restricción a L', entonces su clase en el grupo cociente es la misma. Esto significa que $G/S(L')$ se identifica mediante un isomorfismo con el grupo $Gal(L'/K)$. Así queda concluida la prueba del teorema de Galois.

■

3. Cuerpos de números algebraicos

La teoría de números algebraicos o teoría algebraica de números es una rama de la teoría de números en la cual el concepto de número se expande a los números algebraicos, los cuales son las raíces de los polinomios con coeficientes racionales. Para el estudio de las siguientes secciones se han utilizado las referencias [[1]],[[2]], [[6]],[[7]], [[8]],[[9]],[[12]] y [[13]] principalmente.

Como ya se ha dicho, un cuerpo de números K es una extensión finita del cuerpo de los números racionales $\mathbb{Q}$. En los problemas de teoría de números, además de estudiarse el anillo de los números enteros $\mathbb{Z}$, se considera un subanillo θ_K dentro de cada cuerpo K tal que $K/\mathbb{Q}$ sea una extensión finita. Esto tiene ciertas similitudes con el papel que juega $\mathbb{Z}$ dentro de $\mathbb{Q}$; es decir, se puede ver, y tratar, a un cuerpo de números algebraico como un análogo del cuerpo $\mathbb{Q}$, y a su anillo de enteros como un análogo de $\mathbb{Z}$. Ahora bien, la analogía no es perfecta del todo: algunas de las propiedades familiares de los racionales y los enteros no se conservan, por ejemplo, la factorización única en potencias de elementos irreducible.
Comenzamos entonces con las definiciones precisas:

Definición 3.1. Se denomina cuerpo de números, o cuerpo de números algebraico, a una extensión $K/\mathbb{Q}$ tal que $[K : \mathbb{Q}] < \infty$.

Cuando se tiene que $[K : \mathbb{Q}] = 2$ se dice que K es un cuerpo cuadrático; cuando $[K : Q] = 3$, K es un cuerpo cúbico, y así sucesivamente.

Pongamos algunos ejemplos de estos cuerpos. Uno de los casos más conocidos se lo debemos al prolífico matemático *Johann Carl Friedrich Gauss* (Braunschweig, 1777 - Gotinga, 1855).

Ejemplo 3.1. *Números racionales de Gauss:*
Los números racionales de Gauss, que comunmente se denotan por $\mathbb{Q}(i)$, está formado por los elementos de la forma

$$a + bi$$

donde $a, b \in \mathbb{Q}$, e i es la unidad imaginaria.
Se puede comprobar fácilmente que los racionales de Gauss forman un cuerpo que es bidimensional como espacio vectorial sobre $\mathbb{Q}$; es decir, que $[\mathbb{Q}(i) : \mathbb{Q}] = 2$. Además su anillo de enteros $\theta_{\mathbb{Q}(i)}$ es el de los enteros de Gauss $\mathbb{Z}[i]$; es decir, aquellos elementos $a + bi$ tales que $a, b \in \mathbb{Z}$.

Ejemplo 3.2. De forma general, dado cualquier número entero d, $\mathbb{Q}(\sqrt{d})$ es también un cuerpo de números algebraicos, y se tienen que $[\mathbb{Q}(\sqrt{d}) : \mathbb{Q}] = 2$ si d no es un cuadrado.

Ejemplo 3.3. Como último ejemplo puede considerarse el caso de los cuerpos ciclotómicos, que son los dados por $\mathbb{Q}(z)$, donde z es una raíz primitiva n-ésima de la unidad.
Estos cuerpos serán estudiados en profundidad más adelante a lo largo de este trabajo pues poseen propiedades muy interesantes.

Observación 4. Observemos que tanto $\mathbb{R}$ como $\mathbb{C}$ tienen dimensión infinita como espacios vectoriales sobre $\mathbb{Q}$ y por lo tanto no cumplen la definición de cuerpo de números.

3.1. Elementos enteros sobre un anillo A

Aun que todos los resultados que se van a dar a continuación se enunciar en términos de cuerpos, anillos y módulos arbitrarios, nuestro interés se restringe al estudio de $\mathbb{Q}$, los cuerpos de números algebraicos, y el anillo $\mathbb{Z}$. Además todos estos resultados se dan en términos de un anillo B que contiene a A, lo cual puede particularizarse para el caso en el que se tenga un cuerpo de números, es decir, en el caso de una extensión $L/\mathbb{Q}$ finita.

Teorema 3.1. *Sea B un anillo que contiene como subanillo a un anillo A y x un elemento de B. Los siguientes enunciados son equivalentes:*

1. *Existen $a_0, a_1, ..., a_{n-1} \in A$ tales que*

$$x^n + a_{n-1}x^{n-1} + ... + a_1x + a_0 = 0$$

   Es decir, x es raíz de un polinomio mónico con coeficientes en A.

2. *El anillo $A[x]$ es un A-módulo de tipo finito.*

3. *Existe un subanillo A' de B, que contiene a A y a x, tal que es un A-módulo de tipo finito.*

Demostración. Sea M el A-submódulo de B generado por los elementos $1, x, ..., x^{n-1}$. Por 1), $x^n \in M$.
Si se multiplica $x^n + a_{n-1}x^{n-1} + ... + a_1x + a_0$ por x^j, se obtiene

$$x^{n+j} = -a_{n-1}x^{n+j-1} - ... - a_0x^j$$

De hecho, por inducción sobre j se prueba que $x^{n+j} \in M$, para todo $j \geq 0$.
Como $A[x]$ es el A-módulo generado por los x^k, con $k \geq 0$, se tiene que $A[x] = M$.
Por lo tanto, 1) $\Longrightarrow$ 2) $\Longrightarrow$ 3).

Veamos ahora que 3) $\Longrightarrow$ 1). Sea $\{y_1, y_2, ..., y_n\}$ un conjunto de generadores finito de A' como módulo sobre A; es decir,

$$A' = Ay_1 + Ay_2 + .. + Ay_n$$

Como $x \in A'$ y como además A' es un subanillo de B, se sigue que $xy_i \in A'$ para todo $i \in \{1, ..., n\}$. Por lo tanto,

$$xy_i = \sum_{j=1}^{n} a_{ij}y_j, \text{ para cualquier } i \in \{1, ..., n\}, a_{ij} \in \mathbb{Z}, 1 \leq i, j \leq n.$$

Esto implica que

$$\sum_{j=1}^{n}(\delta_{ij}x - a_{ij})y_j = 0, \quad i \in \{1, ..., n\},$$

donde δ_{ij} es la *Delta de Kroenecker.*
Consideremos entonces este sistema de n ecuaciones lineales homogéneas en las variables $\{y_1, ..., y_n\}$. Llamemos d al determinante $det(\delta_{ij}x - a_{ij})$. Por la *regla de Cramer*, se tiene que $dy_i = 0$, para todo i. Esto significa que $db = 0$, para todo $b \in A'$; y en particular, $d1 = 0$, por lo que $d = 0$.
Sin embargo es evidente que d es un polinomio mónico en la variable x, ya que el término de mayor orden aparece en la expansión del producto $\prod_{i=1}^{n}(x - a_{ij})$ de los elementos de la diagonal principal.
Luego 3) $\Longrightarrow$ 1).

■

Este teorema es de gran importancia ya que permite definir los elementos que son enteros en un anillo B sobre A dando diferentes definiciones.

Definición 3.2. Sea B un anillo que contiene al anillo A como subanillo. Un elemento x de B se dice que es un elemento entero sobre A si satisface las condiciones equivalentes 1), 2) y 3) dadas en el teorema 3.1.
Sea $p \in A[X]$ un polinomio mónico tal que $p(x) = 0$. La relación $p(x) = 0$ se denomina equación de dependencia entera de x en A.

Ejemplo 3.4. El elemento $x = \sqrt{2}$ de $\mathbb{R}$ es un elemento entero sobre el anillo $\mathbb{Z}$; y la relación $x^2 - 2 = 0$ es su ecuación de dependencia entera.

Proposición 3.1. *Sea B un anillo que contiene al anillo A como subanillo y $\{x_i\}_{1\leq i\leq n}$ un conjunto finito de elementos de B. Si, para todo i, x_i es entero sobre $A[x_1, ..., x_{i-1}]$ (en particular si todos los elementos x_i son enteros sobre A), entonces $A[x_1, ..., x_n]$ es un A-módulo de tipo finito.*

Demostración. Se razona por inducción sobre n.
Para $n = 1$, supongamos que $A' = A[x_1, ..., x_{n-1}]$ es un A-módulo de tipo finito. Entonces $A' = \sum_{j=1}^{p} Ab_j$. El caso $n = 1$, implica que $A[x_1, ..., x_n] = A'[x_n]$ es un A'-módulo de tipo finito. Escribamos $A'[x_n] = \sum_{k=1}^{q} A'c_k$, entonces:

$$A[x_1, ..., x_n] = \sum_{k=1}^{q} A'c_k = \sum_{k=1}^{q}\left(\sum_{j=1}^{p} Ab_j\right)c_k = \sum_{j,k} Ab_jc_k$$

Por lo tanto, $\{b_jc_j\}_{1\leq j\leq p, 1\leq k\leq q}$ es un conjunto finito de generadores para $A[x_1, ..., x_n]$ como módulo sobre A.

■

Estos resultados permiten sacar ciertas conclusiones acerca de los elementos enteros sobre A.

Corolario 3.1. *Sea B un anillo que contiene al anillo A como subanillo y x e y elementos de B que son enteros sobre A. Entonces x+y, x-y, y xy son enteros sobre A también.*

Demostración. Es claro que $x+y,\ x-y,\ xy \in A[x,y]$. De acuerdo con la proposición 3.1, $A[x,y]$ es un A-módulo de tipo finito. Además, en virtud del punto 3) del teorema 3.1, $x+y, x-y, xy$ son enteros sobre A.

■

Ahora ya se está en condiciones de probar que los elementos enteros sobre el anillo de los números enteros forman ellos mismos otro anillo.

Corolario 3.2. *Sea B un anillo que contiene a A como subanillo. Sea $\theta_{B/A}$ el conjunto formado por los elementos de B que son enteros sobre A. Entonces $\theta_{B/A}$ es un subanillo de B que contiene a A.*

Demostración. El corolario 3.1 implica que θ_B es un subanillo de B. Además, si $a \in A$, entonces a es raíz del polinomio mónico $p(X) = X - a$, cuyos coeficientes están en A. Luego, $A \subset \theta_B$.

■

Entonces depués de esto se sabe que el conjunto

$$\theta_{B/A} = \{b \in B |\ \text{b es entero sobre } A\}$$

donde $A \subset B$, forma un anillo. A este conjunto se le llama la *clausura entera* de A en B. Si $\theta_{B/A} = A$ se dice que A es *enteramente cerrado*. Es inmediato por definición que la clausura entera $\theta_{B/A}$ es enteramente cerrada sobre B.

Como se ha comentado antes, estos resultados pueden enunciarse en términos de anillos, subanillos, módulos y cuerpos arbitrarios. Nuestro estudio se centra en el caso de elementos enteros de un cuerpo de números sobre $\mathbb{Z}$, es decir, elementos de una extensión $L/\mathbb{Q}$ finita, tales que son raíz de un polinomio mónico de $\mathbb{Z}[t]$.

Observación 5. El anillo de enteros θ_L de un cuerpo de números L, tal que $[L:\mathbb{Q}] = n$ es un $\mathbb{Z}$-módulo libre de rango n; es decir, existen bases $u_1, ..., u_n$ de θ_L de dicho módulo. Esto significa que todo elemento $x \in \theta_L$ puede escribirse de forma única como

$$x = a_1u_1 + ... + a_nu_n$$

con $a_1, ..., a_n \in \mathbb{Z}$.

Además, si $v_1, ...v_n$ es otra base de θ_L como $\mathbb{Z}$-módulo, entonces

$$\begin{pmatrix} v_1 \\ v_2 \\ \vdots \\ v_n \end{pmatrix} = P \begin{pmatrix} u_1 \\ u_2 \\ \vdots \\ u_n \end{pmatrix}$$

donde P es la matriz de cambio entre las dos bases en θ_L, que es una matriz cuadrada con coeficientes en $\mathbb{Z}$ y tal que $det(P) = \pm 1$.

3.2. Ramificación de números primos

En teoría de números, específicamente en el estudio de extensiones de cuerpos y números algebraicos, la ramificación se refiere a cómo los números primos se comportan al descomponerse en extensiones de cuerpos. Cuando consideramos una extensión de un cuerpo, por ejemplo, un cuerpo de números algebraicos, los números primos pueden comportarse de diferentes maneras al factorizarse en esa extensión.

En un cuerpo de números $L/\mathbb{Q}$, el anillo de enteros θ_L juega un papel muy similar al que juega $\mathbb{Z}$ en $\mathbb{Q}$. Como en $\mathbb{Z}$, todo elemento $a \in \theta_L$ que no sea una unidad, puede descomponerse en un producto de elementos irreducibles. Esto es, si a no es un elemento irreducible, puede escribirse como producto de dos elementos $b, c \in \theta_L$ tal que ninguna de ellas es una unidad tampoco: $a = b \cdot c$. La descomposición en factores primos de a se obtiene por recurrencia de las descomposiciones de b y c. Sin embargo, a diferencia de lo que ocurre en $\mathbb{Z}$ esta descomposición puede no ser única. Este fallo en la falta de unicidad de la descomposición es lo que llevó a los matemáticos *Ernst Kummer* (Sorau, 1810 - Berlin, 1893) y *Richard Dedekind* (Brunswick, 1831- Brunswick, 1916) a desarrollar el estudio de los ideales de un anillo. Vayamos primero con la siguiente definición.

Definición 3.3. Dado un anillo conmutativo A, se dice que este es *noetheriano* si todo ideal de A es finitamente generado.

Esta es una de las muchas caracterizaciones que reciben los anillos noetherianos, que deben su nombre a la ilustre matemática *Emmy Noether* (Erlangen, 1882 - Bryn Mawr, 1935).

Recordemos que un ideal $\mathfrak{p}$ de un anillo A es primo si para $a, b \in A$ el hecho de que $a \cdot b \in \mathfrak{p}$ implica que $a \in \mathfrak{p}$ ó $b \in \mathfrak{p}$. Si el anillo es un dominio de factorización única, los ideales principales (p) que son primos son aquellos tales que el elemento que los genera p es irreducible.

En esta sección entonces se va a estudiar el caso de un cuerpo de números K y su anillo de enteros θ_K, y una extensión L de K tal que $[L : K] = n$ y su anillo de enteros θ_L. Ambos anillos θ_K y θ_L son anillos de Dedekind, como se verá más adelante. Es evidente entonces que $\theta_L \subset \theta_K$.

Comencemos con el siguiente teorema.

Teorema 3.2. *Dado un cuerpo de números $L/\mathbb{Q}$, su anillo de enteros θ_L es un anillo noetheriano, enteramente cerrado y todo ideal primo $\mathfrak{p} \neq 0$ en él es maximal.*

Demostración. Que θ_L sea noetheriano se deduce del hecho de que todo ideal $\mathfrak{a}$ de θ_L es un $\mathbb{Z}$-módulo, y entonces implica que también es finitamente generado como θ_L módulo. Esta afirmación se comenta previamente en la observación 5 de la sección [3.1] y se prueba más tarde, tras introducir el concepto de discriminante en la proposición 4.8 de la sección [4.3].

También se ha visto en la sección [3.1] dedicada al estudio de los elementos que son enteros sobre un anillo, que por definición θ_L es enteramente cerrado, por ser la clausura entera del anillo $\mathbb{Z}$ en L.

Por lo tanto, solo resta demostrar que cada ideal primo $\mathfrak{p} \neq 0$ es maximal. Veamos que la intersección $\mathfrak{p} \cap \mathbb{Z}$ es justamente un ideal primo (p) de $\mathbb{Z}$. Que es primo se demuestra fácilmente teniendo en cuenta que si se toma un elemento $y \in \mathfrak{p}$ tal que $y \neq 0$ y se tiene la ecuación

$$y^n + a_1 y^{n-1} + ... + a_n = 0$$

con $a_i \in \mathbb{Z}$, para todo i y $a_n \neq 0$, entonces $a_n \in \mathfrak{p} \cap \mathbb{Z}$.
Por otro lado, el dominio de integridad $\mathcal{O} = \theta_L/\mathfrak{p}$ se genera a partir de $(\mathbb{Z}/p\mathbb{Z})$ agregándole a este elementos algebraicos, y por lo tanto se tiene que es nuevamente un cuerpo (recordemos que $K[x] = K(x)$ si x es algebraico). Se concluye entonces que $\mathfrak{p}$ es un ideal maximal.

■

Estas tres propiedades que acabamos de enunciar para los anillos de enteros de un cuerpo de números son el fundamento del estudio de la divisibilidad de sus ideales.

Definición 3.4. Se denomina *anillo o dominio de Dedekind* a todo dominio de integridad que sea noetheriano, enteramente cerrado y en el que todo ideal primo no nulo es maximal.

Esto quiere decir que, en particular, todo anillo de enteros de un cuerpo de números es un dominio de Dedekind.

Observación 6. De la misma forma en la que se ha formulado la analogía entre θ_L y $\mathbb{Z}$ cuando L es un cuerpo de números, pueden considerarse también que los dominios de Dedekind son una generalización de los dominios de ideales principales.

Existe otra caracterización de los dominios de Dedekind más conocida, relativa a la factorización de ideales primos. Se demostrará a continuación que ambas son equivalentes.

Proposición 3.2. *Un anillo es un dominio de Dedekind si todo ideal propio no nulo se factoriza de forma única como producto de potencias de ideales primos.*

Antes de demostrar esta proposición veamos un poco más acerca de ideales. Consideremos un dominio de Dedekind arbitrario A y dos ideales de este $\mathfrak{a}, \mathfrak{b}$. Se dice que el ideal $\mathfrak{a}$ divide al ideal $\mathfrak{b}$, $\mathfrak{a}|\mathfrak{b}$, si se tiene que $\mathfrak{b} \subseteq \mathfrak{a}$.
A su vez, se define la suma de ideales como

$$\mathfrak{a} + \mathfrak{b} = \{a + b \quad | \quad a \in \mathfrak{a}, b \in \mathfrak{b}\}$$

Se define el producto de ideales como

$$\mathfrak{ab} = \{\sum_i a_i b_i \quad | \quad a_i \in \mathfrak{a}, b_i \in \mathfrak{b}\}$$

Para poder probar la proposición 3.2 se necesitan unos lemas previos. Consideremos ahora un dominio de Dedekind A y K su cuerpo de fracciones.

Lema 3.1. *Para todo ideal* $\mathfrak{a}$ *no nulo de un dominio de Dedekind A existen ideales primos no nulos* $\mathfrak{p}_1, ..., \mathfrak{p}_r$ *tales que*

$$\mathfrak{a} \supseteq \mathfrak{p}_1 \dots \mathfrak{p}_r$$

Demostración. Supongamos que el conjunto M de los ideales que no cumplen la condición anterior es no vacío. Una de las múltiples caracterizaciones de los anillos noetherianos es que toda sucesión creciente para el orden de inclusión en ellos es estacionaria. Por lo tanto para A se da esta condición. Por lo tanto, M posee una relación de orden dada por la relación de inclusión y posee un elemento maximal $\mathfrak{a}$. Este elemento maximal no puede ser un ideal primo por lo que deben existir $b_1, b_2 \in A$ tales que $b_1 b_2 \in \mathfrak{a}$ pero $b_1, b_2 \notin \mathfrak{a}$. Sean $\mathfrak{a}_1 = (b_1) + \mathfrak{a}$ y $\mathfrak{a}_2 = (b_2) + \mathfrak{a}$. Entonces $\mathfrak{a}_1 \subset \mathfrak{a}$, $\mathfrak{a}_2 \subset \mathfrak{a}$ y $\mathfrak{a}_1 \mathfrak{a}_2 \subset \mathfrak{a}$. Por ser $\mathfrak{a}$ maximal, tanto $\mathfrak{a}_1$ como $\mathfrak{a}_2$ deben contener un producto de ideales primos, y el producto de esos dos productos estará contenido en $\mathfrak{a}$, llegando así a una contradicción.

■

Lema 3.2. *Sea* $\mathfrak{p}$ *un ideal no nulo del dominio de Dedekind A. Se define*

$$\mathfrak{p}^{-1} = \{x \in K \quad | \quad x\mathfrak{p} \subset A\}$$

Entonces $\mathfrak{a}\mathfrak{p}^{-1} = \{\sum_i a_i x_i \quad | \quad a_i \in \mathfrak{a}, x_i \in \mathfrak{p}^{-1}\} \neq \mathfrak{a}$*, para todo ideal* $\mathfrak{a} \neq 0$*.*

Demostración. Sea $a \in \mathfrak{p}$, $a \neq 0$ y $\mathfrak{p}_1 \mathfrak{p}_2 \dots \mathfrak{p}_r \subseteq (a) \subseteq \mathfrak{p}$, para el mínimo r posible. Entonces, uno de los $\mathfrak{p}_i$, digamos $\mathfrak{p}_1$ está contenido en $\mathfrak{p}$. Y como $\mathfrak{p}_1$ es un ideal maximal, entonces $\mathfrak{p}_1 = \mathfrak{p}$. Como $\mathfrak{p}_2 \dots \mathfrak{p}_r \not\subseteq (a)$, existe un $b \in \mathfrak{p}_2 \dots \mathfrak{p}_r$ tal que $b \notin aA$; es decir, $a^{-1}b \notin A$.
Por otro lado, se tiene que $b\mathfrak{p} \subseteq (a)$; es decir, $a^{-1}b\mathfrak{p} \subseteq A$, y $a^{-1}b \in \mathfrak{p}^{-1}$. De aquí se sigue que $\mathfrak{p}^{-1} \neq 0$.

Sea $\mathfrak{a}$ un ideal de A y $\{\alpha_1, ..., \alpha_n\}$ un sistema de generadores. Supongamos que $\mathfrak{a}\mathfrak{p}^{-1} = \mathfrak{a}$. Entonces para cada $x \in \mathfrak{p}^{-1}$,

$$x\alpha_i = \sum_j a_{ij}\alpha_j, \quad a_{ij} \in A$$

Llamando $\mathcal{M}$ a la matriz $(x\delta_{ij} - a_{ij})_{ij}$, se obtiene $\mathcal{M}(\alpha_1, ..., \alpha_n) = 0$ Esto significa que $det(\mathcal{M})\alpha_1 = ... = det(\mathcal{M})\alpha_n$, y entonces $det(\mathcal{M}) = 0$. Se tiene entonces que x es la raíz del polinomio $p(t) = det(t\delta_{ij} - a_{ij})$ de $A[t]$. Por lo tanto, x es entero sobre A y $x \in A$. Esto lleva a que $\mathfrak{p}^{-1} = A$, lo que es absurdo.

■

Ahora sí, vayamos con la demostración de la proposición 3.2, que permite definir los dominios de Dedekind de una manera muy concreta.

Demostración. (de la proposición 3.2)
Existencia:

Sea M el conjunto de todos los ideales distintos de (0) y (1) que no admiten una descomposición en producto de ideales primos. Si M es distinto del vacío, se puede razonar como

en la prueba del lema 3.1 y concluir que existe entonces un elemento maximal $\mathfrak{a}$ en M. Este está contenido en un ideal maximal $\mathfrak{p}$, y de la inclusión $A \subseteq \mathfrak{p}^{-1}$ se sigue que

$$\mathfrak{a} \subseteq \mathfrak{a}\mathfrak{p}^{-1} \subseteq \mathfrak{p}\mathfrak{p}^{-1} \subseteq A$$

Por el lema 3.2 se tiene que $\mathfrak{a} \subset \mathfrak{a}\mathfrak{p}^{-1}$ y que $\mathfrak{p} \subset \mathfrak{p}\mathfrak{p}^{-1} \subseteq A$. Como $\mathfrak{p}$ es maximal se tiene que $\mathfrak{p}\mathfrak{p}^{-1} = A$. En virtud de que $\mathfrak{a}$ es maximal en M y que $\mathfrak{a} \neq \mathfrak{p}$, entonces el ideal $\mathfrak{a}\mathfrak{p}^{-1}$ admite una factorización en producto de ideales primos, $\mathfrak{a}\mathfrak{p}^{-1} = \mathfrak{p}_1\mathfrak{p}_2 \dots \mathfrak{p}_r$. Sin embargo, notemos que $\mathfrak{a} = \mathfrak{a}\mathfrak{p}\mathfrak{p}^{-1} = \mathfrak{p}\mathfrak{p}_1 \dots \mathfrak{p}_r$, llegándose así a una contradicción.

Unicidad:

Sea $\mathfrak{a}$ un ideal de A tal que

$$a = \mathfrak{p}_1 \dots \mathfrak{p}_r = \mathfrak{q}_1 \dots \mathfrak{q}_s$$

Es decir, supongamos que existen dos factorizaciones distintas de $\mathfrak{a}$ como producto de ideales primos. Entonces, $\mathfrak{p}_1$ dividirá a uno de los factores $\mathfrak{q}_i$, digamos $\mathfrak{q}_1$. Como ambos son maximales, se tiene que $\mathfrak{p}_1 = \mathfrak{q}_1$. Multiplicando la expresión de $\mathfrak{a}$ por $\mathfrak{p}_1$, como $\mathfrak{p}_1 \neq \mathfrak{p}_1\mathfrak{p}_1^{-1} = A$, se tiene que

$$\mathfrak{p}_2\mathfrak{p}_3 \dots \mathfrak{p}_r = \mathfrak{q}_2\mathfrak{q}_3 \dots \mathfrak{q}_s$$

Por recurrencia se llega a que $r = s$, y tras reordenación a que $\mathfrak{p}_i = \mathfrak{q}_i$, para todo i.

■

Como hemos visto en el teorema 3.2, los anillos de enteros θ_L de cuerpos de números $L/\mathbb{Q}$ cumplen las condiciones de la definición 3.4. Por lo tanto, θ_L es un anillo de Dedekind y pueden aplicarse los lemas y proposiciones previos a este caso. Es decir, tenemos que todo ideal de θ_L puede descomponerse de forma única como producto de ideales primos.

Todo ideal $\mathfrak{p} \neq 0$ de θ_L contiene a un número primo p racional (se llaman así para diferenciarlos de los primos del cuerpo de los números racionales de Gauss), y es por lo tanto un divisor del ideal $p\theta_L$. Entonces la cuestión es estudiar cómo factoriza un número primo p en ideales primos de θ_L.

Veamos este problema desde un punto de vista más general. Tomemos un dominio de Dedekind A arbitrario en vez del anillo $\mathbb{Z}$ y en vez de θ_L la clausura entera $\tilde{A}$ de A en una extensión finita de su cuerpo de fracciones.

Proposición 3.3. *Sea A un dominio de Dedekind, cuyo cuerpo de fracciones es K. Sea L/K una extensión finita y separable de K y $\tilde{A}$ la clausura entera de A en L. Entonces, $\tilde{A}$ es también un dominio de Dedekind.*

Demostración. Tenemos que comprobar las tres condiciones que tiene que cumplir un anillo para poder ser considerado dominio de Dedekind. $\tilde{A}$ es de forma trivial enteramente cerrada por ser la clausura entera de A.

El hecho de que los ideales primos $\mathfrak{B}$ de $\tilde{A}$ son maximales se prueban de forma similar al caso en el que $A = \mathbb{Z}$: Sea $\mathfrak{p} = \mathfrak{B} \cap A$ un ideal primo no nulo de A. Entonces, el

dominio de integridad $\tilde{A}/\mathfrak{B}$ es una extensión del cuerpo $A/\mathfrak{p}$, y en conclusión es en sí mismo un cuerpo. Si no fuera así, $\tilde{A}/\mathfrak{B}$ admitiría un ideal primo no nulo cuya intersección con $A/\mathfrak{p}$ sería de nuevo un ideal primo no nulo de $A/\mathfrak{p}$.

Queda probar que $\tilde{A}$ es noetheriano. Para el caso que nos concierne, que es aquel en el que L/K es separable, la prueba es sencilla. Sea $x_1, ..., x_n$ una base de L/K contenida en $\tilde{A}$. Sabemos que el discriminante $d = D(x_1, ..., x_n)$ es no nulo y por el lema 4.3 de la sección [4.3] que $\tilde{A}$ está contenido en A-módulo finitamente generado, dado por $Ax_1/d + ... + Ax_n/d$. Cada ideal de $\tilde{A}$ está contenido en este A-módulo, y es cada uno de ellos entonces un A-módulo de tipo finito y en conclusión un $\tilde{A}$-módulo de tipo finito. Esto prueba que $\tilde{A}$ es noetheriano.

■

Observación 7. Para un ideal primo $\mathfrak{p}$ de A, siempre se tiene que $\mathfrak{p}\tilde{A} \neq \tilde{A}$. De hecho, sea $q \in \mathfrak{p} - \mathfrak{p}^2$, de tal forma que $qA = \mathfrak{p}\mathfrak{a}$, para un $\mathfrak{a}$ que no es divisible por $\mathfrak{p}$, entonces $\mathfrak{p} + \mathfrak{a} = A$. Tomemos $b \in \mathfrak{p}$, $s \in \mathfrak{a}$, tal que $1 = b + s$. Entonces se tiene que $s \notin \mathfrak{p}$ y $s\mathfrak{p} \subseteq \mathfrak{a}\mathfrak{p} \subset qA$.
Si se tuviera $p\tilde{A} = \tilde{A}$, se tendría que $s\tilde{A} = s\mathfrak{p}\tilde{A} \subseteq q\tilde{A}$, entonces $s = qx$ para algún $x \in \tilde{A} \cap K$.

Ahora, un ideal primo $\mathfrak{p}$ no nulo de A se descompone de forma única en $\tilde{A}$ de la siguiente forma:

$$\mathfrak{p}\tilde{A} = \prod_{i=1}^{r} \mathfrak{B}_i^{e_i} \tag{1}$$

Veamos que en estas condiciones se tiene que si $\mathfrak{p}$ es un ideal primo no nulo de A el número de ideales primos que aparecen en la factorización única del ideal $\mathfrak{p}\tilde{A}$ del anillo $\tilde{A}$, son los ideales primos de $\tilde{A}$ asociados a $\mathfrak{p}$.

Proposición 3.4. *Los $\mathfrak{B}_i$ definidos como antes son precisamente aquellos ideales primos $\mathfrak{B}$ de $\tilde{A}$ tales que*

$$\mathfrak{B} \cap A = \mathfrak{p}$$

Demostración. Para un ideal primo $\mathfrak{B}$ de $\tilde{A}$, la relación $\mathfrak{B} \cap A = \mathfrak{p}$ es equivalente a la relación de inclusión $\mathfrak{B} \supset \mathfrak{p}\tilde{A}$. Probemos esta equivalencia:

$\Longrightarrow$) Es evidente

$\Longleftarrow$) Se sigue de que $\mathfrak{B} \cap A$ es un ideal primo de A y $\mathfrak{p}$ es maximal.

Es claro que $\mathfrak{p}\tilde{A} = \prod_{i=1}^{r} \mathfrak{B}_i^{e_i}$ implica que $\mathfrak{p}\tilde{A} \subset \mathfrak{B}_i$ para cada $i = 1, ..., r.$. Por lo tanto $\mathfrak{B}_i$ aparece en la expresión como producto de $\mathfrak{p}\tilde{A}$ si y sólo si $\mathfrak{B}_i \cap A = \mathfrak{p}$.

■

Nota. Se utilizará la notación $\mathfrak{B}|\mathfrak{p}$ en el caso en el que $\mathfrak{B}$ sea un divisor primo de $\mathfrak{p}$.

Observación 8. Observemos que la proposición anterior permite entonces identificar $A/\mathfrak{p}$ con un subanillo de $\tilde{A}/\mathfrak{B}_i$ para cualquier $i = 1, ..., r$.. Además, tanto $\mathfrak{p}$ como $\mathfrak{B}_i$ son ideales maximales de A y $\tilde{A}$ respectivamente. Esto implica que ambos anillos $A/\mathfrak{p}$ y $\tilde{A}/\mathfrak{B}_i$ son cuerpos; el segundo una extensión del primero.
También como $\tilde{A}$ es un A-módulo de tipo finito entonces $\tilde{A}/\mathfrak{B}_i$ es una extensión finita sobre $A/\mathfrak{p}$.

Observación 9. De la proposición anterior también se deduce que como en particular $\mathfrak{p}\tilde{A} \cap A = \mathfrak{p}$, entonces $\tilde{A}/\mathfrak{p}\tilde{A}$ es también un espacio vectorial de dimensión finita de $A/\mathfrak{p}$.

Definición 3.5. Sea A un dominio de Dedekind, $\tilde{A}$ su clausura entera en una extensión finita de su cuerpo de fracciones. Sea $\mathfrak{p} \neq 0$ un ideal primo no nulo de A cuya descomposición viene dada por la ecuación (1). Entonces, los exponentes enteros e_i se denominan *índices de ramificación*. El grado de la extensión

$$f_i = [\tilde{A}/\mathfrak{B}_i : A/\mathfrak{p}]$$

se llama *grado residual o grado de inercia* de $\mathfrak{B}_i$ sobre $\mathfrak{p}$.

Si consideramos el caso para una extensión L/K separable tal que $[L : K] = n$, los enteros e_i, f_i y n cumplen la siguiente relación.

Proposición 3.5. *Consideremos las condiciones mencionadas previamente. Entonces*

$$\sum_{i=1}^{r} e_i f_i = n \tag{2}$$

Se omite la prueba de esta proposición pues carece de suficiente interés para este trabajo, aun que sin embargo, el resultado se utiliza para probar otras cosas.

Consideremos ahora el caso en el que tenemos una extensión L/K separable, generada por un elemento primitivo $\alpha \in \tilde{A}$, cuyo polinomio irreducible es $p(t) \in A[t]$. Veamos ahora un resultado sobre la descomposición sobre $\tilde{A}$ de los ideales $\mathfrak{p} \in A$.

Definición 3.6. Se define el *conductor* como el mayor ideal $\mathfrak{F}$ de $\tilde{A}$ contenido en $A[\alpha]$. Es decir,

$$\mathfrak{F} = \{a \in \tilde{A} \quad | \quad a\tilde{A} \subseteq A[\alpha]\}$$

Observación 10. Como $\tilde{A}$ es un A-módulo finitamente generado, se tiene que $\mathfrak{F} \neq 0$.

Proposición 3.6. *Sea $\mathfrak{p}$ un ideal primo de un dominio de Dedekind A, que es relativamente primo al conductor $\mathfrak{F}$ de $A[\alpha]$, y sea*

$$\bar{p}(t) = \bar{p_1}(t)^{e_1} \dots \bar{p_r}(t)^{e_r}$$

la factorización del polinomio $\bar{p}(t) = p(t)$ mod $\mathfrak{p}$ en factores irreducibles $\bar{p_i}(t) = p_i(t)$ mod $\mathfrak{p}$ sobre el cuerpo $A/\mathfrak{p}$, con $p_i(t) \in A[t]$ mónicos. Entonces

$$\mathfrak{B}_i = \mathfrak{p}\tilde{A} + p_i(\alpha)\tilde{A}, \quad i = 1, ..., r$$

son los diferentes ideales primos de $\tilde{A}$ sobre $\mathfrak{p}$. El grado residual f_i de $\mathfrak{B}_i$ es el grado de $\bar{p}_i(t)$, y se tiene

$$\mathfrak{p} = \mathfrak{B}_1^{e_1} \dots \mathfrak{B}_r^{e_r}$$

Demostración. Escribamos $A' = A[\alpha]$ y $R = A/\mathfrak{p}$. Se tiene el siguiente isomorfismo canónico

$$\tilde{A}/\mathfrak{p}\tilde{A} \simeq A'/\mathfrak{p}A' \simeq R[t]/(\bar{p}(t))$$

El primer isomorfismo se debe a la condición de ser primos relativos los ideales $\mathfrak{p}\tilde{A}+\mathfrak{F} = A$. Como $\mathfrak{F} \subseteq A'$, se tiene que $\tilde{A} = \mathfrak{p}\tilde{A} + A'$, es decir, el homorfismo $A' \longrightarrow \tilde{A}/p\tilde{A}$ es sobreyectivo. Su núcleo es $\mathfrak{p}\tilde{A} \cap A'$, que es igual a $\mathfrak{p}A'$. Como $\mathfrak{p}$ y $\mathfrak{F} \cap \tilde{A}$ son primos entre sí, $\mathfrak{p}\tilde{A} \cap A' = (\mathfrak{p} + \mathfrak{F})(\mathfrak{p}\tilde{A} \cap A') \subseteq \mathfrak{p}A'$.

El segundo isomorfismo se deduce del homomorfismo sobreyectivo $A[t] \longrightarrow R[t]/(\bar{p}(t))$. Su núcleo es el ideal generado por $\mathfrak{p}$ y $p(t)$, y como $A' = A[\alpha] = A[t]/(p(t))$, se tiene que $A'/\mathfrak{p}A' \simeq R[t]/(\bar{p}(t))$. Como $\bar{p}(t) = \prod_{i=1}^{r} \bar{p}(t)^{e_i}$, por el *teorema chino del resto*, se tiene finalmente el isomorfismo

$$R[t]/(\bar{p}(t)) \simeq \bigoplus_{i=1}^{r} R[t]/(\bar{p}_i(t))^{e_i}$$

Esto prueba que los ideales primos del anillo $B = R[t]/(\bar{p}(t))$ son ideales principales $(\bar{p}_i)$ generados por los polinomios $\bar{p}_i(t)$ *mod* $\bar{p}(t)$, para $i = 1, ..., r$. Además también se deduce de esto el hecho de que $[B/(\bar{p}_i)]$ es igual al grado del polinomio $\bar{p}_i(t)$, y que

$$(0) = (\bar{p}) = \bigcap_{i=1}^{r} (\bar{p}_i)^{e_i}$$

En virtud del isomorfismo $R[t]/(\bar{p}(t)) \simeq \tilde{A}/\mathfrak{p}\tilde{A}$, $f(t) \longrightarrow f(\alpha)$, se tiene la misma situación en $C = \tilde{A}/\mathfrak{p}\tilde{A}$, entonces los ideales primos $\mathfrak{B}'_i$ de C son los ideales primos $(\bar{p}_i)$, y son los ideales generados por $\bar{p}_i(\alpha)$ *mod* $\mathfrak{p}\tilde{A}$. El grado de $[C/\mathfrak{B}'_i : R]$ es igual al del polinomio $\bar{p}_i(t)$, y se tiene que

$$(0) = \bigcap_{i=1}^{r} \mathfrak{B}_i'^{e_i}$$

Ahora, sea $\mathfrak{B}_i = \mathfrak{p}\tilde{A} + p_i(\alpha)\tilde{A}$, la contraimagen de $\mathfrak{B}'_i$ por el homomorfismo canónico $\tilde{A} \longrightarrow \tilde{A}/\mathfrak{p}\tilde{A}$.
Entonces $\mathfrak{B}_i$, con $i = 1, ..., r$ recorre los ideales primos de $\tilde{A}$ sobre $\mathfrak{p}$. $f_i = [\tilde{A}/\mathfrak{B}_i : A/\mathfrak{p}]$ es el grado del polinomio $\bar{p}_i(t)$. Además, $\mathfrak{B}_i^{e_i}$ es la contraimagen de $\mathfrak{B}_i'^{e_i}$ (ya que $e_i = |\{\mathfrak{B}^\nu \quad | \quad \nu \in \mathbb{N}\}|$), y $\mathfrak{p}\tilde{A} \supseteq \bigcap_{i=1}^{r} \mathfrak{B}_i^{e_i}$, luego $\mathfrak{p}\tilde{A} | \prod_{i=1}^{r} \mathfrak{B}_i^{e_i}$, y en consecuencia $\mathfrak{p}\tilde{A} = \prod_{i=1}^{r} \mathfrak{B}_i^{e_i}$ por ser $\sum e_i f_i = n$.

■

Definición 3.7. Se dice que un ideal primo $\mathfrak{p}$ *factoriza completamente* en L si en la descomposición

$$\mathfrak{p} = \mathfrak{B}_1^{e_1} \dots \mathfrak{B}_r^{e_r}$$

se tiene que

$$r = [L : K] = n,$$

y en consecuencia $e_i = f_i = 1$, para todo $i = 1, ..., r$.

Se dice que el ideal $\mathfrak{p}$ ramifica en L si en la descomposición anterior, algún exponente es $e_i > 1$.

Proposición 3.7. *Si L/K es una extensión separable de grado n, entonces sólo existe un número finito de ideales primos de K que ramifican en L.*

Demostración. Sea $\alpha \in \tilde{A}$ un elemento primitivo para L, y sea $p(t) \in A[t]$ su polinomio irreducible. Sea

$$d = d(1, \alpha, ..., \alpha^{n-1}) = \prod_{i<j} (\alpha_i - \alpha_j)^2 \in A$$

donde d representa el discriminante del polinomio $p(t)$. (El discriminante en este sentido se definirá en la sección [4.2] pero dada su sencillez conceptual se utilizará en esta demostración.) Entonces, todo ideal primo $\mathfrak{p}$ de K que sea relativamente primo a d y al conductor $\mathfrak{F}$ de $A[\alpha]$ no ramifica. De hecho por la proposición anterior, los índices e_i son iguales a 1 cuando lo son también en la factorización de $\bar{p}(t) = p(t)\ mod\ \mathfrak{p}$ en $A/\mathfrak{p}$, o lo que es lo mismo, cuando $\bar{p}(t)$ no tiene raices múltiples.
En ese caso, el discriminante $\bar{d} = d\ mod\ \mathfrak{p}$ de $\bar{p}(t)$ es distinto de cero. Las extensiones $\tilde{A}/\mathfrak{B}_i/A/\mathfrak{p}$ están generadas por $\bar{\alpha} = \alpha\ mod\ \mathfrak{B}_i$, y por lo tanto son separables. Luego $\mathfrak{p}$ no ramifica.

■

Observación 11. Cuandd $K = \mathbb{Q}$ en todo lo expuesto anteriormente se tiene que $\theta_{\mathbb{Q}} = \mathbb{Z}$. Puesto que $\mathbb{Z}$ es un dominio de factorización única se puede tomar $\mathfrak{p} = (p)$ donde p es un elemento irreducible de $\mathbb{Z}$ (es decir, un número primo). Entonces, los factores $\mathfrak{B}_i$ de $(p)\theta_L$ son los ideales de θ_L asociados al número primo p, los exponentes $e_i > 0$ son los números de ramificación, y los f_i son los grados residuales de $\mathfrak{B}_i$ sobre $\mathbb{Z}$ (es decir, los grados de las extensiones $(\theta_L/\mathfrak{B}_i)/\mathbb{Z}/(p)$).
Todo lo anterior es también cierto si K es un cuerpo de números tal que θ_K sea un dominio de factorización única, por ejemplo si $K = \mathbb{Q}(i)$.

4. El discriminante

El discriminante es un concepto que como se ha adelantado en la introducción puede tener distintos significados dependiendo del ámbito del que se esté hablando. Existe el discriminante como polinomio simétrico, el discriminante de un polinomio arbitrario y el discriminante de un cuerpo. Este último se define a través de la traza de dos o más elementos. Puede definirse la traza como forma bilineal para un par de elementos que constituyen una base del cuerpo del que se quiere conocer el discriminante.

El objetivo es probar que en ciertos casos, estos discriminantes coinciden.

Los textos de donde se ha obtenido la documentación acerca de los temas a tratar en esta sección es la que se relata en las referencias [[3]], [[4]], [[5]],[[6]],[[7]],[[12]] y [[13]].

4.1. Polinomios simétricos y discriminante

Vamos a considerar ahora un anillo genérico k y el álgebra de polinomios en n variables con coeficientes sobre este anillo $k[\mathbf{X}]$. Sobre este álgebra actúa el grupo simétrico de las permutaciones de n elementos S_n, permutando las variables de un polinomio.

Definición 4.1. Un polinomio de $k[\mathbf{X}]$ se dice que es simétrico cuando permanece invariante por la acción de todos los elementos del grupo S_n.

Ejemplo 4.1. Los siguientes polinomios son ejemplos de polinomios simétricos
$s_1 = X_1 + X_2 + ... + X_n$
$s_n = X_1 \cdot X_2 \cdots X_n$

Los polinomios simétricos elementales son un conjunto específico de polinomios simétricos que se utilizan para expresar simetrías en las raíces de un polinomio. Estos polinomios son muy importantes en numerosas áreas de matemáticas. De esta forma podemos dar la siguiente definición.

Definición 4.2. Se definen los polinomios simétricos elementales, en las n variables $X_1, X_2, ..., X_n$, sobre el anillo k como sigue:

- $s_1 = X_1 + X_2 + ... + X_{n-1} + X_n$
- $s_2 = \sum_{1 \leq i < j \leq n} X_i \cdot X_j$
  $\vdots$
- $s_r = \sum_{1 \leq i_1 < ... < i_r \leq n} X_{i_1} \cdot X_{i_2} \cdots X_{i_r}$
  $\vdots$
- $s_n = X_1 \cdot X_2 \cdots X_n$

Nota. De forma general, dado un polinomio arbitrario $p(Y_1, ..., Y_n)$ perteneciente al anillo $k[\mathbf{Y}]$, pueden sustituirse las variables Y_i por los polinomios elementales simétricos s_i definidos en la definición anterior y obtener un así un polinomio simétrico en el anillo $k[\mathbf{X}]$.

Tras este comentario, es evidente que dado que los polinomios s_i son simétricos, cualquier polinomio definido en terminos de estos será simétrico también. A partir de esto puede enunciarse el que se denomina como *Teorema de las funciones simétricas*, que dice lo siguiente:

Teorema 4.1. *(de las funciones simétricas)* $p(X_1, ..., X_n)$ *es un polinomio simétrico de* $k[\boldsymbol{X}]$ *si y sólo si existe un polinomio* $q(Y_1, ..., Y_n)$ *de* $k[\boldsymbol{Y}]$*, tal que*

$$p(X_1, ..., X_n) = q(s_1, ..., s_n)$$

El polinomio q *definido en estas condiciones es de hecho único.*

Es decir, este teorema afirma que cualquier polinomio de $k[\mathbf{X}]$ puede escribirse de forma única en las variables $s_1, ..., s_n$ y coeficientes en k. Veamoslo con el siguiente ejemplo:

Ejemplo 4.2. Consideremos el siguiente polinomio en las variables X, Y, $p(X, Y) = X^2 + Y^2$. Es trivial comprobar que se trata de un polinomio simétrico, por lo tanto se puede expresar como

$$p = p(X, Y) = X^2 + Y^2 = (X + Y)^2 - 2XY = s_1^2 - 2s_2$$

Entonces, dadas dos variables nuevas, W, Z y el polinomio $q(W, Z) = W^2 - 2Z$ es el único que tras sustituir W por s_1 y Z por s_2, vuelve a darnos el polinomio de partida p.

El estudio de los polinomios simétricos permite introducir uno de los conceptos quizá más utilizados y más importantes del álgebra: el discriminante.
El discriminante es el que podría considerarse como ejemplo más importante de polinomio simétrico y ya ha sido mencionado con anterioridad en la sección [1.2] a la hora de estudiar la separabilidad de una extensión de cuerpos. Sin embargo, es a partir de esta sección donde se realizará un estudio en profundidad de este concepto y se particularizará para el caso de los polinomios y cuerpos ciclotómicos.

Definición 4.3. Sean $X_1, ..., X_n$ n variables y k un anillo arbitario. Se define el discriminante de la siguiente manera:

$$\Delta = \prod_{\substack{1 \leq i < j \leq n \\ i \neq j}} (X_i - X_j)^2 \tag{3}$$

Dado que en el producto anterior hay un total de $\binom{n}{2} = \frac{1}{2}n(n-1)$ factores y además se tiene que $(X_i - X_j)^2 = -(X_i - X_j)(X_j - X_i)$ la expresión del discriminante también puede escribirse como

$$\Delta = (-1)^{\frac{1}{2}n(n-1)} \prod_{\substack{1 \leq i < j \leq n \\ i \neq j}} (X_i - X_j) \tag{4}$$

4.2. Cálculo del polinomio discriminante y discriminante de un polinomio en una variable.

Al ser Δ un polinomio simétrico, puede escribirse en términos de los s_n. Esta expresión resulta de las relaciones que existen entre el discriminante y el resultante de dos polinomios. Los detalles de cómo se llega a tal expresión no van a detallarse ya que son bien conocidos y se han estudiado en el Grado.
Para ello primero va a definirse la noción de resultante de dos polinomios, $Res(p, q)$.

Definición 4.4. Dados los polinomios en una variable $p(t) = a_0t^n+a_1t^{n-1}+...+a_{n-1}t+a_n$ y ,$q(t) = b_0t^m + b_1t^{m-1} + ... + b_{m-1}t + b_m$ en el anillo $k[t]$, se define el resultante como el determinante de la matriz N definida como sigue:

$$N = \begin{pmatrix} a_0 & a_1 & a_2 & \dots & a_n & 0 & 0 & \dots & 0 \\ 0 & a_0 & a_1 & \dots & a_{n-1} & a_n & 0 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & a_0 & a_1 & \dots & a_n & \dots & 0 \\ b_0 & b_1 & b_2 & \dots & \dots & b_m & 0 & \dots & 0 \\ 0 & b_0 & b_1 & \dots & b_{m-1} & b_m & 0 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & b_0 & b_1 & \dots & \dots & \dots & b_m \end{pmatrix} \tag{5}$$

Es decir,

$$Res(p, q) = det(N) \tag{6}$$

Observemos que como el determinante de una matriz sólo se calcula a base de sumas y productos de los elementos de tal matriz, y los elementos de la matriz N pertenecen al anillo k, se tiene que $Res(p, q) \in k$.

El concepto de resultante y su definición permiten introducir nuevas expresiones para el definir lo que se denomina el discriminante de un polinomio, un concepto al que ya nos hemos referido y es importante en este trabajo.

Proposición 4.1. *Se considera un polinomio* $p(t) = (t - x_1)\dots(t - x_n)$*, los polinomios simétricos elementales* $s_1, ..., s_n$ *evaluados en las raíces* $x_1, ..., x_n$ *del polinomio* $p(t)$*. Se define la matriz* M *de dimensiones* $(2n-1) \times (2n-1)$

$$\begin{pmatrix} 1 & & & n & & & \\ -s_1 & \ddots & & -(n-1)s_1 & n & & \\ s_2 & \ddots & 1 & (n-2)s_2 & -(n-1)s_1 & \ddots & \\ \vdots & \ddots & -s_1 & \vdots & (n-2)s_2 & \ddots & n \\ \vdots & & s_2 & \vdots & \vdots & \ddots & -(n-1)s_1 \\ (-1)^{n-1}s_{n-1} & & \vdots & (-1)^{n-1}s_{n-1} & \vdots & & \vdots \\ (-1)^n s_n & \ddots & \vdots & & (-1)^{n-1}s_{n-1} & & \vdots \\ & \ddots & (-1)^{n-1}s_{n-1} & & & \ddots & \vdots \\ & & (-1)^n s_n & & & & (-1)^{n-1}s_{n-1} \end{pmatrix} \tag{7}$$

Entonces se tiene que

$$\Delta = (-1)^{n(n-1)/2} det(M) \tag{8}$$

Ejemplo 4.3. Para $n = 2$ se tiene que $\Delta = (X - Y)^2 = s_1^2 - 4s_2$.
Si se toma el polinomio $q = q(W, Z) = W^2 - 4Z$, se observa que este es el polinomio que corresponde al simétrico Δ., y este se conoce comunmente como el discriminante del polinomio cuadrático $t^2 + Wt + Z$.

Ejemplo 4.4. Para el caso en el que $n = 3$, se tiene que el discriminante en función de los polinomios simétricos $s_1 = X + Y + Z$, $s_2 = XY + XZ + YZ$ y $s_3 = XYZ$ es

$$\Delta = (X - Y)^2(X - Z)^2(Y - Z)^2 = -4s_2^3 - 27s_3^2 + s_1^2 s_2^2 - 4s_1^3 s_3 + 18 s_1 s_2 s_3$$

Otra fórmula interesante para calcular el polinomio simérico discriminante, o en concreto $\sqrt{\Delta}$, es la que viene dada por el determinante de *Vandermonde*. Se tiene $\sqrt{\Delta} = \prod_{1 \le i < j \le n}(X_j - X_i)$ con la fórmula (4).

Proposición 4.2. *Dadas las variables* $X_1, X_2, ..., X_n$ *se tiene que*

$$\sqrt{\Delta} = det \begin{pmatrix} X_1^{n-1} & X_2^{n-1} & \dots & X_n^{n-1} \\ X_1^{n-2} & X_2^{n-2} & \dots & X_n^{n-2} \\ \vdots & \vdots & \ddots & \vdots \\ X_1 & X_2 & \dots & X_n \\ 1 & 1 & \dots & 1 \end{pmatrix} \tag{9}$$

Veamos ahora como se trasladan todas estas ideas a la hora de trabajar con polinomios en una variable t no necesariamente mónicos. Un polinomio $p(t)$ en una única variable con coeficientes en un anillo arbitrario k puede escribirse de dos formas distintas:

1. Por sus coeficientes: $p = p(t) = a_0t^n + a_1t^{n-1} + ... + a_{n-1}t + a_n$,
donde $a_0, a_1, ..., a_n \in k$.

2. Por sus raíces: $p = p(t) = a_0(t - x_1)(t - x_2)\dots(t - x_n)$,
donde $x_1, ..., x_n$ son las raíces del polinomio p que pertenecen a un cuerpo L del que k es un subanillo.

Si para la definición de resultante, en vez de tomar dos polinomios $p(t)$ y $q(t)$ arbitrarios distintos, se toman $p(t)$ y su polinomio derivado $p'(t)$, puede observarse que la matriz R cumple que

$$det(N) = a_0 \cdot det(N') \tag{10}$$

donde N' es la matriz que se obtiene al sustituir N en la primera fila a_0 por 1 y en la n-ésima fila na_0 por n. Se define entonces el discriminante del polinomio p de la siguiente manera:

Definición 4.5. Dado un polinomio en una variable $p(t)$ con coeficientes en un anillo k, se define el discriminante del polinomio p como

$$\Delta(p) = (-1)^{\frac{1}{2}n(n-1)}det(N') \tag{11}$$

De forma análoga que para el resultante, puede observarse que $\Delta(p)$ es un elemento del anillo k al que pertenecen los coeficientes del polinomio.

De esta forma el resultante de los polinomios $p(t)$ y $p'(t)$ y el discriminante de $p(t)$ quedan relacionados de la siguiente forma:

$$Res(p, p') = (-1)^{\frac{1}{2}n(n-1)} \cdot a_0 \cdot \Delta(p) \tag{12}$$

Por último, se termina esta sección aportando una última expresión que facilita el cálculo del discriminante de cualquier polinomio en una variable, en función de sus raíces:

Proposición 4.3. *Dado un polinomio $p(t)$ con coeficientes $a_0, a_1, ..., a_n$ sobre un anillo k y cuyas raíces en algún anillo que contiene a k son $x_1, x_2, ..., x_n$. Entonces,*

$$\Delta(p) = a_0^{2n-2} \prod_{1 \le i < j \le n} (x_i - x_j)^2 \tag{13}$$

Observación 12. Nótese que esta expresión no es otra que la que se consigue evaluando el polinomio simétrico discriminante, Δ, en las raíces del polinomio p.

4.3. El discriminante en un cuerpo de números

Ya se ha comentado al inicio de esta sección que el discriminante es uno de los invariantes con mayor importancia en los cuerpos de números, y lo es especialmente en el caso de los cuerpos ciclotómicos.
Para poder definir el discriminante en un cuerpo primero se necesitan dar ciertas nociones y conceptos básicos de álgebra lineal.

Sea A un anillo, E un A-módulo libre de rango finito y f un endomorfismo de E. En álgebra lineal se definen la *traza*, el *determinante* y el *polinomio característico* de f de la siguiente manera.

Definición 4.6. Sea $\{u_i\}$ una base de E y f un endomorfismo de E. Si (a_{ij}) es la matriz de f en la base $\{u_i\}$, se definen entonces:

- **La traza:**
$$Tr(f) = \sum_{i=1}^{n} a_{ii}$$
- **El determinante:**
$$det(f) = det(a_{ij})$$

Nota. Todos estos elementos de A son independientes de la base elegida para E.

Se toma ahora un anillo B, y un subanillo A de este de tal forma que B es un A-módulo libre de rango finito n. En particular, ahora puede considerarse una extensión finita $L/\mathbb{Q}$, cuyo grado es $[L:\mathbb{Q}] = n$. Dado que $L/\mathbb{Q}$ es separable, por el teorema de las inmersiones (teorema 1.1), visto en la sección [1.2] existen n inmersiones $\psi_1, ..., \psi_n : L \longrightarrow \bar{L} = \bar{\mathbb{Q}}$. Entonces, se tiene la siguiente definición de interpretación galoisiana del concepto de traza y norma:

Definición 4.7. A través de las inmersiones definidas anteriormente $\psi_1, ..., \psi_n$ se define la traza del elemento $x \in L$ como

$$Tr(x) = \psi_1(x) + ... + \psi_n(x)$$

De la misma forma, se define la normal de $x \in L$ como

$$N(x) = \psi_1(x) \cdots \psi_n(x)$$

Observación 13. Es evidente que al ser $\mathbb{Q}$ un cuerpo, tanto la traza, $Tr(x)$, como la norma, $N(x)$, de $x \in L$ son elementos de $\mathbb{Q}$. Más aún, si $x \in \theta_L$, tanto $Tr(x)$ como $N(x)$ son elementos de $\mathbb{Z}$ ya que en este caso el polinomio irreducible de x sobre $\mathbb{Q}$ es mónico y con coeficientes en $\mathbb{Z}$.

Veamos ciertas expresiones, las cuales no se probarán aquí debido a su caracter elemental, que permiten simplificar el cálculo y que se derivan de las propiedades lineales de estos elementos.

Proposición 4.4. *Para $x, x' \in L$, $a \in \mathbb{Q}$ se tiene*

- $Tr(x + x') = Tr(x) + Tr(x')$
- $Tr(a \cdot x) = aTr(x)$
- $Tr(a) = n \cdot a$
- $N(x \cdot x') = N(x)N(x')$
- $N(a) = a^n$
- $N(a \cdot x) = a^n N(x)$

Observación 14. Esto significa que la traza, como aplicación, $Tr : L \longrightarrow \mathbb{Q}$ es lineal; y que la norma, $N : L^* \longrightarrow \mathbb{Q}^*$ es un homomorfismo de grupos abelianos.

Una vez visto que la aplicación traza, Tr, es lineal, puede extenderse este concepto a una aplicación bilineal del producto de $L \times L$ en $\mathbb{Q}$:

Definición 4.8. Se define la traza, como forma bilineal de la siguiente forma:

$$\mathbb{T}r : L \times L \longrightarrow \mathbb{Q}$$

$$(x, y) \to Tr(x \cdot y)$$

Esta aplicación es bilineal y simétrica y por lo tanto da lugar a una forma cuadrática.

Ahora sí estamos en posición de poder definir el concepto de discriminante pero para un cuerpo. Veremos cómo se relaciona esto con el concepto homónimo para los polinomios descrito anteriormente.

Definición 4.9. Sea $L/\mathbb{Q}$ una extensión finita, de grado n. Para $(x_1, ..., x_n) \in L^n$ llamamos discriminante del conjunto $\{x_1, ..., x_n\}$ al elemento de $\mathbb{Q}$ descrito por la siguiente relación

$$D(x_1, ..., x_n) = det(Tr(x_i x_j)) \tag{14}$$

Observación 15. Como la extensión $L/\mathbb{Q}$ es separable, la forma bilineal $\mathbb{T}r$ es no degenerada, o equivalentemente si se tiene que $D(x_1, ..., x_n) \neq 0$ cuando $\{x_1, ..., x_n\}$ son linealmente independientes; es decir, si son una base de L como $\mathbb{Q}$-espacio vectorial.
Se volverá a tratar esto más adelante.

Proposición 4.5. *Si $\{y_1, ..., y_n\} \in L$ es un conjunto de elementos tales que $y_i = \sum_{j=1}^{n} a_{ij} x_j$ con $a_{ij} \in \mathbb{Q}$, entonces*

$$D(y_1, ..., y_n) = (det(a_{ij}))^2 D(x_1, ..., x_n)$$

Demostración.

$$Tr(y_p y_q) = Tr\left(\sum_{i,j} a_{pi} a_{qj} x_{ij}\right) = \sum_{i,j} a_{pi} a_{qj} Tr(x_i y_j)$$

Esto lleva a la siguiente ecuación matricial

$$(Tr(y_p y_q)) = (a_{pi})(Tr(x_i x_j))(a_{qj})^t$$

La demostración se concluye tomando determinantes.

■

Si $\{x_1, ..., x_n\}$ es una base de L como $\mathbb{Q}$-espacio vectorial, y $A = (Tr(x_i x_j))_{ij}$ es la matriz de la forma bilineal (o cuadrática) $\mathbb{T}r$. Si se considera otra base, $\{y_1, ..., y_n\}$, tal que la matriz de la traza en esta base es $B = (Tr(y_i y_j))_{ij}$; entonces, A y B son congruentes. Esto significa que existe una matriz de cambio de base P, con coeficientes en $\mathbb{Q}$, tal que

$$B = P^t A P$$

Como $det(P) = det(P^t)$, se tiene que

$$det(A) = det(B)(det(P))^2$$

Como $det(A), det(B), det(P) \neq 0$, se tiene que las clases de los elementos $det(A), det(B) \in \mathbb{Q}^*$ en el grupo cociente $\mathbb{Q}^*/\mathbb{Q}^{*2}$ son iguales.

Nótese que la razón por la que $D(x_1, ..., x_n) \neq 0$ en el caso separable, es que el cuerpo L tiene un elemeto primitivo x y que, por tanto, se probará finalmente que $D(1, x.x^2, ..., x^{n-1}) \neq 0$.

Más aún, consideremos el anillo de los enteros de L sobre $\mathbb{Z}$, θ_L como $\mathbb{Z}$-módulo, según se ha visto en la sección [3.1]. Si sólo se toman bases $\{u_1, ..., u_n\}$ y $\{v_1, ..., v_n\}$ del módulo libre θ_L, entonces las matrices A, B y P tendrán coeficientes en $\mathbb{Z}$ y $(det(P))^2 = 1.$, por ser P inversible. Por lo tanto, $det(A) = det(B)$ es un entero bien definido. Es por eso que puede definirse el discriminante del cuerpo de números L, sin ambigüedad, de la siguiente forma.

Definición 4.10. Bajo las mismas hipótesis que en la definición 4.9, se llama discriminante de L sobre $\mathbb{Q}$ al elemento de $\mathbb{Z}$ dado por el discriminante de cualquier base de θ_L sobre $\mathbb{Z}$; y se denota por $\mathscr{D}_L$.

Como "recíproco" a lo mencionado en el párrafo anterior respecto a la ambigüedad en la definición del discriminante de un cuerpo se puede enunciar la siguiente proposición.

Proposición 4.6. *Sea L un cuerpo de números tal que $[L : \mathbb{Q}] = n$ y sea $\{u_1, u_2, ..., u_n\}$ una base de L como $\mathbb{Q}$-espacio vectorial, tal que los elementos de tal base pertenecen al anillo de enteros θ_L. Si el discriminante $D(u_1, ..., u_n)$ está libre de cuadrados, entonces $\{u_1, ..., u_n\}$ es también una base de θ_L como $\mathbb{Z}$-módulo.*

Demostración. Sea $\{e_1, ..., e_n\}$ una base de θ_L como $\mathbb{Z}$-módulo. Entonces, $u_i = \sum_{j=1}^{n} a_{ij} e_j$, para cada $i = 1, ..., n$ donde $a_{ij} \in \mathbb{Z}$. Entonces,

$$D(u_1, ..., u_n) = (det(a_{ij}))^2 D(e_1, ..., e_n)$$

Como $D(u_1, ..., u_n)$ está libre de cuadrados, $(det(a_{ij})^2 = \pm 1$, luego $\{u_1, ..., u_n\}$ tiene que ser también una base de θ_L como módulo sobre $\mathbb{Z}$. ■

Veamos un par de proposiciones que nos van a permitir después hacer ciertas afirmaciones sobre el discriminante.

Proposición 4.7. *Sea $L/\mathbb{Q}$ una extensión finita de grado n. Sean $\psi_1, ..., \psi_n : L \longrightarrow \bar{\mathbb{Q}}$ dadas por el teorema de las inmersiones (teorema 1.1 de la sec. [1.1]). Entonces, si $\{x_1, ..., x_n\}$ es una base de L como $\mathbb{Q}$-espacio vectorial,*

$$D(x_1, ..., x_n) = (det(\psi_i(x_j)))^2 \neq 0 \tag{15}$$

Para probar este resultado primero tiene que enunciarse y probarse un lema auxiliar, que se atribuye a Dedekind.

Lema 4.1. ***(de Dedekind)*** *Sea G un grupo, K un cuerpo, y $\psi_1, ..., \psi_n : G \longrightarrow K^*$ n homomorfismos de grupos distintos. Entonces los ψ_i son linealmente independientes sobre K; es decir, si $\sum_i u_i \psi_i(g) = 0$ para todo $g \in G$, entonces $u_i = 0$, para todo i.*

Demostración. Supongamos que los ψ_i son linealmente dependientes, y consideremos la relación no trivial $\sum_i u_i \psi_i = 0.$, con $u_i \in K$ y tal que el número q de coeficientes u_i distintos de cero es mínimo. Reordenando los términos se tiene que

$$u_1 \psi_1(g) + ... + u_q \psi_q(g) = 0 \quad \text{para todo } g \in G$$

Tenemos que $q \geq 2$, ya que los ψ_i son distintos de cero. Para $g, h \in G$ arbitrarios, vemos que

$$u_1 \psi_1(hg) + ... + u_q \psi_q(hg) = u_1 \psi_1(h)\psi_1(g) + ... + u_q \psi_q(h)\psi_q(g) = 0$$

Si se multiplica esta última expresión por $\psi_1(h)$ y se resta, se obtiene

$$u_2(\psi_1(h) - \psi_2(h))\psi_2(g) + ... + u_q(\psi_1(h) - \psi_q(h))\psi_q(g) = 0$$

Como esto se cumple para cualquier $g \in G$, y como q es mínimo, se tiene que

$$u_2(\psi_1(h) - \psi_2(h)) = 0$$

Entonces,

$$\psi_1(h) = \psi_2(h)$$

para todo $h \in G$, ya que $u_2 \neq 0$. Sin embargo esto contradice la hipótesis de que los ψ_i son distintos.
Por lo tanto se concluye que son linealmente independientes.

■

Una vez probado este lema ya estamos en condiciones de poder probar la proposición 4.7.

Demostración. (de la proposición 4.7) La primera igualdad se deduce de hacer lo siguientes simples cálculos:

$$D(x_1,...,x_n) = det(Tr(x_i x_j)) = det(\sum_k \psi_k(x_i x_j)) = det(\sum_k \psi_k(x_i)\psi_k(x_j)) =$$

$$= det(\psi_k(x_i)) \cdot det(\psi_k(x_i)) = (det(\psi_i(x_j)))^2$$

Queda demostrar que $det(\psi_i(x_j)) \neq 0$. Razonemos por reducción al absurdo, supongamos que $det(\psi_i(x_j)) = 0$. Entonces, existen $u_1,...,u_n \in \bar{\mathbb{Q}}$, no todos nulos, tales que $\sum_i u_i\psi_i(x_j) = 0$ para todo j. Por linealidad se conlcuye que

$$\sum_{i=1}^{n} u_i\psi_i(x) = 0 \quad \text{para todo } x \in L$$

Esto contradice lo que dice el lema de Dedekind, llegándose así a una contradicción.

■

Observación 16. Bajo las hipótesis de la proposición 4.7, es la relación

$$D(x_1,...,x_n) \neq 0$$

la que implica que la forma bilineal $\mathbb{T}r(x,y) = Tr(x \cdot y)$ es no degenerada; es decir, si $Tr(x \cdot y) = 0$ para todo $y \in L$, entonces $x = 0$.

Veamos por último una fórmula que facilita el cálculo del discriminante de un cuerpo en ciertos casos, que servirá como lema auxiliar para poder llevar a cabo el cálculo en los cuerpos ciclotómicos.

Lema 4.2. *Sea $L = \mathbb{Q}(x)$ un cuerpo de números tal que $[L:\mathbb{Q}] = n$ y sea $p(t)$ el polinomio irreducible de x sobre $\mathbb{Q}$. Entonces,*

$$D(1,x,...,x^{n-1}) = (-1)^{1/2n(n-1)} N_L(p'(x)) \tag{16}$$

donde $p'(x)$ denota el derivado del polinomio $p(x)$.

Demostración. Sean $x_1,...,x_n$ las raíces del polinomio $p(t)$ en una extensión de números. Sabemos por la proposición 4.7 que

$$D(1,x,...,x^{n-1}) = (det(\psi_i(x^j)))^2 = (det(x_i^j))^2 =$$

$$= \left[\prod_{i<j}(x_i - x_j)\right]^2 = c\prod_{i\neq j}(x_i - x_j) =$$

$$= c\prod_i \left(\prod_{j\neq i}(x_i - x_j)\right) = c\prod_i p'(x_i) = cN_L(p'(x))$$

■

Utilizando el concepto de discriminante pueden demostrarse una serie de resultados que permitirían probar, como avanzamos en la observación 5, que el anillo de enteros θ_L de un cuerpo de números $L/\mathbb{Q}$ es un Z-módulo libre de rango n. Realmente este resultado es cierto para toda extensión L/K que sea galoisiana, pero para lo que a nosotros nos interesa bastará con probar este caso particular.

Lema 4.3. *Sea $L/\mathbb{Q}$ un cuerpo de números, θ_L su anillo de enteros y $\{x_1, ..., x_n\}$ una base de L contenida en θ_L. Si $d = D(x_1, ..., x_n)$ entonces*

$$d\theta_L \subseteq \mathbb{Z}x_1 + ... + \mathbb{Z}x_n$$

Demostración. Sea $b = a_1x_1 + ... + a_nx_n$, con $a_i \in \mathbb{Q}$ para todo i. Entonces los a_i son solución del sistema de ecuaciones lineales

$$Tr_L(x_ib) = \sum_{i=1}^{n} Tr_L(x_jx_i)a_i$$

Como $Tr_L(x_ib) \in \mathbb{Z}$, se tiene que $da_i \in \mathbb{Z}$ y por lo tanto,

$$db \in \mathbb{Z}x_1 + ... + \mathbb{Z}x_n$$

■

Un conjunto de elementos $y_1, ...y_n \in \theta_L$ tal que todo $b \in \theta_L$ puede escribirse de forma única como

$$b = a_1y_1 + ... + a_ny_n$$

con $a_i \in \mathbb{Z}$ se denomina *base de enteros* de θ_L sobre $\mathbb{Z}$ (o $\mathbb{Z}$-base de θ_L). Como tal base es a su vez una base de $L/\mathbb{Q}$, siempre constará de n elementos donde $n = [L : \mathbb{Q}]$. La existencia de tal base significa que θ_L es un $\mathbb{Z}$-módulo libre de tipo finito de rango n. Para los anillos de enteros de cuerpos de números esta base siempre existe, ya que $\mathbb{Z}$ es un dominio de ideales principales.

Proposición 4.8. *Sea $L/\mathbb{Q}$ un cuerpo de números. Entonces todo θ_L-submódulo $M \neq 0$ de L es un $\mathbb{Z}$-módulo de rango $[L : \mathbb{Q}]$. En particular, θ_L admite una base de enteros sobre $\mathbb{Z}$.*

Demostración. Sea $M \neq 0$ un θ_L-submódulo de L finitamente generado y $\{x_1, ..., x_n\}$ una base de L como $\mathbb{Q}$-espacio vectorial. Por el lema 4.3, se tiene que $dB \subseteq \mathbb{Z}x_1 + ...+ \subseteq Zx_n$. En particular, $rang(\theta_L) \leq [L : \mathbb{Q}]$, y como un sistema de generadores de θ_L como $\mathbb{Z}$-módulo es también un sistema de generadores para L como $\mathbb{Q}$-módulo (o como $\mathbb{Q}$-espacio vectorial en este caso), se tiene entonces que $rang(\theta_L) = [L : \mathbb{Q}]$.
Sea $\{u_1, ..., u_r\} \in M$ un sistema de generadores de M como θ_L-módulo. Existe entonces un $a \in \mathbb{Z}$ no nulo tal que $au_i \in \theta_L$ para todo $i = 1, ..., r$, luego $aM \subseteq B$.Entonces

$$adM \subseteq dB \subseteq \mathbb{Z}x_1 + ... + \mathbb{Z}x_n = M_0$$

En virtud del teorema principal sobre módulos finitamente generados sobre dominios de ideales principales, como M_0 es un $\mathbb{Z}$-módulo libre, también lo será adM y en consecuencia

M.

Finalmente,

$$[L:\mathbb{Q}] = rang(\theta_L) \leq rang(M) = rang(adM) \leq rang(M_0) = [L:\mathbb{Q}]$$

y por lo tanto $rang(M) = [L:\mathbb{Q}]$.

■

4.4. Vínculo entre Δ y $\mathscr{D}$

Vayamos ahora con el teorema más relevante de esta sección que, como se mencionaba antes, permite vincular las definiciones de discriminante de un polinomio y discriminante de un cuerpo sin que haya ningún tipo de discrepancia por ser ambos conceptos homónimos.

Teorema 4.2. *Sea L un cuerpo de números y θ_L el anillo de los elementos de L que son enteros sobre $\mathbb{Z}$. Supongamos que existe un elemento $x \in \theta_L$ tal que $\theta_L = \mathbb{Z}[x]$ (es decir, θ_L es el mínimo anillo que contiene a x y a $\mathbb{Z}$). Sea $p(t)$ el polinomio irreducible del elemento x sobre $\mathbb{Q}$. Entonces,*

$$\Delta(p) = \mathscr{D}_L$$

Es decir, el discriminante del polinomio $p(t)$ y el discriminante del cuerpo de números L coinciden.

Demostración. Como se tiene que θ_L es el mínimo anillo que contiene tanto a x como a $\mathbb{Z}$, entonces L es el mínimo cuerpo que contiene a x y a $\mathbb{Q}$; es decir, $L = \mathbb{Q}(x)$. Por lo tanto, el polinomio irreducible de x sobre $\mathbb{Q}$, $p(t)$ tiene grado n.. Además el conjunto $\{1, x, x^2, ..., x^{n-1}\}$ es una base de L como $\mathbb{Q}$-espacio vectorial y también de θ_L como $\mathbb{Z}$-módulo.

Entonces la matriz de la forma bilineal $\mathbb{T}r$ en esta base será

$$A = (Tr(x^i x^j))_{ij}, \quad 0 \leq i, j \leq n-1$$

Por la definición de traza se tiene que

$$Tr(x^i x^j) = Tr(x^{i+j}) = \psi_1(x^{i+j}) + ... + \psi_n(x^{i+j})$$

Comp $\psi_1, ..., \psi_n$ son inmersiones del cuerpo L en $\bar{\mathbb{Q}}$, en particular son homomorfismos de cuerpos y entonces se tiene que

$$Tr(x^i x^j) = (\psi_1(x))^i(\psi_1(x))^j + ... + (\psi_n(x))^i(\psi_n(x))^j$$

Esto puede escribirse en forma matricial de la siguiente forma

$$A = \begin{pmatrix} 1 & \psi_1(x) & (\psi_1(x))^2 & \dots & (\psi_1(x))^{n-1} \\ 1 & \psi_2(x) & (\psi_2(x))^2 & \dots & (\psi_2(x))^{n-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \psi_n(x) & (\psi_n(x))^2 & \dots & (\psi_n(x))^{n-1} \end{pmatrix} \begin{pmatrix} 1 & 1 & \dots & 1 \\ \psi_1(x) & \psi_2(x) & \dots & \psi_n(x) \\ \vdots & \vdots & \ddots & \vdots \\ (\psi_1(x))^{n-1} & (\psi_2(x))^{n-1} & \dots & (\psi_n(x))^{n-1} \end{pmatrix}$$

Es decir, A es el producto matricial entre la matriz de Vandermonde y su transpuesta. Por lo tanto, teniendo en cuenta la formula del determinante de Vandermonde

$$det(A) = \prod_{k<h}(\psi_k(x) - \psi_h(x))^2$$

Entonces, por un lado tenemos que $det(A)$ es el discriminante del cuerpo de números $L \Longrightarrow det(A) = \mathscr{D}_L$.
Por otro lado, por el teorema de inmersiones, $\psi_1(x), ..., \psi_n(x)$ son las raíces en $\bar{L}$ del polinomio $p(t)$, y por tanto, el discriminante de $p(t)$ es $\Delta(p) = \prod_{k<h}(\psi_k(x) - \psi_h(x))^2$.
Entonces, se llega a que

$$\Delta(p) = \prod_{k<h}(\psi_k(x) - \psi_h(x))^2 = det(A) = \mathscr{D}_L,$$

como se quería demostrar.

■

Ejemplo 4.5. Si $L = \mathbb{Q}(i)$ se tiene que $\theta_L = \mathbb{Z}[i]$ y $p(t) = t^2+1$ es el polinomio irreducible de $i = \sqrt{-1}$ sobre $\mathbb{Q}$. Por tanto, $\mathscr{D}_L = \Delta(p) = -4$.
Por otro lado, $\mathscr{D}_L$ también se puede calcular a partir de la base $\{1, i\}$ de θ_L sobre $\mathbb{Z}$ ya que

$$\mathscr{D}_L = det\begin{pmatrix} \mathbb{T}r(1,1) & \mathbb{T}r(1,i) \\ \mathbb{T}r(i,1) & \mathbb{T}r(i,i) \end{pmatrix} = det\begin{pmatrix} Tr(1) & Tr(i) \\ Tr(i) & Tr(-1) \end{pmatrix} = det\begin{pmatrix} 2 & 0 \\ 0 & -2 \end{pmatrix} = -4$$

Esto se debe a que $p = 2$ es el primo que ramifica.

Ejemplo 4.6. Si $L = \mathbb{Q}(\sqrt{5})$, entonces $\theta_L = \mathbb{Z}[x]$, donde $x = \frac{1+\sqrt{5}}{2}$, siendo $p(t) = t^2-t-1$ el polinomio irreducible de x sobre $\mathbb{Q}$. Entonces $\Delta(p) = 5$ y

$$\mathscr{D}_L = det\begin{pmatrix} Tr(1) & Tr(2) \\ Tr(x) & Tr(x^2) \end{pmatrix} = det\begin{pmatrix} 2 & 1 \\ 1 & 3 \end{pmatrix} = 5$$

Se deduce que $p = 5$ es el único primo que ramifica.

4.5. El discriminante y la ramificación

Con la misma notación que se ha introducido en la sección [3.2] dedicada a la introducción a la ramificación de números o ideales primos, se tiene que dada una extensión $L/\mathbb{Q}$ se dice que el número primo p ramifica en L si alguno de los índices de ramificación en la descomposición de $(p)\theta_L$ es mayor que 1.

En términos de la teoría sobre el discriminante descrita en las secciones inmediatamente anteriores a esta [4.1], [4.2], [4.3] y [4.4] se van a caracterizar tales ideales primos de $\theta_{\mathbb{Q}}$, es decir los números primos de $\theta_{\mathbb{Q}} = \mathbb{Z}$ que ramifican en L.

Una forma de estudiar la ramificación de los primos es mediante el estudio de la estructura del anillo $\theta_L/(p)$. Si se tiene la descomposición

$$(p) = p\theta_L = \mathfrak{B}_1^{e_1} \cdots \mathfrak{B}_r^{e_r}$$

y teniendo en cuenta el teorema chino del resto,

$$\theta_L/(p) \simeq \theta_L/\mathfrak{B}_1^{e_1} \times ... \times \theta_L/\mathfrak{B}_r^{e_r} \tag{17}$$

Nuestro objetivo es probar que para un cuerpo de números $L/\mathbb{Q}$, un primo p ramifica en L si y sólo si p divide al discriminante $\mathscr{D}_L$. Como se ha visto que $\mathscr{D}_L \neq 0$, se tiene que sólo existirá un número finito de primos que ramifican en L.

Consideremos primero el caso en el que existe un elemento $\alpha \in \theta_L$ tal que $L = \mathbb{Q}(\alpha)$ y p no divide a $[\theta_L : \mathbb{Z}[\alpha]]$.

Nota. Para el caso en el que $\theta_L = \mathbb{Z}[\alpha]$ puede considerarse el mismo α para todo p. Entonces:

Proposición 4.9. *En las condiciones descritas previamente, se tiene que un primo p ramifica en un cuerpo de números L, si y sólo si, $p|\mathscr{D}_L = \mathscr{D}_{\theta_L}$.*

Demostración. Sea p un primo tal que existe un $\alpha \in \theta_L$ que cumple que $L = \mathbb{Q}(\alpha)$ y p no divide a $[\theta_L : \mathbb{Z}[\alpha]]$. Sea $q(t)$ el polinomio irreducible de α sobre $\mathbb{Q}$. $q(t)$ es mónico en $\mathbb{Z}[t]$. La proposición 3.6 de la sección (3.2) dice que $p\theta_L$ factoriza en ideales primos de la misma forma que lo hace el polinomio $q(t)$ *mod* p en polinomios mónicos irreducibles de $(\mathbb{Z}/p\mathbb{Z})[t]$.
Por definición, $p\theta_L$ ramifica en L si y sólo si, en su factorización, alguno de los índices e_i es mayor que 1. Consideremos entonces la factorización de $q(t)$ módulo p:

$$\bar{q}(t) = \bar{q_1}(t)^{e_1} \cdots \bar{q_r}^{e_r}$$

con $\bar{q_i}(t) \in (\mathbb{Z}/p\mathbb{Z})$ mónicos e irreducibles. Como todo polinomio irreducible sobre un cuerpo finito es separable, lo son en particular los $\bar{q_i}(t)$. Por lo tanto, algún e_i será mayor que 1 si y sólo si, $\bar{q}(t)$ tiene alguna raíz multiple en su descomposición sobre $(\mathbb{Z}/p\mathbb{Z})$. Según se expuso en la definición 1.4 de la sección [1.2], esto es equivalente a que el discriminante $\Delta(\bar{q})$ sea nulo. En conclusión, p ramifica en θ_L si y sólo si $\Delta(\bar{q}) = \bar{0}$ en $(\mathbb{Z}/p\mathbb{Z})$.

Como el discriminante de un polinomio es un elemento del cuerpo o anillo al que pertenecen sus coeficientes, el discriminante de un polinomio mónico tiene un buen comportamiento para la reducción módulo p :

$$\Delta(q(t) \ mod \ p) = \Delta(q(t)) \ mod \ p.$$

Esto significa que $\Delta(\bar{q}(t)) = \bar{0}$ en $(\mathbb{Z}/p\mathbb{Z})$ si y sólo si $\Delta(q) \equiv 0 \ mod \ p$. Como según el teorema 4.2 se tiene que

$$\Delta(q) = \mathscr{D}_{\mathbb{Z}[\alpha]} = [\theta_L : \mathbb{Z}[\alpha]]^2 \mathscr{D}_{\theta_L}$$

y como p no divide a $[\theta_L : \mathbb{Z}[\alpha]]$, tenemos que p divide a $\Delta(q)$ si y sólo si p divide a $\mathscr{D}_{\theta_L}$. ■

Vayamos ahora con el caso general, en el que p puede dividir, o no, al grado $[\theta_L : \mathbb{Z}[\alpha]]$ para un cuerpo $L = \mathbb{Q}(\alpha)$. Para ello tendremos que ver que $\mathscr{D}_{\theta_L} \ mod \ p = \mathscr{D}_{\theta_L/(p)}$.

Nota. Es importante tener en cuenta que $\mathscr{D}_{\theta_L} \in \mathbb{Z}$ y que $\mathscr{D}_{\theta_L/(p)} \in (\mathbb{Z}/p\mathbb{Z})$.

Como hemos visto, la ramificación de p en L está estrechamente relacionada con la estructura del anillo $\theta_L/(p)$. Estudiemos el discriminante de este anillo. Si $[L : \mathbb{Q}] = n$, ya se ha probado que θ_L es un $\mathbb{Z}$-módulo libre de rango n, pongamos

$$\theta_L = x_1\mathbb{Z} + x_2\mathbb{Z} + ... + x_n\mathbb{Z}$$

Si reducimos ambos lados de esta igualdad módulo p se obtiene que

$$\theta_L/(p) = \bar{x_1}(\mathbb{Z}/p\mathbb{Z}) + ... + \bar{x_n}(\mathbb{Z}/p\mathbb{Z})$$

lo que demuestra que $\theta_L/(p)$ es un $(\mathbb{Z}/p\mathbb{Z})$-espacio vectorial de dimensión n.

Lema 4.4.

$$\mathscr{D}_{\theta_L} \ mod \ p = \mathscr{D}_{\theta_L/(p)} \tag{18}$$

Demostración. Sea $\{x_1, ..., x_n\}$ una base de θ_L en $\mathbb{Z}$. Su reducción módulo p, $\{\bar{x_1}, ..., \bar{x_n}\}$ es una base de $\theta_L/(p)$ en $(\mathbb{Z}/p\mathbb{Z})$. Sea (m_y) la matriz de multiplicación para cualquier elemento $y \in \theta_L$, para la base definida antes; y sea $(m_{\bar{y}})$ la reducción módulo p de (m_y) con $\bar{y} \in \theta_L/(p)$ en la base de antes para este anillo. Entonces

$$Tr_{\theta_L/(p)}(\bar{y}) = Tr(m_{\bar{y}}) = Tr(m_y) \ mod \ p = Tr_{\theta_L}(y) \ mod \ p$$

Se concluye tomando determinantes.

■

Lema 4.5. *Sean $L_1, ..., L_q$ cuerpos de números y sea $L = \prod_{i=1}^{q} L_i$ el anillo producto, y $\theta_L = \prod_{i=1}^{q} \theta_{L_i}$. Como θ_L es un $\mathbb{Z}$-módulo libre de tipo finito, se define $\mathscr{D}_L$ como en el caso $q = 1$. Entonces,*

$$\mathscr{D}_L = \prod_{i=1}^{1} \mathscr{D}_{L_i} \tag{19}$$

Demostración. Basta probar este resultado para el caso $q = 2$, ya que se puede generalizar para cualquier q finito por inducción.
Sean $(x_1, ..., x_m)$ y $(y_1, ..., y_n)$ dos bases de L_1 y L_2 respectivamente como espacios vectoriales sobre de $\mathbb{Q}$. Podemos considerar entonces $(x_1, ..., x_m, y_1, ..., y_n)$ como base de $L = L_1 \times L_2$ como $\mathbb{Q}$-espacio vectorial. Por definición de la estructura producto, $x_i y_i = 0$, de donde se sigue que $Tr(x_i y_i) = 0$. En consecuencia el derterminante $D(x_1, ..., x_m, y_1, ..., y_m)$ es el determinante de la siguiente matriz

$$\begin{pmatrix} Tr(x_1x_1) & \dots & Tr(x_1x_m) & 0 & \dots & 0 \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ Tr(x_mx_1) & \dots & Tr(x_mx_m) & 0 & \dots & 0 \\ 0 & \dots & 0 & Tr(y_1y_1) & \dots & Tr(y_1y_n) \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & \dots & 0 & Tr(y_ny_1) & \dots & Tr(y_my_m) \end{pmatrix}$$

El valor de este determinante es

$$det(Tr(x_i x_j)) = det(Tr(y_i y_j))$$

luego,

$$D(x_1, ..., x_m, y_1, ..., y_n) = D(x_1, ..., x_m) \cdot D(y_1, ..., y_n)$$

■

Nota. En este contexto, decir que un ideal (d) generado por un elemento d está contenido en otro ideal (p), generado por p, es equivalente a decir que p divide a d.

Con esta aclaración podemos finalmente demostrar el resultado que estabamos buscando.

Teorema 4.3. *Sea $L/\mathbb{Q}$ una extensión de números y θ_L su cuerpo de números. Para que un ideal primo (p) de $\mathbb{Z}$ ramifique en L es necesario y suficiente que p divida a $\mathscr{D}_{\theta_L}$.*

Demostración. Se tiene que p divide a $\mathscr{D}_{\theta_L}$ si y sólo si $\mathscr{D}_{\theta_L} \equiv 0 \ mod \ p$. Por el lema 4.4,

$$\mathscr{D}_{\theta_L} \ mod \ p = \mathscr{D}_{\theta_L/(p)}$$

Luego, p divide a $\mathscr{D}_{\theta_L}$ si y sólo si $\mathscr{D}_{\theta_L/(p)} = \bar{0}$ en $(\mathbb{Z}/p\mathbb{Z})$.

En la descomposición de $\theta_L/(p)$ dada en (17), cada factor $\theta_L/\mathfrak{B}_i^{e_i}$ es un $(\mathbb{Z}/p\mathbb{Z})$-espacio vectorial, ya que $p \in \mathfrak{B}_i^{e_i}$ para cada i. Entonces, por el lema 4.5,

$$\mathscr{D}_{\theta_L/(p)} = \prod_{i=1}^{r} \mathscr{D}_{\theta_L/\mathfrak{B}_i^{e_i}}$$

Entonces, hay que probar que para cualquier primo p y cualquier ideal que es potencia de un primo $\mathfrak{B}^e$, con (p) que divide a $\mathfrak{B}^e$, se tiene que el discriminante $\mathscr{D}_{\theta_L/\mathfrak{B}^e}$ es $\bar{0}$ en $(\mathbb{Z}/p\mathbb{Z})$ si y sólo si $e > 1$.

Notemos que el valor del discriminante es independiente de la elección de la base. Supongamos que $e > 1$. Entonces, todo elemento $x \in \mathfrak{B} - \mathfrak{B}^e$ es un elemento nilpotente no nulo de $\theta_L/\mathfrak{B}^e$. Denotemos entonces $\bar{x} = \bar{x_1}$ y consoideremos la $(\mathbb{Z}/p\mathbb{Z})$-base de $\theta_L/\mathfrak{B}^e$ $\{\bar{x_1}, ..., \bar{x_n}\}$. Consideremos la matriz de la aplicación lineal de la traza Tr. Los elementos de la primera columna de esta matriz son los números dados por $Tr(\bar{x_i}\bar{x})$. Observemos que $\bar{x_i}\bar{x}$ es nilpotente, entonces la aplicación lineal de la multiplicación $m_{\bar{x_i}\bar{x}}$ en $\theta_L/\mathfrak{B}^e$ es también nilpotente. Por lo tanto, sus autovalores son igual a cero. Esto significa que las trazas $Tr(\bar{x_i}\bar{x}) = \bar{0}$. Entonces toda la primera columna de la matriz de $Tr(\bar{x_i}\bar{x_j})$ es nula, luego $\mathscr{D}_{\theta_L/\mathfrak{B}^e} = \bar{0}$.

Supongamos ahora que $e = 1$. Entonces $\theta_L/\mathfrak{B}^e = \theta_L/\mathfrak{B}$ esun cuerpo finito de característica p. Queremos probar que $\mathscr{D}_{\theta_L/\mathfrak{B}} \neq \bar{0}$. Si este discriminante fuera $\bar{0}$, entonces, como $\theta_L/\mathfrak{B}$ es un cuerpo, la traza como aplicación lineal, $Tr : \theta_L/\mathfrak{B} \longrightarrow (\mathbb{Z}/p\mathbb{Z})$ es

idénticamente nula . En los cuerpos finitos, la traza puede escribirse como una función polinómica

$$Tr(t) = t + t^p + t^{p^2} + ... + t^{p^{s-1}}$$

donde $p^s = |\theta_L/\mathfrak{B}|$. Como el grado de Tr como polinomio es menor que el número de elementos en $\theta_L/\mathfrak{B}$, la función $Tr(t)$ no es idénticamente nula en $\theta_L/\mathfrak{B}$ y por lo tanto, el discriminante de una extensión finita de $(\mathbb{Z}/p\mathbb{Z})$ no es igual a cero.

■

Nota. Un elemento x de un anillo se dice *nilpotente* si existe un entero positivo n tal que $x^n = 0$

5. Raíces primitivas de la unidad

El estudio de esta sección se ha basado en los textos [[5]] y [[8]]. Consideremos el cuerpo de los números complejos, $\mathbb{C}$. Para un entero positivo n, una raíz n-ésima de la unidad es una raíz del polinomio $t^n - 1$. Al ser $\mathbb{C}$ un cuerpo algebraicamente cerrado, el polinomio anterior tiene exactamente n raices distintas en él.
Como se verá a continuación, estas raíces forman un grupo cíclico de orden n, a cuyos generadores z se llaman *raíces primitivas de la unidad*. Habitualmente se maneja por simplicidad la raíz primitiva de la unidad dada por $z = exp\left(\frac{2\pi i}{n}\right)$. Las raíces primitivas de la unidad juegan un papel importante en diversas áreas de las matemáticas, como la teoría de números, la teoría de Galois y la teoría de la información. Además, están relacionadas con conceptos como los grupos cíclicos y los cuerpos ciclotómicos, los cuales se introducirán en la sección [6].

Dada una raíz primitiva de la unidad, z, todas las demás raices primitivas de la unidad son de la forma z^r, donde r es un número entero tal que $1 \leq r \leq n$, y m.c.d(r,n)=1. Como el conjunto formado por los elementos $\{z, z^2, ..., z^{n-1}, z^n = 1\}$ forma el grupo multiplicativo de las raices de la unidad, y los generadores de dicho grupo son las raíces primitivas z^r, existe una correspondencia entre las raíces primitivas n-ésimas de la unidad y los elementos del grupo $(\mathbb{Z}/n\mathbb{Z})^*$ de unidades del anillo de enteros modulares $(\mathbb{Z}/n\mathbb{Z})$.
El grupo de las raíces n-ésimas de la unidad se denotará por μ_n y el subconjunto de μ_n formado por las raíces primitivas por T_n.

Proposición 5.1. *Se define la aplicación $h_r : \mu_n \longrightarrow \mu_n$, que lleva el elemento $\eta \in \mu_n$ en $\eta^r \in \mu_n$; $h_r(\eta) = \eta^r$, con $r \in \mathbb{Z}$ tal que m.c.d(r,n)=1. Entonces, h_r es un automorfismo de grupos.*

Demostración. Probemos que se trata de un homomorfismo de grupos.
Sean η, $\xi \in \mu_n$, entonces $h_r(\eta \cdot \xi) = (\eta \cdot \xi)^r = (\eta)^r \cdot (\xi)^r = h_r(\eta) \cdot h_r(\xi)$

■

Con este resultado ya se está en condiciones de probar y estudiar la relación existente entre el grupo $(\mathbb{Z}/n\mathbb{Z})^*$ (grupo de unidades del anillo de enteros modulares $(\mathbb{Z}/n\mathbb{Z})$) y el grupo de automorfismos de las raíces de la unidad μ_n.

Proposición 5.2. *Existe un isomorfismo canónico f entre el grupo $(\mathbb{Z}/n\mathbb{Z})^*$ y el grupo de automorfismos de μ_n, $Aut(\mu_n)$, que lleva la clase r mod n en el automorfismo h_r definido como antes.*

Demostración. Se considera el grupo $(\mathbb{Z}/n\mathbb{Z})^*$ con la operación producto modular, y el grupo μ_n con el producto complejo, $\cdot$.
Podemos considerar el grupo de las raíces en su forma exponencial,

$$\mu_n = \{1, exp\left(\frac{\theta}{n}\right), exp\left(\frac{2\theta}{n}\right), ..., exp\left(\frac{(n-1)\theta}{n}\right)\},$$

donde $\theta = 2\pi i$.
Tomemos la aplicación, $f : (\mathbb{Z}/n\mathbb{Z})^* \longrightarrow Aut(\mu_n)$, dada por $f(r) = h_r$. La biyectividad

de la aplicación se prueba de forma inmediata a partir de la definición de f.
En efecto, veamos que f es un isomorfismo:

Para $r, s \in (\mathbb{Z}/n\mathbb{Z})^*$ y $\eta \in \mu_n$:
$f(r) \cdot f(s) = h_r(\eta) \cdot h_s(\eta) = h_{r \cdot s}(\eta) = f(r \cdot s)$
lo que demuestra que efectivamente f es un homomorfismo; y en consecuencia, un isomorfismo.

■

El orden del grupo de automorfismos $Aut(\mu_n)$ es por tanto el valor de la *función ϕ de Euler* para n. Además que está función también tiene una estrecha relación con la cardinalidad del subgrupo de raíces primitivas T_n. Por tanto se tiene la siguiente proposición.

Proposición 5.3. *Se cumple $\phi(n) = |Aut(\mu_n)| = |T_n|$, para cada $n \in \mathbb{N}$.*

Demostración. Recuérdese que, por las definiciones, se tiene que

$$\phi(n) = |(\mathbb{Z}/n\mathbb{Z})^*| = |T_n|,$$

y se concluye por la Proposición 5.2.

■

6. Extensiones ciclotómicas

Esta sección se centrará en estudiar los conceptos y propiedades relativos al estudio de extensiones ciclotómicas de cuerpos, para ello se han utilizado las referencias [[5]],[[12]] y [[13]]. Los cuerpos ciclotómicos son casos particulares de los cuerpos de números algebraicos que poseen propiedades muy interesantes. Por ejemplo, son extensiones abelianas (es decir, de Galois y con grupo de Galois abeliano) de los números racionales y tienen una estructura algebraica bien definida. Además, tienen una estrecha relación con la teoría de números, ya que, por ejemplo, los números de Bernoulli, las unidades de cuerpos y las sumas de Gauss están relacionados con ellos.

La teoría de cuerpos ciclotómicos ha sido ampliamente estudiada y aplicada en varios campos de las matemáticas, incluyendo la teoría de números, la teoría de Galois y la geometría algebraica teórica.

Muchas definiciones y resultados que se utilizan en esta sección han sido introducidos previamente en la sección [1].

Definición 6.1. Se llama *extensión ciclotómica* de $\mathbb{Q}$ al cuerpo $\mathbb{Q}(z)$, resultante de adjuntar una raíz primitiva n-ésima de la unidad z al cuerpo de los números racionales.

Nota. El cuerpo $\mathbb{Q}(z)$ es el cuerpo de descomposición del polinomio $t^n - 1$, para $n > 1$. De hecho, cada una de las raíces del polinomio $t^n - 1$ es una potencia de la raíz primitiva z que genera $\mathbb{Q}(z)$, luego $\mathbb{Q}(z)$ es el cuerpo de descomposición del polinomio $t^n - 1$. Es por eso que cuando no se quiere hacer referencia de la raíz primitiva de la unidad elegida se denota la extensión ciclotómica por L_n, simplemente denotando el grado del polinomio antes mencionado.

Proposición 6.1. *Para cada n, la extensión ciclotómica L_n de $\mathbb{Q}$ es una extensión de Galois.*

Demostración. Se deduce del hecho de que L_n es normal por ser cuerpo de descomposición y separable por tratarse de cuerpos de característica 0.

■

Observación 17. En efecto, en característica 0, para todos los polinomios irreducibles $p(t)$ se tiene que $p'(t) \neq 0$; y $p(t)$ es primo con $p'(t)$, por ser $p(t)$ irreducible.

A partir de aquí, lo que se desea es caracterizar el grupo de Galois de la extensión ciclotómica $L_n = \mathbb{Q}(z)/\mathbb{Q}$, determinar el grado de la extensión e identificar el polinomio irreducible de z sobre $\mathbb{Q}$.

6.1. Polinomios ciclotómicos

Definición 6.2. Se define el *m-ésimo polinomio ciclotómico* como

$$h_n(t) = \prod_{z \in T_n} (t - z), \tag{20}$$

donde T_n es el conjunto de las raíces primitivas de la unidad, definido en la sección [5].

El polinomio ciclotómico $h_n(t)$ es el polinomio mónico y separable de $\mathbb{C}[t]$ cuyas raíces son exactamente las raíces n-ésimas primitivas de la unidad. El grado de $h_n(t)$ es entonces igual al número $\phi(n)$, dado por la función de Euler.

Ejemplo 6.1. Polinomios ciclotómicos de grados 1, 2 y 4 respectivamente:

- $h_1(t) = t - 1$
- $h_2(t) = t + 1$
- $h_4(t) = (t - i)(t + i) = t^2 + 1$

Ejemplo 6.2. Sea p un número primo. Estudiemos el caso del polinomio $h_p(t)$. En este caso, se tiene que todas las raíces p-ésimas son primitivas excepto para la raíz que es igual a 1. Entonces,

$$h_p(t) = \frac{(t^p - 1)}{(t - 1)} = t^{p-1} + t^{p-2} + ... + t + 1$$

Lema 6.1. *Sea n un entero positivo y sea $D = \{d \in \mathbb{Z}^+$ tal que d divide a $n\}$.*
Entonces,

$$t^n - 1 = \prod_{d \in D} h_d(t) \tag{21}$$

Además, se deduce, por recurrencia, que $h_n(t) \in \mathbb{Z}[t]$.

Demostración. Sabemos, por definición, que $t^n - 1 = \prod_{z \in \mu_n}(t - z)$.
Sea d el orden de z en $\mathbb{C}^*$. Entonces, d divide a n, y por lo tanto z es una raíz d-ésima primitiva de la unidad.
Recolectando todos los términos correspondientes a las raíces d-ésimas de la unidad en esta factorización se prueba la primera afirmación.

Se probará la segunda afirmación por inducción sobre n.
Para $n = 1$ es evidente, ya que $h_1(t) = t - 1$.
Supongamos ahora que para $d < n$, $h_d(t) \in \mathbb{Z}[t]$. Por la primera afirmación, que se ha demostrado arriba, se cumple que

$$t^n - 1 = \left(\prod_{\substack{d \in D \\ d < n}} h_d(t) \right) h_n(t)$$

Al ser $h_n(t)$ el resultado de la división entre $t^n - 1$ y $h_d(t)$, que son ambos polinomios mónicos con coeficientes en $\mathbb{Z}$, el algoritmo de la división polinómica demuestra por recurrencia que los coeficientes de $h_n(t)$ también deben de pertenecer a $\mathbb{Z}$.

■

Este lema permite calcular polinomios de orden superior de manera sencilla. Veamoslo con los siguientes ejemplos:

Ejemplo 6.3. Calculemos el polinomio ciclotómico de grado 8, $h_8(t)$ a partir de polinomios ciclotómicos de orden inferiores. En virtud del lema anterior se tiene que

$$t^8 - 1 = h_8(t)h_4(t)h_2(t)h_1(t)$$

Por lo tanto,

$$h_8(t) = \frac{t^8 - 1}{(t-1)(t+1)((t-i)(t+i))} = t^4 + 1$$

Ejemplo 6.4. En el caso de que sea p un número primo se tiene que

$$t^p - 1 = h_1(t)h_p(t)$$

y también

$$t^{p^2} - 1 = h_1(t)h_p(t)h_{p^2}(t) \Longrightarrow t^{p^2} - 1 = (t^p - 1)h_{p^2}(t)$$

De aquí se sigue que

$$h_{p^2}(t) = \frac{t^{p^2} - 1}{t^p - 1} = t^{p(p-1)} + t^{p(p-2)} + ... + t^{2p} + t^p + 1.$$

Nota. En los ejemplos de polinomios ciclotómicos que se han mostrado hasta el momento se observa que los coeficientes son siempre 0, 1 ó -1. Esto es cierto para $n < 105$. A medida que aumenta n los coeficientes de estos polinomios pueden ser arbitrariamente grandes.

El lema 6.1 permite hallar los polinomios ciclotómicos de forma implícita y recurrente. Sin embargo existe una forma de hallarlos explícitamente haciendo uso de una propiedad combinatoria, que utiliza la *Función de Möbius*. Definamos primero esta función:

Definición 6.3. Se define la Función de Möbius, $\nu : \mathbb{N}/\{0\} \longrightarrow \mathbb{N}$, de la siguiente manera:

$$\nu(m) = \begin{cases} 1 & si \quad m = 1 \text{ o m factoriza como producto par de primos distintos} \\ -1 & si \quad \text{m factoriza como producto impar de primos distintos} \\ 0 & si \quad \text{m no es libre de cuadrados} \end{cases}$$

Utilizando esta función recién definida se obtiene la siguiente para polinomios ciclotómicos:

Proposición 6.2. *Se puede expresar el polinomio cilotómico $h_n(t)$ como producto alternado de polinomios de la forma $t^d - 1$, donde d es cualquier entero que divide a n, de la siguiente forma:*

$$h_n(t) = \prod_{d \in D} (t^d - 1)^{\nu(n/d)} \tag{22}$$

El siguiente teorema permite deducir el grado de una extensión ciclotómica sobre $\mathbb{Q}$.

Teorema 6.1. *Sea n un entero positivo. Entonces $h_n(t)$ es el polinomio irreducible sobre $\mathbb{Q}$ de z y de todas las raíces primitivas de la unidad.*

Para probar este resultado se utilizará un lema auxiliar, que se atribuye a Gauss, relativo a divisibilidad.

Lema 6.2. ***(de Gauss)*** *Si A un dominio de factorización única y $p \in A$ irreducible, supongamos que se tiene que p divide al producto $a \cdot b$, con $a, b \in A$. Entonces, o bien p divide a a, o bien p divide a b.*

En otras palabras, lo que este lema afirma es que si A es un dominio de factorización única y p es un elemento irreducible de A entonces el ideal (p) es primo.

Veamos primero la demostración del *Lema de Gauss*, para después abordar la demostración del *teorema 6.1.*

Demostración. Razonemos por reducción al absurdo. Supongamos que p es irreducible, que p divide a $a \cdot b$ pero que no divide ni a a ni a b. Si esto sucede, entonces exístiría un elemento $q \in A$ tal que $a \cdot b = p \cdot q$. Si se sustituyen a, b y q por sus factorizaciones únicas en A, se tienen dos factorizaciones distintas para $a \cdot b$. Una de ellas contiene a p, por ser la que se obtiene de multiplicar las faztorizaciones de p y q. La otra se obtiene al multiplicar las factorizaciones de a y b, y no contiene a p, lo cual es absurdo. Entonces se concluye que p divide a a o p divide a b.

■

Nota. El recíproco también es cierto pero para los aspectos que nos interesan en este trabajo nos valdría solo con estudiar esa implicación.

Demostración. (del teorema 6.1)
Se sabe de los lemas anteriores que $h_n(t)$ es un polinomio mónico y que sus coeficientes son enteros. Sea z la raíz de la unidad que genera la extensión ciclotómica $\mathbb{Q}(z)$. Por lo tanto, $h_n(t)$ debe ser múltiplo del polinomio irreducible $p(t)$ de z sobre $\mathbb{Q}$. Se quiere probar que $h_n(t) = p(t)$. Bastaría probar que el grado del polinomio $p(t)$ es igual a $\phi(n)$.
Veamos que todas las raíces n-ésimas primitivas de la unidad, es decir, las z^r tal que $mcd(r, n) = 1$ con $1 \leq r \leq n$, son también raíces de $p(t)$. Observemos que r es producto de números primos que no dividen a n. Esto implica que, por recurrencia, basta ver que para una raíz w de $p(t)$ y un número primo p que no divide a n, entonces w^p es otra raíz de $p(t)$.
Razonemos por reducción al absurdo. Supongamos que w^p no es raíz de $p(t)$. Entonces, w es raíz del polinomio $q(t^p)$, donde $q(t)$ cumple que $h_n(t) = t^n - 1 = p(t)q(t)$. Sabemos que $q(t)$ está bien definido ya que $p(t)$ divide a $h_n(t)$. Además, $p(t)$ y $q(t)$ no tienen raíces en común ya que las raíces de $h_n(t)$ son todas diferentes. Como $p(t)$ es irreducible, es el polinomio irreducible de w. Se tiene entonces que $p(t)$ divide a $q(t^p)$, es decir, existe otro polinomio $f(t)$ mónico y con coeficientes en $\mathbb{Z}$ tal que $q(t^p) = p(t)f(t)$.
Se sustituyen ahora los coeficientes en $\mathbb{Z}$ de estos polinomios, por sus clases módulo p en el cuerpo $\mathbb{Z}/p\mathbb{Z}$. Se obtienen así los polinomios $\bar{h_n}(t), \bar{p}(t), \bar{q}(t), \bar{f}(t)$ de $(\mathbb{Z}/p\mathbb{Z})[t]$, que cumplen las relaciones que existían entre los polinomios originales:

1. $\bar{h_n}(t) = \bar{p}(t)\bar{q}(t)$
2. $\bar{q}(t^p) = \bar{f}(t)\bar{p}(t)$
Además, en este cuerpo, $(\mathbb{Z}/p\mathbb{Z})$, se cumple que $c^p = c$, por lo tanto:
3. $\bar{q}(t^p) = [\bar{q}(t)]^p$
Luego entonces, de 2. se tiene:
4. $[\bar{q}(t)]^p = \bar{f}(t)\bar{p}(t)$
De esta última relación se deduce que $\bar{q}(t)$ y $\bar{p}(t)$ tienen raíces en común. Por lo tanto, de 1., se sigue que $t^n - 1$ tiene raíces múltiples. Esto último es absurdo ya que, como p no divide a n y por tanto n no es $\bar{0}$ en $(\mathbb{Z}/p\mathbb{Z})$, $t^n - 1$ y nt^{n-1} (polinomio derivado de $t^n - 1$), no tienen raíces en común.
Así se concluye que w^p sí es raíz de $p(t)$, y entonces $p(t) = h_n(t)$, como se quería demostrar.
■

6.2. Grupo de Galois de L_n

Estudiemos ahora el grupo de Galois correspondiente a una extensión ciclotómica. Observemos que los automorfismos de L_n actúan únicamente sobre las raíces de la unidad, ya que dejan invariantes los elementos que están en $\mathbb{Q}$.

Primero de todo calculemos el grado de la extensión ciclotómica n-ésima L_n.

Teorema 6.2. *Sea $L_n/\mathbb{Q}$ una extensión ciclotómica. Entonces $[L_n : \mathbb{Q}] = \phi(n)$.*

Demostración. Ya se sabe porque se ha mencionado antes que $L_n = \mathbb{Q}(z)$, donde z es una raíz n-ésima primitiva de la unidad. Al ser $h_n(t)$ el polinomio irreducible de z, cuyo grado es exactamente el valor $\phi(n)$, se tiene entonces que $[L_n : \mathbb{Q}] = \phi(n)$.
■

Corolario 6.1. *Sean n,m enteros positivos tal que mcd(n,m)=1, tal que $\mathbb{Q}(z_m) = L_n$ y $\mathbb{Q}(z_m) = L_m$. Entonces,*

$$\mathbb{Q}(z_n, z_m) = \mathbb{Q}(z_{nm})$$

y

$$\mathbb{Q}(z_n) \cap \mathbb{Q}(z_m) = \mathbb{Q}.$$

Demostración. Probemos primero la primera afirmación. Se tiene que $z_{nm}^n = z_m$ y $z_{nm}^m = z_n$, lo que prueba que $\mathbb{Q}(z_n, z_m) \subset \mathbb{Q}(z_{nm})$.
Por otro lado, como $mcd(n, m) = 1$, existen dos enteros $a, b \in \mathbb{Z}$, tales que $an + bm = 1$. Entonces,

$$z_{nm} = z_{nm}^{an} z_{nm}^{bm} = z_m^a z_m^b \in \mathbb{Q}(z_n, z_m)$$

Veamos la segunda igualdad. Como se acaba de ver, z_{mn}^n es una raíz m-ésima primitiva de la unidad, y $\mathbb{Q}(z_n)\mathbb{Q}(z_m) = \mathbb{Q}(z_{nm})$, donde el primero de estos cuerpos es el generado por los productos de los elementos de $\mathbb{Q}(z_n)$ y $\mathbb{Q}(z_m)$.
El resultado entonces se deduce de que la multiplicidad de la función de Euler, $\phi(nm) = \phi(n)\phi(m)$.
■

Con esto, puede describirse de forma sencilla el grupo de Galois de cualquier extensión ciclotómica que se tenga.
Según se ha mostrado en la sección relativa al estudio de las raíces de la unidad, [5], los automorfismos de μ_n, vienen dados por la función $\eta \longrightarrow \eta^r$. Cada automorfismo de $Gal(L_n/\mathbb{Q})$ está determinado por cómo actúa sobre la raíz que genera la extensión z. De aquí en adelante se denotarán los elementos del grupo $Gal(L_n/\mathbb{Q})$ por σ_s, y actuará de la siguiente manera:

$$\sigma_s\left(\sum_{i=0}^{\phi(n)-1} a_i z^i\right) = \left(\sum_{i=0}^{\phi(n)-1} a_i z^{si}\right), \quad 1 \leq s \leq n, \quad mcd(s,n) = 1$$

Es decir, la potencia s a la que se elevan los elementos $z^i \in L_n$ estará determinada módulo n. Para $\sigma_s, \sigma_r \in Gal(L_n/\mathbb{Q})$ se puede comprobar que

$$\sigma_s\sigma_r(z) = \sigma_s(z^r) = (\sigma_s(z))^r = z^{s\cdot r}$$

para s, r relativamente primos a n.

En otras palabras, existe un homomorfismo f de $Gal(L_n/\mathbb{Q})$ a $(\mathbb{Z}/n\mathbb{Z})^*$ que a cada $\sigma_s \in Gal(L_n/\mathbb{Q})$ le asigna un $f(\sigma) = s \in (\mathbb{Z}/n\mathbb{Z})^*$; y como el entero $s \in (\mathbb{Z}/n\mathbb{Z})^*$ determina el automorfismo σ_s, el homorfismo f será inyectivo, y $Gal(L_n/\mathbb{Q})$ será un grupo abeliano. Más aún, si n es un número primo, $Gal(L_n/\mathbb{Q})$ es de hecho cíclico.

En conlusión, los elementos $\sigma_s \in Gal(L_n/\mathbb{Q})$ elevan cada raíz n-ésima de la unidad a la potencia $f(\sigma_s) = s$. Por lo tanto, el homomorfismo f es independiente de la elección de z.

Definición 6.4. Sea p un número primo que no divide a n. El automorfismo $\sigma_p \in Gal(L_n/\mathbb{Q})$, definido como antes, se denomina el *elemento de Frobenius*.

Tras la caracterización del grupo de Galois de una extensión ciclotómica puede demostrarse el siguiente resultado.

Teorema 6.3. *Sea $L_n/\mathbb{Q}$ una extensión ciclotómica. Se cumple que $Gal(L_n/\mathbb{Q}) \cong Aut(\mu_n) = (\mathbb{Z}/n\mathbb{Z})^*$.*

Demostración. Sea f el homomorfismo entre $(\mathbb{Z}/n\mathbb{Z})^*$ y $Gal(L_n/\mathbb{Q})$ que se ha descrito antes. Entonces, sabemos que los elementos $\sigma \in Gal(L_n/\mathbb{Q})$ elevan todas las raíces n-ésimas de la unidad a la potencia dada por $f(\sigma)$.
Sea p un primo que no divide a n, y consideremos el elemento de Frobenius σ_p. Denotemos por θ_{L_n} al anillo de enteros de la extensión $L_n/\mathbb{Q}$ y sea $\mathfrak{p}$ un ideal primo presente en la factorización de $(p)\theta_{L_n}$. Por definición del elemento de Frobenius, se obtiene la relación $\sigma_p \equiv x^p \ mod\ p$, para todo $x \in \theta_{L_n}$. En particular, si $f = f(\sigma_p)$, se tiene que

$$z^f \equiv z^p \ mod\ p. \tag{23}$$

Recordemos que

$$\prod_{\substack{0\leq r\leq n-1\\ r\not\equiv p \bmod n}} (z^p - z^r) = p'(z^p) = nz^{p(n-1)} \tag{24}$$

donde $p(t) = t^n - 1$. Notemos que n es relativamente primo a p, $\mathfrak{p} \cap \mathbb{Z} = (p)\mathbb{Z}$ y z es una unidad en el anillo θ_{L_n}. Se concluye entonces de la ecuación (24) que

$$\prod_{\substack{0\leq r\leq n-1\\ r\not\equiv p \bmod n}} (z^p - z^r) \notin \mathfrak{p}.$$

La relación (23) implica que f representa la clase del residuo módulo p de n. Entonces, $f(Gal(L_n/\mathbb{Q}))$ contiene la clase del residuo módulo n de todos los primos p que no dividen a n. Pero esto justamente significa que $f(Gal(L_n/\mathbb{Q})) = (\mathbb{Z}/n\mathbb{Z})^*$, que es lo que se quería probar.

■

Nota. Esto significa, en virtud de la proposición 5.2, que el grupo $Gal(L_n/\mathbb{Q})$ es isomorfo a $Aut(\mu_n)$ y al grupo multiplicativo $(\mathbb{Z}/n\mathbb{Z})^*$. Esto último permite concluir que $Gal(L_n/\mathbb{Q})$ es un grupo abeliano.

6.3. Subextensiones de extensiones ciclotómicas.

El hecho de que el grupo de Galois de una extensión ciclotómica se identifique con el grupo de unidades de enteros modulares permite realizar el estudio de extensiones intermedias, mediante el teorema de correspondencia de Galois enunciado al final del capítulo [2].

Ejemplo 6.5. Estudiemos el caso para $n = 8$.
Ya hemos visto que para $n = 8$, $h_8(t) = t^4 + 1$. Como $G = Gal(L_8/\mathbb{Q})$ se corresponde con $(\mathbb{Z}/(8))^*$, que a su vez es isomorfo a $(\mathbb{Z}/(2) \times \mathbb{Z}/(2))^*$, ya que no existen elementos de orden 4 en G. Por lo tanto, $G = \{\bar{1}, \bar{3}, \bar{5}, \bar{7}\}$.
Existen tres subgrupos entonces en G distintos de él mismo y de $\{\bar{1}\}$:

- $S_1 = \{\bar{1}, \bar{3}\}$, que se corresponde con el cuerpo $\mathbb{Q}(\sqrt{-2}) = \mathbb{Q}(z + z^3)$.
- $S_2 = \{\bar{1}, \bar{5}\}$, que se corresponde con $\mathbb{Q}(i) = \mathbb{Q}(z^2)$.
- $S_3 = \{\bar{1}, \bar{7}\}$, correspondiente al cuerpo $\mathbb{Q}(\sqrt{2}) = \mathbb{Q}(z + z^7)$.

Ejemplo 6.6. Como se ha mencionado anteriormente, todos los polinomios ciclotómicos cuyo grado es $n < 105$ tienen coeficientes que son 0, 1 ó -1. Estudiemos entonces el caso $n = 105$.
Este caso en particular tiene un coeficiente igual a -2 acompañando a los términos de grado 41 y 7, en concreto:

$h_{105}(t) = t^{48} + t^{47} - t^{43} - t^{42} - 2t^{41} - t^{40} - t^{39} + t^{36} + t^{35} + t^{34} + t^{33} + t^{32} + t^{31} - t^{28} - t^{26} - t^{24} - t^{22} - t^{20} + t^{17} + t^{16} + t^{15} + t^{14} + t^{13} + t^{12} - t^9 - t^8 - 2t^7 - t^6 + t^5 + t^2 + t + 1.$

El grupo de Galois de esta extensión, $G = Gal(L_{105}/\mathbb{Q})$, es isomorfo al grupo de unidades $(\mathbb{Z}/(105))^*$. Utilizando el teorema de restos chinos, se sabe que este grupo es isomorfo al producto de grupos multiplicativos $(\mathbb{Z}/(3))^* \times (\mathbb{Z}/(5))^* \times (\mathbb{Z}/(7))^*$. Esto a su vez significa que es también isomorfo al producto de grupos aditivos $(\mathbb{Z}/(2)) \times (\mathbb{Z}/(4)) \times (\mathbb{Z}/(6))$.
Sin embargo, dos grupo son isomorfos si y sólo si tienen los mismos factores invariantes, y en este caso se tiene que $\{2, 4, 6\}$ no son los factores invariantes de G, ya que 4 no divide a 6.
G tendrá que ser isomorfo bien a $(\mathbb{Z}/(4)) \times (\mathbb{Z}/(12))$ o bien a $(\mathbb{Z}/(2)) \times (\mathbb{Z}/(2)) \times (\mathbb{Z}/(12))$ ya que los factores invariantes serán bien $\{4, 12\}$ o bien $\{2, 2, 12\}$, por haber en $(\mathbb{Z}/(2)) \times (\mathbb{Z}/(4)) \times (\mathbb{Z}/(6))$ 16 elementos de orden 12.
Observemos que en $(\mathbb{Z}/(4)) \times (\mathbb{Z}/(12))$ existen 26 elementos de orden 12, lo que hace descartar esta opción.
Por otro lado, en $(\mathbb{Z}/(2)) \times (\mathbb{Z}/(2)) \times (\mathbb{Z}/(12))$ hay exactamente 16 elementos de orden 12, lo que implica que G es isomorfo a este producto y sus factores invariantes son $\{2, 2, 12\}$.

Si p es un primo, el teorema 6.3 asegura que

$$Gal(L_p/\mathbb{Q}) \cong (\mathbb{Z}/p\mathbb{Z})^*$$

Mencionemos varias propiedades del grupo $(\mathbb{Z}/p\mathbb{Z})^*$, cuyas demostraciones no van a incluirse ya que pertenecen a la materia de la asignatura *Estructuras algebraicas* del grado, donde se estudian en profundidad los temas correspondientes a la teoría de grupos.

- El grupo $(\mathbb{Z}/p\mathbb{Z})^*$ es cíclico de orden $p - 1$.
- Para cada divisor f de $p - 1$, existe un único subgrupo $H_f \subset (\mathbb{Z}/p\mathbb{Z})^*$ de orden f.
- Sea $e = \frac{p-1}{f}$. Entonces $ef = p - 1$ y H_f tiene índice e en $(\mathbb{Z}/p\mathbb{Z})$.
- Si f y g son ambos divisores de $p - 1$, entonces $H_f \subset H_g$ si y sólo si f divide a g.

Mediante el isomorfismo existente entre $Gal(L_p/\mathbb{Q})$ y $(\mathbb{Z}/p\mathbb{Z})^*$ y en virtud al *teorema de correspondencia de Galois*, quedan determinadas las extensiones intermedias de $L_p/\mathbb{Q}$:

$$L_f = \{x \in L_p | \sigma(x) = x \text{ para todo } \sigma \text{ con } \sigma(z_p) = z_p^i, [i] \in H_f\}$$

donde f es cualquier entero que divida a $p - 1$.

Esta descripción de las subextensiones permite enunciar la siguiente proposición donde se muestran las propiedades y características de estos cuerpos intermedios:

Proposición 6.3. *Sea p un número primo impar, y f un entero positivo que divide a $p-1$. Entonces los cuerpos intermedios $\mathbb{Q} \subset L_f \subset L_p$ satisfacen:*

1. *L_f es una extensión de Galois de grado $e = \frac{p-1}{f}$.*
2. *Si f y g son dos divisores de $p-1$, entonces $L_f \subset L_g$ si y sólo si f divide a g.*
3. *Si f y g son dos divisores de $p-1$, entonces $Gal(L_f/L_g)$ es un grupo cíclico de orden g/f.*

Ejemplo 6.7. Veamos un ejemplo para este caso particular, con $p = 5$.

Se tiene entonces el polinomio ciclotómico

$$h_5(t) = \frac{t^5 - 1}{t - 1} = t^4 + t^3 + t^2 + t + 1$$

Se identifica $G = Gal(L_5/\mathbb{Q})$ con el grupo $(\mathbb{Z}/(5))^* = \{\bar{1}, \bar{2}, \bar{3}, \bar{4}\}$. En virtud de lo expuesto en los comentarios anteriores, este es un grupo cíclico de orden 4, y por lo tanto G también.
El único subgrupo de G distinto de $\{\bar{1}\}$ y de él mismo es $H_2 = \{\bar{1}, \bar{4}\}$, cuyo orden es 2. Este subrgrupo H_2 se identifica con el subcuerpo $L_2 = \mathbb{Q}(z + z^4) = \mathbb{Q}(\sqrt{5})$.

Por último, vamos a dar un teorema que se atribuye a los matemáticos *Leopold Kronecker* (Legnica, 1823 - Berlín, 1891) y *Heinrich Martin Weber* (Heidelberg, 1842 - Estrasburgo, 1913). Este teorema posee una relevancia enorme a la hora de estudiar y caracterizar los cuerpos intermedios de una extensión ciclotómica. Solo se enunciará, omitiéndose su demostración por resultar esta ajena a los temas que se tratan en este trabajo.

Definición 6.5. Se dice que una extensión es abeliana si es de Galois y su grupo de Galois es abeliano.

Teorema 6.4. ***(de Kronecker - Weber).*** *Sea $K/\mathbb{Q}$ una extensión de Galois y abeliana. Entonces, $K/\mathbb{Q}$ es una extensión intermedia de una extensión ciclotómica.*

6.4. El discriminante de un cuerpo ciclotómico

El discriminante es uno de los invariantes más importantes de un cuerpo de números, y es por ello que resulta de alto interés calcular el discriminante de los cuerpos ciclotómicos. Lo haremos en dos pasos. Primero, veremos que el discriminante de los cuerpos ciclotómicos cuyo grado es una potencia de un número primo está determinado, y es, en efecto, una potencia de este primo, salvo signo. El segundo paso consistirá en ver que dos cuerpos ciclotómicos cuyos grados son relativamente primos entre ellos son linealmente disjuntos.

Proposición 6.4. *Sea p un entero primo, y z una raíz primitiva de la unidad de orden p^ν. Entonces, el discriminante D de la base de potencias $\{1, z, ..., z^{\phi(p^\nu)-1}\}$ viene dado por*

$$D = (-1)^{\phi(p^\nu)/2} p^{p^{\nu-1}(p\nu-\nu-1)} \tag{25}$$

Demostración. En virtud del Lema 4.2 de la sección [4.3] aplicado a este caso particular, se obtiene que

$$D(1, z, ..., z^{\phi(p^\nu-1)})) = (-1)^{1/2n(n-1)} N_{\mathbb{Q}(z_{p^\nu})}(h'_{p^\nu}(z))$$

donde en este caso, $n = [\mathbb{Q}(z) : \mathbb{Q}] = p^{\nu-1}(p-1)$ y $h'_{p^\nu}(z)$ es el polinomio derivado del correspondiente polinomio ciclotómico envaluado en la raíz z.
Como $t^{p^\nu} - 1 = (t^{p^{\nu-1}} - 1)h_{p^\nu}(t)$, si se calculan las derivadas y se evalua en z se obtiene

$$h'_{p^\nu}(z) = \frac{p^\nu z^{p^\nu - 1}}{z^{p^{\nu-1}} - 1} = \frac{p^\nu z^{-1}}{z^{p^{\nu-1}}}$$

Notemos que $\eta = z^{p^{\nu-1}}$ es una raíz primitiva p-ésima de la unidad.
Se procede ahora evaluando la norma del numerador y del denominador por separado. Para el numerador, como z^{-1} es una raíz p^ν-ésima primitiva de la unidad, su norma es igual a 1. Entonces,

$$N_{\mathbb{Q}(z_{p^\nu})}(p^\nu z^{-1}) = p^{\nu\phi(p^\nu)} = N_{\mathbb{Q}(z_{p^\nu})}(z^{-1}) = p^{\nu p^{\nu-1}(p-1)}$$

Para el denominador, se va a tener en cuenta que $\mathbb{Q} \subseteq \mathbb{Q}(z_p) \subseteq \mathbb{Q}(z_{p^\nu})$. Se tiene además que $p = u(\eta - 1)^{p-1}$ para una unidad u. Entonces, $N_{\mathbb{Q}(z_p)}(\eta - 1)^{p-1} = N_{\mathbb{Q}(z_p)}(p) = p^{p-1}$, y por lo tanto, $N_{\mathbb{Q}(z_p)}(\eta - 1) = p$. En consecuencia,

$$N_{\mathbb{Q}(z_{p^\nu})}(\eta - 1) = N_{\mathbb{Q}(z_{p^\nu})}(N_{\mathbb{Q}(z_{p^{m\nu}})/\mathbb{Q}(z_p)}(\eta - 1) = (N_{\mathbb{Q}(z_p)}(\eta - 1)^{p^\nu - 1} = p^{p^{\nu-1}}$$

Y juntando las normas obtenidas para el numerador y el denominador se obtiene el resultado que se quería.

■

Vayamos entonces con el cálculo del discriminante para este tipo de cuerpos.

Teorema 6.5. *Sea n un número natural. Entonces el discriminante del cuerpo ciclotómico $\mathbb{Q}(z_n)$ viene dado por*

$$\mathscr{D}_{\mathbb{Q}(z_n)} = (-1)^{\phi(n)/2} \frac{n^{\phi(n)}}{\prod_{p \text{ divisior de } n} p^{\phi(n)/(p-1)}} \tag{26}$$

Demostración. Se va a probar la igualdad, salvo signo. Llamemos $\rho(n)$ al valor absoluto del lado derecho de la igualdad. Puede calcularse de forma sencilla que $\rho(nm) = \rho(n)^{\phi(m)}\rho(m)^{\phi(n)}$, siempre que n y m sean primos entre ellos. De hecho, debido a las buenas propiedades de la función de Euler para el producto, se tienen las siguientes igualdades

$$nm^{\phi(nm)} = (n^{\phi(n)})^{\phi(m)}(m^{\phi(m)})^{\phi(n)}$$

$$\prod_{\text{p divisor de n}} p^{\phi(nm)/(p-1)} = \prod_{p|n}(p^{\phi(n)/(p-1)})^{\phi(m)} \prod_{p|m}(p^{\phi(m)/(p-1)})^{\phi(n)}$$

Se probará el teorema por inducción en el número de factores primos distintos que existan en la descomposición de n. Para $n = 1$, la prueba se reduce al caso descrito en la proposición 6.4. Si n y m son entonces primos entre sí, los discriminantes $\mathscr{D}_{\mathbb{Q}(z_n)}$ y $\mathscr{D}_{\mathbb{Q}(z_m)}$ son también primos entre sí por inducción. Además, en virtud del corolario 6.1 las extensiones $\mathbb{Q}(z_n)$ y $\mathbb{Q}(z_m)$ son linealmente disjuntas. Del lema 4.5 (sección [4.5]), se sigue que

$$\mathscr{D}_{\mathbb{Q}(z_{nm})} = \pm(\mathscr{D}_{\mathbb{Q}(z_n)})^{\phi(m)}(\mathscr{D}_{\mathbb{Q}(z_m)})^{\phi(n)}$$

Se concluye con las igualdades mencionadas relativas a la función de Euler.

■

6.5. El anillo de enteros de un cuerpo ciclotómico

En general es complicado describir el anillo de enteros de un cuerpo de números. En esta sección se va a estudiar en anillo de los enteros sobre $\mathbb{Z}$ en el caso partícular del cuerpo ciclotómico $\mathbb{Q}(z)$, donde z es una raíz primitiva n-ésima primitiva de la unidad. Es muy poco habitual que exista un elemento primitivo concreto o calculable que genere el anillo de enteros de un cuerpo, pero como se ha ido viendo a lo largo de esta sección, los cuerpos ciclotómicos poseen una gran relevancia y son de alto interés debido a que en muchos casos son la excepción que definitivamente confirma la regla. Veamos que el anillo de enteros de $\mathbb{Q}(z)$ está generado por el elemento z.

Comencemos con el siguiente lema.

Lema 6.3. *Sea $n = p^\nu$ una potencia de un número primo p y sea $\lambda = 1 - z$, donde z es una raíz primitiva n-ésima de la unidad. Entonces el ideal (λ) del anillo de enteros $\theta_{\mathbb{Q}(z)}$ del cuerpo ciclotómico $\mathbb{Q}(z)$ es un ideal primo de grado 1, y se tiene que*

$$p\theta_{\mathbb{Q}(z)} = (\lambda)^{\phi(n)}$$

Demostración. El polinomio irreducible de z sobre $\mathbb{Q}$ es ciertamente el n-ésimo polinomio ciclotómico:

$$h_n(t) = \frac{t^{p^\nu} - 1}{t^{p^{\nu-1}} - 1} = t^{p^{\nu-1}(p-1)} + ... + t^{p^{\nu-1}} + 1$$

Para $t = 1$, se obtiene que

$$p = \prod_{r \in (\mathbb{Z}/n\mathbb{Z})} (1 - z^r)$$

Pero, $1 - z^r = \epsilon_r(1 - z)$, donde $\epsilon_r = \frac{1-z^r}{1-z} = 1 + z + ... + z^{r-1}$ es un entero de $\mathbb{Q}(z)$.

Si r es un número entero tal que $rr' \equiv 1 \ mod \ p^\nu$, entonces

$$\frac{1 - z}{1 - z^r} = \frac{1 - (z^r)^{r'}}{1 - z^r} = 1 + z^r + ... + (z^r)^{r'-1}$$

es un elemento entero también. Es decir, ϵ_r es entonces una unidad del anillo de enteros. En consecuencia, $p = \epsilon(1-z)^{\phi(p^\nu)}$, donde $\epsilon = \prod_{r\in(\mathbb{Z}/n\mathbb{Z})^*} \epsilon_r$. Y entonces, $p\theta_{\mathbb{Q}(z)} = (\lambda)^{\phi(p^\nu)}$. Como ya se ha visto que $\phi(p^\nu) = [\mathbb{Q}(z) : \mathbb{Q}]$, por la identidad de la proposición 3.5 de la sección [3.2], se concluye que (λ) es un ideal primo de $\theta_{\mathbb{Q}(z)}$ de grado 1.

■

El anillo de enteros de un cuerpo $\mathbb{Q}(z)$ está determinado, para un n concreto, como sigue:

Proposición 6.5. *Dada una raíz primitiva n-ésima z, el conjunto* $\{1, z, ..., z^{\phi(n)-1}\}$ *es una* $\mathbb{Z}$*-base del anillo de enteros* $\theta_{\mathbb{Q}(z)}$ *del cuerpo* $\mathbb{Q}(z)$*. En otras palabras,*

$$\theta_{\mathbb{Q}(z)} = \mathbb{Z} + z\mathbb{Z} + ... + z^{\phi(n)-1}\mathbb{Z} = \mathbb{Z}[z]$$

Demostración. Primero probaremos la proposición para el caso en el que $n = p^\nu$, con p primo. Se conoce por la proposición 6.4 que

$$D(1, z, ...z^{\phi(p^\nu)-1}) = (-1)^{\phi(p^\nu)/2} p^{p^{\nu-1}(p\nu-\nu-1)} = \pm p^{p^{\nu-1}(\nu p-\nu-1)}$$

Llamemos $s = p^{\nu-1}(\nu p - \nu - 1)$. Por el lema 4.3 de la sección [4.3] sabemos que

$$p^s\theta_{\mathbb{Q}(z)} \subseteq \mathbb{Z}[z] \subseteq \theta_{\mathbb{Q}(z)}$$

Escribamos como antes $\lambda = 1 - z$, por el lema anterior, 6.3, se tiene que

$$\theta_{\mathbb{Q}(Z)}/\lambda\theta_{\mathbb{Q}(z)} \simeq (\mathbb{Z}/p\mathbb{Z})$$

Entonces $\theta_{\mathbb{Q}(z)} = \mathbb{Z} + \lambda\theta_{\mathbb{Q}(z)}$, y en conclusión

$$\lambda\theta_{\mathbb{Q}(z)} + \mathbb{Z}[z] = \theta_{\mathbb{Q}(z)}$$

Multiplicando por λ y sustituyendo que $\lambda^2\theta_{\mathbb{Q}(z)} + \lambda\mathbb{Z}[z] = \theta_{\mathbb{Q}(z)}$, se obtiene que

$$\lambda^2\theta_{\mathbb{Q}(z)} + \mathbb{Z}[z] = \theta_{\mathbb{Q}(z)}$$

Por recurrencia se llega a que

$$\lambda^t\theta_{\mathbb{Q}(z)} + \mathbb{Z}[z] = \theta_{\mathbb{Q}(z)}, \quad t \geq 1$$

Si tomamos $t = s\phi(p^\nu)$, y en virtud de lo que se ha visto en el lema 6.3 de que $p\theta_{\mathbb{Q}(z)} = \lambda^{\phi(p^\nu)}$, se tiene que

$$\theta_{\mathbb{Q}(z)} = \lambda^t\theta_{\mathbb{Q}(z)} + \mathbb{Z}[z] = p^s\theta_{\mathbb{Q}(z)} + \mathbb{Z}[z] = \mathbb{Z}[z]$$

En el caso general, sea $n = p_1^{\nu_1} \cdot p_2^{\nu_2} \dots p_r^{\nu_r}$. Entonces, $z_i = z^{n/p_i^{\nu_i}}$ es una raíz primitiva $p_i^{\nu_i}$-ésima de la unidad, y en virtud del corolario 6.1 y de las propiedades multiplicativas de la función de Euler, se cumple que

$$\mathbb{Q}(z) = \mathbb{Q}(z_1) \dots \mathbb{Q}(z_r)$$

y

$$\mathbb{Q} = \mathbb{Q}(z_1)\dots\mathbb{Q}(z_{i-1}) \cap \mathbb{Q}(z_i)$$

Según lo que acabamos de ver, para cada $i = 1, ..., r$, el conjunto $\{1, z_i, ..., z_i^{\phi(p_i^{\nu_i}-1)}\}$ forman una base de enteros para la extensión $\mathbb{Q}(z_i)/\mathbb{Q}$.

Como los discriminantes de estas bases $D(1, z_i, ..., z_i^{\phi(p_i^{\nu_i})-1}) = \pm p_i^{s_i}$ son relativamente primos a pares, se concluye por el lema 4.5 de la sección [4.5] que el conjunto formado por los elementos de la forma $z_1^{j_1}\dots z_r^{j_r}$ con $j_r = 0, ..., \phi(p_i^{\nu_i}) - 1$, forma una base entera de $\mathbb{Q}(z)/\mathbb{Q}$.

Obserrvemos como cada uno de estos elementos es una potencia de z. Entoces cada $\alpha \in \theta_{\mathbb{Q}(z)}$ puede escribirse como un polinomio $\alpha = p(z)$ con coeficientes en $\mathbb{Z}$. Como el grado del polinomio irreducible de z sobre $\mathbb{Q}$, que es $h_n(t)$, es $\phi(n)$, se tiene que el grado del polinomio $p(z)$ será $\phi(n) - 1$. Así se obtiene que

$$\alpha = a_0 + a_1 z + ... + a_{\phi(n)-1} z^{\phi(n)-1}$$

Entonces se concluye que efectivamente, $1, z, ..., z^{\phi(n)-1}$ es una base entera.

■

Una vez hemos visto la fórmula del discriminante de un cuerpo ciclotómico en la sección [6.4] queda por calcularlo explícitamente y después hacer lo mismo para el polinomio ciclotómico correspondiente a esta, y ver, que según lo expuesto sobre que $\theta_{\mathbb{Q}(z)} = \mathbb{Z}[z]$ y utilizando el teorema 4.2 (sección [4.4]), estos dos discriminantes coinciden.

Ejemplo 6.8. Sea p un primo impar, y z una raíz primitiva p-ésima de la unidad. Consideremos entonces $L = \mathbb{Q}(z)$ el correspondente cuerpo ciclotómico. Se ha visto que $(1, z, ..., z^{p-2})$ es una base del anillo de enteros θ_L como $\mathbb{Z}$-módulo. y que el polinomio irreducible de z sobre $\mathbb{Q}$ es el polinomio ciclotómico, $h_p(t)$ que además satisface la relación $(t-1)h_p(t) = t^p - 1$. Calculemos el discriminante $\mathscr{D}_L$.
La fórmula descrita arriba nos dice que

$$D(1, z, ..., z^{p-2}) = (-1)^{(p-1)(p-2)/2} N(h_p'(z)) \tag{27}$$

Si derivamos a ambos lados de la relación $(t-1)h_p(t) = t^p - 1$, y se evalua en z, teniendo en cuenta que z es raíz de $h_p(t)$, se obtiene que

$$(z-1)h_p'(z) = pz^{p-1}$$

Se tiene además que $N(p) = p^{p-1}$, $N(z) = \pm 1$ y $N(z-1) = \pm p$. Sustituyendo estos valores en la ecuación (27), se tiene que

$$D(1, z, ..., z^{p-2}) = \pm p^{p-2} = \mathscr{D}_L$$

Esto prueba además que p es el único primo que ramifica en el cuerpo $\mathbb{Q}(z)$, si z es una raíz primitiva p-ésima de la unidad.

Calculemos el discriminante, tanto para el polinomio como para el cuerpo ciclotómico para ciertos valores concretos de n.

Ejemplo 6.9. Veamos por ejemplo el caso para $n = 12$:

Para este valor de n el polinomio ciclotómico será

$$h_{12}(t) = \frac{t^{12}-1}{h_6(t)h_4(t)h_3(t)h_2(t)h_1(t)} = \frac{t^{12}-1}{(t^2-t+1)(t^2+1)(t^2+t+1)(t+1)(t-1)} = t^4-t^2+1$$

Calculemos el discriminante de este polinomio, para ello haremos uso de la expresión (12), que expusimos en la sección [4.2] por la que

$$\Delta(h_{12}) = (-1)^{1/2\phi(12)(\phi(12)-1)} Res(h_{12}, h'_{12})$$

Haciendo cuentas se tiene que el resultado del resultante es $Res(h_{12}, h'_{12}) = 144$, y como $\phi(12) = 4$, se tiene que $\Delta(h_{12}(t)) = 144$. Calculemos ahora el discriminante de la extensión y veamos cómo coinciden. Por la fórmula (24) se tiene que

$$\mathscr{D}_{\mathbb{Q}(z_{12})} = (-1)^{\phi(12)/2} \frac{12^{\phi(12)}}{\prod_{p|n} p^{\phi(12)/(p-1)}} = (-1)^2 \frac{12^4}{(2^4)(3^2)} = (2^4)(3^2) = 16 \cdot 9 = 144.$$

Entonces, efectivamente, $\Delta(h_{12}(t)) = \mathscr{D}_{L_{12}}$

6.6. Ramificación de primos en cuerpos ciclotómicos

Conociendo ya explícitamente el anillo de enteros de un cuerpo ciclotómico estamos en condiciones de estudiar las leyes que dan lugar a la descomposición de los números primos sobre los cuerpos ciclotómicos.

Proposición 6.6. *Sea $n = \prod_p p^{\nu_p}$ la descomposición del entero n en factores de potencias de primos. Considérese para cada p, el mínimo entero positivo f_p tal que*

$$p^{f_p} \equiv 1 \ mod \ \frac{n}{p^{\nu_p}}$$

Entonces en $\mathbb{Q}(z)$, con z una raíz n-ésima primitiva de la unidad, se tiene la siguiente factorización

$$\mathfrak{p} = (\mathfrak{p}_1 \cdots \mathfrak{p}_r)^{\phi(p^{\nu_p})}$$

donde $\mathfrak{p}_1, ..., \mathfrak{p}_r$ son ideales primos distintos de grado f_p.

Demostración. Como el anillo de enteros es $\mathbb{Z}[z]$ el conductor es igual a 1, y se puede aplicar la proposición 3.5 de la sección [3.2] a cualquier primo p. En consecuencia, todo primo p se descompone en ideales primos exactamente de la misma forma que lo hace el polinomio ciclotómico $h_n(t)$ en polinomios irreducibles módulo p. Entonces basta demostrar que

$$h_n(t) \equiv (p_1(t) \cdots p_r(t))^{\phi(p^{\nu_p})} \ mod \ p$$

donde $p_1(t), ..., p_r(t)$ son distintos polinomios irreducibles en $(\mathbb{Z}/p\mathbb{Z})$ de grado f_p.
Para probar eso, pongamos que $n = p^{\nu_p}m$. ξ_i, η_j recorren el conjunto de las raíces primitivas de la unidad de orden m y p^{ν_p} respectivamente. Entonces, su producto $\xi_i\eta_j$ recorre el conjunto de las raíces primitivas n-ésimas. Por lo tanto, se tiene la siguiente descomposición sobre $\mathbb{Z}[z]$:

$$h_n(t) = \prod_{i,j}(t - \xi_i\eta_j)$$

Como $t^{p^{\nu_p}} - 1 \equiv (t-1)^{p^{\nu_p}} \ mod\ p$, se tiene que $\eta_j \equiv 1 \ mod\ \mathfrak{p}$, para cualquier $\mathfrak{p}|p$. En otras palabras,

$$h_n(t) \equiv \prod_i (t - \eta_i)^{\phi(p^{\nu_p})} = h_m(t)^{\phi(p^{\nu_p})} \ mod\ \mathfrak{p}$$

Teniendo en cuenta que f_p es el menor entero positivo tal que $p^{f_p} \equiv 1 \ mod\ m$, es obvio que la congruencia anterior nos reduce al caso en el que $p \not| \ n$, y entonces $\phi(p^{\nu_p}) = \phi(1) = 1$.

Como la característica p de $\mathbb{Z}[z]/\mathfrak{p}$ no divide a n, los polinomios $t^n - 1$ y nt^{n-1} no tienen raíces en común en $\mathbb{Z}[z]/\mathfrak{p}$. Luego, $t^n - 1 \ mod\ p$ no tiene raíces múltiples. Entonces, la aplicación de paso al cociente $\mathbb{Z}[z] \longrightarrow \mathbb{Z}[z]/\mathfrak{p}$ conecta de forma biyectiva el grupo de raíces n-ésimas de la unidad μ_n y el grupo de las raíces n-ésimas de la unidad en $\mathbb{Z}[z]/\mathfrak{p}$. En particular, la raíz n-ésima primitiva z módulo $\mathfrak{p}$ sigue siendo una raíz primitiva n-ésima. La mínima extensión de $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ que la contiene es $\mathbb{F}_{p^{f_p}}$ ya que su grupo multiplicativo $(\mathbb{F}_{p^{f_p}})^*$ es cíclico de orden $p^{f_p} - 1$. Por lo tanto el polinomio cilotómico reducido

$$\bar{h_n}(t) = h_n(t) \ mod\ p$$

se descompone en $\mathbb{F}_{p^{f_p}}$.
Como es un divisor de $t^n - 1 \ mod\ p$, este polinomio no tiene raíces múltiples. Si

$$\bar{h_n}(t) = \bar{p_1}(t) \cdots \bar{p_r}(t)$$

es la factorización del polinomio en $\mathbb{F}_p$ entonces cada factor $\bar{p_i}(t)$ es el polinomio irreducible de una raíz pirimitiva n-ésima de la unidad $\bar{\xi} \in (\mathbb{F}_{p^{f_p}})^*$. Su grado es entonces f_p, lo que concluye la demostración.

■

Veamos dos casos particulares que se deducen de aplicar esta proposición:

Corolario 6.2. *Para una extensión $\mathbb{Q}(z)/\mathbb{Q}$ de grado n, un número primo p ramifica en $\mathbb{Q}(z)$ si y sólo si*

$$n \equiv 0 \ mod\ p$$

excepto si $p = 2$.

Proposición 6.7. *Sean q y p dos números primos impares, $q^* = (-1)^{(q-1)q/2}$ y z una raíz primitiva q-ésima de la unidad. Entonces se tiene que p factoriza completamente en $\mathbb{Q}(\sqrt{q^*})$ si y sólo si p factoriza en $\mathbb{Q}(z)$ en un número par de ideales primos.*

Este último deriva de la proposición anterior y de ciertos cálculos llevados a cabo en la prueba de la ley de reciprocidad cuadrática de Gauss.

7. Ley de reciprocidad cuadrática.

En esta sección se pretende dar a conocer uno de los resultados más importantes en la historia del desarrollo de la teoría de números. Como referencias principales para este capítulo se han utilizado [[10]] y [[13]]. La *ley de reciprocidad cuadrática* es una parte importante de la teoría de números que tiene muchas aplicaciones prácticas en la criptografía moderna y otros campos de las matemáticas y la computación. Esta ley establece condiciones bajo las cuales es posible determinar si un número es un residuo cuadrático módulo un número primo p en función de si otro número es un residuo cuadrático módulo otro número primo q. La relación entre p y q determina las condiciones y se expresa en términos de los símbolos de Legendre, introducidos por el matemático francés *Adrien-Marie Legendre* (París, 1752 - Auteuil, 1833).

Existen muchas pruebas, todas sumamente ingeniosas, para este resultado. En este caso va a exponerse una que se basa en las llamadas sumas cuadráticas de Gauss. Esta demostración es la primera que conecta este teorema con los cuerpos ciclotómicos, teniendo en cuenta que cada cuerpo cuadrático $\mathbb{Q}(\sqrt{d})$ con d no cuadrado, es subcuerpo de un cuerpo ciclotómico $\mathbb{Q}(z)$. Esto permitió deducir la ley de reciprocidad cuadrática a partir de un teorema de reciprocidad para el caso ciclotómico.

Definición 7.1. Dado un primo impar p y un entero d que es primo con p, se dice que *"d es residuo cuadrático de p"* si d es un entero congruente con un cuadrado perfecto módulo p. Es decir, si tiene solución la congruencia

$$x^2 \equiv d \ mod \ p \tag{28}$$

Definición 7.2. Dado un entero d y un primo impar p se define el *símbolo de Legendre* de le siguiente manera:

$$\left(\frac{d}{p}\right) = \begin{cases} 0 & \text{si p es divisor de d} \\ +1 & \text{si d es residuo cuadrático mod p} \\ -1 & \text{si d es no residuo cuadrático mod p} \end{cases}$$

Nota. En algunos textos se define el símbolo de Legendre únicamente para los enteros d que son primos con p, y se omite entonces el caso en el que la función pueda valer cero.

Observación 18. Como se tiene que el grupo de unidades $\mathbb{F}_p^*$ es cíclico de orden $p-1$, entonces los cuadrados de este grupo forman un subgrupo $\mathbb{F}_p^{*2}$ cuyo índice es 2, y $\mathbb{F}_p^*/(\mathbb{F}_p^*)^2$ es isomorfo a $-1, 1$. Entonces se tiene la siguiente cadena de homomorfismos,

$$\mathbb{Z} - (p)\mathbb{Z} \to F_p^* \to F_p^*/(\mathbb{F}_p^{*2}) \simeq \{+1, -1\}$$

Veamos primero una ecuación relativa al símbolo de Legendre:

Proposición 7.1. *(Criterio de Euler). Sea p un primo impar y $d \in \mathbb{Z} - (p)\mathbb{Z}$, entonces*

$$\left(\frac{d}{p}\right) = d^{(p-1)/2} (mod \ p) \tag{29}$$

Demostración. Sea w una raíz primitiva *mod* p. Entonces $d \equiv w^j \ (mod\ p)$, con $0 \leq j \leq p-2$, ya que la clase residuo $\bar{w}$ de w genera $\mathbb{F}_p^*$. Es obvio que entonces d es residuo cuadrático si y sólo si j es par. Por lo tanto, $\left(\frac{d}{p}\right) = (-1)^j$.

Por otro lado, $\mathbb{F}_p^*$ contiene únicamente un elemento de orden dos. Este elemento puede escribirse como $\bar{w}^{(p-1)/2}$ o como -1. En $\mathbb{Z}$ se tiene que $-1 \equiv w^{(p-1)/2} \ (mod\ p)$. Entonces,

$$\left(\frac{d}{p}\right) = (-1)^j \equiv w^{j(p-1)/2} \equiv d^{(p-1)/2} \ (mod\ p)$$

■

Nota. Si existe $x \in \mathbb{Z}$, con $0 \leq x \leq p-1$ y tal que todo elemento y que no sea múltiplo de p es congruente módulo p a una potencia de x entonces se dice que x es una raíz primitiva módulo p.

Con esto ya estamos en condiciones de poder enunciar y probar la ley de reciprocidad cuadrática, que como se ha avanzado antes posee una gran importancia en el campo de la teoría de números.

La cadena de homomorfismos descrita en la observación 14 lleva a la siguiente fórmula

$$\left(\frac{dc}{p}\right) = \left(\frac{d}{p}\right)\left(\frac{c}{p}\right), \quad d, c \in \mathbb{Z} - (p)\mathbb{Z}. \tag{30}$$

A partir de esta relación se enuncia el siguiente teorema.

Teorema 7.1. *(Ley de reciprocidad cuadrática de Legendre-Gauss.) Sean p y q dos primos impares distintos. Entonces se cumple que*

$$\left(\frac{q}{p}\right)\left(\frac{p}{q}\right) = (-1)^{(q-1)(p-1)/4} \tag{31}$$

La demostración utiliza las sumas cuadráticas de Gauss, que requiere de ciertos resultados auxiliares para su desarrollo. Estos se enunciarán y probarán a continuación para poder utilizarse en la prueba del teorema. Gauss proporcionó numerosas pruebas para este teorema, siendo esta la cuarta hablando en términos cronológicos.

Proposición 7.2. *Sea p un número primo impar. Entonces, exactamente la mitad de los enteros d, con* $1 \leq d \leq p-1$*, son residuo cuadrático módulo p.*

Demostración. Definamos el conjunto $C = \{1^2, 2^2, ..., \left(\frac{p-1}{2}\right)^2\}$. Observemos que en C no existe ningún par de números que sean congruentes módulo p. Esto significa que al menos existen $\frac{p-1}{2}$ elementos que son residuo cuadrático módulo p.
Ahora, sea d resiudo cuadrático módulo p. Existe entonces un elemento x tal que $x^2 \equiv d\ mod\ p$. También es cierto entonces que $(p-x)^2 \equiv (-x)^2 \equiv d\ mod\ p$. Alguno de estos dos elementos, x o $-x$, debe ser menor que $\frac{p-1}{2}$, por lo que entonces $d \in C$. Esto quiere decir que todo residuo cuadrático módulo p tiene que estar en C, y hay entonces exactamente $\frac{p-1}{2}$ residuos cuadráticos.

■

Consideremos ahora una raíz n-ésima primitiva de la unidad z, entonces por las propiedades de estas expuestas en la sección [5], sabemos que

$$z^r = z^s \Longleftrightarrow r \equiv s \; mod \; n$$

Definición 7.3. Sea d un número entero, p un número primo impar y z una raíz p-ésima primitiva de la unidad. Se define la *suma cuadrática de Gauss*

$$\tau_d = \sum_{s=0}^{p-1} \left(\frac{s}{p}\right) z^{d \cdot s}$$

Lema 7.1.

$$\sum_{s=0}^{p-1} \left(\frac{s}{p}\right) = 0$$

Demostración. Para $s = 0$, ya sabemos que el símbolo de Legendre es nulo, por definición. Por la proposición 7.2, sabemos que existen exactamente $\frac{p-1}{2}$ términos en los que el símbolo de Legendre vale +1, y otros $\frac{p-1}{2}$ en los que vale -1, lo que permite concluir la prueba. ■

Demostración. (*de la ley de reciprocidad cuadrática*)

Sea z una raíz primitiva p-ésima de la unidad, que pertenece una extensión de $\mathbb{F}_q$. Como entonces $z^p = 1$, la potencias z^x está bien definida para $x \in \mathbb{F}_p$. Se considera las suma cuadrática de Gauss, definida como en la definición 7.3,

$$\tau_d = \sum_{x \in \mathbb{F}_p^*} \left(\frac{x}{p}\right) z^{d \cdot x} = \sum_{x=0}^{p-1} \left(\frac{x}{p}\right) z^{d \cdot x}$$

Esta suma pertenece a una extensión del cuerpo $\mathbb{F}_q$. Haciendo $y = d \cdot x$, τ_d queda:

$$\tau_d = \sum_{y \in F_p^*} \left(\frac{yd^{-1}}{p}\right) z^y$$

Esto, según la igualdad (30) es igual a

$$\tau_d = \left(\frac{d^{-1}}{p}\right) \sum_{y \in F_p^*} \left(\frac{y}{p}\right) z^y$$

Por lo tanto,

$$\tau_d = \left(\frac{d}{p}\right) \tau_1 \tag{32}$$

Tengamos en cuenta que se está trabajando sobre un cuerpo cuya característica es q, y que además $\left(\frac{x}{p}\right) \in \mathbb{F}_q$. Entonces, si se identifica q con la clase de su residuo módulo p se tiene que

$$\tau_1^q = \sum_{x \in \mathbb{F}_p^*} \left(\frac{x}{p}\right)^q z^{q \cdot x} = \tau_q \tag{33}$$

Calculemos entonces el valor de τ_1^2:

$$\tau_1^2 = \sum_{x,y \in \mathbb{F}_p^*} \left(\frac{x}{p}\right)\left(\frac{y}{p}\right) z^{x+y}$$

Escribimos $y = tx$. Entonces

$$\tau_1^2 = \sum_{x,t \in \mathbb{F}_p^*} \left(\frac{x}{p}\right)^2 \left(\frac{t}{p}\right) z^{x(1+t)} = \sum_{x,t \in \mathbb{F}_p^*} \left(\frac{t}{p}\right) z^{x(1+t)} = \sum_{t \in \mathbb{F}_p^*} \left[\left(\frac{t}{p}\right) \sum_{x \in \mathbb{F}_p^*} z^{x(1+t)}\right]$$

Ahora debemos distinguir varios casos distintos:

- Si $z^{1+t} \neq 1$, utilizando la fórmula para las sumas geométricas se tiene que $\sum_{j=0}^{p-1} (z^{1+t})^j = 0$. Además, como $(z^{1+t})^0 = 1$, se tiene que

$$\sum_{x \in \mathbb{F}_p^*} z^{x(1+t)} = -1$$

- Si $z^{1+t} = 1$, entonces $\sum_{x \in \mathbb{F}_p^*} z^{x(1+t)} = p - 1$; y como z es una raíz primitiva p-ésima esto ocurre si y sólo si $t = -1$.

Con todo esto, volviendo a la expresión de arriba,

$$\tau_1^2 = \left(\frac{-1}{p}\right)(p-1) - \sum_{\substack{t \in \mathbb{F}_p^* \\ t \neq -1}} \left(\frac{t}{p}\right)$$

Por el lema 7.1, en el segundo término del lado derecho de la igualdad sólo sobrevive un término, ya que el resto son nulos. Entonces,

$$\tau_1^2 = \left(\frac{-1}{p}\right)(p-1) + \left(\frac{-1}{p}\right) = \left(\frac{-1}{p}\right) p$$

Del criterio de Euler que se ha probado en propsición 7.1 se sigue que

$$\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2} mod\ p$$

Y por lo tanto,

$$\tau_1^2 = (-1)^{(p-1)/2} p \tag{34}$$

Observemos que esto en particular significa que $\tau_1 \neq 0$. De las igualdades (32) y (33), se deduce que

$$\tau_1^q = \tau_q = \left(\frac{q}{p}\right) \tau_1$$

luego

$$\tau_1^{q-1} = \left(\frac{q}{p}\right)$$

De (34) se sigue que

$$\left(\frac{q}{p}\right) = (\tau_1^2)^{(q-1)/2} = (-1)^{(p-1)(q-1)/4} p^{(q-1)/2} = (-1)^{(p-1)(q-1)/4} \left(\frac{p}{q}\right)$$

Donde la última igualdad se ha deducido de nuevo aplicando el criterio de Euler. Además, como $\left(\frac{p}{q}\right) = \left(\frac{p}{q}\right)^{-1}$, se concluye entonces que

$$\left(\frac{q}{p}\right)\left(\frac{p}{q}\right) = (-1)^{(p-1)(q-1)/4}$$

■

A partir de esta ley derivan una serie de fórmulas, llamadas *fórmulas complementarias* que se dan a continuación:

Proposición 7.3. *(Fórmulas complementarias.) Sea p un primo impar, entonces:*

a)

$$\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2} = \begin{cases} +1 & si\ p \equiv 1\ mod\ 4 \\ -1 & si\ p \equiv 3\ mod\ 4 \end{cases} \tag{35}$$

b)

$$\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8} = \begin{cases} +1 & si\ p \equiv \pm 1\ mod\ 8 \\ -1 & si\ p \equiv \pm 3\ mod\ 8 \end{cases} \tag{36}$$

Demostración. Observemos como la expresión en a) es un caso particular del criterio de Euler descrito en la proposición 7.1.

Por otro lado, notemos que para $p = 1, 3, 5, 7$ se tiene que $p^2 \equiv 1\ mod\ 8$. Por lo que la fórmula en b) tiene sentido. Además, observemos que en el grupo $H = \{1, 3, 5, 7\}$, que es el grupo de las unidades del anillo $(\mathbb{Z}/8\mathbb{Z})$, el conjunto $H' = \{1, 7\}$ forma un subgrupo dentro de H y este tiene índice 2.
Definamos $f(x) = 1$ para $x \in H'$ y $f(x) = -1$ para $x \in H - H'$, y tal que f cumple que $f(xy) = f(x)f(y)$ para todo $x, y \in H$. Sea z una raíz primitiva de la unidad de orden 8 en una extensión $\mathbb{F}_p$. Consideremos las sumas cuadráticas de Gauss definidas como en 7.3, para $d \in H$,

$$\tau_d = \sum_{x \in H} f(x) z^{dx}$$

Como en la prueba del teorema 7.1, se tiene que $\tau_d = f(x)\tau_1$ y $\tau_1^p = \tau_p$, donde p se identifica con la clase de su residuo módulo 8. De la definición de $f(x)$ y del hecho de que $z^8 = 1, z^4 = -1$ se sigue que

$$\tau_1 = z - z^3 - z^5 + z^7 = (1 - z^2)(z - z^5) = z(1 - z^2)(1 - z^4) = 2z(1 - z^2)$$

En consecuencia,

$$\tau_1^2 = 4z^2(1 - 2z^2 + z^4) = -8z^4 = 8$$

De nuevo, como en la demostración del teorema 7.1 se tiene que $\tau_1^p = \tau_p = f(p)\tau_1$.

También se ve que

$$f(x) = (\tau_1^2)^{(p-1)/2} = 8^{(p-1)/2} = \left(\frac{8}{p}\right) = (*)$$

Por la proposición 7.1 se deduce que esto es igual a

$$(*) = \left(\frac{2}{p}\right)^3 = \left(\frac{2}{p}\right)$$

Por lo tanto,

$$\left(\frac{2}{p}\right) = f(p)$$

Ahora, haciendo los cálculos para $x = 1, 3, 5, 7$, o de forma equivalente para $x = 1, 3, -3, -1$, puede demostrarse que $f(x) = (-1)^{(x^2-1)/8}$ y que $(-1)^{(x^2-1)/8}$ depende únicamente de la clase del residuo de x módulo 8.

■

Terminemos con un par de ejemplos de para qué sirve este teorema.

Ejemplo 7.1. La ley de reciprocidad cuadrática y las posteriores fórmulas complementarias hacen posible el cálculo del símbolo de Legendre realizando sucesivas reducciones:

$$\left(\frac{23}{59}\right) = (-1)^{11\cdot 29}\left(\frac{59}{23}\right) = -\left(\frac{13}{23}\right) = -(-1)^{6\cdot 11}\left(\frac{23}{13}\right) = -\left(\frac{10}{13}\right) =$$

$$= -\left(\frac{-3}{13}\right) = -\left(\frac{-1}{13}\right)\left(\frac{3}{13}\right) = -(-1)^6\left(\frac{3}{13}\right) =$$

$$= -(-1)^{6\cdot 1}\left(\frac{13}{3}\right) = -\left(\frac{1}{3}\right) = -1$$

En consecuencia, 23 no es residuo cuadrático de 59.

Ejemplo 7.2. Veamos otro ejemplo

$$\left(\frac{1569}{6353}\right) = \left(\frac{3}{6353}\right)\left(\frac{523}{6353}\right) = \left(\frac{2}{3}\right)\left(\frac{77}{523}\right) = -\left(\frac{77}{523}\right)$$

Entonces ahora restaría calcular $\left(\frac{7}{523}\right)$:

$$\left(\frac{77}{523}\right) = \left(\frac{7}{523}\right)\left(\frac{11}{523}\right) = (-1)^{261\cdot 3}\left(\frac{523}{7}\right)(-1)^{261\cdot 5}\left(\frac{523}{11}\right) =$$

$$= \left(\frac{5}{7}\right)\left(\frac{6}{11}\right) = (-1)^{2\cdot 3}\left(\frac{2}{5}\right)\left(\frac{2}{11}\right)\left(\frac{3}{11}\right) = (-1)\cdot(-1)\cdot(-1) = -1$$

y por lo tanto, la ecuación $x^2 \equiv 1596 \ mod\ 6353$ no tiene solución.

Bibliografía

[1] M. F. ATIYAH & I. G. MACDONALD,*Introducción al algebra conmutativa*, Reverté, (1973).

[2] N. BOURBAKI, *Algebra*, Hermann, (1974).

[3] K. CONRAD *Discriminants and ramified primes*, University of Conneticut, https://kconrad.math.uconn.edu/blurbs/

[4] D. A. COX, *Galois Theory*, Wiley-Interscience, (2004).

[5] G. ELLINGSRUD, *Cyclotomic fields*, Universitetet i Oslo, (2013).

[6] K. IRELAND & M. ROSEN (1990)*A classical introduction to modern number theory*, Springer, (1990).

[7] G. J. JANUSZ, *Algebraic number fields*, Academic Press New York and London, (1973).

[8] G. A. JONES & J. M. JONES, *Elementary number theory*, Springer, (1998).

[9] S. LANG (2002), *Algebra*, Springer, (2002).

[10] M. LAZCANO COCA, *Ley de reciprocidad cuadrática: Algunas pruebas clásicas*, Universidad de Cantabria, (2017).

[11] P. MORANDI, *Field and Galois theory*, Springer, (1996).

[12] J. NEUKIRCH, *Algebraic number theory*, Springer, (1999).

[13] P. SAMUEL, *Algebraic theory of numbers*, Hermann, (1970).