Universidad Nacional Autónoma de México

Facultad de Ciencias

Teorema de Minkowski y aplicaciones

T E S I S

QUE PARA OBTENER EL TÍTULO DE:
MATEMÁTICO

PRESENTA:
ROLANDO GÓMEZ MACEDO

DIRECTOR DE TESIS:
MARÍA DEL CARMEN HERENDIRA GÓMEZ LAVEAGA

2009

Gómez
Macedo
Rolando
57-35-96-62
Universidad Nacional Autónoma de México
Facultad de Ciencias
Matemáticas

Dra.
María del Carmen
Gómez
Laveaga

Dr.
Hugo Alberto
Rincón
Mejía

Dr.
Juan
Morales
Rodríguez

Dra.
Bertha María
Tome
Arreola

Dr.
Alejandro
Alvarado
García

Teorema de Minkowski y aplicaciones
92 p.
2009

Teorema de Minkowski y aplicaciones.

Rolando Gómez Macedo.
Facultad de Ciencias UNAM
2009

Agradecimientos

A mis padres Adolfo y Emma pues gracias ha ellos tengo la vida y he podido alcanzar esta meta.

A mi hermana Norma, sabes que se te quiere mucho morena.

A mi novia Lupita, gracias por estar incondicionalmente conmigo. Sólo puedo decirte que te amo chaparrita.

A mi mejor amigo Ernesto, que siempre estuvo ahí en los momentos de estrés. Gracias por todas horas de compania en el cubo se ha tomado la molestia de ser mi mejor amigo.

A Carmen Gómez que además de se mi directora de tesis a resultado ser una segunda madre en mi vida. No podia pasar el momento para agradecer a Luis Colavita por todas esas charlas tan amenas e instructivas.

Hugo Alberto Rincón que además de ser un estupendo profesor durante mi carrera es un gran amigo.

Ana Irene Ramírez por enseñarme el maravilloso mundo de la geometría.

Leopoldo Morales y Cesar Guevara pues cada uno me ha enseñado valiosas lecciones de la vida.

A toda la banda que he conocido durante mi estadía en la facultad de ciencias.

Índice

Introducción

En el año de 1896, el matemático alemán Hermann Minkowski $(1864 - 1909)$ presenta la obra Geometrie der Zahlen (Geometría de los números). Entre los enunciados entrega Minkowski en esta obra, encontramos el teorema que a continuación exponemos en su forma moderna

Teorema.*(Minkowski) Sean G un subgrupo discreto de $\mathbb{R}^n$ de dimensión n y X un subconjunto acotado, simétrico y convexo de $\mathbb{R}^n$. Si*

$$V(X) > 2^n V(G)^1,$$

entonces $X \cap G \neq \overline{0}$.

En su "Geometría de los números" Minkowski incorpora la Geometría a la naciente Teoría de los Números, haciendo que emergiera la rama de las matemáticas que ahora se conoce como Geometría de los Números.[2]

> "Las ideas del espacio y el tiempo que deseo exponer ante Vds. han brotado del suelo de la física experimental, y ahí reside su fuerza. Son radicales. En lo sucesivo el espacio por sí mismo, y el tiempo por sí mismo están condenados a desvanecerse en meras sombras, y sólo un tipo de unión de ambos mantendrá una realidad independiente. "
>
> *Hermann Minkowski, 21 de septiembre de 1908.*

El presente trabajo de tesis tiene como una de sus metas principales demostrar el Teorema de Moinkowski y presentar algunas de sus aplicaciones en la Teoría de Números.

El Capítulo 1 *comienza mostrando algunos ejemplos de anillos y módulos, a la vez que se hace una síntesis de conceptos y resultados básicos de ambas teorías. En la sección 2 de este Capítulo, se hace un estudio minucioso del concepto de divisibilidad en un anillo. Se definen los concepto de elemento primo y de elemento irreducible en un dominio entero y se difenrencían. Se presenta al noción de factorizar en irreducibles en un anillo, para luego presentar la definición de Dominio de Factorización y la de Dominio de Factorización Única y se dan algunas equivalencias de éste último concepto que serán de gran utilidad en lo posterior del trabajo. En la sección 3 Capítulo 1 se generalizan algunos resultados clásicos de la Teoría de Grupos Libres a la Teoría de Módulos Libres sobre un Dominios de Ideales Principales. Para terminar de presentar los preliminares generales, la sección 4 del Capitulo 1 presenta algunos resultados sobre la Teoría de Campos, particularmente los relacionados a las extensiones de morfismos de campos y las raíces de polinomios irreducibles sobre campos de característica 0 que se usarán a lo largo del trabajo.*

El Capítulo 2 *esta dedicado totalmente al estudio de Dominios de Dedekind. Primero se presentan el concepto de entero algebraico sobre un dominio entero, que claramente esta inspirado en el estudio que se hizo en los finales del siglo XVIII sobre los enteros algebraicos de los campos numéricos de $\mathbb{Q}$. Se introducen los conceptos de traza, norma y discriminante y se aplican a los anillo de Dedekind. Por último se define lo que es un ideal fraccionario de un anillo de Dedekind y se muestra que el conjunto de ideales fraccionarios no nulos es un grupo abeliano, con el que se construye el grupo de clases de ideales de un dominio de Dedekind.*

En el Capítulo 3 *se hace una caracterización topológica de los subgrupos discretos de $\mathbb{R}^n$ para después se definir el volumen de un subgrupos discretos de $\mathbb{R}^n$. Después se demuestra el teorema*

[1] Donde $V(X)$ y $V(G)$ representan el volumen de X y de G en $\mathbb{R}^n$.

[2] Algunos autores refieren que los métodos geométricos en la Teoría de los Números ya habían sido introducidos por Gustav Lejeune-Dirichlet (1805-1859).

de Minkowski y se presentan tres aplicaciones de éste en la teoría de números siendo tal ves la mas importante la demostración de la finitud del grupos de clases de ideales de un campo numérico de $\mathbb{Q}$.

Capítulo 1

Preliminares

§*1.1 Conceptos y resultados básicos.*

Para el desarrollo de este trabajo se suponen conocidos los conceptos básicos de grupos, anillos, campos y módulos; así como la teoría de espacios vectoriales.

Salvo que se indique lo contrario, a lo largo del trabajo, los anillo se considerarán anillos conmutativos con uno, donde el elemento unitario del anillo es distinto del cero del anillo. También es conveniente señalar que al considerar S un subanillo de un anillo R, el elemento unitario de S debe ser el elemento unitario del anillo R.

A continuación, se presenta un resumen de resultados básico de la teoría de anillos, que serán usados a lo largo trabajo. Se comienza dando una serie de ejemplos de anillos, que por su naturaleza nos proveerán de una gama variada ejemplos.

Ejemplo 1.1.1. Como primer ejemplo, se enumeran algunos anillos bien conocidos.

1) El anillo de los **números enteros**, $\mathbb{Z}$.
2) El campo de los **números racionales**, $\mathbb{Q}$.
3) El campo de los **números reales**, $\mathbb{R}$.
4) El campo de los **números complejos**, $\mathbb{C}$.

Siendo bien sabido que $\mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$. Además se considerará el conjunto de los números naturales como $\mathbb{N} = \{0, 1, 2, \ldots\}$.

Ejemplo 1.1.2. Sea $d \in \mathbb{Z}$ y $\mathbb{Z}\left[\sqrt{d}\,\right] = \{a + b\sqrt{d} \in \mathbb{C} \mid a, b \in \mathbb{Z}\}$.

Si para $a + b\sqrt{d}, a' + b'\sqrt{d} \in \mathbb{Z}\left[\sqrt{d}\,\right]$, se definen

$$\left(a + b\sqrt{d}\right) + \left(a' + b'\sqrt{d}\right) := (a + a') + (b + b')\sqrt{d}$$

y

$$\left(a + b\sqrt{d}\right) \cdot \left(a' + b'\sqrt{d}\right) := (aa' + bb'd) + (ab' + a'b)\sqrt{d}.$$

Se tiene entonces que $(\mathbb{Z}\left[\sqrt{d}\,\right], +, \cdot, 0, 1)$ es un anillo conmutativo con uno.

Nótese que $\mathbb{Z}\left[\sqrt{d}\,\right] = \mathbb{Z}$ si y sólo si $\sqrt{d} \in \mathbb{Z}$.

En el siguiente ejemplo se construye un modelo del anillo de series formales con coeficientes en un anillo R.

Ejemplo 1.1.3. Si R es un anillo. El *conjunto de series sobre el anillo R* esta dado por:

$$R[[x]] = \{f : \mathbb{N} \longrightarrow R \mid f \text{ es función}\}.$$

Dados $f(x), g(x) \in R[[x]]$ y $n \in \mathbb{N}$, se definen

1) $(f+g)(n) := f(n) + g(n)$.

y

2) $(f \cdot g)(n) := \sum\limits_{\substack{k,l \geqslant 0 \\ k+l=n}} f(k)g(l)$. (Nótese que $\sum\limits_{\substack{k,l \geqslant 0 \\ k+l=n}} (f(k)g(l)) = \sum_{j=0}^{n} (f(n-j)g(j))$.)

Si consideramos la funciones $0(x), 1(x) : \mathbb{N} \longrightarrow R$ dadas respectivamente por:

$$0(n) = 0 \ \textit{para todo} \ n \in \mathbb{N} \quad y \quad 1(n) = \begin{cases} 1 & \textit{si } n=0 \\ 0 & \textit{si } n \neq 0 \end{cases}.$$

Tenemos que con las operaciones definidas $(R[[x]], +, \cdot, 0(x), 1(x))$ satisface el ser un anillo conmutativo con uno.

Ahora, para cada $n \in \mathbb{N}$, consideremos el elemento en $R[[x]]$ dado por

$$x^n : \mathbb{N} \longrightarrow R \ \textit{definida por} \ x^n(m) = \begin{cases} 1 & \textit{si} \quad m=n \\ 0 & \textit{si} \quad m \neq n \end{cases}.$$

Y dado $f(x) \in R[[x]]$, tómese

$$\sum_{n=0}^{\infty} f(n)x^n : \mathbb{N} \longrightarrow R \ \textit{dada por} \ \left(\sum_{n=0}^{\infty} f(n)x^n \right)(m) = \sum_{n=0}^{\infty} f(n)x^n(m).$$

Claramente $f(x) = \sum_{i=0}^{\infty} f(n)x^n$ y es entonces que

$$R[[x]] = \left\{ \sum_{n=0}^{\infty} a_n x^n \mid a_n \in R \textit{ para todo } n \in \mathbb{N} \right\}.$$

Usando el hecho de que $x^n \cdot x^m = x^{n+m}$ y las definiciones de $+$ y $\cdot$ en $R[[x]]$. Tenemos que dados $\sum_{n=0}^{\infty} a_n x^n, \sum_{n=0}^{\infty} b_n x^n \in R[[x]]$, las operaciones quedan determinada como sigue:

$$\sum_{n=0}^{\infty} a_n x^n + \sum_{n=0}^{\infty} b_n x^n = \sum_{n=0}^{\infty} (a_n + b_n) x^n$$

y

$$\left(\sum_{n=0}^{\infty} a_n x^n \right) \cdot \left(\sum_{n=0}^{\infty} b_n x^n \right) = \sum_{n=0}^{\infty} \left(\sum_{j=0}^{n} (a_{n-j} b_j) \right) x^n.$$

Al usar esta notación, la suma y producto en $R[[x]]$, imitan formalmente las correspondientes operaciones de las series analíticas estudiadas en los cursos básicos de cálculo. Por tal razón, a $R[[x]]$ se le llama **el anillo de series formales con coeficientes en R**.

Definición 1.1.4. *Si X es un conjunto no vacío, R es un anillo y $f : X \longrightarrow R$ una función. El* ***soporte*** *de $f(x)$ esta dado por:*

$$sop(f(x)) = \{x \in X \mid f(x) \neq 0\}.$$

Se dice que $f(x)$ es de ***soporte finito****, si $sop(f(x))$ es un conjunto finito.*

Ejemplo 1.1.5. Si R es un anillo, el *conjunto de polinomios con coeficientes en R*, esta dado por:

$$R[x] = \{f(x) \in R[[x]] \mid f \textit{ tiene soporte finito } \}.$$

Si $f(x), g(x) \in R[x]$, entonces existen $n_f, m_g \in \mathbb{N}$ tales que $f(n) = 0$ si $n \geqslant n_f$ y $g(m) = 0$ si $m \geqslant m_g$. Y así se tiene que

$$(f+g)(k) = f(k) + g(k) = 0 \quad \textit{para todo} \quad k \geqslant \textit{máx}\,\{n_f, m_g\}$$

y

$$(f\cdot g)(n_f+m_g+k) \underset{Ejem.1.1.3}{=} \sum_{i=0}^{n_f+m_g+k} f(i)g(n_f+m_g+k-i)=0 \quad \textit{para todo} \quad k\in\mathbb{Z}^+.$$

De donde se tienen que $sop(f(x)+g(x))$ y $sop(f(x)\cdot g(x))$ son finitos.

Evidentemente las funciones

$$0(n)=0 \ \textit{para todo}\ n\in\mathbb{N} \quad y \quad 1(n)=\begin{cases} 1 & si\ n=0 \\ 0 & si\ n\neq 0 \end{cases},$$

son elementos de $R[x]$. Entonces $(R[x],+,\cdot,0(x),1(x))$ es un subanillo de $R[[x]]$, llamado el **anillo de polinomios con coeficientes en R**.

Ahora, dado $f(x)\in R[x]-\{0\}$, como $sop(f(x))$ es un conjunto finito, entonces existe $n\in\mathbb{N}$ tal que $n=máx\ \ sop(f)$. A n se le llama el **grado** f y se le denota por $grad(f)$. Nótese que $f(n)\neq 0$ si $n=grad(f(x))$ y $f(m)=0$ si $m>grad(f)$.

Luego si adoptamos la notación se sumas formales ya discutida para $R[[x]]$ en el Ejemplo 1.1.3, cada elemento en $f(x)\in R[x]-\{0\}$, se puede expresar de manera única como

$$f(x)=\sum_{i=0}^{n} a_i x^i,$$

donde $n=grad(f(x))$.

Proposición 1.1.6. *Si R y R' son anillos isomorfos, entonces*

1) *$R[[x]]$ es isomorfo a $R'[[x]]$.*
2) *$R[x]$ es isomorfo a $R'[x]$.*

Observación 1. 1.7. Si R es un anillo la función $\varphi : R \longrightarrow R[x]$ que a cada elemento $r\in R$ le asocia la función $\varphi_x : \mathbb{N}\longrightarrow R$ dada por $\varphi_x(n)=\begin{cases} r & si\ n=0 \\ 0 & si\ n\neq 0 \end{cases}$ es un morfismo inyectivo de anillo. Así tenemos que $R[x]$ contiene una copia isomorfa de R que denotaremos simplemente por R y es entonces posible pensar que $R\subseteq R[x]$.

Ejemplo 1.1.8. Es posible generalizar el concepto de anillo de polinomios a varias indeterminadas, definiendo recursivamente para cada $n\in\mathbb{N}$, con $n\geqslant 2$, **el anillo de polinomios en n indeterminadas $x_1,\ldots,x_n$ con coeficientes R**, por

$$R[x_1,\ldots,x_n]=R[x_1,\ldots,x_{n-1}][x_n].$$

Ejemplo 1.1.9. También se generaliza el concepto de anillo de polinomios en varias variables, como sigue; para cada $n\in\mathbb{Z}^+$, consideramos $R[x_1,\ldots,x_n]$, el anillo de polinomios en n indeterminadas con coeficientes en R. Ahora definimos el *conjuntos de polinomios con una infinidad numerable de indeterminadas* $\{x_n\}_{n\in\mathbb{N}}$, por

$$R[x_\infty]=\bigcup_{n=1}^{\infty} R[x_1,\ldots,x_n]$$

Para definir las operaciones, hay tomar en cuenta que si

$$f(x_\infty), g(x_\infty)\in R[x_\infty],$$

existen $n,m\in Z^+$ tales que $f(x_\infty)\in R[x_1,\ldots,x_n]$ y $g(x_\infty)\in R[x_1,\ldots,x_m]$. Evidentemente

$$f(x_\infty), g(x_\infty)\in R[x_1,x_2,\ldots,x_{max(n,m)}],$$

y así la suma y producto de $f(x_\infty)$ y $g(x_\infty)$ en $R[x_\infty]$, estarán dados por la suma y producto de $f(x_\infty)$ y $g(x_\infty)$ en $R[x_1,x_2,\ldots,x_{max(n,m)}]$. Por la Observación 1.1.7 tenemos que las operaciones están bien definidas y es entonces que con estas operaciones $(R[x_\infty],+,\cdot,0(x),1(x))$ es un anillo conmutativo

con uno, llamado el **anillo de polinomios en una infinidad numerable de indeterminadas con coeficientes en R**.

Los ejemplos 1.1.5, 1.1.8 y 1.1.9 pueden ser generalizados como sigue:

Ejemplo 1.1.10. Si M un monoide conmutativo con neutro e y R es un anillo. Consideremos

$$R[M] = \{f : M \longrightarrow R \mid sop(f) \ \ es\, finito\}.$$

Para $m \in M$ y $f, g \in R[M]$, defínase

$$(f+g)(m) := f(m) + g(m) \ \ y \ \ \ (f \cdot g)(m) := \sum_{\substack{p,q \in M \\ pq=m}} f(p) \cdot g(q).$$

Si definimos las funciones $0, 1 : M \longrightarrow R$ como sigue:

$$0(m) = 0 \ \ \ para\ todo \ \ \ m \in M \ \ y \ \ \ 1(n) = \begin{cases} 1 & si\ n=e \\ 0 & si\ n \neq e \end{cases},$$

entonces tenemos que $(R[M], +, \cdot, 0, 1)$ es un anillo conmutativo con uno, llamado el **anillo de monoide** $R[M]$.

Ahora, para $m \in M$, considérese

$$x^m : M \longrightarrow R \ \ dada\ por \ \ \ x^m(n) = \begin{cases} 1 & si\ n=m \\ 0 & si\ n \neq m \end{cases}.$$

Es posible ver que todo elemento de $f \in R[M]$ con soporte no vacío, se puede expresar de manera única por

$$f = \sum_{i=0}^{n} f(m_i) x^{m_i}$$

donde n es el cardinal del conjunto $sop(f)$ y $\{m_1, \ldots, m_n\} = sop(f)$.

Ejemplo 1.1.11. Si X es un conjunto no vacío, R es un anillo y

$$R^X = \{f : X \longrightarrow R \mid f\ es\ función\ \},$$

es posible dar estructura de anillo a R^X, a partir de la estructura de anillo de R. Esto se hace, definiendo para $f, g \in R^X$ y $x \in X$

$$(f+g)(x) := f(x) + g(x) \ \ y \ \ \ (f \cdot g)(x) := f(x) \cdot g(x).$$

Si definimos las funciones $0, 1 : X \longrightarrow R$ respectivamente por $0(x) = 0$ y $1(x) = 1$ para todo $x \in X$. Entonces $(X^R, +, \cdot, 0, 1)$ es un anillo conmutativo con uno.

*Recordemos que, dado un anillo R y X subconjunto de R, el **ideal generado** por X en R, está dado por:*

$$\langle X \rangle = \left\{ \sum_{i=1}^{n} r_i x_i \in R \mid n \in \mathbb{N}, \ \ r_i \in R \ y \ x_i \in X \right\}.$$

Proposición 1.1.12. *Sea X un subconjunto de un anillo R e I un ideal de R. Son equivalentes para I:*

1) *I es el ideal generado por X.*
2) *$X \subseteq I$ y si J es un ideal de R que contiene a X, entonces $I \subseteq J$.*
3) *$I = \bigcap_{\substack{X \subseteq J \\ J\ es\ ideal\ de\ R}} J$.*

Corolario 1.1.13. *Sean X y Y subconjuntos de un anillo R. Entonces:*

1) *$\langle X \rangle \subseteq \langle Y \rangle$ si $X \subseteq Y$.*
2) *$\langle \langle X \rangle \rangle = \langle X \rangle$.*

Dados I y J ideales de un anillo R, la ***suma*** *y el* ***producto*** *de I con J son definidos respectivamente por*

$$I + J = \{x + y \in R \mid x \in I \text{ y } y \in J\}$$

e

$$IJ = \left\{\sum_{i=1}^{n} x_i y_i \in R \mid x_i \in I \text{ y } y_i \in J\right\}.$$

Proposición 1.1.14. *Sea R un anillo, I y J ideales de R y X y Y subconjuntos de R. Entonces*

1) $I + J$, IJ e $I \cap J$ son ideales de R.
2) $IJ \subseteq I \cap J \subseteq I + J$.
3) $\langle X \cup Y \rangle = \langle X \rangle + \langle Y \rangle$.

También recordemos que si $f : R \longrightarrow S$ es un morfismo de anillos, quedan definidos dos conjuntos intrínsecos a f. El ***núcleo*** *(o* ***kernel****) de f dado por*

$$ker(f) = \{r \in R \mid f(r) = 0\},$$

y la ***imagen*** *de f dado por*

$$Im(f) = \{f(r) \in S \mid r \in R\}.$$

El núcleo de f es un ideal de R, mientras que la imagen de f es un subanillo de S[1].

Proposición 1.1.15. *Sea $f : R \longrightarrow S$ es un morfismo de anillos. Entonces f es inyectivo si y sólo si $ker(f) = \{0\}$.*

Si I es un ideal de un anillo R, estos determinan un anillo R/I llamado el ***anillo cociente*** *de R por I, y cuyos elementos son de la forma*

$$r + I = \{r + s \in R \mid s \in I\},$$

con $r \in R$, donde $r + I = r' + I$ si y sólo si $r - r' \in I$.

Adicionalmente se tiene que la función

$$\pi : R \longrightarrow R/I \text{ dada por } \pi(r) = r + I \text{ para todo } r \in R,$$

es un homomorfismo sobreyectivo de anillos, llamado la ***proyección canónica*** *de R sobre R/I y cuyo núcleo es I.*

Para terminar este preámbulo de anillos, enunciamos cuatro importantes teoremas de la teoría de anillos.

Teorema 1.1.16 *(Primer Teorema de Isomorfismo). Sea $f : R \longrightarrow S$ un homomorfismo de anillos. Entonces existe un único morfismo inyectivo de anillos $\overline{f} : R/ker(f) \longrightarrow S$, tal que $f = \overline{f} \circ \pi$, donde π proyección canónica de R sobre $R/ker(f)$.*

Teorema 1.1.17 *(Segundo Teorema de Isomorfismo). Sea I un ideal de un anillo R y S un subanillo de R. Entonces, $I \cap S$ es un ideal de S, $S + I$ es un subanillo de R y*

$$S/(I \cap S) \cong (S + I)/I.$$

Teorema 1.1.18 *(Tercer Teorema de Isomorfismo). Sean I y J ideales de un anillo R, tales que $I \subseteq J$. Entonces,*

1) $J/I = \{r + I \in R/I \mid r \in J\}$ *es un ideal de R/I.*
2) $(R/I)/(J/I)$ *es isomorfo a R/J.*

Teorema 1.1.19 *(Teorema de correspondencia). Sea R un anillo e I un ideal de R. La correspondencia que asocia a cada ideal J de R que contiene a I el ideal J/I de R/I, es biyectiva.*

---

[1] Dado que se esta trabajando con anillos conmutativos con uno, si $f : R \longrightarrow S$ es un homomorfismo de anillos, se pide que $f(1_R) = 1_S$.

*Si R es un anillo e I un ideal de R, I es un **ideal propio** si $(0) \subseteq I \subsetneq R$. Un **ideal maximal**, es un ideal propio tal que no existe ningún ideal propio J de R que lo contenga propiamente. Es decir, I es un ideal maximal de R si $I \subsetneq R$ y cada vez que $I \subseteq J \subseteq R$ con J ideal de R, se tiene que $I = J$ o $J = R$.*

Proposición 1.1.20. *Sea I un ideal de un anillo R. Entonces, I es un ideal maximal de R si y sólo si R/I es campo.*

Para dar término esta sección, evocaremos algunos resultados de la teoría de módulos. Y al igual que como se hizo para los anillos, se comenzará dando una serie de ejemplos.

Ejemplo 1.1.21. Dado un campo k. Todo espacio vectorial sobre k, es en particular un k-módulo.

Ejemplo 1.1.22. Todo grupo abeliano es un $\mathbb{Z}$-módulo.

Ejemplo 1.1.23. Si R es un anillo, S es un subanillo de R, I un ideal de R y M un monoide conmutativo, se tiene que:

1) I es un R-módulo y un S-módulo.
2) R/I es un R-módulo, un S-módulo y un $S/(S \cap I)$-módulo.
3) $R[[x]]$, $R[x_1, \ldots, x_n]$ y $R[x_\infty]$ son R-módulos y S-módulos.
4) $R[[x]]$ y $R[x_\infty]$ son $R[x]$-módulos.
5) $R[M]$ es un R-módulo y un S-módulo.

Ejemplo 1.1.24. Sean M y N son R-módulos y $Hom(M,N)$ el conjunto de morfismos de R-módulos de M en N. Definiendo para $r \in R$ y $\varphi \in Hom(M,N)$

$$r\varphi : M \longrightarrow N \text{ por } (r\varphi)(m) = r\varphi(m),$$

$Hom(M,N)$ adquiere estructura de R-módulo.

Ejemplo 1.1.25. Consideremos $\{M_i\}_{i\in I}$ una familia no vacía de R-módulos y $\times_{i\in I} M_i$ su producto cartesiano. Para $(m_i), (n_i) \in \times_{i\in I} M_i$ y $r \in R$, tómese

$$(m_i)_{i\in I} + (n_i)_{i\in I} = (m_i + n_i)_{i\in I} \;\; y \;\; r(m_i)_{i\in I} = (rm_i)_{i\in I}.$$

Con estas operaciones, $\times_{i\in I} M_i$ adquiere estructura de R-módulo, el cual se denota por $\prod_{i\in I} M_i$ y es nombrado el ***producto directo*** de la familia $\{M_i\}_{i\in I}$.

Definición 1.1.26. *Sea $\{M_i\}_{i\in I}$ es una familia no vacía de R-módulos. Si $m = (m_i)_{i\in I} \in \prod_{i\in I} M_i$, el **soporte** de m, esta dado por*

$$sop(m) = \{i \in I \mid m_i \neq 0\}.$$

*Un elemento en $\prod_{i\in I} M_i$ tiene **soporte finito**, si su soporte es un conjunto finito.*

Ejemplo 1.1.27. Sea $\prod_{i\in I} M_i$ el producto directo de una familia no vacía de R-módulos $\{M_i\}_{i\in I}$, y sea

$$\bigoplus_{i\in I} M_i = \{m \in \prod_{i\in I} M_i \mid sop(m) \text{ es finito } \}.$$

Dado que para todo $m, n \in \prod_{i\in I} M_i$

$$sop(m+n) \subseteq sop(m) \cup sop(n) \;\; y \;\; sop(rm) \subseteq sop(m),$$

se tiene que $\bigoplus_{i\in I} M_i$ es un submódulo de $\prod_{i\in I} M_i$ llamado la ***suma directa*** de la familia $\{M_i\}_{i\in I}$.

Observación 1.1.28. Nótese que si $\{M_i\}_{i\in I}$ es una familia no vacía de R-módulos e I es un conjunto finito, entonces $\prod_{i\in I} M_i = \bigoplus_{i\in I} M_i$.

Si X es un subconjunto de un R-módulo M, el submódulo generado por X en M está dado por:

$$\langle X\rangle = \left\{\sum_{i=1}^{n} r_i x_i \mid n \in \mathbb{N},\ \ r_i \in R \text{ y } x_i \in X\right\}.$$

Proposición 1.1.29. *Sean X un subconjunto de un R-módulo M y N un submódulo de M. Son equivalentes*

1) *N es el submódulo generado por X.*
2) *$X \subseteq N$ y si L es un submódulo de M que contiene a X, entonces $N \subseteq L$.*
3) $N = \bigcap_{\substack{X\subseteq L \\ L \text{ es submódulo de } M}} L.$

Corolario 1.1.30. *Sean X y Y subconjuntos de un R-módulo M. Entonces:*

1) *$\langle X\rangle \subseteq \langle Y\rangle$ si $X \subseteq Y$.*
2) *$\langle\langle X\rangle\rangle = \langle X\rangle$.*

Dado un R-módulo M y N y L submódulos de M, la ***suma*** *de N con L está dada como sigue:*

$$N + L = \{n + l \in M \mid n \in N \text{ y } l \in L\}.$$

Proposición 1.1.31. *Sea M un R-módulo, N y L submódulos de M y X y Y subconjuntos de R. Entonces*

1) *$N + L$ es un submódulo de M.*
2) *$\langle X \cup Y\rangle = \langle X\rangle + \langle Y\rangle$.*

Es posible extender el concepto de suma de submódulos a una familia arbitraria de submódulos como sigue; si $\{M_i\}_{i\in I}$ es una familia de una familia no vacía de R-módulos de un módulo M, la suma de la familia esta dada por:

$$\sum_{i\in I} M_i = \left\{\sum_{n=1}^{k} m_{i_n} \in M \mid k \in \mathbb{Z}^+ \ \ i_1,\ldots,i_k \in I \ \ \text{y} \ \ m_{i_j} \in M_{i_j} \ \ \text{para} \ \ 1 \leqslant j \leqslant k\right\}.$$

Así como sucede en la teoría de anillos, dado un morfismo de R-módulos, $f : M \longrightarrow N$, quedan definidos dos importantes conjuntos asociados a f. El ***núcleo*** *(o* ***kernel****) de f dado por:*

$$ker(f) = \{m \in M \mid f(m) = 0\}$$

y la ***imagen*** *de f, que está determinada como sigue:*

$$Im(f) = \{f(r) \in S \mid r \in R\}.$$

El núcleo de f es un un submódulo de M, mientras que la imagen de f lo es de N.

También ocurre que si M es un R-módulo y N un submódulo de M, queda determinado el ***R-módulo cociente*** *M/N, cuyos elementos son de la forma $m + N = \{m + n \in M \mid n \in N\}$ para algún $m \in M$, donde $m_1 + N = m_2 + N$ si y sólo si $m_1 - m_2 \in N$, y si $r \in R$ se define $r(m + N) := rm + N$. Además la función*

$$\pi : M \to M/N \text{ dada por } \pi(r) = r + N.$$

es un homomorfismo sobreyectivo de R-módulos, cuyo núcleo es N. A π también se le nombra la ***proyección canónica*** *de M sobre M/N.*

Incluso existen las respectivas versiones de los teoremas de isomorfismos y el teorema de correspondencia, que a continuación se enuncian.

Teorema 1.1.32 *(Primer Teorema de Isomorfismo). Sea $f : M \longrightarrow N$ un morfismo de R-módulos con núcleo K. Entonces existe un único morfismo de R-módulos $\widetilde{f} : M/K \longrightarrow N$ tal que $\widetilde{f} \circ \pi = f$, donde $\pi : M \longrightarrow M/K$ es la proyección canónica de M sobre M/K.*

Teorema 1.1.33 *(Segundo Teorema de Isomorfismo). Sean N y K R-submódulos de M. Entonces $N/(N \cap K)$ es isomorfo a $(N+K)/K$.*

Teorema 1.1.34 *(Tercer Teorema de Isomorfismo). Sean N y K submódulos de un R-módulos M tales que $N \subseteq K$. Entonces $K/N = \{k+N \in M/N \mid k \in K\}$ es un submódulo de M/N y $(M/N)/(K/N)$ es isomorfo a M/K.*

Teorema 1.1.35 *(Teorema de correspondencia). Sea M un R-módulo y N un submódulo de M. La correspondencia que asocia a cada R-submódulo L de M que contiene N el R-submódulo L/N de M/N, es biyectiva.*

La suma directa de módulos es de gran importancia en el estudio de los módulos, es por eso que es importante contar con algunas equivalencias.

Teorema 1.1.36. *Sean M un R-módulo y $\{M_i\}_{i\in I}$ una familia de R-submódulos de M. Son equivalentes*

1) *La función $\varphi : \bigoplus_{i\in I} M_i \longrightarrow M$ definida por $\varphi\left((m_i)_{i\in I}\right) = \sum_{i\in I} m_i$ es un isomorfismo de R-módulos.*
2) *$M = \sum_{i\in I} M_i$ y $M_j \bigcap \sum_{i\in I\setminus\{j\}} M_i = \{0\}$.*
3) *Todo elemento $m \in M$ se puede escribir de manera única como*

$$m = m_{i_1} + \cdots + m_{i_n}$$

con $m_{i_j} \in M_{i_j}$ y $j \in \{1,\ldots,n\}$, para algún $n \in \mathbb{N}$.

Proposición 1.1.37. *Sea $\{M_i\}_{i\in I}$ una familia de R-submódulos de M tal que $M = \bigoplus_{i\in I} M_i$. Supongamos que $\{N_i\}_{i\in I}$ es una familia de submódulo de M tales que $N_i \subseteq M_i$ para todo i y sea $N = \sum_{i\in I} N_i$. Entonces:*

1) *$N = \bigoplus_{i\in I} N_i$.*
2) *$M/N \cong \bigoplus_{i\in I} (M_i/N_i)$.*

§1.2 Divisibilidad en anillos.

Históricamente, el concepto de divisibilidad, surge ante la necesidad de repartir cantidades. Se sabe que el concepto de divisibilidad de los números es conocido ya desde tiempos remotos. Por ejemplo, los egipcios conocían los números pares e impares y los hindúes ya conocían criterios para discriminar si un número era divisible por tres, siete o nueve.

Es el matemático griego Euclides, en los libros VII, VIII y IX de los Elementos, quien sienta los conceptos básicos de la teoría de números y demuestra los teoremas básicos, entre ellos el que ahora se conoce como ***Teorema Fundamental de la Aritmética*** *y que versa así*

Teorema 1.2.1. *Cualquier número entero mayor que 1 puede escribirse de manera única, salvo el orden, como producto de números primos*[2].

Ya posteriormente matemáticos de gran talla, como Pierre de Fermat (1601-1665), Leonhard Euler (1707-1783), Joseph-Louis de Lagrange (1736-1813), Carl Friedrich Gauss (1777-1855), entre otros, trabajaron arduamente en lo que ahora se conoce como teoría de los números y cimentaron lo que actualmente se conoce como teoría algebraica de números.

La generalización de la divisibilidad a cualquier anillo se puede hacer de manera por demás natural.

[2]Su versión original aparece en el libro IX de los Elementos como la Proposición 14 y dice: Si un número es el menor medido por números primos, no será medido por ningún otro número primo fuera de los que le median desde un principio

Definición 1.2.2. *Dado un anillo R y $r, t \in R$, se dice que r **divide** a t y se denota por $r \mid t$, si existe $s \in R$ tal que $rs = t$.*

Proposición 1.2.3. *En un anillo R se tiene que:*

1) $1 \mid t$ *para todo* $t \in R$.
2) Si $r \mid s$ *y* $r \mid t$, *entonces* $r \mid s + t$ *y* $r \mid st$.
3) Si $r \mid s$ *y* $o \mid t$, *entonces* $ro \mid st$.
4) Si $r \mid s + t$ *y* $r \mid s$, *entonces* $r \mid t$.
5) Si $r \mid s$ *y* $s \mid t$, *entonces* $r \mid t$.

Indiscutible es la importancia que juegan el cero y el uno en un anillo. Ahora veremos el papel que tienen sus divisores en el estudio de la divisibilidad de un anillo.

Definición 1.2.4. *Si R es un anillo, $r \in R - \{0\}$ es un **divisor propio de** $\mathbf{0}$ si existe $s \in R - \{0\}$ tal que $rs = 0$.*

Ejemplo 1.2.5.

1) Sea $n \in \mathbb{Z}$, $n \geqslant 2$. Si n es un número no primo, entonces $\overline{m} \in \mathbb{Z}_n$ es un divisor propio de cero si y sólo si $n \nmid m$ y $(n, m) \neq 1$.
2) Sea R un anillo y $f(x) \in R[x] - \{0\}$. Entonces, $f(x)$ es un divisor propio de cero si y sólo si existe $r \in R - \{0\}$ tal que $rf(x) = 0$.

Definición 1.2.6. *Dado un anillo R y $r \in R$, r es un **nilpotente** si existe $n \in \mathbb{Z}^+$ tal que $r^n = 0$.*

Ejemplo 1.2.7.

1) Sea $n \in \mathbb{Z}$, $n \geqslant 2$ y $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ donde p_i es un número primo para cada $i \in \{1, \ldots, r\}$. Si n es un número no primo, entonces $\overline{m} \in \mathbb{Z}_n$ es nilpotente si y sólo si $m = p_1^{\beta_1} \cdots p_r^{\beta_r}$ con $\beta_i \geqslant 1$ para cada $i \in \{1, \ldots, r\}$.
2) Si R es un anillo y $f(x) \in R[x]$ con $f(x) = a_0 + a_1 x + \cdots + a_n x^n$. Entonces $f(x)$ es nilpotente si y sólo si a_i es nilpotente en R para cada $i \in \{1, \ldots, r\}$.
3) Si R es un anillo, X un conjunto no vacío y $f \in R^X$. Entonces f es nilpotente si y sólo si $f[X]$ esta contenido en el conjunto de elementos nilpotentes de R.

Definición 1.2.8. *Sea R un anillo, $u \in R$ es una **unidad**, si existe $v \in R$ tal que $uv = 1$. A una unidad de un anillo R, también le suele llamarsele un elemento **invertible** de R.*

Proposición 1.2.9. *Sea R un anillo y $r \in R$. Entonces r es una unidad en R si y sólo si $rR = R$.*

Proposición 1.2.10. *Las unidades de un anillo R forman un grupo con el producto del anillo como operación, llamado el **grupo de unidades de R** y el cual se designa por $U(R)$.*

Ejemplo 1.2.11.

1) Si $R = \mathbb{Z}$, entonces $U(\mathbb{Z}) = \{-1, 1\}$.
2) Si K es un campo, entonces $U(K) = K \backslash \{0\}$.
3) Sea $n \in \mathbb{Z}$, con $n \geqslant 2$. Entonces $\overline{m} \in \mathbb{Z}_n$ es una unidad en Z_n si y sólo si $(n, m) = 1$.
4) Si $d \in \mathbb{Z}$, entonces $a + b\sqrt{d} \in U(\mathbb{Z}[\sqrt{d}\,])$ si y sólo si $a^2 - db^2 = \pm 1$. En particular,
   I) si $d = -1$ se tiene que $U(\mathbb{Z}[-1\,]) = \{1, -1, i, -i\}$ (donde $i \in \mathbb{C}$).
   II) para todo $d \in \mathbb{Z}^-$ con $d \neq -1$, se tiene que $U(\mathbb{Z}[\sqrt{d}\,]) = \{1, -1\}$.
5) Sea R un anillo y $f(x) = a_0 + a_1 x + \cdots + a_n x^n \in R[x]$. Entonces $f(x)$ es una unidad en $R[x]$ si y sólo si a_0 es una unidad en R y a_i es nilpotente para cada $i \in \{1, \ldots, n\}$.
6) Sea R un anillo y $f(x) = \sum_{i=0}^{\infty} a_i x^i \in R[[x]]$. Entonces $f(x)$ es una unidad si y sólo si a_0 es una unidad en R.

7) Sea R un anillo, X un conjunto no vacío y $f \in R^X$. Entonces f es una unidad en R^X si y sólo si $f[X]$ esta contenida en las unidades de R.

Ejemplo 1.2.12. Sea K un campo y $K[[x]]$ el anillo de series formales con coeficientes en K. Para cada $n \in \mathbb{Z}^+$, el anillo dado por $R = K[[x]]/\langle x^n \rangle$ es un anillo que tiene la peculiaridad de que todo elemento en R es una unidad o es un elemento nilpotente.

Definición 1.2.13. *Un anillo que no tiene divisores propios de cero se llama* ***dominio entero****.*

Proposición 1.2.14. *Sea R un anillo. Son equivalentes para R*

1) R es un dominio entero.
2) Si $x, y \in R$ son tales que $xy = 0$, entonces $x = 0$ o $y = 0$.
3) Dados $x, y, z \in R$, si $xy = xz$ y $x \neq 0$, entonces $y = z$.

Ejemplo 1.2.15.

1) $\mathbb{Z}$ es un dominio entero.
2) Para cada $d \in \mathbb{Z}$, $\mathbb{Z}\left[\sqrt{d}\,\right]$ es un dominio entero.
3) Todo campo es un dominio entero. En particular $\mathbb{Z}_p$ es un dominio entero si y sólo si p es un número primo.
4) D es un dominio entero si y sólo si $D[x]$ es un dominio entero.
5) D es un dominio entero si y sólo si $D[x_\gamma]$ es un dominio entero.
6) D es un dominio entero si y sólo si $D[[x]]$ es un dominio entero.
7) Si $(M, +)$ es un monoide totalmente ordenado (con el orden compatible con $+$) y D es un dominio entero, entonces $D[M]$ es dominio entero.

Proposición 1.2.16. *Todo dominio entero finito es campo.*

Es en los números enteros donde surge el concepto de elemento primo[3]*, después al estudiar el anillo de polinomios $K[x]$, para K un campo, aparece un concepto muy parecido al de número primo, el de polinomio irreducible.*

La importancia de los números primos se manifiesta a través del Teorema Fundamental de la Aritmética. En la versión análoga de este teorema en el anillo de polinomios con coeficientes en un campo K, se muestra el valioso papel que juegan los polinomios irreducible en $K[x]$. Ahora se hará una distinción entre los conceptos de elemento primo y elemento irreducible en un anillo, lo que más adelante se justificará mostrando que estos conceptos en general no coinciden.

Definición 1.2.17. *Sea R un anillo, $r \in R$* ***irreducible*** *en R, si $r \notin U(R)$ y cada vez que $r = st$ con $s, t \in D$, se tiene que $s \in U(R)$ o $t \in U(R)$.*

Obsérvese que si R es un anillo que no es campo, entonces 0 no es irreducible.

Definición 1.2.18. *Sea R un anillo, $p \in R$ es* ***primo*** *en R, si $p \neq 0$, $p \notin U(R)$ y cada vez que $p \mid st$ con $s, t \in D$, se tiene que $p \mid s$ o $p \mid t$.*

Proposición 1.2.19. *Si D es un dominio entero, entonces todo elemento primo en D es irreducible.*

Demostración. *Sea $p \in D$ un elemento primo y supóngase que $p = st$ con $s, t \in D$. Dado que $p \cdot 1 = st$, entonces $p \mid st$ y como p es primo en R, tenemos que $p \mid s$ o $p \mid t$. Sin pérdida de generalidad se puede suponer que $p \mid s$, luego entonces existe $s' \in D$ tal que $s = ps'$. Al sustituir esta última igualada en $p = st$, se obtiene que $p = ps't$. Ahora, D es un dominio entero y $p \neq 0$, entonces de la Proposición 1.2.14, se concluye que $1 = s't$. Es decir $t \in U(D)$ y por lo tanto se tiene que p es irreducible.* ∎

[3]Ver los Elementos de Euclides Libro *VII* definición 12.

Tanto en el anillo de los enteros, como en el anillo de polinomios con coeficientes en un campo, los conceptos de primo e irreducible son equivalentes. Pero en general estos conceptos no coinciden en un dominio entero, como lo muestra el siguiente

Ejemplo 1.2.20. Sea K un campo y sea

$$D = \left\{ \sum_{i=1}^{n} a_i (x^3)^{r_i} (xy)^{s_i} (y^3)^{t_i} \in K[x,y] \mid a_i \in K \;\; r_i, s_i, t_i, n \in \mathbb{N} \;\; con \;\; i = 1, \ldots, n \right\}$$

el dominio entero generado por $\{x^3, xy, y^3\}$ y K en $K[x,y]$[4]. Nótese que xy es irreducible en D, no obstante $xy \mid x^3y^3$ y $xy \nmid x^3$ y $xy \nmid y^3$.

Definición 1.2.21. *Sea R un anillo, $r, s \in R$ son **asociados** en R, si existe $u \in U(R)$ tal que $r = us$.*

Ejemplo 1.2.22.

1) Si $z_1, z_2 \in \mathbb{Z}$, se tiene que z_1 es asociado de z_2 si y sólo si $\mid z_1 \mid = \mid z_2 \mid$.
2) Si K es un campo, y $f(x), g(x)) \in K[x]$. Entonces $f(x)$ es asociado a $g(x)$ si y sólo si existe $a \in K - \{0\}$ tal que $f(x) = ag(x)$.

Proposición 1.2.23. *Sea R un anillo. Entonces*

1) r es asociado a r para todo $r \in R$.
2) Si r es asociado a s, entonces s es asociado a r.
3) Si r es asociado a s y s es asociado a t, entonces r es asociado a t.

Proposición 1.2.24. *Sean r y s dos elementos asociados en un anillo R. Entonces*

1) r es divisor propio de cero si y sólo si s es divisor propio de cero.
2) r es una unidad si y sólo si s es una unidad.
3) r es irreducible si y sólo si s es irreducible.
4) r es primo si y sólo si s es primo.

Proposición 1.2.25. *Sea D un dominio entero y $r, s \in D$. Entonces:*

1) Si r y s son irreducibles en D y $r \mid s$, entonces r es asociado a s.
2) Si r es asociado a s, $s \neq 0$ y $rt = s$ para alguna $t \in D$, entonces $t \in U(R)$.
3) Si r es asociado a s y $t \mid r$, entonces $t \mid s$.

Proposición 1.2.26. *Sea D un dominio entero y $r, s \in D$. Entonces*

1) Si r y s son asociados en D, entonces $r \mid s$ y $s \mid r$.
2) Si $r \mid s$, $s \mid r$ y $r \neq 0$, entonces r y s son asociados en D.

Una lectura que se puede hacer de la anterior proposición es que en un dominio entero los elementos asociados son indistinguibles desde el punto de vista de la divisibilidad.

Por la Proposición 1.2.3 incisos (2) y (3), se obtiene, que dado $r \in R$, el conjunto

$$rR = \{rs \in R \mid s \in R\},$$

*es un ideal de R, llamando **ideal principal generado por r** en R.*

Definición 1.2.27. *Sea R un anillo. Un ideal I de R es un **ideal principal** si $I = rR$ para algún $r \in R$. R se dice que es un **anillo de ideales principales** si todo ideal de R es principal.*

Ejemplo 1.2.28.

1) El anillo de los enteros $\mathbb{Z}$, es un anillo de ideales principales.
2) Si K es un campo, entonces K, $K[x]$ y $K[[x]]$ son anillos de ideales principales.

---

[4] D se puede construir formalmente tomando M el monoide multiplicativo en $K[x,y]$ generado por $\{x^3, xy, y^3\}$ y luego considerar $D = K[M]$.

3) Si R es un anillo de ideales principales e I es un ideal de R, entonces R/I es un anillo de ideales principales. En particular $\mathbb{Z}_n$ es un anillo de ideales principales para cada $n \in \mathbb{Z}^+$.

Proposición 1.2.29. *Sea R un anillo y $r, t \in R$. Entonces $r \mid t$ si y sólo si $tR \subseteq rR$.*

En vista de la Proposición 1.2.29, es posible hacer un tratamiento de la divisibilidad en un anillo, a través del conjunto de ideales principales del anillo.

Proposición 1.2.30. *Sea D un dominio entero y $r, s \in D - \{0\}$. Entonces $rD = sD$ si y sólo si r y s son asociados.*

Observación 1. 2.31. Sea R un anillo y $p \in R$ un elemento primo y consideremos pR el ideal principal generado por p en R. Si $st \in pR$, para algún $s, t \in R$, como $p \mid st$ y es p un primo en R, se concluye que $p \mid s$ o $p \mid t$. Luego, usando la Proposición 1.2.29 obtenemos que $s \in pR$ o $t \in pR$.

La propiedad dada en la Observación 1.2.31 para un elemento primo de un anillo R inspira la siguiente

Definición 1.2.32. *Un ideal P de un anillo R, es un **ideal primo**, si cada vez que $st \in P$ se tiene que $s \in P$ o $t \in P$.*

Proposición 1.2.33. *Sea I un ideal de un anillo R. Son equivalentes para I*

1) *I es un ideal primo de R.*
2) *Si $s, t \in R$ y $s \notin I$ y $t \notin I$, entonces $st \notin I$.*
3) *R/I es dominio entero.*

Corolario 1.2.34. *En un anillo todo ideal maximal es un ideal primo. (Ver Proposición 1.1.20)*

Corolario 1. 2.35. *En un anillo finito todo ideal primo es maximal. (Ver Proposiciones 1.1.20 y 1.2.16)*

Para mostrar el hecho de que existen ideales primos que no son maximales, es suficientes considerar D un dominio entero que no sea campo y $xD[x]$ el ideal principal generado por x en $D[x]$. Luego, como $D[x]/xD[x]$ es naturalmente isomorfo a D, por la Proposición 1.2.33 tenemos que $xD[x]$ es un ideal primo. Ahora dado que D no es campo, de la Proposición 1.1.20 obtenemos que $xD[x]$ no es maximal.

Teorema 1.2.36. *Sea R un anillo y $r \in R$. Entonces,*

1) *si R es dominio entero, r es irreducible en R si y sólo si rR es un ideal maximal en el conjunto de ideales principales propios de R.*
2) *p es primo en R si y sólo si pR es un ideal primo.*

Demostración.

1) $\Rightarrow$) *Sea $r \in R$ irreducible en R y supongamos que $rR \subseteq sR \subsetneq R$ para algún $s \in R$. Como $rR \subseteq sR$, de la Proposición 1.2.29, existe $t \in R$ tal que $st = r$ y como r es irreducible, entonces $s \in U(D)$ o $t \in U(D)$. La Proposición 1.2.9 muestra imposibilidad de que s sea una unidad en R, pues estamos suponiendo que $sR \subsetneq R$. Luego entonces $t \in U(R)$. Así r y s son asociados en R.*
   Ahora, como D es un dominio entero, de la Proposición 1.2.30, se obtiene que $rR = sR$. Por lo tanto rR es maximal en el conjunto de ideales principales propios de R.
   $\Leftarrow$) *Supongamos que rR es un ideal maximal en el conjunto de ideales principales propios de R y sean $s, t \in R$ tales que $r = st$. Como en particular $s \mid r$, de la Proposición*

1.2.29 concluimos que $rR \subseteq sR$. Siendo rR maximal en el conjunto de los ideales propios de R, entonces $rR = sR$ o $sR = R$. Analizaremos los dos casos,

I) Si $rR = sR$, dado que R es dominio entero, de la Proposición 1.2.30, se obtiene que r es asociado de s y como $r = st$, de la Proposición 1.2.25 inciso (2) concluimos que $t \in U(R)$.

II) Si $sR = R$, por la Proposición 1.2.9 se tiene que $s \in U(R)$.

Por lo tanto r es irreducible en R.

2) $\Rightarrow$) Es la Observación 1.2.31.

$\Leftarrow$) Sean $p, s, t \in R$ tales que pR es un ideal primo de R y $p \mid st$.

Supongamos que $p \nmid s$ y que $p \nmid t$, entonces por la Proposición 1.2.29, se deduce que $s \notin pR$ y que $t \notin pR$ y así por la Proposición 1.2.33 tenemos que $st \notin pR$, lo que contradice el hecho de que $p \mid st$. Por lo tanto $p \mid s$ o $p \mid t$, es decir p es un elemento primo de R. ∎

Corolario 1.2.37. *Sea D un dominio entero y $r \in D \backslash U(D)$. Entonces r no es irreducible si y sólo si existe $s \in D$ tal que $rD \subsetneq sD \subsetneq D$.*

Corolario 1.2.38. *En un anillo finito, todo elemento primo es irreducible. (Ver Corolario 1.2.35)*

Corolario 1.2.39. *En un dominio de ideales principales un elemento es primo si y sólo si es irreducible. (Ver Proposición 1.2.19)*

Una de las metas de esta sección, es la de encontrar condiciones en un dominio entero para que en él se pueda enunciar una proposición semejante al Teorema Fundamental de la Aritmética (Teorema 1.2.1).

Definición 1.2.40. *Se D un dominio entero y $d \in D$. Se dice que d se **factoriza en irreducibles** en D si existen $n \in \mathbb{Z}^+$ y $r_1, \ldots, r_n \in D$ irreducibles en D, tales que $d = r_1 \cdots r_n$. Un dominio en el que cada elemento no nulo que no es una unidad se factoriza en irreducibles se llama un **dominio de factorización**.*

Con el siguiente ejemplo ilustraremos la existencia de dominios enteros en los que la factorización en irreducibles no es posible.

Ejemplo 1.2.41. Consideremos el monoide $M = (\mathbb{Q}^+ \cup \{0\}, +)$, K un campo y tomemos $K[M]$. Por el Ejemplo 1.2.15 tenemos que $K[M]$ es un dominio entero.

Como ya se mencionó en el Ejemplo 1.1.10, si f y g son elementos de $K[M]$ con soporte no vacío, entonces

$$f = \sum_{i=0}^{n} f(a_i)x^{a_i} \quad y \quad g = \sum_{i=0}^{m} g(b_i)x^{b_i}$$

donde

$$n = |sop(f)|, \ \ m = |sop(g)| \ \ \{a_1, \ldots, a_n\} = sop(f) \ \ y \ \ \{b_1, \ldots, b_n\} = sop(f).$$

De hecho, como M es un monoide totalmente ordenado, podemos suponer que $a_1 < \cdots < a_n$ y que $b_1 < \cdots < b_m$. Así es fácil ver que si f y g son elementos de $K[M]$ tales que $|sop(f)| \geqslant 2$ o $|sop(g)| \geqslant 2$, entonces $|sop(fg)| \geqslant 2$.

Tomemos $\alpha \in \mathbb{Q}^+$ y $x^\alpha \in K[M]$. Veremos que x^α no es una unidad en K[M]. Para ello procederemos por reducción al absurdo y así supongamos que existe $f \in K[M]$ tal que $x^\alpha f = 1$. Como $|sop(1)| = 1$, es necesario que $|sop(f)| = 1$, de donde se concluye que $f = ax^\beta$ con $a \in K$ y $\beta \in \mathbb{Q}^+ \cup \{0\}$. Luego entonces $ax^{\alpha+\beta} = 1$, de donde obtenemos que $a = 1$ y $\alpha + \beta = 0$. Y como $\alpha \in \mathbb{Q}^+$, concluimos $\beta = -\alpha \in \mathbb{Q}^-$, que es un absurdo ya que $\beta \in \mathbb{Q}^+ \cup \{0\}$. Por lo tanto x^α no es una unidad en $K[M]$.

Notemos que si $\alpha \in \mathbb{Q}^+$, entonces x^α no es irreducible pues $x^\alpha = x^{\frac{\alpha}{2}} x^{\frac{\alpha}{2}}$, donde $x^{\frac{\alpha}{2}} \notin U(K[M])$ dado que $\frac{\alpha}{2} \in \mathbb{Q}^+$.

Ahora estamos en condiciones de mostrar lo que se prometió. Para ello supongamos que x se puede factorizar en irreducibles, y sean $f_1, \ldots, f_n \in K[M]$ irreducibles tales que

$$x = f_1 \cdots f_n.$$

Dado que $|sop(x)| = 1$, se debe tener que $|sop(f_i)| = 1$ para cada $i \in \{1, \ldots, n\}$, y así $f_i = a_i x^{\alpha_i}$ con $a_i \in K$ y $\alpha_i \in \mathbb{Q}^+$ para cada i que ya hemos visto no son irreducibles. Por lo tanto x no se factoriza en irreducible en $K[M]$. Es decir

Entonces tiene sentido preguntarse si existen condiciones bajo las cuales en un dominio entero se de la factorización en irreducibles.

Definición 1.2.42. *Sean D un dominio entero y $r, s \in D$ tales que $r \mid s$, r es un* ***divisor propio*** *de s si $s \nmid r$.*

Proposición 1.2.43. *Sean D un dominio entero y $r, s \in D$. Se tiene que:*

1) *Si $r \mid s$ y existe $t \in D - U(D)$ tal que $rt = s$ entonces r es un divisor propio de s.*
2) *r es un divisor propio de s si y sólo $r \mid s$ y r y s no son asociados.*
3) *r es un divisor propio de s si y sólo $sD \subsetneq rD$. (Ver Proposiciones 1.2.29 y 1.2.30)*

Definición 1.2.44. *Un dominio entero D cumple con la* ***condición finita de divisores (CFD)*** *si D no contiene sucesiones $\{d_n\}_{n\in\mathbb{N}}$ de elementos en D tales que d_{n+1} sea un divisor propio de d_n.*

El Ejemplo 1.2.41 muestra la existencia de dominios enteros que no tiene la CFD.

Proposición 1.2.45. *Sea D un dominio entero que cumple con la CFD. Si $s \in D - (\{0\} \cup U(D))$, entonces existe r irreducible en D tal que $r \mid s$.*

Demostración. *Sea $s \in D - (\{0\} \cup U(D))$, si s es irreducible, como $s = s \cdot 1$ la proposición se cumple trivialmente. Así que supongamos que s es reducible, por lo tanto existen $a_0, b_0 \in D - (\{0\} \cup U(D))$ tales que $s = a_0 b_0$. Si a_0 o b_0 son irreducibles, hemos terminado. Si no, como a_0 y b_0 no son irreducibles. Considerando a_0 existen $a_1, b_1 \in D - (\{0\} \cup U(D))$ tales que $a_0 = a_1 b_1$ y nuevamente, si a_1 o b_1 son irreducibles ya se ha terminado. Si no, entonces a_1 y b_1 no son irreducibles y podemos continuar el proceso.*

La afirmación es que este proceso tiene que producir un elemento irreducible en D que divide a s en un numero finito de pasos, ya que sino fuera así, obtendríamos una sucesión infinita $\{a_n\}_{n\in\mathbb{N}}$ de elementos de $D - (\{0\} \cup U(D))$ tal que a_{n+1} es un divisor propio de a_n, lo que contradice la hipótesis ∎

Teorema 1.2.46. *Si D es un dominio entero que cumple con la CFD, entonces D es un dominio de factorización.*

Ahora se introducirá una clase de anillos en los cuales para el caso de ser dominios enteros, se puede asegurar que satisfacen la CFD y en consecuencia un dominio de factorización.

Definición 1.2.47. *Un anillo R se dice que R es un* ***anillo noetheriano*** *si todo ideal de R es finitamente generado. Es decir, R es noetheriano si para todo ideal I de R, existen $n \in \mathbb{Z}^+$ y $r_1, \ldots, r_n \in I$, tales que $\langle r_1, \ldots, r_n \rangle = I$.*

Ejemplo 1.2.48.

1) Todo anillo de ideales principales es un anillo noetheriano. En particular el anillo de los enteros $\mathbb{Z}$ es un dominio entero noetheriano.
2) Todo anillo finito es un anillo noetheriano.

Teorema 1.2.49. *Para un anillo R, son equivalentes*

1) *R es un anillo noetheriano.*
2) *Toda sucesión creciente (respeto a la inclusión) de ideales de R se estaciona. Es decir, si $\{I_j\}_{j\in\mathbb{N}}$ es una familia de ideales de R tales que $I_n \subseteq I_{n+1}$ para cada $n \in \mathbb{N}$, entonces existe $n_o \in \mathbb{N}$ tal que $I_n = I_{n_o}$ para todo $n \geqslant n_o$.*
3) *Toda familia no vacía de ideales de R (con el orden parcial dado por la inclusión) tiene un maximal.*

Teorema 1.2.50. *Sea D es un dominio entero. Si D es noetheriano, entonces D cumple CFD.*

Demostración. *Para verificarlo, se procederá por contradicción. Entonces supongamos que D es noetheriano y no cumple la CFD. Así, podemos encontrar una sucesión $\{d_n\}_{n\in\mathbb{N}}$ de elementos en D tales que $d_{n+1} \mid d_n$ para cada $n \in \mathbb{N}$ y d_{n+1} es un divisor propio de d_n.*

Ahora, para cada $n \in \mathbb{N}$, tomemos el ideal principal d_nD. Como $d_{n+1} \mid d_n$, de la Proposición 1.2.29 tenemos que $d_nD \subseteq d_{n+1}D$ y de la Proposición 1.2.43 (3) que cada una de estas contenciones es propia. Así se tendría que $\{d_nD\}_{n\in\mathbb{N}}$ es una sucesión estrictamente creciente de ideales de D, contradiciendo la hipótesis de que D es un dominio noetheriano. Por lo tanto D cumple la CFD. ∎

Corolario 1.2.51. *Si D es un dominio entero noetheriano, entonces todo elemento no nulo que no sea una unidad en D se factoriza en irreducibles en D. (Ver Proposición 1.2.46)*

Corolario 1.2.52. *Si D es un dominio de ideales principales, entonces todo elemento no nulo que no sea una unidad en D se factoriza en irreducibles en D.*

El siguiente resultado clásico del Álgebra Conmutativa, nos permite exhibir una gran cantidad de dominios enteros que cumplen CFD.

Teorema 1.2.53 *(Teorema de las bases de Hilbert). Sea R un anillo. Entonces*

$$R \text{ es noetheriano si y sólo si } R[x] \text{ es noetheriano.}$$

Corolario 1.2.54. *Sea R un anillo. Entonces, R es noetheriano si y sólo si $R[x_1, \ldots, x_n]$ es noetheriano para todo $n \in \mathbb{Z}^+$.*

Ejemplo 1.2.55.

1) Todo dominio de ideales principales cumple la CFD. En particular el anillo de los enteros $\mathbb{Z}$ cumple la CFD.
2) Si D es un dominio noetheriano, entonces $D[x_1, \ldots, x_n]$ cumple la CFD.

Definición 1.2.56. *Consideremos D un dominio de factorización y supongamos que para $d \in D - (\{0\} \cup U(D))$ se tiene que:*

$$d = r_1 \cdots r_n \quad y \quad d = r'_1 \cdots r'_m$$

*son dos factorizaciones de d como producto de irreducibles en D. Se dice que las **factorizaciones son esencialmente iguales** si $n = m$ y existe una permutación α en el conjunto $\{1, \ldots, n\}$ tal que r_i es asociado de $r'_{\alpha(i)}$.*

*Si D es un dominio de factorización, D es un **dominio de factorización única** (DFU), si para todo $d \in D - (U(D) \cup \{0\})$, cualesquiera dos factorizaciones de d como producto de irreducibles en D, son esencialmente iguales..*

Ejemplo 1.2.57. Sea K un campo y sea D el dominio entero generado por $\{x^3, xy, y^3\}$ y K en $K[x]$ (Ver Ejemplo 1.2.20). Claramente xy, x^3 y y^3 son irreducibles en D y $x^3y^3 = (xy)(xy)(xy)$, donde xy no es asociado x^3 ni con y^3. Por lo tanto las dos factorizaciones no son esencialmente iguales y entonces D no es un DFU.

El siguiente teorema, es un resultado clásico atribuido a Carl Friedrich Gauss, que nos es útil, para dar ejemplos de anillo de factorización única.

Teorema 1.2.58. *Si D es un DFU, entonces $D[x]$ es un DFU.*

Corolario 1.2.59. *Si D es un DFU, entonces $D[x_1,\ldots,x_n]$ es un DFU para cada $n \in Z^+$.*

Ejemplo 1.2.60.

1) $\mathbb{Z}[x_1,\ldots,x_n]$ es un DFU para cada $n \in \mathbb{Z}^+$.
2) Si k es un campo $k[x_1,\ldots,x_n]$ es un DFU para cada $n \in \mathbb{Z}^+$.
3) Si k es un campo $k[x_\infty]$ es un DFU. Nótese que este es un dominio de factorización única que no es un dominio noetheriano, pues si para cada $n \in \mathbb{N}$ definimos $I_n = \langle x_1,\ldots,x_n\rangle$, se tiene que $\{I_n\}_{i\in\mathbb{N}}$ es una cadena de ideales de $k[x_\infty]$ que no se estaciona.

La tarea que emprenderemos a continuación es la de encontrar propiedades que caractericen a un DFU.

Teorema 1.2.61. *Sea D un DFU. Entonces d es un elemento irreducible en D si y sólo si d es un elemento primo en D.*

Demostración.

$\Longrightarrow$) *Supongamos que D es un DFU, $r \in D$ un elemento irreducible en D y que $r \mid st$ con $s,t \in D$.*

Si $s = 0$ o $t = 0$, trivialmente $r \mid s$ o $r \mid t$. Así que podemos suponer $s \neq 0$ y $t \neq 0$.

Si $s \neq 0$ y $t \neq 0$, podría suceder que $s \in U(D)$ o $t \in U(D)$. Sin pérdida de generalidad supongamos que $s \in U(D)$ y sea $u \in U(D)$ es tal que $su = 1$. Como $r \mid st$, por la Proposición 1.2.3 inciso (3) tenemos que $ru \mid u(st) = t$ y ya que $r \mid ru$, entonces por transitividad (Proposición 1.2.3 inciso (5)) concluimos que $r \mid t$.

Por último supongamos que $s,t \in D - (\{0\} \cup U(D))$ y sea $z \in D - (\{0\} \cup U(D))$ tal que $rz = st$. Como D es un anillo de factorización única podemos escribir

$$s = p_1 \cdots p_n, \quad t = q_1 \cdots q_m, \quad y \quad z = r_1 \cdots r_s$$

donde $n,m,k \in \mathbb{Z}^+$ y $p_i, q_j, r_t \in D$ son elementos irreducibles en D para $i = 1,\ldots,n$, $j = 1,\ldots,m$ y $t = 1,\ldots,k$. Entonces

$$r(r_1 \cdots r_k) = (p_1 \cdots p_n)(q_1 \cdots q_m),$$

por la unicidad de la factorización como producto de elementos irreducibles en D, se deduce entonces que existe algún $i_o \in \{1,\ldots,n\}$ o $j_o \in \{1,\ldots,m\}$ tal que r es asociado a p_{i_o} o r es asociado a q_{j_o}. Sin pérdida de generalidad podemos suponer que r es asociado a p_{i_o} para algún $i_o \in \{1,\ldots,n\}$ y entonces por la Proposición 1.2.26 inciso (1) se tiene que $r \mid p_{i_o}$ y de aquí concluimos que $r \mid s$. Por lo tanto r es un elemento primo en D.

$\Longleftarrow$) *Es la Proposición 1.2.19.* ∎

Si D es un DFU y p es un irreducible en D, tomemos

$$\mathcal{M}_p = \{up \mid u \in U(D)\}.$$

Claramente $r \in \mathcal{M}_p$ si y sólo si r es asociado con p. Luego por la Proposición 1.2.24 inciso (3), tenemos que todos los elementos de $\mathcal{M}_p$ son irreducibles. Es entonces que

$$\Gamma = \{\mathcal{M}_p \subseteq D \mid p \text{ es irreducible en } D\},$$

es una partición en el conjunto de los elementos irreducibles de D. Si f es una función de elección[5] *en Γ, el conjunto dado por $\mathfrak{P} = \{f(\mathcal{M}) \in D \mid \mathcal{M} \in \Gamma\}$ satisface que dado r un irreducible en D, existe un y sólo un elemento $p \in \mathfrak{P}$ tal que r es asociado con p. A una elección de dicho conjunto $\mathfrak{P}$ se le llama un* ***conjunto de representantes de irreducibles****, lo que abreviaremos por CRI en D.*

Si D es un DFU y $\{p_i\}_{i\in I} \subseteq \mathfrak{P}$ es un CRI de D. Dado $d \in D - (U(D) \cup \{0\})$ y

$$d = r_1 r_2 \cdots r_n \tag{2.1}$$

una factorización en irreducibles en D. Para cada $i \in \{1, \ldots, n\}$ tomemos p_{i_j} el respectivo representante de r_j en $\mathfrak{P}$. Como r_j y p_{i_j} son asociados, existe $u_j \in U(D)$ tal que $r_j = u_j p_{i_j}$. Reemplazando estas últimas igualdades en la igualdad (2.1), obtenemos que

$$d = (u_1 p_{i_1})(u_2 p_{i_2}) \cdots (u_n p_{i_n}) = u p_{i_1} p_{i_2} \cdots p_{i_n}, \text{ donde } u = u_1 u_2 \cdots u_n \in U(D). \tag{2.2}$$

Como algunos de los irreducibles que aparecen en la igualdad (2.2) pueden ser iguales, al agruparlos y reindicarlos obtenemos que

$$d = u p_1^{e_1} \cdots p_k^{e_k} \tag{2.3}$$

donde $k, e_i \in \mathbb{Z}^+$, $p_i \in \mathfrak{P}$ para $i \in \{1, \ldots, k\}$ y $u \in U(D)$. Nótese que en esta factorización p_i no es asociado de p_j si $i \neq j$.

Obsérvese que la factorización a la que se llego en la igualdad (2.3) no depende de la factorización en irreducibles de d (dada en 2.1) de la que se parte. Tenemos entonces que dado $d \in D - (U(D) \cup \{0\})$ la pareja definida por $(k, \{e_1, \ldots, e_n\}$ es intrínseca a d.

Observación 1. 2.62. Si D es un DFU, $\mathfrak{P}$ un CRI en D y $r, s \in D - (U(D) \cup \{0\})$. De la igualdad (2.3), es claro que el conjunto dado por:

$$\mathfrak{P}_{r,s} = \{p \in \mathfrak{P} \mid p \mid r \quad o \quad p \mid s\},$$

es un conjunto finito. Entonces existe $n \in \mathbb{Z}^+$ tal que $\mathfrak{P}_{r,s} = \{p_1, \ldots, p_n\}$ con $p_i \in \mathfrak{P}$. Así es posible escribir

$$r = u_r p_1^{e_1} \cdots p_k^{e_k}$$

donde $u_r \in U(D)$ y $e_i = 0$ si $p_i \nmid r$, y

$$s = u_s p_1^{f_1} \cdots p_k^{f_k}$$

con $u_s \in U(D)$ y $f_i = 0$ si $p_i \nmid s$.

Proposición 1.2.63. *Sean D un DFU, $\mathfrak{P}$ un CRI y $d, g \in D - (U(D) \cup \{0\})$ tales que $d = u p_1^{e_1} \cdots p_k^{e_k}$ $k, e_i \in \mathbb{Z}^+$, $p_i \in \mathfrak{P}$ para $i \in \{1, \ldots, k\}$ y $u \in U(D)$ y $g \mid d$. Entonces $g = u' p_1^{f_1} \cdots p_k^{f_k}$ con $f_i \in \mathbb{N}$ para $i = 0, \ldots, k$.*

Proposición 1.2.64. *Sean D un DFU, $\mathfrak{P}$ un CRI y $d, g \in D - (U(D) \cup \{0\})$ tales que $d = u p_1^{e_1} \cdots p_k^{e_k}$ y $g = u' p_1^{f_1} \cdots p_k^{f_k}$ con $k \in \mathbb{Z}^+$, $p_i \in \mathfrak{P}$ y $e_i, f_j \in \mathbb{N}$ para todo $i \in \{1, \ldots, k\}$. Entonces $g \mid d$ si y sólo si $f_i \leqslant d_i$ para cada $i \in \{1, \ldots, k\}$.*

Proposición 1.2.65. *Sean D un DFU y $d \in D - (\{0\} \cup U(D))$. Entonces d tiene un número finito de divisores no asociados.*

Demostración. *Consideremos $d \in D - (\{0\} \cup U(D))$ y sea $\Lambda_d = \{r \in D \mid r \text{ divide a } d\}$. Nótese que la relación en Λ_d dada por $r \approx r'$ si y sólo si r es asociado con r' es una relación de equivalencia en Λ_d. La cual induce una partición $\Lambda_d / \approx$.*

---

[5] El Axioma de Elección es un axioma de la teoría de conjuntos que dice: si $\mathcal{F} = \{C_i\}_{i\in I}$ es una familia no vacía de conjuntos no vacíos, existe $f : \mathcal{F} \longrightarrow \bigcup_{i\in I} C_i$ tal que $f(C_i) \in C_i$ para cada $i \in I$ y a dicha función se le llama una función de selección.

Si $\mathfrak{P}$ es un CRI de D, existen $n, e_1, \ldots, e_n \in \mathbb{Z}^+$ y $p_1, \ldots, p_n \in \mathfrak{P}$ tales que

$$d = up_1^{e_1} \cdots p_k^{e_k}.$$

De la Proposición 1.2.64, es claro que un representante de cada clase en $\Lambda_d/\approx$ esta dado por un elemento de la forma $y = up_1^{e_1'} \cdots p_n^{e_n'}$ con $0 \leqslant e_i' \leqslant e_i$, y como para cada $i \in \{1, \ldots, n\}$ solo existen un número finito de $e_i's$ en $\mathbb{N}$ que cumplen esta propiedad. Entonces $\Lambda_d/\approx$ es un conjunto finito y por lo tanto d solo tiene un número finito de divisores en D. ∎

Corolario 1.2.66. *Si D es un DFU, entonces D es un dominio que cumple la CFD.*

Teorema 1.2.67. *Sea D un dominio entero. Entones D es un DFU si y sólo si D cumple la CFD y todo irreducible es primo.*

Demostración.

⇒) *Supongamos que D es un dominio de factorización única. Por el Corolario 1.2.66, D cumple la CFD y por el Teorema 1.2.61 tenemos que todo elemento irreducible en D es un elemento primo en D.*

⇐) *Supongamos que D cumple la CFD y que todo irreducible es un primo. Como D cumple la CFD, del Teorema 1.2.46 tenemos que todo elemento se puede factorizar como producto de elementos irreducibles en D. Entonces es suficiente verificar que dos posibles factorizaciones en irreducible de D de un elemento no nulo que no sea una unidad en D, son esencialmente iguales.*

Sea $d \in D \backslash U(D)$, $d \neq 0$ y

$$d = p_1 \cdots p_n \;\; y \;\; d = q_1 \cdots q_m$$

dos factorizaciones de d en irreducibles de D.

Se demostrará, por inducción sobre n, que $n = m$ y que $p_i = q_{\alpha(i)}$ con α alguna permutación de $\{1, \ldots, n\}$.

Si $n = 1$, entonces d es irreducible en D. Luego, si suponemos que $d = q_1 \cdots q_m$ es una factorización en irreducibles en D, como $q_1 \mid d$, de la Proposición 1.2.25 inciso (1) tenemos que d y q_1 son asociados. Además como $d = q_1(q_2 \cdots q_m)$, de la Proposición 1.2.25 inciso (2) se tiene que, $q_2 \cdots q_m \in U(D)$. Lo que muestra la imposibilidad que pase que $m \geqslant 2$. Por lo tanto $m = 1$ y d es asociado a q.

Ahora supongamos que la proposición es válida para $n \in \mathbb{Z}^+$ y sean

$$d = p_1 \cdots p_n p_{n+1} \;\; y \;\; d = q_1 \cdots q_m$$

dos factorizaciones en irreducibles de d en D. Claramente se tiene que

$$p_1 \cdots p_n p_{n+1} = q_1 \cdots q_m. \tag{2.4}$$

Como suponemos que todo irreducible es primo en D, en particular tenemos que p_{n+1} es primo, y luego, dado que $p_{n+1} \mid q_1 \cdots q_m$, sin pérdida de generalidad podemos suponer que $p_{n+1} \mid q_m$. Siendo que p_{n+1} y q_m son irreducibles, de la Proposición 1.2.25 inciso (1), se obtiene que p_{n+1} y q_m son asociados y así $up_{n+1} = q_m$ para algún $u \in U(D)$. Sustituyendo esta última igualdad en (2.4), obtenemos que

$$p_1 \cdots p_{n+1} = q_1 \cdots q_{m-1}(up_n),$$

y siendo que $p_{n+1} \neq 0$ y D es un dominio entero, entonces

$$p_1 \cdots p_n = q_1 \cdots q_{m-2}(q_{m-1}u),$$

donde por la Proposición 1.2.24 inciso (3) tenemos que $q_{m-1}u$ es irreducible en D. Luego, por hipótesis de inducción obtenemos que $n = m - 1$ y existe una permutación α en

$\{1,\dots,n\}$ tal que p_i y $q_{\alpha(i)}$ son asociados. Claramente $n+1=m$ y además es posible extender α a una permutación $\overline{\alpha}$ en $\{1,\dots,n+1\}$, definiéndola por $\overline{\alpha}(i)=\alpha(i)$ si $i\in\{1,\dots,n\}$ y $\overline{\alpha}(n+1)=n+1$. Y así $\overline{\alpha}$ es tal que p_i es asociado de $q_{\overline{\alpha}(i)}$ para cada $i\in\{1,\dots,n\}$. Por lo tanto las factorizaciones son esencialmente iguales y así D es un DFU. ∎

Teorema 1.2.68. *Sea D un dominio de ideales principales. Entonces D es un DFU.*

Demostración. *Sea D un dominio de ideales principales, como D es un dominio noetheriano (Ejemplo 1.2.48 inciso (1)), por el Teorema 1.2.50 tenemos que D es un dominio que cumple la CFD. Además del Corolario 1.2.39, tenemos que todo elemento irreducible en D es un elemento primo de D. Luego por el Teorema 1.2.67, D es un DFU.* ∎

Definición 1.2.69. *Sean D un dominio entero y $r,s\in D$. Un elemento $d\in D-\{0\}$ es un **máximo común divisor** de r y s, si cumple que*

1) *$d\mid r$ y $d\mid s$.*
2) *Para todo $c\in D$ tal que $c\mid r$ y $c\mid s$ se tiene que $c\mid d$.*

*Un dominio entero en el que cada par de elementos no nulos tenga máximo común divisor se dice que es un **dominio con la propiedad del Máximo Común Divisor**, que abreviaremos por **MCD***

Si D es un dominio con la propiedad de MCD y $r,s\in D-\{0\}$, se denotará por $\Delta_{r,s}$ al conjunto de los máximos comunes divisores de r y s en D.

Proposición 1.2.70. *Sea D un dominio con la propiedad de MCD y $r,s\in D-\{0\}$. Entonces*

1) *Si $d\in\Delta_{r,s}$, entonces $d\neq 0$.*
2) *$\Delta_{r,s}=\Delta_{s,r}$.*
3) *Si $d,d'\in\Delta_{r,s}$ entonces d y d' son asociados en D.*
4) *Si $d,d'\in D$ son elementos asociados en D y $d\in\Delta_{r,s}$, entonces $d'\in\Delta_{r,s}$.*
5) *Si $r\in U(D)$, entonces $1\in\Delta_{r,s}$.*
6) *Si r' es asociado de r y s' es asociado de s, entonces $\Delta_{r,s}=\Delta_{r',s'}$.*

En virtud de la Proposición 1.2.70 incisos (3) y (4), se tiene que si $r,s\in D$ y $d\in\Delta_{r,s}$, entonces

$$\Delta_{r,s}=\{du\in D\mid u\in U(D)\}.$$

En adelante para representar la elección de un elemento en $\Delta_{r,s}$, usaremos la notación $(\boldsymbol{r,s})$.

Proposición 1.2.71. *Sea D un dominio con la propiedad de MCD y $r,s\in D-\{0\}$. Si r es irreducible en D, entonces*

$$\Delta_{r,s}=U(D)\quad o\quad \Delta_{r,s}=\{ru\in D\mid u\in U(D)\}.$$

Proposición 1.2.72. *Si D es un DFU, entonces D es un dominio que tiene la propiedad del MCD*

Demostración. *Sea D un DFU, y $r,s\in D-\{0\}$. Si $r\in U(D)$ o $s\in U(D)$, claramente $1\in D$ es un máximo común divisor de r y s. Entonces podemos suponer que $r,s\in D-(\{0\}\cup U(D))$.*

Sea $\mathfrak{P}$ un CRI en D. Como $r,s\in D-(U(D)\cup\{0\})$, entonces

$$r=u_r p_1^{e_1}\cdots p_k^{e_k}\quad y\quad s=u_s p_1^{f_1}\cdots p_k^{f_k}$$

donde $u_r,u_s\in U(D)$ y $p_i\in\mathfrak{P}_{r,s}$ y $e_i,f_i\in\mathbb{N}$ para todo $i=1,\dots,n$ (ver Observación 1.2.62).

Si consideramos

$$d=p_1^{g_1}\cdots p_t^{g_t},\quad donde\quad g_i=mín(e_i,f_i).$$

Debido a la Proposición 1.2.64, $d\mid r$ y $d\mid s$. Ahora, si $c\in D$ es tal que $c\mid r$ y $c\mid s$, por la Proposición 1.2.63 tenemos que $c=wp_1^{k_1}\cdots p_t^{k_t}$, donde $w\in U(D)$ y $0\leqslant k_i\leqslant e_i$ y $0\leqslant k_i\leqslant f_i$,

con lo que $k_i \leqslant g_i$ para todo $i = 1, \ldots, t$. Nuevamente por la Proposición 1.2.64 se verifica que $c \mid d$. Por lo tanto d es un máximo común divisor de r y s. Luego entonces D tiene la propiedad del MCD. ∎

Para los resultados 1.2.73 al 1.2.79, se supone D un dominio entero con la propiedad MCM. Y además, como ya se había comentado, el símbolo (r, s) representará la elección de un máximo común divisor en $\Delta_{r,s}$

Lema 1.2.73. *Sean $r, s, t \in D - \{0\}$, entonces $((r, s), t)$ es asociado de $(r, (s, t))$ en D.*

Demostración. *Sea $d_1 = ((r, s), t)$. Dado que $d_1 \in \Delta_{(r,s),t}$, $d_1 \mid t$ y $d_1 \mid (r, s)$. Además tenemos que $(r, s) \mid r$ y $(r, s) \mid s$, luego por transitividad se obtiene que $d_1 \mid r$ y $d_1 \mid s$. Ahora, como $d_1 \mid s$ y $d_1 \mid t$, entonces $d_1 \mid (s, t)$ y como además $d_1 \mid r$. Podemos concluir que $d_1 \mid (r, (s, t))$. Un razonamiento análogo muestra que $(r, (s, t)) \mid ((r, s), t)$. Como $r, s, t \in D - \{0\}$, por la Proposición 1.2.70 inciso (1) tenemos que $(r, (s, t)) \neq 0$ y entonces por la Proposición 1.2.26 inciso (2) podemos concluir que $((r, s), t)$ y $(r, (s, t))$ son asociados en D.* ∎

Lema 1.2.74. *Sean $r, s, t \in D - \{0\}$, entonces $t(r, s)$ es asociado de (tr, ts) en D.*

Demostración. *Por definición $(r, s) \mid r$ y $(r, s) \mid s$. Luego por la Proposición 1.2.3 inciso (3), tenemos que $t(r, s) \mid tr$ y $t(r, s) \mid ts$, entonces podemos concluir que $t(r, s) \mid (tr, ts)$. Por los tanto existe $x \in D$ tal que*

$$(tr, ts) = t(r, s)x. \tag{2.5}$$

Por otro lado, como $(tr, ts) \mid tr$, existe $y \in D$ tal que $(tr, ts)y = tr$. Sustituyendo (2.5) en esta última igualdad obtenemos que $(t(r, s)x)y = tr$ y siendo que $t \neq 0$ y D es un dominio entero, se tiene que $(r, s)xy = r$. Por lo tanto $(r, s)x \mid r$. Un razonamiento análogo muestra que $(r, s)x \mid s$ y entonces tenemos que $(r, s)x \mid (r, s)$. Ahora, por la Proposición 1.2.70 inciso (1) tenemos que $(r, s) \neq 0$ y entonces de la Proposición 1.2.25 inciso (2) se tiene que $x \in U(D)$. Por lo tanto $t(r, s)$ es asociado de (tr, ts). ∎

Lema 1.2.75. *Sean $r, s, t \in D - \{0\}$. Si (r, s) y (r, t) son asociados a 1, entonces (r, st) es asociado a 1.*

Demostración.

Por el Lema 1.2.74 se tiene que (rt, st) es asociado a t y que (r, rt) es asociado a r. Se sigue entonces que

$$1 \underset{\text{Hip.}}{\text{ es asociado a }} (r, t) \underset{\substack{t \text{ es asociado a } (rt,st) \\ \text{Prop. 1.2.70 (6)}}}{\text{ es asociado a }} (r, (rt, st)) \underset{\text{Lema 1.2.73}}{\text{ es asociado a }} ((r, rt), st) \underset{\substack{(r,rt) \text{ es asociado a } r \\ \text{Prop. 1.2.70 (6)}}}{\text{ es asociado a }} (r, st)$$

Por lo tanto (r, st) es asociado al 1. ∎

Lema 1.2.76. *Sea p un elemento irreducible en D. Entonces, (p, t) es asociado a 1 si y sólo si $p \nmid t$.*

Demostración.

- $\Rightarrow$) *Para mostrar este hecho, procederemos por reducción al absurdo. Y así supongamos que $p \mid t$. Entonces $p \mid (p, t)$. Dado que (p, t) es asociado a 1, por la Proposición 1.2.25 inciso (3), se tiene que p divide a 1, produciendo un absurdo pues p es irreducible en D. Por lo tanto $p \nmid t$.*
- $\Leftarrow$) *Supongamos que p es irreducible en D y sea $(p, t) \in \Delta_{p,t}$. Por la Proposición 1.2.71 solo caben dos posibilidades, que p sea asociado a (p, t) o que $(p, t) \in U(d)$. Si suponemos que (p, t) es asociado a p se tendría como consecuencia que $p \mid t$ que no es consistente con la hipótesis. Luego entonces $(p, t) \in U(d)$, es decir (p, t) es asociado a 1.* ∎

Proposición 1.2.77. *Sean $p \in D$ es irreducible en D y $r, s \in D$ tales que $p \mid rs$ y que (p, r) sea asociado a 1. Entonces $p \mid s$*

Demostración. *Supongamos que $p \nmid s$. Entonces por el Lema 1.2.76, (p, s) es asociado a 1, como además por hipótesis tenemos que (p, r) es asociado a 1, del Lema 1.2.75 obtenemos que (p, rs) es asociado a 1. Nuevamente aplicando el Lema 1.2.76, se tiene que $p \nmid rs$ que contradice la hipótesis. Por lo tanto $p \mid s$.* ∎

Corolario 1.2.78. *Sean $p \in D$ irreducible y $\alpha \in \mathbb{N}$. Supongamos que $p^\alpha \mid rs$ y que (p, r) es asociado a 1. Entonces $p^\alpha \mid s$.*

Corolario 1.2.79. *S $p \in D$ irreducible en D, entonces p es un elemento primo en D.*

Teorema 1.2.80. *Sea D un dominio entero. Entones D es un dominio de factorización única si y sólo si D cumple la CFD y la propiedad del MCD.*

Demostración.

⇒) *Si D es un DFU, por el Corolario 1.2.66 D cumple la CFD y de la Proposición 1.2.72, D tiene la propiedad del MCD.*

⇐) *Supongamos que D es un dominio entero que cumple la CFD y la propiedad del MCD. El Corolario 1.2.79 muestra que todo elemento irreducible en D es un elemento primo en D. Entonces, al aplicar el Teorema 1.2.67 se obtiene el resultado.* ∎

Proposición 1. 2.81. *Sea D un dominio de ideales principales y $x, y \in D\backslash\{0\}$. Entonces, $dD = xD + yD$ y sólo si d es un máximo común divisor de x y y.*

Demostración.

⇒) *Supongamos que $d \in D$ es tal que $dD = xD + yD$ y sea $(x, y) \in D$ un máximo común divisor de x y y.*

Como $x, y \in dD$, entonces $d \mid x$ y $d \mid y$ y así se tiene que $d \mid (x, y)$. Por otro lado, tenemos que

$$d = xa + yb \quad \text{para algunos } a, b \in D. \tag{2.6}$$

Dado que $(x, y) \mid x$ y $(x, y) \mid y$, existen $x', y' \in D$ tales que $(x, y)x' = x$ y $(x, y)y' = y$. Sustituyendo estas últimas igualdades en (2.6), obtenemos que

$$d = (x, y)x'a + (x, y)y'b = (x, y)(x'a + y'b),$$

y así $(x, y) \mid d$. Ahora de la Proposición 1.2.70 inciso (1) se tiene que $(x, y) \neq 0$, luego por la Proposición 1.2.26 obtenemos que d y (x, y) son asociados en D. Finalmente de la Proposición 1.2.70 inciso (4) tenemos que d es un máximo común divisor de x y y en D.

⇐) *Sea $(x, y) \in D$ un máximo común divisor de x y y. Como D es un dominio de ideales principales, existe $d \in D$ tal que $dD = xD + yD$. Luego por ⇒) de este teorema, d es máximo común divisor de x y y en D. Entonces por la Proposición 1.2.70 inciso (3) se tiene que (x, y) y d son asociados en D, y de la Proposición 1.2.30 finalmente se tiene que $(x, y)D = dD$.* ∎

Corolario 1.2.82. *Sea D un dominio de ideales principales, $x, y \in D\backslash\{0\}$ y d un máximo común divisor de x y y. Entonces existen $z, w \in D$ tales que $zx + wy = d$.*

Definición 1.2.83. *Sea D un DFU. Si para todo $x, y \in D - \{0\}$ existen $a, b \in D$ tales que $ax + by = d$, donde d es un máximo común divisor de x y y, se dice que D es* ***dominio de Bezout***

Lema 1.2.84. *Si D es un dominio de Bezout, entonces D es un dominio noetheriano.*

Demostración. *Para demostrar el enunciado, vamos a proceder por reducción al absurdo. Supongamos que D no es noetheriano y sea $\{I_n\}_{n\in\mathbb{N}}$ una sucesión creciente de ideales de D que no se estaciona, es decir, para cada $n \in \mathbb{N}$ se tiene que $I_n \subsetneq I_{n+1}$. Nótese que es posible suponer que $I_0 \neq \{0\}$, pues en caso de suceder que $I_0 = \{0\}$, la sucesión $\{I_n\}_{n\in\mathbb{N}} - \{I_0\}$ es una sucesión creciente de ideales de D que no se estaciona donde $I_1 \neq \{0\}$.*

Entonces es posible elegir una sucesión de elementos $\{a_i\}_{i\in\mathbb{N}} \subseteq D$ tales que

$$a_0 \in I_0 - \{0\} \quad y \quad a_n \in I_n - I_{n-1} \quad si \quad n > 0.$$

Tomemos $d_0 = a_0$ y recursivamente constrúyase $d_n = (d_{n-1}, a_n)$. Ahora demostraremos que $\{d_n\}_{n\in\mathbb{N}}$ es una sucesión de divisores propios en D lo que es un absurdo, pues D es un DFU y por la Corolario 1.2.66 se tiene que D cumple la CFD.

Primero mostraremos que $d_n \in I_n$ para todo $n \in \mathbb{N}$.

Claramente $d_0 \in I_0$, pues $d_0 = a_0$. Ahora supongamos que $d_n \in I_n$, como D es un dominio de Bezout y $d_{n+1} = (d_n, a_{n+1})$, existen $x, y \in D$ tales que $d_{n+1} = d_n x + a_{n+1} y$. Dado que suponemos que $d_n \in I_n \subseteq I_{n+1}$ y además pasa que $a_{n+1} \in I_{n+1}$, entonces $d_{n+1} = d_n x + a_{n+1} y \in I_{n+1}$.

Nótese que $d_n \notin I_{n-1}$ para todo $n \geqslant 1$, pues de existir $n \in \mathbb{Z}^+$ tal que $d_n \in I_{n-1}$, como $d_n \mid a_n$, se tendría que $a_n \in I_{n-1}$ lo que contradice la elección de los $a_{n's}$.

Evidentemente $d_{n+1} \mid d_n$. Ahora mostraremos que $d_n \nmid d_{n+1}$ para todo $n \in \mathbb{N}$. Para ello supongamos lo contrario, es decir que supongamos que existe $n \in \mathbb{N}$ tal que $d_n \mid d_{n+1}$, en consecuencia se tendría que $d_{n+1} \in I_n$ que como ya se vio en el párrafo anterior no es posible. Por lo tanto $\{d_n\}_{n\in\mathbb{N}}$ es una sucesión de divisores propios en D, que como ya habíamos mencionado es un absurdo y en consecuencia D es un dominio noetheriano. ∎

Proposición 1.2.85. *Si D es un dominio de Bezout, entonces D es un domino de ideales principales.*

Demostración. *Por el Lema 1.2.84 tenemos que D es un dominio noetheriano y entonces todo ideal de D es finitamente generado. Para mostrar el resultado se procederá por inducción sobre el número de generadores del ideal en cuestión.*

Si I es generado por un sólo elemento, I es ya un ideal principal y entonces la proposición se cumple trivialmente.

Dada su utilidad para el caso general, se demostrará el caso para cuando I es generado por dos elementos. Sea entonces I un ideal de D y $x, y \in I - \{0\}$ tales $I = xD + yD$. Como D es un DFU, existe $(x, y) \in \Delta_{x,y}$ y dado que $(x, y) \mid x$ y $(x, y) \mid y$, se tiene entonces que $(x, y) \mid ax + by$ para todo $a, b \in D$ de donde concluimos que $I \subseteq (x, y)D$. Por otro lado, como D es un dominio de Bezout, existen $z, w \in D$ tales que $zx + wy = (x, y)$ para algún $z, w \in D$ por lo que $(x, y) \in I$ y en consecuencia $(x, y)D \subseteq I$. Por lo tanto $I = (x, y)D$.

Ahora supongamos que la propiedad vale para $n \in \mathbb{N}$ es decir si I es un ideal de D que es generado por n elementos de I, entonces I es un ideal principal.

Sea I un ideal generado por $n+1$ elementos no nulos, digamos $I = \langle\{x_1, \ldots, x_n, x_{n+1}\}\rangle$ con $x_i \in I$ para cada $i \in \{1, \ldots, n\}$. Como

$$\langle\{x_1, \ldots, x_n, x_{n+1}\}\rangle \underset{\text{Pro. 1.1.14 (3)}}{=} \langle\{x_1, \ldots, x_n\}\rangle + x_{n+1}D.$$

Aplicando la hipótesis de inducción en el ideal $\langle\{x_1, \ldots, x_n\}\rangle$, se tiene que existe $x \in D$ tal que $\langle\{x_1, \ldots, x_n\}\rangle = xD$.

Teniendo entonces que

$$\langle\{x_1, \ldots, x_n\}\rangle + x_{n+1}D = xD + x_{n+1}D.$$

Luego, por el caso $n = 2$, si $(x, x_{n+1}) \in \Delta_{x,x_{n+1}}$, entonces $xD + x_{n+1}D = (x, x_{n+1})D$. Por lo tanto $I = (x, x_{n+1})D$ y es así que D es un dominio de ideales principales. ∎

Teorema 1.2.86. *Sea D un DFU. Entonces D es un dominio de ideales principales si y sólo si D es un dominio de Bezout.*

Demostración. $\Rightarrow$) *Es el Corolario 1.2.82.* $\Leftarrow$) *Es la Proposicion 1.2.85.* ∎

§1.3 Módulos sobre dominios de ideales principales.

Las técnicas del álgebra lineal, son tan exitosas en la matemática, que muchas de éstas se han exportado a otras áreas del universo matemático. En esta sección se muestra el particular caso de la aplicación de las técnicas del álgebra lineal en la Teoría de Módulos.

Definición 1.3.1. *Sea M un R-módulo. Un subconjunto $\{m_i\}_{i\in I}$ de M, es **linealmente independiente** en M si para todo subconjunto finito $\{m_{i_1},\dots,m_{i_k}\}$ de elementos distintos en $\{m_i\}_{i\in I}$ tales que*

$$r_1m_{i_1}+\cdots+r_km_{i_k}=0 \quad con \quad r_1,\dots,r_k\in R \quad se\ tiene\ que \quad r_1=\cdots=r_k=0.$$

*Si el conjunto $\{m_i\}_{i\in I}$ genera a M, se dice que M es un **R-módulo libre** con **base** $\{m_i\}_{i\in I}$.*

Recodemos que para un R-módulo M, si $m\in M$, el R-submódulo generado por m en M esta dado por:

$$\langle m\rangle=\{rm\in M \mid r\in R\}.$$

Lo que inspira la notación Rm para representar al R-submódulo $\langle m\rangle$.

Proposición 1.3.2. *Si M es un R-módulo libre y $\{m_i\}_{i\in I}\subseteq M$. Son equivalente para $\{m_i\}_{i\in I}$*

1) *$\{m_i\}_{i\in I}$ es una base de M.*
2) *Todo elemento $m\in M$ se puede escribir de manera única como*

$$m=r_1m_{i_1}+\cdots+r_nm_{i_n}$$

con $m_{i_j}\in\{m_i\}_{i\in I}$, $r_j\in D$ y $j\in\{1,\dots,n\}$, para algún $n\in\mathbb{N}$.
3) *$M=\bigoplus_{i\in I}Rm_i$.*

Proposición 1.3.3. *Sean M y N R-módulos tal que M es un R-módulo libre con base $\{m_i\}_{i\in I}$. Si $f:M\longrightarrow N$ es un morfismo de R-módulos, entonces,*

1) *f es inyectivo si y sólo si $f\big[\{m_i\}_{i\in I}\big]$ es linealmente independiente en N.*
2) *f es suprayectivo si y sólo si $f\big[\{m_i\}_{i\in I}\big]$ genera a N.*

Teorema 1.3.4. *Sean M y N R-módulos libres con bases X y Y respectivamente. Entonces M es isomorfo a N sí y sólo si $|X|=|Y|$.*

Corolario 1.3.5. *Si M es un R-módulo libre y X y Y son bases de M, entonces $|X|=|Y|$.*

Definición 1.3.6. *Sea M un R-módulo libre. El **rango** de M es la cardinalidad de cualquier base de M. Al rango de un R-módulo libre M lo denotaremos por $ran(M)$.*

Si R es un anillo e I es un conjunto de cardinalidad α. Por cada $i\in I$ tomemos R_i una copia de R y construyamos la suma directa de la familia de R-módulos $\{R_i\}_{i\in I}$ (ver Ejemplo 1.1.27). Claramente $\bigoplus_{i\in I}R_i$ es un R-módulo de rango α. Así una lectura que se puede hacer del Teorema 1.3.4, es la siguiente; dado un anillo R y un cardinal α existe un único módulo libre (salvo isomorfismos) de rango α.

Lema 1.3.7. *Se R un anillo y N un R-submódulo de M. Si M/N es un R-módulo libre, entonces N es un sumando directo de M.*

Demostración. *Como M/N es un R-módulo libre, existe $\{m_i\}_{i\in I}\subseteq M$ tal que $\{\overline{m_i}\}_{i\in I}\subseteq M/N$ es una base de N/M.*

Sea $K = \langle \{m_i\}_{i\in I} \rangle$. A continuación vamos a mostrar que $M = N \bigoplus K$.

Si $m \in M$, al tomar $\overline{m} \in M/N$. Como $\{\overline{m_i}\}_{i\in I} \subseteq M/N$ es una base de N/M, entonces existen $t \in \mathbb{N}$, $r_1, \ldots, r_t \in R$ y $m_{i_1}, \ldots, m_{i_t} \in K$ tales que

$$\overline{m} = \sum_{j=1}^{t} r_j \overline{m_{i_j}}$$

de donde

$$\overline{m - \sum_{j=1}^{t} r_j m_{i_j}} = 0.$$

Entonces $m - \sum_{j=1}^{t} r_j m_{i_j} \in N$ y así $m = n + \sum_{j=1}^{t} r_j m_{i_j}$ para algún $n \in N$. Por lo tanto $M = N + K$.

Sólo falta mostrar que la suma $N + K$ es directa. Consideremos $n \in N \cap K$, entonces existen $t \in \mathbb{N}$, $r_1, \ldots, r_t \in R$ y $m_{i_1}, \ldots, m_{i_t} \in K$ tales que $n = \sum_{j=1}^{t} r_j m_{i_j}$, luego al tomar la clase de equivalencia de n en M/N obtenemos que

$$\overline{0} \underset{n\in N}{=} \overline{n} = \overline{\sum_{j=1}^{t} r_j m_{i_j}} = \sum_{j=1}^{t} r_j \overline{m_{i_j}}.$$

Y dado que el conjunto $\{\overline{m_i}\}_{i\in I} \subseteq M/N$ una base de N/M, concluimos que $r_i = 0$ para todo $i \in \{1, \ldots, t\}$. Por lo tanto $n = 0$ y entonces $N \cap M = \{0\}$. Luego por el Teorema 1.1.36, tenemos que $M = N \bigoplus K$. ∎

Lema 1.3.8. *Sean D un dominio entero e I un ideal principal no nulo de D. Entonces I es isomorfo a D como D-módulo.*

Demostración. *Dado que I es un ideal principal no nulo, existe $d \in I - \{0\}$ tal que $I = dD$. Ahora consideremos la función $\varphi : D \longrightarrow I$ dada por $\varphi(x) = dx$. Como $d(rx + y) = r(dx) + dy$ para todo $x, y, r \in D$, φ es un morfismo de D-módulos. Además como $I = dD$, es claro que φ es sobreyectiva. Que $ker(\varphi) = \{0\}$ es consecuencia inmediata de que D es un dominio entero y entonces de la Proposición 1.1.15 tenemos que f es inyectiva. Por lo tanto φ es un isomorfismo de D módulos.* ∎

Teorema 1.3.9. *Si D es un dominio de ideales principales, entonces todo D-submódulo de un D-módulo libre es libre.*

Demostración. *Sea M un D-módulo libre con base $\{m_i\}_{i\in I}$ y N un D-submódulo de M.*

Por el Teorema de Zermelo[6], podemos tomar I bien ordenado. Entonces es posible considerar I como conjunto de ordinales menores que τ, para algún ordinal τ[7].

Para cada $\beta \in I$ definamos $M_\beta = \bigoplus_{\gamma<\beta} Dm_\gamma$, y consideremos $N_\beta = N \cap M_\beta$. Nótese que

$$N_\beta = N \cap M_\beta = N \cap (M_{\beta+1} \cap M_\beta) = (N \cap M_{\beta+1}) \cap M_\beta = N_{\beta+1} \cap M_\beta$$

Usando este hecho, tenemos que para cada $\beta \in I$

$$N_{\beta+1}/N_\beta = N_{\beta+1}/(N_{\beta+1} \cap M_\beta) \underset{\text{Teo. 1.1.33}}{\cong} (N_{\beta+1} + M_\beta)/M_\beta.$$

Ahora, como $N_{\beta+1} + M_\beta < M_{\beta+1}$, se tiene que

$$N_{\beta+1}/N_\beta \cong (N_{\beta+1} + M_\beta)/M_\beta \underset{\text{Teo. 1.1.35}}{<} M_{\beta+1}/M_\beta \underset{\text{Teo. 1.1.37 (2)}}{\cong} Dm_{\beta+1} \cong D.$$

Es decir $N_{\beta+1}/N_\beta$ es isomorfo a un D-submódulo de D. Y así, por el Lema 1.3.8, tenemos que $N_{\beta+1}/N_\beta \cong 0$ o $N_{\beta+1}/N_\beta$ es isomorfo a D. Si $N_{\beta+1}/N_\beta \cong 0$, entonces $N_\beta = N_{\beta+1}$. En caso contrario $N_{\beta+1}/N_\beta$ es isomorfo a D y como D es un D-módulo libre, por el Lema 1.3.7, $N_{\beta+1} = N_\beta \bigoplus Dn_\beta$

[6] Ernst Friedrich Ferdinand Zermelo (1871–1953) fue el primero en demostrar 1904 que: Todo conjunto admite un buen orden.

[7] Para una demostración ver [*Go*] Teorema 4.1.18.

para algún $n_\beta \in N_{\beta+1}$. Así, para cada $\beta+1 \leqslant \tau$ tal que $N_\beta \neq N_{\beta+1}$ elijamos un $n_\beta \in N$ fijo tal que $N_{\beta+1} = N_\beta \bigoplus Dn_\beta$ y tomemos el conjunto $\Gamma = \{n_\beta \in M - \{0\} \mid N_{\beta+1} = N_\beta \bigoplus Dn_\beta\}$. Es claro por la forma en que fueron elegidos los n_β que Γ es un conjunto linealmente independiente en M. Entonces por la Proposición 1.3.2 se tiene que $\langle\Gamma\rangle = \bigoplus_{n_\beta \in \Gamma} Dn_\beta$.

Como $\Gamma \subseteq N$, del Corolario 1.1.30 tenemos que $\langle\Gamma\rangle \subseteq N$. Ahora, si $n \in N$, existen $d_1, \ldots, d_k \in D - \{0\}$ y $m_{\beta_1}, \ldots, m_{\beta_k} \in \{m_i\}_{i\in I}$ tales que

$$n = r_1 m_{\beta_1} + \cdots + r_k m_{\beta_k}.$$

De hecho, como I es bien ordenado, podemos suponer que $\beta_1 < \cdots < \beta_k$. Entonces pasa que $n \in M_{\beta_k}$ y así $n \in N \cap M_{\beta_k} = N_{\beta_k}$. Ahora veremos que $N_\beta \subseteq \langle\Gamma\rangle$ para todo $\beta \in I$ y como consecuencia obtendremos que $N \subseteq \langle\Gamma\rangle$. Supongamos por el contrario que existe $\beta \in I$ tal que $N_\beta \subsetneq \langle\Gamma\rangle$ y sea β_0 el mínimo ordinal en I con esta propiedad. A continuación veremos que la existencia de tal mínimo es imposible

1) *Si suponemos que β_0 es un ordinal limite, siendo β_0 mínimo, entonces $N_\gamma \subseteq \langle\Gamma\rangle$ si $\gamma < \beta_0$ y del hecho que $N_{\beta_0} = \bigcup_{\gamma<\beta_0} N_\gamma$, se tendría entonces que $N_{\beta_0} \subseteq \langle\Gamma\rangle$. Lo que no es consistente con la elección de β_0.*
2) *Ahora, si suponemos que β_0 es un ordinal sucesor, entonces $N_{\beta_0} = N_{\beta_0-1} + Dn_{\beta_0}$. Como β_0 es mínimo, se tiene que $N_{\beta_0-1} \subseteq \langle\Gamma\rangle$ y dado que $n_{\beta_0} \in \langle\Gamma\rangle$, entonces $N_{\beta_0} \subseteq \langle\Gamma\rangle$, lo que es contradictorio.*

Por lo tanto, $N = \bigoplus_{n_\beta\in\Gamma} Dn_\beta$ y así N es un D-módulo libre con base Γ. ∎

Corolario 1.3.10. *Sean D un dominio de ideales principales y M un D-módulo libre. Si N es un D-submódulo de M, entonces N es un D-módulo libre y $ran(N) \leqslant ran(M)$.*

Lema 1.3.11. *Sean D un dominio de ideales principales, M un D-módulo libre de rango finito y N y K R-submódulos de M tales que $M = N \bigoplus K$. Entonces $ran(M) = ran(N) + ran(K)$.*

Teorema 1.3.12. *Sean D un dominio de ideales principales, M un D-módulo libre de rango finito n y N un D-submódulo no nulo de M. Entonces existe una base $\{m_1, \ldots, m_n\}$ de M, un entero positivo $q \leqslant n$ y elementos no nulos $d_1, \ldots, d_q \in D$ tales que $\{d_1e_1, \ldots, d_qe_q\}$ es una base de N y además d_i divide a d_{i+1} para $1 \leqslant i \leqslant q-1$.*

Demostración. *Antes de comenzar propiamente la demostración del enunciado, se realizará una construcción, que si bien es complicada, remunerará al momento de hacer la demostración del teorema.*

Sea $Hom(M,D)$ el D-módulo de homomorfismos de los D-módulos de M en D. Si $\varphi \in Hom(M,D)$, entonces $\varphi[N]$ es un D-submódulo de D y por lo tanto un ideal de D. Siendo que D es un dominio de ideales principales, tenemos entonces que para cada $\varphi \in Hom(M,D)$, existe $d_\varphi \in D$ tal que $\varphi[N] = d_\varphi D$.

Como D es un dominio de ideales principales, entonces D es noetheriano y así por el Teorema 1.2.26 existe $\gamma \in Hom(M,D)$ tal que $d_\gamma D$ es un ideal maximal en el conjunto

$$\{Dd_\varphi \mid d_\varphi D = \varphi[N] \ \ con \ \ \varphi \in Hom(M,D)\}. \tag{3.1}$$

Siendo que M es un D-módulo libre de rango finito n, existe $\{m_1, \ldots m_n\} \subseteq M$ una base de M. Para cada $i \in \{1, \ldots, n\}$, consideremos $\pi_i : M \longrightarrow D$ el morfismo de D-módulos que extiende por linealidad a la función $f_i : \{m_1, \ldots m_n\} \longrightarrow D$ dada por $f_i(m_j) = \begin{cases} 0 & si\ i\neq j \\ 1 & si\ i=j \end{cases}$.

Como $\{m_1, \ldots m_n\}$ es una base de M, entonces todo elemento $m \in M$ se puede escribir de manera única como $r_1m_1 + \ldots + r_mm_n$ con $r_i \in D$ para $i = 1, \ldots, n$, es entonces claro que dados $m, l \in M$

se tiene que

$$m = l \quad \text{si y sólo si} \quad \pi_i(m) = \pi_i(l) \quad \text{para todo} \quad i \in \{1, \ldots, n\}. \tag{3.2}$$

$$\text{En particular} \quad m = 0 \quad \text{si y sólo si} \quad \pi(m) = 0 \quad \text{para todo } i \in \{1, \ldots, n\}. \tag{3.3}$$

Por hipótesis $N \neq \{0\}$ y como consecuencia de (3.3) existe $i \in \{1, \ldots, n\}$ tal que $\pi_i[N] \neq \{0\}$. Luego, por el carácter maximal de d_γ tenemos que $\gamma(N) \neq (0)$ y así podemos concluir que $d_\gamma \neq 0$.

Consideremos $e' \in N$ tal que $\gamma(e') = d_\gamma$. Ahora se va a demostrar que para todo $\varphi \in Hom(M, D)$, d_γ divide a $\varphi(e')$.

Tomemos entonces $\varphi \in Hom(M, D)$. Si $e' \in ker(\varphi)$, se tiene que $\varphi(e') = 0$ y así trivialmente d_γ divide a $\varphi(e')$. Supongamos entonces $\varphi(e') \neq 0$. Como D es un dominio de ideales principales, existe $d \in D - \{0\}$ un máximo común divisor de d_γ y de $\varphi(e')$[8], más aún por el Corolario 1.2.82 existen $a, b \in D$ tales que $ad_\gamma + b\varphi(e') = d$, y como $d_\gamma = \gamma(e')$, tenemos que

$$(a\gamma + b\varphi)(e') = a\gamma(e') + b\varphi(e') = d. \tag{3.4}$$

Donde $a\gamma + b\varphi \in Hom(M, D)$.

Siendo que $d \mid d_\gamma$, por la Proposición 1.2.29 pasa que $d_\gamma D \subseteq dD$. Además se tiene que $d \in (a\gamma + b\varphi)[N]$ y entonces $dD \subseteq (a\gamma + b\varphi)[N]$. Dado el carácter maximal de $d_\gamma D$, tenemos que $d_\gamma D = (a\gamma + b\varphi)[N]$ y en consecuencia $d_\gamma D = dD$. Luego por la Proposición 1.2.30, se tiene que d_γ y d son asociados en D y como consecuencia de que $d \mid \varphi(e')$ podemos concluir que d_γ divide a $\varphi(e')$.

En particular tenemos que d_γ divide a $\pi_i(e')$ para cada $i \in \{1, \ldots, n\}$. Entonces existen $b_1, \ldots, b_n \in D$ tales que $\pi_i(e') = d_\gamma b_i$.

Tomemos

$$e = \sum_{i=1}^{n} b_i m_i. \tag{3.5}$$

Multiplicando la igualdad dada en (3.5) por d_γ, obtenemos que

$$d_\gamma e = d_\gamma \sum_{i=1}^{n} b_i m_i = \sum_{i=1}^{n} d_\gamma b_i m_i = \sum_{i=1}^{n} \pi_i(e') m_i. \tag{3.6}$$

Luego, si aplicamos π_j a (3.6), se tiene que $\pi_j(d_\gamma e) = \pi_j(e')$ para todo $j \in \{1, \ldots, n\}$. Entonces de (3.2), tenemos que $e' = d_\gamma e$. Además se tiene que

$$d_\gamma = \gamma(e') = \gamma(d_\gamma e) = d_\gamma \gamma(e).$$

Y dado que $d_\gamma \neq 0$ y D es un dominio entero, entonces $\gamma(e) = 1$.

Ahora demostraremos que

1) *$M = De \bigoplus ker(\gamma)$.*
2) *$N = De' \bigoplus (N \cap ker(\gamma))$.*

Demostraciones:

1) *Si $y \in M$. Podemos escribir*

$$y = \gamma(y)e + (y - \gamma(y)e), \tag{3.7}$$

donde claramente, $\gamma(y)e \in De$ y $y - \gamma(y)e \in ker(\gamma)$. Ahora, supongamos que

$$y = ze + w, \tag{3.8}$$

con $z \in D$ y $w \in ker(\gamma)$. Aplicando γ a (3.8), se tiene que

$$\gamma(y) = \gamma(ze) = z\gamma(e) = z,$$

[8] Por el Teorema 1.2.68 D es un dominio de factorización única, luego por la Proposición 1.2.72 D tiene la propiedad del *MCD*.

de donde $w = y - \gamma(y)e$. Así la representación dada en (3.7) es única. Por lo tanto $M = De \bigoplus ker(\gamma)$.

2) *Sea $y \in N$. Siendo que $\gamma(y) \in Dd_\gamma$, entonces existe $b \in D$ tal que $\gamma(y) = bd_\gamma$. Luego y se puede escribir de la forma*

$$y = bd_\gamma e + (y - bd_\gamma e) \underset{e'=d_\gamma e}{=} be' + (y - be'),$$

donde es obvio que $be' \in De'$ y que $y - be' \in N$. Además, si aplicamos γ a $y - be'$, obtenemos que

$$\gamma(y - be') = \gamma(y) - \gamma(be') = \gamma(y) - b\gamma(e') = \gamma(y) - bd_\gamma = 0.$$

Entonces $y - be' \in (N \cap ker(\gamma))$.

Ahora notemos que $De' \subseteq De$ y $N \cap ker(\gamma) \subseteq ker(\gamma)$, entonces de la Proposición 1.1.37 inciso (1) se tiene que $N = De' \bigoplus (N \cap ker(\gamma))$.

Ahora se demostrará por inducción sobre el rango de M, la aserción del teorema.

La base es precisamente el Lema 1.3.8.

Supongamos que la afirmación es válida para todo D-módulo de rango n y sea M un D-módulo de rango $n+1$. Por la construcción hecha anteriormente, existen $e, e' \in M - \{0\}$, $\gamma \in Hom(M, D)$ y $d_\gamma \in D$ tales que

$$M = De \bigoplus ker(\gamma), \;\; N = De' \bigoplus (N \cap ker(\gamma)) \;\; y \;\; e = de'.$$

Por el Lema 1.3.11 $ran(ker(\gamma)) = n$, pues claramente $ran(De) = 1$. Entonces por hipótesis de inducción en los D-submódulos $N \cap ker(\gamma)$ y $ker(\gamma)$, existe una base $(e_2, \ldots, e_{n+1})$ de $ker(\gamma)$ y elementos $d_2, \ldots, d_q \in D$ tales que $(d_2e_2, \ldots, d_qe_q)$ es una base de $N \cap ker(\gamma)$ y tales que d_i divide a d_{i+1} para $2 \leqslant i \leqslant q-1$.

Siendo que $M = De \bigoplus ker(\gamma)$ y que $N = De' \bigoplus (N \cap ker(\gamma))$. De la Proposición 1.3.2 concluimos que $\{e, e_2 \ldots, e_n\}$ es una base M y que $\{d_\gamma e = e', d_2e_2 \ldots, d_qe_q\}$ es una base de N.

Solo falta demostrar que $d_\gamma \mid d_2$. Sea $\eta : M \longrightarrow D$ el morfismo extendido por linealidad al definir por $\eta(e_1) = \eta(e_2) = 1$ y $\eta(e_i) = 0$ para $i \in \{3, \ldots, n\}$. Dado que

$$d_\gamma = d_\gamma \cdot 1 = d_\gamma \eta(e_1) = \eta(d_\gamma e_1) = \eta(e') \in \eta(N),$$

entonces $d_\gamma D \subseteq \eta[N]$. Dado que $d_\gamma D$ es un ideal maximal en el conjunto definido en (3.1), entonces $d_\gamma D = \eta[N]$. Ahora, como $d_2e_2 \in N$ y $d_2 = d_2\eta(e_2) = \eta(d_2e_2)$, tenemos que $d_2 \in d_\gamma D$. Por lo tanto $d_\gamma \mid d_2$, con lo que concluimos la demostración. ∎

Corolario 1.3.13. *Sea H un subgrupo de un grupo abeliano libre G de rango finito n. Entonces existe una base $\{g_1, \ldots, g_n\}$ de G y enteros positivos $r_1, \ldots, r_q$ con $q \leqslant n$ tales que $\{r_1g_1, \ldots, r_qg_q\}$ es una base de H y r_i divide a r_{i+1} para $1 \leqslant i \leqslant q-1$.*

Corolario 1.3.14. *Sea G un grupo abeliano finito. Entonces G es isomorfo a un producto de la forma $(\mathbb{Z}/d_1\mathbb{Z}) \times \cdots (\mathbb{Z}/d_n\mathbb{Z})$ donde $d_1, \ldots, d_n \in \mathbb{Z}^+$ y $d_i \mid d_{i+1}$ para todo $i = 1, \ldots, n-1$.*

Corolario 1.3.15. *Sea G un grupo abeliano finito. Entonces existe $z \in G$ cuyo orden n es tal $y^n = 1$ para todo $y \in G$. (Ver el Corolario 1.3.14)*

Proposición 1.3.16. *Sea H un subgrupo de un grupo abeliano libre G de rango n. Entonces G/H es finito si y sólo si $ran(H) = ran(G)$.*

Demostración.

⇒) *Supongamos que G/H es finito y sea s el rango de H. Por el Teorema 1.3.12 existe $\{g_1, \ldots, g_n\}$ base de G y $r_1, \ldots, r_s \in \mathbb{Z} - \{0\}$ con $s \leqslant n$ tales que $\{r_1g_1, \ldots, r_sg_s\}$ es una base de H.*

Ahora, por la Proposición 1.3.2, $G = \bigoplus_{i=1}^{n} \mathbb{Z}g_i$ *y* $H = \bigoplus_{i=1}^{s} \mathbb{Z}(m_i g_i)$*, y entonces*

$$G/H = \bigoplus_{i=1}^{n} \mathbb{Z}g_i / \bigoplus_{i=1}^{s} \mathbb{Z}(r_i g_i) \underset{\text{Teo. 1.1.37 (2)}}{\cong} \bigoplus_{i=1}^{s} (\mathbb{Z}g_i/\mathbb{Z}(r_i g_i)) \bigoplus \left(\bigoplus_{i=s+1}^{n} g_i\mathbb{Z} \right).$$

Luego si sucediera que $s < n$*, entonces* G/H *tendría al menos un sumando directo isomorfo a* $\mathbb{Z}$ *lo que contradice el hecho de que* G/H *es finito. Por lo tanto* $s = n$*.*

$\Leftarrow$) *Supongamos que* $ran(H) = ran(G) = n$*. Por el Teorema 1.3.12 existen* $\{g_1, \ldots, g_n\}$ *base de* G*, y elementos no nulos* $r_1, \ldots, r_n \in \mathbb{Z}$ *tales que* $\{r_1 g_1, \ldots, r_n g_n\}$ *es una base de* H*. De la Proposición 1.3.2 se tiene que* $G = \bigoplus_{i=1}^{n} \mathbb{Z}g_i$ *y que* $H = \bigoplus_{i=1}^{n} \mathbb{Z}(r_i g_i)$*, entonces*

$$G/H = \bigoplus_{i=1}^{n} \mathbb{Z}g_i / \bigoplus_{i=1}^{n} \mathbb{Z}(m_i g_i) \underset{\text{Teo. 1.1.37 (2)}}{\cong} \bigoplus_{i=1}^{n} (\mathbb{Z}g_i/\mathbb{Z}(m_i g_i)) \cong \bigoplus_{i=1}^{n} \mathbb{Z}_{m_i}$$

De donde es claro que G/H *es un módulo finito.* ∎

Corolario 1.3.17. *Sea* H *un subgrupo de un grupo abeliano libre* G *de rango finito, tal que* $ran(H) = ran(G)$*. Si* $\{h_1, \ldots, h_n\}$ *y* $\{g_1, \ldots, g_n\}$ *son bases de* H *y* G *respectivamente, tales que* $h_i = r_i g_i$ *con* $r_i \in \mathbb{Z} - \{0\}$ *para cada* $i \in \{1, \ldots, n\}$*, entonces* $|G/H| = \prod_{i=1}^{n} |r_i|$*.*

Observación 1. 3.18. Si D es un dominio de ideales principales, M un D-módulo de rango finito n con $\{m_1, \ldots, m_n\}$ y $\{m'_1, \ldots, m'_n\}$ bases de M, entonces existen $r_{ij}, s_{ij} \in D$ tales que

$$m_i = \sum_{j=0}^{n} r_{ij} m'_i \quad y \quad m'_i = \sum_{j=0}^{n} s_{ij} m_i.$$

Entonces podemos considerar los arreglos $V = (m_1, \ldots, m_n)$, $W = (m'_1, \ldots, m'_n)$ y las matrices $A = (r_{ij})$ y $B = (s_{ij})$ tales que $V^t = A(W)^t$ y que $(W)^t = BV$ (donde V^t y $(W)t$ son los vectores transpuestos de V y W respectivamente). Podemos concluir entonces que $V^t = ABV^t$, y si $AB = (c_{ij})$ donde $c_{ij} \in D$, se tiene que

$$m_i = \sum_{j=0}^{n} c_{ij} m_i.$$

Y como $\{m_1, \ldots, m_n\}$ es una base de M, de la Proposición 1.3.2 pasa que $c_{ij} = \begin{cases} 0 & si\ i \neq j \\ 1 & si\ i = j \end{cases}$, es decir AB es la matriz identidad en el conjunto de matrices de $n \times n$ con coeficientes en D. Por lo tanto $det(AB) = det(A) \cdot det(B) = 1$ y es entonces que $det(A), det(B) \in U(D)$.

Definición 1.3.19. *Sea* R *un anillo y* $M_n(R)$ *el conjunto de matrices de* $n \times n$ *con coeficientes en* R*. Una matriz* $A \in M_n(R)$ *se dice* ***unimodular*** *si* $det(A) \in U(D)$*.*

Observación 1. 3.20. En el caso de que $R = \mathbb{Z}$, las matrices unimodulares son aquellas cuyo determinante sea ± 1.

Teorema 1.3.21. *Sean* D *un dominio de ideales principales y* M *un* D*-módulo libre de rango finito* n *y una base* $\{m_1, \ldots, m_n\}$ *de* M*. Supongamos que* $(a_{ij}) \in M_n(D)$*, entonces los elementos*

$$m'_i = \sum_{j=1}^{n} a_{ij} m_j$$

en D *forman una base de* M *si y sólo si* (a_{ij}) *es una matriz unimodular.*

Demostración.

$\Rightarrow$) *Es la Observación 1.3.18.*

⇐) *Supongamos que (a_{ij}) es una matriz unimodular. Como $det((a_{ij})) \in U(D)$, entonces $(det((a_{ij})))^{-1} \in D$. Del álgebra lineal sabemos que $A^{-1} = (det(A))^{-1}\widetilde{A}$ donde $\widetilde{A}$ es la matriz adjunta de A. Dado que $\widetilde{A} \in M_n(D)$, entonces podemos concluir que $A^{-1} \in M_n(D)$. Denotemos $A^{-1} = (b_{ij})$ con $b_{ij} \in D$.*

Como

$$\begin{pmatrix} m'_1 \\ \vdots \\ m'_n \end{pmatrix} = (a_{ij}) \begin{pmatrix} m_1 \\ \vdots \\ m_n \end{pmatrix} \tag{3.9}$$

aplicando la matriz inversa de (a_{ij}) por la izquierda a (3.9), obtenemos que

$$(b_{ij}) \begin{pmatrix} m'_1 \\ \vdots \\ m'_n \end{pmatrix} = \begin{pmatrix} m_1 \\ \vdots \\ m_n \end{pmatrix}.$$

Lo que se tiene, es que para cada $i \in \{1, \ldots, n\}$ es posible escribir $m_i = \sum_{j=1}^{n} b_{ij} m'_j$ con $b_{ij} \in D$, es decir $\{m_1, \ldots, m_n\} \subseteq \langle\{m'_1, \ldots, m'_n\}\rangle$. Luego por el Corolario 1.1.30 inciso (1), concluimos que $M = \langle\{m'_1, \ldots, m'_n\}\rangle$.

Ahora supongamos que

$$r_1 m'_1 + \cdots + r_n m'_n = 0 \quad con \quad r_i \in D. \tag{3.10}$$

Como $m'_i = \sum_{j=1}^{n} a_{ij} m_j$, la igualdad planteada en (3.10) induce el sistema de ecuaciones

$$\begin{array}{ccccccc} r_1 a_{11} & + & \cdots & + & r_n a_{n1} & = & 0 \\ \vdots & & \vdots & \vdots & & \vdots & \vdots \\ r_1 a_{1n} & + & \cdots & + & r_n a_{nn} & = & 0. \end{array} \tag{3.11}$$

Ahora, suponemos que (a_{ij}) es una matriz unimodular y entonces $det((a_{ij})) \neq 0$. Una vez más recurriendo al algebra lineal obtenemos que la única solución al sistema lineal homogéneo dado en (3.11) es la trivial. Por lo tanto $r_i = 0$ para cada $i \in \{1, \ldots, n\}$. Y entonces $\{m'_1, \ldots, m'_n\}$ es una base de M. ∎

Proposición 1.3.22. *Sea H un subgrupo de un grupo abeliano libre G de rango finito tal que $ran(H) = ran(G)$ y sean $\{h_1, \ldots, h_n\}$ y $\{g_1, \ldots, g_n\}$ bases de H y G respectivamente, tales que $h_i = \sum_{j=1}^{n} a_{ij} g_j$. Entonces*

$$| G/H | = | det(a_{ij}) | .$$

Demostración. *Por el Teorema 1.3.12, existe $\{u_1, \ldots, u_n\}$ una base de G y $r_1, \ldots, r_n \in \mathbb{Z} - \{0\}$ tales que $\{v_1, \ldots, v_n\}$ es una base de H y $v_i = r_i u_i$ para cada $i \in \{1, \ldots, n\}$.*

Ahora, siendo que $\{g_1, \ldots, g_n\}$ es una base de G, se tiene que

$$u_j = \sum_{i=1}^{n} b_{ij} g_i \ \ con \ \ b_{ij} \in \mathbb{Z} \ \ para \ \ cada \ \ i \in \{1, \ldots, n\}.$$

Y como $\{u_1, \ldots, u_n\}$ es una base de G, por Teorema 1.3.21 se tiene que $B = (b_{ij})$ es una matriz unimodular.

De igual manera, como $\{v_1, \ldots, v_n\}$ es una bases de H, entonces

$$h_j = \sum_{i=1}^{n} d_{ij} v_i \ \ con \ \ d_{ij} \in \mathbb{Z}.$$

Y además $D = (d_{ij})$ es una matriz unimodular.

Si hacemos $c_{ii} = m_i$ y $c_{ij} = 0$ si $i \neq j$, entonces tenemos

$$v_j = \sum_{i=1}^{n} c_{ij} u_i,$$

Y así tomando $C = (c_{ij})$, tenemos que $h_i = (DCB)\begin{pmatrix} g_1 \\ \vdots \\ g_n \end{pmatrix}$. Como la expresión de h_i como combinación D-lineal de los elementos de la base $\{g_1, \ldots, g_n\}$ es única (Teorema 1.1.36) podemos concluir que $(a_{ij}) = DCB$. De donde se tiene que

$$|det((a_{ij}))| = |det(DCB)| = |det(D)det(C)det(B)| \underset{B \text{ y } D \text{ son Unimodulares}}{=} |det(C)| = \prod_{i=1}^{n} r_i \underset{Cor.\ 1.3.17}{=} |G/H| .$$ ∎

§1.4 Resultados de campos.

Para cerrar este capítulo se presentarán algunos resultados de la teoría de campos que en su momento serán de invaluable importancia para el desarrollo del trabajo.

Definición 1.4.1. *Sean F y E campos. Se dice que E es una **extensión** de F, si F es un subcampo de E .*

*Si E es una extensión de un campo F lo que denotaremos por E/F, entonces E es un F espacio vectorial. A la dimensión de F sobre E se le denota por $[E : F]$ y se llama el **grado de extensión** de E sobre F. Una extensión E de un campo F es una **extensión finita**, si $[E : F]$ es finito.*

Proposición 1.4.2. *Sean E K y F, campos tales que $F \subseteq K \subseteq E$. Entonces*

1) *$[E : F] = [E : K][K : F]$.*
2) *$[E : F]$ es finito si y sólo si $[K : F]$ y $[E : K]$ son finitos.*

Proposición 1.4.3. *Si R es un subanillo de un anillo S y $\alpha \in S$, existe un único morfismo de anillos $ev_\alpha : R[x] \longrightarrow S$ tal que $ev_\alpha(x) = \alpha$ y $ev_\alpha(r) = r$ para todo $r \in R$.*

En adelante si tenemos que R es un subanillo de un anillo S, $\alpha \in S$ y el morfismo $ev_\alpha : R[x] \longrightarrow S$, llamado el morfismo evaluación, para cada $f(x) \in R[x]$, denotaremos la imagen de $f(x)$ bajo ev_α simplemente por $f(\alpha)$ y a la imagen del morfismo ev_α en S se denotará por $S[\alpha]$.

Definición 1.4.4. *Sea E es una extensión de un campo F.*

1) *Si $f(x) \in F[x]$. $\alpha \in E$ es una **raíz** de $f(x)$ si $f(\alpha) = 0$.*
2) *$\alpha \in E$ es un **elemento algebraico** sobre F, si existe $f(x) \in F[x]$ tal que α es una raíz de $f(x)$.*
3) *Una extensión E/F es **algebraica** si todo elemento de E es algebraico sobre F.*

Proposición 1.4.5. *Sea E una extensión del campo F, $\alpha \in E$ y $ev_\alpha : F[x] \longrightarrow E$. Entonces α es algebraico sobre F si y sólo si $ker(ev_\alpha) \neq \{0\}$.*

Definición 1. 4.6. *Sea R un anillo y $f(x) \in R[x] - \{0\}$ tal que $f(x) = \sum_{i=0}^{n} a_i x^i$ con $n = grad(f(x))$. $f(x)$ se dice un **polinomio mónico** si $a_n = 1$.*

Proposición 1. 4.7. *Consideremos E una extensión del campo F, $\alpha \in E$ algebraico sobre F y $ev_\alpha : F[x] \longrightarrow E$. Entonces existe un polinomio irreducible y mónico $f(x) \in F[x]$ tal que $ker(ev_\alpha) = f(x)F[x]$.*

Proposición 1. 4.8. *Si $f(x), g(x) \in F[x]$ son polinomios mónicos irreducibles tales que $f(x)F[x] = g(x)F[x]$, entonces $f(x) = g(x)$.*

Definición 1.4.9. *Sea E una extensión del campo F, $\alpha \in E$ algebraico sobre F y $ev_\alpha : F[x] \longrightarrow E$. Al único polinomio mónico $f(x)$ en $F[x]$ que tiene la propiedad de que $ker(ev_\alpha) = f(x)F[x]$ se llama el **polinomio mínimo** de α sobre F y se denotará por $f_\alpha(x)$.*

*Recordemos que si F es campo entonces $F[x]$ es un dominio de ideales principales, luego entonces es posible usar el lenguaje y la teoría de la Sección 2 de este capítulo para el desarrollo de esta sección. Así, diremos que un **polinomio es irreducible** en $F[x]$ si es un elemento irreducible en el anillo $F[x]$, lo que significa que no se puede escribir como el prosuctor de dos polinomios de grado menor al grado de $f(x)$.*

Proposición 1.4.10. *Sea E/F una extensión, $f(x) \in F[x]$ y $\alpha \in E$. Entonces α es una raíz de $f(x)$ si y sólo si $x - \alpha$ divide a $f(x)$ en $E[x]$.*

Corolario 1.4.11. *Sea F un campo y $f(x) \in F[x]$ tal que $grad(f(x)) > 1$. Si $f(x)$ es irreducible en $F[x]$ entonces $f(x)$ no tiene raíces en F.*

Ejemplo 1.4.12. Consideremos el polinomio $f(x) = x^4+2x^2+1 \in \mathbb{R}[x]$, se tiene que $x^4+2x^2+1 = (x^2+1)^2$. Claramente las raíces de $f(x)$ son i y $-i$ que no pertenecen a $\mathbb{R}$ sin embargo el polinomio $x^4 + 2x^2 + 1$ no es irreducible.

Un morfismo de campos es un morfismo de anillos enter dos campos.

Lema 1.4.13. *Los homomorfismo de campos son inyectivos.*

Teorema 1.4.14. *Sea F un campo y $f(x) = \sum_{i=0}^{n} a_i x^i \in F[x]$ un polinomio irreducible. Entonces, existe una extensión de campo de F donde $f(x)$ tiene una raíz.*

Demostración. *Siendo $F[x]$ un dominio de ideales principales y $f(x)$ irreducible en $F[x]$. Por el Teorema 1.2.36 inciso (1), $f(x)F[x]$ es un ideal maximal en F[x], luego por la Proposición 1.1.20 $E = F[x]/f(x)F[x]$ es un campo.*

Ahora, si $\pi : F[x] \longrightarrow E$ es la proyección canónica, notemos que $\pi\mid_F$ es un morfismo de campos. Entonces por el Lema 1.4.13, $\pi\mid_F$ es inyectivo, de donde se tiene que F es isomorfo a $\pi[F]$. Ahora si identificamos los elementos de F con sus respectivas imágenes en $\pi[F]$, podemos ver a E como una extensión de F.

Luego para Para $\overline{x} \in E$ se tiene que

$$f(\overline{x}) = \sum_{i=0}^{n} a_i \overline{x^i} = \overline{\sum_{i=0}^{n} a_i x^i} = \overline{0}.$$

Y así $\overline{x} \in E$ es una raíz de $f(x)$. ∎

Corolario 1.4.15. *Sean F un campo y $f(x) \in F[x]$ un polinomio irreducible. Entonces, existe una extensión E de F donde $f(x)$ se puede descomponer como producto de irreducibles de grado 1 en $E[x]$.*

Corolario 1.4.16. *Sea F un campo y $f(x) \in F[x]$. Entonces existe una extensión E de F donde $f(x)$ se puede descomponer como producto de irreducibles de grado 1 en $E[x]$.*

Corolario 1.4.17. *Sea F un campo y $f_1(x), \ldots, f_n(x) \in F[x]$. Entonces existe una extensión E de F que contiene a las raíces del conjunto de polinomios $\{f_1(x), \ldots, f_n(x)\}$.*

Proposición 1.4.18. *Sea E un campo y $\{F_i\}_{i\in I}$ una familia de subcampos de E. Entonces $F = \bigcap_{i\in I} F_i$ es un subcampo de E.*

Definición 1.4.19. *Sea E una extensión de un campo F y $\alpha_1, \ldots, \alpha_n \in E$. Consideremos*

$$\Gamma = \{K \subseteq E \mid F \cup \{\alpha_1, \ldots, \alpha_n\} \subseteq K \quad y \quad K \quad es\ subcampo\ de \quad E\}$$

y tomemos

$$F(\alpha_1, \ldots, \alpha_n) = \bigcap_{K\in\Gamma} K.$$

Nótese que por definición $F(\alpha_1, \ldots, \alpha_n)$ el menor subcampo de E (en el sentido de la contención) que contiene a $F \cup \{\alpha_1, \ldots, \alpha_n\}$.

Definición 1.4.20. *Una extensión E de un campo F es **simple** si existe $\alpha \in E$ tal que $E = F(\alpha)$.*

Proposición 1.4.21. *Sea E una extensión de un campo F y $\alpha \in E$. Entonces,*

1) *Si $\alpha \in E$ es algebraico sobre F, entonces $F(\alpha) = F[\alpha]$.*
2) *Si $\alpha \in E$ no es algebraico sobre F, entonces $F(\alpha)$ es el campo de cocientes del anillo $F[\alpha]$.*

Proposición 1.4.22. *Sea E una extensión de un campo F y $\alpha \in E$ algebraico sobre F tal que $f_\alpha(x) = a_0 + a_1x + \cdots + x^n \in F[x]$. Entonces $\{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$ es una base de $F(\alpha)$ sobre F como espacio vectorial.*

Corolario 1.4.23. *Sea E una extensión de un campo F y $\alpha \in E$ algebraico sobre F tal que $f_\alpha(x) = a_0 + a_1x + \cdots + x^n \in F[x]$. Entonces $[F(\alpha) : F] = grad(f_\alpha(x))$.*

Corolario 1.4.24. *Sea E una extensión de un campo F y $\alpha \in E$ algebraico sobre F. Si $\beta \in F(\alpha)$ entonces $grad(f_\beta(x)) \leqslant [F(\alpha) : F]$.*

Proposición 1.4.25. *Sea E una extensión de campos de F y $\alpha \in E$. Entonces α es algebraico sobre F si y sólo si $[F(\alpha) : F]$ es finito.*

Corolario 1.4.26. *Si E es un extensión de un campo F y $\alpha_1, \ldots, \alpha_n \in E$. Entonces $\alpha_1, \ldots, \alpha_n$ son algebraicos sobre F si y sólo si $[F(\alpha_1, \ldots, \alpha_n) : F]$ es finito.*

Corolario 1.4.27. *Si E es un extensión de un campo F y $\alpha_1, \alpha_2 \in E$ algebraicos sobre F, entonces $\alpha_1 + \alpha_2$ y $\alpha_1 \cdot \alpha_2$ son algebraicos sobre F.*

Definición 1.4.28. *Un campo F es **algebraicamente cerrado** si todo polinomio $f(x) \in F[x]$ tiene un cero en F, es decir F es algebraicamente cerrado si todo polinomio se descompone como producto de polinomios lineales en $F[x]$. Una extensión E de F es una **cerradura algebraica** de F, si E es una extensión algebraica de F que es algebraicamente cerrada.*

Las demostraciones de los Teoremas 1.4.29 y 1.4.30 se pueden encontrar en [Mc] Pág. 21.

Teorema 1.4.29. *Si F es un campo, entonces existe una extensión E de F que es una cerradura algebraica de F.*

Teorema 1.4.30. *Si F es un campo, dos cerraduras algebraicas de F son isomorfas.*

En virtud de los Teoremas 1.4.29 y 1.4.30 si F es un campo a la cerradura algebraica de F la denotaremos por $\overline{F}$.

Definición 1.4.31. *Sea F un campo y $f(x) \in F[x]$. Por el Corolario 1.4.16 existe una extensión K de F, donde $f(x)$ tiene todas sus raíces. Si $\alpha_1, \ldots, \alpha_n$ son las distintas raíces de $f(x)$ en K. El campo*

subcampo de K, dado por

$$E = F(\alpha_1, \ldots, \alpha_n)$$

es llamado un ***campo de descomposición de $f(x)$.***

Ejemplo 1.4.32. Consideremos el polinomio $x^p - 1 \in \mathbb{Q}[x]$ donde p es un número primo y $\xi \neq 1$ una raíz de $x^p - 1$, entonces $\mathbb{Q}(\xi)$ es un campo de descomposición del polinomio $x^p - 1$.

A continuación se presentan una serie de resultados sobre homomorfismos de campos.

Proposición 1.4.33. *Sea $\eta : F \longrightarrow K$ un isomorfismo de campos. Entonces existe un único isomorfismo de anillos $\widetilde{\eta} : F[x] \longrightarrow K[x]$ tal que $\widetilde{\eta}\,|_F = \eta$ y $\widetilde{\eta}(x) = x$.*

Proposición 1.4.34. *Sea $\eta : F \longrightarrow K$ un isomorfismo de campos, $\widetilde{\eta}$ el isomorfismo de anillos entre $F[x]$ y $K[x]$ inducido por η y $f(x) \in F[x]$. Entonces $\alpha \in F$ es una raíz de $f(x)$ si y sólo si $\widetilde{\eta}(\alpha) \in K$ es una raíz de $\widetilde{\eta}(f(x))$.*

Proposición 1.4.35. *Sea $\eta : F \longrightarrow K$ un isomorfismo de campos, $\widetilde{\eta}$ el isomorfismo de anillos entre $F[x]$ y $K[x]$ inducido por η y $f(x) \in F[x]$. Entonces $f(x)$ es irreducible en $F[x]$ si y sólo si $\widetilde{\eta}(f(x))$ es irreducible sobre $K[x]$.*

Definición 1.4.36. *Sean R' y S' anillos, R y S subanillos de R' y S' respectivamente y $\eta : R \longrightarrow S$ un morfismo de anillos. Un morfismo de anillos $\eta' : R' \longrightarrow S'$ es una* ***extensión del morfismo*** *η si $\eta'(r) = \eta(r)$ para todo $r \in R$.*

Lema 1.4.37. *Sean $\eta : F \longrightarrow K$ un isomorfismo de los campos y E y L extensiones de campos F y K respectivamente. Supongamos que $\alpha \in E$ es algebraico sobre F con polinomio mínimo $f_\alpha(x)$ y sea $\widetilde{\eta}$ el correspondiente isomorfismo de $F[x]$ en $K[x]$ que extiende a η. Entonces:*

1) *η se puede extender a un morfismo $\zeta : F(\alpha) \longrightarrow L$ si y sólo si $\widetilde{\eta}(f(x)) \in K[x]$ tiene una raíz en L.*
2) *Si η puede extenderse al menos a un homomorfismo de $F(\alpha)$ en L, entonces el número de extensiones distintas es igual al número de raíces distintas de $\widetilde{\eta}(f(x))$ en L.*

Demostración.

1) $\Rightarrow$) *Sea $f_\alpha(x) = \sum_{i=0}^{n} a_i x^i$ y supongamos que $\zeta : F(\alpha) \longrightarrow L$ es un morfismo que extiende a η. Por el Lema 1.4.13 tenemos que $\zeta : F(\alpha) \longrightarrow \zeta[F(\alpha)]$ es un isomorfismo de campos, luego por la Proposición 1.4.33 ζ se puede extender un isomorfismo $\widetilde{\zeta} : F(\alpha)[x] \longrightarrow \zeta[F(\alpha)][x]$ tal que $\widetilde{\zeta}\,|_{F(\alpha)} = \zeta$ y entonces por la Proposición 1.4.34 $\zeta(\alpha)$ es una raíz de $\widetilde{\zeta}(f_\alpha(x))$. Por último notemos que*

$$\widetilde{\zeta}(f_\alpha(x)) = \widetilde{\zeta}\Big(\sum_{i=0}^{n} a_i x^i\Big) = \sum_{i=0}^{n} \widetilde{\zeta}(a_i) x^i \underset{\widetilde{\zeta}|_{F(\alpha)} = \zeta}{=} \sum_{i=0}^{n} \zeta(a_i) x^i \underset{\text{extiende a } \eta}{\underset{\zeta}{=}} \sum_{i=0}^{n} \eta(a_i) x^i = \widetilde{\eta}(f_\alpha(x)).$$

   Por lo tanto $\zeta(\alpha)$ es una raíz de $\widetilde{\eta}(f_\alpha(x))$.

   $\Leftarrow$) *Supongamos que $\widetilde{\alpha} \in L$ es una raíz de $\widetilde{\eta}(f_\alpha(x))$. Como $f_\alpha(x)$ es el polinomio mínimo de α, de la Proposición 1.4.7 tenemos que $f_\alpha(x)$ es irreducible en $F[x]$. Luego, por la Proposición 1.4.35 $\widetilde{\eta}(f_\alpha(x))$ es irreducible en $K[x]$, de donde podemos concluir que $\widetilde{\eta}(f_\alpha(x))$ es el polinomio mínimo de $\widetilde{\alpha}$ sobre K.*
   Luego entonces tenemos que

$$\xi : K[x]/\widetilde{\eta}(f_\alpha(x))K[x] \longrightarrow K(\widetilde{\alpha}) \quad \text{dado por} \quad \xi\left(\overline{\textstyle\sum_{i=0}^{n} a_i x^i}\right) = \textstyle\sum_{i=0}^{n} a_i \widetilde{\alpha}^i.$$

   y que

$$\theta : F(\alpha) \longrightarrow F[x]/f_\alpha(x)F[x] \quad \text{dado por} \quad \theta\left(\overline{\textstyle\sum_{i=0}^{n} a_i \alpha^i}\right) = \overline{\textstyle\sum_{i=0}^{n} a_i x^i}.$$

son isomorfismos de campos.
Ahora, como $\eta : F \longrightarrow K$ un isomorfismo de campos, este induce un isomorfismo de anillos

$$\widehat{\eta} : F[x]/f_\alpha F[x] \longrightarrow K[x]/\widetilde{\eta}(f_\alpha(x))K[x] \quad \textit{dado por} \quad \widehat{\eta}\left(\overline{\sum_{i=0}^{n} a_i x^i}\right) = \left(\overline{\sum_{i=0}^{n} \eta(a_i) x^i}\right)$$

Entonces tenemos que $\xi \circ \overline{\eta} \circ \theta : F(\alpha) \longrightarrow K(\widetilde{\alpha}) \subseteq L$ es un isomorfismo de campos, donde claramente $\xi \circ \overline{\eta} \circ \theta \mid_F = \eta$ y además $\xi \circ \overline{\eta} \circ \theta(\alpha) = \widetilde{\alpha}$

2) *Como se vio ya en $\Longleftarrow$) de i) de este teorema. Para cada raíz $\widetilde{\alpha}$ de $\widetilde{\eta}(f_\alpha(x))$ en L es posible encontrar un isomorfismo de campos $\zeta : F(\alpha) \longrightarrow K(\widetilde{\alpha})$ tal que $\zeta \mid_F = \eta$ y $\zeta(\alpha) = \widetilde{\alpha}$. Luego entonces, existen a lo menos tantos morfismos de estos como raíces distintas de $\widetilde{\eta}(f_\alpha(x))$ en L.*

Por otro lado, si $\zeta : F(\alpha) \longrightarrow L$ es una extensión de η, entonces por la Proposición 1.4.34 se tiene que $\zeta(\alpha)$ es una raíz de $\widetilde{\eta}(f_\alpha(x))$ y entonces $\zeta : F(\alpha) \longrightarrow K(\widetilde{\alpha})$ es un isomorfismo de campos que cumple $\zeta \mid_F = \eta$ y $\zeta(\alpha) = \widetilde{\alpha}$, es decir ζ es uno de los morfismos construidos en $\Longleftarrow$) de i) de este teorema. ∎

Lema 1.4.38. *Sea E una extensión del campo F, $\alpha \in E$ algebraico sobre F y $f_\alpha(x) \in F[x]$ el polinomio mínimo de α sobre F. Si $g(x) \in F[x]$ es tal que α es una raíz de $g(x)$, entones $f_\alpha(x) \mid g(x)$ en $F[x]$.*

Teorema 1.4.39. *Sea $\eta : F \longrightarrow K$ un isomorfismo de campos, $f(x) \in F[x]$ un polinomio mónico de grado $n \geqslant 1$, $\widetilde{\eta}(f(x))$ el correspondiente polinomio a $f(x)$ en $K[x]$ bajo el isomorfismo $\widetilde{\eta} : F[x] \longrightarrow K[x]$ que extiende a η y E y L campos de descomposición de $f(x)$ y $\widetilde{\eta}(f_\alpha(x))$ sobre F y $\widetilde{F}$ respectivamente. Entonces*

1) *η se puede extender a un isomorfismo de E en L.*
2) *El número de extensiones de η a E es menor o igual que $[E : F]$.*

Demostración. *Se demostrará por inducción sobre [E:F].*

Si $[E : F] = 1$, entonces $E = F$ y así $f(x) = \prod_{i=1}^{n}(x - r_i)$ donde $x - r_i \in F[x]$ para cada $i \in \{1, \ldots, n\}$. Aplicando $\widetilde{\eta}$ a $f(x)$ tenemos que:

$$\widetilde{\eta}(f(x)) = \widetilde{\eta}(\prod_{i=1}^{n}(x - r_i)) = \prod_{i=1}^{n}(x - \widetilde{\eta}(r_i)) = \prod_{i=1}^{n}(x - \eta(r_i))$$

Por lo tanto $\widetilde{\eta}(f(x))$ se factoriza en $K[x]$, y entonces $L = K$. De donde trivialmente se obtiene el resultado.

Supongamos que la proposición es válida para todo $k < n$ y sea $[E : F] = n > 1$. Como $n > 1$ y E es un campo de descomposición de $f(x)$ sobre F, existe $\alpha \in E - F$ que es raíz de $f(x)$.

Sea $f_\alpha(x)$ el polinomio mínimo de α sobre F, por el Lema 1.4.38 $f_\alpha(x) \mid f(x)$ en $F[x]$. Entonces todas la raíces de $f_\alpha(x)$ son raíces de $f(x)$ y como E es campo de descomposición de $F(x)$, pasa que $f_\alpha(x) = \prod_{i=1}^{m}(x - s_i)$ en $E[x]$. Además por la Proposición 1.4.22 se tiene que $[F(\alpha) : F] = grad(f_\alpha(x))$. Por el Lema 1.4.37, η se puede extender a k morfismos de campos $\xi_1, \ldots, \xi_k$ en L, donde k es el número de raíces distinta de $f_\alpha(x)$ en E.

Ahora tomemos ξ_i con $i \in \{1, \ldots, k\}$. Claramente $f(x) \in F(\alpha)[x]$ y $\widetilde{\eta}(f(x)) \in \xi_i(F(\alpha))[x]$ y E y L son sus respectivos campos de descomposición sobre $F(\alpha)$. Por el la Proposición 1.4.2, se tiene que $[E : F] = [E : F(\alpha)][F(\alpha) : F]$ y como $\alpha \in E - F$, entonces $1 < grad(f_\alpha(x)) = [F(\alpha) : F]$. De donde tenemos que $[E : F(\alpha)] < n$. Luego por hipótesis de inducción cada ξ_i se puede extender a un isomorfismo de E en L y el número de tales extensiones es menor o igual que $\leqslant [E : F(\alpha)]$, como a lo más existen $[F(\alpha) : F]$ morfismos ξ_i que extienden a η, entonces el número de extensiones de η a E es a lo más $[E : F(\alpha)][F(\alpha) : F] = [E : F]$. ∎

Corolario 1.4.40. *Dos campos de descomposición de $f(x) \in F[x]$ son isomorfos.*

Definición 1.4.41. *Si F es un campo, $f(x) \in F[x]$ y E el campo de descomposición de $f(x)$ sobre F. Entonces*

$$f(x) = \prod_{i=1}^{k} (x - \alpha_i)^{n_i}.$$

Donde $\{\alpha_1, \ldots, \alpha_n\}$ es el conjunto de las distintas raíces de $f(x)$ en E. Se define la ***multiplicidad de la raíz*** *α_i como el exponente n_i.*

Proposición 1.4.42. *Sea F un campo $f(x) \in F[x]$ y E un campo de descomposición de $f(x)$ sobre F. Si $f(x)$ es irreducible en $F[x]$, entonces todos los cero de $f(x)$ tienen la misma multiplicidad en E.*

Demostración. *Consideremos el morfismo identidad $Id : F \longrightarrow F$ y $\alpha, \beta \in E$ dos raíces de $f(x)$ de multiplicidad n_α y n_β. Por el Lema 1.4.37, el morfismo Id puede extenderse a un isomorfismo $\xi : F(\alpha) \longrightarrow F(\beta)$, el cual por el Teorema 1.4.39 se puede extender a un isomorfismo $\kappa : E \longrightarrow E$. κ induce un isomorfismo $\widetilde{\kappa} : E[x] \longrightarrow E[x]$ que deja fijo a F (ver Proposición 1.4.33).*

Nótese que como $\widetilde{\kappa}$ deja fijo a F, entonces $\widetilde{\kappa}(f(x)) = f(x)$. Ahora, como la multiplicidad de α es n_αy la multiplicidad de β es n_β, entonces $f(x) = (x - \alpha)^{n_\alpha}(x - \beta)^{n_\beta} h(x)$ donde $h(x) \in E[x]$ y $x - \alpha \nmid h(x)$ y $x - \beta \nmid h(x)$.

$$f(x) = \widetilde{\kappa}(f(x)) = \widetilde{\kappa}((x - \alpha)^{n_\alpha}(x - \beta)^{n_\beta} h(x)) = (x - \beta)^{n_\alpha}(x - \alpha)^{n_\beta} \widetilde{\kappa}(h(x))$$

Por un lado tenemos que $(x-\beta)^{n_\alpha} \mid f(x)$ y entonces por la Proposición 1.2.63 se tiene que $n_\alpha \leqslant n_\beta$, pero como también $(x - \alpha)^{n_\beta} \mid f(x)$, entonces $n_\beta \leqslant n_\alpha$. Por lo tanto $n_\alpha = n_\beta$. ∎

Teorema 1.4.43 *(Teorema de la Multinomial). Sean R un anillo y $x_1, \ldots, x_n \in R$. Entonces*

$$(x_1 + \cdots + x_n)^m = \sum_{\substack{k_1, k_2, \ldots, k_n \geqslant 0 \\ k_1 + k_2 + \cdots + k_n = m}} \binom{m}{k_1, k_2, \cdots k_n} x_1^{k_1} x_2^{k_2} \cdots x_n^{k_n}.$$

Donde $\binom{m}{k_1, k_2, \cdots k_n} = \frac{m!}{k_1! k_2! \cdots k_n!}$.

Corolario 1.4.44. *Sean R un anillo y $f(x) = \sum_{i=0}^{n} a_i x^i \in R[x]$. Si $m \in \mathbb{Z}^+$, entonces*

$$(f(x))^m = \sum_{i=0}^{nm} \left(\sum_{\substack{k_0, k_1, \ldots, k_n \geqslant 0 \\ k_0 + k_1 + \cdots + k_n = m \\ k_1 + 2k_2 + \cdots + nk_n = i}} \binom{m}{k_0, k_1, \cdots k_n} a_0^{k_0} a_1^{k_1} \cdots a_n^{k_n} \right) x^i.$$

Proposición 1.4.45. *Sean $m, n \in \mathbb{Z}^+$, $k_1, \ldots, k_m \in \{0, 1, \ldots, n\}$ y $j \in \{0, 1, \ldots, n\}$ tales que*

$$k_1 + \cdots + k_m = nm - n + j.$$

Entonces $k_i \geqslant j$ para todo $i \in \{1, \ldots, m\}$.

Demostración. *Si $j = 0$ la proposición se cumple trivialmente, entonces podemos suponer que $j \in \{1, \ldots, n\}$.*

Supongamos que $k_i < j$ para alguna $i \in \{0, 1, \ldots, m\}$, de hecho sin perdida de generalidad podemos suponer que $k_m < j$. Entonces

$$(k_1 + \cdots + k_{m-1}) + k_m < (k_1 + \cdots + k_{m-1}) + j.$$

Como $k_1+\cdots+k_m = nm-n+j$, *tenemos que* $nm-n+j < (k_1+\cdots+k_{m-1})+j$. *Así concluimos que* $nm - n < k_1 + \cdots + k_{m-1}$, *que es un absurdo pues como* $k_i \leqslant n$, *entonces* $k_1 + \cdots + k_{m-1} \leqslant (m-1)n$.

Por lo tanto $k_i \geqslant j$ *para todo* $i \in \{1,\ldots,m\}$. ∎

Corolario 1.4.46. *Sean* $m,n \in \mathbb{Z}^+$, $k_1,\ldots,k_n \in \{0,1,\ldots,n\}$ *y* $j \in \{0,1,\ldots,n\}$ *tales que*

$$k_1 + k_2 + k_3 + \cdots + k_n = m \quad y \quad k_1 + 2k_2 + 3k_3 + \cdots + nk_n = nm - n + j.$$

Entonces $k_i = 0$ *para todo* $i < j$.

Proposición 1.4.47. *Sean* R *un anillo y* $f(x) = \sum_{i=0}^{n} a_i x^i \in R[x]$. *Si* $m \in \mathbb{Z}^+$ *y* $j \in \{0,1,\ldots,n\}$, *entonces el coeficiente del término* x^{nm-n+j} *en el polinomio* $(f(x))^m$ *esta dado por*

$$\sum_{\substack{k_j+k_{j+1}+\cdots+k_n=m \\ jk_j+(j+1)k_{j+1}+\cdots+nk_n=nm-n+j \\ k_j,k_{j+1},\ldots,k_n\geqslant 0}} \binom{m}{k_j, k_{j+1}, \cdots k_n} a_j^{k_j} a_{j+1}^{k_{j+1}} \cdots a_n^{k_n}.$$

Lema 1.4.48. *Sea* E *una extensión de* F. *Si* $m \in \mathbb{Z}^+$ *es tal que* $m1 \neq 0$ *en* F *y* $e \in E - F$, *entonces* $me \in E - F$.

Lema 1.4.49. *Sea* E *una extensión de* F *y* $f(x) = \sum_{i=0}^{n} a_i x^i \in E[x]$ *un polinomio mónico tal que* E *es un campo de descomposición de* $f(x)$. *Si* $m \in \mathbb{Z}^+$ *es tal que* $(f(x))^m \in F[x]$ *y* $m1 \neq 0$ *en* F, *entonces* $f(x) \in F[x]$.

Demostración. *Por la Proposición 1.4.47 el coeficiente del termino* x^{nm-1} *esta dado por*

$$\binom{m}{1, m-1} a_{n-1} a_n^{m-1} \underset{f(x) \text{ es mónico}}{=} \frac{m!}{1!(m-1)!} a_{n-1} = m a_{n-1}.$$

Entonces $(m1)a_{n-1} \in F$, *y como* $m1 \neq 0$ *en* F, *por el Lema 1.4.48 tenemos que* $a_{n-1} \in F$.

A continuación se demostrará que $a_i \in F$ *para todo* $i \in \{1,\ldots,n\}$, *para los cual procederemos por reducción al absurdo. Entonces supongamos que existe un coeficiente de* $f(x)$ *que no pertenece a* F *y sea* k *el grado del monomio de* $f(x)$ *de grado máximo tal que* a_k *no esta en* F. *Es decir* $a_k \in E - F$ *y* $a_j \in F$ *para todo* $j > k$.

De la Proposición 1.4.47, tenemos que el coeficiente de x^{mn-n+k} *en* $(f(x))^m$ *es de la forma*

$$m a_k + g(a_{n-1}, a_{n-2}, \ldots, a_{k+1}) \in F. \tag{4.1}$$

Donde $g(a_{n-1}, a_{n-2}, \ldots, a_{k+1})$ *es un polinomio en* $n-k-1$ *variables evaluado en* $a_{n-1}, a_{n-2}, \ldots, a_{k+1}$.

Como a_k *es mínimo con la propiedad de que* $a_k \in E - F$, *entonces* $a_{n-1}, a_{n-2}, \ldots, a_{k+1} \in F$ *y así* $g(a_{n-1}, a_{n-2}, \ldots, a_{k+1}) \in F$. *Luego podemos concluir por (4.1) que* $(m1)a_k$. *Y entonces por el Lema 1.4.48 tenemos que* $a_k \in F$. *Lo que es un absurdo pues suponemos que* $a_k \in E - F$. *Por lo tanto todos los coeficiente de* $f(x)$ *pertenecen a* F *y así* $f(x) \in F[x]$. ∎

Corolario 1.4.50. *Sea* F *un campo de característica 0 y* $f(x) \in F[x]$ *un polinomio irreducible y mónico. Entonces* $f(x)$ *tiene todas sus raíces distintas.*

Demostración. *Sea* $f(x) \in F[x]$ *y* E *un campo de descomposición de* $f(x)$ *sobre* F. *Entonces por la Proposición 1.4.42*

$$f(x) = \left(\prod_{i=1}^{k} x - \alpha_i \right)^s \quad \text{para algún} \quad s \in \mathbb{Z}^+,$$

donde $\{\alpha_1,\ldots,\alpha_n\}$ *son las distintas raíces de* $f(x)$ *en* E.

Si tomamos $g(x) = \prod_{i=1}^{k}(x-\alpha_i) \in F[x]$, *entonces* $(g(x))^s \in F[x]$, *luego como F es de característica cero,* $s1 \neq 0$ *y así al aplicar el Lema 1.4.49 tenemos que* $g(x) \in F[x]$. *Ahora,* $f(x)$ *es irreducible* $F[x]$ *y* $g(x) \mid f(x)$, *además de que* $g(x)$ *no es una unidad en* $F[x]$. *Luego entonces* $f(x)$ *y* $g(x)$ *son asociados en* $F[x]$, *entonces por la Proposición 1.2.30* $f(x)F[x] = g(x)F[x]$, *y de la Proposición 1.4.8 concluimos que* $f(x) = g(x)$. *Por lo tanto* $f(x)$ *tiene todas sus raíces distintas.* ∎

Lema 1.4.51. *Sean E es un extensión de un campo F y* $f(x), g(x) \in F[x]$. *Si* $d_E(x) \in E[x]$ *es un máximo común divisor* $f(x)$ *y* $g(x)$ *en* $E[x]$ *y* $d_F(x) \in E[x]$ *es un máximo común divisor* $f(x)$ *y* $g(x)$ *en* $F[x]$, *entonces existe* $h(x) \in E[x]$ *tal que* $d_E(x)h(x) = d_F(x)$.

Lema 1. 4.52. *Sea E una extensión algebraica y finita de un campo F. Entonces existen* $\alpha_1, \ldots, \alpha_n \in E$ *tales que* $E = F(\alpha_1, \ldots, \alpha_n)$.

Teorema 1.4.53 *(Teorema del elemento primitivo). Si F es un campo de característica cero, entonces toda extensión algebraica y finita de F es una extensión simple de F.*

Demostración. *Se probará el caso para* $E = F(\alpha,\beta)$ *con* α *y* β *algebraicos sobre F, luego el razonamiento de inducción es obvio a partir del Lema 1.4.52.*

Sea E algebraica y finita de F y $\alpha,\beta \in E$ *tales que* $E = F(\alpha,\beta)$. *Consideremos* $f_\alpha(x)$ *y* $f_\beta(x)$ *respectivamente los polinomios mínimos de* α *y* β *sobre F. Por el corolario 1.4.17 existe una extensión K de E que contiene a* $\alpha = \alpha_1, \ldots, \alpha_m$ *y* $\beta = \beta_1, \ldots, \beta_n$ *las raíces distintas de* $f_\alpha(x)$ *y* $f_\beta(x)$.

Tenemos F es infinito, pues es de característica cero, entonces es posible encontrar $a \in F$ *tal que* $a \neq (\beta_i - \beta)/(\alpha - \alpha_j)$ *para todas las* $i \in \{1, \ldots, n\}$ *y* $j \in \{2, \ldots, m\}$. *De donde tenemos que* $\beta + a\alpha \neq \beta_i + a\alpha_j$ *para todas las* $i \in \{1, \ldots, n\}$ *y* $j \in \{2, \ldots, m\}$. *Y en consecuencia*

$$\beta + a\alpha - a\alpha_j \neq \beta_i \quad \text{para todo} \quad i \in \{1, \ldots, n\} \quad \text{y para todo} \quad j \in \{2, \ldots, m\}. \tag{4.2}$$

Como $\beta + a\alpha \in F(\alpha,\beta)$, *claramente se tiene que* $F(\beta + a\alpha) \subseteq F(\alpha,\beta)$.

Ahora consideremos $h(x) = f_\beta(\beta + a\alpha - ax) \in F(\beta + a\alpha)[x]$. *Notemos que* $h(\alpha) = 0$, *además por (4.2) es claro que* α *es la única raíz común de* $h(x)$ *y* $f_\alpha(x)$. *Entonces podemos concluir que un máximo común divisor de* $h(x)$ *y* $f_\alpha(x)$ *en* $K[x]$ *es* $x - \alpha$.

Si $d(x)$ *un máximo común divisor de* $h(x)$ *y* $f_\alpha(x)$ *en* $F(\beta + a\alpha)[x]$, *por el Lema 1.4.51 tenemos que* $x - \alpha \mid d(x)$ *usando una vez más el hecho de que* α *es la única raíz común de* $h(x)$ *y* $f_\alpha(x)$ *tenemos que* $x - \alpha$ *es asociado a* $d(x)$ *y entonces* $x - \alpha$ *es un máximo común divisor de* $h(x)$ *y* $f_\alpha(x)$ *en* $F(\beta + a\alpha)[x]$. *Por la tanto* $x - \alpha \in F(\beta + a\alpha)[x]$. *En consecuencia se tiene que* $\alpha \in F(\beta + a\alpha)$ *de donde se obtiene que* $\beta \in F(\beta + a\alpha)$ *y así* $F(\alpha,\beta) \subseteq F(\beta + a\alpha)$. *Por lo tanto* $F(\alpha,\beta) = F(\beta + a\alpha)$. ∎

Ahora se presenta un interesante resultado que describe los subgrupos finitos del grupo de unidades de un campo.

Teorema 1.4.54. *Sea K un campo. Todo subgrupo finito del grupo multiplicativo* $U(K)$ *está formado por raíces de la unidad y es cíclico.*

Demostración. *Sea G un subgrupo finito de* $U(K)$. *Como* $(U(K), \cdot)$ *son un grupo abeliano, entonces G es un grupo abeliano finito. Luego por el Corolario 1.3.15, existe* $z \in G$ *cuyo orden n es tal* $y^n = 1$ *para todo* $y \in G$. *Como un polinomio de grado n puede tener a lo mas n raíces distintas como máximo y todos los elementos de G son ceros del polinomio* $x^n - 1$, *se tiene entonces que* $|G| \leqslant n$. *Por otro lado* $z \in G$ *se tiene que el subgrupo generado por z esta contenido en G y como el orden el subgrupo generado por z es n entonces* $n \leqslant |G|$. *Por lo tanto* $|G| = n$ *y así G esta generado por z y los elementos de G son las raíces del polinomio* $x^n - 1$. ∎

Por último se presentan dos resultados que concluirán con dos ejemplos que ilustran el Teorema 1.4.39.

Definición 1.4.55. *Sea K un campo $f(x) = \sum_{i=1}^{n} a_i x^i \in K[x]$. La **derivada formal** de $f(x)$ es el polinomio*

$$f'(x) = a_1 + 2a_2x + 3a_3x^2 + \cdots + (n-1)a_{n-1}x^{n-2} + na_nx^{n-1}.$$

Teorema 1.4.56. *Sea K un campo $f(x) \in K[x]$. Entonces $f(x)$ no tiene raíces multiples si y sólo si $(f(x), f'(x)) \in K$.*

Teorema 1. 4.57 *(Criterio de Eiseinstein). Sea D un dominio de factorización única con campo de cocientes $Q(D)$ y sea $f(x) = \sum_{i=1}^{n} a_i x^i \in D[x]$. Supongamos que existe $r \in D$ un elemento irreducible tal que $r \nmid a_n$ $r \mid a_i$ para $i = 0, \ldots, n-1$ y $r^2 \nmid a_0$, entonces $f(x)$ es irreducible en $Q(D)[x]$.*

Ejemplo 1.4.58. Consideremos K un campo de característica 0 y el polinomio $f(x) = x^n - 1 \in K[x]$ con $n \in \mathbb{Z}^+$. Si Γ es el conjunto de raíces de $f(x)$. Claramente $1 \in \Gamma$ y para $\alpha, \beta \in \Gamma$ se tiene que $(\alpha\beta^{-1})^n - 1 = \alpha^n (\beta n)^{-1} - 1 = 0$, es decir $\alpha\beta^{-1} \in \Gamma$. Por lo tanto Γ es un subgrupo de $U(K)$.

Ahora, $f' = nx^{n-1}$ y entonces

$$f(x) - (\frac{1}{n}x)f' = 1.$$

Luego, por el Corolario 1.2.82, tenemos que $(f(x), f'(x)) \in K$ y así por el Teorema 1.4.56 el polinomio $f(x) = x^n - 1$ tiene n todas sus raíces distintas, y entonces por el Teorema 1.4.54 Γ es un grupo cíclico isomorfo a $\mathbb{Z}_n$.

Así, si ξ es un generador de Γ, entonces $\Gamma = \{1, \xi, \xi^2, \ldots, \xi^{n-1}\}$. De donde podemos concluir que $K(\xi)$ es el campo de descomposición de $f(x) = x^n - 1$.

Por el Lema 1.4.37, tenemos que el morfismo identidad $Id : K \longrightarrow K$ se puede extender a n morfismos distintos, $\sigma_i : K(\xi) \longrightarrow K(\xi)$. Donde para cada $i \in \{1, \ldots, n\}$, el morfismo σ_i que extiende al morfismo identidad queda determinado por $\sigma_i(\xi) = \xi^i$.

Ejemplo 1.4.59. Consideremos K un campo de característica 0 y $d \in K - d\{0\}$. Un argumento similar al empleado en el Ejemplo 1.4.58 muestra que para cada $n \in \mathbb{Z}^+$ el polinomio $x^n - d$ tiene n raíces distintas.

Si ξ es un generador de grupo multiplicativo generado por las raíces del polinomio $x^n - 1$ y α es una raíz del polinomio $x^n - d$. Por inspección se verifica que $\alpha, \xi\alpha, \xi^2\alpha, \ldots, \xi^{n-1}\alpha$ son la distintas raíces del polinomio $x^n - d$. Y entonces tenemos que el campo de descomposición del polinomio $x^n - d$ es $K(\alpha, \xi)$.

Luego, por el Lema 1.4.37, el morfismo identidad $Id : K \longrightarrow K$ se puede extender a n morfismos distintos de $K(\alpha)$ en $K(\alpha, \xi)$. Siendo el i-simo morfismo $\sigma_i : K(\xi) \longrightarrow K(\xi)$ que extiende a el morfismo identidad determinado por $\sigma(\alpha) = \xi^i\alpha$.

Capítulo 2

Anillo de enteros algebraicos

§*2.1 Enteros algebraicos.*

Definición 2.1.1. *Sea S un anillo y R un subanillo de S. Un elemento $s \in S$ es **entero algebraico sobre** R si existe $f(x) \in R[x]$ mónico tal que $f(s) = 0$.*

Ejemplo 2.1.2.

1) Si F es un campo y E es una extensión F, entonces $\alpha \in E$ es entero algebraico sobre F si y sólo si $\alpha \in E$ es algebraico sobre F.
2) Consideremos el anillo de enteros $\mathbb{Z}$. Tenemos que $\frac{1}{\sqrt{2}}$ es un elemento algebraico sobre $\mathbb{Q}$ que no es entero algebraico sobre $\mathbb{Z}$.

Si S es un anillo y R es un subanillo de S, por la Proposición 2.4.3 sabemos que dado $s \in S$ existe un único morfismo $ev_x R[x] \longrightarrow S$ tal $ev_\alpha(x) = s$ y $ev_\alpha(r) = r$ para todo $r \in R$. A la imagen del morfismo ev_s en S la denotaremos por $R[s]$.

Proposición 2.1.3. *Sean S un anillo, R un subanillo de S y $s \in S$, Entonces*

$$R[s] = \bigcap_T \{T \subseteq S \mid T \quad es\ subanillo\ de \quad S \quad y \quad R \cup \{s\} \subseteq T\}.$$

Observación 2. 1.4. Nótese que $R[s]$ está generado como R-módulo por el conjunto $\{s^n\}_{n\in\mathbb{N}}$.

Si S un anillo, R un subanillo S y $s_1, \ldots, s_n \in$, definimos

$$R[s_1, \ldots, s_n] = \bigcap_T \{T \subseteq S \mid T \quad es\ subanillo\ de \quad S \quad y \quad R \cup \{s_1, \ldots, s_n\} \subseteq T\}.$$

Proposición 2.1.5. *Sean S un anillo, R un subanillo S y $s_1, \ldots, s_n \in$. Entonces*

$$R[s_1, \ldots, s_n] = R[s_1, \ldots, s_{n-1}][s_n].$$

Definición 2.1.6. *Si R un anillo y M es un R-módulo, M se dice **finitamente generado** si existen $n \in \mathbb{N}$ y $m_1, \ldots, m_n \in M$ tales que $M = \langle\{m_1, \ldots, m_n\}\rangle$.*

Teorema 2.1.7. *Sean S un anillo, R un subanillo de S y $s \in S$. Son equivalentes*

1) s es entero algebraico sobre R
2) El anillo $R[s]$ es un R-módulo finitamente generado.
3) Existe un subanillo T de S que contiene a R y a s, y que es un R-módulo finitamente generado.

Demostración.

i) $\Rightarrow$ *ii)* *Supongamos que* $s \in S$ *es un entero algebraico sobre R. Entonces existe*

$$f(x) = \sum_{i=0}^{n} a_i x^i \in R[x] \text{ polinomio mónico tal que } f(s) = 0.$$

Sea M el R-submódulo de S generado por el conjunto $\{1, s, \ldots, s^{n-1}\}$. *Claramente* $M \subseteq R[s]$.

Ahora vamos a demostrar por inducción sobre k que $s^{n+k} \in M$ *para todo* $k \in \mathbb{N}$.

Primero verificaremos para $k = 0$. *Dado que* $f(s) = 0$, *entonces*

$$s^n + a_{n-1}s^{n-1} + \cdots + a_1 s + a_0 = 0 \tag{1.1}$$

y así $s^n = -(a_{n-1}s^{n-1} + \cdots + a_1 s + a_0)$, *entonces* $s^n \in M$.

Supongamos la proposición válida para todo $k < m$, *es decir, si* $0 \leqslant k < m$ *entonces* $s^{n+k} \in M$, *además como* $s^i \in M$ *para todo* $i \in \{0, 1, \ldots, n-1\}$, *entonces tenemos que* $s^i \in M$ *para todo* $i < n + m$.

Ahora, multiplicando (1.1) por s^m, *se tiene que*

$$s^{n+m} + a_{(n-1)+m}s^{n-1} + \cdots + a_1 s^{m+1} + a_0 s^m = 0$$

Así $s^{n+m} = -(a_{(n-1)+m}s^{n-1} + \cdots + a_1 s^{m+1} + a_0 s^m) \in M$. *Por lo tanto tenemos que* $s^n \in M$ *para todo* $n \in \mathbb{N}$. *Luego podemos concluir que* $R[s] \subseteq M$ *y entonces* $M = R[s]$ *por lo que* $R[s]$ *es finitamente generado.*

ii) $\Rightarrow$ *iii)* *Por hipótesis* $R[s]$ *es un R-módulo finitamente generado y claramente* $R \cup \{s\} \subseteq R[s]$, *luego el enunciado se sigue trivialmente.*

iii) $\Rightarrow$ *i)* *Supongamos que T es un R-submódulo finitamente generado de S que contiene a* $R \cup \{s\}$, *entonces existen* $t_1, \ldots, t_n \in T$ *tales que el conjunto* $\{t_1, \ldots, t_n\}$ *genera a T como R-módulo. Siendo T un subanillo de S y que* $s \in T$, *tenemos entonces que* $st_i \in T$ *para todo* $i \in \{1, \ldots, n\}$ *y así se tenemos que*

$$st_i = \sum_{j=1}^{n} a_{ij}t_j,$$

yY entonces, para cada $i \in \{1, \ldots, n\}$,

$$-a_{i1}t_1 - \ldots + a_{ii-1}t_{i-1} + (s - a_{ii})t_i - a_{ii+1}t_{i+1} \ldots - a_{in}t_n = 0.$$

Si consideremos la delta de Kronecker dada por $\delta_{ij} = \begin{cases} 0 & si\ i \neq j \\ 1 & si\ i = j \end{cases}$, *tenemos n igualdades de la forma*

$$\sum_{j=1}^{n} (\delta_{ij}s - a_{ij})t_j = 0, \tag{1.2}$$

una para cada $i \in \{1, \ldots, n\}$.

Consideremos $f(x) = det(\delta_{ij}x - a_{ij})$. *Dado que* $a_{ij} \in R$, *entonces* $f(x) \in R[x]$ *siendo este un polinomio mónico.*

Ahora consideremos el sistema de ecuaciones

$$\begin{array}{ccccccccccccc}
(s-a_{11})x_1 & + & \cdots & + & -a_{1i}x_i & + & \cdots & + & -a_{1n}x_n & = & 0 \\
\vdots & & & & \vdots & & & & \vdots & & \vdots \\
-a_{i1}x_1 & + & \cdots & + & (s-a_{ii})x_i & + & \cdots & + & -a_{in}x_n & = & 0 \\
\vdots & & & & \vdots & & & & \vdots & & \vdots \\
-a_{n1}x_1 & + & \cdots & + & -a_{ni}x_i & + & \cdots & + & (s-a_{nn})x_n & = & 0
\end{array} \tag{1.3}$$

Lo primero que tenemos que notar es que el determinante del sistema de ecuaciones de $n \times n$ dado en (1.3) es $f(s)$. Por otro lado, claramente $(t_1, \ldots, t_n) \in T^n$ es una solución del sistema de ecuaciones (1.3). Entonces por las formulas de Crammer[1]

tenemos que $f(s)y_i = 0$ para todo $i \in \{1, \ldots, n\}$.

Por ultimo como $1 \in T$, existen $b_1, \ldots, b_n \in R$ tales que

$$1 = \sum_{i=0}^{n} b_j y_i$$

y entonces

$$f(s) = f(s)1 = f(s)\left(\sum_{i=0}^{n} b_j y_i\right) = \sum_{i=0}^{n} b_j (f(s)y_i) \underset{f(s)y_i=0}{=} 0$$

Siendo que $f(x) \in R[x]$ y es un polinomio mónico, tenemos en consecuencia que s es entero algebraico sobre R. ∎

Corolario 2.1.8. *Sean S un anillo, R un subanillo de S y $s_1, \ldots, s_n \in S$ tales que s_1 es entero algebraico sobre R y s_i es entero algebraico sobre $R[s_1, \ldots, s_{i-1}]$ para $i = 2, \ldots, n$. Entonces $R[s_1, \ldots, s_n]$ es un R-módulo finitamente generado.*

Demostración. *La demostración se hará por inducción sobre n.*

El caso $n = 1$ es precisamente el Teorema 2.1.7.

Supongamos que la proposición es válida para n, es decir, si $s_1, \ldots, s_n \in S$ son tales que s_1 es entero algebraico sobre R y s_i es entero algebraico sobre $R[s_1, \ldots, s_{i-1}]$ para $i = 2, \ldots, n$. Entonces $R[s_1, \ldots, s_n]$ es un R-módulo finitamente generado.

Sean entonces $s_1, \ldots, s_{n+1} \in S$ tales que s_1 es entero algebraico sobre R y s_i es entero algebraico sobre $R[s_1, \ldots, s_{i-1}]$ para $i = 2, \ldots, n+1$. Por hipótesis de inducción $T = R[s_1, \ldots, s_n]$ es un R-módulo finitamente generado sobre R, y así existen $m \in \mathbb{Z}^+$ y $b_1, \ldots, b_m \in T$ tales que

$$T = \sum_{j=0}^{m} R b_j. \tag{1.1}$$

Como s_{n+1} es entero algebraico sobre T, luego por el Teorema 2.1.7 $T[s_{n+1}]$ es un T–módulo finitamente generado y entonces existen $k \in \mathbb{Z}^+$ y $c_1, \ldots, c_k \in T[s_{n+1}]$ tales que

$$T[s_{n+1}] = \sum_{i=0}^{k} T c_i. \tag{1.2}$$

Así tenemos que

$$R[s_1, \ldots, s_{n+1}] \underset{Prop.\ 2.5.11}{=} R[s_1, \ldots, s_n][s_{n+1}] = T[s_{n+1}] \underset{por\ (1,2)}{=} \sum_{i=0}^{k} T c_i \underset{por\ (1,1)}{=} \sum_{i=0}^{k} \left(\sum_{j=0}^{m} R b_j\right) c_i = \sum_{i=0}^{k} \left(\sum_{j=0}^{m} R(b_j c_i)\right)$$

Es decir $R[s_1, \ldots, s_{n+1}]$ es un R-módulo finitamente generado por el conjunto $\{b_i c_j\}_{i=1}^{k}{}_{j=1}^{m}$. ∎

---

[1] Sea R un anillo y $\begin{matrix} a_{11}x_1 + \cdots + -a_{1n}x_n = c_1 \\ \vdots \qquad\qquad \vdots \quad \vdots \\ a_{n1}x_1 + \cdots + s{-}a_{nn}x_n = c_1 \end{matrix}$ un sistema de n ecuaciones con n incógnitas ecuaciones con coeficientes en R y sea $A = (a_{ij})$ la matriz del sistema de ecuaciones. Si A_i es la matriz que se obtiene al sustituir en la matriz A la columna i por el vector $\begin{pmatrix} c_1 \\ \vdots \\ c_n \end{pmatrix}$ y si $\begin{pmatrix} y_1 \\ \vdots \\ yc_n \end{pmatrix}$ es una solución al sistema de ecuaciones, entonces $det(A)y_i = det(A_i)$ para cada $i \in \{1, \ldots, n\}$.

Corolario 2.1.9. *Sea R un subanillo de un anillo S y $x, y \in S$. Si x, y son enteros algebraicos sobre R, entonces $x \pm y$ y xy son enteros algebraicos sobre R.*

Demostración. *Como $x, y \in S$ son enteros algebraicos sobre R, entonces por el Corolario 2.1.8 $R[x, y]$ es un R-módulo finitamente generado. Como $x \pm y$ y xy son elementos de $R[x, y]$, del Teorema 2.1.7 concluimos que $x \pm y$ y xy son enteros algebraicos sobre R.* ∎

Corolario 2.1.10. *Sea R un subanillo de una anillo S. El conjunto R' de los elementos en S que son enteros algebraicos sobre R es un subanillo de S que contiene a R.*

Definición 2.1.11. *Sean S un anillo y R un subanillo de un anillo S. Por el Corolario 2.1.10 tenemos que*

$$R' = \{s \in S \mid s \text{ es algebraico sobre } R\}$$

*es un subanillo de S que contiene a R. A R' se le llama la **cerradura entera de R en S**. Se dice que S es **entero** sobre R si todo elemento de S es entero algebraico sobre R.*

Proposición 2.1.12. *Sea T un anillo, S un subanillo de T y R un subanillo de S. Si T es entero sobre S y S es entero sobre R, entonces T es entero sobre R*

Demostración. *Sea $t \in T$. Como t es entero algebraico sobre S, existe $f(x) = x^n + \sum_{i=0}^{n-1} a_i x^i \in S[x]$ tal que $f(t) = 0$. Consideremos el anillo $B = R[a_0, \ldots, a_{n-1}]$. Dado que $a_i \in B$ para $i = 0, \ldots, n-1$, tenemos que $f(x) \in B[x]$. Además como $f(t) = 0$ concluimos que t es entero algebraico sobre B.*

Ahora, para cada $i \in \{0, \ldots, n-1\}$, $a_i \in S$ es entero algebraico sobre R pues S es entero sobre R. Entonces sucede que a_0 es entero algebraico sobre R, a_i es entero algebraico sobre $R[a_0, \ldots, a_{i-1}]$ para $i = 1, \ldots, n-1$, además de que t es entero algebraico sobre $B = R[a_0, \ldots, a_{n-1}]$. Entonces por el Corolario 2.1.8, $R[a_0, \ldots, a_{n-1}, t]$ es un R-modulo finitamente generado que contiene a t, luego aplicando el Teorema 2.1.7 obtenemos que t es entero algebraico sobre R. Por lo tanto T es entero sobre R. ∎

Definición 2.1.13. *Si D es un dominio entero con campo de cocientes Q y $\overline{Q}$ es la cerradura algebraica de Q. A la cerradura algebraica de D en $\overline{Q}$ se le llama la **cerradura entera** de D. Un dominio entero D es **enteramente cerrado** si la cerradura entera de D en Q es D.*

Proposición 2.1.14. *Si D es un dominio de factorización única, entonces D es enteramente cerrado.*

Demostración. *Sea Q el campo de cocientes de D y supongamos que $\frac{p}{q} \in Q$ con $(p, q) \in U(D)$ es entero algebraico sobre D. Vamos a demostrar que bajo estas condiciones q es un elemento invertible en D y en consecuencia $\frac{p}{q} \in D$.*

Procedamos por reducción al absurdo. Para ello supongamos que $q \in D - U(D)$.

Como $\frac{p}{q}$ es entero algebraico sobre D, entonces existe $\sum_{i=0}^{n} a_i x^i \in D[x]$ un polinomio mónico tal que

$$\left(\frac{p}{q}\right)^n + a_{n-1}\left(\frac{p}{q}\right)^{n-1} + \cdots + a_1\left(\frac{p}{q}\right) + a_0 = 0 \tag{1.3}$$

Multiplicando la igualdad (1.3) por q^n tenemos que

$$p^n + a_{n-1}p^{n-1}q + \cdots + a_1 pq^{n-1} + a_0 q^n = 0$$

y así

$$q(-a_{n-1}p^{n-1} - \cdots - a_1 pq^{n-2} - a_0 q^{n-1}) = p^n.$$

De donde obtenemos que $q \mid p^n$.

Ahora, dado que $q \in D - U(D)$, y D es un dominio de factorización única, existe $r \in D$ irreducible tal que $r \mid q$. Entonces, por transitividad se tiene que $r \mid p^n$. Luego, por Corolario 2.2.78 podemos concluir que $r \mid p$. Por lo tanto $r \mid (p,q)$, que es un absurdo pues r es un elemento irreducible en D. ∎

Corolario 2.1.15. *Todo dominio de ideales principales es enteramente cerrado.*

Corolario 2.1.16. *El anillo de los enteros $\mathbb{Z}$ es enteramente cerrado.*

Proposición 2.1.17. *Sean D un dominio entero y F un campo que contiene a D. Si D' es la cerradura entera de D en F, entonces D' es enteramente cerrado.*

Demostración. *Dado que $D' \subseteq F$, entonces su campo de cocientes Q' esta contenido en F. Ahora si $\alpha \in Q'$ es entero algebraico sobre D', por la Proposición 2.1.12 se tiene que α es un entero algebraico sobre D y dado que $\alpha \in F$, por construcción se tiene que $\alpha \in D'$. Por lo tanto D' es enteramente cerrado.* ∎

Proposición 2.1.18. *Sea D un dominio entero y R un subanillo de D, tal que D es entero sobre R. Entonces D es campo si y sólo si R es campo.*

Demostración.

⇒) *Supongamos que D es un campo y sea $r \in R - \{0\}$. Como $r^{-1} \in D$ y D es entero sobre R, existe $\sum_{i=0}^{n} a_i x^i \in D[x]$ un polinomio mónico tal que*

$$\left(r^{-1}\right)^n + a_{n-1}\left(r^{-1}\right)^{n-1} + \cdots + a_1\left(r^{-1}\right) + a_0 = 0 \tag{1.1}$$

multiplicando (1.1) por r^n tenemos que

$$1 + a_{n-1}r + \cdots + a_1 r^2 + a_0 r^n = 0.$$

Y así $r(-a_{n-1} - \cdots - a_1 r^{n-2} - a_0 r^{n-1}) = 1$ donde $-a_{n-1} - \cdots - a_1 r^{n-2} - a_0 r^{n-1} \in R$. Por lo tanto R es un campo.

⇐) *Supongamos que R es campo y tomemos $d \in D - \{0\}$. Como D es entero sobre R, por el Teorema 2.1.7 $R[d]$ es un espacio vectorial de dimensión finita sobre R.*

Por otro lado la función $\varphi : R[d] \longrightarrow R[d]$ dada por $\varphi(r) = rd$, es una transformación R-lineal inyectiva pues $R[d]$ es un dominio entero. Como $R[d]$ un espacio vectorial de dimensión finita sobre R, entonces φ es un isomorfismo de R espacios vectoriales[2]*. Luego entonces existe $d' \in R[d]$ tal que $dd' = 1$. Por lo tanto D es un campo.* ∎

§2.2 Anillos de Dedekind.

"Los números son la libre creación de la mente humana. "

R. Dedekind.

[2]Si V es un k-espacio vectorial de dimensión finita y $\varphi : V \longrightarrow V$ es un k-homomorfismo de espacios vectoriales. Son equivalentes:

1) φ es un isomorfismo de espacios vectoriales.
2) φ es inyectiva.
3) φ es sobreyectiva.

Para fines prácticos, durante esta sección todos los anillo y campos serán considerados de característica cero. Si K es un campo se denotará a la cerradura algebraica de K por $\overline{K}$.

Sea E/K una extensión finita de un campo K, si $\alpha \in E$ por la Proposición 1.4.25, tenemos que α es algebraico sobre K. Si consideramos $f_\alpha(x) \in K[x]$ el polinomio mínimo de α sobre K, tal que $grad(f_\alpha(x)) = n$, por la Proposición 1.4.7 tenemos que $f_\alpha(x)$ es un polinomio irreducible en $K[x]$, luego, del Corolario 1.4.50 $f_\alpha(x)$ tiene n raíces distintas en $\overline{K}$. Y entonces por el Lema 1.4.37, el morfismo identidad $Id : K \longrightarrow K$ dado por $Id(k) = k$ para toda $k \in K$, se existen exactamente a n morfismos distintos de campo, digamos

$$\sigma_i : K(\alpha) \longrightarrow \overline{K} \quad con \quad i = 1, \ldots, n.$$

*Bajo estas condiciones, se define la función **norma** relativa a $K(\alpha)$ y K por*

$$N_{K(\alpha)/K} : K(\alpha) \longrightarrow \overline{K} \quad dada\ por \quad N_{K(\alpha)/K}(\beta) = \prod_{i=1}^{n} \sigma_i(\beta) \quad para\ todo \quad \beta \in K(\alpha).$$

*y la función **traza** relativa a $K(\alpha)$ y K por:*

$$T_{K(\alpha)/K} : K(\alpha) \longrightarrow \overline{K} \quad dada\ por \quad Tr_{K(\alpha)/K}(\beta) = \sum_{i=1}^{n} \sigma_i(\beta) \quad para\ todo \quad \beta \in K(\alpha).$$

En adelante, si no hay lugar a confusión, se denotará la norma y la traza de β sobre K simplemente por $N(\beta)$ y $Tr(\beta)$ respectivamente.

Ejemplo 2. 2.1. Sean D un dominio de factorización única con campo de cocientes Q y $f(x) = x^n - r \in Q[x]$ donde r es un elemento irreducible en D.

Por la Proposición 1.4.57, $f(x)$ es un polinomio irreducible en Q, luego si α es una raíz de $f(x)$, tenemos que $f(x)$ es el polinomio irreducible de α sobre Q.

Como ya se vio en el Ejemplo 1.4.59, existen n morfismo de $Q(\alpha)$ en $\overline{Q}$, donde el i-ésimo morfismo esta dado por $\sigma_i(\alpha) = \xi^i\alpha$, donde ξ es un generador de las raíces del polinomio $x^n - 1$.

Por la Proposición 14.22 tenemos que $\{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$ es una base de $Q(\alpha)$ sobre Q, por lo que todo elemento $\beta \in Q(\alpha)$ se puede escribir de la forma

$$\beta = q_0 + q_1\alpha + q_2\alpha^2 + \cdots + q_{n-1}\alpha^{n-1} \quad con \quad a_i \in Q \quad para \quad i = 0, \ldots, n-1.$$

Y así tenemos que para $\beta \in Q(\alpha)$, la función $N : Q(\alpha) \longrightarrow \overline{Q}$ esta dada para por

$$N(\beta) = \prod_{i=1}^{n} \sigma_i(\beta) = \prod_{i=1}^{n} \sigma_i \left(\sum_{j=0}^{n-1} q_j\alpha^j \right) = \prod_{i=1}^{n} \left(\sum_{j=0}^{n-1} q_j\sigma_i\left(\alpha^j\right) \right) = \prod_{i=1}^{n} \left(\sum_{j=0}^{n-1} q_j\xi^{ij}\alpha^j \right).$$

y la función traza $T : Q(\alpha) \longrightarrow Q(\alpha, \xi)$ esta dada para por

$$T(\beta) = \sum_{i=1}^{n} \sigma_i(\beta) = \sum_{i=1}^{n} \sigma_i \left(\sum_{j=0}^{n-1} q_j\alpha^j \right) = \sum_{i=1}^{n} \left(\sum_{j=0}^{n-1} q_j\sigma_i\left(\alpha^j\right) \right) = \sum_{i=1}^{n} \left(\sum_{j=0}^{n-1} q_j\xi^{ij}\alpha^j \right) = n_0q_0 + \left(\sum_{i=1}^{n-1} q_i\alpha^i \right) \left(\sum_{i=0}^{n-1} \xi^i \right).$$

Proposición 2.2.2. *Sea $K(\alpha)/K$ una extensión finita y $\beta, \gamma \in K(\alpha)$. Entonces*

1) $N_{K(\alpha)/K}(\beta) = 0$ *si y sólo si* $\beta = 0$.
2) $Tr_{K(\alpha)/K}(\beta + \gamma) = Tr_{K(\alpha)/K}(\beta) + Tr_{K(\alpha)/K}(\gamma)$.
3) $N_{K(\alpha)/K}(\beta\gamma) = N_{K(\alpha)/K}(\beta)N_{K(\alpha)/K}(\gamma)$.
4) *Si* $\beta \in K$ *entonces* $N_{K(\alpha)/K}(\beta) = \beta^n$ *y* $Tr_{K(\alpha)/K}(\beta) = n\beta$.

Proposición 2.2.3. *Sea $K(\alpha)/K$ una extensión finita. Entonces $N_{K(\alpha)/K}(\alpha)$ y $T_{K(\alpha)/K}(\alpha)$ son elementos de K.*

Demostración. *Sea $f_\alpha(x) = \sum_{i=0}^{n} x^i a_i \in K[x]$ el polinomio mínimo de α sobre K y supongamos que $grad(f_\alpha(x)) = n$.*

Siendo que K es de característica 0, entonces por el Corolario 1.4.50 $f_\alpha(x)$ tiene n raíces distintas y luego por el Lema 1.4.37 la identidad en K se puede extender a n morfismos de campos de $K(\alpha)$ en $\overline{K}$, digamos $\sigma_1, \ldots, \sigma_n$. Ahora por la Proposición 1.4.34 tenemos que $\sigma_1(\alpha), \ldots, \sigma_n(\alpha)$ son las distintas raíces de f_α en $\overline{K}$. Por lo tanto $f_\alpha(x)$ se factoriza en $\overline{K}[x]$ como

$$f_\alpha(x) = (x - \sigma_1(\alpha)) \cdots (x - \sigma_n(\alpha)). \tag{2.1}$$

Ahora solo hay que notar que al hacer el producto de la factorización de $f_\alpha(x)$ dada en (2.1), obtenemos que $a_0 = \sigma_1(\alpha) \cdots \sigma_n(\alpha) = N_{K(\alpha)/K}(\alpha)$ y que $a_{n-1} = \sigma_1(\alpha) + \cdots + \sigma_n(\alpha) = T_{K(\alpha)/K}(\alpha)$, y como $f_\alpha(x) \in K[x]$, entonces $a_0, a_{n-1} \in K$. Así podemos concluir que $N_{K(\alpha)/K}(\alpha), T_{K(\alpha)/K}(\alpha) \in K$. ∎

Lema 2.2.4. *Sea $K(\alpha)/K$ una extensión finita y $\beta \in K(\alpha)$. Si $\overline{K}$ es la cerradura algebraica de K y $\varphi : K(\beta) \longrightarrow \overline{K}$ es un morfismo de campos, entonces el número de extensiones de φ a $K(\alpha)$ en $\overline{K}$ es $[K(\alpha) : K(\beta)]$.*

Demostración. *Sea $f_{\alpha,K(\beta)}(x)$ el polinomio mínimo de α sobre $K(\beta)$. Como K es de característica 0, por el Corolario 1.4.50, $f_{\alpha,K(\beta)}(x)$ tiene todas sus raíces distintas. Luego, del Lema 1.4.37, tenemos que el número de extensiones de φ a $K(\alpha)$ en $\overline{K}$, está dado por el grado de $f_{\alpha,K(\beta)}(x)$.*

Por otro lado, por el Corolario 1.4.22, se tiene que $grad(f_{\alpha,K(\beta)}(x)) = [(K(\beta))(\alpha) : K(\beta)]$. Ahora notemos que dado que $\beta \in K(\alpha)$, entonces $(K(\beta))(\alpha) = K(\alpha)$. Por lo tanto el número de extensiones de φ a $K(\alpha)$ en $\overline{K}$ es $[K(\alpha) : K(\beta)]$. ∎

Proposición 2.2.5. *Sea $K(\alpha)/K$ una extensión finita. Si $\beta \in K(\alpha)$, entonces*

1) $N_{K(\alpha)/K}(\beta) = \left(N_{K(\beta)/K}(\beta)\right)^{[K(\alpha):K(\beta)]}$.
2) $T_{K(\alpha)/K}(\beta) = [K(\alpha) : K(\beta)]\left(T_{K(\beta)/K}(\beta)\right)$.

Demostración. *Sea $f_\beta(x)$ el polinomio mínimo de β sobre K. Si $r = grad(f_\beta(x))$ y $\varphi_1, \ldots, \varphi_r$ son los morfismo de $K(\beta)$ en $\overline{K}$ que extienden al morfismo identidad $Id : K \longrightarrow K$. Tenemos que para $\gamma \in K(\beta)$*

$$N_{K(\beta)/K}(\gamma) = \prod_{i=1}^{r} \varphi_i(\gamma) \quad y \quad Tr_{K(\beta)/K}(\gamma) = \sum_{i=1}^{r} \varphi_i(\gamma) \tag{2.2}$$

Si hacemos $t = [K(\alpha) : K(\beta)]$, por el Lema 2.2.4, tenemos que para cada $i \in \{1, \ldots, r\}$, φ_i se extiende exactamente a t morfismos de $K(\alpha)$ en $\overline{K}$. Digamos que $\sigma_{i1}, \ldots, \sigma_{it}$ son las distintas extensiones de φ_i, entonces el conjunto

$$\{\sigma_{ij} \mid i = 1, \ldots, r \ \ y \ \ j = 1, \ldots, t\} \tag{2.3}$$

tiene rt elementos.

Por otro lado tenemos que el número de morfismo de $K(\alpha)$ en $\overline{K}$ que extienden a la identidad $Id : K \longrightarrow K$, esta dado por el grado del polinomio mínimo α sobre K, que por la Proposición 1.4.22 coincide con $[K(\alpha) : K]$. Además por la Proposición 1.4.2, se tiene que

$$[K(\alpha) : K] = [K(\alpha) : K(\beta)][K(\beta) : K] = tr,$$

y como cada morfismo dado en el conjunto descrito en (2.3) es una extensión del morfismo identidad $Id : K \longrightarrow K$. Podemos concluir que los morfismos de $K(\beta)$ en $\overline{K}$ que extienden al morfismo

identidad $Id : K \longrightarrow K$ son precisamente los morfismos dado en el conjunto descrito en (2.3). Y entonces si $\gamma \in K(\beta)$, tenemos que

$$N_{K(\alpha)/K}(\gamma) = \prod_{i=1}^{r}\left(\prod_{j=1}^{t}\sigma_{ij}(\gamma)\right) \quad y \quad Tr_{K(\alpha)/K}(\gamma) = \sum_{i=1}^{r}\left(\sum_{j=1}^{t}\sigma_{ij}(\gamma)\right) \tag{2.4}$$

Luego en particular para β tenemos que

$$N_{K(\alpha)/K}(\beta) = \prod_{i=1}^{r}\left(\prod_{j=1}^{t}\sigma_{ij}(\beta)\right) \underset{\sigma_{ij}|_{K(\beta)}=\varphi_i}{=} \prod_{i=1}^{r}(\varphi_i(\beta)^t) \underset{t=[K(\alpha):K(\beta)]}{=} \left(\prod_{i=1}^{r}\varphi(\beta)\right)^{[K(\alpha):K(\beta)]} \underset{De\ (1)}{=} \left(N_{K(\beta)/K}(\beta)\right)^{[K(\alpha):K(\beta)]}.$$

$$T_{K(\alpha)/K}(\beta) = \sum_{i=1}^{r}\left(\sum_{j=1}^{t}\sigma_{ij}(\beta)\right) \underset{\sigma_{ij}|_{K(\beta)}=\varphi_i}{=} \sum_{i=1}^{r}(t\varphi_i(\beta)) \underset{t=[K(\alpha):K(\beta)]}{=} [K(\alpha):K(\beta)]\left(\prod_{i=1}^{r}\varphi(\beta)\right) \underset{De\ (1)}{=} [K(\alpha):K(\beta)]\left(T_{K(\beta)/K}(\beta)\right).$$

Lo que concluye la demostración. ∎

Corolario 2.2.6. *Sea $K(\alpha)/K$ una extensión finita. Si $\beta \in K(\alpha)$, entonces $N_{K(\alpha)/K}(\beta)$ y $T_{K(\alpha)/K}(\beta)$ son elementos de K. (Ver Proposiciones 2.2.3 y 2.2.5)*

Proposición 2.2.7. *Sean D un dominio entero, K un campo que contiene a D y $K(\alpha)/K$ una extensión finita. Si $\beta \in K(\alpha)$ es un entero algebraico sobre D, entonces $N_{K(\alpha)/K}(\beta)$ y $T_{K(\alpha)/K}(\beta)$ son enteros algebraicos sobre D.*

Demostración. *Como β es entero algebraico sobre D, entonces existe $f(x) \in D[x]$ polinomio mónico tal que β es una raíz de $f(x)$.*

Ahora, supongamos que $[K(\alpha) : K] = n$ y sean $\sigma_1, \ldots, \sigma_n$ los distintos morfismo de $K(\alpha)$ en $\overline{K}$ que extienden a la identidad $Id : K \longrightarrow K$. Por la proposición 2.4.33, para cada $i \in \{1, \ldots, n\}$, σ_i induce un morfismo $\widetilde{\sigma}_i : K[x] \longrightarrow \overline{K}[x]$ tal que $\widetilde{\sigma}_i\,|_K = \sigma_i$ y $\widetilde{\sigma}_i(x) = x$. Notemos que bajo estas condiciones $\widetilde{\sigma}_i(f(x)) = f(x)$ para todo $i \in \{1, \ldots, n\}$, pues $D \subseteq K$.

Dado que β es una raíz de $f(x)$, de la Proposición 1.4.34 tenemos que $\sigma_i(\beta)$ es una raíz de $\widetilde{\sigma}_i(f(x)) = f(x)$, y como $f(x) \in D[x]$ y es un polinomio mónico, entonces tenemos que $\sigma_i(\beta)$ es un entero algebraico sobre D para $i = 1, \ldots, n$.

Recordemos que

$$N_{K(\alpha)/K}(\beta) = \prod_{i=1}^{r}\sigma_i(\beta) \quad y \quad Tr_{K(\alpha)/K}(\beta) = \sum_{i=1}^{r}\sigma_i(\beta).$$

Entonces por el Corolario 2.1.10 podemos concluir que $N_{K(\alpha)/K}(\beta)$ y $T_{K(\alpha)/K}(\beta)$ son enteros algebraicos sobre D. ∎

Corolario 2.2.8. *Sean D un dominio entero con campo de cociente Q y $Q(\alpha)/Q$ una extensión finita. Si $\beta \in Q(\alpha)$ es un entero algebraico sobre D y D es enteramente cerrado, entonces $N(\beta), T(\beta) \in D$.*

Proposición 2.2.9. *Sean D un dominio entero con campo de cociente Q, $Q(\alpha)/Q$ una extensión finita de grado n y D' el anillo de enteros algebraicos de $Q(\alpha)$ sobre D. Si $\beta, \gamma \in D'$ y D es enteramente cerrado, entonces*

1) *$\beta \in U(D')$ si y sólo si $N(\beta) \in U(D)$.*
2) *Si β y γ son asociados en D' entonces $N(\beta)$ y $N(\gamma)$ son asociados en D.*
3) *Si $N(\beta)$ es irreducible en D, entonces β es irreducible en D'.*

Demostración.

1)

⇒) *Supongamos que* $\beta \in U(D')$. *Entonces* $\beta\delta = 1$ *para algún* $\delta \in U(D')$. *Como* D *es enteramente cerrado, por el Corolario 2.2.8 se tiene que* $N(\beta), N(\delta) \in D$.
Por otro lado

$$N(\beta)N(\delta) = N(\beta\delta) = N(1) = 1.$$

En consecuencia tenemos que $N(\beta) \in U(D)$.

⇐) *Supongamos que* $\beta \in D'$ *y es tal que* $N(\beta) \in U(D)$. *Sean* $\sigma_1, , \sigma_n$ *los n distintos morfismos de campos de* $Q(\alpha)$ *en* $\overline{Q}$ *que extienden a la identidad y recordemos que por definición*

$$N(\beta) = \prod_{i=1}^{n} \sigma_i(\beta)$$

Como para alguna $i \in \{1, \ldots, n\}$, $\sigma_i = Id : Q(\alpha) \longrightarrow Q(\alpha)$, *sin perdida de generalidad podemos suponer que* $\sigma_1 = Id_{Q(\alpha)}$ *y entonces*

$$N(\beta) = \beta \prod_{i=2}^{n} \sigma_i(\beta).$$

Ahora por hipótesis $N(\beta) \in U(D)$, *entonces existe* $\delta \in D$ *tal que*

$$\beta \left(\prod_{i=2}^{n} \sigma_i(\beta)\delta \right) = 1$$

Como $\beta \in D'$, *entonces* β *es un entero algebraico sobre* D. *Ya se vio durante la demostración de la Proposición 2.2.7 que* $\sigma_i(\beta)$ *es un entero algebraico sobre* D *para* $i \in \{2, \ldots, n\}$ *y claramente* $\delta \in D'$. *Entonces por el Corolario 2.1.9 se tiene que* $\prod_{i=2}^{n} \sigma_i(\beta)\delta \in D'$. *Por lo tanto* $\beta \in U(D')$.

2) Supongamos que β *es asociado a* γ *en* D'. *Entonces existe* $\delta \in U(D')$ *tal que* $\beta = \delta\gamma$. *Luego por la Proposición 2.2.2 se tiene que*

$$N(\beta) = N(\delta\gamma) = N(\delta)N(\gamma).$$

Donde por el inciso (1) *de este Teorema se tiene que* $N(\delta) \in U(D)$. *Por lo tanto* $N(\beta)$ *y* $N(\gamma)$ *son asociados en* D.

3) Supongamos que $N(\beta) \in D$ *es irreducible en* D *y que* $\beta = \gamma\delta$ *con* $\gamma, \delta \in D'$. *Como*

$$N(\beta) = N(\gamma\delta) = N(\gamma)N(\delta).$$

Siendo que D *es enteramente cerrado, del Corolario 2.2.8 tenemos que*

$$N(\gamma), N(\delta) \in D.$$

Ahora por hipótesis $N(\beta)$ *es irreducible en* D. *Entonces* $N(\gamma) \in U(D)$ *o* $N(\delta) \in U(D)$ *y es por el inciso* (1) *de este teorema tenemos que* $\gamma \in U(D')$ *o* $\delta \in U(D')$. *Por lo tanto* β *es irreducible en* D'. ∎

Sea $K(\alpha)/K$ *una extensión finita de grado n y sean* $\sigma_1, \ldots, \sigma_n$ *los distintos morfismo de* $K(\alpha)$ *en* $\overline{K}$. *Si* $\{\alpha_1, \ldots, \alpha_n\} \subseteq K(\alpha)$, *el* ***discriminate*** *de* $\{\alpha_1, \ldots, \alpha_n\}$ *esta dado por*

$$\Delta[\alpha_1, \ldots, \alpha_n] = \left[\det(\sigma_i(\alpha_j))\right]^2. \tag{2.5}$$

Si $\beta = \{\beta_1, \ldots, \beta_n\}$ *es una base* F *sobre* K, *entonces par todo* $k \in \{1, \ldots, n\}$ *se tiene que*

$$\alpha_k = \sum_{j=1}^{n} c_{kj}\beta_j \quad con \quad c_k j \in K. \tag{2.6}$$

Luego

$$\begin{aligned}
\Delta[\alpha_1,\ldots,\alpha_n] &\underset{Por\ \ def.\ \ (2,6)}{=} \left(\det\begin{pmatrix}\sigma_1(\alpha_1) & \ldots & \sigma_1(\alpha_n)\\ \vdots & & \vdots\\ \sigma_n(\alpha_1) & \ldots & \sigma_n(\alpha_n)\end{pmatrix}\right)^2\\
&\underset{Sustituyendo\ \ (2,7)}{=} \left(\det\begin{pmatrix}\sigma_1(\sum_{j=1}^n c_{1j}\beta_j) & \ldots & \sigma_1(\sum_{j=1}^n c_{nj}\beta_j)\\ \vdots & & \vdots\\ \sigma_n(\sum_{j=1}^n c_{1j}\beta_j) & \ldots & \sigma_n(\sum_{j=1}^n c_{nj}\beta_j)\end{pmatrix}\right)^2\\
&\underset{\sigma_i\ \ son\ \ morfismos}{=} \left(\det\begin{pmatrix}\sum_{j=1}^n c_{1j}\sigma_1(\beta_j) & \ldots & \sum_{j=1}^n c_{nj}\sigma_1(\beta_j)\\ \vdots & & \vdots\\ \sum_{j=1}^n c_{1j}\sigma_n(\beta_j) & \ldots & \sum_{j=1}^n c_{nj}\sigma_n(\beta_j)\end{pmatrix}\right)^2\\
&= \left[\det\left(\begin{pmatrix}\sigma_1(\beta_1) & \ldots & \sigma_1(\beta_n)\\ \vdots & & \vdots\\ \sigma_n(\beta_1) & \ldots & \sigma_n(\beta_n)\end{pmatrix}\begin{pmatrix}c_{11} & \ldots & c_{n1}\\ \vdots & & \vdots\\ c_{1n} & \ldots & c_{nn}\end{pmatrix}\right)\right]^2\\
&\underset{Propiedad\ \ del\ \ det}{=} \left[\det\begin{pmatrix}\sigma_1(\beta_1) & \ldots & \sigma_1(\beta_n)\\ \vdots & & \vdots\\ \sigma_n(\beta_1) & \ldots & \sigma_n(\beta_n)\end{pmatrix}\det\begin{pmatrix}c_{11} & \ldots & c_{n1}\\ \vdots & & \vdots\\ c_{1n} & \ldots & c_{nn}\end{pmatrix}\right]^2\\
&\underset{det(A)=det(A^t)}{=} \left[\det\begin{pmatrix}\sigma_1(\beta_1) & \ldots & \sigma_1(\beta_n)\\ \vdots & & \vdots\\ \sigma_n(\beta_1) & \ldots & \sigma_n(\beta_n)\end{pmatrix}\det\begin{pmatrix}c_{11} & \ldots & c_{1n}\\ \vdots & & \vdots\\ c_{n1} & \ldots & c_{nn}\end{pmatrix}\right]^2\\
&= \left[\det\begin{pmatrix}\sigma_1(\beta_1) & \ldots & \sigma_1(\beta_n)\\ \vdots & & \vdots\\ \sigma_n(\beta_1) & \ldots & \sigma_n(\beta_n)\end{pmatrix}\right]^2\left[\det\begin{pmatrix}c_{11} & \ldots & c_{1n}\\ \vdots & & \vdots\\ c_{n1} & \ldots & c_{nn}\end{pmatrix}\right]^2\\
&= (\det(c_{kj}))^2\,\Delta[\beta_1,\ldots,\beta_n]
\end{aligned}$$

Proposición 2.2.10. *Sea $K(\alpha)/K$ una extensión finita de grado n. Si $\alpha_1,\ldots,\alpha_n$ y $\beta_1,\ldots,\beta_n$ son bases de $K(\alpha)$ sobre K, entonces $\Delta[\alpha_1,\ldots,\alpha_n] = (\det(c_{kj}))^2\,\Delta[\beta_1,\ldots,\beta_n]$ donde (c_{kj}) es la matriz de cambio de base de la base $\alpha_1,\ldots,\alpha_n$ en la base $\beta_1,\ldots,\beta_n$.*

Proposición 2.2.11. *Sean D un dominio entero con campo de cocientes Q y $Q(\alpha)/Q$ una extensión finita y sea D' la cerradura entera de D en $Q(\alpha)$. Entonces existe $q \in D - \{0\}$ tal que $q\beta \in D'$.*

Demostración. *Como β es algebraico sobre Q, existen $\frac{p_{n-1}}{a_{n-1}},\ldots,\frac{p_0}{q_0} \in Q$ con $p_i, q_j \in D$ y $q_i \neq 0$ para $i = 1,\ldots,n-1$, tales que*

$$\beta^n + \frac{p_{n-1}}{q_{n-1}}\beta^{n-1}\cdots + \frac{p_1}{q_1}\beta + \frac{p_0}{q_0} = 0. \tag{2.7}$$

Sea $q = \prod_{i=i}^n q_i$, dado que $q_i \neq 0$ para $i = 1,\ldots,n-1$ y que D es un dominio entero tenemos que $q \neq 0$.

Multiplicando (2.7) por q^n se tiene que

$$q^n\beta^n + q^n\frac{p_{n-1}}{q_{n-1}}\beta^{n-1}\cdots + q^n\frac{p_1}{q_1}\beta + q^n\frac{p_0}{q_0} = 0,$$

de donde

$$(q\beta)^n + q\frac{p_{n-1}}{q_{n-1}}(q\beta)^{n-1} \cdots + q^{n-1}\frac{p_1}{q_1}(q\beta) + q^n\frac{p_0}{q_0} = 0,$$

con $q^j\frac{p_{n-j}}{q_{n-j}} \in D$ *pues* $q_{n-j} \mid q^j$ *para cada* $j \in \{0,\ldots,n-1\}$. *Por lo tanto* $q\beta \in D'$. ∎

Corolario 2.2.12. *Sean D un dominio entero con campo de cociente Q,* $Q(\alpha)/Q$ *una extensión finita y* D' *la cerradura entera de D en* $Q(\alpha)$. *Entonces* $Q(\alpha) = Q(\beta)$ *para algún* $\beta \in D'$.

Demostración. *Como* $Q(\alpha)/Q$ *es una extensión finita, por la Proposición 2.4.25* α *es algebraico sobre Q. Luego de la Proposición 2.2.11 existe* $q \in D - \{0\}$ *tal que* $q\alpha \in D'$.

Tomemos $f_{q\alpha}(x) = a_0 + a_1x + \cdots + a_{n-1}x^{n-1} + x^n \in Q[x]$ *el polinomio mínimo de* $q\alpha$ *sobre Q. De la Proposición 1.4.22, tenemos que* $[Q(q\alpha) : Q] = n$. *Ahora, por la Proposición 1.4.2, sabemos que* $[Q(\alpha) : Q] = [Q(\alpha) : Q(q\alpha)][Q(q\alpha) : Q]$ *y entonces tenemos que* $n \leqslant [Q(\alpha) : Q]$. *Como* $q\alpha$ *es raíz de* $f_{q\alpha}(x)$, *entonces*

$$a_0 + a_1(q\alpha) + \cdots + a_{n-1}(q\alpha)^{n-1} + (q\alpha)^n = 0,$$

de donde

$$a_0 + a_1q(\alpha) + \cdots + a_{n-1}q^{n-1}\alpha^{n-1} + q^n\alpha^n = 0. \tag{2.8}$$

Siendo que $q \neq 0$, *podemos dividir la igualdad dada en (2.8) por* q^n *y obtener que*

$$\frac{1}{q^n}a_0 + \frac{1}{q^{n-1}}a_1(\alpha) + \cdots + \frac{1}{q}a_{n-1}\alpha^{n-1} + \alpha^n = 0$$

Así si consideramos el polinomio $g(x) = \frac{a_0}{q^n} + \frac{a_1}{q^{n-1}}x + \cdots + \frac{a_{n-1}}{q}x^{n-1} + x^n \in Q[x]$, *tenemos que* α *es una raíz de* $g(x)$ *y entonces el grado del polinomio mínimo de* α *sobre Q es menor o igual que n. Luego por la Proposición 1.4.22 concluimos que* $[Q(\alpha) : Q] \leqslant n$. *Por lo tanto* $[Q(\alpha) : Q] = [Q(q\alpha) : Q]$ *y en consecuencia* $[Q(\alpha) : Q(q\alpha)] = 1$. *De donde tenemos que* $Q(\alpha) = Q(q\alpha)$. ∎

Corolario 2.2.13. *Sean D un dominio entero con campo de cociente Q,* $Q(\alpha)/Q$ *una extensión finita y* D' *la cerradura entera de D en* $Q(\alpha)$. *Entonces existe* $\beta \in D'$ *tal que* $\{1,\beta,\ldots,\beta^{n-1}\}$ *es una base de* $Q(\alpha)$ *sobre Q. (Ver Proposición 1.4.22)*

Definición 2.2.14. *Sean D un dominio entero con campo de cocientes Q,* $Q(\alpha)/Q$ *una extensión finita de grado n y* D' *la cerradura entera de D en* $Q(\alpha)$. *Una base* $\{\alpha_1,\alpha_2,\ldots,\alpha_n\}$ *de* $Q(\alpha)$ *sobre Q es una* ***base entera*** *si* $\{\alpha_1,\alpha_2,\ldots,\alpha_n\} \subseteq D'$.

Si K es un campo y $\alpha = \{\alpha_1,\ldots,\alpha_n\} \subseteq K$, *se define la* ***matriz de Vandermonde*** *de* α *por*

$$M_\alpha = \begin{pmatrix} 1 & \alpha_1 & \alpha_1^2 & \ldots & \alpha_1^{n-1} \\ 1 & \alpha_2 & \alpha_2^2 & \ldots & \alpha_2^{n-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \alpha_n & \alpha_n^2 & \ldots & \alpha_n^{n-1} \end{pmatrix}$$

Proposición 2.2.15. *Sean K un campo y* $\alpha = \{\alpha_1,\ldots,\alpha_n\} \subseteq K$. *Entonces* $det(M_\alpha) = \prod_{i<j}(\alpha_i - \alpha_j)$

Demostración. *La demostración se hará por inducción sobre n. Para* $n = 1$ *tenemos que la matriz de Vandermonde esta dada por la matriz* (1). *Por otro lado* $\prod_{i<j}(\alpha_i - \alpha_j)$ *es el producto vacío y por lo tanto es la unidad de L, lo que muestra la aserción.*

Supongamos que la proposición es válida para todo $k < n$ *y sea* $\alpha = \{\alpha_1,\ldots,\alpha_n\} \subseteq L$ *y* M_α *la matrix de Vandermonde de* α.

Consideremos la siguiente matriz en $M_n(K[x])$

$$M(x) = \begin{pmatrix} 1 & x & x^2 & \dots & x^{n-1} \\ 1 & \alpha_2 & \alpha_2^2 & \dots & \alpha_2^{n-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \alpha_n & \alpha_n^2 & \dots & \alpha_n^{n-1} \end{pmatrix}$$

Notemos que $det(M(x))$ *es un polinomio* $f(x) \in K[x]$ *de grado* $n-1$*, cuyo coeficiente principal* a_{n-1} *es precisamente el determinante del menor* $(1,n)$ *de la matriz* $M(x)$*, que está dado por*

$$det(\widehat{M_\alpha(x)}_{1n}) = det \begin{pmatrix} 1 & \alpha_2 & \alpha_2^2 & \dots & \alpha_2^{n-2} \\ 1 & \alpha_3 & \alpha_3^2 & \dots & \alpha_3^{n-2} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \alpha_n & \alpha_n^2 & \dots & \alpha_n^{n-2} \end{pmatrix}$$

Ahora $\widehat{M_\alpha(x)}_{1n}$ *es la matriz de Vandermonde del conjunto* $\{\alpha_2, \dots, \alpha_n\}$*, luego entonces por hipótesis de inducción* $a_{n-1} = det(\widehat{M_\alpha(x)}_{1n}) = \prod_{i<j}(\alpha_i - \alpha_j)$ *con* $i, j \in \{2, \dots, n\}$.

Por otro lado tenemos que $f(\alpha_i) = det(M_\alpha(\alpha_i)) = 0$ *para cada* $i \in \{2, \dots, n\}$*. Dado que el grado de* $f(x)$ *es* $n-1$*, entonces* $\alpha_2, \dots, \alpha_n$ *son todas las raíces de* $f(x)$*, y así se tiene que* $f(x)$ *se factoriza en* $\overline{K}[x]$ *como:*

$$f(x) = a_{n-1}(x - \alpha_2) \cdots (x - \alpha_n).$$

Por último como $det(M(x)) = f(x)$*, entonces tenemos que*

$$det(M_\alpha) = f(\alpha_1) = a_{n-1}(\alpha_1 - \alpha_2) \cdots (\alpha_1 - \alpha_n) = \prod_{i<j}(\alpha_i - \alpha_j). \qquad \blacksquare$$

Lema 2.2.16. *Sea* K *un campo,* F *una extensión de* K *y* $\alpha \in F$ *algebraico sobre* K*. Si* $[K(\alpha) : K] = n$ *y* $\{\alpha_1, \dots, \alpha_n\} \subseteq K(\alpha)$*, entonces* $\Delta[\alpha_1, \dots, \alpha_n] = det(Tr(\alpha_i \alpha_j))$.

Demostración.

$$\Delta[\alpha_1, \dots, \alpha_n] \underset{Por\ def.\ (1)}{=} \left(\det \begin{pmatrix} \sigma_1(\alpha_1) & \sigma_1(\alpha_2) & \dots & \sigma_1(\alpha_n) \\ \sigma_2(\alpha_1) & \sigma_2(\alpha_2) & \dots & \sigma_2(\alpha_n) \\ \vdots & \vdots & & \vdots \\ \sigma_n(\alpha_1) & \sigma_n(\alpha_2) & \dots & \sigma_n(\alpha_n) \end{pmatrix} \right)^2$$

$$= \det \begin{pmatrix} \sigma_1(\alpha_1) & \sigma_1(\alpha_2) & \dots & \sigma_1(\alpha_n) \\ \sigma_2(\alpha_1) & \sigma_2(\alpha_2) & \dots & \sigma_2(\alpha_n) \\ \vdots & \vdots & & \vdots \\ \sigma_n(\alpha_1) & \sigma_n(\alpha_2) & \dots & \sigma_n(\alpha_n) \end{pmatrix} \det \begin{pmatrix} \sigma_1(\alpha_1) & \sigma_1(\alpha_2) & \dots & \sigma_1(\alpha_n) \\ \sigma_2(\alpha_1) & \sigma_2(\alpha_2) & \dots & \sigma_2(\alpha_n) \\ \vdots & \vdots & & \vdots \\ \sigma_n(\alpha_1) & \sigma_n(\alpha_2) & \dots & \sigma_n(\alpha_n) \end{pmatrix}$$

$$
\begin{aligned}
&\underset{det(A)=det(A^t)}{=} && \det\begin{pmatrix} \sigma_1(\alpha_1) & \sigma_2(\alpha_1) & \dots & \sigma_n(\alpha_1) \\ \sigma_1(\alpha_2) & \sigma_2(\alpha_2) & \dots & \sigma_n(\alpha_2) \\ \vdots & \vdots & & \vdots \\ \sigma_1(\alpha_n) & \sigma_2(\alpha_n) & \dots & \sigma_n(\alpha_n) \end{pmatrix} \det\begin{pmatrix} \sigma_1(\alpha_1) & \sigma_1(\alpha_2) & \dots & \sigma_1(\alpha_n) \\ \sigma_2(\alpha_1) & \sigma_2(\alpha_2) & \dots & \sigma_2(\alpha_n) \\ \vdots & & & \vdots \\ \sigma_n(\alpha_1) & \sigma_n(\alpha_2) & \dots & \sigma_n(\alpha_n) \end{pmatrix} \\
&\underset{Propiedad\ \ del\ \ det}{=} && \det\left(\begin{pmatrix} \sigma_1(\alpha_1) & \sigma_2(\alpha_1) & \dots & \sigma_n(\alpha_1) \\ \sigma_1(\alpha_2) & \sigma_2(\alpha_2) & \dots & \sigma_n(\alpha_2) \\ \vdots & \vdots & & \vdots \\ \sigma_1(\alpha_n) & \sigma_2(\alpha_n) & \dots & \sigma_n(\alpha_n) \end{pmatrix}\begin{pmatrix} \sigma_1(\alpha_1) & \sigma_1(\alpha_2) & \dots & \sigma_1(\alpha_n) \\ \sigma_2(\alpha_1) & \sigma_2(\alpha_2) & \dots & \sigma_2(\alpha_n) \\ \vdots & & & \vdots \\ \sigma_n(\alpha_1) & \sigma_n(\alpha_2) & \dots & \sigma_n(\alpha_n) \end{pmatrix}\right) \\
&= && \det\begin{pmatrix} \sum_{j=1}^n \sigma_k(\alpha_1)\sigma_k(\alpha_1) & \sum_{j=1}^n \sigma_k(\alpha_1)\sigma_k(\alpha_2) & \dots & \sum_{j=1}^n \sigma_k(\alpha_1)\sigma_k(\alpha_n) \\ \sum_{j=1}^n \sigma_k(\alpha_2)\sigma_k(\alpha_1) & \sum_{j=1}^n \sigma_k(\alpha_2)\sigma_k(\alpha_2) & \dots & \sum_{j=1}^n \sigma_k(\alpha_2)\sigma_k(\alpha_n) \\ \vdots & \vdots & & \vdots \\ \sum_{j=1}^n \sigma_k(\alpha_n)\sigma_k(\alpha_1) & \sum_{j=1}^n \sigma_k(\alpha_2)\sigma_k(\alpha_2) & \dots & \sum_{j=1}^n \sigma_k(\alpha_n)\sigma_k(\alpha_n) \end{pmatrix} \\
&\underset{\sigma_i\ \ es\ \ morfismo}{=} && \det\begin{pmatrix} \sum_{j=1}^n \sigma_k(\alpha_1\alpha_1) & \sum_{j=1}^n \sigma_k(\alpha_1\alpha_2) & \dots & \sum_{j=1}^n \sigma_k(\alpha_1\alpha_n) \\ \sum_{j=1}^n \sigma_k(\alpha_2\alpha_1) & \sum_{j=1}^n \sigma_k(\alpha_2\alpha_2) & \dots & \sum_{j=1}^n \sigma_k(\alpha_2\alpha_n) \\ \vdots & \vdots & & \vdots \\ \sum_{j=1}^n \sigma_k(\alpha_n\alpha_1) & \sum_{j=1}^n \sigma_k(\alpha_2\alpha_2) & \dots & \sum_{j=1}^n \sigma_k(\alpha_n\alpha_n) \end{pmatrix} \\
&= && \det(Tr(\alpha_i\alpha_j)).
\end{aligned}
$$

■

Corolario 2.2.17. *Sean D un dominio entero con campo de cocientes Q, $Q(\alpha)/Q$ una extensión finita de grado n, D' la cerradura entera de D en $Q(\alpha)$ y $\{\alpha_1,\dots,\alpha_n\}$ una base de D'. Entonces $\Delta[\alpha_1,\dots,\alpha_n] \in D'$.*

Teorema 2.2.18. *Sean D un dominio entero con campo de cocientes Q, $Q(\alpha)/Q$ una extensión finita de grado n y D' la cerradura entera de D en $Q(\alpha)$. Entonces el discriminante de una base de $Q(\alpha)$ sobre Q es un elemento no nulo de Q.*

Demostración. *Sean $\sigma_1,\dots,\sigma_n$ los distintos morfismo de $Q(\alpha)$ en $\overline{Q}$ que extienden a la identidad $Id : Q \longrightarrow Q$.*

Por el Corolario 2.2.12 existe $\vartheta \in D'$ tal que $Q(\alpha) = Q(\vartheta)$, entonces tenemos por el Corolario 2.2.13 que $\{1,\vartheta,\dots,\vartheta^{n-1}\}$ una base entera de $Q(\alpha)$ sobre Q. Primero mostraremos que el discriminante de $\{1,\vartheta,\dots,\vartheta^{n-1}\}$ es un elemento de Q.

Si hacemos $\theta_i = \sigma_i(\vartheta)$, entonces

$$\Delta[1,\vartheta,\dots,\vartheta^{n-1}] = \det\begin{pmatrix} 1 & \theta_1 & \theta_1^2 & \dots & \theta_1^{n-1} \\ \vdots & & \vdots & & \\ 1 & \theta_n & \theta_n^2 & \dots & \theta_n^{n-1} \end{pmatrix}.$$

Es decir $\Delta[1,\vartheta,\dots,\vartheta^{n-1}]$ es el determinante de Vandermonde del conjunto $\{\theta_1,\dots,\theta_n\}$ y así por la Proposición 2.2.15, tenemos que

$$\Delta[1,\vartheta,\dots,\vartheta^{n-1}] = \left(\prod_{i<j}(\theta_i - \theta_j)\right).$$

Ahora por el Corolario 1.4.50 tenemos que $f_\vartheta(x)$ tiene n raíces distintas y del Lema 1.4.37 tenemos que θ_i son las n raíces distintas de $f_\vartheta(x)$. Luego entonces se tiene que $\Delta[1,\vartheta,\dots,\vartheta^{n-1}] \neq 0$.

Por otro lado, como ϑ es entero algebraico sobre D, por el Corolario 2.1.9 tenemos que ϑ^i es entero algebraico sobre D para todo $i \in \mathbb{N}$. Entonces por el Corolario 2.2.6 $Tr(\vartheta^i\vartheta^j) \in Q$ y así por el Lema 2.2.16, podemos concluir que $\Delta[1,\vartheta,\dots,\vartheta^{n-1}] = det(Tr(\vartheta^i\vartheta^j)) \in Q$.

Ahora consideremos $\{\alpha_1, \ldots, \alpha_n\}$ una base de $Q(\alpha)$ sobre Q, por la Proposición 2.2.10 tenemos que

$$\Delta[\alpha_1, \ldots, \alpha_n] = (\det(c_{kj}))^2 \, \Delta[1, \vartheta, \ldots, \vartheta^{n-1}]$$

donde (c_{kj}) es la matriz de cambio de base de la base $\alpha_1, \ldots, \alpha_n$ en la base $1, \vartheta, \ldots, \vartheta^{n-1}$. Claramente $\det(c_{kj})^2 \in Q - \{0\}$ y además $\Delta[1, \vartheta, \ldots, \vartheta^{n-1}] \in Q - \{0\}$. Por lo tanto $\Delta[\alpha_1, \ldots, \alpha_n] \in Q - \{0\}$. ∎

Corolario 2.2.19. *Sean D un dominio entero con campo de cocientes Q, $Q(\alpha)/Q$ una extensión finita de grado n, D' la cerradura entera de D en $Q(\alpha)$ y $\{\alpha_1, \ldots, \alpha_n\}$ y $\{\beta_1, \ldots, \beta_n\}$ dos bases de D'. Entonces $\Delta[\alpha_1, \ldots, \alpha_n]$ y $\Delta[\beta_1, \ldots, \beta_n]$ son asociados en D.*

Corolario 2.2.20. *Sean D un dominio entero con campo de cocientes Q, $Q(\alpha)/Q$ una extensión finita de grado n. Si $\beta \in Q(\alpha)$ es tal que $Tr(\beta y) = 0$ para todo $y \in Q$, entonces $\alpha = 0$.*

Demostración. *Procedamos reducción al absurdo. Para ello supongamos que $\beta \neq 0$, del álgebra lineal sabemos que existe $\{\beta = \beta_1, \ldots, \beta_n\}$ una base de $Q(\alpha)$ sobre Q. Por el Lema 2.2.16 tenemos que*

$$\Delta[\beta_1, \ldots, \beta_n] = det(Tr(\beta_i \beta_j)) = 0 \;\; pues \;\; Tr(\beta y) = 0 \;\; para \;\; todo \;\; y \in Q.$$

Esto nos lleva a un absurdo con el Teorema 2.2.18. Por lo tanto $\beta = 0$. ∎

Observación 2.2.21. Sean D un dominio entero con campo de cociente Q, $Q(\alpha)/Q$ una extensión finita de grado n. Si $\theta \in Q(\alpha)$, claramente la función

$$Tr(\theta \cdot \_) : Q(\alpha) \longrightarrow Q \;\; dada \;\; por \;\; Tr(\theta \cdot \_)(y) = Tr(\theta y) \;\; para \;\; todo \;\; y \in Q(\alpha)$$

es una transformación Q-lineal.

Entonces podemos considerar la transformación lineal

$$\varphi : Q(\alpha) \longrightarrow Hom(Q(\alpha), Q) \;\; dada \;\; por \;\; \varphi(\theta) = Tr(\alpha \cdot \_) \;\; para \;\; todo \;\; \theta \in Q(\alpha)$$

Por el Corolario 2.2.20 tenemos que φ es inyectiva. Además como $dim_Q(Q(\alpha))$ es finita, entonces $dim_Q(Q(\alpha)) = dim_Q(Hom(Q(\alpha), Q))$ y por lo tanto φ es un isomorfismo de espacios vectoriales. Así, si $\{\alpha_1, \ldots, \alpha_n\}$ es una base de $Q(\alpha)$ sobre Q, entonces $\{Tr(\alpha_1 \cdot \_), \ldots, Tr(\alpha_n \cdot \_)\}$ es una base de $Hom(Q(\alpha), Q)$ sobre $Q(\alpha)$.

Por otro, tenemos que para cada $\theta \in Q(\alpha)$ se puede definir la transformación lineal $ev_\theta : Hom(Q(\alpha), Q) \longrightarrow Q$ dada por $ev_\theta(\varphi) = \varphi(\theta)$ para todo $\varphi \in Hom(Q(\alpha), Q)$.

Y entonces podemos definir la transformación lineal

$$ev : Q(\alpha) \longrightarrow Hom(Hom(Q(\alpha), Q), Q) \;\; dada \;\; por \;\; ev(\theta) = ev_\theta \;\; para \;\; todo \;\; \theta \in Q(\alpha).$$

Como el núcleo de ev es el cero y $dim_Q(Q(\alpha))$ es finita tenemos que ev es un isomorfismo de espacios vectoriales.

Así, si $\{Tr(\alpha_1 \cdot \_), \ldots, Tr(\alpha_n \cdot \_)\}$ es una base de $Hom(Q(\alpha), Q)$, por el Teorema de Existencia de Bases para el espacio dual[3] existe $\{\beta_1, \ldots, \beta_n\}$ base de Q tal que $Tr(\alpha_i \beta_j) = \delta_{ij}$[4].

Teorema 2.2.22. *Sean D un dominio entero enteramente cerrado con campo de cociente Q, $Q(\alpha)/Q$ una extensión finita de grado n y D' la cerradura entera de D en $Q(\alpha)$. Entonces D' es un D-submódulo de un D-módulo libre de rango n.*

---

[3] Sea V es un K-espacio vectorial y $\{v_1, \ldots, v_n\}$ con $n \in \mathbb{Z}^+$ es una base de V sobre K. Si para cada $i \in \{1, \ldots, n\}$ definimos $f_i : V \longrightarrow K$ por $f_i(v_j) = \delta_{ij}$, entonces $\{f_1, \ldots, f_n\}$ es una base del dual de V.

[4] La función Delta de Kronecker esta dada por $\delta_{ij} = \begin{cases} 0 & si\ i \neq j \\ 1 & si\ i = j \end{cases}$.

Demostración. *Sea $\{\alpha_1,\dots,\alpha_n\}$ una base entera de $Q(\alpha)$ sobre Q.*

Por la Observación 2.2.21, existe una base $\beta=\{\beta_1,\dots,\beta_n\}$ de $Q(\alpha)$ sobre Q, tal que $Tr(\alpha_i\beta_j)=\delta_{ij}$. Ahora, si $z\in D'$ como β es una base de $Q(\alpha)$ sobre Q, entonces podemos escribir $z=\sum_{i=1}^n b_i\beta_i$, con $b_i\in Q$ para todo $i\in\{1,\dots,n\}$. A continuación vamos a mostrar que $b_i\in D$ para todo $i\in\{1,\dots,n\}$.

Notemos que para todo $k\in\{1,\dots,n\}$

$$Tr(\alpha_k z)=Tr\left(\alpha_k\sum_{i=1}^n b_i\beta_i\right)=Tr\left(\sum_{i=1}^n b_i\alpha_k\beta_i\right)\underset{Tr(\alpha_i\beta_j)=\delta_{ij}}{=}\sum_{i=1}^n b_i Tr(\alpha_k\beta_i)=b_k.$$

Ahora, como $\alpha_k z\in D'$ y puesto que D es enteramente cerrado, por el Corolario 2.2.8 tenemos que $Tr(\alpha_k z)\in D$, es decir $b_k\in D$ para todo $i\in\{1,\dots,n\}$. Por lo tanto $D'\subseteq\bigoplus_{i=1}^n D\beta_i$. ∎

Corolario 2.2.23. *Sean D es un dominio de ideales principales con campo de cociente Q, $Q(\alpha)/Q$ una extensión finita de grado n y D' la cerradura entera de D en $Q(\alpha)$. Entonces D' es un D-módulo libre de rango n.*

Demostración. *Como D es de ideales principales, por el Corolario 2.1.15, tenemos que D es enteramente cerrado. Por el Teorema 2.2.22 D' es un D-submódulo de un D-módulo libre de rango n. Luego del Corolario 1.3.10 concluimos que D' es libre de rango menor o igual a n.*

Ahora, si $\{\alpha_1,\dots,\alpha_n\}$ una base entera de $Q(\alpha)$ sobre Q y consideramos M el D-submódulo de D' generado por $\{\alpha_1,\dots,\alpha_n\}$. Claramente $M=\bigoplus_{i=1}^n D\alpha_i$, y entonces por el Teorema 1.3.12 existe una base de D' con cardinalidad mayor o igual que n. Por lo tanto el rango de D' es n. ∎

Dado su importancia en lo siguiente de este trabajo, es conveniente introducir la siguiente

Definición 2.2.24. *Un R-módulo M es un **módulo noetheriano** si todo R-submódulo de M es finitamente generado.*

Ejemplo 2.2.25. Si R es un anillo, claramente $R[x_\infty]$ es un $R[x_\infty]$-módulo finitamente generado y sin embargo no es un $R[x_\infty]$-módulo noetheriano.

Teorema 2.2.26. *Para un anillo R y M un R-módulo son equivalentes*

1) *M es un R-módulo noetheriano.*
2) *Toda sucesión creciente (respecto a la inclusión) de R-submódulos de M se estaciona. Es decir, si $\{M_n\}_{n\in\mathbb{N}}$ es una familia de ideales de R tales que $M_n\subseteq M_{n+1}$ para cada $n\in\mathbb{N}$, entonces existe $n_o\in\mathbb{N}$ tal que $I_n=I_{n_o}$ para todo $n\geqslant n_o$.*
3) *Toda familia no vacía de R-submódulos de M (con el orden dado por la inclusión) tiene un maximal.*

Proposición 2.2.27. *Sean M un R-módulo y N un R-submódulo de M. Entonces M es noetheriano si y sólo si N y M/N son noetherianos.*

Corolario 2.2.28. *Sean M_1 y M_2 R-módulos. Entonces $M_1\bigoplus M_2$ es un R-módulo noetheriano si y sólo si M_1 y M_2 son R-módulos noetherianos.*

Corolario 2.2.29. *Sean $M_1,\dots,M_n$ R-módulos. Entonces $\bigoplus_{i=1}^n M_i$ es un R-módulo noetheriano si y sólo si $M_1,\dots,M_n$ son R-módulos noetherianos.*

Proposición 2.2.30. *Sea D un dominio entero noetheriano y enteramente cerrado con campo de cocientes Q, $Q(\alpha)/Q$ una extensión finita de grado n y D' la cerradura entera de D en $Q(\alpha)$. Entonces*

1) *D' es un D-módulo noetheriano.*
2) *D' un anillo noetheriano.*

Demostración.

1) *Por el Teorema 2.2.22 D' es un D-módulo de rango n, entonces existe $\{\alpha_1, \ldots, \alpha_n\} \subseteq D'$ tales que $D' \subseteq \bigoplus_{i=1}^{n} D\alpha_i$. Como $D\alpha_i$ es un D-módulo noetheriano para cada $i \in \{1, \ldots, n\}$. Del Corolario 2.2.27 sabemos que D' es noetheriano.*
2) *Para ver que D' es un anillo noetheriano basta hacer notar que los ideales de D' en particular son D-submódulos de D', y entonces toda sucesión creciente de ideales de D' es una sucesión creciente de D-submódulos de D', y como D' es un D-módulo noetheriano entonces ésta se estaciona, luego por la Proposición 1.2.26 D' es un anillo noetheriano.* ∎

Definición 2.2.31. *Un dominio entero D es un **dominio de Dedekind** si es noetheriano, enteramente cerrado y todo ideal primo no nulo de D es maximal.*

Ejemplo 2.2.32. Todo dominio de ideales principales es un dominio de Dedekind. Claramente si D es un dominio de ideales principales, entonces D es noetheriano. D es enteramente cerrado, pues por ser un dominio de ideales principales, de la Proposición 1.2.68 se tiene que D es un DFU y luego por la Proposición 2.1.14 tenemos que D es enteramente cerrado. Por último, el que todo ideal primo no nulo sea un ideal maximal en D es consecuencia del la Proposición 1.2.36

Lema 2.2.33. *Sea S un anillo, R un subanillo de S y $\mathfrak{P}$ un ideal primo de S. Entonces $\mathfrak{P} \cap R$ es un ideal primo de R.*

Demostración. *Consideremos $i : R \hookrightarrow S$ el homomorfismo inclusión y $\pi : S \longrightarrow S/\mathfrak{P}$ la proyección canónica. Dado que $ker(\pi i) = \mathfrak{P} \cap R$, entonces $\mathfrak{P} \cap R$ es un ideal de R. Luego por la Proposición 1.1.16 existe un morfismo inyectivo de $R/(\mathfrak{P} \cap R)$ en $S/\mathfrak{P}$. Ahora, siendo $\mathfrak{P}$ un ideal primo de S, por la Proposición 1.2.33 $S/\mathfrak{P}$ es un dominio entero y dado que todo subanillo de un dominio entero es dominio entero, entonces tenemos que $R/(\mathfrak{P} \cap R)$ isomorfo a un dominio entero y por lo tanto $R/(\mathfrak{P} \cap R)$ es un dominio entero. Aplicando la Proposición 1.2.33 a $\mathfrak{P} \cap R$ obtenemos que es un ideal primo de R.* ∎

Teorema 2.2.34. *Sean D un dominio de Dedekind con campo de cocientes Q, $Q(\alpha)/Q$ una extensión finita de grado n y D' la cerradura entera de D en $Q(\alpha)$. Entonces D' es un dominio de Dedekind y un D-módulo noetheriano.*

Demostración. *Por la Proposición 2.2.30 se tiene que D' es un anillo noetheriano y un D-módulo noetheriano y de la Proposición 2.1.17 que D' es un dominio enteramente cerrado. Así para demostrar que D' es un dominio de Dedekind sólo falta verificar que todo ideal primo no nulo de D' es un ideal maximal en D'.*

Tomemos $\mathfrak{P}$ un ideal primo no nulo de D' y $\alpha \in \mathfrak{P}'$, $\alpha \neq 0$. Siendo que α es un entero algebraico sobre D, entonces existe $f(x) = \sum_{i=1}^{n} a_i x^i \in D[x]$ un polinomio mónico tal que $f(\alpha) = 0$, de hecho podemos suponer que $f(x)$ es de grado mínimo con la propiedad de que $f(\alpha) = 0$ y así tenemos que $a_0 \neq 0$. Además de que

$$\alpha(-\alpha^{n-1} - a_{n-1}\alpha^{n-2} - \cdots - a_2\alpha - a_1) = a_0,$$

donde $\alpha \in \mathfrak{P}$ y $-\alpha^{n-1} - a_{n-1}\alpha^{n-2} - \cdots - a_2\alpha - a_1 \in D'$ y así tenemos que $a_0 \in \alpha D' \cap D \subseteq \mathfrak{P} \cap D$. Por lo tanto $\mathfrak{P} \cap D \neq \{0\}$.

Por el Lema 2.2.33 $\mathfrak{P} \cap D$ es un ideal primo D que además es no nulo, como ya vimos. Siendo D un dominio de Dedekind, entonces $\mathfrak{P} \cap D$ es maximal en D, luego por la Proposición 1.1.20 se tiene que $D/(\mathfrak{P} \cap D)$ es campo.

Ahora consideremos el morfismo de anillos dado por

$$\begin{aligned} D &\xrightarrow{\varphi} D'/\mathfrak{P} \ . \\ d &\longmapsto \overline{d} \end{aligned}$$

Dado que $ker(\varphi) = \mathfrak{P} \cap D$, *por la Proposición 1.1.16 existe un morfismo inyectivo de anillos* $\tilde{\varphi} : D/(\mathfrak{P} \cap D) \longrightarrow D'/\mathfrak{P}$ *y así* $D/(\mathfrak{P} \cap D)$ *es isomorfo a un subanillo de* $D'/\mathfrak{P}$, *el cual denotaremos también por* $D/(\mathfrak{P} \cap D)$.

Como D' *es entero sobre D, entonces* $D'/\mathfrak{P}$ *es entero sobre* $D/(\mathfrak{P} \cap D)$. *Luego, de la Proposición 2.1.18* $D'/\mathfrak{P}$ *es campo y entonces por la Proposición 1.1.20 obtenemos que* $\mathfrak{P}$ *es un ideal maximal de* D'. *Por lo tanto* D' *es un anillo de Dedekind.* ∎

Corolario 2.2.35. *Sea D es dominio de ideales principales con campo de cocientes Q,* $Q(\alpha)/Q$ *una extensión finita de grado n y* D' *la cerradura entera de D en* $Q(\alpha)$. *Entonces* D' *es un anillo de Dedekind y un D-módulo noetheriano.*

Definición 2.2.36. *Consideremos el anillo de los enteros* $\mathbb{Z}$ *y su campo de cocientes* $\mathbb{Q}$. *A una extensión finita* $\mathbb{Q}(\alpha)$ *sobre* $\mathbb{Q}$ *se le llama un campo numérico y a la cerradura entera* $\mathbb{Z}'$ *de* $\mathbb{Z}$ *en* $\mathbb{Q}(\alpha)$ *se le llama el anillo de enteros del campo numérico* $\mathbb{Q}(\alpha)$.

Proposición 2.2.37. *Si* $\mathbb{Q}(\alpha)$ *es un campo numérico, entonces el anillo de enteros* $\mathbb{Z}'$ *del campo numérico* $\mathbb{Q}(\alpha)$ *es un anillo de Dedekind.*

Ahora vamos a presentar una gran cantidad de ejemplos de dominios eenteros en los que es posible la factorización en irreducibles, sin embargo no son DFU. Para ello necesitamos del siguiente resultado

Proposición 2.2.38. *Sea d un entero libre de cuadrados*[5] *Entonces el anillo de enteros algebraicos de* $Q(\sqrt{d})$ *esta dado por*

1) $\mathbb{Z}\left[\frac{1}{2} + \frac{1}{2}\sqrt{d}\ \right]$ *si y sólo si* $d \equiv 1 \pmod 4$.
2) $\mathbb{Z}\left[\sqrt{d}\ \right]$ *si y sólo si* $d \not\equiv 1 \pmod 4$.

Demostración. *Por la Proposición 1.4.22 tenemos que* $\left\{1, \sqrt{d}\right\}$ *es una base de* $\mathbb{Q}(\sqrt{d})$ *sobre* $\mathbb{Q}$. *Así todo elemento* $\alpha \in \mathbb{Q}(\sqrt{d})$ *se puede escribir como* $\alpha = r + s\sqrt{d}$ *con* $r, s \in \mathbb{Q}$, *de donde es posible escribir*

$$\alpha = \frac{a + b\sqrt{d}}{c},$$

con $a, b, c \in Z$, $c > 0$ *y* $(a, b, c) = 1$.

Siendo que $\sqrt{d}$ *es un entero algebraico sobre* $\mathbb{Z}$, *podemos tomar* $\alpha \in \mathbb{Z}' - \mathbb{Z}$ *y dado que* $\mathbb{Z}$ *es enteramente cerrado, tenemos que* $\alpha \notin \mathbb{Q}$, *luego entonces el polinomio mínimo de* α *esta dado por*

$$f(x) = \left(x - \left(\frac{a + b\sqrt{d}}{c}\right)\right)\left(x - \left(\frac{a - b\sqrt{d}}{c}\right)\right) = x^2 - \left(\frac{2a}{c}\right)x + \frac{a^2 - b^2 d}{c^2}.$$

Además como $N(\alpha) = \frac{a^2 - b^2 d}{c^2}$ *y* $Tr(\alpha) = \frac{2a}{c}$, *aplicando el Corolario 2.2.8 obtenemos que* α *es un entero algebraico sobre* $\mathbb{Z}$ *si y sólo si* $f(x) \in \mathbb{Z}[x]$. *Así, si* $\alpha \in Q(\sqrt{d})$ *es un entero algebraico sobre* $\mathbb{Z}$, *entonces*

$$\frac{a^2 - b^2 d}{c^2} \in \mathbb{Z} \tag{2.9}$$

[5] Un elemento $d \in \mathbb{Z} - \{0\}$ es libre de cuadrados, para todo $p \in \mathbb{Z}$ con p primo se tiene que $p^2 \nmid d$.

y

$$\frac{2a}{c} \in \mathbb{Z} \tag{2.10}$$

Si suponemos que un primo $p \in \mathbb{Z}$*, es tal que* $p \mid a$ *y* $p \mid c$*, de la ecuación (2.9) se tendría que* $p^2 \mid b^2 d$ *y siendo p libre de cuadrados entonces* $p \mid b$ *que es contradictorio con la elección de a, b y c. Luego entonces se tiene que* $(a, c) = p$ *y así de la ecuación (2.10) tenemos que* $c \mid 2$*, de donde* $c = 1, 2$ *pues suponemos que c es positivo.*

Supongamos que existe $\frac{a+b\sqrt{d}}{2} \in \mathbb{Z}'$ *con* $(a, b, 2) = 1$*, como ya se vio en el párrafo anterior se tiene que* $(a, 2) = 1$ *y como consecuencia* $(b, 2) = 1$*. Luego entonces tenemos que* $a^2 \equiv 1 \pmod 4$ *y* $b^2 \equiv 1 \pmod 4$ *y así se tiene que* $a^2 - b^2 d \equiv 1 - d \pmod 4$ *es decir* $d \equiv 1 \pmod 4$*. Recíprocamente si* $d \equiv 1 \pmod 4$*, para* $a, b \in \mathbb{Z}$ *impares tenemos que* $\frac{a+b\sqrt{d}}{2} \in \mathbb{Z}'$*.*

Ahora

$$d \equiv 1 \pmod 4 \Longleftrightarrow N\left(\frac{1}{2} + \frac{1}{2}\sqrt{d}\right) = \frac{1+d}{4} \in \mathbb{Z} \Longleftrightarrow \frac{1}{2} + \frac{1}{2}\sqrt{d} \in \mathbb{Z}'.$$

Y como para todo $a, b \in \mathbb{Z}$ *se tiene que* $\frac{a}{2} + \frac{b}{2}\sqrt{d} = \frac{a-b}{2} + \left(\frac{1}{2} + \frac{1}{2}\sqrt{d}\right)$*, es claro que entonces que* $\mathbb{Z}' = \mathbb{Z}[\frac{1}{2} + \frac{1}{2}\sqrt{d}\,]$ *si y sólo si* $d \equiv 1 \pmod 4$ *y como consecuencia* $\mathbb{Z}' = \mathbb{Z}[\sqrt{d}\,]$ *si y sólo si* $d \not\equiv 1 \pmod 4$ ∎

Ejemplo 2.2.39. Sea $d \in \mathbb{Z}^- - \{-1, -2\}$ un entero libre de cuadrados impar tal que $d \not\equiv 1 \pmod 4$. Por la Proposición 2.2.38 tenemos que el anillo de enteros algebraicos de $Q(\sqrt{d})$ es $\mathbb{Z}\left[\sqrt{d}\,\right]$. Además tenemos por el Corolario 2.2.35 que $\mathbb{Z}\left[\sqrt{d}\,\right]$ es un anillo noetheriano y entonces por el Teorema 1.2.50 $\mathbb{Z}\left[\sqrt{d}\,\right]$ cumple la *CFD*, luego por la Proposición 2.2.45 todo elemento en $\mathbb{Z}\left[\sqrt{d}\,\right]$ se puede factorizar en irreducibles.

Por otro lado notemos que los morfismo de $Q(\sqrt{d})$ en $\overline{\mathbb{Q}}$ que extienden a la identidad $Id : \mathbb{Q} \longrightarrow \mathbb{Q}$ están dados por

$$Id : Q(\sqrt{d}) \longrightarrow Q(\sqrt{d}) \;\; donde \;\; Id(a + b\sqrt{d}\,]) = a + b\sqrt{d} \;\; para \;\; todo \;\; a + b\sqrt{d} \in Q(\sqrt{d})$$

y por

$$\varphi : Q(\sqrt{d}) \longrightarrow Q(\sqrt{d}) \;\; donde \;\; \varphi(a + b\sqrt{d}\,]) = a - b\sqrt{d} \;\; para \;\; todo \;\; a + b\sqrt{d} \in Q(\sqrt{d}).$$

Así $N(a + b\sqrt{d}) = a^2 - b^2 d$ para todo $a + b\sqrt{d} \in Q(\sqrt{d})$.

Ahora veremos que 2 es un elemento irreducible en $\mathbb{Z}\left[\sqrt{d}\,\right]$. Para ello procedamos por reducción al absurdo y supongamos que 2 no es irreducible, entonces existen $a_1 + b_1\sqrt{d}, a_2 + b_2\sqrt{d} \in \mathbb{Z}\left[\sqrt{d}\,\right]$ no unidades tales que $2 = (a_1 + b_1\sqrt{d})(a_2 + b_2\sqrt{d})$. Por los incisos 3) y 4) de la Proposición 2.2.2 tenemos que

$$4 = N(2) = N((a_1 + b_1\sqrt{d})(a_2 + b_2\sqrt{d})) = N(a_1 + b_1\sqrt{d})N(a_2 + b_2\sqrt{d}) = (a_1^2 + b_1^2 d)(a_2^2 + b_2^2 d).$$

Claramente $a_1^2 - b_1^2 d, a_2^2 - b_2^2 d > 0$ y como suponemos que no son unidades entonces de la Proposición 2.2.9 tenemos que $a_1^2 - b_1^2 d, a_2^2 - b_2^2 d > 1$. Dejando como única posibilidad que $a_1^2 - b_1^2 d = a_2^2 - b_2^2 d = 2$, ecuaciones que no son solubles en $\mathbb{Z}$, pues $-d \geqslant 3$. Por lo tanto 2 es irreducible en $\mathbb{Z}\left[\sqrt{d}\,\right]$.

Ahora notemos que $1 - d = (1 + \sqrt{d})(1 + \sqrt{d})$ y que $2 \mid d - 1$ pues suponemos d impar Claramente $2 \nmid 1 + \sqrt{d}$ y $2 \nmid 1 - \sqrt{d}$. Es decir 2 es un irreducible en $\mathbb{Z}[\sqrt{d}\,]$ que no es primo en $\mathbb{Z}[\sqrt{d}\,]$ y entonces por el Teorema 1.2.67 tenemos que $\mathbb{Z}\left[\sqrt{d}\,\right]$ no es un dominio de factorización única.

En particular tenemos que

$$\mathbb{Z}\left[\sqrt{-5}\right],\ \mathbb{Z}\left[\sqrt{-13}\right],\quad \mathbb{Z}\left[\sqrt{-17}\right],\ \mathbb{Z}\left[\sqrt{-21}\right],\ \mathbb{Z}\left[\sqrt{-29}\right],\ \ldots$$

son dominios de factorización que no son dominios de factorización única.

Si R es un anillo y E es un R-módulo libre de rango n. Análogo a como se hace en el álgebra lineal, dado φ un endomorfismo de E y $\alpha = \{e_1, \ldots, e_n\}$ una base de E sobre R y (a_{ij}) la matriz asociada a φ en la base α se definen la ***traza*** *de φ respecto a α, la* ***norma*** *de φ respecto a α y el* ***polinomio característico*** *de φ respecto a α, respectivamente por*

$$Tr_\alpha(\varphi) = \sum_{i=1}^{n} a_{ii},\ \ N_\alpha(\varphi) = det((a_{ij}))\ \ y\ \ P_{\alpha,\varphi}(x) = det(xI_n - (a_{ij})),$$

donde $I_n \in M_n(R)$ es la matriz identidad. Y al igual que en el álgebra lineal tenemos que estos valores son independientes de la base y entonces los denotaremos solamente por

$$Tr(\varphi) = \sum_{i=1}^{n} a_{ii},\ \ N(\varphi) = det((a_{ij}))\ \ y\ \ P_\varphi(x) = det(xI_n - (a_{ij})),$$

Proposición 2.2.40. *Sea R es un anillo y E es un R-módulo libre libre de rango n. Si ϕ y φ son endomorfismos de E, entonces*

1) $Tr(\phi + \varphi) = Tr(\phi) + Tr(\varphi)$.
2) $N(\phi \circ \varphi) = N(\phi)N(\varphi)$.
3) $P_\varphi(x) = x^n - Tr(\varphi)x^{n-1} + \cdots + (-1)^n N(\varphi)$.

Notación 2.2.41. *Sea R es un anillo y S un subanillo de R. Si $r \in R$ denotaremos por m_r al S-endomorfismo lineal de R dado por $m_r(t) = rt$ para todo $t \in R$.*

Teorema 2.2.42. *Sea D es dominio de Dedekind con campo de cocientes Q, $Q(\alpha)/Q$ una extensión finita de grado n y D' la cerradura entera de D en $Q(\alpha)$. Si $\beta \in Q(\alpha)$, entonces $N(m_\beta) = N_{Q(\alpha)/Q}(\beta)$.*

Demostración. *Primero mostraremos que esto es válido para α. Sea entonces $f_\alpha(x) = \sum_{i=1}^{n} a_i x^i$ el polinomio mínimo de α sobre Q, entonces por la Proposición 14.22, $\Gamma = \{1, \alpha, \ldots, \alpha^{n-1}\}$ es una base de $Q(\alpha)$ sobre Q. Nótese que*

$$m_\alpha(1) = \alpha,\ \ m_\alpha(\alpha) = \alpha^2,\ \ \ldots,\ \ m_\alpha(\alpha^{n-2}) = \alpha^{n-1}$$

y como $a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1} + \alpha^n = 0$ entonces.

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

Y así la matriz de m_α asociada a la base Γ está dada por

$$M = \begin{pmatrix} 0 & 0 & \ldots & -a_0 \\ 1 & 0 & \ldots & -a_1 \\ 0 & 1 & \ldots & -a_2 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \ldots & -a_{n-1} \end{pmatrix}$$

Luego tenemos que

$$P_{m_\alpha}(x) = \det(xI_n - M) = det \begin{pmatrix} x & 0 & \ldots & a_0 \\ -1 & x & \ldots & a_1 \\ 0 & -1 & \ldots & a_2 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \ldots & x + a_{n-1} \end{pmatrix} = (-1)^n a_0 + (-1)^{n-1} a_1 x + \cdots - a_{n-1}x^{n-1} + x^n.$$

Por un lado por la Proposición 2.2.40 inciso (3)*, tenemos que* $N(m_\alpha) = a_0$ *y por otro en la demostración de la Proposición 2.2.3 se hace notar que* $a_0 = N_{Q(\alpha)/Q}(\alpha)$*. Por lo tanto* $N(m_\alpha) = N_{Q(\alpha)/Q}(\alpha)$*.*

Ahora consideremos $\beta \in Q(\alpha)$*, virtud de la Proposición 2.2.5 es suficiente demostrar mostrar que el polinomio característico del endomorfismo*

$$m_\beta : Q(\alpha) \longrightarrow Q(\alpha) \text{ dado por } m_\beta(\gamma) = \beta\gamma \text{ para todo } \gamma \in \mathbb{Q}(\alpha)$$

es igual a la $[Q(\alpha) : Q(\beta)]$*-esima potencia del polinomio característico del endomorfismo*

$$m_{\beta,Q(\beta)} : Q(\beta) \longrightarrow Q(\beta) \text{ dado por } m_{\beta,Q(\beta}(\gamma) = \beta\gamma \text{ para todo } \gamma \in \mathbb{Q}(\beta)$$

Sean $r = [Q(\alpha) : Q(\beta)]$ *y* $s = [Q(\beta) : Q]$*. Tomemos* $Y = \{y_i\}_{i=1}^{s}$ *una base de* $Q(\beta)$ *sobre* Q *y*

$$N = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1s} \\ a_{21} & a_{22} & \dots & a_{2s} \\ a_{31} & a_{32} & \dots & a_{3s} \\ \vdots & \vdots & \ddots & \vdots \\ a_{s1} & a_{s2} & \dots & a_{ss} \end{pmatrix}$$

la matriz del morfismo $m_{\beta,Q(\beta)}$ *en la base* Y*. Entonces tenemos que el polinomio característico del endomorfismo* $m_{\beta,Q(\beta)}$ *esta dado por* $P_{\beta,Q(\beta)} = \det(x1_s - M)$*.*

Si $Z = \{z_j\}_{j=1}^{r}$ *es una base de* $Q(\alpha)$ *sobre* $Q(\beta)$*, entonces*

$$W = \{y_i z_j\}_{i=1}^{s}{}_{j=1}^{r}{}^{6}$$

es una base de $Q(\alpha)$ *sobre* Q*. Así para todo* $i \in \{1, \dots, s\}$ *y* $j \in \{1, \dots, r\}$

$$\alpha(y_i z_j) = (\alpha y_i)z_j = (\sum_i^s a_{ik} y_k)z_j = \sum_i^s a_{ik}(y_k z_j).$$

Ordenando W *con el orden lexicográfico, obtenemos que la matriz del morfismo* m_β *en la base* W *esta dada por*

$$N' = \begin{pmatrix} & & & \\ N & 0 & \dots & 0 \\ 0 & N & \dots & 0 \\ 0 & 0 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & N \\ \underbrace{\qquad\qquad}_{r-veces} & & & \end{pmatrix}$$

Así el polinomio característico del endomorfismo m_β *esta dado por:*

$$P_\beta(x) = det(x1_n - M') = (det(x1_s - N))^r. \ \blacksquare$$

Proposición 2.2.43. *Consideremos el anillo de los enteros* $\mathbb{Z}$ *y sea* $\mathbb{Q}(\alpha)/\mathbb{Q}$ *una extensión finita de grado* n *y* $\mathbb{Z}'$ *el anillo de enteros algebraicos de* $\mathbb{Q}(\alpha)$ *sobre* $\mathbb{Z}$*. Si* $\alpha \in \mathbb{Z}'$*, entonces* $|N_{Q(\alpha)/\mathbb{Q}}(\alpha)| = |\mathbb{Z}'/\mathbb{Z}'\alpha|$*.*

Demostración. *Como* $\mathbb{Z}$ *es un dominio de ideales principales, por el Corolario 2.2.23 se tiene que* $\mathbb{Z}'$ *es un* $\mathbb{Z}$*-módulo libre de rango* n*. Dado que* $\mathbb{Z}'$ *es un dominio entero, si* $\alpha \in \mathbb{Z}'$ *el morfismo* m_α *es inyectivo, y entonces tenemos que* $\mathbb{Z}'$ *es isomorfo como* $\mathbb{Z}$*-módulo a* $\mathbb{Z}'\alpha$ *y en consecuencia*

[6] Una demostración de este echo se puede encontrar en [Fr] pág. 349.

el rango de $\mathbb{Z}'\alpha$ es n. Luego entonces por el Teorema 1.3.12 existe una $\mathbb{Z}$-base $\{e_1,\dots,e_n\}$ de $\mathbb{Z}'$ y $c_1,\dots,c_n \in \mathbb{N}\backslash\{0\}$ tales que $\{c_1e_1,\dots,c_ne_n\}$ es una $\mathbb{Z}$-base de $\mathbb{Z}'\alpha$. Así

$$\mathbb{Z}'/\mathbb{Z}'\alpha \cong \bigoplus_{i=1}^{n}\mathbb{Z}e_i/\bigoplus_{i=1}^{n}/\mathbb{Z}c_ie_i \cong \bigoplus_{i=1}^{n}\mathbb{Z}e_i/\mathbb{Z}c_ie_i \cong \bigoplus_{i=1}^{n}\mathbb{Z}/\mathbb{Z}c_i.$$

Por lo tanto $|\mathbb{Z}'/\mathbb{Z}'\alpha| = \prod_{i=1}^{n} c_i$.

Ahora consideremos $\varphi : \mathbb{Z}' \longrightarrow \mathbb{Z}'\alpha$ dada por $\varphi(e_i) = c_ie_i$. Claramente

$$N(\varphi) = \prod_{i=1}^{n} c_i. \tag{2.11}$$

Por otra parte $\{\alpha e_1,\dots,\alpha e_n\}$ es una base de $\mathbb{Z}'\alpha$, luego entonces la transformación $\mathbb{Z}$-lineal $\psi : \mathbb{Z}'\alpha \longrightarrow \mathbb{Z}'\alpha$ dada por $\psi(c_ie_i) = \alpha e_i$ es un automorfismo de $\mathbb{Z}'\alpha$, y así por el Teorema 1.3.21 tenemos que $N(\psi) = \pm 1$.

Ahora notemos que $m_\alpha = \psi \circ \varphi$, entonces

$$|N_{Q(\alpha)/\mathbb{Q}}(\alpha)| \underset{\text{Teo. 2.2.40}}{=} |N(m_\alpha)| = |N(\psi\circ\varphi)| \underset{\text{Prop. 2.2.38}}{=} |N(\psi)N(\varphi)| = |\pm 1|\,|N(\varphi)| = \prod_{i=1}^{n} c_i$$

Por lo tanto $|N_{Q(\alpha)/\mathbb{Q}}(\alpha)| = |\mathbb{Z}'/\mathbb{Z}'\alpha|$. ∎

Corolario 2.2.44. *Consideremos el anillo de los enteros $\mathbb{Z}$ y sea $\mathbb{Q}(\alpha)/\mathbb{Q}$ una extensión finita de grado n y $\mathbb{Z}'$ el anillo de enteros algebraicos de $\mathbb{Q}(\alpha)$ sobre $\mathbb{Z}$. Si $\mathfrak{A}$ es un ideal no nulo de $\mathbb{Z}'$, entonces $\mathbb{Z}'/\mathfrak{A}$ es un anillo finito.*

Demostración. *Como $\mathfrak{A}$ es un ideal no nulo de $\mathbb{Z}'$ podemos tomar $\alpha \in \mathfrak{A} - \{0\}$. Tenemos por el Corolario 2.1.13 que $\mathbb{Z}'\alpha \subseteq \mathfrak{A}$, luego del Teorema 1.1.18*

$$\mathbb{Z}'/\mathfrak{A} \cong (\mathbb{Z}'/\mathbb{Z}'\alpha)/(\mathfrak{A}/\mathbb{Z}'\alpha)$$

y como $\mathbb{Z}'/\mathbb{Z}'\alpha$ es un anillo finito entonces $\mathbb{Z}'/\mathfrak{A}$ es un anillo finito. ∎

Definición 2.2.45. *Consideremos el anillo de los enteros $\mathbb{Z}$ y sea $\mathbb{Q}(\alpha)/\mathbb{Q}$ una extensión finita de grado n y $\mathbb{Z}'$ el anillo de enteros algebraicos de $\mathbb{Q}(\alpha)$ sobre $\mathbb{Z}$. Si $\mathfrak{A}$ es un ideal no nulo de $\mathbb{Z}'$ se define* ***norma del ideal*** *$\mathfrak{A}$ y se denota por $N(\mathfrak{A})$ a la cardinalidad de $\mathbb{Z}'/\mathfrak{A}$.*

Proposición 2.2.46. *Consideremos el anillo de los enteros $\mathbb{Z}$ y sea $\mathbb{Q}(\alpha)/\mathbb{Q}$ una extensión finita de rango n y $\mathbb{Z}'$ el anillo de enteros algebraicos de $\mathbb{Q}(\alpha)$ sobre $\mathbb{Z}$. Si $\mathfrak{A}$ es un ideal no nulo de $\mathbb{Z}'$, entonces $N(\mathfrak{A}) \in \mathfrak{A}$.*

Demostración. *Por definición $N(\mathfrak{A}) = |\mathbb{Z}'/\mathfrak{A}|$. Notemos que $\mathbb{Z}'/\mathfrak{A}$ es un grupo finito. Así, si $\overline{x} \in \mathbb{Z}'/\mathfrak{A}$ se tiene que $N(\mathfrak{A})\overline{x} = \overline{0}$, pues el orden de un elemento divide al orden del grupo. Por lo tanto $N(\mathfrak{A})x \in \mathfrak{A}$ para todo $x \in \mathbb{Z}'$, en particular para $x = 1$ por lo que $N(\mathfrak{A}) \in \mathfrak{A}$.* ∎

§2.3 Grupo de clases de ideales.

Esta sección se muestra como el comportamiento de un ideal primo no nulo en el conjunto de ideales no nulos de un dominio de Dedekind es semejante al de un elemento irreducible en un anillo de factorización única.

Lema 2.3.1. *Sea R un anillo y $\mathfrak{P}$ un ideal primo que contiene un producto $I_1\cdots I_n$ de ideales. Entonces $\mathfrak{P}$ contiene a uno de los ideales.*

Demostración. *Supongamos lo contrario, es decir que $I_j \not\subseteq \mathfrak{P}$ para todo $j \in \{1,\dots,n\}$, luego existe $r_j \in I_j$ tal que $r_j \notin \mathfrak{P}$. Siendo $\mathfrak{P}$ un ideal primo, por la Proposición 1.2.33 $r_1 \cdots r_n \notin \mathfrak{P}$, lo cual es contradictorio pues $r_1 \cdots r_n \in I_1 \cdots I_n \subseteq \mathfrak{P}$. Por lo tanto existe $j_o \in \{1,\dots,n\}$ tal que $I_{j_o} \subseteq \mathfrak{P}$.* ∎

Ahora se presenta un resultado técnico que será de gran ayuda en nuestro propósito.

Proposición 2.3.2. *Sea D un dominio entero noetheriano. Entonces todo ideal no nulo contiene un producto de ideales primos no nulos.*

Demostración. *Se procederá por reducción al absurdo, para ello supongamos que la familia Φ de ideales no nulos de D que no contienen ningún producto de ideales primos no nulos es no vacía.*

Como D es noetheriano, Φ admite un elemento maximal $\mathfrak{d}$; $\mathfrak{d}$ no puede ser primo pues se contiene a sí mismo, luego entonces por la Proposición 1.2.33 existen $x, y \in D\backslash\mathfrak{d}$ tales que $xy \in \mathfrak{d}$. Como $x, y \notin \mathfrak{d}$ los ideales $\mathfrak{d} + \langle x\rangle$ y $\mathfrak{d} + \langle y\rangle$ contienen estrictamente a $\mathfrak{d}$, y dada la maximalidad de este último, ambos ideales contienen un producto de ideales primos no nulos. Supongamos entonces que

$$P_1 \cdots P_n \subseteq \mathfrak{d} + \langle x\rangle \text{ y } R_1 \cdots R_m \subseteq \mathfrak{d} + \langle y\rangle$$

son los productos de ideales no nulo contenidos en cada ideal. Luego

$$P_1 \cdots P_n R_1 \cdots R_m \subseteq (\mathfrak{d} + \langle x\rangle)(\mathfrak{d} + \langle y\rangle) \underset{xy\in\mathfrak{d}}{\subseteq} \mathfrak{d}.$$

Lo que es una contradicción. Concluimos entonces que Φ es vacío y así se sigue el resultado. ∎

*Dados D un dominio entero y Q su campo de cocientes, se dice que $I \subseteq Q$ es un **ideal fraccionario** de D si*

1) *I es un D-submódulo de Q.*
2) *Existe $d \in D\backslash\{0\}$ tal que $dI \subseteq D$.*

*Obsérvese que la condición 2) equivale a decir que los elementos de I tienen un "común denominador" $d \in D$. Además, nótese que los ideales ordinarios de D, son ideales fraccionarios, tomando $d = 1$. En adelante para referirnos a un ideal de D pensado en él como ideal fraccionario usaremos el término de **ideal entero** de D.*

Sean I y J son ideales fraccionarios de un dominio entero D. El producto de los ideales fraccionarios I y J esta dado por

$$IJ = \left\{ \sum_{i=1}^{n} x_i y_i \in Q \mid x_i \in I \text{ y } y_i \in J \right\}.$$

Claramente IJ es un D-submódulo del campo de cocientes de D. Además si $d_1, d_2 \in D\backslash\{0\}$ son tales que $d_1 I \subseteq D$ y $d_2 J \subseteq D$, se tiene que $d_1 d_2 \in D\backslash\{0\}$ por ser D un domino entero y como $(d_1 d_2)IJ \subseteq D$ podemos concluir que IJ es un ideal fraccionario de D.

Proposición 2.3.3. *Sean D un dominio entero y Q su campo de cocientes e $I, J, K \subseteq Q$ ideales fraccionarios de Q. Entonces*

1) *Si $d \in D - \{0\}$ es tal que $dI \subseteq D$, entonces dI es un ideal de D.*
2) *Si $J \subseteq K$, entonces $IJ \subseteq IK$*

Es evidente que el producto de ideales fraccionarios de un dominio entero D es asociativo, que conmuta y además D actúa como neutro multiplicativo. Es decir el conjunto de ideales fraccionarios de un dominio entero es un monoide conmutativo respecto al producto.

Ahora nos enfocaremos a demostrar que el conjunto de ideales fraccionarios no nulos de un dominio de Dedekind, forman un grupo conmutativo y para ello necesitamos el siguiente resultado.

Proposición 2.3.4. *Sea D un dominio entero y Q su campo de cocientes. Si I es un D-submódulo finitamente generado de Q, entonces I es un ideal fraccionario de D.*

Demostración. *Como I es un D-submódulo de Q finitamente generado, existen $\frac{p_1}{q_1}, \ldots, \frac{p_n}{q_n} \in Q$ con $q_i \neq 0$ tales que $\left\langle \frac{p_1}{q_1}, \ldots, \frac{p_n}{q_n} \right\rangle = I$ como D-módulo. Sea $d = \prod_{i=1}^{n} q_i$, siendo D un domino entero se tiene que $d \neq 0$, además de que $\frac{d}{q_i} \in D$ para cada $i \in \{1, \ldots, n\}$. Ahora, si $x \in I$, entonces $x = \sum_{i=1}^{n} d_i \left(\frac{p_i}{q_i}\right)$ con $d_i \in D$, luego $dx = d \sum_{i=1}^{n} d_i \left(\frac{p_i}{q_i}\right) = \sum_{i=1}^{n} d_i d \left(\frac{p_i}{q_i}\right) = \sum_{i=1}^{n} \left(\frac{d}{q_i}\right)(d_i p_i)$. Dado que $d_i p_i \in D$ para $i \in \{1, \ldots, n\}$, se tiene que $dx \in D$. Por lo tanto $dI \subseteq D$, es decir I es un ideal fraccionario de D.* ∎

Proposición 2.3.5. *Sea D un dominio entero noetheriano. Entonces todo ideal fraccionario es un D-módulo finitamente generado.*

Demostración. *Sea I un ideal fraccionario de D. Por definición existe $d \in D - \{0\}$ tal que $dI \subseteq D$. Como dI un ideal de D y D es noetheriano, entonces dI es finitamente generado. Por último notemos que $\varphi : dI \longrightarrow I$ dado por $\varphi(dx) = x$ es un isomorfismo de D-módulos. Por lo tanto I es noetheriano.*
∎

Teorema 2.3.6. *Sea D un dominio de Dedekind que no es campo. Entonces todo ideal maximal de D es invertible en el monoide de ideales fraccionarios de D.*

Demostración. *Sea $\mathfrak{M}$ un ideal maximal de D; como D no es campo se tiene que $\mathfrak{M} \neq (0)$. Sea Q el campo de cocientes de D y hagamos*

$$\mathfrak{M}' = \{x \in Q \mid x\mathfrak{M} \subseteq D\}$$

Es claro que $0 \in \mathfrak{M}'$, y que si $x, y \in \mathfrak{M}'$, entonces $(x - y)m = xm - ym \in D$ para todo $m \in \mathfrak{M}$, luego entonces $x - y \in \mathfrak{M}'$. Por lo tanto $\mathfrak{M}'$ es un D-submódulo de Q. Por como se definió $\mathfrak{M}'$, si $d \in \mathfrak{M} \backslash \{0\}$, entonces $d\mathfrak{M}' \subseteq D$ y así tenemos que $\mathfrak{M}'$ es un ideal fraccionario de D.

A continuación vamos a demostrar que $\mathfrak{M}\mathfrak{M}' = D$. Primero notemos que $D \subseteq \mathfrak{M}'$, luego entonces $\mathfrak{M} = D\mathfrak{M} \subseteq \mathfrak{M}'\mathfrak{M}$, además tenemos que $\mathfrak{M}'\mathfrak{M} \subseteq D$, es decir $\mathfrak{M} \subseteq \mathfrak{M}'\mathfrak{M} \subseteq D$. Ahora por ser $\mathfrak{M}$ un ideal maximal de D, sólo tenemos dos posibilidades para el ideal $\mathfrak{M}'\mathfrak{M}$, que son

$$\mathfrak{M}'\mathfrak{M} = \mathfrak{M} \quad o \quad \mathfrak{M}'\mathfrak{M} = D.$$

Veremos que $\mathfrak{M} = \mathfrak{M}'\mathfrak{M}$ no es posible, por lo que automáticamente se tendrá que $\mathfrak{M}'\mathfrak{M} = D$, lo que completará el resultado.

Supongamos entonces que $\mathfrak{M} = \mathfrak{M}'\mathfrak{M}$. Luego si $x \in \mathfrak{M}'$ se tiene que $x\mathfrak{M} \subseteq \mathfrak{M}$ y por un proceso recursivo verificamos que $x^{n+1}\mathfrak{M} \subseteq x^n\mathfrak{M}$ para toda $n \in \mathbb{N}$. Es decir, si $a \in \mathfrak{M} - \{0\}$, entonces $ax^n \in \mathfrak{M}$ para todo $n \in \mathbb{N}$ y en consecuencia $a\mathfrak{M}' \subseteq D$. De este modo se verifica que si $x \in \mathfrak{M}'$, entonces $D[x]$ es un ideal fraccionario de D, y al ser D noetheriano, por la Proposición 2.3.5, $D[x]$ es noetheriano y por el Teorema 2.1.7 concluimos que x es entero algebraico sobre D. Y como D es enteramente cerrado, tenemos que $x \in D$, es decir $\mathfrak{M}' \subseteq D$. Así $\mathfrak{M} = \mathfrak{M}'\mathfrak{M}$ implica $\mathfrak{M}' = D$. Ahora se mostrará que esto es imposible.

Supongamos entonces que $\mathfrak{M}' = D$ y consideremos $d \in \mathfrak{M} \backslash \{0\}$. Siendo que $dD \neq \{0\}$, por la Proposición 2.3.2 el ideal $dD (\neq (0))$ contiene un producto $P_1 \cdots P_s$ de ideales primos no nulos. Supongamos que s es mínimo con la propiedad de que $P_1 \cdots P_s$ esta contenido en dD. Si $s = 1$ entonces $P_1 \subseteq dD \subseteq \mathfrak{M}$, siendo que D es un dominio de Dedekind y P_1 es un ideal primo de D entonces P_1 es maximal y en consecuencia obtenemos que $dD = \mathfrak{M}$, luego por el Teorema 1.2.36 d es irreducible en D y por lo tanto $d \notin U(D)$. Por otro lado tenemos que $d^{-1}\mathfrak{M} = d^{-1}(dD) = D$ y entonces por definición del conjunto $\mathfrak{M}'$ se tiene que $d^{-1} \in \mathfrak{M}' = D$, lo que es contradictorio pues

$d \notin U(D)$. Ahora, si suponemos que $s > 1$, como $dD \subseteq \mathfrak{M}$, entonces $P_1 \cdots P_s \subseteq \mathfrak{M}$; al ser $\mathfrak{M}$ maximal se tiene que éste es primo, luego por el Lema 2.3.1 $\mathfrak{M}$ contiene alguno de ellos, digamos a P_1. Por ser D un dominio de Dedekind P_1 es maximal, por lo que debe suceder que $P_1 = \mathfrak{M}$. Hagamos $\mathfrak{B} = P_2 \cdots P_s$, entonces se tiene que $dD \supseteq \mathfrak{M}\mathfrak{B}$ y que $dD \not\supseteq \mathfrak{B}$, esto último por el carácter minimal de s. Luego entonces, existe $b \in \mathfrak{B}$ tal que $b \notin dD$, o equivalentemente $bd^{-1} \notin D$. Por otro lado, como $b \in \mathfrak{B}$ entonces $b\mathfrak{M} \subseteq dD$ y así $bd^{-1}\mathfrak{M} \subseteq D$. Por como se definió $\mathfrak{M}'$, se tiene que $bd^{-1} \in \mathfrak{M}'$. Ahora recordemos que estamos suponiendo que $\mathfrak{M}' = D$ y por lo tanto $bd^{-1} \in D$, lo que contradice la elección de b. Por lo tanto no puede ser que $\mathfrak{M} = \mathfrak{M}'\mathfrak{M}$ quedando como única posibilidad entonces que $\mathfrak{M}'\mathfrak{M} = D$, que muestra que $\mathfrak{M}$ es invertible en el monoide de ideales fraccionarios de D. ∎

Teorema 2.3.7. *Sea D un dominio de Dedekind y $\mathfrak{P}$ el conjunto de los ideales primos no nulos de D. Entonces todo ideal entero no nulo $\mathfrak{B}$ de D se escribe de modo único en la forma*

$$\mathfrak{B} = \prod \mathfrak{p}_{i_j} \ \ con \ \ \mathfrak{p}_{i_j} \in \mathfrak{P} \ \ para j \in \{1, \ldots, n\}.$$

Demostración. *Procedamos como en la Proposición 2.3.2, y consideremos Φ la familia de ideales no nulos de D que no son producto de ideales primos no nulos y supongamos que Φ es no vacío.*

Como D es noetheriano, Φ admite un elemento maximal $\mathfrak{A}$. Tenemos que $\mathfrak{A} \neq D$, pues D es el producto de la familia vacía de ideales primos de D. Entonces $\mathfrak{A}$ está contenido en un ideal maximal $\mathfrak{M}$. Sea $\mathfrak{M}'$ el ideal fraccionario inverso de $\mathfrak{M}$ descrito en el Teorema 2.3.6. Como $\mathfrak{A} \subseteq \mathfrak{M}$ se deduce entonces que $\mathfrak{A}\mathfrak{M}' \subseteq \mathfrak{M}\mathfrak{M}' = D$. Por otro lado, dado que $D \subseteq \mathfrak{M}'$, tenemos entonces que $\mathfrak{A} \subseteq \mathfrak{M}'\mathfrak{A}$. Si suponemos que $\mathfrak{A} = \mathfrak{M}'\mathfrak{A}$, entonces para cada $x \in \mathfrak{M}'$, tendríamos por recurrencia que $x^n\mathfrak{A} \subseteq \mathfrak{A}$ para todo $n \in \mathbb{N}$ y como en el Teorema 2.3.6, x sería un entero algebraico sobre D, por lo que se tendría que $x \in D$ lo que es imposible para todo $x \in \mathfrak{M}'$ pues $D \subsetneq \mathfrak{M}'$. Por lo tanto $\mathfrak{A} \subsetneq \mathfrak{M}'\mathfrak{A}$, luego como $\mathfrak{A}$ es un ideal maximal en Φ, se tiene que $\mathfrak{M}'\mathfrak{A} \notin \Phi$ y entonces $\mathfrak{M}'\mathfrak{A}$ es producto de ideales primos no triviales, es decir existen $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ ideales primos no nulos de D tales que

$$\mathfrak{M}'\mathfrak{A} = \mathfrak{p}_1 \cdots \mathfrak{p}_n \tag{3.1}$$

Multiplicando (3.1) por $\mathfrak{M}$ tenemos que

$$\mathfrak{A} = \mathfrak{M}\mathfrak{p}_1 \cdots \mathfrak{p}_n$$

lo que contradice la elección de $\mathfrak{A}$ y por lo tanto Φ es vacía.

Ahora supongamos que

$$\prod_{i=1}^{s} \mathfrak{p}_i = \prod_{j=1}^{t} \mathfrak{q}_j \tag{3.2}$$

Por la Proposición 1.1.12 tenemos que $\prod_{j=1}^{t} \mathfrak{q}_j \subset \mathfrak{p}_1$, luego por el Lema 2.3.1, $\mathfrak{p}_1$ contiene a alguno de los $\mathfrak{q}_{i's}$, sin perdida de generalidad podemos suponer que $\mathfrak{q}_1 \subseteq \mathfrak{p}_1$. Ahora, como D es un dominio de Dedekind, $\mathfrak{q}_1$ es un ideal maximal, entonces $\mathfrak{q}_1 = \mathfrak{p}_1$. Luego multiplicando por $\mathfrak{p}_1^{-1}$ a ambos lado de (3.2), obtenemos que

$$\prod_{i=2}^{s} \mathfrak{p}_i = \prod_{i=2}^{t} \mathfrak{q}_i.$$

De donde se claro el proceso de inducción que muestra el resultado. ∎

Corolario 2.3.8. *Sea D un dominio de Dedekind y $\mathfrak{P}$ el conjunto de los ideales primos no nulos de D. Entonces todo ideal entero $\mathfrak{B} \neq (0)$ de D se escribe de modo único en la forma*

$$\mathfrak{B} = \prod_{\mathfrak{p} \in \mathfrak{P}} \mathfrak{p}^{\eta_{\mathfrak{p}}}$$

donde $\eta_{\mathfrak{p}}$ son enteros no negativos, casi todos cero.

Corolario 2.3.9. *Sea D un dominio de Dedekind. Entonces todo ideal entero de D es invertible en el monoide de las ideales fraccionarios de D.*

Así pues para ver que el conjunto de ideales fraccionarios es un grupo sólo nos falta ver que cada ideal fraccionario de D que no es un ideal entero, es invertible; lo que muestra el siguiente resultado.

Corolario 2.3.10. *Sea D un dominio de Dedekind y $\mathfrak{P}$ el conjunto de los ideales primos no nulos de D. Entonces todo ideal fraccionario $\mathfrak{B} \neq (0)$ de D se escribe de modo único en la forma*

$$\mathfrak{B} = \prod_{\mathfrak{p} \in \mathfrak{P}} \mathfrak{p}^{\eta_{\mathfrak{p}}}$$

donde $\eta_{\mathfrak{p}}$ son enteros, casi todos cero.

Demostración. *Sea $\mathfrak{B}$ un ideal fraccionario de D, si $\mathfrak{B}$ es entero el resultado se tiene por el Teorema 2.3.7, así podemos suponer que $\mathfrak{B}$ es un ideal fraccionario no entero de D. Como $\mathfrak{B}$ es un ideal fraccionario existe $d \in D\backslash\{0\}$ tal que $d\mathfrak{B} \subseteq D$. Siendo $d\mathfrak{B}$ un ideal entero de D, por el Corolario 2.3.8*

$$d\mathfrak{B} = \prod_{\mathfrak{p} \in \mathfrak{P}} \mathfrak{p}^{\eta_{\mathfrak{p}}}$$

donde los $\eta_{\mathfrak{p}}$ son enteros no negativos.

Ahora notemos que $d\mathfrak{B} = (dD)\mathfrak{B}$. Como dD es un ideal entero de D, se tiene que

$$dD = \prod_{\mathfrak{p} \in \mathfrak{P}} \mathfrak{p}^{\mu_{\mathfrak{p}}}.$$

Como $(dD)^{-1} = \prod_{\mathfrak{p} \in \mathfrak{P}} \left(\mathfrak{p}^{-1}\right)^{\mu_{\mathfrak{p}}}$. Obtenemos que

$$\mathfrak{B} = (dD)^{-1}(dD)\mathfrak{B} = \prod_{\mathfrak{p} \in \mathfrak{P}} \mathfrak{p}^{-\mu_{\mathfrak{p}}} \prod_{\mathfrak{p} \in \mathfrak{P}} \mathfrak{p}^{\eta_{\mathfrak{p}}} = \prod_{\mathfrak{p} \in \mathfrak{P}} \mathfrak{p}^{\eta_{\mathfrak{p}} - \mu_{\mathfrak{p}}}.$$

Lo que demuestra el resultado. ∎

Corolario 2.3.11. *El monoide de los ideales fraccionarios de un dominio de Dedekind es un grupo.*

Definición 2.3.12. *Sea D un dominio de Dedekind e I y J ideales fraccionarios de D. Se dice que I divide a J si existe un ideal fraccionario K tal que $IK = J$.*

Corolario 2.3.13. *Sea D un dominio de Dedekind y $\mathfrak{A}$ un ideal no nulo de D. Entonces $\mathfrak{A}$ sólo tiene un número finito de divisores.*

Definición 2.3.14. *Sea D un dominio de Dedekind. Un ideal fraccionario I de un dominio de Dedekind con campo de cocientes Q es **principal** si $I = Dx$ para algún $x \in Q$.*

Proposición 2.3.15. *Sea D un dominio de Dedekind con campo de cocientes Q. Entonces el conjunto de ideales fraccionarios principales forman un subgrupo del grupo de ideales fraccionarios de D.*

Demostración. *Claramente D es un ideal fracionario principal. Además tenemos que para $x, y \in Q$ se tiene que $(Dx)(Dy)^{-1} = D(xy^{-1})$.* ∎

Definición 2.3.16. *Sea D un dominio de Dedekind. Si F es el grupo de ideales fraccionarios de D, y P es el grupo de ideales principales de D al cociente $C(D) = P/F$ se le denomina el **grupo de clases de ideales** de D.*

Nótese que para que D sea un dominio de ideales principales es necesario y suficiente que $C(D)$ sea un grupo con un solo elemento.

Dado un dominio de Dedekind D y $\mathfrak{p}$ un ideal primo no nulo de D, para un ideal fraccionario $\mathfrak{A}$ no nulo de D, designamos por $\eta_{\mathfrak{p}}(\mathfrak{A})$ al máximo exponente de $\mathfrak{p}$ en la factorización de $\mathfrak{A}$ como producto de ideales primos.

Proposición 2.3.17. *Sea D un anillo de Dedekind, $\mathfrak{p}$ un ideal primo no nulos de D y $\mathfrak{A}$ y $\mathfrak{B}$ ideales fraccionarios no nulo de D. Entonces*

1) $\eta_{\mathfrak{p}}(\mathfrak{AB}) = \eta_{\mathfrak{p}}(\mathfrak{A}) + \eta_{\mathfrak{p}}(\mathfrak{B})$.
2) $\eta_{\mathfrak{p}}(\mathfrak{A}^{-1}) = -\eta_{\mathfrak{p}}(\mathfrak{A})$
3) *$\mathfrak{A}$ es un ideal entero de D si y sólo si $\eta_{\mathfrak{p}}(\mathfrak{A}) \geqslant 0$ para todo $\mathfrak{p} \in \mathfrak{P}$.*
4) $\eta_{\mathfrak{p}}(\mathfrak{A} + \mathfrak{B}) = inf(\eta_{\mathfrak{p}}(\mathfrak{A}), \eta_{\mathfrak{p}}(\mathfrak{B}))$.
5) $\eta_{\mathfrak{p}}(\mathfrak{A} \cap \mathfrak{B}) = sup(\eta_{\mathfrak{p}}(\mathfrak{A}), \eta_{\mathfrak{p}}(\mathfrak{B}))$.

Proposición 2.3.18. *Sea D un anillo de Dedekind y $\mathfrak{A}$ y $\mathfrak{B}$ ideales fraccionarios no nulos de D. Entonces, $\mathfrak{A} \subseteq \mathfrak{B}$ si y sólo si $\eta_{\mathfrak{p}}(\mathfrak{A}) \geqslant \eta_{\mathfrak{p}}(\mathfrak{B})$ para todo $\mathfrak{p} \in \mathfrak{P}$.*

Demostración. *Notemos que $\mathfrak{A} \subseteq \mathfrak{B}$ es equivalente a $\mathfrak{AB}^{-1} \subseteq D$ y sean $\mathfrak{A} = \mathfrak{p}_1^{\alpha_1} \cdots \mathfrak{p}_n^{\alpha_n}$ y $\mathfrak{B} = \mathfrak{p}_1^{\beta_1} \cdots \mathfrak{p}_n^{\beta_n}$ las descomposiciones de $\mathfrak{A}$ y $\mathfrak{B}$ como producto de ideales primos.*

- $\Rightarrow$) *Como $\mathfrak{AB}^{-1} = \mathfrak{p}_1^{\alpha_1-\beta_1} \cdots \mathfrak{p}_n^{\alpha_n-\beta_n}$ es un ideal entero de D. Por el inciso 3) de la Proposición 2.3.17 se tiene que $\alpha_i - \beta_i \geqslant 0$, es decir $\alpha_i \geqslant \beta_i$. Por lo tanto $\eta_{\mathfrak{p}}(\mathfrak{A}) \geqslant \eta_{\mathfrak{p}}(\mathfrak{B})$ para todo $\mathfrak{p} \in \mathfrak{P}$.*
- $\Leftarrow$) *Supongamos que $\eta_{\mathfrak{p}}(\mathfrak{A}) \geqslant \eta_{\mathfrak{p}}(\mathfrak{B})$ para todo $\mathfrak{p} \in \mathfrak{P}$, así en particular tenemos que $\alpha_i - \beta_i \geqslant 0$ para cada $i \in \{1, \ldots, n\}$. Por otro lado, si aplicamos los incisos 2) y 3) de la Proposición 2.3.17, obtenemos que $\eta_{\mathfrak{p}}(\mathfrak{AB}^{-1}) = \eta_{\mathfrak{p}}(\mathfrak{A}) - \eta_{\mathfrak{p}}(\mathfrak{B})$, nuevamente aplicando la Proposición 2.3.17 inciso 3) se tiene entonces que $\mathfrak{AB}^{-1} \subseteq D$ y por lo tanto $\mathfrak{A} \subseteq \mathfrak{B}$.* ∎

Corolario 2.3.19. *Sea D un anillo de Dedekind y $\mathfrak{p}$ un ideal primo de D. Si $\mathfrak{A}$ es un ideal de D tal que $\mathfrak{A} \subseteq \mathfrak{p}$, entonces $\mathfrak{p}$ divide a $\mathfrak{A}$.*

Lema 2.3.20. *Sea D un anillo de Dedekind y $\mathfrak{m}$ un ideal maximal de D. Si $\mathfrak{A}$ es un ideal fraccionario no nulo de D, entonces no existe un ideal $\mathfrak{t}$ de D tal que $\mathfrak{Am} \subset \mathfrak{t} \subset \mathfrak{A}$.*

Demostración. *Por el Corolario 2.3.10 $\mathfrak{A} = \mathfrak{p}_1^{\alpha_1} \cdots \mathfrak{p}_n^{\alpha_n}$ con $\mathfrak{p}_i \in \mathfrak{P}$, así se tiene que $\mathfrak{Am} = \mathfrak{p}_1^{\alpha_1} \cdots \mathfrak{p}_n^{\alpha_n}\mathfrak{m}$. Ahora, como D es un anillo de Dedekind, $\mathfrak{m}$ es un ideal primo de D. Claramente $\eta_{\mathfrak{m}}(\mathfrak{Am}) = \eta_{\mathfrak{m}}(\mathfrak{A}) + 1$ y $\eta_{\mathfrak{p}_i}(\mathfrak{Am}) = \eta_{\mathfrak{p}_i}(\mathfrak{A})$ si $\mathfrak{p}_i \neq \mathfrak{m}$.*

Así $\mathfrak{Am} \subseteq \mathfrak{t} \subseteq \mathfrak{A}$, entonces

$$\eta_{\mathfrak{p}}(\mathfrak{Am}) = \eta_{\mathfrak{p}}(\mathfrak{t}) = \eta_{\mathfrak{p}}(\mathfrak{A}) \quad si \quad \mathfrak{p}_i \neq \mathfrak{m}$$

y

$$\eta_{\mathfrak{m}}(\mathfrak{Am}) \leqslant \eta_{\mathfrak{m}}(t) \leqslant \eta_{\mathfrak{m}}(\mathfrak{A}) + 1$$

Entonces por la Proposición 2.3.18 tenemos que $\mathfrak{t} = \mathfrak{mA}$ o $\mathfrak{t} = \mathfrak{A}$. ∎

Proposición 2.3.21. *Sea F una extensión finita de $\mathbb{Q}$ y D' el anillo de enteros de F. Si $\mathfrak{A}$ y $\mathfrak{B}$ son ideales enteros no nulos de D', entonces $N(\mathfrak{AB}) = N(\mathfrak{A})N(\mathfrak{B})$.*

Demostración. *Primero demostraremos la afirmación para el caso en que $\mathfrak{B}$ sea un ideal maximal de D'. Dado que $\mathfrak{AB} \subset \mathfrak{A}$, se tiene por el Teorema 1.1.34 que $D'/\mathfrak{A} \cong (D'/\mathfrak{AB})/(\mathfrak{A}/\mathfrak{AB})$ como D'-módulos. Luego entonces $|D'/\mathfrak{A}|\,|\mathfrak{A}/\mathfrak{AB}| = |D'/\mathfrak{AB}|$, esto es $N(\mathfrak{A})\,|\mathfrak{A}/\mathfrak{AB}| = N(\mathfrak{AB})$. Así que es suficiente demostrar que $|\mathfrak{A}/\mathfrak{AB}| = |D'/\mathfrak{B}|$.*

Ahora, $\mathfrak{A}/\mathfrak{AB}$ es un D'-módulo que es anulado por los elementos de $\mathfrak{B}$, entonces es posible darle a $\mathfrak{A}/\mathfrak{AB}$ estructura de $D'/\mathfrak{B}$-espacio vectorial. Ahora por el Teorema 1.1.35 tenemos que todo $D'/\mathfrak{B}$-subespacio de $\mathfrak{A}/\mathfrak{AB}$ es de la forma $\overline{\mathfrak{q}} = \mathfrak{q}/\mathfrak{AB}$ donde $\mathfrak{q}$ es un ideal entero que cumple que $\mathfrak{AB} \subseteq \mathfrak{q} \subseteq \mathfrak{A}$, luego al aplicar el Lema 2.3.20, podemos concluir que $\mathfrak{A}/\mathfrak{Am}$ no tiene $D'/\mathfrak{B}$-subespacios. Por lo tanto $dim_{D'/\mathfrak{B}}(\mathfrak{A}/\mathfrak{AB}) = 1$, es decir $\mathfrak{A}/\mathfrak{AB}$ es isomorfo a $D'/\mathfrak{B}$ como $D'/\mathfrak{B}$-espacio vectorial. En particular $|\mathfrak{A}/\mathfrak{AB}| = |D'/\mathfrak{B}|$ y así $N(\mathfrak{AB}) = N(\mathfrak{A})N(\mathfrak{B})$. El resultado se sigue al aplicar inducción sobre el número de factores de primos en $\mathfrak{B}$ al aplicar el Teorema 2.3.7 a $\mathfrak{B}$. ∎

Lema 2.3.22. *Sea R un anillo e I y J ideales principales de R. Entonces IJ es un ideal principal de R.*

Demostración. *Como I y J son principales, entonces existen $a, b \in R$ tales que $I = Ra$ y $J = Rb$. Claramente $IJ = Rab$.* ∎

Teorema 2.3.23. *Sean D un dominio de Dedekind con campo de cocientes Q, F una extensión finita de $\mathbb{Q}$ y D' el anillo de enteros de F. D' es un dominio de factorización única si y sólo si D' es un dominio de ideales principales.*

Demostración.

$\Rightarrow$) *En virtud del Lema 2.3.22 es suficiente demostrar que todo ideal primo no nulo de D' es principal.*

Sea $\mathfrak{p}$ un ideal primo no nulo de D', por el Corolario 2.2.44, existe $m \in \mathbb{N}$ tal que $N(\mathfrak{p}) = m$. Ahora $m = r_1 \cdots r_n$ donde r_i son elementos irreducibles en D'. El Corolario 2.2.46 nos asegura que $m \in \mathfrak{p}$, y dado que $\mathfrak{p}$ es un ideal primo, existe $i_0 \in \{1, \ldots, n\}$ tal que $r_{i_0} \in \mathfrak{p}$ y así $D'r_{i_0} \subseteq \mathfrak{p}$.

Siendo D' un dominio de ideales principales, por el Teorema 1.2.67 se tiene que r_{i_0} es un elemento primo de D' y por el Lema 1.2.36, $D'r_{i_0}$ es un ideal primo de D' y dado que D' es un dominio de Dedekind entonces D' es maximal. Luego entonces $D'r_{i_0} = \mathfrak{p}$, por lo que $\mathfrak{p}$ es un ideal principal.

$\Leftarrow$) *Es el Corolario 2.2.35.* ∎

Capítulo 3

Teorema de Minkowski

§*3.1 Subgrupos discretos de* $\mathbb{R}^n$

Consideremos $m \leqslant n$ *números naturales y* $v_1, \ldots, v_m$ *un conjunto de vectores linealmente independiente de* $\mathbb{R}^n$ *y* G *el subgrupo de* $(\mathbb{R}^n, +)$ *generado por* $v_1, \ldots, v_m$*. Nótese que* G *es un grupo libre de rango* m*, que esta generado por* m *vectores linealmente independientes en* $\mathbb{R}^n$*, bajo estas condiciones diremos que* G *es una* ***red*** *de* $\mathbb{R}^n$ *de dimensión* m*.*

En adelante consideraremos $\mathbb{R}^n$ *con la métrica usual:* $d(x,y) = \|x - y\|$*, donde para todo* $(a_1, \ldots, a_n) \in \mathbb{R}^n$ *se tiene que* $\|(a_1, \ldots, a_n)\| = \left[\sum_{i=1}^n a_i^2\right]^{\frac{1}{2}}$*. Además denotaremos a la bola cerrada con centro en* x *y radio* $r \in \mathbb{R}^+$ *por* $B_r[x]$*.*

Recordemos que un subconjunto $X \subseteq \mathbb{R}^n$ *es* ***acotado*** *si* $X \subseteq B_r[0]$ *para algún* $r \in \mathbb{R}^+$*, y que* X *es* ***discreto*** *si* $X \cap B_r[0]$ *es finito para todo* $r \in \mathbb{R}^+$*.*

Teorema 3.1.1. *Sea* $U \subseteq \mathbb{R}^n$ *abierto y* $f : U \longrightarrow \mathbb{R}^m$ *una función diferenciable en* $x_0 \in U$*. Entonces* f *es una función continua en* x_0[1]*.*

Teorema 3.1.2. *Sea* $D \subseteq \mathbb{R}^n$ *cerrado y acotado y* $f : D \longrightarrow \mathbb{R}$ *una función continua en* D*. Entonces* f *alcanza su máximo y su mínimo absoluto en* D[2]*.*

Corolario 3.1.3. *Sea* $D \subseteq \mathbb{R}^n$ *cerrado y acotado y* $f : D \longrightarrow \mathbb{R}^m$ *una función continua en* D*. Entonces* $f[D]$ *es acotado en* $\mathbb{R}^m$*.*

Corolario 3.1.4. *Sea* $D \subseteq \mathbb{R}^n$ *acotado y* $f : D \longrightarrow \mathbb{R}$ *una función continua en* D*. Entonces* $f[D]$ *es acotado en* $\mathbb{R}^m$*.*

Teorema 3.1.5. *Sea* G *un subgrupo aditivo de* $\mathbb{R}^n$*. Entonces* G *es una red de* $\mathbb{R}^n$ *de dimensión* m *si y sólo si* G *es un subgrupo discreto no trivial.*

Demostración. *Dado un subgrupo* G *de* $\mathbb{R}^n$*, podemos trabajar dentro del subespacio vectorial de* $\mathbb{R}^n$ *generado por* G*, y así suponer que* $m = n$*.*

$\Longrightarrow$) *Sea* G *un subgrupo libre de* $\mathbb{R}^n$ *y* $\beta = \{v_1, \ldots, v_n\}$ *un conjunto linealmente independiente en* $\mathbb{R}^n$ *el cual es un conjunto libre de generadores de* G*. En particular tenemos que* β *es una base de* $\mathbb{R}^n$*.*

Defínase $f : \mathbb{R}^n \longrightarrow \mathbb{R}^n$ *por* $f(v) = [v]_\beta$*, donde* $[v]_\beta$ *denota el vector de coordenadas del vector* v *respecto a la base* β*. Como* f *es lineal, entonces es una función diferenciable y así por el Teorema 3.1.1 tenemos que* f *es una función continua. Luego por el 3.1.4*

[1] Ver [*Ma*] Sección 2.3. Teorema 8.

[2] Ver [*Ma*] Sección 3.3. Teorema 7.

se tiene que para todo $r \in \mathbb{R}^+$, $f[B_r[0]]$ es acotado. Es decir para cada $r \in \mathbb{R}^+$, existe $k_r \in \mathbb{R}^+$ tal que si $v \in B_r[0]$, entonces $\|f(v)\| \leqslant k_r$.

Ahora, sea $v \in B_r[0] \cap G$. Como β es una base de $\mathbb{R}^n$ tenemos que $v = \sum_{i=1}^{n} a_i v_i$, donde $a_i \in \mathbb{Z}$ para $i = 1, \ldots, n$. El valor de cada una de las $a_{i's}$ sólo tiene un número finito de posibilidades, debido a que

$$|a_i| \leqslant \|(a_1, \ldots, a_n)\| = \|f(\sum_{i=1}^{n} a_i v_i)\| = \|f(v)\| \leqslant k_r$$

Por lo tanto $B_r[0] \cap G$ es finito. Y así concluimos que G es discreto es un subgrupo discreto de $\mathbb{R}^n$.

$\Longleftarrow$) *La demostración se hará por inducción sobre n.*

***Base**: Sea G un subgrupo discreto no trivial de $\mathbb{R}$. Tomemos $g \in G - \{0\}$ y consideremos el conjunto $G \cap B_{\|g\|}[0]$. Claramente $B_{\|g\|}[0]$ es no vacío pues $g \in G \cap B_{\|g\|}[0]$. Siendo G un subgrupo discreto de $\mathbb{R}$, entonces $G \cap B_{\|g\|}[0]$ es finito, luego podemos considerar*

$$g_0 = mín\{h \in G \cap B_{\|g\|}[0] \mid h > 0\}.$$

Mostraremos que g_0 genera a G. Notemos que $-h \in G \cap \mathbb{R}^-$ si y sólo si $h \in G \cap \mathbb{R}^+$, luego es suficiente demostrar que $G \cap \mathbb{R}^+ \subseteq \langle g_0 \rangle$. Si $h \in G \cap \mathbb{R}^+$, por el Principio de Arquímedes sabemos que existe $k \in \mathbb{R}^+$ tal que $h \leqslant kg_0$, esto asegura la existencia de

$$k_h = mín\{k \in \mathbb{Z}^+ \mid h \leqslant kg_0\},$$

De la minimalidad de k_h, se tiene que $(k_h - 1)g_0 < h \leqslant k_h g_0$, de donde se deduce que $0 < h - (k_h - 1)g_0 \leqslant g_0$, con $(h - (k_h - 1)g_0) \in G$ y dado que g_0 mínimo en $G \cap \mathbb{R}^+$ obtenemos que $h - (k_h - 1)g_0 = g_0$. Luego entonces $h \in \langle g_0 \rangle$ y así $h = k_h g_0$. Por lo tanto $G = \langle g_0 \rangle$.

Al ser g_0 linealmente independiente en $\mathbb{R}$, se obtiene que G libre de dimensión 1.

***Paso inductivo**. Supongamos que $n > 1$ y que la proposición es válida para todo natural $k < n$, y sea G un subgrupo discreto no trivial de $\mathbb{R}^n$. Dado que $\mathbb{R}^n$ es generado, como espacio vectorial, por G, podemos tomar $\{g_1, \ldots, g_n\} \subseteq G$ que forme una base de $\mathbb{R}^n$. Sea V el subespacio vectorial de $\mathbb{R}^n$ generado por $\{g_1, \ldots, g_{n-1}\}$ y consideremos*

$$G_0 = G \cap V.$$

Tomemos $r \in \mathbb{R}^+$ y denotemos por $V_r = V \cap B_r[0]$, claramente $V_r \subseteq B_r[0]$, si además consideramos el hecho de que $G_0 \subseteq G$, tenemos que

$$G_0 \cap V_r \subseteq G \cap B_r[0],$$

y como G es un subgrupo discreto de $\mathbb{R}^n$, tenemos que $G \cap B_r[0]$ es finito para todo $r \in \mathbb{R}^+$, y así $G_0 \cap_V B_r[0]$ es finito para todo $r \in \mathbb{R}^+$. Además G_0 es no trivial en V pues $\{g_1, \ldots, g_{n-1}\} \subseteq G_0$. En resumen G_0 es un subgrupo discreto no trivial de V y como $dim_{\mathbb{R}}(V) = n - 1 < n$, por hipótesis de inducción G_0 es un subgrupo libre de V que es generado, como grupo libre, por k vectores linealmente independientes en V, digamos $\{h_1, \ldots, h_k\}$. Por otro lado V está generado como espacio vectorial por G_0, así $\{h_1, \ldots, h_k\}$ es un conjunto de generadores de V, luego entonces $\{h_1, \ldots, h_k\}$ es una base de V y así $k = n - 1$.

Como $g_n \notin V$, concluimos que $\{h_1, \ldots, h_{n-1}, g_n\}$ es linealmente independiente en $\mathbb{R}^n$ y por lo tanto es una base de $\mathbb{R}^n$.

Sea

$$T = \left\{ \sum_{i=1}^{n-1} a_i h_i + a_n g_n \in G \mid 0 \leqslant a_i < 1 \text{ si } i = 1, \ldots, n-1 \text{ y } 0 \leqslant a_n \leqslant 1 \right\}.$$

Al considerar $M = \sum_{i=1}^{n-1} \|h_i\| + \|g_n\|$, *se tiene que para todo* $v \in T$, $\|v\| \leqslant M$. *es decir,* T *es un subconjunto acotado de* $\mathbb{R}^n$.

Como $g_n \in T$, *éste es no vacío, además de ser discreto por estar contenido en* G. *Luego siendo que* T *es acotado, entonces* T *es finito, es así que podemos tomar*

$$x = b_1h_1 + \cdots + b_{n-1}h_{n-1} + b_ng_n \in T \tag{1.1}$$

con la propiedad de ser b_n *mínimo positivo. Nótese que* $0 < b_n \leqslant 1$.

Recordemos que $\{h_1, \ldots, h_{n-1}, g_n\}$ *es una base de* $\mathbb{R}^n$, *y que al ser* x *combinación lineal no trivial de ésta última (con* $b_n \neq 0$*), se tiene que* $\{h_1, \ldots, h_{n-1}, x\}$ *es otra base de* $\mathbb{R}^n$ *que está formada por vectores que pertenecen a* G. *Así es suficiente mostrar que* $\{h_1, \ldots, h_{n-1}, x\}$ *genera a* G *como grupo abeliano libre para verificar* G *es libre de dimensión* n.

Consideremos $g \in G$, *y sean* $c_i \in \mathbb{R}$ *con* $i \in \{1, \ldots, n\}$ *tales que*

$$g = c_1h_1 + \cdots + c_{n-1}h_{n-1} + c_ng_n. \tag{1.2}$$

Recordemos que b_n *es un entero positivo, así es posible encontrar un entero* d_n *tal que*

$$\frac{c_n}{b_n} - 1 < d_n \leqslant \frac{c_n}{b_n}.$$

Ahora, para cada $i \in \{1, \ldots, n-1\}$ *definamos* $d_i = [c_i - d_nb_i]$, *donde los corchetes representan la parte entera y los* $b_{i's}$ *están dados en la ecuación (1.1).*

Sea

$$g' = g - (d_1h_1 + \cdots + d_{n-1}h_{n-1} + d_nx)$$

Luego podemos jugar con esta última expresión y obtener

$$\begin{aligned}
g' &\underset{(1.1)}{=} g - (d_1h_1 + \cdot + d_{n-1}h_{n-1} + d_n(b_1h_1 + \cdots + b_{n-1}h_n - 1 + b_ng_n)) \\
&= g - ((d_1 + d_nb_1)h_1 + \cdots + (d_{n-1} + d_nb_{n-1})h_{n-1} + d_nb_ng_n) \\
&\underset{(1.2)}{=} (c_1h_1 + \cdots + c_{n-1}h_{n-1} + c_ng_n) - ((d_1 + d_nb_1)h_1 + \cdots + (d_{n-1} + d_nb_{n-1})h_{n-1} + d_nb_ng_n) \\
&= ((c_1 - d_nb_1) - d_1)h_1 + \cdots + ((c_{n-1} - d_nb_{n-1}) - d_{n-1})h_{n-1} + (c_n - d_nb_n)g_n
\end{aligned}$$

Por la elección de los $d_{i's}$ *tenemos que* $0 \leqslant (c_i - d_nb_i) - d_i < 1$ *y por como se tomó* d_n, *se tiene que* $0 \leqslant c_n - d_nb_n < b_n \leqslant 1$. *Así* $g' \in T$. *Ahora considerando la minimalidad de* b_n, *concluimos que* $c_n - d_nb_n = 0$. *Por lo tanto* $g' \in V$ *y como por construcción* $g' \in G$, *entonces* $g' \in V \cap G = G_0$. *Luego, concluimos que*

$$g = \underbrace{g' + d_1h_1 + \cdots + d_{n-1}h_{n-1}}_{G_0} + d_nx$$

Siendo que G_0 *es un grupo libre con base* $\{h_1, \ldots, h_{n-1}\}$, *tenemos entonces que* G *es un grupo libre con base* $\{h_1, \ldots, h_{n-1}, x\}$. ∎

En vista del Teorema 3.1.5, si G *es una red de dimensión* m *en* $\mathbb{R}^n$, *en adelante nos referiremos a* G *por* ***subgrupo discreto de dimensión*** m *de* $\mathbb{R}^n$.

Si G *es un grupo discreto de* $\mathbb{R}^n$ *de dimensión* m, *con una base* $\beta = \{g_1, \ldots, g_m\}$, *el* ***dominio fundamental*** *respecto a la base* β *(también llamado región fundamental o dominio de Dedekind), está dado por*

$$D_\beta = \{\sum_{i=1}^{m} a_ig_i \mid a_i \in \mathbb{R} \text{ y } 0 \leqslant a_i < 1 \text{ para } i = 1, \ldots, m\}.$$

Obsérvese que el dominio fundamental depende de la elección de la base. Por ejemplo, si tomamos $\beta = \{e_1, e_2\}$ *la base canónica de* $\mathbb{R}^2$*, y* $\beta' = \{e_1, e_1 + e_2\}$*, tenemos que* β *y* β' *generan el mismo grupo discreto de dimensión 2 en* $\mathbb{R}^2$*, sin embargo* $D_\beta \neq D_{\beta'}$*. Como se muestra en la figura*

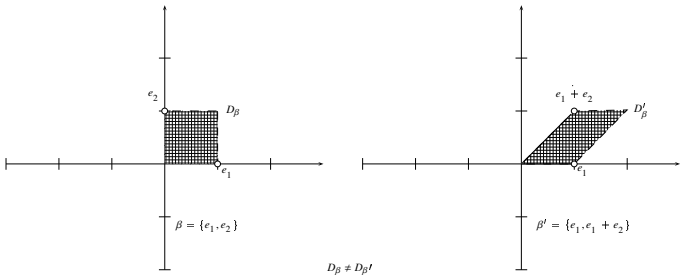

FIGURA 1. Dos bases del mismo subgrupo discreto de $\mathbb{R}^n$ pueden generar dos regiones fundamentales distintas.

Consideremos G un subgrupo discreto de $\mathbb{R}^n$ *de dimensión n, con base* $\beta = \{g_1, \ldots, g_n\}$*. Si* $g \in \mathbb{R}^n$ *este se puede escribir de manera única como*

$$g = \alpha_1 g_1 + \ldots, \alpha_n g_n \text{ con } \alpha_i \in \mathbb{R}$$

Para cada $i = 1, \ldots, n$ *tomemos* $a_i = [\alpha_i]$ *y sea* $l = a_1 g_1 + \cdots + a_n g_n \in G$*. Notemos que* $g - l \in D_\beta$*. Ahora vamos a verificar que l es el único elemento en G que tiene esta propiedad para con g. Para ello tomemos* $m = \sum_{i=1}^n b_i g_i \in G$ *tal que* $g - m \in D_\beta$*, como* $g - m = \sum_{i=1}^n (\alpha_i - b_i) g_i$*, se tiene que* $0 \leqslant \alpha_i - b_i < 1$ *para* $i = 1, \ldots, n$*. Como también* $0 \leqslant \alpha_i - a_i < 1$ *si* $i = 1, \ldots, n$*, podemos concluir que* $\mid (\alpha_i - b_i) - (\alpha_i - a_i) \mid = \mid a_i - b_i \mid < 1$ *para cada* $i = 1, \ldots, n$*.*

Ahora, dado que $l - m = \sum_{i=1}^n (a_i - b_i) g_i \in G$*,* $a_i - b_i \in \mathbb{Z}$ *y como* $\mid a_i - b_i \mid < 1$*, forzosamente* $a_i - b_i = 0$ *para todo* $i \in \{1, \ldots, n\}$*. Por lo tanto* $l = g$ *y así verificamos que l es el único elemento en G tal que* $g - l \in D_\beta$*.*

Consideremos β *una base de G y definamos para cada* $l \in G$

$$l + D_\beta = \{l + d \mid d \in D_\beta\}.$$

y obsérvese $g \in l + D_\beta$ *si y sólo si* $g - l \in D_\beta$*.*

Notemos que $\{l + D_\beta \mid l \in G\}$ *cumple con las siguientes propiedades*

i) *Para cada* $l \in G$ *se tiene que* $l + D_\beta$*, pues* $l \in l + D_\beta$*.*
ii) $(l_1 + D_\beta) \cap (l_2 + D_\beta) = \varnothing$ *si* $l_1 \neq l_2$*.*
iii) $\bigcup_{l \in G} l + D_\beta = \mathbb{R}^n$*.*

En resumen hemos visto que $\{l + D_\beta \mid l \in G\}$ *es un partición de* $\mathbb{R}^n$*.*

§3.2 *El toro cociente*

En esta sección se estudiará el grupo cociente $\mathbb{R}^n/G$*, con G un subgrupo discreto de dimensión m de* $\mathbb{R}^n$*. En adelante S denotará el conjunto de los números complejos de norma 1, que es un subgrupo del grupo multiplicativo* $(U(C), \cdot)$*.*

Lema 3.2.1. *El grupo cociente* $(\mathbb{R}/\mathbb{Z}, +)$ *es isomorfo al grupo* $(S, \cdot)$*.*

Demostración. *Defínase* $\phi : \mathbb{R} \longrightarrow S$*, dada por* $\phi(r) = e^{2\pi i r}$*. Recordemos que* $e^{2\pi i r} = cos(2\pi r) + isen(2\pi r)$*, luego para* $r \in \mathbb{R}$ $\|e^{2\pi i r}\| = cos^2(2\pi r) + sen^2(2\pi r)$=1*, así aseguramos que* ϕ *esta bien definida. Si* $r_1, r_2 \in \mathbb{R}$*, tenemos que*

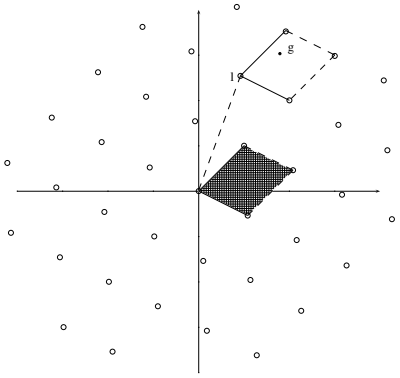

FIGURA 2. Si G es un subgrupo discreto de $\mathbb{R}^n$, entonces $\{l + D_\beta \mid l \in G\}$ es una partición de $\mathbb{R}^n$.

$$\begin{aligned}
\phi(r_1 + r_2) &= e^{2\pi i(r_1+r_2)} \\
&= cos(2\pi(r_1 + r_2)) + isen(2\pi(r_1 + r_2)) \\
&= [cos(2\pi r_1)cos(2\pi r_2) - sen(2\pi r_1)sen(2\pi r_2)] + i\,[sen(2\pi r_1)cos(2\pi r_2) + sen(2\pi r_2)cos(2\pi r_1)] \\
&= \big[cos(2\pi r_1) + isen(2\pi r_1)\big]\,\big[cos(2\pi r_2) + isen(2\pi r_2)\big] \\
&= e^{2\pi i r_1} e^{2\pi i r_1} \\
&= \phi(r_1)\phi(r_2).
\end{aligned}$$

Lo que asegura que ϕ es un homomorfismo de grupos.

Si $z \in S$, sabemos que existe $\theta \in \mathbb{R}$ tal que $cos(\theta) + isen(\theta) = z$, al hacer $r = \frac{\theta}{2\pi}$ se tiene que $\phi(r) = z$, es decir ϕ es sobreyectiva. Por otro lado $r \in ker(\phi)$ si y sólo si $cos(2\pi r) + isen(2\pi r) = 1$, y esto último pasa si y sólo si $cos(2\pi r) = 1$ y $sen(2\pi r) = 0$. Luego entonces $r \in ker(\phi)$ si y sólo si $r \in \mathbb{Z}$.

Aplicando el Primer Teorema de Isomorfismo de grupos ϕ, concluimos que $\mathbb{R}/\mathbb{Z} \cong S$. ∎

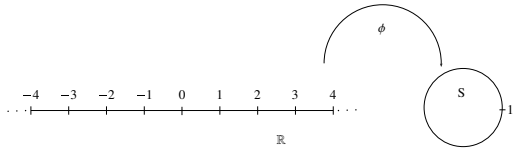

FIGURA 3. Lema 3.2.1

Denótese por T^n el producto directo de n copias de S; T^n recibe el nombre de ***toro*** *$n-$**dimensional**. Por ejemplo para $n = 2$ se puede identificar con el toro $2-$dimensional con el toro geométrico de revolución.*

Teorema 3.2.2. *Sea G un subgrupo discreto de $\mathbb{R}^n$ de dimensión n entonces $\mathbb{R}^n/G$ es isomorfo a T^n.*

Demostración. *Sea $\beta = \{g_1, \ldots, g_n\}$ una $\mathbb{Z}$-base de G. Dado que β es una base de $\mathbb{R}^n$, si $v \in \mathbb{R}^n$, se tiene que*

$$v = \alpha_1 g_1 + \cdots + \alpha_n g_n \text{ con } \alpha_i \in \mathbb{R}.$$

Defínase $\Phi_\beta : \mathbb{R}^n \longrightarrow T^n$ como $\Phi_\beta(v) = (e^{2\pi i\alpha_1}, \ldots, e^{2\pi i\alpha_n})$ para $v \in \mathbb{R}^n$. Claramente Φ_β es un morfismo suprayectivo de grupos y tenemos que $v = \sum_{i=1}^n \alpha_i g_i \in ker(\Phi)$ si y sólo si $e^{2\pi i\alpha_i} = 1$ para

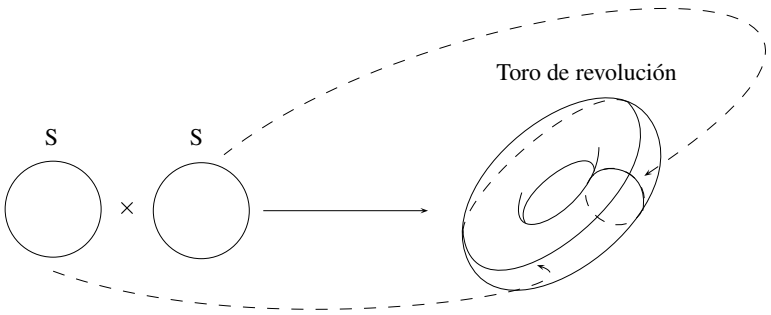

FIGURA 4. Identificación del toro 2−dimensional con el toro de revolución.

cada $i \in \{1,\ldots,n\}$. Esto último pasa si y solo si $\alpha_i \in \mathbb{Z}$ para cada $i \in \{1,\ldots,n\}$, luego entonces $ker(\Phi) = G$. Aplicando el Primer Teorema de Isomorfismo de Gupos obtenemos que $\mathbb{R}^n/G \cong T^n$. ∎

Topológicamente se puede obtener T^n por el "pegado "(la identificación) de caras opuestas de un dominio fundamental (Fig 5).

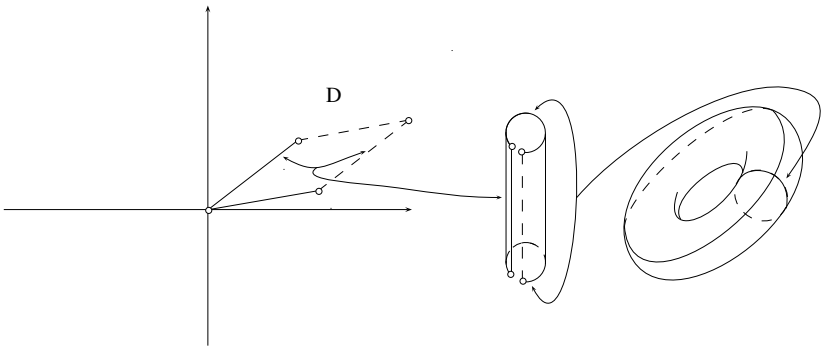

FIGURA 5. Idealización geométrica de T^n.

Si G es un subgrupo discreto de $\mathbb{R}^n$ de dimensión m, hemos visto que G puede considerarse un subgrupo de $\mathbb{R}^m$, así que, es natural el siguiente

Corolario 3.2.3. *Sea G un subgrupo discreto de $\mathbb{R}^n$ de dimensión m. Entonces $\mathbb{R}^n/G \cong (T^m \times R^{n-m})$.*

Demostración. *Sea V el subespacio generado por G y sea W un complemento directo de V, es decir $\mathbb{R}^n = V \oplus W$, además $V \cong \mathbb{R}^m$ y $W \cong \mathbb{R}^{n-m}$. Luego*

$$\begin{aligned}\mathbb{R}^n/G &= (V \oplus W)/G \\ &\underset{\text{Prop. 1.1.36}}{\cong} V/G \oplus W \\ &\underset{\text{Teo. 2.2.2}}{\cong} T^m \oplus W \\ &\underset{W \cong \mathbb{R}^{n-m}}{\cong} T^m \oplus \mathbb{R}^{n-m}.\end{aligned}$$ ∎

Corolario 3.2.4. *Sea G un subgrupo discreto de $\mathbb{R}^n$ de dimensión n con base $\beta = \{g_1, \ldots, g_n\}$, y sea D_β el dominio fundamental respecto a la base β. Consideremos el morfismo Φ_β dado en la demostración del Teorema 3.2.2 y sea*

$$\begin{aligned}\Phi|_{D_\beta} : D_\beta &\longrightarrow T^n \\ \textstyle\sum_{i=1}^n \alpha_i g_i &\longmapsto (e^{2\pi i \alpha_1}, \ldots, e^{2\pi i \alpha_n})\end{aligned}$$

Entonces $\Phi|_{D_\beta}$ es una biyección.

Demostración. *Primero veremos que $\Phi|_{D_\beta}$ es una función sobreyectiva. Para ello tomemos $t \in T^n$, en el Teorema 3.2.2 vimos que Φ_β es sobreyectiva, entonces existe $g \in \mathbb{R}^n$ tal que $\Phi(g) = t$. Dado que $\{l + D_\beta \mid l \in G\}$ es una partición de $\mathbb{R}^n$ (ver página 71) tenemos que existe $l \in G$ tal que $g \in l + D_\beta$ o equivalentemente $g - l \in D_\beta$. Ahora*

$$\begin{aligned}\Phi|_{D_\beta}(g - l) &= \Phi_\beta(g - l) \\ &= \Phi_\beta(g)\Phi_\beta(l)^{-1} \\ &\underset{l \in G = ker(\Phi_\beta)}{=} \Phi_\beta(g) \\ &= t\end{aligned}$$

Luego entonces $\Phi|_{D_\beta}$ es una función sobreyectiva.

Ahora verificaremos la inyectividad de $\Phi|_{D_\beta}$, supongamos que existen $h_1, h_2 \in D_\beta$ tales que $\Phi|_{D_\beta}(h_1) = \Phi|_{D_\beta}(h_2)$, en particular $\Phi_\beta(h_1) = \Phi_\beta(h_2)$, y así $h_1 - h_2 \in ker(\Phi_\beta) = G$. Como β es una base de $\mathbb{R}^n$ tenemos que $h_1 = \sum_{i=1}^n \alpha_i g_i$ y $h_2 = \sum_{i=1}^n \beta_i g_i$, y además $0 \leqslant \alpha_i, \beta_i < 1$ para $i \in \{1, \ldots, n\}$, notemos que esto último implica que $0 \leqslant \mid \alpha_i - \beta_i \mid < 1$. Siendo que $h_1 - h_2 = \sum_{i=1}^n (\alpha_i - \beta_i) g_i \in G$, entonces $\alpha_i - \beta_i \in \mathbb{Z}$ para $i \in \{1, \ldots, n\}$, por lo que forzosamente $\alpha_i - \beta_i = 0$ para cada $i \in \{1, \ldots, n\}$. Es decir $\Phi|_{D_\beta}$ es una función inyectiva.

Concluimos que $\Phi|_{D_\beta}$ es una biyección entre D_β y T^n. ∎

En cálculo de varias variables se define el volumen de un subconjunto X de $\mathbb{R}^n$ por

$$V(X) = \int_X dx_1 \ldots dx_n.^3$$

Notemos que el volumen existe sólo cuando la integral existe.

Usando la biyección $\Phi|_{D_\beta}$ del Corolario 3.2.4 se generará el concepto de volumen en T^n. Para ello consideremos G un subgrupo discreto de $\mathbb{R}^n$ de dimensión n con base β y $Y \subseteq T^n$. Se define el volumen de Y con respecto a la base β como

$$V_\beta(Y) = V(\Phi|_{D_\beta}^{-1}(Y)).$$

Notemos que el volumen de Y depende de la base β que se ha elegido para trabajar.

[3] Demostración ver $[Ap]$ Secc. 11.33.

Definición 3.2.5. *Sean $f : \mathbb{R}^n \longrightarrow \mathbb{R}^m$ una función diferenciable en $\overline{x_0} \in \mathbb{R}^n$ dada por*

$$f(x_1, \ldots, x_n) = (f_1(x_1, \ldots, x_n), \ldots, f_m(x_1, \ldots, x_n)),$$

entonces la matriz Jacobiana de f en $\overline{x_0}$ esta dado por

$$J_g(\overline{x_0}) \begin{pmatrix} \frac{\partial f_1}{\partial x_1}(\overline{x_0}) & \ldots & \frac{\partial f_1}{\partial x_n}(\overline{x_0}) \\ \vdots & & \vdots \\ \frac{\partial f_m}{\partial x_1}(\overline{x_0}) & \ldots & \frac{\partial f_m}{\partial x_n}(\overline{x_0}) \end{pmatrix}.$$

Teorema 3.2.6 *(de Cambio de variables.). Sean $f : U \subseteq \mathbb{R}^n \longrightarrow \mathbb{R}$ una función integrable en U y $g : V \subseteq \mathbb{R}^n \longrightarrow U$ un difeomorfismo de clase C^1. Entonces $f \circ g$ es integrable en V y además*

$$\int_U f(\overline{y}) d\overline{y} = \int_V (f \circ g)(\overline{x}) \mid D_g(x) \mid d\overline{x}.$$

Donde D_g es el Jacobiano (el determinante de la matriz Jacobiana) de g.[4]

Lema 3.2.7. *Sean $L : \mathbb{R}^n \longrightarrow \mathbb{R}^m$ una función lineal, entonces $J_L(\overline{x}) = L(\overline{x})$ para todo $\overline{x} \in \mathbb{R}^n$.*

Proposición 3.2.8. *Sea G un subgrupo discreto de $\mathbb{R}^n$ con base $\beta = \{g_1, \ldots, g_n\}$. Para cada $i \in \{1, \ldots, n\}$, supongamos que $g_i = (a_{1i}, \ldots, a_{1n})$. Entonces el volumen de la región fundamental D_β esta dado por*

$$V(D_\beta) = \mid det(a_{ij}) \mid .$$

Demostración. *Por definición*

$$V(D_\beta) = \int_{D_\beta} dx_1 \ldots dx_n.$$

Ahora, defínanse nuevas variables dadas por

$$x_i = \sum_{j=1}^{n} a_{ij} y_j \; con \; y_i \in [0, 1).$$

Quedando definida la parametrización

$$\lambda : \underbrace{[0,1) \times \cdots \times [0,1)}_{n-veces} \longrightarrow D_\beta \qquad .$$

$$(y_1, \ldots, y_n) \longmapsto \left(\sum_{j=1}^{n} a_{1j} y_j, \ldots, \sum_{j=1}^{n} a_{nj} y_j \right)$$

Nótese que λ es la restricción de una transformación lineal biyectiva que tiene como imagen a D_β y por el Lema 3.2.7 tiene como matriz jacobiana (a_{ij}). Así el Jacobiano del sistema esta dado por $J_\lambda \mid det(a_{ij}) \mid$, que es constante en $\mathbb{R}^n$.

Si denotamos a $\underbrace{[0,1) \times \cdots \times [0,1)}_{n-veces}$ por D, y aplicamos el teorema de cambio de variables (Teorema 3.2.6). Obtenemos que

[4] Demostración ver $[Ap]$ Secc. 11.32.

$$\begin{aligned}
\int_{D_\beta} dx_1 \dots dx_n &\underset{\text{Teo. 3.2.6}}{=} \int_D \mid det(a_{ij}) \mid dy_1 \dots dy_n \\
&\underset{J_\lambda \ \text{constante}}{=} \mid det(a_{ij}) \mid \int_D dy_1 \dots dy_n \\
&= \mid det(a_{ij}) \mid \int_0^1 dy_1 \cdots \int_0^1 dy_n \\
&= \mid det(a_{ij}) \mid
\end{aligned}$$

Por lo tanto $V(D_\beta) = \mid det(a_{ij}) \mid$. ∎

Corolario 3.2.9. *Sea G un subgrupo discreto de* $\mathbb{R}^n$ *con* $\beta = \{g_1, \dots, g_n\}$ $\beta' = \{g'_1, \dots, g'_n\}$ *bases de G. Entonces*

$$V(D_\beta) = V(D_{\beta'}).$$

Demostración. *Supongamos que* $g_i = (a_{1i}, \dots, a_{1n})$ *y* $g'_i = (a'_{1i}, \dots, a'_{1n})$ *para cada* $i \in \{1, \dots, n\}$. *Al ser* β *y* β' *bases de G, por el Teorema 3.3.21 se tiene que existe* (b_{ij}) *una matriz unimodular que lleva la base* β *en la base* β'. *Es decir*

$$\begin{pmatrix} b_{11} & \cdots & b_{1n} \\ \vdots & \vdots & \vdots \\ b_{n1} & & b_{nn} \end{pmatrix} \begin{pmatrix} a_{1j} \\ \vdots \\ a_{nj} \end{pmatrix} = \begin{pmatrix} a'_{1j} \\ \vdots \\ a'_{nj} \end{pmatrix}$$

y además $det(b_{ij}) = 1$. *Luego entonces*

$$\begin{aligned}
V(D_{\beta'}) &\underset{\text{Teo. 3.2.8}}{=} \mid det(a'_{ij}) \mid \\
&= \mid det(b_{ij})(a_{ij}) \mid \\
&\underset{\text{Pro. del determinante}}{=} \mid det(b_{ij}) det(a_{ij}) \mid \\
&= \mid det(b_{ij}) \mid\mid det(a_{ij}) \mid \\
&\underset{(b_{ij}) \ \text{es unimodular.}}{=} \mid det(a_{ij}) \mid \\
&\underset{\text{Teo. 3.2.8}}{=} V(D_\beta).
\end{aligned}$$

Por lo tanto $V(D_\beta) = V(D_{\beta'})$. ∎

Corolario 3.2.10. *Sea G un subgrupo discreto de* $\mathbb{R}^n$ *con base* $\beta = \{g_1, \dots, g_n\}$. *Si H es un subgrupo de G de rango n, entonces existe* $\gamma = \{h_1, \dots, h_n\}$ *base de H*

$$V(D_\gamma) = \mid G/H \mid V(D_\beta).$$

Demostración. *Por el Teorema 1.3.13 sabemos que existe una base* $\{g_1, \dots, g_n\}$ *de G y* $\alpha_1, \dots, \alpha_n$ *enteros tales que* $\gamma = \{\alpha_1 g_1, \dots, \alpha_n g_n\}$ *es una base de H. Como en el Teorema 3.2.8 supongamos que* $g_i = (a_{i1}, \dots, a_{in})$, *luego* $\alpha_j g_j = (\alpha_j a_{ji}, \dots, \alpha_j a_{jn})$. *Resumiendo tenemos que*

$$\begin{aligned}
V(D_\gamma) &\underset{\text{Teo. 3.2.8}}{=} \mid det(\alpha_i a_{ij}) \mid \\
&= \mid \left(\prod_{i=1}^{n} \alpha_i \right) det(a_{ij}) \mid \\
&= \mid \prod_{i=1}^{n} \alpha_i \mid\mid det(a_{ij}) \mid \\
&\underset{\text{Cor. 1.3.21}}{=} \mid G/H \mid\mid det(a_{ij}) \mid \\
&\underset{\text{Teo. 3.2.8}}{=} \mid G/H \mid V(D_\beta).
\end{aligned}$$

∎

En relación al Corolario 3.2.9 es posible definir el ***volumen de un subgrupo discreto*** *de* $\mathbb{R}^n$ *como el volumen de cualquiera de sus bases, y así, si G es un subgrupo discreto de* $\mathbb{R}^n$ *denotarlo simplemente por* $V(G)$.

Teorema 3.2.11. *Sea G un subgrupo discreto de $\mathbb{R}^n$ de dimensión n con base β. Sea Φ como en el Teorema 3.2.2. Consideremos X un subconjunto acotado de $\mathbb{R}^n$ tal que $V(X)$ existe. Si $V(\Phi_\beta(X)) \neq V(X)$, entonces $\Phi_\beta \mid_X$ no es inyectiva.*

Demostración. *Supongamos que $\Phi_\beta \mid_X$ es inyectiva. Al ser X acotado, existen $h_1, \ldots, h_m \in G$ distintos tales que $X \subseteq \bigcup_{i=1}^{m}(h_i + D_\beta)$.*

Para cada $i \in \{1, \ldots, m\}$ tomemos $X_i = X \cap (h_i + D_\beta)$ y $Y_i = \{x - h_i \mid x \in X_i\}$. Nótese que $X = \bigcup_{i=1}^{n} X_i$.

Por otro lado, para todo $i \in \{1, \ldots, n\}$ se tiene que $Y_i \subseteq D_\beta$. Además si $y \in Y_i \cap Y_j$ con $i \neq j$, entonces $y = x_i - h_i$ y $y = x_j - h_j$ para algún $x_i \in X_i$ y $x_j \in X_j$, y así

$$\Phi_\beta(x_i) = \Phi_\beta(y + h_i) = \Phi_\beta(y + h_j) = \Phi_\beta(x_j)$$

al ser Φ_β inyectiva se tendría que $x_i = x_j$ y así $h_i = h_j$ lo que sería contradictorio pues $i \neq j$ y sabemos que el conjunto $\{h + D_\beta \mid h \in G\}$ es una partición de $\mathbb{R}^n$. Luego entonces, $Y_i \cap Y_j = \varnothing$ si $i \neq j$.

Siendo que las traslaciones son funciones funciones isométricas tenemos que

$$V(Y_i) = V(X_i) \text{ para cada } i \in \{1, \ldots, m\}$$

Además tenemos que $\Phi_\beta \mid_{D_\beta} (Y_i) = \Phi(X_i)$, luego $Y_i = \Phi \mid_{D_\beta}^{-1} (\Phi(X_i))$.

Entonces

$$\begin{aligned}
V(\Phi_\beta(X)) &= V(\Phi_\beta(\bigcup_{i=1}^{n} X_i)) \\
&\underset{X_{i's} \text{ son ajenos}}{=} V(\bigcup_{i=1}^{n} \Phi_\beta(X_i)) \\
&= V(\Phi_\beta^{-1}(\bigcup_{i=1}^{n} \Phi_\beta(X_i))) \\
&= V(\bigcup_{i=1}^{n} \Phi_\beta^{-1}(\Phi_\beta(X_i))) \\
&= V(\bigcup_{i=1}^{n} Y_i) \\
&\underset{Y_{i's} \text{ son ajenos}}{=} \sum_{i=1}^{n} V(Y_i) \\
&= \sum_{i=1}^{n} V(X_i) \\
&= V(X).
\end{aligned}$$

lo que es una contradicción y por lo tanto $\Phi_\beta \mid_X$ no es inyectiva. ∎

§3.3 Teorema de Minkowski

*Recordemos que un subconjunto $X \subseteq \mathbb{R}^n$ se dice **convexo** si para cualesquiera $x, y \in X$, el segmento que los une está contenido en X. En términos algebraicos, X es convexo si para todo $x, y \in X$*

$$\{\lambda x + (1 - \lambda)y \mid \lambda \in [0, 1]\} \subseteq X.$$

Se dice que un subconjunto $X \subseteq \mathbb{R}^n$ es simétrico respecto al origen si $x \in X$ implica que $-x \in X$.

Teorema 3.3.1 *(Minkowski). Sea G un subgrupo discreto de $\mathbb{R}^n$ de dimensión n , y sea X un subconjunto acotado simétrico y convexo de $\mathbb{R}^n$. Si*

$$V(X) > 2^n V(G),$$

entonces $X \cap G \neq \{\overline{0}\}$.

Demostración. *Consideremos $\beta = \{g_1, \ldots, g_n\}$ una base de G con dominio fundamental D_β y sea $2G$ el subgrupo libre generado por $2\beta = \{2g_1, \ldots, 2g_n\}$. Por la Proposición 3.2.8 tenemos que*

$$V(2G) = 2^n V(G)$$

Por otro lado si consideramos $\Phi_{2\beta}$ el homomorfismo natural con núcleo $2G$ definido en el Teorema 3.2.2, se tiene que

$$V(\Phi_{2\beta}(X)) \leqslant V(2G) = 2^n V(G) < V(X)$$

Por el Teorema 3.2.11 $\Phi_{2\beta}\,|_X$ no es inyectiva, por lo que existen $x_1, x_2 \in X$ con $x_1 \neq x_2$ tales que $\Phi_{2\beta}(x_1) = \Phi_{2\beta}(x_2)$, o equivalentemente $x_1 - x_2 \in 2G$.

Siendo X simétrico y como $x_2 \in X$, tenemos que $-x_2 \in X$. Y como X es convexo $\lambda x_1 + (1-\lambda)(-x_2) \in X$, en particular para $\lambda = \frac{1}{2}$ se tiene que $\frac{1}{2}(x_1 - x_2) \in X$.

Por otro lado $x_1 - x_2 \in 2G$, luego $\frac{1}{2}(x_1 - x_2) \in G$. Así $0 \neq \frac{1}{2}(x_1 - x_2) \in X \cap G$.

Por último si suponemos que $\frac{1}{2}(x_1 - x_2) = 0$, entonces $x_1 - x_2 = 0$ lo que sería una contradicción. ∎

§3.3.1 Aplicaciones en teoría de números clásica

En esta sección se demostrarán dos teoremas clásicos en la teoría de números, los cuales tardaron mucho tiempo en resolver matemáticos de la talla de Euler y Lagrange con técnicas sofisticadas y complejas. Sin embargo usando el Teorema Minkowski estos resultados pueden demostrarse de manera bastante sencilla.

Teorema 3.3.1 *(Teorema de la suma de dos cuadrados). Si p es un número primo de la forma $4k+1$ entonces p es la suma de dos cuadrados enteros.*

Demostración. *Consideremos p un número primo de la forma $4k+1$. $\mathbb{Z}_p$ es un campo finito, luego por el Teorema 1.4.54 tenemos que $(U(\mathbb{Z}_p), \cdot)$ es un grupo abeliano cíclico y de orden $p - 1 = 4k$. Como 4 divide al orden del grupo, existe $\overline{u} \in \mathbb{Z}_p^*$ tal que $ord(\overline{u}) = 4$. Siendo $\overline{-1}$ el único elemento de orden 2 en $U(Z_p)$, se tiene que $\overline{u}^2 = \overline{-1}$.*

Sea $G = \{(a,b) \in \mathbb{Z}^2 \mid b \equiv ua(\text{mód } p)\}$. Claramente $(0,0) \in G$, además si $(a,b),(c,d) \in G$, como $b \equiv ua(\text{mód } p)\}$ y $d \equiv uc(\text{mód } p)\}$, luego entonces $(b-d) \equiv u(a-c)(\text{mód } p)\}$, lo que significa que $(a-c, b-d) \in G$, y por lo tanto G es un subgrupo de $\mathbb{Z}^2$.

Ahora, dado que $\overline{u} \in \mathbb{Z}_p^*$, existe $v \in \mathbb{Z}$ tal que $uv \equiv 1 (mod\ \ p)$, siendo así que $(v,1) \in G$, y por lo tanto G es no trivial.

Ahora si $(a,b) \in \mathbb{Z}^2$, se tiene que $p(a,b) = (pa, pb) \in G$ y por lo tanto a $\mathbb{Z}^2/G$ se le puede dar estructura de $\mathbb{Z}_p$ espacio vectorial. Como $\{(1,0),(0,1)\}$ es un conjunto libre de generadores de $\mathbb{Z}^2$, en particular $\{\overline{(1,0)}, \overline{(0,1)}\}$ es un conjunto que genera a $\mathbb{Z}^2/G$ como $\mathbb{Z}_p$ espacio vectorial, notemos que $\overline{v}\overline{(1,0)} + \overline{(0,1)} = \overline{(v,1)} = \overline{(0,0)}$, es decir $\{\overline{(1,0)}, \overline{(0,1)}\}$ es $\mathbb{Z}_p$-linealmente dependiente y por lo tanto $\{\overline{(1,0)}\}$ es una base de $\mathbb{Z}^2/G$. Entonces $|\ \mathbb{Z}^2/G\ | = p$.

Ahora de la Proposición 3.2.8 tenemos que $V(\mathbb{Z}^2) = 1$ y por el Corolario 3.2.10 es necesario que $V(G) = p$. Luego por el Teorema de Minkowski (3.3.1), todo círculo con centro en el origen de radio r y con área $\pi r^2 > 4p = 2^2 p$ contiene un punto no trivial de G.

Tomando $r^2 = \frac{3p}{2}$, se obtiene que $\pi\frac{3p}{2} > \frac{9p}{2} > 4p$, así que para este r en particular, existe un punto $(a,b) \in G$, con $(a,b) \neq (0,0)$ tal que

$$0 \neq a^2 + b^2 \leqslant r^2 = \frac{3p}{2} < 2p.$$

Por otro lado

$$\overline{a}^2 + \overline{b}^2 = \overline{a}^2 + \overline{ua}^2 = \overline{a}^2 + \overline{u}^2\overline{a}^2 = \overline{a}^2 - \overline{a}^2 = \overline{0},$$

es decir $p \mid a^2 + b^2$, *obteniendo que* $p \leqslant a^2 + b^2 < 2p$, *y al ser* $a^2 + b^2$ *un entero, forzosamente deber ser que* $p = a^2 + b^2$. ∎

Lema 3.3.2. *El volumen de una n-esfera de radio a esta dado por* $\frac{\pi^{\frac{n}{2}} r^n}{\Gamma(\frac{n}{2}+1)}$, *donde* $\Gamma(n) = \int_0^\infty t^{n-1}e^{-t}dt$.[5]

Teorema 3.3.3 *(La suma de cuatro cuadrados). Todo entero positivo es la suma de cuatro cuadrados.*

Demostración. *Primero se demostrará el resultado para los números primos, para luego extenderlo a todos los enteros.*

Como $2 = 1^2 + 1^2 + 0 + 0$, *podemos suponer que p es un número primo impar.*

Si $u \in \mathbb{Z}$, *entonces* $\overline{u}^2$ *toma exactamente* $\frac{p+1}{2}$ *valores distintos en* $\mathbb{Z}_p$, *a saber son los tomados al hacer* $u = 0, \ldots, \frac{p-1}{2}$; *en consecuencia si* $v \in \mathbb{Z}$, *entonces* $1 + v^2$ *toma* $\frac{p+1}{2}$ *en* $\mathbb{Z}_p$. *Ahora* $\mathbb{Z}_p$ *tiene exactamente p elementos, entonces existen* $u, v \in \mathbb{Z}$ *tales que* $u^2 + v^2 + 1 \equiv 0 (\textit{mód}\ p)\}$. *Nótese que no puede ser que* $p \mid u$ *y* $p \mid v$, *pues en ese caso* $1 \equiv 0 (\textit{mód}\ p)\}$, *que no es posible. Sin pérdida de generalidad supongamos que* $(p, u) = 1$.

Sea

$$G = \{(a, b, c, d) \in \mathbb{Z}^4 \mid c \equiv ua + vb\,(\textit{mód}\ p)\}, d \equiv ub - va\,(\textit{mód}\ p)\}\}$$

Tenemos que $(0, 0, 0, 0) \in G$. *Además, si* $(a, b, c, d), (a', b', c', d') \in G$ *se cumple que*

$$c \equiv ua + vb\,(\textit{mód}\ p)\ \ y\ \ d \equiv ub - va\,(\textit{mód}\ p) \tag{3.1}$$

y que

$$c' \equiv ua' + vb'\,(\textit{mód}\ p)\ \ y\ \ d' \equiv ub' - va'\,(\textit{mód}\ p) \tag{3.2}$$

así pasa

$$c - c' \underset{\textit{Por 3.1}}{\equiv} u(a - a') + v(b + b')\,(\textit{mód}\ p)$$

y

$$d - d' \underset{\textit{Por 3.2}}{\equiv} u(b - b') - v(a - a')\,(\textit{mód}\ p).$$

Es decir $(a, b, c, d) - (a', b', c', d') \in G$. *Luego entonces G es un subgrupo de* $\mathbb{Z}^4$. *Además para todo* $\overline{g} \in \mathbb{Z}^4/G$ *se tiene que* $p\overline{g} = \overline{0}$, *así* $\overline{g} \in \mathbb{Z}^4/G$ *es un* $\mathbb{Z}_p$*-espacio vectorial.*

Ahora vamos a mostrar que $\{\overline{(1, 0, 0, 0)}, \overline{(0, 0, 0, 1)}\}$ *es una base de* $\mathbb{Z}^4/G$, *lo que es equivalente a mostrar que para todo* $(a, b, c, d) \in \mathbb{Z}^2$ *existen* $x, y \in \mathbb{Z}$ *tales que* $(a, b, c, d) - x(1, 0, 0, 0) - y(0, 0, 0, 1) \in G$, *lo que pasa si y sólo si*

$$c \equiv u(a - x) + vb\,(\textit{mód}\ p)\ \ y\ \ d - y \equiv ub - v(a - x)\,(\textit{mód}\ p)$$

Ahora la ecuación $c \equiv u(a - x) + vb\,(\textit{mód}\ p)$ *tiene como solución*

$$x_0 \equiv a + u^{-1}vb - u^{-1}c\,(\textit{mód}\ p)$$

de donde se tiene que la solución a $d - y \equiv ub - v(a - x)\,(\textit{mód}\ p)$ *esta dada por*

$$y_0 \equiv d - ub + v(a - x_0)\,(\textit{mód}\ p)$$

Por lo tanto $\{\overline{(1, 0, 0, 0)}, \overline{(0, 0, 0, 1)}\}$ *es un conjunto de generadores de* $\mathbb{Z}^4/G$.

Ahora supongamos que

$$\overline{a}\overline{(1, 0, 0, 0)} + \overline{d}\overline{(0, 0, 0, 1)} = \overline{(0, 0, 0, 0)}$$

[5]Demostración ver [*Ap*] Secc. 11.33. pág. 411.

Entonces se tiene que $0 \equiv ua\,(\text{mód } p)$ *y que* $d \equiv -va\,(\text{mód } p)$, *como* $p \nmid u$, $p \mid a$ *y así* $d \equiv 0\,(\text{mód } p)$, *es decir* $\{\overline{(1,0,0,0)}, \overline{(0,0,0,1)}\}$ *es una base de* $\mathbb{Z}^4/G$. *Por lo tanto* $\mid \mathbb{Z}^4/G \mid = p^2$

Por le Lema 3.3.2 se tiene que el área de una 4-esfera de radio r es $\frac{\pi^2 r^4}{2}$. *Tomando* r^2 *=(1.9)p se tiene que* $16p^2 < \frac{\pi^2(1{,}9p^2)}{2}$. *Luego por el Teorema de Minkowski existe un elemento* $(a,b,c,d) \in G - \{\}$ *tal que*

$$0 < a^2 + b^2 + c^2 + d^2 \leqslant r^2 = (1.9)p < 2p$$

Dado que $c \equiv ua + vb\,(\text{mód } p)$ *y* $d \equiv ub - va\,(\text{mód } p)$*vvv se tienen las siguientes congruencias*

$$\begin{aligned} a^2 + b^2 + c^2 + d^2 &\equiv a^2 + b^2 + (u^2a^2 + 2uvab + v^2b^2) + (u^2b^2 - 2uvab + v^2a^2)\,(\text{mód } p) \\ &\equiv a^2 + b^2 + u^2(a^2 + b^2) + v^2(b^2 + a^2)\,(\text{mód } p) \\ &\equiv (a^2 + b^2)(1 + u^2 + v^2)\,(\text{mód } p) \\ &\equiv 0\,(\text{mód } p) \end{aligned}$$

Por lo tanto $p \mid a^2 + b^2 + c^2 + d^2$. *En resumen* $p \leqslant a^2 + b^2 + c^2 + d^2 < 2p$ *y al ser* $a^2 + b^2 + c^2 + d^2$ *entero obtenemos que* $p = a^2 + b^2 + c^2 + d^2$.

Como para todo $a, b, c, d, A, B, C, D \in \mathbb{Z}$ *se tiene que*

$$(a^2+b^2+c^2+d^2)(A^2+B^2+C^2+D^2) = (aA-bB-cC-dD)^2 + (aB+bA+cD-dC)^2 + (aC-bD+cA+dB)^2 + (aD+bC-cB+dA)^2$$

Aplicando inducción sobre el número de primos que aparecen al factorizar un entero positivo n se sigue el resultado. ∎

§3.3.2 Finitud del grupos de clases de un campo numérico

Para F un campo numérico de dimensión n sobre Q y $\sigma : F \longrightarrow \overline{\mathbb{Q}}$ *un monomorfismo que deja fijos los elementos de* $\mathbb{Q}$, *decimos que* σ *es* ***real*** *si* $\sigma(F) \subseteq \mathbb{R}$ *y que es* ***complejo*** *en caso contrario.*

En virtud el Teorema 1.4.53 y dado que $\mathbb{Q}$ *es de característica cero, si F un campo numérico de dimensión n sobre Q se tiene que* $F = \mathbb{Q}(\theta)$ *para algún* $\theta \in F$. *Por otro lado por el Lema 1.4.37, tenemos que todo morfismo de campos* $\sigma : F \longrightarrow \overline{\mathbb{Q}}$ *que extienda a la identidad en* $\mathbb{Q}$ *esta determinado por* $\sigma(\theta)$. *Podemos entonces concluir el siguiente*

Proposición 3.3.1. *Sean* $\mathbb{Q}(\theta)$ *un campo numérico de dimensión n sobre de* $\mathbb{Q}$, $\sigma : F \longrightarrow \overline{\mathbb{Q}}$ *un morfismo de campo que extiende a la identidad en* $\mathbb{Q}$. *Entonces*

1) σ *es real si y sólo si* $\sigma(\theta) \in \mathbb{R}$.
2) σ *es complejo si y sólo si* $\sigma(\theta)$ *es un complejo no real.*

Sean $\mathbb{Q}(\theta)$ *es un campo numérico de dimensión n sobre* $\mathbb{Q}$ *y* $f_\theta(x)$ *el polinomio mínimo de* θ *sobre* $\mathbb{Q}$. *Por el Lema 3.4.37 tenemos que existe una biyección entre la raíces de* $f_\theta(x)$ *y los morfismos de campos de* $\mathbb{Q}(\theta)$ *en* $\overline{\mathbb{Q}}$ *que extienden a la identidad en* $\mathbb{Q}$. *Por otro lado del Corolario 3.4.23 tenemos que* $\big[\mathbb{Q}(\theta) : \mathbb{Q}\big] = grad(f_\alpha(x))$, *por lo que existen n distintos extensiones de la identidad de la identidad en* $\mathbb{Q}$ *a* $\mathbb{Q}(\theta)$.

Proposición 3.3.2. *Sean* $f(x) \in \mathbb{R}[x]$ *y* $z \in \mathbb{C}$ *una raíz de* $f(x)$. *Entonces* $\overline{z}$ *es una raíz de* $f(x)$.

En vista de las Proposiciones 3.3.2 y 3.3.1 podemos concluir que existen $2t$ *monomorfismos complejos de* $\mathbb{Q}(\theta)$ *en* $\overline{\mathbb{Q}}$ *que extienden a la identidad en* $\mathbb{Q}$, *para algún* $t \in \mathbb{N}$. *Si r es el número de monomorfismo reales de* $\mathbb{Q}(\theta)$ *en* $\overline{\mathbb{Q}}$ *que extienden a la identidad en* $\mathbb{Q}$, *tenemos que* $r + 2t = n$, *donde* $n = \big[\mathbb{Q}(\theta), \mathbb{Q}\big]$. *Notemos que r y t son dos números naturales asociados intrínsecamente a la extensión de campos* $\mathbb{Q}(\theta)$ *sobre* $\mathbb{Q}$.

Definición 3.3.3. *Sean* $\mathbb{Q}(\theta)$ *un campo numérico de dimensión n sobre de* $\mathbb{Q}$ *y* $\sigma_1, \ldots, \sigma_n$ *los distintos morfismos de campo de* $\mathbb{Q}(\theta)$ *en* $\overline{\mathbb{Q}}$ *que extienden a la identidad en* $\mathbb{Q}$. *Decimos que* σ_i *es conjugado de* σ_j *si* $\sigma_i(\theta) = \overline{\sigma_j(\theta)}$.

Teorema 3.3.4. *Sean $\mathbb{Q}(\theta)$ un campo numérico de dimensión n sobre de $\mathbb{Q}$ y σ un morfismo de campos de $\mathbb{Q}(\theta)$ en $\overline{\mathbb{Q}}$ que extiende a la identidad en $\mathbb{Q}$. Entonces $\overline{\sigma}$ es un morfismo de campos de $\mathbb{Q}(\theta)$ en $\overline{\mathbb{Q}}$ que extiende a la identidad en $\mathbb{Q}$.*

Sean $\mathbb{Q}(\theta)$ un campo numérico de dimensión n sobre de $\mathbb{Q}$ y $\sigma_1, \ldots, \sigma_n$ los distintos morfismos de campo de $\mathbb{Q}(\theta)$ en $\overline{\mathbb{Q}}$ que extienden a la identidad en $\mathbb{Q}$. Si r es el número de morfismo reales de F en $\overline{\mathbb{Q}}$ y 2t el número de morfismos complejos, podemos ordenar los σ_i de tal modo que σ_i sea real si $1 \leqslant i \leqslant r$ y σ_i sea un morfismo complejo si $r+1 \leqslant i \leqslant r+t$ y además σ_i sea conjugado con σ_{i+t} para $r+1 \leqslant i \leqslant r+t$. Así los primeros $r+t$ morfismos determinan los restantes. Definamos

$$\sigma : \mathbb{Q}(\theta) \longrightarrow \mathbb{R}^r \bigtimes \mathbb{C}^t \text{ por } \sigma(x) = (\sigma_1(x), \ldots, \sigma_{r+t}(x))$$

*σ se llama la **inmersión canónica** de $\mathbb{Q}(\theta)$ en $\mathbb{R}^r \times \mathbb{C}^t$. Recordemos que para $r+1 \leqslant j \leqslant r+t$ podemos σ_j es un morfismo complejo, entonces $\sigma_j(x) = Re(\sigma_j(x)) + iIm(\sigma_j(x))$, donde $Re(\sigma_j(x))$ y $Im(\sigma_j(x))$ son la parte real y la parte imaginaria de $\sigma_j(x)$. De esta forma podemos pensar que es una función $\sigma : \mathbb{Q}(\theta) \longrightarrow \mathbb{R}^n$ dada por*

$$\sigma(x) = (\sigma_1(x), \ldots, \sigma_r(x), Re(\sigma_{r+1}(x)), Im(\sigma_{r+1}(x)), \ldots, Re(\sigma_{r+t}(x)), Im(\sigma_{r+t}(x)))$$

Como cada σ_i es un morfismo de campos, por el Lema 14.13 cada σ_i es un morfismo inyectivo de anillos y así tenemos que $\sigma(x)$ es un morfismo inyectivo de grupos.

Proposición 3.3.5. *Sea $\mathbb{Q}(\theta)$ un campo numérico de dimensión n sobre Q y M un $\mathbb{Z}$-submódulo libre de rango n de F. Si $\{\alpha_1, \ldots, \alpha_n\}$ es una $\mathbb{Z}$-base de M y σ es la inmersión canónica de $\mathbb{Q}(\theta)$ en $\mathbb{R}^n$, entonces $\sigma(M)$ es una red de dimensión n de $\mathbb{R}^n$ cuyo volumen está dado por*

$$v(\sigma(M)) = 2^{-t} \left| \underset{1 \leqslant i,j \leqslant n}{det} (\sigma_i(\alpha_j)) \right|.$$

Demostración. *Para α_i en la base de M tenemos que $\sigma(\alpha_i)$ en la base canónica de $\mathbb{R}^n$ está dado por*

$$\sigma(\alpha_i) = (\sigma_1(\alpha_i), \ldots, \sigma_r(\alpha_i), Re(\sigma_{r+1}(\alpha_i)), Im(\sigma_{r+1}(\alpha_i)), \ldots, Re(\sigma_{r+t}(\alpha_i)), Im(\sigma_{r+t}(\alpha_i)))$$

Ahora consideremos la matriz N que tiene como i-ésimo renglón el vector $\sigma(\alpha_i)$, es decir

$$N = \begin{pmatrix} \sigma_1(\alpha_1) & \ldots & \sigma_r(\alpha_1) & Re(\sigma_{r+1}(\alpha_1)) & Im(\sigma_{r+1}(\alpha_1)) & \ldots & Re(\sigma_{r+t}(\alpha_1)) & Im(\sigma_{r+t}(\alpha_1)) \\ \vdots & & \vdots & \vdots & \vdots & & \vdots & \vdots \\ \sigma_1(\alpha_n) & \ldots & \sigma_r(\alpha_n) & Re(\sigma_{r+1}(\alpha_n)) & Im(\sigma_{r+1}(\alpha_n)) & \ldots & Re(\sigma_{r+t}(\alpha_n)) & Im(\sigma_{r+t}(\alpha_n)) \end{pmatrix}.$$

Usando las identidades $Re(z) = \frac{1}{2}(z + \overline{z})$ e $Im(z) = \frac{1}{2i}(z - \overline{z})$ para $z \in \mathbb{C}$ y la n-linealidad del determinante, se obtiene que

$$det(N) = (-1)^t (\frac{1}{2i})^t det(\sigma_i(\alpha_j)). \tag{3.3}$$

Ahora notemos que dado que $\{\alpha_1, \ldots, \alpha_n\}$ es $\mathbb{Z}$-linealmente independiente, entonces es un conjunto $\mathbb{Q}$-linealmente independiente y por lo tanto es una base de $\mathbb{Q}(\theta)$ sobre $\mathbb{Q}$, cuyo discriminante esta dado por

$$\Delta[\alpha_1, \ldots, \alpha_n] = (det(\sigma_i(\alpha_j)))^2.$$

Por el Teorema 3.2.18 $\Delta[\alpha_1, \ldots, \alpha_n] \in \mathbb{Q}$ y además es no nulo, es decir $(det(\sigma_i(\alpha_j)))^2 \neq 0$, de donde $det(\sigma_i(\alpha_j)) \neq 0$. Por lo tanto $det(N) \neq 0$ y así los vectores renglón de N son linealmente independientes, de donde se concluye que $\sigma(M)$ es una red de dimensión n de $\mathbb{R}^n$.

Por último de la Proposición 3.2.8, obtenemos que

$$V(\sigma(M)) = \mid det(N) \mid = 2^{-t} \left| \underset{1 \leqslant i,j \leqslant n}{det} (\sigma_i(\alpha_j)) \right|. \quad \blacksquare$$

Nota 3. 3.6. En adelante $\mathfrak{D}$ denotará el anillo de enteros de un campo numérico $\mathbb{Q}(\theta)$ de dimensión n sobre $\mathbb{Q}$ y σ la inmersión canónica de $\mathbb{Q}(\theta)$ en $\mathbb{R}^r \times \mathbb{C}^t$, donde r es el número de homomorfismos reales y $2t$ el de los homomorfismos complejos.

Como consecuencia del Corolario 2.2.19, tenemos que los discriminantes de dos bases de $\mathfrak{D}$ son asociados en $\mathbb{Z}$, es más, de la Proposición 2.2.10 se tiene que difieren en un cuadrado. Es decir, si $\mathfrak{D}$ es un campo numérico y α y β son $\mathbb{Z}$-bases de $\mathfrak{D}$, entonces $\Delta[\alpha] = \Delta[\beta]$, así, si $\mathbb{Q}(\theta)$ es un campo numérico se define el ***discriminante de*** *$\mathbb{Q}(\theta)$ como el discriminante de cualquier base de $\mathfrak{D}$.*

Corolario 3.3.7. *Si d es el discriminante de F, $\mathfrak{D}$ su anillo de enteros, y $\mathfrak{A}$ un ideal entero no nulo de $\mathfrak{D}$, entonces $\sigma(\mathfrak{D})$ y $\sigma(\mathfrak{A})$ son subgrupos discretos de $\mathbb{R}^n$. Además*

$$v(\sigma(\mathfrak{D})) = 2^{-t} \mid d \mid^{\frac{1}{2}} \quad y \quad v(\sigma(\mathfrak{A})) = 2^{-t} \mid d \mid^{\frac{1}{2}} N(\mathfrak{A})$$

Demostración. *$\sigma(\mathfrak{D})$ y $\sigma(\mathfrak{A})$ son subgrupos discretos de $\mathbb{R}^n$ por la Proposición 3.3.5, esta última además muestra que $V(\sigma(\mathfrak{D})) = 2^{-t} \mid d \mid^{\frac{1}{2}}$. La segunda igualdad se deduce teniendo en cuenta que $\sigma(\mathfrak{A})$ (ver Definición 2.2.45) es es un subgrupo de índice $N(\mathfrak{A})$ de $\sigma(\mathfrak{D})$, para luego aplicar el Corolario 2.2.10.* ∎

Lema 3.3.8. *Consideremos $s \in \mathbb{R}^+$ un número fijo y sea*

$$\Lambda_{r,t,s} = \left\{ (y_1, \ldots, y_r, z_1, \ldots, z_t) \in \mathbb{R}^r \bigtimes \mathbb{C}^t \;\middle|\; \sum_{i=1}^{r} \mid y_i \mid + 2\sum_{i=1}^{t} \parallel z_i \parallel \leqslant s \right\},$$

donde $\mid\ \mid$ denota el valor absoluto en $\mathbb{R}$ y $\parallel\ \parallel$ la norma de un número complejo.

Entonces $\Lambda_{r,t,s}$ es un conjunto compacto, convexo y simétrico respecto al origen, cuyo volumen está dado por $V(\Lambda_{r,t,s}) = 2^r \left(\frac{\pi}{2}\right)^t \frac{s^n}{n!}$, donde $n = s + 2t$.

Demostración. *Claramente $\Lambda_{r,t,s}$ es compacto y simétrico respecto al origen. Ahora consideremos $v_1, v_2 \in \Lambda_{r,t,s}$, es decir*

$$v_1 = (y_1, \ldots, y_r, z_1, \ldots, z_t) \quad y \quad v_2 = (y'_1, \ldots, y'_r, z'_1, \ldots, z'_t)$$

y sea $\Xi = \{(1-\lambda)v_1 + \lambda v_2 \mid 0 \leqslant \lambda \leqslant 1\}$ el segmento que une a los vectores v_1 y v_2. Recordemos que para todo $x_1, x_2 \in \mathbb{R}$, $w_1, w_2 \in \mathbb{C}$ y $\lambda \in [0,1]$, se tiene que

$$|(1-\lambda)x_1 + \lambda x_2| \leqslant (1-\lambda)|x_1| + \lambda|x_2| \quad y \quad \|(1-\lambda)w_1 + \lambda w_2\| \leqslant (1-\lambda)\|w_1\| + \lambda\|w_2\|.$$

Así, si $v \in \Xi$, como $v = (1-\lambda)v_1 + \lambda v_2$ para alguna $\lambda \in [0,1]$, tenemos que

$$\sum_{i=1}^{r} |(1-\lambda)y_i + \lambda y'_i| + 2\sum_{i=1}^{t} \|(1-\lambda)z_i + \lambda z'_i\| \leqslant \sum_{i=1}^{r} [(1-\lambda)|y_i| + \lambda|y'_i|] + 2\sum_{i=1}^{t} [(1-\lambda)\|z_i\| + \lambda\|z'_i\|].$$

Como

$$\sum_{i=1}^{r} [(1-\lambda)|y_i| + \lambda|y'_i|] + 2\sum_{i=1}^{t} [(1-\lambda)\|z_i\| + \lambda\|z'_i\|] = (1-\lambda)\left[\sum_{i=1}^{r} |y_i| + 2\sum_{i=1}^{t} \|z_i\|\right] + \lambda\left[\sum_{i=1}^{r} |y'_i| + 2\sum_{i=1}^{t} \|z'_i\|\right]$$

y

$$(1-\lambda)\left[\sum_{i=1}^{r} |y_i| + 2\sum_{i=1}^{t} \|z_i\|\right] + \lambda\left[\sum_{i=1}^{r} |y'_i| + 2\sum_{i=1}^{t} \|z'_i\|\right] \leqslant (1-\lambda)s + \lambda s = s,$$

obtenemos que $v \in \Lambda_{r,t,s}$ y por lo tanto $\Lambda_{r,t,s}$ es convexo.

Ahora vamos a demostrar que $V(\Lambda_{r,t,s}) = 2^r \left(\frac{\pi}{2}\right)^t \frac{s^m}{m!}$. Se va a proceder por doble recurrencia sobre r y t.

Se tiene que $V(1,0,s) = 2s$ pues es la longitud del segmento $[-s, s]$ y que $V(0,1,s) = \frac{\pi s^2}{4}$, lo que es conforme con la fórmula.

Supongamos que la fórmula es válida para r, y para todo $t \in \mathbb{N}$ y $s \in \mathbb{R}$, y tomemos

$$\Lambda_{r+1,t,s} \subseteq \mathbb{R} \times \mathbb{R}^r \times \mathbb{C}^t$$

Por definición, si $(y_1, \ldots, y_k, y, z_1, \ldots, z_t) \in \Lambda_{k+1,t,s}$*, satisface que*

$$\mid y \mid + \sum_{i=1}^{k} \mid y_i \mid + 2 \sum_{i=1}^{t} \parallel z_i \parallel \leqslant s$$

Notemos que cada $y \in [-s, s]$*, define un subconjunto de* $\mathbb{R}^k \times \mathbb{C}^t$*, dado por* $\Lambda_{k,t,s-|y|}$*, el cual resulta ser un corte de* $\Lambda_{r+1,t,s}$*. Así, por la formula de integración por "rebanadas "tenemos que*

$$V(\Lambda_{r+1,t,s}) = \int_{-s}^{s} V(\Lambda_{r,t,s-|y|}) dy.$$

Y como $\Lambda_{r+1,t,s}$ *es simétrico respecto al origen, entonces*

$$\int_{-s}^{s} V(\Lambda_{r,t,s-|y|}) dy = 2 \int_{0}^{s} V(\Lambda_{r,t,s-y}) dy$$

Ahora, por hipótesis de inducción $V(\Lambda_{r,t,s-y}) = 2^r \left(\frac{\pi}{2}\right)^t \frac{(s-y)^n}{(n)!}$ *donde* $n = r + 2t$*, entonces*

$$V(\Lambda_{r+1,t,s}) = 2 \int_{0}^{s} 2^r \left(\frac{\pi}{2}\right)^t \frac{(s-y)^n}{(n)!} dy = 2^{r+1} \left(\frac{\pi}{2}\right)^t \frac{(s)^{n+1}}{(n+1)!}.$$

Para finalizar supongamos que la proposición, ahora es válida para t y para todo $r \in \mathbb{N}$ *y* $s \in \mathbb{R}$*, y consideremos*

$$\Lambda_{r,t+1,s} \subseteq \mathbb{R}^r \times \mathbb{C}^t \times \mathbb{C}.$$

Como para todo $(y_1, \ldots, y_r, z_1, \ldots, z_t, z) \in V(\Lambda_{r,t+1,s})$ *se tiene que*

$$\sum_{i=1}^{r} \mid y_i \mid + 2 \sum_{i=1}^{t} \parallel z_i \parallel + 2 \parallel z \parallel \leqslant s$$

Nuevamente por la fórmula de integración por "rebanadas "tenemos que

$$V(\Lambda_{r,t+1,s}) = \int_{|z| \leqslant \frac{s}{2}} V(\Lambda_{r,t,s-2\|z\|}) dz$$

Dado que $z = \rho e^{i\theta}$*, donde* $\rho \in \mathbb{R}^+$ *y* $\theta \in [0, 2\pi]$*, tenemos que* $dz = \rho d\rho d\theta$*. Y como por hipótesis de inducción* $V(\Lambda_{r,t,s-2\|z\|}) = 2^r \left(\frac{\pi}{2}\right)^t \frac{(s-2\|z\|)^n}{n!}$ *donde* $n = r + 2t$*, se deduce que*

$$V(\Lambda_{r,t+1,s}) = \int_{0}^{\frac{s}{2}} \int_{0}^{2\pi} 2^r \left(\frac{\pi}{2}\right)^t \frac{(s-2\rho)^n}{n!} \rho d\rho d\theta = 2^r \left(\frac{\pi}{2}\right)^t \frac{2\pi}{n!} \int_{0}^{\frac{1}{2}} (s-2\rho)^n \rho d\rho.$$

Usando integración por partes para calcular $\int (s-2\rho)\rho d\rho$*, obtenemos que*

$$\int (s-2\rho)^n \rho d\rho = -\frac{1}{4}(s-2\rho)^{n+1} \left(\frac{2(n+2)\rho + (s-2\rho)}{(n+1)(n+2)}\right) + C.$$

De donde obtenemos que

$$V(\Lambda_{r,t+1,s}) = 2^r \left(\frac{\pi}{2}\right)^{t+1} \frac{s^{n+2}}{(n+2)!}.$$

Lo que demuestra la formula. ∎

Lema 3.3.9 *(Desigualdad de la media geométrica). Sea* $a_1, \ldots, a_n \in \mathbb{R}$*, entonces*

$$\left(\prod_{i=1}^{n} a_i\right)^n \leqslant \frac{\sum_{i=1}^{n} a_i}{n}.$$ [6]

[6] Demostración ver [Sp] pág. 42.

Proposición 3.3.10. *Sea $\mathbb{Q}(\theta)$ un campo numérico de dimensión n sobre $\mathbb{Q}$ con discriminante d y sea $\mathfrak{A}$ un ideal de $\mathfrak{D}$. Entonces $\mathfrak{A}$ contiene un elemento no nulo x tal que*

$$N(x) \leqslant \left(\frac{4}{\pi}\right)^t \frac{n!}{n^n} \mid d \mid^{\frac{1}{2}} N(\mathfrak{A})$$

Demostración. *Con la notación del Lema 3.3.8, consideremos $r,t \in \mathbb{N}$ y $s \in \mathbb{R}^+$ de tal forma que $V(\Lambda_{r,t,s}) = 2^{n+1}v(\mathfrak{A})$, es decir $V(\Lambda_{r,t,s}) = 2^{n-t+1} \mid d \mid^{\frac{1}{2}} N(\mathfrak{A})$ (ver Corolario 3.3.7). Para ello es suficiente tomar $s \in \mathbb{R}^+$ tal que*

$$s^n = n! \left(\frac{4}{\pi}\right)^t 2 \mid d \mid^{\frac{1}{2}} N(\mathfrak{A}).$$

Ahora, aplicando nuevamente el Lema 3.3.8, tenemos que $\Lambda_{r,t,s}$ es un conjunto compacto, convexo y simétrico respecto al origen, con la propiedad de que $2^n V(\sigma(\mathfrak{A})) < V(\Lambda_{r,t,s})$. Por el Teorema de Minkowski (3.3.1), existe $y \in \Lambda_s \cap \sigma(\mathfrak{A})$, tal que $y \neq 0$ y como σ es un morfismo inyectivo de grupos, entonces existe $x \in \mathfrak{A}\backslash\{0\}$ tal que $\sigma(x) = y$.

Sean $\sigma_1, \ldots, \sigma_r$ los morfismo reales de $\mathbb{Q}(\theta)$ en $\overline{\mathbb{Q}}$ que extienden a $I_{\mathbb{Q}}$ y $\sigma_{r+1}, \ldots, \sigma_n$ los $2t$ morfismos complejos, ordenados de tal forma que $\sigma_i = \overline{\sigma_{i+t}}$ para $r+1 \leqslant i \leqslant r+t$. Si calculamos la norma de x, tenemos que

$$N(x) = \prod_{i=1}^{n} \sigma_i(x) = \prod_{i=1}^{r} \sigma_i(x) \prod_{i=r+1}^{n} \sigma_i(x) = \prod_{i=1}^{r} \sigma_i(x) \prod_{i=r+1}^{r+t} \sigma_i(x) \prod_{i=r+1}^{r+t} \overline{\sigma_i(x)}$$

Ahora recordemos que para $z \in C$ se tiene que $z\overline{z} = \| z \|$, donde $\| z \|$ es la norma de z. Así

$$\mid N(x) \mid = \prod_{i=1}^{r} \mid \sigma_i(x) \mid \prod_{j=1}^{t} \| \sigma_{r+j}(x) \|^2$$

Por la desigualdad de la media geométrica (Lema 3.3.9), se tiene que

$$\mid N(x) \mid \leqslant \left[\frac{1}{n} \sum_{i=1}^{r} \mid \sigma_i(x) \mid + \frac{2}{n} \sum_{i=1}^{r+t} \| \sigma_i(x) \| \right]^n.$$

Por otro lado $x \in \Lambda_s$, entonces

$$\left[\frac{1}{n} \sum_{i=1}^{r} \mid \sigma_i(x) \mid + \frac{2}{n} \sum_{i=1}^{r+t} \| \sigma_i(x) \| \right]^n \leqslant \frac{s^n}{n^n}.$$

De donde $\mid N(x) \mid \leqslant \frac{s^n}{n^n}$ y así $\mid N(x) \mid \leqslant \frac{n!}{n^n} \left(\frac{4}{\pi}\right)^t 2 \mid d \mid^{\frac{1}{2}} N(\mathfrak{A})$ ∎

Corolario 3.3.11. *Sea $\mathbb{Q}(\theta)$ un campo numérico de dimensión n sobre $\mathbb{Q}$ con discriminante d. Entonces toda clase de ideales en el grupo de clases de ideales de $\mathfrak{D}$ contiene un ideal $\mathfrak{A}$ tal que*

$$N(\mathfrak{A}) \leqslant \left(\frac{4}{\pi}\right)^t \frac{n!}{n^n} \mid d \mid^{\frac{1}{2}}.$$

Demostración. *Sea G el grupo de clases de ideales de $\mathfrak{D}$. Primero veremos que para todo $g \in G$ existe $\mathfrak{A} \in g$ tal que $\mathfrak{A}$ es un ideal fraccionario no entero.*

Sea entonces $g \in G$ y $\mathfrak{A} \in g$. Si $\mathfrak{A}$ es un ideal fraccionario no entero ya hemos terminado. Entonces supongamos que $\mathfrak{A} \in g$ es un ideal entero de $\mathfrak{D}$ y $q \in F\backslash\mathfrak{D}$, y sea $\mathfrak{B} = \mathfrak{D}q\mathfrak{A}$. Claramente $\mathfrak{B}$ es un ideal fraccionario no entero de $\mathfrak{D}$ que esta relacionado con $\mathfrak{A}$, y así $\mathfrak{B} \in g$.

Ahora sea $g \in G$, por lo anterior podemos tomar $\mathfrak{A} \in g$ un ideal fraccionario no entero, entonces $\mathfrak{A}^{-1}$ es un ideal entero de $\mathfrak{D}$, por la Proposición 3.3.10, existe $x \in \mathfrak{A}^{-1}$ un elemento no nulo tal que $N(x) \leqslant \frac{n!}{n^n}\left(\frac{4}{\pi}\right)^t 2 \mid d \mid^{\frac{1}{2}} N(\mathfrak{A})^{-1}$. Sea

$$\mathfrak{B} = \mathfrak{D}x\mathfrak{A},$$

claramente $\mathfrak{B} \in g$, pues $\mathfrak{B}\mathfrak{A}^{-1} = \mathfrak{D}x$.

Por último notemos por el Teorema 2.2.43 tenemos que $N(\mathfrak{D}x) = N(x)$ de donde

$$N(\mathfrak{B}\mathfrak{A}^{-1}) = N(\mathfrak{B})N(\mathfrak{A}^{-1}) \leqslant \frac{n!}{n^n}\left(\frac{4}{\pi}\right)^t 2 \mid d \mid^{\frac{1}{2}} N(\mathfrak{A}^{-1})$$

Y siendo que $N(\mathfrak{A}^{-1})$, Podemos concluir que $N(\mathfrak{B}) \leqslant \frac{n!}{n^n}\left(\frac{4}{\pi}\right)^t 2 \mid d \mid^{\frac{1}{2}}$ ∎

***Teorema 3.3.12** (Dirichlet). Para todo campo numérico, el grupo de las clases de ideales de F es finito.*

***Demostración.** En virtud del Corolario 3.3.11 es suficiente demostrar que el conjunto de ideales enteros de $\mathfrak{D}$, cuya norma es un entero dado es finito.*

Entonces tomemos q un entero no negativo y $\mathfrak{B}$ un ideal entero de $\mathfrak{D}$ tal que $N(\mathfrak{B}) = q$. Ahora recordemos que $N(\mathfrak{B}) = |\mathfrak{D}/\mathfrak{B}|$, es decir $\mathfrak{D}/\mathfrak{B}$ es un grupo de orden q, de donde tenemos que $q\overline{g} = \overline{0}$ para todo $\overline{g} \in \mathfrak{D}/\mathfrak{B}$, pues en un grupo el orden de un elemento divide al orden del grupo, en particular se tiene que $q\overline{1} = \overline{0}$, luego entonces $q \in \mathfrak{B}$ y así $\mathfrak{D}q \subseteq \mathfrak{B}$. Luego entonces $\mathfrak{B}$ se encuentra entre los ideales de $\mathfrak{D}$ que contienen a $\mathfrak{D}q$.

Ahora, por el Teorema 2.2.43 $\mathfrak{D}/\mathfrak{D}q$ es finito, luego el Teorema de correspondencia (3.1.19) muestra que solo hay un número finito de ideales enteros de $\mathfrak{D}$ tales que $\mathfrak{D}q$ este contenido en ellos.

En conclusión podemos afirmar que sólo hay un número finito de ideales enteros de $\mathfrak{D}$ que tengan norma q y así el grupo de las clases de ideales de F es finito. ∎

***Corolario 3.3.13.** Sea F un campo numérico y $\mathfrak{D}$ su anillo de enteros. Entonces $\mathfrak{D}$ es un dominio de factorización única si y sólo si el grupo de clases de ideales es el grupo trivial.*

***Demostración.** Por el Teorema 2.3.23 es suficiente hacer notar que $\mathfrak{B}$ es un ideal principal entero de $\mathfrak{D}$ si y sólo si $\mathfrak{B}^{-1}$ es un ideal fraccionario principal de $\mathfrak{D}$.* ∎

Conclusiones

Si bien el estudio de la Teoría de los Números ha evolucionado de manera drástica desde la época en que Minkowski presentó el resultado que inspiró este trabajo, los alcances que han tenido las técnicas introducida por Minkowski a finales del siglo XVII en la matemática moderna son invaluables.

El grupo de clases de ideales de una dominio de Dedekind surge ante la necesidad de resolver algunas cuestiones relacionadas con el último teorema de Fermat, este por su naturaleza por demás interesante. Siendo posible el calculo del grupo de clases de ideales para algunos campos numéricos hasta el momento no se conoce alguna técnica que permita calcular el grupo de clases de ideales para cualquier campo numérico.

Tabla de notaciones

Conjuntos

$\in$	*Pertenecer a ..., esta en ...*
$\notin$	*No pertenecer a ..., no esta en ...*
$\subseteq$; $\subsetneq$	*Esta contenido en ...; esta propiamente contenido en ...*
$\supseteq$, $\supsetneq$	*Contiene a ..., contiene propiamente a...*
$\cap$	*Intersección.*
$\cup$	*Unión.*
$-$	*Diferencia de conjuntos.*
$\varnothing$	*Conjunto vacío.*
$\mathfrak{P}(A)$	*Potencia de A, partes de A.*
$\times$	*Producto cartesiano.*
$\{A_i\}_{i\in I}$	*Conjunto indicado por I.*
$\lvert A\rvert$	*Cardinal del conjunto A.*

Conjuntos numéricos

$\mathbb{N}$	*El monoide de los números naturales.*
$\mathbb{Z}$	*El anillo de los números enteros.*
$\mathbb{Q}$	*El campo de los números racionales.*
$\mathbb{R}$	*El campo de los números reales.*
$\mathbb{C}$	*El campo de los números complejos.*

Anillos

$U(R)$	*Grupo de unidades del anillo R.*
$grad(f(x))$	*Grado del polinomio $f(x)$.*
$R[x]$	*Anillo de polinomios en x con coeficientes en R.*
f_α	*Polinomio mínimo de α.*
$R[x_1,\ldots,x_n]$	*Anillo de polinomios en $x_1,\ldots,x_n$ con coeficientes en R.*
$R[x_\infty]$	*Anillo de polinomios en una infinidad de indeterminadas con coeficientes en R.*
$R[[x]]$	*Anillo de series formales con coeficientes en R.*
$R[M]$	*Anillo de monoide. (Pág. 4)*
$\bigtimes_{i\in I} R_i$	*Anillo producto de la familia $\{R_i\}_{i\in I}$.*
$\langle X\rangle$	*Ideal generado por X.*
rR	*Ideal principal generado por r en el anillo R.*
$I+J$	*Suma del ideal I con el ideal J.*
IJ	*Producto del ideal I con el ideal J.*
R/I	*El anillo cociente de R por el ideal I.*
$ker(f)$	*Núcleo de un homomorfismo f de anillos.*
$Im(f)$	*Imagen de un homomorfismo f de anillos.*
$\cong$	*Anillos isomorfos.*
$r \mid t$	*r divide a t.*
$r \mid s$	*r divide a s.*
$r \nmid s$	*r divide a s.*
CFD	*Dominio con la condición finita de divisores. (Pág. 14)*
DFU	*Dominio de Factorización Única. (Pág. 15)*

CRI	*Conjuntos de representantes de irreducibles. (Pág. 17)*
$\mathfrak{P}_{r,s}$	*Irreducibles comunes a r y s en* $\mathfrak{P}$. *(Pág. 17)*
MCD	*Dominio con la propiedad del Máximo Común Divisor. (Pág. 19)*
$\Delta_{r,s}$	*Conjunto de los máximos comunes divisores de r y s en D. (Pág. 19)*
$\Delta_{r,s}$	*Conjunto de los máximos comunes divisores de r y s en D. (Pág. 19)*
$M_n(R)$	*El anillo de matrices con coeficientes en el anillo R.*
$\Delta[\alpha_1, \ldots, \alpha_n]$	*El discriminante de* $\{\alpha_1, \ldots, \alpha_n\}$.

Módulos

$\prod_{i\in I} M_i$	*Producto directo de módulos.*
$\bigoplus_{i\in I} M_i$	*Suma directa de módulos.*
$<$	*Submódulo.*
$\langle X \rangle$	*Submódulo generado por X.*
$N + L$	*Suma de los submódulos N y L.*
$ker(f)$	*Núcleo de un homomorfismo* f *de R-módulos.*
$Im(f)$	*Imagen de un homomorfismo* f *de R-módulos.*
$\cong$	*Módulos isomorfos.*
Rm	*R-submódulo generado por m en M.*

Campos

ev_α	*Morfismo evaluar. (Pág. 30)*
$f_\alpha(x)$	*Polinomio mínimo de* α. *(Pág. 31)*
$F(\alpha_1, \ldots, \alpha_n)$	*Extensión generada por* $\alpha_1, \ldots, \alpha_n$. *(Pág. 32)*
$\overline{F}$	*Cerradura algebraica del capo F. (Pág.* **??***)*

Bibliografía

[An] Anerson, F. W., *Rings and categories of modules*, Springer-verlag New york-Heiderlberg-Berlin; Madrid, 1973.

[Ap] Apostol, T. M., *Calculus*, John Wiley and Sons; New York London Sydney Toronto, 1969.

[Co] Collette, J. P., *Historia de las matemáticas (volúmenes 1 y 2, Traducción de Alfonso Casal)*, Siglo XXI Editores S.A.; Madrid, 1985.

[Fr] Fraleigh, J. B., *Álgebra abstracta*, Addison-Wesley Iberoamericana; Wilmington, Delaware E.U.A., 1987.

[Go] Gómez, C., *Introducción a la teoría intuitiva de los conjuntos (Cardinales y ordinales)*, Las prensas de ciencias, Facultad de Ciencais UNAM; México D.F., 2007.

[Ja] Jacobson, N., *Basic Algebra 1*, W. H. Freeman and Company; New York, E.U.A., 1985.

[Ka] Kasch, *Modules and rings*, Academis Press, 1982.

[Ma] Marsden, J., *Calculo vectorial*, Addison-Wesley Iberoamericana; Wilmington, Delaware E.U.A., 1991.

[Mc] McCarthy, P. J., *Algebraic extensions of Fields*, Dover plublications; New York, 1991.

[Ni] Niven, I., *An introduction to the Theory of Numbres Fifth edition*, John Wiley and Sons,. Inc; New York-Chischester-Brisbane-Toronto-Singapure, 1991.

[Ro] Rotman, J., *Galois Theory*, Springer-Verlag; New York, Inc, 1990.

[Sg] Sagan, H., *Advanced Calculus*, Houghton Mifflin Company, Boston, 1974.

[Sm] Samuel, P., *Teoría Algebraica de Números*, Ediciones omega, S.A., Barcelona, 1972.

[Sp] Spivak, M., *Cálculo infinitesimal*, Editorial Reverté, S. A., México D. F., 1996.

[St1] Stewart, I., *Algebraic Number Theory*, Chapman and hall, New York, 1987.

[St2] Stewart, I., *Historia de las matemáticas en los últimos 10000 años*, Editorial Crítica, New York, 1987.

Índice alfabético