Notas de Álgebra Moderna 2

Facultad de Ciencias, UNAM

Frank Patrick Murphy Hernandez

Jaime García Villeda

Índice general

Preliminares

Las presentes notas contienen el material correspondiente al curso del Álgebra Moderna II en la Facultad de Ciencias de UNAM, impartido en el semestre 2021-II por lo autores. Estás han sido escritas por Eduardo León Rodríguez.

Aunque estas notas no están basadas en ningún texto en especial, los textos básicos en los que se apoyan se encuentran en la bibliografía. De manera general la referencia [**3**] es la versión más básica en la que aparece todo el material del temario oficial. En nuestro caso incluimos a esta el famoso libro de Atiyah y MacDonald [**2**] para desarrollar distintos temas de los capítulos 1 y 2. Para la parte de teoría de campos y Galois se usan los textos [**1**] y [**5**], de estos últimos la primera referencia escrita por Artin tiene un valor histórico en el desarrollo de la teoría más allá del gran texto que es en sí. Para concluir, algunas ideas del libro [**4**] se usan a lo largo de todas las notas. A esto hay que agregar que a lo largo de algunas secciones se recomiendan algunos otros textos para complementar el material que se esté tratando.

Como comentarías matemáticos generales:

- El conjunto de los naturales $\mathbb{N}$ incluye al 0. La notación $\mathbb{N}^+$ indica al conjunto de naturales positivos.
- El grado de un polinomio $f \in R[x]$ se denota por $\partial(f)$

Capítulo 1

Conceptos básicos de Teoría de Anillos

1. Básico de anillos

DEFINICIÓN 1. *Sea R un grupo abeliano con operación $+$ y una segunda operación $\cdot : R \times R \to R$ que escribiremos $xy := \cdot(x,y)$, si estas operaciones cumplen:*

1. $(xy)z = x(yz)\ \forall x,y,z \in R$
2. $\exists e \in R$ *tal que* $\forall x \in R$, $xe = x = xe$ *a "e" lo llamamos una unidad de* R
3. $(x+y)z = xz+yz, x(y+z) = xy+xz$, $\forall x,y,z \in R$ *diremos que* R *es un anillo asociativo con 1. Si además se cumple que* $xy = yx\ \forall x,y \in R$, *diremos que es un anillo conmutativo.*

EJEMPLO 1.
1. *Los enteros* $\mathbb{Z}$
2. *Los reales* $\mathbb{R}$
3. *Los racionales* $\mathbb{Q}$
4. *Los complejos* $\mathbb{C}$
5. *Para* $n \in \mathbb{N}$, *los enteros módulo n.*
6. *Para* K *un campo, el anillo de polinomios en una indeterminada* $K[X]$.
7. *Las funciones continuas* $C_0([a,b])$ *en el intervalo* $[a,b]$. *Todos los anteriores son ejemplos de anillos conmutativos.*
8. *Los naturales* $\mathbb{N}$ *no son un anillo porque no forman ni un grupo abeliano.*
9. *Para* K *un campo y* $n \in \mathbb{N}$, *el conjunto de matrices de n por n,* $M_n(K)$ *es un anillo. Si* $n \geq 2$ *entonces* $M_n(K)$ *no es conmutativo.*

PROPOSICIÓN 1. *(Tarea) Sea K un campo y $n \in \mathbb{N}$. Entonces $M_n(K)$ es un anillo conmutativo si y sólo si $n \geq 2$.*

PROPOSICIÓN 2. *Sea R un anillo. Entonces la unidad es única.*

DEMOSTRACIÓN. Sean $e, e' \in R$ unidades, entonces

$$e' = ee' = e$$

□

Notación. Como la unidad es única, la denotaremos por 1.

PROPOSICIÓN 3. *(Tarea) Sea R un anillo y $x \in R$, entonces $x0 = 0 = 0x$*

Todos los anillos que consideremos en el curso serán conmutativos.

DEFINICIÓN 2. *Sea R un anillo y $u \in R$. Decimos que u es una unidad si existe $r \in R$ tal que $ur = 1$. El conjunto de unidades de R lo denotamos por $U(R)$.*

PROPOSICIÓN 4. *Sea R un anillo. Entonces $U(R)$ es un grupo(abeliano).*

DEMOSTRACIÓN.
1. La asociatividad se hereda de la asociatividad de R
2. El neutro de $U(R)$ es 1
3. Para $u \in U(R)$ existe $v \in U(R)$ tal que $uv = 1$

□

Notemos que para $u \in U(R)$ el inverso es único, porque los inversos son unicos en los grupos. Por lo que replicaremos la notación y denotaremos a los inversos por u^{-1}.

DEFINICIÓN 3. *Sea R un anillo. Denotaremos por R^* a $R - \{0\}$.*
Decimos que R es un campo si $R^* \neq \emptyset$ y $R^* = U(R)$

EJEMPLO 2.
1. *Los racionales son un campo*
2. *Los reales son un campo*
3. *Los complejos son un campo*
4. *Sea p primo, $\mathbb{Z}_p$ es un campo*

DEFINICIÓN 4. *Sea R un anillo. Decimos que R es un dominio entero si $xy = 0$ implica que $x = 0$ o $y = 0$. Equivalentemente si $x \neq 0$ y $y \neq 0$ entonces $xy \neq 0$.*

PROPOSICIÓN 5. *Todo campo es un dominio entero*

DEMOSTRACIÓN. Sean $x, y \in R$ tales que $xy = 0$. Si $x = 0$ ya terminamos.
Si $x \neq 0$ entonces existe $x^{-1} \in R$ tal que $y = x^{-1}xy = x^{-1}0 = 0$ □

PROPOSICIÓN 6 (Tarea). *Sea $n \in \mathbb{Z}$. Entonces $\mathbb{Z}_n$ es dominio entero si y sólo si n es primo.*

DEFINICIÓN 5. *Sea R un anillo y $x \in R$. Decimos que $x \in R$ es nilpotente si existe $n \in \mathbb{N}$ tal que $x^n = 0$*

PROPOSICIÓN 7. *Sea R un anillo y $x \in R$ nilpotente, entonces $1-x \in U(R)$.*

DEMOSTRACIÓN. Sea $n \in \mathbb{N}$ tal que $x^n = 0$, entonces

$$(1-x)\sum_{k=0}^{n-1} x^k = 1 - x^n = 1 - 0 = 1$$

□

PROPOSICIÓN 8. *(Tarea) Sea R un anillo. Si $u \in U(R)$ y x es nilpotente, entonces $u+x \in U(R)$.*

2. Subestructuras

En esta sección se introducirán y estudiarán dos tipos especiales de subestructuras asociadas a un anillo, a saber, los subanillos e ideales. Las definiciones presentadas se darán en el contexto no necesariamente conmutativo como una muestra de la complejidad de dichas definiciones, sin embargo, más allá de esta sección se tratará la teoría en el contexto conmutativo como se mencionó en la sección anterior. Por lo tanto, en esta parte de las notas *R* es un anillo no necesariamente conmutativo.

2.1. Subanillos.

DEFINICIÓN 6. *Sea $S \subseteq R$. Decimos que S es un subanillo de R si se satisfacen las siguientes propiedades:*

1. $(S,+)$ *es un subgrupo de* $(R,+)$
2. *Para cualesquiera $x,y \in S$, $xy \in S$*
3. $1 \in S$

Observación: Una definción alterna de subanillo (la que muestra que es efectivamente esta es una subestructura para un anillo) dice que $S \subseteq R$ es subanillo si $(S, +_{S\times S}, \cdot_{S\times S})$ es un anillo. Es decir, un subanillo es un subconjunto de *R* que es anillo con las operaciones inducidas por *R*. En particular esto dice que todo subanillo es por derecho propio un anillo.

EJEMPLO 3. *Todo anillo es subanillo de si mismo. En particular, $\mathbb{Z}$ es el único subanillo de $\mathbb{Z}$ y para cualquier $n \in \mathbb{N}^+$, el único subanillo de $\mathbb{Z}_n$ es $\mathbb{Z}_n$*

EJEMPLO 4. *Los enteros Gaussianos $\mathbb{Z}[i] := \{a+bi \mid a,b \in \mathbb{Z}\}$ son un subanillo de $\mathbb{C}$*

EJEMPLO 5. *Existe una cadena de subanillos:*

$$\{a+b\sqrt{5} : a,b \in \mathbb{Z}\} \subseteq \{q_1+q_2\sqrt{5} : q_1,q_2 \in \mathbb{Q}\} \subseteq \mathbb{R} \subseteq \mathbb{C}$$

EJEMPLO 6. $\begin{pmatrix} \mathbb{R} & \mathbb{R} \\ 0 & \mathbb{R} \end{pmatrix} := \{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \mid a,b,c \in \mathbb{R}\}$ *es subanillo de* $M_2(\mathbb{R})$. *De hecho esto sigue siendo valido al reemplazar a* $\mathbb{R}$ *por cualquier anillo conmutativo.*

De la observación realizada anteriormente se puede intuir que el concepto de subanillo es el claro análogo al de subgrupo de la teoría de grupos. Por tal razón varias de las construcciones realizadas para subgrupos son válidas para subanillos. Por ejemplo, se tiene el siguiente resultado:

PROPOSICIÓN 9. *Sea* $\{S_\alpha\}_{\alpha\in\Lambda}$ *una familia no vacía de subanillos de R. Entonces* $\bigcap_{\alpha\in\Lambda} S_\alpha$ *es un subanillo de R*

DEMOSTRACIÓN. Es claro □

Entre otras cosas, al recordar la proposición análoga a la anterior en el contexto de la teoría de grupos, dicho resultado permitía probar la existencia del subgrupo generado por un conjunto. Para el caso de subanillos se tiene la propiedad análoga, para la cual la definición correspondiente es:

DEFINICIÓN 7. *Sea* $X \subseteq R$. *El subanillo generado por el conjunto X es el* $\subseteq -$*minimo subanillo de R que contiene a X. Es decir, si este se denota por* $S_R(X)$, *este cumple las siguientes propiedades:*

1. $X \subseteq S_R(X)$ *y* $S_R(X)$ *es subanillo de R*
2. *Si existe S subanillo de R tal que* $X \subseteq S$ *entonces* $S_R(X) \subseteq S$.

En la definición anterior se ha usado el árticulo "el" y se ha puesto una notación para el subanillo generado por un conjunto. Insistiremos en que esto se hace cuando dicha construcción tiene unicidad, independientemente de si esta exista o no para cualquier subconjunto. El siguiente resultado justifica dicha convención y ademas dice que este siempre existe.

PROPOSICIÓN 10. *Si* $X \subseteq R$, *entonces existe un único subanillo generado por X*.

DEMOSTRACIÓN. Defina $S_R(X) := \bigcap\{S \subseteq R \ : \ S$ es subanillo de R y $X \subseteq S\}$. Esta construcción da la existencia de dicho subanillo y la unicidad se deduce desde la definición de subanillo generado sin usar la definición dada en esta prueba. □

EJEMPLO 7. *Sea $x \in R$. En este caso se tiene que*

$$S_R(\{x\}) = \{a_0 1 + a_1 x + \ldots + a_n x^n : n \in \mathbb{N},\ a_0, a_1, \ldots, a_n \in \mathbb{Z}\}$$

Observe que en este caso el conjunto de la derecha se puede identificar con $\mathbb{Z}[x]$.[1] *Esta ultima observación justifica la notación usada para los enteros Gaussianos y muestra que dicho anillo es el subanillo generado por $i \in \mathbb{C}$.*

Observación: El ejemplo anterior da lugar a una notación estándar que se usa en teoría de números y teoría de anillos, a saber, que para cualquier $q \in \mathbb{Z}$ libre de cuadrados, se escriba

$$\mathbb{Z}[\sqrt{q}] := \{a + b\sqrt{q} \ :\ a, b \in \mathbb{Z}\}.$$

Además, el ejercicio 13 generaliza la idea tratada en el ejemplo anterior.

EJERCICIO 1. *Sea $X \subseteq R$ con R abeliano. Demuestra que $S_R(X) = \{f(x_1, \ldots x_n) \ :\ f \in \mathbb{Z}[y_1, \ldots y_n], n \in \mathbb{N}^+\}$*

Para concluir esta subsección se van a hacer un par de comentarios. El primero de ellos tiene que ver con el hecho de que la suma de subanillos (como subgrupos abelianos) no es subanillo. Para ser más específicos, si $S_1, S_2 \subseteq R$ son subanillos, observe que el grupo abeliano $S_1 + S_2 \subseteq R$ no tiene por que ser un subanillo. El ejemplo mas simple se da al considerar $R = \mathbb{Z}[x,y]$, $S_1 = \mathbb{Z}[x]$ y $S_2 = \mathbb{Z}[y]$. Observe que $x, y \in S_1 + S_2$, pero $xy \notin S_1 + S_2$.

La segunda observación tiene que ver con cocientes. Recuerde que en teoría de grupos y álgebra lineal es importante introducir la idea de estructura cociente por muchas razones, como por ejemplo, los teoremas de isomorfismo. Luego, respecto a esta discusión se va a realizar la siguiente discusión: Considere $S \subseteq R$ un subanillo. Asociado a este se puede considerar el grupo abeliano R/S cuya operación esta definida por

$$(x + S) + (y + S) := (x + y) + S.$$

La pregunta es entonces si R/S tiene una estructura de anillo que se herede por la estructura de R, es decir, que si al definir la asignación $\cdot : R/S \times R/S \to R/S$ mediante la regla de correspondencia $(x+S)\cdot(y+S) := xy + S$, esta da una estructura de anilllo en R/S.
No es dificil ver que esta definición de producto satisface todos los axiomas necesarios para que R/S sea un anillo. Sin embargo, hay un problema fundamental: esta asignación no es una función, es decir, depende de representantes.
Un ejemplo concreto se obtiene al considerar $R = \mathbb{C}$ y $S = \mathbb{Z}[i]$. Observe que $(3/2) + S = (1/2 + i) + S$. Sin embargo, por un lado $((3/2) + S)(1/2 + S) = (3/4) + S$, mientras que $((1/2 + i) + S)(1/2 + S) = (1/4 + i/2) + S$. Observe que $(1/4 + i/2) + S \neq 3/4 + S$

[1] Para que esto se haga de manera formal se tiene que introducir el concepto de morfismo de anillos. Además es importante observar que en este momento para $m \in \mathbb{Z}$ y $x \in R$, mx es simplemente una notación que proviene de la teoría de grupos abelianos.

Esta observación realizada hace que la estructura de subanillo pase a segundo plano pues como se ha visto esta no es buena para definir cocientes. Luego, la siguiente sección está dedicada al estudio de aquellos subgrupos aditivos de un anillo que permiten darle estructura de anillo al grupo cociente respectivo.

2.2. Ideales.

DEFINICIÓN 8. *Sea $I \subseteq R$ un subgrupo aditivo. Decimos que I es un ideal izquierdo si para cualquier $r \in R$ y $x \in I$, se tiene que $rx \in I$. Dualmente, I es un ideal derecho si para cualquier $r \in R$ y $x \in I$, se tiene que $xr \in I$.*

Finalmente I es un ideal bilateral si es ideal izquierdo y derecho simultáneamente.

Notación: Si $I \subseteq R$ es un ideal izquierdo, esto se denotará por ${}_RI \leq R$. Cuando I sea un ideal derecho se escribirá $I_R \leq R$. En el caso que I sea bilateral escribiremos ${}_RI_R \leq R$.

Observaciones:

1. Si R es un anillo conmutativo, son equivalentes para $I \subseteq R$ un subgrupo aditivo:
   a) ${}_RI \leq R$
   b) $I_R \leq R$
   c) ${}_RI_R \leq R$

   Por tal razón, en este caso se suele decir que I es un ideal de R (a secas) y esto se denota simplemente por $I \leq R$
2. Asociado a cualquier anillo R, se puede considerar al anillo apuesto, el que se denota por R^{op}, y se define como sigue: Como grupo abeliano $(R^{op},+) = (R,+)$, mientras que si $\cdot : R \times R \to R$ denota el producto del anillo R, el producto en el anillo opuesto $\cdot_{op} : R^{op} \times R^{op} \to R^{op}$ está definido por

   $$x \cdot_{op} y = y \cdot x.$$

   Observe que en efecto $(R^{op}, +_{op}, \cdot_{op})$ es un anillo con los mismos elementos distinguidos que R. Mas aún, R es conmutativo si y sólo si $R = R^{op}$. Además nótese que para un subgrupo aditivo $I \subseteq R$ son equivalentes:
   a) ${}_RI \leq R$
   b) $I_R \leq R^{op}$.

   Por lo tanto, todo resultado que se pruebe para ideales izquierdos es automáticamente valido para ideales derechos y vicevera. Note que esto implica que dicho resultados también serán validos para ideales biaterales.

EJEMPLO 8. *Para cualquier anillo R son ideales bilaterales 0 y R. Dado que ${}_R0_R \leq R$ y 0 no es un subanillo, esto proporciona un ejemplo de un ideal que no es un subanillo. A los ideales de este ejemplo se les conoce como ideales triviales.*

El ejemplo anterior muestra una dirección de comparación entre los conceptos de ideal y subanillo. Para la comparación restante se puede usar el siguiente resultado de carácter general.

PROPOSICIÓN 11. *Para un anillo R son equivalentes para ${}_RI \leq R$:*

1. $I = R$
2. $1 \in I$
3. $U(R) \cap I \neq \emptyset$

DEMOSTRACIÓN. $a) \Rightarrow b)$ Es claro.

$b) \Rightarrow c)$ Es obvio pues $1 \in U(R)$

$c) \Rightarrow a)$ Sea $u \in U(R) \cap I$. Observe que como $I \subseteq R$, para probar la contención faltante sea $a \in R$. Como ${}_RI \leq R$, $a = a1 = (au^{-1})u \in I$, lo que prueba la afirmación. □

COROLARIO 1. *Sea $S \subseteq R$ un subanillo. Son equivalentes:*

1. ${}_RS \leq R$
2. $S_R \leq R$
3. ${}_RS_R \leq R$
4. $S = R$

En resumen, la discusión anterior muestra que salvo un caso trivial, los conceptos de subanillo e ideales no coinciden en general.

Continuando con los ejemplos se tiene lo siguiente:

EJEMPLO 9. *Para cualquier $n \in \mathbb{Z}, n\mathbb{Z} \leq \mathbb{Z}$. De hecho, todo ideal de $\mathbb{Z}$ (el cual es bilateral pues $\mathbb{Z}$ es conmutativo) es de esta forma.*

EJEMPLO 10. *Sea $R = M_2(\mathbb{R})$. Entonces,*

$$ {}_R\begin{pmatrix} 0 & \mathbb{R} \\ 0 & \mathbb{R} \end{pmatrix} \leq R $$

$$ \begin{pmatrix} \mathbb{R} & \mathbb{R} \\ 0 & 0 \end{pmatrix}_R \leq R. $$

Esto nos proporciona un ejemplo de un ideal izquierdo que no es derecho y que no es bilateral.

De hecho, resulta que en los anillos de matrices se pueden caracterizar los ideales bilaterales:

EJERCICIO 2. *Para A conmutativo. Sea $J \leq M_n(A)$ un ideal bilateral. Demuestre que existe $I \leq A$ tal que $J = M_n(I)$*

Queda claro de los ejemplos y discusiones anteriores que no todo subconjunto de un anillo es un ideal. Nuevamente se tiene una construcción que asocia a cada uno de estos subconjuntos un ideal.

DEFINICIÓN 9. *Sea $X \subseteq R$. El ideal izquierdo (derecho o bilateral) generado por X es el $\subseteq -$minimo ideal izquierdo (derecho o bilateral) que contiene a X. Este se denota por ${}_R\langle X\rangle$ ($\langle X\rangle_R$ o ${}_R\langle X\rangle_R$ según sea el caso).*

Como siempre la unicidad de dicha construcción puede demostrarse de la definición directamente tomando como hipótesis la existencia. Esto justifica las cuestiones de notación introducidas en la definición. La existencia se deduce del siguiente resultado.

LEMA 1. *La intersección de cualquier familia no vacía de ideales izquierdos (derechos o bilaterales) es un ideal izquierdo (derecho o bilateral).*

DEMOSTRACIÓN. Es directo de la definición □

PROPOSICIÓN 12. *El ideal izquierdo, derecho y bilateral generado por cualquier conjunto existen.*

DEMOSTRACIÓN. Para un anillo R y $X \subseteq R$ definimos:

$$
\begin{aligned}
{}_R\langle X\rangle &= \bigcap\{{}_R I \leq R \,:\, X \subseteq I\} \\
\langle X\rangle_R &= \bigcap\{I_R \leq R \,:\, X \subseteq I\} \\
{}_R\langle X\rangle_R &= \bigcap\{{}_R I_R \leq R \,:\, X \subseteq I\}
\end{aligned}
$$

Dichos conjuntos dan la construcción mencionada en cada caso □

Sean ${}_R\mathscr{I}$ el conjunto de ideales izquierdos de R, $\mathscr{I}_R$ el conjunto de ideales derechos de R, así como ${}_R\mathscr{I}_R$ el conjunto de ideales bilaterales de R. Observe que estos son diferentes del vació pues $0, R \in {}_R\mathscr{I}, \mathscr{I}_R, {}_R\mathscr{I}_R$.

De la última proposición se deduce que existen funciones:

$$\begin{gathered} {}_R\langle \_ \rangle : \mathscr{P}(R) \to {}_R\mathscr{I} \\ \langle \_ \rangle_R : \mathscr{P}(R) \to \mathscr{I}_R \\ {}_R\langle \_ \rangle_R : \mathscr{P}(R) \to {}_R\mathscr{I}_R \end{gathered}$$

Las cuales son monótonas y por lo tanto morfismos de órdenes parciales al considerar en el dominio y el codominio el orden definido por la contención. Esta y otras propiedades se encuentran en el ejercicio 3

EJERCICIO 3. *Sean $X, Y \subseteq R$. Demuestre que:*

1. ${}_R\langle \emptyset \rangle = \langle \emptyset \rangle_R = {}_R\langle \emptyset \rangle_R = 0$
2. *Si $X \subseteq Y$, entonces ${}_R\langle X \rangle \subseteq {}_R\langle Y \rangle$*
3. ${}_R\langle {}_R\langle X \rangle \rangle = {}_R\langle X \rangle$
4. *$X \subseteq R$ es un ideal izquierdo si y sólo si $X =_R \langle X \rangle$.*

EJEMPLO 11. *Para $x \in R$, observe que ${}_R\langle x \rangle := {}_R\langle \{x\} \rangle = \{rx : r \in R\} := Rx$. De forma análoga se puede probar que $\langle x \rangle_R := \langle \{x\} \rangle_R =: xR$ y que ${}_R\langle x \rangle_R := {}_R\langle \{x\} \rangle_R =: RxR$.*[2]

Observe que cuando $R = \mathbb{Z}$, todo ideal de R es de la forma $I = n\mathbb{Z} = \langle n \rangle$. Este tipo de dominios son importantes y se discutirán en una sección posterior.

Antes de continuar con nuestra discusión, vale la pena mencionar un resultado. Para esto se requiere una definición.

DEFINICIÓN 10. *Un anillo de división, R, es un anillo en el que todo elemento no cero tiene un inverso.*

Observe que de la definición se tiene que un campo es un anillo con división conmutativo. De hecho, la diferencia entre anillos de división y campos es simplemente la propiedad de conmutatividad. Por tal razón en muchos textos se les conoce a los anillos de división como semicampos.

PROPOSICIÓN 13. *Las siguientes afirmaciones son equivalentes para un anillo R:*

[2] Esto justifica el porque en muchos libros de texto se denota al ideal izquierdo generado por $x \in R$ por Rx, así como las notaciones restantes para los ideales en cuestión.

1. *R es anillo con división*
2. ${}_R\mathscr{I} = \{0, R\}$
3. $\mathscr{I}_R = \{0, R\}$

DEMOSTRACIÓN. Se va a probar $1 \Leftrightarrow 2$ pues esta prueba se puede adaptar para el otro caso.

$1 \Rightarrow 2)$ Sea $I \in {}_R\mathscr{I}$ con $I \neq 0$. Entonces $I \cap U(R) \neq \emptyset$ y así $I = R$.

$2 \Rightarrow 1)$ Sea $x \in R$ con $x \neq 0$. Observe que ${}_R\langle x \rangle \leq R$ es no cero y así ${}_R\langle x \rangle = R$. Luego existe $a \in R$ tal que $ax = 1$. Por otro lado ${}_R\langle a \rangle = R$, lo que implica existe $b \in R$ tal que $ba = 1$. Esto implica $b = x$ y así $x \in U(R)$ □

De la observación previa al resultado se deduce que un anillo conmutativo es un campo si y sólo si sus únicos ideales son los triviales.

Regresando a nuestra discusión principal, para lo cual es importante mencionar que hay una generalización del ejemplo 11, la cual se muestra en el siguiente resultado, el cual básicamente dice que el ideal generado por un conjunto se puede ver como el conjunto de combinaciones $R-$*lineales* de elementos en dicho conjunto.

PROPOSICIÓN 14. *Sea $X \subseteq R$. Entonces,*

$$
\begin{aligned}
{}_R\langle X \rangle &= \{\sum_{i=1}^{n} a_i x_i \ : \ n \in \mathbb{N}, a_1, \ldots, a_n \in R, x_1, \ldots, x_n \in X\} \\
\langle X \rangle_R &= \{\sum_{i=1}^{n} x_i a_i \ : \ n \in \mathbb{N}, a_1, \ldots, a_n \in R, x_1, \ldots, x_n \in X\} \\
{}_R\langle X \rangle_R &= \{\sum_{i=1}^{n} a_i x_i b_i \ : \ n \in \mathbb{N}, a_1, b_1, \ldots, a_n, b_n \in R, x_1, \ldots, x_n \in X\}
\end{aligned}
$$

DEMOSTRACIÓN. Solamente se va a probar las primera de las igualdades pues las restantes se demuestran de la misma forma. Además observe que si $X = \emptyset$ la demostración es obvia, por lo que supóngase que $X \neq \emptyset$.
Sea $\alpha = \sum_{i=1}^{n} a_i x_i$ con $a_1, ..., a_n \in R$ y $x_1, .., x_n \in X$. Observe que como $X \subseteq {}_R\langle X \rangle$, entonces $x_1, \ldots, x_n \in {}_R\langle X \rangle$ y así $a_1 x_1, \ldots, a_n x_n \in {}_R\langle X \rangle$. Luego, $\alpha \in {}_R\langle X \rangle$, lo que demuestra la contención de derecha a izquierda.

Para la contención de izquierda a derecha observe que $X \subseteq \{\sum_{i=1}^{n} a_i x_i : n \in \mathbb{N}, a_1, \ldots, a_n \in R, x_1, \ldots, x_n \in X\}$. Por otro lado observe que el conjunto de combinaciones R-lineales considerado es un ideal izquierdo pues 0 es una combinación $R-$*lineal* y además la

diferencia de dos combinaciones $R-lineales$ en X es $R-lineal$. Esto prueba que dicho conjunto es un subgrupo. Para ver que es un ideal izquierdo observe que dado $a \in R$ y $\sum_{i=1}^{n} a_i x_i$ una combinación $R-lineal$ de elementos en X, se tiene por distributividad que

$$a(\sum_{i=1}^{n} a_i x_i) = \sum_{i=1}^{n} a a_i x_i,$$

lo que es una combinación $R-lineal$ de elementos en X. Así como dicho conjunto de combinaciones $R-lineales$ es un ideal que contiene a X, por minimalidad de ${}_R\langle X\rangle$, se concluye la igualdad □

Para concluir esta sección se va a ver que el concepto de ideal es el que permite hacer cocientes. Esto se muestra en la siguiente afirmación.

PROPOSICIÓN 15. *Sea ${}_R I_R \leq R$. Entonces el grupo abeliano R/I tiene estructura de anillo con el producto $(x+I)(y+I) = xy+I$. En dicha estructura el neutro es $1+I$.*

DEMOSTRACIÓN. La prueba se reduce a demostrar que la asignación mencionada es una función pues al demostrar esto el resto de las propiedades son obvias. En efecto, supóngase que,

$$x+I = x'+I$$
$$y+I = y'+I$$

Esto dice que $x-x', y-y' \in I$. Como I es en particular un ideal derecho, $(x-x')y \in I$ y al ser este en particular ideal izquierdo $x'(y-y') \in I$. Luego esto implica que

$$(x-x')y + x'(y-y') \in I.$$

Observe que

$$(x-x')y + x'(y-y') = xy - x'y',$$

lo que nos dice que

$$xy+I = x'y'+I$$

y prueba la afirmación. □

Es importante hacer notar que en la prueba se usa de forma fuerte el hecho de que el ideal sea bilateral, por tal razón los ideales bilaterales son los que permiten dar estructura de anillo a R/I. De hecho observe que:

PROPOSICIÓN 16. *Sea $I \subseteq R$ un subgrupo aditivo. R/I tiene estructura de anillo con el producto $(x+I)(y+I) = xy+I$ si y sólo si ${}_R I_R \leq R$*

DEMOSTRACIÓN. $\Leftarrow$) Proposición anterior.

$\Rightarrow$) Sean $x \in I$ y $a \in R$. Entonces $ax+I = (a+I)(x+I) = (a+I)(0+I) = 0+I$ así $ax \in I$ y prueba que ${}_RI \leq R$. De forma análoga se tiene que $xa+I = (x+I)(a+I) = (0+I)(a+I) = 0+I$, así $xa \in I$ y esto prueba que $I_R \leq R$, concluyendo la prueba. □

Otra observación es que para $I, J \leq R$ ideales izquierdos, el subgrupo $I+J \leq R$ es un ideal izquierdo como consecuencia de la propiedad distributiva. Esto muestra que nuevamente el concepto de ideal cumple otra propiedad que no es valida para subanillos en general.

Más aún, puede verse que las familias ${}_R\mathscr{I}$, $\mathscr{I}_R$ y ${}_R\mathscr{I}_R$ son retículas completas pues estas familias son cerradas bajo intersecciones. Además, en lo que respecta al supremo de una familia de ideales, puede considerarse el generado de la unión de estos, lo que notacionalmente se suele llamar la suma de ideales pues coincide con esta en el caso finito. Para ser específicos, si $\{I_\alpha\}_{\alpha\in\Lambda}$ es una familia de ideales izquierdos de R, entonces

$$\bigwedge_{\alpha\in\Lambda} I_\alpha = \bigcap_{\alpha\in\Lambda} I_\alpha$$

$$\bigvee_{\alpha\in\Lambda} I_\alpha = {}_R\left\langle \bigcup_{\alpha\in\Lambda} I_\alpha \right\rangle := \sum_{\alpha\in\Lambda} I_\alpha$$

Observe que en el caso del supremo los elementos se pueden describir como combinaciones R-lineales finitas de elementos en los ideales de la familia en cuestión, de ahí el nombre de esta operación.

Para concluir, es importante mencionar que estas retículas no son distributivas, pero sí modulares. Estas propiedades se tratarán en los ejercicios.

3. Morfismos

DEFINICIÓN 11. *Sean R, S anillos y $f : R \to S$ una función. Decimos que f es un morfismo de anillos si f cumple:*

1. $f(x+_R y) = f(x) +_S f(y)$ *para todo* $x, y \in R$
2. $f(xy) = f(x)f(y)$ *para todo* $x, y \in R$
3. $f(1_R) = 1_S$

EJEMPLO 12. *Sea $f : \mathbb{C} \to \mathbb{C}$ definida como $f(z) = \bar{z}\ \forall z \in \mathbb{C}$ es un morfismo de anillos.*

DEFINICIÓN 12. *Si $f : R \to S$ es un morfismo de anillos. Decimos que f es un isomorfismo si es f biyectiva.*

PROPOSICIÓN 17. *Sea R un anillo e $I \leq R$. Entonces $\pi : R \to R/I$ definido como $\pi(x) = x+I$. Es un morfismo de anillos.*

DEMOSTRACIÓN. Sean $x, y \in R$, entonces

$$\begin{aligned}\pi(x+y) &= (x+y)+I \\ &= x+I+y+I \\ &= \pi(x)+\pi(y)\end{aligned}$$

Ademas

$$\begin{aligned}\pi(xy) &= xy+I \\ &= (x+I)(y+I) \\ &= \pi(x)\pi(y)\end{aligned}$$

por ultimo se tiene que

$$\pi(1) = 1+I = 1_{R/I}$$

□

PROPOSICIÓN 18. *(Tarea) Sea R un anillo y $S \subseteq R$ un subanillo. Entonces la incluisión $i : S \to R$ es un morfismo de anillos.*

PROPOSICIÓN 19. *Sea $f : R \to S$ un morfismo de anillos. Entonces $Nuc(f) \leq R$ es un ideal de R e $im(f) \subseteq S$ es un subanillo de S.*

DEMOSTRACIÓN. Sean $x, y \in Nuc(f)$ y $a \in R$. Entonces

$$f(ax+y) = af(x)+f(y) = a0+0 = 0$$

por lo tanto $ax+y \in Nuc(f)$ así $Nuc(f) \leq R$

Sean $x, y \in R$, entonces

$$\begin{aligned}f(x)+f(y) &= f(x+y) \in Im(f) \\ f(x)f(y) &= f(xy) \in Im(f) \\ 1 &= f(1) \in Im(f)\end{aligned}$$

Por lo que $Im(f)$ es subanillo de S. □

PROPOSICIÓN 20. *Sea R un anillo. Entonces existe un único morfismo de anillos $\eta_R : \mathbb{Z} \to R$.*

DEMOSTRACIÓN. Definimos $\eta_R(n) = n \cdot 1$
Observemos que,

$$\eta_R(n+m) = (n+m)\cdot 1 = n\cdot 1 + m\cdot 1 = \eta_R(n) + \eta_R(m)$$

$$\eta_R(nm) = nm\cdot 1 = n\cdot 1\cdot m\cdot 1 = \eta_R(n)\eta_R(m)$$

$$\eta_R(1) = 1\cdot 1 = 1$$

si $g : \mathbb{Z} \to R$ es un morfismo de anillos entonces $g(n) = ng(1) = n\cdot 1 = \eta_R(n)$ por lo tanto el morfismo es único. □

DEFINICIÓN 13. *Sea R un anillo. Como* $Nuc(\eta_R) \leq \mathbb{Z}$ *entonces* $Nuc(\eta_R) = n\mathbb{Z}$ *para alguna* $n \in \mathbb{N}$. *Definimos la característica de R como n. Y la denotamos por* $car(R) = n$

PROPOSICIÓN 21. *(Tarea) Sea R un anillo. Entonces* $car(R) = n$ *si y sólo si* $n = min\{k \in \mathbb{N} : kx = 0, \forall x \in R\}$

PROPOSICIÓN 22. *Sea R un dominio entero. Entonces* $car(R) = p$ *con p primo o* $car(R) = 0$

DEMOSTRACIÓN. Si $car(R) = n = mk$ con $n > m > 1$ y $n > k > 1$, entonces

$$(m\cdot 1)(k\cdot 1) = mk\cdot 1 = n\cdot 1 = 0$$

notemos que $m\cdot 1 \neq 0$ y $k\cdot 1 \neq 0$,
Si $m\cdot 1 = 0$ entonces $mx = m\cdot 1x = 0$. Lo cual contradice la minimalidad de n. Análogamente para k.
Por lo que R no seria dominio entero. □

COROLARIO 2. *Sea K un campo. Entonces* $car(K) = 0$ *0* $car(K) = p$ *con p primo.*

LEMA 2. *(Técnico) Sea* $f : R \to S$ *un morfismo de anillos e* $I \leq R$ *con* $I \subseteq Nuc(f)$. *Entonces* $\bar{f} : R/I \to S$ *dada por* $\bar{f}(x+I) = f(x)$ *para* $x+I \in R/I$ *esta bien definida y es un morfismo de anillos. Mas aun,* $\bar{f}$ *es inyectiva si y sólo si* $I = Nuc(f)$

DEMOSTRACIÓN. Que esta bien definida se sigue de la teoría de grupos, también que sea morfismo de grupos.

Sean $x, y \in I$,

$$\begin{aligned}\bar{f}((x+I)(y+I)) =& \bar{f}(xy+I)\\ =& f(xy)\\ =& f(x)f(y)\\ =& \bar{f}(x+I)\bar{f}(y+I)\end{aligned}$$

□

PROPOSICIÓN 23. *(Primer Teorema de Isomorfismo) Sea $f : R \to S$ un morfismo de anillos. Entonces $\bar{f} : R/Nuc(f) \to Im(f)$ es un isomorfismo.*

PROPOSICIÓN 24. *(Tarea) Sea $f : R \to S$ un isomorfismo. Entonces f^{-1} es un morfismo de anillos.*

DEFINICIÓN 14. *Sea $f : R \to S$ un morfismo de anillos.*

1. *Decimos que f es un monomorfismo, si para $g, h : T \to R$ morfismo de anillo, tales que $f \circ g = f \circ h$ implica $g = h$.*
2. *Decimos que f es un epimorfismo de anilos, si para $g, h : S \to T$ morfismos de anillos tales que $g \circ f = h \circ f$ implica $g = h$*

Observemos que si f es un morfismo de anillos inyectivo entonces f es un monomorfismo.
Si f es suprayectivo entonces f es un epimorfismo.
Los monomorfismos son funciones inyectivas, pero se vera mas adelante. Pero los epimorfismos no son funciones suprayectivas.

Si $f : R \to S$ es un morfismo de anillos e $I \leq R$ entonces $f(I)$ no tiene por que ser un ideal de S.
Por ejemplo $i : \mathbb{Z} \to \mathbb{Q}$ con $I = \mathbb{Z}$. Sabemos que $\mathbb{Z}$ no puede ser un ideal de $\mathbb{Q}$.

DEFINICIÓN 15. *Sea $f : R \to S$ un morfismo e $I \leq R$. Definimos $I^f := \langle f(I) \rangle$ como el ideal generado por $f(I)$ en S. A I^f lo llamamos la extensión de I.*

PROPOSICIÓN 25. *(Tarea) Sea $f : R \to S$ un morfismo de anillos e $I \leq R$ entonces*

$$I^f = \{\sum_{i=1}^{n} s_i f(x_i) : s_i \in S, x_i \in I\}$$

PROPOSICIÓN 26. *(Tarea) Si $f : R \to S$ es un morfismo de anillos e $I \leq S$, entonces $f^{-1}(I) \leq R$.*

Notemos que $Nuc(f) = f^{-1}(0)$

DEFINICIÓN 16. *Sea $f : R \to S$ un morfismo de anillos e $I \leq S$.*

Definimos $I_f := f^{-1}(I)$. A I_f lo llamamos la contracción de I.

PROPOSICIÓN 27. *(Tarea) Sea $f : R \to S$ un morfismo de anillos, $I \leq R$ y $J \leq S$. Entonces:*

1. $I \leq I_f^f$, $J_f^f \subseteq J$
2. $J_f = J_{ff}^f$, $I^f = I_f^{ff}$

PROPOSICIÓN 28. *(Tarea) Sea $f : R \to S$ un morfismo de anillos. $I,J \leq R$ y $K,L \leq S$. Entonces:*

1. $(I+J)^f = I^f + J^F$, $K_f + L_f \subseteq (K+L)_f$
2. $(I \cap J)^f \subseteq I^f \cap J^f$, $(K \cap L)_f = K_f \cap L_f$
3. $(IJ)^f = I^f J^f$, $K_f L_f \subseteq (KL)_f$
4. $(I : J)^f \subseteq (I^f : J^f)$, $(K : L)_f \subseteq (K_f : L_f)$

DEFINICIÓN 17. *Sea A un anillo. Ponemos como $\mathscr{L}(A)$ como la retícula completa de ideales de A. Si I es un ideal de A definimos $\mathscr{L}_I(A)$ como la retícula de ideales de A que contienen a I.*

PROPOSICIÓN 29 (Teorema de la correspondencia biyectiva). *Sea A un anillo e I un ideal de A. Entonces hay un isomosrfismo de retículas entre $\mathscr{L}(A/I)$ y $\mathscr{L}_I(A)$.*

DEMOSTRACIÓN. Tarea □

4. Dominios

En esta sección se van a estudiar algunos ejemplos de dominios enteros con propiedades especiales. Esta teoría es relevante pues como se verá, se generalizan varias propiedades básicas de la teoría de números para el contexto de anillos. Entre otras cosas, esto permitirá explicar de forma general algunas propiedades comunes de los anillos $\mathbb{Z}$ y $k[x]$.

A lo largo de esta sección R denotará a un dominio entero. Recuerde que $R^* = R \setminus \{0\}$.

DEFINICIÓN 18.

1. *Sean $x,y \in R$. Decimos que x divide a y, lo que se denotará por $x|y$, si existe $z \in R$ tal que $y = xz$.*
2. *$x \in R^* \setminus U(R)$ es irreducible si siempre que $x = yz$ con $y,z \in R$, entonces $y \in U(R)$ ó $z \in U(R)$.*
3. *$x \in R^* \setminus U(R)$ es primo si siempre que $x|yz$ se tiene que $x|y$ o $x|z$.*

Observaciones:

1. Dados $x, y \in R$, Si $x|y$ y $x \neq 0$, el testigo de divisibilidad es único.
2. Todo elemento primo es irreducible. Se sabe que en $\mathbb{Z}$ y $k[x]$ dichas nociones coinciden, pero esto no sucede en general (Ejercicio 4).

EJERCICIO 4. *Dar un ejemplo de un dominio entero en el que exista un elemento irreducible que no sea primo.*

La primera noción especial de dominio que se va a introducir en esta sección axiomatiza a aquellos dominios que tienen un algoritmo de la división.

DEFINICIÓN 19. *Un dominio entero R es un Dominio Euclidiano (DE) si existe una función*

$$\delta : R^* \to \mathbb{N}$$

tal que:

1. *Si $x|y$ con $x, y \in R^*$, entonces*

$$\delta(x) \leq \delta(y)$$

2. *Para cualesquiera $x, y \in R$ con $y \neq 0$, existen $q, r \in R$ tales que*

$$x = qy + r,$$

con $r = 0$ ó $\delta(r) < \delta(y)$.

A dicha función δ se le conoce como función euclidiana. Además, es común representar a los DE como parejas (R, δ).

EJEMPLO 13. *Todo campo es un DE con función euclidiana $\delta = 0$.*

EJEMPLO 14. *$\mathbb{Z}$ es un DE con función euclidiana $\delta = |\_|$, el valor absoluto. Observe que esto muestra un ejemplo de un DE que no es un campo.*

EJEMPLO 15. *Si k es un campo, $k[x]$ es un DE con función euclidiana el grado. En general $R[X]$ no es un DE incluso cuando R lo sea. Un ejemplo de esta última afirmación se da cuando $R = \mathbb{Z}$ (Ejemplo 17).*

EJEMPLO 16. *Los enteros Gaussianos $\mathbb{Z}[i]$ con la función*

$$\delta : \mathbb{Z}[i]^* \to \mathbb{N}$$

definida como

$$\delta(a+bi) = a^2 + b^2,$$

es un DE.[3]

El siguiente tipo especial de dominio que se va a introducir tiene que ver con aquellos anillos en los que sus ideales son lo más simples posibles, es decir, son generados por un elemento.

DEFINICIÓN 20. *Un dominio entero R es un Dominio de Ideales Principales (DIP) si todo ideal es principal, es decir, es generado por un elemento.*

El siguiente resultado da la relación entre las dos definiciones dadas.

PROPOSICIÓN 30. *Todo DE es un DIP.*

DEMOSTRACIÓN. Suponga que R es un DE y sea $I \leq R$. Si $I = 0$, entonces no hay nada que demostrar pues $I = \langle 0 \rangle$. Así, supóngase que $I \neq 0$. Luego, considere el conjunto

$$M = \{\delta(x) \ : \ x \in I \text{ con } x \neq 0\} \subseteq \mathbb{N}.$$

Dado que $M \neq \emptyset$, por el Principio del Buen Orden, existe $m \in M$ mínimo. Sea $x_0 \in I$ tal que $m = \delta(x_0)$. Lo que se afirma es que $I = \langle x_0 \rangle$.

En efecto, primero observe que obviamente $\langle x_0 \rangle \subseteq I$. En lo respecta a la contención faltante, considere $x \in I$. Por ser R un DE existe $q, r \in R$ tales que $x = qx_o + r$ con $r = 0$ ó $\delta(r) < \delta(x_0)$. Observe que no puede suceder que $\delta(r) < \delta(x_0)$ ya que como $r = x - qx_0 \in I$, esto contradice la minimalidad de x_0. Luego, $r = 0$ y así $x = qx_0 \in \langle x_0 \rangle$. Esto demuestra la contención faltante y prueba la afirmación. □

EJEMPLO 17. *El ideal $\langle 2, x \rangle \leq \mathbb{Z}[x]$ no es principal. Por lo tanto, $\mathbb{Z}[x]$ no es un DIP. Al usar la contrapositiva del resultado anterior se deduce que $\mathbb{Z}[x]$ no es un DE.*

[3]En muchos libros de teoría de números a la función δ se le llama norma gaussiana o simplemente norma.

El siguiente ejemplo muestra que aunque se tiene una implicación, los conceptos definidos no son equivalentes.

EJEMPLO 18. *(Tarea) El anillo*

$$\{a+b\frac{1+\sqrt{19}i}{2} \ : \ a,b \in \mathbb{Z}\}$$

es un DIP que no es DE.

Vale la pena comentar que la prueba de la proposición anterior es una generalizacioń de la prueba que se hace para demostrar que todo ideal de $\mathbb{Z}$ es de la forma $n\mathbb{Z}$. De hecho observe que el hecho de que $\mathbb{Z}$ y $k[x]$ tengan únicamente ideales principales es consecuencia de que estos son DE. Además recuerde que en estos anillos el concepto de elemento primo e irreducible coinciden. Esto es nuevamente un hecho que se deduce de un resultado general.

PROPOSICIÓN 31. *Si R es un DIP, entonces todo elemento irreducible es primo.*

DEMOSTRACIÓN. (Tarea) □

Nota: Observe que en un dominio entero se puede definir la idea de mínimo común múltiplo y máximo común divisor de la forma obvia, los cuales son únicos salvo una unidad. En un DIP un mínimo común múltiplo de dos elementos x y y se puede obtener como un generador del ideal

$$\langle x\rangle \cap \langle y\rangle,$$

mientras que el máximo común divisor de dichos elementos como un generador del ideal

$$\langle x\rangle + \langle y\rangle$$

. La intuición de estas ideas se encuentra inspirada en lo que sucede en la teoría de $\mathbb{Z}$, ya que es bien sabido que:

$$n\mathbb{Z} \cap m\mathbb{Z} = [n,m]\mathbb{Z}$$
$$n\mathbb{Z} + m\mathbb{Z} = (n,m)\mathbb{Z}.$$

Retomando la discusión de la nota previa a la última proposición y la nota, vale la pena dar un resultado que caracteriza cuándo los anillos de polinomios en una variable son DIP, ya que observe que esto no sucede cuando se tiene más de una variable pues el ideal generado por las variables no es principal (Ver ejemplo 20).

PROPOSICIÓN 32. *Para R un dominio entero son equivalentes:*

1. *R es un campo*
2. *R*$[x]$ *es un DE*
3. *R*$[x]$ *es un DIP*

DEMOSTRACIÓN. Es bien conocida la implicación $1 \Rightarrow 2$. Por otro lado en esta sección se demostró que $2 \Rightarrow 3$. Lo único que falta demostrar es $3 \Rightarrow 1$, para lo que se va a demostrar es que los únicos ideales de R son los triviales. Para esto observe que considerar el ideal $\langle x \rangle \leq R[x]$, el primer teorema de isomorfismo aplicado el morfismo evaluación en cero, $ev_0 : R[x] \to R$, implica que existe un isomorfismo entre $R[x]/\langle x \rangle = R$. El teorema de la correspondencia biyectiva dice que todo $I \leq R$, corresponde a un ideal $\bar{I} \leq R[x]$ tal que $\langle x \rangle \subseteq \bar{I}$. Dado que $R[x]$ es un DIP, entonces existe $f \in R[x]$ tal que $\bar{I} = \langle f \rangle$. De esto se deduce que existe $g \in R[x]$ tal que $x = gf$, por lo que al aplicar la función grado se tiene que $1 = \partial(x) = \partial(g) + \partial(f)$. Esta igualdad da lugar a dos casos:

Caso 1: $\partial(g) = 0$ y $\partial(f) = 1$. Dado que $f = a_0 + a_1 x$, entonces la igualdad $x = gf$ implica que $ga_0 = 0$ y $ga_1 = 1$. Observe que dado que la segunda igualdad dice que $g \in U(R)$, entonces de la primera igualdad se deduce que $a_0 = 0$. Como además la segunda igualdad también dice que $a_1 \in U(R)$, entonces $\bar{I} = \langle f \rangle = \langle a_1 x \rangle = \langle x \rangle$. Del teorema de la correspondencia biyectiva se deduce que $I \cong \bar{I}/\langle x \rangle = 0$.

Caso 2: $\partial(g) = 1$ y $\partial(f) = 0$. En este caso al ser $g = a_0 + a_1 x$, la igualdad $x = gf$ implica que $a_0 f = 0$ y $a_1 f = 1$. En particular la segunda igualdad implica que $f \in U(R[x])$, luego $\bar{I} = R[x]$. Por lo tanto, del teorema de la correspondencia biyectiva se deduce que $I \cong R[x]/\langle x \rangle \cong R$. □

La última noción que se va a introducir axiomatiza a aquellos dominios en los que existe un teorema fundamental de la aritmética.

DEFINICIÓN 21. *Un dominio entero R es un Dominio de Factorización Única (DFU) si todo elemento no cero y no unidad se puede expresar como el producto de elementos irreducibles. Además, dicha descomposición es única en el siguiente sentido: Si $x \in R^* \backslash U(R)$ tiene dos factorizaciones como producto de elementos irreducibles $x = p_1 \cdot \ldots \cdot p_n = q_1 \cdot \ldots \cdot q_m$, entonces $n = m$ y existe $\sigma \in S_n$ tal que para cada $i \in \{1, \ldots, n\}$, $p_i = u_i q_{\sigma(i)}$ para alguna $u_i \in U(R)$ (la cual es necesariamente única).*

La relación con los conceptos definidos se da con la proposición siguiente.

PROPOSICIÓN 33. *Todo DIP es un DFU.*

DEMOSTRACIÓN. Procediendo por contradicción, sea R un DIP y supóngase que existe $x \in R^* \backslash U(R)$ tal que x no se puede expresar como producto de irreducibles. Defina

$$\mathscr{S} = \{\langle a \rangle \leq R : a \neq 0,\ a \notin U(R),\ \text{y a no se puede expresar como producto de irreducibles}\}.$$

Por hipótesis $\mathscr{S} \neq \emptyset$ y además $(\mathscr{S}, \subseteq)$ es un conjunto parcialmente ordenado. Se quiere aplicar el Lema de Zorn en dicho conjunto. Para esto considere una cadena no vacía en $\mathscr{S}$, $\{\langle a_\lambda \rangle : \lambda \in \Lambda\}$. Nótese que $\bigcup_{\lambda \in \Lambda} \langle a_\lambda \rangle \leq R$ y esta es cota superior de la cadena considerada en $\mathscr{P}(R)$. Además, como R es un DIP, existe $b \in R$ tal que

$$\bigcup_{\lambda \in \Lambda} \langle a_\lambda \rangle = \langle b \rangle.$$

Observe que trivialmente $b \neq 0$. Además, $b \notin U(R)$ pues en caso contrario algún a_λ lo sería. Veamos que b no se puede expresar como un producto de irreducibles, para lo cual nótese que existe $\lambda_0 \in \Lambda$ y $r \in R$ tal que $b = r a_{\lambda_0}$. Dado que $b = rsb$ y al ser R un dominio, $rs = 1$, lo que implica que $r \in U(R)$ y así, como $b = r a_{\lambda_0}$, b no puede ser producto de irreducibles pues a_{λ_0} satisface dicha propiedad.
Esto implica que la cadena tomada es acotada superiormente en $\mathscr{S}$ y así, por el Lema de Zorn existe $\langle y \rangle \in \mathscr{S}$ máximo. Dado que y no es irreducible, existen $u, v \in R$ no unidades tales que $y = uv$. Esto implica que $\langle y \rangle \subsetneq \langle u \rangle$ y $\langle y \rangle \subsetneq \langle v \rangle$, luego u y v se puede expresar como producto de irreducibles , lo cual es una contradicción. De esto se deduce que $\mathscr{S} = \emptyset$ y prueba la existencia de la factorización.

En lo que respecta a la unicidad supóngase que $x \in R^* \backslash U(R)$ se escribe como

$$x = p_1 \cdot \ldots \cdot p_n = q_1 \cdot \ldots \cdot q_m$$

con p_i, q_i irreducibles. Sin pérdida de generalidad supónga que $n \leq m$. Dado que $p_1 | q_1 \cdot \ldots \cdot q_m$, al ser p_1 primo, existe $\sigma(1) \in \{1, \ldots, m\}$ tal que $p_1 | q_{\sigma(1)}$, por lo que existe $v_1 \in R$ tal que $q_{\sigma(1)} = v_1 p_1$. Observe que como $q_{\sigma(1)}$ y p_1 son irreducibles, entonces $v_1 \in U(R)$. Además como

$$x = p_1 \cdot \ldots \cdot p_n = q_1 \cdot \ldots \cdot q_m = q_{\sigma(1)} \left(\prod_{i=1, i \neq \sigma(1)}^{m} q_i \right),$$

esto implica que

$$p_2 \cdot \ldots \cdot p_n = v_1 \left(\prod_{i=1, i \neq \sigma(1)}^{m} q_i \right).$$

Observe que el proceso anterior puede repetirse $(n-1)$ veces más, encontrando $v_2,..,v_n \in U(R)$ tales que $q_{\sigma(i)} = v_i p_i$ con $i \in \{2,..,n\}$ y además se tiene la igualdad

$$1 = (v_1 \cdot ... \cdot v_n)\left(\prod_{i=1, i\notin\{\sigma(1),..,\sigma(n)\}}^{m} q_i\right).$$

Esto ultimo implica que $m = n$ ya que cada uno de los $q_i's$ son irreducibles. Por tal razón observe que los índices $\sigma(1),..,\sigma(n)$ definen un elemento en $\sigma \in S_n$. Además, de esto se deduce que $p_i = u_i q_{\sigma(i)}$ para $i \in \{1,..,n\}$ con $u_i = v_i^{-1}$. □

EJEMPLO 19. *Como consecuencia del resultado anterior se deduce que $\mathbb{Z}[i]$ es un DFU. Este anillo fue introducido por Gauss para estudiar sus teoremas de reciprocidad cuadrática y de hecho Gauss demostró que dicho anillo es un DFU por métodos distintos a los mostrados en esta sección.*

Para ver que nuevamente las implicación anterior no da una equivalencia entre los conceptos invulucrados, se requiere del ejercicio 5.

EJERCICIO 5. *Suponga que A es un DFU. Demuestre que $A[X]$ es un DFU.*

EJEMPLO 20. *Considere el anillo de polinomios en dos variables $\mathbb{Q}[x_1,x_2]$. Observe que como $\mathbb{Q}[x_1,x_2] = (\mathbb{Q}[x_1])[x_2]$, del ejercicio 5 se deduce que $\mathbb{Q}[x_1,x_2]$ es un DFU. Sin embargo, observe que $\mathbb{Q}[x_1,x_2]$ no es un DIP pues el ideal $\langle x_1,x_2\rangle$ no es principal.*

A manera de resumen, en esta seccioón se ha visto que los conceptos de dominios definidos presentan implicaciones entre sí, pero en general no coinciden. Esquemáticamente las implicaciones son

$$\text{Campos} \Rightarrow \text{DE} \Rightarrow \text{DIP} \Rightarrow \text{DFU} \Rightarrow \text{Dominio entero}$$

Salvo la última implicación se han dado ejemplos de que las implicaciones recíprocas no son necesariamente ciertas. Para completar la teoría se va a desarrollar un ejemplo, el cual muestra cómo demostrar ciertas propiedades aritméticas de una familia de anillos muy importante en teoría de números. Los métodos que se usarán son elementales y en el siguiente capítulo se verán técnicas generales para demostrar de una forma menos elemental algunas afirmaciones de la siguiente discusión.

Considere el anillo $R = \mathbb{Z}[\sqrt{-5}] \subseteq \mathbb{C}$, el cual es un dominio entero. Sin embargo, este no es un DFU ya que $6 = 2\cdot 3 = (1+\sqrt{-5})(1-\sqrt{-5})$. Para completar la prueba, lo que se quiere ver es que los elementos $2, 3, 1+\sqrt{-5}, 1-\sqrt{-5} \in R$ son irreducibles y que no se pueden obtener por pares mediante una unidad.

Primero observe que se puede definir una función $N : \mathbb{Z}[\sqrt{-5}] \to \mathbb{N}$ mediante la regla de correspondencia $N(a+b\sqrt{-5}) = a^2+5b^2$. Es sencillo demostrar que esta función es multiplicativa, es decir, para cualesquiera $z, w \in \mathbb{Z}[\sqrt{-5}]$, se tiene que:

$$N(zw) = N(z)N(w).$$

De esta afirmación se deduce que $U(\mathbb{Z}[\sqrt{-5}]) = \{z \in \mathbb{Z}[\sqrt{-5}] \,:\, N(z) = 1\} = \{1,-1\}$. Así, en el conjunto $\{2,3,1+\sqrt{-5},1-\sqrt{-5}\}$ ningún elemento se obtiene al hacer producto de otro de dicho conjunto con una unidad.

Ahora veamos que $2 \in R$ es irreducible. Para esto suponga que $2 = zw$ con $z, w \in R$. Al aplicar la función N, se deduce que $4 = N(2) = N(zw) = N(z)N(w)$. Dado que esta igualdad se da en los enteros, se tienen que $N(z) \in \{1,2,4\}$. Observe que si $N(z) = 1$, se ha concluido la prueba pues $z \in U(R)$. Si $N(z) = 4$, entonces $N(w) = 1$ y así $w \in U(R)$. Para concluir, $N(z) \neq 2$ pues no existen enteros $a, b \in \mathbb{Z}$ tales que $a^2+5b^2 = 2$.

De forma análoga se demuestra los casos restantes. Para ver esto, solamente se va a tratar el caso de $1+\sqrt{-5}$. Para esto supóngase que $1+\sqrt{-5} = zw$ con $z, w \in R$. Al aplicar la función N, $6 = N(z)N(w)$, luego $N(z) \in \{1,2,3,6\}$. Si $N(z) = 1$ y $N(z) = 6$, la conclusión requerida se tiene. No puede suceder que $N(z) = 2,3$ pues no se pueden resolver las ecuaciones $a^2+5b^2 = 2$ y $a^2+5b^2 = 3$ en $\mathbb{Z}$.

5. Productos de anillos y teorema chino del residuo

DEFINICIÓN 22. *Sea $\{R_i\}_{i\in I}$ una familia de anillos. El producto de estos es el producto cartesiano de los anillos como conjuntos, es $\prod_{i\in I} R_i$ y se le brinda estructura de anillo de la siguiente forma.*

Para $\varphi, \psi \in \prod_{i\in I} R_i$,

$$(\varphi+\psi)(i) = \varphi(i)+\psi(i)\ \forall i \in I$$
$$(\varphi\psi)(i) = \varphi(i)\psi(i)\ \forall i \in I$$
$$1(i) = 1\ \forall i \in I$$
$$0(i) = 0\ \forall i \in I$$

PROPOSICIÓN 34. *(Tarea) Sea $\{R_i\}_{i\in I}$ una familia de anillos. Entonces $\prod_{i\in I} R_i$ es un anillo con las operaciones descritas anteriormente.*

DEFINICIÓN 23. *Sea $\{R_i\}_{i\in I}$ una familia de anillos. Para $j \in I$, definimos $p_j : \prod_{i\in I} R_i \to R_j$ dado por $p_j(\varphi) = \varphi(j)$, $\forall \varphi \in \prod_{i\in I} R_i$*

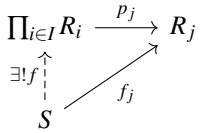
PROPOSICIÓN 35. *Sea $\{R_i\}_{i\in I}$ una familia de anillos. Entonces $p_j : \prod_{i\in I} R_i \to R_j$ es un morfismo de anillos para toda $j \in I$.*

DEMOSTRACIÓN. Sean $\varphi, \psi \in \prod_{i\in I} R_i$, entonces

$$p_j(\varphi+\psi) = (\varphi+\psi)(j) = \varphi(j)+\psi(j) = p_j(\varphi)+p_j(\psi)$$
$$p_j(\varphi\psi) = (\varphi\psi)(j) = \varphi(j)\psi(j) = p_j(\varphi)p_j(\psi)$$
$$p_j(1) = 1(j) = 1$$

□

PROPOSICIÓN 36. *Sea $\{R_i\}_{i\in I}$ una familia de anillos y S un anillo.*
Si $\{f_i : S \to R_i\}$ es una familia de morfismos de anillos, entonces existe un único morfismo de anillos $f : S \to \prod_{i\in I} R_i$ tal que $p_j \circ f = f_j$ para toda $j \in I$, esto es, el siguiente diagrama conmuta:



DEMOSTRACIÓN. Definimos $f : S \to \prod_{i\in I} R_i$ como $f(s)(i) = f_i(s)$ para toda $i \in I$, primero hay que ver que f es un morfismo de anillos,
Sean $s,t \in S$

$$f(s+t)(i) = f_i(s+t) = f_i(s)+f_i(t) = f(s)(i)+f(t)(i)$$
$$f(st)(i) = f_i(st) = f_i(s)f_i(t) = f(s)(i)f(t)(i)$$
$$f(1)(i) = f_i(1) = 1$$

Para toda $i \in I$, por lo que

$$f(s+t) = f(s)+f(t)$$
$$f(st) = f(s)f(t)$$
$$f(1) = 1$$

Por lo tanto f es un morfismo de anillos. Por otro lado $p_i \circ f(s) = f(s)(i) = f_i(s)$ se sigue que $p_i \circ f = f_i$.
Por ultimo veamos que f es único.
Si $g : S \to \prod_{i\in I} R_i$ es un morfismo de anillos tal que $p_i \circ g = f_i$. Sean $i \in I$ y $s \in S$, entonces

$$g(s)(i) = p_i(g(s)) = f_i(s) = f(s)(i)$$

entonces

$$g(s) = f(s)$$

y por lo tanto $f = g$. □

PROPOSICIÓN 37. *Sea R un anillo y $\{I_i\}_{i\in I}$ una familia de ideales de R. Consideramos el morfismo $f : R \to \prod_{i\in I} R/I_i$ inducido por las proyecciones canónicas $\pi_j : R \to R/I_j$. Notamos que $nuc(f) = \bigcap_{i\in I} I_i$.*

DEMOSTRACIÓN. Sea $x \in nuc(f)$. Entonces $f(x) = 0$. Pero esto significa que $0 = f(x)(i) = \pi_i(x) = x + I_i$ y esto pasa si y solo si $x \in I_i$, $\forall i \in I$, es decir $x \in \bigcap_{i\in I} I_i$.

Si $x \in \bigcap_{i\in I} I_i$, entonces $x + I_i = 0$ para toda $i \in I$, entonces $\pi_i(x) = 0$ para toda $i \in I$, entonces $f(x) = 0$ es decir $x \in nuc(f)$. □

COROLARIO 3. *f es inyectivo si y sólo si $\bigcap_{i\in I} I_i = 0$.*

DEFINICIÓN 24. *Sea R un anillo e $I, J \leq R$. Decimos que I y J son coprimos, si $I + J = R$*

PROPOSICIÓN 38. *Sea R un anillo e $I_1, ..., I_n \leq R$. Si $I_i + I_j = R \; \forall i \neq j$ entonces*

$$\prod_{i=1}^{n} I_i = \bigcap_{i=1}^{n} I_i$$

DEMOSTRACIÓN. Por inducción sobre n.

Para $n = 2$, sea $x \in I_1 \cap I_2$ y por hipótesis existen $x_1 \in I_1$ y $x_2 \in I_2$ tales que $x_1 + x_2 = 1$ entonces $x = 1 \cdot x = (x_1 + x_2) \cdot x = x_1x + x_2x$ notemos que $x_1x \in I_1I_2$ y $x_2x \in I_2I_1$ por lo que $x \in I_1I_2$.

Suponemos valido para n y ponemos $J = \prod_{i=1}^{n} I_i = \bigcap_{i=1}^{n} I_i$ por hipótesis de inducción.

Por hipótesis tenemos que $I_i + I_{n+1} = R$ entonces existe $x_x \in I_i$ y $y_i \in I_{n+1}$ tales que $x_i + y_i = 1$ para $i = 1, ..., n$ por lo que $1 - y_i = x_i \in I_i$ para $i = 1, ..., n$.

De aqui

$$\prod_{i=1}^{n} x_i = \prod_{i=1}^{n} (1 - y_i)$$

Notemos que

$$\prod_{i=1}^{n} (1 - y_i) + I_{n+1} = 1 + I_{n+1}$$

por lo que

$$\prod_{i=1}^{n} x_i + I_{n+1} = 1 + I_{n+1}$$

de donde $\prod_{i=1}^{n} x_i - 1 \in I_{n+1}$, de aquí existe $-y \in I_{n+1}$, $\prod_{i=1}^{n} x_i - 1 = -y$ así $\prod_{i=1}^{n} x_i + y = 1$.

Regresamos a $n = 2$ □

PROPOSICIÓN 39. *Sea R un anillo e $\{I_\alpha\}_{\alpha=1}^n$ una familia de ideales de R. Entonces $f: R \to \prod_{\alpha=1}^n R/I_\alpha$ es suprayectivo si y sólo si $I_\alpha + I_\beta = R \; \forall \alpha \neq \beta$.*

DEMOSTRACIÓN. $\Rightarrow$

Como f es supra existe $x \in R$ tal que $f(x) = \delta_{1i}$. Por lo que $x + I_1 = 1 + I_1$, y $x + I_2 = I_2$. De aquí $1 = (1-x) + x \in I_1 + I_2$, sin perdida de generalidad, esto aplica para cualquier $\alpha, \beta = 1, .., n$ con $\alpha \neq \beta$.

$\Leftarrow$

Como $I_1 + I_J = R$ entonces existen $x_j \in I_1$, $y_j \in I_j$ con $j = 2, .., n$ tales que $x_j + y_j = 1$. Ponemos $X = \prod_{i=2}^n$ tenemos $x = \prod_{i=2}^n (1 - x_j)$.

Por lo que $x + I_1 = 1 + I_1$ y $x_j + I_j = I_j$ para $j = 2, ..., n$. Por lo tanto $f(x) = \delta_{1i}$. De aqui podemos encontrar a todas las deltas de Kronecker. Notando el hecho de que $f(rx) = r\delta_{1i}$ y usando que f es un morfismo de anillos, concluimos que f es suprayecitvo. □

6. Ejercicios del capítulo

En esta tarea R denotará un anillo, A, B anillos conmutativos y k un campo. Recuerde que los anillos considerados siempre son unitarios.

EJERCICIO 1. *Demuestre que para cualquier $x \in R$, $x0 = 0 = 0x$.*

EJERCICIO 2. *Demuestre que el anillo de matrices $M_n(k)$ es no conmutativo si y sólo si $n \geq 2$.*

EJERCICIO 3. *Demuestre que si G es un subgrupo finito de k^*, entonces G es un grupo cíclico.*

EJERCICIO 4. *Sea $n \in \mathbb{N}^+$. Demuestre que son equivalentes:*

1. *$\mathbb{Z}_n$ es un dominio entero*
2. *$\mathbb{Z}_n$ es un campo*
3. *n es primo*

EJERCICIO 5. *Encontrar todos los $n \in \mathbb{N}^+$ tales que en $\mathbb{Z}_n$, todo divisor de cero sea nilpotente.*

EJERCICIO 6. *Demuestre que ningún polinomio mónico $f \in A[x]$, puede ser divisor de cero.*

EJERCICIO 7. *Demuestre que si $u \in U(A)$ y $x \in A$ es nilpotente, entonces $u+x \in U(A)$.*

EJERCICIO 8.

1. *Sean A un dominio entero y $k \subseteq A$ un campo tales que A es un espacio vectorial sobre k de dimensión finita. Demuestra que A es un campo.*
2. *Usar el inciso anterior para demostrar que todo dominio entero finito es un campo.*

EJERCICIO 9. *Dar una caracterización de todos los subanillos de $\mathbb{Q}$.*

EJERCICIO 10.

1. *¿Qué relación tienen los subanillos $\mathbb{Z}[\sqrt{2}]+\mathbb{Z}[\sqrt{3}], \mathbb{Z}[\sqrt{2}+\sqrt{3}] \subseteq \mathbb{Q}$?*
2. *¿Qué relación tienen los subanillos $\mathbb{Q}[\sqrt{2}]+\mathbb{Q}[\sqrt{3}], \mathbb{Q}[\sqrt{2}+\sqrt{3}] \subseteq \mathbb{R}$?*

EJERCICIO 11. *Considere $\mathbb{Q}(\sqrt{2}) = \{q_1+q_2\sqrt{2} \mid q_1, q_2 \in \mathbb{Q}\}$ y $\mathbb{Q}(\sqrt{3}) = \{q_1+q_2\sqrt{2} \mid q_1, q_2 \in \mathbb{Q}\}$. Demuestre lo siguiente:*

1. *$\mathbb{Q}(\sqrt{2}), \mathbb{Q}(\sqrt{3}) \subseteq \mathbb{C}$ son campos con las operaciones inducidas por $\mathbb{C}$.*
2. *$\mathbb{Q}(\sqrt{2})$ y $\mathbb{Q}(\sqrt{3})$ son isomorfos como $\mathbb{Q}$-espacios vectoriales, pero no lo son como campos.*[4]

EJERCICIO 12. *Suponga que $S \subseteq A$ es un subanillo. Demuestre lo siguiente:*

[4]La definición de isomorfismo de campos es exactamente la misma que la de como anillos, es decir, dos campos son isomorfos si lo son como anillos. Observe que esta definición es parecida a lo que sucede con el caso de grupos y grupos abelianos.

1. *La inclusión $\iota : S \to A$ es un morfismo de anillos.*
2. *$S[x]$ es subanillo de $A[x]$*

EJERCICIO 13. *Sea $X \subseteq R$ con R conmutativo. Demuestre que $S_R(X) = \{f(x_1, \ldots x_n) : f \in \mathbb{Z}[y_1, \ldots y_n], n \in \mathbb{N}^+\}$*

DEFINICIÓN 25. *Un elemento $e \in R$ es **idempotente** si $e^2 = e$.*

EJERCICIO 14. *Sea $e \in R$ un idempotente no trivial. Demuestre que los conjuntos Re, eR, eRe son anillos con las operaciones heredadas de las de R, sin embargo no son subanillos de este.*

EJERCICIO 15. *Demuestre las siguientes afirmaciones:*

1. *En un dominio entero los únicos elementos idempotentes son 0 y 1.*
2. *Demuestre que el anillo de funciones continuas en el intervalo $[a,b]$ es un anillo que tiene como únicos idempotentes al 0 y 1, sin embargo, este no es un dominio entero.*

DEFINICIÓN 26. *Sean $I, J \leq A$. Defina el producto de dichos ideales, el que se va a denotar por IJ, como el ideal generado por el conjunto $\{xy \mid x \in I, y \in J\}$. Observe que esto permite definir I^n para $n \in \mathbb{N}^+$.*

EJERCICIO 16. *Sean $I, J \leq A$ ideales coprimos. Demuestre que para cualquier $n \in \mathbb{N}^+$, I^n y J^n son coprimos.*

EJERCICIO 17. *Sean $n, m \in \mathbb{Z}^*$. Demuestre lo siguiente:*

1. $n\mathbb{Z} \cap m\mathbb{Z} = [n,m]\mathbb{Z}$
2. $n\mathbb{Z} + m\mathbb{Z} = (n,m)\mathbb{Z}$
3. $n\mathbb{Z} \cdot m\mathbb{Z} = nm\mathbb{Z}$.

EJERCICIO 18. *Sean $I,J,K \leq A$. Decir si las siguientes afirmaciones son verdaderas ó falsas dando una demostración o contrajemplo según sea el caso:*

1. $I(J+K) = IJ + IK$
2. *(Ley distributiva)* $I \cap (J+K) = (I \cap J) + (I \cap K)$
3. *(Ley modular) Si* $J \subseteq I$ *o* $K \subseteq I$*, entonces* $I \cap (J+K) = (I \cap J) + (I \cap K)$.

EJERCICIO 19. *Sea $J \leq M_n(A)$ un ideal bilateral. Demuestre que existe $I \leq A$ tal que $J = M_n(I)$*

EJERCICIO 20.

1. *Dar ejemplos de funciones entre dos anillos que satisfagan dos de las condiciones de la definición de morfismo de anillos, pero no la tercera.*[5]
2. *Sea $f : R \to A$ una función que satisface las primeras dos condiciones en la definición de morfismo de anillos y suponga que A es un dominio entero. Demuestre que f tiene que ser un morfismo de anillos.*

EJERCICIO 21. *Sea X un conjunto.*

1. *Demuestre que el conjunto de funciones de X en R, R^X, tiene estructura de anillo al definir las operaciones de forma puntual.*
2. *Considere el anillo conjunto potencia $(\wp(X), \triangle, \cap)$. Demuestre que este anillo es isomorfo a $\mathbb{Z}_2^X$.*

EJERCICIO 22. *Demuestre que $I \subseteq A$ es ideal si y sólo si existe un morfismo de anillos $f : A \to B$ tal que $I = nuc(f)$.*

EJERCICIO 23. *Demuestre lo siguiente:*

1. *$f \in C_0([a,b])$ es unidad si y sólo si $0 \notin im(f)$*

[5]En términos lógicos este ejercicio dice que las propiedades que dan la definición de morfismo de anillos son independientes.

2. *Para todo $x \in [a,b]$, el conjunto $\mathfrak{m}_x := \{f \in C_0([a,b]) \mid f(x) = 0\}$, es un ideal de $C_0([a,b])$. ¿Determinar el cociente $C_0([a,b])/\mathfrak{m}_x$?*

EJERCICIO 24. *Demuestre que son equivalentes para A no trivial:*

1. *A es un campo*
2. *Todo morfismo de anillos no trivial $f : A \to B$, es inyectivo.*

EJERCICIO 25. *Demuestre que* $car(A) = \min\{k \in \mathbb{N}^+ \ : \ \forall x \in A(kx = 0)\} = \min\{k \in \mathbb{N}^+ \ : \ k1_A = 0\}$.

EJERCICIO 26. *Sea $f : A \to B$ un morfismo de anillos biyectivo. Demuestre que $f^{-1} : B \to A$ es un morfismo de anillos.*

EJERCICIO 27. *Si $f : A \to B$ es un morfismo de anillos e $I \leq B$, demuestre que $f^{-1}(I) \leq A$. Además, dar un ejemplo que muestre que en general la imagen directa de un ideal mediante un morfismo de anillos no es necesariamente un ideal.*

EJERCICIO 28. *Sean $f : A \to B$ un morfismo de anillos, $I \leq A$ y $J \leq B$. Demuestre que:*

1. *$I \subseteq (I^f)_f$ y $(J_f)^f \subseteq J$. Dar un ejemplo donde estas contenciones sean propias.*
2. *$J_f = ((J_f)^f)_f$ y $I^f = ((I^f)_f)^f$*
3. *Existe una correspondencia biyectiva entre los conjuntos $\{I^f \mid I \leq A\}$ y $\{J^f \mid J \leq B\}$.*

DEFINICIÓN 27. *Para $I,J \leq A$, se define el ideal cociente de estos como $(I : J) = \{x \in A \mid xJ \subseteq I\}$. El anulador de I se define por $Ann(I) := (0 : I)$.*

EJERCICIO 29. *Sean $I,J,K \leq A$. Demuestre lo siguiente:*

1. *$(I : J)$ es en efecto un ideal.*
2. *$((I : J) : K) = (I : JK)$*

3. *Si* $\{I_\alpha\}_{\alpha\in\Lambda}$ *es una familia de ideales, entonces* $(\bigcap_{\alpha\in\Lambda} I_\alpha : J) = \bigcap_{\alpha\in\Lambda}(I_\alpha : J)$.
4. *Si* $\{I_\alpha\}_{\alpha\in\Lambda}$ *es una familia de ideales, entonces* $(J : \sum_{\alpha\in\Lambda} I_\alpha) = \bigcap_{\alpha\in\Lambda}(J : I_\alpha)$
5. *Determine explícitamente los elementos de* $\bigcup_{x\in A^*} Ann(\langle x\rangle)$.

EJERCICIO 30. *Sea* $f : A \to B$ *un morfismo de anillos.* $I,J \leq A$ *y* $K,L \leq B$. *Demuestre las siguientes afirmaciones:*

1. $(I+J)^f = I^f + J^f$, $K_f + L_f \subseteq (K+L)_f$
2. $(I\cap J)^f \subseteq I^f \cap J^f$, $(K\cap L)_f = K_f \cap L_f$
3. $(IJ)^f = I^f J^f$, $K_f L_f \subseteq (KL)_f$
4. $(I : J)^f \subseteq (I^f : J^f)$, $(K : L)_f \subseteq (K_f : L_f)$

EJERCICIO 31. *(Segundo teorema de isomorfismo para anillos conmutativos) Sean A un anillo,* $S \subseteq A$ *un subanillo e* $I \leq A$ *un ideal bilateral. Demuestre que* $S+I \subseteq A$ *es un subanillo,* $S\cap I \leq A$ *y* $(S+I)/I \cong S/(S\cap I)$.

EJERCICIO 32. *(Tercer teorema de isomorfismo para anillos conmutativos) Sean* $I,J \leq A$ *tales que* $I \subseteq J$. *Demuestre que* $J/I \leq A/I$ *y* $(A/I)/(J/I) \cong A/J$.

EJERCICIO 33. *Demuestre el teorema de la correspondencia biyectiva: Dado* $I \leq A$, *existe un isomorfismo entre la retícula de ideales de* A/I *y la retícula de ideales de A que contienen a I.*

EJERCICIO 34. *Supóngase que A es un dominio entero con más de dos elementos y* $f : A \to A$ *es un automorfismo de anillos (morfismo biyectivo de A en sí mismo). Demuestre lo siguiente:*

1. $x \in U(A)$ *si y sólo si* $f(x) \in U(A)$
2. $x \in A$ *es irreducible si y sólo si* $f(x) \in A$ *es irreducible.*
3. $x \in A$ *es primo si y sólo si* $f(x) \in A$ *es primo.*

DEFINICIÓN 28. *Supóngase que A es un dominio entero y sean $x, y \in A$. Decimos que x es* ***asociado*** *a y, si existe $u \in U(A)$ tales que $x = uy$.*

EJERCICIO 35. *Demuestre las siguientes afirmaciones para A un dominio entero.*

1. *La relación de ser asociados es de equivalencia.*
2. *Para $x, y \in A$ son equivalentes:*
   - *x es asociado a y*
   - *$x|y$ y $y|x$*
   - *$\langle x \rangle = \langle y \rangle$.*
3. *Determine explícitamente todos los elementos asociados a un elemento arbitrarío de $\mathbb{Z}[i]$.*

EJERCICIO 36. *Sea A un dominio entero.*

1. *Demuestre que todo elemento primo es irreducible. Dar un ejemplo donde se muestre que estos conceptos pueden no coincidir.*
2. *Demuestre que si $x \in A$ es irreducible, entonces todo elemento asociado a x es irreducible. ¿Sucede esto para los elementos asociados a un elemento primo?*
3. *Sea $x \in R$. Demuestre que x es irreducible si y sólo si el ideal $\langle x \rangle$ es máximo en el conjunto de ideales principales de A.*

EJERCICIO 37.

1. *Demuestre que para cualesquiera $a, b \in \mathbb{Z}$ con $b \neq 0$, existen $q, r \in \mathbb{Z}$ tales que $a = bq + r$ con $0 \leq |r| < \frac{1}{2}|b|$.*
2. *Demuestre que si $\alpha, \beta \in \mathbb{Z}[i]^*$ y $\alpha|\beta$, entonces $\delta(\alpha) \leq \delta(\beta)$, donde δ es la función euclidiana de $\mathbb{Z}[i]$.*
3. *Usar el inciso 1 para demostrar que para cualesquiera $\alpha, \beta \in \mathbb{Z}[i]$, con $\beta \neq 0$, existen $\gamma, \rho \in \mathbb{Z}[i]^*$ tales que $\alpha = \beta\gamma + \rho$.*

EJERCICIO 38. *Sea (A, δ) un Dominio Euclidiano. Demuestre que son equivalentes:*

1. *$x \in U(A)$*

2. $\delta(x) = \delta(1)$
3. $x \neq 0$ *y para todo* $y \in A$, $\delta(x) \leq \delta(y)$.

EJERCICIO 39. *Demuestre que el anillo* $\{a + b\frac{1+\sqrt{-19}}{2} \mid a,b \in \mathbb{Z}\}$ *es un DIP que no es DE.*

EJERCICIO 40. *Considere* $A = \mathbb{Z}[x]$ *y* $p \in \mathbb{N}$ *un primo, así como el conjunto* $I = \{f \in \mathbb{Z}[x] :$ *p divide todos los coeficientes de* $f\}$.

1. *Demuestre que* $I \leq A$.
2. *Probar que* A/I *es un DIP.*

EJERCICIO 41. *Sea* $p \in \mathbb{N}$ *un primo y considere* $A = \{\frac{a}{b} \in \mathbb{Q} \mid p \nmid b\} \subseteq \mathbb{Q}$.

1. *Caracterizar los elementos de* $U(A)$.
2. *Demuestre que A es un DIP.*

EJERCICIO 42. *Demuestre que en un DIP todo elemento irreducible es primo.*

EJERCICIO 43. *Demuestre que si A es un DFU, entonces* $A[x]$ *es un DFU.*

EJERCICIO 44. *Demuestre que* $\mathbb{Z}[\sqrt{10}]$ *es un dominio entero que no es un DFU.*

EJERCICIO 45. *Sea* $\{R_\alpha\}_{\alpha\in\Lambda}$ *una familia de anillos. Demuestre que* $\prod_{\alpha\in\Lambda} R_\alpha$ *es un anillo con las operaciones definidas de forma puntual.*

EJERCICIO 46. *Para k un campo, sea* $A = k[x,y]/\langle xy\rangle$. *Demuestre lo siguiente:*

1. *Todo elemento en A tiene una única descomposición de la forma* $a + xf(x) + yg(y)$, *con* $a \in k$, $f(x) \in k[x]$ *y* $g(y) \in k[y]$.
2. *A se encaja como subanillo de* $k[x] \times k[y]$.

DEFINICIÓN 29. *Sea $\{I_\alpha\}_{\alpha\in\Lambda}$ una familia de ideales en A. Decimos que A es suma directa de dicha familia, lo que se denota por $A = \bigoplus_{\alpha\in\Lambda} I_\alpha$, si:*

1. $\sum_{\alpha\in\Lambda} I_\alpha = A$
2. *Para cualquier $\beta \in \Lambda$, $I_\beta \cap (\sum_{\alpha\in\Lambda,\alpha\neq\beta} I_\alpha) = 0$.*

EJERCICIO 47. *Sea $\{I_\alpha\}_{\alpha\in\Lambda}$ una familia de ideales. Demuestre que si $A = \bigoplus_{\alpha\in\Lambda} I_\alpha$, entonces existe $\Gamma \subseteq \Lambda$ finito tal que $A = \bigoplus_{\alpha\in\Gamma} I_\alpha$.*

DEFINICIÓN 30.

1. *Sea $E \subseteq A$ un subconjunto donde todos los elementos son idempotentes. Decimos que E es ortogonal si para cualesquiera $e, f \in E$, $ef = 0$. Dos elementos idempotentes $e, f \in A$ son ortogonales si el conjunto $\{e, f\}$ lo es.*
2. *Un elemento $e \in A$ idempotente no cero es primitivo si siempre que $e = e_1 + e_2$ con $e_1, e_2 \in A$ idempotentes ortogonales, se tiene que $e_1 = 0$ ó $e_2 = 0$.*
3. *Un conjunto finito de idempotentes $\{e_1, ..., e_n\}$ se llama completo si $\sum_{i=1}^n e_i = 1$.*

EJERCICIO 48. *Sean $I_1, ..., I_n \leq A$. Demuestre que $A = \bigoplus_{i=1}^n I_i$ si y sólo si existe una familia de idempotentes ortogonal, $\{e_1, ..., e_n\} \subseteq A$, tal que para cualquier $i \in \{1, ..., n\}$, $I_i = \langle e_i \rangle$.*

DEFINICIÓN 31. *Un ideal $I \leq A$ es un **sumando directo** de A si existe un ideal J tal que $A = I \oplus J$. Un ideal I de A es **inescindible** si siempre que $I = J \oplus K$ con J, K ideales de A, se tiene que $J = 0$ o $K = 0$.*

EJERCICIO 49. *Sea $I = Ae \leq A$ un sumando directo de A con $e \in A$ idempotente. Demuestre que I es inescindible si y sólo si e es primitivo.*

EJERCICIO 50. *Demuestre las siguientes afirmaciones.*

1. *Un anillo A se descompone como suma directa de una familia de ideales si y sólo si existe un conjunto completo, ortogonal y finito de idempotentes primitivos de A.*
2. *Para un anillo A son equivalentes:*

- *A es inescindible*
- 1 *es idempotente primitivo*
- 0 *y* 1 *son los únicos idempotentes de A*

DEFINICIÓN 32. *Sea k un campo. Un* ***valor absoluto*** *sobre k es una función* $|\_| : k \to \mathbb{R}^+ \cup \{0\}$ *que satisface las siguientes propiedades:*

1. *Para todo* $x \in k$, $|x| = 0$ *si y sólo si* $x = 0$.
2. *Para cualesquiera* $x, y \in k$, $|xy| = |x||y|$.
3. *Para cualesquiera* $x, y \in k$, $|x+y| \leq |x| + |y|$.

Un valor absoluto sobre un campo k es ***no arquimediano*** *si satisface que para cualesquiera* $x, y \in k$, $|x+y| \leq \text{máx}\{|x|, |y|\}$.

EJERCICIO 51. *Sea k un campo con un valor absoluto no arquimediano* $|\_|$. *Demuestre lo siguiente:*

1. $\overline{B}_1(0) := \{x \in k \ : \ |x| \leq 1\}$ *es un subanillo de k.*
2. $B_1(0) := \{x \in k \ : \ |x| < 1\}$ *es un ideal de* $\overline{B}_1(0)$.

EJERCICIO 52. *Sea* $p \in \mathbb{N}$ *un primo. Nótese que para cualquier* $x \in \mathbb{Q}^*$, *existen únicos* $k, n, m \in \mathbb{Z}$ *tales que* $x = p^k \frac{n}{m}$ *con* $(n, p) = (m, p) = (n, m) = 1$. *En dicha descomposición, decimos que k es la* ***valuación p-ádica*** *de x y esta se denota por* $v_p(x)$.

Así, defina una función $|\_|_p : \mathbb{Q} \to \mathbb{R}$ *mediante la regla de correspondencia:*

$$|x|_p := \begin{cases} 0 & Si\ x = 0 \\ p^{-v_p(x)} & Si\ x \neq 0 \end{cases}$$

1. *Demuestre que la función* $|\_|_p$ *define un valor absoluto no arquimediano en* $\mathbb{Q}$.
2. *Determinar explícitamente al cociente* $\overline{B}_1(0)/B_1(0)$.

EJERCICIO 53. *Sea k un campo finito. Demuestre lo siguiente:*

1. *Existen* $p, n \in \mathbb{N}$ *con p primo, tales que* $|k| = p^n$.

2. *La función* $|\_|_t : k \to \mathbb{R}^+ \cup \{0\}$ *definida por la regla de corrrespondencia*

$$|x|_t = \begin{cases} 0 & Si\ x = 0 \\ 1 & Si\ x \neq 0 \end{cases}$$

es un valor absoluto en k, al cual se le conoce como el valor absoluto trivial. Más aún, bajo la hipótesis de k finito, el único valor absoluto definido en k es el trivial.

EJERCICIO 54. *Para k un campo, sean* $f \in k[x_1,...,x_n]$ *no cero e* $I := \langle f \rangle$. *Defina* $A := k[x_1,...,x_n]/I$. *Demuestre lo siguiente:*

1. f *tiene factores múltiples si y sólo si A tiene divisores de cero.*
2. f *se factoriza como producto de dos polinomios si y sólo si A tiene divisores de cero no nilpotentes.*

DEFINICIÓN 33. *Un ideal* $I \leq R$ *es* ***finitamente generado*** *si existen* $x_1,...,x_n \in R$ *tales que* $I = \langle x_1,...,x_n \rangle$.

EJERCICIO 55. *Sea* $A[[x]]$ *el anillo de series formales de potencias con coeficientes en A.*

1. *Demuestre que* $A[x] \subseteq A[[x]]$ *es un subanillo.*
2. *Defina la función orden,* $ord : A[[x]] \to \mathbb{N}$, *cuya regla de correspondencia es* $ord(f) = \min\{n \in \mathbb{N} \mid a_n \neq 0\}$. *Demuestre que si A es un dominio entero, entonces* $ord(fg) = ord(f) + ord(g)$.
3. *Demuestre que si A es un dominio entero, entonces* $A[x]$ *y* $A[[x]]$ *son dominios enteros.*

EJERCICIO 56. *Demuestre lo siguientes:*

1. *Si* $I \leq A$, *entonces* $I[x] \leq A[x]$ *y* $I[[x]] \leq A[[x]]$. *Más aún,* $A[x]/I[x] \cong (A/I)[x]$ *y* $A[[x]]/I[[x]] \cong (A/I)[[x]]$.
2. *Demuestre que si* $I \leq A$, *entonces* $I \cdot A[x] = I[x]$.
3. *Demuestre que si* $I \leq A$ *es finitamente generado, entonces* $I \cdot A[[x]] = I[[x]]$. *¿Qué sucede con esta afirmación si I no es finitamente generado?*

DEFINICIÓN 34. *Un anillo R es de* ***Boole*** *si todos sus elementos son idempotentes.*

EJERCICIO 57. *Supóngase que R es un anillo de Boole. Demuestre lo siguiente:*

1. *Para cualquier $x \in R$, $2x = 0$.*
2. *R es un anillo conmutativo.*
3. *Todo ideal de R finitamente generado es principal.*

DEFINICIÓN 35. *Un anillo A es* ***ordenado*** *si existe un orden total en A, $\leq$, tal que:*

1. *Para cualesquiera $x, y \in A$ tales que $x \leq y$, se cumple que $x + z \leq y + z$, para cualquier $z \in A$.*
2. *Si $x, y \in A$ son tales que $x < y$, entonces para todo $z \geq 0$, $xz \leq yz$.*

Un campo que cumple los axiomas de anillo ordenado se llama ***campo ordenado****. Un campo es* ***real*** *si -1 no es suma de cuadrados.*

EJERCICIO 58. *Sea k un campo. Demuestre lo siguiente:*

1. *Si k es ordenado, entonces su característica es 0. ¿Es cierta la afirmación recíproca?*
2. *k es ordenado si y sólo si es real.*
3. *Sea k un campo real y $x \in k$. Entonces, existe un orden $\leq$ en k tal que $x < 0$ si y sólo si x no se expresa como suma de cuadrados.*

Ejercicios extra

Estos ejercicios pretenden explorar un poco de la teoría general de anillos quitando las hipótesis de conmutatividad e incluso el uno del anillo. Otros de estos ejercicios requieren manejar nociones básicas de análisis real o topología.

EJERCICIO 59. *Sea $x \in R$. Demuestre que si x tiene un único inverso derecho, entonces x es una unidad.*

EJERCICIO 60. *Demuestre que si $x \in R$ tiene más de un inverso derecho, entonces tiene una infinidad.*

EJERCICIO 61. *(Teorema pequeño de Weddenburn) Demuestre que si R es un anillo con división finito, entonces R es un campo.*

EJERCICIO 62. *Considere $\mathbb{Q}$ como subespacio métrico de $\mathbb{R}$, donde $\mathbb{R}$ tiene la métrica usual.*

1. *Para cualquier conjunto abierto-cerrado de $\mathbb{Q}$, construir un elemento idempotente en $C_0(\mathbb{Q})$. Usar esto para demostrar que la cardinalidad de los idempotentes en dicho anillo es $2^{\aleph_0}$*
2. *Sean $U_1,...,U_n$ una colección de abiertos-cerrados en $\mathbb{Q}$. Demuestre que $\{\chi_{U_1},...,\chi_{U_n}\}$ es un conjunto ortogonal completo en $C_0(\mathbb{Q})$ si y sólo si $\{\chi_{U_1},...,\chi_{U_n}\}$ es una partición de $\mathbb{Q}$.*

EJERCICIO 63. *Demuestre lo siguiente:*

1. *$C_0([0,1])$ es inescindible.*
2. *$C_0(\mathbb{Q})$ no tiene sumandos directos inescindibles*

DEFINICIÓN 36. *Un anillo R se llama regular (von Neumann) si para todo $a \in R$, existe $x \in R$ tal que $axa = a$.*

EJERCICIO 64. *Sea R un anillo regular. Demuestre lo siguiente:*

1. *R no tiene divisores de cero.*
2. *Si para $a,x \in R$ se cumple que $axa = a$, entonces $xax = x$*
3. *Supóngase que no se pide que R sea unitario. Demestre que R tiene que un uno.*
4. *R es un anillo con división.*

EJERCICIO 65. *Sea R un anillo. Demuestre que son equivalentes:*

1. *R es regular*
2. *Todo ideal principal izquierdo (derecho) de R es generado por un elemento idempotente.*

3. *Todo ideal izquierdo (derecho) finitamente generado de R es generado por un iempotente.*

EJERCICIO 66. *Demuestre que el anillo de enteros de Eisenstein, $\mathbb{Z}[\omega]$, con $\omega = e^{\frac{2\pi i}{3}} \in \mathbb{C}$, es un DFU.*

DEFINICIÓN 37.

1. *El centro de R se define como el conjunto, $Z(R) := \{x \in R \mid \forall y \in R(xy = yx)\}$.*
2. *Un número natural $n > 1$ es una potencia de R si para todo $x \in R$, $x^n = x$. El conjunto de potencias de R se denota por $P(R)$ y si este es no vacío, se dice que al anillo R tiene potencia.*

EJERCICIO 67. *Sea R un anillo con potencia. Demuestre lo siguiente:*

1. *Si $x, y \in R$ tales que $xy = 0$, entonces $yx = 0$.*
2. *El conjunto de elementos nilpotentes de R está contenido en el centro.*
3. *Si $n \in P(R)$, entonces $x^{n-1} \in R$ es idempotente.*
4. *Si $m = q(n-1) + r$ con $q \geq 0$ y $0 < r < n-1$, entonces $x^m = x^r$.*

EJERCICIO 68. *Demuestre las siguientes afirmaciones:*

1. *Si $3 \in P(R)$, entonces R es conmutativo.*
2. *Si un número par no cero es elemento de $P(R)$, entonces $car(R) = 2$.*
3. *Si $4 \in P(R)$, entonces R es conmutativo.*

EJERCICIO 69. *Considere $\mathscr{L}_1(\mathbb{R})$ el conjunto de funciones integrables de $\mathbb{R}$ en $\mathbb{R}$. Demuestre que $(\mathscr{L}_1(\mathbb{R}), +, *)$ satisface todos los axiomas de anillo conmutativo excepto la existencia de un uno, donde $+$ se define de forma puntual y $*$ es el producto de convolución.*

EJERCICIO 70. *Considere R un conjunto que satisface todos los axiomas de anillo excepto la existencia de un uno. Considere $\overline{R} = R \times \mathbb{Z}$ y defina las operaciones $+, \cdot : \overline{R} \times \overline{R} \to \overline{R}$ mediante:*

$$(a,n)+(b,n) := (a+b,n+m)$$
$$(a,n)\cdot(b,m) = (ab+na+mb,nm)$$

Demuestre que $\overline{R}$ es un anillo unitario.

Capítulo 2

Algunas construcciones básicas en el contexto conmutativo

1. Anillos de polinomios

En esta sección se vana estudiar distintas cuestiones en torno a anillos de polinomios, usando principalmente técnicas desarrolladas en el capítulo anterior. Asimismo se puntualizarán algunos resultados respecto a anillos de polinomios con coeficientes en un campo, los cuales serán importantes para los siguientes capítulos. Se recuerda que en este capítulo todos los anillos son conmutativos.

1.1. Propiedad universal. El primer resultado que se requiere puntualizar tiene que ver con una propiedad que caracteriza a los anillos de polinomios, la cual básicamente dice que cuando se quiere definir un morfismo de anillos con dominio un anillo de polinomios, basta con especificar a donde se envían las variables.

PROPOSICIÓN 40. *(Propiedad Universal del Anillo de Polinomios) Sean $f : R \to S$ un morfismo de anillos y $a_1, ..., a_n \in S$. Entonces, existe un único morfismo $\overline{f} : R[x_1, ..., x_n] \to S$ tal que $\overline{f} \circ \iota = f$ y $\overline{f}(x_i) = a_i$, con $\iota : R \to R[x_1, ..., x_n]$ la inclusión canónica. En un diagrama conmutativo:*

$$\begin{array}{ccc} R & \xrightarrow{\iota} & R[x_1, ..., x_n] \\ & \searrow^{f} & \downarrow \overline{f} \\ & & S \end{array}$$

DEMOSTRACIÓN. Para $\sum r_{(k_1,...,k_n)} x_1^{k_1} \cdots x_n^{k_n} \in R[x_1, ..., x_n]$, definir

$$\overline{f}(\sum r_{(k_1,...,k_n)} x_1^{k_1} \cdots x_n^{k_n}) = \sum f(r_{(k_1,...,k_n)}) a_1^{k_1} \cdots a_n^{k_n}$$

.

El hecho de que f sea un morfismo implica que $\overline{f}$ lo es pues las operaciones en $R[x_1, ..., x_n]$ se definen a partir de los coeficientes. Además es claro que $\overline{f}$ es el único morfismo con las propiedades mencionadas. □

Observación:

- Como se ve en la prueba del resultado anterior, escribir polinomios en anillos que tienen muchas variables puede ser muy complicado. Existe una notación conocida como **multi-índices** donde un polinomio en $R[x_1,...,x_n]$ se escribe como $\sum_I r_I x^I$, donde $I \subseteq \mathbb{N}^n$. En esta notación, dado $i = (i_1,...,i_n) \in \mathbb{N}^n$, $x^I := x_1^{i_1} \cdots x_n^{i_n}$. Esto aligera la forma de escribir polinomios.

EJEMPLO 21. *Dado cualquier $r \in R$, existe un morfismo que se conoce como morfismo de evaluación en r, $ev_r : R[x] \to R$, el cual evalúa al cualquier polinomio en r. Observe que este se puede construir directamente de la propiedad universal al considerar dicho elemento y el morfismo identidad, $1_R : R \to R$.*

Un resultado de carácter teórico que se deduce de la propiedad universal del anillo de polinomios, es una caracterización de los monomorfismos en la categoría de anillos conmutativos unitarios, a saber:

COROLARIO 4. *Sea $f : R \to S$ un morfismo de anillos. Entonces, f es un mono si y sólo si f es inyectivo.*

DEMOSTRACIÓN. El regreso es claro. Para la ida suponga que $a, b \in R$ son tales que $f(a) = f(b)$. Con dichos elementos y el morfismo canónico $i : \mathbb{Z} \to R$, la propiedad universal del anillo de polinomios implica que existen morfismos $\overline{a}, \overline{b} : \mathbb{Z}[x] \to R$ tales que $\overline{a}(x) = a$, $\overline{b}(x) = b$, $\overline{a} \circ \imath = i = \overline{b} \circ \imath$.
Las hipótesis aunadas al hecho de que f es morfismo implican que $f \circ \overline{a} = f \circ \overline{b}$, por lo que al usar que f es mono se deduce que $\overline{a} = \overline{b}$ y así, $a = b$ al evaluar en el polinomio x. □

Del resultado anterior podemos recapitular algunos resultados, ya que en este momento se tiene una caracterización de los monos como morfismos inyectivos y morfismos con núcleo 0. Anteriormente se mencionó que el caso de epimorfismos es más delicado y de hecho se mencionó que los morfismos suprayectivos son epimorfismos, pero que hay epimorfismos que no son morfismos suprayectivos. Por desgracia no se va dar una caracterización de los epimorfismos en la categoría de anillos pues esto desviaría la dirección de lo que se busca, pues requiere introducir el concepto de producto tensorial. Por completez, el resultado es que $f : R \to S$ es epi si y sólo si $S \otimes_R S$ se cumple que $r \otimes 1 = 1 \otimes r$, lo que a su vez es equivalente a decir que el morfismo obvio $S \to S \otimes_R S$ sea suprayectivo.

1.2. Unidades. Regresando al estudio general del anillo de polinomios, el siguiente paso a dar tiene que ver con caracterizar elementos especiales en $R[x]$ en término de sus coeficientes.
Para el primer resultado de estos, se requiere introducir un concepto.

DEFINICIÓN 38. *Si R es un anillo (no necesariamente conmutativo), un elemento $x \in R$ se llama nilpotente si existe $n \in \mathbb{N}^+$ tal que $x^n = 0$.*

Con la definición anterior en mente se tiene lo siguiente.

LEMA 3. *El conjunto de elementos nilpotentes de un anillo conmutativo es un ideal.*

DEMOSTRACIÓN. Trivialmente $0 \in R$ es un elemento nilpotente. Por otro lado, si $x, y \in R$ son elementos nilpotentes, existen $n, m \in \mathbb{N}^+$ tales que $x^n = y^m = 0$. Observe que

$$(x-y)^{n+m} = \sum_{i=0}^{n+m} \begin{pmatrix} n+m \\ i \end{pmatrix} x^i y^{n+m-i} = \sum_{i=0}^{n-1} \begin{pmatrix} n+m \\ i \end{pmatrix} x^i y^{n+m-i} + \sum_{i=n}^{n+m} \begin{pmatrix} n+m \\ i \end{pmatrix} x^i y^{n+m-i}$$

Luego, para $i \in \{n, .., n+m\}$, $x^i = 0$, por lo que el segundo sumando en la igualdad anterior es cero. Por otro lado, para $i \in \{0, .., n-1\}$ se tiene que $y^{n+m-i} = 0$, por lo que el primer sumando también en cero. Esto muestra que $(x-y)^{n+m} = 0$ y así, se ha probado que el conjunto de elementos nilpotentes es un subgrupo (aditivo) de R.

Para concluir, si $a \in R$ y $x \in R$ es nilpotente, sea $n \in \mathbb{N}^+$ tal que $x^n = 0$. Luego $(ax)^n = a^n x^n = 0$, así $ax \in R$ es nilpotente. □

El siguiente resultado da una caracterización de las unidades en $R[x]$.

PROPOSICIÓN 41. *Sea $f \in R[x]$ con $f = \sum_{i=0}^{n} a_i x^i$. Entonces $f \in U(R[x])$ si y sólo si $a_0 \in U(R)$ y $a_1, ..., a_n$ son nilpotentes.*

DEMOSTRACIÓN. $\Rightarrow$) Por inducción fuerte sobre n.

Base n=0. No hay nada que probar pues $f = a_0$, que debe ser unidad, y no hay más coeficientes en este polinomio.

Paso inductivo: Supóngase que el resultado es valido para polinomios con grado menor a n. Considere entonces $f^{-1} = \sum_{i=0}^{m} b_i x^i$, el inverso de $f \in R[x]$. Para cualquier $k \in \{0,...,n+m\}$ denote por $c_k = \sum_{j=0}^{k} a_j b_{k-j}$, donde para $i \in \{n+1,...,n+m\}$, $a_i = 0$ y para $i \in \{m+1,...,n+m\}$, $b_i = 0$. Además recuerde que c_k son los coeficientes del producto ff^{-1}, así que de la hipótesis se deduce que $c_0 = 1$ y $c_k = 0$ para $k \in \{1,...,n+m\}$. Más aún, observe que la primera condición implica que $a_0 \in U(R)$.

Afirmación: Para todo $r \in \{1,...,m+1\}$ se tiene que $a_n^r b_{m+1-r} = 0$. La prueba de esto se va a hacer por inducción generalizada en r:
Base r=1. Dado que $c_{n+m} = 0$, entonces $a_n b_m = 0$ y esto prueba la afirmación.
Paso inductivo: Si el resultado vale para $s \in \{1,..,r\}$, considere

$$0 = c_{n+m-r} = \sum_{j=0}^{n+m-r} a_j b_{n+m-r-j}$$

Al multiplicar por a_n^r, esto implica que

$$\begin{aligned}
0 =& a_n^r \left(\sum_{j=0}^{n+m-r} a_j b_{n+m-r-j} \right) \\
=& a_n^r \left(\sum_{j=0}^{n} a_j b_{n+m-r-j} \right) \\
=& a_n^r \left(\sum_{j=0}^{n-1} a_j b_{n+m-r-j} + a_n b_{m-r} \right) \\
=& \sum_{j=0}^{n-1} a_n^r a_j b_{n+m-r-j} + a_n^{r+1} b_{m-r} \\
=& \sum_{j=0}^{n-1} a_n^{r+j+1-n} b_{n+m-r-j} (a_n^{n-j-1} a_j) + a_n^{r+1} b_{m-r}
\end{aligned}$$

Como por hipótesis $a_n^{r+j+1-n} b_{n+m-r-j} = 0$, ambos sumandos son cero y esto prueba la afirmación

Al usar la afirmación, si eso se particulariza para $r = m+1$, se deduce que $a_n^{m+1} b_0 = 0$ y como $b_0 \in U(R)$ esto implica que $a_n^{m+1} = 0$, es decir, a_n es nilpotente. Además, observe que esto implica que $a_n x^n \in R[x]$ es nilpotente y entonces por el lema anterior

$$f - a_n x^n \in U(R[x]).$$

Como $\partial(f - a_n x^n) < n$, entonces de la hipótesis de inducción se concluye que $a_1,..,a_{n-1}$ son nilpotentes y se concluye la prueba.

$\Leftarrow$) Si $a_1,...,a_n \in R$ son nilpotentes, entonces $a_1x,...,a_nx^n \in R[x]$ son nilpotentes, luego por el lema anterior, $\sum_{i=1}^{n} a_ix^i \in R[x]$ es nilpotente. Dado que $a_0 \in U(R)$, entonces $a_0 \in U(R[x])$ y entonces $f = a_0 + \sum_{i=1}^{n} a_ix^i \in U(R[x])$ por un resultado del capítulo 1. □

Observe que el resultado anterior tiene como caso particular el siguiente hecho conocido, el cual se da cuando los coeficientes se toman en un campo, ya que en este caso existe un único elemento nilpotente, a saber el 0.

COROLARIO 5. *Para k un campo, $f \in k[x]$ es unidad si y sólo si f es constante no cero.*

1.3. Elementos nilpotentes. El siguiente resultado caracteriza los elementos nilpotentes en $R[x]$.

PROPOSICIÓN 42. *Sea $f \in R[x]$ con $f = \sum_{i=0}^{n} a_ix^i$. Entonces f es nilpotente si y sólo si $a_0,...,a_n$ son nilpotentes.*

DEMOSTRACIÓN. $\Rightarrow$) Por inducción fuerte sobre n.

Base n=0. No hay nada que probar pues $f = a_0$ y la condición de nilpotencia de f es equivalente a la nilpotencia de a_0.

Paso inductivo. Supóngase que el resultado es valido para polinomios con grado menor a n. Dado que $f^m = 0$, observe que el coeficiente principal de f^m es a_n^m y la igualdad anterior implica que $a_n^m = 0$. Esto implica que $a_nx^n \in R[x]$ es nilpotente y así $f - a_nx^n \in R[x]$ es nilpotente. Como $\partial(f - a_nx^n) < n$, la hipótesis de inducción permite concluir que $a_0,..,a_{n-1}$ son nilpotentes, lo que concluye la prueba

$\Leftarrow$) Para cada $i \in \{0,...,n\}$ se tiene que $a_ix^i \in R[x]$ es nilpotente. El resultado se sigue de que la suma de nilpotentes es nilpotente. □

Observe que al particularizar el resultado anterior a polinomios con coeficientes en un campo, este dice que el único elemento nilpotente en $k[x]$ es el polinomio 0.

1.4. Divisores de cero. El siguiente resultado pretende caracterizar los divisores de cero de $R[x]$.

PROPOSICIÓN 43. *Sea $f \in R[x]$. Entonces f es divisor de cero si y sólo si existe $a \in R^*$ tal que $af = 0$.*

DEMOSTRACIÓN. $\Rightarrow$) Si $f \in R[x]$ es un divisor de cero, existe $g \in R[x]$ tal que $fg = 0$. Además, puede suponerse que g es un polinomio con grado mínimo que satisface dicha condición. Si $f = \sum_{i=0}^{n} a_i x^i$ y $g = \sum_{i=0}^{m} b_i x^i$, se afirma que $b_m f = 0$.
Para probar esto se va a usar inducción fuerte sobre n.

Base n=0. Es obvio pues como $fg = 0$ entonces $a_0 b_i = 0$ para cualquier $i \in \{0, .., m\}$. En particular $0 = a_0 b_m = f b_m$.

Paso inductivo. Supóngase que el resultado es valido para polinomios con grado menor a n. Observe que el hecho de que $fg = 0$ implica que $a_n b_m = 0$. Así, $a_n g \in R[x]$ satisface que $\partial(a_n g) < m$ y además $f(a_n g) = a_n fg = 0$. Por minimalidad de g se concluye que $a_n g = 0$. Considere entonces $f - a_n x^n \in R[x]$, el cual cumple que $\partial(f - a_n x^n) < n$ y $(f - a_n x^n)g = fg - a_n x^n g = 0$. Al usar la hipótesis de inducción se concluye que $b_m(f - a_n x^n) = 0$. Entonces $b_m f = b_m f - b_m a_n x^n = 0$, lo que prueba la afirmación.

$\Leftarrow$) Es claro.

□

En este caso es importante observar que en el caso de coeficientes en un campo, el resultado anterior dice que $k[x]$ no tiene divisores de cero, cosa que ya se sabía pues $k[x]$ es un dominio entero.

1.5. Ideas de irreducibilidad. Para concluir con esta sección se quiere hacer una discusión respecto al concepto de irreducibilidad en $R[x]$. Hacer esto en el contexto general es complicado pero se tienen unos resultados muy generales:

1. Los polinomios de grado 0 son irreducibles
2. Si R es un dominio entero, entonces los polinomios de grado 1 también irreducibles. Esta afirmación no es cierta si se quita dicha hipótesis pues en $\mathbb{Z}_6[x]$, $f = 2x$ no lo es irreducible pues $(3x+1)(2x) = 2x$.

Los mejores resultados son para dominios enteros, sin embargo estos no se pueden dar pues falta teoría, pero a forma de introducción se estudian un poco para el prototipo de anillo conmutativo unitario que es $\mathbb{Z}$. Los resultados generales aparecerán en los ejercicios y se plantearán algunas ideas de estos en las siguientes secciones.

PROPOSICIÓN 44. *Sea $f \in \mathbb{Z}[x]$ con $f = \sum_{i=0}^{n} a_i x^i$. Si f es irreducible, entonces todos los coeficientes de f son primos relativos entre sí.*

DEMOSTRACIÓN. Es claro. □

Observe que sin embargo la afirmación anterior no caracteriza el concepto de irreducibilidad pues el polinomio $f = x^2 + 5x + 6 \in \mathbb{Z}[x]$ satisface que $(1,5,6) = 1$, pero dicho polinomio no es irreducible pues $f = x^2 + 5x + 6 = (x+2)(x+3)$.

La importancia del resultado anterior radica en el hecho de que motiva lo siguiente.

DEFINICIÓN 39. *Decimos que $f \in R[x]$ es primitivo si el ideal generado por sus coeficientes es R.*

Observaciónes:

- Si $f \in \mathbb{Z}[x]$ es irreducible, entonces f es primitivo. El regreso de esta afirmación no es cierto como se vio en el ejemplo previo a la definición.
- $f \in \mathbb{Z}[x]$ es primitivo si y sólo si todos sus coeficientes son primos relativos.

Antes de continuar con el problema que se quiere tratar que es la búsqueda de criterios de irreducibilidad, vale la pena presentar el siguiente resultado clásico demostrado por Gauss en su famoso libro "Disquisitiones Arithmeticae". Una generalización para cualquier anillo conmutativo se encuentra en el ejercicio 71

PROPOSICIÓN 45. *(Lema de Gauss) Sean $f, g \in \mathbb{Z}[x]$. El polinomio fg es primitivo si y sólo si f y g son primitivos.*

DEMOSTRACIÓN. $\Rightarrow$) Argumentando por contrapositiva, supóngase sin pérdida de generalidad que f no es primitivo. Al usar la observación anterior sea $p \in \mathbb{N}$ un primo tal que p divide al máximo comun divisor de los coeficientes de f. Así, observe que p divide a los coeficientes de fg, luego fg no es primitivo.

$\Leftarrow$) Sea $p \in \mathbb{N}$ un primo. Si $f = \sum_{i=0}^{n} a_i x^i$ y $g = \sum_{i=0}^{m} b_i x^i$, por hipótesis existen $l \in \{0,...,n\}$ y $k \in \{0,...,m\}$ mínimos indices tales que $p \nmid a_l$ y $p \nmid b_k$. Observe que para fg el $(l+k)$-ésimo coeficiente es

$$\sum_{i=0}^{l+k} a_{l+k-i} b_i = \sum_{i=0}^{k-1} a_{l+k-i} b_i + a_l b_k + \sum_{i=k+1}^{l+k} a_{l+k-i} b_i$$

Note que $p|\sum_{i=0}^{k-1} a_{l+k-i}b_i$ pues $p|b_i$ para cada $i \in \{0,...,k-1\}$, y análogamente $p|\sum_{i=k+1}^{l+k} a_{l+k-i}b_i$. Sin embargo $p \nmid a_l b_k$ por lo que $p \nmid \sum_{i=0}^{l+k} a_{l+k-i}b_i$. Esto prueba que para cualquier primo, existe un coeficiente de fg que no es dividido por dicho primo, lo que implica que todos sus coeficientes son primos relativos. Por lo tanto, fg es primitivo. □

Uno de los resultados más famosos en torno a la irreducibilidad de polinomios con coeficientes enteros se muestra a continuación.

PROPOSICIÓN 46. *(Criterio de Eisenstein) Sea $f = \sum_{i=0}^{n} a_i x^i \in \mathbb{Z}[x]$ no constante. Si existe un número primo $p \in \mathbb{Z}$ tal que:*

1. $p \nmid a_n$
2. *Para cualquier $i \in \{0,...,n-1\}$, $p|a_i$*
3. $p^2 \nmid a_0$

Entonces $f \in \mathbb{Z}[x]$ es irreducible.

DEMOSTRACIÓN. Supóngase que $f = gh$ con $g,h \in \mathbb{Z}[x]$ y suponga que $g = \sum_{i=1}^{m} b_i x^i$ y $h = \sum_{i=0}^{k} c_i x^i$, con $m,k \geq 1$. Observe que como $p \nmid a_n$, entonces $p \nmid b_m$ y $p \nmid c_k$. Por otro lado $p|a_0$ y $p^2 \nmid a_0$. Como $a_0 = b_0 c_0$, entonces puede suponerse sin pérdida de generalidad que $p \nmid b_0$ y $p|c_0$. Sea $l \in \{1,...,k\}$ el mínimo indice tal que $p \nmid c_l$, el cual existe pues $p \nmid c_k$. Al comparar l y m se tienen dos casos.

Caso 1: $m \geq l$.

Al tomar

$$a_l = \sum_{i=0}^{l} b_i c_{l-i} = b_0 c_l + \sum_{i=1}^{l} b_i c_{l-i}$$

Se tiene que como $p \nmid b_0 c_l$ entonces $l = n$. Luego $m \geq n$ y como $m + k = n$, de esto se deduce que $k = 0$, lo que es una contradicción.

Caso 2: $m < l$.

Dado que

$$a_l = \sum_{i=0}^{l} b_{l-i} c_i = \sum_{i=0}^{l-1} b_{l-i} c_i + b_0 c_l$$

Como $p \nmid b_0 c_l$ entonces $l = n$. Así como $l \leq k$ entonces $n \leq k$. Dado que $k + m = n$ entonces $m = 0$ y así nuevamente se llega a una contradicción. □

Observación: El criterio de Eisenstein se suele enunciar teniendo como conclusión que el polinomio es irreducible sobre $\mathbb{Q}[x]$, sin embargo, la prueba se termina haciendo tal y como se hizo en estas notas, es decir, haciendo una reducción a coeficientes enteros. La razón por la que esto puede hacerse radica en el hecho de que $f \in \mathbb{Z}[x]$ se factoriza como producto de dos polinomios en $\mathbb{Z}[x]$ si y sólo si se factoriza como producto de dos polinomios en $\mathbb{Q}[x]$, los cuales tienen el mismo grado que los de la factorización sobre $\mathbb{Z}$.

EJEMPLO 22. *Considere $f \in \mathbb{Z}[x]$ definido por $f = x^2 - 8x - 2$. Al aplicar el criterio de Eisenstein usando el primo $2 \in \mathbb{Z}$ se concluye que f es irreducible en $\mathbb{Z}[x]$.*

Una generalización del criterio de Eisenstein aparece en el ejercicio 118, sin embargo, esta no puede verse en este momento pues se requiere desarrollar más teoría.

Regresando al problema que se está tratando, una forma usual de encontrar elementos irreducibles de $R[x]$ es el encajar dicho anillo de polinomios en otro anillo de polinomios. El ejemplo clásico se da con $\mathbb{R}[x]$, ya que como $\mathbb{R}[x] \subseteq \mathbb{C}[x]$ y en $\mathbb{C}[x]$ se tiene el teorema fundamental del álgebra, dicho teorema permite caracterizar elementos irreducibles, con lo que se concluye que los polinomios irreducibles en $\mathbb{R}[x]$ son los polinomios de grado 1 y los polinomios de grado 2, $f = ax^2 + bx + c$ con $b^2 - 4ac < 0$.

Usando las misma idea, es plausible llevar el estudio de irreducibiidad en $\mathbb{Z}[x]$ a $\mathbb{Q}[x]$, ya que observe que si $f \in \mathbb{Z}[x]$ es tal que f es irreducible en $\mathbb{Q}[x]$, entonces f es irreducible en $\mathbb{Z}[x]$. Más aún, si $f \in \mathbb{Z}[x]$ es irreducible, entonces $f \in \mathbb{Q}[x]$ es irreducible. Por lo que en este caso la irreducibilidad de un polinomio con coeficientes enteros es equivalente cuando se considera con coeficientes racionales. El porque este tipo resultados se tienen se dicuturán posteriormente con mayor generalidad.

2. Ideales máximos y primos

DEFINICIÓN 40. *Sea A un anillo e $I \leq A$. Decimos que I es un ideal máximo si $I \subsetneq A$ y para $J \leq A$ si $I \subseteq J \subseteq A$ entonces $J = I$ o $J = A$*

PROPOSICIÓN 47. *Sea A un anillo e $I \leq A$. Entonces I es máximo si y solo si A/I es campo.*

DEMOSTRACIÓN. $\Rightarrow$ Sea $x + I \in A/I$. Entonces $(A/I)(x+I) = Ax + I$. Notemos que por hipótesis $Ax + I = I$ o $Ax + I = A$, pero $I \subsetneq Ax + I$ porque $x \notin I$. De aqui $Ax + I = A$ entonces existe $a \in A$, $y \in I$ tal que $ax + y = 1$. Por lo que $ax - 1 = y \in I$ es decir, $(a+I)(x+I) = (1+I)$. Así tenemos que A/I es campo.

$\Leftarrow$ Sea $J \leq A$ con $I \subseteq J \subseteq A$. Entonces $J/I \leq A/I$. Si $J = I$ ya terminamos. Suponemos entonces que $I \neq J$, por lo que existe $x \in J$ tal que $x \notin I$. Por lo que $x + I \neq 0$ entonces

existe $y+I$ con $(x+I)(y+I) = (1+I)$, como $x+I \in J/I$ entonces $1+I \in J/I$ y de aqui concluimos que $A/I = J/I$. Por lo tanto $A = J$. □

EJERCICIO 6. *(Tarea) Sea A un anillo y $I, J \leq A$ con $I \subseteq J$. Entonces $J/I = A/I$ si y solo si $J = A$.*

COROLARIO 6. *Sea A un anillo. Entonces A es campo si y solo si 0 es un ideal máximo.*

COROLARIO 7. *(Tarea) Sea A un anillo. Son equivalentes:*

1. *A es campo*
2. *A tiene exactamente dos ideales*
3. *Todo morfismo de anillos $f : A \to B$ es inyectivo*

DEFINICIÓN 41. *Sea A un anillo e $I \leq A$. Decimos que I es un ideal primo, si $I \subsetneq A$ y $xy \in I$ implica que $x \in I$ o $y \in I$. Note que la contrapositiva nos dice que $x, y \notin I$ entonces $xy \notin I$*

PROPOSICIÓN 48. *Sea A un anillo e $I \leq A$. Son equivalentes:*

1. *I es primo*
2. *A/I es un dominio*
3. *Si $J, K \leq A$ con $JK \subseteq I$ entonces $J \subseteq I$ o $K \subseteq I$*
4. *Si $x, y \in A$ con $Axy \subseteq I$ entonces $Ax \subseteq I$ o $Ay \subseteq I$*

DEMOSTRACIÓN. 1) $\Rightarrow$ 2) Sean $x+I, y+I \neq 0$ entonces $x \notin I$ y $y \notin I$. Entonces $xy \notin I$, por lo que $xy * i \neq 0$. Por lo tanto A/I es un dominio entero.

2) $\Rightarrow$ 3) Sea $J, K \leq I$ con $JK \subseteq I$. Si $J \subseteq I$ entonces ya terminamos, por lo que suponemos que $J \nsubseteq I$, entonces existe $x \in J$ tal que $x \notin I$. De aqui $x+I \neq 0$. Sea $y \in K$. Entonces $xy \in JK \subseteq I$. Por lo que $xy+I = 0$, como A/I es dominio entero y $x+I \neq 0$ entonces $y+I = 0$, se sigue que $y \in I$. Por lo tanto $K \subseteq I$.

3) $\Rightarrow$ 4) Es un caso particular.

4) $\Rightarrow$ 1) Sean Sean $x, y \in A$ tales que $xy \in I$. Entonces $Axy \subseteq I$ por lo que $Ax \subseteq I$ o $Ay \subseteq I$. Por lo que $x \in I$ o $i \in I$. □

COROLARIO 8. *Sea A un anillo. Entonces A es un dominio entero si y solo si O es ideal primo.*

COROLARIO 9. *Sea A un anillo e $I \leq A$. Si I es un ideal máximo entonces es un ideal primo.*

PROPOSICIÓN 49. *Sea $f : A \to B$ un morfismo de anillos, y $P \leq B$ un ideal primo. Entonces $f^{-1}(P)$ es un ideal primo.*

DEMOSTRACIÓN. Sean $x, y \notin f^{-1}(P)$. Entonces $f(x), f(y) \notin P$. Por lo que $f(xy) = f(x)f(y) \notin P$. De aquí $xy \notin f^{-1}(P)$. Por lo tanto $f^{-1}(P)$ es un ideal primo. □

EJEMPLO 23. *Notemos que 0 es un ideal primo en $\mathbb{Z}$ puesto que $\mathbb{Z}$ es un dominio entero. Por otro lado, 0 no es máximo porque $\mathbb{Z}$ no es campo. Por otro lado $p\mathbb{Z}$ es un ideal máximo para todo p primo. Así $p\mathbb{Z}$ es un ideal primo para todo p primo.*

EJERCICIO 7. *Si $f : \mathbb{Z} \to \mathbb{Q}$ notemos que 0 es un ideal máximo en $\mathbb{Q}$ pero $f^{-1}(0) = 0$ no es máximo en $\mathbb{Z}$.*

DEFINICIÓN 42. *Sea A un anillo y $x, y \in A$. Decimos que x divide a y y se denota $x|y$, si existe $a \in A$ tal que $ax = y$.*

PROPOSICIÓN 50. *(Tarea) Sea A un anillo y $x, y, z \in A$, entonces:*

1. *Si $x|y$ y $y|z$ entonces $x|z$*
2. *Si $x|y$ y $x|z$ entonces $x|y+z$*
3. *Si $x|y$ entonces $x|yz$*
4. *$x|0$*

PROPOSICIÓN 51. *Sea A un anillo y $x, y \in A$. Entonces $x|y \Leftrightarrow Ry \subseteq Rx$*

DEFINICIÓN 43. *Sea A un anillo y $x \in A$. Entonces Decimos que x es primo si Ax es un ideal primo*

PROPOSICIÓN 52. *Sea A un anillo y $x \in A$. Entonces x es primo si y solo si $x|yz$ implica $x|y$ o $x|z$.*

DEMOSTRACIÓN. $\Rightarrow$ Si $x|yz$ entonces $Ryz \subseteq Rx$. Como Rx es un ideal primo entonces $Ry \subseteq Rx$ o $Rz \subseteq Rx$. Entonces $x|y$ o $x|z$.

$\Leftarrow$ Si $Ryz \subseteq Rx$ entonces $x|yz$. Por lo que $x|y$ o $x|z$. Entonces $Ry \subseteq Rx$ o $Rz \subseteq Rx$. Por lo tanto Rx es un ideal primo. □

DEFINICIÓN 44. *Sea A un anillo y $x \in A$. Decimos que x es irreducible si $y|x$ entonces $y \in U(A)$ o $y = xu$ con $u \in U(A)$.*

En general, la noción que tenemos de elemento primo es de elemento irreducible. Estas nociones no tienen porque coincidir.

EJEMPLO 24. *Sea $4 \in \mathbb{Z}_{12}$, veamos que $\mathbb{Z}_{12}/4\mathbb{Z}_{12} \cong \mathbb{Z}_3$ campo. Por lo que 4 es primo en $\mathbb{Z}_{12}$. Por otro lado $2|4$ en $\mathbb{Z}_{12}$, veamos que $2 \cdot 6 = 12 = 0$ por lo que 2 no es unidad. Por otro lado las unidades de $\mathbb{Z}_{12}$ son los primos relativos con 12, digamos $1,5,7,11$ ahora*

$$\begin{aligned} 4 \cdot 1 &= 4 = 4 \\ 4 \cdot 5 &= 20 = 8 \\ 4 \cdot 7 &= 28 = 4 \\ 4 \cdot 11 &= 44 = 8 \end{aligned}$$

Por lo que no existe unidad u tal que $4 \cdot u = 2$ entonces 4 es primo pero no es irreducible en $\mathbb{Z}_{12}$

EJEMPLO 25. *Sea $A = \mathbb{Z}[i\sqrt{5}] = \{x + i\sqrt{5} : x, y \in \mathbb{Z}\}$ el subanillo de $\mathbb{C}$. Notemos que*

$$2 \cdot 3 = (1 + i\sqrt{5})(1 - i\sqrt{5})$$

de aqui

$$2|(1 + i\sqrt{5})(1 - i\sqrt{5})$$

ahora

$$2(x + y\sqrt{5}i) = 2x + 2y\sqrt{5}i$$

Notemos que esto implica

$$\begin{aligned} 2x &= 1 \\ 2y &= \pm 1 \end{aligned}$$

Como x, y debe ser enteros, entonces el sistema no tiene solución. Por lo que 2 no divide a $1 + i\sqrt{5}$ ni a $1 - i\sqrt{5}$. De aquí, 2 no es primo en $\mathbb{Z}[i\sqrt{5}]$.

Ahora consideremos la función $N(x + i\sqrt{5}y) = x^2 + 5y^2$. Veamos que $N(2) = 4$ y que $N(ab) = N(a)N(b)$(Tarea).
Si $ab = 2$ entonces $N(a)N(b) = 4$. De aquí $N(a) = 1, 2, 4$. Es claro que $N(a) \neq 2$.
Ahora si $N(a) = 1$ entonces $a = \pm 1$ y si $N(a) = 4$ entonces $a = \pm 2$. Sin perdida de generalidad tenemos que $a = \pm 1$ y $b = \pm 2$. Por lo que 2 es irreducible en $\mathbb{Z}[i\sqrt{5}]$

PROPOSICIÓN 53. *(Tarea) Sea A un dominio de factorización única y $x \in A$ con $x \neq 0$. Entonces x es primo $\Leftrightarrow$ x es irreducible.*

PROPOSICIÓN 54. *Sea $A \neq 0$ un anillo. Entonces A tiene un ideal máximo.*

DEMOSTRACIÓN. Sea $\mathscr{S}$ el conjunto de los ideales I de A tales que $I \neq A$ es decir, $\mathscr{S} = \{I \leq A : I \neq A\}$, notemos que $\mathscr{S}$ esta ordenado por la relación de contención y $\mathscr{S}$ es no vació porque $0 \in \mathscr{S}$. Sea $\mathscr{C} = \{I_k\}_{k=0}^{\infty}$ una cadena ascendente $I_o \subseteq I_1 \subseteq \dots$ en $\mathscr{S}$. Afirmamos que $\bar{I} = \bigcup_{k=0}^{\infty} I_k$ es una cota superior de $\mathscr{C}$. Sean $x, y \in \bar{I}$, entonces $x \in I_n$, $y \in I_m$ para alguna $n, m \in \mathbb{N}$.
Sin perdida de generalidad $n \leq m$, por lo que $x + y \in I_m \subseteq \bar{I}$. Sean $x \in I$ y $a \in A$, entonces $x \in I_n$ para alguna $n \in \mathbb{N}$. De aquí $ax \in I_n \subseteq \bar{I}$. Por lo que $\bar{I}$ es un ideal, notemos que $\bar{I} \neq A$ puesto que si $\bar{I} = A$ entonces $1 \in \bar{I}$, por lo que $1 \in I_n$ para alguna $n \in \mathbb{N}$. De aquí $A = I_n$ lo cual es una contradicción pues $I_n \in \mathscr{S}$. Por lo que $\bar{I} \in \mathscr{S}$. Por lema de Zorn, $\mathscr{S}$ tiene elemento un elemento máximo M. Por construcción $M \leq A$ es ideal máximo. □

PROPOSICIÓN 55. *(Tarea) Sea A un anillo e $I \leq A$ con $I \neq A$. Entonces existe $M \leq A$ máximo tal que $I \subseteq M$.*

COROLARIO 10. *(Tarea) Sea A un anillo y $x \notin U(A)$. Entonces existe $M \leq A$ máximo tal que $x \in M$*

Observación. Si A es un anillo neteriano, esto se puede hacer sin usar lema de Zorn.

DEFINICIÓN 45. *Sea A un anillo. Decimos que A es un anillo local si tiene exactamente un ideal máximo.*

PROPOSICIÓN 56. *Sea A un anillo y $M \lneq A$ tal que $A \backslash M \subseteq U(A)$. Entonces A es un anillo local y M es el ideal máximo.*

DEMOSTRACIÓN. Notemos que como $M \neq A$ entonces $M \cap U(A) = \emptyset$, por lo que tenemos que $M = A \backslash U(A)$, por otro lado todo ideal $I \lneq A$ propio no contiene unidades, es decir, $I \cap U(A) = \emptyset$. Por lo tanto $I \subseteq M$ y así M el ideal máximo. □

PROPOSICIÓN 57. *Sea A un anillo y M ideal máximo de A. Si todo elemento $y = 1 + x$ con $x \in M$ es una unidad, entonces A es un anillo local.*

DEMOSTRACIÓN. Sea $x \in A \backslash M$. Como M es máximo entonces $M + Rx = A$. Por lo que existe $a \in A$ y $m \in M$ tales que $ax + m = 1$. De aquí $ax = 1 - m$ por lo que ax es

una unidad. Notemos que este implica que x es unidad. Podemos aplicar la proposición anterior □

PROPOSICIÓN 58. *Sea D un dominio de ideales principales. Si $P \leq A$ es primo y $P \neq 0$ entonces P es máximo.*

PROPOSICIÓN 59. *Sea A un anillo y $P_1, P_2, \ldots P_n \leq A$ ideales primos e $I \leq A$ tal que $I \subseteq \bigcup_{i=1}^{n} P_i$, entonces $I \subseteq P_j$ para algún $j = 1, ..., n$*

DEMOSTRACIÓN. Lo demostraremos por inducción sobre n y por contrapuesta, si $I \nsubseteq P_i$ para toda $i = 1, ..., n$ entonces $I \nsubseteq \bigcup_{i=1}^{n} P_I$.
Es claro para $n = 1$.
Suponemos valido para n y lo demostraremos para n+1.
Para cada $i = 1, ..., n+1$ existe $x_i \in I$ tal que $x_i \notin P_j$ para $j \neq i$. Esto porque si no pasara para algún $k = 1, ..., n+1$ entonces para todo $x \in I$ existe $j \neq k$ tal que $x \in P_j$. Es decir $I \subseteq \bigcup_{i=1, i\neq k}^{n+1} P_i$ contradiciendo la hipótesis de inducción.
Si fuese el caso de que para algún j, $x_j \notin P_j$ terminamos. Si no, $x_i \in P_i$ para toda $i = 1, ..., n+1$ y consideramos el elemento

$$y = \sum_{i=1}^{n+1} \prod_{j \neq i}^{n+1} x_j$$

Por construcción $y \in I$. Notemos que como P_i es primo entonces $\prod_{j\neq i}^{n+1} x_j \notin P_i$, ahora bien $\prod_{j\neq k}^{n+1} x_j \in P_i$ para $j \neq i$. Por lo que si $y \in P_i$ para algún $i = 1, ..., n+1$ entonces $\prod_{j\neq i}^{n+1} \in P_i$, lo cual es una contradicción. Así $y \in P_i$ para todo $i = 1, ..., n+1$, por lo tanto $I \nsubseteq \bigcup_{i=1}^{n+1} P_i$ □

PROPOSICIÓN 60. *Sea A un anillo, $I_1, ..., I_n \leq A$ y P un ideal primo tal que $\bigcap_{i=1}^{n} I_i \subseteq P$. Si $P = \bigcap_{i=1}^{n} I_i$ entonces $P = I_j$ para algún $j = 1, ..., n$*

DEMOSTRACIÓN. Como $\prod_{i=1}^{n} I_i \subseteq \bigcap_{i=1}^{n} I_i \subseteq P$ entonces I_j para algún $j = 1, ..., n$. Por otro lado $P = \bigcap_{i=1}^{n} I_i \subseteq I_j$, por lo tanto $P = I_j$ □

PROPOSICIÓN 61. *Sea A un anillo tal que para todo $x \in A$ existe $n \in \mathbb{N}^+$ tal que $x^n = x$ entonces todo ideal primo es máximo.*

DEMOSTRACIÓN. Sea P un ideal primo y $x \in A$,$x \notin P$. Entonces existe $n \in \mathbb{N}^+$ tal que $x^n = x$. De aquí $x(x^{n-1} - 1) = 0 \in P$. Como P es un ideal primo, debe pasar que $x^{n-1} - 1 \in P$, por lo que $x^{n-1} + P = 1 + P$. De aquí, tenemos que A/P es un campo y por lo tanto P es máximo. □

PROPOSICIÓN 62. *Sea A un anillo. Entonces existe un ideal primo mínimo.*

DEMOSTRACIÓN. Sea $\{P_i\}_{i=0}^{\infty}$ una cadena descendente de ideales primos de A. Denotamos $P = \bigcap_{i=0}^{n} P_i$. Si $x, y \notin P$, entonces existen $n, m \in \mathbb{N}$ tales que $x \in P_n$ y $y \notin P_m$. Sin perdida de generalidad suponemos que $m \geq n$. Así $x, y \notin P_m$. Por lo que $xy \notin P_m$. De esto $xy \notin P$ y así P es un ideal primo. Por el lema de Zorn tenemos que el conjunto de ideales primos tiene un mínimo. □

DEFINICIÓN 46. *Sea A un anillo. Decimos que A es de Boole si* $x^2 = x$ *para todo* $x \in A$.

PROPOSICIÓN 63. *Sea A un anillo de Boole. Entonces* $2x = 0$ *para todo* $x \in A$.

DEMOSTRACIÓN. Sea $x \in A$,

$$0 = (x+1)^2 - (x+1) = x^x + 2x + 1 - x - 1 = 2x$$

□

PROPOSICIÓN 64. *Sea A un anillo de Boole. Entonces todo ideal primo P es máximo y* A/P *tiene dos elementos.*

DEMOSTRACIÓN. Sea P un ideal primo y $x \notin P$. Entonces $x(x-1) = 0 \in P$, como P es primo entonces $x - 1 \in P$. Por lo que $x + P = 1 + P$, de aquí A/P solo tiene dos clases. □

PROPOSICIÓN 65. *Sea A un anillo de Boole. Todo ideal finitamente generado es principal.*

DEMOSTRACIÓN. La demostración es por inducción pero basta hacerla para el caso de dos generadores.

Sea $I = Ax + Ay \leq A$. Ponemos $z = x + y + xy$ y vemos que

$$xz = x(x + y + xy) = x^2 + xy + xy = x$$

Análogamente $yz = y$, por lo que $Ax + Ay = Az$ □

3. El nilradical e ideales radicales

DEFINICIÓN 47. *Sea* $I \leq R$. *El radical de I, el cual se denota por* $\sqrt{I}$, *es el conjunto* $\{x \in R \,:\, \exists n \in \mathbb{N}^+ (x^n \in I)\}$.

Observaciónes:

- Por definición $\sqrt{0}$ es el nilradical de R. Usualmente se denota $N(R) := \sqrt{0}$.
- La proposición 42 se puede parafrasear mediante la igualdad $N(R[x]) = N(R)[x]$.

La observación anterior muestra que el radical de un ideal es una generalización del nilradical. De hecho, este sigue siendo un ideal.

PROPOSICIÓN 66. *Si $I \leq R$, entonces $\sqrt{I} \leq R$.*

DEMOSTRACIÓN. Considere la proyección

$$\pi : R \to R/I.$$

Nótese que $\sqrt{I} = \pi^{-1}(N(R/I))$, como $N(R/I) \leq R/I$, esta última igualdad implica el resultado deseado. □

Algunas de las propiedades básicas de los ideales radicales se muestran en el siguiente resultado.

PROPOSICIÓN 67. *Sean $I, J \leq R$. Entonces,*

1. $I \subseteq \sqrt{I}$
2. *Si $I \subseteq J$ entonces $\sqrt{I} \subseteq \sqrt{J}$*
3. $\sqrt{\sqrt{I}} = \sqrt{I}$
4. $\sqrt{IJ} = \sqrt{I \cap J} = \sqrt{I} \cap \sqrt{J}$
5. $\sqrt{I+J} = \sqrt{\sqrt{I} + \sqrt{J}}$
6. *$\sqrt{I} = R$ si y solo si $I = R$*
7. *Para cualquier $\mathfrak{p} \leq R$ primo y $n \in \mathbb{N}^+$ se tiene $\sqrt{\mathfrak{p}^n} = \mathfrak{p}$*

DEMOSTRACIÓN. Las propiedades 1 y 2 son claras.

Respecto a 3 observe que por 1, $\sqrt{I} \subseteq \sqrt{\sqrt{I}}$. Por otro lado, si $x \in \sqrt{\sqrt{I}}$, existe $n \in \mathbb{N}^+$ tal que $x^n \in \sqrt{I}$. Además, existe $m \in \mathbb{N}^+$ tal que $(x^n)^m \in I$. Esto implica que $x \in \sqrt{I}$ y prueba lo contención restante.

Respecto a 4, como $IJ \subseteq I \cap J \subseteq I, J$ entonces $\sqrt{IJ} \subseteq \sqrt{I \cap J} \subseteq \sqrt{I} \cap \sqrt{J}$. Observe que si se prueba que $\sqrt{I} \cap \sqrt{J} \subseteq \sqrt{IJ}$, esto implica la igualdad buscada. En efecto, si $x \in \sqrt{I} \cap \sqrt{J}$, existen $n, m \in \mathbb{N}^+$ tales que $x^n \in I$ y $x^m \in J$, observe que

$$x^{n+m} = x^n x^m \in IJ$$

esto prueba que $x \in \sqrt{IJ}$.

Para la propiedad 5 observe que

$$I+J \subseteq \sqrt{I}+\sqrt{J}$$

luego

$$\sqrt{I+J} \subseteq \sqrt{\sqrt{I}+\sqrt{J}}$$

Para la contención restante considere $x \in \sqrt{\sqrt{I}+\sqrt{J}}$, entonces existe $n \in \mathbb{N}^+$ tal que $x^n \in \sqrt{I}+\sqrt{J}$. Así, existen $y \in \sqrt{I}$ y $z \in \sqrt{J}$ tales que

$$x^n = y+z$$

Sean $m,k \in \mathbb{N}^+$ tales que $y^m \in I$ y $z^k \in J$. Entonces por el teorema del binomio

$$(y+z)^{m+k} = \sum_{l=0}^{m+k} \left(\begin{array}{c} m+k \\ l \end{array} \right) y^l z^{m+k-l}$$

Para $l \in \{0,...,m\}$ se tiene que $z^{m+k-l} \in J$ y para $l \in \{m+1,...,m+k\}$ se tiene que $y^l \in I$. Esto implica que $(x^n)^{m+k} = (y+z)^{m+k} \in I+J$ y prueba que $x \in \sqrt{I+J}$.

Para la propiedad 6, la ida se deduce del hecho de que como $1 \in \sqrt{I}$, entonces existe $n \in \mathbb{N}^+$ tal que $1^n \in I$. Luego $1 \in I$ y así $I = R$. El regreso se deduce del hecho de que si $I = R$ entonces $R \subseteq \sqrt{I} \subseteq R$.

En lo que respecta a la propiedad 7 observe que para $\mathfrak{p} \leq R$ primo y $n \in \mathbb{N}^+$, es claro $\mathfrak{p} \subseteq \sqrt{\mathfrak{p}^n}$. Por otro lado como $\mathfrak{p}^n \subseteq \mathfrak{p}$, entonces $\sqrt{\mathfrak{p}^n} \subseteq \sqrt{\mathfrak{p}}$. Observe que si $x \in \sqrt{\mathfrak{p}}$ existe $m \in \mathbb{N}^+$ tal que $x^m \in \mathfrak{p}$. Como $\mathfrak{p}$ es primo entonces $x \in \mathfrak{p}$. Esto prueba que $\sqrt{\mathfrak{p}} \subseteq \mathfrak{p}$ y concluye la prueba. □

En la proposición anterior hay varios ejemplos de ideales que quedan fijos al aplicar el radical, el cual dicho sea de paso es una función monótona entre las retículas de ideales del anillo en cuestión. Esto da lugar a lo siguiente:

DEFINICIÓN 48. *Un ideal $I \leq R$ es radical si*

$$\sqrt{I} = I.$$

EJEMPLO 26. *Para cualquier $I \leq R$, $\sqrt{I}$ es un ideal radical. En particular $N(R)$ es un ideal radical.*

EJEMPLO 27. *R es un ideal radical de si mismo.*

EJEMPLO 28. *Todo ideal primo $\mathfrak{p} \leq R$ es radical.*

EJEMPLO 29. *No todo ideal es radical. Un ejemplo se obtiene al considerar $4\mathbb{Z} \leq \mathbb{Z}$, ya que $2 \in \sqrt{4\mathbb{Z}}$ pero $2 \notin 4\mathbb{Z}$, luego $4\mathbb{Z} \subsetneq \sqrt{4\mathbb{Z}}$.*

De hecho observe que como $2 \in \sqrt{4\mathbb{Z}}$ entonces $2\mathbb{Z} \subseteq \sqrt{4\mathbb{Z}}$. Por otro lado, si $x \in \sqrt{4\mathbb{Z}}$ existe $n \in \mathbb{N}^+$ tal que $x^n = 4k$. Esto implica que $2|x^n$ y entonces $2|x$. Así $x \in 2\mathbb{Z}$ y esto prueba que $\sqrt{4\mathbb{Z}} = 2\mathbb{Z}$.

Hay un resultado general que permite calcular el ideal radical de cualquier ideal de $\mathbb{Z}$. Este se encuentra en el ejercicio 101 .

Los ideales radicales tienen un papel fundamental en geometría algebraica pues estos definen una clase especial de subconjuntos del espacio afín, los cuales se conocen como conjuntos algebraicos afines. De hecho estos estaán en correspondencia biyectiva con dichos objetos geométricos. Dicha correspondencia empieza por el siguiente resultado.

PROPOSICIÓN 68. *Si $I \leq R$. Entonces,*

$$\sqrt{I} = \bigcap \{\mathfrak{p} \leq R \ : \ \mathfrak{p} \text{ es primo}, I \subseteq \mathfrak{p}\}$$

DEMOSTRACIÓN. Sea $\mathfrak{p} \leq R$ primo tal que $I \subseteq \mathfrak{p}$. Entonces $\sqrt{I} \subseteq \sqrt{\mathfrak{p}} = \mathfrak{p}$. Esto implica que $\sqrt{I} \subseteq \bigcap \{\mathfrak{p} \leq R \ : \ \mathfrak{p} \text{ es primo}, I \subseteq \mathfrak{p}\}$.

Para la contención restante se va a probar la condición equivalente al tomar complementos relativos en R. Sea $x \in R$ con $x \notin \sqrt{I}$. Esto dice que para cualquier $n \in \mathbb{N}^+$, $x^n \notin I$. Defina el conjunto $S = \{x^n : n \in \mathbb{N}^+\}$ y considere $\Gamma = \{J \leq R : I \subseteq J, J \cap S = \emptyset\}$. Observe que $\Gamma \neq \emptyset$ y ademas $(\Gamma, \subseteq)$ es un COPO. Así, para usar lema de Zorn considere $\{J_\alpha\}_{\alpha \in A}$ una cadena no vacía en Γ. Note que $\bigcup_{\alpha \in A} J_\alpha \leq R$ e $I \subseteq \bigcup_{\alpha \in A} J_\alpha$. Además

$$\left(\bigcup_{\alpha \in A} J_\alpha \right) \cap S = \bigcup_{\alpha \in A} (J_\alpha \cap S) = \emptyset$$

Por lo tanto, dicha cadena es acotada superiormente. Luego, el Lema de Zorn implica que existe $\mathfrak{p} \in \Gamma$ máximo.

Afirmación: $\mathfrak{p} \leq R$ es primo. En efecto, si $y,z \in R\backslash\mathfrak{p}$, entonces $\mathfrak{p}+\langle y\rangle, \mathfrak{p}+\langle z\rangle \notin \Gamma$, por lo que estos ideales intersectan a S. Dado que

$$(\mathfrak{p}+\langle y\rangle)(\mathfrak{p}+\langle z\rangle) \subseteq \mathfrak{p}+\langle yz\rangle$$

Entonces

$$(\mathfrak{p}+\langle yz\rangle) \cap S \neq \emptyset$$

y así

$$\mathfrak{p}+\langle yz\rangle \notin \Gamma.$$

Por lo tanto, como

$$\mathfrak{p} \subsetneq \mathfrak{p}+\langle yz\rangle$$

esto implica que

$$yz \in R\backslash\mathfrak{p}.$$

Esto prueba que $\mathfrak{p} \subseteq R$ es primo.

Para concluir observe que como $x \notin \mathfrak{p}$, por definición,

$$x \in R\backslash\bigcap\{\mathfrak{q} \leq R \,:\, I \subseteq \mathfrak{q}, \mathfrak{q} \text{ es primo}\},$$

lo que prueba la afirmación. □

Se deduce directamente del resultado anterior que,

COROLARIO 11. $N(R) = \bigcap\{\mathfrak{p} \leq R \,:\, \mathfrak{p} \textit{ es primo}\}$

El último resultado a tratar tiene que ver con una clase especial de anillos que no tienen nilpotentes. Estos son importantes en geometría algebraica.

DEFINICIÓN 49. *Un anillo R es reducido si no tiene elementos nilpotentes distintos del trivial.*

Observe que trivialmente todo dominio entero es un anillo reducido. Sin embargo, el regreso no es cierto. Un ejemplo lo da el anillo de funciones continuas $C_0([0,1])$ que no es dominio entero, sin embargo es reducido. El siguiente resultado da una caracterización de anillos reducidos en términos de dominios enteros.

PROPOSICIÓN 69. *Un anillo conmutativo R es reducido si y sólo si se encaja en un producto de dominios enteros.*

DEMOSTRACIÓN. $\Rightarrow$) Considere para cada $\mathfrak{p} \leq R$ primo, la proyección

$$\pi_{\mathfrak{p}} : R \to R/\mathfrak{p}$$

Observe que $R/\mathfrak{p}$ es un dominio entero. Además, por la propiedad universal del producto, existe un único morfismo

$$f : R \longrightarrow \prod_{\mathfrak{p} \leq R, \mathfrak{p} \text{ es primo}} R/\mathfrak{p},$$

tal que para cualquier $\mathfrak{p} \leq R$ con $\mathfrak{p}$ primo,

$$p_{\mathfrak{p}} \circ f = \pi_{\mathfrak{p}}.$$

Note que $a \in Nuc(f)$ si y sólo si para cualquier $\mathfrak{p} \leq R$ primo, $a + \mathfrak{p} = \mathfrak{p}$, es decir $a \in N(R)$. Dado que R es reducido, entonces $N(R) = 0$, y por lo tanto, del primer teorema de isomorfismo se deduce que

$$R \cong R/Nuc(f) \cong Im(f) \subseteq \prod_{\mathfrak{p} \leq R, \mathfrak{p} \text{ es primo}} R/\mathfrak{p},$$

lo que prueba el resultado.

$\Leftarrow$) Es claro. □

4. Radical de Jacobson

5. Anillos de fracciones y anillos locales

En esta sección se va a estudiar una construcción que generaliza la construcción de $\mathbb{Q}$ a partir de $\mathbb{Z}$. Dicha construcción tiene una contraparte geométrica que de manera vaga se puede pensar como dada una variedad, considerar vecindades alrededor de un punto.

DEFINICIÓN 50. *Sea $S \subseteq R$. Decimos que S es multiplicativo si*

1. *Para cualesquiera $x, y \in S$, $xy \in S$.*
2. $1 \in S$.

EJEMPLO 30. *Dado $\mathfrak{p} \leq R$ primo, el conjunto $R \backslash \mathfrak{p}$ es multiplicativo. De hecho observe que esta propiedad caracteriza el concepto de primo.*

EJEMPLO 31. *Sea $x \in R$. El conjunto $S = \{x^n : n \in \mathbb{N}\}$ es multiplicativo de la definición de "elevar a la n".*

EJEMPLO 32. *Todo subanillo es un conjunto multiplicativo del anillo en cuestión.*

A continuación se mencionará como obtener la construcción mencionada: Considere R un anillo y $S \subseteq R$ un conjunto multiplicativo. Defina una relación $\sim \subseteq (R \times S)^2$ mediante:

$$(a,s) \sim (b,t)$$

si existe $u \in S$ tal que

$$u(at - bs) = 0$$

PROPOSICIÓN 70. *La relación anterior es de equivalencia.*

DEMOSTRACIÓN. Dado $(a,s) \in R \times S$, observe que $1(as - as) = 0$, es decir, $(a,s) \sim (a,s)$.

Supónga que $(a,s) \sim (b,t)$. Entonces existe $u \in S$ tal que $u(at - bs) = 0$. Al multiplicar por -1, $u(bs - at) = 0$, es decir $(b,t) \sim (a,s)$.

Para la transitividad suponga que $(a,t) \sim (b,s)$ y $(b,t) \sim (c,v)$. Entonces existen $u, u' \in S$ tales que

$$\begin{aligned} u(at - bs) &= 0 \\ u'(bv - ct) &= 0 \end{aligned}$$

Estas igualdades implican que

$$\begin{aligned} u'vu(at - bs) &= 0 \\ usu'(bv - ct) &= 0 \end{aligned}$$

De donde

$$\begin{aligned} u'vuat - usu'ct &= 0 \\ u'ut(av - cs) &= 0 \end{aligned}$$

Dado que $u'ut \in S$ entonces $(a,s) \sim (c,v)$ □

Denote por $S^{-1}R = (R \times S)/\sim$. Además, notacionalmente se va a escribir

$$\frac{a}{s} := [(a,s)]$$

Observación: Si $R = \mathbb{Z}$ y $S = \mathbb{Z}\backslash\{0\}$, entonces la relación definida es equivalente a la relación que define a $\mathbb{Q}$ a partir de $\mathbb{Z}$ pues $\mathbb{Z}$ es un dominio entero. Además, salvo que el conjunto S no tenga divisores de cero, no puede eliminarse en la definición de la relación el producto con el elemento de S (113).

La siguiente meta es definir operaciones en $S^{-1}R$ que hagan de este un anillo. Para esto, inspirados en la intuición de la construcción de $\mathbb{Q}$ a partir de $\mathbb{Z}$ se definen las asignaciones:

$$+,\cdot : S^{-1}R \times S^{-1}R \to S^{-1}R$$

mediante las reglas de correspondencia:

$$\begin{aligned}\frac{a}{s} + \frac{b}{t} =& \frac{at+bs}{st}\\ \frac{a}{s} \cdot \frac{b}{t} =& \frac{ab}{st}\end{aligned}$$

En estas definiciones hay un detalle de carácter técnico asociado al hecho de que los elementos de $S^{-1}R$ son clases de equivalencia, por lo tanto hay que ver que estas asignaciones no dependen de representantes. Veamos que esto sucede:
Suponga que

$$\begin{aligned}\frac{a}{s} =& \frac{a'}{s'}\\ \frac{b}{t} =& \frac{b'}{t'}\end{aligned}$$

Entonces existen $u, v \in S$ tales que

$$\begin{aligned}u(as' - a's) =& 0\\ v(bt' - b't) =& 0\end{aligned}$$

De estas igualdades se deduce que

$$\begin{aligned}vt'tu(as' - a's) =& 0\\ uss'v(bt' - b't) =& 0\end{aligned}$$

Entonces

$$vt'tuas' - t'tua'sv + ss'vbt'u - ss'vb'yu = 0$$

Luego

$$\begin{aligned}0 =& (at+bs)s't'uv - (a't' + b's')stuv\\ =& uv[(at+bs)s't' - (a't' + b's')st]\end{aligned}$$

Esto implica que

$$\frac{at+bs}{st} = \frac{a't'+b's'}{s't'}$$

Lo que prueba que $+$ es en efecto una función. Además, la prueba de la afirmación correspondiente para el caso $\cdot$ es análoga, así que se va a omitir. Mas aún, al copiar la prueba usada para ver que $\mathbb{Q}$ es un anillo, se tiene lo siguiente.

PROPOSICIÓN 71. *Dado $S \subseteq R$ multiplicativo, el conjunto $(S^{-1}R, +, \cdot)$ es un anillo con los elementos distinguidos $\frac{0}{1}$ para la suma y $\frac{1}{1}$ el producto.*

DEFINICIÓN 51. *Al anillo $S^{-1}R$ se le conoce como el anillo de fracciones de R respecto al conjunto multiplicativo S.*

EJEMPLO 33. *Para $R = \mathbb{Z}$ y $S = \mathbb{Z}\backslash\{0\}$, entonces $S^{-1}R = \mathbb{Q}$. En este caso el anillo de fracciones son los racionales.*

Siguiendo la intuición que da el ejemplo anterior surgen dos posibles observaciones:

- La primera de ellas tiene que ver con el hecho de que hay un morfismo de inclusión de $\mathbb{Z}$ en $\mathbb{Q}$.
- La segunda es si el anillo de fracciones es siempre un campo como sucede en el ejemplo anterior.

Trataremos las cuestiones análogas para la construcción realizada a continuación.
Primero observe que hay una función canónica

$$f : R \to S^{-1}R$$

cuya regla de correspondencia es

$$f(a) = \frac{a}{1}$$

Mas aún, esta es claramente un morfismo de anillos. Sin embargo, a diferencia de lo que sucede en el ejemplo mencionado, esta no encaja en general al anillo R en su anillo de fracciones. El siguiente resultado caracteriza el núcleo de dicho morfismo canónico.

PROPOSICIÓN 72. *Sea $f : R \to S^{-1}R$ el morfismo canónico de R en $S^{-1}R$. Entonces $Nuc(f) = \{a \in R \ : \ \exists s \in S(sa = 0)\}$*

DEMOSTRACIÓN. $a \in Nuc(f)$ si y solo si $\frac{a}{1} = f(a) = \frac{0}{1}$. Esto sucede si y sólo si existe $s \in S$ tal que $s(a \cdot 1 - 0 \cdot 1) = 0$. □

COROLARIO 12. *Si $S \subseteq R$ es un conjunto multiplicativo sin divisores de cero, entonces el morfismo canónico*

$$f : R \to S^{-1}R$$

es inyectivo y viceversa. En particular, dicho resultado es válido si R es un dominio entero.

Respecto a la segunda pregunta, resulta que $S^{-1}R$ no es en general un campo. Lo que hizo la construcción simplemente es encontrar un anillo en el que todos los elementos de S tienen un inverso. Cuando se analicen ejemplos concretos se verá que efectivamente $S^{-1}R$ no es un campo en general. Antes de pasar a esto se va a ver que el anillo de fracciones cumple una propiedad universal que lo caracteriza salvo isomorfismo, de hecho se va a ver que la propiedad mencionada lo caracteriza.

PROPOSICIÓN 73. *Sea $f : R \to S^{-1}R$ el morfismo canónico. Entonces*

1. *Para cualquier $s \in S$*

$$f(s) \in U(S^{-1}R)$$

   es decir

$$f(S) \subseteq U(S^{-1}R)$$

2. *Todo elemento $\frac{a}{s} \in S^{-1}R$ se puede escribir como*

$$\frac{a}{s} = f(a)f(s)^{-1}$$

DEMOSTRACIÓN. Para 1, dado que $s \in S$ se tiene que $f(s) = \frac{s}{1}$. Observe que $\frac{1}{s} \in S^{-1}R$ y ademas $\frac{s}{1} \cdot \frac{1}{s} = \frac{1}{1}$, lo que prueba la afirmación.

Para la segunda afirmación, sea $\frac{a}{s} \in S^{-1}R$. Se tiene que

$$\frac{a}{s} \cdot \frac{s}{1} = \frac{a}{1}$$

Entonces

$$\frac{a}{s} \cdot f(s) = f(a)$$

Como $f(s) \in U(S^{-1}R)$ entonces

$$\frac{a}{s} = f(a)f(s)^{-1}$$

□

PROPOSICIÓN 74. *(Propiedad universal del anillo de fracciones) Sean $S \subseteq R$ un subconjunto multiplicativo y $f : R \to S^{-1}R$ el morfismo canónico de R en $S^{-1}R$. Dicha construcción satisface lo siguiente: Dado cualquier morfismo de anillos $g : R \to A$ tal que $g(S) \subseteq U(A)$, existe un único morfismo de anillos $\bar{g} : S^{-1}R \to A$ tal que $\bar{g} \circ f = g$*

DEMOSTRACIÓN. Dado el morfismo $g : R \to A$ con la propiedad mencionada, defina

$$\bar{g} : S^{-1}R \to A$$

mediante la regla de correspondencia

$$\bar{g}\left(\frac{a}{s}\right) = g(a)g(s)^{-1}$$

Veamos que en efecto $\bar{g}$ es una función.
Suponga que $\frac{a}{s} = \frac{a'}{s'}$. Entonces existe $u \in S$ tal que

$$u(as' - a's) = 0$$

Al aplicar g y al usar que este es morfismo de anillos se tiene

$$g(u)(g(a)g(s') - g(a')g(s)) = 0$$

Como $u \in S$, $g(u) \in U(A)$, entonces

$$g(a)g(s') - g(a')g(s) = 0,$$

lo que implica que

$$g(a)g(s') = g(a')g(s)$$

y muestra que $\bar{g}(\frac{a}{s}) = \bar{g}(\frac{a'}{s'})$.

Ahora hay que ver que $\bar{g}$ es morfismo de anillos. En efecto, sean $\frac{a}{s}, \frac{b}{t} \in S^{-1}R$. Luego

$$\begin{aligned}
\bar{g}\left(\frac{a}{s} + \frac{b}{t}\right) &= \bar{g}\left(\frac{at + bs}{st}\right) \\
&= g(at + bs)g(st)^{-1} \\
&= (g(a)g(t) + g(b)g(s))(g(s)^{-1}g(t)^{-1}) \\
&= g(a)g(s)^{-1} + g(b)g(t)^{-1} \\
&= \bar{g}\left(\frac{a}{s}\right) + \bar{g}\left(\frac{b}{t}\right)
\end{aligned}$$

Por otro lado,

$$\begin{aligned}\bar{g}\left(\frac{a}{s}\cdot\frac{b}{t}\right) =& \bar{g}\left(\frac{ab}{st}\right)\\ =& g(ab)g(st)^{-1}\\ =& g(a)g(b)g(s)^{-1}g(t)^{-1}\\ =& (g(a)g(s)^{-1})(g(b)g(t)^{-1})\\ =& \bar{g}\left(\frac{a}{s}\right)\bar{g}\left(\frac{b}{t}\right)\end{aligned}$$

Además,

$$\bar{g}\left(\frac{1}{1}\right) = g(1)g(1)^{-1} = 1$$

El siguiente paso es ver que $\bar{g}\circ f = g$. Para esto, dado $a \in R$,

$$\bar{g}\circ f(a) = \bar{g}\left(\frac{a}{1}\right) = g(a)g(1)^{-1} = g(a)$$

Lo único que falta demostrar es la unicidad. Para esto suponga que $l : S^{-1}R \to A$ es otro morfismo tal que $l\circ f = g$. Recuerde que todo elemento $\frac{a}{s} \in S^{-1}R$ se escribe como

$$\frac{a}{s} = f(a)f(s)^{-1}$$

Entonces

$$\begin{aligned}l\left(\frac{a}{s}\right) =& l(f(a)f(s)^{-1})\\ =& l(f(a))k(f(s)^{-1})\\ =& g(a)g(s)^{-1}\\ =& \bar{g}(\frac{a}{s})\end{aligned}$$

□

Una vez que se ha caracterizado la construcción del anillo de fracciones, se va a proceder a estudiar ejemplos.

EJEMPLO 34. *Si $S \subseteq R$ es un conjunto multiplicativo tal que $0 \in S$, entonces*

$$S^{-1}R = 0$$

.

Por esta razón en muchos libros se suele pedir que el conjunto multiplicativo no tenga al cero (lo cual es equivalente a decir que no tenga nilpotentes), pues como muestra el ejemplo, en este caso la construcción se trivializa.

EJEMPLO 35. *Si $f \in R$, al considerar el conjunto multiplicativo $S = \{f^n : n \in \mathbb{N}\}$, se suele denotar $R_f := S^{-1}R$. La intuición dice que en R_f se están invirtiendo todas las potencias de f, y en efecto se puede demostrar que*

$$R_f \cong R\left[\frac{1}{f}\right]$$

Al considerar este isomorfismo observe que cuando $R = \mathbb{Z}$ y $S = \{2^n : n \in \mathbb{N}\}$, entonces

$$R_2 \cong \mathbb{Z}\left[\frac{1}{2}\right]$$

Observe que $\mathbb{Z}[\frac{1}{2}]$ es lo que se conoce como el anillo de los enteros diádicos. Además este ejemplo muestra que en general el anillo de fracciones no es un campo pues $3 \in \mathbb{Z}[\frac{1}{2}]$ y $3 \notin U(\mathbb{Z}[\frac{1}{2}])$.

EJEMPLO 36. *Si $\mathfrak{p} \leq R$ es un ideal primo, para el conjunto $S = R\backslash\mathfrak{p}$ se tiene que $R_\mathfrak{p} := S^{-1}R$. A este anillo de fracciones se le conoce como la localización de R en el primo $\mathfrak{p}$, y geométricamente corresponde a tomar vecindades sobre el punto $\mathfrak{p}$.*
En particular si R es dominio entero, $S = R\backslash 0$ es multiplicativo. Este caso particular generaliza a $R = \mathbb{Z}$ y se suele denotar

$$Frac(R) := R_0$$

En este caso, el anillo de fracciones es un campo y se le conoce como el ***campo de fracciones o cocientes*** *del dominio R. Además note que R se encaja en $Frac(R)$. En particular $\mathbb{Q}$ es el campo de cocientes de $\mathbb{Z}$.*

EJEMPLO 37. *Si k es un campo, $Frac(k[x]) = k(x)$ es el campo de funciones racionales de $k[x]$.*

EJEMPLO 38. *Considere el dominio $Z[\sqrt{2}] \subseteq \mathbb{R}$. Dado que $\frac{\sqrt{2}}{2} \in Frac(Z[\sqrt{2}])$ y obviamente $\mathbb{Q} \subseteq Frac(\mathbb{Z}[\sqrt{2}])$, entonces*

$$Frac(\mathbb{Z}[\sqrt{2}]) = \mathbb{Q}(\sqrt{2}).$$

Este mismo cálculo se generaliza al tomar cualquier raíz de un entero positivo no 1 libre de cuadrados.

EJEMPLO 39. *Un ejemplo mas elaborado se obtiene al considerar $U \subseteq \mathbb{C}$ un abierto conexo. Como consecuencia del teorema de factorización de Weierstrass el campo de fracciones de funciones holomorfas en U es el campo de funciones meromorfas en U.*

El ejemplo 36 es importante pues además de darnos una forma de generar ejemplos donde el anillo de fracciones es un campo, introduce una forma de dar ejemplos de un tipo especial de anillos, introducidos anteriormente, a saber, los anillos locales. Recordamos la definición básica.

DEFINICIÓN 52. *Un anillo R se llama local si este tiene un unico ideal máximo. Se suele denotar a un anillo local como una pareja $(R, \mathfrak{m})$ donde $\mathfrak{m}$ es el único ideal máximo de R. A $R/\mathfrak{m}$ se le llama el campo de residuos de R.*

PROPOSICIÓN 75. *Si $\mathfrak{p} \leq R$ es primo, entonces la localización $R_{\mathfrak{p}}$ es un anillo local con ideal máximo $\mathfrak{p}R_{\mathfrak{p}}$.*

DEMOSTRACIÓN. Por la proposición 56 basta con ver que $R_{\mathfrak{p}} \backslash \mathfrak{p}R_{\mathfrak{p}} \subseteq U(R_{\mathfrak{p}})$. En efecto, si $\frac{a}{s} \notin \mathfrak{p}R_{\mathfrak{p}}$, entonces $a \notin \mathfrak{p}$. Así $\frac{s}{a} \in R_{\mathfrak{p}}$ y $\frac{s}{a} = (\frac{a}{s})^{-1}$. □

A continuación se va a discutir un ejemplo concreto de esto.

EJEMPLO 40. *Considere $R = \mathbb{Z}$ y $\mathfrak{p} = 5\mathbb{Z}$. Observe que*

$$R_{\mathfrak{p}} \cong \{\frac{a}{b} \in \mathbb{Q} \ : \ s \nmid b\}$$

De acuerdo al resultado anterior

$$\mathfrak{p}R_{\mathfrak{p}} \leq R_{\mathfrak{p}}$$

es el único ideal máximo. En este caso

$$\mathfrak{p}R_{\mathfrak{p}} \cong \{\frac{a}{b} \in \mathbb{Q} : 5 \nmid b, \ 5|a\} = 5R_{\mathfrak{p}}$$

Para este caso, el campo de residuos de $(R_{\mathfrak{p}}, 5R_{\mathfrak{p}})$ es

$$R_{\mathfrak{p}}/5R_{\mathfrak{p}} \cong \mathbb{Z}/5\mathbb{Z} \cong \mathbb{Z}_5$$

Para concluir esta sección, vamos a regresar a un resultado de polinomios, el cual muestra la idea básica de como se generalizan los resultados de irreducibiidad para polinomios estudiados en la primera sección del presente capítulo. La idea por la que estos funcionan es que $\mathbb{Z}$ tiene por campo de fracciones a $\mathbb{Q}$, por lo que básicamente las generalizaciones se obtienen al cambiar $\mathbb{Z}$ por un dominio entero y $\mathbb{Q}$ por el campo de fracciones de dicho

dominio. Este tipo de resultados aparecen en los ejercicios y vale la pena checar el ejercicio 78 que se usará para la siguiente prueba.

PROPOSICIÓN 76. *Sea R un DFU, $k = Frac(R)$ y $f = \sum_{i=0}^{n} a_i x \in R[x]$ tiene una raíz $\frac{b}{c} \in k$ con $\langle b, c\rangle = R$. Entonces, $b|a_0$ y $c|a_n$. Además, si $\partial(f) \leq 3$, entonces $f \in k[x]$ es irreducible si y sólo si f no tiene raices en k.*

DEMOSTRACIÓN. Dado que $f(\frac{b}{c}) = 0$, entonces $c^n a_0 + a_1 c^{n-1} b + ... + a_n b^n = 0$. Esto implica que $b \mid c^n a_0$ y por el ejercicio 78 se deduce que $b|a_0$. Además de esta igualdad también se deduce que $c \mid a_n b^n$ y por dicho ejercicio nuevamente $c \mid a_n$.

Para la segunda afirmación, la ida es clara por contrapositiva. Para el regreso, si $f \in k[x]$ no tiene raíces, observe que $k[x]$ es un DFU. Al factorizar $f = gh$ con $g, h \in k[x]$, nótese que dado que $\partial(f) \leq 3$, ambos polinomios no pueden tener grado mayor a 1 pues en tal caso alguno de ellos está obligado a tener grado exactamente 1, lo cual debe ser imposible pues en ta caso la raíz de dicho polinomio debe ser raíz de f. □

6. Ejercicios del capítulo

En esta parte de la tarea R es un anillo conmutativo (unitario) y k es un campo.

EJERCICIO 71. *Sean $f, g \in R[x]$. Demuestre que fg es primitivo si y sólo si f y g son primitivos.*

EJERCICIO 72. *Sea $n > 1$*

1. *Determinar las unidades de $R[x_1, ..., x_n]$*
2. *Determinar los elementos nilpotentes de $R[x_1, ..., x_n]$*
3. *Determinar los elementos divisores de cero de $R[x_1, ..., x_n]$*

EJERCICIO 73. *Sea R un anillo y $R[[x]]$ el anillo de series formales de potencias con coeficientes en R. Considere $f = \sum_{i=0}^{\infty} a_i x^i$. Demuestre lo siguiente:*

1. *$f \in U(R[[x]])$ si y sólo si $a_0 \in U(R)$*

2. *Si f es nilpotente, entonces para cualquier $n \in \mathbb{N}$, a_n es nilpotente. ¿Es cierta la afirmación recíproca?*
3. *$f \in J(R[[x]])$ si y sólo si $a_0 \in J(R)$*
4. *La contracción de un ideal máximo de $\mathfrak{m} \leq R[[x]]$ es un ideal máximo de R y $\mathfrak{m}$ es generado por $\mathfrak{m}^e$ y x*
5. *Todo ideal primo de R es contracción de un ideal primo de $R[[x]]$*

EJERCICIO 74. *Sea $p \in \mathbb{N}$ un primo. Definimos el **p-ésimo polinomio ciclotómico** sobre $\mathbb{Z}$, se define como*

$$\Phi_p = \sum_{i=0}^{p-1} x^i$$

Demuestre que Φ_p es irreducible sobre $\mathbb{Z}[x]$ y $\mathbb{Q}[x]$.

EJERCICIO 75.

1. *Demuestre que un polinomio $f \in k[x]$ de grado 2 o 3 es reducible si y sólo si f tiene un cero en k.*
2. *Pruebe que el polinomio $f = x^4 + 2x^2 + 9 \in \mathbb{Q}[x]$ no tiene ceros racionales, pero es reducible en $\mathbb{Q}[x]$.*

EJERCICIO 76. *Demuestre que si la reducción de un polinomio mónico $f \in \mathbb{Z}[x]$ usando un número primo $p \in \mathbb{N}$ es irreducible en $\mathbb{Z}_p[x]$, entonces $f \in \mathbb{Q}[x]$ es irreducible.*

EJERCICIO 77.

1. *Sean $f,g,h \in \mathbb{C}[t]$ primos relativos por pares tales que $f+g=h$. Denote por $V(fgh) = \{x \in \mathbb{C} \mid (fgh)(x) = 0\}$. Demuestre que: $\max\{\partial(f), \partial(g), \partial(h)\} \leq |V(fgh)| - 1$*
2. *(Teorema de Fermat para polinonios) Si $f,g,h \in \mathbb{C}[t]$ son polinomios primos relativos por pares con alguno de grado mayor o igual a1 y además $f^n + g^n = z^n$, entonces $n \leq 2$.*

EJERCICIO 78. *Para un dominio entero R sean $a,b,c \in R$ tales que $a \mid bc$ y $\langle a,b\rangle = R$. Demuestre que $a \mid c$.*

EJERCICIO 79. *¿Es la extensión de un ideal primo un ideal primo?*

EJERCICIO 80. *Sea $I \leq R$ propio. Demuestre que existe $\mathfrak{m} \leq R$ máximo tal que $I \subseteq \mathfrak{m}$*

EJERCICIO 81. *Suponga que $x \notin U(R)$. Demuestre que existe $\mathfrak{m} \leq R$ máximo tal que $x \in \mathfrak{m}$*

EJERCICIO 82. *Dar 5 ejemplos de ideales primos en $\mathbb{Z}[x,y]$, donde x y y son indeterminadas. Dar 2 ejemplos de ideales máximos de $\mathbb{Z}[x,y]$, y 2 ejemplos de ideales máximos de $\mathbb{Q}[x,y]$.*

EJERCICIO 83. *Hipótesis y notación del ejercicio **??**. Denotar por $Max(C_0([a,b]))$ al conjunto de ideales máximos del anillo $C_0([a,b])$. Defina una función $\mu : [a,b] \to Max(C_0([a,b]))$ mediante $\mu(x) = \mathfrak{m}_x$. Demuestre lo siguiente:*

1. *μ es inyectivo*
2. *μ es suprayetivo. Sugerencia: Para $\mathfrak{m} \in Max(C_0([a,b]))$, considere $V(\mathfrak{m}) = \{x \in [a,b] \mid \forall f \in \mathfrak{m}(f(x) = 0)\}$. Demuestre que $V(\mathfrak{m}) \neq \emptyset$. Tome $x \in V(\mathfrak{m})$ y demuestre que $\mathfrak{m} = \mathfrak{m}_x$*

EJERCICIO 84. *Considérese el anillo $\mathbb{Z}[\phi]$, donde ϕ es la razón áurea. Demuestre que todo ideal máximo en dicho anillo es principal.*

EJERCICIO 85. *Sea R un anillo conmutativo con un único ideal primo $\mathfrak{p}$. Demuestre que todo divisor de cero de R es nilpotente.*

EJERCICIO 86. *Sea $f \in k[x]$. Demuestre que f es irreducible si y sólo si $\langle f\rangle \leq k[x]$ es máximo. Concluir de esto que en $k[x]$ todo ideal primo es máximo.*

EJERCICIO 87. *Sean k un campo y $a_1,...,a_n \in k$.*

1. *Demuestre que $\langle x_1 - a_1,...,x_n - a_n\rangle \leq k[x_1,...,x_n]$ es un ideal máximo.*
2. *Pruebe mediante un ejemplo que existen ideales máximos en $k[x_1,...,x_n]$ que no tienen la forma del ideal del inciso anterior.*
3. *Demuestre que si $k = \mathbb{C}$, todo ideal máximo es de la forma propuesta en el inciso 1.*

EJERCICIO 88. *Sea $\mathfrak{p} \leq R_1 \times R_2$. Demuestre que $\mathfrak{p}$ es primo si y sólo si existe $\mathfrak{q}_2 \leq R_2$ tal que $\mathfrak{p} = R_1 \times \mathfrak{q}_2$ ó $\mathfrak{q}_1 \leq R_1$ tal que $\mathfrak{p} = \mathfrak{q}_1 \times R_2$.*

EJERCICIO 89. *Demuestre que si $\mathfrak{p} \leq R$ es primo, entonces $\mathfrak{p}[x] \leq R[x]$ y $\mathfrak{p}[[x]] \leq R[[x]]$ son primos.*

EJERCICIO 90. *Demuestre que $(\sqrt{I},I) = \bigcap\{\mathfrak{p} \leq R \mid I \subseteq \mathfrak{p},\ J \nsubseteq \mathfrak{p},\ \mathfrak{p}\ primo\}$*

EJERCICIO 91. *Considere $\mathbb{Z}[x]$, $p \in \mathbb{Z}$ primo y considere el ideal $I = \{\sum_{i=0}^{n} a_i x^i \mid p|a_i\}$. Demuestre que $\mathbb{Z}[x]/I$ es un DIP.*

EJERCICIO 92.

1. *Sea $\mathfrak{m} \leq R[[x_1,...,x_n]]$ un ideal máximo. Demuestre que $\langle x_1,...,x_n\rangle \subseteq \mathfrak{m}$. ¿Qué sucede con la afirmación análoga para el anillo $R[x_1,...,x_n]$?*
2. *Sea $\mathfrak{m} \leq R[[x_1,...,x_n]]$ un ideal máximo. Demuestre que $\mathfrak{m} \cap R \leq R$ es un ideal máximo.*

EJERCICIO 93. *Sea R un DIP y $\mathfrak{p} \leq R$ primo distinto de cero y R. Demuestre lo siguiente:*

1. *$\mathfrak{p}$ está generado por un elemento irreducible*
2. *$\mathfrak{p}$ es un ideal máximo.*

EJERCICIO 94. *Determinar los ideales primos en los siguientes anillos*

1. $\mathbb{Z}$
2. $k[x]$

EJERCICIO 95. *Determinar los elementos primos de los siguientes conjuntos.*

1. *Para k campo*
2. *Para* $\mathbb{Z}$
3. *Para* $\mathbb{R}[x]$
4. *Para* $\mathbb{C}[x]$

EJERCICIO 96. *Suponga que* $R \neq 0$*. Demuestre que todo ideal primo contiene un ideal primo* $\subseteq$*-mínimo.*

EJERCICIO 97. *Sea R un anillo sin nilpotentes y con un número finito de ideales primos mínimos* $\mathfrak{p}_1, ..., \mathfrak{p}_n$*. Probar que el morfismo* $R \to \prod_{i=1}^{n} R/\mathfrak{p}_i$ *es inyectivo. Más aún, la imagen tiene intersección no cero con cada uno de los anillos del producto.*

DEFINICIÓN 53. *Sea* $J \leq R$ *un ideal propio. Decimos que J es* ***primario*** *si para cualesquiera* $x, y \in R$ *tales que* $xy \in J$ *y* $x \notin J$*, se tiene que existe* $n \in \mathbb{N}^*$ *tal que* $y^n \in J$*.*

EJERCICIO 98. *Sea* $J \leq R$*. Demuestre lo siguiente:*

1. *J es primario si y sólo si los divisores de cero de* R/J *son nilpotentes.*
2. *Si J es primario, entonces* $\sqrt{J}$ *es primo.*

EJERCICIO 99. *Sea A un DFU. Demuestre que si todo ideal primo es principal, entonces A es un DIP. ¿Es cierta la afirmación si se reemplaza la hipótesis por ideales máximos?*

EJERCICIO 100. *Sea* $f : R \to S$ *un morfismo de anillos,* $I \leq R$ *y* $J \leq S$*. Demuestre lo siguiente:*

1. $\sqrt{J}_f = \sqrt{J_f}$

2. $(\sqrt{I})^f \subseteq \sqrt{J^f}$

EJERCICIO 101. *Sea $n \in \mathbb{Z}\backslash U(\mathbb{Z})$. Demuestre que $\sqrt{n\mathbb{Z}} = m\mathbb{Z}$ con m el producto de todos los factores primos distintos que dividen a n.*

EJERCICIO 102. *Considere el ideal $\langle x_1^2, x_1x_2\rangle \leq k(x_1,x_2)$. Determinar $\sqrt{I}$*

EJERCICIO 103. *Demuestre que en R el conjunto de divisores de cero es unión de ideales primos.*

EJERCICIO 104. *Supóngase que R tiene divisores de cero. Demuestre que R tiene elementos nilpotentes distintos de cero ó más de un ideal primo mínimo.*

EJERCICIO 105. *Demuestre que las siguientes definiciones son equivalentes:*

1. *R tiene un único ideal primo*
2. *$R = U(R) \cup N(R)$*
3. *$R/N(R)$ es un campo*

EJERCICIO 106. *Demuestre que $I \leq R$ es radical si y sólo si R/I es un anillo reducido.*

EJERCICIO 107.

1. *¿Es la suma de ideales radicales un ideal radical?*
2. *¿Es la intersección de ideales radicales un ideal radical?*

EJERCICIO 108. *Sea $I \leq R$ un ideal. Demuestre que I es radical si y sólo si I es intersección de ideales primos.*

EJERCICIO 109. *Sea $I \leq R$ tal que $I \subseteq N(R)$. Demuestre que si $x \in R$ es tal que $x+I \in U(R/I)$, entonces $x \in U(R)$.*

EJERCICIO 110. *Sea R un anillo y sea $R_{red} := R/N(R)$. Demostrar lo siguiente:*

1. *R_{red} es reducido*
2. *Si existe un morfismo de anillos $R \to S$ un morfismo de anillos con S reducido, este se factoriza de forma única a partir de R_{red}*

EJERCICIO 111. *Considere el anillo de polinomios $k[x,y]$ con k un campo, y sea $R = k[x,y]/\langle x - xy^2, y^3\rangle$. Sean $\overline{x}, \overline{y}$ las clases de residuos de x, y en R. Demostrar lo siguiente:*

1. *$N(R) = \langle \overline{x}, \overline{y}\rangle$. Más aún, este es el único ideal primo de R.*
2. *$R_{red} \cong k$*

EJERCICIO 112. *Demuestre que el nilradical de $R[x]$ es igual a su radical de Jacobson.*

EJERCICIO 113. *Encuentre un anillo R y un conjunto multiplicativo S tal que la relación $(a,b) \sim (b,t)$ si y sólo si $at - bs = 0$, no sea una relación de equivalencia.*

EJERCICIO 114. *Sea $S \subseteq R$ un conjunto multiplicativo e $I \leq R$ un ideal tal que $I \cap S = \emptyset$. Demuestre que existe $\mathfrak{p} \leq R$ primo tal que $I \subseteq \mathfrak{p}$ y $\mathfrak{p} \cap S = \emptyset$.*

EJERCICIO 115. *Demuestre que los únicos idenpotentes en un anillo local son 0 y 1.*

EJERCICIO 116. *Sea R un DFU y $k = Frac(R)$. Demuestre que $f \in R[x]$ es irreducible si y sólo si $f \in k[x]$ es primitivo e irreducible.*

EJERCICIO 117. *Sea R un dominio entero y $S \subseteq R$ un conjunto multiplicativo tal que $0 \notin S$. Demuestre que el morfismo canónico $f : R \to S^{-1}R$ es inyectivo y que $S^{-1}R$ es isomorfo como anillo unitario a un subanillo unitario del campo de fracciones de R.*

EJERCICIO 118. *Sean R un DFU, $k = Frac(R)$ y $f = \sum_{i=0}^{n} a_i x^i \in R[x]$. Demuestre lo siguiente:*

1. *Si existe $p \in R$ primo tal que $p \mid a_0, \ldots, a_{n-1}$, $p \nmid a_n$ y $p^2 \nmid a_0$, entonces $f \in k[x]$ es irreducible.*
2. *Si existe $p \in R$ primo tal que $p \mid a_1, \ldots, a_n$, $p \nmid a_0$ y $p^2 \nmid a_n$, entonces $f \in k[x]$ es irreducible.*

EJERCICIO 119. *Demuestre que el polinomio $f = y^3 + x^2y^2 + xy + x \in k[x,y]$ es irreducible. Sugerencia: Usar el criterio de Eisenstein (ejercicio 118) de forma adecuada.*

EJERCICIO 120. *Sea R un DFU y $k = Frac(R)$. Demuestre que $f \in R[x]$ es mónico y existe $p \in R$ irreducible tal que $\overline{f} \in R/\langle p \rangle[x]$ es irreducible, entonces $f \in k[x]$ es irreducible.*

EJERCICIO 121. *Sea R un dominio entero y $p \in R$ un elemento primo. Pruebe que si R_p es un DFU, entonces R también lo es.*

EJERCICIO 122. *Sea $K = Frac(k[x])$ y $u \in K$. Demuestre que $K = k(u)$ si y sólo si $u = \frac{ax+b}{cx+d}$ para algunos $a,b,c,d \in k$ tales que $ad - bc \neq 0$.*

EJERCICIO 123. *(Truco de Rabonowicz) Sea $x \in A$. Demuestre que la asignación $\varphi : A[t]/\langle xt - 1 \rangle \to A_x$ definida mediante*

$$\varphi\left(\sum_{k=0}^{n} a_k t^k\right) = \sum_{k=0}^{n} \frac{a_k}{x^k}$$

es una función. Más aún, es un isomorfismo de anillos.

EJERCICIO 124. *Sea $A = k[x_1, x_2]/\langle x_1 x_2 \rangle$ y $S = \{x_1^n \mid n \in \mathbb{N}\}$. Demuestre que*

$$S^{-1}A \cong k[t, t^{-1}]$$

EJERCICIO 125. *Sea $S \subseteq R$ un conjunto multiplicativo.*

1. *Defina* $\hat{S} = \{a \in R \mid \exists b \in R(ab \in S)\}$. *Demuestre que* $\hat{S}$ *es un conjunto multiplicativo y que* $\hat{S} = \{a \in R \mid a \in U(S^{-1}R)\}$.
2. *Demuestre que* $S^{-1}R = \hat{S}^{-1}A$ *y que además, si* $T \subseteq R$ *es un conjunto multiplicativo tal que* $S^{-1}R = T^{-1}R$ *, entonces* $T \subseteq \hat{S}$.

DEFINICIÓN 54. *Una valuación sobre un dominio entero A es una función* $u : A \to \overline{\mathbb{R}}$ *que satisface las propiedades:*

1. $u(x) = \infty$ *si y sólo si* $x = 0$
2. *Para cualesquiera* $x, y \in A$, $u(x+y) \geq \min\{u(x), u(y)\}$
3. *Para cualesquiera* $x, y \in A$, $u(xy) = u(x) + u(y)$

EJERCICIO 126. *Sea* $u : A \to \overline{\mathbb{R}}$ *una valuación y* $k = Frac(A)$. *Defina una asignación* $v : k \to \overline{R}$ *mediante la regla de corresopondencia:*

$$v\left(\frac{a}{b}\right) = u(a) - u(b)$$

Demuestre lo siguiente:

1. *v es una función. Más aún, esta es una valuación en k.*
2. $im(v)$ *es un subgrupo de* $(\mathbb{R}, +)$.

EJERCICIO 127. *Sea* $(R, \leq)$ *un dominio entero ordenado. Demuestre que el orden de R se extiende de manera única a su campo de fracciones.*

EJERCICIO 128. *Sea* $(R, \mathfrak{m})$ *un anillo local. Demuestre que si* $I \leq R$ *es finitamente generado e* $I\mathfrak{m} = I$, *entonces* $I = 0$.

EJERCICIO 129. *Sea* $S \subseteq R$ *multiplicativo. Demuestre las siguientes afirmaciones:*

1. *Si* $I \leq R$, *entonces* $IS^{-1}R \leq S^{-1}R$. *Más aun, si* $\mathfrak{p} \leq R$ *es primo, entonces* $\mathfrak{p}S^{-1}R \leq S^{-1}R$ *es primo.*
2. *Todo ideal de* $S^{-1}R$ *tiene la forma* $IS^{-1}R$ *con* $I \leq R$

3. *Todo ideal primo de $S^{-1}R$ tiene la forma $\mathfrak{p}S^{-1}R$ con $\mathfrak{p} \leq R$ tal que $\mathfrak{p} \cap S = \emptyset$*

EJERCICIO 130. *Sea $S \subseteq R$ un conjunto multiplicativo e $I \leq R$. Sea $\overline{S} = f(S)$, con $f : R \to S^{-1}R$, el morfismo canónico. Demuestre que $\overline{S}$ es un conjunto multiplicativo y que $S^{-1}R/IS^{-1}R \cong \overline{S}^{-1}(R/I)$*

EJERCICIO 131. *Sea R un DFU, $k = Frac(R)$ y $f \in R[x]$ un polinomio mónico. Demuestre que $\alpha \in k$ es una raíz de f, entonces $\alpha \in R$.*

EJERCICIO 132. *Considere el anillo de polinomios con dos indeterminadas $R = \mathbb{C}[x,y]$. Además, sea $S = \{x^n y^m \mid n,m \in \mathbb{N}\}$.*

1. *Demuestre que S es un conjunto multiplicativo. Más aún, pruebe que $S^{-1}R \cong \mathbb{C}[x,y,x^{-1},y^{-1}]$*
2. *Describir los ideales máximos de $S^{-1}R$*

EJERCICIO 133. *Para un anillo conmutativo R y un ideal primo $\mathfrak{p} \leq R$, demuestre que hay un isomorfismo canoónico*

$$Frac(R/\mathfrak{p}) \cong R_{\mathfrak{p}}/\mathfrak{p}R_{\mathfrak{p}}$$

EJERCICIO 134. *Demuestra que:*

1. *Todo anillo local artiniano reducido es un campo.*
2. *Todo dominio entero artiniano es un campo.*

EJERCICIO 135. *Demuestre que son equivalentes:*

1. *R es neteriano*
2. *Todo ideal $I \leq R$ es finitamente generado*
3. *Toda familia no vacía de ideales tiene un elemento máximo.*

EJERCICIO 136. *Demuestre que un dominio entero neteriano R, todo elemento no cero o no unidad se puede expresar como producto de una unidad y potencias de elementos irreducibles.*

EJERCICIO 137. *Sea $R[[x]]$ el anillo de series formales de potencias con coeficientes en R. Defina una función, que se conoce como orden, $ord : R[[x]] \to \mathbb{N}$ cuya regla de correspondencia es la siguiente: Dado $f \in R[[x]]$ con la forma $f = \sum_{i=0}^{\infty} a_i x^i$, $ord(f) = \text{mín}\{n \mid a_n \neq 0\}$. Demuestre lo siguiente:*

1. *Si R es un dominio entero, entonces para cualesquiera $f, g \in R[[x]]$ se cumple que $ord(fg) = ord(f) + ord(g)$*
2. *Si $f \in R[[x]]$ con la forma $f = \sum_{i=0}^{\infty} a_i x^i$, entonces f es unidad si y sólo si $a_0 \in U(R)$*
3. *Si k es un campo, entonces $k[[x]]$ es un anillo local*
4. *Si R es noetheriano, entonces $R[[x]]$ es noeteriano.*

EJERCICIO 138. *Sean $f : U \to \mathbb{R}$ y $g : V \to \mathbb{R}$ funciones continuas con $U, V \subseteq \mathbb{R}$ vecindades del $0 \in \mathbb{R}$, donde $\mathbb{R}$ tiene la topología usual. Decimos que $f \sim g$, si existe $W \subseteq U \cap V$ vecindad del 0 tal que $f|_W = g|_W$.*

1. *Demuestre que $\sim$ es una ralación de equivalencia. A una clase de equivalencia de esta relación se le conoce como un germen en el cero.*
2. *Demuestre que el conjunto de gérmenes en 0 tiene estructura de anillo conmutativo y denótese a este por $\mathscr{E}_0$*
3. *Demuestre que $\mathscr{E}_0$ es un anillo local*
4. *¿Es $\mathscr{E}_0$ un anillo neteriano?*

EJERCICIO 139. *Sea $f : R \to R$ un morfismo suprayectivo de anillos con R neteriano. Demuestre que f es un isomorfismo.*

EJERCICIO 140. *Sea R un dominio entero artiniano. Demuestre que R es un campo. También pruebe que todo ideal primo en un anillo artiniano máximo.*

EJERCICIO 141. *Demuestre que si todos los ideales primos de un anillo R son finitamente generados, entonces R es neteriano.*

EJERCICIO 142. *Demuestre que si $S \subseteq R$ es un conjunto multiplicativo y R es neteriano (artiniano), entonces $S^{-1}R$ es neteriano (artiniano).*

EJERCICIO 143. *Para k un campo, considere $R = k[x, y, z_n]$ con $z_n = xy^{-n}$ y $n \in \mathbb{N}^+$. Demuestre que R no es un anillo neteriano.*

EJERCICIO 144. *¿Son los subanillos de una anillo neteriano neterianos? Demuestre o de un contraejemplo para esta afirmación.*

Capítulo 3

Teoría de Campos

En el presente capítulo se estudiarán los conceptos y definiciones básicas de la teoría de campos los cuales nos permitirán establecer la definición de extensión de Galois la cual nos permitirá a su vez establecer las bases para un primer acercamiento a la teoría de Galois clásica. Es importante decir que la teoría de Galois clásica trata de extensiones finitas, por tal razón nos centraremos en los conceptos en dimensión finita, aunque siempre que sea posible se establecerán las definiciones y resultados en el carácter mas general posible. Sin embargo, no daremos la teoría de Galois de dimensión infinita ya que dejando a un lado los requisitos algebraicos para esta(los cuales podríamos ver) esta requiere de tener ciertas ideas de grupos topológicos, cosa que no es un requisito del curso.
Con todo y esta reducción ls teoría que trataremos permitirá demostrar los teoremas clásicos relativos a teoría de Galois, a saber: la solubilidad por radicales y los problemas griegos clásicos, asi como otros tópicos también considerados básicos pero con menos fama a los antes mencionados, sin embargo, este tipo de resultados se tratarán hasta el siguiente capítulo que es propiamente de Teoría de Galois.

1. Extensiones algebraicas y el Teorema de Kronecker

DEFINICIÓN 55. *Un campo K es extensión de un campo k si k es un subcampo de K. En tal caso esto se va a denotar por*

$$K|k.$$

Una torre de campos $K|F_n|\cdots|F_1|k$ es una sucesión de campos tales que cada dos términos consecutivos definen una extensión de campos.

Observación. Si $K|k$ es una extensión de campos, note que K tiene estructura de k-espacio vectorial. Luego, definimos el **grado de la extensión** $K|k$ como $\dim_k K$, la cual se va a denotar por

$$[K:k]$$

Una extensión $K|k$ es finita si $[K:k] < \aleph_0$.

EJEMPLO 41. *La extensión $\mathbb{C}|\mathbb{R}$ es finita. De hecho,*

$$[\mathbb{C}:\mathbb{R}] = 2.$$

EJEMPLO 42. *La extensión $\mathbb{R}|\mathbb{Q}$ no es finita. De hecho, se puede demostrar que:*

$$[\mathbb{R}:\mathbb{Q}] = 2^{\aleph_0}$$

EJEMPLO 43. *Considere la extensión $\mathbb{Q}(i)|\mathbb{Q}$. Observe que como $i^2 = -1$, entonces*

$$[\mathbb{Q}(i);\mathbb{Q}] = 2.$$

EJEMPLO 44. *Considere la extensión $\mathbb{Q}(\sqrt[3]{2})|\mathbb{Q}$. Observe que $\{1, \sqrt[3]{2}, \sqrt[3]{4}\}$ es base de $\mathbb{Q}(\sqrt[3]{2})$ como $\mathbb{Q}-$espacio, por lo tanto dicha extensión es finita y además*

$$[\mathbb{Q}(\sqrt[3]{2});\mathbb{Q}] = 3.$$

EJEMPLO 45. *Sea $\omega \in \mathbb{C}$ una raíz n-ésima de la unidad primitiva, esto es $\langle\omega\rangle = \{e^{\frac{2\pi ik}{n}} \mid k \in \mathbb{Z}\}$. Siguiendo la lógica del ejemplo anterior, $\{1, \omega, \ldots, \omega^{n-1}\}$ es una base de $\mathbb{Q}(\omega)$ como $\mathbb{Q}$-espacio vectorial. Por lo tanto la extensión de campos $\mathbb{Q}(\omega)|\mathbb{Q}$ es finita y más aún*

$$[\mathbb{Q}(\omega);\mathbb{Q}] = n.$$

EJEMPLO 46. *Sea $\mathbb{Q}(\mu)$ el campo que se obtiene al adjuntar a $\mathbb{Q}$ todas las raíces n-ésimas de la unidad para $n \geq 2$. Entonces la extensión $\mathbb{Q}(\mu)|\mathbb{Q}$ es una extensión infinita. En este caso*

$$[\mathbb{Q}(\mu);\mathbb{Q}] = \aleph_0$$

Observe que si $K|k$ y $L|K$ son extensiones de campo, entonces $L|k$ es una extensión de campo. Más aún, se tiene el siguiente resultado que relaciona los grados de las extensiones en cuestión.

PROPOSICIÓN 77. *(Multiplicatividad del índice) Si $K|k$ y $L|K$ son extensiones de campo, entonces $L|k$ lo es y además*

$$[L:k] = [L:K][K:k]$$

DEMOSTRACIÓN. Basta con demostrar la afirmación respecto a los grados. Sean $\{x_j\}_{j\in\Lambda}$ una base de K como $k-$espacio y $\{\ell_a\}_{a\in\Gamma}$ una base de L como $K-$espacio. El resultado se sigue si se demuestra que el conjunto $\beta = \{\ell_a x_j \mid a\in\Gamma, j\in\Lambda\}$ es una base de L como $k-$espacio, pues todos los elementos de dicho conjunto son distintos entre sí por independencia lineal de $\{\ell_a\}_{a\in\Gamma}$.

Afirmación: β es linealmente independiente.

En efecto, veamos que todo subconjunto finito de β es l.i., por lo que suponga que

$$\sum_{s=1}^{n} \alpha_s \ell_{a(s)} x_{j(s)} = 0$$

con $\alpha_s \in k$. Note que

$$\sum_{s=1}^{n} \alpha_s \ell_{k(s)} x_{j(s)} = \sum_{s=1}^{n} (\alpha_s x_{j(s)}) \ell_{a(s)}$$

como $\alpha_s x_{j(s)} \in K$, por independencia lineal de $\{\ell_a\}_{a\in\Gamma}$ se deduce que para cualquier $s\in\{1,\dots,n\}$, $\alpha_s x_{j(s)} = 0$. Más aún, los elementos de $x_{j(s)}$ pertenecen a una base, por lo que son distintos de cero y así, para cualquier $s\in\{1,\dots,n\}$, $\alpha_s = 0$. Esto prueba la independencia lineal.

Afirmación: β es generador.

Es claro, pues si $y\in L$, dado que $\{\ell_a\}_{a\in\Gamma}$ son base de $L|K$, existen $\alpha_1,\dots,\alpha_n \in K$ y elementos de la base $\ell_{a(1)},\dots,\ell_{a(n)}$ tales que

$$y = \sum_{i=1}^{n} \alpha_i \ell_{a(i)}$$

Por otro lado, como cada $\alpha_i \in K$ y $\{x_j\}_{j\in\Lambda}$ son una base de K como $k-$espacio, existen $\mu_1^i,\dots,\mu_{m(i)}^i \in k$ y $x_{j(1)},\dots,x_{j(m)}$ en la base tales que

$$\alpha_i = \sum_{j=1}^{m(i)} \mu_j^i x_{i(j)}$$

entonces

$$y = \sum_{i=1}^{n}\sum_{j=1}^{m(i)} \mu_j^i x_{j(i)} \ell_{a(i)},$$

lo que concluye la prueba. □

Recuerde que en anillos de polinomios se puede hablar del máximo común divisor. Tenemos el siguiente resultado.

PROPOSICIÓN 78. *(Invariancia del mcd) Sea $K|k$ una extensión de campos y $f,g \in k[x]$. Entonces,*

1. *$f|g$ en $k[x]$ si y sólo si $f|g$ en $K[X]$.*
2. *$(f,g)_{k[x]} = (f,g)_{K[x]}$*
3. *f y g son primos relativos en $k[x]$ si y sólo si lo son en $K[x]$*

DEMOSTRACIÓN. Tarea □

Las siguientes observaciones que se quieren realizar son relativas a la retícula de subcampos de una extensión $K|k$, es decir, los **campos intermedios** entre K y k. Para esto, una primera observación de carácter general es que si E y K son campos tales que $E \subseteq K$ es subanillo, entonces E es subcampo, es decir, se tiene una extensión $K|E$. Teniendo en cuenta esta última observación note que todas las construcciones respecto a subanillos se pueden repetir para subcampos, por lo que dado un campo K, uno puede considerar la retícula de subcampos de K.

Una construcción con gran relevancia es el subcampo generado por un subconjunto $S \subseteq K$. Mas aún, en el caso de una extensión $K|k$, uno puede considerar el $\subseteq -$mínimo subcampo intermedio generado por un conjunto $S \subseteq K$ como el subcampo generado por

$$S \cup k$$

Dicho subcampo se denota por $k(S)$. Además, si $S = \{a_1, \ldots, a_n\}$, entonces dicho subcampo de denota mediante

$$k(a_1, \ldots, a_n) := k(S)$$

De acuerdo a un resultado del capítulo anterior o demostrando directamente las contenciones, se tienen los siguientes resultados.:

PROPOSICIÓN 79. *Para una extensión $K|k$ y $a_1, \ldots, a_n \in K$,*

$$k(a_1, \ldots, a_n) = \left\{ \frac{f(a_1, \ldots, a_n)}{g(a_1, \ldots, a_n)} \;\middle|\; f,g \in k[x_1, \ldots, x_n],\ g(a_1, \ldots, a_n) \neq 0 \right\}$$

PROPOSICIÓN 80. *Para una extensión $K|k$ y $a_1, \ldots, a_n \in K$. Se tiene*

$$k(a_1, \ldots, a_n) = k(a_1, \ldots, a_{n-1})(a_n)$$

Regresando a cuestiones retículares, considere campos intermedios $k \subseteq E$, $F \subseteq K$. Definimos el **compositum** de dichos campos como el $\subseteq -$mínimo subcampo intermedio que contiene a E y F. Este se denota por EF. Observe que la definición de compositum se extiende de manera obvia a cualquier colección de campos intermedios de $K|k$.

El resultado básico mas importante en torno a la operación definida se muestra a continuación.

PROPOSICIÓN 81. *Sea $K|k$ una extensión y considere campos intermedios $k \subseteq E$, $F \subseteq K$, tales que $[F:k] < \aleph_0$. Entonces,*

1. $EF = \left\{ \sum_{i=0}^{n} e_i f_i \mid n \in \mathbb{N}, \forall 0 \leq i \leq n (e_i \in E, f_i \in F,) \right\}$
2. $[EF:E] \leq [F:k]$
3. $[EF:k] \leq [E:k][F:k]$

DEMOSTRACIÓN. Como $[F:k] < \aleph_0$, considere $\beta \subseteq F$ base la cual es finita. Observe que si $A := \left\{ \sum_{i=1}^{n} e_i f_i \;\middle|\; n \in \mathbb{N}, \forall 0 \leq i \leq n (e_i \in E, f_i \in F) \right\}$, entonces β genera a A como un $E-$espacio vectorial. Por lo tanto,

$$dim_E A \leq [F:k] \tag{1}$$

Por otro lado, observe que A es un subanillo de K. Mas aún, es un dominio entero. Por un resultado previo esto implica que A es un campo. Como trivialmente A es un campo intermedio a la extensión $K|k$ y contiene a E y F, entonces

$$EF \subseteq A$$

Además, observe que claramente $A \subseteq EF$, por lo que se concluye que $A = EF$ y esto prueba 1. Mas aún, de esta ultima igualdad y la expresión (1) se deduce 2. Para 3, por multiplicatividad del indice y el inciso 2 de esta proposición,

$$[EF:k] = [EF:E][E:k] \leq [F:k][E:k]$$

□

Vale la pena comentar que la descripción del compositum dada en el resultado anterior, usa fuertemente el hecho de que $[F:k] < \aleph_0$. El siguiente ejercicio proporciona una descripción general de dicha operación.

EJERCICIO 145. *Para una extensión $K|k$ y campos intermedios $k \subseteq E$, $F \subseteq K$.*

$$EF = \left\{ \left(\sum_{i=1}^{n} e_i f_i \right) \left(\sum_{j=1}^{m} e'_j f'_j \right)^{-1} \;\middle|\; n \in \mathbb{N}, e_i e'_j \in E, f_i f j' \in F \right\}$$

Observación: Para una extensión $K|k$ y $a_1, \ldots, a_n \in K$,

$$k(a_1, \ldots, a_n) = k(a_1) \cdot \cdots \cdot k(a_n)$$

Al usar la observación anterior se puede dar un ejemplo que muestre que en la última proposición las desigualdades pueden ser estrictas. Para esto considere $k = \mathbb{Q}$, $E = \mathbb{Q}(\sqrt[3]{2})$,

$F = \mathbb{Q}(\sqrt[3]{4})$ y $K = \mathbb{R}$. Observe que $[F : k] = 3 < \aleph_0$.
Dado que $EF = \mathbb{Q}(\sqrt[3]{2})\mathbb{Q}(\sqrt[3]{4}) = \mathbb{Q}(\sqrt[3]{2})$, pues $\sqrt[3]{4} \in \mathbb{Q}(\sqrt[3]{2})$, entonces $[EF : E] = 1$. Por lo tanto $[EF : E] < [F : k]$. Ademas,

$$[EF : k] = [\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$$
$$[E : k] = 3$$
$$[F : k] = 3$$

Así que

$$[EF : k] < [E : k][F : k]$$

1.1. Extensiones algebraicas. El siguiente paso a dar es introducir un tipo especial de extensiones.

DEFINICIÓN 56. *Sea $K|k$ una extensión de campos.*

1. *Un elemento $\alpha \in K$ es algebraico sobre k si existe $0 \neq f \in k[x]$ tal que $f(\alpha) = 0$*
2. *Si $\alpha \in K$ no es algebraico sobre k, diremos que α es trascendente sobre k.*
3. *La extensión $K|k$ es algebraica si todo elemento $\alpha \in K$ es algebraico sobre k.*

Observación: Existe una noción para anillos que se puede considerar como la equivalente a la de elemento algebraico y extensión algebraica que se conoce como elemento entero y extensión entera.

EJEMPLO 47. *La extensión $k|k$ es siempre algebraica.*

EJEMPLO 48. *La extensión $\mathbb{R}|\mathbb{Q}$ no es algebraica pues $\pi \in \mathbb{R}$ es trascendente. Otro ejemplo típico que muestra la afirmación se da con $e \in \mathbb{R}$ es trascendente.*

EJEMPLO 49. *La extensión $\mathbb{C}|\mathbb{R}$ es algebraica. Para ver esto considere $z \in \mathbb{C}$ con $z = a + ib$. Observe que $(z-a)^2 = -b^2$. Por lo tanto $f := (x-a)^2 + b^2 \in \mathbb{R}[x]$ y satisface que $f(z) = 0$.*

El determinar si una extensión es algebraica o no puede ser complicado como se muestra en el ejemplo 48, pues demostrar que π o e son trascendentes es una tarea dificil. Uno de los criterios que permite obtener una fuente de ejemplos se presenta a continuación.

PROPOSICIÓN 82. *Toda extension finita es algebraica.*

DEMOSTRACIÓN. Sea $K|k$ una extensión finita, con $[K:k]=n$. Considere $\alpha \in K$. Observe que si existe $m \in \{1,\ldots,n\}$ tal que $\alpha^m = 1$, no hay nada que probar pues α es raíz del polinomio $f = x^m - 1$. En caso contrario el conjunto $\{1,\alpha,\alpha^2,\ldots,\alpha^n\}$ tiene $n+1$ elementos, por lo que es linealmente dependiente. Esto dice que existen $\lambda_0,\ldots,\lambda_n \in k$ tales que $\sum_{i=0}^{n} \lambda_i \alpha^i = 0$ con no todos los $\lambda_i = 0$. Entonces α es raíz del polinomio $f = \sum_{i=0}^{n} \lambda_i x^i$. □

Observación: Las extensiones de los ejemplos 41, 43, 44 y 45 son algebraicas pues estas son finitas. Note que muchos de estos ejemplos son extensiones finitas sobre $\mathbb{Q}$. Dichas extensiones son importantes en teoría de números y geometría aritmética; a estas se les conocen como **campos numéricos**.

El ejemplo 46 proporciona un ejemplo de una extensión algebraica que no es finita.

El siguiente resultado muestra un ejemplo no trivial de cuándo una extensión algebraica tiene que ser finita.

PROPOSICIÓN 83. *Sea $K|k$ una extensión de campos y $\alpha \in K$. Las siguientes afirmaciones son equivalentes:*

1. *α es algebraico sobre k*
2. *$k(\alpha)|k$ es finita*
3. *$k(\alpha) = k[\alpha]$*
4. *Existe una extensión finita $F|k$ tal que $\alpha \in F$*

DEMOSTRACIÓN. $1 \Rightarrow 2)$ Sea $f \in k[x]^*$ tal que $f(\alpha) = 0$. Observe que dado cualquier $g \in k[x]$, existen únicos $q,r \in k[x]$ tales que $g = qf + r$ con $r = 0$ ó $\partial r < \partial f$. De esto se deduce que $g(\alpha) = r(\alpha)$ y por lo tanto el conjunto $\{1,\alpha,\ldots,\alpha^{\partial f - 1}\}$ generan a $k[\alpha]$ como k-espacio, por lo cual este tiene dimensión finita. Entonces este es un campo y así se cumplen 2 (y de hecho 3).

$2 \Rightarrow 3)$ Dado que $k[\alpha] \subseteq k(\alpha)$ es un subanillo, este es un dominio y además tiene estructura de k-espacio de dimensión finita, luego este es un campo y por lo tanto se cumple la contención faltante en la igualdad.

$3 \Rightarrow 1)$ Por hipótesis existe $f \in k[x]$ tal que $\alpha^{-1} = f(\alpha)$. Observe que al definir $g = xf - 1 \in k[x]$, α es cero de dicho polinomio, lo que concluye la prueba.

Es claro que $2 \Rightarrow 4)$. Además, por multiplicatividad del índice $4 \Rightarrow 2$. □

Un importante resultado que se deduce del anterior y que es muy complicado de demostrar directamente de la definición se presenta a continuación.

PROPOSICIÓN 84. *Sea $K|k$ una extensión de campos y defina $A = \{\alpha \in K \mid \alpha$ es algebraico sobre $k\}$. Entonces A es una extensión intermedia.*

DEMOSTRACIÓN. Observe que $k \subseteq A \subseteq K$. Por lo tanto, lo que se quiere probar es que A es subcampo de K. Entonces consideremos $\alpha, \beta \in A$. Del resultado anterior $k(\alpha), k(\beta)|k$ son finitas. Observe que $\alpha^{-1}, \alpha - \beta, \alpha\beta \in k(\alpha)k(\beta) = k(\alpha, \beta)$. Además $[k(\alpha,\beta) : k] < \aleph_0$ por un resultado previo. De esto se deduce que las extensiones $k(\alpha^{-1})|k$, $k(\alpha - \beta)|k$, $k(\alpha\beta)|k$ son finitas y por lo tanto, del resultado anterior se deduce que $\alpha^{-1}, \alpha - \beta, \alpha\beta$ son algebraicos sobre k, lo que concluye la prueba. □

Otro importante resultado con exactamente la misma estrategia de prueba al anterior se presenta a continuación.

PROPOSICIÓN 85. *Considere una torre de extensiones $K|E|k$. Entonces, $K|k$ es algebraica si y sólo si $K|E$, $E|k$ son algebraicas.*

DEMOSTRACIÓN. $\Rightarrow$) Es claro.

$\Leftarrow$) Sea $\alpha \in K$. Como $K|E$ es algebraica, existe $f \in E[x]^*$, digamos $f = \sum_{i=0}^{n} e_i x^i$, tal que $f(\alpha) = 0$. Como cada $e_i \in E$ es algebraico sobre k, las extensiones $[k(e_i) : k] < \aleph_0$. Esto implica que $[k(e_0, \ldots, e_n) : k] < \aleph_0$. Además, $\alpha \in K$ es algebraico sobre $k(e_0, \ldots, e_n)$, lo que implica que $k(e_0, \ldots, e_n)(\alpha)|k$ es finita y por lo tanto algebraica. De esto se deduce que α es algebraico sobre k □

1.2. Polinomio mínimo. En esta subsección, los últimos resultados a tratar tienen que ver con un polinomio que se le puede asociar a cualquier elemento algebraico.

PROPOSICIÓN 86. *Sea $K|k$ una extensión de campos y $\alpha \in K$ algebraico sobre k. Entonces, existe un único generador mónico del ideal $\{f \in k[x] \mid f(\alpha) = 0\}$. Dicho generador coincide con:*

1. *El mínimo polinomio mónico respecto al grado tal que*

$$f(\alpha) = 0$$

2. *El único polinomio mónico irreducible tal que*

$$f(\alpha) = 0$$

DEMOSTRACIÓN. Como observación inicial note que el conjunto mencionado es en efecto un ideal pues es igual a $nuc(ev_\alpha)$. La existencia del polinomio es consecuencia de que $k[x]$ es un DIP y de que si $g \in k[x]$ genera al ideal $\{f \in k[x] \mid f(\alpha) = 0\}$ y este no es mónico, al multiplicar g por el inverso de su coeficiente principal se obtiene el generador deseado. La unicidad se deduce del hecho de que dos elementos que generan al mismo ideal deben ser asociados y al ser mónicos, el coeficiente entre ambos debe ser 1.

Sea m el único generador mónico del ideal $\{f \in k[x] \mid f(\alpha) = 0\}$ y sea $m_0 \in k[x]$ el mínimo polinomio mónico respecto al grado tal que $m_0(\alpha) = 0$. Como $m_0 \in \{f \in k[x] \mid f(\alpha) = 0\} = \langle m \rangle$, entonces existe $p \in k[x]$ tal que $m_0 = pm$. Dado que m_0 es mínimo respecto al grado entre los polinomios que tienen a α por raíz, $\partial(p) = 0$, es decir, p es un polinomio constante. Al ser m_0 y m moñicos, se deduce que $p = 1$.

Ahora considere m_1 el polinomio mónico irreducible tal que

$$m_1(\alpha) = 0$$

como $m_1 \in \{f \in k[x] \mid f(\alpha) = 0\} = \langle m \rangle$ existe $p \in k[x]$ tal que

$$m_1 = pm$$

Al ser m_1 irreducible y m no constante, p tiene que ser unidad, por lo que p es un polinomio constante. Al usar que m_1 y m son mónicos, se deduce que $p = 1$ y se concluye la prueba del resultado. □

DEFINICIÓN 57. *El polinomio que satisface una, y por lo tanto todas las condiciones del resultado anterior, se conoce como polinomio mínimo de α y se denota por*

$$min_k(\alpha).$$

EJEMPLO 50. *Sea $K|k$ extensión de campo y $\alpha \in K$. $min_k(\alpha) = x - \alpha$ si y sólo si $\alpha \in k$.*

Observación: En la notación del polinomio mínimo es importante indicar el campo base que se esta tratando[1] pues

$$min_{\mathbb{R}}(i) = x^2 + 1$$
$$min_{\mathbb{C}}(i) = x - i$$

El siguiente resultado tiene distintas ideas en torno al polinomio mínimo de un elemento algebraico, incluso un ejemplo donde este se puede calcular.

PROPOSICIÓN 87. *Sea $K|k$ extensión y $\alpha \in K$ algebraico sobre k. Denote por $d = \partial(min_k(\alpha))$. Entonces,*

1. $\beta = \{1, \alpha, \ldots, \alpha^{d-1}\} \subseteq k(\alpha)$ *es base. Por lo tanto,*
$$[k(\alpha) : k] = d$$
2. *La función $T : k(\alpha) \to k(\alpha)$ cuya regla de correspondencia es $T(x) = \alpha x$, es lineal sobre k. Mas aún, $min_k(\alpha) = p_T$, con $p_T \in K[x]$ el polinomio característico de T.*

DEMOSTRACIÓN. Suponga que $\sum_{i=0}^{d-1} \lambda_i \alpha^i = 0$ con $\lambda_i \in k$. Observe que al considerar $\sum_{i=0}^{d-1} \lambda_i x^i \in k[x]$, este polinomio no puede ser distinto de cero, pues en caso contrario se puede construir de el un polinomio mónico que anula a α con menor grado que $min_k(\alpha)$. Por lo tanto, todos los $\lambda_i = 0$ y así β es linealmente independiente.

Observe que el morfismo evaluación en α,

$$ev_\alpha : k[x] \to k[\alpha],$$

es suprayectivo. El primer teorema de isomorfismo implica que

$$k[x]/Nuc(ev_\alpha) \cong k[\alpha]$$

Recuerde que $Nuc(ev_\alpha) = \langle min_k(\alpha) \rangle$. Por otro lado, como α es algebraico sobre k, se tiene que:

$$k[\alpha] = k(\alpha)$$

Esto dice que

$$k[x]/\langle min_k(\alpha) \rangle \cong k(\alpha).$$

De esto se deduce que:

[1] De hecho formalmente también se tendría que incluir la extensión algebraica sobre la que se está trabajando, pero esta es más sencilla de deducir de los datos que conforman la notación del polinomio mínimo.

$$\begin{aligned}[k(\alpha):k] =& [k[x]/\langle min_k(\alpha)\rangle : k] \\ =& \partial(min_k(\alpha)) \\ =& d\end{aligned}$$

De esto se deduce que β es linealmente independiente máximo y por lo tanto una base.

Para 2 observe que es claro que la T definida es lineal. Por otro lado si,

$$min_k(\alpha) = \sum_{i=0}^{d} \lambda_i x^i,$$

como $\lambda_d = 1$, entonces

$$0 = min_k(\alpha)(\alpha) = \alpha^d + \sum_{i=0}^{d-1} \lambda_i \alpha^i.$$

De esto se deduce que

$$\alpha^d = -\sum_{i=0}^{d-1} \lambda_i \alpha^i$$

Luego observe que $T(1) = \alpha, T(\alpha) = \alpha^2, \ldots, T(\alpha^{d-1}) = \alpha^d = -\sum_{i=0}^{d-1} \lambda_i \alpha^i$. Esto dice que

$$[T]_\beta = \begin{pmatrix} 0 & 0 & \cdots & -\lambda_0 \\ 1 & 0 & \cdots & -\lambda_1 \\ 0 & 1 & \cdots & -\lambda_2 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & -\lambda_{d-1} \end{pmatrix}$$

De álgebra lineal se deduce que $p_T = \sum_{i=0}^{d-1} \lambda_i x^i$. □

1.3. Teorema de Kronecker. El último resultado a discutir es un teorema de Kronecker, el cual básicamente dice que dado un polinomio, siempre puede encontrarse una extensión de campos en el que este tiene una raíz.

PROPOSICIÓN 88. *(Kronecker) Sea $f \in k[x]$ con $\partial(f) \geq 1$. Entonces existe una extensión $K|k$ tal que f tiene una raíz en K.*

DEMOSTRACIÓN. Dado que $k[x]$ es un DFU, existe $p_1 \in k[x]$ irreducible tal que $p_1|f$. Dado que $\langle p_1\rangle \leq k[x]$ es máximo, entonces $k[x]/\langle p_1\rangle$ es un campo y denote este por K. Observe que se tienen morfismos de anillos

$$k \xrightarrow{i} k[x] \xrightarrow{\pi} K.$$

Al considerar la composición de estos, se tiene un morfismo no cero con dominio un campo, por lo que este debe ser inyectivo, así que k se encaja como subcampo de K. Para concluir hay que ver que $f \in k[x] \subseteq K[x]$ tiene una raíz en K. Para esto consideramos $a \in K$ dada por $a = x + \langle p_1 \rangle$. Al evaluar $f(a) = f(x) + \langle p_1 \rangle = 0 + \langle p_1 \rangle$ pues como $p_1 | f$ entonces $f \in \langle p_1 \rangle$. Así, a es raíz de f. □

Vale la pena comentar que como se habrá podido observar, en el resultado anterior se está forzando la construcción de la raíz, por lo que esta puede considerarse una prueba teórica y en efecto, hay que quedarse simplemente con el resultado que lo que nos dice es que dado un polinomio, siempre podemos ir construyendo campos en los que dicho polinomio vaya teniendo raíces. En la siguiente sección se verá que esto puede hacerse de manera uniforme en el sentido de que funcione para todos los polinomios con coeficientes en un campo base, que es lo que se conoce como la cerradura algebraica de un campo. Por otro lado, observe que cuando se obtiene la raíz de f en una extensión $K|k$, la cual es α, dicha raíz aparece de manera mínima en el campo intermedio $k(\alpha)$.

2. Extensiones normales y campos de descomposición

Esta sección esta dividida en dos partes, cada una estudia uno de los dos temas del titulo. Ademas se discutirá la relación entre estos.

2.1. Campos de descomposición.

DEFINICIÓN 58. *Sea $f \in k[x]$. Si $K|k$ es una extensión algebraica tal que f se escinde en factores lineales en $K[x]$, y no existe un campo intermedio en dicha extensión que cumpla esta última propiedad, diremos que K un campo de descomposición de f.*

EJEMPLO 51. *Considere $f = x^2 - 2 \in \mathbb{Q}[x]$. Observe que el campo de descomposición de f debe tener los elementos para factorizar a f en factores lineales (las raíces de f), por tal razón dicho campo debe tener como elementos a $\sqrt{2}$ y $-\sqrt{2}$. Así, en este caso el campo de descomposición es $\mathbb{Q}(\sqrt{2})$.*

EJEMPLO 52. *Considere el polinomio $f = x^2 + 1 \in \mathbb{Q}[x]$. Siguiendo el argumento del ejemplo anterior se puede ver que el campo de descomposición de f es $\mathbb{Q}(i)$.*

Vale la pena discutir algunas ideas "ocultas" en los ejemplos anteriores, pues si bien es cierto que ambos polinomios se escinden en factores lineales sobre $\mathbb{C}$, la idea del campo de descomposición es buscar el campo más pequeño en el que el polinomio en cuestión se escinda en factores lineales.

Regresando a las generalidades de la teoría, la primera pregunta que se nos puede ocurrir es acerca de la existencia de campos de descomposición. El siguiente resultado dice que estos siempre existen.

PROPOSICIÓN 89. *Si $f \in k[x]$ es un polinomio no constante, entonces f tiene un campo de descomposición.*

DEMOSTRACIÓN. Por inducción generalizada sobre $n = \partial(f)$.

Base: $n = 1$. En este caso $f = a_1x + a_0$ y como la única raíz de f es $-a_1^{-1}a_0 \in k$, entonces k es el campo de descomposición de f.

Paso inductivo: Supongamos que el resultado es cierto para los polinomios con grado menor a n. Por el teorema de Kronecker existe $F|k$ tal que f tiene una raíz, digamos $\alpha_1 \in F$. Mas aún, podemos considerar $F = k(\alpha_1)$. Por lo tanto $f = (x-\alpha_1)g$ con $g \in F[x]$. Por hipótesis de inducción, existe $K|F$ campo de descomposición de g, en particular $g = b_0(x-\alpha_2)\cdot\cdots\cdot(x-\alpha_n)$ en $K[x]$, luego $f = b_0(x-\alpha_1)\cdot\cdots\cdot(x-\alpha_n)$ en $K[x]$ y muestra que f se escinde sobre K. Observe que $F(\alpha_2,\ldots,\alpha_n) \subseteq K$. Ademas, como K es campo de descomposición de g, entonces

$$\begin{aligned} K =& F(\alpha_2,\ldots,\alpha_n) \\ =& k(\alpha_1)(\alpha_2,\ldots,\alpha_n) \\ =& k(\alpha_1,\ldots,\alpha_n) \end{aligned}$$

Esto muestra que K es el campo buscado. □

Antes de pasar a la siguiente pregunta que se nos puede ocurrir, a saber, la unicidad del campo de descomposición, vamos a estudiar algunos resultados previos. El primero de ellos da ecuaciones para el índice de dicho campo.

PROPOSICIÓN 90. *Sea $f \in k[x]$ un polinomio no constante con $d = \partial(f)$. Ademas sea K un campo de descomposición de f. Entonces,*

$$[K : k] \leq d!$$

Si ademas f es irreducible, entonces $d|[K:k]$.

DEMOSTRACIÓN. La prueba de la desigualdad es por inducción sobre d. Además, podemos suponer sin pérdida de generalidad que f es mónico.

Base: $d=1$. En este caso $f=x+a_0$ y $K=k$. Luego $[K:k]=1$ y se cumple el resultado.

Paso inductivo: Supongamos que el resultado es valido para todos los polinomios con grado $d-1$. Como K es campo de descomposición de f, sea $\alpha_1 \in K$ raíz de f. Entonces

$$f=(x-\alpha_1)g$$

con $g \in k(\alpha_1)[x]$. Dado que f es mónico y $f(\alpha_1)=0$, entonces $min_k(\alpha_1)|f$, luego

$$\begin{aligned}[k(\alpha_1):k] =& \partial(min_k(\alpha_1)) \\ &\leq \partial(f)=d\end{aligned}$$

Por otro lado, como $\partial(g)=d-1$, si K es campo de descomposición de g, entonces

$$[K:k(\alpha_1)] \leq (d-1)!$$

Por lo tanto

$$\begin{aligned}[K:k] =& [K:k(\alpha_1)][k(\alpha_1):k] \\ &\leq (d-1)!\cdot d = d!\end{aligned}$$

Por otro lado, si f es irreducible y al suponer es mónico

$$f=min_k(\alpha)$$

Entonces $d=[k(\alpha):k]$. Como

$$\begin{aligned}[K:k] =& [K:k(\alpha)][k(\alpha):k] \\ =& [K:K(\alpha)]\cdot d,\end{aligned}$$

Se sigue el resultado □

EJEMPLO 53. *Sea $k=\mathbb{Q}$ y K el campo de descomposición de $f=x^3-2$. Observe que $\sqrt[3]{2}$ es raíz de f, y si ω es raíz del $x^2+x+1=0$, entonces*

$$\omega, \sqrt[3]{2} \in K.$$

En este ejemplo $[K:k] \leq 3! = 6$. *Ademas, por el criterio de Einsestein para* $2 \in \mathbb{Z}$ *se concluye* f *es irreducible. Por lo tanto* $3|[K:k]$. *Dado que* $\sqrt[3]{2}, \sqrt[3]{4}, \omega, \omega\sqrt[3]{2} \in K$, *entonces* $[K:k] = 6$. *De hecho* $K = \mathbb{Q}(\omega, \sqrt[3]{2})$.

EJEMPLO 54. *Sea* $k = \mathbb{Q}(\omega)$ *con* ω *raíz de* $x^2 + x + 1 = 0$ *y* K *el campo de descomposición de* $f = x^3 - 2 \in k[x]$. *Entonces* f *no es irreducible. Por otro lado es fácil ver que*

$$K = k(\sqrt[3]{2})$$

Por lo tanto

$$[K:k] = 3 < 3! = 6$$

Esto muestra que la desigualdad puede ser estricta en el resultado anterior.

Del resultado anterior se obtiene directamente lo siguiente.

COROLARIO 13. *Si* k *es un campo.* $f \in k[x]$ *es un polinomio no constante y* K *es su campo de descomposición, entonces la extensión* $K|k$ *es finita y por lo tanto algebraica.*

En este momento podemos pasar al problema de la unicidad del campo de descomposición de un polinomio. Para obtenerlo es necesario demostrar algunos resultados resultados preliminares que pueden considerarse técnicos, pero que en el fondo llevan consigo la filosofía moderna de la teoría de Galois: “el estudio de los diferentes tipos isomorfismos entre dos campos".

LEMA 4. *(Extensión de isomorfismos) Sea* $\sigma_0 : k_1 \to k_2$ *un isomorfismo de campos. Considere* $f_1 \in k_1[x]$ *irreducible y defina* $f_2 := \sigma_0 f_1 \in k_2[x]$ *como el polinomio que resulta al aplicar* σ_0 *a los coeficientes de* f. *Sea* α_1 *una raíz de* f_1 *y* α_2 *una raíz de* f_2. *Entonces* σ_0 *se extiende a un único isomorfismo*

$$\sigma : k_1(\alpha_1) \to k_2(\alpha_2)$$

tal que $\sigma(\alpha_1) = \alpha_2$.

DEMOSTRACIÓN. Puede suponerse sin pérdida de generalidad que f_1 y f_2 son mónicos. Por lo tanto, se tiene que $f_1 = min_{k_1}(\alpha_1)$ y $f_2 = min_{k_2}(\alpha_2)$. Ademas, para $i \in \{1,2\}$ se tienen isomorfismos de campo

$$k_i[x]/\langle f_i \rangle \cong k_i(\alpha_i)$$

Por la propiedad universal del anillo de polinomios aplicada al morfismo $i_2\sigma_0 : k_1 \to k_2[x]$, con $i_2 : k_2 \to k_2[x]$ la inclusión canónica, y el elemento $x \in k_2[x]$, existe un morfismo de anillos;

$$\tilde{\sigma_0} : k_1[x] \to k_2[x]$$

tal que $\tilde{\sigma_0}(x) = x$ y $\tilde{\sigma_0} i_1 = i_2\sigma_0$.

Este morfismo es claramente un isomorfismo, por lo que este induce un isomorfismo de campos.

$$\overline{\sigma_0} : k_1[x]/\langle f_1\rangle \to k_2[x]/\langle f_2\rangle$$

Por lo tanto el isomorfismo buscado es la composición

$$k(\alpha_1) \xrightarrow{\cong} k_1[x]/\langle f_1\rangle \xrightarrow{\overline{\sigma_0}} k_2[x]/\langle f_2\rangle \xrightarrow{\cong} k_2(\alpha_2).$$

La unicidad es clara de las construcciones. □

Un corolario directo del resultado anterior dice básicamente que siempre pueden encontrarse automorfismos que permuten raíces. Mas aún, entre dos raíces fijas siempre hay un único automorfismo que manda una de ellas en las otras.

COROLARIO 14. *Sea $f \in k[x]$ irreducible y α_1, α_2 raíces de f. Entonces existe un único isomorfismo*

$$\sigma : k(\alpha_1) \to k(\alpha_2)$$

tal que $\sigma|k = 1_k$ y $\sigma(\alpha_1) = \alpha_2$.

Observe que este resultado nos dice que todas raíces de un polinomio irreducible producen básicamente la misma extensión. A continuación se presentará el resultado del cual se dedue el teorema buscado.

LEMA 5. *Sean $\sigma_0 : k_1 \to k_2$ un isomorfismo de campos y $f_1 \in k_1[x]$. Denote por $f_2 = \sigma_0 f_1$. Si K_1 es el campo de descomposición de f_1 y K_2 es el campo de descomposición de f_2, entonces existe un isomorfismo*

$$\sigma : K_1 \to K_2$$

que extiende a σ_0.

DEMOSTRACIÓN. Dado que $k_1[x]$ es un DFU, f_1 se descompone como producto de polinomios irreducibles de forma única, y sea k el número de estos, Defina

$$m(f_1) = \partial(f_1) - k \in \mathbb{N}$$

La prueba se va a hacer por inducción en $m(f_1)$.

Base: $m(f_1) = 0$. En este caso, $\partial(f_1) = k$. Esto dice que f_1 se descompone como producto de factores lineales, entonces $k_1 = K_1$ y lo mismo sucede con f_2. Por lo tanto hay que tomar

$$\sigma := \sigma_0.$$

Paso inductivo: Suponga que el resultado es valido para polinomios g con $m(g) < m(f_1)$. Ahora considere g_1 un factor irreducible de f_1 con grado mayor o igual a 1.
Sean α_1 una raíz de g_1 y α_2 raíz de $g_2 = \sigma_0 g_1$. Por el lema de extensión de isomorfismos σ_0 se extiende a un isomorfismo

$$\sigma_1 : k_1(\alpha_1) \to k_2(\alpha_2)$$

con $\sigma_1|k_1 = \sigma_0$ y $\sigma_1(\alpha_1) = \alpha_2$.

Ahora considere $F = k_1(\alpha_1)$ y $f_1 \in F[x]$. Dado que $g_1 \in F[x]$ tiene el factor $x - \alpha_1$, entonces f_1 tiene al menos $k+1$ factores irreducibles en $F[x]$ y $m_F(f_1) < m_k(f_1)$. Dado que K_1 es campo de descomposición de f_1 como polinomio en $k_1[x]$ y $F \subseteq K_1$, entonces por la observación anterior K_1 es campo de descomposición de $f_1 \in F[x]$ y lo mismo para K_2, entonces la hipótesis de inducción permite encontrar la extensión de σ_1 buscada. □

COROLARIO 15. *Si $f \in k[x]$ cualesquiera dos campos de descomposición de f son isomorfos.*

El resultado anterior nos permite introducir lo siguiente:

Notación. El campo de descomposición de $f \in k[x]$ se denotará por

$$k(f).$$

2.2. Extensiones normales.

DEFINICIÓN 59. *Una extensión algebraica $K|k$ es normal si para cualquier $f \in k[x]$ tal que existe $\alpha \in K$ con $f(\alpha) = 0$, se tiene que f se escinde en factores lineales en K.*

La intuición detrás de este tipo de extensiones está en el hecho de que lo que se busca es una extensión en el cual al encontrar una raíz de cualquier polinomio con coeficientes en k, esto baste para encontrado todas las raíces de cada uno de dichos polinomios.

EJEMPLO 55. *La extensión $\mathbb{Q}(\sqrt[3]{2})|\mathbb{Q}$ no es normal pues el polinomio $f = x^3 - 2 \in \mathbb{Q}[x]$ satisface $f(\sqrt[3]{2}) = 0$ pero f no se escinde en $\mathbb{Q}(\sqrt[3]{2})$.*

EJEMPLO 56. *Las extensiones $\mathbb{C}|\mathbb{Q}$ y $\mathbb{C}|\mathbb{R}$ son normales*

El primer resultado respecto a este tipo de extensiones muestra que el proceso de probar que una extensión es normal puede reducirse a checar la propiedad buscada para una clase especial de polinomios.

PROPOSICIÓN 91. *Sea $K|k$ una extensión algebraica. son equivalentes:*

1. *$K|k$ es normal*
2. *Para cualquier $\alpha \in K$ $min_k(\alpha)$ se escinde en $K[x]$*

DEMOSTRACIÓN. $1 \Rightarrow 2)$ Es claro.

$2 \Rightarrow 1)$ Sea $f \in k[x]$ tal que $f(\alpha) = 0$ para $\alpha \in K$. Podemos suponer sin perdida de generalidad que f es mónico. Ademas, como $k[x]$ es un DFU,

$$f = p_1 \cdot \ldots \cdot p_k$$

con $p_1, \ldots, p_k \in k[x]$ irreducibles y mónicos. Observe que si $p_1(\alpha) = 0$, $p_1 = min_k(\alpha)$ por lo que la hipótesis implica que p_1 se escinde. Ademas, el mismo proceso se usa con los factores restantes. □

Existe un teorema de caracterización de extensiones normales que conecta el concepto introducido con los conceptos tratados en la subsección anterior. Es importante decir que en este se usa como hipótesis la finitud de la extensión.

PROPOSICIÓN 92. *Sea $K|k$ finita. Entonces, $K|k$ es normal si y solo si K es campo de descomposición de un polinomio con coeficientes en k.*

DEMOSTRACIÓN. $\Rightarrow$) Considere $\{x_1,\ldots,x_n\} \subseteq K$ base de K como $k-$espacio vectorial. Considere entonces $f := \prod_{i=1}^{n} min_k(x_i) \in k[x]$.

Afirmación: $k(f) = K$.

Sea $\alpha \in K$. Por hipótesis, existen $\lambda_1,\ldots,\lambda_n \in k$ tales que

$$\alpha = \sum_{i=1}^{n} \lambda_i x_i \in k(f).$$

Por otro lado es claro de la hipótesis de normalidad que $k(f) \subseteq K$ lo que concluye la prueba.

$\Leftarrow$) Suponga que existe $f \in k[x]$ tal que $K = k(f)$. Considere $g \in k[x]$ tal que existe $\alpha \in K$ con $g(\alpha) = 0$. Ademas podemos suponer sin pérdida de generalidad que g es irreducible. Al considerar $k(g)$ el campo de descomposición de g, sea $\beta \in k(g)$ raíz de g. Por el lema de extensión de isomorfismos, existe

$$\sigma : k(\alpha) \to k(\beta)$$

tal que $\sigma|k = 1_k$ y $\sigma(\alpha) = \beta$. Observe que $K = k(\alpha)(f)$ y que $K(\beta)$ es el campo de descomposición de f sobre $k(\beta)$, entonces, existe un isomorfismo

$$\tau : K(\alpha) \to K(\beta)$$

que extiende a σ y $\tau(\alpha) = \beta$. Observe que $\tau|k = 1_k$ y $K = K(\alpha)$. Entonces τ permuta con las raíces de f. Como $\alpha \in K$, si $\gamma_1,\ldots,\gamma_n$ son las raíces de f, entonces

$$\alpha = h(\gamma_1,\ldots,\gamma_n)$$

para algún $h \in k[x_1,\ldots,x_n]$. Entonces,

$$\beta = \tau(\alpha) = \tau h(\gamma_1,\ldots,\gamma_n) = h(\tau(\gamma_1),\ldots,\tau(\gamma_n))$$

por lo tanto $\beta \in K$. Esto muestra que

$$k(g) = k(f) = K$$

□

EJEMPLO 57. *La extensión* $\mathbb{Q}(\sqrt{2})|\mathbb{Q}$ *es normal pues* $\mathbb{Q}(\sqrt{2}) = \mathbb{Q}(x^2-2)$.

3. Extensiones separables, campos perfectos y cerradura separable

3.1. Extensiones separables.

DEFINICIÓN 60. *Sea $f \in k[x]$. Decimos que f es separable si para cualquier campo de descomposición K de f, f se descompone como distintos factores lineales. Esto es, existen $a_1, \ldots, a_n \in K$ tales que*

$$f(x) = a_0(x-a_1)\cdot\cdots\cdot(x-a_n)$$

con $a_i \neq a_j$ si $i \neq j$ con $i, j = 1, \ldots, n$.

DEFINICIÓN 61. *Sean K una extensión algebraica de k y $\alpha \in K$. Decimos que α es irreducible, si el polinomio $irr_k(\alpha)$ es separable. Si no es separable diremos que α es inseparable.*

DEFINICIÓN 62. *Sea K una extensión algebraica de k. Decimos que K es una extensión separable de k, si todo elemento $\alpha \in K$ es separable.*

DEFINICIÓN 63. *Sea K una extensión algebraica de k y $f \in k[x]$ y $\alpha \in K$ con $f(\alpha) = 0$. Decimos que α es una raíz simple si $x-\alpha | f$ y $(x-\alpha)^2$*
nmid f. Dicho de otro modo, un polinomio es separable si sus raíces son simples.

DEFINICIÓN 64. *Sea $f \in k[x]$ con $\sum_{i=0}^{n} a_i x^i$. Definimos la derivada de f denotada por f', como*

$$f'(x) = \sum_{i=1}^{n} i a_i x^{i-1}$$

LEMA 6. *Sea $K|k$ una extensión algebraica, $f \in k[x]$ y $\alpha \in K$ con $f(\alpha) = 0$. Entonces α es una raíz simple si y sólo si $f'(\alpha) \neq 0$.*

DEMOSTRACIÓN. Como $f(\alpha) = 0$ entonces $x-\alpha | f$ y de aquí existe $g(x) \in K[x]$ tal que

$$f(x) = (x-\alpha)g(x)$$

Entonces

$$f'(x) = (x-\alpha)g'(x) + g(x)$$

Evaluando en α tenemos

$$f'(\alpha) = g(\alpha)$$

aplicando el algoritmo de la división, tenemos que

$$\begin{aligned} g(x) =&(x-\alpha)h(x)+g(\alpha) \\ =&(x-\alpha)h(x)+f'(x) \end{aligned}$$

por lo que

$$\begin{aligned} f(x) =&(x-\alpha)g(x) \\ =&(x-\alpha)[(x-\alpha)h(x)+f'(\alpha)] \\ =&(x-\alpha)^2h(x)+(x-\alpha)f'(\alpha) \end{aligned}$$

de aquí tenemos que $(x-\alpha)^2|f$ si y sólo si $f'(\alpha)=0$ □

PROPOSICIÓN 93. *Sea $f\in k[x]$ irreducible. Si $f'(x)\neq 0$, entonces f es separable.*

DEMOSTRACIÓN. Sea α una raíz de f en una extensión K de k. Como f es irreducible y sin perdida de generalidad podemos suponer que f es monico, entonces $f=irr_k(\alpha)$. Ahora bien, como $f'(x)\neq 0$ y el grado de f' es menor que el grado de f, entonces α no puede ser raíz de f' puesto que esto contradice la minimalidad de $irr_k(\alpha)$. Por el lema anterior, todas las raíces de f son simples y así f es separable. □

COROLARIO 16. *Sea $f\in k[x]$ irreducible. Si $car(k)=0$ entonces f es separable.*

DEMOSTRACIÓN. Si $car(k)=0$ entonces $\partial f'=\partial f-1$ por lo que si f es un polinomio no constante, entonces $f'\neq 0$. □

COROLARIO 17. *Sea $f\in k[x]$. Si $car(k)=p$ entonces f es separable o $f(x)=\sum_{i=1}^{n}a_ix^{ip}$*

DEMOSTRACIÓN. Si $f(x)=\sum_{i=0}^{n}a_ix^i$ entonces $f'(x)=\sum_{i=1}^{n}ia_ix^{i-1}$. Sabemos que si $f'\neq 0$ entonces f es separable.
Si $f=0$ entonces $ia_i=0$ para todo $i=1,\ldots,n.$ entonces $a_i=0$ o $p|a_i$ por lo cual los coeficientes de f distintos de cero son múltiplos de p. □

COROLARIO 18. *Sea $K|k$ una extensión algebraica. Si $car(k)=0$ entonces $K|k$ es separable.*

EJEMPLO 58. *Vamos a construir un ejemplo de un polinomio inseparable.*
Sea $k=\mathbb{Z}_p(t)$ el campo de funciones racionales con coeficientes en $\mathbb{Z}_p$ en la variable t.
Sea K el campo de descomposición de de $f(x)=x^p-t$. Consideramos $s\in K$ raíz de f. Por

lo que $s^p = t$. Ahora bien, $f(x) = x^p - t = x^p - s^p = (x-s)^p$ por lo que f no es separable. Notamos que $k(s) = K$.

DEFINICIÓN 65. *Sea k un campo. Decimos que k es perfecto, si cualquier extensión algebraica es separable.*

PROPOSICIÓN 94. *Sea k un campo. Si p es un primo, entonces $\varepsilon : k \to k$ dado por $\varphi(x) = x^p$ es un morfismo de campos.*

Al morfismo φ se le llama el morfismo de Frobenius. Note que $Im(\varphi) = k^p$.

LEMA 7. *Sea k un campo, con $car(k) = p$ y $\alpha \in k$ con $\alpha \notin k^p$. Entonces*

$$f(x) = x^{p^n} - \alpha \in k[x]$$

es irreducible para $n \geq 1$.

DEMOSTRACIÓN. Consideremos la factorización de $f = g_1, \ldots, g_n$ polinomios monicos irreducibles, ponemos $K = k(\beta)$ con $g_1(\beta) = 0$. Entonces $g_1 = irr_k(\beta) \in k[x]$ puesto que g_1 es irreducible. Por otro lado, $g_1(\beta) = 0$ implica

$$0 = f(\beta) = \beta^p - \alpha$$

por lo que $\alpha = \beta^{p^n}$ y

$$f(x) = x^{p^n} - \alpha = x^{p^n} - \beta^{p^n} = (x-\beta)^{p^n} \in K[x]$$

para cada $i = 1, \ldots, m$ $g_i | f$ en $K[x]$, esto es $g_i | (x-\beta)^{p^n}$ en $K[x]$. De donde g_i es una potencia de $(x-\beta)$ por lo que $g_i(\beta) = 0$ y de aquí $g_1 | g_i$ pero como g_i es irreducible tenemos $g_1 = g_i$ para $i = 1, \ldots, m$. Así tenemos que $f = {g_1}^m$. Como

$$g_1 | (x-\beta)^{p^n}$$

tenemos que

$$g_1(x) = (x-\beta)^k$$

para algún k. Tenemos que $(x^{p^n} - \alpha) = ((x-\beta)^k)^m$ por lo que $k = p^s$ y $m = p^{t-s}$ para algún $s \leq t$.

Suponemos que $s \leq t-1$. Así que $g_1(x) = (x-\beta)^{p^s} \in k[x]$ como consecuencia $g_1(x)^{p^{t-s-1}} \in k[x]$. Pero

$$g_1(x)^{p^{t-s-1}} = (x-\beta)^{p^{t-1}} = x^{p^{t-1}} - \gamma$$

con $\gamma = \beta^{p^{t-1}}$ y así $\gamma \in k$. Aún así, $\gamma^p = (\beta^{p^{t-1}})^p = \beta^p = \alpha$. Así $\alpha \in k^p$, lo que es una contradicción. Por lo tanto, $s = t$, $m = 1$ y $f = g$ irreducible en $k[x]$. □

PROPOSICIÓN 95. *k es un campo perfecto si y sólo si $car(k) = 0$ 0 $car(k) = p$ y $k^p = k$.*

DEMOSTRACIÓN. $\Rightarrow$. Si k es perfecto, Sea $\alpha \in k$ con $\alpha \notin k^p$ y $f(x) = x^p - \alpha \in k[x]$. Por el lema anterior f es irreducible. Sea $K = k(\beta)$ con β raíz de f. Por lo que en K, tenemos $\beta^p = \alpha$, así

$$x^p - \alpha = x^p - \beta^p = (x - \beta)^p$$

por lo que $p \in K$ y β es inseparable. Contradiciendo el hecho de que k es perfecto. Así $k = k^p$.

$\Leftarrow$ .Si $car(k) = 0$ entonces k es perfecto.

Si $car(k) = p$ y $k^p = k$, sea K una extensión algebraica de k y $\alpha \in K$ inseparable. Tenemos que:

$$irr_k(\alpha)(x) = \sum_{i=0}^{n} a_i x^{pi}$$

como $k = k^p$, tenemos que $a_i = b_i^p$ para algún $b_i \in k$. Entonces

$$irr_k(\alpha)(x) = \sum_{i=0}^{n} a_i x^{pi} = \sum_{i=0}^{n} b_i^p x^{pi} = (\sum_{i=0}^{n} b_i x^i)^p$$

contradiciendo que sea irreducible $irr_k(\alpha)$. Por oo que α es separable y k es perfecto. □

COROLARIO 19. *Sea k un campo finito. Entonces k es perfecto.*

DEMOSTRACIÓN. Como k es finito entonces $car(k) = p$ para p un primo. El morfismo de Frobenius es inyectivo y como k es finito entonces es suprayectivo y así $k^p = k$. Por lo tanto k es perfecto. □

4. Extensiones de Galois

Considere $K|k$ una extensión algebraica, así como el conjunto

$$Aut(K|k) = \{\sigma : K \to K : \sigma \text{ es un automorfismo y } \sigma|_k = 1_k\}$$

Observe que dados $\sigma, \tau \in Aut(K|k)$ se tiene $\sigma \circ \tau \in Aut(K|k)$. Mas aún, la composición es asociativa, $1_K \in Aut(K|k)$ y además, dado $\sigma \in Aut(K|k)$, se tiene que $\sigma^{-1} : K \to K$ existe y mas aún, $\sigma^{-1} \in Aut(K|k)$. Por lo tanto

$$(Aut(K|k), \circ)$$

es un grupo.

DEFINICIÓN 66. *Para una extensión algebraica $K|k$, definimos su grupo de Galois como*

$$Gal(K|k) = (Aut(K|k), \circ)$$

EJEMPLO 59. *Para la extensión algebraica $\mathbb{C}|\mathbb{R}$ considere $\sigma \in Gal(\mathbb{C}|\mathbb{R})$. Observe que para $z = a+ib \in \mathbb{C}$,*

$$\begin{aligned}\sigma(z) =& \sigma(a+ib)\\ =& \sigma(a)+\sigma(i)\sigma(b)\\ =& a+\sigma(i)b\end{aligned}$$

Por lo tanto, σ queda determinado por su valor en $\sigma(i)$. Además, usando nuevamente que este es un morfismo:

$$\sigma(i)^2 = \sigma(i^2) = \sigma(-1) = -1$$

Por lo tanto, $\sigma(i) \in \{i,-i\}$, lo que nos lleva a dos casos:

1. *Si $\sigma(i) = i$, entonces*
$$\sigma = 1_{\mathbb{C}}$$
2. *Si $\sigma(i) = -i$, entonces $\sigma = \overline{(\ )}$ es la conjugación compleja.*

De esto se puede probar que

$$Gal(\mathbb{C}|\mathbb{R}) = \{1_{\mathbb{C}}, \overline{(\ )}\}$$

Como existe un único grupo con orden 2, entonces

$$Gal(\mathbb{C}|\mathbb{R}) \cong \mathbb{Z}/2$$

y este es generado por la conjugación compeja.

Como se verá posteriormente, en general es muy complejo determinar explicitamente el grupo de Galois de una extensión, sin embargo, entre otras cosas, se desarrollarán algunas ideas en torno al cálculo de estos en los siguientes temas. Por ahora presentaremos un par de ejemplos en los que los cálculos se pueden hacer a pie con el objetivo de ir ganando intuición en los cálculos.

EJEMPLO 60. *Considere $k = \mathbb{Q}$ y $K = \mathbb{Q}(x^4-5x^2+6)$. Observe que $x^4-5x^2+6 = (x^2-3)(x^2-2)$. De esto resulta sencillo ver que $K = \mathbb{Q}(\sqrt{3},\sqrt{2})$. Además, por un resultado previo la extensión $K|k$ es normal. Mas aún, no es difícil ver que*

$$[K:k] = 4$$

Pues una base de K como k- espacio vectorial es $\{1,\sqrt{2},\sqrt{3},\sqrt{6}\}$. En lo que respecta a determinar $Gal(K|k)$, sea $\sigma \in Gal(K|k)$. Observe que σ manda una raíz del polinomio

x^2-2 es una raíz de dicho polinomio y lo mismo sucede con x^2-3, es decir, $\sigma(\sqrt{2})=\pm\sqrt{2}$ y $\sigma(\sqrt{3})=\pm\sqrt{3}$. Esto implica que hay cuatro posibilidades para σ:

1. $\sigma(\sqrt{2})=\sqrt{2}$ *y* $\sigma(\sqrt{3})=\sqrt{3}$, *en cuyo caso* $\sigma=1_K$.
2. $\sigma(\sqrt{2})=-\sqrt{2}$ *y* $\sigma(\sqrt{3})=\sqrt{3}$. *Dado que todo elemento de K tiene la forma* $a+b\sqrt{2}+c\sqrt{3}+d\sqrt{6}$ *con* $a,b,c,d\in k$, *entonces*
$$\sigma(a+b\sqrt{2}+c\sqrt{3}+d\sqrt{6})=a-b\sqrt{2}+c\sqrt{3}-d\sqrt{6}$$
3. $\sigma(\sqrt{2})=\sqrt{2}$ *y* $\sigma(\sqrt{3})=-\sqrt{3}$, *de donde*
$$\sigma(a+b\sqrt{2}+c\sqrt{3}+d\sqrt{6})=a+b\sqrt{2}-c\sqrt{3}-d\sqrt{6}$$
4. $\sigma(\sqrt{2})=-\sqrt{2}$ *y* $\sigma(\sqrt{3})=-\sqrt{3}$, *por lo que en este caso*
$$\sigma(a+b\sqrt{2}+c\sqrt{3}+d\sqrt{6})=a-b\sqrt{2}-c\sqrt{3}+d\sqrt{6}$$

De lo anterior se deduce que:

$$|Gal(K|k)|=4.$$

Dado que existen dos grupos de orden 4, hay que resolver esta ambigüedad para determinar explícitamente $Gal(K|k)$. Sin embargo, observe que los elementos no triviales de $Gal(K|k)$ tiene orden 2, por lo que $Gal(K|k)\ncong\mathbb{Z}_4$. Por lo tanto,

$$Gal(K|k)\cong\mathbb{Z}_2\oplus\mathbb{Z}_2$$

El último ejemplo a presentar muestra que contrario a la "intuición" que se puede formar de los ejemplos anteriores, hay ejemplos de grupos de Galois no abelianos.

EJEMPLO 61. *Considere $k=\mathbb{Q}$ y $K=\mathbb{Q}(x^3-2)$. Para determinar K de forma explícita observe que obviamente $\sqrt[3]{2}\in K$. Por otro lado, si $\omega\in\mathbb{C}$ es una raíz cubica de la unidad con $\omega^2+\omega+1=0$, entonces $\omega\sqrt[3]{2}\in K$ y así $\omega\in K$. Observe que $\mathbb{Q}(\sqrt[3]{2},\omega)\subseteq K$ y además $[K:k]\leq 3!=6$. Por otro lado, note que $\mathbb{Q}(\sqrt[3]{2},\omega)$ es generado como $\mathbb{Q}-$espacio por la base $\{\sqrt[3]{2},\sqrt[3]{4},\omega,\omega\sqrt[3]{2},\omega\sqrt[3]{4},1\}$. Note que ω^2 no aparece como generador pues $\omega^2=-\omega-1$ y tampoco ω^3 pues $\omega^3=1$. Lo mismo sucede con $\sqrt[3]{2}\sqrt[3]{4}=\sqrt[3]{8}=2$. Esto dice que*

$$[\mathbb{Q}(\sqrt[3]{2},\omega):\mathbb{Q}]=6$$

Por lo tanto,

$$K=\mathbb{Q}(\sqrt[3]{2},\omega)$$

Además observe que por un resultado previo $\mathbb{Q}(\sqrt[3]{2},\omega)|\mathbb{Q}$ *es normal. Por otro lado, para determinar* $Gal(K|k)$*, sea* $\sigma \in Gal(K|k)$*. Dado que* σ *manda una raíz del polinomio* x^3-2 *en otra raíz, entonces* $\sigma(\sqrt[3]{2}) \in \{\sqrt[3]{2}, \omega\sqrt[3]{2}, \omega^2\sqrt[3]{2}\}$*. Como en el primero de estos ejemplos falta determinar que sucede con* $\sigma(\omega)$*. Para esto observe que* ω *es raíz de* $f = x^2+x+1$*, además* ω^2 *también es raíz pues*

$$\begin{aligned}\omega^4+\omega^2+1 =& \omega^3\omega+\omega^2+1\\ =& \omega+\omega^2+1\\ =& 0\end{aligned}$$

Por lo tanto

$$\sigma(\omega) \in \{\omega, \omega^2\}$$

Luego, como

$$\sigma(a+b\sqrt[3]{2}+c\sqrt[3]{4}+d\omega+e\omega\sqrt[3]{2}+f\omega\sqrt[3]{4}) = a+b\sigma(\sqrt[3]{2})+c\sigma(\sqrt[3]{4})+d\sigma(\omega)+e\sigma(\omega)\sigma(\sqrt[3]{2})+e\sigma(\omega)\sigma(\sqrt[3]{2})$$

Esto dice que

$$|Gal(K|k)| = 6$$

Recuerde que hay dos grupos de orden 6: $\mathbb{Z}_6$ *y* S_3*. Para eliminar la ambigüedad observe que se tienen* $\sigma, \tau \in Gal(K|k)$ *definidos mediante:*

$$\sigma(\sqrt[3]{2}) = \omega\sqrt[3]{2},\ \sigma(\omega) = \omega$$

$$\tau(\sqrt[3]{2}) = \sqrt[3]{2},\ \tau(\omega) = \omega^2$$

Note que

$$\begin{aligned}\sigma\tau(\sqrt[3]{2}) =& \sigma(\sqrt[3]{2}) = \omega\sqrt[3]{2}\\ \tau\sigma(\sqrt[3]{2}) =& \tau(\omega\sqrt[3]{2}) = \tau(\omega)\tau(\sqrt[3]{2}) = \omega^2\sqrt[3]{2}\end{aligned}$$

Por lo tanto, $\sigma\tau \neq \tau\sigma$*. De esto se deduce que*

$$Gal(K|k) \cong S_3$$

Observación: Recuerde $S_3 \cong D_3$. No es difícil probar que con la notación anterior $\sigma^3 = \tau^2 = 1_K$ y $\tau\sigma\tau = \sigma^{-1}$, lo que proporciona la presentación estándar de D_3.

EJERCICIO 146. *Con la misma metodología de los ejemplos anteriores demuestre que si* $k = \mathbb{Q}$ *y* $K = \mathbb{Q}(x^4+x^3+x^2+x+1)$*, entonces*

$$Gal(K|k) \cong \mathbb{Z}_4$$

Como se mencionó anteriormente, una de la teoría es establecer formas de calcular grupos de Galois. En esta dirección, el siguiente resultado es útil en los cálculos. Quizá en este momento no se va a utilizar para ejemplificar su utilidad, sin embargo, dada su simplicidad aprovechamos para enunciarlo.

PROPOSICIÓN 96. *Sea* $K|k$ *extensión algebraica y considere la torre de extensiones* $K|F|k$*. Entonces,*

$$Gal(K|F) \leq Gal(K|k)$$

DEMOSTRACIÓN. Es claro. □

EJEMPLO 62. *Para* $k = \mathbb{Q}$ *y* $K = \mathbb{Q}(\sqrt{2},\sqrt{3})$*, un campo intermedio es* $F = \mathbb{Q}(\sqrt{2})$*. Note que* $Gal(K|F) \cong \mathbb{Z}_2$ *y esto proporciona la inclusión canónica de* $\mathbb{Z}_2$ *en* $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \cong Gal(K|k)$ *como la inclusión en una de las coordenadas.*

DEFINICIÓN 67. *Sea G un grupo de automorfismos de un campo k, esto es un morfismo de grupos* $G \to Aut(k)$*. Definimos el campo fijo* k^G *como el conjunto*

$$\{a \in k \mid \forall \sigma \in G(\sigma(\alpha) = \alpha)\}$$

Observe que el nombre de campo fijo está justificados por el siguiente resultado.

PROPOSICIÓN 97. *Para G un grupo de automorfismos de un campo k,* k^G *es subcampo de k.*

DEMOSTRACIÓN. Es claro. □

Observe que $Gal(K|k)$ actúa como grupo de automorfismos en K. Además, trivialmente

$$k \subseteq K^{Gal(K|k)}$$

EJEMPLO 63. . *Considere $k = \mathbb{Q}$ y $K = \mathbb{Q}(\sqrt[3]{2})$. La extensión $K|k$ es algebraica y observe que esta tiene grado 3. Si $\sigma \in Gal(K|k)$, observe que σ debe mandar una raíz de $f = x^3 - 2$ es otra raíz. Pero para el caso que se esta tratando la única raíz real de este polinomio es $\sqrt[3]{2}$, por lo que*

$$\sigma(\sqrt[3]{2}) = \sqrt[3]{2}$$

Por lo tanto, $\sigma = 1_K$. Luego, $Gal(\mathbb{Q}(\sqrt[3]{2})|\mathbb{Q}) = 0$. Así,

$$K^{Gal(K|k)} = K \supsetneq \mathbb{Q} = k$$

Por lo tanto, la extensión mostrada nos da un ejemplo donde se ve que la contención puede ser estricta. Esto nos lleva a introducir lo siguiente.

DEFINICIÓN 68. *(Emil Artin) Una extensión algebraica $K|k$ es de Galois si*

$$k = K^{Gal(K|k)}$$

El ejemplo anterior muestra que la extensión $\mathbb{Q}(\sqrt[3]{2})|\mathbb{Q}$ no es de Galois. Por otro lado, los ejemplos 60 y 61 son extensiones de Galois pues en estos se han descrito explicítamente sus elementos y esto permite ver que se cumple la definición. En estos momentos puede parecer complejo saber si una extensión algebraica dada es de Galois, y en efecto, no se tiene ningún teorema que las caracterice. Dicho resultado se va a posponer para la siguiente sección, donde como es costumbre dicho resultado tendrá como hipótesis la finitud de la extensión. Por ahora daremos algunas definiciones y resultados previos.

DEFINICIÓN 69. *Sean $K|k$ una extensión algebraica y $\alpha \in K$. La órbita de α con la acción $Gal(K|k) \circlearrowright K$ se conoce como el conjunto de conjugados (de Galois) de α en K.*

Un resultado directo de la teoría de acciones de grupos se presenta a continuación.

LEMA 8. *Para una extensión algebraica $K|k$ considere $\alpha \in K$. Sea $H = \{\sigma \in Gal(K|k) : \sigma(\alpha) = \alpha\}$. Entonces $H \leq Gal(K|k) =: G$ y el número de conjugados de α en K es igual al indice*

$$[G : H]$$

DEMOSTRACIÓN. Observe que $H = G_\alpha$, por lo que $G_\alpha \leq G$. Ademas, por el teorema índice-estabilizador:

$$|G\alpha| = [G : G_\alpha] = [G : H]$$

□

También se tiene el siguiente resultado.

PROPOSICIÓN 98. *Sea $K|k$ extensión de Galois finita y $\alpha \in K$. Entonces:*

1. $|G\alpha| < \aleph_0$
2. *Si* $G\alpha = \{\alpha_1, \ldots, \alpha_n\}$, *entonces*

$$min_k(\alpha) = \prod_{i=1}^{n}(x - \alpha_i)$$

DEMOSTRACIÓN. Para 1, como $min_k(\alpha) \in k[x]$ y para cada $\sigma \in Gal(K|k)$, $\sigma(\alpha)$ es raíz de $min_k(\alpha)$, entonces

$$|G\alpha| \leq \partial(min_k(\alpha)) < \aleph_0$$

En lo que respecta a 2, sea $f = \prod_{i=1}^{n}(x - \alpha_i)$. Observe que $\sigma(f) = f$, entonces σ fija todos los coeficientes de f. Como la permutación tomada fue arbitraria y la extensión $K|k$ es de Galois, todos los coeficientes pertenecen a k, por lo que $f \in k[x]$. Dado que para cada $i \in \{1, ..., n\}$, $min_k(\alpha)(\alpha_i) = 0$, entonces $x - \alpha_i | min_k(\alpha)$, luego $f | min_k(\alpha)$ en $K[x]$ y por un lema previo, $f | min_k(\alpha)$ en $k[x]$. Dado que $min_k(\alpha)$ es irreducible y mónico, entonces

$$min_k(\alpha) = f$$

□

De lo anterior se deduce lo siguiente:

COROLARIO 20. *Si $K|k$ es una extensión de Galois finita y $\alpha \in K$, entonces $[k(\alpha) : k]$ es igual al número de conjugados de α en K.*

DEMOSTRACIÓN. Como $[k(\alpha) : k] = \partial(min_k(\alpha))$ y $\partial(min_k(\alpha))$ es el número de conjugados de α en K, el resultado se sigue del anterior. □

El último resultado a mostrar da algunas propiedades de la acción estudiada hasta el momento cuando la extensión es definida por un campo de descomposición.

PROPOSICIÓN 99. *Sea $f \in k[x]$ un polinomio no constante que es separable y sea $V(f) \subseteq k(f)$ el conjunto de raíces de f. Entonces,*

1. *$Gal(k(f)|k)$ actúa en $V(f)$*
2. *$Gal(k(f)|k) \leq S_n$ con $n = \partial(f) = |V(f)|$*
3. *f es irreducible sobre k si y sólo si la acción descrita en el inciso 1 es transitiva*

DEMOSTRACIÓN. La primera afirmación es clara. Para la segunda, la acción es equivalente a un morfismo $\rho : Gal(k(f)|k) \to S_{V(f)} \cong S_n$, donde $\partial(f) = |V(f)| = n$ pues f es separable. Además observe que ρ es claramente un monomorfismo de grupos, lo que concluye la afirmación.

Para la tercera observe que si $\mathscr{O}_1, ..., \mathscr{O}_m$ son las órbitas de la acción, entonces $f = \beta \prod_{i=1}^{m} \prod_{\alpha \in \mathscr{O}_i} (x - \alpha)$ en $k(f)[x]$. Además observe que para cada $i \in \{1, ..., m\}$ se tiene que $\prod_{\alpha \in \mathscr{O}_i} (x - \alpha) = min_k(\alpha_i)$ para un $\alpha_i \in \mathscr{O}_i$. Por lo tanto, f es irreducible sobre $k[x]$ si y sólo si $m = 1$, lo que precisamente dice que la acción es transitiva. □

Observación: Dado que $Gal(\mathbb{C}|\mathbb{R})$ es generado por la conjugación compleja, observe que la propiedad 1 del resultado anterior dice el conocido hecho de que todo polinomio con coeficientes reales que tiene una raíz compleja, tiene a su conjugado como raíz.

5. Caracterización de extensiones de Galois finitas

PROPOSICIÓN 100. *Sea K una extensión finita de k. Entonces son equivalentes:*

1. *$K|k$ es una extensión de Galois*
2. *$K|k$ es una extensión normal y separable*
3. *$K|k$ es campo de descomposición de algún $f \in k[x]$ separable*

DEMOSTRACIÓN. 1) $\Rightarrow$ 2). Sea $K|k$ una extensión de Galois y $\alpha \in K$.
Si $\{\alpha_i\}_{i=1}^{n}$ es el conjunto de conjugados de α, entonces

$$irr_k(\alpha) = \prod_{i=1}^{n} (x - \alpha_i)$$

Este polinomio es separable puesto que sus raíces son distintas, por lo que la extensión es separable y normal.

2) $\Rightarrow$ 3). Sea $\{\varepsilon_i\}_{i=1}^{n}$ una base de K sobre k y

$$f = \prod_{i=1}^{n} irr_k(\varepsilon_i)$$

Entonces f es separable porque cada $irr_k(\varepsilon_i)$ tiene distintas raíces por hipotesis y f se escinde en K, debe contener a cada ε_i. Por lo cual es el campo de descomposición de f, un polinomio separable.

3) $\Rightarrow$ 1). Vamos a hacer la demostración por inducción sobre todas las extensiones $K|k$ y su grado $[K : k]$

Si $[K:k]=1$ entonces $K=k$ y $Gal(K|k)=e$.

Suponemos que es valido para todas las extensiones de grado $[K:k]<n$.

Factorizamos $f=f_1\cdots f_m$ como producto de irreducibles en $k[x]$. Algún f_i debe tener grado mayor estricto que 1. Sin perdida de generalidad decimos que es f_1. Decimos que $\partial(f_1)=r$. Sea $\alpha\in K$ una raíz de f_1, $f_1(\alpha)=0$. Entonces, $f_1=irr_k(\alpha)$, notamos que $\alpha\notin k$, en caso contrario $\partial(f_1)=1$. Por hipótesis f_1 es separable, por lo que tiene raíces distintas $\alpha_1,...,\alpha_n\in K$.
Observamos que

$$irr_k(\alpha_i)=irr_k(\alpha)$$

para $i=1,...,r$. Así existirán, isomorfismos $\sigma_i:k(\alpha)\to k(\alpha_1)$ tales que $\sigma_i|_k=1_k$ y $\sigma_i(\alpha)=\alpha_i$ para $i=1,...,r$.
Consideramos $k\subseteq k(\alpha_i)\subseteq K$. Entonces K es el campo de descomposición de $f_1\in k(\alpha_i)[x]$, por lo que existe un automorfismo de K, γ_i tal que γ_i extiende a σ_i, es decir, $\gamma_i|_k=1_k$ por lo que $\gamma_i\in Gal(K|k)$. Notamos que $\gamma_i(k(\alpha_j))=k(\alpha_s)$ para algún s, por que un automorfismo de K debe permutar las raíces de un polinomio irreducible f_1.
Ahora tenemos K como extensión de $k(\alpha)$. Entonces

$$[K:k(\alpha)]<[K:k]$$

y K es el campo de descomposición del polinomio separable $f_1\in k(\alpha)[x]$. Por lo que por hipótesis de inducción K es una extensión de Galois de $k(\alpha)$, esto es, $k((\alpha)$ es el campo fijado por $Gal(K|k(\alpha))$. Sabemos que $Gal(K|k(al))$ es un subgrupo de $Gal(K|k)$. De aquí

$$L=Fix(Gal(K|k))\subseteq k(\alpha)$$

Sea $irr_L(\alpha)\in L[x]$, entonces

$$\begin{aligned}\partial(irr_L(\alpha))&=[L(\alpha):L]=[k(\alpha):L]\\&\leq[k(\alpha):k]=\partial(irr_k(\alpha))\end{aligned}$$

y esta es igualdad si y sólo si $k=L$.

Sabemos que $irr_L(\alpha)|irr_k(\alpha)$ y que $irr_k(\alpha)=\prod_{i=1}^{r}(x-\alpha_i)$.
Tenemos que para cada α_i existe $\gamma_i\in Gal(K|k)$ con $\gamma_i(\alpha)=\alpha_i$. Pero $L=Fix(Gal(K|k))$ así

$\gamma_i|_L = 1_L$ y $\gamma_i \in Gal(K|k)$ por lo que $\gamma_i(irr_L(\alpha)) = irr_L(\alpha)$ y así $\gamma_i(irr_L(\alpha)) \in L[x]$, tenemos que:

$$\begin{aligned} irr_L(\alpha)(\alpha_i) =& irr_L(\alpha)(\gamma_i(\alpha)) = \gamma_i(irr_L(\alpha)(\alpha)) \\ =& \gamma_i(0) = 0 \end{aligned}$$

Por lo que α_i es una raíz de $irr_L(\alpha)$ para toda i. Así

$$irr_L(\alpha) = irr_k(\alpha)$$

por lo tanto $L = k$. □

COROLARIO 21. *Si $K|k$ es una extensión de Galois finita y F es un campo intermedio, entonces $K|F$ es de Galois.*

DEMOSTRACIÓN. Por el teorema anterior existe $f \in k[x]$ separable tal que $K = k(f)$. Dado que $k[x] \subseteq F[x]$, observe que $K = F(f)$ y es claro que f es separable como polinomio con coeficientes en F. El resultado se sigue del teorema anterior. □

6. Ejercicios del capítulo

A lo largo de los ejercicios K, k, F, L son campos.

EJERCICIO 147. *Sean $d_1, d_2 \in \mathbb{Z}$ libres de cuadrados con $d_1 \neq \pm d_2$. Demuestre que $\mathbb{Q}(\sqrt{d_1})$ y $\mathbb{Q}(\sqrt{d_2})$ son isomorfos como $\mathbb{Q}$-espacios vectoriales, pero no como campos.*

EJERCICIO 148. *Sea $K|k$ una extensión de campos y $f, g \in k[x]$. Demuestre lo siguiente:*

1. *$f|g$ en $k[x]$ si y sólo si $f|g$ en $K[x]$.*
2. *$(f,g)_{k[x]} = (f,g)_{K[x]}$*
3. *f y g son primos relativos en $k[x]$ si y sólo si lo son en $K[x]$*

EJERCICIO 149.

1. *Sean $f \in k[x]$ irreducible con $\partial(f) = n$ y $K|k$ extensión con $[K:F] = m$. Demuestre que si $(n,m) = 1$, entonces f es irreducible sobre K.*
2. *Demuestre que el polinomio $f = x^5 - 9x^3 + 15x + 6 \in \mathbb{Q}(\sqrt{2}, \sqrt{3})[x]$ es irreducible.*

EJERCICIO 150. *¿Qué relación respecto al orden tienen los subcampos* $\mathbb{Q}(\sqrt{5},\sqrt{7}), \mathbb{Q}(\sqrt{5}+\sqrt{7}) \subseteq \mathbb{R}$*?*

EJERCICIO 151. *Sea* $\alpha \in \mathbb{C}$*. Demuestre que* α *es raíz de un polinomio mónico con coeficientes enteros si y sólo si* $\mathbb{Z}[\alpha]$ *es un grupo abeliano finitamente generado.*

EJERCICIO 152. *Sean* $K|k$ *una extensión del campo y* $\alpha, \beta \in K$ *tales que* α *es algebraico sobre k y* β *es algebraico sobre* $k(\alpha)$*. Demuestre que* β *es algebraico sobre k.*

EJERCICIO 153. *Considere la extensión de campos* $K|k$*,* $\alpha \in K$ *algebraico sobre k y* $f = min_k(\alpha)$*. Demuestre que si f tiene grado impar, entonces* $k(\alpha) = k(\alpha^2)$*.*

EJERCICIO 154. *Sean* L, F *extensiones intermedias de* $K|k$*. Demuestre lo siguiente:*

1. $LF|k$ *es finita si y sólo si* $L|k$ *y* $F|k$ *son finitas*
2. $LF|k$ *es algebraica si y sólo si* $L|k$ *y* $F|k$ *son algebraicas*

EJERCICIO 155.

1. *Sea* $K|k$ *una extensión de campos y* $\alpha \in K \setminus k$ *tal que* $\alpha^2 \in k$*. Demuestre que*

$$k(\alpha) = \{a + b\alpha \mid a, b \in k\}$$

2. *Sea* $K|k$ *una extensión de campos,* $\alpha, \beta \in k$ *tales que* $\alpha\beta \neq 0$ *y existen* $\sqrt{\alpha}, \sqrt{\beta}$*. Demuestre que* $k(\sqrt{\alpha}) = k(\sqrt{\beta})$ *si y sólo si existe* $\gamma \in k$ *tal que* $\alpha\beta = \gamma^2$*.*

EJERCICIO 156.

1. *Demuestre que el conjunto de matrices*

$$C = \left\{ \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \;\middle|\; a, b \in k \right\}$$

forma un campo respecto a la suma y producto usuales de matrices si y sólo si $f = x^2 + 1 \in k[x]$ *no tiene raíces en k.*

2. *Demuestre que C tiene un subcampo isomorfo a k*
3. *Usar los incisos anteriores para construir un campo con 9 elementos y encontrar su característica.*

EJERCICIO 157. *Considere $K|k$ una extensión algebraica y $\alpha \in K$. Demuestre lo siguiente:*

1. *El residuo de dividir $f \in k[x]$ al dividirlo por $x-a$ es igual a $f(\alpha)$.*
2. *α es cero de $f \in k[x]$ si y sólo si $(x-\alpha)|f$ en $K[x]$.*

EJERCICIO 158. *Demuestre que si $f \in k[x]$ es irreducible y $K|k$ es una extensión finita de campos tal que $\partial(f)$ y $[K:k]$ son primos relativos, entonces $f \in K[x]$ es irreducible.*

EJERCICIO 159. *Encontrar el polinomio mínimo y el grado de α sobre k para los siguientes ejemplos:*

1. $k = \mathbb{Q}(i)$ *y* $\alpha = \sqrt{2}$
2. $k = \mathbb{Q}(\sqrt{2})$ *y* $\alpha = \sqrt[3]{2}$
3. $k = \mathbb{Q}$, $\alpha^p = 1$ *con* $\alpha \neq 1$ *y* $p \in \mathbb{N}$ *primo.*

EJERCICIO 160. *Encuentre el grado de las extensiones $K|k$ y una base en los siguientes casos:*

1. $k = \mathbb{R}(x+\frac{1}{x})$, $K = \mathbb{R}(X)$
2. $k = \mathbb{Z}_2$, $K = \mathbb{Z}_2(\alpha)$ *con* $\alpha^4 + \alpha + 1 = 0$.
3. $k = \mathbb{Z}_3$, $K = \mathbb{Z}_3(\alpha)$ *con* $\alpha^3 + \alpha^2 + 2 = 0$.

EJERCICIO 161. *Considere una extensión $K|Q$ con $[K:\mathbb{Q}] = 2$. Demuestre que existe un único $d \neq 1$ libre de cuadrados tal que $K = \mathbb{Q}(\sqrt{d})$.*

EJERCICIO 162. *Demuestre que si $r \in \mathbb{Q}$, entonces* $\sin(rx)$ *y* $\cos(rx)$ *son algebraicos sobre* $\mathbb{Q}$

EJERCICIO 163.

1. *Demuestre que si $K|\mathbb{C}$, entonces $K \cong \mathbb{C}$*
2. *Pruebe que si $K|\mathbb{R}$, entonces $K \cong \mathbb{R}$ ó $K \cong \mathbb{C}$.*

EJERCICIO 164. *Es un hecho conocido que $e, \pi \in \mathbb{R}$ con trascendentes, pero no se sabe si $e+\pi$ y $e\pi$ son trascendentes. Demuestre que al menos uno de dicho números tiene que ser trascendentes. Sugerencia: Analizar una torre de extensiones adecuada.*

EJERCICIO 165. *Considere $A \subseteq \mathbb{C}$ el conjunto cuyos elementos son los complejos que son algebraicos sobre $\mathbb{Q}$.*[2] *Demuestre lo siguiente:*

1. *$A|\mathbb{Q}$ es algebraica*
2. *La extensión $A|\mathbb{Q}$ no es finita*

EJERCICIO 166. *Considere $K|k$ una extensión de campos. Demuestre las siguientes afirmaciones:*

1. *Si K está generado sobre k por un número finito de elementos algebraicos sobre k, entonces la extensión $K|k$ es finita.*
2. *Si $F = \{\alpha \in K \mid \alpha$ es algebraico sobre $k\}$, entonces F es subcampo de K.*

EJERCICIO 167. *Demuestre que $f = x^2 + 1 \in \mathbb{Z}_7[x]$ es irreducible y que $\mathbb{Z}_7[x]/\langle f \rangle$ es un campo con 49 elementos.*

EJERCICIO 168. *Sea $K|k$ extensión tal que $[K : k] < \aleph_0$. Además suponga que cualesquiera dos campos intermedios son comparables respecto a la contención. Demuestre que existe $\alpha \in K$ tal que $K = k(\alpha)$.*

EJERCICIO 169. *Encuentre el grado y una base de la extensión $k(f)|k$ con $f \in k[x]$ para los siguientes casos:*

[2] A dichos elementos se les llaman números algebraicos

1. $k = \mathbb{Q}$ *y* $f = (x^2-2)(x^2-5)$
2. $k = \mathbb{Q}(i)$ *y* $f = x^4-2$
3. $k = \mathbb{Q}(i)$ *y* $f = (x^2-2)(x^2-3)$

EJERCICIO 170. *Determina el campo de descomposición del polinomio* $f = x^4+5x^2+5 \in \mathbb{Q}[x]$ *y el grupo de Galois correspondiente. Sugerencia: Verifica que si* α *es un cero de* f *también lo es* $\alpha^3+3\alpha$.

EJERCICIO 171. *Encuentre el campo de descomposición sobre* $\mathbb{Q}$ *del polinomio* $f = x^4-5x^2+6$ *y encuentra su dimensión sobre* $\mathbb{Q}$.

EJERCICIO 172.

1. *Sea K el campo de descomposición del polinomio* $f = x^n-1 \in k[x]$. *Demuestre que los ceros de este polinomio forman un grupo cíclico finito y que si* α *es un generador de dicho grupo, entonces* $K = k(\alpha)$
2. *Muestra que el número de raíces n-ésimas de la unidad en el campo de descomposición de* $f = x^n-1 \in k[x]$ *es n si y sólo si la característica de k es 0 o primo relativo con n*
3. *Sea K el campo de descomposición de* $f = x^n-a \in k[x]$ *con* $a \in k^*$. *Demuestre que* $K = k(\varepsilon,\alpha)$ *con* ε *generando el grupo de soluciones de* $x^n-1=0$ *en K y* α *es una solución fija de la ecuación* $x^n-a=0$. *Además pruebe que las soluciones de la ecuación* $x^n-a=0$ *son de la forma* $\eta\alpha$ *con* η *variando en todas las raíces n-ésimas de la unidad.*

EJERCICIO 173. *Decir si cada una de las siguientes extensiones* $K|k$ *son normales. En el caso en el que no lo sean, determinar la clausura normal.*

1. $K = \mathbb{Q}(\sqrt[4]{2})$ *y* $k = \mathbb{Q}$
2. $K = \mathbb{Q}(\sqrt[4]{2}, i)$ *y* $k = \mathbb{Q}$
3. $K = \mathbb{Z}_3(x)$ *y* $k = \mathbb{Z}_3(x^4)$

EJERCICIO 174. *Considere una torre de extensiones $K|F|k$. Decir si las siguientes afirmaciones son verdaderas o falsas dando una demostración o un contraejemplo según sea el caso.*

1. *Si $K|F$ y $F|k$ son normales, entonces $K|k$ es normal*
2. *Si $K|k$ es normal, entonces $K|F$ es normal*
3. *Si $K|k$ es normal, entonces $F|k$ es normal*

EJERCICIO 175. *Consideren F,L extensiones intermedias en $K|k$. Demuestre lo siguiente:*

1. *Si $F|k$ y $L|k$ son normales, entonces $FL|k$ y $(F\cap L)|k$ son normales*
2. *Si $F|k$ es normal, entonces $FL|L$ es normal*

EJERCICIO 176. *Sea k un campo de característica $p\in\mathbb{N}$ primo, y sea $\alpha\in k$. Demuestre que el polinomio $f=x^p-\alpha$ es irreducible sobre k o se expresa como $(x-\beta)^p$ en $k[x]$.*

EJERCICIO 177. *Encuentre el campo de descomposición del polinomio $f=x^5-2\in\mathbb{Q}[x]$. Además determine el grado de la extensión que este define sobre $\mathbb{Q}$.*

EJERCICIO 178. *Sea $S\subseteq k[x]$ un subconjunto no vacío. Demuestre que existe un único campo tal que todo elemento de S tiene sus raíces en dicho campo. Este campo se conoce como el campo de descomposición del conjunto S.*

EJERCICIO 179. *Para una extensión algebraica $K|k$, denote por $\overline{K}^{nor}$ al campo de descomposición del conjunto $\{min_k(\alpha)\mid\alpha\in K\}$, al cual se le llamará la clausura normal de K. Demuestre lo siguiente:*

1. *La extensión $\overline{K}^{nor}|k$ es normal y $\overline{K}^{nor}|K$. Además, $\overline{K}^{nor}$ es la $\subseteq$-mínima extensión normal de k que cumple dicha propuedad.*
2. *Si $K=k(\alpha_1,...,\alpha_n)$, entonces $\overline{K}^{nor}$ es el campo de descomposición del conjunto $\{min_k(\alpha_1),...,min_k(\alpha_n)\}$, el cual coincide con el campo de descomposición del polinomio $f=\prod_{i=1}^n min_k(\alpha_i)$.*
3. *Si $K|k$ es finita, entonces $\overline{K}^{nor}|k$ también lo es.*

4. *Si $K|k$ es separable, entonces $\overline{K}^{nor}|k$ es de Galois.*

EJERCICIO 180. *Suponga que se tiene una torre de campos $K|F|k$ donde K es campo de descomposición de $S \subseteq k[x]$ un subconjunto no vacío de polinomios no constantes. Demuestre que K es campo de descomposición de S al considerar a los elementos de dicho conjunto como polinomios con coeficientes en F.*

EJERCICIO 181.

1. *Demuestre que la extensión $\mathbb{Z}_2(x)|\mathbb{Z}_2(x^2)$ no es separable*
2. *Demuestre que la extensión del inciso anterior es normal.*
3. *Para cualquier primo $p \in \mathbb{N}$ dar un ejemplo de una extensión no separable de un campo adecuado de característica p.*

EJERCICIO 182. *Demuestre las siguientes afirmaciones:*

1. *La extensión $K = k(\alpha_1, ..., \alpha_n)|k$ es separable si y sólo si los elementos $\alpha_1, ..., \alpha_n \in L$ son separable sobre k*
2. *La clausura normal de una extensión finita y separable $K|k$ es una extensión separable de k*

EJERCICIO 183. *Considere la torre de extensiones $K|F|k$ con $K|k$ finita. Demuestre que $K|k$ es separable si y sólo si $K|F$ y $F|k$ son separables*

EJERCICIO 184. *Considere una extensión $K|k$. Demuestre que el conjunto de elementos $\alpha \in K$ que son separables sobre k forma un campo intermedio a dicha extensión.*

DEFINICIÓN 70. *Con la notación del ejercicio anterior, dicho campo se conoce como la clausura separable y se denota por K_s. El grado separable de una extensión $K|k$ se define mediante $[K_s : k]$. Este se suele denotar por $[K : k]_s$.*

EJERCICIO 185. *Sea $K|F|k$ una torre de campos con $K|k$ finita. Demuestre que:*

$$[K:k]_s = [K:F]_s[F:k]_s$$

EJERCICIO 186. *Consideren F,L extensiones intermedias en $K|k$. Demuestre que si las extensiones $F|k$ y $L|k$ son separables, entonces las extensiones $FL|k$ y $(F \cap L)|k$ también lo son.*

EJERCICIO 187. *Suponga que $K|k$ es una extensión finita. Demuestre que dicha extensión es de Galois si y sólo si $|Gal(K|k)| = [K:k]$.*

EJERCICIO 188. *Suponga que k es campo con $car(k) \neq 2$ y sea una $K|k$ extensión de grado 2. Demuestre que $K|k$ es de Galois.*

EJERCICIO 189.

1. *Dar un ejemplo de una extensión normal pero no de Galois*
2. *Dar un ejemplo de una extensión separable pero no de Galois*

EJERCICIO 190. *Consideren las torre de extensiones $K|F|k$. Demuestre lo siguiente:*

1. *Si $F|k$ es normal y $\sigma \in Gal(K|k)$, entonces $\sigma F = F$*
2. *Si $K|k$ es normal, entonces $F|k$ es normal si y sólo si para cualquier $\sigma \in Gal(K|k)$ se tiene que $\sigma F = F$.*

EJERCICIO 191.

1. *Considere la torre de extensiones $K|F|k$ con $K|k$ normal finita. Demuestre que el número de diferentes restricciones $\sigma|_L$ de elementos $\sigma \in Gal(K|k)$ es igual a $[F:k]_s$.*
2. *Sea $K|k$ una extensión finita y F un campo algebraicamente cerrado. Además considere un morfismo de campos $\tau : k \to F$. Demuestre que $[K:k]_s$ es igual al número de distintos morfismos de campos $\sigma : K \to F$ tal que $\sigma|_k = \tau$.*

EJERCICIO 192. *Sea $f = x^3 - a \in \mathbb{Q}[x]$ y sea $K = \mathbb{Q}(f)$, el campo de descomposición de f. Obtener $Gal(K|\mathbb{Q})$ y determinar si la extensión $K|\mathbb{Q}$ es de Galois.*

EJERCICIO 193. *Demuestre que el grupo de Hamilton no es el grupo de Galois del campo de descomposición para un polinomio irreducible de grado 4 con coeficientes en algún campo.*

EJERCICIO 194. *Sea $K|k$ una extensión algebraica y $\alpha \in K$. Demuestre que*

$$|Gal(k(\alpha)|k)| = |\{\beta \in k(\alpha) \mid min_k(\alpha)(\beta) = 0\}|$$

EJERCICIO 195. *Sean $K|k$ una extensión algebraica y $\alpha \in K$. Demuestre que la extensión $k(\alpha)|k$ es de Galois si y sólo si:*

1. *$min_k(\alpha)$ se escinde $k(\alpha)[x]$ como producto de factores lineales.*
2. *Para cualesquiera $F = \overline{k(\alpha)}$ y $\beta \in F$, si $(x-\beta)|min_k(\alpha)$ en $F[x]$, entonces $(x-\beta)^2 \nmid min_k(\alpha)$ en $F[x]$.*

Capítulo 4

Teoría de Galois

El presente capítulo está dedicado a establecer y demostrar el teorema fundamental de la teoría de Galois para extensiones finitas, así como las aplicaciones más famosas de este. Además se tratará un poco del problema inverso de la teoría de Galois. Así como sucedió en el capítulo pasado, el desarrollo de la teoría está basado en la formulación moderna debida a Emil Artin, quien en su famoso libro de texto [**1**] dio la primera formulación moderna de dicha teoría.

1. Teorema fundamental de la teoría de Galois

Esta sección está dedicada a demostrar el teorema más importante del curso y uno de los teoremas fundamentales de la matemática moderna pues este se ha encontrado en muchos otros contextos fuera del álgebra como lo es en topología algebraica (aplicaciones cubrientes regulares) o geometría algebraica (cubrientes étale finitos), incluso se ha estudiado de forma puramente categórica (categorías de Galois).

Para empezar con el planteamiento de dicho teorema observe que para una extensión algebraica $K|k$, existe una asignación dada por tomar el campo fijo:

$$K^{-} : Sub(Gal(K|k)) \to \mathscr{E}_{K|k}$$

donde $Sub(Gal(K|k))$ es la retícula de subgrupos de $Gal(K|k)$ y $\mathscr{E}_{K|k}$ es la retícula de campos intermedios en la extensión $K|k$.

Uno de los incisos más importantes del teorema buscado dice que si la extensión $K|k$ es de Galois y finita, la asignación anterior es una biyección. En la búsqueda de este resultado se requieren algunos resultados previos que de hecho son importantes por sí mismos. Para establecerlos se requiere introducir un concepto.

DEFINICIÓN 71. *Un carácter de un grupo G en un campo k, es un morfismo* $\chi : G \to k^*$

EJEMPLO 64. *Todo morfismo de campos* $F \to E$ *da lugar a un carácter*

$$\chi : G \to E^*,$$

donde $G = F^*$.

La teoría de carácteres juega un papel muy importante en muchas áreas de la matemática, por ejemplo, estos permiten determinar las representaciones de un grupo finito. Toda esta interesante teoría no será de nuestro interés pues para nuestros fines requerimos de la siguiente definición y resultado

DEFINICIÓN 72. *Un conjunto de caracteres $\{\chi_1, ..., \chi_n\}$ de un grupo G en un campo k son independientes si siempre que*

$$\sum_{i=1}^{n} \lambda_i \chi_i = 0,$$

se tiene que $\lambda_1 = \cdots = \lambda_n = 0$. En otro caso se dirá que los caracteres son dependientes.

PROPOSICIÓN 101. *(Dirichlet) Sea $\{\chi_1, ..., \chi_n\}$ un conjunto de caracteres de un grupo G en k distintos dos a dos. Entonces $\{\chi_1, ..., \chi_n\}$ es independiente.*

DEMOSTRACIÓN. (Artin) Por inducción generalizada en n.

Base: $n = 1$. Es claro pues los carácteres no tienen a 0 en su imagen.

Paso inductivo: Si el resultado vale para conjuntos de caracteres con menos de n elementos y suponemos que

$$\sum_{i=1}^{n} \lambda_i \chi_i = 0$$

con algún coeficiente no cero, uno de los cuales podemos suponer que es $\lambda_1 \neq 0$. Como $\chi_1 \neq \chi_n$, sea $g \in G$ tal que $\chi_1(g) \neq \chi_n(g)$. Dado que para cada $h \in G$,

$$\sum_{i=1}^{n} \lambda_i \chi_i(h) = 0, \tag{2}$$

en particular esta igualdad implica que para cualquier $h \in G$,

$$\sum_{i=1}^{n} \lambda_i \chi_i(gh) = 0. \tag{3}$$

Por otro lado, al multiplicar por $\chi_n(g)$ a 2, se deduce que:

$$\sum_{i=1}^{n} \lambda_i \chi_n(g) \chi_i(h) = 0 \tag{4}$$

Al tomar la diferencia de 3 y 4 se tiene que

$$0 = \sum_{i=1}^{n} \lambda_i (\chi_i(g) - \chi_n(g)) \chi_i(h) = \sum_{i=1}^{n-1} \lambda_i (\chi_i(g) - \chi_n(g)) \chi_i(h)$$

Ademas, esto vale para cada $h \in G$, por lo que al usar la hipótesis de inducción cada coeficiente debe ser cero, en particular,

$$\chi_1(g) - \chi_n(g) = 0,$$

lo que es una contradicción. □

El siguiente ingrediente para establecer el resultado buscado se presenta a continuación. Este es una aplicación del resultado anterior.

PROPOSICIÓN 102. *Sea $G = \{\sigma_1, ..., \sigma_n\} \subseteq Aut(K)$ un grupo de orden n y $k = K^G$. Entonces,*

$$[K : k] = n$$

DEMOSTRACIÓN. (Artin) La igualdad se va a probar por antisimétria.

Afirmación 1: $[K : k] \geq n$.

Procediendo por contradicción, suponga que $[K : k] < n$. Sea $\{x_1, ..., x_r\}$ base de K como $k-$espacio. Considere el sistema de ecuaciones:

$$\begin{pmatrix} \sigma_1(x_1) & \cdots & \sigma_n(x_1) \\ \vdots & \ddots & \vdots \\ \sigma_1(x_r) & \cdots & \sigma_n(x_r) \end{pmatrix} \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix} = 0$$

Este sistema tiene r ecuaciones, n incógnitas y $r < n$, entonces tiene una solución no trivial, digamos

$$(\alpha_1, ..., \alpha_n) \in K^n$$

Esto dice, que para cada $k \in \{1, ..., r\}$

$$\sum_{j=1}^{n} \alpha_j \sigma_j(x_k) = 0$$

Ahora considere $x \in K$ y expresamos x como $k-$combinación lineal de la base

$$x = \sum_{i=1}^{r} \lambda_i x_i$$

Entonces,

$$\begin{aligned} \sum_{j=1}^{n} \alpha_j \sigma_j(x) &= \sum_{j=1}^{n} \sum_{i=1}^{r} \alpha_j \sigma_j(\lambda_i x_i) \\ &= \sum_{j=1}^{n} \sum_{i=1}^{r} \alpha_j \lambda_i \sigma_j(x_i) \\ &= \sum_{i=1}^{r} \lambda_i \left(\sum_{j=1}^{n} \alpha_j \sigma_j(x_i) \right) \\ &= 0 \end{aligned}$$

Como el elemento $x \in K$ fue arbitrario, esto implica que

$$\sum_{j=1}^{n} \alpha_j \sigma_j = 0.$$

con algunos coeficientes no triviales, lo cual contradice el teorema de caracteres de Dirichlet. Por lo tanto $[K : k] \geq n$.

Afirmación 2: $[K : k] \leq n$.

Procediendo por contradicción, suponga que $[K : k] > n$. Dado que G es un grupo, podemos suponer sin pérdida de generalidad que $\sigma_1 = 1_K$. Considere $\{x_1, ..., x_{n+1}\} \subseteq K$ un conjunto $k-$linealmente independiente y considere el sistema de ecuaciones:

$$\begin{pmatrix} \sigma_1(x_1) & \cdots & \sigma_n(x_{n+1}) \\ \vdots & \ddots & \vdots \\ \sigma_1(x_r) & \cdots & \sigma_n(x_{n+1}) \end{pmatrix} \begin{pmatrix} y_1 \\ \vdots \\ y_{n+1} \end{pmatrix} = 0$$

Dicho sistema tiene $n+1$ incógnitas y n ecuaciones, por lo que existe una solución no trivial, digamos

$$(\beta_1, ..., \beta_{n+1}) \in K^{n+1}$$

con un mínimo número de elementos igual a 0; sea s el número de valores no cero. Salvo una permutación de subindices se puede suponer que la solución tiene la forma:

$$(\beta_1, ..., \beta_s, 0, ..., 0) \in K^{n+1}$$

Observe que $s > 1$ y ademas, podemos suponer sin perdida de generalidad que $\beta_s = 1$. Note que no puede suceder que $\{\beta_1, ..., \beta_s\} \subseteq k$ pues en caso contrario, como

$$0 = \sum_{j=1}^{n+1} \beta_j \sigma_1(x_j) = \sum_{j=1}^{s} \beta_j \sigma_1(x_j),$$

lo que implica que

$$\sum_{j=1}^{s} \beta_j x_j = 0,$$

lo que contradice la independencia lineal de $\{x_1, ..., x_s\}$. Entonces podemos suponer que $\beta_1 \notin k$. Por lo tanto, para $m \in \{1, ..., n\}$ se tiene que:

$$\sum_{j=1}^{s} \beta_j \sigma_m(x_j) = 0 \tag{5}$$

Como existe $\sigma_\ell \in G$ tal que $\sigma_\ell(\beta_1) \neq \beta_1$ y al ser G un grupo, para cada $\sigma_i \in G$ existe $\sigma_{t(i)} \in G$ tal que

$$\sigma_i = \sigma_\ell \sigma_{t(i)}.$$

Al aplicar σ_ℓ a 5 para $m = t(i)$, se tiene que:

$$\sigma_\ell\left(\sum_{j=1}^{s}\beta_j\sigma_{t(i)}(x_j)\right) = 0.$$

Así

$$\sum_{j=1}^{s}\sigma_\ell(\beta_j)\sigma_i(x_j) = 0 \tag{6}$$

Al tomar la diferencia de 5 y 6 se tiene que:

$$\sum_{j=1}^{s-1}(\beta_j - \sigma_\ell(\beta_j))\sigma_i(x_j) = 0,$$

igualdad que vale para cada $i \in \{1,...,n\}$. Como $\beta_1 - \sigma_\ell(\beta_1) \neq 0$, la igualdad anterior tiene menos que s coeficientes no cero, lo que es una contradicción. □

Los resultados tratados permiten establecer el siguiente, el cual es una parte clave del teorema fundamental.

COROLARIO 22.

1. *Sea G un grupo finito de automorfismos de K y $k = K^G$. Entonces $Gal(K|k) \subseteq G$.*
2. *Sean G_1 y G_2 dos grupos finitos de automorfismos de K distintos y sean $k_1 = K^{G_1}$ y $k_2 = K^{G_2}$. Entonces,*

$$k_1 \neq k_2$$

DEMOSTRACIÓN. Para 1, si existe $\sigma \in Gal(K|k)$ tal que $\sigma \notin G$, entonces k debería ser fijado por al menos $|G|+1$ automorfismos, lo cual contradice el resultado anterior, pues

$$[K:k] = |G|$$

En lo que respecta a 2, se va probar la contrapositiva: si $k_1 = k_2$, entonces k_1 es fijado por G_2, luego $Gal(K|k_1) \subseteq G_2$. Además observe que $G_1 \subseteq Gal(K|k_1)$ y esto prueba que $G_1 \subseteq G_2$. Además, la contención $G_1 \subseteq G_2$ se obtiene de forma análoga. □

Regresemos a la asignación

$$K^- : Sub(Gal(K|k)) \to \mathscr{E}_{K|k}.$$

El resultado anterior dice que si $Gal(K|k)$ es finito, esta asignación es inyectiva. Al recordar que la meta será demostrar que cuando la extensión $K|k$ es de Galois finita, dicha función es una biyección, es de esperar que haya un resultado que relacione la finitud de una extensión con el cardinal del grupo de Galois. Dicho resultado se presenta a continuación.

PROPOSICIÓN 103. *Sea $K|k$ una extensión finita. Entonces, $Gal(K|k)$ es finito. Más aún,*

$$|Gal(K|k)| \leq [K:k]$$

DEMOSTRACIÓN. Por hipótesis $K = k(\alpha_1, ..., \alpha_n)$ con $n = [K:k]$. Observe que como cada $\sigma \in Gal(K|k)$ debe mandar una raíz de $min_k(\alpha_i)$ en sí misma, entonces $Gal(K|k)$ es finito, por lo tanto, escribamos $Gal(K|k) = \{\sigma_1, ..., \sigma_m\}$. Considere el sistema de ecuaciones:

$$\begin{pmatrix} \sigma_1(\alpha_1) & \cdots & \sigma_m(\alpha_1) \\ \vdots & \ddots & \vdots \\ \sigma_1(\alpha_n) & \cdots & \sigma_m(\alpha_n) \end{pmatrix} \begin{pmatrix} y_1 \\ \vdots \\ y_m \end{pmatrix} = 0$$

Note que si $n < m$, existen más incógnitas que ecuaciones, por lo que dicho sistema tiene una solución no trivial, digamos $(\beta_1, ..., \beta_m) \in K^m$, es decir, para cada $j \in \{1, ..., n\}$,

$$\sum_{i=1}^{m} \beta_i \sigma_i(\alpha_j) = 0$$

Observe que dado cualquier $\alpha \in K$, existen $\lambda_1, ..., \lambda_n \in k$ tales que $\alpha = \sum_{j=1}^{n} \lambda_j \alpha_j$. Luego,

$$\begin{aligned} \sum_{i=1}^{m} \beta_i \sigma_i(\alpha) &= \sum_{i=1}^{m} \beta_i \sigma_i \left(\sum_{j=1}^{n} \lambda_j \alpha_j \right) \\ &= \sum_{i=1}^{m} \sum_{j=1}^{n} \beta_i \lambda_j \sigma_i(\alpha_j) \\ &= \sum_{j=1}^{n} \lambda_j \left(\sum_{i=1}^{m} \beta_i \sigma_i(\alpha_j) \right) \\ &= 0 \end{aligned}$$

Dado que los elementos de $Gal(K|k)$ son caracteres distintos al considerar $G = K^*$, y la igualdad anterior implica que la combinación $\sum_{i=1}^{m} \beta_i \sigma_i = 0$, entonces todos los coeficientes deben ser cero, lo que es una contradicción. Por lo tanto, no puede suceder que $n < m$ y así, $m \leq n$. □

COROLARIO 23. *Sea $K|k$ una extensión de Galois finita. Entonces,*

$$|Gal(K|k)| = [K:k]$$

DEMOSTRACIÓN. Por la proposición 103, basta demostrar que $[K:k] \leq |Gal(K|k)|$. Para ver que esto sucede, por el teorema de caracterización de extensiones de Galois finitas existe $f \in k[x]$ separable tal que $K = k(f)$. Si $\{\alpha_1, ..., \alpha_n\} \subseteq K$ son la raíces diferentes de f, entonces vea que para cada $i \in \{1, ..., n\}$ se puede definir $\sigma_i \in Gal(K|k)$ con

$$\sigma_i(\alpha_j) = \begin{cases} \alpha_i & \text{Si } j = 1 \\ \alpha_1 & \text{Si } j = i \\ \alpha_j & \text{e.o.c} \end{cases}$$

Esto muestra la desigualdad buscada. □

Antes de dar el resultado que se busca, se requiere de un resultado previo.

LEMA 9. *Sean $H \leq G \leq Gal(K|k)$. Si $F = K^H$, entonces para cualquier $\sigma \in G$,*

$$\sigma(F) = K^{\sigma H \sigma^{-1}}$$

DEMOSTRACIÓN. Sean $\alpha \in F$ y $\tau \in H$. Observe que

$$\sigma\tau\sigma^{-1}(\sigma(\alpha)) = \sigma\tau(\alpha) = \sigma(\alpha)$$

Esto prueba que

$$\sigma(F) \subseteq K^{\sigma H \sigma^{-1}}$$

Para la contención restante, sea $\alpha \in K^{\sigma H \sigma^{-1}}$. Esto dice que para cada $\tau \in H$, $\sigma\tau\sigma^{-1}(\alpha) = \alpha$, lo que implica que para todo $\tau \in H$, $\tau\sigma^{-1}(\alpha) = \sigma^{-1}(\alpha)$. Es decir, $\sigma^{-1}(\alpha) \in K^H = F$, por lo que $\alpha \in \sigma(F)$. □

PROPOSICIÓN 104. *(Teorema fundamental de la teoría de Galois -para extensiones finitas-) Sea $K|k$ una extensión de Galois finita. Entonces,*

1. *La función*

$$K^- : Sub(Gal(K|k)) \to \mathscr{E}_{K|k}$$

establece una correspondencia biyectiva entre campos intermedios a la extensión $K|k$ y subgupos de $Gal(K|k)$. Esta correspondencia invierte el orden.

2. *Para $F \in \mathscr{E}_{K|k}$, la extensión $F|k$ es normal si y sólo si $Gal(K|F) \trianglelefteq Gal(K|k)$. Este es el caso si y sólo si $F|k$ es una extensión de Galois. En tal caso*

$$Gal(F|k) \cong Gal(K|k)/Gal(K|F)$$

3. *Para cada $F \in \mathscr{E}_{K|k}$,*

$$[F : k] = [Gal(K|k) : Gal(K|F)]$$

$$[K : F] = |Gal(K|F)|$$

DEMOSTRACIÓN. Para 1, como se menciono anteriormente dicha función es inyectiva. Para la suprayectividad, sea $F \in \mathscr{E}_{K|k}$ y considere $Gal(K|F) \leq Gal(K|k)$. Ademas, como la extensión es de Galois y finita, existe $f \in k[x]$ separable tal que

$$K = k(f)$$

Dado que $f \in F[x]$, observe que $K = F(f)$. Esto muestra que la extensión $K|F$ es de Galois, luego la definición dice que $F = K^{Gal(K|F)}$, lo que muestra la suprayectividad. Para concluir observe que es claro que si $G, H \in Sub(Gal(K|k))$ y $G \subseteq H$, entonces $K^H \subseteq K^G$, por lo que dicha biyección invierte el orden.

Respecto a 3 la segunda igualdad es clara, de hecho esta es equivalente a que la extensión $K|F$ es de Galois. Para la primera igualdad, por multiplicatividad del índice

$$\begin{aligned} |Gal(K|k)| &= [K : k] \\ &= [K : F][F : k] \\ &= |Gal(K|F)|[F : k] \end{aligned}$$

Dado que

$$|Gal(K|k)| = |Gal(K|F)|[Gal(K|k) : Gal(K|F)]$$

se deduce el resultado.

Respecto a 2, observe primero que como $K|k$ es en particular separable, entonces $F|k$ es separable para cada $F \in \mathscr{E}_{K|k}$. Entonces, por el teorema de caracterización de extensiones de Galois finitas, $F|k$ es normal si y sólo si es de Galois. Ahora demostraremos el bicondicional de la afirmación.

$\Leftarrow$) Suponga que $Gal(K|F) \trianglelefteq Gal(K|k)$. Del lema anterior, para cualquier $\sigma \in Gal(K|k)$,

$$\begin{aligned}\sigma(F) =& K^{\sigma Gal(K|F)\sigma^{-1}}\\ =& K^{Gal(K|F)}\\ =& F\end{aligned}$$

Así, al considerar la asignación

$$\begin{aligned} f : Gal(K|k) &\longrightarrow Gal(F|k)\\ \sigma &\longmapsto \sigma\mid_F,\end{aligned} \tag{7}$$

esta es una función. Ademas es claramente un morfismo de grupos. Por otro lado,

$$Nuc(f) = \{\sigma \in Gal(K|k) : \sigma|_F = 1_F\} = Gal(K|F)$$

Entonces, el primer teorema de isomorfismo (para grupos) implica que

$$Gal(K|k)/Gal(K|F) \cong Im(f)$$

Por otro lado, dado $\sigma \in Gal(F|k)$, observe que como la extensión $K|F$ es de Galois finita, K es campo de descomposición de un polinomio con coeficientes en F. Así, por el lema de extensión de isomorfismos, existe $\tilde{\sigma} : K \to K$ automorfismo tal que $\tilde{\sigma}|_F = \sigma$. En particular $\tilde{\sigma}|_k = 1_k$. Por lo tanto $f(\tilde{\sigma}) = \sigma$, lo que prueba que f es un morfismo suprayectivo, entonces

$$Im(f) = Gal(F|k),$$

lo que concluye la afirmación.

$\Rightarrow$) Suponga que $F|k$ es de Galois y sea $\sigma \in Gal(K|k)$. Del teorema de caracterización de extensiones de Galois finitas, existe $f \in k[x]$ separable tal que $F = k(f)$. Dado que $\sigma(f) = f$, entonces σ permuta las raíces de f. En particular $\sigma(F) = F$. Al usar nuevamente el lema previo se tiene que

$$K^{Gal(K|F)} = F = \sigma(F) = K^{\sigma Gal(K|F)\sigma^{-1}}$$

De 1, se deduce que

$$Gal(K|F) = \sigma Gal(K|F)\sigma^{-1},$$

lo que prueba que

$$Gal(K|F) \trianglelefteq Gal(K|k)$$

$\square$

Las siguientes secciones tendrán como objetivo el uso de este resultado. En este momento presentaremos otras formas en las que se presenta el TFTG en la literatura. Para la primera de ellas se presenta el siguiente ejercicio de carácter retícular.

EJERCICIO 196. *Para $K|k$ extensión finita de Galois. Sean $F,L \in \mathscr{E}_{K|k}$ con $F = K^G$ y $L = K^H$. Demuestre lo siguiente:*

1. $FL = K^{(G\cap H)}$
2. $F \cap L = K^{G+H}$

El resultado anterior dice que la función

$$K^- : Sub(Gal(K|k))^{op} \to \mathscr{E}_{K|k}$$

es un morfismo de retículas. Por lo tanto, una primera forma de parafrasear el TFTG es:

PROPOSICIÓN 105. *La asignación $K^- : Sub(Gal(K|k))^{op} \to \mathscr{E}_{K|k}$ es un isomorfismo de retículas.*

Si el lector maneja un poco de lenguaje categórico, recuerde que todo orden parcial tiene una estructura de categoría. Por lo que el resultado anterior se puede parafrasear como sigue:

PROPOSICIÓN 106. *Sea $\mathscr{C}$ la categoría asociada al orden parcial $Sub(Gal(K|k))$ y $\mathscr{D}$ la categoría asociada al orden parcial $\mathscr{E}_{K|k}$. Entonces existe un isomorfismo de categorías:*

$$\mathscr{C}^{op} \cong \mathscr{D}$$

Observe que ambos resultados reescriben únicamente la parte de la biyección en el TFTG, cosa que es de esperarse pues en las teorías correspondientes (la de órdenes parciales en el primer caso y categorías en el segundo), sólo la idea de biyección que preserva estructura está axiomátizada en dichos términos; las otras afirmaciones son algebraicas, por lo que habría que decirse un poco mas para poder obtener análogos categóricos de estas. Además, a dichos resultados se suma otra formulación usando la categoría de órbitas de un grupo, sin embargo, por obvias razones esto no será discutido en mayor profundidad. Lo que si se quiere discutir un poco es que la hipótesis de finitud fue fundamental en todo momento pues para extensiones no necesariamente finitas hay que cambiar las hipótesis en los subgrupos de $Gal(K|k)$ pues resulta que $Gal(K|k)$ tiene una topología (que en nuestro caso es la discreta) y el TFTG establece nuevamente una biyección pero entre subgrupos cerrados de $Gal(K|k)$ y extensiones intermedias. Previamente a la formulación de este teorema que se conoce como TFTG no necesariamente finitas (el cual se debe a Krull), Dedekind demuestra que sólo en el caso de subgrupos cerrados se tiene una correspondencia pues si el subgrupo no es cerrado, este no tiene porque corresponder a un campo intermedio como se muestra en

un ejemplo que él mismo construye usando una extensión de $\mathbb{Q}$ y que de hecho motivó a Krull a generar un argumento aplicable a cualquier extensión infinitaria.

Lo anterior empieza a mostrar la complejidad que tiene la teoría en el contexto infinito. La pregunta entonces es si vale la pena estudiar esta teoría; desde el punto de vista teórico, la respuesta es si, pues como se hace ver en las otras versiones del TFTG, esta teoría encierra ideas muy potentes. La formulación infinita ya lleva una contraparte topológica, por lo que esta debe ser razón suficiente para justificar la idea. Sin embargo y de forma mas contundente, la teoría infinita contiene como ejemplo $Gal(\bar{\mathbb{Q}}|\mathbb{Q})$. Este grupo es muy importante en el estudio moderno de la teoría de números pues Serre comentó en alguno de sus libros que toda la teoría de números se encontraba contenida en este grupo. Estas últimas líneas lo único que pretenden es hacer ver que hay mucho mas por explorar en la teoría de Galois, cosa que no haremos pues nos concentraremos en las aplicaciones de la teoría finita, pero creo que vale la pena tener idea de que esta es un área en la que hoy en día se hace investigación.

1.1. Dos aplicaciones teóricas del TFTG. Como se mencionó anteriormente la definición dada de extensión de Galois es debida a Artin y su importancia radica en que esta no depende de si la extensión es finita. Por otro lado, como primer acercamiento a la teoría de Galois se suele presentar una definición que sirve para extensiones finitas la cual dice que una extensión (finita) es de Galois si se cumple la igualdad en la desigualdad de la proposición 103. El primer resultado a discutir dice que dichas definiciones coinciden. Para este se requiere de un resultado previo.

PROPOSICIÓN 107. *Sea $K|k$ una extensión de campos, $G \in Sub(Gal(K|k))$ y $F \in \mathscr{E}_{K|k}$. Entonces, $F \subseteq K^G$ si y sólo si $G \subseteq Gal(K|F)$.*

DEMOSTRACIÓN. $\Rightarrow$) Si $F \subseteq K^G$, entonces observe que $Gal(K|K^G) \subseteq Gal(K|F)$. Además observe que $G \subseteq Gal(K|K^G)$, de lo que se deduce el resultado.

$\Leftarrow$) Si $G \subseteq Gal(K|F)$, como el tomar campo fijo invierte el orden, se tiene que $K^{Gal(K|F)} \subseteq K^G$. El resultado se sigue al recordar que $F \subseteq K^{Gal(K|F)}$. □

En el lenguaje de la teoría de órdenes el resultado anterior dice que las funciones $Gal(K|\_)$ y K^{-} definen una **conexión de Galois**. Además de este resultado se deduce lo siguiente:

COROLARIO 24. *Sea $K|k$ una extensión de campos. Entonces, la extensión $K|K^{Gal(K|k)}$ es de Galois.*

DEMOSTRACIÓN. De acuerdo a la definición, basta con ver que $K^{Gal(K|K^{Gal(K|k)})} \subseteq K^{Gal(K|k)}$, lo que por el resultado anterior es equivalente a probar que $Gal(K|k) \subseteq Gal(K|K^{Gal(K|K^{Gal(K|k)})})$, lo que es claro. □

Con el resultado anterior se puede dar el teorema de caracterización buscado.

PROPOSICIÓN 108. *Sea $K|k$ una extensión finita. Son equivalentes:*

1. *$K|k$ es de Galois*
2. $|Gal(K|k)| = [K:k]$

DEMOSTRACIÓN. $1 \Rightarrow 2)$ Es directamente el corolario 23.

$2 \Rightarrow 1)$ La extensión $K|K^{Gal(K|k)}$ es de Galois con grupo de Galois $Gal(K|k)$. Entonces

$$[K:k] = |Gal(K|k)| = |Gal(K|K^{Gal(K|k)})| \leq [K:K^{Gal(K|k)}] \leq [K:k]$$

De esto se deduce que $[K^{Gal(K|k)}:k] = 1$ y de esto que $k = K^{Gal(K|k)}$. □

El segundo resultado a presentar será importante para una sección posterior, sin embargo, aprovechamos para presentarlo en este punto.

PROPOSICIÓN 109. *(Teorema de las irracionalidades naturales) Sean $K|k$ una extensión de campos y F,L extensiones intermedias tales que $F|k$ es de Galois finita y $L|k$ es una extensión algebraica. Entonces $FL|L$ es de Galois y*

$$Gal(FL|L) \cong Gal(F|F \cap L)$$

DEMOSTRACIÓN. Para empezar observe que $F = k(f)$ para $f \in k[x]$ separable. Al usar la proposición 81 se deduce que $FL|L$ es finita y más aún es generada por los generadores de F que son las raíces de f. Luego, al considerar $f \in L[x]$, note que FL es campo de descomposición de dicho polinomio el cual es separable sobre $L[x]$ pues lo es sobre $k[x]$. Así, el teorema de caracterización de extenciones de Galois finita implica que la extesión $FL|L$ es de Galois.

Considere la asignación

$$f : Gal(FL|L) \to Gal(F|k)$$

definida por

$$f(\sigma) = \sigma|_F.$$

Observe que f está bien definida pues al ser la extensión $F|k$ en particular normal, entonces $\sigma(F) \subseteq F$. Además, de esta última afirmación se deduce que f es un morfismo de grupos. Más aún, es un monomorfismo de grupos pues dado $\sigma \in Nuc(f)$, por definición $\sigma|_F = 1_F$.

Además, por definición de f se tiene que $\sigma|_L = 1_L$. Luego, por el ejercicio 145 esto implica que $\sigma|_{FL} = 1_{FL}$, lo que prueba la contención no trivial en la igualdad $Nuc(f) = \{1_{FL}\}$ y prueba la afirmación.

Por otro lado, dado que $Im(f) \in Sub(Gal(F|k))$, el TFTG afirma que existe un único $E \in \mathscr{E}_{F|k}$ tal que $Im(f) = Gal(F|E)$.

Afirmación: $E = F \cap L$. En efecto, sea $\alpha \in F \cap L$. Entonces para cualquier $\sigma \in Gal(FL|L)$ se tiene que $\sigma|_F(\alpha) = \alpha$, lo que dice que $\alpha \in F^{Im(f)} = E$. Para la contención restante observe que por construcción $E \subseteq F$ es un subcampo. Por otro lado, dado $\alpha \in E$, se tiene que para cualquier $\sigma \in Gal(FL|L)$ se tiene que $\sigma|_F(\alpha) = \alpha$, lo que implica que $\alpha \in FL^{Gal(FL|L)} = L$ y por lo tanto que $E \subseteq L$. Esto muestra la contención restante y el isomorfismo es consecuencia del primer teorema de isomorfismo para grupos. □

1.2. Algunos ejemplos particulares. Esta pequeña subsección está dedicada a desarrollar ejemplos donde se muestre cómo se usa el TFTG en la práctica para ejemplos concretos.

EJEMPLO 65. *Considere la extensión $\mathbb{Q}(\sqrt{2})|\mathbb{Q}$ la cual es de Galois pues $\mathbb{Q}(\sqrt{2}) = \mathbb{Q}(x^2-2)$ y $x^2-2 \in \mathbb{Q}[x]$ es separable.*[1].

Por la proposición 108 se deduce que $|Gal(\mathbb{Q}(\sqrt{2})|\mathbb{Q})| = 2$ y por lo tanto,

$$Gal(\mathbb{Q}(\sqrt{2})|\mathbb{Q}) \cong \mathbb{Z}_2$$

De esto se deduce que el TFTG implica que $|\mathscr{E}_{\mathbb{Q}(\sqrt{2})|\mathbb{Q}}| = 2$, por lo que la extensión tiene únicamente como campos intermedios a las extensiones triviales. Así,

$$\mathscr{E}_{\mathbb{Q}(\sqrt{2})|\mathbb{Q}} = \{\mathbb{Q}, \mathbb{Q}(\sqrt{2})\}$$

Es común representar mediante un diagrama de Hasse la retícula de subgrupos del grupo de Galois de una extensión de Galois, así como la retícula de campos intermedios. Esto es trivial para los ejemplos tratados, pero se va a incluir por completez.

[1] Una segunda prueba de este hecho se puede hacer mediante el ejercicio 188

$$\begin{array}{ccc} Gal(\mathbb{Q}(\sqrt{2})|\mathbb{Q}) \cong \mathbb{Z}_2 & & \mathbb{Q}(\sqrt{2})^{Gal(\mathbb{Q}|\mathbb{Q})} = \mathbb{Q}(\sqrt{2}) \\ \Big| & \cong & \Big| \\ Gal(\mathbb{Q}|\mathbb{Q}) = 0 & & \mathbb{Q}(\sqrt{2})^{Gal(\mathbb{Q}(\sqrt{2})|\mathbb{Q})} = \mathbb{Q} \end{array}$$

Nota: Observe que el argumento del ejemplo anterior es aplicable a cualquier extensión de grado dos en un campo con característica distinta a 2.

EJEMPLO 66. *En el capítulo anterior (ejemplo 60) se estudió la extensión* $\mathbb{Q}(\sqrt{2},\sqrt{3})|\mathbb{Q}$*, la cual se demostró que es de Galois y que*

$$Gal(\mathbb{Q}(\sqrt{2},\sqrt{3})|\mathbb{Q}) \cong \mathbb{Z}_2 \oplus \mathbb{Z}_2$$

A continuación se usará el TFTG para determinar los campos intermedios de la extensión. Observe que para $Gal(\mathbb{Q}(\sqrt{2},\sqrt{3})|\mathbb{Q})$ *se tienen 5 subgrupos, a saber:*

$$G_1 = 0$$
$$G_2 = \mathbb{Z}_2 \oplus 0 = \langle (1,0) \rangle \cong \mathbb{Z}_2$$
$$G_3 = 0 \oplus \mathbb{Z}_2 = \langle (0,1) \rangle \cong \mathbb{Z}_2$$
$$G_4 = \langle (1,1) \rangle \cong \mathbb{Z}_2$$
$$G_5 = Gal(\mathbb{Q}(\sqrt{2},\sqrt{3})|\mathbb{Q})$$

Dado que $Gal(\mathbb{Q}(\sqrt{2},\sqrt{3})|\mathbb{Q})$ *es abeliano, las extensiones correspondientes todos los subgrupos anteriores con todas de Galois. Además, hay cinco campos intermedios en la extensión que se está considerando, para determinar cada uno de estos analicemos con más cuidado el ejemplo.*

Recuerde que $Gal(\mathbb{Q}(\sqrt{2},\sqrt{3})|\mathbb{Q}) = \{1, \sigma_2, \sigma_3, \sigma_4\}$ *donde cada* σ_i *estada determinado por lo que hacía a los generadores como sigue:*

$$\sigma_2(\sqrt{2}) = -\sqrt{2}, \quad \sigma_2(\sqrt{3}) = \sqrt{3}$$
$$\sigma_3(\sqrt{2}) = \sqrt{2}, \quad \sigma_3(\sqrt{3}) = -\sqrt{3}$$
$$\sigma_4\sqrt{2}) = -\sqrt{2}, \quad \sigma_4(\sqrt{3}) = -\sqrt{3}$$

Con estas etiquetas observe que:

$$G_2 = \langle \sigma_2 \rangle, \quad G_3 = \langle \sigma_3 \rangle, \quad G_4 = \langle \sigma_4 \rangle$$

Observe que las elecciones del generador de G_2 y G_3 son arbitrarias entre σ_2 y σ_3, la que queda obligada es la de G_4 pues $\sigma_4 = \sigma_2\sigma_3$.

Con lo anterior ahora se pueden determinar los campos fijos en cada caso. Vamos a hacer un caso de forma explícita:

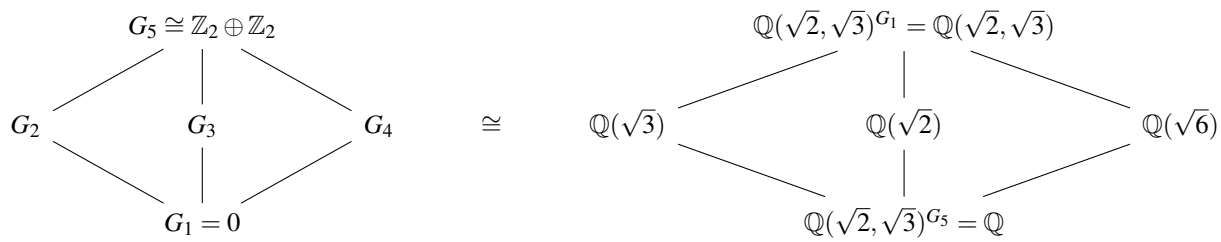
$$\begin{aligned}
\mathbb{Q}(\sqrt{2},\sqrt{3})^{G_2} =& \{a+b\sqrt{2}+c\sqrt{3}+d\sqrt{6} \mid \sigma_2(a+b\sqrt{2}+c\sqrt{3}+d\sqrt{6}) = a+b\sqrt{2}+c\sqrt{3}+d\sqrt{6}\} \\
=& \{a+b\sqrt{2}+c\sqrt{3}+d\sqrt{6} \mid a-b\sqrt{2}+c\sqrt{3}-d\sqrt{6}) = a+b\sqrt{2}+c\sqrt{3}+d\sqrt{6}\} \\
=& \{a+b\sqrt{2}+c\sqrt{3}+d\sqrt{6} \mid b\sqrt{2}+d\sqrt{6} = 0\} \\
=& \{a+b\sqrt{2}+c\sqrt{3}+d\sqrt{6} \mid b = d = 0\} \\
=& \mathbb{Q}(\sqrt{3})
\end{aligned}$$

De la misma forma se puede demostrar que:

$$\mathbb{Q}(\sqrt{2},\sqrt{3})^{G_3} = \mathbb{Q}(\sqrt{2})$$

$$\mathbb{Q}(\sqrt{2},\sqrt{3})^{G_4} = \mathbb{Q}(\sqrt{6})$$

En este caso los diagramas de Hasse correspondientes a $Gal(\mathbb{Q}(\sqrt{2},\sqrt{3})|\mathbb{Q})$ y $\mathscr{E}_{\mathbb{Q}(\sqrt{2},\sqrt{3})|\mathbb{Q}}$ son:



EJEMPLO 67. *Considere la extensión* $\mathbb{Q}(\omega, \sqrt[3]{2})|\mathbb{Q}$ *estudiada en el ejemplo 61 que se sabe es de galois y que*

$$Gal(\mathbb{Q}(\omega, \sqrt[3]{2})|\mathbb{Q}) \cong S_3$$

Nuevamente se quiere usar el TFTG para determinar la extensiones intermedias de esta. Para esto recuerde que se definieron $\sigma, \tau \in Gal(\mathbb{Q}(\omega, \sqrt[3]{2})|\mathbb{Q})$ *que estaban determinadas por:*

$$\sigma(\sqrt[3]{2}) = \omega\sqrt[3]{2}, \quad \sigma(\omega) = \omega$$
$$\tau(\sqrt[3]{2}) = \sqrt[3]{2}, \quad \tau(\omega) = \omega^2$$

las cuales permiten dar una presentación de dicho grupo definida por:

$$Gal(\mathbb{Q}(\omega, \sqrt[3]{2})|\mathbb{Q}) \cong \langle \sigma, \tau \mid \sigma^3 = \tau^2 = e, \tau\sigma\tau = \sigma^{-1} \rangle$$

Para conocer las extensiones intermedias, deben conocerse los sungrupos de $Gal(\mathbb{Q}(\omega, \sqrt[3]{2})|\mathbb{Q})$. *Para determinar estos, recuerde que el teorema de Lagrange afirma que estos tienen que tener orden* $1, 2, 3, 6$. *Note que quitando los casos triviales, los órdenes restantes tienen que ser generados precisamente por un 2-ciclo y un 3-ciclo. Por lo tanto, en este caso la lista de subgrupos es:*

$$G_1 = e$$
$$G_2 = \langle \tau \rangle \cong \mathbb{Z}_2$$
$$G_3 = \langle \sigma\tau \rangle \cong \mathbb{Z}_2$$
$$G_4 = \langle \sigma^2\tau \rangle \cong \mathbb{Z}_2$$
$$G_5 = \langle \sigma \rangle \cong \mathbb{Z}_3$$
$$G_6 = Gal(\mathbb{Q}(\omega, \sqrt[3]{2})|\mathbb{Q})$$

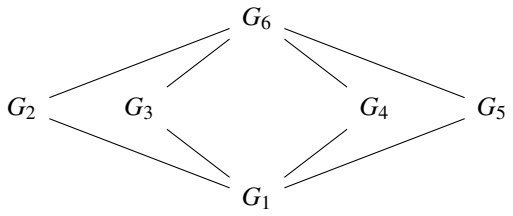
Una forma de justificar el porque en este caso la lista anterior proporciona todos los subgrupos del grupo en cuestión se puede hacer mediante el conteo de estructuras cíclicas en S_3. *Dicho conteo dice que el número de transposiciones en* S_3 *es:*

$$\frac{1}{2}\frac{3!}{(3-2)!} = 3$$

Para los triciclos se tienen

$$\frac{1}{3}\frac{3!}{(3-3)!} = 2$$

Ademas observe que todos los triciclos están necesariamente en la misma órbita. Por lo tanto, el diagrama de Hasse correspondiente a $Sub(Gal(\mathbb{Q}(\omega, \sqrt[3]{2})|\mathbb{Q}))$ *es:*



Para los campos que corresponden a cada grupo, es claro de las definiciones que:

$$\mathbb{Q}(\omega, \sqrt[3]{2})^{G_6} = \mathbb{Q}$$
$$\mathbb{Q}(\omega, \sqrt[3]{2})^{G_1} = \mathbb{Q}(\omega, \sqrt[3]{2})$$
$$\mathbb{Q}(\omega, \sqrt[3]{2})^{G_2} = \mathbb{Q}(\sqrt[3]{2})$$
$$\mathbb{Q}(\omega, \sqrt[3]{2})^{G_5} = \mathbb{Q}(\omega)$$

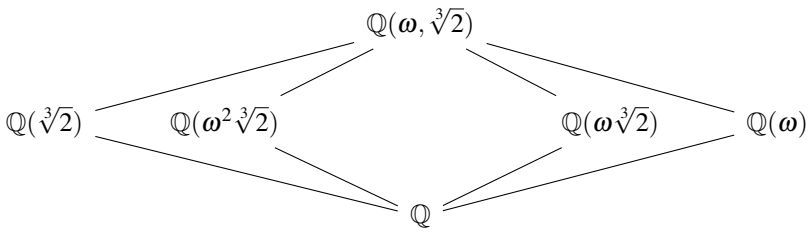
Para el caso de G_3 *observe que* $\sigma\tau(\omega^2) = \omega$ *y* $\sigma\tau(\sqrt[3]{2}) = \omega\sqrt[3]{2}$. *Por lo tanto,* $\sigma\tau(\omega^2\sqrt[3]{2}) = \omega^2\sqrt[3]{2}$ *y de aqui no es difícil ver que:*

$$\mathbb{Q}(\omega, \sqrt[3]{2})^{G_3} = \mathbb{Q}(\omega^2\sqrt[3]{2})$$

Por otro lado se tiene que $\sigma^2\tau(\sqrt[3]{2}) = \omega^2\sqrt[3]{2}$ *y* $\sigma^2\tau(\omega) = \omega^2$. *Entonces* $\sigma^2\tau(\omega\sqrt[3]{2}) = \omega\sqrt[3]{2}$, *por lo que en este caso:*

$$\mathbb{Q}(\omega, \sqrt[3]{2})^{G_4} = \mathbb{Q}(\omega\sqrt[3]{2})$$

Por lo tanto, el diagrama de Hasse para $\mathscr{E}_{\mathbb{Q}(\omega, \sqrt[3]{2})|\mathbb{Q}}$ *es:*



En este caso no todos los subgrupos son normales por lo tanto el TFTG afirma que para los subgrupos que no lo sean, las extensiones intermedias correspondientes no son de Galois. Un ejemplo se da con G_2 pues $\sigma\tau\sigma^{-1} = \sigma\tau\sigma^2 = \tau\sigma^4 = \tau\sigma \neq \tau$. Por lo tanto, esta extensión no es de Galois, cosa que ya se había visto directamente de la definición en el ejemplo 63. Además de esto observe que G_3 tampoco es normal pues $\tau(\sigma\tau)\tau^{-1} = \tau\sigma = \sigma^{-1}\tau = \sigma^2\tau \neq \sigma\tau$. Esto dice que la extensión $\mathbb{Q}(\omega^2\sqrt[3]{2})|\mathbb{Q}$ no es de Galois. En el caso de G_4, este tampoco es normal pues $\tau(\sigma^2\tau)\tau^{-1} = \tau\sigma^2 = \sigma\tau \neq \sigma^2\tau$, por lo que la extensión $\mathbb{Q}(\omega\sqrt[3]{2})|\mathbb{Q}$ tampoco es de Galois.

Por otro lado, como G_5 tiene indice 2, este subgrupo es normal y por lo tanto, al extensión que define es de Galois.

A manera de comentario final es importante notar como el TFTG es un teorema que transporta un problema de clasificar subcampos a un problema de analizar subgrupos. Por supuesto que aún y con este diccionario la tarea puede ser muy difícil ya que determinar cuales son los subgrupos de un grupo puede ser una tarea difíci, sin embargo, pese a estas complicaciones no deja de ser un teorema sorprendente desde el punto de vista práctico y mucho más desde el punto de vista teórico. Esperamos que las siguientes páginas muestren de forma adecuada la potencia de la teoría.

2. Teorema del elemento primitivo

La extensiones de la forma $k(\alpha)$ son muy importantes por distintas razones las cuales deben ser ya comprendidas a estas alturas. Una pregunta muy interesante es si se puede determinar cuándo una extensión tiene esta forma.

DEFINICIÓN 73. *Sea $K|k$ una extensión, decimos que $K|k$ es simple si existe $\alpha \in K$ tal que $K = k(\alpha)$.*

PROPOSICIÓN 110. *Sea $K|k$ una extensión finita. Entonces $K|k$ es simple si y sólo si hay un número finito de campos entre k y K.*

DEMOSTRACIÓN. $\Rightarrow$. Consideramos el caso cuando k es finito. Como K es un $k-$espacio vectorial, entonces K es finito. Por lo que hay un número finito de campos intermedios. Recordemos que: Todo subgrupo finito de un grupo multiplicativo de un campo es cíclico. Por lo que el grupo multiplicativo de K es cíclico, así existe $\alpha \in K$ tal que $\langle\alpha\rangle = K$ y $K = k(\alpha)$.

Si k es infinito y $K|k$ es simple, entonces $\exists \alpha \in K$, $k(\alpha) = K$. Sea L un campo intermedio de $K|k$, entonces $K = L(\alpha)$. Por lo que $[K : L] = \partial(irr_L(\alpha))$, ponemos M como el campo obtenido tras añadir los coeficientes de $irr_L(\alpha)$ a k.

Ahora bien, tenemos que $k \subseteq M \subseteq L$, como $irr_L(\alpha)$ es irreducible en L, entonces $irr_L(\alpha)$ es irreducible en M.
Por lo que $irr_L(\alpha) = irr_M(\alpha)$. Si notamos que $K = M(\alpha)$ entonces

$$[K : M] = \partial(irr_L(\alpha)) = [K : L]$$

Por lo que $M = L$. Por lo que el campo L esta determinado por $irr_L(\alpha)$ pero $irr_L(\alpha)|irr_k(\alpha)$ en L. Pero esto implica que $irr_L(\alpha)|irr_k(\alpha)$ en K. Pero $irr_k(x)$ tiene solo un número finito de factores en K. Por lo que solo existe un número finito de posibilidades para $irr_L(\alpha)$ y así para L.

$\Leftarrow$. Suponemos que hay un número finito de campos entre k y K.
Como $K|k$ es finito, entonces $K = k(\alpha_1, ..., \alpha_n)$ para algunos $\alpha_1, .., \alpha_n \in K$. Sean $\alpha, \beta K$ y consideramos los campos intermedios $k(\alpha + t\beta)$ con $t \in k$. Como k es infinito, deben existir $t_1, t_2 \in k$ tales que

$$k(\alpha + t_1\beta) = k(\alpha + t_2\beta)$$

ponemos $\gamma_1 = \alpha + t_1\beta$ y $\gamma_2 = \alpha + t_2\beta$ tenemos que $\gamma_2 \in k(\gamma_1)$ y $\gamma_1 \in k(\gamma_1)$ por lo que $\gamma_2 - \gamma_1 = (t_2 - t_1)\beta \in k(\gamma_1)$. De aquí $\beta \in k(\gamma_1)$. Por otro lado $\gamma_1 - t_1\beta = \alpha \in k(\gamma_1)$. Así

$$k(\gamma_1) \subseteq k(\alpha, \beta) \subseteq k(\gamma_1)$$

Por lo tanto

$$k(\alpha, \beta) = k(\gamma_1)$$

Aplicando inducción tenemos que existe $\gamma \in K$ tal que $k(\gamma) = K$. □

COROLARIO 25. *(Teorema del elemento primitivo) Si $K|k$ es una extensión finita separable. Entonces $K|k$ es una extensión simple.*

DEMOSTRACIÓN. Como $K|k$ es una extensión finita, entonces existen $\alpha_1, ..., \alpha_n \in K$ tales que $K = k(\alpha_1, ..., \alpha_n)$. Como $K|k$ es separable entonces $irr_k(\alpha_i)$ es separable y así

$$f = \prod_{i=1}^{n} irr_k(\alpha_i)$$

es separable. □

3. Problemas griegos clásicos

Los tres problemas clásicos griegos son:

1. Duplicación del cubo: Hallar un cubo cuyo volumen sea el doble de un cubo dado
2. Trisección del ángulo: Dividir en tres un ángulo dado
3. Cuadratura del círculo: Hallar un cuadrado cuya área sea la de un círculo dado.

Con ideas de teoría de campos puede demostrarse que los problemas anteriores no pueden resolverse usando únicamente regla y compás. Como preliminares que daremos por sentado acerca de estas construcciones se tienen los siguientes resultados:

1. Pueden obtenerse usando regla y compás la suma, resta, producto, división de segmentos. Además puede obtenerse la raíz cuadrada de cualquier segmento.
2. Un punto se puede construir usando únicamente regla y compás si se obtiene como sucesión finita de los procesos siguientes:
   i) Intersección de dos lineas
   ii) Intersección de una línea y una circunferencia
   iii) Intersección de dos circunferencias

El último paso previo al resultado que se busca es recordar que uno de los modelos de $\mathbb{C}$ se da al considerar $\mathbb{R}^2$ con su operación habitual de grupo abeliano aditivo en el cual se introduce un producto. Usando esta identificación se tiene el siguiente resultado.

PROPOSICIÓN 111. *Sea $z \in \mathbb{C}$. Entonces, z se puede construir con regla y compás si y sólo si z es algebraico sobre $\mathbb{Q}$ y existe una sucesión de campos*

$$k_0 = \mathbb{Q} \subseteq k_1 \subseteq \cdots \subseteq k_l$$

tal que:

1. $\mathbb{Q}(z) \subseteq k_l$
2. *Para cada $i \in \{1,...,n\}$, $[k_i : k_{i-1}] = 2$*

DEMOSTRACIÓN. $\Rightarrow$) Basta con ver que cada uno de los procesos i)-iii) da lugar a una extensión de grado a lo más 2. Para i) note que si el punto (x_0, y_0) se construye como solución de un sistema simultáneo con coeficientes en un campo k,

$$\begin{cases} a_1 x + b_1 y = c_1 \\ a_2 x + b_2 y = c_2 \end{cases}$$

entonces $x_0, y_0 \in k$, por lo que en este caso la extensión tiene grado 1.

En lo que respecta a ii), se busca encontrar (x_0, y_0) que resuelva el sistema:

$$\begin{cases} (x-a_1)^2+(y-b_1)^2=c_1^2 \\ a_2x+b_2y=c_2 \end{cases}$$

Al despejar en 2 y sustituir en 1, se observa que $x_0, y_0 \in k(\alpha)$ con $[k(\alpha):k]=1,2$.

Para iii) se quiere resolver el sistema:

$$\begin{cases} (x-a_1)^2+(y-b_1)^2=c_1^2 \\ (x-a_2)^2+(y-b_2)^2=c_2^2 \end{cases}$$

Al sustraer una de las ecuaciones anteriores a la otra, esto permite obtener una ecuación más lineal de la forma $a_3x+b_3y=c_3$ con coeficientes en k. Al usar esta ecuación con alguno de los dos círculos esta operación se reduce al caso anterior.

$\Leftarrow$) Basta con hacer hacer el caso de $k_0 \subseteq k_1$ pues el resultado se sigue por inducción. Así, como $[k_1:k_0]=2$, esta extensión es de Galois y por lo tanto $k_1=\mathbb{Q}(x^2+\alpha)$ con $x^2+\alpha \in \mathbb{Q}[x]$ separable. Por lo tanto, $k_1=\mathbb{Q}(\sqrt{\alpha})$ y además todo elemento de $\mathbb{Q}(\sqrt{\alpha})$ puede construirse con regla y compás. De esto de deduce el resultado. □

Con el resultado anterior puede verse que los problemas griegos clásicos no se pueden resolver con regla y compás.

PROPOSICIÓN 112. *Los problemas griegos clásicos no pueden resolverse usando únicamente regla y compás.*

DEMOSTRACIÓN. Problema de trisección de un ángulo: Sea θ un ángulo. Dado que dicho ángulo intersecta al circulo unitario en un punto, digamos P, observe que $P=(\cos\theta, \operatorname{sen}\theta)$. Por lo tanto, puede construirse el ángulo $\frac{\theta}{3}$ si y sólo si puede construirse el número real $\cos(\frac{\theta}{3})$. Además, basta con ver que este proceso no puede realizarse para $\theta=\frac{\pi}{3}$ y observe que dado que para cualquier ángulo φ se cumple que $\cos(3\varphi)=4\cos^4(\varphi)-3\cos(\varphi)$, al considerar $\varphi=\frac{\theta}{3}$ y denotar por $z_0=\cos\varphi$ la identidad anterior implica que x_0 es raíz de polinomio $f=4x^3-3x-1 \in \mathbb{Q}[x]$. Observe que este polinomio es irreducible sobre $\mathbb{Q}$ pues $f(x+1)=x^3+3x^2-3$ y el criterio de Eisenstein implica que este es irreducible al usar $3 \in \mathbb{Z}$ primo. De esto se deduce que $f=min_{\mathbb{Q}}(z_0)$ y por lo tanto

$$[\mathbb{Q}(z_0):\mathbb{Q}]=3$$

Esto contradice el resultado anterior pues dicho índice no divide a ninguna potencia de 2.

Problema de duplicación del cubo: Note que dado un cubo de volumen 1, el cual puede construirse trivialmente, si se supone que puede construirse un cubo con volumen 2 usando únicamente regla y compás, entonces necesariamente puede construirse con dichos métodos el lado de dicho cubo que tiene longitud $\sqrt[3]{2}$. Pero como

$$[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$$

, esto nos lleva a una contradicción pues dicho índice no divide a ninguna potencia de 2.

Problema de cuadratura del círculo: Es claro que puede construirse el radio de un circulo con área π. Sin embargo, no puede construirse un cuadrado con dicha área pues esto implicaría que puede construirse con regla y compás el número $z = \sqrt{\pi}$. Sin embargo, esto contradice el hecho de que π sea trascendente pues $\mathbb{Q}(\sqrt{\pi})|\mathbb{Q}$ sería finita y por lo tanto algebraica. □

4. Solubilidad por radicales

En esta sección se va a tratar la segunda aplicación básica de la teoría de Galois: La solubilidad de ecuaciones polinomiales. Este problema se remonta a la antigüedad empezando por la ecuación cuadrática con coeficientes reales ($a \neq 0$):

$$ax^2 + bx + c = 0$$

Una de los primeros métodos de solución se debe a Diofanto cuyo método no daba la solución completa pues incluso en el caso real solamente se podía obtener una solución. Hay que decir que la solución completa fue desarrollada por Al-Juarisimi y hoy en día se sabe que por un argumento de completación de cuadrados las soluciones están dadas por la fórmula general:

$$\frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$$

En 1545 Cardano publica el método de solución de la ecuación de tercer grado, el cual de hecho es válido para campos con característica distinta de 2 y 3. La idea del método es considerar el polinomio

$$f = x^3 + bx^2 + cx + d \in \mathbb{R}[x]$$

y hacer una reducción al notar que

$$g := f\left(x - \frac{b}{3}\right) = x^3 + px + q \in \mathbb{R}[x]$$

Es decir, este método permite eliminar el término cuadrático. Luego, se trabaja con la ecuación

$$g(x) = 0$$

Para resolverla la idea es escribir $x = u + v$ y obtener un par de ecuaciones al sustituir en la ecuación anterior. Estas son

$$\begin{cases} u^3 + v^3 + q = 0 \\ 3uv + p = 0 \end{cases}$$

De la segunda ecuación

$$v = -\frac{p}{3u}$$

al sustituir esto en la primera de estas ecuaciones se llega a la ecuación

$$4u^6 + qu^3 - \frac{p^3}{27} = 0$$

Al aplicar la fórmula cuadrática

$$u^3 = \frac{-q \pm \sqrt{q^2 + \frac{4}{27}p^3}}{2}$$

Con esto se encuentra una solución pues se han encontrado tanto u como v. Además, en este punto se pueden encontrar las soluciones restantes con la fórmula general de segundo grado.

Para la ecuación de cuarto grado la solución se atribuye a Ferrari y se encuentra publicada en el libro de Cardano “Ars Magna, or the Rules of algebra".

Este empieza por considerar el polinomio $f = x^4 + ax^3 + bx^2 + cx + d$ y busca las soluciones $f(x) = 0$ notando que esta igualdad implica por completación de cuadrados la ecuación:

$$\left(x^2 + \frac{1}{2}ax\right)^2 = \left(\frac{1}{4}a^2 - b\right)x^2 - cx - d$$

Luego, se suma a ambos lados de la ecuación anterior el término

$$y\left(x^2 + \frac{ax}{2}\right) + \frac{b^2}{4}$$

La idea de este paso es intentar que lo que aparece de lado izquierdo sea un trinomio cuadrado perfecto. Este proceso nos lleva a la ecuación:

$$\left(x^2 + \frac{1}{2}ax + \frac{1}{2}y\right)^2 = \left(\frac{1}{4}a^2 - b + y\right)x^2 + \left(\frac{1}{2}ay - c\right)x + \frac{1}{4}y^2 - d$$

Luego, se quiere elegir ”y” para que el lado derecho sea un cuadrado perfecto. Escribiendo esta ecuación como $Ax^2 + Bx + C$, esto sucede si $B^2 - 4AC = 0$. Esta ecuación se puede resolver para “y” con lo que se llega a:

$$\left(x^2 + \frac{1}{2}ax + \frac{1}{2}y\right)^2 = (ex + f)^2$$

Esto permite escribir dos ecuaciones de grado 2, las cuales al resolver dan la solución buscada.

Sin duda, los resultados anteriores muestran cómo los matemáticos de la época hacían transformaciones que hacían que en todos los casos la solución se llevara a la formula general de segundo grado. Además, es en este momento cuando la pregunta obvia es qué sucede con las ecuaciones de grado 5 o mayor. Fue hasta 1824 cuando Abel publica un artículo donde demuestra que la ecuación de grado 5 no se puede resolver por métodos algebraicos, es decir, no se puede encontrar fórmula que exprese las raíces en términos de los coeficientes, operaciones arítmeticas (suma, resta, producto y división) y radicales. Más

tarde Galois muestra que el fenómeno encontrado por Abel no es exclusivo de la ecuación de quinto grado, sino que las ecuaciones de grado mayor tienen el mismo comportamiento y es para este resultado que Galois introduce la teoría que lleva su nombre y dicho sea de paso, introduce la idea de grupo, que es una de las estructuras recurrentes en su teoría. La idea de esta sección es dar una presentación moderna de dicho resultado de Galois (y Abel).

DEFINICIÓN 74. *Un extensión $K|k$ es radical si $K = k(a_1,...,a_r)$ para algunos $a_1,...,a_r \in K$, tales que existen $n_1,...,n_r \in \mathbb{N}^+$ tales que $a_1^{n_1} \in k$ y para cada $i \in \{2,...,r\}$, $a_i^{n_i} \in k(a_1,...,a_{i-1})$.*

Si $n = n_1 = ... = n_r$, diremos que K es una extensión $n-$radical de k.

EJEMPLO 68. *Considere el polinomio $f = x^4 - 6x^2 + 7 \in \mathbb{R}[x]$. Las raíces de f son*

$$\pm\sqrt{3 \pm \sqrt{2}}$$

Esto da lugar a una cadena de extensiones.

$$\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2}) \subseteq \mathbb{Q}(\sqrt{2}, \sqrt{3+\sqrt{2}}) \subseteq \mathbb{Q}(\sqrt{2}, \sqrt{3+\sqrt{2}}, \sqrt{3-\sqrt{2}})$$

Si $a_1 = \sqrt{2}$, $a_2 = \sqrt{3+\sqrt{2}}$, y $a_3 = \sqrt{3-\sqrt{2}}$, observe que $K = k(a_1, a_2, a_3)$ es una extensión radical pues $a_1^2 \in \mathbb{Q}$, $a_2^2 \in \mathbb{Q}(a_1)$ y $a_3^2 \in \mathbb{Q}(a_1) \subseteq \mathbb{Q}(a_1, a_2)$. De hecho, la extensión $K|\mathbb{Q}$ es 2-radical.

El ejemplo anterior deja ver que las extensiones radicales son el concepto que parece ser el necesario para tratar la solubilidad de radicales. Esto nos lleva a introducir lo siguiente.

DEFINICIÓN 75. *Si $f \in k[x]$, entonces f es soluble por radicales si existe una extensión radical $K|k$ tal que f se escinde sobre K.*

EJEMPLO 69. *El polinomio $f = x^4 - 6x^2 + 7$ es soluble por radicales según el ejemplo 68.*

Observaciones:

1. Si $K|k$ es una extensión radical con $K = k(a_1,..,a_r)$, $a_1^{n_1} \in k$, $a_i^{n_i} \in k(a_1,...,a_{i-1})$, observe que $K|k$ es n-radical con $n = n_1 \cdot ... \cdot n_r$.
2. Si $K|k$ es una extensión algebraica, entonces K es radical si y sólo si existe una torre de extensiones
$$F_r|F_{r-1}|...|F_1|F_0$$
con $F_0 = k$, $F_r = K$ y $F_{i+1} = F_i(a_i)$ para algún $a_i \in F_{i+1}$ con $a_i^{n_i} \in F_i$.

3. Observe que si las extensiones $K|F$ y $F|k$ son radicales, entonces la extensión $K|k$ también es radical.

EJERCICIO 197. *¿Es cierto que si la extensión $K|k$ es radical entonces $K|F$ y $F|k$ son radicales?*

Es importante notar que el "grado de radicalidad"de una extensión no está univocamente determinado como se muestra a continuación.

EJEMPLO 70. *Si $K = \mathbb{Q}(\sqrt[4]{2})$, la extensión $K|\mathbb{Q}$ es trivialmente 4-radical. Sin embargo también es 2-radical como lo muestra la torre de extensiones*

$$K|\mathbb{Q}(\sqrt{2})|\mathbb{Q},$$

con $K = \mathbb{Q}(\sqrt{2})(\sqrt{\sqrt{2}})$

Una fuente de ejemplos interesantes se muestra a continuación:

EJEMPLO 71. *Sea $c \in \mathbb{R}$. Recuerde que c es constructible si y solo si existe una torre de campos*

$$F_r|F_{r-1}|...|F_1|F_0$$

con $F_0 = \mathbb{Q}$ y $F_{i+1} = F_i(\sqrt{a_i})$ para $a_i \in F_i$ y $c \in F_r$.

Por lo tanto, c es constructible si y solo si existe un campo intermedio a $\mathbb{R}|\mathbb{Q}$, K, tal que $K|\mathbb{Q}$ es 2-radical.

Observación: Si $f \in k[x]$ es soluble, sea $K|k$ extensión radical, donde f se escinde. Observe que

$$k(f) \subseteq K$$

Sin embargo $k(f)$ no tiene porque definir una extensión radical de k.(Ver ejercicio 198)

EJERCICIO 198. *Sea $f \in k[x]$ soluble por radicales. Si k contiene una raíz n-ésima primitiva de la unidad, para cada $n \in \mathbb{N}^+$, entonces la extensión $k(f)|k$ es radical.*

Para dar el teorema de Galois respecto a la solubilidad se requieren dos ingredientes. Uno de ellos es la idea de grupo soluble el cual se puede encontrar en uno de los anexos. La segunda idea es el siguiente resultado. Para este se requieren recordar que para $K|k$ algebraica, la clausura normal de dicha extensión se puede definir como el campo de descomposición del conjunto

$$\{min_k(\alpha)|\alpha \in K\}$$

Si esta se denota por

$$\overline{K}^{nor}$$

esta es la mínima extensión normal de k que contiene a K. Otras propiedades aparecen en el ejercicio 179

LEMA 10. *Sea $K|k$ extensión n-radical. Entonces, $\overline{K}^{nor}|k$ es n-radical.*

DEMOSTRACIÓN. Suponga que $a_1,...,a_r \in K$ son tales que $K = k(a_1,...,a_r)$ con $a_1^{n_1} \in k$ y $a_i^{n_i} \in k(a_1,...,a_{i-1})$ para $i > 1$. La prueba es por inducción sobre r.

Base: r=1. Como $K = k(a_1)$ entonces $\overline{K}^{nor} = k(\beta_1,...,\beta_m)$ con $\beta_1,...,\beta_m$ raíces de $min_k(a_1)$. Dado que $min_k(a_1)|x^{n_1} - a_1^{n_1}$, entonces para $i \in \{1,...,m\}$ se tiene que:

$$\beta_i^{n_i} = a_1^{n_1} \in k$$

Entonces $\overline{K}^{nor}|k$ es n-radical.

Paso inductivo: Si el resultado vale para campos que se obtienen de adjuntar $r-1$ elementos a k, sea

$$N = \overline{k(a_1,...,a_{r-1})}^{nor}$$

Por hipótesis de inducción $N|k$ es radical. Como N es campo de descomposición de $\{min_k(a_1),...,min_k(a_{r-1})\}$, entonces

$$\overline{K}^{nor} = N(\beta_1,...,\beta_m),$$

con $\beta_1,...,\beta_m$ raíces de $min_k(a_r)$. Entonces, $a_r^n \in k(a_1,...,a_{r-1})$ y al usar el teorema de extensión de isomorfismos, para cada i existe $\sigma_i \in Gal(\overline{K}^{nor}|k)$ tal que

$$\sigma_i(a_r) = \gamma_i$$

Como $N|k$ es normal, $a_r^n \in N$, entonces $\sigma_i(a_r^n) = \gamma_i^n \in N$. Entonces cada γ_i es la n-ésima potencia de un elemento en N, entonces $\overline{K}^{nor}|N$ es n-radical. De esto se deduce que $\overline{K}^{nor}|k$ es n-radical. □

A continuación se va a probar el teorema que se ha estado buscando. Es importante hacer notar que este es más general que el teorema más conocido que es para polinomios con coeficientes reales, ya que este está formulado para cualquier campo con característica cero.

PROPOSICIÓN 113. *(Galois) Sea k campo con $car(k) = 0$ y $f \in k[x]$. Entonces f es soluble por radicales si y solo si $Gal(k(f)|k)$ es un grupo soluble.*

DEMOSTRACIÓN. $\Rightarrow$) Suponga que f es soluble por radicales y sea $K|k$ una extensión n-radical de f testigo de dicha propiedad. Dado que $car(k) = 0$, sea ω una raíz n-ésima primitiva de la unidad, la cual existe en alguna extensión de K. Dado que $K(\omega)|K$ es n-radical, entonces $K(\omega)|k$ lo es. Si $N = \overline{K(\omega)}^{nor}$, entonces por el lema anterior $N|k$ es n-radical, más aún $N|k(\omega)$ es n-radical. Por lo tanto existe una torre de campos

$$F_r|F_{r-1}|...|F_1|F_0$$

con $F_r = N$, $F_0 = k$ y $F_1 = k(\omega)$ donde $F_{i+1} = F_i(a_i)$ para $a_i^n \in F_i$. Como F_i contiene una raíz n-ésima primitiva de la unidad la extensión $F_{i+1}|F_i$ es de Galois y cíclica. Ademas $F_1|F_0$ es extensión de Galois abeliana pues es ciclotómica. Dado que $car(k) = 0$ y $N|k$ es normal, entonces $N|k$ es de Galois. Esto produce una cadena de subgrupos

$$0 \leq G_r \leq G_{r-1} \leq ... \leq G_0 = Gal(N|k)$$

con $G_i = Gal(N|F_i)$. Por el TFTG, el hecho de que $F_{i+1}|F_i$ sea de Galois implica que $G_{i+1} \trianglelefteq G_i$ y además

$$G_i/G_{i+1} \cong Gal(F_{i+1}|F_i)$$

Entonces G_i/G_{i+1} es abeliano. Esto prueba que $Gal(N|k)$ es soluble y esto implica que $Gal(K|k)$ lo es, pues

$$Gal(K|k) \cong Gal(N|k)/Gal(N|K)$$

$\Leftarrow$) Si $K = k(f)$ y $Gal(K|k)$ es soluble, considere una serie soluble de dicho grupo:

$$0 \leq G_r \leq G_{r-1} \leq ... \leq G_0 = Gal(K|k)$$

Denote por $F_i = K^{G_i}$ y entonces, por el TFTG las extensiones $F_{i+1}|F_i$ son de Galois y $Gal(F_{i+1}|F_i) \cong G_i/G_{i+1}$. Considere n un exponente de $Gal(K|k)$ y considere ω una raíz n-ésima primitiva de la unidad, la cual pertenece a alguna extensión de K. Si denotamos $L_i = F_i(\omega)$, existe una torre de extensiones

$$L_r|L_{r-1}|...|L_1|L_0|k$$

donde $K \subseteq L_r$. Dado que $L_{i+1} = L_i K_{i+1}$ y $K_{i+1}|K_i$ es de Galois, por el teorema de las irracionalidades naturales la extensión $L_{i+1}|L_i$ es de Galois y

$$Gal(L_{i+1}|L_i) \leq Gal(K_{i+1}|K_i),$$

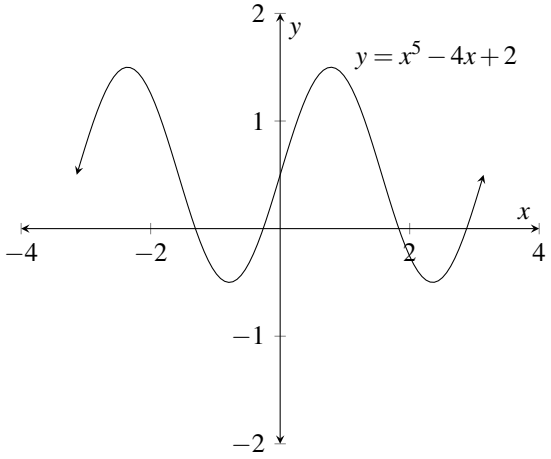
lo que implica que $Gal(L_{i+1}|L_i)$ es abeliano y ademas el exponente de este grupo divide a n.

Esto implica que la extensión $L_{i+1}|L_i$ es de Kummer de grado n y entonces es n-radical. Como $L_0 = k(\omega)|k$ es radical, esto implica que $L_r|k$ es radical. Dado que $L_r|K$ entonces $L_r|k$ es radical y así f es soluble por radicales. □

Nota. Existe un teorema análogo al anterior para campos con característica positiva. Para este tiene que modificarse la noción de extensión radical. Dicha modificación y resultado se encuentra en los ejercicios.

Del resultado anterior se deduce que todo polinomio de grado mayor o igual a 5 sobre un campo de característica 0 no es soluble por radicales. La prueba de esto requiere de un pequeño calculo que se va a realizar en una sección posterior, pero explicaremos la idea con un ejemplo concreto.

EJEMPLO 72. *Sea $f = x^5 - 4x + 2 \in \mathbb{Q}[x]$. Este polinomio es irreducible sobre $\mathbb{Q}[x]$ por el criterio de Eisenstein para $2 \in \mathbb{Z}$. Una gráfica de este polinomio se muestra en la figura:*



Por lo que f tiene 3 raíces reales y 2 complejas. Dado que cada raíz de f genera un campo de dimensión 5 sobre $\mathbb{Q}$, entonces $[\mathbb{Q}(f) : \mathbb{Q}] \in 5\mathbb{Z}$ y ademas como $Gal(K(f)|\mathbb{Q})$ permuta dichas raíces entonces

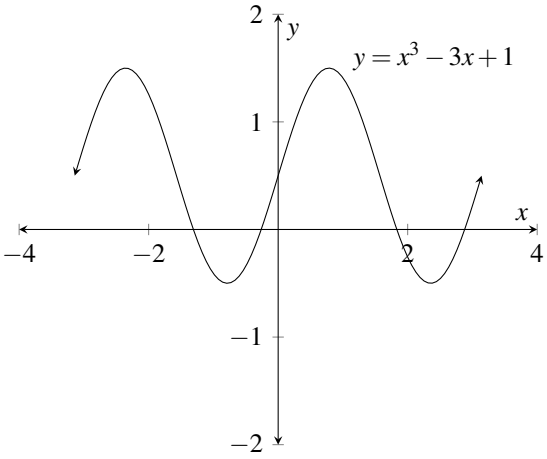
$$Gal(\mathbb{Q}(f)|\mathbb{Q}) \leq S_5$$

Dado que $5||Gal(\mathbb{Q}(f)|\mathbb{Q})|$*, entonces por el teorema de Cayley* $Gal(\mathbb{Q}(f)|\mathbb{Q})$ *tiene un elemento de orden 5, es decir, un 5-ciclo. Observe que como* $\mathbb{Q}(f) \subseteq \mathbb{C}$*, si* $\overline{(\_)} : \mathbb{C} \to \mathbb{C}$ *es la conjugación compleja, al restringir a* $\mathbb{Q}(f)$ *dicho automorfismo permuta las raíces complejas de* f *y fija las 3 reales, es decir,* $\overline{(\_)}$ *corresponde a una transposición con la identificación* $Gal(\mathbb{Q}(f)|\mathbb{Q}) \leq S_5$*. Así,* $Gal(\mathbb{Q}(f)|\mathbb{Q})$ *tiene un 5-ciclo y una transposición luego,*

$$Gal(\mathbb{Q}(f)|\mathbb{Q}) = S_5$$

Pero S_5 *no es soluble, luego,* f *no es soluble por radicales.*

EJEMPLO 73. *Sea* $f = x^3 - 3x + 1 \in \mathbb{Q}[x]$.



Observe que f *es irreducible. En este caso*

$$Gal(\mathbb{Q}(f)|\mathbb{Q}) \cong A_3$$

y A_3 *es soluble, luego,* f *es soluble por radicales. Sin embargo* $\mathbb{Q}(f)|\mathbb{Q}$ *no es radical. Para ver esto note que como* $[\mathbb{Q}(f) : \mathbb{Q}] = 3$*, entonces toda torre de campos con extremos* $\mathbb{Q}(f)$ y $\mathbb{Q}$ *debe ser trivial. Entonces, si* $\mathbb{Q}(f)|\mathbb{Q}$ *es radical, entonces* $\mathbb{Q}(f) = \mathbb{Q}(z)$ *para* $z \in \mathbb{Q}(f)$ *con* $z^n \in \mathbb{Q}$*. Dado que* $min_{\mathbb{Q}}(z)$ *se escinde en* $\mathbb{Q}(f)$*, considere* w *otra raíz de* $min_{\mathbb{Q}}(z)$ *en* $\mathbb{Q}(f)$*. Luego,* $z^n = w^n$ *y así* $\frac{z}{w}^n = 1$*. Si* $\mu = \frac{z}{w}$ *es raíz primitiva de la unidad entonces* $m|n$*. Luego,* $\mathbb{Q}(\mu) \subseteq \mathbb{Q}(f)$ *y como* $[\mathbb{Q}(\mu) : \mathbb{Q}] = \phi(m)$ *entonces* $\phi(m) \in \{1,3\}$ *pero* $\phi(m) \neq 3$*, entonces*

$$[\mathbb{Q}(\mu) : \mathbb{Q}] = 1$$

Luego $\mu \in \mathbb{Q}$, luego $\mu \in \{1,-1\}$ lo que implica que $z \in \{w,-w\}$. Así que f tiene a lo mas dos raíces, luego

$$[\mathbb{Q}(z):\mathbb{Q}] \leq 2 < [\mathbb{Q}(f):\mathbb{Q}]$$

lo cual contradice el hecho de que $\mathbb{Q}(z) = \mathbb{Q}(f)$.

En lo que respecta al caso general considere para k un campo de característica 0 el polinomio $f = (x-t_1)\cdot\ldots\cdot(x-t_n) = x^n - s_1x^{n-1} + \ldots + (-1)^n s_n$, donde

$$s_i = \sum_{1<j_1<\ldots<j_i<n} t_{j_1}\cdot\ldots\cdot t_{j_i}$$

Note que $f \in k(t_1,\ldots,t_n)[x]$ y que si se pudiera encontrar una fórmula para las raíces de f en términos de sus coeficientes, entonces se podría encontrar una fórmula para cualquier polinomio de grado $n \geq 5$. Pero si $K = k(t_1,\ldots,t_n)$ note que S_n es grupo de automorfismos de K y

$$K^{S_n} = k(s_1,\ldots,s_n)$$

Note que

$$Gal(K|K^{S_n}) \cong S_n$$

y S_n no es soluble para $n \geq 5$. Por lo tanto;

COROLARIO 26. *Si k es un campo de característica 0 entonces existe $f \in k[x]$ con $\partial(f) \geq 5$ que no es soluble por radicales.*

5. Ejercicios del capítulo

EJERCICIO 199. *Demuestra que toda extensión finita, normal y separable $K|k$ tiene un número finito de campos intermedios.*

DEFINICIÓN 76. *Sean $n \in \mathbb{N}^+$ y k un campo que contiene una raíz n-ésima primitiva de la unidad. Una extensión de Galois $K|k$ se llama **n-extensión de Kummer** si $Gal(K|k)$ es abeliano y su exponente divide a n.*

EJERCICIO 200. *Sea k un campo que contiene una raíz n-ésima primitiva de la unidad y $K|k$ una extensión finita. Demuestre que la extensión $K|k$ es de Kummer si y sólo si existen $\alpha_1,\ldots,\alpha_m \in k$ tales que $K = k(\sqrt[n]{a_1},\ldots,\sqrt[n]{a_m})$.*

EJERCICIO 201. *Demuestre que el polinomio $f = x^5 - 4x + 2 \in \mathbb{Q}[x]$ no es soluble por radicales.*

EJERCICIO 202. *Sea $f = x^4 - 2x^2 - 3 \in \mathbb{Q}[x]$ y $K = \mathbb{Q}(f)$. Demuestre que $Gal(K|\mathbb{Q}) \cong \mathbb{Z}_2 \times \mathbb{Z}_2$.*

EJERCICIO 203. *Sean ω una raíz cúbica primitiva de 1 sobre $\mathbb{Q}$ y β la raíz cúbica real de 3. Defina $K = \mathbb{Q}(\omega, \beta)$.*

1. *Demuestre que la extensión $K|\mathbb{Q}$ es de Galois.*
2. *Calcule $Gal(K|\mathbb{Q})$*

EJERCICIO 204. *Demuestre que si $K|k$ es una extensión de Galois tal que $Gal(K|k)$ es abeliano. Demuestre que todo campo intermedio $K|k$ es una extensión de Galois.*

EJERCICIO 205. *Sean $f \in k[x]$ y $K|k$ una extensión de campos. Demuestre que el grupo de Galois de f sobre k es isomorfo a un subgrupo del grupo de Galois de f sobre K.*

EJERCICIO 206.

1. *Determinar el grupo de Galois $G = Gal(\mathbb{Q}(\sqrt{-3}, \sqrt[3]{5})|\mathbb{Q})$.*
2. *Determinar los subgrupos de G y determine los suncampos intermedios correspondientes.*
3. *Hacer un el diagrama de Hasse correspondiente a la retícula de subgrupos y a los campos intermedios.*

EJERCICIO 207. *Sea $f = x^3 - 2 \in \mathbb{Q}[x]$.*

1. *Demuestre que f es irreducible sobre $\mathbb{Q}$*
2. *Encontrar $\mathbb{Q}(f)$. Determine el grado de la extensión que este define dando una base explícita de $\mathbb{Q}(f)$ sobre $\mathbb{Q}$.*
3. *Demuestre que $Gal(\mathbb{Q}(f)|\mathbb{Q}) \cong S_3$*
4. *Para cada subgrupo de $Gal(\mathbb{Q}(f)|\mathbb{Q})$ determine el campo fijo correspondiente.*

EJERCICIO 208. *Demuestre que toda ecuación de grado a lo más 4 es soluble por radicales*

EJERCICIO 209. *Sea $f \in \mathbb{Q}[x]$ un polinomio con $\partial(f) = 5$ que tiene exactamente 3 raíces reales. Demuestre que*

$$Gal(\mathbb{Q}(f)|\mathbb{Q}) \cong S_5.$$

Use esto para probar que unu de tales polinomios no es soluble por radicales.

EJERCICIO 210. *Demuestre que pueden construirse con regla y compas el producto de dos segmentos, el cociente de dos segmentos y la raíz de un segmento.*

DEFINICIÓN 77. *Sea k un campo con característica $p > 0$. Un extensión $K|k$ es radical si existe una torre de extensiones*

$$F_n|\cdots|F_1|F_0$$

tales que $F_0 = k$, $F_n = K$ y $F_{i+1} = F_i(\alpha_i)$ para algún α_i tal que $\alpha_i^{n_i} \in F_i$ para algún n_i, ó $u_i^p - u_i \in F_i$

EJERCICIO 211. *Demuestre que el teorema de Galois de solubilidad de radicales (Proposición 113) es válido con la definición de extensión radical 77.*

Anexos

6. Retículas

DEFINICIÓN 78. *Sea P un conjunto y $\leq$ una relación sobre P. Decimos que P con $\leq$ es un conjunto parcialmente ordenado.*

1. *Para toda $x \in P$, $x \leq x$*
2. *Para todo $x, y \in P$, si $x \leq y$ e $y \leq x$, entonces $x = y$*
3. *Para todo $x, y, z \in P$, si $x \leq y$ e $y \leq z$, entonces $x \leq z$*

Una notación común es escribir $(P, \leq)$ para un conjunto parcialmente ordenado con conjunto subyacente P y orden $\leq$.

EJEMPLO 74. *Sea X un conjunto. Entonces el conjunto potencia $\mathscr{P}(X)$ es un conjunto parcialmente ordenado con la contención $\subseteq$.*

DEFINICIÓN 79. *Sea L un conjunto parcialmente ordenado. Decimos que L tiene un elemento máximo x. Si para todo $y \in L$, $y \leq x$. Por la asimetría el elemento máximo es único y lo denotamos por $\bar{1}$.*

En el caso de $\mathscr{P}(X)$ su elemento máximo es X.

DEFINICIÓN 80. *Sea L un conjunto parcialmente ordenado. Decimos que L tiene un elemento mínimo x. Si para todo $y \in L$, $x \leq y$. Por la asimetría el elemento máximo es único y lo denotamos por $\bar{0}$.*

En el caso de $\mathscr{P}(X)$ su elemento mínimo es $\emptyset$.

DEFINICIÓN 81. *Sea L un conjunto parcialmente ordenado, $S \subseteq L$ y $a \in L$. Decimos que a es una cota superior de S, si $x \leq a$ para toda $x \in S$.*

En caso de S sea vacío, cualquier elemento de L es cota superior.

DEFINICIÓN 82. *Sea L un conjunto parcialmente ordenado, $S \subseteq L$ y $a \in L$. Decimos que a es el supremo de S, si a es la menor cota superior, es decir, si a cumple:*

- *Para todo $x \in S$, $x \leq a$.*
- *Si $b \in L$ es tal que para todo $x \in S$ tenemos que $x \leq b$, entonces $a \leq b$*

NOTACIÓN 1. *Sean L un conjunto parcialmente ordenado, $S \subseteq L$ y $x, y \in L$. Denotamos por $\bigvee S$ al supremo de S. En caso de que $S = \{x, y\}$, ponemos $x \vee y$ para denotar al supremo.*

En caso de S sea vacío, $\bigvee S = \bar{0}$.

DEFINICIÓN 83. *Sea L un conjunto parcialmente ordenado, $S \subseteq L$ y $a \in L$. Decimos que a es una cota inferior de S, si $a \leq x$ para toda $x \in S$.*

En caso de S sea vacío, cualquier elemento de L es cota inferior.

DEFINICIÓN 84. *Sea L un conjunto parcialmente ordenado, $S \subseteq L$ y $a \in L$. Decimos que a es el ínfimo de S, si a es la menor cota inferior, es decir, si a cumple:*

- *Para todo $x \in S$, $a \leq x$.*
- *Si $b \in L$ es tal que para todo $x \in S$ tenemos que $b \leq x$, entonces $b \leq a$*

NOTACIÓN 2. *Sean L un conjunto parcialmente ordenado, $S \subseteq L$ y $x, y \in L$. Denotamos por $\bigwedge S$ al ínfimo de S. En caso de que $S = \{x, y\}$, ponemos $x \wedge y$ para denotar al ínfimo.*

En caso de S sea vacío, $\bigwedge S = \bar{1}$.

DEFINICIÓN 85. *Sea L un conjunto parcialmente ordenado. Decimos que L es una retícula, si para todo $x, y \in L$ $x \wedge y$ y $x \vee y$ existen.*

EJEMPLO 75. *$\mathbb{N}$ con el orden inducido por divisibilidad, es decir si $x|y$ entonces $x \leq y$. Para cualesquiera $x, y \in \mathbb{N}$ se tiene que $x \wedge y = (x, y)$ y $x \vee y = [x, y]$.*

EJEMPLO 76. *Sea G un grupo. Denotemos por $Sub(G)$ al conjunto de subgrupos de G, entonces el COPO $(Sub(G), \subseteq)$ es una retícula. Donde $H \vee K = \langle H \cup K \rangle$ y $H \wedge K = H \cap K$ para cualesquiera $H, K \in Sub(G)$.*

El ejemplo por el cual introducimos la noción de retícula se presenta a continuación.

EJEMPLO 77. *Sea R un anillo. Denotemos por $\mathfrak{I}$ al conjunto de ideales del anillo R. Entonces el COPO $(\mathfrak{I}, \subseteq)$ es una retícula. Donde $I \vee J = I + J$ y $I \wedge J = I \cap J$ para cualesquiera $I, J \in \mathfrak{I}$.*

Podemos hablar de propiedades del anillo en términos de su retícula de ideales, como por ejemplo.

PROPOSICIÓN 114. *Sea R un anillo, R es un campo si y sólo si* $\mathfrak{I} = \{0, R\}$

DEFINICIÓN 86. *Una retícula L es completa si para todo subconjunto S de L,* $\bigvee S$ *y* $\bigwedge S$ *existen.*

Tenemos que $\mathscr{P}(X)$ es una retícula completa.

PROPOSICIÓN 115. *Sean L una retícula tal que existen todos los infimos. Entonces L es una retícula completa.*

DEMOSTRACIÓN. Sea $S \subseteq L$, debemos probar que $\bigvee S$ y $\bigwedge S$ existen.
Como por hipótesis existen todos los infimos de L entonces $\bigwedge S$ existe. Falta probar la existencia de $\bigvee S$.
Notemos que $\bigvee S = \bigwedge\{x \in L : (\forall y \in S, y \leq x)\}$ como todos los infimos existen, en particular existe $\bigwedge\{x \in L : (\forall y \in S, y \leq x)\}$ es decir $\bigvee S$ existe, concluimos que L es una retícula completa. □

Observación. Si L es una retícula completa L tiene elemento mínimo y máximo, es decir $\bar{1}, \bar{0} \in L$.

DEFINICIÓN 87. *Una retícula L es modular, si* $a \leq b$ *implica* $a \vee (x \wedge b) = (a \vee x) \wedge b$ *para cualesquiera* $a, b, x \in L$.

DEFINICIÓN 88. *Una retícula L es distributiva, si* $x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z)$ *para cualesquiera* $x, y, z \in L$.

PROPOSICIÓN 116. *Sea R un anillo. Consideremos a la retícula* $\mathfrak{I}$ *de ideales de R.* $\mathfrak{I}$ *es modular.*

DEMOSTRACIÓN. Sea $I, J, K \leq R$ ideales de R, ademas $I \subseteq J$, entonces

Comencemos probando que $I \vee (K \wedge J) = I + (K \cap J) \leq (I + K) \cap J = (I \vee K) \wedge J$

Basta verificar que $I, (K \cap J) \leq (I + K) \cap J$, por un lado es claro que $I \leq J$ por hipótesis y $I \leq I + K$, así $I \leq (I + K) \cap J$. Por otro lado, como $K \leq I + K$ entonces $K \cap J \leq (I + K) \cap J$ por lo tanto $I + (K \cap J) \leq (I + K) \cap J$

Probemos ahora que $(I + K) \cap J \leq I + (K \cap J)$ es decir, veamos que $(I + K) \cap J \subseteq I + (K \cap J)$.

Sea $x \in (I+K)\cap J$, entonces $x \in (I+K)$ y $x \in J$, así $x = i+k$ para alguna $i \in I$ y $k \in K$, nos gustaría ver que x es de la forma $x = i+p$ donde $p \in K\cap J$. Notemos que $x-i = k \in J$ ya que $x \in J$ y como $i \in I \subseteq J$, entonces $k \in K\cap J$ y como $x = i+k$ entonces $x \in I+(K\cap J)$. Concluimos que $(I+K)\cap J \leq I+(K\cap J)$ y por lo tanto $I\vee(K\wedge J) = I+(K\cap J) = (I+K)\cap J = (I\vee K)\wedge J$ es decir $\mathfrak{I}$ es modular. □

EJERCICIO 8. *(Tarea) En general para un anillo R, su retícula de ideales $\mathfrak{I}$ no es distributiva. Dar un ejemplo de un anillo para el cual su retícula de ideales no sea distributiva.*

Presentamos ahora los conceptos de átomo y co-átomo, que resultan ser ideales distinguidos en la retícula de ideales de un anillo R.

DEFINICIÓN 89. *Sea L una retícula con elemento mínimo $\bar{0}$, decimos que $a \in L$ es un átomo de L si:*

- $\bar{0} \leq a$
- *Para todo $x \in L$ tal que $\bar{0} \leq x \leq a$ entonces $x = \bar{0}$ o $x = a$*

DEFINICIÓN 90. *Sea L una retícula, decimos que L es átomica si para todo $x \in L$ existe un átomo $a \in L$ tal que $a \leq x$.*

EJEMPLO 78. *Consideremos a la retícula $(\mathscr{P}(X),\subseteq)$ para algún conjunto X, esta es átomica ya que para cualquier subconjunto $S \subseteq X$ tenemos que $\{s\} \subseteq S$ donde $s \in S$.*

EJEMPLO 79. *Sea K un campo y V un K-espacio vectorial. Consideremos a la retícula $(Sub_K(V),\subseteq)$ donde $Sub_K(V)$ denota al conjunto de K-subespacios del K-espacio vectorial V, entonces $(Sub_K(V),\subseteq)$ es átomica y los átomos son los subespacios de dimension 1.*

De manera análoga podemos introducir la idea de co-átomo

DEFINICIÓN 91. *Sea L una retícula con elemento máximo $\bar{1}$, decimos que $c \in L$ es un co-átomo de L si:*

- $c \leq \bar{1}$
- *Para todo $x \in L$ tal que $c \leq x \leq \bar{1}$ entonces $x = \bar{1}$ o $x = c$*

Observación
Sea R un anillo. Para todo ideal $I \neq R$ existe un ideal máximo $J_M \leq R$ tal que $I \subseteq J_M$. Para probar tal afirmación se debe hacer uso del lema de Zorn, es decir, debemos considerar un copo $(\mathscr{F},\leq)$ y probar que toda cadena tiene cota superior. Así para cualquier anillo R, existen los ideales máximos. Note que estos son los co-átomos en la reticula de ideales $\mathfrak{J}$ de R.

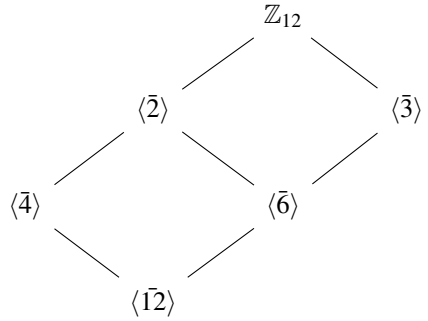
DEFINICIÓN 92. *Sea L una retícula con elemento máximo* $\bar{1}$ *y elemento mínimo* $\bar{0}$*, decimos que L es complementada si para todo* $x \in L$ *existe* $y \in L$ *tal que* $x \vee y = \bar{1}$ *y* $x \wedge y = \bar{0}$

DEFINICIÓN 93. *Sean L una retícula, y* $x, y \in L$*. Decimos que y es un pseudocomplemento de x si:*

- $x \wedge y = \bar{0}$.
- *Si* $z \in L$ *es tal que* $z \wedge x = \bar{0}$ *y* $y \leq z$*, entonces* $z = y$.

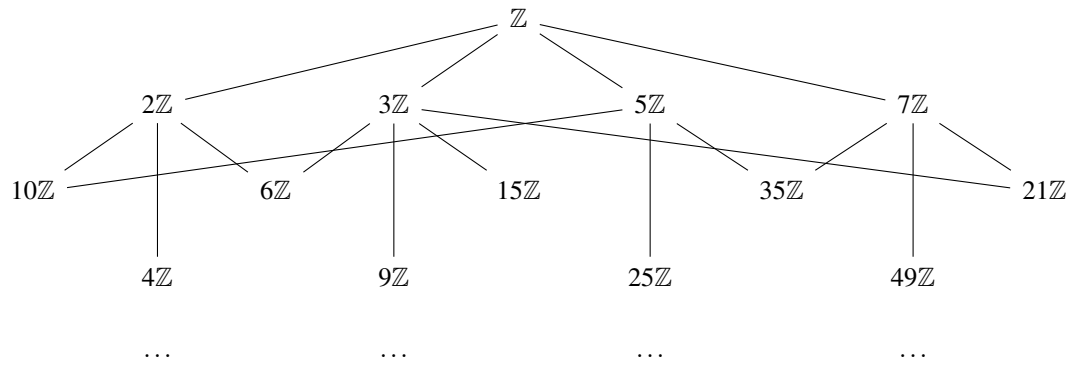
A continuación presentamos algunos ejemplos sobre retículas de ideales para anillos. Comencemos con un ejemplo sencillo.

EJEMPLO 80. *Consideremos al anillo* $\mathbb{Z}_{12}$*. No es difícil convencerse que los ideales de* $\mathbb{Z}_{12}$ *son* $\langle\bar{2}\rangle$*,* $\langle\bar{3}\rangle$*,* $\langle\bar{4}\rangle$*,* $\langle\bar{6}\rangle$*,* $\langle\bar{1}\bar{2}\rangle$*. Un argumento mas formal es el siguiente, los ideales* $\bar{J} \leq \mathbb{Z}_{12}$ *estan en correspondencia biyectiva con los ideales* $J \leq \mathbb{Z}$ *tales que* $J \subseteq 12\mathbb{Z}$*. El siguiente diagrama ilustra la retícula de ideales de* $\mathbb{Z}_{12}$*:*



El diagrama anterior se conoce como Diagrama de Hasse.

EJEMPLO 81. *Consideremos a nuestro arquetipo de anillo, es decir* $\mathbb{Z}$*. Es bien sabido que si* $I \leq \mathbb{Z}$ *es un ideal, entonces* $I = \langle m\rangle$ *para algún* $m \in \mathbb{Z}$*, es decir* $I = m\mathbb{Z}$*. A continuación ilustramos su retícula de ideales* $\mathfrak{I}$*:*



Podemos notar que en la primera fila se encuentras los ideales máximos(los co-átomos de la retícula).

7. Lema de Zorn

El lema de Zorn, o Kuratowski-Zorn, es quizás el enunciado equivalente al axioma de elección que más se utiliza en álgebra pues permite garantizar la existencia de estructuras con alguna característica de maximalidad.

La meta de esta sección es enunciarlo, para lo cual se va a hacer una pequeña discusión respecto a los conceptos previos que se requieren para ello.

DEFINICIÓN 94. *Sea $(P,\leq)$ un conjunto parcialmente ordenado y $S \subseteq P$. Decimos que S tiene un:*

1. *Elemento máximo si existe $x \in S$ tal que no existe $y \in S$ con la propiedad de que $x \lneq y$. En tal caso se dice que x es un elemento máximo.*
2. *Elemento mayor si existe $x \in S$ tal que para cualquier $y \in S$, $y \leq x$. En tal caso se dice que x es el mayor elemento de S.*

Es importante mencionar que en muchos libros de texto de habla hispana la primera de las definiciones presentadas se suele llamar elemento maximal y la segunda elemento máximo. La terminología seguida en estas notas es debida a Francisco Raggi quien comentaba que el término maximal es una mala traducción del inglés del concepto correspondiente. Mucha gente que pertenece a la escuela de Raggi usa la terminología, que es la que adoptaremos en estas notas.

Por otro lado el lector se imaginará como se definen los conceptos duales que son mínimo y menor elemento. Además recuerde que un conjunto puede tener muchos elementos máximos, pero tiene un único mayor elemento. Además, de que todo mayor elemento es un elemento máximo, pero el concepto de elemento máximo es más débil que el de elementos mayor, y lo análogo sucede con elementos mínimos y el menor elemento.

EJEMPLO 82. *Para $X = \{a,b,c\}$, si $P \subseteq \mathscr{P}(X)$ es el subconjunto formado por los subconjuntos propios de X, observe que $(P,\subseteq)$ es un conjunto parcialmente ordenado. Son elementos máximos los conjuntos $\{a,b\},\{a,c\},\{b,c\}$. Este conjunto parcialmente ordenado no tiene mayor elemento pero si tiene menor elemento a saber $\emptyset$. Observe que si $Q \subseteq \mathscr{P}(X)$ es el subconjunto formado por los subconjuntos propios de X no vacíos, se tienen los mismos máximos que antes pero ahora no hay menor elemento, sin embargo hay tres elementos mínimos $\{a\},\{b\},\{c\}$.*

EJEMPLO 83. *Considere $(\mathbb{N}\setminus\{0,1\},\leq)$, donde el orden está definido por:*

$$a \leq b, \text{ si } b|a.$$

Dicho conjunto parcialmente ordenado tiene como elementos máximos a cualquier primo positivo. Pero es obvio que no tiene un elemento mayor.

El ejemplo anterior hace ver que cuál es el problema en torno a por qué los elementos máximos no pueden ser el mayor elemento de un conjunto pues estos pueden ser no comparables. Por tal razón observe que en un conjunto totalmente ordenado ambos conceptos coinciden. Esto nos lleva a formular una definición general.

DEFINICIÓN 95. *Sea $(P,\leq)$ un conjunto parcialmente ordenado. Una cadena es un subconjunto $S \subseteq P$ que es totalmente ordenado, es decir, cualesquiera dos elementos de S son comparables.*

Retomando el ejemplo de $(\mathbb{N} \setminus \{0,1\},\leq)$ observe que el conjunto $\{2^n \mid n \in \mathbb{N}\}$ es una cadena y que en esta el elemento máximo es 2, que es de hecho el elemento mayor en dicha cadena.

El ejemplo anterior muestra que en las cadenas de un conjunto parcialmente ordenado los conceptos de máximo y mayor elemento coinciden, lo que es más general que la afirmación correspondiente para el conjunto totalmente ordenado.

Una vez discutidos estos importantes y sutiles conceptos podemos enunciar el resultado que se quiere.

PROPOSICIÓN 117. *(Lema de Zorn) Cualquier conjunto parcialmente ordenado no vacío en el que toda cadena es acotada superiormente, tiene un elemento máximo.*

Para más información del lema de Zorn se recomienda consultar el libro “Axiom of Choice” de Horst Herrlich.

8. Acciones de grupos

El material de esta sección incluyendo los detalles se pueden consultar con mayor profundidad en el libro de Rotmann "An introduction of theory of groups".

DEFINICIÓN 96. *Sea G un grupo. Un G-conjunto X, es un conjunto X y una función $\rho\colon G\times X\longrightarrow X$. Notacionalmente escribiremos $gx:=\rho(g,x)$ para toda $g\in G$ y $x\in X$. Esta tiene que cumplir:*

- *$ex=x$ para toda $x\in X$.*
- *$(gh)x=g(hx)$ para toda $g,h\in G$ y $x\in X$.*

También se dice G actúa sobre X, esto porque a ρ se le llama una acción de G sobre X.

La siguiente proposición nos dice que toda acción induce un morfismo de grupo y viceversa.

PROPOSICIÓN 118. *Sea G un grupo y X un conjunto.*

1. *Si X es un G-conjunto, definimos $\rho\colon G\longrightarrow S_X$ dada por $\rho(g)(x)=gx$ para $g\in G$ y $x\in X$. Entonces ρ es un morfismo de grupos.*
2. *Sea $\rho\colon G\longrightarrow S_X$ un morfismo de grupos. Entonces la función $\lambda\colon G\times X\longrightarrow X$ dada por $\lambda(g,x)=\rho(g)(x)$ con $g\in G$ y $x\in X$, es una acción.*

Más aún,las dos construcciones anteriores son inversas una de la otra.

Continuando con las definiciones.

DEFINICIÓN 97. *Sea X es un G-conjunto y $x\in X$. Definimos:*

1. *la orbita de x, como el conjunto $Gx:=\{gx\in X\mid g\in G\}$.*
2. *el estabilizador de x, G_x, son los elementos $g\in G$ tales que $gx=x$.*

Uno de los resultados más importantes de acciones de grupos se presenta a continuación.

PROPOSICIÓN 119 (Teorema de Orbita-Estabilizador). *Sean X un G-conjunto y $x\in X$. Entonces,*

$$|Gx|=[G:G_x]$$

DEFINICIÓN 98. *Una acción de G en un conjunto X es transitiva si cualquiera, y por lo tanto ambas de las siguientes condiciones equivalentes, se cumplen:*

1. *Para cualesquiera $x, y \in X$ existe $g \in G$ tal que $y = gx$*
2. *La acción tiene una única órbita*

9. Grupos Solubles

DEFINICIÓN 99.

1. *Una serie normal de un grupo G es una sucesión de subgrupos de G,*

$$e = G_0 \leq G_1 \leq \cdots \leq G_n = G$$

tales que $G_i \trianglelefteq G_{i+1}$ para $i = 0, \ldots, n-1$. Llamamos a n la longitud de la serie normal. A G_{i+1}/G_i los llamamos los grupos factor de la serie.

2. *Una serie normal se llama soluble si todos sus grupos factor son abelianos. Un grupo es soluble si tiene una serie soluble.*

Los siguientes dos resultados dan dos importantes familias de ejemplos donde la condición de solubilidad se hereda.

PROPOSICIÓN 120. *Sea G un grupo soluble. Entonces todo subgrupo de G es soluble.*

DEMOSTRACIÓN. Sea $H \leq G$ y $e = G_0 \leq G_1 \leq \cdots \leq G_n = G$ una serie soluble de G. Consideramos la serie

$$e = G_0 \cap H \leq G_1 \cap H \leq \cdots \leq G_n \cap H = G \cap H = H$$

Aplicando el segundo teorema de isomorfismo a $H \cap G_{i+1} \leq G_{i+1}$ y $G_i \trianglelefteq G_{i+1}$ tenemos que $H \cap G_i = (H \cap G_{i+1}) \cap G_i \trianglelefteq H \cap G_{i+1}$. Por lo que la tenemos una serie normal. También por el segundo teorema de isomorfismo tenenmos que:

$$(H \cap G_{i+1})/(H \cap G_i) \cong G_i(H \cap G_{i+1})/G_i \leq G_{i+1}/G_i$$

Por lo que $(H \cap G_{i+1})/(H \cap G_i)$ es un subgrupo de un grupo abeliano. Por lo que es abeliano y así la serie es soluble. Por lo tanto H es soluble. □

PROPOSICIÓN 121. *Sea G un grupo soluble. Entonces todo grupo cociente de G es soluble.*

DEMOSTRACIÓN. Sea $H \leq G$, $\pi\colon G \longrightarrow G/H$ la proyección canónica y $e = G_0 \leq G_1 \leq \cdots \leq G_n = G$ una serie soluble de G. Consideramos la serie

$$e = \pi(G_0) \leq \pi(G_1) \leq \cdots \leq \pi(G_n) = G/H$$

Sea $\pi(x) \in \pi(G_i)$ con $x \in G_i$ y $\pi(y) \in \pi(G_{i+1})$ con $y \in G_{i+1}$. Entonces $yxy^{-1} \in G_i$ por lo que $\pi(y)\pi(x)\pi(y)^{-1} \in \pi(G_i)$. Por lo que la serie es normal. Consideramos los epimorfismos $G_i \longrightarrow \pi(G_{i+1})$ y $\pi(G_{i+1}) \longrightarrow \pi(G_{i+1})/\pi(G_i)$ y su composición $\phi\colon G_{i+1} \longrightarrow$

$\pi(G_{i+1})/\pi(G_i)$. Como $G_i \leq nuc(\phi)$, entonces se induce un epimorfismo $\psi\colon G_{i+1}/G_i \longrightarrow \pi(G_{i+1})/\pi(G_i)$. Por lo que $\pi(G_{i+1})/\pi(G_i)$ es el cociente de un grupo abeliano y así es un grupo abeliano. Por lo tanto la sucesión es soluble y así G/H es soluble. □

El siguiente resultado dice que los grupos solubles son cerrados bajo extensiones.

PROPOSICIÓN 122. *Sea G un grupo y H un subgrupo normal de G tal que H y G/H es soluble. Entonces G es soluble.*

DEMOSTRACIÓN. Sea $e = G_0 \leq G_1/H \leq \cdots \leq G_n/H = G/H$ una serie soluble de G/H y $e = H_0 \leq H_1 \leq \cdots \leq H_m = H$ una serie soluble de H. La serie

$$e = H_0 \leq H_1 \leq \cdots \leq H_m \leq G_0 \leq G_1 \leq \ldots G_n = G$$

es soluble. □

COROLARIO 27. *Si G y H son grupos solubles. Entonces $G \times H$ es un grupo soluble.*

A continuación se mencionan los ejemplos básicos de grupos solubles.

EJEMPLO 84. *Todo grupo abeliano es soluble.*

EJEMPLO 85. *Sea p un primo. Entonces todo p-grupo finito es soluble.*

EJEMPLO 86. *Ningún grupo no abeliano simple es soluble. En particular A_n no es simple para $n \geq 5$.*

EJEMPLO 87. *S_n no es soluble para $n \geq 5$.*

Bibliografía

[1] Emil Artin. *Galois Theory*. University of Notre Dame Press, 1971.

[2] Michael Atiyah and Ian Macdonald. *Introduction to Commutative Algebra'*. Adisson-Wesley Publishing Company, 1906.

[3] John Fraleigh. *A first course in abstrac algebra*. Addison-Wesley, 1998.

[4] Jürgen Neukirch. *Algebraic Number Theory*. Springer-Verlag Berlin, 1999.

[5] Steven Weintraub. *Galois Theory'*. Springer Universitext, 2009.