

MATE6201-0U1
Prof. Luis A. Medina
10.00 - 11.20
CNL-A-207

Algebra Moderna

Alec Zabel-Mena

Universidad de Puerto Rico, Recinto de Rio Piedras

12.12.2022

Lectura 1: Grupos y Subgrupos

Definición. Sea G un conjunto no vacío junto a una operación binaria \cdot . Decimos que el par (G, \cdot) es un **grupo** si:

- (1) $a \cdot b \in G$ para $a, b \in G$.
- (2) $a \cdot (b \cdot c) = (a \cdot b) \cdot c$, para $a, b, c \in G$
- (3) Existe un $e \in G$ tal que $a \cdot e = e \cdot a = a$ para toda $a \in G$.
- (4) Para toda $a \in G$, existe una $a^{-1} \in G$ tal que $a \cdot a^{-1} = a^{-1} \cdot a = e$.

Si $a \cdot b = b \cdot a$ para toda $a, b \in G$, entonces decimos que G es un grupo **Abeliano**.

Ejemplo 1. (1) Los naturales \mathbb{N} junto a la multiplicación se satisface los primeros tres axiomas, pero no es un grupo. De hecho, \mathbb{N} forma un estructura llamado un “monoide”.

- (2) El grupo mas pequeño es el conjunto $\{e\}$, que denotamos como $\langle e \rangle$. $\langle e \rangle$ es, trivialmente, un grupo Abeliano.
- (3) Los enteros \mathbb{Z} junto con adición $+$ forma un grupo Abeliano por la commutatividad de adición de los enteros.
- (4) El conjunto $GL(n, \mathbb{R})$ de matrices $n \times n$ con entradas reales, nosingular forman un grupo con respecto a multiplicación de matrices. $GL(n, \mathbb{R})$ no es un grupo Abeliano.
- (5) Sea S cualquier conjunto y $A(S)$ el conjunto de todas las funciones 1–1 y sobre llevando elementos de S a elementos de S . Entonces $A(S)$ es un grupo no Abeliano con respecto a composición de funciones, \circ . Si S tiene n elementos, entonces exscribimos $A(S) = S_n$. $A(S)$ también no se Abeliano ya que para funciones cualesquiera f, g , $f \circ g \neq g \circ f$.

Definición. Sea G un grupo. El **orden** de un grupo es su cardinalidad, y escribimos $\text{ord } G = |G|$. Decimos que G es **finito** si $\text{ord } G$ es finito; de lo contrario, G es **infinito**.

Definición. Sea G un grupo, y $a \in G$. El **orden** de a , denotado $\text{ord } a$, es el menor entero positivo n tal que $a^n = e$ y escribimos $\text{ord } a = n$. Si tal n no existe, entonces decimos que a es de orden **infinita**, y decimos que a es un elemento **torsión**.

Ejemplo 2. (1) Considera $\mathbb{C}^* = \mathbb{C} \setminus \{0\}$, entonces \mathbb{C}^* tiene orden infinita, note que si $\alpha = \exp(\frac{2i\pi}{5}) \in \mathbb{C}^*$, entonces $\alpha \neq 1$, para $j \neq 1, 2, 3, 4$, pero $\alpha^5 = 1$. Entonces $\text{ord } \alpha = 5$.

(2) Considere $A \in GL(6, \mathbb{R})$ con la forma

$$A = \begin{pmatrix} 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \end{pmatrix}$$

Entonces

$$A^3 = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

entonces, $A^3 = I$.

(3) En $\mathbb{R}^* = \mathbb{R} \setminus \{0\}$, \mathbb{R}^* es infinito, y $\text{ord } 2$ es infinito.

Definición. Sea G un grupo y $H \subseteq G$ no vacío. Entonces decimos que H es un **subgrupo** de G si H es un grupo bajo la misma operación de G . Escribimos $H \leq G$.

Ejemplo 3. (1) Considere $GL(n, \mathbb{R})$ y sea $SL(n, \mathbb{R})$ los elementos $A \in GL(n, \mathbb{R})$ tales que $\det A = 1$. Entonces $SL(n, \mathbb{R}) \leq GL(n, \mathbb{R})$.

(2) Sea $C(\mathbb{R})$ el conjunto de todas las funciones continuas sobre \mathbb{R} . Entonces $C(\mathbb{R})$ es un grupo bajo la suma de funciones $+$. Sea $C^1(\mathbb{R})$ el conjunto de funciones primer diferenciables continuas sobre \mathbb{R} . Es decir, que f' existe y es continua. Observe lo siguiente:

- (a) $(f + g)' = f' + g'$
- (b) $f' + (g + h)' = (f + g)' + h'$.
- (c) $c' = 0$, entonces $0 \in C^1(\mathbb{R})$
- (d) $f' - f' = -f' + f' = 0$.

Suponiendo que $f', g', h' \in C^1(\mathbb{R})$, son continuas, entonces vemos que las funciones de arriba también son continuas. Entonces $C'(\mathbb{R}) \leq C(\mathbb{R})$.

Lema 1. Sea G un grupo y $H \subseteq G$ no vacío. Si tenemos que $ab \in H$, implicat que $ab^{-1} \in H$, entonces $H \leq G$.

demostración. Como $H \neq \emptyset$, sea $a \in H$. Entonces $aa^{-1} = e \in H$. Luego, también tenemos que $ea^{-1} = a^{-1} \in H$. Finalmente, tenemos que si $b \in H$, entonces $ab^{-1} \in H$, por lo tanto $b^{-1} \in H$, entonces $a(b^{-1})^{-1} = ab \in H$. ■

Ejemplo 4. (1) Considere a los enteros pares $2\mathbb{Z}$. Sean $2n, 2m \in 2\mathbb{Z}$. Noten que $2n - 2m = 2(n - m) \in 2\mathbb{Z}$. Entonces $2\mathbb{Z} \leq \mathbb{Z}$.

- (2) Si G es un grupo, entonces $\langle e \rangle$ y G son subgrupos de G . Llamamos a $\langle e \rangle$ el grupo **trivial**.
- (3) Si G es un grupo, y $a \in G$, entonces el conjunto $\langle a \rangle = \{a^j : j \in \mathbb{Z}\}$ es un subgrupo de G , llamado el **subgrupo generado por a** .
- (4) Si G es un grupo, y $a \in G$, entonces $C(a) = \{g \in G : ag = ga\}$ y $Z(G) = \{g \in G : ag = ga \text{ para toda } a \in G\}$ son subgrupos. Nota que $Z(G) = \bigcap C(a)$. Llamamos a $C(a)$ el **centralizador** de a y $Z(G)$ el **centro** de G .
- (5) Sea G un grupo y $H \leq G$, y sea $a \in G$, entonces $a^{-1}Ha \leq G$. Llamamos a $a^{-1}Ha$ el **conjugado** de H **con respecto** a a .

Definición. Suponga que G y H son grupos. Un mapa $\phi : G \rightarrow H$ se llama un **homomorfismo** si para toda $a, b \in G$, $\phi(ab) = \phi(a)\phi(b)$. Si ϕ es 1-1 y sobre, entonces lo llamamos un **isomorfismo**. Si ϕ es un isomorfismo, y $G = H$, entonces llamamos a ϕ un **automorfismo**.

Lectura 2: Grupos y Subgrupos

Ejemplo 5. (1) Considera \mathbb{R} bajo la suma $+$ y \mathbb{R}^+ bajo la multiplicación, \cdot . Sea $\phi : \mathbb{R} \rightarrow \mathbb{R}^+$ definido por $\phi : x \rightarrow \exp x$. Entonces ϕ es un homomorfismo, ya que

$\exp(x + y) = \exp x + \exp y$. De igual forma, nota que ϕ es $1 - 1$ y sobre, por lo tanto, existe inverso; de hecho, $\phi^{-1} = \log$, que tambien es un homomorfismo. Pues, tenemos ϕ es un isomorphismo y que $\mathbb{R} \simeq \mathbb{R}^+$.

- (2) Sea $\phi : GL(n, \mathbb{R}) \rightarrow \mathbb{R}^*$ dado por $\phi : A \rightarrow \det A$. Entonces ϕ es un homomorphismo ya que $\det AB = \det A \det B$. Nota que $GL(n, \mathbb{R})$ no es Abelian, pero \mathbb{R}^* si, por lo tanto $GL(n, \mathbb{R}) \not\simeq \mathbb{R}^*$. Esto también dice que no existe inverso \det^{-1} . Esto nos dice que los homomorfismos solo preservan el estructura de grupos, pero nada mas de eso.
- (3) Considere $\phi : \mathbb{Z} \rightarrow \mathbb{Z}/n\mathbb{Z}$ dado por $\phi(m) = m \bmod n$. Entonces $\phi(m + k) = (m + k) \bmod n \equiv m \bmod n + k \bmod n = \phi(m) + \phi(k)$. Así que ϕ es un homomorfismo.
- (4) Sea G y H grupos, y sea $\phi : G \rightarrow H$ un homomorfismo de G sobre H . Entonces si G es Abelian, también lo es H . Nota que para $h, h' \in H$, exists $g, g' \in G$ con $\phi(g) = h$ y $\phi(g') = h'$. Entonces $hh' = \phi(g)\phi(g') = \phi(gg') = \phi(g'g) = \phi(g')\phi(g) = h'h$.
- (5) Sea $\phi : \mathbb{Z} \rightarrow \mathbb{Z}$ dado por $x \rightarrow 5x$. Entonces $\phi(x + y) = 5(x + y) = 5x + 5y = \phi(x) + \phi(y)$.
- (6) Suponga que G es Abelian y defina $\phi : G \rightarrow G$ por la regla $\phi(a) = a^{-1}$. Entonces tenemos que $\phi(ab) = (ab)^{-1} = b^{-1}a^{-1} = a^{-1}b^{-1} = \phi(a)\phi(b)$. Así que ϕ es un homomorfismo. Nota también que por la ley de inversos de elementos, que ϕ es sobre. También tenemos que ϕ es $1 - 1$ ya que $a^{-1} = b^{-1}$ implica que $a = b$, por unicidad de inversos. Por lo tanto ϕ es un automorfismo.
- (7) Sea $\phi : \mathbb{Z} \rightarrow \mathbb{Z}$ dado por $x \rightarrow x^2$. ϕ no es un homomorfismo ya que en general, $(x + y)^2 \neq x^2 + y^2$. Pero, si tomamos la mapa $\psi : \mathbb{Z} \rightarrow \mathbb{Z}/2\mathbb{Z}$ dado por la misma regla, entonces ψ es un homomorfismo.

Definición. Sea G y H grupos, y $\phi : G \rightarrow H$ un homomorfismo de G hacia H . Definimos el **kernel** de ϕ como el conjunto $\ker \phi = \{a \in G : \phi(a) = e'\}$ donde e' es la identidad de H . Definimos también la **imagen** del homomorfismo como el conjunto $\Im \phi = \phi(G) = \{\phi(a) : a \in G\}$.

Lema 2. Sea G y H grupos y $\phi : G \rightarrow H$ un homomorfismo de G hacia H . Entonces $\ker \phi \leq G$ y $\phi(G) \leq H$.

demostración. Nota por definicion que $\ker \phi \subseteq G$. Tambien tenemos que $e \in \ker \phi$ por el ley de homomorfismo. Entonces $\ker \phi$ no es vacio. Ahora, sea $a, b \in \ker \phi$. Entonces, tenemos $\phi(ab^{-1}) = \phi(a)\phi(b^{-1}) = \phi(a)(\phi(b))^{-1} = e'e' = e'$, pues $ab^{-1} \in \ker \phi$. ■

Ejemplo 6. (1) Considere $\phi : \mathbb{Z} \rightarrow \mathbb{Z}/12\mathbb{Z}$ dado por $m \rightarrow m \bmod 12$. Entonces $\ker \phi = \langle 12m \rangle = 12\mathbb{Z}$. Tambien $\phi(\mathbb{Z}) = \mathbb{Z}/12\mathbb{Z}$; pues ϕ es sobre.

- (2) Considere $\phi : \mathbb{Z}/12\mathbb{Z} \rightarrow \mathbb{Z}/12\mathbb{Z}$ dado por $m \rightarrow 3m$. ϕ es un homomorfismo, y $\ker \phi = \{x \in \mathbb{Z}/12\mathbb{Z} : 3x \equiv_{12} 0\} = \{0, 4, 8\} = \langle 4 \rangle$. De igual manera, $\phi(\mathbb{Z}/12\mathbb{Z}) = \{0, 3, 6, 9\} = \langle 3 \rangle$.
- (3) Sea $\phi : \mathbb{Z} \rightarrow \mathbb{Z}$ dado por $m \rightarrow 5m$. Entonces $\ker \phi = \langle 5m \rangle = \langle 0 \rangle = 5\mathbb{Z}$. Nota que como ϕ es 1-1, si $a \in 5\mathbb{Z}$, entonces $a = 5m \equiv_5 0$. Note tambien que $\phi(\mathbb{Z}) = 5\mathbb{Z}$, por lo tanto ϕ es sobre, asi que tenemos $\mathbb{Z} \simeq 5\mathbb{Z}$.
- (4) Sea D_n el grupo dihedral sobre un poligono regular de n -vertices. Recuerda que $r^n = t^2 = e$ y que $tr^j = r^{n-j}t$. Considere la homomorfismo $\phi : D_8 \rightarrow \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, donde $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ es un grupo bajo la suma de productos directos. Entonces si $\phi(r) = (1, 0)$ y $\phi(t) = (0, 1)$ entonces tenemos que $\ker \phi = \langle r^2 \rangle$ y $\phi(D_8) = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Lectura 3: Grupos Cíclicos, Clases Laterales, y La Teorema de Lagrange.

Definición. Sea G un grupo. Definimos un **grupo cíclico** de G **generado** por un elemento $a \in G$ de ser el subgrupo de G $\langle a \rangle = \{a^j : j \in \mathbb{Z}\}$. Llamamos a a el **generador** del grupo. Si $G = \langle a \rangle$ para algun $a \in G$, entonces decimos que G es **cíclico**.

Ejemplo 7. (1) Considere el grupo $\langle A \rangle$, donde

$$A = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \end{pmatrix}$$

Nota que $A^4 = I$, entonces $\langle A \rangle = \{I, A, A^2, A^3\}$ es un subgrupo de orden $\text{ord } A = 4$ del grupo $GL(4, \mathbb{R})$.

- (2) Considere el grupo dihedral $D_3 = \{e, r, r^2, t, rt, r^2t\}$ Los sobgrupos de D_3 son los sigu-

ientes en la reticulo de subgrupos siguiente con los ordenes anotados:



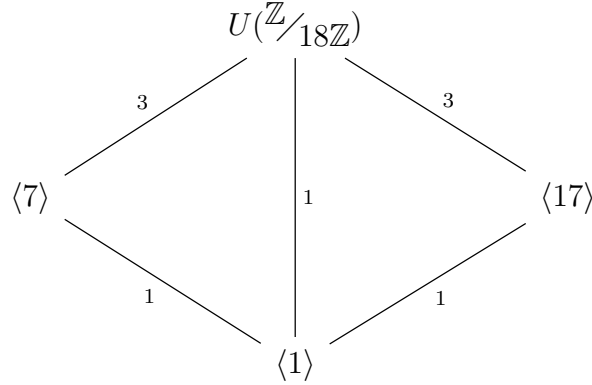
Teorema 3 (Teorema Fundamental de Grupos Cíclicos). *Todo subgrupo de un grupo cíclico es cíclico. mas aún si $G = \langle a \rangle$ es un grupo cíclico de orden $G = n$, entonces G tiene un subgrupo de orden d por cada divisor d de n .*

demostración. Sea $G = \langle a \rangle$ y $H \leq G$. Observe qu si $H = \langle e \rangle$, entonces terminamos. Pues suponga que $H \neq \langle e \rangle$. Entonces existe un $h \in H$ con $h \neq e$. Es decir, que $h = a^j$ para alguna $j \in \mathbb{Z}$. Nota que si $j > 0$ entonces h es una potencia positiva de j ; de igual manera, si $j < 0$ entonces $h^{-j} = (h^{-1})^j$ es una potencia psotiva de j . Es decir, H tiene potencias positivas. Por lo tanto, por el principio de buen orden, existe una potencia positiva mas pequeño, sea a^m . Sea $h \in H$, entonces $h = a^k$ para algún $k \in \mathbb{Z}$. Entonces por la teorema de división, existe $q, r \in \mathbb{Z}$ tales que $k = qm + r$ y $0 \leq r < m$. Entonces $a^k = a^{qm+r} = a^{qm}a^r = (a^m)^qa^r$. Como $a^k \in H$, y $a^m \in H$, es necesario tener $(a^m)^qa^r \in H$ para preservar que $H \leq G$. Entonces, si $a^r \neq e$, tenemos una potencia de a mas pequeño que a^m , lo cual no puede pasar. Es decir $a^r = e$, y $a^k = (a^m)^q$. Es decir todo elemento de h es una potencia del elemento a^m , por lo tanto $H = \langle a^m \rangle$ es cíclico.

Ahora sea $\text{ord } G = n$ y sea d un divisor positivo de n . Como $d|n$, entonces existe un $k \in \mathbb{Z}^+$ con $n = kd$. Ahora considere el subgrupo $\langle a^k \rangle$ Entonces sea $j \in \mathbb{Z}$ y considere $(a^k)^j$. Nota que $(a^k)^d = a^{kd} = a^n = e$, y si $0 < d < j$ entonces $(a^k)^j = a^{kj} \neq e$ por lo tanto $\text{ord } a^k = d$, lo cual dice que $\text{ord } \langle a^k \rangle = d$. ■

Ejemplo 8. (1) Sea $U(\mathbb{Z}/18\mathbb{Z}) = \{1, 5, 7, 11, 13, 17\}$ el grupo de unidades dde $\mathbb{Z}/18\mathbb{Z}$. Observe que $U(\mathbb{Z}/18\mathbb{Z}) = \langle 5 \rangle$, y que $\text{ord } U(\mathbb{Z}/18\mathbb{Z}) = \text{ord } \langle 5 \rangle = 6$. Entonces $U(\mathbb{Z}/18\mathbb{Z})$

tiene los siguientes subgrupos mostrado en la siguiente retículo con ordenes anotados:



- (2) El grupo de unidades de $\mathbb{Z}/50\mathbb{Z}$, $U(\mathbb{Z}/50\mathbb{Z}) = \langle 3 \rangle$ tiene el siguiente retículo de subgrupos:



Teorema 4 (Criterio de Igualdad de Potencias). *Suponga que G es un grupo. Sea $a \in G$, y sea $i, j \in \mathbb{Z}$ tales que $a^i = a^j$. Si a es de orden infinito, entonces $i = j$; de igual manera, si $\text{ord } a = n$, entonces $i \equiv j \pmod{n}$.*

Corolario. *Sí $j \in \mathbb{Z}^+$, entonces $\langle a^j \rangle = \langle a^{(j,n)} \rangle$, y $\text{ord } a^j = \frac{n}{(j,n)}$, donde (j, n) es el máximo común divisor de j y n .*

Corolario. *Sí $G = \langle a \rangle$, y $\text{ord } G = \text{ord } \langle a \rangle = n$, entonces a^j es generador de G sí y solo sí $(j, n) = 1$. La cantidad de generadores de G está dado por $\phi(n)$ donde ϕ es la función Euler- ϕ .*

Ejemplo 9. Considere de nuevo $U(\mathbb{Z}/50\mathbb{Z}) = \langle 3 \rangle$. Tenemos que $\phi(50) = 20$, así que los

generadores de $U(\mathbb{Z}/50\mathbb{Z})$ son potencias 3^j donde $(j, 50) = 1$. Es decir, los generadores son:

$$3^1 \quad 3^3 \quad 3^7 \quad 3^9 \quad 3^{11} \quad 3^{13} \quad 3^{17} \quad 3^{19}$$

Teorema 5. Sea G un grupo cíclico. Entonces $G \simeq \mathbb{Z}$ ó $G \simeq \mathbb{Z}/n\mathbb{Z}$ para algún $n \in \mathbb{Z}^+$.

demostración. Sea G un grupo cíclico. Suponga que G es infinito. Como los elementos de G son de la forma a^j para $j \in \mathbb{Z}$, considere el mapa $\phi : G \rightarrow \mathbb{Z}$ dado por $a^j \rightarrow j$. Entonces ϕ es un homomorfismo de G sobre \mathbb{Z} , ya que j corresponde a la potencia de uno de los infinito elementos de G . Mas aún, ϕ es 1-1, ya que $a^i = a^k$ implica que $i = k$. Es decir ϕ define un isomorfismo entre G y \mathbb{Z} .

De igual forma, suponga que $\text{ord } G = n$. Nota entonces que G tiene la forma $G = \{a^j : j \in \mathbb{Z}/n\mathbb{Z}\}$. Define entonces $\phi : G \rightarrow \mathbb{Z}/n\mathbb{Z}$ dado por $a^j \rightarrow j \pmod n$. ϕ es un homomorfismo de G sobre $\mathbb{Z}/n\mathbb{Z}$, por definición. ϕ también es 1-1 ya que $a^i = a^j$ implica $i \equiv j \pmod n$. Esto define un isomorfismo de G sobre $\mathbb{Z}/n\mathbb{Z}$. ■

Ejemplo 10. Considere \mathbb{C} y sea $i \in \mathbb{C}$. Entonces $\langle i \rangle = \{1, i, -1, -i\}$ por multiplicación, así que $\text{ord } \langle i \rangle = \text{ord } i = 4$. Por la teorema anterior, esto hace $\langle i \rangle \simeq \mathbb{Z}/4\mathbb{Z}$.

Definición. Sea G un grupo y $H \leq G$. Si $a \in G$ definimos la **clase lateral por la derecha** de H **generado** por a de ser el conjunto $Ha = \{ha : h \in H\}$. De igual forma, definimos la **clase lateral por la izquierda** de H **generado** por a de ser el conjunto $aH = \{ah : h \in H\}$.

Definición. Sea G un grupo y $H \leq G$. Defina la relación \equiv sobre G de la siguiente forma: $a \equiv b$ si y solo si $ab^{-1} \in H$. Llamamos a \equiv **congruencia modulo H** . Escribimos $a \equiv b \pmod H$, ó simplemente $a \equiv_H b$.

Lema 6. Sea G un grupo y $H \leq G$. Entonces la relación de congruencia modulo H sobre G es una relación de equivalencia.

demostración. Como $H \leq G$, tenemos que $e = aa^{-1} \in H$, así que $a \equiv a \pmod H$. Ahora, suponga que $a \equiv b \pmod H$, entonces $ab^{-1} \in H$. Entonces $(ab^{-1})^{-1} = ba^{-1} \in H$, por lo tanto $b \equiv a \pmod H$. Finalmente, sea $a \equiv b \pmod H$, y $b \equiv c \pmod H$. Entonces $ab^{-1}, bc^{-1} \in H$, así que $(ab^{-1})(bc^{-1}) = a(bb^{-1})c^{-1} = ac^{-1} \in H$, así que $a \equiv c \pmod H$. ■

Corolario. Las clases de equivalencia de \equiv_H sobre G son precisamente las clases laterales por la izquierda aH .

demostración. Exercise. ■

Corolario. Tenemos que $\text{ord } H = |aH|$.

demostración. Considere la mapa $f : H \rightarrow aH$ dado por la regla $h \rightarrow ah$. A todo $ah \in aH$ podemos asignarlo a h , así que f lleva H sobre aH . De igual forma, si $ah = ah'$ para $h, h' \in H$, entonces por cancelación $h = h'$. Es decir f es 1-1. ■

Corolario. La cantidad de clases laterales por la izquierda de H en G es la misma que la de las clases laterales por la derecha de H en G .

demostración. Considere la mapa $f : aH \rightarrow Ha$. ■

Definición. Sea G un grupo y $H \leq G$. Definimos el **índice** de H en G , denotado por $[G : H]$, de ser la cantidad de clases laterales de H en G .

Teorema 7 (La Teorema de Lagrange). Sea G un grupo y $H \leq G$. Entonces tenemos

$$\text{ord } G = [G : H] \text{ord } H$$

demostración. Sabemos que $G = \bigcup_{a \in H} aH$ es una unión disjunta. Como $aH \cap bH = \emptyset$ si y solo si $a \neq b$, entonces tenemos repeticiones. Ahora suponga que el conjunto de clases laterales de H en G está indexado por J . Entonces tenemos que

$$\text{ord } G = \sum_{j \in J} |a_j H| = \sum_{j \in J} \text{ord } H = |J| \text{ord } H$$

Nota que $|J| = [G : H]$. ■

Corolario. Si G y H son finitos, entonces el orden de H divide el orden de G . Mas aún, tenemos que $\frac{\text{ord } G}{\text{ord } H} = [G : H]$

Lectura 4: Grupos Cocientes

Definición. Dado un grupo G y un subgrupo H de G , definimos el **producto de clases laterales** de ser el producto $aHbH = abH$.

Definición. Sea G un grupo. Decimos que un subgrupo H de G es **normal** si para cualquier $a \in G$, $aH = Ha$. Escribimos $H \trianglelefteq G$.

Lema 8. Sea H un subgrupo normal de un grupo G . Entonces los siguientes son equivalentes para todo $a \in H$:

(1) $aHa^{-1} \subseteq H$.

(2) $aHa^{-1} = H$.

(3) Para todo $a \in G$, existe un $b \in G$ tal que $aH = Hb$.

demostración. Sí $aHa^{-1} = H$, entonces $aHa^{-1} \subseteq H$. Por el otro lado, si $aHa^{-1} \subseteq H$, entonces para $h, h' \in H$, $aha^{-1} = h'$, así que $h' \in aHa^{-1}$, así que $H \subseteq aHa^{-1}$.

Ahora, si $aHa^{-1} = H$, entonces tenemos que $aH = Ha$ para todo $a \in H$, por el otro lado, suponga que $a, b \in H$ tal que $aH = Hb$. Entonces nota que $a \in Hb$ y $a \in Ha$, así que $Ha \cap Hb \neq \emptyset$. Como Ha y Hb son clases de equivalencias, esto fuerza a $a = b$. ■

Ejemplo 11. $SL(n, \mathbb{R}) \trianglelefteq GL(n, \mathbb{R})$, nota que para cualquier $A \in SL(n, \mathbb{R})$ y $B \in GL(n, \mathbb{R})$ que $\det(BAB^{-1}) = (\det B)(1)(\det B^{-1}) = 1$.

Teorema 9. Sí G es un grupo y $H \trianglelefteq G$ es subgrupo normal de G , entonces las clases laterales de H en G forman un grupo bajo el producto de clases.

demostración. Define la operación $(aH, bH) \rightarrow aHbH = \{ahbh' : h, h' \in H\} = abH$. Ya que aH y bH son clases de equivalencia, el producto es bien definida.

Ahora sea aH y bH , como $H \trianglelefteq G$, tenemos que $aHbH = abHH = abH$, así que abH es clase lateral de H en G ; nota también que $aH(bHcH) = aH(bcH) = a(bc)H = abcH = (ab)cH = abHcH = (aHbH)cH$, así que el producto es asociativa.

Ahora toma la identidad de H , $e \in H \trianglelefteq G$ y para cada $a \in G$, toma a^{-1} . Entonces tenemos que $aHeH = aeH = eaH = eHaH = H$ y que $eH = H$. De igual forma $aHa^{-1}H = aa^{-1}H = a^{-1}aH = a^{-1}HaH = H$. Así que H es la identidad, y $a^{-1}H$ la inversa de aH . ■

Definición. Sea G un grupo. Denotamos el conjunto de todas las clases laterales de un subgrupo H en G como G/H . Sí H es un subgrupo normal, entonces G/H forma un grupo llamado el **grupo cociente** de G sobre H .

Lema 10. Sea G un grupo. Todo subgrupo de G es normal sí y solo sí H es el kernel de algún homomorfismo ϕ en G .

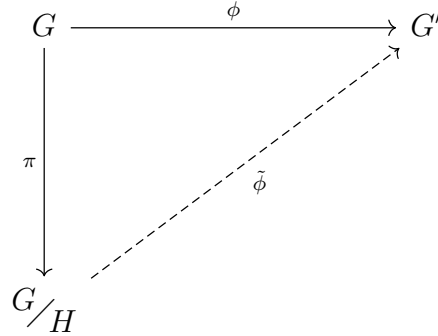
demostración. Sea $H \trianglelefteq G$. Considere la mapa $\phi : G \rightarrow G/H$ tal que $\phi : a \rightarrow aH$. Entonces $\ker \phi = \{a \in G : aH = H\}$. Así que si $a \in \ker \phi$, tenemos $aH = H$, que nos dice que $a \in H$. Por otro lado, $a \in H$ implica $aH = H$, así que $a \in \ker \phi$. Es decir $H = \ker \phi$.

Por otro lado considere $\ker \phi$ para algún mapa en G . Considere cualquier $a \in G$ y $h \in \ker \phi$. Entonces $\phi(a)\phi(h)\phi^{-1}(a) = \phi(a)e'\phi^{-1}(a) = \phi(a)\phi^{-1}(a) = e'$, donde e' es la identidad de G' . Entonces como a y h eran arbitrarios, vemos que $\phi(a)\ker \phi\phi^{-1}(a) \subseteq \ker \phi$. Así que $\ker \phi \trianglelefteq G$. ■

Lema 11. Sea G un grupo y $\phi : G \rightarrow G'$ un homomorfismo. Entonces tenemos que Si $H \trianglelefteq G$ y ϕ es sobre, entonces $\phi(H) \trianglelefteq G'$. Mas aún si $H' \trianglelefteq G'$, entonces $\phi^{-1}(H') \trianglelefteq G$.

demostración. Sea $\phi : G \rightarrow G'$ una mapa de G sobre G' . Suponga tambien que $H \trianglelefteq G$. Entonces tome $y \in G'$. Pues entonces existe un $x \in G$ tal que $y = \phi(x)$. Tambien existe un $h \in H$ con $\alpha = \phi(h)$. Entonces considere $y\alpha y^{-1} = \phi(x)\phi(h)\phi^{-1}(y) = \phi(xhx^{-1}) = \phi(h')$. Por lo tanto $y\alpha y^{-1} \in \phi(H)$ lo que hace $y\phi(H)y^{-1} \subseteq \phi(H)$. Así que $\phi(H)$ es normal en G' . Ahora considere $H' \trianglelefteq G'$, entonces para todo $a' \in G$ y $h' \in H'$, $a'h'a'^{-1} \in H$. Como ϕ es sobre, tenemos que existen $x \in G$ y $h \in H$ con $x = \phi(a')$ y $h = \phi(h')$, osea $x \in \phi^{-1}(G')$ y $h \in \phi^{-1}(H')$. Entonces $xhx^{-1} = \phi(a')\phi(h)\phi^{-1}(a') = \phi(a'h'a'^{-1}) \in \phi^{-1}(H')$. Entonces $x\phi^{-1}(H')x^{-1} \subseteq \phi^{-1}(H')$, así que $\phi^{-1}(H') \trianglelefteq G$. ■

Teorema 12 (Teorema del Factor). Suponga que G y G' son grupos y $H \trianglelefteq G$. Sea $\phi : G \rightarrow G'$ y $\pi : G \rightarrow G/H$ dado por $\pi : a \rightarrow aH$. Enotnces existe un único $\tilde{\phi} : G/H \rightarrow G'$ tal que $\phi = \tilde{\phi} \circ \pi$.



demostración. Suponga primero que existe tal $\tilde{\phi}$. Sea $\bar{\phi} : G/H \rightarrow G'$ otro homomorfismo tal que $\phi = \bar{\phi} \circ \pi$. Entonces tenemos que $\tilde{\phi} \circ \pi(a) = \bar{\phi} \circ \pi(a)$. Es decir que $\tilde{\phi}(aH) = \bar{\phi}(aH) = \phi(a)$. Esto hace que $\tilde{\phi}(G/H) = \bar{\phi}(G/H) = \phi(G)$, así que tienen el misma imagen y misma relación. Así que $\tilde{\phi} = \bar{\phi}$.

Ahora define la mapa $\tilde{\phi} : G/H \rightarrow G'$ dado por $aH \rightarrow \phi(a)$. Sea entonces $sb \in aH$, así que $aH = bH$, entonces tenemos $a^{-1}b \in H = \ker \phi$. Entonces $\phi(a^{-1}b) = e'$, la identidad de G' , entonces $\phi(a) = \phi(b)$. Pues $\tilde{\phi}$ esta bien definida. Por ultimo, note que $\tilde{\phi}(aH) = \tilde{\phi}(\pi(a)) = \tilde{\phi} \circ \pi(a)$. ■

Corolario. ϕ es sobre sí y solo si $\tilde{\phi}$ es sobre, y ϕ es 1-1 sí y solo si $\ker \phi = H$.

demostración. Nota que como $\tilde{\phi}(G/H) = \phi(G)$, entonces si $\tilde{\phi}$ es sobre, entonces ϕ tiene que ser sobre. Por el otro lado, el mismo es cierto.

Ahora si $\ker \phi = H$, como H es identidad del G/H , entonces ϕ es 1-1. Por el otro lado, si ϕ es 1-1, entonces $\ker \phi = \langle e_{G/H} \rangle$, donde $e_{G/H}$ es la identidad de G/H ; pero $e_{G/H} = H$. ■

Lectura 5: Teoremas de Isomorfismo.

Teorema 13 (Primer Teorema del Isomorfismo). *Sí $\phi : G \rightarrow H$ es un homomorfismo con kernel K , entonces*

$$\phi(G) \simeq H/K$$

demostración. Por el teorema del factor, sea $\tilde{\phi} : H/K \rightarrow H$. Entonces $\tilde{\phi}$ es un isomorfismo sí y solo sí ϕ es sobre. Nota que $\phi : G \rightarrow \phi(G)$ hace ϕ sobre. ■

Ejemplo 12. $SL(n, \mathbb{R}) \trianglelefteq GL(n, \mathbb{R})$. Considere entonces $\det : GL(n, \mathbb{R}) \rightarrow \mathbb{R}^*$, entonces $\ker \det = SL(n, \mathbb{R})$, así que por el primer teorema del isomorfismo, $\det(GL(n, \mathbb{R})) = \mathbb{R}^* \simeq GL(n, \mathbb{R})/SL(n, \mathbb{R})$.

Definición. Sea $\{G_n\}$ una colección de grupos, y $\{\phi_n\}$ una colección de homomorfismos de $G_i \rightarrow G_{i+1}$. Llamamos la secuencia $\rightarrow G_1 \xrightarrow{\phi_1} G_2 \xrightarrow{\phi_2} \dots \xrightarrow{\phi_{n-1}} G_n \xrightarrow{\phi_n} \dots$ una **secuencia exacta en un punto** G_i sí $\phi_i(G_i) = \ker \pi_{i+1}$. Llamamos la secuencia **exacta** sí es exacta en todo G_i para $i \in \mathbb{Z}^+$.

Definición. Una **secuencia exacta corta** es una secuencia exacta de la forma:

$$\langle e \rangle \xrightarrow{i} G_1 \xrightarrow{\phi_1} G_2 \xrightarrow{\phi_2} G_3 \xrightarrow{j} \langle e \rangle$$

Donde $i : \langle e \rangle \rightarrow G_1$ es la inclusión y $j : G_3 \rightarrow \langle e \rangle$ es la constante dado por $j : g \rightarrow e$ para todo $g \in G_3$.

Lema 14. *Dada una secuencia exacta corta, tenemos que ϕ_1 es 1-1 y que ϕ_2 es sobre.*

demostración. De seguro, tenemos que $i(\langle e \rangle) = \langle e \rangle = \ker \phi_1$ por definición, así que ϕ_1 es 1-1. Igualmente, tenemos que $\phi_2(G_2) = \ker j = G_3$, como j es la constante, así que ϕ_2 es sobre. ■

Lema 15. *Dada una secuencia exacta corta, $\phi_1(G_1) \trianglelefteq G_2$ y $G_2/\phi_1(G_1) \simeq G_3$.*

demostración. Como $\langle e \rangle \xrightarrow{i} G_1 \xrightarrow{\phi_1} G_2 \xrightarrow{\phi_2} G_3 \xrightarrow{j} \langle e \rangle$ es exacta corta, tenemos que $\phi_1(G_1)$ es un kernel, así que $\phi_1(G_1)$ es normal en G_2 . Mas aún, por el primer teorema del isomorfismo, como $\phi_2 : G_1 \rightarrow G_3$, lo cual tiene kernel $\phi_1(G_1)$, y como $\phi_2(G_2) = G_3$ tenemos que

$$G_2/\phi_1(G_1) \simeq G_3$$

■

Teorema 16 (Segundo Teorema del Isomorfismo). *Sí G es un grupo con $H \leq G$ un subgrupo, y $N \trianglelefteq G$ un subgrupo normal en G , entonces:*

$$HN/N \simeq H/H \cap N$$

Teorema 17 (Tercer Teorema del Isomorfismo). *Sí G es un grupo, y $H, N \trianglelefteq G$ subgrupos normales en G , con $N \leq H$, entonces*

$$(G/N)/(H/N) \simeq G/H$$

Ejemplo 13. Nota que $8\mathbb{Z} \leq 4\mathbb{Z}$, así que $4\mathbb{Z}/8\mathbb{Z} = \{8\mathbb{Z}, 4 + 8\mathbb{Z}\}$. De igual forma, $\mathbb{Z}/8\mathbb{Z} = \{8\mathbb{Z}, 1 + 8\mathbb{Z}, 2 + 8\mathbb{Z}, 3 + 8\mathbb{Z}, 4 + 8\mathbb{Z}, 5 + 8\mathbb{Z}, 6 + 8\mathbb{Z}, 7 + 8\mathbb{Z}\}$. Entonces vemos que

$$(\mathbb{Z}/8\mathbb{Z})/(4\mathbb{Z}/8\mathbb{Z}) = \{4\mathbb{Z}/8\mathbb{Z}, (1 + 8\mathbb{Z}) + 4\mathbb{Z}/8\mathbb{Z}, (2 + 8\mathbb{Z}) + 4\mathbb{Z}/8\mathbb{Z}, (3 + 8\mathbb{Z}) + 4\mathbb{Z}/8\mathbb{Z}\}$$

Nota que $(\mathbb{Z}/8\mathbb{Z})/(4\mathbb{Z}/8\mathbb{Z})$ es cíclico de 4 elementos, así que $(\mathbb{Z}/8\mathbb{Z})/(4\mathbb{Z}/8\mathbb{Z}) \simeq \mathbb{Z}/4\mathbb{Z}$, con acuerdo a la tercer teorema del isomorfismo.

Teorema 18 (Teorema de la Correspondencia). *Sea $\phi : G \rightarrow G'$ u homomorfismo de G sobre G' con kernel K . Sí $H' \leq G'$, y $\phi^{-1}(H') = H$, entonces $H \leq G$, $K \trianglelefteq H$, y $H/K \simeq H'$.*

demostración. Tenemos que $e \in H$, como $\phi(e) = e' \in H'$. Ahora sí $a, b \in H$, entonces $\phi(a), \phi(b) \in H'$, así que $\phi(ab^{-1}) \in H'$, lo que hace $ab^{-1} \in H$. Por lo tanto $H \leq G$. Tambien tenemos que $\phi(K) = \langle e' \rangle$, lo que hace $K \trianglelefteq H$.

Ahora considere la mapa $\phi' : H \rightarrow H'$ dado por $\phi' : h \rightarrow \phi(h)$. Entonces ϕ' es sobre, por definición de H , y $\ker \phi' = K$. Por lo tanto el primer teorema del isomorfismo garantiza que $H/K \simeq H'$. ■

Corolario. *Sí $H' \trianglelefteq G'$, entonces $H \trianglelefteq G$.*

demostración. Sí $H' \trianglelefteq G'$, entonces como $H = \phi^{-1}(H')$, sí $a \in G$ y $h \in H$, entonces por normalidad, $\phi(a)\phi(h)\phi^{-1}(a) = \phi(aha^{-1}) \in H'$, tenemos que $aha^{-1} \in H$. Esto hace $H \trianglelefteq G$. ■

Ejemplo 14. Sea $\phi : \mathbb{Z} \rightarrow \mathbb{Z}/24\mathbb{Z}$. Los subgrupos de $\mathbb{Z}/24\mathbb{Z}$ y \mathbb{Z} estan desplegados en los siguientes reticulos del figura 1. Nota, que en el reticulo de \mathbb{Z} , se reproduce el reticulo de $\mathbb{Z}/24\mathbb{Z}$. Así que $\mathbb{Z}/24\mathbb{Z}$ tiene subreticulo en el reticulo de \mathbb{Z} , deplegado por el figura 2.

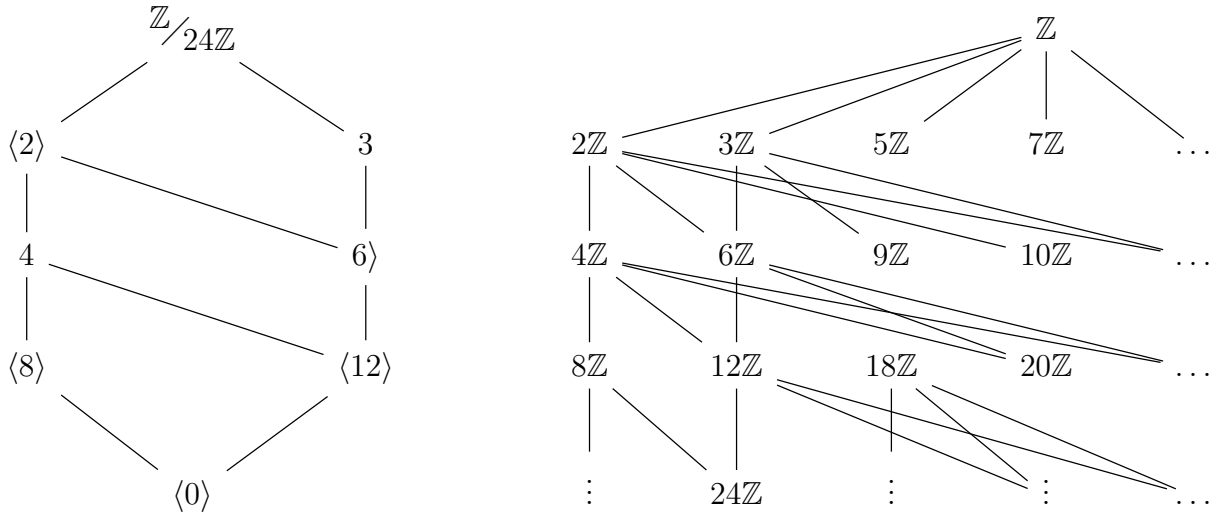


Figure 1: El reticulo de subgrupos de $\mathbb{Z}/24\mathbb{Z}$ al lado del reticulo de subgrupos de \mathbb{Z} .

Lectura 6: Sumas Directas y Productos Semidirectas.

Definición. Dado grupos G y H , definimos el **producto directo** de G y H de ser el grupo $G \times H$ bajo la operacion $((a, b), (g, h)) \rightarrow (ah, bg)$.

Lema 19. Sean G y H grupos, entonces el producto directo de G y H es un grupo bajo su operación.

Ejemplo 15. (1) El grupo Klein-4 es un producto directo, $V_4 \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

(2) $\mathbb{Z}/6\mathbb{Z} \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$.

(3) $\mathbb{Z}/70\mathbb{Z} \simeq \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/7\mathbb{Z}$.

Lema 20. Sí $G \times H$ es un producto directo, entonces $G \times H$ contine subgrupos G' y H' con $G' \simeq G$ y $H' \simeq H$.

demostración. Sea $G' = \{(g, e_H) : g \in G\}$ y $H' = \{(e_G, h) : h \in H\}$. Considere entonces las proyecciones del primer y segundo partes, $\pi_1 : G \times H \rightarrow G$ y $\pi_2 : G \times H \rightarrow H$ dados por $\pi_1 : (g, e_H) \rightarrow g$ y $\pi_2 : (e_G, h) \rightarrow h$. Entonces π_1 y π_2 son isomorfismos. ■

Corolario. G' y H' son normales en $G \times H$.

Corolario. $G'H' = G \times H$ y $G' \cap H' = \langle e \rangle$, donde $e = (e_G, e_H)$ es la identidad de $G \times H$.

Definición. Decimos que G es un **producto directo interior** sí existen subgrupos G' y H' tales que:

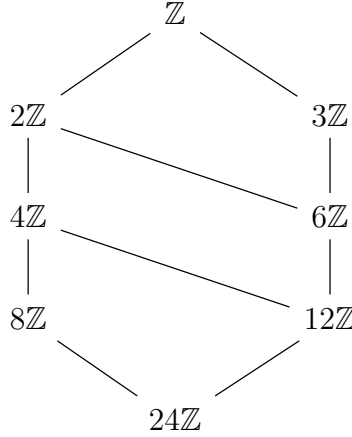


Figure 2: $\mathbb{Z}/24\mathbb{Z}$ como subreticulo del reticulo de \mathbb{Z} .

- (1) G' y H' son normales en G .
- (2) $G' \cap H' = \langle e \rangle$.
- (3) $G'H' = G$.

Teorema 21. *Sí $G = HK$ es un grupo donde $H, K \leq G$, entonces $G \simeq H \times K$.*

demostración. Defina $\phi : H \times K \rightarrow HK$ pro $(h, k) \rightarrow hk$. Nota que $h \in H$ y $k \in K$ implica que $hk = kh$. Sí $(h^{-1}k^{-1}h)K \in K$ y $h^{-1}(k^{-1}hk) \in H$, entonces $h^{-1}k^{-1}hk \in H \cap K = \langle e \rangle$. Nota que sí (h_1, k_1) y $(h_2, k_2) \in H \times K$, entonces $\phi((h_1, k_1), (h_2, k_2)) = (h_1h_2, k_1k_2) = h_1h_2k_1k_2 = h_1k_1h_2k_2 = \phi(h_1, k_1)\phi(h_2, k_2)$. Entonces ϕ es un homomorfismo

Ahora suponga que $\phi(h, k) = e$. Entonces $hk = e$, así loq que dice que $h \in K$ y $k \in H$, entonces $h = k = e$. Por lo tanto $\ker \phi = \langle e \rangle$. Mas aún, ϕ es sobre por definición, así que $HK \simeq H \times K$. ■

Definición. Sí G es un grupo que contiene subgrupos normales $\{H_i\}_{i=1}^n$, y $g \in G$ se puede escribir unicamente como $g = h_1 \dots h_n$, donde h_i , entonces se llama G el **producto directo interno** de $\{H_i\}$.

Lema 22. *Suponga que $H = H_1 \dots H_n$ donde $H_i \trianglelefteq G$ para toda $1 \leq i \leq n$. Los siguientes enunicados son equivalente:*

- (1) G es producto directo interno de $\{H_i\}$.
- (2) $(H_1 \dots H_{i-1}) \cap H_i = \langle e \rangle$ para todo $1 \leq i \leq n$.

demostración. Supong que G es producto directo interno de $\{H_i\}$. Entonces, para todo $g \in G$, $g = h_1 \dots h_n$. Sea que $g \in (H_1 \dots H_{i-1}) \cap$

H_i . Entonces $g \in H_1 \dots H_{i-1}$, entonces $g = h_1 \dots h_{i-1} e_{i-1} e_i e_{i+1} \dots e_n$. Ahora tambien tenemos que $g \in H_i$, así que $g = e_1 \dots e_{i-1} g e_{i+1} \dots e_n$. Como g es de representacion unica, $h_1 \dots h_{i-1} e_i \dots e_n = e_1 e_2 \dots g e_{i+1} \dots e_n$. Por correspondencia, tenemos que $g = e$. Por lo tanto $(H_1 \dots H_{i-1}) \cap H_i = \langle e \rangle$.

Suponga ahora que $(H_1 \dots H_{i-1}) \cap H_i = \langle e \rangle$. Suponga que $g = h_1 \dots h_{i-1} \in (H_1 \dots H_{i-1})$ y $g = k_1 \dots k_n \in H_i$. Como $H_i \trianglelefteq G$, tenemos que $h_i k_i = k_i h_i$. Por lo tanto, como $h_1 \dots h_n = k_1 \dots k_n$. Entonces tenemos $h_2 \dots h_n = (h_1^{-1} k_1) k_2 \dots k_n$, y que $h_3 \dots h_n = (h_1^{-1} k_1) (h_2^{-1} k_2) k_3 \dots k_n$. Procediendo recursivamente, tenemos que $(h_1^{-1} k_1) \dots (h_{n-1}^{-1} k_{n-1}) = h_n k_n^{-1}$, y como $h_n k_n^{-1} \in H_n \cap (H_1 \dots H_{n-1})$, tenemos que $h_i^{-1} k_i = e$ para todo i . Por lo tanto $h_i = k_i$ y g tiene representación unica. Como $G = H_1 \dots H_n$, esto hace G el producto directo interno de $\{H_i\}$. ■

Ejemplo 16. $D_3 = \langle r \rangle \langle t \rangle$ y es una representacion unica, pero $\text{ord } \langle r \rangle = 3$ y $\text{ord } \langle t \rangle = 2$, pero D_3 no es abeliano, así que D_3 no puede ser el producto directo interno de $\langle r \rangle$ y $\langle t \rangle$.

Definición. Sea G un grupo, definimos a $\text{Aut } G$ el **grupo de automorfismos** de G sobre si mismo.

Lema 23. Sean H, K grupos, y sea $r : K \rightarrow \text{Aut } H$ dado por $k \xrightarrow{r} r_k$ y $r_k : H \rightarrow H$ es un autmorfismo de H . Considere la operacion bianria $(H \times K) \times (H \times K) \rightarrow H \times K$ dado por $(h_1, k_1), (h_2, k_2) \rightarrow (h_1 r_k(h_2), k_1 k_2)$. Esta operación induce un grupo sobre $H \times K$.

demostración. Como r_k es un automorfismo de H , es un homomorfismo, así que tenemos que $r(kn) = r_{kn} = r_k r_n = r(k) r(n)$, así que r es un homorfismo, y se cierra la operación en $H \times K$.

Ahora nota que $(h, k)(e_H, e_K) = (h r_k(e_H), k e_K) = (h e_H, k e_K) = (h, k)$ y $(e_H, e_K)(h, k) = (e_H r_{e_K}(h), e_K k) = (e_H h, e_K k) = (h, k)$, como r_{e_H} es la identidad. Así que $e = (e_H, e_K)$ es la identidad.

De igual manera, tenemos $(h, k)(r_k^{-1}(h^{-1}), k^{-1}) = (h r_k(r_k^{-1}(h^{-1})), k k^{-1}) = (h h^{-1}, k k^{-1}) = e$, y $(r_k^{-1}(h^{-1}), k^{-1})(h, k) = (r_k^{-1}(h^{-1}) r_h(h), k^{-1} k) = (r_{e_H}(h^{-1}), k^{-1} k) = (h^{-1} h, k^{-1} k) = e$, con $r_k^{-1} r_k = r_{e_H}$, la identidad. Así que $H \times K$ tiene inversos.

Finalmente, nota que

$$\begin{aligned}
((h_1, k_1)(h_2, k_2))(h_3, k_3) &= (h_1 r_{k_1}(h_2), k_1 k_2)(h_3, k_3) \\
&= ((h_1 r_{k_1}(h_2)) r_{k_3}(h_3), k_1 k_2 k_3) \\
&= (h_1 h_2 r_{k_1 k_3}(h_3), k_1 k_2 k_3)
\end{aligned}$$

$$\begin{aligned}
(h_1, k_1)((h_2, k_2)(h_3, k_3)) &= (h_1, k_1)(h_2 r_{k_3}(h_3), k_2 k_3) \\
&= (h_1 h_2 r_{k_1 k_3}(h_3), k_1 k_2 k_3)
\end{aligned}$$

y asociatividad se preserva. ■

Definición. Sea H, K grupos, y $r : K \rightarrow \text{Aut } H$ un homomorfismo. Definimos el **producto semidirecto externo** de ser el grupo $H \times_r K$ bajo la operación $(h_1, k_1)(h_2, k_2) = (h_1 r_{k_1}(h_2), k_1 k_2)$.

Ejemplo 17. (1) $D_3 \simeq \langle r \rangle \times_r \langle t \rangle \simeq \mathbb{Z}/3\mathbb{Z} \times_r \mathbb{Z}/2\mathbb{Z}$, donde $r : x \rightarrow -x$. En ambos grupos.

(2) Sea $G = H \times_r K$. Sea $H' = \{(h, e_K), h \in H\}$ y $K' = \{(e_H, k) : k \in K\}$. Nota que $H' \simeq H$, que $K' \simeq K$, y que $H' \trianglelefteq H \times_r K$, pero no necesariamente $K' \trianglelefteq H \times_r K$. Tambien tenemos que $H' \cap K' = \langle e \rangle$. Ahora, $(h, e_K)(e_H, k) = (h r_{e_H}(e_H), e_K k) = (h e_H, e_K k) = (h, k)$, así que $H \times_r K = H' K'$.

Definición. Sea G un grupo, y $H \trianglelefteq G$ y $K \leq G$. Decimos que G es el **producto semidirecto interno** sí $G = HK$ y $H \cap K = \langle e \rangle$. Lo denotamos como $G = H \rtimes K$.

Ejemplo 18. $D_n \simeq \mathbb{Z}/n\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z} \simeq \langle r \rangle \rtimes \langle t \rangle$. Nota que $\langle r \rangle \trianglelefteq D_n$ y que $[D_n, \langle r \rangle] = 2$.

Lema 24. Suponga que G es un grupo semidirecto interno de $H \trianglelefteq G$, y $K \leq G$. Entonces $G \simeq H \times_r K$, donde $r : K \rightarrow \text{Aut } H$ esta dado por $r_k : h \rightarrow khk^{-1}$.

demostración. Note que r_k es un automorfismo de H , como $H \trianglelefteq G$ así que r esta bien definida. Por la lemma 22, todo $g \in G$ se escribe unicamenet como hk . Por lo tanto, sea $\phi : H \times_r K \rightarrow G$ dado por $(h, k) \rightarrow hk$. Vemos que ϕ es 1-1, y que es sobre.

Ahora dado (h, k) y (h', k') , tenemos que $\phi((h, k)(h', k')) = \phi(h r_k(h'), k k') = \phi(h k h k^{-1}, k k') = (h k h' k^{-1})(k k') = (h k)(h' k') = \phi(h, k)\phi(h', k')$. Por lo tanto ϕ es un isomorfismo y terminamos. ■

Lema 25. Sea G un grupo y $H, K \leq G$. Suponga que $G = HK$, y que $H \cap K = \langle e \rangle$. Entonces para todo $g \in G$, se puede escribir de manera unica de la forma $g = hk$ donde $h \in H$ y $k \in K$.

Lectura 7: Acciones de Grupos.

Teorema 26 (EL Teorema de Cayley). Todo grupo es isomorfo a un subgrupo del grupo de simetrico.

demostración. Sea G un grupo y $A(G)$ el grupo simetrico de G . Definia $\lambda : G \rightarrow A(G)$ dado por $g \rightarrow \lambda_g$, donde $\lambda_g : G \rightarrow G$ esta dado por $x \rightarrow gx$. Note que λ_g es un permutacion de los elementos de G , es sobre, y es 1-1 por cancelacion, así que $\lambda_g \in A(G)$. Así que λ es bien definido.

Ahora suponga que $\lambda(g) = \lambda(h)$, entonces para algún $x \in G$, $\lambda_g(x) = \lambda_h(x)$, pues $gx = hx$. Por cancelación, tenemos que $g = h$. sí que λ es 1-1. Ahora dado $x \in G$, que $(gh)(x) = \lambda_{gh}(x) = (gh)x = g(hx) = g(\lambda_h(x)) = \lambda_g(\lambda_h(x)) = \lambda_g \lambda_h(x)$. Así que λ definia una isomorfismo de G hacía $\lambda(G)$ lo cual es subgrupo de $A(G)$. ■

Ejemplo 19. Por la teorema de Cayley, tenemos que $D_3 \simeq S_6$.

Definición. Un grupo G **actua** sobre un conjunto X sí para todo $g \in G$, existe una mapa $G \times X \rightarrow X$ dado por $(g, x) \rightarrow g \cdot x$ tal que:

- (1) $h \cdot (g \cdot x) = (hg) \cdot x$.
- (2) $e \cdot x = x$ para todo $x \in X$.

Ejemplo 20. (1) Todo grupo actua sobre si mismo bajo multiplicacion pr la izquierda. Llamamos esto el **accion regular**.

- (2) Todo grupo actua sobre si mismo via la accion de **conjugacion** definido pro $(g, x) \rightarrow gxg^{-1}$. Nota que $h \cdot (g \cdot x) = h \cdot (gxg^{-1}) = hgxg^{-1}h^{-1} = (hg)x(hg)^{-1} = (hg) \cdot x$. Tambein $e \cdot x = exe^{-1} = x$.

Definición. Definimos el **kernel** de una accion $G \times X \rightarrow X$ de ser el conjunto $= \{g \in G : g \cdot x = x\}$.

Ejemplo 21. (1) Sí G actua sobre si mismo via conjugacion, entonces si $gxg^{-1} = x$, tenemos que $gx = xg$ para todo $x \in G$. Por lo tanto $\ker = \{g \in G : gx = xg \text{ para todo } x \in G\}$. Llamamos este kernel el **centro** de G , y lo denotamos como $Z(G)$.

- (2) Considere \mathcal{B}_n el conjunto de todas funciones booleanas $f : \mathbb{F}_2^n \rightarrow \mathbb{F}_2^n$ en n variables. Defina una operacion de S_n sobre \mathcal{B}_n definida por $s \cdot f(x_1, \dots, x_n) = f(x_{s(1)}, \dots, x_{s(n)})$. Este operaci3n defina una acci3n de grupos de S_n sobre \mathcal{B}_n . Nota que el kernel de este acci3n es trivial.

Definici3n. Sea G un grupo que actua sobre un conjunto X . La **3rbita** de un $x \in X$ es el conjunto $\mathcal{O}(x) = \{g \cdot x : g \in G\}$.

Ejemplo 22. (1) Sea G un grupo actuando sobre si mismo por su multiplicaci3n (por izquierda). Suponga que $x \in G$ y sea $g \in G$ un elemento cualquiera. Entonces existe un $g_0 \in G$ tal que $g = g_0 x$. Esto hace $G \subseteq \mathcal{O}(x)$. Por lo tanto $\mathcal{O}(x) = G$.

- (2) Considere un grupo G actuando sobre si mismo mediante conjugaci3n. Sea $x \in G$. Entonces $\mathcal{O}(x) = \{gxg^{-1} : g \in G\} = \text{cl } x$. Llamamos a $\text{cl } x$ la **clase de conjugaci3n** de x .

- (3) Considere \mathcal{B}_3 y defina $f(x_1, x_2, x_3) = x_1 + x_2 x_3 + x_1 x_2 x_3$. Sea $S_3 = \{(1), (2\ 3), (1\ 2), (1\ 2\ 3), (1\ 3\ 2), (1\ 3)\}$. Entonces:

$$\begin{aligned} (1) \cdot f &= x_1 + x_2 x_3 + x_1 x_2 x_3 = f \\ (2\ 3) \cdot f &= x_1 + x_3 x_2 + x_1 x_3 x_2 = f \\ (1\ 2) \cdot f &= x_2 + x_1 x_3 + x_2 x_1 x_3 = f_1 \\ (1\ 2\ 3) \cdot f &= x_2 + x_3 x_1 + x_3 x_2 x_1 = f_1 \\ (1\ 3\ 2) \cdot f &= x_3 + x_1 x_2 + x_3 x_1 x_2 = f_2 \\ (1\ 3) \cdot f &= x_3 + x_2 x_1 + x_3 x_2 x_1 = f_2 \end{aligned}$$

As3 que $\mathcal{O}(f) = \{f, f_1, f_2\}$. Nota que $|\mathcal{O}(f)|$ divide a $\text{ord } S_3$.

Lema 27. Sea G un grupo que actua sobre un conjunto X . Entonces las 3rbitas de X particionan a X .

demostraci3n. Sea $x \in \mathcal{O}(y)$ y $x \in \mathcal{O}(z)$ para $x, y, z \in X$. Entonces vemos que $x = gy$ y $x = hz$, por lo tanto $gy = hz$. Es decir $y = (g^{-1}h)z$, por lo tanto $y \in \mathcal{O}(z)$. De igual forma, $z \in \mathcal{O}(y)$. Esto hace que $\mathcal{O}(y) = \mathcal{O}(y)$. ■

Definici3n. Sea G un grupo actuando sobre un conjunto X . El **estabilizador** de $x \in X$ es el conjunto $\text{stab } x = \{g \in G : g \cdot x = x\}$.

Lema 28. Sea G un grupo que actua sobre un conjunto X . Entonces el estabilizador de todo $x \in X$ es subgrupo de G .

demostración. Sea $x \in X$ y sea $g, h \in \text{stab } x$. Entonces $x = gx$ y $x = h^{-1}x$. Por lo tanto $(gh^{-1}) \cdot x = x$. ■

Ejemplo 23. Para cualquier grupo actuando sobre si mismo bajo conjugacion, $\text{stab } x = \{g : gx = xg\} = C(x)$ que se llama el **centralizador** de x .

Teorema 29 (Teorema del Órbita-Estabilizador.). Suponga que G es un grupo que actua sobre un conjunto X . Sean $\mathcal{O}(x)$ y $\text{stab } x$ la órbita y estabilizador de un $x \in X$. Entonces:

$$|\mathcal{O}(x)| = [G : \text{stab } x]$$

demostración. Suponga que $y \in \mathcal{O}(x)$. Entonces $y = g \cdot x$ para algún $g \in G$. Defina ahora la mapa $f : \mathcal{O}(x) \rightarrow G/\text{stab } x$ dado por $y = g \cdot x \rightarrow g \text{stab } x$. Sea ahora $y = g \cdot x = h \cdot x$. Entonces vemos que $x = (g^{-1}h) \cdot x$, así que $g^{-1}h \in \text{stab } x$. Esto hace que $g \text{stab } x = h \text{stab } x$. Por lo tanto f es bien definida.

Ahora, vemos que f es sobre; sí $y \in \mathcal{O}(x)$, entonces $y = g \cdot x$ para algún $g \in G$, así que a cada $y \in \mathcal{O}(x)$ está asignada a un $g \text{stab } x$. Más aun, f es 1-1. Sean $y = gx$ y $y' = hx$. Sí $g \text{stab } x = h \text{stab } x$, entonces $g^{-1}h \in \text{stab } x$, así que $gx = hx$, es decir $y = y'$. Por lo tanto, tenemos una mapa 1-1 de $\mathcal{O}(x)$ sobre el conjunto $G/\text{stab } x$, que tiene cardinalidad $[G : \text{stab } x]$. ■

Corolario. Sí G es un grupo finito, entonces $|\mathcal{O}(x)|$ divide a $\text{ord } G$. En particular

$$|\mathcal{O}(x)| = \frac{\text{ord } G}{\text{ord } (\text{stab } x)}$$

Ejemplo 24. Sea G un grupo finito y sea la accion de G sobre si mismo la conjugacion. Entonces $\mathcal{O}(x) = \text{cl } x$. Nota que $x \in \text{cl } x$. Suponga que $|\text{cl } x| = 1$, entonces $gxg^{-1} = x$ así que $gx = xg$ lo que hace $x \in Z(G)$. Nota igualmente que $G = \bigcup \text{cl } x$. Entonces

$$\text{ord } G = \sum \text{cl } x = \text{ord } Z(G) + \sum [G : C(x)] = \text{ord } Z(G) + \sum \text{cl } x$$

Llamamos a esta equacion la **ecuacion de clase**.

Teorema 30 (Conteo de Órbitas). Sea G un grupo finito que actua sobre un conjunto finitio X . Denota $X^g = \{x \in X : g \cdot x = x\}$. Sea \mathcal{O} la colleccion de todas las orbitas de $x \in X$. Entonces:

$$|\mathcal{O}| = \frac{1}{\text{ord } G} \sum |X^g|$$

demostración. Sabemos que $X^g = \{(g, x) \in G \times X : g \cdot x = x\}$. Sea:

$$\begin{array}{ccccccc} (g_1, x_1) & & (g_1, x_3) & & (g_1, x_4) & & \\ & (g_2, x_2) & & (g_2, x_3) & & & (g_2, x_5) \\ (g_3, x_1) & & (g_3, x_3) & & (g_3, x_4) & & \dots \\ \vdots & & & & & & \end{array}$$

Nota que las columnas de este arreglo forman los estabilizadores de los x_i , ahora vemos que

$$\sum |X^g| = \sum \text{stab } x = \sum \frac{\text{ord } G}{|\mathcal{O}(x)|}$$

Por el teorema del órbiata estabilizador, tenemos que

$$\text{ord } G \sum \frac{1}{|\mathcal{O}(x)|} = \text{ord } G \sum_{\mathcal{O}(x) \in \mathcal{O}} \sum_x |\mathcal{O}(x)| = \text{ord } G |\mathcal{O}|$$

Rearreglando los terminos, tenemos el resultado. ■

Lectura 8: Las Teoremas de Sylow

Definición. Sea $p \in \mathbb{Z}^+$ un primo. Llamamos a un grupo G un **p -grupo** sí cada $g \in G$ es una potencia de p .

Ejemplo 25. (1) El grupo Klein $V_4 = \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ es un 2-grupo.

(2) Los grupos $\mathbb{Z}/14\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ y D_{16} son 2-grupos.

(3) El grupo $\bigoplus_{n=1}^{\infty} \mathbb{Z}/5^n\mathbb{Z}$ es un 5-grupo, pero $\prod_{n=1}^{\infty} \mathbb{Z}/5^n\mathbb{Z}$ solo es un 5-grupo cuando $n = 1$.

Definición. Sí G es un grupo con orden $p^r m$ donde p es primo y $p \nmid m$, entonces llamamos un subgrupo $P \leq G$ un **p -subgrupo de Sylow**, o un **p -Sylow** sí $\text{ord } P = p^r$.

Lema 31. Sí G es un grupo de orden $p^r m$ con p primo, y $p \nmid m$ y $P \leq G$ es un p -Sylow de G , entonces P es de orden lo máximo posible.

demostración. Por el teorema de Lagrange. ■

Ejemplo 26. $|D_6| = 2^2 \cdot 3$. Nota que $P_1 = \{e, r^3, tr^3t\}$, $P_2 = \{e, r^3, rt, r^4t\}$, y $P_3 = \{e, r^3, r^2t, r^5t\}$ son 2-Sylows de D_6 y $P = \{e, r, r^4\}$ es 3-Sylow.

Lema 32. *Sí $n = p^r m$ con p primo y $p \nmid m$, entonces*

$$\binom{n}{p^r} \equiv m \pmod{p}$$

demostración. Nota que $(x+1)^{p^r} = \sum_{k=1}^{p^r} \binom{p^r}{k} x^{p^r-k} \equiv x^{p^r m} + 1 \pmod{p}$. Entonces $(x+1)^{p^r m} \equiv (x^{p^r} + 1)^m \pmod{p}$, así que

$$\sum \binom{p^r m}{k} x^{p^r m - k} \equiv \sum \binom{m}{k} (x^{p^r})^{m-k} \pmod{p}$$

Mirando el coeficiente de x^{p^r} , en la izquierda, tenemos que este término ocurre cuando $k = p^r(m-1)$, y obtenemos $\binom{p^r m}{p^r} = \binom{n}{p^r}$. Por el lado derecho, el término x^{p^r} ocurre cuando $k = m-1$ y por simetría obtenemos $\binom{m}{1} = m$. ■

Teorema 33 (El Primer Teorema de Sylow). *Sea G un grupo finito de orden $p^r m$ donde p es primo, y $p \nmid m$. Entonces existe al menos un p -subgrupo de Sylow, de G .*

demostración. Sea $X = \binom{G}{p^r}$. Note que G actúa sobre X vía la multiplicación por la izquierda. Ahora, esta acción induce en X una partición de X en órbitas. Es decir

$$\binom{G}{p^r} = \bigcup \mathcal{O}(S)$$

entonces $p \nmid \sum |\mathcal{O}(S)|$. Por lo tanto, existe un $S \in X$ con $p \nmid |\mathcal{O}(S)|$. Sea $P = \text{stab } S$. Entonces por el teorema del órbita-estabilizador, tenemos

$$|\mathcal{O}(S)| = \frac{\text{ord } G}{\text{ord } P} = \frac{p^r m}{\text{ord } P}$$

Como $p \nmid |\mathcal{O}(S)|$, $\text{ord } P$ tiene que ser un múltiplo de p^r , es decir que $p^r \mid \text{ord } P$, por lo tanto $p^r \leq \text{ord } P$.

Por otro lado, defina la mapa $\lambda_x : P \rightarrow S$, para $x \in S$ dado por $\lambda_x : g \rightarrow \lambda_x(g) = g \cdot x$. Vemos que esta mapa es bien definida, y que es 1-1. Por lo tanto $\text{ord } P \leq |S| = p^r$. Por lo tanto P es un p -subgrupo de Sylow. ■

Ejemplo 27. Sea $GL(n, \mathbb{F}_p)$, y escoja una matriz $A \in GL(n, \mathbb{F}_p)$. Note que para la fila k de A , hay $p^n - p^k$ posibles entradas, así que $\text{ord } GL(n, \mathbb{F}_p) = p^n - p^k = p^{\frac{n(n-1)}{2}} p^j - 1$. Entonces cualquier p -Sylow de $GL(n, \mathbb{F}_p)$ tiene orden $p^{\frac{n(n-1)}{2}}$.

Teorema 34 (El Teorema de Cauchy). *Sí p es un primo y $p \mid \text{ord } G$, entonces G tiene un elemento de orden p .*

demostración. Sea P un p -Sylow de G y escoja $g \in P$ tal que $g \neq e$. Entonces $\text{ord } g = p^l$ para $l \in \mathbb{Z}^+$. Sí $l = 1$, terminamos, y sí $l > 1$, note que $(g^{p^{l-1}})^p = g^{p^l} = e$. ■

Lema 35. Sean H y K subgrupos de un grupo G . Entonces:

$$\text{ord } HK = \frac{\text{ord } H \text{ ord } K}{|H \cap K|}$$

demostración. Considere la mapa $f : H \times K \rightarrow HK$ dado por $(h, k) \rightarrow hk$. Entonces f es sobre y $\text{ord } HK \leq |H \times K|$. Sea entonces h_1k_1, \dots, h_dk_d los elementos distintos de HK . entoncece $H \times K = \bigcup f^{-1}(h_ik_i)$, para todo $1 \leq i \leq d$. Ahora, $f^{-1}(hk) = \{(hk, g^{-1}k) : g \in H \cap K\}$. Entonces $|f^{-1}(hk)| = |H \cap K|$. Entonces tenemos que $|H \times K| = \text{ord } H \text{ ord } K |H \cap K| = \text{ord } HK |H \cap K|$. ■

Teorema 36 (El Segundo Teorema de Sylow). Sea G un grupo finito con orden $p^r m$ donde p es primo y $p \nmid m$. Sea $n_p(G)$ el numero de todos los p -subgrupos de Sylow de G , entonces:

$$n_p(G) \equiv 1 \pmod{p}$$

demostración. Considere $X = \{P \leq G : P \text{ es } p\text{-Sylow}\}$. Por el primer teorema de Sylow, $X \neq \emptyset$. Entonces $|X| = n_p(G)$. Sea que $P \in X$ actua sobre X mediante conjugacion. Sea Q un p -Sylow de G , entonces por el teorema órbita-estabilizador, tenemos que

$$|\mathcal{O}(Q)| = \frac{p^r}{\text{ord } \text{stab } Q} \in \mathbb{Z}^+$$

así que $|\mathcal{O}(Q)| \mid p^r$. Asíque $\mathcal{O}(Q)$ tiene largo 1, o tiene largo p . Ahora, como

$$|X| = \sum |\mathcal{O}(Q)| = \sum |\mathcal{O}(Q')| + \sum |\mathcal{O}(Q'')|$$

donde Q' y Q'' son subgrupos cuyas orbitas tiene 1 o 2 elementos, respectivamente, tenemos que $p \mid \sum |\mathcal{O}(Q'')|$, por lo tanto

$$|X| \equiv |\mathcal{O}''| \pmod{p}$$

donde \mathcal{O}'' es la coleccion de todas las orbitas de largo 1.

Ahora, nota que $\mathcal{O}(P) = \{P\}$. Suponga entonces que existe un p -Sylow Q tal que $g \cdot Q = gQg^{-1} = Q$ para todo $g \in P$. Entonces, $gQ = Qg$, así que $PQ = QP$ y $PQ \leq G$. Entonces por el lema de arriba, tenemos que

$$\text{ord } PQ = \frac{\text{ord } P \text{ ord } Q}{|P \cap Q|}$$

Pero $p^r \leq \text{ord } PQ \leq p^r$, por lo tanto $Q \subseteq P$. Como P y Q tienen el mismo orden, tenemos que $P = Q$, así que $|\mathcal{O}''| = 1$ ■

Teorema 37 (El Tercer Teorema de Sylow). *Sea G un grupo finito con orden $p^r m$, donde p es primo y $p \nmid m$. Entonces todos los p -subgrupos de Sylow son conjugados.*

demostración. Sea P un p -Sylow de G y R un p -subgrupo de G . Deje que R actúa sobre G/P (no necesariamente el grupo cociente) mediante multiplicación. Por el teorema de Lagrange, tenemos que $\text{ord } G/P = [G : P] = \frac{p^r m}{p^r} = m$. También nota que $G/P = \bigcup \mathcal{O}(gP)$, así que

$$\sum |\mathcal{O}(gP)| = m$$

y existe una órbita cuya longitud no está dividida por p , como $p \nmid m$. Por el teorema del órbita-estabilizador, tenemos que $|\mathcal{O}(gP)| \mid \text{ord } R = p^l$, para $l \in \mathbb{Z}^+$. Así que $\mathcal{O}(gP)$ tiene largo 1, o p^l . Ahora, sea $gP \in G/P$, un elemento cuya órbita tiene largo 1. Entonces $g \cdot gP = (hg)P = gP$, para todo $h \in R$, lo que dice que $g^{-1}hg \in P$, por lo tanto $h \in gPg^{-1}$ lo que hace $R \subseteq gPg^{-1}$. El resultado entonces se obtiene escogiendo a R un p -Sylow. ■

Corolario. *Todo p -subgrupo de G está contenido en un p -subgrupo de Sylow. Además, tenemos que $n_p(G) \mid m$*

Lectura 9: Grupos Simples

Definición. Un grupo $G \neq \langle e \rangle$ es **simple** si sus únicos subgrupos normales son el mismo y $\langle e \rangle$.

Ejemplo 28. (1) $\mathbb{Z}/5\mathbb{Z}$ tiene como subgrupos $\langle 0 \rangle$ y $\mathbb{Z}/5\mathbb{Z}$. Entonces $\mathbb{Z}/5\mathbb{Z}$ es simple.

(2) El grupo dihedral D_n no es normal porque tiene $\langle r \rangle$ como subgrupo simple; pues $[D_n : \langle r \rangle] = 2$.

Lema 38. *Sí P es un p -grupo finito no trivial, entonces $Z(P)$ no es trivial.*

demostración. Deje que P actúe sobre sí mismo vía conjugación. Las órbitas de esta acción son las clases de conjugación $\text{cl } g$, donde $g \in P$. Tenemos que $x \in P$ está en una clase de tamaño 1 si y solo si $x \in Z(P)$. Por el teorema del órbita-estabilizador, tenemos que el tamaño de los $\text{cl } g$ divide a $\text{ord } P = p^r$, donde $p, r \in \mathbb{Z}^+$ y p es primo.

Ahora, si $Z(P) = \langle e \rangle$, entonces hay una sola órbita de tamaño 1. Entonces los demás $\text{ord } \text{cl } x \mid \text{ord } P$. Esto es una contradicción de que P es un p -grupo. ■

Corolario. *Sí P es un p -grupo no isomorfo a $\mathbb{Z}/p\mathbb{Z}$, para p primo, entonces P no es simple.*

demostración. Nota que $Z(P) \trianglelefteq P$. ■

Lema 39. *El subgrupo P de un grupo G es un p -Sylow normal de G si y solo si es el único p -Sylow de G .*

Lema 40. *Sea G un grupo finito noabeliano y simple. Si $p \mid \text{ord } G$, para p primo, entonces $n_p(G) > 1$.*

demostración. Si p es unico, entonces $\text{ord } G = p^r$ y G es un p -grupo no trivial. Entonces $Z(G)$ tambien no es trivial. Como $Z(G) \trianglelefteq G$ y G es simple entonces $Z(G) = G$, lo cual no puede pasar.

Ahora, si P es un p -Sylow de G , entonces $\langle e \rangle \leq P \leq G$, donde la segundo inclusión es estricta. Si $n_p(G) = 1$, entonces $P \trianglelefteq G$, lo cual no puede pasar. Por lo tanto $n_p(G) > 1$. ■

Lema 41. *Sea G un grupo de orden pq , donde p y q son primos distintos. Entonces:*

- (1) *Si $q \not\equiv 1 \pmod{p}$, entonces G tiene un p -Sylow normal.*
- (2) *Si $q \not\equiv 1 \pmod{p}$, y $p \not\equiv 1 \pmod{q}$, entonces G es ciclico.*
- (3) *G no es simple.*

demostración. Note que $n_p(G) \equiv 1 \pmod{p}$ y $n_p(G) \mid q$ por el tercer teorema de Sylow. Entonces o $n_p(G) = 1$, o $n_p(G) = q$. Como $q \not\equiv 1 \pmod{p}$, tenemos que $n_p(G) = 1$ y G tiene un unico p -Sylow, y es normal.

Ahora, suponga que $q \not\equiv 1 \pmod{p}$ y $p \not\equiv 1 \pmod{q}$. Tenemos que G tiene un p -Sylow unico P , y un q -Sylow unico Q . Mas aún P y Q son ciclicos. Existen $x \in P$ y $y \in Q$ con $P = \langle x \rangle$ y $Q = \langle y \rangle$. Por supuesto $\text{ord } P = p$ y $\text{ord } Q = q$. Ahora, como $P, Q \trianglelefteq G$ y $P \cap Q = \langle e \rangle$ entonces tenemos que $xy = yx$; entonces $(xy)^n = x^n y^n$. Por lo tanto $(xy)^{pq} = e$. Esto hace G ciclico.

Por ultimo, sin perder la generalidad, asume que $p > q$. Por lo tanto, tenemos que $p \nmid q - 1$ y $q \not\equiv 1 \pmod{p}$. Por arriba, G tiene un unico p -Sylow normal, lo que hace que G no sea simple. ■

Lema 42. *Sea G un grupo con noabeliano orden p^2q con p y q primos distintos. Entonces G contiene un p -Sylow normal o un q -Sylow normal.*

demostración. Supong lo contrario. Sea $n_p(G) > 1$ y $n_q(G) > 1$. Note que un q -Sylow tiene orden q , y por lo tanto es ciclico. Entonces tenemos $q - 1$ elementos de orden q . Entonce cualquier y del q -Sylow genera un unico q -Sylow. Por lo tanto $q = n_q(q - 1)$. Ahora, $n_q(G) \mid p^2$ así que o $n_q(G) = p$ o $n_q(G) = p^2$. Si $n_q(G) = p^2$, entonces el unmero de elementos de orden

diferente a q es $p^2q - p^2(q-1) = p^2$ lo que dice que hay un p -Sylow unico. Por lo tanto, G no es simple.

Por otro lado, sí $n_q(G) = p$, entonces $n_q(G) \equiv 1 \pmod{q}$ y $p \equiv 1 \pmod{q}$, lo que dice $p > q$. Pero $n_p(G) \equiv 1 \pmod{p}$ y como q es primo, entonces $n_p(G) = q$, luego, $n_p(G) \equiv 1 \pmod{p}$ implica que $q \equiv 1 \pmod{p}$ lo que dice que $q > p$. Una contradiccion. ■

Corolario. G no es simple.

Ejemplo 29. (1) Por los resultados arriba, el primer grupo noabeliano simple es el grupo A_5 de orden $60 = 2^2 \cdot 3 \cdot 5$.

(2) Suponga que G es u grupo de orden $2552 = 2^3 \cdot 11 \cdot 29$. Suponiendo que G es simple, entonces $n_{11} > 1$ y $n_{29} > 1$. Ahora, como $n_{11}(G) \equiv 1 \pmod{11}$, y $n_{11}(G) | 2^3 \cdot 29$. los divisores positivos de $8 \cdot 29$ son dados por

1 2 4 8 29 58 116 232

Por lo tanto $n_{11}(G) = 232$, y hay 232 11-Sylows. Como el orden de cada uno de ellos es 11, entonces ellos son ciclicos, con interseccion trivial entre ellos, y por lo tanto G tiene 2320 elementos de orden 11.

Por el mismo lado, tenemos $n_{29} \equiv 1 \pmod{29}$ y $n_{29} | 8 \cdot 11$ lo que tiene divisores

1 2 4 8 11 22 44 88

Así que $n_{29} = 88$ y G tiene 2464 elementos de orden 29. Por lo tanto $\text{ord } G \geq 2320 + 2464 > 2552$ una contradiccion. Así que G no es simple.

Lectura 10: El Teorema de Jordan-Hölder

Definición. Sea G un grupo y G_0, \dots, G_n donde $G_n = \langle e \rangle$ y $G_0 = G$ tal que $G_{i+1} \trianglelefteq G_i$. Entonces se llama el serie

$$G_n \trianglelefteq \dots \trianglelefteq G_0$$

una **serie subnormal** de G .

Ejemplo 30.

(1) Coje $G_0 = D_8$, $D_1 = \langle r \rangle$, $G_2 = \langle r^2 \rangle$, $G_3 = \langle r^4 \rangle$ y $G_4 = \langle e \rangle$. Entonces $G_4 \trianglelefteq G_3 \trianglelefteq G_2 \trianglelefteq G_1 \trianglelefteq G_0$.

Definición. Sea G un grupo y $\{G_i\}_{i=0}^n$ una colección de subgrupos de G tales que $G_n = \langle e \rangle$, y $G_{i+1} \trianglelefteq G_i$ son subgrupos normales maximales. Entonces la serie subnormal

$$\langle e \rangle = G_n \trianglelefteq \cdots \trianglelefteq G_0 = G$$

se llama una **serie de composicion** para G . Llamamos los factores G_i/G_{i+1} los **factores** de la serie.

Lema 43. *En cualquier serie de composicion, los factores son grupos simples.*

demostración. Esto viene por el teorema de la correspondencia, junto a que los $G_{i+1} \trianglelefteq G_i$ son normales maximales. ■

Lema 44. *Sea G un grupo con serie de composicion $\langle e \rangle = G_n \trianglelefteq \cdots \trianglelefteq G_0 = G$. Para cualquier $K \trianglelefteq G$, removiendo las repeticiones de la serie $\langle e \rangle = K \cap G_n \trianglelefteq \cdots \trianglelefteq K \cap G_0 = K$, obtenemos una serie de composicion para K .*

demostración. Sea $x \in K \cap G_i$ y $g \in K \cap G_{i+1}$. Entonces $ngx^{-1} \in K$ y $ngx^{-1} \in G_{i+1}$, pues $G_{i+1} \trianglelefteq G_i$. Por lo tanto $K \cap G_{i+1} \trianglelefteq K \cap G_i$.

Ahora miremos a $(K \cap G_i)/(K \cap G_{i+1})$. Como G_i/G_{i+1} es simple, entonces G_{i+1} es normal maximal en G_i . Entonces los unicos subgrupos de G_i que contienen a G_{i+1} son G_i ó G_{i+1} . Ahora $K \cap G_i \trianglelefteq G_i$, y por lo tanto $G_{i+1} \trianglelefteq (K \cap G_i)G_{i+1} \trianglelefteq G_i$. Por lo tanto $G_{i+1} = (K \cap G_i)G_{i+1}$, o $G_i = (K \cap G_i)G_{i+1}$. Por el segundo toerema del isomorfismo,

$$((K \cap G_i)G_{i+1})/G_{i+1} \simeq (K \cap G_i)/(K \cap G_i \cap G_{i+1}) = (K \cap G_i)/(K \cap G_{i+1})$$

Sí $G_{i+1} = (K \cap G_i)G_{i+1}$, entonces $K \cap G_i = K \cap G_{i+1}$ y tenemos una repeticion. Sí $G_i = (K \cap G_i)G_{i+1}$, entonces tenemos que $G_i/G_{i+1} \simeq (K \cap G_i)/(K \cap G_{i+1})$ y terminamos. ■

Ejemplo 31. Considere el serie de composicion $\langle 0 \rangle \trianglelefteq \langle 6 \rangle \trianglelefteq \langle 2 \rangle \trianglelefteq \mathbb{Z}/12\mathbb{Z}$. Escoja $\langle 3 \rangle \trianglelefteq \mathbb{Z}/12\mathbb{Z}$ y obtenemos la serie de composicion para 3 de ser $\langle 0 \rangle \trianglelefteq \langle 6 \rangle \trianglelefteq \langle 3 \rangle$.

Teorema 45 (El Teorema Jordan-Hölder). *Sea G un grupo que tiene una serie de composicion. Entonces cualquier dos series de composicion para G tiene el mismo largo, mas aún sí*

$$\langle e \rangle = G_n \trianglelefteq \cdots \trianglelefteq G_0 = G \text{ y } \langle e \rangle = H_n \trianglelefteq \cdots \trianglelefteq H_0 = G$$

son series de composiciones para G , y $s \in S_n$ es una permutacion, entonces

$$G_i/G_{i+1} \simeq H_{s(i)}/H_{s(i)+1}$$

Ejemplo 32. (1) Sea $\langle e \rangle \trianglelefteq \langle r^4 \rangle \trianglelefteq \langle r^2 \rangle \trianglelefteq D_8$ Escoja tambien $H = \{e, r^4, t, r^4 t\}$ normal y maximas, entonces tenemos que $\langle e \rangle \trianglelefteq \langle r^4 \rangle \trianglelefteq H \trianglelefteq D_8$.

(2) Sea $\langle 0 \rangle \trianglelefteq \langle 6 \rangle \trianglelefteq \langle 2 \rangle \trianglelefteq \mathbb{Z}/12\mathbb{Z}$ escoja $\langle 0 \rangle \trianglelefteq \langle 6 \rangle \trianglelefteq \langle 3 \rangle \trianglelefteq \mathbb{Z}/12\mathbb{Z}$ y $\langle 0 \rangle \trianglelefteq \langle 4 \rangle \trianglelefteq \langle 2 \rangle \trianglelefteq \mathbb{Z}/12\mathbb{Z}$.

Lectura 11: Grupos Resolubles y Nilpotentes

Definición. Sea G un grupo. Un subgrupo H de G se llama **característica** sí para cada automorfismo ϕ de G , $\phi(H) = H$; es decir que ϕ restringido a H es sobre. Escribimos $H \text{ char } G$

Lema 46. Sea G un grupo y $H \leq K \leq G$ subgrupos. Entonces

(1) Sí $H \text{ char } K$ y $K \text{ char } G$, entonces $H \text{ char } G$.

(2) Sí $H \text{ char } K$ y $K \trianglelefteq G$, entonces $H \trianglelefteq G$.

demostración. Suponga que $H \leq K \leq G$. Sea ϕ un automorfismo de G , entonces $\phi(K) = K$. Es decir que $\phi' = \phi|_K$ es sobre. Entonces vemos tambien que $\phi'(H) = H$, pero $\phi'(H) = \phi(H)$, así que $H \text{ char } G$.

Ahora considere el automorfismo de K dado por $k \rightarrow gkg^{-1}$ para $g \in G$. Para cualquier g tenemos un automorfismo bien definido de K . Por lo tanto esta preserva a H , como $H \text{ char } K$, es decir que $gHg^{-1} = H$. ■

Definición. El **subgrupo conmutador** G' de un grupo G es el subgrupo de G generado por todos los elements conmutadores de G , $[x, y] = xyx^{-1}y^{-1}$. Tambien llamamos a G' la **derivada** de G .

Lema 47. El subgrupo conmutador de un grupo verdaderamente es un subgrupo.

Lema 48. Sea G' el conmutador de G . Entonces los sigueintes enunciados son ciertos.

(1) $G' \text{ char } G$.

(2) Sí G es abeliano, entonces $G' = \langle e \rangle$.

(3) G/G' es abeliano.

(4) Si $N \trianglelefteq G$, entonces G/N es abeliano si y solo si $G' \leq N$.

demostración. (1) Sea $\phi \in \text{Aut } G$, entonces $\phi([x, y]) = \phi(xyx^{-1}y^{-1}) = \phi(x)\phi(y)\phi^{-1}(x)\phi^{-1}(y) = [\phi(x), \phi(y)]$. Así que $\phi(G') = G'$.

(2) Suponga que G es abeliano, entonces para todo $[x, y] \in G'$, $xyx^{-1}y^{-1} = xx^{-1}yy^{-1} = e$.

(3) Como $G' \trianglelefteq G$, G/G' es un grupo. Ahora, sean $xG', yG' \in G/G'$, entonces $xG'yG' = xyG'$ lo que dice que $xyx^{-1}y^{-1} = (xy)(yx)^{-1} \in G'$, entonces $(xy)G' = (yx)G'$.

(4) Por ultimo, si $N \trianglelefteq G$ y G/N es abeliano, entonces $xNyN = xyN = yxN = yNxn$, lo que dice que $(xy)(yx)^{-1} \in N$, lo que dice $[x, y] \in N$; así que $G' \leq N$. Por otro lado, si $G' \leq N$, entonces $[x, y] = (xy)(yx)^{-1} \in N$ lo que dice que $xyN = yxN$. ■

Corolario. G/G' es el grupo abeliano mas grande que se puede formar por factores.

Lema 49. Si G es un grupo, y $H \leq G$ un subgrupo de G entonces $H' \leq G'$.

demostración. Como $H \leq G$, $x, y, g, h \in H$ implica $(xg)(yh)(xg)^{-1}(yh)^{-1} \in H$, así que $[xg, yh] \in H'$ cuando $[x, y], [g, h] \in H'$. Mas aún si $[x, y] \in H'$, entonces $xyx^{-1}y^{-1} \in H$, así que $y^{-1}x^{-1}yx \in H$ entonces $[y^{-1}, x^{-1}] \in H'$. ■

Definición. Sea G un grupo. Para cualquier $n \in \mathbb{N}$, definimos recursivamente el **n -esima derivada** de G como:

(1) $G^{(0)} = G$ y $G^{(1)} = G'$.

(2) $G^{(n+1)} = (G^{(n)})'$ para todo $n \geq 0$.

Definición. Llamamos una serie subnormal $\langle e \rangle = G_n \trianglelefteq \dots \trianglelefteq G_0 = G$ una **serie normal** si para todo $0 \leq i \leq j \leq n$, tenemos $G_j G_i$.

Definición. Un grupo G se llama **resoluble** si en algun momento la n -esima derivada de G es trivial para algún $n \geq 0$. Mas precisamente, existe una serie normal

$$\langle e \rangle = G^{(n)} \trianglelefteq G^{(n-1)} \trianglelefteq \dots \trianglelefteq G^{(0)} = G$$

Lema 50. Todo grupo abeliano es resoluble.

demostración. Por supuesto, si G es un grupo abeliano, entonces $G' = \langle e \rangle$ lo cual es la 1-esmia derivada. Pues G tiene el serie normal $\langle e \rangle = G^{(1)} = G' \trianglelefteq G^{(0)} = G$. ■

Corolario. G es un grupo simple y resoluble si G es ciclico de orden p , p un primo.

demostración. Con G simple y resoluble. Entonces los unicos subgrupos normales de G son $\langle e \rangle$ y si mismo, así que $G' = G$ o $G' = \langle e \rangle$. Pero como G es resoluble, $G' \neq G$, al contrario $G^{(n)} = G$ para todo $n \geq 0$ seria cierto. Por lo tanto G es abeliano, lo que dice que $G \simeq \mathbb{Z}/p\mathbb{Z}$ para p primo. ■

Corolario. Un grupo noabeliano y simple no puede ser resoluble.

demostración. Al no ser abeliano, tenemos $G' \neq \langle e \rangle$, así que $G' = G$. ■

Teorema 51. Las siguientes enunciados son equivalentes.

(1) G es un grupo resoluble.

(2) G tiene una serie normal

$$\langle e \rangle = G_n \trianglelefteq \cdots \trianglelefteq G_0 = G$$

con todos los factores abelianas.

(3) G tiene una serie subnormal

$$\langle e \rangle = G_n \trianglelefteq \cdots \trianglelefteq G_0 = G$$

con todos los factores abelianas.

demostración. Ciertamente, si G es resoluble, entonces la serie $\langle e \rangle = G^{(n)} \trianglelefteq \cdots \trianglelefteq G^{(0)} = G$ es una serie normal cuyas factores son abelianas. Además, de esto ser cierto, tenemos que todo serie normal es subnormal; así que $\langle e \rangle = G_n \trianglelefteq \cdots \trianglelefteq G_0 = G$ es una serie subnormal con los factores abelianas.

Ahora, suponga que $\langle e \rangle = G_n \trianglelefteq \cdots \trianglelefteq G_0 = G$ es una serie subnormal donde G_i/G_{i+1} es abeliana para todo $0 \leq i \leq n-1$. Para $i=0$, tenemos que $G_1 \trianglelefteq G$ y G/G_1 es abeliano, por lo tanto $G' = G^{(1)} \leq G_1$. Por inducción, suponga que para todo $i \geq 0$ que $G^{(i)} \leq G_i$. Como $G^{(i+1)} = (G^{(i)})'$, por hipotesis tenemos que $G^{(i+1)} \trianglelefteq G'_i$. Mas aún, $G'_i \leq G_{i+1}$ pues G_i/G_{i+1} es abeliano y $G^{(i+1)} \leq G_{i+1}$. Por lo tanto existe una $n \geq 0$ tal que $G^{(n)} = \langle e \rangle$, lo que hace G resoluble. ■

Ejemplo 33. (1) D_8 es resoluble. Escoja $\langle e \rangle \trianglelefteq \langle r^4 \rangle \trianglelefteq \langle r^2 \rangle D_8$.

(2) Tenemos la serie subnormal $\langle e \rangle \trianglelefteq C_2 \times C_2 \trianglelefteq A_4 \trianglelefteq S_4$. Donde $C_2 \times C_2 = \{(1), (1\ 2)(3\ 4), (1\ 3)(2\ 4)\}$. Nota que $C_2 \times C_2 / \langle e \rangle = C_2 \times C_2 \simeq V_4$, que $A_4 / C_2 \times C_2 \simeq \mathbb{Z}/3\mathbb{Z}$ y $S_4 / A_4 \simeq \mathbb{Z}/2\mathbb{Z}$. Así que S_4 es resoluble.

Lema 52. *Subgrupos y cocientes de grupos resolubles son resolubles.*

demostración. Sea $H \leq G$, entonces $H' \leq G'$, por lo tanto $H^{(r)} \leq G^{(r)} = \langle e \rangle$, así que $H^{(r)} = \langle e \rangle$.

Ahora, sea $N \trianglelefteq G$, pues G/N es un grupo. Entonces los conmutadores de G/N son de la forma $xNyNx^{-1}Ny^{-1}N = xyN(xy)^{-1}N = (xy(xy)^{-1})N = [x, y]N$. Así que $(G/N)' = G'/N \simeq G'/G' \cap N$, por el segundo teorema de isomorfismo. Entonces por inducción tenemos que $(G/N)^{(r)} \simeq G^{(r)}/G^{(r)} \cap N = \langle e \rangle / \langle e \rangle = \langle e \rangle$. Por lo tanto G/N es resoluble. ■

Lema 53. *Las siguientes enunciados son equivalentes para cualquier grupo G .*

- (1) G es el producto directo de sus subgrupos de Sylow.
- (2) Todo p -subgrupo de Sylow de G es normal en G para todo $p \mid \text{ord } G$.

demostración. Suponga que $G = P_1 \times \cdots \times P_k$, para P_k un p_k -Sylow de G . Entonces por definición de lo que es un producto directo, todo $P_i \trianglelefteq G$ para $1 \leq i \leq k$.

Por otro lado, suponga que los p -Sylows de G son normales. Entonces todo p -Sylow de G es único. Sea P_i un p_i -Sylow de G , donde $p_i \mid \text{ord } G$, para todo $1 \leq i \leq k$. Tenemos entonces que $\text{ord } P_1 P_2 = \text{ord } P_1 \text{ord } P_2$ ya que $P_1 \cap P_2 = \langle e \rangle$. Por lo tanto $\text{ord } P_1 \cdots P_k = \text{ord } P_1 \cdots P_k$, entonces $G = P_1 \cdots P_k$ y $P_i \cap \prod_{i \neq j} P_j = \langle e \rangle$. Por definición, G es el producto directo de sus p_i -subgrupos de Sylow. ■

Definición. Un grupo finito G lo cual es producto directo de sus subgrupos de Sylow se llama **nilpotente**.

Lema 54. *Todos los subgrupos abelianos, y p -grupos son nilpotentes.*

demostración. Vemos que un grupo abeliano solo tiene p -Sylows normales, así que por lema 53, los abelianos son nilpotentes.

Sea P un p -grupo finito. Entonces P tiene un solo p -subgrupo de Sylow, así que es nilpotente. ■

Lectura 12: Anillos

Definición. Un **anillo** R es un grupo abeliano bajo una operación binaria $+$ junto a una operación binaria $\cdot : (a, b) \rightarrow ab$ tal que

- (1) \cdot es asociativa.
- (2) $a(b + c) = ab + ac$ y $(a + b)c = ac + bc$.

Sí existe un elemento $1 \in R$ tal que $a_1 = 1a = a$, entonces llamamos a R un anillo con **unidad**. Denotamos el elemento de identidad de R bajo $+$ como 0 . Sí $ab = ba$ para todo $a, b \in R$, entonces llamamos R **commutativa**.

Definición. Sea R un anillo con unidad, y $a, b \in R$. Sí $ab = 0$ donde $a \neq 0$, y $b \neq 0$, entonces llamamos a a y b **divisores de cero**. Sabemos $1a = a1 = a$, entonces llamamos a 1 **unidades**.

Definición. Un **dominio integral** es un anillo commutativa sin divisores de 0 . Llamamos la **característica** de un anillo R de ser el entero mas pequeño n tal que $na = \underbrace{a + \dots + a}_{n-\text{veces}} = 0$, para todo $a \in R$.

Definición. Sean R y S anillos. Llamamos a un mapa $\phi : R \rightarrow S$ un **homomorfismo de anillos** sí

$$(1) \quad \phi(a + b) = \phi(a) + \phi(b)$$

$$(2) \quad \phi(ab) = \phi(a)\phi(b)$$

Ejemplo 34. (1) Sea $\phi : \mathbb{Z}/6\mathbb{Z} \rightarrow \mathbb{Z}/6\mathbb{Z}$ dado por $n \rightarrow 3n$. Entonces $\phi(x+y) = 3(x+y) = 3x+3y$ y $\phi(xy) = 3(xy) = 3x_3y$, como $3 \cdot 3 \equiv 3 \pmod{6}$. Así que ϕ es un homomorfismo de anillos.

Definición. Sea $\phi : R \rightarrow S$ un homomorfismo de anillos. Entonces $\ker \phi = \{a \in R : \phi(a) = 0\}$.

Lema 55. Sea $\phi : R \rightarrow S$ un homomorfismo de anillos, y que los únicos ideales de R sean (0) y R . Entonces ϕ es $1-1$.

demostración. Nota que $\ker \phi$ es ideal, así que $\ker \phi = (0)$ o $\ker \phi = R$. Como $\phi(1) = 1$, tenemos que $\ker \phi \neq R$. ■

Lectura 13: Anillos Cocientes

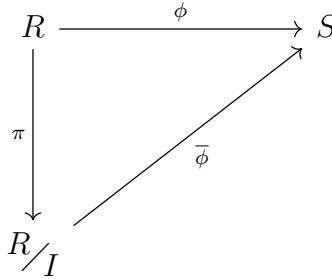
Definición. Sea R un anillo y I un ideal, entonces $R/I = \{r + I : r \in R\}$ se llama el **anillo cociente** de R sobre I .

Lema 56. Sea R un anillo, y I un ideal, entonces el anillo cociente R/I es un anillo bajo la suma de R y la multiplicación \cdot dado por $(a + I, b + I) \rightarrow (a + I)(b + I) = ab + I$.

Lema 57. Todo ideal es el kernel de un homomorfismo de anillos.

demostración. Escoje $\pi : R \rightarrow R/I$, entonces $\ker \pi = I$. ■

Teorema 58 (El Teorema del Factor). *Cualquier homomorfismo de anillos $\phi : R \rightarrow S$ con kernel K que contiene a un ideal I se puede factorizar via R/I , como $\phi = \bar{\phi} \circ \pi$ donde $\pi : R \rightarrow R/I$ y $\bar{\phi} : R/I \rightarrow S$ es el unico homomorfismo con $\bar{\phi}$ sobre si y solo si ϕ es sobre y $\bar{\phi}$ 1-1 si y solo si $K = I$.*



Teorema 59 (Primer Teorema de Isomorfismo). *Si $\phi : R \rightarrow S$ es un homomorfismo, entonces $\phi(R) \simeq R/K$ donde $K = \ker \phi$.*

Teorema 60 (Segundo Teorema de Isomorfismo). $R + I/I \simeq R/R \cap I$.

Ejemplo 35. Considere $\phi : \mathbb{R}[x] \rightarrow \mathbb{C}$ dado por $\phi(p(x)) = p(i)$, la valuacion de p en i . Entonces $\ker \phi = \{p(x) : p(i) = 0\} = \mathbb{R}[x](x^2 + 1)$, como $i^2 + 1 = 0$, tenemos que $\mathbb{R}[x]/(x^2 + 1) \simeq \mathbb{C}$.

Lectura 14: Ideales Maximales y Primos.

Definición. El ideal generado por el conjunto no vacio X , de un anillo R escrito $I = (X)$, es el ideal mas pequeño de R tal que $X \subseteq I$, y se llama el ideal **generado** por X .

Definición. Un ideal **maximal** en un anillo R es un ideal propio que no esta contenido en ningun otro ideal propio. Es decir si M es maximal y $M \subseteq I$, entonces $M = I$ o $M = R$.

Teorema 61. *Sea M un ideal de un anillo conmutativo con identidad. Entonces M es maximal si y solo si R/M es un cuerpo.*

demostración. Suponga que M es maximal. Entonces como R/M es un anillo conmutativo con identidad, sea $a + M \in R/M$ donde $a + M \neq M$ note que $M \subseteq Ra + M$, y como M es maximal, tenemos que $Ra + M = R$. Por lo tanto, $1 \in Ra + M$, y existen r, m tales que $1 = ra + m$. Note que $(r + M)(a + M) = ra + M = (1 - m) + M = 1 + M$. Por lo tanto $(a + M)^{-1} = r + M \in R/M$. Esto hace a R/M un cuerpo.

Suponga, por otro lado, que R/M es cuerpo, sea N un ideal tal que $M \subseteq N \subseteq R$, con $N \neq R$. Considere la mapa $\pi : R \rightarrow R/M$ dado por $a \rightarrow a + M$. Como N es ideal, entonces

por el teorema de la correspondencia $\pi(N)$ es un ideal de R/M . Por lo tanto $\pi(N) = (0)$, ó $\pi(N) = R/M$. Como π es 1-1, tenemos que $\pi(N) \neq R/M$, así que $\pi(N) = (0)$. Esto hace $N = M$, M es maximal. ■

Definición. Un ideal P en un anillo conmutativo con identidad es **primo** si para todo $a, b \in R$, si $ab \in P$ implica que $a \in P$, ó $b \in P$.

Teorema 62. Sea R un anillo conmutativo con identidad. Entonces un ideal P de R es primo si, y solo si R/P es un dominio integral.

demostración. Suponga que P es primo, y suponga que $(a+P)(b+P) = ab+P = 0+P = P$. Entonces tenemos que $ab \in P$. Como P es primo, $a \in P$ ó $b \in P$, así que $a+P = P$ o $b+P = P$, es decir, o $a = 0$ ó $b = 0$.

Por otro lado, suponga que R/P es un dominio integral. Entonces P es un ideal propio, es decir, $P \neq R$, y si $(a+P)(b+P) = ab+P = P$, entonces tenemos que $a+P = P$ ó $b+P = P$. Es decir, si $ab \in P$, entonces $a \in P$ ó $b \in P$. ■

Corolario. Todo ideal maximal es primo.

Corolario. Sea $\phi : R \rightarrow S$ un homomorfismo de anillos 1-1 con identidad. Las siguientes enunciadas son ciertos

(1) Si S es un cuerpo, entonces $\ker \phi$ es un ideal maximal de R .

(2) Si S es un dominio integral, entonces $\ker \phi$ es un ideal primo de R .

demostración. Por el primer teorema del isomorfismo, nota que $S \simeq R/\ker \phi$. ■

Ejemplo 36. Sean $\phi : \mathbb{Z}[x] \rightarrow \mathbb{Z}$ dado por $f(x) \rightarrow f(0)$, es decir, la mapa valuación. Entonces tenemos que $\mathbb{Z} \simeq \mathbb{Z}[x]/(x)$.

Lectura 15: Anillos de Polinomios

Lema 63. Si R es un anillo conmutativo con identidad, entonces el conjunto $R[x]$, definido por

$$R[x] = \{f(x) = \sum_{i=0}^n a_i x^i : a_i \in R \text{ para } 0 \leq i \leq n \text{ y } n \geq 0\}$$

Es un anillo conmutativo con identidad bajo la suma y multiplicación de polinomios.

Definición. Sea R un anillo conmutativo con identidad. Llamamos al anillo $R[x]$ el **anillo de polinomios** con coeficientes en R .

Lema 64. La mapa valuación $R[x] \rightarrow R$ dado por $f(x) \rightarrow f(0)$ es un homomorfismo de anillos.

Definición. Sea R un anillo. El **grado** de un polinomio $f \in R[x]$ es la potencia del termino líder de f ; es decir, si $f(x) = a_0 + a_1x + \cdots + a_nx^n$, y $a_n \neq 0$, entonces $\deg f = n$. Definimos el grado del polinomio $0 = 0(x)$ de ser $\deg 0 = -\infty$. Llamamos a f **mónico** si $a_n = 1$.

Teorema 65. Si $f, g \in R[x]$ son polinomios mónicos, entonces existen $q, r \in R[x]$, únicos, tales que

$$f(x) = q(x)g(x) + r(x), \text{ y}$$

$$\deg r < \deg g.$$

Definición. Sea $f \in R[x]$ un polinomio. Llamamos a un elemento $a \in R$ un **raíz** (ó una **cero**) de f si $f(a) = 0$.

Teorema 66. Si $f \in R[x]$, y $a \in R$, existe un unico $q \in R[x]$ tal que

$$f(x) = q(x)(x - a) + f(a)$$

$$\text{y } f(a) = 0 \text{ si y solo si } (x - a) | f.$$

demostración. Si f no tiene raíces, terminamos. Ahora si f tiene al menos una raíz $a_1 \in R$, entonces $f(x) = q_1(x)(x - a_1)^{n_1}$ donde $q_1(a_1) \neq 0$ y $\deg q_1 = n - n_1$, como R es dominio integral. Si a_1 es la única raíz de f , terminamos. Si no, procede recursivamente usando el teorema 65. Esta recursión concluye, y por lo tanto se enumera las raíces de f . ■

Lectura 16: Factorización Única

Definición. Sea R un dominio integral. Dos elementos $a, b \in R$ son **asociados** si $a = ub$ para algún unidad $U \in R$. Si $a \neq 0$ y no es unidad, entonces llamamos a a **irreducible** si $a = bc$ implica que b ó c es unidad. Llamamos a a **primo** si $a | bc$ implica que $a | b$ ó $a | c$.

Lema 67. Si a es primo, entonces a es irreducible.

demostración. Sea a primo con $a = bc$. Suponga que $a | b$, lo que dice que $ba = bcd = b(1 - cd) = 0$, entonces $1 = cd$ lo que hace c unidad. De igual manera si $c | a$, entonces b es unidad. ■

Ejemplo 37. Sea $\mathbb{Z}(\sqrt{-3}) = \{a + ib\sqrt{3} : a, b \in \mathbb{Z}\}$. Sea $2 = (a + ib\sqrt{3})(c + id\sqrt{3})$. Como $2 \in \mathbb{R}$, tenemos que $4 = 2 \cdot \bar{2} = (a + ib\sqrt{3})(c + id\sqrt{3})(a - ib\sqrt{3})(c - id\sqrt{3}) = (a^2 + 3b^2)(c^2 + 3d^2)$. Entonces $(a^2 + 3b^2) | 4$ pero $(a^2 + 3b^2) \nmid 2$; en seguida, tenemos $4a^2 + 3b^2 = 4$ implica que $c^2 + 3d^2 = 1$, lo que nos lleva a $d = 0$ y $c = \pm 1$ y 2 es irreducible en $\mathbb{Z}(\sqrt{-3})$. Ahora nota que $2 | (1 + i\sqrt{3})(1 - i\sqrt{3}) = 4$, pero $2 \nmid (1 + i\sqrt{3})$ y $2 \nmid (1 - i\sqrt{3})$, así que 2 no es primo en $\mathbb{Z}(\sqrt{-3})$.

Definición. Un **dominio de factorización única** es un dominio integral R , que satisface las siguientes

- (1) Para todo $a \neq 0$, se puede escribir a como el producto de irreducibles, salvo a unidad; es decir:

$$a = up_1 \dots p_n \text{ para } p_1, \dots, p_n \in R \text{ irreducibles.}$$

Sea llama a este producto una **factorización** de a .

- (2) El factorización de a es única.

Lema 68. En un dominio de factorización única, R , a es irreducible sí y solo sí a es primo.

demonstración. Por supuesto, sí a , es irreducible. Ahora, suponga que a es irreducible, y que $a | bc$ Entonces $bc = ad$ para algún $d \in R$. Descomponga, entonces, b , c , y d en productos de irreducibles:

$$a(ud_1 \dots d_r) = (vb_1 \dots b_s)(wc_1 \dots c_k)$$

donde $u, v, w \in R$ son unidades. Por unicidad de la factorización, a tiene que ser asociado de algún b_i ó c_j , entonces $a | b$ ó $a | c$ haciendo a a primo. ■

Definición. Sea R un dominio integral y suponga que $a_1, a_2, a_3, \dots \in R$ tales que

$$(a_1) \subseteq (a_2) \subseteq (a_3) \subseteq \dots (a_n) \subseteq \dots$$

se estabiliza; es decir, $(a_n) = (a_{n+1}) = \dots$ para algún $n \in \mathbb{Z}^+$ Entonces decimos que R satisface la **condición de cadena ascendente** para ideales primos. Si sateifaces esta condición para todo ideal, llamamos a R un anillo **Noeteriano**.

Ejemplo 38. (1) $\mathbb{R}[x_1, x_2, x_3, \dots]$ tiene la cadena $(x_1) \subseteq (x_1, x_2) \subseteq (x_1, x_2, x_3) \subseteq \dots$ que se estabiliza.

- (2) $\mathbb{Z} + x\mathbb{Q}[x]$ tiene la cadena $(x) \subseteq (\frac{x}{2}) \subseteq \frac{x}{4} \subseteq \dots$ que no estabiliza.

Teorema 69. Sea R un dominio integral. Entonces las siguientes enunciadas son ciertos.

- (1) *Sí R es un dominio de factorización única, entonces satisfaces la condición de la cadena ascendente.*
- (2) *Sí R satisface la condición ascendente, entonces todo $a \in R$ se puede factorizar en irreducibles (no necesariamente de forma única).*
- (3) *Sí R es tal que todo $a \in R \setminus \{0\}$ se puede factorizar en irreducibles primos, entonces R es un dominio de factorización única.*

demostración. (1) Considera la cadena $(a_1) \subseteq (a_2) \subseteq (a_3) \subseteq \dots$, donde R es un dominio de factorización única. Tenemos entonces que cada $a_{i+1} | a_i$. Por lo tanto, los factores primos de a_{i+1} consisten de algunos primos de a_i . Como a_1 tiene factorización única, entonces los factores primos en la cadena terminarán siendo los mismos y la cadena estabiliza.

- (2) Tome $a_1 \neq 0$. Sí a_1 es irreducible, terminamos. De lo contrario, $a_1 = a_2 b_2$, no unidades. Como $a_2 | a_1$, $(a_1) \subseteq (a_2)$. Sí a_2 es irreducible, terminamos. De lo contrario, procede recursivamente, y siempre que tengamos un factor no irreducible, podemos añadir un nuevo ideal principal a la cadena:

$$(a_1) \subseteq (a_2) \subseteq (a_3) \subseteq \dots$$

lo cual tiene que estabilizar. Por lo tanto, a_1 se puede factorizar.

- (3) Ahora, por lo anterior, sabemos que podemos factorizar los elementos $a \neq 0$ de R . Sea que $a = up_1 \dots p_n$ y $a = vq_1 \dots q_m$ con $u, v \in R$ unidades, y los p_i, q_j irreducibles para todo $1 \leq i \leq n$ y $1 \leq j \leq m$. Ahora, p_1 es irreducible y también es primo.....

■

Teorema 70. *Sí R es un dominio de ideal principal, entonces R es un dominio de factorización única.*

demostración. Considere la cadena $(a_1) \subseteq (a_2) \subseteq (a_3) \subseteq \dots$. Sea $I = \bigcup (a_i)$. Note que I es un ideal de R , así que $I = (b)$ para algún $b \in R$. Entonces $b \in I$, lo que dice $b \in (a_n)$ para algún n , entonces $I = (b) \subseteq (a_n)$. Por lo tanto la cadena estabiliza.

Suponga ahora que $a \in R$ es irreducible. Sí $(a) = R$, entonces $1 \in (a)$ y a es unidad, lo cual es imposible. Entonces (a) está contenido en un ideal maximal M , entonces $M = (b)$ y $(a) \subseteq (b)$, y $b | a$. Es decir $a = bd$. Como a es irreducible, y b no es unidad, entonces d está forzado a ser unidad.

■

Lectura 17: Dominios Euclideos

Definición. Sea R un dominio integral. Llamamos a R un **dominio Euclideo** si existe una mapa $d : R \setminus \{0\} \rightarrow \mathbb{N}$ donde para todo $a, b \in R$, existen $q, r \in R$ únicos tales que

$$a = qb + r \text{ donde } r = 0 \text{ ó } d(r) < d(b)$$

Teorema 71. *Si R es un dominio Euclideo, entonces R es un dominio de ideal principal.*

demostración. Sea I un ideal de R . Si $I = (0)$, terminamos; pues, suponga que $I \neq (0)$. Considere entonces el conjunto

$$\mathcal{D} = \{d(b) : b \in I \text{ y } b \neq 0\}$$

Nota que $\mathcal{D} \subseteq \mathbb{N}$, así que por el principio de buen orden, tenemos que hay un elemento mínimo $m \in \mathcal{D}$. Sea entonces $b \in I$, con $b \neq 0$ tal que $d(b) = m$. Sea $a \in I$, entonces existen $q, r \in R$ únicas tales que

$$a = qb + r \text{ donde } r = 0 \text{ ó } d(r) < d(b)$$

Ahora, note que como $d(b) = m$ es mínimo, $d(r) \not< d(b)$, mas aún, tenemos que

$$r = a - qb \in I$$

lo que nos dice que $r = 0$, y $a = qb$. Es decir $I = (a)$. ■

Ejemplo 39. (1) Considere $\mathbb{Z}(\sqrt{D}) = \{a + b\sqrt{D} : a, b \in \mathbb{Z}\}$, donde D no tiene cuadrados. Y sea $d(a + b\sqrt{D}) = |a^2 - Db^2|$. Note que $\mathbb{Z}(\sqrt{D})$ es dominio integral, pues, tome $a, b \neq 0$. Considere entonces el cuerpo $\mathbb{Q}(\sqrt{D})$ que contenga a $\mathbb{Z}(\sqrt{D})$. Entonces

$$\frac{a}{b} = q' \text{ con } q' = x + y\sqrt{D}, \text{ y } x, y \in \mathbb{Q}$$

Sean x_0, y_0 tal que $|x - x_0| \leq \frac{1}{2}$ y $|y - y_0| \leq \frac{1}{2}$. Tome $q = x_0 + y_0\sqrt{D}$ y $r = b((x - x_0) + (y - y_0)\sqrt{D})$. Pues, tenemos que $q \in \mathbb{Z}(\sqrt{D})$ mas aún

$$a = bq + r$$

Así que $r \in \mathbb{Z}(\sqrt{D})$, y

$$\begin{aligned} d(r) &= d(b)d((x - x_0) + (y - y_0)\sqrt{D}) \\ &= d(b)|((x - x_0)^2 - D(y - y_0)^2)| \\ &\leq d(b)|((x - x_0)^2| + |D|| (y - y_0)^2| \leq d(b)\left(\frac{1}{4} + \frac{|D|}{4}\right) \end{aligned}$$

Pues, si $D = -2, -1, 2$ entonces $d(r) \leq d(b)$ y $\mathbb{Z}(\sqrt{D})$ es un dominio Euclideo. En el caso de que $D = -1$, poniendo $i = \sqrt{D}$, llamamos a $\mathbb{Z}(i)$ los **enteros Gaussianos**. Nota que $\mathbb{Z}(i) \subseteq \mathbb{C}$.

- (2) Los enteros \mathbb{Z} son un dominio Euclidean con $d = |\cdot|$.
- (3) Para cualquier cuerpo K , $K[x]$ es un dominio Euclidean con $d(f) = \deg f$ para todo $f \in K[x]$.
- (3) El anillo $\mathbb{Z}[\frac{1+i\sqrt{19}}{2}]$ es un dominio de ideal principal, pero no un dominio Euclidean.

Lectura 18: Polinomios Irreducibles

En el caso de un cuerpo F , las unidades de $F[x]$ son las unidades de F no cero y los polinomios irreducibles son aquellos de grado $\deg = 1$ o grado $\deg > 1$ que no se puede factorizar en polinomios de grado menor.

Ejemplo 40. $4x + 2$ es irreducible en \mathbb{Q} , pero $4x + 2 = 2(2x + 1)$ en \mathbb{Z} .

Teorema 72. Sea R un dominio integral, y defina la relación de equivalencia \sim sobre $R \times R \setminus \{0\}$ dado por

$$(a, b) \sim (c, d) \text{ si y solo si } ad - bc = 0$$

Sea $Q = R \times R \setminus \{0\} / \sim$ el conjunto factor y defina las operaciones $+$ y \cdot dados por

$$(a, b) + (c, d) = (ad + bc, bd)(a, b)(c, d) = (ac, bd)$$

Entonces Q forma un cuerpo bajo estas operaciones.

demostración. Nota que $(Q, +)$ forma un grupo abeliano con identidad $(0, 1)$ y inversos $(-a, b)$. De igual forma, (Q, \cdot) forma un grupo abeliano con la identidad $(1, 1)$ y inversos

(b, a) . Por ultimo, note que

$$(a, b)((c, d) + (e, f)) = (a, b)(cf + de, df) = (acf + ade, bdf) = (a, b)(c, d) + (a, b)(e, f)$$

■

Definición. Sea R un dominio integral y considera la relación de equivalencia \sim dado sobre $R \times R \setminus \{0\}$ por

$$(a, b) \sim (c, d) \text{ sí y solo sí } ad - bc = 0$$

Entonces llamamos al cuerpo $Q = R \times R \setminus \{0\} / \sim$ el **cuerpo de fracciones** sobre R .

Ejemplo 41. (1) El cuerpo de fracciones de $\mathbb{Z}(\sqrt{D})$ es precisamente el cuerpo $\mathbb{Q}(\sqrt{D})$.

(2) El cuerpo de fracciones de \mathbb{Z} es \mathbb{Q} .

Lema 73. *Un dominio integral R se puede encrustar en su cuerpo de fracciones.*

demostración. Toma la mapa $a \rightarrow \frac{a}{1}$.

■

Suponga que D es un dominio de factorización única, y tome $f(x) = a + abx$, D con $a \neq 0$ y a no una unidad. Entonces

$$f(x) = a(1 + bx)$$

y f es irreducible.

Definición. Sea D un dominio de factorización única, y sea $f \in D[x]$ con $f(x) = \sum_{i=0}^n a_i x^i$. Llamamos al gcd (a_0, \dots, a_n) de los coeficientes de f el **contenido** de f y escribimos

$$c(f) = (a_0, \dots, a_n)$$

Sí $c(f)$ es unidad, entonces llamamos a f un polinomio **primitivo** y en la factorización $f = c(f)f^*$, llamamos a f^* la **parte primitiva** de f .

Lema 74. *Sea D un dominio de factorización única, y sea $f \in D[x]$, $f \neq 0$, tal que $pf = gh$ para $g, h \in D$ y $p \in \mathbb{Z}^+$ un primo. Entonces p divide a $c(g)$ ó a $c(h)$.*

demostración. Sea que $pf = gh$, y suponga lo contrario. Sea $g(x) = g_0 + g_1x + \dots + g_sx^s$, y $h(x) = h_0 + h_1x + \dots + h_tx^t$. Suponga que $p \nmid c(g)$ y que $p \nmid c(h)$. Sean g_u y h_u los coeficientes de los terminos con los potencias mas pequeñas que no son divididos por p . Nota, que el coeficiente del termino x^{u+v} en gh es $\sum_{i=0}^{u+v} g_i h_{u+v-i}$. Entonces por definición de g_u y h_v , p divide a todos los terminos de la suma que no sean $g_u h_v$. Por lo tanto $p \sum g_i h_{u+v-i}$ y por lo tanto los coeficientes no son divisibles por p . Pero $pf = gh$, esto es una contradicción. ■

Lema 75 (Lemma de Gauss). Sean $f, g \in D[x]$ polinomios no constantes y D un dominio integral. Entonces $c(fg) = c(f)c(g)$. En particular, el producto de polinomios primitivos son primitivos.

demostración. Nota, que $f = c(f)f^*$, y $g = c(g)g^*$, con f^*, g^* las partes primitivas de f y g respectivamente. Entoncec $fg = c(f)c(g) = f^*g^*$. Como $c(f)c(g)|fg$, entionces $c(f)c(g)|c(fg)$. Suponga pues, sea p^a cualquier potencia de un primo que aparece en la factorización de $c(fg)$. omo $fg = c(fg)(fg)^*$, $(fg)^*$ la parte primitiva de fg , entonces tenemos que $c(fg)|fg$. Es decir que $p^a|fg$. Entonces $p^a|f$ ó $p^a|g$. En cualquier de los casos, tenemos que $p^a|c(f)c(g)$. Por lo tanto $c(fg)|c(f)c(g)$. Por lo tanto $c(fg) = c(f)c(g)$. ■

Teorema 76. Sea D un dominio de factorización única con cuerpo de fracciones F . Sí $f \in D[x]$, no es una constante, entonces f es irreducible sobre D sí y solo sí f es primitivo en $D[x]$, y irreducible en $F[x]$.

demostración. Suponga, que f es irreducible en $D[x]$. Entonces f es primitivo. Mas aún, por lo contrario, factoriza a $c(f)$ de f . Supong ahora que $f = gh$ en f , con $g, h \in F[x]$ no unidades con $\deg g < \deg f$ y $\deg h < \deg f$. Como F es cuerpo de fracciones, tenemos

$$g(x) = \frac{a}{b}g^*(x) \text{ y } h(x) = \frac{e}{d}h^*$$

Con $a, b, e, d \in D$ y $g^*, h^* \in D[x]$ las partes primitivos de g y h . Es decir que $c(g) = \frac{a}{b}$ y $c(h) = \frac{e}{d}$. Por lo tanto,

$$f = c(g)c(h)g^*h^* = c(gh)g^*h^* = \frac{ae}{bd}g^*h^*$$

Por el lema de Gauss, g^*h^* es primitivo. Como f es primitivo, tenemos $c(f) = c(gh) = 1$, así que $\frac{ae}{bd} = 1$ implica a, b, e, d son unidades. Esto contradice que f sea irreducible en $D[x]$.

Por otro lado, sea f primitivo en $D[x]$, y irreducible en $F[x]$. Como se puede encrustar a D en F , y por ende encrustar a $D[x]$ en $F[x]$, pues tenemos que f es irreducible en $D[x]$. ■

Teorema 77 (El Criterio de Eisenstein). Sea f un polinomio no constante en D , de la forma $f(x) = a_0 + a_1x + \cdots + a_nx^n$ donde $a_n \neq 0$. Sí $p \in \mathbb{Z}^+$ es primo tal que $p|a_0$, pero $p^2 \nmid a_n$, entonces f es irreducible.

demostración. Sí perder la generalidad, suponga que f es irreducible en $D[x]$. Suponga que

$f = gh$ con

$$g(x) = g_0 + g_1x + \cdots + g_rx^r$$

$$h(x) = h_0 + h_1x + \cdots + h_sx^s$$

Note, que $r \neq 0$, pues tendríamos que $g_0 = g|f$ y que es unidad, lo que contradice que f sea irreducible.

Ahora, sea $p|a_0 = g_0h_0$ y que $p^2 \nmid a_0$, entonces $p|g_0$ o $p|h_0$, pero no los dos. Suponga que $p|g_0$. Como $a_n = g_rh_s$, entonces $p \nmid g_r$, sea $i \in \mathbb{Z}^+$ el entero menor tal que $p \nmid g_i$. Entonces note que para $1 \leq i \leq r$

$$a_i = g_0h_i + g_1h_{i-1} + \cdots + g_ih_0$$

y por selección, $p|(g_0, \dots, g_{i-1})$. Como $p|a_i$, entonces $p|g_ih_0$, que es una contradicción. ■

Lectura 19: Extensiones de Cuerpos

Definición. Sea F y E cuerpos tal que $F \subseteq E$. Entonces decimos que E es un **extensión** de F y escribimos E/F como el extensión.

Ejemplo 42. Los siguientes son extensiones de cuerpos.

(1) \mathbb{C}/\mathbb{R} .

(2) \mathbb{R}/\mathbb{Q}

(4) $\mathbb{Q}(i)/\mathbb{Q}$ donde $\mathbb{Q}(i) = \{a + ib : a, b \in \mathbb{Q}\}$, y $i^2 + 1 = 0$.

(5) $\mathbb{F}_2[x]/(p)$ es una extensión de \mathbb{F}_2 , donde $p(x) = x^3 + x + 1$.

Definición. Sea E un extension de F . El **grado** de E/F , denotado $[E : F]$ es la dimension de E como espacio vectorial sobre F , es decir, $\dim_F E = [E : F]$. Si $[E : F]$ es finita, entonces llamamos a E/F una extensión **finita**.

Ejemplo 43. (1) $[\mathbb{C} : \mathbb{R}] = 2$, note que \mathbb{C} y \mathbb{R} son ambos conjuntos finitos.

(2) $[\mathbb{R} : \mathbb{Q}]$ es infinito.

(3) $[\mathbb{Q}(i) : \mathbb{Q}] = 2$.

(4) $[\mathbb{F}_2[x]/(p) : \mathbb{F}_2] = 3$, donde $p(x) = x^3 + x + 1$.

Lema 78. Sea F y E cuerpos, E no necesariamente una extensión de F , y sea $\phi : F \rightarrow E$ un homomorfismo de cuerpos. Entonces ϕ es 1-1.

demostración. Note que, como F es un cuerpo, los únicos ideales que tienes es (0) y $(1) = F$. Nota que, como F tiene al menos $0, 1 \in F$, las identidades, entonces tenemos que $\phi : 0_F \rightarrow 0_E$ y $\phi : 1_F \rightarrow 1_E$. Así que tenemos que $\ker \phi = (0)$. ■

Corolario. Si E es extensión de F , se puede enrustar a F en E .

Teorema 79. Sea $f(x)$ un polinomio no constante sobre el cuerpo F , entonces existe una extensión E/F y un $\alpha \in E$ tal que $f(\alpha) = 0$.

demostración. Sabemos que $F[x]$ es un dominio de factorización única, así que f tiene factorización única en irreducibles. Entonces suponga sin perder la generalidad que f es irreducible. Considere ahora el ideal (f) , como f es irreducible, y F es dominio de factorización única, entonces f es primo, es decir, que (f) es primo. Ahora, como $F[x]$ es un dominio de ideales principales, tenemos que $(f) \subseteq (q)$, donde (q) es un ideal maximal. Entonces $q|f$ y como f es irreducible, tenemos que $q = f$ y $(q) = (f)$. Como f no es constante, y $(q) \neq F[x]$, q no es unidad, así que, sea

$$E = F[x]/(f)$$

enrusta a F en E vía el homomorfismo $a \rightarrow a + (f)$. Entonces sea $\alpha = x + (f)$ y sea $f(x) = a_0 + a_1x + \cdots + a_nx^n$, entonces

$$\begin{aligned} f(\alpha) &= (a_0 + (f)) + (a_1 + (f))(x + (f)) + \cdots + (a_n + (f))(x + (f))^n \\ &= (a_0 + (f)) + (a_1x + (f)) + \cdots + (a_nx^n + (f)) \\ &= (a_0 + a_1x + \cdots + a_nx^n) + (f) \\ &= f + (f) \\ &= (f) \end{aligned}$$

Por lo tanto $f(\alpha) = 0$. ■

Definición. Si f es un polinomio sobre un cuerpo F , y E/F es una extensión, llamamos a un $\alpha \in E/F$ una **raíz** de f si $f(\alpha) = 0$. Si todo elemento de E/F es raíz de un polinomio, entonces llamamos a E/F **algebraico**, y decimos que sus elementos también son **algebraicos**. De lo contrario, decimos que $\alpha \in E/F$ es **transcendental**.

Ejemplo 44. \mathbb{C} es algebraico sobre \mathbb{R} , lo que dicta la teorema fundamental del álgebra, pero \mathbb{R} no es algebraico sobre \mathbb{Q} . Considere $\pi, e \in \mathbb{R} \setminus \mathbb{Q}$.

Definición. Sea F un cuerpo y E/F una extensión algebraica. El **polinomio mínimo** de F es el polinomio m mónico, y mínimo tal que $E = F[x]_{(m)}$.

Lema 80. Sean f y g polinomios distintos sobre un cuerpo F . Entonces f y g son coprimos sí y solo sí no tienen una raíz en común. Mas aún, si f y g son mónicos y irreducibles, entonces no tienen raíz en común en ninguna extensión de F .

demostración. Suponga que $(f, g) = c$, donde $c(x)$ es constante. Entonces existen $a, b \in F[x]$ tales que

$$a(x)f(x) + b(x)g(x) = c(x)$$

Si α es raíz común, obtendríamos que $c(\alpha) = 0$, lo que no puede pasar.

Por otro lado, sea $(f, g) = d$ y $d(x)$ no constante. Entonces existe una extensión E/F con una raíz α de $d(x)$. Por definición, tenemos que α es raíz común de f y g .

Ahora, suponga que f y g son mónicos y irreducibles. Suponga que $(f, g) = d$, con $d(x)$ no constante. Entonces $f(x) = f'(x)d(x)$ y $g(x) = g'(x)d(x)$. Como f y g son irreducibles, entonces f' y g' son constantes, así que tenemos que

$$d(x) = \frac{f}{f'}(x) = \frac{g}{g'}(x)$$

Y $f = \frac{f'}{g'}g$. Como f y g son mónicos, $\frac{f'}{g'} = 1$ lo que lleva a $f = g$, una contradicción. ■

Definición. Sea E/F una extensión y $\alpha \in E$ una raíz de un $f \in F[x]$. Llamamos a $F(\alpha)$, mas pequeño que contiene a F y a α el **cuerpo generado** por F y α .

Lema 81. Sea F un cuerpo y $\alpha \in E$ una raíz de $f \in F[x]$, donde E/F es extensión. Entonces $F(\alpha)$ es el cuerpo de fracciones de $F[x]$.

Teorema 82. Sea α algebraico sobre F , y $m(x)$ el polinomio mínimo de α sobre F , con $\deg m = n$. Si $f(x)$ es un polinomio sobre F , con $\deg f \leq n - 1$, entonces m y f son coprimos y f es invertible.

Corolario. Sea $F_{n-1}[\alpha]$ el conjunto de polinomios en α con grado a lo sumo $n - 1$. Entonces $F_{n-1}[\alpha]$ es un cuerpo.

Corolario. $F(\alpha) = F_{n-1}[\alpha]$

Corolario. La extensión $F(\alpha)/F$ tiene grado $[F(\alpha) : F] = n$, con base $\{1, \alpha, \dots, \alpha^{n-1}\}$

Ejemplo 45. (1) Considere $\mathbb{F}_2[x]$ y sea $m(x) = x^3 + x + 1$. m es monico, y por el criterio de Eisenstein, es irreducible, así que es polinomio minimo de un α . Entonces $[\mathbb{F}_2(\alpha) : \mathbb{F}_2] = 3$ y tenemos que

$$\mathbb{F}_2(\alpha) = \{a_0 + a_1x + a_2x^2 : a_i \in \mathbb{F}_2 \text{ y } \alpha^3 = \alpha + 1\}$$

y $\mathbb{F}_2(\alpha)$ tiene 8 elementos. Lo escribimos como

$$\mathbb{F}_8 = \mathbb{F}_2(\alpha) = \mathbb{F}_2[x]/(m)$$

(2) Sea ξ la quinta raíz unitaria primitiva, es decir que $\xi^5 = 1$, y $\xi^k \neq 1$ para todo $1 \leq k \leq 4$. Tenemos que $\xi \in \mathbb{Q}(\xi)$ y ξ es algebraico sobre \mathbb{Q} con polinomio minimo $x^4 + x^3 + x^2 + x + 1$; note que $x^5 - 1 = (x - 1)(x^4 + x^3 + x^2 + x + 1)$. Entonces $[\mathbb{Q}(\xi) : \mathbb{Q}] = 4$ y tiene un infinitud de elementos.

Lema 83. Considere la torre de extensiones $E-K-F$. Entonces si $\{\alpha_i\}$ es base para E/K , y $\{\beta_j\}$ es base para K/F , entonces $\{\alpha_i\beta_j\}$ es base para E/F .

demostración. Sea $\gamma \in E/K$. Entonces $\gamma = \sum a_i \alpha_i = \sum (\sum b_{ij} \beta_j) \alpha_i$, así que $\text{span} \{\alpha_i \beta_j\} = E$. Ahora, suponga que

$$\sum \lambda_{ij} \alpha_i \beta_j = 0$$

entonces $\sum \lambda_{ij} \beta_j = 0$, y como $\{\beta_j\}$ es base, entonces $\lambda_{ij} = 0$ para todo i y j . Por lo tanto $\{\alpha_i \beta_j\}$ es base de E/F . ■

Corolario. $[E : F] = [E : K][K : F]$. Es decir el grado de extensiones es multiplicativo.

demostración. Como $\{\alpha_i \beta_j\}$ es base de E/F , entonces si $[E : K] = m$ y $[K : F] = n$, entonces $[E : F] = mn = [E : K][K : F]$. ■

Lectura 20: Cuerpos de Descomposición

Lema 84. Si f es un polinomio con grado $\deg f = n$, entonces f tiene un cuerpo de descomposición K sobre F tal que $[K : F] \leq n!$.

demostración. Asumamos que $n \geq 1$. Entonces f tiene al menos una raíz α_1 . Como $f(\alpha_1) = 0$, entonces el polinomio minimo de α_1 , m_1 divide a f ; es decir, que $f(x) = m_1(x)f_1(x)$ para algún $f_1 \in F[x]$. Como $\deg m_1 \leq n$, tenemos que $[F(\alpha_1) : F] \leq n$.

Ahora, escribe $f(x) = (x - \alpha_1)^{r_1} g(x)$, donde $g \neq 0$ y $\deg g \leq n - 1$. Si g es constante, terminamos. Al contrario, sea α_2 raíz de g , entonces es raíz de f . Sea m_2 el polinomio

minimo de α_2 , entonces $m_2|g$, es decir, $g(x) = m(x)g_2(x)$, y como $\deg m_2 \leq n - 1$, tenemos que $[F(\alpha_1, \alpha_2) : F] \leq n(n - 1)$.

Siguiendo este proceso, sea $\alpha_1, \dots, \alpha_m$ raíces de f , entonces $f(x) = (x - \alpha_1)^{r_1} \dots (x - \alpha_m)^{r_m}$ y tiene cuerpo de descomposición $F(\alpha_1, \dots, \alpha_m)$ con $[F(\alpha_1, \dots, \alpha_m) : F] \leq n!$. ■

Teorema 85. *Sí α y β son raíces de un polinomio irreducible $f \in F[x]$ en una extensión E , entonces $F(\alpha) \simeq F(\beta)$. Es decir los cuerpos de descomposición son únicos hasta el isomorfismo.*

demostración. Suponga que f es mónico. Como $f(\alpha) = f(\beta) = 0$, tenemos que f es polinomio minimo de α y de β . Digamos que $\deg f = n$, sí $a_1 F(\alpha)$, entonces tenemos

$$a = a_0 + a_1\alpha + \dots + a_{n-1}\alpha^{n-1}$$

Pues, considere el mapa $a \rightarrow b$, donde

$$b = b_0 + b_1\beta + \dots + b_{n-1}\beta^{n-1}$$

que es un isomorfismo entre $F(\alpha)$ y $F(\beta)$. ■

Ejemplo 46. (1) Sea $x^3 - 2 \in \mathbb{Q}[x]$ con raíz $\sqrt[3]{2}, \xi\sqrt[3]{2}$, y $\xi^2\sqrt[3]{2}$, donde $\xi^3 = 1$. Entonces el cuerpo de descomposición de $x^3 - 2$ sobre \mathbb{Q} es $\mathbb{Q}(\sqrt[3]{2}, i\sqrt{3})$ con $[\mathbb{Q}(\sqrt[3]{2}, i\sqrt{3})] = 6 = 3!$. Aquí ξ es la tercera raíz unitario primitiva.

Lectura 21: Clausuras Algebraicas.

Definición. Sí E y K son extensiones de F y $\iota : E \rightarrow K$ es una homomorfismo, entonces decimos que ι es un **F -homomorfismo** sí $\iota(a) = a$ para todo $a \in F$. Es decir que $\iota|_F$ es una inclusión. Sí ι es un isomorfismo, entonces llamamos a ι un **F -isomorfismo**.

Lema 86. *Sí C es un cuerpo, las siguientes enunciados son equivalentes.*

- (1) *Todo polinomio no constante sobre C tiene al menos una raíz en C .*
- (2) *Todo polinomio no constante sobre C se descompone sobre C .*
- (3) *Todo polinomio irreducible en C tiene $\deg = 1$.*
- (4) *C no tiene extensión algebraica propia.*

Definición. Un cuerpo que satisface uno de los enunciados de lemma 86 se llama **algebraicamente cerrado**. Sí F es un cuerpo, entonces llamamos el cuerpo mas pequeño C que contine a F , y que sea algebraicamente cerrado la **clausura algebraica** de F , y lo denotamos como $C = \text{cl } F$ ó $C = \overline{F}$.

Ejemplo 47. (1) \mathbb{R} no es algebraicamente cerrado. Note que el polinomio $x^2 + 1$ no tiene raíces en \mathbb{R} .

(2) Los numeros complejos \mathbb{C} son algebraicamente cerrado. De hecho, $\mathbb{C} = \text{cl } \mathbb{R}$.

(3) Todo cuerpo finito \mathbb{F}_n no es algebraicamente cerrado. Escoje el polinomio $(x - \alpha_1)(x - \alpha_2) \dots (x - \alpha_n) + 1$, lo cual no tiene raíces.

Teorema 87. Las siguientes enunciados son ciertos.

(1) Todo cuerpo F tiene clausura algebraica.

(2) Cualquiera dos clausuras de F , C y C' son F -isomorfos.

(3) Sí E es una extensión de F , C la clausura algebraica de F , y $i : F \rightarrow C$ un encrustamiento, entonces i se puede extender a un encrustamiento de $E \rightarrow C$. A nivel de categorias, es decir, la siguiente diagrama commuta.

$$\begin{array}{ccc} E & \xrightarrow{\hat{i}} & C/F \\ \uparrow j & & \nearrow i \\ F & & \end{array}$$

donde $j : F \rightarrow E$ es una inclusión.

Lema 88. Sí E y K son extensiones de un cuerpo F , y E es algebraico sobre K , y K algebraica sobre F , entonces, E es algebraico sobre F . Mas aún, sí E es generado sobre F por una cantidad finita de elementos algebraicos sobre F entonces E es extensión algebraica.

demostración. Sea $E_0 = F$, $E_k = F(\alpha_1, \dots, \alpha_k)$ para todo $1 \leq k \leq n$, donde $\alpha_1, \dots, \alpha_n$ son elementos algebraicos sobre F ; y, por lo tanto, sobre E_{k-1} . Nota, que $[E_k : E_{k-1}] = \deg m_k$, donde m_k es el polinomio minimo de α_k sobre E_{k-1} , lo cual es finito. Por lo tanto, tenemos que

$$[E : F] = \prod [E_k : E_{k-1}]$$

es finito. Por lo tanto, E tiene que ser algebraico sobre F .

Ahora, sea $\alpha \in E$ con polinomio minimo

$$m(x) = b_0 + b_1x + \cdots + b_{n-1}x^{n-1} + x^n$$

los coeficientes b_0, \dots, b_{n-1} son algebraicas sobre F . Sea

$$L = F(b_0, \dots, b_{n-1})$$

por lo demostrado anteriormente. L es una extensión finita y por lo tanto es algebraico sobre F . Es decir que $m \in L[x]$ es algebraico sobre L y $L(\alpha)$ es extensión finita de L . Como $[L(\alpha) : L]$ y $[L : F]$ son finitas, entonces

$$[L(\alpha) : F] = [L(\alpha) : L][L : F]$$

es finita, lo que hace $L(\alpha)$ algebraico sobre F . En particular, α es algebraico sobre F , lo que hace E algebraico sobre F . ■

Corolario. *Sí E es una extensión de F y A consiste de todos los elementos de E que son algebraicos sobre F , entonces A es un subcuerpo de E .*

Lectura 22: Separabilidad.

Definición. Sea F un cuerpo. Un polinomio $f \in F[x]$ irreducible es **separable** sí f no tiene raíces repetidas. Sí f no es irreducible, entonces es **separable** si todo sus factores irreducibles son separables.

Ejemplo 48. $f(x) = (x-1)^2(x-2)(x^2+1)$ es separable sobre \mathbb{Q} .

Definición. Sea F un cuerpo y $f \in F[x]$ de la forma $f(x) = a_0 + a_1x + \cdots + a_nx^n$. Definimos la **derivada** de f de ser el polinomio $Df \in F[x]$, con la forma

$$Df(x) = a_1 + 2a_2x + \cdots + na_nx^{n-1}$$

La derivada tambien lo denotamos $f'(x)$.

Lema 89. *Sea F un cuerpo, y considere el polinomio $f \in F[x]$, junto a su derivada Df . Entonces f tiene al menos una raice repetida en su cuerpo de descomopsición sí y solo sí $\deg(f, Df) \geq 1$, donde (f, Df) es le maximum común divisor de f y Df .*

demostración. Suponga que f tiene una raíz repetida α . Entonces $f(x) = (x - \alpha)^r h(x)$, donde $r \geq 2$. Entonces su derivada tiene la forma

$$Df(x) = r(x - \alpha)^{r-1}h(x) + (x - \alpha)^r Dh(x)$$

como $r - 1 \geq 1$, entonces α es raíz de Df y $(x - \alpha)^{r-1} | Df$. Por lo tanto, $\deg(f, Df) \geq r - 1 \geq 1$.

Recíprocamente, suponga que $\deg(f, Df) \geq 1$. Sea α raíz de (f, Df) . Por definición, tenemos que $(f, Df) | f$ y $(f, Df) | Df$; mas aún $(x - \alpha) | (f, Df)$, por lo tanto, α es raíz de f y de Df , por lo tanto, es raíz repetida de f por el argumento de arriba. ■

Corolario. *Las siguientes enunciados son ciertos.*

- (1) *Todo polinomio es separable sobre un cuerpo de característica $\text{char} = 0$.*
- (2) *Sobre todo cuerpo de $\text{char} = p$, p primo, un polinomio irreducible es inseparable sí y solo sí $Df = 0$.*

demostración. Suponga, que f es irreducible sobre $F[x]$, donde $\text{char } F = 0$. Si f es un polinomio de $\deg f = n$, entonces $\deg Df = n - 1$. Como f es irreducible, entonces (f, Df) es constante ó f . Pero $(f, Df) = f$ es imposible, por lo tanto (f, Df) es constante y f no tiene raíces repetidas. Por lo tanto es separable.

Suponga ahora que $\text{char } F = p$, con p primo. Suponga que $f \in F[x]$ es irreducible de grado $\deg f = n$. Si $Df \neq 0$ podemos usar el mismo argumento del lemma 89. Ahora, si $Df = 0$ entonces tenemos que $(f, Df) = p \equiv 0 \pmod{p}$. Por lemma 89, tenemos que f tiene raíces repetidas, y como f es irreducible, esto hace a f inseparable. ■

Lema 90 (El Automorfismo de Frobenius). *Sea F un cuerpo finito de $\text{char } F = p$. Considere el mapa de $F \rightarrow F$ dado por $\alpha \rightarrow \alpha^p$. Entonces esta mapa es un automorfismo. En particular, para todo $\alpha \in F$, existe una $\beta \in F$ con $\alpha = \beta^p$.*

demostración. Nota que $1 \rightarrow 1^p = 1$. Mas aún $(\alpha + \beta) \rightarrow (\alpha + \beta)^p = \alpha^p + \beta^p$ y $(\alpha\beta) \rightarrow (\alpha\beta)^p = \alpha^p\beta^p$. Mas aún, nota, que por definición, que la mapa $\alpha \rightarrow \alpha^p$ es sobre. Ahora, si $\alpha^p = \beta^p$, entonces $\alpha^p - \beta^p = (\alpha - \beta)^p = 0$, lo que hace $\alpha = \beta$, y la mapa es 1-1. ■

Definición. Sea F un cuerpo finito de $\text{char } F = p$. Llamamos a la mapa de $F \rightarrow F$ dado por $\alpha \rightarrow \alpha^p$ el **automorfismo de Frobenius**.

Lema 91. *Todo polinomio es separable sobre un cuerpo finito.*

demostración. Sea F un cuerpo finito con $\text{char } F = p$, y sea $f \in F[x]$ irreducible, que, por contradicción, tiene raíces repetidas. Entonces nota que $f \in F[x^p]$, y $f(x) = a_0 + a_1x^p + \cdots + a_nx^{np}$. Ahora, por el automorfismo de Frobenius, tenemos que $f(x) = \beta^p$ para algún $\beta \in F$. Es decir que $a_0 + a_1x^p + \cdots + a_nx^{np} = b_0^p + b_1^px^p + \cdots + b_n^px^{np} = (b_0 + b_1x + \cdots + b_nx^n)^p$ lo que dice que f no es irreducible; una contradicción. Por lo tanto, f no puede tener raíces repetidas, y como es irreducible, esto lo hace separable. ■

Definición. Si E/F es una extensión, llamamos a un $\alpha \in E$ **separable** si su polinomio mínimo es separable. Si todo elemento de E es separable, entonces llamamos a E **separable** sobre F .

Lema 92. Si tenemos la torre de extensiones $E-K-F$, y E es separable sobre F , entonces K es separable sobre F y E es separable sobre K .

demostración. Nota que como E es separable sobre F y $K \subseteq E$, pues K es separable sobre F . Toma, $\alpha \in E$. Como E/F es separable, entonces α es algebraico. Sea μ el polinomio mínimo de α sobre F , y η lo mismo sobre K . Entonces $\mu(\alpha) = \eta(\alpha) = 0$, y $\mu|\eta$. Como η es el mínimo de E sobre K , y μ es separable, entonces η también es separable; de lo contrario, μ teniendo raíces repetidas implica raíces repetidas en η . Como η es separable, esto hace E/K separable. ■

Ejemplo 49. Considere el cuerpo $\mathbb{F}_p(t)$. Note que $\text{char } \mathbb{F}_p(t) = p$, pero que $\mathbb{F}_p(t)$ es infinito. Considere $\mathbb{F}_p(t, \alpha)$, donde α es raíz del polinomio $x^p - t \in \mathbb{F}_p(t)[x]$. Note que $x^p - t = x^p - \alpha^p = (x - \alpha)^p$ y $x^p - t$ tiene raíces repetidas. Mas aún, como $x^p - t$ es irreducible por el criterio de Eisenstein, esto hace a $F(t, \alpha)$ inseparable sobre $\mathbb{F}_p(t)$. De hecho, $\mathbb{F}_p(t)$ es inseparable sobre \mathbb{F}_p .

Lema 93 (Galois). Sea E un extensión de un cuerpo F y sea $\sigma : E \rightarrow E$ un F -homomorfismo 1-1. Suponga que $f \in F[x]$ se descomponga en $E[x]$. Entonces σ permuta a las raíces de f .

demostración. Sea que $f(x) = a_0 + a_1x + \cdots + a_nx^n$ y sea α raíz de f . Nota que $f(\alpha) = 0 = a_0 + a_1\alpha + \cdots + a_n\alpha^n$. Pues, nota que $\sigma(f(\alpha)) = (0) = 0 = \sigma(a_0) + \sigma(a_1)\sigma(\alpha) + \cdots + \sigma(a_n)\sigma(\alpha)^n = a_0 + a_1\sigma(\alpha) + \cdots + a_n\sigma(\alpha)^n$, lo que hace $\sigma(\alpha)$ raíz de f . ■