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

09.11.2022

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 $a, b \in G$, entoces 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 funciónes 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 funciónes, $\circ$. Si S tiene n elementos, entonces exscribimos $A(S) = S_n$. $A(S)$ también no se Abeliano ya que para funciónes cualquieras f, g, $f \circ g \neq g \circ f$.

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

Definición. Sea G un grupo, y $a \in G$. El **orden** de a, denotado $\operatorname{ord} a$, es el menor entero positivo n tal que $a^n = e$ y escribimos $\operatorname{ord} a - n$. 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 $\mathbb{C}^* = \mathbb{C} \backslash 0$, 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 $\operatorname{ord} \alpha = 5$.

(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 $\mathbb{R}^* = \mathbb{R} \backslash 0$, $\mathbb{R}^*$ es infinito, y $\operatorname{ord} 2$ 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 opearación 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 funciónes $+$. Sea $C^1(\mathbb{R})$ el conjunto de funciónes 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 los funciones de arriba tambien 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, tambien tenemos qie $ea^{-1} = a^{-1} \in H$. 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 **cnetralizador** 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 $\phi : G \to H$ se llama un **homomorphismo** si para toda $a, b \in G$, $\phi(ab) = \phi(a)\phi(b)$. Si ϕ es $1-1$ y sobre, entonces lo llamamos un **isomorphismo**. Si ϕ es un isomorphismo, y $G = H$, entonces llamamos a ϕ un **automorphismo**.

Lectura 2: Grupos y Subgrupos

Ejemplo 5. (1) Considera $\mathbb{R}$ bajo la suma $+$ y $\mathbb{R}^+$ bajo la multiplicacón, $\cdot$. Sea $\phi : \mathbb{R} \to \mathbb{R}^+$ definido por $\phi : x \to \exp x$. 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 $\phi : GL(n, \mathbb{R}) \to \mathbb{R}^*$ dado por $\phi : A \to \det A$. Entonces ϕ es un homomorphismo ya que $\det AB = \det A \det B$. Nota que $GL(n, \mathbb{R})$ no es Abeliano, 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 $\phi : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ dado por $\phi(m) = m \mod n$. Entonces $\phi(m+k) = (m+k) \mod n \equiv m \mod n + k \mod n = \phi(m) + \phi(k)$. Así que ϕ es un homomorfismo.

(4) Sea G y H grupos, y sea $\phi : G \to H$ un homomorfismo de G sobre H. Entonces si G es Abeliano, 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 $\phi : \mathbb{Z} \to \mathbb{Z}$ dado por $x \to 5x$. Entonces $\phi(x+y) = 5(x+y) = 5x+5y = \phi(x)+\phi(y)$.

(6) Suponga que G es Abeliano y defina $\phi : G \to G$ 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 $\phi : \mathbb{Z} \to \mathbb{Z}$ dado por $x \to x^2$. ϕ no es un homomorfismo ya que en general, $(x+y)^2 \neq x^2 + y^2$. Peros, si tomamos la mapa $\psi : \mathbb{Z} \to \mathbb{Z}/2\mathbb{Z}$ dado por la misma regla, entonces ψ es un homomorfismo.

Definición. Sea G y H grupos, y $\phi : G \to H$ 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 identitad de H. Definimos también la **imagen** del homoorphismo como el conjunto $\Im\phi = \phi(G) = \{\phi(a) : a \in G\}$.

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

demostración. Nota por definicion qiue $\ker \phi \subseteq G$. Tambien tenemos que $e \in \ker \phi$ por el ley de homomorpfismo. 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 $\phi : \mathbb{Z} \to \mathbb{Z}/12\mathbb{Z}$ dado por $m \to m \mod 12$. Entonces $\ker \phi = \langle 12m \rangle = 12\mathbb{Z}$. Tambien $\phi(\mathbb{Z}) = \mathbb{Z}/12\mathbb{Z}$; pues ϕ es sobre.

(2) Considere $\phi : \mathbb{Z}/12\mathbb{Z} \to \mathbb{Z}/12\mathbb{Z}$ dado por $m \to 3m$. 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 $\phi : \mathbb{Z} \to \mathbb{Z}$ dado por $m \to 5m$. 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 polygano regular de n-vertices. Recuerda que $r^n = t^2 = e$ y que $tr^j = r^{n-j}t$. Considere la homomorfismo $\phi : D_8 \to \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, 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 $\langle a \rangle = \{aj : j \in \mathbb{Z}\}$. Llamamos a a el **generador** del grupo. Si $G = \langle a \rangle$ para algun $a \in G$, entonces decimos que G es **cíclico**.

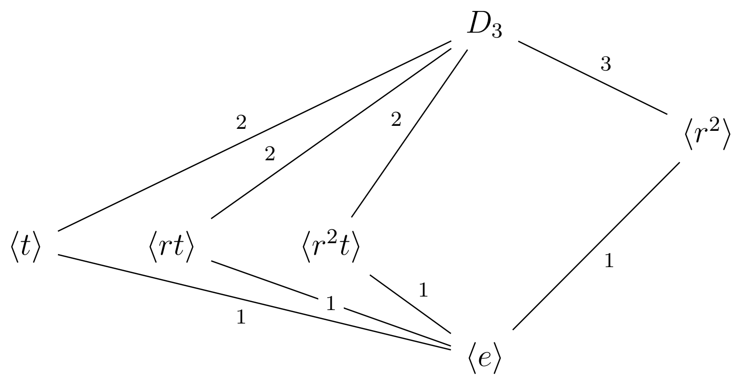
Ejemplo 7. (1) Considere el grupo $\langle A \rangle$, donde

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

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

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

ientes en la reticulo de subgrupos sigueinte 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 peqeño, 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 $a^k = a^{qm+r} = a^{qm} a^r i = (a^m)^q a^r$. Como $a^k \in H$, y $a^m \in H$, es necesario tener $(a^m)^q a^r \in H$ 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 $\operatorname{ord} G = n$ 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 $\operatorname{ord} a^k = d$, lo cual dice que $\operatorname{ord} \langle a^k \rangle = d$. ■

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 $\operatorname{ord} U(\mathbb{Z}/_{18\mathbb{Z}}) = \operatorname{ord} \langle 5 \rangle = 6$. Entonces $U(\mathbb{Z}/_{18\mathbb{Z}})$

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

$$\begin{tikzcd}
& U(\mathbb{Z}/18\mathbb{Z}) \arrow[dl, dash, "3"'] \arrow[dd, dash, "1"] \arrow[dr, dash, "3"] & \\
\langle 7\rangle \arrow[dr, dash, "1"'] & & \langle 17\rangle \arrow[dl, dash, "1"] \\
& \langle 1\rangle &
\end{tikzcd}$$

(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:

$$\begin{tikzcd}
& U(\mathbb{Z}/18\mathbb{Z}) \arrow[dl, dash] \arrow[ddd, dash] \arrow[dr, dash] & \\
\langle 9\rangle \arrow[d, dash] & & \langle 7\rangle \arrow[d, dash] \\
\langle 11\rangle \arrow[dr, dash] & & \langle 49\rangle \arrow[dl, dash] \\
& \langle 1\rangle &
\end{tikzcd}$$

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* $\operatorname{ord} a = n$*, entonces $i \equiv j \mod n$.*

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

Corolario. *Sí $G = \langle a\rangle$, y $\operatorname{ord} G = \operatorname{ord}\langle a\rangle = n$, 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 $(j,n)=1$. Es decir, los generadores son:

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

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 $\phi : G \to \mathbb{Z}$ dado por $a^j \to j$. 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 isomprfismo entre G y $\mathbb{Z}$.

De igaul forma, suponga que $\operatorname{ord} G = n$. Nota entonces que G tiene la forma $G = \{a^j : j \in \mathbb{Z}/_{n\mathbb{Z}}\}$. Define entonces $\phi : G \to \mathbb{Z}/_{n\mathbb{Z}}$ dado por $a^j \to j \mod n$. ϕ es un homomorfismo de G sobre $\mathbb{Z}/_{n\mathbb{Z}}$, por definición. ϕ tambien es 1–1 ya que $a^i = a^j$ implica $i \equiv j \mod n$. 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 $\operatorname{ord}\langle i \rangle = \operatorname{ord} i = 4$. Por la teorema anterior, esto hace $\langle i \rangle \simeq \mathbb{Z}/_{4\mathbb{Z}}$.

Definición. Sea G un grupo y $H \leq G$. Sí $a \in G$ 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: $a \equiv b$ sí y solo sí $ab^{-1} \in H$. Llamamos a $\equiv$ **congruencia modulo** H. Escribimos $a \equiv b \mod H$, ó simplements $a \equiv_H b$.

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

Corolario. *Los clases de equivalencia de $\equiv_H$ sobre G son precisamente los clases laterales por la izquierda aH.*

demostración. Exercise. ■

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

demostración. Considere la mapa $f : H \to aH$ dado por la regla $h \to ah$. A todo $ah \in H$ 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 del los clases laterales por la derecha de H en G.*

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

Definición. Sea G un grupo y $H \leq G$. Definimos el **indice** 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*

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

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

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

Nota que $|J| = [G : H]$. ■

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

Lectura 4: Gurpos 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 **noraml** 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 forza 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 notmal de* G*, entonces las clases laterales de* H *en* G *forman un grupo bajo el producto de clases.*

demostración. Define la operación $(aH, bH) \to aHbH = \{ahbh' : h, h' \in H\} = abH$. 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 tambien que $aH(bHcH) = aH(bcH) = a(bc)H = abcH = (ab)cH = abHcH - (aHbH)cH$, así que el producto es associativa.

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 todos 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 $\phi : G \to {}^{G}\!/_{H}$ tal que $\phi : a \to aH$. 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 arbitraros, 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 $\phi : G \to G'$ un homomorfismo. Entonces tenemos que Si $H \trianglelefteq G$ y ϕ es sobre, entonces $\phi(H) \trianglelefteq G'$. Mas aún sí $H' \trianglelefteq G'$, entonces $\phi^{-1}(H') \trianglelefteq G$.*

demostración. Sea $\phi : G \to G'$ 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 $xhx^{-1} = \phi(a')\phi h\phi^{-1}(a') = \phi(a'ha'^{-1}) \in \phi^{-1}(H')$. 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 $H \trianglelefteq H$. Sea $\phi : G \to G'$ y $\pi : G \to {}^{G}\!/_{H}$ dado por $\pi : a \to aH$. Enotnces existe un uúnico $\tilde{\phi} : {}^{G}\!/_{H} \to G'$ tal que $\phi = \tilde{\phi} \circ \pi$.*

$$\begin{tikzcd}
G \arrow[r, "\phi"] \arrow[d, "\pi"'] & G' \\
{}^{G}\!/_{H} \arrow[ur, dashed, "\tilde{\phi}"'] &
\end{tikzcd}$$

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

Ahora define la mapa $\tilde{\phi} : {}^{G}\!/_{H} \to G'$ dado por $aH \to \phi(a)$. Sea entonce$_3$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 sý y solo sí $\tilde{\phi}$ es sobre, y ϕ es 1–1 sí y solo sí $\ker \phi = H$.*

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

Ahora sí $\ker \phi = H$, como H es identidad del ${}^{G}\!/_{H}$, entonces ϕ es 1–1. Por el otro lado, sí 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 Isomorphismo)**.** *Sí $\phi : G \to H$ es un homomorfismo con kernel K, entonces*

$$\phi(G) \simeq {}^{H}\!/_{K}$$

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

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

Definición. Sea $\{G_n\}$ una colección de grupos, y $\{\phi_n\}$ una colección de homomorfismos de $G_i \to G_{i+1}$. Llamamos la secuencia $\to G_1 \xrightarrow{\phi_1} G_2 \xrightarrow{\phi_2} \ldots \xrightarrow{\phi_{n-1}} G_n \xrightarrow{\phi_n} \ldots$ 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 $i : \langle e \rangle \to G_1$ es la inclusión y $j : G_3 \to \langle e \rangle$ es la constante dado por $j : g \to e$ 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 $\phi_2 : G_1 \to G_3$, 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 Isomorphismo)**.** *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 Isomorphismo)**.** *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 q ue $(\mathbb{Z}/8\mathbb{Z})/(4\mathbb{Z}/8\mathbb{Z}) \simeq \mathbb{Z}/4\mathbb{Z}$, con acuerdo a la tercer teorema del isomorfismo.

Teorema 18 (Teorema de la Correspondencia)**.** *Sea $\phi : G \to G'$ 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 $\phi(a), \phi(a) \in H'$, así que $\phi(ab^{-1}) \in H'$, lo que hace $ab^{-1} \in H$. Por lo tanto $H \leq G$. Tambi$n$ tenemos que $\phi(K) = \langle e' \rangle$, lo que hace $K \trianglelefteq H$.

Ahora considere la mapa $\phi' : H \to H'$ dado por $\phi' : h \to \phi(h)$. 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 $h \in H$, entonce 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 $\phi : \mathbb{Z} \to \mathbb{Z}/24\mathbb{Z}$. 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 repreduce 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.

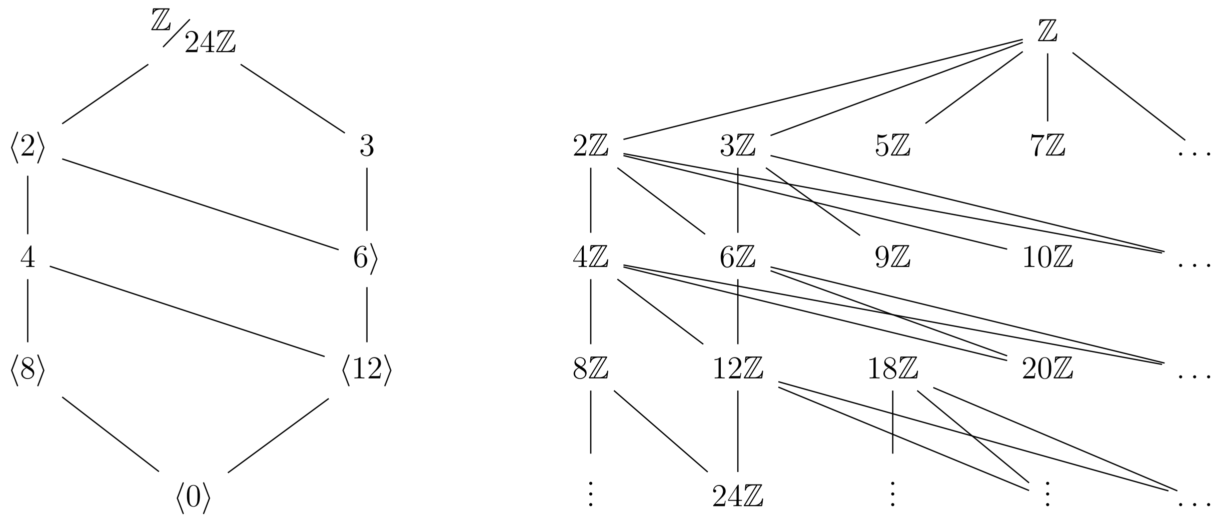


Figure 1: El reticulo de subgrupos de $\mathbb{Z}/24\mathbb{Z}$ al lado del reticulo de subgrupos de $\mathbb{Z}$.

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 $((a,b),(g,h)) \to (ah, bg)$.

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, $\pi : G \times H \to G$ y $\pi_2 : G \times H \to H$ dados por $\pi_1 : (g, e_H) \to g$ y $\pi_2 : (e_G, h) \to h$. 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:

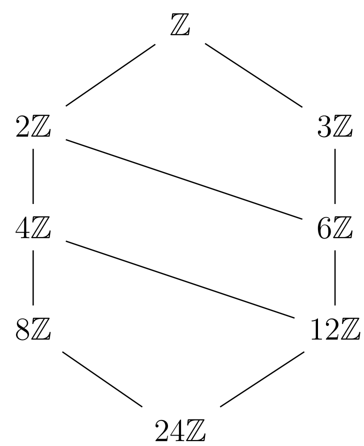


Figure 2: $\mathbb{Z}/_{24\mathbb{Z}}$ como subreticulo del reticulo de $\mathbb{Z}$.

(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 $\phi : H \times K \to HK$ pro $(h, k) \to hk$. 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 contienes 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 sigueintes 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 $g = h_1 \dots h_i - 1e_i e_{i+1} \dots e_n$. 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 $(h_1^{-1} k_1) \dots (h_{n-1}^{-1} k_{n-1}) = h_n k k_n^{-1}$, y comoe $h_n k_n^{-1} \in H_n \cap (H_1 \dots H_{n-1})$, 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 ord $\langle r \rangle = 3$ y ord $\langle t \rangle = 2$, pero D_3 no es abeliano, asi 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 $\operatorname{Aut} G$ el **grupo de automorfismos** de G sobre si mismo.

Lema 23. *Sean H, K grupos, y sea $r : K \to \operatorname{Aut} H$ dado por $k \xrightarrow{r} r_k$ y $r_k : H \to H$ es un autmorfismo de H. Considere la operacion bianria $(H \times K) \times (H \times K) \to H \times K$ dado por $(h_1, k_1), (h_2, k_2) \to (h_1 r_k(h_2), k_1 k_2)$. 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 $r(kn) = r_{kn} = r_k r_n = r(k) r(n)$, as i 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. Aís que $e = (e_H, e_K)$ es la identidad.

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

Finalmente, nota que

$$\begin{aligned}((h_1,k_1)(h_2,k_2))(h_3,k_3) &= (h_1 r_{k_1}(h_2), k_1k_2)(h_3,k_3)\\ &= ((h_1 r_{k_1}(h_2)) r_{k_3}(h_3), k_1k_2k_3)\\ &= (h_1h_2 r_{k_1k_3}(h_2h_3), k_1k_2, k_3)\end{aligned}$$

$$\begin{aligned}(h_1,k_1)((h_2,k_2)(h_3,k_3)) &= (h_1,k_1)(h_2 r_{k_3}(h_3), k_2k_3)\\ &= (h_1h_2 r_{k_1k_3}(h_2h_3), k_1k_2k_3)\end{aligned}$$

y associatividad se preserva. ■

Definición. Sea H, K grupos, y $r : K \to \operatorname{Aut} H$ un homomorfismo. Definimos el **producto semidirecto externo** de ser el grupo $H \times_r K$ bajo la operación $(h_1,k_1)(h_2,k_2) = (h_1 r_{k_1}(h_2), k_1k_2)$.

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 $r : x \to -x$. 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, $(h, e_K)(e_H, k) = (hr_{e_H}(e_H), e_K k) = (he_H, e_K, k) = (h, k)$, 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 $r : K \to \operatorname{Aut} H$ esta dado por $r_k : h \to khk^{-1}$.*

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 $\phi : H \times_r K \to G$ dado por $(h,k) \to hk$. Vemos que ϕ es 1–1, y que es sobre.

Ahora dado (h,k) y (h',k'), tenemos que $\phi((h,k)(h',k')) = \phi(hr_k(h'), kk') = \phi(hkhk^{-1}, kk') = (hkh'k^{-1})(kk') = (hk)(h'k') = \phi(h,k)\phi(h',k')$. Por lo tanto ϕ es un ismomorfismo y termianmos. ■

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. Defnia $\lambda : G \to A(G)$ dado por $g \to \lambda_g$, donde $\lambda_g : G \to G$ esta dado por $x \to gx$. 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 que $\lambda(g) = \lambda(h)$, entonces para algún $x \in G$, $\lambda_g(x) = \lambda_g(h)$, pues $gx - gh$. Por cancelación, tenemos que $g = h$. sí que λ es 1–1. Ahora dado $x \in G$, que $(gh)(x) = \lambda_{gh}(x) = (gh)x = g(hx) = g({}_h(x)) = \lambda_g(\lambda_h(x)) = \lambda_G \lambda_h(x)$. 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 $G \times X \to X$ dado por $(g, x) \to g \cdot x$ 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 $(g, x) \to gxg^{-1}$. 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 $G \times X \to X$ 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 $= \{g \in G : gx = xg$ para todo $x \in G\}$. Llamamos este kernel el **centro** de G, y lo denotamos como $Z(G)$.

(2) Conisdere $\mathcal{B}_n$ el conjunto de todos funciones booleanas $f : \mathbb{F}_2^n \to \mathbb{F}_2^n$ en n variables. Defina una operacion de S_n sobre $\mathcal{B}_n$ definida por $s \cdot f(x_1, \ldots, x_n) = f(x_{s(1)}, \ldots, x_{s(n)})$. Este operación defina una acción de grupos de S_n sobre $\mathcal{B}_n$. Nota que el kernel de este accion es trivial.

Definición. Sea G un grupo que actua sobre un conjunto X. La **órbita** 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 multiplicacion (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 conjugacion. Sea $x \in G$. Entonces $\mathcal{O}(x) = \{gxg^{-1} : g \in G\} = \operatorname{cl} x$. Llamamos a $\operatorname{cl} x$ la **clase de conjugacion** de x.

(3) Considere $\mathcal{B}_3$ y defina $f(x_1, x_2, x_3) = x_1 + x_2x_3 + x_1x_2x_3$. Sea $S_3 = \{(1), (2\,3), (1\,2), (1\,2\,3), (1\,3\,2), (1\,3)$ Entonces:

$$
\begin{aligned}
(1) \cdot f &= x_1 + x_2x_3 + x_1x_2x_3 = f \\
(2\ 3) \cdot f &= x_1 + x_3x_2 + x_1x_3x_2 = f \\
(1\ 2) \cdot f &= x_2 + x_1x_3 + x_2x_1x_3 = f_1 \\
(1\ 2\ 3) \cdot f &= x_2 + x_3x_1 + x_3x_2x_1 = f_1 \\
(1\ 3\ 2) \cdot f &= x_3 + x_1x_2 + x_3x_1x_2 = f_2 \\
(1\ 3) \cdot f &= x_3 + x_2x_1 + x_3x_2x_1 = f_2
\end{aligned}
$$

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

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

demostración. 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 $\mathcal{O}(y) = \mathcal{O}(y)$. ∎

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

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

demostración. Sea $x \in X$ y sea $g, h \in \operatorname{stab} x$. 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, $\operatorname{stab} x = \{g : gx = xg\} = C(x)$ 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 $\operatorname{stab} x$ la órbita y estabilizador de un $x \in X$. Entonces:*

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

demostración. Suponga que $y \in \mathcal{O}(x)$. Entonces $y = g \cdot x$ para algún $g \in G$. Defina ahora la mapa $f : \mathcal{O}(x) \to {}^{G}\!/_{\operatorname{stab} G}$ dado por $y = g \cdot x \to g \operatorname{stab} x$. Sea ahora $y = g \cdot x = h \cdot x$. Entonces vemos que $x = (g^{-1}h) \cdot x$, así que $g^{-1}h \in \operatorname{stab} x$. Esto hace que $g \operatorname{stab} x = h \operatorname{stab} x$. 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 $g \operatorname{stab} x$. Más aun, f es 1–1. Sean $y = gx$ y $y' = hx$. Sí $g \operatorname{stab} x = h \operatorname{stab} x$, entonces $g^{-1}h \in \operatorname{stab} x$, así que $gx = hx$, es decir $y = y'$. Por lo tanto, tenemos una mapa 1–1 de $\mathcal{O}(x)$ sobre el conjunto ${}^{G}\!/_{\operatorname{stab} x}$, que tiene cardinalidad $[G : \operatorname{stab} x]$. ■

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

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

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

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

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:*

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

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

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

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

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

Por el teorema del órbiata estabilizador, tenemos que

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

Rearreglando los terminos, tenemos el resultado. ■

Lectura 8: Las Teoremas de Sylow

Definición. Sea $p \in \mathbb{Z}^+$ un primo. Llamos 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 grupose $\mathbb{Z}/14\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ 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 $\operatorname{ord} P = p^r$.

Lema 31. *Sí G es u 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 maximo 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 $p \not| m$, entonces*

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

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

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

Mirando el coeficiente de x^{p^r}, en la izquierd, tenemos que este termino occure cuando $k = p^r(m-1)$, y obtenemeos $\binom{p^r m}{p^r} = \binom{n}{p^r}$. Por el lado derecho, el termino x^{p^r} occure cuando $k = m - 1$ y por simetria 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 $p \not| m$. Entonces existe al menos un p-subgrupo de Sylow, de G.*

demostración. Sea $X = \binom{G}{p^r}$. Note que G actua sobre X vá la multiplicacion por la izquierda. Ahora, este accion induce en X una particion de X en orbitas. Es decir

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

entonces $p \not| \sum |\mathcal{O}(S)|$. Por lo tanto, existe un $S \in X$ con $p \not| |\mathcal{O}(S)|$. Sea $P = \operatorname{stab} S$ Entonces por el teoream del órbita-estabilizador, tenemos

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

Como $p \not| |\mathcal{O}(S)|$, $\operatorname{ord} P$ tiene que ser un multiplo de p^r, es decir que $p^r | \operatorname{ord} P$, por lo tanto $p^r \leq \operatorname{ord} P$.

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

Ejemplo 27. Sea $GL(n, \mathbb{F}_p)$, y escoje una matriz $A \in GL(n, \mathbb{F}_p)$. Note que para la fila k de A, hay $p^n - p^k$ posubles entradas, asi que $\operatorname{ord} GL(n, \mathbb{F}_p) = p^n - p^k = p^{\frac{n(n-1)}{2}} p^j - 1$. 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 $p | \operatorname{ord} G$, 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 $\operatorname{ord} g = p^l$ para $l \in \mathbb{Z}^+$. Sí $l = 1$, terminamos, y sí $l > 1$, note que $(g^{pl-1})^p = g^{p^l} = e$. ■

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

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

demostración. Considere la mapa $f : H \times K \to HK$ dado por $(h,k) \to hk$. Entonces f es sobre y $\operatorname{ord} HK \leq |H \times K|$. 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 $|H \times K| = \operatorname{ord} H \operatorname{ord} K |H \cap K| = \operatorname{ord} HK |H \cap K|$. ■

Teorema 36 (El Segundo Teorema de Sylow)**.** *Sea G un grupo finito con orden $p^r m$ donde p es primo y $p \not| m$. Sea $n_p(G)$ el numero de todos los p-subgrupos de Sylow de G, entonces:*

$$n_p(G) \equiv 1 \mod p$$

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 ub p-Sylow de G, entonces por el teorema órbita-estabilizador, tenemos que

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

así que $|\mathcal{O}(Q)| | p^r$. As'ıque $\mathcal{O}(Q)$ 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 $p | \sum |\mathcal{O}(Q'')|$, por lo tanto

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

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

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

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

Teorema 37 (El Tercer Teorema de Sylow)**.** *Sea G un grupo finito con orden $p^r m$, donde p es primo y $p \not| m$. 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 actua sobre ${}^{G}\!/\!_{P}$ (no necesariamente el grupo cociente) mediante multiplicacion. Por el teorema de Lagrange, tenemos que $\operatorname{ord} {}^{G}\!/\!_{P} = [G : P] = \frac{p^r m}{p^r} = m$. Tambien nota que ${}^{G}\!/\!_{P} = \bigcup \mathcal{O}(gP)$, así que

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

y existe una orbita cuya longitud no esta dividido por p, como $p \not| m$. Por el teorema del órbita-establilizador, tenemos que $|\mathcal{O}(gP)| |\operatorname{ord} R = p^l$, 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 orbita 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. Ademas, tenemos que $n_p(G)|m$*

Lectura 9: Grupos Simples

Definición. Un grupo $G \neq \langle e \rangle$ es **simple** sí sus unicons 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 actue sobre si mismo via conjugacion. Las órbitas de este accion son las clases de conjugacion $\operatorname{cl} g$, donde $g \in P$. Tenemos que $x \in P$ esta en una clase de tamaño 1 sí y solo sí $x \in Z(P)$. Por el teorema del órbita-estabilizador, tenemos que el tamaño de los $\operatorname{cl} g$ divide a $\operatorname{ord} P = p^r$, donde $p, r \in \mathbb{Z}^+$ y p es primo.

Ahora, sí $Z(P) = \langle e \rangle$, entonces hay una sola órbita de tamaño 1. Entonces los demas $\operatorname{ord} \operatorname{cl} x | \operatorname{ord} P$. 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 $Z(P) \trianglelefteq P$. $\blacksquare$

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

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

demostración. Sí p es unico, entonces $\operatorname{ord} G = p^r$ 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, sí P es un p-Sylow de G, entonces $\langle e \rangle \leq P \leq G$, donde la segundo inclusión es estricta. Sí $n_p(G) = 1$, entonces $P \trianglelefteq G$, lo cual no puede pasar. Por lo tanto $n_p(G) > 1$. $\blacksquare$

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

(1) Sí $q \not\equiv 1 \mod p$, entonces G tiene un p-Sylow normal.

(2) Sí $q \not\equiv 1 \mod p$, y $p \not\equiv 1 \mod q$, entonces G es ciclico.

(3) G no es simple.

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

Ahora, suponga que $q \not\equiv 1 \mod p$ y $p \not\equiv 1 \mod q$. 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 $\operatorname{ord} P = p$ y $\operatorname{ord} Q = q$. 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 $p \not| q - 1$ y $q \not\equiv 1 \mod p$. Por arriba, G tiene un unico p-Sylow normal, lo que hace que G no sea simple. $\blacksquare$

Lema 42. *Sea G un grupo con noabeliano orden $p^2 q$ 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, $n_q(G) | p^2$ así que o $n_q(G) = p$ o $n_q(G) = p^2$. Sí $n_q(G) = p^2$, 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 $n_q(G) \equiv 1 \mod q$ y $p \equiv 1 \mod q$, lo que dice $p > q$. Peron $n_p(G)|q$ y como q es primo, entonces $n_p(G) = q$, luego, $n_p(G) \equiv 1 \mod p$ implica que $q \equiv 1 \mod p$ 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 $n_{11}(G) \equiv 1 \mod 11$, 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 $n_{29} \equiv 1 \mod 29$ 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 $\operatorname{ord} G \geq 2320 + 2464 > 2552$ una contradiccion. Así que G no es simple.

Lectura 10: El Teorema de Jordan-Hölder

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

$$G_n \trianglelefteq \cdots \trianglelefteq G_0$$

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 coleccion 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 $\langle e\langle >= G_n \trianglelefteq \cdots \trianglelefteq G_0 = G$. 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 $xgx^{-1} \in K$ y $xgx^{-1} \in G_{i+1}$, 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} so 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

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

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, entones 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 **characteristica** sí para cada automorfismo ϕ de G, $\phi(H) = H$; es decir que ϕ restringido a H es sobre. Escribimos $H \operatorname{char} G$

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

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

(2) Sí $H \operatorname{char} K$ 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 $H \operatorname{char} G$.

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

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

Lema 47. *El subgrupo commutador de un grupo verdaderamente es un subgrupo.*

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

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

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

(3) $G \big/ G'$ es abeliano.

(4) Sí $N \trianglelefteq G$, entonces ${}^{G}\!/\!_{N}$ es abeliano sí y solo sí $G' \leq N$.

demostración. (1) Sea $\phi \in \operatorname{Aut} G$, 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, sí $N \trianglelefteq G$ 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, sí $G' \leq N$, 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. *Sí 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 sí $[x,y] \in H'$, 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 $\langle e \rangle = G_n \trianglelefteq \cdots \trianglelefteq G_0 = G$ una **serie normal** sí para todo $0 \leq i \leq j \leq n$, tenemos $G_j G_i$.

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

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

Lema 50. *Todo grupo abeliano es resoluble.*

demostración. Por supuesto, sí G es un grupo abeliano, entonces $G' = \langle e \rangle$ lo cuale 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 sí G es ciclico de orden p, p un primo.*

demostración. Con G simple y resoluble. Entonces los unicos subgrupos normales de G so $\langle e\rangle$ 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, sí 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. Ademas, 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 $H^{(r)} \leq G^{(r)} = \langle e \rangle$, as'i que $H^{(r)} = \langle e \rangle$.

Ahora, sea $N \trianglelefteq G$, pues ${}^{G}\!/_{N}$ es un grupo. Entonces los commutadores 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 siguentes 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 $p | \operatorname{ord} G$.

demostración. Suponga que $G = P_1 \times \cdots \times P_k$, para P_k un p_k-Sylow de G. Entonces por definicion 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 unico. Sea P_i un p_i-Sylow d e G, donde $p_i | \operatorname{ord} G$, para todo $1 \leq i \leq k$. Tenemos entonces que $\operatorname{ord} P_1P_2 = \operatorname{ord} P_1 \operatorname{ord} P_2$ ya que $P_1 \cap P_2 = \langle e \rangle$. Por lo tanto $\operatorname{ord} P_1 \dots P_k = \operatorname{ord} P_1 \dots P_k$, entonces $G = P_1 \dots P_k$ y $P_i \cap \prod_{i \neq j} P_i = \langle e \rangle$. Por definicion, 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 lemma 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 operacion binaria $+$ junto a una operacion binarai $\cdot : (a,b) \to ab$ tal que

(1) $\cdot$ es associativa.

(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**. Sab=ba=1, $entoncesllamamosa$ayb**unidades**.

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

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

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

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

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

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

Lema 55. *Sea $\phi : R \to S$ un homomorfismo de anillos, y que los unicos idealse 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 multiplicacion $\cdot$ dado por $(a + I, b + I) \to (a + I)(b + I) = ab + I$.*

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

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

Teorema 58 (El Teorema del Factor)**.** *Cualquier homomorfismo de anillis $\phi : R \to S$ con kernel K que contiene a un ideal I se puede factorizarse via ${}^{R}\!/_{I}$, como $\phi = \overline{\phi} \circ \pi$ donde $\pi : R \to {}^{R}\!/_{I}$ y $\overline{\phi} : {}^{R}\!/_{I} \to S$ es el unico homomorfismo con $\overline{\phi}$ sobre si y solo si ϕ es sobre y $\overline{\phi}$ 1–1 si y solo si $K = I$.*

$$\begin{tikzcd} R \arrow[r, "\phi"] \arrow[d, "\pi"'] & S \\ {}^{R}\!/_{I} \arrow[ur, "\overline{\phi}"'] & \end{tikzcd}$$

Teorema 59 (Primer Teorema de Isomorfismo)**.** *Sí $\phi : R \to S$ 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 $\phi : \mathbb{R}[x] \to \mathbb{C}$ 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 commutativo 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 commutativo 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 $\pi : R \to {}^{R}\!/_{M}$ dado por $a \to a + M$. Como N es ideal, entonces por el teoream 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 commutativo con identidad es **primo** sí para todo $a, b \in R$, sí $ab \in P$ implica que $a \in P$, ó $b \in P$.

Teorema 62. *Sea R un anillo commutativo con identidad. Entonce un ideal P de R es primo sí, y solo sí ${}^{R}\!/_{P}$ 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 sí $(a + P)(b + P) = ab + P = P$, entonces tenemos que $a + P = P$ ó $b + P = P$. Es decir, sí $ab \in P$, entonces $a \in P$ ó $b \in P$. ■

Corolario. *Todo ideal maximal es primo.*

Corolario. *Sea $\phi : R \to S$ un homomorfismo de anillos 1–1 con identidad. Las siguentes enunciadas son ciertos*

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

(2) Sí 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 $\phi : \mathbb{Z}[x] \to \mathbb{Z}$ dado por $f(x) \to f(0)$, es decir, la mapa valuación. Entonces tenemos que $\mathbb{Z} \simeq {}^{\mathbb{Z}[x]}\!/_{(x)}$.

Lectura 15: Anillos de Polinomios

Lema 63. *Sí R es un anilloc commutativo con identidad, entonces el conjunto $R[x]$, definido por*

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

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

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

Lema 64. *La mapa valuación $R[x] \to R$ dado por $f(x) \to f(0)$ 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, sí $f(x) = a_0 + a_1 x + \cdots + a_n x^n$, 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** sí $a_n = 1$.

Teorema 65. *Sí $f, g \in R[x]$ 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 polínomio. Llamamos a un elemento $a \in R$ un **raíz** (ó una **cero**) de f sí $f(a) = 0$.

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

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

y $f(a) = 0$ sí y solo sí $(x - a)|f$.

demostración. Sí f no tiene raíces, terminamos. Ahora s'i 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. Sí a_1 es la única raíz de f, terminamos. Sí no, procede recursivamente usando el teoram 65. Este recursión concluye, y por lo tanto se enumera las raices de f. ■

Lectura 16: Factorización Única

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

Lema 67. *Sí a es primo, entonces a es irreducible.*

demostración. Sea a primo con $a = bc$. Suponga que $a|b$, lo que dces que $ba = bcd = b(1 - cd) = 0$, entonces $1 = cd$ lo que hace c unidad. De igual manera sí $c|a$, 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 $4 = 2 \cdot \overline{2} = (a+ib\sqrt{3})(c+id\sqrt{3})(a-ib\sqrt{3})(c-id\sqrt{3}) = (a^2+3b^2)(c^2+3d^2)$. 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 unica** es un dominio integral R, que satisface las siguentes

(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.*

demostración. Por supuesto, sí a, es irreducible. Ahora, suponga que a es irreducible, y que $a|bc$ Entonces $bc = ad$ para algúin $d \in R$. Descomponga, entonces, b, c, y d en productios 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 satiface la **condicion de cadena acendiente** para ideales primos. Sí sateifaces esta condicion para todo ideal, llamamos a R un anillo **Noeteriano**.

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

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

(1) Sí R es un dominio de factorización única, entonces satisfaces la condición de la cadena acendiente.

(2) Sí R satisface la condición acendiente, entonces todo $a \in R$ se puede factorizar en irreducibles (no necesariamente de forma única).

(3) Sí R es tal que todo $a \in R \backslash \{0\}$ se puede factorizar en irreducibles primos, entonces R es un dominio de factorización única.

demostración. (1) COnsidere la cadena $(a_1) \subseteq (a_2) \subseteq (a_3) \subseteq \dots$, donde R es un dominio de factorización única. Tenemos enconces que cada $a_{i+1}|a_i$. Por lo tanto, los factores primos de a_{i+1} consiste de algunos primos de a_i. Como a_1 tiene factorización única,entonces los factores primos en la cadena terminarán sinendo 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 al a 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 elements $a \neq 0$ 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 tambien es primo.....

■

Teorema 70. *Sí R es un dominio de ideal principal, entonces R es un dominio de factorizacón 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** sí existe una mapa $d : R\backslash\{0\} \to \mathbb{N}$ 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. *Sí R es un dominio Euclideo, entonces R es un dominio de ideal principal.*

demostración. Sea I un ideal de R, Sí $I = (0)$, 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 minimo $m \in \mathcal{D}$. 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 minimo, $d(r) \not< d(b)$, 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

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

Pues, sí $D = -2, -1, 2$ 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 Euclideano con $d = |\cdot|$.

(3) Para cualquier cuerpo K, $K[x]$ es un dominio Euclideano 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 Euclideano.

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 $R \times R \backslash \{0\}$ dado por*

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

Sea $Q = {R \times R\backslash\{0\}}/{\sim}$ 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 estos operaciones.

demostración. Nota que $(Q,+)$ forma un grupo abeliano con identidad $(0,1)$ y inversos $(-a,b)$. De igaul 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 $R \times R \backslash \{0\}$ por

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

Entonces llamamos al cuerpo $Q = {R \times R \backslash \{0\}} / {\sim}$ 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 $a \to \frac{a}{1}$. ■

Suponga que D es un dominio de factorización únoca, 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 $(a_0, \ldots, a_n)$ de los coeficientes de f el **contenido** de f y escribimos

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

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 divida a $c(g)$ ó a $c(h)$.*

demostración. Sea que $pf = gh$, y suponga lo contrario. Sea $g(x) = g_0 + g_1 x + \cdots + g_s x^s$, y $h(x) = h_0 + h_1 x + \cdots + h_t x^t$. Suponga que $p \nmid c(g)$ y que $p \nmid c(h)$. Sean g_u y h_u los coefficientes de los terminos con los potencias mas pequeñas que no son dividios por p. Nota, que el coefficiente 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 pop 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 $\frac{ae}{db} = 1$ 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 $D[x]$. ■