NOTAS DEL CURSO DE ÁLGEBRA MODERNA I

Fernando Sánchez Castellanos Villafuerte

27 de julio de 2007

El fin de estas notas es llevar un registro ordenado (hasta donde me sea posible) de los temas vistos en la clase de *Álgebra Moderna I* con la Dra. Claudia Reynoso. Se copiaron íntegramente los teoremas, las proposiciones y corolarios vistos en clase, además de sus demostraciones. También he copiado todas las tareas que nos asignaron en el curso. La mayoría de las demostraciones fueron las que se vieron en clase, propuestas por la maestra, o resueltas por algún compañero. Algunas demostraciones son de mi inventiva.

Índice general

Capítulo 1

Teoría de Grupos

1.1. Introducción

Definición 1.1. Un conjunto S no vacío se llama semigrupo si tiene una operación binaria asociativa.

$$\cdot_S : S \times S \to S$$
$$\text{Si } x, y, x \in S \text{ entonces } (x \cdot y) \cdot z = x \cdot (y \cdot z)$$

Definición 1.2. Un semigrupo S se llama monoide si existe un elemento $1 \in S$ (llamado elemento identidad) tal que:

$$1 \cdot x = x \cdot 1 = x, \forall x \in S$$

En ocasiones, el elemento identidad se denota por e.

Ejemplos de Monoide: $\mathbb{R}, \mathbb{N}$ bajo la suma.

Proposición 1.3. *El elemento identidad de un monoide es único.*

Demostración 1.4. Sean 1 y $1'$ identidades en S, entonces

$$1 = 1 \cdot 1' = 1'$$

Notación 1.5. Algunas veces se utilizara la notación $xy := x \cdot y$ por comodidad durante el libro. También usaremos $x \cdot_G y$ cuando sea necesario indicar en que conjunto actúa la operación binaria. De igual manera se utilizará la notación 1_G para indicar el grupo al que pertenece la identidad cuando se pueda prestar a confusiones.

Definición 1.6. Dado $x \in G$, un elemento $y \in G$ tal que $x \cdot y = y \cdot x = 1$ se llama el elemento inverso de x en G.

Definición 1.7. Un monoide G es un grupo si para cada $x \in G$ existe el elemento inverso de x.

Proposición 1.8. *El inverso de $x \in G$ es único.*

Demostración 1.9. Sean $y, z \in G$ inversos de x, entonces:

$$y = y \cdot 1 = y \cdot (x \cdot z) = (y \cdot x) \cdot z = 1 \cdot z = z$$

Notación 1.10. El inverso de x se denota por x^{-1}

Definición 1.11. Un grupo G se llama Abeliano (o conmutativo) si:

$$x \cdot y = y \cdot x, \forall x, y \in G$$

Usualmente, la operación binaria en grupos abelianos se denota por $+$, la identidad por 0 y el inverso de x por $-x$.

Notación 1.12. Sea G un grupo con identidad 1 y sea $x \in G$, entonces definimos:

1. $x^0 := 1$
2. $x^n := x^{n-1} \cdot x, n \in \mathbb{Z}^{>0}$
3. $x^{-n} := (x^{-1})^n$ si $n \in \mathbb{Z}^{\geq 0}$

Definición 1.13. Sea S un conjunto no vacío. Una permutación de S es una función $\phi : S \to S$, biyectiva.

Sea $G = \{\phi : S \to S | \phi \text{ es permutación}\}$. Entonces $(G, \circ)$ es un grupo y lo denotamos por $Perm(S)$.

Sea S finito, i.e. $S = \{1, 2, ..., n | n \in \mathbb{N}\}$ entonces $Perm(S) := Sim_n := S_n$

Si $\phi \in Sim_n$ usaremos la siguiente notación: $\phi = \begin{pmatrix} 1 & 2 & \cdots & n \\ \phi(1) & \phi(2) & \cdots & \phi(n) \end{pmatrix}$

Como ejemplo, podemos tomar un triángulo equilátero en el plano, T, con centro en O. Sea D_3 el grupo de simetrías de T. Una simetría es una función del plano en el plano que lleva a T sobre T y preserva distancias. Bajo la composición, D_3 es un grupo. Denominamos cada uno de los elementos de D_3 de la siguiente manera:

- 1_T la función identidad.
- ϕ_1 la función que rota T 120°
- ϕ_2 la función que rota T 240°
- σ_1 la función que refleja T sobre el vértice 1
- σ_2 la función que refleja T sobre el vértice 2
- σ_3 la función que refleja T sobre el vértice 3

1.2. Orden, Generadores, Grupos Cíclicos

Definición 1.14. La cardinalidad de un grupo G se llama el órden de G.

Notación 1.15. El órden de un grupo G se denotará por $|G|$.

Si G es infinito, entonces diremos que G tiene órden infinito.

Definición 1.16. Un subconjunto H de un grupo G es un subgrupo de G, si la operación binaria de G, restringida a H, hace de H un grupo.

Notación 1.17. Si H es un subgrupo de G, entonces escribimos $H \leq G$.

Observación 1.18. La identidad en H es la identidad en G, y el inverso de x en H es el inverso de x en G.

Proposición 1.19. *Un subconjunto $H \neq \emptyset$ de un grupo G es un subgrupo de G si, y sólo si*

$$\forall x, y \in H \Rightarrow x \cdot y^{-1} \in H$$

Demostración 1.20. ($\Rightarrow$) Si $H \leq G$ entonces $\forall x, y \in H \Rightarrow x \cdot y^{-1} \in H$.
($\Leftarrow$) Supongamos que para todo $x, y \in H$ tenemos que $x \cdot y^{-1} \in H$. Entonces:

- Sea $x \in H$ entonces $x \cdot x^{-1} = 1 \in H$.
- Sea $y \in H$ entonces $1 \cdot y^{-1} = y^{-1} \in H$.
- Sean $x, y \in H$, entonces $x, y^{-1} \in H$, entonces $x \cdot (y^{-1})^{-1} = x \cdot y \in H$.

Por lo tanto $H \leq G$.

Proposición 1.21. *Si $\{G_\alpha\}_{\alpha \in \Lambda}$ es una familia de subgrupos de un grupo G, entonces $\bigcap_{\alpha \in \Lambda} G \leq G$.*

Demostración 1.22. Sean $x, y \in \bigcap_{\alpha \in \Lambda} G$, entonces $x, y \in G_\alpha \forall \alpha \in \Lambda$ así que $x, y^{-1} \in G_\alpha \forall \alpha \in \Lambda$ por lo tanto $x, y^{-1} \in \bigcap_{\alpha \in \Lambda} G \Rightarrow \bigcap_{\alpha \in \Lambda} G \leq G$.

Observación 1.23. La unión de subgrupos no es un grupo.
Ejemplo Sea $H = \{2n | n \in \mathbb{Z}\} \cup \{3n \ n \in \mathbb{Z}\}$ entonces $H \nleq \mathbb{Z}$ pues $2, 3 \in H$ y $2 + 3 = 5 \notin H$.

Definición 1.24. Sea S un subconjunto de un grupo G. Definimos $\langle S \rangle = \cap H$ tal que $S \subset H \leq G$.

$\langle S \rangle$ es el más pequeño subgrupo de G que contiene a S, en el sentido que si H es un subgrupo que contiene a S, entonces $\langle S \rangle \subseteq H$.

Definición 1.25. Un grupo generado por un único elemento, se llama grupo cíclico

Notamos que un grupo cíclico G se define por $G = \langle x \rangle$ para algún $x \in G$. De esta manera, tenemos que $G = \{x\} = \{x^k | k \in \mathbb{Z}\}$

Definición 1.26. El órden de un elemento x en un grupo G es el órden del grupo cíclicoque genera. $|x| := |\langle x \rangle|$

Entonces, el órden de un elemento puede ser infinito, o un entero positivo. Si es un entero positivo, i.e. $|x| = n \in \mathbb{Z}^{>0}$, entonces n es el mínimo entero positivo tal que $x^n = 1$.

Proposición 1.27. *Si x es un elemento de orden finito n de un grupo G, y si $x^m = 1$ para algún $m \in \mathbb{Z}^{>0}$, entonces $n|m$*

Demostración 1.28. Sea $m = nq + rn,\ q \in \mathbb{Z},\ 0 \leq r < n$. Entonces:

$$1 = x^m = x^{nq+r} = (x^n)^q \cdot x^r = 1^q \cdot x^r = 1 \cdot x^r \Rightarrow r = 0$$

Corolario 1.29. *Si $G = \langle x \rangle$ tiene orden finito n y $k|n$ con $0 < k \in \mathbb{Z}$ entonces $\langle x^{\frac{n}{k}} \rangle$ es el único subgrupo de G de orden k.*

Demostración 1.30. Primero notemos que $\langle x^{\frac{n}{k}} \rangle$ tiene orden k. Sea entonces $x^s \in G$ un elemento de órden k. P.D: $\langle x^s \rangle = \langle x^{\frac{n}{k}} \rangle$
Observamos que $(x^s)^k = x^{sk} = 1$, entonces $n|sk$, es decir $sk = nm$, por lo tanto $x^s = (x^{\frac{n}{k}})^m \in \langle x^{\frac{n}{k}} \rangle$

Proposición 1.31. *Un subgrupo de un grupo cíclico es cíclico.*

Demostración 1.32. Sea $H \leq \langle x \rangle$. Si $H = \{1\}$, entonces es cíclico. Supongamos que $H \neq \{1\}$. Sea m el mínimo entero positivo tal que $x^m \in H$.
P.D: $H = \langle x^m \rangle$.
Sea $x^s \in H$, sea $s = mq + r,\ q, r \in \mathbb{Z},\ 0 \leq r < m$. Entonces $x^s = x^{mq+r} = (x^m)^q \cdot x^r \in H$
$\Rightarrow\ x^{s-mq} = x^r \in H \rightarrow x^r = 0$ y $H \ni x^s = (x^m)^q\ \therefore\ H = \langle x^m \rangle$

Se recomienda revisar los problemas de la Tarea 1.

Capítulo 2

Teoremas de Homomorfismos

2.1. Clases Laterales

Definición 2.1. Sea H un subgrupo de un grupo G. Diremos que x es congruente con y módulo H si, y sólo si $y^{-1} \cdot x \in H$.

Lo denotamos por $x \equiv y \pmod{H}$.

Ejemplo: $G = \mathbb{Z}, H = \langle n \rangle$.

Sabemos que $\equiv$ define una relación en G que depende de H.

Proposición 2.2. *$\equiv$ es una relación de equivalencia en G.*

Demostración 2.3.

- Reflexividad: Como H subgrupo:

$$\Rightarrow 1 = x \cdot x^{-1} \in H \Rightarrow x \equiv x \pmod{H}.$$

- Simetría: Sea $x \equiv y \pmod{H} \Rightarrow y^{-1} \cdot x \in H$ como H es subgrupo:

$$\Rightarrow (y^{-1} \cdot x)^{-1} = x^{-1} \cdot y \in H \Rightarrow y \equiv x \pmod{H}.$$

- Transitividad: Sean $x \equiv y$ y $y \equiv z \pmod{H}$. Como H es subgrupo:

$$\Rightarrow (y^{-1} \cdot x), (z^{-1} \cdot y) \in H \Rightarrow (z^{-1} \cdot y) \cdot (y^{-1} \cdot x) = z^{-1} \cdot x \in H \Rightarrow x \equiv z \pmod{H}.$$

$\therefore \equiv$ es una relación de equivalencia

Por ser $\equiv$ una relación de equivalencia, "parte" a G en clases de equivalencias.

Si $x \equiv y \pmod{H}$ entonces $y^{-1} \cdot x = h \in H \rightarrow x = yh$. Entonces, la clase de equivalencia que contienes a y es $\{yh | h \in H\} := yH$.

Definición 2.4. Sea $y \in G$, entonces yH se llama la clase lateral izquierda de H en G que contiene a y.

Entonces tenemos que:

$$G = \bigcup_{y \in G} yH \tag{2.1.0.1}$$

Definición 2.5. Sea $H \leq G$ el número (posiblemente infinito) de clases laterales izquierda de equivalencia de H en G. Este número se llama el índice de H en G y se denota por $[G : H]$.

Teorema 2.6 (Teorema de Lagrange)**.** *Sea G un grupo de órden finito y H un subgrupo de G. entonces $|G| = |H| \cdot [G : H]$, en particular, el órden de H es un divisor del órden de G.*

Demostración 2.7. Sea $y \in G$. Definimos $f : H \longrightarrow yH$ con $f(h) = yh$ y notamos que es una biyección.Como G es la unión disjunta de las clases laterales, entonces:

$$|G| = |yH| \cdot [G : H] = |H| \cdot [G : H] \tag{2.1.0.2}$$

2.2. Homomorfismos

Definición 2.8. Un homomorfismo f de un grupo $(G, \cdot_G)$ en un grupo $(H, \cdot_H)$ es una función $f : G \longrightarrow H$ tal que $f(x \cdot_G y) = f(x) \cdot_H f(y)\ \forall x, y \in G$

Ejemplos:

- Sea $H \leq G$ y $f : H \longrightarrow G$, $f(h) = h$.
- Sean $G = (\mathbb{R}, +)$, $H = (\mathbb{R}^{\geq 0}, \cdot)$ y $f : G \longrightarrow H$, $f(r) = e^r$.
- Sea $f : \mathbb{Z} \longrightarrow \mathbb{Z}$ tal que $f(n) = mn$, $m \in \mathbb{Z}$

Definición 2.9.
- Si f es inyectiva, entonces se llama monomorfismo.
- Si f es suprayectiva, entonces se llama epimorfismo.
- Si f es inyectiva y suprayectiva, entonces se llama isomorfismo.
- Si existe un isomorfismo entre los grupo G y H, entonces decimos que son isomorfos, y lo denotamos por $G \simeq H$.
- Un homomorfismo de $G \longrightarrow G$ se llama endomorfismo.
- Un isomorfismo de $G \longrightarrow G$ se llama automorfismo.

Notación 2.10. $Aut(G) = \{f : G \longrightarrow G |$ f es automorfismo$\}$

Definición 2.11. Si $f : G \longrightarrow H$ es un homomorfismo, entonces el kernel (o núcleo) de f es el conjunto $Ker(f) = \{g \in G | f(g) = 1_H\}$

Ejemplo: Sean $SL(n, \mathbb{C}) = \{A \in GL(n, \mathbb{C}) | det(A) = 1\}$ y $PGL(n, \mathbb{C}) = \{[A] | A \in GL(n, \mathbb{C})\}$ con $[A] = \left\{\lambda A | \lambda \in \mathbb{C}^{\neq 0}\right\}$. Entonces $f : SL(n, \mathbb{C}) \longrightarrow PGL(n, \mathbb{C})$ tal que f(A)=[A] es un homomorfismo.

Proposición 2.12. *Sea $f : G \longrightarrow H$ un homomorfismo, entonces:*

- $f(1_G) = 1_H$ *con* $1_G, 1_H$ *el elemento neutro de* G *y* H *respectivamente.*
- $f(x^{-1}) = (f(x))^{-1}$ $\forall x \in G$
- $Ker(f) \leq G$
- f *es un monomorfismo si, y sólo si* $Ker(f) = \{1_G\}$

Demostración 2.13.
- $f(1_G) = f(1_G \cdot 1_G) = f(1_G) \cdot f(1_G) \Rightarrow$
$\Rightarrow (f(1_G))^{-1} \cdot f(1_G) \cdot f(1_G) = (f(1_G))^{-1} f(1_G) \Rightarrow f(1_G) = 1_H \therefore 1_G \in Ker(f)$

- $1_H = f(1_G) = f(x \cdot x^{-1}) = f(x) \cdot f(x^{-1}) \Rightarrow f(x^{-1}) = (f(x))^{-1}$
- Sean $x, y \in Ker(f)$ P.D. $x \cdot y^{-1} \in Ker(f)$.
  $\Rightarrow f(x \cdot y^{-1}) = f(x) \cdot f(y^{-1}) = f(x) \cdot (f(y))^{-1} = 1 \cdot 1^{-1} = 1 \cdot 1 = 1 \Rightarrow x \cdot y^{-1} \in Ker(f)$
- (Parte 1) Sea $Ker(f) = \{1_G\}$. Sean $x, y \in G$ tales que $f(x) = f(y)$, entonces $f(x) \cdot (f(y))^{-1} = 1_H$, pero por otro lado $f(x) \cdot (f(y))^{-1} = f(x) \cdot f(y^{-1}) = f(x \cdot y^{-1})$
  $\Rightarrow f(x \cdot y^{-1}) = 1_H$ así que $x \cdot y^{-1} \in Ker(f) = \{1_G\} \Rightarrow x \cdot y^{-1} = 1_G \Rightarrow x = y$
  $\therefore f$ es monomorfismo.
  (Parte 2) Sea $Ker(f) \neq \{1_G\}$. Sea entonces $x \in Ker(f)$ tal que $x \neq 1_G$, entonces $f(x) = 1_H = f(1_G)$ $\therefore f$ no es monomorfismo

Como ejemplo, podemos tomar $G = D_3$ y $H = \{1, -1\}$. Definimos $f : G \longrightarrow H$ con $f(\phi) = 1$ si ϕ es rotación, $f(\phi) = -1$ si ϕ es reflexión. Entonces $Ker(f) = \{\phi \in D_3 | \phi \text{ es rotación}\} \leq 3$, $|Ker(f)| = 3$

Proposición 2.14. *Si f es isomorfismo de G a H, entonces f^{-1} es un isomorfismo de G a H.*

Demostración 2.15. Sea $f : G \longrightarrow H$ un isomorfismo de grupos.
P.D. $f^{-1}(g \cdot h) = f^{-1}(g) \cdot f^{-1}(h) \forall g, h \in G$

Sean $h = f(x)$, $g = f(y) \in H$. Entonces $f^{-1}(h) = x$ y $f^{-1}(g) = y$ por lo tanto $h \cdot g = f^{-1}(x \cdot y) = f(x) \cdot f(y) \Rightarrow f^{-1}(h \cdot g) = x \cdot y = f^{-1}(h) \cdot f^{-1}(g)$.

Proposición 2.16. *Sea G un grupo, entonces $Aut(G)$ es un grupo con la composición de funciones.*

Demostración 2.17. $Aut(G) \in Perm(G)$ P.D. $Aut(G) \leq Perm(G)$. Sean $f, g \in Aut(G)$ y sean $x, y \in G$
$(f \circ g^{-1})(x \cdot y) = f(g^{-1}(x \cdot y)) = f(g^{-1}(x) \cdot g^{-1}(y)) = f(g^{-1}(x)) \cdot f(g^{-1}(y)) =$
$(f \circ g^{-1}(x)) \cdot (f \circ g^{-1}(y))$, entonces $f \circ g^{-1} \in Aut(G) \Rightarrow Aut(G) \leq Perm(G)$

2.3. Subgrupos Normales

Definición 2.18. Sea $H \leq G$. Diremos que H es un subgrupo normal de G si $x^{-1}Hx := \left\{x^{-1} \cdot y \cdot x | y \in H\right\} \subseteq H, \forall x \in G$

Notación 2.19. $H \lhd G$

Observación 2.20. Si $H \lhd G$, entonces $x^{-1}Hx, \forall x \in G$

Demostración 2.21. Sabemos que $xHx^{-1} \subseteq H$, luego, sea $h \in H$ entonces $h = xx^{-1}hx^{-1}x = (xx^{-1})h(xx^{-1})^{-1} \in xHx^{-1}$.

Proposición 2.22. *Sea $f : G \longrightarrow H$ un homomorfismo, entonces $Ker(f) \lhd G$*

Demostración 2.23. Sea $x \in G$; P.D. $x^{-1}Ker(f)x \subseteq Ker(f)$. Sea $y \in Ker(f)$
$f(x^{-1}\cdot y\cdot x) = (f(x))^{-1}\cdot f(y)\cdot f(x) = (f(x))^{-1}\cdot 1\cdot f(x) = 1 \Rightarrow x^{-1}\cdot y\cdot x \in Ker(f)$

Observación 2.24. De hecho, todo subgrupo normal de un grupo G es el kernel de un homomorfismo $f : G \to H$. Esta demostración se deja en la tarea 3.

Ejemplos:

- Si G es abeliano, entonces todo subgrupo de G es normal.
- $H = \left\langle \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \right\rangle \lhd S_3$, la demostración se deja como ejercicio.
- $H = \left\langle \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \right\rangle \not\lhd S_3$

  Demostración 2.25. $\begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \cdot \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \cdot \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \notin H$

Definición 2.26. Sea G un grupo. El centro de G es el conjunto:

$$Z(G) = \{x \in G | xy = yx \ \forall y \in G\}$$

Proposición 2.27.
- $Z(G) \lhd G$
- *$Z(G)$ es abeliano.*

Demostración 2.28.
- $Z(G) \leq G$. Sean $x, z \in Z(G),\ y \in G$; P.D. $xz^{-1} \in Z(G)$, i.e. $(xz^{-1})y = y(xz^{-1})$).
  Si $z \in Z(G) \Rightarrow zy = yz \Rightarrow z^{-1}zyz^{-1} = z^{-1}yzz^{-1} \Rightarrow yz^{-1} = z^{-1}y \Rightarrow$

$z^{-1} \in Z(G)$
$\Rightarrow (xz^{-1})y = x(z^{-1}y) = x(yz^{-1}) = (xy)z^{-1} = (yx)z^{-1} = y(xz^{-1}) \Rightarrow$
$xz^{-1} \in Z(G) \quad \therefore Z(G) \leq G$

- $Z(G) \lhd G$. Sea $z \in G$; P.D. $zZ(G)z^{-1} \subseteq Z(G)$.
  Sea $x \in Z(G)$; P.D. $zxz^{-1} \in Z(G)$.
  Sea $y \in G$; P.D. $(zxz^{-1})y = y(zxz^{-1})$
  $\Rightarrow (zxz^{-1})y = (xzz^{-1})y = xy = yx = y(xzz^{-1}) = y(zxz^{-1}) \Rightarrow Z(G) \lhd G.$

- $Z(G)$ es abeliano. Sean $x, y \in Z(G)$
  $\Rightarrow xy = yx \Rightarrow Z(G)$ es abeliano.

Un par de cosas que hay que notar:
Si G es abeliano $\Rightarrow Z(G) = G$.
Si $H \leq G$ es abeliano $\Rightarrow H \subseteq Z(G)$.

Proposición 2.29. *Si H es un subgrupo de un grupo G, entonces H es normal si, y sólo si toda clase lateral izquierda de H en G es una clase lateral derecha de H en G. Es decir, para xH existe Hy tal que $xH = Hy$.*

Demostración 2.30. ($\Rightarrow$)Supongamos que $H \lhd G$. Entonces, para todo $x \in G$, $xHx^{-1} = H$. Sea $h \in H$. Sea $h \in H$, entonces $xHx^{-1} = h \in h \ \Rightarrow xh = hx \ \therefore \ xH = Hx$
($\Leftarrow$) Sea $x \in G$; P.D. xHx^{-1}. Sabemos que para xH existe $y \in G$ tal que $xh = Hy \Rightarrow xHx^{-1} = Hyx^{-1} = zH$ para algún $z \in H$ (por la propiedad supuesta). Entonces $xHx^{-1} = zH$ es una clase lateral por la izquierda que contiene a 1, por lo tanto $zH = 1H = H \ \therefore xHx^{-1} = H$.

Definición 2.31. Sea $H \leq G$. Definimos ${}^{G}/_{H} := \{xH | x \in G\}$, como el conjunto de clases laterales izquierdas de H en G.

Podemos notar que $\left|{}^{G}/_{H}\right| = |G : H|$, y por el teorema de Lagrange, si G es finito, entonces: $\left|{}^{G}/_{H}\right| = \frac{|G|}{|H|}$.

Teorema 2.32. *Si $H \lhd G$, entonces ${}^{G}/_{H}$ toma estructura de grupo con la siguiente operación binaria ${}^{G}/_{H} \times {}^{G}/_{H} \longrightarrow {}^{G}/_{H}$ tal que $(xH, yH) \longrightarrow (x \cdot y)H$. Este grupo se llama el grupo cociente de G módulo H. Con identidad $H = 1H$*

Para probar esto, se utiliza la normalidad de H en G para ver que la operación está bien definida. Las demás propiedades de grupo las hereda de G.

Notación 2.33. Si G es abeliano y la operación binaria la denotamos por $+$, entonces ${}^{G}/_{H} = \{x + H | x \in G\}$.

El ejemplo 0 de este grupo es cuando $G = (\mathbb{Z}, +)$; $H = \{nk | k \in \mathbb{Z}\} = n\mathbb{Z}$, entonces $H \leq G$ y H es normal porque G es abeliano.
$\Rightarrow {}^{G}/_{H} = \{m + H | m \in \mathbb{Z}\}$ tiene estructura de grupo con la operacińn ${}^{G}/_{H} \times {}^{G}/_{H} \longrightarrow {}^{G}/_{H}$ que manda $(m_1 + H, m_2 + H) \mapsto (m_1 + m_2) + H$.

Notación 2.34. Definimos $m + H = [m]$

Entonces tenemos que ${}^{G}/_{H} = \{[0], [1], \ldots, [n-1]\}$ y nuestra operación binaria en ${}^{G}/_{H}$ es tal que $[m_1] + [m_2] = [m_1 + m_2]$. Además, en este ejemplo se utiliza la notación ${}^{G}/_{H} := {}^{\mathbb{Z}}/_{n\mathbb{Z}} := \mathbb{Z}_n$

Se recomienda revisar los problemas correspondientes a la Tarea 2.

2.4. La aplicación cociente

Sea $H \lhd G$. Definimos $\pi : G \longrightarrow {}^{G}/_{H}$, con $\pi(x) = [x]$. Llamamos a π la aplicación cociente.

Proposición 2.35. *La aplicación cociente π es un epimorfismo y $Ker(\pi) = H$.*

Demostración 2.36.

- π es homomorfismo. $\pi(xy) = [xy] = [x][y] = \pi(x)\pi(y)$.
- π es epimorfismo. Sea $xH \in {}^{G}/_{H}$, entonces $\pi(x) = xH$.
- $Ker(\pi) = \{x \in G | \pi(x) = xH = H\} = H$.

Entonces tenemos que todo subgrupo normal es el kernel de un homomorfismo.

Teorema 2.37 (Teorema fundamental de homomorfismos de grupos (TFH))**.** *Sea, G y H grupos y $f : G \longrightarrow H$ un epimorfismo. Denotamos $K = Ker(f)$, entonces $H \simeq {}^{G}/_{K}$.*

Demostración 2.38. Tenemos que demostrar que existe un isomorfismo entre H y ${}^{G}/_{K}$. Definimos $\bar{f} : {}^{G}/_{H} \longrightarrow H$ tal que $\bar{f}(xK) = f(x)$. Ahora probaremos que $\bar{f}$ es isomorfismo.

- Esta bien definido. Suponer $xK = yK$; P.D. $f(x) = f(y)$
  $xK = yK \iff xy^{-1} \in K$, entonces $f(xy^{-1}) = e \Rightarrow f(x)(f(y))^{-1} = 1 \Rightarrow f(x) = f(y)$.

- Es homomorfismo. Sean $xK, yK \in {}^{G}/_{K}$
  $\bar{f}(xK \cdot yK) = \bar{f}((x \cdot y)K) = f(x \cdot y) = f(x) \cdot f(y) = \bar{f}(xK) \cdot \bar{f}(yK)$.

- Es inyectiva.
  $Ker(\bar{f}) = \{xK | \bar{f}(xK) = f(x) = 1\} = \{K\} \subset {}^{G}/_{K} \Rightarrow \bar{f}$ es inyectiva.

- Es sobreyectiva. Sea $y \in H$. Como f es sobreyectiva, entonces $\exists x \in G$ tal que $f(x) = y \Rightarrow xK \in {}^{G}/_{H} \Rightarrow \bar{f}(xK) = f(x) = y \ \therefore \ \bar{f}$ es isomorfismo.

Para ver un ejemplo de la aplicación de este teorema, tomemos G un grupo y $a \in G$. Definimos la aplicación $T_a : G \longrightarrow G$ tal que $T_a(x) = axa^{-1}$. Entonces T_a es un automorfismo y todos los automorfismos de este tipo se denominan automorfismos internos, $Aut_{int}(G) : \{T_a : G \longrightarrow G | a \in G\}$. Notar que $Aut_{int}(G) \leq Aut(G)$. Definimos $f : G \longrightarrow Aut_{int}(G)$ tal que $f(a) = T_a \ \forall a \in G$

Proposición 2.39.

- *f es homomorfismo.*
- *f es sobreyectiva.*
- *$Ker(f) = Z(G)$.*

Demostración 2.40.

- f es homomorfismo. Sean $a, b, x \in G$, entonces $f(ab)(x) = T_{ab}(x) = (ab)x(ab)^{-1} = abxb^{-1}a^{-1} = a(T_b(x))a^{-1} = T_a(T_b(x)) = (T_a \circ T_b)(x) = (f(a) \circ f(b))(x)$.

- f es sobreyectiva. Sea $a \in G$ y $T_a \in Aut_{int}(G)$, entonces $f(a) = T_a$.
- $Ker(f) = Z(G)$. Por definición $Ker(f) = \{a \in G | T_a(x) = x \ \forall x \in G\} = \{a \in G | axa^{-1} = x \ \forall x \in G\} = Z(G)$

Y por el TFH: ${}^{G}/_{Z(G)} \simeq Aut_{int}(G)$

Proposición 2.41. *Sea $f : G \longrightarrow H$ un epimorfismo con $Ker(f) = K$. Entonces:*
$\{L | L \leq H\} \longleftrightarrow \{S | K \leq S \leq G\}$ con $L \mapsto f^{-1}(L)$ es una correspondencia biyectiva. Además $L \lhd H$ si, y sólo si $f^{-1}(L) \lhd G$

Corolario 2.42. *Si $K \lhd G$ entonces todos los subgrupos del grupo cociente ${}^{G}/_{K}$ tiene la forma ${}^{M}/_{K}$ donde M es un subgrupo de G, y ${}^{M}/_{K} \lhd {}^{G}/_{K}$ si, y sólo si $M \lhd G$.*

Se dejan como ejercicio las demostraciones de la proposición anterior y su corolario.

Teorema 2.43 (Teorema de Freshman)**.** *Sea G un grupo, $H \lhd G$, $K \lhd H$, $K \lhd G$, entonces: ${}^{H}/_{K} \lhd {}^{G}/_{K}$ y además ${}^{G}/_{H} \simeq {}^{({}^{G}/_{K})}/_{({}^{H}/_{K})}$*

Demostración 2.44. Definimos $f : {}^{G}/_{K} \longrightarrow {}^{G}/_{H}$ con $f(xK) = xH$.

- f esta bien definida: Sean $x, y \in G$, entonces $xK = yK \Rightarrow xKH = yKH$ y como $K \subset H \Rightarrow xKH = yKH \Rightarrow xH = yH$. f es homomorfismo: Sean $x, y \in G$, entonces $f(xK \cdot yK) = f((xy)K) = (xy)H = xH \cdot yH = f(xK) \cdot f(yK)$.
- f es sobreyectiva. Sea $xH \in {}^{G}/_{H}$, entonces $xK \in {}^{G}/_{K} \Rightarrow f(xK) = xH$.

$\Rightarrow Ker(f) = \{xK \in {}^{G}/_{K} | f(xK) = xH = H\} = \{xK \in {}^{G}/_{H} | x \in H\} = {}^{G}/_{K}$. Entonces ${}^{H}/_{K} \lhd {}^{G}/_{K}$, y por el TFH: ${}^{G}/_{H} \simeq {}^{({}^{G}/_{K})}/_{({}^{H}/_{K})}$

2.5. Acciones de Grupos

Definición 2.45. Sea G un grupo y S un conjunto. Una aplicación $\phi : G \times S \longrightarrow S$ tal que $(x, s) \mapsto \phi(x, s) := xs$, que satisface:

- $\phi(x_1, \phi(x_2, s)) = \phi(x_1 \cdot x_2, s)\ \forall s \in S$, es decir $x_1(x_2 s) = (x_1 x_2)s$.
- $\phi(1_G, s) = s\ \forall s \in S$, es decir $1_G s = s$.

Se llama acción izquierda del grupo G en S.

Si además satisface: $xs = s \Rightarrow x = 1$, diremos que la acción de G es fiel.

Como ejemplo, podemos tomar $G = GL(n, \mathbb{R}),\ S = \mathbb{R}^n$ y definimos $\phi : G \times S \longrightarrow S$ tal que $(A, v) \mapsto Av$.

Definición 2.46. Sea G un grupo actuando en un conjunto S. Sea $s \in S$. Definimos el estabilizador de s respecto a la acción de G como:

$$Est_G(s) = Stab_G(s) = \{x \in G | xs = s\} \subseteq G.$$

Definición 2.47. Sea G un grupo actuando en un conjunto S. Sea $s \in S$. definimos la orbita de s respecto a la acción de G como:

$$Orb_G(s) = \{xa | x \in G\}.$$

Si existe $s \in S$ tal que $Orb_G(s) = S$, entonces diremos que la acción es transitiva. Esto significa que dados $s_1, s_2 \in S \Rightarrow \exists\ x \in G$ tal que $xs_1 = s_2$.

Si G actúa en un conjunto S, entonces la acción define una partición en S, dada por la siguiente relación de equivalencia: $s_1 \sim s_2 \iff \exists x \in G$ tal que $xs_1 = s_2$. Esta demostración de deja en los problemas de tarea.

La clase de equivalencia de s es $Orb_G(s)$.

Observación 2.48. Si existe $s \in S$ tal que $Orb_G(s) = S$, entonces, para todo $s_1 \in S$ se cumple que $Orb_G(s_1) = S$.

Proposición 2.49. *Si un grupo G actúa en un conjunto S, entonces $Stab_G(s) \leq G$ y $[G : Stab_G(s)] = |Orb_G(s)|$, para todo $s \in S$.*

Demostración 2.50. Parte 1:

Sea $s \in S$ y sean $x, y \in Est_G(s) \Rightarrow xs = s,\ ys = s \Rightarrow xs = s,\ s = y^{-1}s \Rightarrow (xy^{-1})s = x(y^{-1}s) = xs = s \Rightarrow xy^{-1} \in Stab_G(s) \therefore Stab_G(s) \leq G$.

Parte 2:

Definimos $Orb_H(s) \longrightarrow {}^{G}/_{Stab_G(s)}$ tal que $xs \mapsto xStab_G(s)$.

- Está bien definido: Si $x_1S = x_2S \Rightarrow (x_2^{-1}x_1)s = s \Rightarrow x_2^{-1}x_1 \in Stab_G(s) \Rightarrow x_1Stab_G(s) = x_2Stab_G(s)$.
- Es sobreyectiva: Dado $xStab(s) \in {}^{G}/_{Stab_G(s)}$, entonces $xs \mapsto xStab_G(s)$.
- Es inyectiva: Supongamos $x_1Stab_G(s) = x_2Stab_G(s) \Rightarrow x_2^{-1}x_1 \in Stab_G(s) \Rightarrow (x - 2^{-1}x_1)s = s \Rightarrow x_1s = x_2s$

$\therefore\ |Orb_G(s)| = \left|{}^{G}/_{Stab_G(s)}\right| = [G : Stab_G(s)]$

Teorema 2.51 (Teorema de Cayley)**.** *Sea G un grupo. Entonces G es isomorfo a un subgrupo de un grupo de permutaciones, es decir, existe S tal que $G \leq Perm(S)$.*

Demostración 2.52. Definamos $f_x : G \longrightarrow G$ con $f_x(y) = xy$, $\forall x \in G$, es claro que $f \in Perm(G)$. Entonces, definamos $f : G \longrightarrow Perm(G)$ tal que $f(x) = f_x$, y probemos que f es un homomorfismo de grupos.
P.D. $f_{x_1x_2} = f_{x_1} \circ f_{x_2}$. Sea $y \in G$, entonces $f_{x_1x_2}(y) = x_1x_2y = x_1f_{x_2}(y) = f_{x_1}(f_{x_2}(y)) = (f_{x_1} \circ f_{x_2})(y)$.
Ahora tenemos que $Ker(f) = \{x \in G | f_x = Id\} = \{x \in G | f_x(y) = xy = y\ \forall y \in G\} = \{1\}$.
Y por el TGH $G \simeq {}^{G}/_{Ker(f)} \simeq Im(f) \leq Perm(G)$.

Ahora vamos a definir algunos conjuntos que se obtienen a partir de acciones de grupo particulares:

Sea G un grupo y sea $G \times G \longrightarrow G$ tal que $(x, y) \mapsto xyx^{-1}\ \forall x, y \in G$. Sea $y \in G$, entonces definimos:

- $cl(y) := Orb_G(y) = \left\{xyx^{-1} | x \in G\right\}$, La clase conjugada de y en G.
- $C_G(y) := Est_G(y) = \left\{x \in G | xyx^{-1} = y\right\}$, el centralizador de y en G.

Corolario 2.53. $|cl(y)| = [G : C_G(y)]$

Observación 2.54.
- $cl(y) = \{y\} \iff y \in Z(G)$.
- $ordcl(y) \iff y \in Z(G)$.

Demostración 2.55. $cl(y) = \{xyx^{-1} | x \in G\} = \{y\} \iff xyx^{-1} = y \ \forall x \in G \iff y \in Z(G)$.

Ahora, ya sabemos que una acción de G en S define una relación de equivalencia. Es decir que "parte" a S en clases de equivalencia.

Si G es un grupo finito, entonces $|G|$ es la suma de la cardinalidad de las distintas clases conjugadas $cl(y)$.

Sean $y_1, y_2, \ldots, y_k$ representantes de las distintas clases conjugadas $cl(y_i)$ que tienen más de un elemento, entonces:

$$|G| = |Z(G)| + \sum_{i=1}^{k} |cl(y_i)| \tag{2.5.0.3}$$

Corolario 2.56. *Si $p \in \mathbb{Z}$ es primo, $n \in \mathbb{N}$ y G es un grupo de orden p^n, entonces $|Z(G)| \neq 1$ y de hecho, p divide a $|Z(G)|$*

Demostración 2.57. Primero notemos que, por definición, $C_G(y_i) \leq G \ \forall i$, entonces, por el teorema de Lagrange: $|C_G(y_i)|$ divide $|G|$.

Como $[G : C_G(y_i)] > 1$, entonces $[G : C_G(y_i)] = p^r$, con $0 < r < n$ y luego $[G : C_G(y_i)] = \frac{|G|}{|C_G(y_i)|}$, por lo tanto $Z(G) = |G| - \sum_{i=1}^{k} [G : C_G(y_i)] = mp$ para algún $m \in \mathbb{N}$.

Otro caso: Sea G un grupo y $S = \{A | A \subset G\}$. Definimos $G \times S \longrightarrow S$ tal que $(x, A) \mapsto xAx^{-1}$ y acordamos que $x\emptyset x^{-1} = \emptyset$. Entonces, esto es una acción de G en S.

Sea $A \in S$. Entonces definimos:

- $Orb_g(A) = \{xAx^{-1} | x \in G\}$ como los conjuntos G-conjugados de A.
- $N_G(A) := Est_G(A) = \{x \in G | xAx^{-1} = A\} = \{x \in G | xA = Ax\}$ como normalizador de A en G.

Corolario 2.58. *El número de conjuntos G-conjugados de A es $[G : N_G(A)]$.*

Teorema 2.59 (teorema de homomorfismos)**.** *Supongamos que $H, K \leq G$ y $K \leq N_G(H)$. Entonces $KH = HK \leq G$, $H \lhd KH$, $K \cap H \lhd K$ y $^{KH}/_{H} \simeq {}^{K}/_{K \cap H}$.*

Demostración 2.60.

- Vamos a probar que $KH = \{xy | x \in K \ y \in H\} \leq G$.
  Sean $x, u \in K$, $y, v \in H$; P.D. $(xy)(uv)^{-1} \in KH$.
  $(xy)(uv)^{-1} = xy(v^{-1}u^{-1}) = xu^{-1}uyv^{-1}u^{-1}$, y como $x, u \in K \Rightarrow \ xu^{-1} \in K$.
  Además, $K \subset N_G(H) = \left\{x \in G | xhx^{-1} = h \ \forall h \in H\right\} \Rightarrow u(yv^{-1})u^{-1} \in H \ \therefore (xu^{-1})(uyv^{-1}u^{-1}) \in KH$.

- $KH = HK$. Sea $xy \in KH$, entonces $xy = (xyx^{-1})x$ y como $x \in K \subset N_G(H) \Rightarrow xyx^{-1} \in H$, entonces $xy = (xyx^{-1})x \in HK$.

- $H \lhd KH$. Sean $xy \in KH \Rightarrow (xy)H(xy)^{-1} = xyHy^{-1}x^{-1} = xHx^{-1} = H$.

- ${}^{KH}/_{H} \simeq {}^{K}/_{K\cap H}$. Definimos $f : K \longrightarrow {}^{KH}/_{H}$ tal que $x \mapsto xH$.

  - f es homomorfismo: $f(x_1x_2) = x_1x_2H = x_1H \cdot x_2H = f(x_1) \cdot f(x_2)$.
  - f es sobreyectiva: Sea $xyH \in {}^{KH}/_{H}$, entonces $xyH = xH$, pues $y \in H$ así que $f(x) = xH = xyH$.
  - $Ker(f) = \{x \in K | xH = H\} = \{x \in K | x \in H\} = K \cap H$.

  Por lo tanto, ${}^{KH}/_{H} \simeq {}^{K}/_{Ker(f)} = {}^{K}/_{K\cap K}$.

Teorema 2.61 (Teorema de Cauchy)**.** *Sea G un grupo finito cuyo orden es divisible por un primo p. Entonces, existe un elemento $x \in G$ de orden p, i.e. G tiene un subgrupo de orden p, $\langle x \rangle$.*

Demostración 2.62. Sea
$S = \{(x_1, x_2, \ldots, x_p) \in G \times G \times \cdots \times G | x_1x_2 \cdots x_k = 1\} - \{(1, 1, \ldots, 1)\}$.
Calculemos $|S|$: podemos elegir $x_1, x_2, \ldots, x_{p-1}$, entonces $x_p = (x_1x_2 \cdots x_{p-1})^{-1}$, por lo tanto $|S| = |G|^{p-1} - 1$. Notemos que, como $|G|$ es divisible entre p, $|S|$ no es divisible entre p.
Sea $C = \langle z \rangle$ un grupo cíclico de orden p. Definimos $\varphi : C \times S \longrightarrow S$ tal que $\varphi(z^r, (x_1, x_2, \ldots, x_p)) = (x_{1+r}, x_{2+r}, \ldots, x_r)$. Veamos que φ es una acción de grupo.

- $\varphi(1, (x_1, x_2, \ldots, x_p)) = \phi(z^0, (x_1, x_2, \ldots, x_p)) = (x_1, x_2, \ldots, x_p)$.

- $\varphi(z^n z^m, (x_1, x_2, \ldots, x_p)) = \varphi(z^{n+m}, (x_1, x_2, \ldots, x_p)) =$
  $= (x_{1+n+m}, x_{2+n+m}, \ldots, x_{(p+n+m \pmod p)}) = \varphi(z^n, (x_{1+m}, x_{2+m}, \ldots, x_m)) =$
  $= \varphi(z^n, \varphi(z^m, (x_1, x_2, \ldots, x_p)))$.

Por lo tanto φ es una acción de C en S.
Entonces $|Orb_C(x_1, x_2, \ldots, x_p)| = [C : Est_C(x_1, x_2, \ldots, x_p)] = \frac{p}{Est_C(x_1, x_2, \ldots, x_p)} = 1$ ó p.
Si todas las órbitas tienen orden p, entonces $|S|$ es divisible entre p, y eso es una contradicción. Así que existe $(x_1, x_2, \ldots, x_p \in S)$ tal que $|Orb_C(x_1, x_2, \ldots, x_p)| = 1$, así que $Orb_C = \{(x, x, \ldots, x)\}$ para algún $x \in G$ tal que $x \neq 1$, entonces $x^p = 1$.

Recordemos que Lagrange dice que si $H \leq G$, entonces $|H|$ divide a $|G|$. Luego veremos que existe un grupo finito G y un divisor n de $|G|$ tal que G no tiene subgrupos de orden n.

Capítulo 3

Grupo simétrico y Grupo alternante

3.1. Introducción

Recordemos que $S_n = \{\sigma : \{1, 2, \ldots, n\} \longrightarrow \{1, 2, \ldots, n\} \,|\sigma \text{ es biyección}\}$, es el grupo simétrico de n letras. Sea $S = \{1, 2, \ldots, n\}$, entonces S_n actúa de manera natural en S: $S_n \times S \longrightarrow S$ tal que $(\sigma, k) \mapsto \sigma(k)$.
Sea $\sigma \in S_n$. Consideramos $\langle\sigma\rangle$ y vemos que actúa sobre S al definir $\langle\sigma\rangle \times S \longrightarrow S$ tal que $(\sigma^r, k) \mapsto \sigma^r(k)$. Entonces tenemos que $Orb_{\langle\sigma\rangle}(k) = \left\{k, \sigma(k), \sigma^2(k), \ldots, \sigma^{|\sigma|-1}(k)\right\}$. Sean $T_1, T_2, \ldots, T_l$ las distintas órbitas de esta acción, y definamos $\sigma_1, \ldots, \sigma_l$ como sigue:

$$\sigma_i(k) = \begin{cases} \sigma(k) & \text{si } k \in T_i \\ k & \text{si } k \in S - T_i \end{cases}$$

Entonces, tenemos que $\sigma = \sigma_1\sigma_2 \cdots \sigma_l$.

Definición 3.1. Sea $T \subset S$ un subconjunto de k elementos. Una permutación $\sigma \in S_n$ se llama k-ciclo asociado a T si σ permuta todos los elementos de T y deja fijos todos los elementos de $S - T$.

Notación 3.2. Si σ es un k-ciclo, escribimos $\sigma = \begin{pmatrix} s & \sigma(s) & \sigma^2(s) & \cdots & \sigma^{k-1}(s) \end{pmatrix}$ Donde cada elemento esta siendo enviado pro σ al siguiente, y el último elemento es enviado al primero.

Definición 3.3. Si los ciclos $\sigma_1,\ \sigma_2$ permutan los elementos de T_1 y T_2 respectivamente, y además $T_1 \cap T_2 = \emptyset$, entonces diremos que los ciclos son disjuntos.

Observación 3.4. Los ciclos disjuntos conmutan.

Proposición 3.5. *Si σ es una permutación de n elementos, entonces σ puede expresarse como un producto de ciclos disjuntos. La expresión es única excepto por el órden de los factores.*

Definición 3.6. Un 2-ciclo se llama transposición.

Podemos ver que cada ciclo se puede expresar como un producto de transposiciones:

$$(i_1\ i_2\ \ldots\ \imath_k) = (i_1\ i_k)(i_1\ i_{k-1})\cdots(i_1\ i_3)(i_1\ i_2)$$

Entonces, por la proposición, toda permutación puede expresarse como producto de transposiciones.

Definición 3.7. Diremos que σ es una permutación par, si puede expresarse como el producto de un número par de transposiciones. Es permutación impar en otro caso.

Si $G = \{-1, 1\}$ bajo la multiplicación, y definimos $f : S_n \longrightarrow G$ tal que:

$$\sigma \mapsto f(\sigma) = \begin{cases} 1 & \text{si } \sigma \text{ es par} \\ -1 & \text{si } \sigma \text{ es impar} \end{cases}$$

Definición 3.8. Entonces f es un homomorfismo de grupos, y definimos $A_n := Ker(f) = \{\sigma \in S_n | \sigma \text{ es par}\}$, el grupo alternante de n letras.

Teorema 3.9. $[S_n : A_n] = 2,\ n \geq 2$

Demostración 3.10. Si $f : S_n \longrightarrow H = \{1, -1\}$ es sobreyectiva, entonces, por el TFH: ${}^{S_n}/_{A_n} \simeq H$ y $[S_n : A_n] = \frac{|S_n|}{|A_n|} = 2$. Para probar que f es sobre tenemos que probar que existe en S_n una permutación impar. Probemos que (12) es impar. Si (12) es par, entonces la identidad de puede expresar como el producto de un número impar de transposiciones. A saber $1 = (ab)\cdots$ usando el número mínimo de transposiciones y el menor número de a's. Como $1(a) = b$ con $a \neq b$, entonces debe existir en el producto de transposiciones de 1 por lo menos una más que contenga a a. Sea (ac) la primera que aparece después de (ab), entonces $1 = (ab)\cdots(ac)\cdots$.
Notemos que $(de)(ac) = (ac)(de)$ si son disjuntos, y además $(dc)(ac) = (ad)(cd)$, entonces podemos escribir $1 = (ab)\cdots(ac)\cdots = (ab)(af)\cdots$ con las mismas condiciones de minimalidad.
Si $b = f$, entonces podemos reducir el número de transposiciones. Si $b \neq f$, entonces $(ab)(af) = (af)(bf)$ y estaríamos reduciendo el número de a's. En ambos caos llegamos a una contradicción.

Sea $\sigma = (a_1\ a_2\ \ldots\ a_k)$ un k-ciclo y sea $\tau \in S_n$, tal que $\tau(a_i) = b_i,\ 1 \leq i \leq k$, y convenimos que $a_{k+1} = a_1$ y $b_{k+1} = b_1$. Entonces $\tau\sigma\tau^{-1}(b_i) = \tau\sigma\tau^{-1}(\tau(a_i)) = \tau(\sigma(a_1)) = t(a_{i+1}) = b_{i+1},\ \forall\ 1 \leq i \leq k$, y si $s \notin \{b_1, b_2, \ldots, b_k\}$, entonces $s \notin \{\tau(a_1), \tau(a_2), \ldots, \tau(a_k)\} \Rightarrow \tau^{-1}(s) \notin \{a_1, a_2, \ldots, a_k\} \Rightarrow \tau\sigma\tau^{-1}(s) = s$. Así que $\tau\sigma\tau^{-1}$ es $(b_1\ b_2\ \ldots\ b_k) = (\tau(a_1)\ \tau(a_2)\ \ldots\ \tau(a_k))$, un k-ciclo.

Definición 3.11. Sea $\sigma \in S_n$, supongamos que σ se expresa como el producto de ciclos disjuntos con k_j j-ciclos, con $1 \leq j \leq n$. Diremos entonces que σ tiene tipo cíclico $(k_1, k_2, \ldots, k_n)$.

Notemos que $\sum_{i=1}^{n} ik_i = k_1 + 2k_2 + \cdots + nk_n = n$.

Proposición 3.12. *Sea $\sigma \in S_n$, entonces $cl(\sigma)$ consiste de todos los elementos $\tau \in S_n$ que tienen el mismo tipo cíclico de σ.*

Demostración 3.13. Recordemos que dada una acción de grupo $S_n \times S_n \longrightarrow S_n$ tal que $(\tau, \sigma) \mapsto \tau\sigma\tau^{-1}$, entonces $cl(\sigma) = Orb_{s_n}(\sigma) = \left\{\tau\sigma\tau^{-1} | \tau \in S_n\right\}$. Primero veamos que $cl(\sigma) \subseteq \{\tau | \tau$ tiene el mismo tipo cíclico que $\sigma\}$:

Sea $\sigma \in S_n$, con $\sigma = \sigma_1\sigma_2\cdots\sigma_m$ como un producto de ciclos disjuntos incluyendo los 1-ciclos. Sea $\tau \in S_n$, entonces $\tau\sigma\tau^{-1} = \tau\sigma_1\tau^{-1}\tau\sigma_2\tau^{-1}\cdots\tau\sigma_m\tau^{-1}$, entonces, si σ_j es un k_j-ciclo, $\tau\sigma_j\tau^{-1}$ también lo es.
$\{\tau|\tau$ tiene el mismo tipo cíclico que $\sigma\} \subseteq cl(\sigma)$:
Supongamos que $\phi \in S_n$ tiene el mismo tipo cíclico que σ. Y digamos que $\sigma = (a_1\ a_2\ \cdots)(b_1\ b_2\ \cdots)\cdots$, $\phi = (a_1'\ a_2'\ \cdots)(b_1'\ b_2'\cdots)\cdots$ donde los ciclos están ordenados de manera creciente respecto a su longitud. Definimos $\tau \in S_n$ como $\tau(a_i) = a_i'$, $\tau(b_i) = b_i'$, etc. Entonces $\tau\sigma\tau^{-1} = \phi \in cl(\sigma)$.

Lema 3.14. *Sea G un grupo finito y $H \leq G$. Si $[G : H] = 2$, entonces $H \lhd G$.*

Como ejercicio, se sugiere demostrar que el inverso del Teorema de Lagrange es falso (ubicar los subgrupos de A_4).

Capítulo 4

Teoremas de Sylow

Notación 4.1. Sean $n, m \in \mathbb{Z}$. Decimos que $n^k \| m$ si, y sólo si $n^k | m$ y $n^{k+1} \nmid m$.

Definición 4.2. Sea G un grupo finito y p un primo. Un subgrupo $P \leq G$ se llama p-subgrupo de Sylow si $|P| = p^k,\ k \in \mathbb{Z}$ y $p^k \| |G|$.

Teorema 4.3 (Primer Teorema de Sylow)**.** *Si G es un grupo finito y p un primo, entonces existe un p-subgrupo de Sylow P en G.*

Demostración 4.4. Probémoslo por inducción en $|G|$. Si $|G| = 1$ o si $p \nmid |G|$, entonces $P = \{1\}$. Supongamos entonces que $|G| > 1$ y que $p | |G|$. La hipótesis de inducción nos dice que el teorema se satisface para todos los grupos de orden menor a $|G|$. Si existe $H \leq G$, $H \neq G$ tal que $p \nmid [G : H]$, entonces, por la hipótesis de inducción, H tiene un p-subgrupo de Sylow P. Y este p-subgrupo también es p-subgrupo de Sylow de G. Supongamos que $p | [G : H]$ para todo $H \leq G$ con $H \neq G$. Recordemos que si tenemos una acción de grupo $G \times G \longrightarrow G$ con $(y, x) \mapsto yxy^{-1}$ tenemos que $|G| = |Z(G)| + \sum_{i=1}^{k} [G : C_G(x_i)]$. Entonces $p | |Z(G)|$, y por el teorema de Cauchy, existe $x \in Z(G)$ con $|x| = p$. Sea $K = \langle x \rangle$. Como $x \in Z(G)$, entonces $yxy^{-1} = x\ \forall y \in G \Rightarrow yx^m y^{-1} = x^m\ \forall y \in G$, así que $K \lhd G$. por hipótesis de inducción $\left| {}^{G}/_{K} \right|$ tiene un p-subgrupo de Sylow $P_1 = {}^{P}/_{K}$ con $K \leq P \leq G$, entonces $|P_1| = p^{m-1} \Rightarrow |P| = |P_1| |K| = p^m$.

Definición 4.5. Sea p un primo. Un grupo G se llama p-grupo si todo elemento en G tiene como orden una potencia de p.

En la tarea se demuestra que G es un p-grupo si, y sólo si $|G| = p^k$, $k \in \mathbb{Z}^{\geq 0}$.

Observación 4.6. Todo p-subgrupo de Sylow es un p-grupo.

Lema 4.7. *Supongamos que P es un p-subgrupo de Sylow de un grupo finito G, y supongamos que $H \leq G$ es un p-grupo. Entonces $H \cap N_G(P) = H \cap P$.*

Teorema 4.8 (Segundo Teorema de Sylow)**.** *Si G es un grupo finito, p es un primo, y P es un p-subgrupo de Sylow de G y $H \leq G$ un p-grupo, entonces existe $x \in H$ tal que $H \subset xPx^{-1}$ En particular, todos los p-subgrupos de Sylow de G son conjugados entre si.*

Demostración 4.9. Sea $S = \{xPx^{-1} \ x \in G\}$. Construyamos la acción $H \times S \longrightarrow S$ tal que $(y, xPx^{-1}) \mapsto yxPx^{-1}y^{-1}$. Sean $S_1, S_2, \ldots, S_k$ las distintas H-órbitas en S y sea $P_i = x_i P x_i^{-1} \subset S_i$, $1 \leq i \leq k$. Entonces $S_i = \{yP_iy^{-1} | y \in H\}$ y $Est_H(P_i) = \{y \in H | yP_iy^{-1} = P_i\} = H \cap N_G(P_i) = H \cap P_i$, así que $|S_i| = [H : Esto_G(P_i)] = [H : H \cap P_i]$.
Ahora, recordemos que cuando tenemos una acción de grupo $G \times mathscrS = \{A | A \subset G\} \longrightarrow mathscrS$ con $(y, A) \mapsto yAy^{-1}$ y definimos $S = Orb_G(P) = \{yPy^{-1} | y \in G\}$, entonces $|S| = |Orb_G(P)| = [G : Est_G(P)] = [G : N_G(P)]$. Entonces tenemos (por la primera acción definida) que $|S| = \sum_{i=1}^{k} |S_i| = \sum_{i=1}^{k} [H : H \cap P_i]$. Como $[H : H \cap P_i]$ es una potencia de p ya que H es un p-grupo, y como $p \nmid |S|$, entonces existe i tal que $[H : P_i] = p^0 = 1$, por lo tanto $H \cap P_i = H$, es decir $H \subset P_i = xPx^{-1}$.

Corolario 4.10. *Si G tiene un único p-subgrupo de Sylow P, entonces $P \lhd G$.*

Demostración 4.11. Sea $x \in G$, entonces xPx^{-1} es p-subgrupo de Sylow, por lo tanto $xPx^{-1} = P \Rightarrow xP = Px \Rightarrow P \lhd G$.

Teorema 4.12 (Tercer Teorema de Sylow)**.** *Sea G un grupo finito y p un primo, entonces el número de p-subgrupos de Sylow de G es congruente con 1 módulo p.*

Demostración 4.13. Sea P un p-subgrupo de Sylow de G, sea $S = \{xPx^{-1}|x \in G\}$. Entonces $|S|$ es el número de conjuntos de p-subgrupos de Sylow de G.
Consideramos la acción $P \times S \longrightarrow S$ con $(y, xPx^{-1}) \mapsto yxPx^{-1}y^{-1}$, sean $S_1, S-2, \ldots, S_n$ las distintas órbitas de la acción. Entonces $|S| = \sum_{i=1}^{n} |S_i|$. Sea $S_1 = Orb_P(P) = \{yPy^{-1}|y \in P\} = \{P\}$, entonces $|S| = 1 + \sum_{i=2}^{n} |S_i|$. Recordemos que $|Orb_P(S)| = [G : Est_P(S)]$. Sean pues $P_i \in S_i$, $2 \leq i \leq n$, luego $Est_P(P_i) = \{y \in P|yP_iy^{-1} = P_i\} = P \cap N_G(P_i) \Rightarrow |S_i| = [P : P \cap N_G(P_i)] = [P : P \cap P_i]$. Como $P \neq P_i \Rightarrow P \cap P_i \neq P$, por lo tanto $[P : P \cap P_i]$ es múltiplo de p. Entonces $|S| = 1 + \sum_{i=2}^{n} |S_i| = 1 + \sum_{i=2}^{n} p^{k_i}$, $k_i \geq 1$, por lo tanto $|S| \equiv 1 \pmod{p}$

Ejemplo: Demostrar que un grupo de orden 28 tiene un subgrupo normal de orden 7.
Solución: $28 = 2^2 \cdot 7$. Por el Teorema 3 de Sylow, puedo tener $1, 8, 15, 22, \ldots$ p-subgrupos de Sylow. Tomamos $S = \{A|A \subseteq G\}$ y definimos la acción $G \times S \longrightarrow S$ con $(x, S) \mapsto xSx^{-1} \Rightarrow Orb_G(P) = \{xPx^{-1}|x \in G\}$, entonces $|Orb_G(P)| = [G : Est_G(P)]$ que es un divisor de 28, y de nuestra lista, solo 1 divide a 28, entonces solo existe un 7-grupo de Sylow, por el corolario, es normal.

4.1. Caracterización de grupos Abelianos Finitos

Sean $(G_1, \cdot_1)$ y $(G_2, \cdot_2)$ grupos, entonces el conjunto $G_1 \times G_2$ tiene estructura de grupo con la operación binaria $(G_1 \times G_2) \times (G_1 \times G_2) \longrightarrow G_1 \times G_2$ donde $(x_1, x_2) \cdot (y_1, y_2) \mapsto (x_1 \cdot_1 y_1, x_2 \cdot_2 y_2)$.

La identidad en $G_1 \times G_2$ es $(1_1, 1_2)$ y $(x_1, x_2)^{-1} = (x_1^{-1}, x_2^{-1})$ $\forall (x_1, x_2) \in G_1 \times G_2$. $G_1 \times G_2$ con esta operación se llama el producto directo de G_1 y G_2.
En general, si $G_1, G_2, \ldots, G_n$ son grupos, podemos construir e producto directo $G_1 \times G_2 \times \cdots \times G_n$. Cuando $G_1, G_2, \ldots, G_n$ son abelianos, el producto directo se denota por $G_1 \oplus G_2 \oplus \cdots \oplus G_n$.

Lema 4.14. *Sea G un grupo y sean $G_1, G_2 \lhd G$ tales que $G_1 \cap G_2 = \{1\}$ y*

$G_1G_2 = \{x_1x_2 | x_1 \in G_1, x_2 \in G_2\} = G$, *entonces* $G \simeq G_1 \times G_2$

Teorema 4.15. *Sea G un grupo abeliano finito, entonces G es isomorfo a la suma directa de sus subgrupos de Sylow.*

Ejercicio: Demostrar el teorema anterior.

Teorema 4.16 (Frobenius)**.** *Si G es un grupo abeliano finito, entonces es la suma directa de sus subgrupos cíclicos. Cada uno de estos subgrupos tiene orden p^k para algún p primo y $k \in \mathbb{Z}^{\geq 0}$*

Demostración 4.17. Sea G abeliano finito. Denotamos la operación por $+$, y el neutro por 0. G es suma directa de sus subgrupos de Sylow, entonces, podemos suponer que G es un p-grupo abeliano. Vamos a probar que todo p-grupo abeliano finito es suma directa de cíclicos. Usamos inducción en $|G| = p^n$. Sea $a \in G$ de orden p^k maximal (i.e. si $b \in G$ tiene orden p^{k_1} entonces $k \geq k_1$). Sea H es subgrupo maximal de G tal que $H \cap \langle a \rangle = \{0\}$. Sea $G_1 = H \oplus \langle a \rangle = \{(h, na) | h \in H, n \in \mathbb{Z}\}$ Notemos que: i) , $\langle a \rangle \leq G$; ii) $H \cap \langle a \rangle = \{0\}$; iii) $H + \langle a \rangle \leq G$. Entonces $G_1 \simeq H + \langle a \rangle$. Si $G = G_1$ terminamos, pues aplicamos la hipótesis de inducción en H. Supongamos que $G_1 \subsetneq G$. Sea $x + G_1 \in {}^{G}\!/_{G_1}$ con $x + G_1 \neq G_1$ (i.e. $x \notin G_1$) de orden p, entonces $px \in G_1 = H + \langle a \rangle$. Así que existen $h \in H, m \in \mathbb{Z}$ tal que $px = h + ma$. Como p^k es el orden maximal en G, entonces $0 = p^k x = p^{k-1}(px) = p^{k-1}(h + ma) = p^{k-1}h + p^{k-1}ma$. Como $|a| = p^k \Rightarrow p^k \| p^{k-1}m \Rightarrow p \| m$. Sea $m = pr$. Entonces $h = px - ma = px - pra = p(x - ra) \in H$. Como $x \notin G_1 = H, H + \langle a \rangle \Rightarrow x - ra \notin H$. Por la maximalidad de H, tenemos que $H + \langle x - ra \rangle \cap \langle a \rangle \neq 0$. Sea $h_1 \in H$; $t, s \in \mathbb{Z}$ tales que $sa = h_1 + t(x - ra) \neq 0$, entonces $tx = sa - h_1 + tra = -h_1 + (s + rt)a \in H_1$. Vamos a probar que $p \nmid t$. Supongamos que $t = up$, entonces $t(x - ra) = up(x - ra) = uh$, entonces $sa = h_1 + uh \in H$!!, pues $H \cap \langle a \rangle = \{0\}$. Así que $p \not| t$, por lo tanto son primos relativos, entonces existen enteros s_1, s_2 tales que $ps_1 + ts_2 = 1$, así que $x = 1x = (ps_1 + ts_2)x = s_1(px) + s_2(tx) \Rightarrow x \in G_1$!!.

Capítulo 5

Anillos

5.1. Introducción

Definición 5.1. Un anillo es un grupo abeliano $(R, +, 0)$ con una operación binaria asociativa $\cdot : R \times R \longrightarrow R$ tal que $(a, b) \mapsto ab$, que llamaremos multiplicación. Las operaciones $+$ y $\cdot$ se relacionan mediante las siguientes propiedades distributivas:

$$(a + b)x = ax + bx$$
$$x(a + b) = xa + xb).$$

Si $ab = ba \ \forall a, b \in R$, entonces el anillo se llama conmutativo.
Si existe $1 \in R$, $1 \neq 0$ tal que $a1 = 1a = a \ \forall a \in R$, entonces R se llama anillo con 1 (uno).

Observación 5.2. Para todo $a \in R$, se cumple que $0a = a0 = 0$.

Demostración 5.3. $a0 = a(0 + 0) = a0 + a0 \Rightarrow a0 = 0$. $0a = (0 + 0)a = 0a + 0a \Rightarrow 0a = 0$.

Definición 5.4. Un anillo R conmutativo con 1 se llama campo si $\forall x \in R - \{0\}$ existe $y \in R$ tal que $xy = yx = 1$, es decir, $R - \{0\}$ es un grupo con la multiplicación.

Ejemplos de anillos: $(\mathbb{Z}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$.

Definición 5.5. Un subconjunto S de un anillo R es un subanillo de R si, con las operaciones de R restringidas a S, S es un anillo.

Ejemplo: $\mathbb{Z}$ es un subanillo de $\mathbb{Q}$, $\mathbb{R}$ y $\mathbb{C}$. $\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$. En este caso, el 1 de $\mathbb{Z}$ es el 1 de $\mathbb{Q}, \mathbb{R}, \mathbb{C}$. Aunque esto no siempre se cumple.

Proposición 5.6. *Un subconjunto no vacío S de un anillo R es un subanillo si, y sólo si $x - y, xy \in S$ para todos $x, y \in S$.*

Demostración 5.7. $\Rightarrow$) Si S es un subanillo de R, entonces $x-y, xy \in S \forall x, y \in S$.
$\Leftarrow$) i) si $x - y \in S$ para todos $x, y \in S$, entonces S es subgrupo de R. ii) Si $\forall x, y \in S$ se cumple que $xy \in S$, entonces $\cdot : S \times S$ es binaria asociativa (lo hereda de R).

Definición 5.8. Sean R y S anillos. Una función $f : R \longrightarrow S$ se llama homomorfismo de anillos si $f(x + y) = f(x) + f(y)$ y $f(xy) = f(x)f(y)$ para todo $x, y \in R$. Un homomorfismo se llama monomorfismo si es inyectivo. Se es sobre se llama epimorfismo, y se llama isomorfismo si es inyectivo.
Dos anillos se llaman isomorfos si existe un isomorfismo entre ellos.
El kernel de un homomorfismo de anillos f se define como $Ker(f) = \{x \in R | f(x) = 0\}$.
La imagen de un homomorfismo f se define como $Im(f) = \{f(x) | x \in R\}$.

Notemos que si $x, y \in Ker(f) \Rightarrow f(x - y) = f(x) - f(y) = 0 - 0 = 0$ y $f(xy) = f(x)f(y) = 0 \cdot 0 = 0$ por lo tanto $Ker(f)$ es un subanillo de R.
Si $f(x), f(y) \in Im(f) \Rightarrow f(x) - f(y) = f(x - y)$ y $f(x)f(y) = f(xy)$ por lo tanto $Im(f)$ es un subanillo de S.

Observación 5.9. El kernel de un homomorfismo de anillos $f : R \longrightarrow S$ satisface la siguiente propiedad: Si $x \in Ker(f)$ y $y \in R$ entonces $xy, yx \in Ker(f)$.

Definición 5.10. Un subanillo I de un anillo R se llama ideal derecho si para todos $x \in I, y \in R$ se tiene que $xy \in I$. Se llama ideal izquierdo si para todos

$x \in I, y \in R$ se cumple que $yx \in I$. Se llama ideal si para todos $x \in I, y \in R$ se cumple que $xy, yx \in I$.

Ejemplo: El kernel de un homomorfismo es ideal.

Definición 5.11 (Ver tarea 6)**.** Sea R un anillo. Un elemento $a \in R$ se llama nilpotente si $a^n = 0$ para algún entero positivo n.

Si R es un anillo conmutativo, entonces el conjunto $\{a \in R | a \text{ es nilpotente}\}$ es un ideal de R.

Definición 5.12 (Ver tarea 6)**.** Si R_1 y R_2 son anillos, entonces las operaciones binarias

$$\begin{gathered}(R_1 \times R_2) \times (R_1 \times R_2) \longrightarrow R_1 \times R_2 \\ + : ((a_1, b_1), (a_2, b_2)) \mapsto (a_1 + a_2, b_1 + b_2) \\ \cdot : ((a_1, b_1), (a_2, b_2)) \mapsto (a_1 a_2, b_1 b_2)\end{gathered}$$

definen un anillo en $R_1 \times R_2$. Llamaremos a este anillo suma directa de R_1 y R_2 y lo denotamos $R_1 \oplus R_2$.

Definición 5.13. Sea R un anillo con 1. Entonces $x \in R$ se llama unidad si existe $y \in R$ tal que $xy = yx = 1$. El conjunto de unidades en R se denota por $U(R)$ y se llama el grupo de unidades.

Notación 5.14. $R^* = R - \{0\}$

Definición 5.15. Sea R un anillo y sean $x, y \in R^*$ tales que $xy = 0$, entonces x se llama divisor de cero izquierdo de y y y se llama divisor de cero derecho de x. Si R es conmutativo, no hay distinción entre divisores de cero izquierdos y derechos y se llaman divisores de cero.

Ejemplos: Sea $R = M_2(\mathbb{R})$, entonces $\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} 1 & -1 \\ -1 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$.
Si $R = \mathbb{Z}_{mn}$ y m, n son primos relativos, entonces $\bar{n} \cdot \bar{m} = \bar{0}$.

Definición 5.16. Un anillo conmutativo $R \neq \{0\}$ se llama dominio entero si no tiene divisores de cero.

Definición 5.17. Un anillo R con 1 tal que todo elemento $x \in R^*$ tiene inverso multiplicativo se llama anillo con división.

Observación 5.18. Un anillo con división conmutativo es un campo.

Observación 5.19. Un campo es un dominio entero.

Demostración 5.20. Sean $x, y \in R^*$ con $xy = 0$, entonces $x = xyy^{-1} = 0y^{-1} = 0$ y esto es una contradicción.

Proposición 5.21. *Un subconjunto no vacío I de un anillo R es un ideal si, y sólo si para todo $x, y \in I$, $r \in R$ tenemos que $x - y, rx, xr \in I$.*

Demostración 5.22. Si I cumple que para todo $x, y \in I \Rightarrow x - y \in I$ entonces es subgrupo si además cumple que para todo $r \in R \rightarrow xr, rx \in I$, tomamos $r = y \in I \subseteq R \Rightarrow xy \in I$ entonces I es un subanillo de R y además, como $rx, xr \in I \ \forall r \in R$, I es ideal.

Definición 5.23. Si $\emptyset \neq X \subset R$ con R anillo, el ideal

$$\langle X \rangle = \bigcap_{\substack{I \supset X \\ I \text{ ideal}}} I$$

se llama el ideal generado por X y tiene la propiedad de maximalidad: si J es un ideal de R tal que $X \subset J$, entonces $\langle X \rangle \subset J$.
Un ideal generado por un elemento $a \in R$ se llama ideal principal y se denota por $\langle a \rangle$.

Observación 5.24. Si R es conmutativo y $a \in R$, entonces $\langle a \rangle = \{ra | r \in R\} = Ra$

Si I es un ideal de un anillo R, entonces, en particular, es un subgrupo normal, así que ${}^{R}\!/_{I} = \{r + I | r \in R\}$ es un grupo abeliano con la suma

$$+ : {}^{R}\!/_{I} \times {}^{R}\!/_{I} \longrightarrow {}^{R}\!/_{I}$$
$$(x + I, y + I) \mapsto (x + y) + I$$

Lo que queremos ahora, es darle a este grupo cociente estructura de anillo con el producto:

$$
\begin{aligned}
{}^{R}\!/_{I} \times {}^{R}\!/_{I} &\longrightarrow {}^{R}\!/_{I} \\
(x+I, y+I) &\mapsto (xy)+I
\end{aligned}
$$

Hay que ver que esta función esta bien definida. Sean $x+I = r+I, y+I = s+I \in {}^{R}\!/_{I}$.P.D.$(x+I)(y+I) = (r+I)(s+I)$ y esto pasa si, y sólo si $xy-rs \in I$. Consideremos $x(y-s), (x-r)s \in I \Rightarrow x(r-s)+(x-r)s = xy-xs+xs-rs = xy-rs \in I$ por lo tanto $xy+I = rs+I$.
Entonces ahora tenemos la aplicación cociente $\pi : R \to {}^{R}\!/_{I}$ donde $x \mapsto x+I$ y es un epimorfismo con $Ker(\pi) = I$, entonces, todo ideal es el kernel de un homomorfismo de anillos.

Teorema 5.25 (Teorema Fundamental de Homomorfismos de Anillos (TFHA))**.** *Sean R, S anillos y $f : R \longrightarrow S$ un homomorfismo. Entonces ${}^{R}\!/_{Ker(f)} \simeq Im(f)$.*

Demostración 5.26. Sea $g : {}^{R}\!/_{Ker(f)} \longrightarrow Im(f)$ tal que $x+I \mapsto f(x)$. Ya sabemos que g es un isomorfismo de grupos, así que solo basta demostrar que $g[(x+I)(y+I)] = g(x+I)g(y+I)$ para todos $x+I, y+I \in {}^{R}\!/_{Ker(f)}$, entonces vemos que $g[(x+I)(y+I)] = g(xy+I) = f(xy) = f(x)f(y) = g(x+I)g(y+I)$, por lo tanto g es un isomorfismo de anillos.

Proposición 5.27. *Sean R, S anillos y $f : f \longrightarrow S$ un epimorfismo, entonces existe una correspondencia biyectiva entre los ideales de S y los ideales de R que contienen a $I = Ker(f)$:*

$$
\begin{aligned}
\{J | J \text{ es ideal de } S\} &\longleftrightarrow \{K | K \text{ es idel de } R, R \supset I\} \\
J &\longmapsto f^{-1}(J).
\end{aligned}
$$

En particular, todo ideal del anillo cociente ${}^{R}\!/_{I}$ es de la forma ${}^{K}\!/_{I}$ donde K es un ideal de R y $K \supset I$.

Demostración 5.28. Sea $J \subset S$ un ideal, entonces $f^{-1}(J) \subset R$. P.D. $f^{-1}(J)$ es ideal. Sean $x, y \in f^{-1}(J), z \in R$. f^{-1} es subgrupo, así que $x-y \in f^{-1}(J)$. Luego $f(xz) = f(x)f(z) \in J$ y $f(zx) = f(z)f(x) \in J$ pues $f(x) \in J$ por lo tanto $f^{-1}(J)$ es ideal.

Definición 5.29. Un anillo R se llama simple si sus únicos ideales son $\{0\}$ y R.

Ejemplo: $M_2(R)$ con R un campo.

Proposición 5.30. *Sea R un anillo conmutativo, entonces R es simple si, y sólo si R es campo.*

Demostración 5.31. Sea $I \neq \{0\}$ un ideal en R. Sea $a \in I^*$, entonces, si R es campo, existe $b \in R^*$ tal que $ab = 1$, entonces $1 \in I$ por lo tanto $r \in I,\ \forall r \in R \Rightarrow I = R$. Ahora supongamos que R es simple: sea $a \in R^*$, entonces $\langle a \rangle = R$ así que $1 \in \langle a \rangle = \{ra | r \in R\} \Rightarrow$ existe $b \in R$ tal que $ba = 1$, por lo tanto R es campo.

Definición 5.32. Sea R un anillo conmutativo con 1 y sea I un ideal de R. Definimos el radical de I como:

$$\sqrt{I} = \left\{x \in R | x^k \in I \text{ para algún entero } k \geq 0\right\}$$

El ideal I se llama radical si $I = \sqrt{I}$.

En la tarea 7 se demuestran algunas propiedades del radical de un ideal I de un anillo R.

Definición 5.33. Sea R un anillo. Un ideal M de R se llama maximal si se satisface que si J es un ideal de R tal que $M \subset J \subset R$, entonces $J = M$ o $J = R$.

Definición 5.34. Un orden parcial en un conjunto $\mathcal{S}$ es una relación $\leq$ que satisface:

- Reflexión: $A \leq A$ para todo $A \in \mathcal{S}$.
- Antisimetría: $A \leq B$, $B \leq A \Rightarrow A = B$.
- Transitividad: $A \leq B$, $B \leq C \Rightarrow A \leq C$.

Un conjunto con un orden parcial se llama conjunto parcialmente ordenado, Copo o *poset*. Si el orden parcial, cumple además con:

- Totalidad: $\forall A, B \in \mathcal{S}\ A \leq B$ o $B \leq A$ o $A = B$.

entonces se llama orden lineal u orden total y un conjunto con un orden lineal se llama conjunto linealmente ordenado o *loset*.

Definición 5.35. Sea $\mathcal{S}$ un poset. Una cadena $\mathcal{C}$ en $\mathcal{S}$ es un subconjunto no-vacío de $\mathcal{S}$ tal que el orden parcial de $\mathcal{S}$ es un orden lineal en $\mathcal{C}$.
Una cota superior de $\mathcal{C}$ es un elemento $B \in \mathcal{S}$ tal que $A \leq B\ \forall A \in \mathcal{C}$.
Un maximal es un elemento $M \in \mathcal{S}$ que cumple que si $A \in \mathcal{S}$ tal que $M \leq A$, entonces $A = M$.

Lema 5.36 (Lema de Zorn)**.** *Si $\mathcal{S}$ es un* poset *no-vacío y toda cadena $\mathcal{C}$ en $\mathcal{S}$ tiene una cota superior, entonces $\mathcal{S}$ tiene un elemento maximal.*

Proposición 5.37. *Sea R un anillo con* 1 *y sea $I \subset R$ un ideal propio. Entonces existe un ideal maximal M de R tal que $I \subset M$.*

Demostración 5.38. Sea $\mathcal{S} = \{J | J \subsetneq R \text{ es ideal}, I \subset J\}$, entonces $\mathcal{S}$ es un *poset* con $\subseteq$. Sea $\mathcal{C} \subset \mathcal{S}$ una cadena. Sea $\mathcal{L} = \bigcap_{\mathcal{J}_\alpha \in \mathcal{C}} \mathcal{J}_\alpha$. P.D. $\mathcal{L}$ es cota superior de $\mathcal{C}$:

1. $\mathcal{L} \in \mathcal{S}$: Sean $x, y \in \mathcal{L} \Rightarrow x \in \mathcal{J}_\alpha,\ y \in \mathcal{J}_\beta$, s.p.d.g. supongamos que $\mathcal{J}_\alpha \subseteq \mathcal{J}_\beta \Rightarrow x, y \in \mathcal{J}_\beta$, por lo tanto $x - y, xz, zx \in \mathcal{J}_\beta\ \forall z \in R$. Luego $I \subset \mathcal{J}_\alpha\ \forall \alpha \Rightarrow I \subset \bigcup \mathcal{J}_\alpha = \mathcal{L}$. Después, tenemos que $\mathcal{L} \subsetneq R \Leftrightarrow 1 \notin \mathcal{L}$ y como $1 \notin \mathcal{J}_\alpha\ \forall \alpha \Rightarrow 1 \notin \mathcal{J} \therefore \mathcal{L} \subset R \Rightarrow \mathcal{L} \in \mathcal{S}$

2. Por construcción, $\mathcal{L}$ es cota superior de $\mathcal{C}$.

Luego, por el lema de Zorn, $\mathcal{S}$ tiene un elemento maximal.

Definición 5.39. Sea R un anillo. Un ideal P de R se llama ideal primo si siempre que $ab \in P$ se tiene que $a \in P$ o $b \in P$.

Definición 5.40. Un anillo R es dominio de ideales principales (DIP) si todo ideal $I \subset R$ es principal.

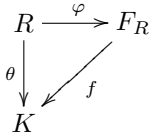
Lema 5.41 (Ver tarea 7)**.** *Todo ideal maximal en un anillo conmutativo con* 1 *es primo.*

Lema 5.42. *Si R es un DIP, dominio entero, conmutativo con* 1*, entonces todo ideal primo es maximal*

Demostración 5.43. Sea $P \subset R$ un ideal primo. Sea $J \subsetneq R$ tal que $P \subseteq J$. Luego $P = \langle a \rangle \subseteq J = \langle b \rangle \Rightarrow a = bc \in P$. Si $b \in P$, entonces $P = J$ y ya terminamos. Supongamos $b \notin P \Rightarrow c \in P$, entonces $c = c_1 a \Rightarrow a = bc_1 a \Rightarrow a = abc_1 \Rightarrow bc_1 = 1 \Rightarrow J = R$ y esto es una contradicción, por lo tanto $P = J$.

Ahora, queremos construir, a partir de un dominio entero R, un campo que lo contenga y que sea el mínimo campo que contiene a los inversos multiplicativos de lo elementos de R.

Definición 5.44. Un campo de fracciones para un dominio entero $R \neq \{0\}$, es un campo F_R con un monomorfismo $\varphi : R \longrightarrow F_R$ tal que si K es un campo y $\theta : R \longrightarrow K$ es monomorfismo, entonces existe un único monomorfismo $f : F_R \longrightarrow K$ tal que $f \circ \varphi = \theta$. Es decir:



conmuta.

Proposición 5.45. *El campo de fracciones de un dominio entero $R \neq \{0\}$ es único, salvo isomorfismo.*

Demostración 5.46. Supongamos que F_R y F'_R son campos fraccionarios de R. Entonces $\varphi : R \longrightarrow F_R$ y $\varphi' : R \longrightarrow F'_R$ son monomorfismos, y por lo tanto, existen únicos monomorfismos $f : F_R \longrightarrow F'_R$ y $f' : F'_R \longrightarrow F_R$ con $f \circ f' = id = f' \circ f$, y entonces f es un isomorfismo.

Teorema 5.47. *Sea $R \neq \{0\}$ un dominio entero. Entonces R tiene un campo de fracciones F_R.*

Demostración 5.48. Sea $X = \{(a,b)|a \in R, b \in R^*\}$. Definimos en X la siguiente relación: $(a,b) \sim (c,d) \Leftrightarrow ad = bc$. Esta es una relación de equivalencia:

- Reflexión: $(a,b) \sim (a,b) \Leftrightarrow ab = ba$ y como R es dominio entero, conmuta.
- Simetría: $(a,b) \sim (c,d) \Leftrightarrow ad = bc \Leftrightarrow bc = ad \Leftrightarrow (c,d) \sim (a,b)$.
- Transitividad: Sea $(a,b) \sim (c,d)$ y $(c,d) \sim (e,f) \Leftrightarrow ad = bc$ y $cf = de \Rightarrow adf = bcf \Rightarrow adf = bde \Rightarrow (af - be)d = 0$ y como $d \neq 0 \Rightarrow af = be \Rightarrow (a,b) \sim (e,f)$.

Denotamos la clase de equivalencia de (a,b) por $\frac{a}{b}$. Sea $F_R = {}^{X}\!/_{\sim} = \left\{\frac{a}{b}|a \in R, b \in R^*\right\}$. Definimos ahora $+ : F_R \times F_R \longrightarrow F_R$ con $(\frac{a}{b}, \frac{c}{d}) \mapsto \frac{ad+bc}{bd}$ y $\cdot : F_R \times F_R \longrightarrow F_R$ tal que $(\frac{a}{b}, \frac{c}{d}) \mapsto \frac{ac}{bd}$

Ahora, es sencillo notar que F_R es en realidad un campo, sin embargo es tedioso y un atentado contra la ecología, así que si el lector lo quiere verificar, lo puede hacer por su cuenta.

Capítulo 6

Polinomios

Sea R un anillo. Consideremos $P(R) = \{(a_0, a_1, \dots, a_n) | a_i \in R$ y $a_i \neq 0$ para un número finito$\}$. Definimos $(a_i) = (a_1, a_2, \dots, a_n) \in P(R)$ Le damos a $P(R)$ estructura de anillo con $(a_i) + (b_i) = (a_i + b_i)$ y con $(a_i)(b_i) = (\sum_{j=0}^{i} a_i b_{i-j})$.

Proposición 6.1. *Si R es anillo, entonces $P(R)$ es anillo. $P(R)$ es conmutativo si, y sólo si R es conmutativo. $P(R)$ es anillo con $1_{P(R)}$ si, y sólo si R es un anillo con 1_R.*

Sea R un anillo con 1 y sea $x = (0, 1, 0, \dots) \in P(R)$. Notemos que $x^2 = (0, 0, 1, 0, \dots), x^3 = (0, 0, 0, 1, \dots)$, en general, x^n tiene n ceros antes del primer, y único 1, y ceros después. Luego, podemos escribir un elemento $(a_i) \in P(R)$ como $f(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n + \cdots$ y tenemos un monomorfismo de anillos $R \longrightarrow P(R)$ con $a \mapsto (a, 0, \dots)$, así que R es un subanillo de $P(R)$.

Definición 6.2. Si $a_n \neq 0$ y $a_m = 0$ para toda $m > n$ entonces diremos que (a_i) tiene grado n y escribimos $\deg(a_i) = n$. Una convención es decir que (0) tiene grado $-\infty$.
Si $f(x) \in R[x]$ tiene grado n y $f(x) = a_0 + a_1 x + \cdots + a_n x^n$ entonces a_n se llama coeficiente principal de $f(x)$.

Dado $(a_i) \in P(R)$, podemos definir una función $P(R) \longrightarrow \{R \longrightarrow R\}$ con $(a_i) = f(x) \mapsto \{r \mapsto f(r) = a_0 + a_1 r + \cdots + a_n r^n + \cdots\}$.

Notación 6.3. $P(R) = R[x]$.

Proposición 6.4. *Sea R un anillo con 1 y sean $f(x), g(x) \in R[x]$. Entonces*

1. $\deg f(x) + g(x) \leq \text{máx}\{\deg f(x), \deg g(x)\}$.
2. $\deg f(x)g(x) \leq \deg f(x) + \deg g(x)$.

En el segundo inciso, si R no tiene divisores de cero, entonces se cumple la igualdad.

Demostración 6.5. Supongamos $\deg f(x) = m$ y $\deg g(x) = n$ entonces:

1. $f(x) = (a_0, a_1, \dots, a_m, 0, \dots), g(x) = (b_0, b_1, \dots, b_n, 0, \dots)$ si $j > \text{máx}\{m, n\} \Rightarrow a_j + b_j = 0 \therefore \deg f(x) + g(x) \leq \text{máx}\{m, n\}$.
2. Sea $(c_i) = f(x)g(x) = (\sum_{j=0}^{i} a_j b_{i-j})$ entonces $c_{n+m+k} = \sum_{j=0}^{n+m+k} a_j b_{n+m+k-j}$. Si $j > m$ entonces $a_j = 0$ y si $n + m + k - j > n \rightarrow m + k > j$ entonces $b_j = 0$ y como siempre sucede uno de estos dos caso, entonces $c_{n+m+k} = 0$ para todo $k \geq 1$ por lo tanto $\deg f(x)g(x) \leq m + n$. Ahora, si R no tiene divisores de cero, entonces $c_{n+m} = \sum_{j=0}^{n+m} a_j b_{n+m-j} = \sum_{j=0}^{m} a_j b_{n+m-j} = a_m b_n$ como $a_m, b_n \neq 0$ entonces $a_m b_n \neq 0$ por lo tanto $\deg f(x)g(x) = m + n$

Proposición 6.6. *Supongamos que R es un anillo con 1 sin divisores de cero, entonces $f(x) \in U(R[x]) \Leftrightarrow f(x) \in U(R)$.*

Demostración 6.7. Si $f(x) \in U(R)$ entonces existe $r \in U(R)$ tal que $f(x)r = 1$, como $R \subset R[x]$ entonces $r \in R[x]$ por lo tanto $f(x) \in U(R[x])$. Luego, si $f(x) \in U(R[x])$ entonces existe $g(x) \in R[x]$ tal que $f(x)g(x) = 1$, luego, por la proposición anterior, $0 = \deg f(x)g(x) = \deg f(x) + \deg g(x) \Rightarrow \deg f(x) = \deg g(x) = 0 \Rightarrow f(x), g(x) \in R \Rightarrow f(x) \in U(R)$.

Proposición 6.8. *R no tiene divisores de cero si, y sólo si $P(R)$ no tiene divisores de cero.*

Demostración 6.9. Si R tiene divisores de cero, entonces $P(R)$ tiene divisores de cero, pues $R \subset P(R)$. Supongamos que R no tiene divisores de cero. Sean

$(a_i), (b_i) \in P(R)$ tales que $(a_i)(b_i) = (0)$ entonces $a_0 b_0 = 0$, como R no tiene divisores de cero, suponemos $a_0 \neq= 0 \rightarrow b_0 = 0$. Sea $i = \text{mín}\,\{j | b_j \neq 0\}$ entonces la entrada i es $0 = a_0 b_i + a_1 b_{i-1} + cdots + a_i b_0 = a_0 b_i \Rightarrow b_i = 0$ y esto es una contradicción, así que $(b_i) = (0)$, por lo tanto $P(R)$ no tiene divisores de cero.

Definición 6.10. Si R, S son conmutativos, con $R \subseteq S$ y $1_r = 1_s$, entonces un elemento $a \in S$ se llama algebraico sobre R si existe $f(x) \in R[x]$ con $f(x) \neq 0$ tal que $f(a) = 0$. Si no es algebraico sobre R entonces se llama trascendente.

Teorema 6.11 (Algoritmo de la división para polinomios)**.** *Sea R un anillo conmutativo con 1 y sean $f(x), g(x) \neq 0 \in R[x]$. Entonces, si b es el coeficiente principal de $g(x)$, existen $k \in \mathbb{Z}$, $q(x), r(x) \in R[x]$ tales que $b^k f(x) = q(x)g(x) + r(x)$ y $\deg r(x) < \deg g(x)$. Si b no es divisor de cero, entonces $q(x)$ y $r(x)$ son únicos. Si $b \in U(R)$ entonces podemos tomar $k = 0$.*

Demostración 6.12. Si $\deg f(x) < \deg g(x)$ escribimos $f(x) = 0.g(x) + f(x) \Rightarrow k = 0, q(x) = 0, r(x) = f(x)$ y terminamos. Supongamos entonces que $\deg f(x) = m \geq n = \deg g(x)$. Lo probaremos por inducción sobre m. Sea a el coeficiente principal de $f(x)$. Sea $f_1(x) = bf(x) - ax^{m-n} g(x)$. Entonces $\deg f_1(x) < m$, por hipótesis de inducción existen $k \in \mathbb{Z}$ y $q(x), r(x) \in R[x]$ tales que $b^k f_1(x) = q(x)g(x) + r(x)$, entonces $b^{k+1} f(x) = b^k (bf(x)) = b^k (f_1(x) + ax^{m-n} g(x)) = q(x)g(x) + r(x) + b^k a x^{m-n} g(x) \Rightarrow b^{k+1} f(x) = (q(x) + b^k a x^{m-n}) g(x) + r(x)$.
Supongamos que b no es divisor de cero y que $b^k f(x) = q(x)g(x) + r(x) = q_1(x)g(x) + r_1(x)$, entonces $(q(x) - q_1(x))g(x) = r_1(x) - r(x)$.
Como $\deg r(x), \deg r_1(x) < \deg g(x) \Rightarrow \deg g(x) > \deg r_1(x) + r(x) = \deg(q(x) - q_1(x))g(x)$ entonces, como b no es divisor de cero, se cumple que $\deg g(x) = \deg q(x) - q_1(x) + \deg g(x) \Rightarrow \deg q(x) - q_1(x) = -\infty \Rightarrow q(x) - q_1(x) = 0 \Rightarrow q(x) = q_1(x)$.
Supongamos ahora que $b \in U(R)$, entonces tomamos $q'(x) = b^{-k} q(x)$ y $r'(x) = b^{-k} r(x) \Rightarrow f(x) = q'(x)g(x) + r'(x)$.

Capítulo 7

Divisibilidad

Definición 7.1. Sea R un dominio entero con 1, sean $a, b \in R$. Diremos que a divide a b o que b es múltiplo de a si existe $c \in R$ tal que $b = ac$. Lo denotamos por $a|b$. Si $a|b$ y $b|a$ entonces diremos que a y b están asociados y lo denotamos por $a \sim b$.

Lema 7.2. *La relación $a \sim b$ en R es de equivalencia.*

Demostración 7.3.

- Reflexividad) $a \sim a \Leftrightarrow a|a \Leftrightarrow a = ac$ y si tomamos $c = 1$ esto es cierto.
- Simetría) $a \sim b \Leftrightarrow a|b$ y $b|a \Leftrightarrow b \sim a$.
- Transitividad) $a \sim b, b \sim c \Rightarrow a|b, b|a, b|c, c|b \Rightarrow a = a_1 b, b = b_1 a, b = b_2 c, c = c_1 b \Rightarrow a = a_1 b_2 c, c = c_1 b_1 a \Rightarrow a|c$ y $c|a \Rightarrow a \sim c$.

Si R es dominio entero con 1, entonces ¿Quién es la clase de $a \in R$ con $\sim$?

Proposición 7.4. *La clase de $a \in R$ bajo $\sim$ es $aU(R)$.*

Demostración 7.5. Sea $ar \in U(R)$, entonces como $a|ar$ y como $arr^{-1} = a \Rightarrow ar|a$ entonces $a \sim ar$. Supongamos $a \sim b \Rightarrow a|b, b|a \Rightarrow a = a_1 b, b = b_1 a \Rightarrow a = a_1 b_1 a \Rightarrow a_1 b_1 = 1 \Rightarrow b_1 \in U(R) \Rightarrow b = b_1 a \in aU(R)$.

Definición 7.6. Sea R un dominio entero con 1. Diremos que $b \in R$ es irreducible si sus únicos divisores son unidades de R y asociados de b. Un elemento $p \in R^*$ es primo si satisface que: $p|ab \Rightarrow p|a$ ó $p|b$.

Proposición 7.7. *Si p es primo, entonces p es irreducible.*

Demostración 7.8. Supongamos $p = ab$ con $a, b \notin U(R)$, entonces $p|ab$. Supongamos $p|a \Rightarrow a = pc \Rightarrow p = pcb \Rightarrow p(1 - cb) = 0 \Rightarrow cb = 1 \Rightarrow b \in U(R)$ y esto es una contradicción, por lo tanto p es irreducible.

Lema 7.9. *Si R es un anillo conmutativo con 1, entonces el conjunto $\langle a \rangle = \{ar | r \in R\}$ es un ideal.*

Definición 7.10. Un dominio entero con 1, R,es un dominio de ideales principales (DIP) si todo ideal en R es principal, es decir, es de la forma $\langle a \rangle$ para algún $a \in R$.

Proposición 7.11 (Ver tarea 8)**.** *Si R es un DIP, entonces todo elemento irreducible en R es primo.*

Definición 7.12. Un dominio entero R con 1 se llama Euclideano si existe una función $d : \mathbb{R}^* \longrightarrow \mathbb{Z}^{\geq 0}$ tal que:

- Si $a, b \in R^*$ y $a|b$ entonces $d(a) \leq d(b)$.
- Si $a, b \in R, b \neq 0$ entonces existen $q, r \in R$ tales que $a = bq + r$ con $r = 0$ ó $d(r) < d(b)$.

Lema 7.13. *Si R es Euclideano, entonces $U(R) = \{a \in R | d(a) = d(1)\}$.*

Demostración 7.14. Supongamos $a \in U(R)$, entonces existe $b \in R^*$ tal que $ab = 1 \Rightarrow a|1 \Rightarrow d(a) \leq d(1)$ y como $1 \cdot a = a \Rightarrow 1|a \Rightarrow d(1) \leq d(a)$ por lo tanto $d(a) = d(1)$.
Supongamos ahora que $d(a) = d(1)$, entonces existen $q, r \in R$ tales que $1 = aq + r$. Supongamos $r \neq 0$ entonces $1|r \Rightarrow d(1) \leq d(r) < d(a) = d(1)$!! y esto es una contradicción, por lo tanto $r = 0$, entonces $1 = aq \Rightarrow a \in U(R)$.

Proposición 7.15. *Si R es Euclideano, entonces R es DIP.*

Demostración 7.16. Sea $I \subset R$ un ideal distinto de cero. Sea $b \in I^*$ tal que $d(b)$ es mínimo. Es claro que $\langle b \rangle \subseteq I$. Sea $a \in I$, entonces existen $q, r \in R$ tales que $a = bq + r$ con $r = 0$ o $d(r) < d(b)$, luego $r = a - bq \in I$. Supongamos $r \neq 0$, entonces $d(r) < d(b)$, pero como $d(b)$ es mínimo en I, es una contradicción, por lo que $r = 0$, entonces $a = bq \Rightarrow a \in \langle b \rangle$ por lo tanto $I = \langle b \rangle$.

Definición 7.17. Un común divisor de dos elementos a y b en un dominio entero con 1, R, es un elemento $c \in R$ tal que $c|a$ y $c|b$.
Un común divisor $d \in R$ de a y b es un máximo común divisor (mcd) si todo común divisor de a y b divide a d.

Proposición 7.18. *Sea R un DIP y $a, b \in R$. Entonces existe un mcd de a y b al que denotaremos por (a, b). Este mcd es único salvo por asociados y se puede expresar como $xa + yb$ para algunos $x, y \in R$.*

Demostración 7.19. Consideremos $I = \langle a, b \rangle = \{au + bv | u, v \in R\}$. Como R es DIP, existe $d \in R$ tal que $\langle a, b \rangle = \langle d \rangle$. Como $a, b \in \langle d \rangle \Rightarrow d|a, d|b$. Supongamos que $c|a$ y $c|b$. Como $d \in \langle a, b \rangle \Rightarrow \exists x, y \in R$ t.q. $d = xa + yb \Rightarrow c|d$. Si d_1 es un mcd de a y b, entonces $d_1|d$ y $d|d_1$ por lo tanto $d_1 \sim d$.

Corolario 7.20. *Si R es un DIP, todo elemento irreducible es primo.*

Demostración 7.21. Sea $p \in R$ irreducible. Supongamos que $p|ab$ y $p \nmid a$. Notemos que $(p, a) = 1$ pues los únicos divisores de p son unidades y asociados. Entonces existen $x, y \in R$ tales que $1 = xp + ya \Rightarrow b = xbp + yab$ como $p|yab$ y $p|xbp$ entonces $p|b$.

Definición 7.22. Una cadena ascendente infinita $I_1 \subseteq I_2 \subseteq \cdots$ de ideales de un anillo R termina si existe $k \in \mathbb{Z}^{\geq 1}$ tal que $I_l = I_k$ para todo $l \geq k$.
Un anillo R tiene la condición de cadenas ascendentes (CCA) si toda cadena ascendente termina.
Un anillo con esta condición se llama Noetheriano.

Proposición 7.23. *Si R es un DIP, entonces R es Noetheriano.*

Demostración 7.24. Sea R un DIP y $I_1 \subseteq I_2 \subseteq \cdots$ una cadena ascendente de ideales de R, entonces $I = \cup_{k\geq 1} I_k$ es un ideal. Entonces existe $a \in R$ tal que $I = \langle a \rangle$ así que $a \in I_l$ para algún $l \in \mathbb{Z}^{\geq 1} \Rightarrow \langle a \rangle = I \subseteq I_l \subseteq I_k \subseteq I$ para todo $k \geq l \Rightarrow I_l = I = I_k$ para todo $k \geq l$. Por lo tanto R en Noetheriano.

Definición 7.25. un dominio de factorización única (DFU) es un dominio entero con 1, R, en el cual todo elemento $r \in R^* - U(R)$ es el producto de elementos irreducibles y todo elemento irreducible es primo.

Proposición 7.26. *SI R es un DIP, entonces R es un DFU.*

Demostración 7.27. Sea $X = \{x \in R^* - U(R)\}$ tal que x no puede expresarse como el producto de irreducibles. Sea $a_1 \in X$. Como $a \notin U(R)$ entonces $\langle a \rangle \subsetneq R$. Construimos una cadena de ideales $\langle a \rangle \subseteq I_1 \subseteq I_2 \subseteq \cdots$ Como R es DIP, entonces existen $a_i \in X$ tales que $\langle a_i \rangle = I_i$. Como R es Noetheriano, existe a_n tal que $\langle a_n \rangle = I_l$ para todo $l \geq n$. Como $a_n \in X$, entonces a_n no es irreducible, entonces $a_n = a_{n+1}b$. Supongamos, sin pérdida de generalidad que $a_{n+1} \in X$, entonces $\langle a_n \rangle \subsetneq \langle a_{n+1} \rangle$ pues si $a_{n+1} = a_n c = a_{n+1}bc \Rightarrow bc = 1 \Rightarrow b \in U(R)$ y la cadena termina, entonces no sucede.

Recordemos que si R, S son anillos, entonces $R \oplus S$ es un anillo con las operaciones ya definidas. y se llama la suma directa de los anillos R y S. Si $R_1, R_2, \ldots, R_n$ son anillos, entonces $R_1 \oplus \cdots \oplus R_n$ es un anillo, y es conmutativo si, y sólo si R_i es conmutativo para toda i, y tiene 1 si, y sólo si R_i tiene 1 para toda i y $1 = (1_1, 1_2, \ldots, 1_n)$.

Si I y J son ideales de un anillo R, podemos definir $IJ := \{ab : a \in I, b \in J\}$ y $I + J = \{a + b : a \in I, b \in J\}$. Una observación es que $IJ \subset I \cap J$.
En general podemos definir para $I_1, \ldots, I_n$ ideales de R, $\prod_{i=1}^n I_i = \{a_1 a_2 \cdots a_n | a_i \in I_i\} \subset \cap_{i=1}^n I_i$.

Proposición 7.28. *Sea R un anillo con 1. Sean I, J ideales de R tales que $I+J = R$. Dados $r_1, r_2 \in R$ existe $r \in R$ tal que $r \equiv r_1 \mod I$ y $r \equiv r_2 \mod J$.*

Esto quiere decir que el sistema:

$$\begin{aligned} x &\equiv r_1 \mod I \\ x &\equiv r_2 \mod J \end{aligned}$$

tiene solución en R.

Demostración 7.29. Como $R = I + J$ entonces existen $a \in I$ y $b \in J$ tales que $1 = a + b$. Sea $r = r_2a + r_1b$. Entonces:

- $r - r_1 = r_2a + r_1(b-1) = r_2a + r_1(-a) = (r_2 - r_1)a \in I \Rightarrow r \equiv r_1 \mod I$.
- $r - r_2 = r_1b + r_2(a-1) = r_1b + r_2(-b) = (r_1 - r_2)b \in J \Rightarrow r \equiv r_2 \mod J$.

En general, se puede definir un morfismo de anillos

$$\begin{aligned} \varphi : R &\longrightarrow {}^{R}\!/_{I} \oplus {}^{R}\!/_{J} \\ r &\longmapsto (r + I, r + J) \end{aligned}$$

y $ker(\varphi) = \{r \in R : r \in I, r \in J\} = I \cap J$ y por la proposición anterior, tenemos que φ es suprayectiva si $I + J = R$. Entonces ${}^{R}\!/_{I+J} \simeq {}^{R}\!/_{I} \oplus {}^{R}\!/_{J}$.

Teorema 7.30 (Chino del Residuo)**.** *Sea R un anillo con 1. Sean $I_1, \ldots, I_n$ ideales de R tales que $I_j + I_k = R$ si $j \neq k$. Dados $r_1, \ldots, r_n \in R$, existe $r \in R$ tal que $r \equiv r_i \mod I_i$. Es decir, el sistema:*

$$\begin{aligned} x &\equiv r_1 \mod I_1 \\ &\vdots \\ x &\equiv r_n \mod I_n \end{aligned}$$

tiene solución en R. Además, si $\tilde{r} \equiv r_i \mod I_i$ entonces $\tilde{r} \equiv r \mod \cap_{i=1}^{n} I_i$.

Demostración 7.31. Sean $a_i \in I_1, b_j \in I_j$ para $1 < j \leq n$ tales que $1 = a_j + b_j$, luego $1 = 1^{n-1} = (a_2 + b_2)(a_3 + b_3) \cdots (a_n + b_n) \in I + \prod_{j=2}^{n} I_j = R$. Por la proposición anterior, existe $s_1 \in R$ tal que $s_1 \equiv 0 \mod \prod_{j=2}^{n} I_j$ y $s_1 \equiv 1 \mod I_1$. Como $\prod_{j=2}^{n} I_j \subset I_k \forall\ 1 < k \leq n$, entonces $s_1 \equiv 0 \mod I_k \forall\ 1 < k \leq n$. Haciendo la misma construcción fijando los demás I_j para $1 < j \leq n$ tenemos que existen $s_k \in R$ tales que $s_k \equiv 0 \mod I_j$ con $j \neq k$ y $s_k \equiv 1 \mod I_k$ para

toda $1 \leq k \leq n$. Sea $r = \sum_{i=1}^{n} r_i s_i$, entonces $r - r_j = \sum_{i \neq j} r_i s_i + r_j s_j - r_j = \sum_{i \neq j} r_i s_i + r_j(s_j - 1) \in I_j$.

Si $\tilde{r} \equiv r_j \mod I_j$ para toda $1 \leq k \leq n$, entonces $\tilde{r} \equiv r \mod I_j$ para toda $1 \leq k \leq n$ por lo tanto $r - \tilde{r} \in \cap_{j=1}^{n} I_j \Rightarrow \tilde{r} \equiv r \mod \cap_{j=1}^{n} I_j$.

Capítulo 8

Problemas

8.1. Tarea 1

Problema 1. Da la definición de grupo.

Problema 2. Da tres ejemplos de grupos abelianos.

Problema 3. Sea G un grupo con elemento identidad e. Demuestra que si $aa = e$, entonces $a = e$.

Problema 4. Da un ejemplo de un grupo no abeliano.

Problema 5. Describe todos los grupos de orden 3.

Problema 6. Demuestra que todo grupo G con elemento identidad e tal que $xx = e$ es abeliano.

Problema 7. Probar que un conjunto no vacío G con una operación binaria en G tal que las ecuaciones:

$$ax = b \tag{8.1.0.1}$$

$$ya = b \tag{8.1.0.2}$$

tienen solución en G para todo $a, b \in G$, es un grupo.

Problema 8. Sea G un grupo de orden $2n$. Demuestra que existe un elemento $a \in G$, distinto a la identidad e tal que $a^2 = e$.

Problema 9. Sea G un grupo. Demuestra que para doto $x \in G$ y $m, n \in \mathbb{Z}$, se tiene que $x^m x^n = x^{m+n}$ y $(x^m)^n = x^{mn}$.

Problema 10. Sea $G = \langle x \rangle$ un grupo cíclicode orden n. Sean $m, k \in \mathbb{Z}$, demuestra que $x^m = x^k$ si, y sólo si :

$$m \equiv k \pmod{n}$$

Demuestra que el elemento x^m genera a G si, y sólo si m, n son primos relativos.

Problema 11. Demuestra que Sim_n tiene $n!$ elementos.

8.1.1. Extras a Tarea 1

Problema 12. Demostrar que las simetrías del triángulo son 1_T, ϕ_1, ϕ_2, σ_1, σ_2, σ_3 y nada más.

Problema 13. Sea $S^{-1} := \{x^{-1} | x \in S\}$.
Demostrar que $\langle S \rangle = \{x_1 \cdot x_2 \cdot \cdots \cdot x_k | x_i \in S \cup S^{-1}, k \in \mathbb{Z}\}$

8.2. Tarea2

Problema 14. Si G es un grupo y $f : G \longrightarrow G$ está definido por $f(x) = x^{-1}$ para todo $x \in G$, demostrar que f es homomorfismo si, y sólo si G es abeliano.

Problema 15. Sea G un grupo y $H \leq G$. Sean $x, y \in G$. Demostrar que $xH = yH$ o $xH \cap yH = \emptyset$

Problema 16. Demostrar que un grupo de orden primo es cíclico.

Problema 17. Sea G un grupo y sea $a \in G$. Demuestra que la aplicación: $T_a : G \longrightarrow G$ con $x \mapsto a^{-1}xa$, es un automorfismo.

Problema 18. Probar que si N y M son subgrupos normales de un grupo G, entonces $N \cap M$ es normal en G.

Problema 19. Demostrar que si H y N son subgrupos de un grupo G, y N es un subgrupo normal en G, entonces $H \cap N$ es normal en H.

Problema 20. Sea G un grupo que contiene un subgrupo de orden finito s. Demostrar que la intersección de todos los subgrupos de orden s es un subgrupo normal en G.

Problema 21. Sea N un subgrupo normal de un grupo finito G, y sea $m = |G| \,/\, |N|$. Demostrar que $a^m \in N$ para todo $a \in G$.

Problema 22. Demostrar que si H y N son subgrupos normales de G y $H \cap N = \{e\}$, entonces $hn = nh$ para todo $h \in H,\ n \in N$

Problema 23. Demuestra usando el Teorema de Lagrange que si a es un entero y p un primo, entonces $a^p \equiv a \pmod{p}$.

Problema 24. Demostrar que un grupo de orden p^m donde p es un primo y m un entero positivo, tiene un subgrupo de orden p.

Problema 25. Demostrar que los elementos de orden finito de un grupo abeliano G forman un subgrupo.

8.3. Tarea 3

[Problemas con (*) valen puntos extras]

Problema 26. Sean H y K subgrupos de un grupo G tales que $H \leq K \leq G$. Supongamos que los índices $[G : K]$ y $[H : K]$ son finitos. Demuestra que $[G : K]$ es finito y que $[G : K] = [G : H]/[H : K]$.

Problema 27. (*) Supongamos que G es un grupo finito, K es un subgrupo normal en G y H un subgrupo de G. Si $|K|$ es primo relativo con $[G : H]$ demostrar que $K \leq H$.

Problema 28. Si $A, B \leq G$ y $[G : A]$, $[G : B]$ son finitos, demostrar que $[G : a \cap B] \leq [G : A][G : B]$, con igualdad si, y sólo si $G = AB$.

Problema 29. Supongamos que S es un subconjunto de un grupo finito G, con $|S| > \frac{|G|}{2}$. Definimos $S^2 = \{xy|x, y \in S\}$, demostrar que $G = S^2$.

Problema 30. Si $[G : A]$ y $[G : B]$ son finitos y primos relativos, demostrar que $G = AB$.

Problema 31. (*) Si G no es abeliano demostrar que $Z(G)$ esta contenido de manera propia en un subgrupo abeliano de G.

Problema 32. Supongamos que un grupo G actúa en S. Sean $x \in G$, $s \in S$. Demostrar que $Stab_G(xs) = xStab_G(s)x^{-1}$.

Problema 33. Considera el grupo de racionales $\mathbb{Q}$ con la suma. Demuestra que todo automorfismo de $\mathbb{Q}$ es de la forma $\mathbb{Q} \longrightarrow \mathbb{Q}$ con $x \mapsto cx$, para algún $c \in \mathbb{Q} - \{0\}$

Problema 34. Demuestra que todo subgrupo normal de un grupo G es el kernel de un homomorfismo con dominio G.

Problema 35. Demuestra que si G es un grupo actuando en un conjunto S, entonces el estabilizador de todo elemento $s \in S$ es un subgrupo de G.

Problema 36. Sea G un grupo actuando en un conjunto S. Demuestra que esta acción induce una parición en G.

Problema 37. Demuestra que la aplicación $\mathbb{R}^* \times \mathbb{R}^2 \longrightarrow \mathbb{R}^2$ con $(t, (x, y)) \mapsto (tx, t^{-1}y)$, define una acción del grupo multiplicativo $\mathbb{R}^*$ en el conjunto $\mathbb{R}^2$ y que las hipérbolas $\{(x, y)|xy = c \in \mathbb{R}\}$ son órbitas de ésta acción. Describe el resto de las órbitas.

Sea G un grupo y $S = \{A \subset G\}$, es decir, la familia de todos los subconjuntos de G. Considerar la aplicación $G \times S \longrightarrow S$ tal que $(x, A) \mapsto xAx^{-1} = \left\{xax^{-1}|a \in A\right\}$

Problema 38. Demostrar que la aplicación anterior es una acción del grupo G en S.

Los elementos de $Orb_G(A)$ se llaman conjuntos G-conjugados de A, $Stab_G(A)$ se llama el normalizador de A en G y se denota por $N_G(A)$.

Problema 39. Sea G un grupo y H un subgrupo de G, demuestra que:

- $N_G(H) \leq G$,
- H es un subgrupo normal de $N_G(H)$,
- H en normal en G si, y sólo si $N_G(H) = G$

Problema 40. (*) Sea G un grupo y H, K subgrupo de G. Supongamos que K es subgrupo de $N_G(H)$. demuestra que ${}^{KH}/_{H}$ es isomorfo a ${}^{K}/_{H\cap K}$

8.4. Tarea 4

Problema 41. Sea G un grupo y sean A, B subgrupos finitos de G. Demostrar que $|AB|\,|A \cap B| = |A|\,|B|$.

Problema 42. Sea G un grupo finito, $H \leq G$, $[G : H] = n$ y $|G|$ no divide a $n!$. Demostrar que existe un subgrupo normal K de G, $K \neq \{1\}$, tal que $K \leq H$

Problema 43. Si $|G| = p^n$, con p primo, demostrar que G tiene subgrupos $G_0, G_1, \ldots, G_n$, tales que $i = G_0 \leq G_1 \leq \cdots \leq G_n = G$ y $[G_i : G_{i-1}] = p$, $1 \leq i \leq n$.

Problema 44. Demuestra que $\sigma \in S_n$ no puede expresarse como el producto de un número par de transposiciones y como el producto de un número impar de transposiciones.

Problema 45. Encontrar un subgrupo normal de orden 4 en A_4.

Problema 46. Sea S_n el grupo de permutaciones de n elementos con $n \geq 2$. Demuestra que:

a) toda permutación en S_n puede escribirse como un producto de $n - 1$ transposiciones.

b) toda permutaci—'on en S_n que no es un ciclo, puede escribirse como un producto de a los más $n-2$ transposiciones.

Problema 47. Enumera las permutaciones impares de 3 elementos. Encuentra A_3.

Problema 48. Probar que toda permutación de 8 elementos de orden 10 es impar.

Problema 49. Expresa las siguientes permutaciones de 8 elementos como producto de ciclos disjuntos y como producto de transposiciones:

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 8 & 2 & 6 & 3 & 7 & 4 & 5 & 1 \end{pmatrix}, \quad \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 6 & 4 & 1 & 8 & 2 & 5 & 7 \end{pmatrix}, \quad \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 1 & 4 & 7 & 2 & 5 & 8 & 6 \end{pmatrix}.$$

Problema 50. Demuestra que si $\sigma \in S_n$ es un k-ciclo, entonces $|\sigma| = k$. Si $\sigma = \sigma_1\sigma_2\cdots\sigma_m$, donde los σ_i son los k_i-ciclos disjuntos, entonces $|\sigma|$ es el mínimo común múltiplo de los k_is

8.5. Primer Parcial

La calificación máxima del examen se obtiene acumulando 10 puntos.

Problema 51 (1 punto)**.** Demuestra que un grupo de orden primo es cíclico.

Problema 52 (1 punto)**.** Sea G un grupo finito u H un subgrupo de G. Demuestra que si $[G : H] = 2$, entonces H es normal en G.

Problema 53 (1 punto)**.** Supongamos que un grupo G actúa en S. Sean $x \in G$, $s \in S$. Demostrar que

$$Est_G(xs) = xEsto_G(s)x^{-1}.$$

Problema 54 (1 punto)**.** Sea G un grupo y N un subgrupo normal, demuestra que N es el kernel de un homomorfismo con dominio G.

Problema 55 (2 puntos)**.** Sea G un grupo, S un subgrupo de G y N un subgrupo normal de G. Demostrar que si $S \cap N = \{1\}$ y $S \cup N = G$, entonces G/N es isomorfo a S.

Problema 56 (2 puntos)**.** Demuestra que si $\sigma \in S_n$ es un k-ciclo, entonces $|\sigma| = k$. Si $\sigma = \sigma_1\sigma_2 \cdots \sigma_m$, donde los σ_i con k_i-ciclos disjuntos, entonces $|\sigma|$ es el mínimo común múltiplo de los k_is.

Problema 57 (1 punto)**.** Demuestra que todo grupo G con elemento identidad 1 tal que $xx = 1$ para todo $x \in G$ es abeliano.

Problema 58 (2 puntos)**.** Demostrar que si un grupo abeliano con 6 elementos tiene un elemento de orden 3, entonces es cíclico.

Problema 59 (1 punto)**.** Probar que toda permutación de 8 elementos de orden 10 es impar.

8.6. Tarea 5

Problema 60. Encuentra todos los 3-subgrupos de S_4 y verifica que son conjugados entre si.

Problema 61. Sea G un grupo finito y sea p un primo que divide al orden de G. Probar que si G tiene sólo un p-subgrupo de Sylow, éste es normal y, por lo tanto, G no es simple.

Problema 62. Demuestra que todo grupo de orden 45 tiene un subgrupo normal de orden 9.

Problema 63. Demostrar que todo grupo de orden $(35)^3$ tiene un subgrupo normal de orden 125.

Problema 64. Demostrar que si P es un p-subgrupo de Sylow de un grupo finito G, entonces $g^{-1}Pg$ es un p-subgrupo de Sylow de G para todo $g \in G$.

Problema 65. Demuestra que todo p-subgrupo normal de un grupo finito G esta contenido en un p-subgrupo de Sylow de G.

Problema 66. Demostrar que no existen grupos simples de orden 255.

Problema 67. Para todo real r, $[r]$ denota el mayor entero menor o igual que r. Si p es un primo, demostrar que los p-subgrupos de Sylow de S_n tienen orden p^m, donde $m = [\frac{n}{p}] + [\frac{n}{p^2}] + [\frac{n}{p^3}] + \ldots$.

Problema 68. Demostrar que un grupo finito G es un p-grupo si, y sólo si $|G|$ es una potencia del primo p.

Problema 69. Demostrar que los únicos grupos simples de orden menor que 36 son aquellos de orden primo.

Problema 70. Supongamos que G es un grupo finito y H un subgrupo normal de G. Sea P un p-subgrupo de Sylow de H. Demostrar que $G = N_G(P)H$.

Problema 71. Demostrar que no existen grupos simples de orden 104, 176, 182 o 312.

Problema 72. Si G es un p-grupo. Demostrar que $Z(G)$ es cíclico si, y sólo si G tiene un único subgrupo normal de orden p.

8.7. Tarea 6

Problema 73. Sean $n, m \in \mathbb{Z}_{>0}$. Demuestra que $\mathbb{Z}_m \oplus \mathbb{Z}_n$ es isomorfo a $\mathbb{Z}_{nm}$ si, y sólo si n, m son primos relativos.

Problema 74. Describe todos los grupos abelianos de orden $24, 200, 1000, p^3, p^4$, donde p es un primo.

Problema 75. Demuestra que si ${}^{G}/_{Z(G)}$ es cíclico, entonces $G = Z(G)$ es abeliano. Concluir que si p es primo y $|G| = p^2$, entonces G es abeliano.

Problema 76. Sea G un grupo y A, B subgrupos normales de G. Demostrar que ${}^{G}/_{A\cap B}$ es isomorfo a un subgrupo de ${}^{G}/_{A} \times {}^{G}/_{B}$.

Problema 77. Sea R un anillo y sean $a, b \in R$. Demuestra que $0 \cdot a = 0 = a \cdot 0$, $(-a)(-b) = ab$.

Problema 78.

- Demostrar que $U(R)$ es un grupo con el producto de R.
- Encontrar $U(R)$ para $R = \mathbb{Z}$ y $R = \mathbb{Z}_n$.
- Si $R = M_2(\mathbb{Z})$, demostrar que $U(R)$ es el grupo de matrices $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ tales que $ad - bc = \pm 1$

Problema 79. Demostrar que si R_1 y R_2 son anillos, entonces las operaciones binarias

$$\begin{gathered}(R_1 \times R_2) \times (R_1 \times R_2) \longrightarrow R_1 \times R_2 \\ + : ((a_1, b_1), (a_2, b_2)) \mapsto (a_1 + a_2, b_1 + b_2) \\ \cdot : ((a_1, b_1), (a_2, b_2)) \mapsto (a_1 a_2, b_1 b_2)\end{gathered}$$

definen un anillo en $R_1 \times R_2$. Llamaremos a este anillo suma directa de R_1 y R_2 y lo denotamos $R_1 \oplus R_2$.

Problema 80. Sea R un anillo y sea R_1 el grupo $R \oplus \mathbb{Z}$. Definimos en R_1 la multiplicación

$$\begin{gathered}R_1 \times R_1 \longrightarrow R_1 \\ ((r, n), (s, m)) \mapsto (rs + mr + na, nm).\end{gathered}$$

Demostrar que con esta operación R_1 es un anillo con 1. Si $r \in R$ es identificado con $(r, 0) \in R_1$ demostrar que R es un subanillo de R_1. Concluir que todo anillo es subanillo de un anillo con 1.

Problema 81. Si $\{I_\alpha\}_{\alpha \in A}$ es una colección de ideales de un anillo R, demostrar que $\cap_{\alpha \in A} I_\alpha$ es un ideal de R.

Problema 82. Demostrar que el conjunto de elementos nilpotentes de un anillo conmutativo R es un ideal de R.

8.8. Tarea 7

Problema 83. Demuestra que un subconjunto no vacío I de un anillo R es un ideal si, y sólo si para todos $x, y \in I$, $z \in R$ se tiene que $x - y, zx, xz \in I$.

Problema 84. Demuestra que todos los ideales de $\mathbb{Z}$ son principales.

Problema 85. Demuestra que si R es un anillo e I y J son ideales de R y $J \subset I$, entonces ${}^{I}\!/_{J}$ es un ideal de ${}^{R}\!/_{J}$ y $({}^{R}\!/_{J})({}^{I}\!/_{J}) \simeq {}^{R}\!/_{I}$

Problema 86. Demuestra que si R es un anillo e I y J son ideales de R, entonces $I+J = \{x+y | x \in I, y \in J\}$ y $J \cap I$ son ideales y además ${}^{(I+J)}\!/_{I} \simeq {}^{J}\!/_{(J\cap I)}$.

Problema 87. Demuestra que el ideal $\langle n \rangle$ de $\mathbb{Z}$ es maximal si, y sólo si n es primo.

Problema 88. Sea R un anillo conmutativo con 1. Demuestra que un ideal I de R es maximal si, y sólo si ${}^{R}\!/_{I}$ es un campo.

Problema 89. Sea R un anillo conmutativo. Demuestra que

- un ideal P es primo si, y sólo si ${}^{R}\!/_{P}$ es un dominio entero.
- si R es un anillo con 1, entonces todo ideal maximal es primo.

Problema 90. Demuestra que $\sqrt{I}$ es un ideal de R y que si I es primo, entonces es radical.

Problema 91. Demuestra que si I y J son ideales de un anillo R, entonces $\sqrt{I \cap J} = \sqrt{I} \cap \sqrt{J}$.

Problema 92. Demuestra que:

$$\sqrt{I} = \bigcap_{\substack{P \text{ primo} \\ P \supset I}} P$$

En particular, la intersección de todos los ideales primos de R s el radical de $\langle 0 \rangle$, el cual es el ideal de elementos nilpotentes de R.

Sea R un anillo conmutativo con 1 y sea $S \subset R^*$ un semigrupo multiplicativo que no contiene divisores de cero. Sea $X = R \times S$, definimos en X la siguiente relación: $(a,b) \sim (c,d)$ si $ad = bc$.

Problema 93. Demuestra que $\sim$ es de equivalencia.

Problema 94. Denotar la clase de (a, b) por $\frac{a}{b}$, y el conjunto de estas clases por R_S. demostrar que R_S es un anillo conmutativo con 1.

Problema 95. Si $a \in S$, demostrar que $\left\{ \frac{ra}{a} | r \in R \right\}$ es un subanillo de R_S y que la aplicación $R \to R_S$, $r \mapsto \frac{ra}{a}$ es un monomorfismo, así R puede ser identificado con un subanillo de R_S.

Problema 96. Demostrar que todo elemento $s \in S$ es una unidad en R_S.

Problema 97. Dar una definición universal de R_S y demostrar que R_S es único salvo isomorfismo.

8.9. Tarea 8

Problema 98. Demuestra que el producto definido en $P(R)$ es asociativo.

Problema 99. Encontrar $U(\mathbb{Z}_4[x])$.

Problema 100. Sea R un anillo conmutativo con 1, $f(x) \in R[x]$ y $a \in R$. Demuestra que el residuo de la división de $f(x)$ por $x - a$ es $f(a)$.

Problema 101. Demuestra que $\sqrt{2} + \sqrt{3}$ es algebraico sobre $\mathbb{Z}$.

Problema 102. Si R es un anillo conmutativo con 1, $f(x) \in R[x]$ y $a \in R$, entonces existe una función $f : R \longrightarrow R$ con $a \mapsto f(a)$ a la que llamaremos función polinomial.

a) Si R es finito, demostrar que existen polinomios $f(x), g(x) \in R[x]$, tales que $f(x) \neq g(x)$, pero las funciones polinomiales asociadas son la misma, es decir $f(a) = g(a)$ para todo $a \in R$.

b) Dar ejemplos explícitos de funciones que satisfagan lo anterior.

c) Demostrar que si R es infinito, entonces la asignación $f(x) \to f$ es 1-1.

Problema 103. Sea $R = \left\{ a + b\sqrt{-5} : a, b \in \mathbb{Z} \right\} \subset \mathbb{C}$

a) Demostrar que R es un dominio entero con 1.

b) Demostrar que $U(R) = \{\pm 1\}$.

c) Demostrar que $3, a = 2 + \sqrt{-5}, b = 2 - \sqrt{-5}$ son irreducibles en R.

d) Demostrar que 3 no divide a a ni a b.

e) Concluir que 3 es irreducible, pero no primo.

Problema 104. Demuestra que si R es un DIP, entonces todo elemento irreducible de R es primo.

Problema 105. Sean R y S anillos conmutativos con $R \subset S, 1_R = 1_S$ y supongamos que R es un dominio entero. Demostrar que si $a \in S$ es trascendente sobre R y $g(x)$ es un polinomio no constante en $R[x]$, entonces $g(a)$ es trascendente sobre R.

Problema 106. Sea F un campo y sean $a_1, \ldots, a_n \in F$ elementos distintos, y sean $b_1, \ldots, b_n \in F$ elementos arbitrarios. Sean

$$p_i(x) = \prod_{j \neq i}(a - a_j), \;\; f(x) = \sum_{1 \leq i \leq n} \frac{b_i p_i(x)}{p_i(a_i)}.$$

Demostrar que f(x) es el único polinomio de grado menos o igual que $n-1$ sobre F tal que $f(a_i) = b_i$, para $1 \leq i \leq n$.

8.10. Tarea 9

Problema 107 (REVISAR!!)**.** Demostrar que $I = \langle 3, 2 + \sqrt{-5} \rangle = R = \left\{ a + b\sqrt{-5} : a, b \in \mathbb{Z} \right\}$

Problema 108. Demostrar que los anillos $\mathbb{Z}_6$ y $Z_3 \oplus \mathbb{Z}_2$ son isomorfos.

Problema 109. Resolver las congruencias $x \equiv 1(\text{mod}8), \; x \equiv 4(\text{mod}7), x \equiv 9(\text{mod}11)$ en el anillo $\mathbb{Z}$.

Problema 110. Sea R un dominio entero con 1. Demostrar que un ideal principal $P = \langle p \rangle$ es primo si, y sólo si p es primo en R

Problema 111. Demostrar que si R es un dominio Euclidiano, entonces R es un DFU

Problema 112. Un anillo R satisface la condición maximal si todo conjunto no vacío S de ideales de R contiene un elemento I_0 maximal respecto a la inclusión, es decir, si $I \in S$ y $I_0 \subset I$ entonces $I_0 = I$.
Demostrar que un anillo conmutativo con 1 es Noetheriano si, y sólo si satisface la condición maximal.

Problema 113. Sea R un anillo conmutativo. Demostrar que R es Noetheriano si, y sólo si todo ideal en R es finitamente generado, es decir, si I es un ideal de R, entonces existen $a_1, \ldots, a_n \in R$ tales que $I = \langle a_1, \ldots, a_n \rangle$.

Problema 114. Si R es un DIP, demostrar que todo ideal primo P no cero es maximal.

Problema 115. Sea R un dominio Euclideano y sean $a, b \in R$ tales que $ab \neq 0$. Considerar

$$\begin{aligned} a &= bq_1 + r_1 && d(r_1) < d(b) \\ b &= r_i q_2 + r_2 && d(r_2) < d(r_1) \\ r_1 &= r_2 q_3 + r_3 && d(r_3) < d(r_2) \\ &\vdots \\ r_{k-2} &= r_{k-1} q_k + r_k && d(r_k) < d(r_{k-1}) \\ r_{k-1} &= r_k q_{k+1} \end{aligned}$$

con $r_i, q_i \in R$. Demostrar que $r_k(a, b)$ y encontrar u, v rales que $(a, b) = ua + bv$.

Problema 116. Sea R un dominio Euclidiano y sean $a, b \in R^*$ tales que $a|b$ y $d(a) = d(b)$. Demostrar que a y b están asociados.

Problema 117. Sean $R_1, \ldots, R_n$ anillos con 1. Demostrar que $U(R_1 \oplus \cdots \oplus R_n) = U(R_1) \times \cdots \times U(R_n)$.

Problema 118. Resolver las congruencias $x \equiv i (\text{mod } 1+i)$, $x \equiv 1 (\text{mod } 2-i)$, $x \equiv 1+i (\text{mod } 3+4i)$, en el anillo de enteros Gaussianos $R = \left\{a + bi : a, b \in \mathbb{Z}\ i^2 = -1\right\}$

Problema 119. Resolver las congruencias $f(x) \equiv 1 (\text{mod } x-1)$, $f(x) \equiv x (\text{mod } x^2+1)$, $f(x) \equiv x^3 (\text{mod } x+1)$ en el anillos $F[x]$, donde F es un campo tal que $1+1 \neq 0$