Extraordinaria Estructuras Algebraicas

Antonio Cabrera Landín

23 de junio de 2025

Índice

1. Teoremas

Teorema 1.1 (Propiedad cancelativa)**.** *Para todo grupo $G = \{X, \cdot\}$ se cumple*

$$a \cdot c = b \cdot c \implies a = b \tag{1}$$

$$c \cdot a = c \cdot b \implies a = b \tag{2}$$

Demostración.

$$a \cdot c = b \cdot c \iff a \cdot c \cdot c^{-1} = b \cdot c \cdot c^{-1} \iff a \cdot e = b \cdot e \iff a = b \tag{3}$$

$$c \cdot a = c \cdot b \iff c^{-1} \cdot c \cdot a = c^{-1} \cdot c \cdot b \iff e \cdot a = e \cdot b \iff a = b \tag{4}$$

□

Teorema 1.2. *En cada grupo solo puede existir un elemento neutro.*

Demostración. Sea el grupo $G = \{X, \cdot\}$ asumamos que tenga dos elementos neutros e_1 y e_2, entonces

$$\begin{cases} x \cdot e_1 = x \\ x \cdot e_2 = x \end{cases} \implies x \cdot e_1 = x \cdot e_2 \iff x^{-1} \cdot x \cdot e_1 = x^{-1} \cdot x \cdot e_2 \iff e \cdot e_1 = e \cdot e_2 \iff e_1 = e_2 \tag{5}$$

□

Teorema 1.3. *Dado un grupo $G = \{X, \cdot\}$, si para cualquier elemento $a \in G$ se cumple que $a \cdot a = e$, entonces G es abeliano.*

$$\forall a \in G : a \cdot a = e \implies \forall a, b \in G : a \cdot b = b \cdot a \tag{6}$$

Demostración.

$$a \cdot b \in G \implies (ab)^2 = ab \cdot ab = e \tag{7}$$

$$\begin{aligned} &aabb = e \cdot e = e = (ab)^2 \implies a^{-1}(aabb) = a^{-1}(abab) \iff \\ &abb = bab \iff (abb)b^{-1} = (bab)b^{-1} \iff ab = ba \end{aligned} \tag{8}$$

□

Teorema 1.4. *Dado un grupo $G = \{X, \cdot\}$, si para todo $a, b \in G$ se cumple que $(a \cdot b)^2 = a^2 \cdot b^2$, entonces G es abeliano*

$$\forall a, b \in G : (a \cdot b)^2 = a^2 \cdot b^2 \implies \forall a, b \in G : a \cdot b = b \cdot a \tag{9}$$

Demostración.

$$\begin{aligned} &(a \cdot b)^2 = a^2 \cdot b^2 \implies abab = aabb \iff a^{-1}(abab) = a^{-1}(aabb) \iff \\ &bab = abb \iff (bab)b^{-1} = (abb)b^{-1} \iff ba = ab \end{aligned} \tag{10}$$

□

Teorema 1.5. *$\mathbb{Z}_n$ tiene $\varphi(n)$ generadores*

Demostración. Sea $g \in \mathbb{Z}_n$ y $n = |G|$ entonces:

$$\text{m.c.m.}(g, n) = \frac{gn}{\text{m.c.d.}(g, n)} = k \cdot g = l \cdot n \equiv 0 \mod n \implies \frac{gn}{\text{m.c.d.}(g, n)} = k \cdot g \iff k = \frac{n}{\text{m.c.d.}(g, n)} \tag{11}$$

Sabemos que este k es el orden de g ya que como $g \cdot k = n \cdot l \equiv 0 \mod n$ y además como es el mínimo común múltiplo será el primero en ser cero. Por lo tanto, g será un generador cuando $k = n$ y esto solo ocurre cuando el m.c.d.$(g, n) = 1$, es decir, cuando g es coprimo con n.
Como $\varphi(n)$ mide el número de números coprimos menores que n, además será el número de generadores en $\mathbb{Z}_n$ □

Teorema 1.6. *Dado un grupo $G = \{X, \cdot\}$, para todos sus elementos $a \in G$ el inverso del inverso de a es a.*

$$\forall a \in G : (a^{-1})^{-1} = a \tag{12}$$

Demostración.

$$(a^{-1})^{-1} \cdot a^{-1} = e \iff (a^{-1})^{-1} \cdot a^{-1} \cdot a = e \cdot a \iff (a^{-1})^{-1} = a \tag{13}$$

□

Lema 1.7. *Dado un grupo $G = \{X, \cdot\}$, para cada pareja $a, b \in G$ se cumple que $(a \cdot b)^{-1} = b^{-1}a^{-1}$*

Demostración.

$$\begin{aligned} &(a \cdot b)^{-1}(a \cdot b) = e \iff (a \cdot b)^{-1}(a \cdot b) \cdot b^{-1} = e \cdot b^{-1} \iff \\ &(a \cdot b)^{-1}a = b^{-1} \iff (a \cdot b)^{-1}a \cdot a^{-1} = b^{-1}a^{-1} \iff \\ &(a \cdot b)^{-1} = b^{-1}a^{-1} \end{aligned} \tag{14}$$

□

Teorema 1.8. *Dado un grupo $G = \{X, \cdot\}$, para cada pareja $a, b \in G$ el orden de ab es el mismo que el de ba*

$$\forall a, b \in G : (a \cdot b)^k = e \iff (b \cdot a)^k = e \tag{15}$$

Demostración.

$$\begin{aligned} &(ab)^k = ab \cdot ab \cdots ab = a \cdot (ba \cdots ba) \cdot b = a \cdot (ba)^{k-1} \cdot b = e \iff \\ &a^{-1} \cdot a \cdot (ba)^{k-1} \cdot b = a^{-1} \iff (ba)^{k-1} \cdot b = a^{-1} \iff \\ &(ba)^{k-1} \cdot b \cdot b^{-1} = a^{-1}b^{-1} \iff (ba)^{k-1} = a^{-1}b^{-1} \overset{\text{lema 1.7}}{=} (ba)^{-1} \iff \\ &(ba)^{k-1}(ba) = (ba)^{-1}(ba) \iff (ba)^k = e \end{aligned} \tag{16}$$

□

Teorema 1.9 (Teorema de Caley)**.** *Todo grupo G es isomorfo a un subgrupo de las biyecciones de G, $B(G)$, que es el grupo simétrico.*

Demostración. Consideremos las acciones de un elemento $\varphi_g(x) = gx$. Primero demostraremos que son biyectivas:

- Las acciones de un elemento son inyectivas ya que si consideramos $x \neq y$ entonces:

$$\begin{cases} \varphi_g(x) = gx \\ \varphi_g(y) = gy \end{cases} \tag{17}$$

  Por lo tanto:

$$x \neq y \implies gx \neq gy \implies \varphi_g(x) \neq \varphi_g(y) \tag{18}$$

- Las acciones son sobreyectivas ya que para cualquier imágen $x \in \mathrm{Im}f$ existe la preimagen $g^{-1}x$:

$$\varphi(g^{-1}x) = gg^{-1}x = x \in \mathrm{Im}f \tag{19}$$

  Por lo tanto como las acciones de un elemento son sobreyectivas e inyectivas, son también biyectivas.

A continuación, demostraremos las biyecciones de G, $B(G)$, es un grupo:

- Está correctamente definido:
  $\varphi_a \circ \varphi_b(x) = \varphi_a(\varphi_b(x)) = \varphi_a(bx) = abx \implies \varphi_a \circ \varphi_b = \varphi_{ab}$

- Como la operación es la composición de funciones, cumple con la propiedad asociativa.
- El neutro es $\varphi_e \in B(G)$:

$$\varphi_a \circ \varphi_e = \varphi_{a\cdot e} = \varphi_a \tag{20}$$

- El inverso de $\varphi_a \in B(G)$ es $\varphi_{a^{-1}} \in B(G)$:

$$\varphi_a \circ \varphi_{a^{-1}} = \varphi_{a\cdot a^{-1}} = \varphi_e \tag{21}$$

Ahora falta demostrar que es isomorfo al grupo original.

$$G \cong B(G) \tag{22}$$

Consideremos el morfismo $f : G \to B(G)$ tal que $f(g) = \varphi_g$. Demostraremos primero que se trata de un homomorfismo:

$$f(a \cdot b) = \varphi_{ab} = \varphi_a \circ \varphi_b \iff \varphi_a(\varphi_b(x)) = \varphi_a(bx) = abx = \varphi_{ab}(x) \tag{23}$$

Por último, demostraremos que este homomorfismo es biyectivo:

- El homomorfismo es inyectivo: Supongamos $a, b \in G : a \neq b$:

$$a \neq b \implies \forall x \in G : ax \neq bx \iff \varphi_a(x) \neq \varphi_b(x) \iff \varphi_a \neq \varphi_b \tag{24}$$

- El homomorfismo es suprayectivo, ya que para cada imagen $\varphi_a \in B(G)$ existe la preimagen $a \in G$.

Como el homomorfismo es biyectivo, hemos encontrador un isomorfismo de G a $B(G)$, por lo tanto, cualquier grupo G es isomorfo a un subgrupo de las biyecciones $B(G)$. □

Teorema 1.10. *El centro de un grupo es un subgrupo y es normal.*

Demostración. El centro $Z(G)$ es un subgrupo de G

1. El centro $Z(G)$, al mantener la operación de G, seguirá cumpliendo la propiedad asociativa.
2. El centro mantiene el neutro:

$$\forall x \in G : e \cdot x = x \cdot e \implies e \in Z(G) \tag{25}$$

3. Si x está en el centro entonces su inverso x^{-1} también:

$$\begin{aligned} &x \in Z(G) \implies \forall g \in G : g \cdot x^{-1} = x \cdot x^{-1} \cdot g \cdot x^{-1} = \\ &x^{-1} \cdot g \cdot x \cdot x^{-1} = x^{-1} \implies x^{-1} \in Z(G) \end{aligned} \tag{26}$$

□

Demostración. El centro $Z(G)$ es un subgrupo normal

$$\begin{aligned} &\forall h \in Z(G), g \in G : g \cdot h \cdot g^{-1} = g \cdot g^{-1} \cdot h = h \implies \\ &gHg^{-1} = H \implies Z(G) \text{ subgrupo normal} \end{aligned} \tag{27}$$

□

Teorema 1.11. *Todos los subgrupos de índice 2 son normales*

Demostración. Si un subgrupo tiene índice 2, significa que solo tiene dos clases laterales izquierdas y 2 clases laterales derechas.
Tendremos dos clases laterales izquierdas, aH y bH. Como e estará en una de las dos, podemos hablar de H y xH. Lo mismo ocurre con las clases laterales derechas, tendremos H y Hx

$$\begin{cases} H \cup xH = G \\ H \cup Hx = G \end{cases} \implies xH = Hx \implies H \text{ es normal} \tag{28}$$

□

Lema 1.12. *Si $a \in xH$ entonces $xH = aH$*

Demostración.

$$a \in xH \implies \exists h \in H : a = xh \iff aH = xhH \implies aH = xH \tag{29}$$

□

Teorema 1.13. *Las clases laterales izquierdas o coinciden o no tienen intersección.*

Demostración. Dado un grupo $G = \{X, \cdot\}$ con un subgrupo $H \subseteq G$. Supongamos que $\exists a \in xH$ que además $a \in yH$, entonces:

$$\begin{cases} a \in xH \implies \exists h_1 \in H : a = xh_1 \\ a \in yH \implies \exists h_2 \in H : a = yh_2 \end{cases} \implies xh_1 = yh_2 \iff$$
$$xh_1 \cdot h_1^{-1} = yh_2h_1^{-1} \iff x = yh_2h_1^{-1} = yh_3,\ h_3 \in H \implies x \in yH \tag{30}$$

Utilizando el lema 1, sabemos que $x \in yH \implies xH = yH$. □

Teorema 1.14 (Teorema de Lagrange)**.** *El orden del grupo es múltipo del orden del subgrupo*

$$H \subseteq G \implies |G| = |H| \cdot n \quad n \in \mathbb{N} \tag{31}$$

Demostración. Dado un grupo G con un subgrupo H y con clases laterales x_iH, por el teorema 1.13 sabemos que las clases laterales no tienen intersección. Como tienen que abarcar a todo el grupo G y no tienen intersección, entonces necesariamente el orden de G será múltiplo del orden de las clases laterales.

$$\sum_{i=1}^{\text{índice}} |x_iH| = |G| \implies |G| = |x_iH| \cdot n \quad n \in \mathbb{N} \tag{32}$$

Las clases laterales x_iH tienen el mismo orden que H, ya que se construyen operando x_i con los elementos de H, entonces el orden de G es múltiplo del orden de H.

$$|x_iH| = |H| \implies |G| = |H| \cdot n \quad n \in \mathbb{N} \tag{33}$$

□

Colorario 1.15. *El orden del grupo es múltiplo del orden de un elemento*

$$x \in G : x^k = e \implies |G| = k \cdot n \quad n \in \mathbb{N} \tag{34}$$

Teorema 1.16. *Cualquier grupo de orden primo es cíclico*

$$|G| = p \text{ primo} \implies \exists x \in G : x^p = e \tag{35}$$

Demostración. Por el colorario 1.15 sabemos que el orden del grupo tiene que ser múltiplo del orden de los elementos. Como el orden del grupo es primo, los elementos solo pueden tener orden 1 u orden p. Por el teorema 1.2, el único elemento de orden 1 es el neutro, entonces el resto de elementos del grupo tienen orden p. Como existe al menos un elemento de orden p, el grupo es cíclico. □

Teorema 1.17. *Si $H \subset G$ es un subgrupo, entonces gHg^{-1}, con $g \in G$, también lo es.*

$$H \subset G \implies gHg^{-1} \subset G \quad g \in G \tag{36}$$

Demostración. gHg^{-1} cumple con las tres propiedades del los subgrupos:

1. gHg^{-1} seguirá manteniendo la propiedad asociativa ya que solo hemos operado los elementos de H con elementos de G.

2. El elemento neutro $e \in G$ está en gHg^{-1}:

$$e \in H \implies g \cdot e \cdot g^{-1} = g \cdot g^{-1} = e \implies e \in gHg^{-1} \tag{37}$$

3. Cada elemento $x = ghg^{-1} \in gHg^{-1}$ tiene inverso x^{-1}:

$$ghg^{-1} \cdot g(h^{-1})g^{-1} = gh(h^{-1})g^{-1} \cdot g^{-1} = gg^{-1} = e \implies g(h^{-1})g = x^{-1} \in gHg^{-1} \tag{38}$$

□

Teorema 1.18. *Para todo grupo $G = \{X, \cdot\}$ con un subgrupo $H \subset G$:*

$$gHg^{-1} = H \quad g \in G \iff xH = Hx \tag{39}$$

Demostración. $\implies$

$$gHg^{-1} = H \iff gHg^{-1} \cdot g = Hg \iff gH = Hg \quad h \in G \tag{40}$$

□

Demostración. $\impliedby$

$$xH = Hx \implies xH \cdot x^{-1} = Hx \cdot x^{-1} \iff xHx^{-1} = H \quad x \in G \tag{41}$$

□

Teorema 1.19. *Las clases laterales izquierdas x_iH de un subgrupo H normal, forman un grupo.*

Demostración. Las clases laterales izquierdas de un subgrupo H cumplen con las tres propiedades de los grupos:

1. La operación no se sale del conjunto y por tanto conserva la propiedad asociativa:

$$xH = Hx \implies \forall a \in xH : xH \cdot yH = xyHH = xyH \implies ab \in xyH \tag{42}$$

2. El neutro pertenece a la clase lateral izquierda eH.

3. Todo elemento $a \in xH$ tiene inverso $a^{-1} \in (x^{-1})H$:

$$\forall a = xh_1 \in xH \; \exists a^{-1} = (x^{-1})h_2 \in (x^{-1})H : h_1x \cdot (x^{-1})h_2 = h_1h_2 \in eH \quad h_1, h_2 \in H \tag{43}$$

□

Teorema 1.20. *El conmutador es un subgrupo y es normal.*

Demostración. El conmutador $G' = \{< [a, b] >: a, b \in G\}$ es un subgrupo.

1. Como estamos operando elementos de G con la misma operación, se seguirá conservando la propiedad asociativa.

2. El elemento neutro $[a, e] = e$ pertenece a C:

$$[a, e] = a \cdot e \cdot a^{-1} \cdot e^{-1} = a \cdot e \cdot a^{-1} \cdot e = a \cdot a^{-1} = e \implies e \in C \quad a, b \in G \tag{44}$$

3. Todo elemento $x = [a, b]$ tiene inverso $x^{-1} = [b, a]$

$$\begin{aligned} &\forall x = [a, b] = aba^{-1}b^{-1} \in C \exists x^{-1} = [b, a] = bab^{-1}a^{-1} \in C : x \cdot x^{-1} = \\ &aba^{-1}b^{-1} \cdot bab^{-1}a^{-1} = aba^{-1}ab^{-1}a^{-1} = abb^{-1}a^{-1} = aa^{-1} = e \end{aligned} \tag{45}$$

□

Demostración. El conmutador $C =< [a,b] >$ es un subgrupo normal.

$$\forall h \in G' : aha^{-1} = aha^{-1}h^{-1}h = [a,h] \cdot h \in G' \implies g(G')g = G' \tag{46}$$

□

Teorema 1.21. *El núcleo de un homomorfismo es un subgrupo y es normal.*

Demostración. La operación está contenida en $\mathrm{Ker}f$:

$$\forall a,b \in \mathrm{Ker}f : f(a \cdot b) = f(a) \cdot f(b) = e \cdot e = e \implies a \cdot b \in \mathrm{Ker}f \tag{47}$$

1. El subgrupo del nucleo al mantener la operación, sigue manteniendo también la propiedad asociativa.

2. El neutro pertenece al nucleo:
$$f(e) = e \implies e \in \mathrm{Ker}f \tag{48}$$

3. Si $x \in \mathrm{Ker}f$ entonces su inverso también.
$$\begin{aligned} &x \in \mathrm{Ker}f : f(e) = e \implies f(x \cdot x^{-1}) = e \implies f(x) \cdot f(x^{-1}) = e \implies \\ &e \cdot f(x^{-1}) = e \implies f(x^{-1}) = e \implies x^{-1} \in \mathrm{Ker}f \end{aligned} \tag{49}$$

Por lo tanto, el nucleo es un homomorfismo.
Además, es normal ya si llamamos $H = \mathrm{Ker}f$ que se cumple que $\forall g \in G : gHg^{-1} = H$.

$$f(gHg^{-1}) = f(g) \cdot f(H) \cdot f(g^{-1}) = f(g) \cdot f(g^{-1}) = f(g) \cdot f^{-1}(g) = e \implies gHg^{-1} = H \tag{50}$$

□

Teorema 1.22. *La imagen de un homomorfismo es un subgrupo.*

Demostración. La operación está contenida en $\mathrm{Im}f$:

$$f(a) \cdot f(b) = f(a \cdot b) \in \mathrm{Im}f \tag{51}$$

1. Como se conserva la operación, se sigue conservando la propiedad asociativa.

2. Como $f(e) = e$, el neutro pertenece a $\mathrm{Im}f$.
$$f(e) = e \implies e \in \mathrm{Im}f \tag{52}$$

3. Si $x = f(a) \in \mathrm{Im}f$, entonces $x^{-1} = f(a^{-1})$:
$$x \cdot x^{-1} = f(a) \cdot f(a^{-1}) = f(a \cdot a^{-1}) = f(e) = e \tag{53}$$

□

Teorema 1.23. *La aplicación $G \to G/H : \pi(g) = gH$ es un homomorfismo suprayectivo.*

Demostración. La aplicación $G \to G/H : \pi(g) = gH$ es un homomorfismo:

$$\pi(g_1) \cdot \pi(g_2) = g_1H \cdot g_2H = g_1g_2HH = g_1g_2H = \pi(g_1 \cdot g_2) \tag{54}$$

La aplicación $\pi(g)$ es suprayectiva ya que toda imagen gH tiene al menos g como preimagen. □

Teorema 1.24 (Pimer teorema de isomorfía)**.** *Sea $f : G \to G'$ un homomorfismo. Entonces podemos establecer el isomorfismo $\bar{f} : G/Kerf \to G' \cong Im(f)$*

Demostración. Renombremos $\text{Ker}f = H$. Conocemos el homorfismo cañonico $\pi : G \to G/H$ $\phi(g) = gH$. El inverso será $\pi_{-1}(gH) = g$ tal que $\pi^{-1} : G/H \to G$. Entonces:

$$\pi^{-1}(gH) = g \iff f(\pi^{-1}(gH)) = f(g) \tag{55}$$

Si a $f \circ \pi^{-1} = \bar{f}$, entonces:

$$f(\pi^{-1}(gH)) = f(g) \implies \bar{f}(gH) = f(g) \quad \bar{f} : G/H \to G' \tag{56}$$

Primero demostremos que es un homomorfismo:

$$\bar{f}(aH \cdot bH) = \bar{f}(abHH) = \bar{f}(abH) = f(ab) = f(a) \cdot f(b) \tag{57}$$

Ahora que es un isomorfismo:

- $\bar{f}$ es sobreyectiva ya que para cualquier imagen $f(a)$ existe la preimagen aH.
- $\bar{f}$ es inyectiva:

  Queremos demostrar que $aH \neq bH \implies f(a) \neq f(b)$, podemos demostrar que $\neg\bar{f}(aH) \neq \bar{f}(bH) \implies \neg aH \neq bH$, es decir, que $\bar{f}(aH) = \bar{f}(bH) \implies aH = bH$.

$$\begin{aligned} &\bar{f}(aH) = \bar{f}(bH) \iff f(a) = f(b) \iff f(a) \cdot f(b^{-1}) = f(b) \cdot f(b^{-1}) \iff \\ &f(ab^{-1}) = f(bb^{-1}) = f(e) = e \implies ab^{-1} \in H \implies ab^{-1}H = H \iff \\ &ab^{-1}H \cdot b = H \cdot b \iff ab^{-1}bH = Hb \iff aH = Hb = bH \iff aH = bH \end{aligned} \tag{58}$$

Por lo tanto, hemos encontrado un isomorfismo $\bar{f} : G/\text{Ker}f \to G' \cong \text{Im}f$. □

Teorema 1.25. *Todo cuerpo es dominio de integridad*

$$G \text{ cuerpo} \implies G \text{ D.I.} \tag{59}$$

Demostración. Supongamos que G es un cuerpo pero que no es un dominio de integridad.
Entonces como G no es un dominio de integridad se cumple que:

$$\exists a, b \in G : ab = 0 \quad a, b \neq 0 \tag{60}$$

Como G es un cuerpo todos sus elementos menos el 0 tienen inverso multiplicativo, por lo tanto:

$$ab \cdot b^{-1}a^{-1} = 1 \implies 0 \cdot (ab)^{-1} = 1 \tag{61}$$

Pero el inverso aditivo no puede tener inverso multiplicativo ya que G es un cuerpo. Contradicción. □

Teorema 1.26. *Un ideal I que posee al neutro multiplicativo coincide con el anillo que lo contiene.*

$$1 \in I \subseteq R \implies I = R \tag{62}$$

Demostración. Como $1 \in I$ entonces, por definición:

$$\forall x \in R : 1 \cdot x \in I \implies \forall x \in R : x \in I \implies I = R \tag{63}$$

□

Teorema 1.27. *Todos los ideales en $\mathbb{Z}$ son principales.*

Demostración. Si el ideal es el trivial entonces ya es principal.
Como los ideales contienen a los inversos aditivos $-a$ de los elementos $a \neq 0$, hablaremos siempre de números positivos.
Consideremos m como el elemento más pequeño del ideal:
si $m = 1$ el ideal coincide con todo $\mathbb{Z}$ y por lo tanto ya es principal.
En caso contrario $m \neq 1$, si el ideal no fuese principal, entonces el resto de elementos no serían múltiplos de m:

$$i \in I : m \mid i \implies i = mk + r \quad r < m \implies r = i - mk \tag{64}$$

Pero por definición de ideal, como $k \in \mathbb{Z}$, entonces $mk \in I$. Como I es un subgrupo de $\mathbb{Z}$:

$$i - mk \in I \implies r \in I \tag{65}$$

Contradicción. Hemos encontrado un elemento $r \in I$ más pequeño que m cuando hemos dicho que m era el más pequeño. Por lo tanto, hemos demostrado por reducción al absurdo que todos los ideales en $\mathbb{Z}$ son principales. □

Teorema 1.28. *En un anillo conmutativo A con un ideal I, el anillo cociente A/I es D.I. si y solo si I es un ideal primo.*

Demostración. $\implies$

$$\begin{aligned} &(a+I)(b+I) = ab + I = e + I \implies ab \in I \\ &A/I \text{ D.I} \implies ab \in I \implies (a+I)(b+I) = ab + I = I \implies \\ &a + I = I \text{ o } b + I = I \implies a \in I \text{ o } b \in I \end{aligned} \tag{66}$$

$\impliedby$

$$\begin{aligned} &I \text{ primo} : ab \in I \implies a \in I \text{ o } b \in I \iff a \notin I \text{ y } b \notin I \implies ab \notin I \implies \\ &\forall (a+I) \neq I, (b+I) \neq I : ab + I = (a+I)(b+I) \neq I \implies A/I \text{ D.I.} \end{aligned} \tag{67}$$

□

Teorema 1.29. *En un anillo conmutativo unitario R; el ideal M es maximal si y sólo si el anillo cociente R/M es un cuerpo.*

Demostración. $\implies$
Consideremos el elemento $a + M \in R/M$. Si $a \in M$ entonces $a + M = M$, por lo que no puede tener inverso multiplicativo ya que $(a+M)(b+M) = M(b+M) = Mb + M = M + M = M$
Si $a \notin M$ entonces podemos construir el ideal $I = \{ra + m : r \in R,\ m \in M\}$.
Primero demostraremos que es subanillo viendo que está correctamente definido:

$$\begin{aligned} &(ra+m) + (r'a+m') = (r+r')a + (m+m') = r''a + m'' \\ &(ra+m) \cdot (r'a+m') = rr'a^2 + rm'a + r'ma + mm' = (rr'a + rm' + r'm)a + (mm') = r''a + m'' \end{aligned} \tag{68}$$

Ahora veremos que I es un ideal ya que como M lo es, entocnes $r'm = m'$:

$$(ra+m) \cdot r' = (rr')a + r'm = r''a + m' \tag{69}$$

$M \subseteq I$, pero M maximal, entonces $I = R$.
Como R es unitario, entonces $1 \in R \iff 1 \in I$, por lo que:

$$\exists r \in R,\ m \in M : ra + m = 1 \tag{70}$$

Entonces podemos sustituir:

$$1 + M = ra + m + M = (a+M)(r+M) \implies (a+M)^{-1} = (r+M) \tag{71}$$

Por lo tanto, R/M es un cuerpo.
$\impliedby$
Tenemos a M ideal, supongamos por reducción al absurdo que existe $M \subseteq I$ (M no maximal).

Consideremos $a+M \in R/M$ con $a \in I,\ a \notin M$. Como R/M es un cuerpo, entonces tendrá inverso (ya que no se trata del neutro M):

$$(a+M)(b+M) = 1+M \iff ab+M = 1+M \iff ab = 1 \implies 1 \in I \tag{72}$$

Como $1 \in I$, entonces por el teorema 1.26 sabemos que $I = R$. Por lo tanto, M es maximal. □

Colorario 1.30. *En un anillo conmutativo unitario. Todos los ideales maximales son primos.*

Demostración. Sea R un anillo conmutativo unitario. Primero, por el teorema 1.29 sabemos que si M es maximal entonces R/M es un cuerpo (ya que R es conmutativo y unitario). Por el teorema 1.25 sabemos que todo cuerpo es dominio de integridad, por lo que si R/M es maximal, entonces será cuerpo y además será D.I. Utilizando el teorema 1.28 sabemos que si R/M es maximal y por tanto cuerpo y D.I., entonces necesariamente es primo (ya que R es conmutativo).

$$\begin{aligned} &M \text{ maximal} \iff R/M \text{ cuerpo} \implies R/M \text{ D.I.} \iff M \text{ primo} \\ &M \text{ maximal} \implies M \text{ primo} \end{aligned} \tag{73}$$

□

Teorema 1.31. *La imagen de un homomorfismo es un subanillo e ideal si el homomorfismo es suprayectivo. El núcleo de un homomorfismo es siempre ideal.*

Demostración. □

Teorema 1.32. *Los polinomios irreducibles en reales tienen grado uno o dos.*

Demostración. Por el teorema fundamental del álgebra sabemos que un polinomio tiene n raíces en los complejos. Además, las raíces complejas vienen en pares de conjugados.
Los polinomios de grado 1 son siempre irreducibles en los reales.
Un polinomio de grado 2 puede o tener 2 raíces reales (reducible) o dos complejas (irreducible en los reales).
Para el resto de grados siempre va a tener o 1 raíz real o 4 o más raíces complejas las cuales como mínimo formarán 2 polinomios reales (una factorización que hará al polinomio reducible). □

Teorema 1.33 (Criterio de reducibilidad de Eisenstein)**.**

Demostración. □

Teorema 1.34 (Kronecker)**.** *Cualquier polinomio tiene raíz en algún cuerpo.*

Demostración. Sea $P(x)$ un polinomio irreducible con coeficientes en un cuerpo C, consideremos el cuerpo cociente $C_{P(x)} = C[x]/ < P(x) >$.
Por el teorema 1.35, el ideal $< P(x) >$ es principal ya que todos los ideales en un anilo de polinomios con coeficientes en un cuerpo son principales.
Además $< P(x) >$ es D.I. ya que no existen dos polinomios $A(x)B(x)$ que multiplicados den cero. Por lo tanto, al ser $D.I.P.$, el ideal $< P(x) >$ es además maximal, y por lo tanto, por el teorema 1.29, sabemos que $C[x]/ < P(x) >$ es un cuerpo.
Si ahora consideramos la extensión de este cuerpo $C_{P(x)}[x]$, entonces $x+ < P(x) >$ siempre será raíz de $P(x)$:

$$\begin{aligned} &P(x+ < P(x) >) = a_0 + a_1(x+ < P(x) >) + a_2(x+ < P(x) >)^2 + \ldots + a_n(x+ < P(x) >)^n = \\ &a_0 + a_1(x+ < P(x) >) + a_2(x^2+ < P(x) >) + \ldots + a_n(x^n+ < P(x) >) = \\ &a_0 + a_1x + a_2x^2 + \ldots + a_nx^n+ < P(x) >= P(x)+ < P(x) >= 0+ < P(x) > \end{aligned} \tag{74}$$

□

Teorema 1.35. *Todos los ideales en un anillo de polinomios con coeficientes en un cuerpo son principales.*

Demostración. Consideremos en un anillo con coeficientes en un cuerpo $C[x]$ el ideal $I \subset C[x]$ y su polinomio de menor grado $P(x) \in I$. Supongamos por reducción al absurdo que el ideal I no es principal, es decir que existe un polinomio $E(x)$ de mayor grado que no sea múltiplo de $P(x)$, entonces:

$$E(x) = P(x)Q(x) + R(x) \tag{75}$$

Pero $R(x)$ tiene menor grado que $P(x)$, contradicción.
Esto solo ocurre en cuerpos ya que en no cuerpos $C[x, 2]$ sería ideal, pero no sería principal. □

2. Contraejemplos

Contraejemplo 2.1. *Todos los ideales en $\mathbb{Z}[x]$ son principales.*

Demostración. $\mathbb{Z}[x,2]$ (polinomios con termino independiente par) es un ideal ya que si se multiplica con cualquier otro $P(x) \in \mathbb{Z}[x]$ o el termino independiente es cero o es par (ya que par por impar es par). Pero no es principal ya que tanto 2 como x tendrían que ser generados por un mismo $P(x)$:

$$\begin{cases} 2 = P(x)Q_1(x) \\ x = P(x)Q_2(x) \end{cases} \tag{76}$$

□

Contraejemplo 2.2. *La imagen y el núcleo de un homomorfismo de anillos son ideales.*

Demostración. Es cierto que el núcleo es siempre un ideal, pero la imagen solo si se trata de un homomorfismo suprayectivo. Si consideramos por ejemplo el homomorfismo $f : \mathbb{R} \to M_2(\mathbb{R})$ tal que:

$$f(x) = \begin{pmatrix} x & 0 \\ 0 & 0 \end{pmatrix} \tag{77}$$

Entonces $\mathrm{Im}f$ ya no es un ideal ya que la multiplicación de un elemento de $M_2(\mathbb{R})$ con la imágen se puede salir de $\mathrm{Im}f$:

$$\begin{pmatrix} x & 0 \\ 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} x & x \\ 0 & 0 \end{pmatrix} \notin \mathrm{Im}f \tag{78}$$

□

Contraejemplo 2.3. *Un homomorfismo de anillos siempre pasa el elemento neutro multiplicativo del anillo.*

Demostración. Consideremos el homomorfismo $f : \mathbb{R} \to M_2(\mathbb{R})$:

$$f(x) = \begin{pmatrix} x & 0 \\ 0 & 0 \end{pmatrix} \tag{79}$$

El inverso multiplicativo del espacio de salida $1 \in \mathbb{R}$ pasa al $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \neq \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ □

Contraejemplo 2.4. *Un polinomio de grado n no puede tener más de n raíces.*

Demostración. En el anillo $\mathbb{Z}_6$ el polinomio $P(x) = (x-2)(x-3)$ tiene más de 2 raíces:

$$\begin{aligned} P(0) &= (0-2)(0-3) = (-2)(-3) = 6 \equiv 0 \mod 6 \\ P(2) &= (2-2)(2-3) = 0 \cdot (-3) = 0 \\ P(3) &= (3-2)(3-3) = 1 \cdot 0 = 0 \\ P(5) &= (5-2)(5-3) = 3 \cdot 2 = 6 \equiv 0 \mod 6 \end{aligned} \tag{80}$$

□

Contraejemplo 2.5. $\mathbb{Q}[\sqrt{2}]$ *es isomorfo a* $\mathbb{Q}[\sqrt{5}]$

Demostración. Como estamos diciendo que es isomorfo, el neutro multiplicativo se tiene que conservar:

$$f(1) = 1 \implies f(a) = a \tag{81}$$

Entonces, necesariamente $f(\sqrt{2}) = a\sqrt{5}$.

$$2 = f(2) = f(\sqrt{2}\sqrt{2}) = f(\sqrt{2})f(\sqrt{2}) = (a\sqrt{5})^2 = 5a^2 \implies a^2 = \frac{2}{5} \tag{82}$$

Pero, $a^2 \neq \frac{2}{5}$ (misma demostración que $\sqrt{2}$ irracional). □

Contraejemplo 2.6. *Si un anillo es un dominio de integridad, el anillo cociente por un ideal también es un D.I.*

Demostración. Consideremos $\mathbb{Z}/6\mathbb{Z}$. $\mathbb{Z}$ es un D.I. pero el anillo cociente no:

$$(2+6\mathbb{Z})(3+6\mathbb{Z}) = 6+6\mathbb{Z} = 0+6\mathbb{Z} \tag{83}$$

□

Contraejemplo 2.7. *Todos los subanillos de anillos conmutativos son ideales.*

Demostración. Consideremos el subanillo $A = \{(n,n) : n \in \mathbb{Z}\}$ el cual es subanillo de un anillo conmutativo $A \subset \mathbb{Z} \times \mathbb{Z}$. Este subanillo no es un ideal:

$$(n,n)\cdot(1,0) = (n,0) \notin A \tag{84}$$

□

Contraejemplo 2.8. *El neutro multiplicativo del subanillo coincide con la del anillo principal.*

Demostración. $\{0,2,4\} \subset \mathbb{Z}_6$ tiene como neutro multiplicativo al 4:

$$\begin{aligned} &0\cdot 4 = 0 \\ &2\cdot 4 = 8 \equiv 2 \mod 4 \\ &4\cdot 4 = 16 \equiv 4 \mod 4 \end{aligned} \tag{85}$$

Pero en $\mathbb{Z}_6$ el neutro multiplicativo es el 1. □

Contraejemplo 2.9. $\mathbb{Z}[\sqrt{-7}]$ *es D.F.U.*

Demostración. El elemento 8 tiene dos factorizaciones:

$$\begin{aligned} &8 = 2\cdot 2\cdot 2 \\ &8 = (1+\sqrt{-7})(1-\sqrt{-7}) \end{aligned} \tag{86}$$

Por lo tanto, hemos encontrado un elemento que no tiene una descomposición única. □

Contraejemplo 2.10. *Cualquier dominio de factorización es dominio de factorización única.*

Demostración. El anillo $\mathbb{Z}[\sqrt{-7}]$ es dominio de factorización ya que los coeficientes de los elementos $a+b\sqrt{-7}$ pueden ser descompuestos en primos.
Sin embargo, no es dominio de factorización única ya que el elemento 8 tiene más de una factorización:

$$\begin{aligned} &8 = 2\cdot 2\cdot 2 \\ &8 = (1+\sqrt{-7})(1-\sqrt{-7}) \end{aligned} \tag{87}$$

□