Universidad Nacional Autónoma de México
Facultad de Ciencias

MATEMÁTICAS

Algebra Moderna II

1ra lista de ejercicios

Por: Lorenzo Antonio Alvarado Cabrera

---

1. ANILLOS

Problema 1.1. –

Sean X un conjunto y $\mathcal{P}(X)$ el conjunto potencia de X. Demuestra que $(\mathcal{P}(X), +, \cdot)$ es un anillo conmutativo, donde

$$A + B = A \triangle B = (A \setminus B) \cup (B \setminus A) = (A \cup B) \setminus (A \cap B).$$

Y

$$A \cdot B = A \cap B.$$

Más aún, demuestra que si $X \neq \varnothing$ entonces este es, además, un anillo unitario.

Demostración: Veamos el caso en que $X = \varnothing$.

⊙ Si $X = \varnothing$ entonces tendremos que $\wp(X) = \{\varnothing\} \neq \varnothing$, con lo que efectivamente es un anillo conmutativo pues por una parte es el anillo trivial y:

$$\varnothing \cdot \varnothing = \varnothing = \varnothing \cdot \varnothing$$

$\therefore$ la operación $\cdot$ es conmutativa.

⊙ Si $X \neq \varnothing$ entonces veamos que tendremos un anillo conmutativo con uno. Sean $A, B, C \in \wp(X)$, entonces:

$(\wp(X), +)$:

- La operación $+$ es cerrada, pues las operaciones conjuntistas lo son:

$$A + B = (A \setminus B) \cup (B \setminus A) = (A \cap B^c) \cup (B \cap A^c) \in \wp(X)$$

- La operación $+$ es asociativa, sean $A, B, C \in \wp(X)$ entonces

$$\begin{aligned}(A+B)+C &= [(A\cap B^c)\cup(B\cap A^c)]+C\\ &= ([(A\cap B^c)\cup(B\cap A^c)]\cap C^c)\cup(C\cap[(A\cap B^c)\cup(B\cap A^c)]^c)\\ &= ((A\cap B^c\cap C^c)\cup(B\cap A^c\cap C^c))\cup(C\cap[(A^c\cup B)\cap(B^c\cup A)])\\ &= (A\cap B^c\cap C^c)\cup(B\cap A^c\cap C^c)\cup(C\cap(A^c\cup B)\cap(B^c\cup A))\\ &= (A\cap B^c\cap C^c)\cup(B\cap A^c\cap C^c)\cup(([C\cap A^c]\cup[C\cap B])\cap(B^c\cup A))\\ &= (A\cap B^c\cap C^c)\cup(B\cap A^c\cap C^c)\cup(C\cap A^c\cap B^c)\cup(C\cap B\cap A)\end{aligned}$$

Por otro lado

$$\begin{aligned}A+(B+C) &= A+[(B\cap C^c)\cup(C\cap B^c)]\\ &= (A\cap[(B\cap C^c)\cup(C\cap B^c)]^c)\cup([(B\cap C^c)\cup(C\cap B^c)]\cap A^c)\\ &= (A\cap[(B^c\cup C)\cap(C^c\cup B)])\cup((B\cap C^c\cap A^c)\cup(C\cap B^c\cap A^c))\\ &= (A\cap(B^c\cup C)\cap(C^c\cup B))\cup(B\cap C^c\cap A^c)\cup(C\cap B^c\cap A^c)\\ &= (([A\cap B^c]\cup[A\cap C])\cap(C^c\cup B))\cup(B\cap C^c\cap A^c)\cup(C\cap B^c\cap A^c)\\ &= (A\cap B^c\cap C^c)\cup(A\cap C\cap B)\cup(B\cap C^c\cap A^c)\cup(C\cap B^c\cap A^c)\end{aligned}$$

$\Rightarrow\ (A+B)+C = A+(B+C)$.

• La operación $+$ es conmutativa

$$A+B=(A\setminus B)\cup(B\setminus A)=(B\setminus A)\cup(A\setminus B)=B+A$$

• Existe neutro aditivo, siendo $\varnothing$

$$A+\varnothing=(A\setminus\varnothing)\cup(\varnothing\setminus A)=(A)\cup(\varnothing)=A=\varnothing\cup A=(\varnothing\setminus A)\cup(A\setminus\varnothing)=\varnothing+A$$

• Existen inversos aditivos, dado $A\in\wp(X)$ el inverso es él mismo

$$A+A=(A\setminus A)\cup(A\setminus A)=(\varnothing)\cup(\varnothing)=\varnothing$$

$\therefore\ (\wp(X),+)$ es un grupo abeliano.

$(\wp(X),\cdot):$

• La operación $\cdot$ es cerrada, pues si $A,B\in\wp(X)\ \Rightarrow\ A,B\subseteq X$ y entonces

$$\Rightarrow\ A\cdot B=A\cap B\subseteq A\subseteq X\ \Rightarrow\ A\cdot B\in\wp(X)$$

• La operación $\cdot$ es asociativa se da pues la intersección es asociativa

$$(A\cdot B)\cdot C = (A\cap B)\cap C = A\cap(B\cap C) = A\cdot(B\cdot C)$$

• La operación $\cdot$ es conmutativa pues

$$A\cdot B = A\cap B = B\cap A = B\cdot A$$

• Existe neutro para $\cdot$, siendo X (pues $X\neq\varnothing$).

$$A\cdot X = A\cap X = A = X\cap A = X\cdot A$$

* Finalmente se cumple la distribución, pues

$$\begin{aligned}
A\cdot B + A\cdot C = A\cap B + A\cap C &= [(A\cap B)\cap(A\cap C)^c]\cup[(A\cap C)\cap(A\cap B)^c]\\
&= [(A\cap B)\cap(A^c\cup C^c)]\cup[(A\cap C)\cap(A^c\cup B^c)]\\
&= [(A\cap B\cap A^c)\cup(A\cap B\cap C^c)]\cup[(A\cap C\cap A^c)\cup(A\cap C\cap B^c)]\\
&= [(B\cap\varnothing)\cup(A\cap B\cap C^c)]\cup[(C\cap\varnothing)\cup(A\cap C\cap B^c)] = [A\cap B\cap C^c]\cup[A\cap C\cap B^c]\\
&= [A\cap B\cap C^c]\cup[A\cap C\cap B^c] = A\cap([B\cap C^c]\cup[C\cap B^c])\\
&= A\cdot([B\setminus C]\cup[C\setminus B]) = A\cdot(B+C)
\end{aligned}$$

$\therefore$ $(\wp(X),+,\cdot)$ es anillo conmutativo con 1.

■

Problema 1.2. –

Sean $X\neq\emptyset$, $(R,+,\cdot)$ un anillo y

$$R^X = \{f : X \longrightarrow R \mid f \text{ es función}\}.$$

Demuestra que $(R^X,+,\cdot)$ es un anillo, donde para todo $x\in X$, $(f+_{R^X} g)(x) = f(x)+g(x)$ y y $(f\cdot_{R^X} g)(x) = f(x)\cdot g(x)$.
Más aún, si $(R,+,\cdot)$ es un anillo conmutativo entonces $(R^X,+_{R^X},\cdot_{R^X})$ es un anillo conmutativo.
Si $(R,+,\cdot)$ es un anillo unitario, entonces $(R^X,+_{R^X},\cdot_{R^X})$ es un anillo unitario y el uno es la función $1_{R^X} : X\to R$, definida por: para $x\in X$, $1_{R^X}(x) = 1_R$.

Demostración:

1) Veamos que $(R^X,+,\cdot)$ es un anillo.

$(R^X,+)$:

• La operación $+$ es cerrada, pues dadas $f,g\in R^X$ y $x\in X$

$$(f +_{R^X} g)(x) = f(x) + g(x)$$

y entonces $(f+g): X \to R \ \therefore \ f+g \in R^X$.

• La operación + es asociativa, sean $f, g, h \in R^X$ y $x \in X$, entonces

$$\begin{aligned}([f +_{R^X} g] +_{R^X} h)(x) &= [f +_{R^X} g](x) + h(x) = f(x) + g(x) + h(x) \overset{\alpha}{=} f(x) + [g +_{R^X} h](x) \\ &= (f +_{R^X} [g +_{R^X} h])(x)\end{aligned}$$

$\Rightarrow \ (f +_{R^X} g) +_{R^X} h = f +_{R^X} (g +_{R^X} h)$.

• La operación + es conmutativa, sean $f, g \in R^X$ y $x \in X$, se tiene que

$$(f +_{R^X} g)(x) = f(x) + g(x) \overset{\alpha}{=} g(x) + f(x) = (g +_{R^X} f)(x)$$

• Existe neutro aditivo, siendo $\overline{0} : X \to R$ dada por $\overline{0}(x) = 0_R$

$$(f +_{R^X} \overline{0})(x) = f(x) + \overline{0}(x) \overset{\alpha}{=} f(x) = \overline{0}(x) + f(x) = (\overline{0} +_{R^X} f)(x)$$

• Existen inversos aditivos, dada $f \in R^X$ el inverso es la función $\tilde{f} : X \to R$ dada por $\tilde{f}(x) = -f(x) \ \ \forall x \in R$, pues

$$(f +_{R^X} \tilde{f})(x) = f(x) + (-f(x)) \overset{\alpha}{=} 0_R = \overline{0}(x)$$

$\therefore \ (R^X, +)$ es un grupo abeliano.

$(R^X, \cdot)$:

• La operación $\cdot$ es cerrada, pues si $f, g \in R^X$ y $x \in X$, entonces

$$(f \cdot_{R^X} g)(x) = f(x)g(x)$$

y entonces $(f \cdot g): X \to R \ \therefore \ f \cdot g \in R^X$.

• La operación $\cdot$ es asociativa, sean $f, g, h \in R^X$ y $x \in X$

$$([f\cdot_{R^X} g]\cdot_{R^X} h)(x)=[f\cdot_{R^X} g](x)h(x)=f(x)g(x)h(x)\overset{\alpha}{=}f(x)[g\cdot_{R^X} h](x)=(h\cdot_{R^X}[f\cdot_{R^X} g])(x)$$

∗ Finalmente se cumple la distribución, pues dados $f,g,h\in R^X$ y $x\in X$

$$\begin{aligned}(f\cdot_{R^X}[g+_{R^X} h])(x)&=f(x)[g+_{R^X} h](x)=f(x)[g(x)+h(x)]\overset{\alpha}{=}f(x)g(x)+f(x)h(x)\\&=(f\cdot_{R^X} g)(x)+(f\cdot_{R^X} h)(x)=[(f\cdot_{R^X} g)+_{R^X}(f\cdot_{R^X} h)](x)\end{aligned}$$

$\therefore$ $(R^X,+,\cdot)$ es un anillo.

$\blacksquare$

2) Supongamos que $(R,+,\cdot)$ es un anillo conmutativo.

Por lo anterior sabemos que $(R^X,+,\cdot)$ es un anillo, veamos que se cumplirá la conmutatividad.

En efecto, sean $f,g\in R^X$ y $x\in X$, entonces

$$(f\cdot_{R^X} g)(x)=f(x)g(x)\underset{R\text{ conmuta}}{=}g(x)f(x)=(g\cdot_{R^X} f)(x)$$

$\therefore$ si $(R,+,\cdot)$ es un anillo conmutativo entonces $(R^X,+,\cdot)$ es anillo conmutativo.

$\blacksquare$

3) Supongamos que $(R,+,\cdot)$ es un anillo unitario.

Por lo anterior sabemos que $(R^X,+,\cdot)$ es un anillo, veamos que la función $1_{R^X}\in R^X$ dada por $1_{R^X}(x)=1_R\ \ \forall x\in X$ es el elemento identidad para $\cdot_{R^X}$ (dicha función está bien definida pues R es anillo unitario y existe 1_R).

En efecto, sea $f\in R^X$ y $x\in X$, entonces

$$\begin{aligned}(f\cdot_{R^X} 1_{R^X})(x)&=f(x)1_{R^X}(x)=f(x)1_R\underset{\text{identidad}}{=}f(x)\\(1_{R^X}\cdot_{R^X} f)(x)&=1_{R^X}(x)f(x)=1_R f(x)\underset{\text{identidad}}{=}f(x)\end{aligned}$$

$\therefore$ si $(R,+,\cdot)$ es un anillo unitario entonces $(R^X,+,\cdot)$ es anillo unitario.

$\blacksquare$

[α] Estas igualdades son debidas a las propiedades del anillo R, asociatividad, conmutatividad y distributividad.

Problema 1.3. –

Sea $(R,+,\cdot)$ un anillo distinto del anillo trivial. Considera

$$R^n = \{(r_1, r_2, \ldots, r_n) : r_1, r_2, \ldots, r_n \in R\}$$

y definamos en el conjunto R^n las operaciones de adición y multiplicación dadas por:

$$(r_1, r_2, \ldots, r_n) +_{R^n} (s_1, s_2, \ldots, s_n) = (r_1 + s_1, r_2 + s_2, \ldots, r_n + s_n)$$

y

$$(r_1, r_2, \ldots, r_n) \cdot_{R^n} (s_1, s_2, \ldots, s_n) = (r_1 \cdot s_1, r_2 \cdot s_2, \ldots, r_n \cdot s_n).$$

a) Demuestra que el sistema $(R^n, +_{R^n}, \cdot_{R^n})$ es un anillo.

b) Demuestra que si R es un anillo con uno, entonces R^n es un anillo con uno.

c) Demuestra que si R es un anillo conmutativo, entonces R^n es un anillo conmutativo.

d) Considera el conjunto $R_1 = \{(0, r_2, \ldots, r_n) : r_2, \ldots, r_n \in R\}$. Demuestra que el sistema $(R_1, +_{R^n}, \cdot_{R^n})$ es un subanillo de R^n.

e) Verifica que si R es un anillo con uno, entonces R_1 es un anillo con uno. ¿Son ambos unos iguales? ¿Qué podemos decir sobre el uno del subanillo?

Demostración:

a) Veamos que $(R^n, +_{R^n}, \cdot_{R^n})$ es un anillo.

$(R^n, +_{R^n})$:

• La operación $+_{R^n}$ es cerrada, pues dados $r, s \in R^n$

$$r +_{R^n} s = (r_1 + s_1, \ldots, r_n + s_n) \in R^n$$

• La operación $+_{R^n}$ es asociativa, sean $r, s, q \in R^n$, entonces

$$(r +_{R^n} s) +_{R^n} q = (r_1 + s_1, \ldots, r_n + s_n) +_{R^n} q = ((r_1 + s_1) + q_1, \ldots, (r_n + s_n) + q_n)$$
$$\overset{\alpha}{=} (r_1 + (s_1 + q_1), \ldots, r_n + (s_n + q_n)) = r +_{R^n} (s_1 + q_1, \ldots, s_n + q_n) = r +_{R^n} (s +_{R^n} q)$$

$\Rightarrow (r +_{R^n} s) +_{R^n} q = r + ({}_{R^n} s +_{R^n} q)$.

• La operación $+_{R^n}$ es conmutativa, sean $r, s \in R^n$, se tiene que

$$r +_{R^n} s = (r_1 + s_1, \ldots, r_n + s_n) \overset{\alpha}{=} (s_1 + r_1, \ldots, s_n + r_n) = s +_{R^n} r$$

• Existe neutro aditivo, siendo $0_{R^n} := (0_R, \ldots, 0_R)$:

$$r +_{R^n} 0_{R^n} = (r_1 + 0_R, \ldots, r_n + 0_R) =^{\alpha} (r_1, \ldots, r_n) = r$$

• Existen inversos aditivos, dado $r \in R^n$ el inverso será $-r := (-r_1, \ldots, -r_n)$, pues

$$r +_{R^n} (-r) = (r_1 + (-r_1), \ldots, r_n + (-r_n)) =^{\alpha} (0_R, \cdots, 0_R) = 0_{R^n}$$

$\therefore$ $(R^n, +_{R^n})$ es un grupo abeliano.

$(R^n, \cdot_{R^n})$:

• La operación $\cdot$ es cerrada, pues si $r, s \in R^n$, entonces

$$r \cdot_{R^n} s = (r_1 \cdot s_1, \ldots, r_n \cdot s_n) \in R^n$$

• La operación $\cdot$ es asociativa, sean $r, s, q \in R^n$, entonces

$$\begin{aligned} r \cdot_{R^n} (s \cdot_{R^n} q) &= r \cdot_{R^n} (s_1 \cdot q_1, \ldots, s_n \cdot q_n) = (r_1 \cdot (s_1 \cdot q_1), \ldots, r_n \cdot (s_n \cdot q_n)) \\ &=^{\alpha} ((r_1 \cdot s_1) \cdot q_1), \ldots, (r_n \cdot s_n) \cdot q_n) = (r_1 \cdot s_1, \ldots, r_n \cdot s_n) \cdot_{R^n} q = (r \cdot_{R^n} s) \cdot_{R^n} q \end{aligned}$$

* Finalmente se cumple la distribución, pues dados $r, s, q \in R^n$

$$\begin{aligned} r \cdot_{R^n} (s +_{R^n} q) &= r \cdot_{R^n} (s_1 + q_1, \ldots, s_n + q_n) = (r_1 \cdot (s_1 + q_1), \ldots, r_n \cdot (s_n + q_n)) \\ &\overset{\alpha}{=} (r_1 s_1 + r_1 q_1, \ldots, r_n s_n + r_n q_n) = (r_1 s_1, \ldots, r_n s_n) +_{R^n} (r_1 q_1, \ldots, r_n q_n) \\ &= (r \cdot_{R^n} s) +_{R^n} (s \cdot_{R^n} q) \end{aligned}$$

$\therefore$ $(R^n, +_{R^n}, \cdot_{R^n})$ es un anillo.

■

b) Supongamos que $(R, +, \cdot)$ es un anillo unitario.

Por lo anterior sabemos que $(R^n, +_{R^n}, \cdot_{R^n})$ es un anillo, veamos que $1_{R^n} := (1_R, \ldots, 1_R)$ es el elemento identidad para $\cdot_{R^n}$ (dicho punto existe pues R es anillo unitario y existe 1_R).

En efecto, sea $r \in R^n$, entonces

$$r \cdot_{R^n} 1_{R^n} = (r_1 \cdot 1_R, \ldots, r_n \cdot 1_R) \underset{\text{identidad}}{=} (r_1, \ldots, r_n) = r$$
$$1_{R^n} \cdot_{R^n} r = (1_R \cdot r_1, \ldots, 1_R \cdot r_n) \underset{\text{identidad}}{=} (r_1, \ldots, r_n) = r$$

α Estas igualdades son debidas a las propiedades del anillo R, asociatividad, conmutatividad y distributividad.

$\therefore$ si $(R,+,\cdot)$ es un anillo unitario entonces $(R^n,+_{R^n},\cdot_{R^n})$ es anillo unitario.

■

c) Supongamos que $(R,+,\cdot)$ es un anillo conmutativo.

Por lo anterior sabemos que $(R^n,+_{R^n},\cdot_{R^n})$ es un anillo, veamos que se cumplirá la conmutatividad. En efecto, sean $r,s\in R^n$, entonces

$$r\cdot_{R^n} s=(r_1\cdot s_1,\ldots,r_n\cdot s_n)\underset{R\text{ conmuta}}{=}(s_1\cdot r_1,\ldots,s_n\cdot r_n)=s\cdot_{R^n} r$$

$\therefore$ si $(R,+,\cdot)$ es un anillo conmutativo entonces $(R^n,+_{R^n},\cdot_{R^n})$ es anillo conmutativo.

■

d) PD $(R_1,+_{R^n},\cdot_{R^n})$ es subanillo de R^n.

- Como $R_1=\{(0,r_2,\ldots,r_n):r_2,\ldots,r_n\in R\}$ entonces $0_{R^n}=(0_R,0_R,\ldots,0_R)\in R_1$ por lo que $R_1\neq\varnothing$.
- Sean $r,s\in R_1$, entonces

$$r-s=r+_{R^n}(-s)\overset{\omega}{=}(0_R+(-0_R),r_2+(-s_2),\ldots,r_2+(-s_2))=(0_R,r_2-s_2,\ldots,r_2-s_2)$$

y como R es anillo se tiene que $r_i-s_i\in R\ \forall 2\leq i\leq n\ \therefore\ r-s\in R_1$.

- Sean $r,s\in R_1$, entonces

$$r\cdot_{R^n} s=(0_{R^n}\cdot 0_{R^n},r_2\cdot s_2,\ldots,r_n\cdot s_n)=(0_{R^n},r_2\cdot s_2,\ldots,r_n\cdot s_n)$$

y como R es anillo se tiene que $r_i\cdot s_i\in R\ \forall 2\leq i\leq n\ \therefore\ r\cdot_{R^n} s\in R_1$.

$\therefore$ $(R_1,+_{R^n},\cdot_{R^n})$ es subanillo de R^n.

■

e) Supongamos que $(R,+,\cdot)$ es un anillo unitario.

Por lo hecho anteriormente sabemos que $(R_1,+_{R^n},\cdot_{R^n})$ será un anillo. Veamos que con esta nueva hipótesis será un subanillo unitario. Para ello demostraremos que $1_{R_1}:=(0,1_{R},\ldots,1_R)$ es el elemento identidad para R_1 (dicho punto existe pues R es anillo unitario y existe 1_R). En efecto, sea $r\in R_1$, entonces

$$r\cdot_{R^n} 1_{R_1}=(0_R\cdot 0_R,r_2\cdot 1_R,\ldots,r_n\cdot 1_R)\underset{\text{identidad}}{=}(0,r_2,\ldots,r_n)=r$$
$$1_{R_1}\cdot_{R^n} r=(0_R\cdot 0_R,1_R\cdot r_2,\ldots,r_n\cdot 1_R)\underset{\text{identidad}}{=}(0,r_2,\ldots,r_n)=r$$

[ω] Esto es por la suma y los inversos aditivos definidos en este anillo.

$\therefore$ si $(R,+,\cdot)$ es un anillo unitario entonces $(R_1,+_{R^n},\cdot_{R^n})$ es anillo unitario.

Sin embargo $1_{R_1} \neq 1_{R^n}$ por lo que $(R_1,+_{R^n},\cdot_{R^n})$ no es subanillo unitario de R^n.

■

Problema 1.4. –

Demuestra que Si R es un anillo, entonces para cualesquiera $a,b,c \in R$, se tiene.

a) $a(b-c) = ab - ac$;

b) $(b-c)a = ba - ca$.

Demostración:

a) En efecto, sean $a,b,c \in R$, entonces

$$a(b-c) \underset{def}{=} a(b+(-c)) \underset{distributividad}{=} ab + a(-c) \underset{clase}{=} ab - ac$$

b) En efecto, sean $a,b,c \in R$, entonces

$$(b-c)a \underset{def}{=} (b+(-c))a \underset{distributividad}{=} ba + (-c)a \underset{clase}{=} ba - ca$$

■

2. SUBANILLOS

Problema 2.1. –

Sean R un anillo unitario y S un subanillo de R tal que $1_R \in S$. Demuestra que si u es invertible en S, entonces u es invertible en R.

Demostración: Como $1_R \in S$ entonces $1_S = 1_R$ pues $\forall s \in S,\ s \cdot 1_R = s = 1_R \cdot s$.

Sea $u \in S$ invertible, entonces existe $v \in S$ tal que $us = su = 1_S$, pero como $S \subseteq R$ entonces para $u \in R$ estamos encontrando $v \in R$ tal que $us = su = 1_S = 1_R$ $\therefore$ s es invertible en R.

■

Problema 2.2. –

Sean R un anillo conmutativo unitario, 1_R el uno de R y S un subanillo de R tal que S tiene un elemento uno con $1_S \neq 1_R$.

a) Demuestra que existe $r \in R$ tal que $r1_S = 0_S$ es un divisor de cero en R;

b) Da un ejemplo de un anillo R y un subanillo S de R tales que $1_S \neq 1_R$.

Demostración:

a) Como R es anillo, se tendrá que $1_R - 1_S \in R$ y entonces

$$(1_R - 1_S)1_S = 1_R 1_S - 1_S 1_S \underset{\text{neutros aditivos}}{=} 1_S - 1_S = 0_S$$

por lo que $1_R - 1_S$ es el elemento buscado.

b) El ejemplo es el problema 1.3.

■

3. CARACTERÍSTICA

Problema 3.1. –

Sea R un anillo, $a, b \in R$ y $n, m \in \mathbb{Z}$. Demuestra los siguientes resultados.

a) $(n+m)a = na + ma$;

b) $(nm)a = n(ma)$;

c) $n(a+b) = na + nb$;

d) $n(ab) = (na)b = a(nb)$;

e) $(na)(mb) = (nm)(ab)$.

Demostración: Sean $a, b \in R$ y $m \in \mathbb{Z}$.

a) Tendremos dos casos:

⊗ Para $n \in \mathbb{N}$

• Si $m \geq 0$. Por inducción sobre n., el enunciado es trivial cuando $n = 0$, para $n = 1$

$$(1+m)a = \underbrace{a + \cdots + a}_{m+1\text{-veces}} = a + ma = 1a + ma$$

por lo que se cumple para él 1, ahora supongamos que el resultado es válido para alguna $k \in \mathbb{N}$, y demostraremos que se cumplirá para $k+1$. En efecto:

$$((k+1)+m)a = (k+(m+1))a \overset{\mu}{=} ka+(m+1)a = ka+(1+m)a = ka+a+ma = (k+1)a+ma$$

donde los últimos pasos se dan por el caso base. Por lo tanto, por inducción matemática queda demostrado.

• Si $m<0$. Se tendrá que $m=-b$ con $b \in \mathbb{N}$. Entonces demostraremos que $(n-b)a = na-ba$ Por inducción sobre $n.$, el enunciado es trivial cuando $n=0$, para $n=1$

$$(1-b)a = -(b-1)a = -(\underbrace{a+\cdots+a}_{b-1\text{-veces}}) = -(\underbrace{a+\cdots+a+a}_{b\text{-veces}}-a) = -(ba-a) = a-ba$$

por lo que se cumple para él 1, ahora supongamos que el resultado es válido para alguna $k \in \mathbb{N}$, y demostraremos que se cumplirá para $k+1$. En efecto:

$$\begin{aligned}((k+1)-b)a = (k+(-b+1))a = (k-(b-1))a \overset{\mu}{=} ka-(b-1)a = ka-(ba-a)\\ = ka-ba+a = (k+1)a-ba\end{aligned}$$

donde los últimos pasos se dan por el caso base y por subcaso anterior. Por lo tanto, por inducción matemática queda demostrado.

⊗ Para $n<0$

• Si $m \geq 0$. Se tendrá que $n=-b$ y entonces por lo demostrado

$$(n+m)a = (-b+m)a = (m-b)a = ma-ba = -ba+ma$$

• Si $m<0$. Se tendrá que $n=-b$ y $m=-c$ entonces por lo demostrado

$$(n+m)a = (-b-c)a = -(b+c)a = -(ba+ca) = -ba-ca$$

con esto queda demostrado que $\forall n,m \in \mathbb{Z}$ $(n+m)a = na+ma$.

■

$b)$ Tendremos dos casos:

⊗ Para $n \in \mathbb{N}$

• Si $m \geq 0$. Usando el resultado del inciso $a)$ tendremos

$$(nm)a = (\underbrace{m+\cdots+m}_{n-\text{veces}})a = (m+[\underbrace{m+\cdots+m}_{n-1-\text{veces}}])a = ma+[\underbrace{m+\cdots+m}_{n-1-\text{veces}}]a = \cdots = \underbrace{ma+\cdots+ma}_{n-\text{veces}} = n(ma)$$

[μ] Por hipótesis de inducción.

• Si $m < 0$. Se tendrá que $m = -b$ con $b \in \mathbb{N}$. Entonces

$$(n(-b))a = -((nb)a) = -(n(ba)) = n(-(ba)) = n((-b)a) = n(ma)$$

⊗ Para $n < 0$

• Si $m \geq 0$. Se tendrá que $n = -b$ y entonces por lo demostrado

$$(nm)a = ((-b)m)a = -((bm)a)) = -(b(ma)) = (-b)(ma) = n(ma)$$

• Si $m < 0$. Se tendrá que $n = -b$ y $m = -c$ entonces por lo demostrado

$$(nm)a = ((-b)(-c))a = (bc)a = b(ca) = (-b)(-(ca)) = n(ma)$$

con esto queda demostrado que $\forall n, m \in \mathbb{Z}$ $(nm)a = n(ma)$.

■

c) Tendremos dos casos:

⊗ Para $n \in \mathbb{N}$, se tiene que

$$n(a+b) = \underbrace{(a+b)+\cdots+(a+b)}_{n-\text{veces}} = \underbrace{(a+\cdots+a)}_{n-veces} + \underbrace{(b+\cdots+b)}_{n-veces} = na + nb$$

⊗ Para $n < 0$, tenemos que $n = -c$ con $c \in \mathbb{N}$, entonces por el caso anterior

$$n(a+b) = (-c)(a+b) = -(c(a+b)) = -(ca+cb) = -ca - cb = na + nb$$

con esto queda demostrado que $\forall n \in \mathbb{Z}$ $n(a+b) = na + nb$.

■

d) Tendremos dos casos:

⊗ Para $n \in \mathbb{N}$, se tiene que

$$n(ab) = \underbrace{ab+\cdots+ab}_{n-\text{veces}} = (\underbrace{a+\cdots+a}_{n-\text{veces}})b = (na)b$$

y también tendremos que

$$n(ab) = \underbrace{ab+\cdots+ab}_{n-\text{veces}} = a(\underbrace{b+\cdots+b}_{n-\text{veces}}) = a(nb)$$

estos dos se dan por la distributividad.

⊗ Para $n < 0$, tenemos que $n = -c$ con $c \in \mathbb{N}$, entonces por el caso anterior

$$n(ab) = -c(ab) = -[c(ab)] = -[(ca)b] = ((-c)a)b = (na)b$$

e igualmente

$$n(ab) = -c(ab) = -[c(ab)] = -[a(cb)] = (-a)(cb) = a((-c)b) = a(nb)$$

■

e) Usando el inciso anterior tenemos que

$$(na)(mb) \underset{d)}{=} ((na)m)b \underset{b)}{=} ((nm)a)b \underset{d)}{=} (nm)(ab)$$

con esto queda demostrado.

■

Problema 3.2. –

Sea R un anillo unitario y consideremos el conjunto

$$\mathbb{Z}1_R = \{n1_R \,:\, n \in Z\}$$

.

a) Demuestra que $\mathbb{Z}1_R$ es un anillo conmutativo con uno;

b) Demuestra que si $\operatorname{char}(R)$ es positiva, entonces el orden del grupo cíclico $(\mathbb{Z}1_R, +)$ es la característica del anillo R .

c) Demuestra que si $\operatorname{char}(R) = 0$, entonces el orden del grupo cíclico $(\mathbb{Z}1_R, +)$ es infinito.

Demostración:

a) Veamos que $(\mathbb{Z}1_R, +, \cdot)$ es un anillo.

$(\mathbb{Z}1_R, +)$:

• La operación + es cerrada, pues dados $n1_R, m1_R \in \mathbb{Z}1_R$, y por el problema anterior

$$n1_R + m1_R = (n+m)1_R$$

y entonces $n1_R + m1_R \in \mathbb{Z}1_R$.

• La operación + es asociativa, sean $n1_R, m1_R, \tilde{n}1_R \in \mathbb{Z}1_R$, entonces

$$n1_R + (m1_R + \tilde{n}1_R) = n1_R + (m+\tilde{n})1_R = (n + (m+\tilde{n}))1_R$$
$$= ((n+m)+\tilde{n})1_R = (n+m)1_R + \tilde{n}1_R = (n1_R + m1_R) + \tilde{n}1_R$$

• La operación $+$ es conmutativa, sean $n1_R, n1_R \in \mathbb{Z}1_R$, se tiene que

$$n1_R + m1_R = (n+m)1_R = (m+n)1_R = m1_R + n1_R$$

• Existe neutro aditivo, siendo 01_R, pues

$$n1_R + 01_R = (n+0)1_R = n1_R$$

• Existen inversos aditivos, dado $n1_R \in \mathbb{Z}1_R$ el inverso será $(-n)1_R$, en efecto

$$n1_R + (-n)1_R = (n+(-n))1_R = (0)1_R = 01_R$$

$\therefore$ $(\mathbb{Z}1_R, +)$ es un grupo abeliano.

$(\mathbb{Z}1_R, \cdot)$:

• La operación $\cdot$ es cerrada, pues si $n1_R, m1_R \in \mathbb{Z}1_R$, entonces

$$n1_R \cdot m1_R = (nm)1_R$$

y entonces $n1_R \cdot m1_R \in \mathbb{Z}1_R$.

• La operación $\cdot$ es asociativa, sean $n1_R, m1_R, \tilde{n}1_R \in \mathbb{Z}1_R$, entonces

$$n1_R \cdot (m1_R \cdot \tilde{n}1_R) = n1_R \cdot (m\tilde{n})1_R = (nm\tilde{n})1_R = ((nm)\tilde{n})1_R = (nm)1_R \cdot \cdot \tilde{n}1_R = (n1_R \cdot m1_R) \cdot \tilde{n}1_R$$

• La operación $\cdot$ es conmutativa, pues si $n1_R, m1_R \in \mathbb{Z}1_R$, entonces

$$n1_R \cdot m1_R = (mn)1_R = m1_R \cdot n1_R$$

• Existe neutro multiplicativo, siendo 11_R, pues

$$n1_R \cdot 11_R = (n \cdot 1)1_R = n1_R$$

* Finalmente se cumple la distribución, pues dados $n1_R, m1_R, \tilde{n}1_R \in \mathbb{Z}1_R$

$$\begin{aligned} n1_R \cdot (m1_R + \tilde{n}1_R) &= n1_R \cdot (m+\tilde{n})1_R = (n(m+\tilde{n}))1_R = (nm+n\tilde{n})1_R = (mn)1_R + (n\tilde{n})1_R \\ &= n1_R \cdot m1_R + n1_R \cdot \tilde{n}1_R \end{aligned}$$

$\therefore$ $(\mathbb{Z}1_R,+,\cdot)$ es un anillo conmutativo con uno.

■

b) Supongamos que $\text{char}(R)=n>0$, entonces como R es anillo unitario se tiene por el *Teorema 1.3.5* de las notas que n es el menor número positivo tal que $n\cdot 1_R=0_R$. *PD* $\text{ord}(\mathbb{Z}1_R)=n$.

Supongamos que existe $m\in\mathbb{N}^+$, $m<n$ tal que $ord(\mathbb{Z}1_R)=m$, entonces en particular tendremos que

$$m(11_R)=01_R=0_R \;\Rightarrow\; \underbrace{11_R+\cdots+11_R}_{m-\text{veces}}=0_R \;\Rightarrow\; (\underbrace{1+\cdots+1}_{m-\text{veces}})1_R=0_R \;\Rightarrow\; (m1)1_R=0_R$$
$$\Rightarrow\; m1_R=0_R \text{ !!!}$$

pero esto contradice el hecho de que n fuera el menor numero positivo que lo cumpliera $\therefore$ $ord(\mathbb{Z}1_R)=n$ ya que, junto a lo anterior, $n(a1_R)=(na)1_R=1_R1_R=1_R$.

■

c) Supongamos que $\text{char}(R)=0$, entonces como R es anillo unitario se tiene como consecuencia del *Teorema 1.3.5* que no existe $n\in\mathbb{N}^+$ tal que $n\cdot 1_R=0_R$. *PD* $\text{ord}(\mathbb{Z}1_R)=\infty$.

Supongamos que existe $m\in\mathbb{N}^+$ tal que $ord(\mathbb{Z}1_R)=m$, entonces en particular tendremos que

$$m(11_R)=01_R=0_R \;\Rightarrow\; \underbrace{11_R+\cdots+11_R}_{m-\text{veces}}=0_R \;\Rightarrow\; (\underbrace{1+\cdots+1}_{m-\text{veces}})1_R=0_R \;\Rightarrow\; (m1)1_R=0_R$$
$$\Rightarrow\; m1_R=0_R \text{ !!!}$$

pero esto contradice el hecho de que no exista ningún número positivo que lo cumpliera $\therefore$ $ord(\mathbb{Z}1_R)=\infty$.

■

Problema 3.3. –

Denotemos por R al anillo $(\mathbb{Z}_6,+,\cdot)$.

a) Muestra que $\mathbb{Z}1_R=\{n1_R : n\in\mathbb{Z}\}=\mathbb{Z}_6$.

b) Muestra que el subconjunto $\{2n1_R : n\in\mathbb{Z}\}$ de $\mathbb{Z}1_R$ es un subanillo de $\mathbb{Z}1_R$ que no tiene uno.

c) Encuentra otro subanillo de $\mathbb{Z}1_R$.

d) Encuentra $\text{char}(R)$.

e) Encuentra $\text{char}(\mathbb{Z}1_R)$.

Demostración:

a) En efecto, se tiene que $1_R = \overline{1}_6$, entonces

$$\mathbb{Z}1_R = \{n1_R : n \in \mathbb{Z}\} = \{n\overline{1}_6 : n \in \mathbb{Z}\} = \{\overline{n}_6 : n \in \mathbb{Z}\} = \mathbb{Z}_6$$

■

b) Notemos que $\{(2n)1_R; n \in \mathbb{Z}\} = \{2(n1_R); n \in \mathbb{Z}\} = 2(\mathbb{Z}1_R) = 2\mathbb{Z}_6 = \{\overline{2}_6, \overline{4}_6, \overline{6}_6\}$. Donde es claro que será subanillo y además con unas cuentas sencillas podemos ver que no hay elemento uno para la multiplicación.

■

c) Por lo ya visto en clase sabemos que otro subanillo será $3\mathbb{Z}_6$.

■

d) Veamos que $\mathrm{char}(R) = 6$. En efecto, sea $\overline{n}_6 \in \mathbb{Z}_6$ entonces $6\overline{n}_6 = \overline{6n}_6 = \overline{0}_6$ y este es el mínimo, pues los primos relativos con 6 la única manera en que sean congruentes con 6 es que sean multiplicados por 6.

■

d) Con ello y por el problema 3.2 $\mathrm{char}(\mathbb{Z}1_R) = 6$

■

4. MORFISMOS E IDEALES

Problema 4.1. –

Sea $f : R \to R'$ un homomorfismo de anillos. Demuestra lo siguiente: Si R y R' son anillos con 1 y $f(R) = R'$. Demuestra lo siguiente:

i) $f(1) = 1'$;

ii) $f(a^{-1}) = f(a)^{-1}$, para cualquier elemento invertible a de R.

Demostración: Como $f(R) = R'$ tendremos que f es suprayectiva.

i) Como f es morfismo de anillos y R es anillo unitario, entonces por el *Lema 1.4.8* de las notas se da que $f(1) = f(1')$.

■

ii) Sea $a \in R$ un elemento invertible. Veamos que entonces $f(a)$ será invertible en R'.

En efecto se tiene que $f(a) \cdot f(a^{-1}) = f(a \cdot a^{-1}) = f(1) = 1'$ $\therefore$ $f(a)$ es invertible en R' y $f(a)^{-1} = f(a^{-1})$.

■

Problema 4.2. –

Sea $f : R \to R'$ un homomorfismo de anillos. Demuestra lo siguiente:

a) Para cada ideal I' de R', el anillo $f^{-1}(I')$ es un ideal de R;

b) Si $f(R) = R'$ entonces para cada ideal I de R, el anillo $f(I)$ es un ideal de R'.

Demostración:

a) Veamos que $f^{-1}[I']$ es ideal de R. Sean $r, s \in R$ y $a \in f^{-1}[I']$. PD $ras \in f^{-1}[I']$.
En efecto, como I' es ideal de R', $f(a) \in I'$ y $f(r), f(s) \in R'$ entonces $f(r)f(a)f(s) \in I'$ por lo que $f(ras) \in I'$ $\therefore$ $ras \in f^{-1}[I']$.

$\blacksquare$

b) Como $f(R) = R'$ se tendrá que f es suprayectiva. Veamos que $f[I]$ es ideal de R'. Sean $r', s' \in R'$ y $a' \in f[I']$. PD $r'a's' \in f[I]$.
En efecto, como f es suprayectiva, existen $r, s \in R$ tales que $f(r) = r'$, $f(s) = s'$, además existe $a \in I$ tal que $f(a) = a'$, así como I es ideal de R se concluye que $ras \in I$ por lo que $f(ras) \in I'$ $\Rightarrow$ $f(ras) \in f[I]$ $\Rightarrow$ $f(r)f(a)f(s) \in f[I]$ $\Rightarrow$ $r'a's' \in f[I]$.

$\blacksquare$

Problema 4.3. –

Demuestra el siguiente resultado. Sea $f : F \to F'$ un homomorfismo del campo F en el campo F'. Entonces f es el homomorfismo trivial o f es un monomorfismo.

Demostración: Como f es morfismo de campos, tenemos por lo visto en clase que $\ker(f)$ es un ideal de F. Entonces tendremos dos casos, $\ker(f) = \{0_F\}$ con lo que tendríamos un monomorfismo o $\ker(f) \neq \{0_F\}$ y en ese caso tomando $x \in \ker(f)$, como F es campo, existe x^{-1} inverso multiplicativo, y dado que $\ker(f)$ es un ideal, necesariamente $x \cdot x^{-1} \in \ker(f)$ $\Rightarrow$ $1_F \in \ker(f)$, con lo que $\forall y \in F$ $f(y) = f(y \cdot 1_F) = f(y)f(1_F) = f(y)0_{F'} = 0_{F'}$ entonces $\ker(f) = F$, es decir, $f \equiv 0$ (morfismo trivial).

$\blacksquare$

Problema 4.4. –

Demuestra el siguiente resultado: Sea I un ideal del anillo R. Entonces la función $\pi_I : R \to R/I$ dada por $\pi_I(r) = r + I$ es un epimomorfismo de anillos (y si R es un anillo unitario, π es un epimorfismo de anillos unitario). Además $\ker\pi_I = I$.

A este epimorfismo se le conoce como la **proyección canónica**.

Demostración: Veamos que es un morfismo.

- Sean $r, s \in R$ entonces $\pi_I(r+s) = (r+s) + I = (r+I) + (s+I) = \pi_I(r) + \pi_I(s)$.
- Sean $r, s \in R$ entonces $\pi_I(r \cdot s) = (r \cdot s) + I = (r+I) \cdot (s+I) = \pi_I(r) \cdot \pi_I(s)$.

Por lo que efectivamente, es un morfismo de anillos que, además, será suprayectiva pues dado $r+I \in R/I$, se tiene que $\pi_I(r) = r+I$.

Ahora supongamos que R es anillo unitario. Entonces $\pi_I(r)$ será un epimorfismo de anillos unitarios, pues $\pi_I(1_R) = 1_R + I$ que es el uno de R/I.

Finalmente veamos cual es el kernel de este epimorfismo, serán aquellos $r \in R$ tales que $\pi_I(r) = 0_{R/I} = 0_R + I \iff r + I = 0_R + I \iff r - 0_R \in I \iff r \in I$ por lo que $\ker(\pi_I) = I$.

■

Problema 4.5. –

Demuestra el siguiente resultado: Sea $f : R \to R'$ un isomorfismo de anillos. Entonces la función $f^{-1} : R' \to R$ dada por $f^{-1}(r') = r$ (donde $r \in R$ es el único elemento tal que $f(r) = r'$) es un isomorfismo de anillos.

Demostración: En efecto:

- Sean $r', s' \in R'$, como f es isomorfismo existen únicos $r, s \in R$ tales que $f(r) = r'$ y $f(s) = s'$, con lo que $f(r)f(s) = r's' \Rightarrow f(rs) = r's'$ y entonces $f^{-1}(r's') = rs = f^{-1}(r')f^{-1}(s')$.
- Sean $r', s' \in R'$, como f es isomorfismo existen únicos $r, s \in R$ tales que $f(r) = r'$ y $f(s) = s'$, con lo que $f(r) + f(s) = r' + s' \Rightarrow f(r+s) = r' + s'$ y entonces $f^{-1}(r'+s') = r + s = f^{-1}(r') + f^{-1}(s')$.

Con lo anterior f^{-1} es morfismo de anillos, y además como f es biyectiva, entonces f^{-1} también $\therefore$ f^{-1} es isomorfismo de anillos.

■

Problema 4.6. –

Demuestra que el anillo $\mathbb{Z}_n$ de los enteros módulo n tiene exactamente un ideal por cada entero positivo m que divida a n.

Sugerencia: Usa el Teorema de la Correspondencia.

Demostración: Consideremos el anillo de los enteros $(\mathbb{Z}, +, \cdot)$ y sea $I \subseteq \mathbb{Z}$ un ideal.
Por el teorema de la correspondencia sabemos que existe una biyección entre el conjunto de los ideales de $\mathbb{Z}$ que contienen a I y los ideales del conjunto $\mathbb{Z}/I$, por lo tanto, la cantidad de ideales de $\mathbb{Z}/I$ será igual a la cantidad de ideales J de $\mathbb{Z}$ tales que $I \subseteq J$.

Reescribamos este enunciado sabiendo la forma de los ideales en $\mathbb{Z}$. Primeramente, sea J ideal de $\mathbb{Z}$ tal que $I \subseteq J$, como I y J son ideales de $\mathbb{Z}$ existen $n, m \in \mathbb{Z}^+$ tales que $I = n\mathbb{Z}$ y $J = m\mathbb{Z}$, y entonces $n\mathbb{Z} \subseteq m\mathbb{Z} \iff m \mid n$ (por teoría de grupos), con lo que

$$\{J : I \subseteq J,\ J \text{ ideal de } \mathbb{Z}\} = \{m\mathbb{Z} : m \mid n\}$$

entonces la cantidad de ideales de $\mathbb{Z} / n\mathbb{Z}$ será igual a la cantidad de enteros m tales que $m \mid n$, i.e, hay un ideal en $\mathbb{Z} / n\mathbb{Z}$ por cada entero que divida a n, y finalmente como $\mathbb{Z} / n\mathbb{Z} \cong \mathbb{Z}_n$ se tiene lo pedido (ya que entonces existe un isomorfismo entre ambos).

■

Problema 4.7. –

Demuestra el siguiente resultado. Sea $f : R \to R'$ un epimomorfismo de anillos. Si I' es un ideal de R', entonces $R/f^{-1}(I')$ es isomorfo a R'/I'.

Demostración: Sea $g : R' / I' \to R / f^{-1}(I')$ dada por $g(r' + I') = f^{-1}(r') + f^{-1}(I')$. Veamos que dicha función es el isomorfismo buscado.

- Esta bien definida, pues como f es epimorfismo, se tiene que $\forall r' \in R',\ \exists r \in R$ tal que $f(r) = r' \iff f^{-1}(r') = r$ y por el problema 4.2 $f^{-1}(I')$ es un ideal de R.

- Sean $r' + I', s' + I' \in R' / I'$ entonces

$$g((r' + I') + (s' + I')) = g((r' + s') + I') = f^{-1}(r' + s') + f^{-1}(I')$$

y como f es epimorfismo existen $r, s \in R$ tales que $f(r) = r' \wedge f(s) = s'$ por lo que $f(r + s) = f(r) + f(s) = r' + s' \Rightarrow f^{-1}(r' + s') = r + s = f^{-1}(r') + f^{-1}(s')$, así

$$f^{-1}(r' + s') + f^{-1}(I') = [f^{-1}(r') + f^{-1}(s')] + f^{-1}(I')$$
$$= [f^{-1}(r') + f^{-1}(I')] + [f^{-1}(s') + f^{-1}(I')] = g(r' + I') + g(s' + I')$$

- Sean $r' + I', s' + I' \in R' / I'$ entonces

$$g((r' + I') \cdot (s' + I')) = g((r's') + I') = f^{-1}(r's') + f^{-1}(I')$$

y como f es epimorfismo existen $r, s \in R$ tales que $f(r) = r' \wedge f(s) = s'$ por lo que $f(rs) = f(r)f(s) = r's' \Rightarrow f^{-1}(r's') = rs = f^{-1}(r')f^{-1}(s')$, así

$$f^{-1}(r's') + f^{-1}(I') = [f^{-1}(r')f^{-1}(s')] + f^{-1}(I')$$
$$= [f^{-1}(r') + f^{-1}(I')][f^{-1}(s') + f^{-1}(I')] = g(r' + I')g(s' + I')$$

- Es inyectiva. Supongamos que $g(r' + I') = g(s' + I') \iff f^{-1}(r') + f^{-1}(I') = f^{-1}(s') + f^{-1}(I')$

$\Leftrightarrow \quad f^{-1}(r') - f^{-1}(s') \in f^{-1}(I') \quad \Leftrightarrow \quad f^{-1}(r'-s') \in f^{-1}(I') \Leftrightarrow \quad r'-s' \in I' \quad \Leftrightarrow \quad r'+I' = s'+I'$.

• Es suprayectiva. Pues dado $r + f^{-1}(I') \in R / f^{-1}(I)$, existe $f(r) + I' \in R' / I'$ tal que $g(f(r)+I') = f^{-1}(f(r)) + f^{-1}(I') = r + f^{-1}(I')$.

Por todo lo anterior se tiene que g es un isomorfismo $\therefore R / f^{-1}(I) \cong R' / I'$.

■

Problema 4.8. –

Segundo Teorema de isomorfismo.: Si I y J son ideales de un anillo R, entonces $I/(I \cap J)$ es isomorfo a $(I+J)/J$.

Demostración: Primeramente, veamos que todo está bien definido.
En efecto por la proposición 1.4.12 sabemos que I y J son anillos por lo que $I+J$ es anillo (pues como es suma de elementos de cada anillo todas las propiedades se siguen valiendo) y como $J \subseteq J+I,\ I \cap J \subseteq I$ estos serán ideales.

Sea $f : I \to R / J$ dada por $f(i) = i + J$, dicha función es un morfismo con las operaciones canónicas, con ello por el primer teorema de isomorfismo tenemos que $I / \ker(f) \cong \mathrm{Im}(f)$, veamos quienes son explícitamente el kernel y la imagen.

- $\ker(f) = \{i \in I : f(i) = 0\} = \{i \in I : i + J = 0 + J\} = \{i \in I : i \in J\} = I \cap J$
- $\mathrm{Im}(f) = \{f(i) : i \in I\} = \{i + J : i \in I\} = \{i + J + (0 + J) : i \in I\} \underset{j \in J}{=} \{(i + j) + J : i \in I\} = (I + J) / J$

$\therefore$ tenemos que $I / (I \cap J) \cong (I + J) / J$.

■

Problema 4.9. –

Demuestra el siguiente resultado: Sea $f : R \to R'$ un epimorfismo de anillos, y sea I un ideal de R. Si $\ker f \subseteq I$, entonces R/I es isomorfo a $R'/f(I)$.
Este resultado es equivalente al **Tercer Teorema de isomorfismo**.

Demostración: Sea $g : R / I \to R' / f(I)$ dada por $g(r + I) = f(r) + f(I)$. Veamos que dicha función es el isomorfismo buscado.

• Está bien definida, pues como f es epimorfismo, se tiene que $\forall r', s' \in R'$, $\exists r, s \in R$ tal que $f(r) = r'$, $f(s) = s'$ y entonces $\forall a' \in f(I) \quad r'a's' = f(r)f(a)f(s) = f(ras) \in f(I)$, entonces si es ideal.

• Sean $r+I, s+I \in R/I$ entonces

$$g((r+I)+(s+I)) = g((r+s)+I) = f(r+s)+f(I)$$

y como f es epimorfismo

$$f(r+s)+f(I) = [f(r)+f(s)]+f(I) = [f(r)+f(I)]+[f(s)+f(I)] = g(r+I)+g(s+I)$$

• Sean $r+I, s+I \in R/I$ entonces

$$g((r+I)\cdot(s+I)) = g((rs)+I) = f(rs)+f(I)$$

y como f es epimorfismo

$$f(rs)+f(I) = [f(r)f(s)]+f(I) = [f(r)+f(I)][f(s)+f(I)] = g(r+I)g(s+I)$$

• Es inyectiva. Supongamos que $g(r+I) = g(s+I) \iff f(r)+f(I) = f(s)+f(I)$
$\iff f(r)-f(s) \in f(I) \iff f(r-s) \in f(I) \iff r-s \in I \iff r+I = s+I$.

• Es suprayectiva. Pues dado $r'+f(I) \in R/f(I)$, existe $f^{-1}(r)+I \in R/I$ (ya que es suprayectiva) tal que $g(f^{-1}(r')+I) = f(f^{-1}(r'))+f(I) = r+f(I)$.

Por todo lo anterior se tiene que g es un isomorfismo $\therefore R/f(I) \cong R/I$.

■

Problema 4.10. –

Tercer Teorema de Isomorfismo:

Sean I y J ideales de R con $I \subseteq J$. Entonces

a) J/I es ideal de R/I;

b) $(R/I)/(J/I) \simeq R/J$.

c) Verifica que el Tercer Teorema de isomorfismo es válido para anillos con uno.

Demostración:

a) Como $I \subseteq J$ se tiene que I es subgrupo con la suma, pues J lo es, por lo que J/I está bien definido, y con ello $J/I \subseteq R/I$.

Ahora sea $j' \in J/I$ y $r', s' \in R/I$ entonces $a' = j+I$ para alguna $j \in J$ y $r' = r+I$, $s' = s+I$ para algunas $r, s \in R$, entonces

$$r'j's' = (r+I)(j+I)(s+I) = (rj+I)(s+I) = (rjs+I)$$

y dado que J es ideal, se tiene que $rjs \in J$ por lo que $r'j's' \in J/I$ por lo que J/I es ideal de R/I.

■

b) Sea $f : R/I \to R$ dada por $f(r+I) = r$ dicha función es un epimorfismo (siguiendo el mismo procedimiento del problema 4.4) y es tal que

$$\ker(f) = \{r+I \in R/I : f(r+I) = 0\} = \{r+I : r = 0\} = I$$

por lo tanto, tenemos $f : R/I \to R$ epimorfismo, J/I ideal de R/I y $\ker(f) = I \subseteq J/I$ con lo que por el problema 4.9 (el anterior) $(R/I)/(J/I)$ es isomorfo a $R/f(J/I)$, pero notemos que $f(J/I) = \{f(j+I) : j \in J\} = \{j : j \in J\} = J \therefore (R/I)/(J/I) \cong R/J$.

■

c) ¿El procedimiento es análogo?

■

Problema 4.11. –

Demuestra el siguiente resultado (caracterización de un ideal I).

Sea I un subconjunto no vacío de una anillo R. Entonces I es un ideal (bilateral) de R, si y sólo si,

a) $a, b \in I$ implica $a - b \in I$ para todo $a, b \in I$;

b) $r \in R$ y $a \in I$ implica $ra, ar \in I$.

Demostración:

⇒] Supongamos que I es ideal de R, demostraremos *a*) y *b*).

a) Sean $a, b \in I$, y $r, s \in R$ entonces $r(a-b)s = (ra-rb)s = ras - rbs$ y dado que I es ideal, tenemos que $ras, rbs \in I$ y como es subgrupo con la suma, se tiene que $ras - rbs \in I \therefore r(a-b)s \in I \therefore a - b \in I$.

b) Sea da pues I es ideal.

⇐] Supongamos que se cumplen *a*) y *b*), veamos que entonces I es ideal.
Por el inciso *b* como $\forall a, b \in I \;\; a - b \in I$ tendremos que I es subgrupo con la suma. Y por el inciso a tendremos que dados $r, s \in R$ y $a \in I$, $ra \in I \Rightarrow (ra)s = ras \in I$ por lo que efectivamente I será ideal.

■