Chapter 1

Anillos

1. Sean $R_1, \dots, R_n$ anillos. El producto cartesiano
$$S = R_1 \times \cdots \times S_N$$
tiene estructura de anillo con las operaciones evidentes. Además,
$$\overline{R_i} := \{0\} \times \cdots \times R_i \times \cdots \times \{0\} \subseteq S$$
es un subanillo.

   El anillo S es conmutativo si y sólo si para todo $i = 1, \dots, n$, R_i es conmutativo. Si para todo i, R_i tiene identidad, entonces S tiene identidad y ésta es
$$1_S = (1_{R_1}, \dots, 1_{R_n}).$$
Notamos que la identidad de $\overline{R_i}$ es
$$(0, \dots, 0, 1_{R_i}, 0, \dots, 0),$$
y si n es mayor o igual que 2, no coincide con la identidad de S para ningún i. Notamos también que si $i \neq j$, entonces
$$1_{\overline{R_i}} \cdot 1_{\overline{R_j}} = 0,$$
es decir, S tiene divisores de 0. En particular, el producto cartesiano de cuerpos no es cuerpo.

2. Sea R un anillo, y $X \neq \emptyset$ un conjunto. Definimos
$$R^X := \{f : X \longrightarrow R : \ f \text{ aplicación}\}.$$
R^X es un anillo con las operaciones de suma y producto de funciones:
$$(f+g)(x) = f(x) + g(x), \quad (f \cdot g)(x) = f(x) \cdot g(x).$$
Si R tiene identidad, la aplicación $1(x) = 1_R$ es la identidad en R^X. Además, R es conmutativo si y sólo si R^X también lo es.

Si $|X| \geq 2$ y $|R| \geq 2$, R^X tiene divisores de 0: Sea a un elemento no nulo de R y x_1, x_2 dos elementos distintos de X. Entonces las funciones f_a, $\overline{f_a}$ dadas por

$$\begin{aligned} f_a(x_1) &= a, \quad f_a(z) = 0 \text{ si } z \neq x_1, \\ \overline{f_a}(x_2) &= a, \quad \overline{f_a}(z) = 0 \text{ si } z \neq x_2, \end{aligned}$$

son funciones no nulas cuyo producto es la función cero.

Nótese que si $X = \mathbb{N}$, el conjunto R^X es el anillo de sucesiones en R.

3. Sea R un anillo con identidad y sea $(G, \cdot)$ un grupo (¿finito?). Definimos el *anillo de grupo*

$$RG = \left\{ \sum_{g \in G} a_g \cdot g \;\middle|\; a_g \in R,\ g \in G \right\}.$$

con las operaciones de suma y producto dadas por

$$\begin{aligned} &\sum_{g \in G} a_g g + \sum_{g \in G} b_g g = \sum_{g \in G} (a_g + b_g) g, \\ &\left(\sum_{g \in G} a_g g \right) \cdot \left(\sum_{x \in G} b_x x \right) = \sum_{x \in G} \left(\sum_{g \in G} (a_g b_{g^{-1}x}) \right) x. \end{aligned}$$

Vamos a ver por qué se define así el producto. Si trabajamos con elementos de la forma $a \cdot g$ y $b \cdot h$, es natural que el producto se defina como

$$(ag) \cdot (bh) = (ab) \cdot (gh).$$

Generalizando,

$$(ag) \cdot \left(\sum_{x \in G} b_x x \right) = \sum_{x \in G} (ab_x)(gx) = \sum_{z \in G} (ab_{g^{-1}z}) z = \sum_{z \in G} (ab_{g^{-1}x}) x$$

Por último,

$$\left(\sum_{g \in G} a_g g \right) \cdot \left(\sum_{x \in G} b_x x \right) = \sum_{g \in G} \sum_{x \in G} (a_g b_{g^{-1}x}) x = \sum_{x \in G} \left(\sum_{g \in G} (a_g b_{g^{-1}x}) \right) x$$

Nótese que los elementos cero e identidad del anillo son

$$0 = \sum_{g \in G} a_G \cdot g, \quad 1 = 1_R 1_G + \sum_{g \in G - \{1_G\}} 0 \cdot g.$$

y el elemento opuesto de

$$a = \sum_{g \in G} a_g g$$

viene dado por

$$-a = \sum_{g \in G} -a_g g.$$

Si consideramos el elemento

$$a = \sum_{g \in G} g,$$

se tiene que para todo x en G,

$$xa = \sum_{g \in G} xg = \sum_{g \in G} g = a.$$

En particular,

$$a^2 = \left(\sum_{x \in G} x \right) a = \sum_{x \in G} xa = \sum_{x \in G} a = |G|a.$$

Ahora distinguimos casos según la característica de R. Si car$R$ divide a $|G|$, se tiene que $a^2 = 0$, por lo que R tiene divisores de 0. Si car$R \neq 0$ y $|G|$ son coprimos entre sí, entonces por la identidad de Bezout existen enteros m, n tales que $m|G| + n\text{car}G = 1$. Por tanto, si tomamos

$$b := \overbrace{1_S + \cdots + 1_S}^{m \text{ veces}}, \quad c = \overbrace{1_S + \cdots + 1_S}^{n \text{ veces}},$$

se tiene $b|G| = 1 - c\text{car}G = 1$. Así, definido

$$\lambda = b \cdot a,$$

se tiene

$$\lambda^2 = b \cdot a \cdot b \cdot a = b^2 a^2 = b^2 a^2 = b^2(|G|a) = ba = \lambda.$$

Donde hemos usado que b conmuta con a, y realmente con cualquier otro elemento de RG (esto es fácil de comprobar). A los elementos cuyo cuadrado coincide con ellos mismos se los denomina *idempotentes*. Si a estas condiciones le añadimos $G \neq 1$, obtenemos

$$a^2 - a = a(a-1) = 0,$$

siendo tanto a como $a - 1$ elementos no nulos.

Por último, notamos que si $|G| = m$, para cualquier elemento g de G, $g^m = 1$. Por tanto, si $g \neq 1$,

$$(1 - g)(1 + g + \cdots + g^{m-1}) = 1 - g^m = 0,$$

siendo ambos factores distintos de cero. Es otra forma de ver que RG tiene divisores de 0, incluso si car$R = 0$.

4. Sea $(A, +)$ un grupo abeliano y $R = \text{End}(A)$. Entonces R es un anillo con las operacioes

$$(f + g)(x) = f(x) + g(x), \quad (f \cdot g)(x) = f(g(x)).$$

En particular, consideramos $S = R^{\mathbb{N}}$, $T = \text{End}(S)$. Sea $f \in T$ dado por

$$f((a_i)_{i \geq 1}) = (b_j)_{j \geq 1}, \quad b_1 = 0,\ b_{j+1} = a_j, j \geq 2,$$

de modo que f es inyectiva pero no sobreyectiva. Consideramos la función g dada por

$$g((a_i)_{i\geq 1}) = (b_j)_{j\geq 1}, \quad b_j = a_{j+1}, j \geq 1$$

de modo que f es sobreyectiva pero no inyectiva. Entonces

$$g \circ f = id_T, \quad f \circ g \neq id_T$$

Es decir, hay elementos con inversos a izquierda que no son inversos a derecha.

Nota: Sea R anillo con identidad, y sea $a \in R$ tal que existen $x, y \in R$ satisfaciendo

$$xa = 1 = ay.$$

Entonces $x = y$:

$$x = x \cdot 1 = x(ay) = (ax)y = 1 \cdot y = y.$$

5. $X := \{1, i, j, k\}$, y sea D el $\mathbb{R}$-espacio vectorial con base X. Es decir,

$$D = \mathbb{R} \oplus \mathbb{R}i \oplus \mathbb{R}j \oplus \mathbb{R}k.$$

Definimos la operación:

$$1 \cdot x = x \cdot 1 = x, \quad x \in \{i, j, k\}, \quad i^2 = j^2 = k^2 = -1,$$
$$ij = k,\ jk = i,\ ki = j,\ ji = -k,\ kj = -i,\ ik = -j.$$

Esta operación se extiende a un producto en D

$$(ax)(by) = (ab)(xy), \quad a, b \in \mathbb{R},\ x, y \in X.$$

y se extiende por distributividad a todo D. Sea $z \in D$,

$$z = a + bi + cj + dk \neq 0, \quad a, b, c, d \in \mathbb{R}.$$

entonces alguno de los números a, b, c, d es no nulo. Por tanto

$$a^2 + b^2 + c^2 + d^2 \neq 0.$$

Así,

$$z \cdot (a - bi - cj - dk) = a^2 + b^2 + c^2 + d^2 =: l.$$

Definimos

$$y := \frac{a}{l} - \frac{b}{l}i - \frac{c}{l}j - \frac{d}{l}k.$$

Entonces

$$z \cdot y = y \cdot z = 1.$$

Por lo que D es un anillo de división que no es cuerpo.

Si $R = \mathbb{R}$ y $G = Q_8$, entonces notamos que $RG = \mathbb{R}Q_8$ tiene "dimensión 8" por ser RG el conjunto de las sumas formales sobre un conjunto de 8 elementos, Q_8, mientras que

$$\mathbb{R} \oplus \mathbb{R}i \oplus \mathbb{R}j \oplus \mathbb{R}k$$

tiene dimensión 4. Es decir, son anillos distintos.

Definición 1.0.1. Sea R un anillo, $a \in R$. Sea

$$\begin{array}{rccc} \phi_a: & R & \longrightarrow & R \\ & x & \longmapsto & ax \end{array}$$

Entonces ϕ_a es un endomorfismo de R como grupo abeliano. Podemos definir

$$\begin{array}{rccc} \phi: & R & \longrightarrow & \mathrm{End}(R) \\ & a & \longmapsto & \phi_a \end{array}$$

Se puede comprobar que ϕ es homomorfismo de anillos. El núcleo de este homomorfismo se denomina *anulador de a*.

$$\mathrm{an}_R(a) = \ker \phi = \{a \in R : \ a \cdot x = 0 \text{ para todo } x \in R\}.$$

Definición 1.0.2. Sea $X \subseteq R$, donde R es un anillo. Entonces el *anulador de X* es

$$\mathrm{an}_R(X) = \{a \in R : \ a \cdot x = 0 \text{ para todo } x \in X\}.$$

Definición 1.0.3. Sea R un anillo con identidad. Un elemento $a \in R$ es *unidad* si existe $b \in R$ tal que

$$ab = ba = 1.$$

Denotamos por $U(R)$ al conjunto de unidades de R.

Proposición 1.0.1. *Si R es un anillo con identidad, $(U(R), \cdot)$ es un grupo.*

Demostración. Sea R un anillo con identidad. El elemento neutro del grupo será el $1 \in U(R)$. Sean $a, b \in U(R)$. Entonces $a^{-1}, b^{-1} \in U(R)$. Así,

$$(ab)^{-1} = b^{-1}a^{-1} \in U(R),$$

por lo que $U(R)$ es cerrado para el producto. Si $a \in U(R)$, su inverso para el producto es evidentemente $a^{-1} \in U(R)$. Notamos que $(a^{-1})^{-1} = a$. La propiedad asociativa se hereda de R. Por tanto, $(U(R), \cdot)$ es un grupo. ∎

Veamos algunos ejemplos:

1. Las unidades de $\mathbb{Z}$ son $U(\mathbb{Z}) = \{1, -1\}$.

2. Si R es un anillo con identidad,

$$U(\mathrm{M}_n(R)) = \mathrm{GL}(n, R).$$

3. Si $D = \mathbb{R} \oplus \mathbb{R}i \oplus \mathbb{R}j \oplus \mathbb{R}k$, y tomamos

$$A = \mathbb{Z} \oplus \mathbb{Z}i \oplus \mathbb{Z}j \oplus \mathbb{Z}k \subseteq D,$$

entonces $(A, +, \cdot)$ es un anillo y $U(A) = \{\pm 1, \pm i, \pm j, \pm k\}$.

4. Si R es un anillo con identidad y G es finito,

$$U(R) \cup G \subseteq U(RG).$$

5. El anillo $\mathbb{Z}[i]$ de enteros de Gauss, dado por

$$\mathbb{Z}[i] = \{a + bi : \ a, b \in \mathbb{Z}\}$$

con las operaciones heredadas del cuerpo $\mathbb{C}$, tiene unidades $U(\mathbb{Z}[i]) = \{\pm 1, \pm i\} \cong C_4$.

Definición 1.0.4. Sea R un anillo, y sea $0 \neq a \in R$. Se dice que a es *divisor de 0* a izquierda si $\exists b \neq 0$ tal que $ab = 0$. Análogamente, se dice que a es *divisor de 0* a derecha si $\exists b \neq 0$ tal que $ba = 0$. Si a es divisor de 0 a izquierda y a derecha, se dice que a es *divisor de 0*.

Existen divisores de 0 a izquierda que no lo son a derecha. Por ejemplo, consideramos el siguiente anillo

$$R = \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \;\middle|\; a, c \in \mathbb{Z}, \ b \in \mathbb{Z}/2\mathbb{Z} \right\}.$$

Los elementos

$$A = \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix}, \quad B = \begin{pmatrix} 0 & \overline{1} \\ 0 & 0 \end{pmatrix}$$

satisfacen $A \cdot B = 0$, por lo que A es divisor de 0 a izquierda. Sin embargo, para cualquier elemento X de R,

$$X = \begin{pmatrix} x & y \\ 0 & z \end{pmatrix},$$

se tiene

$$XA = \begin{pmatrix} 2x & 2y \\ 0 & z \end{pmatrix}.$$

Esta matriz es 0 si y sólo si $2x = 2y = z = 0$, si y sólo si $X = 0$. Por tanto, A no es divisor de 0 a derecha. Por último, $B^2 = 0$, por lo que es tanto divisor de 0 a izquierda como a derecha.

Definición 1.0.5. Sea R un anillo. Un elemento $a \in R$ es *nilpotente* si $a^n = 0$ para algún entero positivo n. Al conjunto de elementos nilpotentes del anillo se lo denota por $\mathrm{Nil}(R)$, en honor al matemático Nil Ojeda.

Definición 1.0.6. Sea R un anillo con identidad. Un elemento $a \in R$ es *cuasirregular* si $1 - a \in U(R)$.

Todo elemento nilpotente es irregular, pues si $a^n = 0$ para algún entero positivo n, entonces

$$(1 - a)(1 + a + \cdots + a^{n-1}) = 1 - a^n = 1.$$

Definición 1.0.7. Un *dominio* es un anillo sin divisores de 0. Si el anillo es conmutativo, con identidad, y es un dominio, entonces se lo denomina *dominio de integridad* o *dominio íntegro*.

Definición 1.0.8. Un anillo con identidad en el que $U(R) = R - \{0\}$ se lo denomina *anillo de división*. Un *cuerpo* es un anillo de división conmutativo.

Definición 1.0.9. Si R es un anillo, el *anillo opuesto*, R^{op}, es la terna $(R, +_{op}, \cdot_{op})$ con las operaciones

$$a +_{op} b = a + b, \qquad a \cdot_{op} b = b \cdot a.$$

1.1 Subanillos e ideales

Definición 1.1.1. Sea R un anillo. Un subconjunto $S \subseteq R$ es un *subanillo* si S es un anillo con las operaciones de R.

Veamos algunos ejemplos:

1. Si R es un anillo,
$$\{r \in R : \ \forall x \in R, ; rx = xr\}$$
es un subanillo de R. Se lo denota por $Z(R)$.

2. Sea R es un anillo con identidad, y sea S es un anillo tal que R es subanillo de S y $1_R = 1_S$. Si $\alpha_1, \ldots, \alpha_t \in S$, entonces definimos
$$R[\alpha_1, \ldots, \alpha_t] := \{f(\alpha_1, \ldots, \alpha_t) : \ f \in R[x_1, \ldots, x_t]\},$$
que es un subanillo de S. de hecho, es el menor subanillo de S que contiene a R y a $\{\alpha_1, \ldots, \alpha_t\}$.

Definición 1.1.2. Sea R un anillo. Un subanillo $I \subseteq R$ se dice

1. *i-ideal* de R si para todo $a \in I$ y para todo $r \in R$, $ra \in I$.
2. *d-ideal* de R si para todo $a \in I$ y para todo $r \in R$, $ar \in I$.
3. *ideal* de R si es i-ideal y d-ideal.

Veamos algunos ejemplos:

1. El 0 y R son siempre ideales de R. Además, si estos son sus únicos ideals y R tiene identidad, se dice que R es *simple*.

2. Los ideales de $\mathbb{Z}$ son los subgrupos de $(\mathbb{Z}, +)$.

3. Sea R anillo con identidad, $S = \mathrm{M}_n(R)$, $n \geq 1$. Entonces
$$A(d, i) := \{(a_{kl}) : \ a_{kl} = 0 \text{ si } k \neq i\}$$
es un d-ideal pero no un i-ideal de S. La "d" viene de "derecha". Análogamente,
$$A(i, j) := \{(a_{kl}) : \ a_{kl} = 0 \text{ si } l \neq j\}$$
es un i-ideal pero no un d-ideal

Proposición 1.1.1. *Sea R un anillo con identidad e I un d-ideal (o i-ideal, o ideal) de R. Entonces $I = R$ si y sólo si $I \cap U(R) \neq \emptyset$.*

Demostración. Sólo haremos el caso en el que I es i-ideal. Si $I = R$, entonces $1 \in I \cap U(R)$. Recíprocamente, si $I \cap U(R) \neq \emptyset$, entonces dado $u \in I \cap U(R)$ se tiene $u \cdot u^{-1} = 1 \in I$. Por tanto, para todo $r \in R$, $r = r \cdot 1 \in I$, es decir, $I = R$. ■

Nota: Si R tiene identidad y $a \in R$, aR es un d-ideal de R, Ra es un i-ideaal de R, y $a \in aR \cap Ra$.

Teorema 1.1.2 (Le mola al adolfo)**.** *Sea R anillo con identidad. Entonces R es anillo de división si y sólo si sus únicos d-ideales (resp. i-ideales) son $0, R$.*

Demostración. Supongamos que R es un anillo de división. Sea I d-ideal, $I \neq 0$. Entonces existe $0 \neq r \in I$, y por tanto $r \cdot r^{-1} = 1 \in I$. Por tanto, $I = R$. Recíprocamente, si $0 \neq r \in R$, entonces $0 \neq rR$, siendo rR un d-ideal de R. Por tanto, $rR = R$, y por tanto existe $s \in R$ tal que $rs = 1$, es decir, r es unidad. Por tanto R es anillo de división. ■

Corolario 1.1.2.1. *Sea R anillo conmutativo con identidad. Entonces R es cuerpo si y sólo si R es anillo simple.*

La hipótesis de conmutatividad es necesaria, pues si consideramos $R = \mathrm{M}_n(D)$ para algún anillo de división D, se tiene que R es simple pero no es un anillo de división porque $A(d,i), A(i,j)$ son d-ideales o i-ideales distintos de 0 y del total.

Definición 1.1.3. Sea R anillo, $X \subseteq R$, $I \subseteq R$ ideal. Entonces:

1. El siguiente conjunto es un i-ideal de R
$$IX \coloneqq \left\{ \sum_{i=1}^{n} a_i x_i : \ a_i \in I, \ x_i \in X, \ n \in \mathbb{N} \right\}$$
2. El siguiente conjunto es un d-ideal de R
$$IX \coloneqq \left\{ \sum_{i=1}^{n} x_i a_i : \ a_i \in I, \ x_i \in X, \ n \in \mathbb{N} \right\}$$

Definición 1.1.4. Sea R anillo y $X \subseteq R$. El d-ideal generado por X es la intersección de los d-ideales de R que contienen a X, y es denotado por $(X)_d$. Análogamente se define el i-ideal generado por X, denotado $(X)_i$, y el ideal generado por X, (X). Si $X = \emptyset$, el d-ideal, el i-ideal y el ideal generado por X se define como el conjunto vacío.

Teorema 1.1.3. *Sea $X \neq \emptyset$. Sea R anillo con identidad. Entonces*

1. $(X)_d = XR$.

2. $(X)_i = RX$.

3. $(X) = RXR$.

*Demostración.*Probamos 3. En primer lugar, notamos que $X \subseteq RXR$, ya que si $x \in X$, $x = 1 \cdot x \cdot 1 \in RXR$. Además, es fácil ver que
$$RXR = \left\{ \sum_{i=1}^{n} a_i x_i b_i : \ a_i \in I, \ b_i \in I, \ n \in \mathbb{N} \right\}$$

es ideal de R. Por último, si $I \subseteq R$ es un ideal tal que $X \subseteq I$, entonces cualquier elemento de RXR es de la forma

$$\sum_{i=1}^{n} a_i x_i b_i, \quad a_i \in R,\ b_i \in R,\ n \in \mathbb{N}$$

y como $x_i \in I$ para todo $i \in \{1, \ldots, n\}$, se tiene que $a_i x_i \in I$ y por tanto $a_i x_i b_i \in I$, por ser I ideal. Así,

$$\sum_{i=1}^{n} a_i x_i b_i \in I.$$

Y por tanto $RXR \subseteq I$. Es decir, RXR es el menor ideal de R que contiene a X. Concluimos así que $(X) = RXR$. ■

Nota: Si $X = \{a_1, \ldots, a_t\} \subseteq R$, entonces

1. $(X)_i = \left\{\sum_{i=1}^{t} r_i a_i :\ r_i \in R,\ 1 \leq i \leq t\right\}$
2. $(X)_d = \left\{\sum_{i=1}^{t} a_i s_j :\ s_i \in R,\ 1 \leq i \leq t\right\}$
3. $(X) = \left\{\sum_{i=1}^{t} r_i a_i s_j :\ r_i, s_j \in R,\ 1 \leq i \leq t\right\}$

Definición 1.1.5. Un i-ideal (d-ideal, ideal) de R es *finitamente generado*, abreviado *f.g.*, si existen elementos $a_1, \ldots, a_t \in R$, $t \in \mathbb{N}$, tales que

$$I = (\{a_1, \ldots, a_t\}) =: (a_1, \ldots, a_t)$$

Si $t = 1$, I es un *ideal principal* de R. En este caso, y si R tiene identidad, $I = (a) = RaR$, $(a)_i = Ra$, $(a)_d = aR$.

Definición 1.1.6. Un anillo con identidad es *anillo principal* si todo ideal es principal. Si, además, es un dominio, se lo denomina *dominio de ideales principales*, abreviado DIP.

Veamos algunos ejemplos.

1. $\mathbb{Z}$ es un DIP.

2. Si R es un dominio de integridad, $R[x]$ es un DIP si y sólo si R es cuerpo (ejercicio).

3. Sea $R = \mathbb{R}^{[0,1]}$. Sea $a \in [0,1]$. El subconjunto

   $$R_a := \{f \in R :\ f(a) = 0\}$$

   es un ideal principal. Sea

   $$\begin{array}{rlcl} \ell: & [0,1] & \longrightarrow & \mathbb{R} \\ & x & \longmapsto & 1 \text{ si } x \neq a \\ & x & \longmapsto & 0 \text{ si } x = a, \end{array}$$

   de modo que $\ell \in R_a$. Por tanto (ℓ) es un subideal de R_a. Por otro lado, dado $f \in R_a$, se tiene que $f = f\ell$. Por tanto, $f \in (\ell)$. Concluimos así que $R_a = (\ell)$ es un ideal principal.

4. Sea $S = \{f : [0,1] \longrightarrow \mathbb{R} :\ f \text{ es continua}\}$. Es un subanillo de $\mathbb{R}^{[0,1]}$. Sea $a \in [0,1]$. Definimos $S_a = \{f \in S :\ f(a) = 0\}$, que es un ideal de S. Este ideal no es finitamente generado (ejercicio).

5. Sea K un cuerpo, y consideramos la cadena de anillos

$$K[x_1] \subseteq K[x_1, x_2] \subseteq \cdots .$$

Definimos

$$K[x_1, x_2, \dots] := \bigcup_{i \geq 1} K[x_1, \dots, x_i].$$

Este es un anillo conmutativo con identidad. El ideal I generado por todas las indeterminadas no es finitamente generado.

1.2 Anillo cociente

Sea R un anillo, $I \subseteq R$ un ideal. Entonces $(I, +)$ es un subgrupo normal de $(R, +)$, por lo que podemos considerar el cociente R/I como grupo. A este grupo le añadimos una operación $\cdot$ dada por

$$(a + I) \cdot (b + I) = ab + I, \quad a, b \in R.$$

Comprobamos que $\cdot$ es aplicación. Si $a + I = a_1 + I$ y $b + I = b_1 + I$, el hecho de que I es ideal garantiza lo siguiente

$$ab - a_1 b_1 = ab - a_1 b + a_1 b - a_1 b_1 = (a - a_1) b + a_1 (b - b_1) \in I.$$

La terna $(R/I, +, \cdot)$ es el anillo denominado "anillo cociente" de R por I.

1.2.1 Homomorfismo de anillos

Definición 1.2.1. Sean R_1, R_2 anillos. Una aplicación $f : R_1 \longrightarrow R_2$ es *homomorfismo de anillos*, abreviado *HM* de anillos, si

$$f : (R_1, +) \longrightarrow (R_2, +)$$

es homomorfismo de grupos y además $f(xy) = f(x)f(y)$ para todo $x, y \in R_1$.

Si $f : R_1 \longrightarrow R_2$ es un HM de anillos, de la definición se derivan las siguientes propiedades:

1. $f(0_{R_1}) = 0_{R_2}$.
2. $f(-a) = -f(a)$.
3. Si R_1 y R_2 tienen identidad, en general $f(1_{R_1}) \neq 1_{R_2}$. Basta considerar la aplicación constante 0, que es HM de anillos. Sin embargo, si f es sobreyectiva, entonces $f(1_{R_1}) = 1_{R_2}$.

Teorema 1.2.1. *Sea $f : R_1 \longrightarrow R_2$ un HM de anillos. Entonces*

1. *Si $A \subseteq R_1$ es un subanillo, entonces $f(A)$ es un subanillo de R_2. En particular,*

$$\operatorname{Im}(f) := f(R_1) \subseteq R_2$$

es subanillo de R_2.

2. *Si* $I \subseteq R_1$ *es un ideal, entonces no necesariamente* $f(I)$ *es un ideal de* R_2. *Sin embargo, si* f *es sobreyectiva, entonces* $f(I)$ *es un ideal de* R_2.

3. *Si* A *es un subanillo (resp. ideal) de* R_2*, entonces* $f^{-1}(A)$ *es un subanillo (resp. ideal) de* R_1. *En particular,*

$$\ker(f) \coloneqq f^{-1}(0_{R_2}) \subseteq R_1$$

es un ideal de R_1 *contenido en cada* $f^{-1}(J)$, J *ideal de* R_2.

4. *Se cumple el teorema de isomofía para anillos*

$$R_1/\ker(f) \cong \operatorname{Im}(f).$$

Demostración.

1. Sean $r, s \in f(A)$, donde A es un subanillo de R_1. Entonces $r = f(a), s = f(b)$ para algunos $a, b \in R_1$. Por tanto

$$rs = f(a)f(b) = f(ab) \in f(A), \quad r + s = f(a) + f(b) = f(a + b) \in f(A),$$

concluyendo que $f(A)$ es un subanillo de R_2. En particular, $\operatorname{Im}(f)$ es subanillo de R_2.

2. Como contraejemplo consideramos el ideal $n\mathbb{Z}$ de $\mathbb{Z}$ y la aplicación inclusión $i : \mathbb{Z} \longrightarrow \mathbb{Q}$. El conjunto $i(n\mathbb{Z})$ no es un ideal de $\mathbb{Q}$ para ningún n entero positivo.

   Supongamos que f es sobreyectiva. Veamos que $f(I)$ sí es un ideal de R_2. Sea $r \in R_2$, $a \in f(I)$. Dado que f es sobreyectiva existe $s \in R_1$ tal que $f(s) = r$. Sea $i \in I$ tal que $a = f(i)$. Entonces $ra = f(s)f(i) = f(si) \in f(I)$, dado que al ser I ideal, $si \in I$.

3. Supongamos que A es un subanillo de R_2. Sean $r, s \in f^{-1}(A)$. Entonces $f(r), f(s) \in A$. Como A es subanillo, $f(r)+f(s), f(r)f(s) \in A$. Como f es homomorfismo, $f(r+s), f(rs) \in A$. Concluimos que $r + s, rs \in f^{-1}(A)$, luego $f^{-1}(A)$ es subanillo. Además, si J es un ideal de R_2, dado que $0 \in J$ se tiene que $\ker f = f^{-1}(\{0\}) \subseteq f^{-1}(J)$.

4. Son isomorfos como grupos. Consideramos

$$\begin{array}{rccc} \overline{f}: & R_1/\ker(f) & \longrightarrow & \operatorname{Im}(f) \\ & x + \ker(f) & \longmapsto & f(x). \end{array}$$

   Entonces

$$\overline{f}[(x+\ker(f))(y+\ker(f))] = \overline{f}[xy+\ker(f)] = f(xy) = f(x)f(y) = \overline{f}(x+\ker(f))\overline{f}(y+\ker(f)),$$

   concluyendo así que $\overline{f}$ es homomorfismo de anillos. ∎

Veamos algunos ejemplos

1. Sea I un ideal de R. La aplicación $\rho : R \longrightarrow R/I$ es un epimorfismo que satisface $\ker \rho = I$.

2. Sea I un ideal de R. La aplicación $\overline{\rho} : \mathrm{M}_n(R) \longrightarrow \mathrm{M}_n(R/I)$ dada por

$$\overline{\rho}[(a_{ij})] = (\rho(a_{ij}))$$

es un epimorfismo de anillos que satisface $\ker \overline{\rho} = \mathrm{M}_n(I)$. ■

A continuación nos disponemos a mostrar qué forma tienen los ideales del anillo cociente. Sea R un anillo, $I \subseteq R$ un ideal. Sea J cualquier otro ideal de R. Dado que ρ es un epimorfismo, $\rho(J)$ es un ideal de R/I.

$$\rho(J) = \{j + I : \ j \in J\} = \{j + i + I : \ j \in J, i \in I\}.$$

Consideramos el siguiente ideal de R

$$I + J := \{i + j : \ i \in I, j \in J\}.$$

Este ideal satisface $I \subseteq I + J$. Así, I es ideal de $I + J$. Por tanto,

$$\rho(J) = (I + J)/I$$

es un ideal de R/I. Reciprocamente, si A es un ideal de R/I, tomamos el ideal de R

$$B := \rho^{-1}(A),$$

que satisface $\ker \rho = I \subseteq B$. Al ser ρ epimorfismo,

$$A = \rho(\rho^{-1}(A)) = \rho(B) = (I + B)/I = B/I.$$

Por último, si se da la igualdad

$$A_1/I = A_2/I$$

para ideales A_1, A_2 de R, entonces

$$A_1 = \rho^{-1}(A_1/I) = \rho^{-1}(A_2/I) = A_2.$$

Esto nos permite concluir lo siguiente

Teorema 1.2.2. *Los ideales del anillo cociente R/I son los cocientes de la forma J/I donde $J \subseteq R$ es un ideal que contiene a I.*

Teorema 1.2.3 (Segundo teorema de isomorfía)**.** *Sea R un anillo, $I, J \subseteq R$ ideales. Entonces*

$$J/(I \cap J) \cong (I + J)/I.$$

Demostración. Consideramos el epimorfismo

$$\overline{\rho} = \rho|_J : J \longrightarrow \rho(J) = (I + J)/I.$$

con núcleo $\ker \overline{\rho} = I \cap J$. Por el primer teorema de isomorfía,

$$J/(I \cap J) \cong (I + J)/I.$$

■

Teorema 1.2.4 (Tercer teorema de isomorfía)**.** *Sea R un anillo, $I \subseteq J \subseteq R$ ideales tales. Entonces*

$$(R/I)/(J/I) \cong R/J.$$

Demostración. Consideramos la correspondencia

$$\begin{array}{rccc} \varphi: & R/I & \longrightarrow & R/J \\ & r+I & \longmapsto & r+J. \end{array}$$

Esta correspondencia es una aplicación, pues

$$r + I = r_1 + I \implies r - r_1 \in I \subseteq J \implies \varphi(r) = r + J = r_1 + J = \varphi(r_1).$$

Es más, φ es un epimorfismo de anillos con núcleo $\ker \varphi = J/I$. Por el primer teorema de isomorfía,

$$(R/I)/(J/I) \cong R/J.$$

■

1.3 Operaciones con ideales.

Definición 1.3.1. Sea $\{L_i\}_{i\in I}$ una familia de ideales de un anillo R. Entonces

$$\sum_{i\in I} L_i := \left(\bigcup_{i\in I} L_i \right).$$

Si R tiene identidad, entonces

$$\sum_{i\in I} L_i = \left\{ \sum_{j=1}^{t} l_j : \ l_j \in L_{i_j},\ i_j \in I,\ 1 \leq j \leq t \in \mathbb{N} \right\}$$

Se dice que la suma es *directa* si para todo índice $i \in I$, se cumple

$$L_i \cap \left(\sum_{j\neq i} L_j \right) = 0$$

En este caso, denotamos a la suma por

$$\bigoplus_{i\in I} L_i.$$

Proposición 1.3.1. *Si $\{L_i\}_{i\in I}$ es una familia de ideales de un anillo R cuya suma es directa, para todo elemento x de la suma existen índices únicos $i_1, \ldots, i_t \in I$ y elementos no nulos únicos $x_1 \in L_{i_1}, \ldots, x_t \in L_{i_t}$ tales que*

$$x = x_1 + \cdots + x_t.$$

Además, si la suma es finita

$$L_1 \oplus L_2 \oplus \cdots \oplus L_n \cong L_1 \times L_2 \times \cdots \times L_n.$$

Demostración. Veamos primero que el cero no se puede expresar como suma de elementos no nulos. Por reducción al absurdo, si $0 = x_1 + \cdots + x_n$, para $0 \neq x_i$ en sus respectivos L_{j_i}, todos los L_{j_i} distintos dos a dos, entonces

$$x_1 = -x_2 - \cdots - x_n \in L_{i_1} \cap \left(\sum_{j \neq i_1} L_{i_j} \right) = 0.$$

lo que supone una contradicción.

Sea $x \in \oplus_{i \in I} L_i$. Supongamos que existen $x_1, \ldots, x_t, y_1, \ldots, y_s$ elementos no nulos de $L_{i_1}, \ldots, L_{i_t}, L_{j_1}, \ldots, L_{j_s}$ respectivamente tales que

$$x = x_1 + \cdots + x_t = y_1 + \cdots + y_s.$$

Supongamos que $t > s$. Entonces

$$x_1 + \cdots + x_t - y_1 - \cdots - y_s = 0.$$

Y esto implica necesariamente que alguno de los x_i ha de ser 0, en contradicción con lo supuesto. Análogamente se prueba que $t < s$ no es posible. Por tanto, $t = s$. Supongamos ahora que existe algún L_{i_k} que es distinto a todos los L_{j_l}, $1 \leq k, l \leq t$. Entonces podríamos expresar x_{i_k} como suma de elementos que no están en L_{i_k}, lo que implica $x_{i_k} = 0$. Esta contradicción nos dice que podemos reordenar los elementos x_i, y_j de forma que $x_i, y_i \in L_i$ para todo $i \in 1, \ldots, t$. Ahora, tenemos

$$(x_1 - y_1) + \cdots + (x_t - y_t) = 0,$$

y por tanto cada término es 0. Esto demustra que la expresión es única. ■

Definición 1.3.2. Sean $L_1, \ldots, L_n \subseteq R$ ideales. El producto $L_1 \cdot \cdots \cdot L_n$ es el ideal generado por el conjunto

$$\{x_1 \cdots x_n : \; x_i \in L_i, \; 1 \leq i \leq n\}.$$

En concreto:

$$L_1 \cdots L_n = \left\{ \prod_{i=1}^{n} l_i : \; l_i \in L_i \right\}$$

Además, si I es un ideal de R, se define $I^1 := I$, $I^{n+1} := I^n \cdot I$.

Definición 1.3.3. Se dice que un ideal I de un anillo R es *nilpotente* si $I^n = 0$ para algún entero positivo n.

Por ejemplo, si $I \subseteq R$ es un ideal, para cualquier entero positivo n, I/I^n es ideal nilpotente. Esto es fácil de comprobar.

Teorema 1.3.2. *Sea R un anillo con identidad. Entonces su caracteristica es un número primo o 0.*

Demostración. Considérese el homomorfismo

$$\begin{array}{rccc} \varphi: & \mathbb{Z} & \longrightarrow & R \\ & n & \longmapsto & n \cdot 1_R, \end{array}$$

cuyo núcleo es un ideal de $\mathbb{Z}$. Por ser $\mathbb{Z}$ un dominio de ideales principales, $\ker \varphi = (t)$, para algún $t \in \mathbb{Z}$. Si $t = 0$, para todo $n \in \mathbb{Z}$, $n \cdot 1_R = 0$, y por tanto la característica de R es 0. Si $t \neq 0$, entonces t es un número primo, y por tanto la característica de R es t. ■

Lema 1.3.3 (Binomio de Newton)**.** *Sea R un anillo conmutativo con identidad. Entonces*

$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}$$

Proposición 1.3.4. *Sea R un anillo conmutativo con identidad. Entonces*

$$\mathrm{Nil}(R) = \{x \in R : \ x \ \textit{es nilpotente}\}$$

es ideal de R.

Demostración. Sea $x \in \mathrm{Nil}(R)$, $r \in R$. Entonces

$$(rx)^n = r^n x^n = 0,$$

y por tanto $rx \in \mathrm{Nil}(R)$. Además, si $a, b \in \mathrm{Nil}(R)$, existen enteros positivos n, m tales que

$$a^n = b^m = 0.$$

Por el binomio de Newton,

$$(a+b)^{n+m} = 0,$$

y por tanto $a + b \in \mathrm{Nil}(R)$. ■

Si un ideal es nilpotente, todos sus elementos son nilpotentes. El recíproco no es cierto. Por ejemplo, si K es un cuerpo, tomamos

$$S \coloneqq K[x_1, x_2, \dots], \quad J \coloneqq K[x_1^2, x_2^3, \dots] \subseteq (x_1, x_2, \dots) \eqqcolon I, \quad R \coloneqq S/J$$

Todo elemento de I/J es nilpotente: si $x_l \in I$ entonces $x_l^{l+1} \in J$, luego

$$x_l + J \in \mathrm{Nil}(R)$$

Sin embargo, el ideal I/J no es nilpotente (ejercicio).

1.4 Ideales primos y maximales

A partir de aquí, todo anillo será considerado con identidad, aunque no se diga, salvo que se indique lo contrario.

Definición 1.4.1. Un ideal P de un anillo R se dice *primo* si verifica las siguientes condiciones:

1. $P \neq R$.

2. Si I, J son ideales de R tales que $IJ \subseteq P$, entonces $I \in P$ o $J \in P$.

Notación:

$$\operatorname{Spec}(R) := \{P \mid P \text{ ideal primo de } R\}.$$

Si D es un anillo de división, $\operatorname{Spec}(\mathrm{M}_n(D)) = \{0\}$, ya que los ideales de $\mathrm{M}_n(D)$ son $\{0, \mathrm{M}_n(D)\}$.

Proposición 1.4.1. *Sea R un anillo y sea $P \subsetneq R$ un ideal. Entonces P es primo si y sólo si para todo a, b en R tales que $ab \in P$, se tiene $a \in P$ o $b \in P$.*

Proposición 1.4.2. *Sea R anillo con identidad y $P \subsetneq R$ un ideal. Las siguientes afirmaciones son equivalentes:*

1. *P es primo.*
2. *Si $a, b \in R$ son tales que $(a)(b) \subseteq P$ entonces $(a) \subseteq P$ o $(b) \subseteq P$.*
3. *Si $a, b \in R$ son tales que $aRb \in P$ entonces $a \in P$ o $b \in P$. [Importante]*
4. *Si A, B son i-ideales de R tales que $AB \subseteq P$, entonces $A \subseteq P$ o $B \subseteq P$.*
5. *Si A, B son d-ideales de R tales que $AB \subseteq P$, entonces $A \subseteq P$ o $B \subseteq P$.*

Demostración. 1 implica 2 trivialmente. Supongamos que 2 se cumple.

Si $aRb \subseteq P$, entonces

$$(RaR)(RbR) \subseteq RPR = P,$$

y por tanto

$$(a)(b) \subseteq P,$$

y por la condición 2, $a \in P$ o $b \in P$.

Supongamos que se satisface la condición 3. Sean A, B i-ideales de R tales que $AB \subseteq P$. Supongamos $A \subsetneq P$, y sea $a \in A - P$. Sea $b \in B$. Como A es i-ideal, $Ra \subseteq A$. Análogamente, $Rb \subseteq B$. Por tanto,

$$aRb \subseteq (Ra)(Rb) \subseteq AB \subseteq P.$$

Así, $aRb \subseteq P$, y por la condición 3, $a \in P$ o $b \in P$. Como $a \notin P$, necesariamente $b \in P$. Concluimos que $B \subseteq P$.

Veamos que 4 implica 5. Sean A, B d-ideales de R tales que $AB \subseteq P$. Entonces

$$R\underbrace{AR}_{A}B \subseteq RP = P.$$

Como RA, RB son i-ideales, se tiene que $RA \subseteq P$ o $RB \subseteq P$. Por tanto, $A \subseteq P$ o $B \subseteq P$.

Todo ideal es d-ideal, por lo que 5 implica 1. ■

Ejercicio: Sean A un i-ideal, B es d-ideal tales que $AB \subseteq P$. Esto no es condición suficiente para asegurar $A \subseteq P$ o $B \subseteq P$.

Proposición 1.4.3. *Sea R un anillo conmutativo con identidad, y sea $P \neq R$ un ideal. El ideal P es primo si y sólo si R/P es un dominio de integridad.*

Demostración. Si P es primo, entonces $P \neq R$, luego $1 \notin P$, luego

$$1 + P \neq 0 + P.$$

Así, R/P es un dominio. Si $[a], [b]$ son elementos de R/P cuyo producto es cero, entonces

$$[ab] = [a][b] = 0.$$

Por tanto, $ab \in P$. Como P es primo, o bien a está en P, o b está en P. Por tanto, $[a] = 0$ o $[b] = 0$, y por tanto R/P es un dominio.

Recíprocamente, si A/P es un dominio íntegro, necesariamente

$$1 + P \neq 0 + P,$$

por lo que $1 \notin P$, luego $P \neq R$. Así, si a, b son elementos de R tales que $ab \in P$, entonces

$$(a + P)(b + P) = (ab + P) = 0,$$

y como R/P es dominio íntegro, necesariamente $(a + P) = 0 + P$ o $(b + P) = 0 + P$, es decir, $a \in P$ o $b \in P$. Por tanto, P es primo. ■

Ejemplo: Sea $R = K[x, y]$, con K cuerpo. Usaremos la proposición anterior para demostrar que $(x), (y)$ son ideales primos de R. Consideramos el epimorfismo de anillos

$$\begin{array}{rccc} \varphi : & K[x,y] & \longrightarrow & K[x] \\ & f(x,y) & \longmapsto & f(x,0). \end{array}$$

Un elemento $f \in K[x, y]$, que podemos escribir de la forma

$$f(x,y) = a_0(x) + \sum_{i=1}^{n} a_i(x) y^i,$$

pertenece al núcleo de φ si y sólo si

$$f(x,0) = a_0(x) = 0.$$

Por tanto,

$$\ker \varphi = (y).$$

Por otro lado, al ser φ epimorfismo, el primer teorema de isomorfía nos dice que

$$K[x,y]/(y) \cong K[x],$$

y dado que $K[x]$ es dominio íntegro, (y) es ideal primo en $K[x, y]$.

1.5 Subconjuntos multiplicativos y m-conjuntos.

Definición 1.5.1. Seaa R un anillo, $\emptyset \neq S \subseteq R$. Entonces

1. S es *multiplicativo* si $1 \in S$ y si $a, b \in S$ entonces $ab \in S$.
2. S es un m-conjunto si $a, b \in S$ implica la existencia de un elemento $r \in R$ tal que $arb \in S$.

Veamos algunos ejemlos:

1. Si S es un subconjunto multiplicativo de R, entonces S es un m-conjunto. El recíprono no es cierto, como veremos en el siguiente ejemplo.
2. $S := \{1, a, a^2, a^4, a^8, \dots\}$ es un m-conjunto que no es multiplicativo, ya que $a \cdot a^2 = a^3 \notin S$.
3. Si P es un ideal primo de R, entonces $R - P$ es un m-conjunto. La siguiente proposición muestra que el recíproco es cierto.

Proposición 1.5.1. *Sea $P \neq R$ ideal. Entonces P es primo si y sólo si $S = R - P$ es un m-conjunto.*

Demostración. Supongamos que P es primo, y $a, b \in S$. Supongamos por reducción al absurdo que $a, b \notin P$. En este caso, $aRb \subsetneq P$. Sea $r \in R$ tal que $arb \notin P$. Entonces

$$arb \in R - P = S$$

concluimos que S es un m-conjunto.

Recíprocamente, si S es un m-conjunto, sean $a, b \in R$ tales que $aRb \subseteq P$. Supongamos por reducción al absurdo que $a, b \notin P$. Entonces $arb \in S$ para algún elemento r de R. Así,

$$arb \in S \cap aRb \subseteq S \cap P = \emptyset,$$

lo cual es una contradicción. faf

Lema 1.5.2. *Sea S un m-conjunto de R. Sea $P \subsetneq R$ un ideal maximal respecto a la condición $S \cap P = \emptyset$. Entonces P es un ideal primo.*

Demostración. Sean $a, b \in R$ tales que $(a)(b) \in P$. Supongamos por reducción al absurdo que $(a) \nsubseteq P$ y $(b) \subsetneq P$. Entonces $P \subsetneq P + (a)$ y $P \subsetneq P + (b)$. Por tanto

$$S \cap (P + (a)) \neq \emptyset \neq S \cap (P + (b)).$$

Por tanto, existe $s_i = p_i + \lambda_i \in S$ con $p_i \in P$, $\lambda_1 \in (a)$, $\lambda_2 \in (b)$, $i = 1, 2$. Dado que S es un m-conjunto, existe un elemento r de R tal que $s_1 r s_2 \in S$. Ahora bien,

$$s_1 r s_2 = (p_1 + \lambda_1) r (p_2 + \lambda_2) \in (P + (a))(P + (b)) \subseteq P + (a)(b) \subseteq P.$$

Por tanto, $s_1 r s_2 \in S \cap P = \emptyset$, lo cual es una contradicción.

Definición 1.5.2. Sea $I \subsetneq R$ un ideal. Definimos el radical de I, $\mathrm{Rad}(I)$, como

$$\mathrm{Rad}(I) = \{x \in R : \; x \in S \subseteq R, \, S \text{ m-conjunto} \implies S \cap I = \emptyset\}.$$

Proposición 1.5.3. *Sea $I \subsetneq R$ un ideal. Entonces*

$$\mathrm{Rad}(I) \subseteq \{x \in R : \; \exists x^n = 1 \textit{ para algún } n \geq 1\}.$$

Si R es conmutativo, se da la igualdad.

Demostración. Sea $x \in \mathrm{Rad}(I)$. El conjunto

$$S_x = \{1, x, x^2, \dots\}$$

es multiplicativo, y por tanto un m-conjunto. Además, dado que $x \in S$, se tiene que $S \cap I \neq \emptyset$. Sea $y \in S \cap I$. Entonces $y = x^n$ para algún $n \geq 1$.

Supongamos que R es conmutativo. Sea $x \in R$ tal que $x^n = I$ para algún $n \geq 1$. Sea S un m-conjunto de R tal que $x \in S$. Entonces existe $r_1 \in S$ tal que $x r_1 x = x^2 r_1 \in S$. Por inducción se prueba que existe r_{n-1} tal que $x^n r_{n-1} \in S$. Por tanto $x^n r_{n-1} \in S \cap I \neq \emptyset$. Deducimos así que x pertenede a $\mathrm{Rad}(I)$.

Proposición 1.5.4. *Sea R un anillo conmutativo e $I \subseteq R$ un ideal. Entonces:*

1. $\mathrm{Rad}(0) = \mathrm{Nil}(R) \subseteq R$ *es un ideal.*
2. $\mathrm{Rad}(I)$ *es un ideal de R.*
3. $I \subseteq \mathrm{Rad}(I)$.
4. $\mathrm{Rad}(I)/I = \mathrm{Nil}(R/I)$.

Demostración.

1. Se deduce de la proposición anterior.
2. Sean $x, y \in \mathrm{Rad}(I)$. Entonces existen $n, m \geq 1$ tales que $x^n, y^m \in I$. Así,
$$(x+y)^{n+m} = \sum_{k=0}^{n+m} \binom{n+m}{k} x^k y^{m+n-k} \in I.$$
Por tanto $x + y \in \mathrm{Rad}(I)$. Además, si $r \in R$, entonces $(rx)^n = r^n x^n \in I$. Por tanto $rx \in \mathrm{Rad}(I)$. Concluimos así que $\mathrm{Rad}(I)$ es un ideal.
3. Dado $x \in I$, se tiene $x^n \in I$ para $n = 1$, luego $x \in \mathrm{Rad}(I)$.
4. Sea $x + I \in \mathrm{Rad}(I)/I$. Entonces existe $n \geq 1$ tal que $x^n \in I$. Por tanto,
$$(x+I)^n = 0 + I.$$
Por tanto, $x + I \in \mathrm{Nil}(R/I)$. Recíprocamente, sea $x + I \in \mathrm{Nil}(R/I)$. Entonce existe $n \geq 1$ tal que
$$(x+I)^n = 0 + I,$$
y por tanto $x^n \in I$, luego $x \in \mathrm{Rad}(I)$. Así, $x + I \in \mathrm{Rad}(I)/I$. Concluimos que $\mathrm{Rad}(I)/I = \mathrm{Nil}(R/I)$.

Teorema 1.5.5. *Sea R un anillo, $I \neq R$ un ideal. Entonces*

$$\mathrm{Rad}(I) = \bigcap_{I \subseteq P \in \mathrm{Spec}(R)} P.$$

Demostración. Sea $x \in \mathrm{Rad}(I)$. Sea $n \geq 1$ tal que $x^n \in I$. Si $P \in \mathrm{Spec}(R)$ contiene a I, entonces $x^n \in P$, y como P es primo, necesariamente $x \in P$. Esto implica la siguiente inclusión:

$$\mathrm{Rad}(I) \subseteq \bigcap_{I \subseteq P \in \mathrm{Spec}(R)} P.$$

Sea ahora $x \in R$ contenido en todos los ideales primos de R que contienen a I. Supongamos por reducción al absurdo que $x \notin \mathrm{Rad}(I)$. Entonces existe un m-conjunto S tal que $S \cap I = \emptyset$. Consideramos el siguiente conjunto con el objetivo de aplicar el lema de Zorn

$$\tau = \{J \neq R \ \mathit{ideal} \colon \ J \subseteq I, \wedge J \cap S = \emptyset\}.$$

Este conjunto es no vacío porque contiene al elemento I. Además, es un conjunto ordenado por inclusión. Sea $\{C_k\}_{k \in K}$ una cadena de τ. Tomamos el conjunto

$$C \coloneqq \bigcup_{k \in K} C_k.$$

Veamos que $C \in \tau$. En efecto,

$$C \cap S = \left(\bigcup_{k \in K} C_k \right) \cap S = \bigcup_{k \in K} (C_k \cap S) = \emptyset.$$

y si $c \in C$, entonces $c \in C_k$ para algún $k \in I$, y por tanto $c \in I$. Así, $C \subseteq I$. Vemos además que C es una cota superior de la cadena. Concluimos por el lema de Zorn que existe un elemento maximal de τ. Sea P ese elemento maximal. Por el lema 1.5.2, el ideal P es maximal, por lo que $x \in P$. Pero entonces $x \in P \cap S = \emptyset$, lo que supone una contradicción. Concluimos que $x \in \mathrm{Rad}(I)$. ■

Proposición 1.5.6. *Seaa $I \subseteq R$ un ideal. Entonces*

1. *Si $I \in \mathrm{Spec}(R)$, entonces $\mathrm{Rad}(I) = I$.*

2. *Sea $P \in \mathrm{Spec}(R)$. Entonces $I \subseteq P$ si y sólo si $\mathrm{Rad}(I) \subseteq P$. En particular,*

$$\mathrm{Rad}(\mathrm{Rad}(I)) = \mathrm{Rad}(I).$$

3. *Si I, J son ideales de R, entonces*

$$\mathrm{Rad}(IJ) = \mathrm{Rad}(I \cap J).$$

En particular, para todo entero positivo n,

$$\mathrm{Rad}(I^n) = \mathrm{Rad}(I).$$

Demostración.

1. Se sigue del teorema anterior. Si I no es primo, no tiene por qué cumplirse: basta tomar el ideal $I = (p^n) \subseteq \mathbb{Z}$ para cualquier $n \geq 2$.

2. Sea $P \in \mathrm{Spec}(R)$ tal que $I \subseteq P$. Entonces

$$\mathrm{Rad}(I) = \bigcap_{\substack{I \subseteq Q \\ Q \in \mathrm{Spec}(R)}} Q \subseteq P.$$

   Recíprocamente, $\mathrm{Rad}(I) \subseteq P$, del hecho de que $I \subseteq \mathrm{Rad}(I)$ se deduce directamente que $I \subseteq P$. En este caso,

$$\mathrm{Rad}(\mathrm{Rad}(I)) = \bigcap_{\substack{\mathrm{Rad}(I) \subseteq P \\ P \in \mathrm{Spec}(R)}} P = \bigcap_{\substack{I \subseteq P \\ P \in \mathrm{Spec}(R)}} P = \mathrm{Rad}(I)$$

3. Sea $P \in \mathrm{Spec}(R)$. Si $L \subseteq M \subseteq R$ son ideales y $M \subseteq P$, entonces $L \subseteq P$. Es decir, hay más primos conteniendo a L que a M. Al intersectarlos, obtenemos que

$$\mathrm{Rad}(L) \subseteq \mathrm{Rad}(M).$$

   Es decir, el radical conserva inclusiones. En particular, dadas las inclusiones

$$IJ \subseteq I, \quad IJ \subseteq J, \quad IJ \subseteq I \cap J,$$

   se obtienen las inclusiones

$$\mathrm{Rad}(IJ) \subseteq \mathrm{Rad}(I)\mathrm{Rad}(J), \quad \mathrm{Rad}(IJ) \subseteq \mathrm{Rad}(I \cap J) \subseteq \mathrm{Rad}(I) \cap \mathrm{Rad}(J).$$

   Además, como P es primo, si $IJ \subseteq P$, entonces $I \subseteq P$ o $J \subseteq P$. En cualquier caso, $I \cap J \subseteq P$. Esto implica que

$$\mathrm{Rad}(I \cap J) \subseteq \mathrm{Rad}(IJ).$$

   Concluimos con la iguadad

$$\mathrm{Rad}(IJ) = \mathrm{Rad}(I \cap J).$$

   En particular,

$$\mathrm{Rad}(I^n) = \mathrm{Rad}(I \cap \cdots \cap I) = \mathrm{Rad}(I).$$

■

Definición 1.5.3. Sea $M \subseteq R$ un i-ideal (d-ideal). M es *i-maximal* (*d-maximal*) si se satisfacen las dos condiciones siguientes

1. $M \neq R$.

2. Si $M \subseteq L \subseteq R$, siendo L un i-ideal (d-ideal), entonces $L = R$ o $L = M$.

Al conjunto de i-ideales i-maximales (d-ideales d-maximales) de R se lo denota por $\mathrm{Max}_i(R)$ ($\mathrm{Max}_d(R)$). Al conjunto de ideales maximales de R se lo denota por $\mathrm{Max}(R)$.

Nótese que un ideal M de R es maximal si y sólo si los únicos ideales de R/M son el 0 y R/M. En particular, si R es conmutativo, un ideal es maximal si y sólo si R/M es cuerpo. Esto es falso si R es conmutativo: basta considerar cualquier anillo de división no conmutativo D y obtenemos que $R = M_n(D)$ no tiene ideales (sí tiene i-ideales y d-ideales). Esto se debe a que cualquier ideal no nulo de R contiene a todos los e_{ij}, como el lector comprobará fácilmente. Y por tanto, el ideal se trata de el anillo entero, R. Así, el 0 es ideal maximal, pero $R/0$ es un anillo isomorfo a R, que no es un cuerpo.

Por otro lado, notamos que si M es un ideal maximal de R e I es otro ideal que no está contenido en M, entonces $M + I$ es un ideal que contiene estrictamente a R, lo que, por la maximalidad de M, implica $R = M + I$.

Proposición 1.5.7. *Todo ideal maximal es primo.*

Demostración. Sea M un ideal maximal de R, y supongamos que A, B son ideales de R tales que $AB \subseteq M$. Si ninguno de los dos ideales estuviera contenido en M, por el párrafo previo a esta proposición se tiene

$$R = M + A = M + B.$$

Por tanto,

$$R = R^2 = (M + A)(M + B) \subseteq M + AB \subseteq M,$$

lo que contradice la maximalidad de M.

Veamos algunos ejemplos:

1. No todo ideal primo es maximal. Por ejemplo, el idea primo $0 \in \mathrm{Spec}\mathbb{Z}$ no es maximal.

2. Sea K un cuerpo. Sea $R = K[x, y]$. Considérese el epimorfismo de anillos

$$\begin{array}{rccc} \varphi: & R & \longrightarrow & K \\ & f(x,y) & \longmapsto & f(0,0). \end{array}$$

   Entonces $\ker \varphi = (x, y)$, lo que implica

$$K[x, y]/(x, y) \cong K$$

   y dado que K es cuerpo, el ideal (x, y) es maximal.

3. Considérese el anillo

$$R \coloneqq \{f : [0,1] \longrightarrow \mathbb{R} |\ f \text{ es continua.}\} \subseteq \mathbb{R}^{[0,1]}.$$

   Sea $\alpha \in [0, 1]$. Considérese el homomorfismo de anillos

$$\begin{array}{rccc} \varphi_\alpha: & R & \longrightarrow & \mathbb{R} \\ & f & \longmapsto & f(\alpha), \end{array}$$

   cuyo núcleo es $M(\alpha) \coloneqq \ker(\varphi_\alpha) = \{f \in R |\ f(\alpha) = 0\}$. Este ideal es maximal porque $R/M(\alpha) \cong R$.

Teorema 1.5.8. *Sea $I \subseteq R$ un ideal (i-ideal, d-ideal) tal que $I \neq R$, siendo R un anillo con identidad. Entonces existe un ideal (i-ideal, d-ideal) $M \subseteq R$ maximal (i-maximal, d-maximal) que contiene a I.*

Demostración. Lo probaremos para i-ideales y usaremos el lema de Zorn. Considérese el siguiente conjunto, que está ordenadado por inclusión y que es no vacío por contener a I:

$$\tau := \{J \subseteq R \text{ i-ideal}|\ I \subseteq J \neq R\}$$

Sea $\{C_k\}_{k\in K}$ una cadena de τ. Considérese el siguiente candidado a cota superior:

$$C := \bigcup_{k\in K} C_k.$$

Es conocido que C es un i-ideal, y este contiene a I claramente. Supongamos por reducción al absurdo que $C = R$. Entonces $1 \in C$. Entonces $1 \in C_k$ para algún $k \in K$. Esto implica $C_k = R$, lo que no es posible. Así, $C \neq R$. Concluimos $C \in \tau$. Además, es cota superior. Por el lema de Zorn, existe un elemento maximal M de τ. Esto prueba el resultado. ■

Definición 1.5.4. El *radical de Jacobson* de R se define de la siguiente forma:

$$\mathrm{J}(R) := \bigcap M \in \mathrm{Max}_i(R) M.$$

Veamos un ejemplo: Si R es un anillo y M es un ideal maximal, entonces

$$S = R/M^n$$

Supongamos que P/M^n es un ideal primo de S. Entonces P es primo en R y $M^n \subseteq P$. Como P es primo, necesariamente $M \subseteq P$. Por la maximalidad de M, o $P = R$ o $P = M$. Por la primalidad de P, $P \neq R$. Concluimos así que $P = M$. Obtenemos el siguiente resultado:

$$\mathrm{Spec}\left(R/M^n\right) = \left\{M/M^n\right\}.$$

En particular,

$$\mathrm{J}(R/M^n) = M/M^n \neq 0.$$

Teorema 1.5.9. *Sea R un anillo. Son equivalentes:*

1. $y \in J(R)$.
2. *Para todo $x \in R$, $1 - xy$ tiene un inverso a izquierda en R.*
3. *Para todo $x, z \in R$, $1 - xyz$ es unidad en R.*

Demostración. Veamos que 1 implica 2. Al ser $J(R)$ i-ideal se tiene $xy \in J(R)$. Supongamos que

$$R(1 - xy)$$

es un i-ideal propio. Entonces existe M un i-ideal maximal de R tal que

$$R(1 - xy) \subseteq M.$$

Así, $1 - xy \in M$, por lo que
$$1 = (1 - xy) + xy \in M.$$
Esto implica que $M = R$, lo cual no es posible. Concluimos que $R(1-xy) = R$, luego $v(1-xy) = 1$ para algún v elemento de R. Es decir, $1 - xy$ es unidad.

Veamos que 2 implica 3. Sean $x, z \in R$. Por hipótesis,
$$1 - (zx)y$$
tiene inverso a izquierda. Sea $v \in R$ tal que
$$v(1 - zxy) = 1.$$
Entonces
$$v - vzxy = 1 \implies v = 1 + vzxy = 1 - (-vzx)y = 1 - \overline{x}y,$$
donde $\overline{x} = -vzx$. Por hipótesis, $1 - \overline{x}y$ tiene inverso a izquierda. Sea $w \in R$ tal que
$$w(1 - \overline{x}y) = 1 = wv.$$
Entonces
$$w = w \cdot 1 = w(v(1 - zxy)) = (wv)(1 - zxy) = 1 - zxy.$$
Como $v(1 - zxy) = 1$, tenemos que $vw = 1$. Así, w es unidad con inverso v. El ejercicio 3 de la hoja de problemas dice que si R es un anillo con identidad y a, b son dos elementos tales que $1 - ab$ tiene inverso a izquierda, entonces $1 - ba$ tiene inverso a izquierda. Aplicado a este caso con $a = z, b = xy$, se tiene que $1 - xyz$ tiene inverso a izquierda. Y aplicando el problema con la versión correspondiente a derecha, concluimos que $1 - xyz$ tiene inverso a derecha. Por tanto, $1 - xyz$ es unidad.

Veamos que 3 implica 1. Supongamos por reducción al absurdo que M es un i-ideal maximal de R tal que $y \neq M$. Entonces
$$Ry \nsubseteq M.$$
Al ser Ry un i-ideal, necesariamente $R = M + Ry$. Sean $m \in M$, $x \in R$ tales que
$$1 = m + xy.$$
Entonces
$$m = 1 - xy$$
es unidad por 3 con $z = 1$. Pero m no puede ser una unidad dado que M es maximal. Esta contradicción implica que $y \in M$. Como M era un i-ideal maximal arbitrario, concluimos $y \in J(R)$.

Podemos definir $J'(R)$ como la intersección de los d-ideales maximales de R, y obtener el teorema anterior con su versión a derecha. Entonces:

Teorema 1.5.10. *$J(R) = J'(R)$. Así, $J(R)$ es un ideal de R.*

Demostración. Un elemento y de R pertenece a $J(R)$ si y sólo si $1 - xyz$ es unidad para todo $x, z \in R$, si y sólo si $y \in J'(R)$.

Corolario 1.5.10.1. *Sea I un i-ideal de R tal que $1+I \subseteq \mathcal{U}(R)$. Entonces*

$$I \subseteq J(R).$$

Así, $J(R)$ es el mayor i-ideaal de R tal que $1+J(R) \subseteq \mathcal{U}(R)$.

Demostración. Sea $y \in I$. Para todo $x \in R$, $-xy \in I$ por ser I ideal. Por hipótesis,

$$1 - xy \in 1 + I \subseteq \mathcal{U}(R).$$

Por tanto, $1 - xy$ es invertible a izquierda. Por la condición 2 del Teorema 1.5.9, $y \in J(R)$.
Nota: Sea $(R, +, \cdot)$ un anillo. Definimos

$$a \circ b = a + b - ab.$$

Es una ley asociativa. Se satisface:

$$a \circ 0 = a + 0 - 0 \cdot a = a,$$

por lo que 0 es el elemento neutro. Así $(R, \circ)$ es un *monoide*. Un monoide es una estructura algebraica que cumple todas las condiciones de grupo salvo la de elemento inverso. Si R tiene identidad, la aplicación

$$\begin{array}{rccc} \phi : & (R, \circ) & \longrightarrow & (R, \cdot) \\ & a & \longmapsto & 1 - a. \end{array}$$

Es un morfismo de monoides:

$$(1-a)(1-b) = 1 - b - a + ab = 1 - (a + b - ab) = 1 - (a \circ b).$$

Esto motiva la siguiente definición:

Definición 1.5.5. Sea R un anillo con identidad. Un elemento $a \in R$ es *cuasirregular a izquierda* (resp. a derecha) si existe $b \in R$ tal que $b \circ a = 0$ (resp. $a \circ b = 0$). El elemento a es *cuasirregular* si es cuasirregular a izquierda y a derecha.

Se tiene que

$$J(R) = \{a \in R |\ a \text{ es cuasirregular}\}.$$

En efecto: si $x \in J(R)$, entonces $1 - x$ es unidad por la condición 2 del teorema 1.5.9 para $y = 1$. Sea v el elemento inverso de $1 - x$. Sea $w := 1 - v$. Entonces

$$(1-x)(1-w) = (1-x)v = 1 = 1 - (x \circ w),$$

por lo que $x \circ w = 0$. Asimismo, $w \circ x = 0$. Es decir, x es cuasirregular. Recíprocamente, si x es cuasirregular, entonces existe $b \in R$ tal que $a \circ b = 0$ y existe $c \in R$ tal que $c \circ a = 0$. Así,

$$c = c \circ 0 = c \circ (a \circ b) = (c \circ a) \circ b = 0 \circ b = b.$$

Además,

$$(1-x)(1-b) = 1 - x \circ b = 1 = 1 - b \circ x = (1-b)(1-x)$$

es decir, $1 - x$ es unidad. Por tanto, el i-ideal Rx satisface $1 + Rx \subseteq \mathcal{U}(R)$. Por el corolario anterior, $Rx \subseteq J(R)$. En particular, $x \in J(R)$.

Además, $J(R) = R$ si y sólo si $(R, \circ)$ es un grupo. En este caso, R es un *anillo radical*, y $(R, +, \circ)$ se llama *braza*.

Chapter 2

Módulos

En este capítulo, todos los anillos poseen identidad aunque no se mencione.

2.1 Definición, Ejempos, Submódulos

Definición 2.1.1. Sea R un anillo. Un *módulo a izquierda sobre* R, o simplemente R*-módulo*, es un grupo abeliano $(M,+)$ y una aplicación $\cdot : R \times M \longrightarrow M$ que cumple para todo $r_1, r_2 \in R$, $m_2, m_2 \in M$, lo siguiente:

M1. $r_1(m_1 + m_2) = r_1 m_1 + r_1 m_2$.

M2. $(r_1 + r_2)m_1 = r_1 m_1 + r_2 m_1$.

M3. $(r_1 r_2)m_1 = r_1(r_2 m_1)$.

M4. $1_R m = m$.

Denotamos por ${}_R M$ la clase de R-módulos a izquierda. Nótese que si $S \subseteq R$ es un subanillo tal que $1_S = 1_R$, entonces cualquier R-módulo es un S-módulo.

Sea M un R-módulo. Por la condición M1, si $r \in R$, la aplicación

$$\begin{array}{rccc} \varphi_r : & M & \longrightarrow & M \\ & m & \longmapsto & rm \end{array}$$

pertenece a $\mathrm{End}(M)$. Además, la aplicación

$$\begin{array}{rccc} \varphi : & R & \longrightarrow & \mathrm{End} M \\ & r & \longmapsto & \varphi_r \end{array}$$

es un homomorfismo de grupos abelianos:

$$\varphi(r_1 + r_2)(m) = \varphi_{r_1+r_2}(m) = (r_1 + r_2)(m) \overset{\text{M2.}}{=} r_1 m + r_2 m = \varphi(r_1)(m) + \varphi(r_2)(m).$$

Por tanto, $\varphi(r_1 + r_2) = \varphi(r_1) + \varphi(r_2)$. Además,

$$\varphi(r_1 r_2)(m) = \varphi_{r_1 r_2}(m) = (r_1 r_2)m \overset{\text{M3}}{=} r_1(r_2 m) = \varphi_{r_1}(\varphi_{r_2}(m)),$$

por lo que $\varphi(r_1 r_2) = \varphi_{r_1} \circ \varphi_{r_2}$. Concluimos que φ es un homomorfismo de anillos. Su núcleo es, por tanto, un ideal de R, que recibe el nombre de *anulador de* M, denotado por $\mathrm{An}_R(M)$.

$$\mathrm{An}_R(M) = \{r \in R| \ \forall m \in M,\, rm = 0\}.$$

Esto motiva la siguiente definición:

Definición 2.1.2. Seaa $X \subseteq M$. El *anulador de* X es el i-ideal de R

$$\mathrm{An}_R(X) = \{r \in R| \ \forall x \in X,\, rx = 0\}.$$

Definición 2.1.3. Se dice que un R-módulo es *fiel* si $\mathrm{An}_R(M) = 0$.

Proposición 2.1.1. *Sea* $M \in_R M$. *Entonces para todo* $r \in R$, $m \in M$,*:*

1. $0_R m = 0_M = r \cdot 0_M$.
2. $-r \cdot m = r \cdot (-m) = -(rm)$.

Demostración.

1. Se da la siguiente situación:

$$0_R m = (0_R + 0_R)m = 0_R m + 0_R m,$$

lo que implica que $0_R m = 0_M$.

2. Se da la siguiente situación:

$$\begin{aligned}(-r)m + rm = (-r + r)m = 0_R m = 0_M,\\ r(-m) + rm = r(-m + m) = r0_M = 0_M.\end{aligned}$$