Sobre la estructura algebraica de anillo. Característica de un anillo

01. Anillos
02. Subanillos
03. Característica
04. Ordenación.
05. Bibliografía

01.Anillos

Definición 01.1 (Concepto de anillo)
Se define el anillo como una estructura algebraica constituida por un conjunto y dos leyes de composición interna, que denominaremos ley aditiva y ley multiplicativa, cumpliendo las siguientes condiciones:

a) La ley aditiva confiere al conjunto estructura de grupo abeliano.
b) La ley multiplicativa confiere al conjunto estructura de semigrupo.
c) La ley multiplicativa es distributiva, a ambos lados, con respecto a la ley aditiva.

Notas:

- Representamos el anillo por (A, +, .), donde A es el conjunto, + es la ley aditiva, y . es la ley multiplicativa. El elemento neutro del grupo conmutativo lo representaremos por 0.
- Si la ley multiplicativa fuera también conmutativa, diremos que el anillo es conmutativo.
- Si la ley multiplicativa tuviera también elemento neutro, diremos que se trata de un anillo con elemento unidad. Tal elemento lo representaremos mediante 1.
- Un anillo nunca es vacío, pues contiene necesariamente al elemento 0, neutro de la ley aditiva, ley que, tal como se ha indicado, ha de conferir a A estructura de grupo abeliano.
- Si un anillo tiene como único elemento el 0, éste sería también su elemento unidad. Se conviene en excluir este caso cuando hacemos referencia a un anillo con elemento unidad.

Teorema 01.1:

1) Si (A,+,.) es un anillo se verifica que $x.0 = 0, \forall x \in A.$
2) Si un anillo no está reducido al elemento 0, entonces cumple que $1 \neq 0.$

Demostración:

1) $\forall y \in A, x.y = x.(y+0) = x.y + x.0 \rightarrow x.y = x.y + x.0 \rightarrow x.0 = 0, \forall x \in A$

2) Veamos que si se supone $1 = 0$ se llegará a una contradicción:
$1 = 0 \rightarrow \forall x \in A, x = x.1 = x.0 = 0 \rightarrow \forall x \in A, x = 0$ y el anillo se reduce al elemento 0, contradiciendo la hipótesis.

Definición 01.2 (Divisor de cero):
Sea un anillo (A,+,.).

Se llama *divisor de cero a la izquierda* a un elemento $a \in A - \{0\}$ que cumple que $\exists b \in A / a.b = 0$.
Se llama *divisor de cero a la derecha* a un elemento $a \in A - \{0\}$ que cumple que $\exists b \in A / b.a = 0$.
Un elemento $a \in A, a \neq 0$, se dice *divisor de cero* si es divisor de cero a la izquierda y también es divisor de cero a la derecha.

Definición 01.3 (Dominio de integridad):
Se llama anillo *cancelativo* a un anillo sin divisores de cero.
Se llama anillo *íntegro* a un anillo cancelativo y conmutativo.
Se llama *dominio íntegro* o *dominio de integridad* a un anillo con elemento unidad, conmutativo y sin divisores de cero, es decir, a un anillo cancelativo, conmutativo y con elemento unidad.

Definición 01.4 (Elemento nilpotente):
Un elemento $a \in A$ se dice *nilpotente* si existe algún número natural *n* tal que $a^n = \overbrace{a...a}^{--n--} = 0$
Es obvio que si $a \neq 0$ es nilpotente, entonces a es divisor de cero.
Asimismo, en un dominio de integridad, solo el cero es nilpotente.

Teorema 01.2:
En todo anillo cancelativo se verifica la ley de cancelación o simplificación para el producto.
Demostración:
$\forall x, y, z \in A / c.a = c.b \wedge c \neq 0 \rightarrow c.a - c.b = 0 \rightarrow c.(a-b) = 0 \rightarrow c \neq 0 \wedge$
$\wedge c.(b-a) = 0 \rightarrow b - a = 0 \rightarrow a = b$

02.Subanillos

Definición 02.1:
Se dice que una parte B de un anillo A es un subanillo de A si tiene estructura de anillo con respecto a las mismas leyes internas que confieren estructura de anillo a A.
Es decir, (A,+,.) anillo $\rightarrow$ $(B,+,.)$ anillo, por lo cual ha de cumplirse que:

1) (B,+) es subgrupo de (A,+).
2) B es parte estable de A para la ley multiplicativa.

Recíprocamente, si se verifican ambas condiciones, ello es suficiente para que B sea subanillo de A.

Notas:
En el conjunto de todos los subanillos de un anillo (A,+,.) se encuentran el mismo A y el conjunto $\{0\}$. Ambos se dicen subanillos *impropios.* Los restantes subanillos de A se dicen *propios.*
Un subanillo de un anillo con divisores de cero podría no tenerlos, es decir, ser cancelativo.
Asimismo pueden darse casos de anillos con elemento unidad con subanillos que no lo tienen, o bien que tienen un elemento unidad distinto.

Teorema 02.1:
La familia Γ de los subanillos de A es una familia de Moore.
Demostración:

Una familia de Moore de partes de un conjunto es un conjunto de partes del mismo que verifica las condiciones:

a) El conjunto es una de las partes de la familia.
b) La intersección de dos partes de la familia es también una parte de la familia.

En el caso de la familia de los subanillos de A, sabemos que es la intersección de la familia de Moore de los subgrupos conmutativos de A (con respecto a la ley aditiva), y la familia de Moore de las partes estables de A con respecto a la ley multiplicativa, por lo que también es, consecuentemente, familia de Moore.

Si Γ es familia de Moore, para toda parte M de A existe lo que podemos llamar *clausura de Moore de M,* $\overline{M}$ *,* que es el mínimo subanillo de Γ que contiene a M. Se dice que $\overline{M}$ es el subanillo engendrado por M.

Definición 02.2:

Si B es un subanillo de A, se dice también que A es superanillo de B. Un anillo A se dice que es extensión de un anillo B, si A contiene un subanillo B' isomorfo a B.

Definición 02.3:

Sea A un anillo y sea B un subanillo de A. Si $S \subseteq A$ es una parte cualquiera de A, diremos que el subanillo J de A es obtenido por adjunción de B y S si J es la intersección de todos los subanillos de A que contienen a B y a S, es decir, si J es la clausura de Moore de la unión $B \cup S$. Se puede representar mediante $J = B[S]$, o, con la notación de la clausura de Moore, $J = \overline{BUS}$.

O sea:

$$J = B[S] = \overline{B \cup S}$$

Teorema 02.2:

Se verifica que $B[S_1][S_2] = B[S_1 \cup S_2]$

Demostración:

$$B[S_1 \cup S_2] = \overline{B \cup (S_1 \cup S_2)} = \overline{(B \cup S_1) \cup S_2} = \overline{\overline{B \cup S_1} \cup S_2} = \overline{B[S_1] \cup S_2} = B[S_1][S_2]$$

Definición 02.4:

En un anillo A con elemento unidad 1, se dice que un elemento $u \in A$ es una unidad, o que es un elemento unitario, si es inversible, es decir, si existe otro elemento del anillo, v^{-1} tal que $u.v^{-1} = 1$.

Teorema 02.3:

El conjunto U de las unidades de un anillo es grupo con respecto a la ley multiplicativa del anillo.

Demostración:

Se trata de comprobar que $\forall u_1, u_2 \in U, u_1.u_2^{-1} \in U$:

$\forall u_1, u_2 \in U \rightarrow u_1^{-1}, u_2^{-1} \in U$.

Por tanto: $(u_1.u_2^{-1}).(u_2.u_1^{-1}) = (u_2.u_1^{-1}).(u_1.u_2^{-1}) = 1 \rightarrow (u_1.u_2^{-1}) \in U$

03.Característica

Definición 03.1:
Se llama *característica* de un anillo A al número natural positivo mínimo, *n*, tal que $n.x = 0, \forall x \in A$
Si no existe ningún número natural positivo tal que $n.x = 0, \forall x \in A$, se dice que el anillo A es de característica nula, pues siempre se verifica, por teorema 01.1, que $0.x = 0, \forall x \in A$.

Teorema 03.1:
Sea un anillo con característica $n > 0$ y sea x un elemento dado del anillo. Si v_x es el mínimo entero positivo tal que $v_x.x = 0$ se verifica que v_x divide a *n*.
Demostración:
Si no fuera así, se tendría que $n = q.v_x + \mathrm{r}$, con $0 \le \mathrm{r} \le \mathrm{v_x}$.
Como es $n.x = 0$ se tendrá: $n.x = q.v_x x + \mathrm{r.x} \to 0 = 0 + \mathrm{r.x} \to \mathrm{r.x} = 0$ contra la hipótesis de que es v_x el mínimo entero tal que $v_x.x = 0$. Luego *r=0*.

Teorema 03.2:
Sea A un anillo.
a) Si A es de característica nula, entonces los elementos no divisores de cero a izquierda y derecha generan grupos cíclicos aditivos infinitos.
b) Si A es de característica n no nula, entonces los elementos no divisores de cero a izquierda y derecha generan grupos cíclicos aditivos de orden *n*.

Demostración:
Sea $r \in A$ un elemento no divisor de cero a derecha (por ejemplo), lo que nos indica que si *a.r=0* entonces *a=0*.
Por otra parte, siempre se cumple que $\forall x \in A, (n.x).r = x.(n.r)$, ya que es $(n.x).r = (x + ... + x).r = x.r + ... + x.r = x.(r + ... + r) = x.(n.r)$.

a) Si A es de característica nula no existirá nunca un $n \in Z^+ / nx = 0, \forall x \in A$. Ahora bien, ¿para un r no divisor de cero a derecha determinado puede existir un $v_r \in Z^+$ tal que $v_r.r = 0$?. Si fuera así, se tendría de la relación anterior:
$\forall x \in A, (v_r.x).r = x.(v_r.r) = x.0 = 0 \to (v_r.x).r = 0 \wedge r \; no \; div \; cero \; a \; der \to$
$\to v_r x = 0$.
Es decir, sería $\forall x \in A, v_r.x = 0 \to$ A no es de característica nula.
Por tanto, nunca podrá existir un $v_r \in Z^+$ tal que $v_r.r = 0$. Lo mismo podemos razonar si consideramos un r que no sea divisor de cero a izquierda.
Entonces, el grupo aditivo (r) engendrado por un elemento r no divisor de cero a derecha y a izquierda es cíclico infinito, ya que nunca $v.r = 0, \forall v \in Z^+$

b) Si A no es de característica nula ($n \neq 0$)
Si para un r dado no divisor de cero a derecha existiera un $v_r \in Z^+$ tal que $v_r.r = 0$, entonces ha de ser $v_r = n$, pues si fuera $v_r < n$ se tendría que $\forall x \in A, (v_r.x).r = x.(v_r.r) = x.0 = 0 \to (v_r.x).r = 0 \wedge r \; no \; div \; cero \; derch \to$
$\to v_r.x = 0$, con lo que la característica no sería n, sino $v_r < n$, contra la hipótesis.

Luego $n.r = 0$, y (r) es un grupo aditivo cíclico de orden n.

Corolario 03.2.1:
Si A es anillo íntegro y no reducido al cero, entonces todos los grupos cíclicos aditivos (x) distintos del (0) tienen el mismo orden, infinito si A es de característica nula o igual a la característica si ésta es no nula.

Corolario 03.2.2:
En un anillo A con elemento unidad se verifica que si $v_1 \in Z^+$ es finito, entonces A es de característica $n = v_1 \neq 0$, en caso contrario ($v_1 = 0$), A es de característica nula.

Teorema 03.3:
La característica de un anillo íntegro es nula o bien es un número primo.
Demostración:
Como en A existe algún elemento distinto de cero, la característica n es distinta de 1: $n \neq 1$.
Supongamos que la característica n no es un número primo, sino que puede descomponerse en producto de al menos dos enteros y veamos que esto implicaría una contradicción:
$n = n_1.n_2 \rightarrow \forall x \in A,\, n_1.x \neq 0 \wedge n_2.x \neq 0 \rightarrow (n_1.x)(n_2.x) \neq 0 \rightarrow n_2.n_2x.x \neq 0 \rightarrow$
$\rightarrow n.x.x \neq 0 \wedge x.x \in A \rightarrow n$ no es característica de A.

Corolario 1:
Para *A* conmutativo con característica p no nula se cumple que, $\forall x_1, x_2 \in A$:
a) $(x_1 + x_2)^p = x_1^p + x_2^p$
b) $(x_1 - x_2)^p = x_1^p - x_2^p$
Demostración:
a)
$$(x_1 + x_2)^p = \sum_{k=1}^{p} \binom{p}{k} x_1{}^{p-k}.x_2{}^{k} = \binom{p}{0} x_1{}^{p} + \binom{p}{1} x_1{}^{p-1}.x_1 + \ldots + \binom{p}{p-1} x_1.x_2{}^{p-1} + \binom{p}{p} x_2{}^{p} =$$
$$= x_1^p + 0 + \ldots + 0 + x_2^p = x_1^p + x_2^p$$
b)Si sustituimos en la fórmula anterior x_1 por x_1-x_2:
$x_1^p = (x_1 - x_2)^p + x_2^p \rightarrow (x_1 - x_2)^p = x_1^p - x_2^p$

Corolario 2: (Pequeño Teorema de Fermat)
Si p es un número primo, entonces para cada número natural m se verifica que
$$m^p - m \equiv 0 \pmod{p}$$
Demostración:
Aplicando la fórmula del corolario anterior para m elementos del anillo:
$$(x_1 + \ldots + x_m)^p = x_1^p + \ldots + x_m^p$$
y para el elemento unidad del anillo, haciendo $x_1 = \ldots = x_m = 1$:
$$\left.\begin{array}{l} (x_1 + \ldots + x_m)^p = (1 + \ldots + 1)^p = m^p \\ x_1^p + \ldots x_m^p = 1 + \ldots + 1 = m \end{array}\right\} \rightarrow m^p \equiv m \pmod{p}$$

04.Ordenación

Definición 04.1:
Un anillo A se dice ordenado si existe una relación de orden compatible con la estructura de anillo. Es decir, si existe una clase positiva $P \subset A.$

Definición 04.2:
Se define la idea de valor absoluto en un anillo ordenado como una aplicación $\left|\ \right| : A \to P \bigcup \{0\}$, dada por la condición:

$$\forall x \in A, |x| = \max\{x, -x\}$$

05.Bibliografía:

Abellanas C., P.; "Elementos de Matemáticas". Ediciones Romo, Madrid, 1975.
Atiyah, Michael; "Introducción al álgebra conmutativa". Editorial Reverté, 1973.
Birkhoff, G.-McLane, S.; "Álgebra moderna". Vicens Vives, 1974.
Bourbaki, N.; "Elements of mathematics. Commutative algebra". Addison-Wesley, 1972.
Dubreil, P.-Jacotin, M.L.; "Lecciones de álgebra moderna". Reverté, 1975.
Godement, R.; "Algebra". Tecnos, 1978.
Kaplansky,I.; "Commutative rings" , Allyn & Bacon, 1970.
Lang, S.; "Algebra". Aguilar, 1977.
Lentin, A.-Rivaud, J.-Motilva, E.; "Algebra moderna". Aguilar, 1982
Queysanne, M.; "Algebra Básica". Vicens Vives, 1974.