Estructuras Algebraicas

Abel Doñate Muñoz

Contents

0 Notación y definiciones preeliminares **2**

0.1 Notación . . . 2

0.2 Definiciones estructuras . . . 2

1 Anillos **2**

1.1 Ideales . . . 2

1.2 Ideales primos y maximales . . . 3

1.3 Elementos primos e irreductibles . . . 4

1.4 Anillos de polinomios . . . 5

1.5 Cadena de contenciones anillos . . . 5

2 Cuerpos **5**

2.1 Implicaciones de cuerpos . . . 5

2.2 Cuerpos finitos . . . 5

3 Grupos **6**

3.1 Fundamentals . . . 6

3.2 Acciones de grupo . . . 6

3.3 Subgrupos de Sylow . . . 7

3.4 Grupos abelianos . . . 7

4 Apéndice con Anillos, cuerpos y grupos **7**

4.1 Anillos . . . 7

0 Notación y definiciones preeliminares

0.1 Notación

Convenimos la siguiente notación:

- **PC**. Propiedad conmutativa
- **PA**. Propiedad Asociativa
- **PD**$(*, +)$. Propiedad distributiva $*$ con respecto a $+$
- **EN**. Existe un elemento neutro y es único
- **PI**. Todo elemento tiene inverso

0.2 Definiciones estructuras

Definition (Semigrupo)**.** $(G, *)$ *con PA, EN*

Definition (Grupo)**.** $(G, *)$ *con PA, EN, PI*

Definition (Anillo)**.** *(A, +, *) con* $\begin{cases} (A,+) \text{ grupo abeliano} \\ (A,*) \text{ semigrupo} \\ PD(*,+) \end{cases}$

Definition (Cuerpo)**.** $(A, +, *)$ *donde todo elemento diferente de* 0 *es una unidad*

Definition (Módulo)**.** $(M, +)$ *es un módulo sobre el anillo* A *si:*

- $(M, +)$ *grupo abeliano*
- $A \times M \to M$
- $a * (m_1 + m_2) = a * m_1 + a * m_2$
- $(a + b) * m = a * m + b * m$
- $(a * b) * m = a * (b * m)$
- $1_A * m = m$

1 Anillos

Definition (Morfismo de anillos)**.** *Una aplicación* $f : A \to B$ *es un morfismo si preserva las operaciones:*

1. $f(1_A) = 1_B$
2. $f(x +_A y) = f(x) +_B f(B)$
3. $f(x *_A y) = f(x) *_B f(y)$

Definition (Tipos de morfismo)**.** *Los tipos de morfismo son*

- ***Monomorfismo o inmersión*** $\iff$ *inyectivo*
- ***Epimorfismo*** $\iff$ *exhaustivo*
- ***Isomorfismo*** $\iff$ *biyectivo*

1.1 Ideales

Definition (Característica)**.** *La característica de un anillo es el menor* $n \in \mathbb{N}$ *tal que* $n \cdot 1_A = 0$*. En caso de no cumplirse la característica es* 0

Definition (Ideal). *$I \subseteq A$ es un ideal si*

- $\forall a \in I \ \forall \lambda \in A \Rightarrow \lambda a \in I$
- $\forall a, b \in I \Rightarrow a + b \in I$

Proposition. *$J \subseteq B$ ideal $\Rightarrow f^{-1}(J)$ ideal*

Definition (Ideales generados). *Sean $I, J \subseteq A$ ideales. Son ideales*

- $I + J := \{a + b : a \in I, b \in J\}$
- $I \cap J$
- $IJ = \{\sum a_i b_j : a_i \in I, b_j \in J\}$

Definition (Ideal principal). *El ideal principal generado por a es*

$$I = (a) := \{ra : r \in A\}$$

Theorem (Propiedad universal del cociente). .

$$\begin{cases} f : A \to B \text{ morfismo de anillos.} \\ I \subseteq Kerf \text{ ideal.} \end{cases} \Rightarrow \exists! \text{ morfismo } \tilde{f} : A/I \to B \text{ tq} \qquad \begin{array}{ccc} A & \xrightarrow{f} & B \\ & \searrow^{\pi} & \uparrow \tilde{f} \\ & & A/I \end{array}$$

Theorem (Teorema de Isomorfismo). *$f : A \to B$ morfismo de anillos. Hay un isomorfismo canónico $\tilde{f}$*

$$\tilde{f} : A/\ker f \to Imf \qquad \text{tal que} \qquad A/\ker f \simeq Imf$$

1.2 Ideales primos y maximales

Definition (Ideal primo). *Sea $\mathfrak{p} \subseteq A$ un ideal.*

$$\mathfrak{p} \text{ es primo} \iff \forall a, b \in A \quad ab \in \mathfrak{p} \Rightarrow a \in \mathfrak{p} \ / \ b \in \mathfrak{p}$$

o una definición equivalente y más útil a veces

$$\mathfrak{p} \text{ es primo} \iff \forall a, b \in A \quad a \notin \mathfrak{p} \text{ y } b \notin \mathfrak{p} \Rightarrow ab \notin \mathfrak{p}$$

Definition (Anillo integro). *A es integro si no tiene divisores de cero (tiene ley de cancelación)*

Definition (Ideal maximal). *El ideal $\mathfrak{m} \subset A$ es maximal si no está contenido en ningún otro ideal propio de A.*

Definition (Anillo fracción). *Sean $F(A) = A \times (A - \{0\})$ y la clase de equivalencia $(a, s) \sim (b, t) \iff at - bs = 0$. Entonces*

1. *Si $\frac{a}{s} := (a, s)$, entonces $\frac{a}{s} + \frac{b}{t} := \frac{at+bs}{st}$ y $\frac{a}{s} * \frac{b}{t} := \frac{ab}{st}$*
2. *$Fr(A) = F/\sim$ es un cuerpo con las operaciones anteriores*

Theorem (Propiedad universal del anillo de fracciones). *Sea A anillo integro y $f : A \to B$ morfismo tal que $f(A - \{0\}) \subseteq B^*$. Entonces*

1. *Esiste un único morfismo $\varphi \circ \iota = f$* $\qquad \begin{array}{ccc} A & \xrightarrow{f} & B \\ & \searrow^{\iota} & \uparrow \varphi \\ & & Fr(A) \end{array}$
2. *Si $A \overset{\iota'}{\hookrightarrow} F$ con F cuerpo que satisface (1), ha de ser $F \simeq Fr(A)$*

Algunas implicaciones sobre anillos e ideales son:

- A integro $\iff$ el ideal (0) es primo
- $\mathfrak{p}$ primo $\iff$ $A/\mathfrak{p}$ integro
- $\mathfrak{m}$ maximal $\iff$ $A/\mathfrak{m}$ cuerpo $\Rightarrow$ $\mathfrak{m}$ primo

1.3 Elementos primos e irreductibles

Definition (Irreductible). *$a \in A$ es irreductible si*

1. $a \notin A^*$
2. $a = bc \Rightarrow b \in A^*$ / $c \in A^*$

Definition (Primo). *$a \in A$ es primo si $a|bc \Rightarrow a|b$ / $a|c$*

Definition (Anillo factorial (UFD)). *A integro donde cada elemento admite una única descomposición en irreductibles (up to unidades).*

$$a = p_1^{e_1} \cdots p_r^{e_r} \qquad p_i = u_i q_i \quad u_i \in A^*$$

Definition (Anillo principal (PID)). *A integro en el que todo ideal es principal.*

Definition (Anillo euclideo). *A es euclideo si existe una función $\delta : A - \{0\} \to \mathbb{N}$ tal que*

1. $\delta(ab) \geq \delta(a)$
2. $\forall a, b \ \exists q, r : a = bq + r \quad y \quad r = 0$ / $\delta(r) < \delta(b)$

Estos tres tipos de anillos se relacionan por $\boxed{A \text{ Euclideo} \Rightarrow A \text{ PID} \Rightarrow A \text{ UFD}}$

Definition (Máximo común divisor). *$m \in A$ es un mcd si*

1. $m|a, \quad m|b$
2. $d|a, \quad d|b \Rightarrow d|m$

Definition (Mínimo común múltiplo). *$M \in A$ es un MCM si*

1. $a|M, \quad b|M$
2. $a|c, \quad b|c \Rightarrow M|c$

El mcd y el MCM no tienen por que ser únicos.

Theorem (Enteros de Gauss). *$\mathbb{Z}[i]$ es el anillo PID de los enteros de Gauss. Definimos la norma $N(a + bi) = a^2 + b^2$*

1. *Las unidades son $1, -1, i, -i$*
2. *$z = a + bi$ es primo $\iff$ $z = p(\cdot u) \equiv 3 \mod 4$ o $N(z) = p$*

Definition (Anillo MCD (GCDD)). *A integro en el que todos dos elementos tienen mcd*

Proposition ($\mathbb{Z}(\sqrt{-5})$ no es UFD). $6 = 2 \cdot 3 = (1 + \sqrt{-5}) \cdot (1 - \sqrt{-5})$

Algunas propiedades de los anillos:

- A PID: a irreductible $\iff$ a primo
- A UFD: a irreductible $\iff$ a primo
- A integro: a primo $\Rightarrow$ a irreductible
- A integro: a irreductible $\iff$ (a) maximal
- A euclideo: $\exists! mcd(a, b)$ (up to unidades)
- A UFD $\Rightarrow$ $A[X]$ UFD
- $A[X]$ PID, A integro $\Rightarrow$ A cuerpo
- K cuerpo $\Rightarrow$ $K[X]$ Euclideo

1.4 Anillos de polinomios

Durante toda la sección A es UFD y $K = Fr(A)$ el cuerpo de fracciones.

Theorem. *Si K es un cuerpo $\Rightarrow K[X]$ es Euclideo*

Definition (Contenido)**.** *El contenido de un polinomio $f \in A[X]$ es el mcd de sus coeficientes*

$$f = a_0 + a_1 x + \cdots + a_n x^n \qquad \Rightarrow \qquad c(f) = mcd(a_0, a_1, \dots a_n)$$

Llamamos primitivo a $f \iff c(f) = 1$

Theorem (Lema de Gauss)**.** *f, g primitivos $\Rightarrow fg$ primitivo ($\Rightarrow c(fg) = c(f)c(g)$)*

Theorem (Criterio de Eisenstein)**.** *A UFD, $p \in A$ primo. $f = \sum a_i x^i \in A[X]$. Si se cumple*

$$p|a_0, \quad p|a_1, \quad \dots \quad p|a_{n-1}, \quad p \not| a_n, \quad p^2 \not| a_0 \qquad \Rightarrow \qquad f \text{ irreducible en } K[X]$$

Theorem (Criterio de reducción)**.** *A, B anillos, B íntegro. $\varphi : A \to B$, $\tilde{\varphi} : A[X] \to B[X]$*

$$\begin{cases} deg(\tilde{\varphi}(f) = deg(f) \\ \tilde{\varphi}(f) \text{ irreductible en } Fr(B) \end{cases} \Rightarrow f \text{ no se puede descomponer como } f = gh$$

1.5 Cadena de contenciones anillos

Cuerpos $\subseteq$ Anillo Euclideo $\subseteq$ PID $\subseteq$ UFD $\subseteq$ GCDD $\subseteq$ Anillo Integro $\subseteq$ Anillo

2 Cuerpos

Definition (Extensión de cuerpo)**.** *Una extensión de cuerpo $F = K(\alpha)$ es el mínimo cuerpo F tal que $K \subseteq F$ y $\alpha \in F$*

Definition (Dimensión de la extensión)**.** *Sea F/K una extensión de cuerpo.*

Llamamos $[F : K] = \dim_K(F)$ a la dimensión del espacio vectorial de F con coeficientes en K.

2.1 Implicaciones de cuerpos

- α algebraico sobre $K \iff K(\alpha) = K[\alpha] \iff K(\alpha)/K$ extensión finita
- α, β algebraicos sobre $K \Rightarrow \alpha \pm \beta,\ \alpha\beta,\ \alpha/\beta$ algebraicos sobre K

(FALTA TODAS LAS RELACIONES CON EL POLINOMIO IRREDUCIBLE)

2.2 Cuerpos finitos

Definition (Cuerpo cerrado algebraicamente)**.** *El cuerpo K es cerrado algebraicamente si cualquier polinomio $f(x) \in K[X]$ tiene al menos una raíz $\alpha \in K$.*

Esto es equivalente a decir que cualquier polinomio en $K[X]$ descompone en factores lineales en $K[X]$.

Definition (Clausura algebraica)**.** *Llamamos $K \subseteq \overline{K}$ al menor cuerpo algebraicamente cerrado tal que todo elemento de $\overline{K}$ es algebraico sobre K.*

Theorem (Wedderbrun)**.** *Todo cuerpo finito es conmutativo*

Definition (Unicidad de los cuerpos finitos). *Fijado p primo y n natural hay un único cuerpo finito $\mathbb{F}_{p^n}$ de tamaño p^n*

$\mathbb{F}_{p^n}$ es el conjunto de soluciones de $x^{p^n} - x = 0$ en la clausura algebraica de $\mathbb{F}_p$

Definition (Construcción de un cuerpo finito). *Dado p^n elegimos un polinomio $P \in \mathbb{Z}/p\mathbb{Z}$ tal que $Irred(P) = n$. Tenemos entonces $\mathbb{F}_{p^n} \simeq (\mathbb{Z}/p\mathbb{Z})[X]/(P)$*

Theorem (Pequeño teorema de Fermat). *$x^p - x \in (\mathbb{Z}/p\mathbb{Z})[X]$ descompone en factores lineales en $\mathbb{Z}/p\mathbb{Z}$*

$$x^p - x = x(x-1)(x-2)\cdots(x-(p-1))$$

Una generalización es que $x^{p^n} - x = \prod_{a \in \mathbb{F}_{p^n}} (x - a)$

Proposition. $\mathbb{F}_{p^m} \subseteq \mathbb{F}_{p^n} \iff m|n$

Theorem ($\mathbb{F}_{p^n}^*$ es cíclico). $\exists \zeta \in \mathbb{F}_{p^n} : \mathbb{F}_{p^n}^* = \langle \zeta \rangle = \{1, \zeta, \ldots, \zeta^{p^n-2}\}$

3 Grupos

3.1 Fundamentals

Theorem (Cayley). *Todo grupo finito es isomorfo a un subgrupo de un grupo simétrico*

Theorem (Wilson). *p primo* $\iff (p-1)! \equiv -1 \ (mod\ p)$

Definition (Clase lateral). $G/H = \{aH : a \in G\}$

Theorem (Lagrange). $[G : H] = \frac{|G|}{|H|}$

Definition (Subgrupo normal). $H \triangleleft G \iff ghg^{-1} \in H \ \forall g \in G \ \forall h \in H$

Definition (Grupo cociente). *Si $H \triangleleft G \Rightarrow G/H$ grupo cociente*

Theorem (Primer teorema de isomorfismo). *Sea $f : G \to H$ morfismo. Entonces $G/Ker(f) \simeq Im(f)$*

Theorem (Segundo teorema de isomorfismo). *Sean $K \subseteq G, H \triangleleft G$. Entonces $K/(K \cap H) \simeq HK/H$*

Theorem (Tercer teorema de isomorfismo). *Sean $H \triangleleft K \triangleleft G$. Se cumple*

1. *$K/H \triangleleft G/H$*
2. *$G/K \simeq (G/H)/(K/H)$*

Definition (Producto directo). *G es producto directo de sus subgrupos H, K si*

$$H \times K \to G, \qquad (h,k) \mapsto hk \quad \text{es isomorfismo}$$

Entonces $H, K \triangleleft G$, $HK = G$ y $H \cap K = \{e\}$

3.2 Acciones de grupo

Definition (Acción de grupo). *Sea G grupo y S un conjunto definimos la acción de G sobre S como*

$$G \times S \to S \qquad \begin{cases} 1) \ \forall s \in S & e_G s = s \\ 2) \ \forall g, h \in G & g(hs) = (gh)s \end{cases}$$

Definition (Órbita). *La órbita de $s \in S$ es $GS = \{gs : g \in G\}$*

Definition (Estabilizador). *Estabilizador de $s \in S$ es el subgrupo $G_s = \{g \in G : gs = s\}$*

Definition (Acción por conjugación). *Tomamos $S = G$ y el morfismo*

$$G \times G \to G, \qquad g, s \mapsto gsg^{-1}$$

Definition (Centralizador). *Elementos que conmutan con s. $Z(s) = \{g : gs = sg\}$. Es el estabilizador de la acción por conjugación.*

Definition (Centro). $Z(G) = \{g \in G : \ \forall h \in G \ gh = hg\} \triangleleft G$

Definition (Clase de conjugación). $C_x = \{gxg^{-1} : g \in G\}$

Proposition. *Hay una biyección $Gs \leftrightarrow G/G_s$ tal que $gs \leftrightarrow gG_s$*

Theorem (Fórmula de las clases). *G actua sobre S, $|S| < \infty$*

$$|S| = \sum [G : G_{s_i}] \xRightarrow[G=Z(G)\cup C_{x_1}\cup\cdots\cup C_{x_t}]{Conjugación} |G| = |Z(G)| + \sum [G : Z(x_i)]$$

Proposition. $|G| = p^n \Rightarrow Z(G) \neq \{e\}$

Proposition. *Si $|G| = p^2$ es abeliano*

Theorem (Cauchy). *Si $p||G| \Rightarrow \ \exists H \subseteq G : |H| = p$*

3.3 Subgrupos de Sylow

Definition ($p-$grupo). *Subgrupo de orden p^k*

Definition ($p-$Sylow). *$p-$grupo maximal (no contenido en otro $p-$subgrupo)*

Proposition. *$H \subseteq G$ $p-$ Sylow $\Rightarrow \ \forall g \in G gHg^{-1}$ también lo es.*

Theorem (Sylow). *Sea $|G| = p^n M$ con p primo, $p \not| M$*

1. *G tiene un $p-$Sylow de orden p^n*
2. *Todos los $p-$Sylows de G son conjugados*
3. *El número n_p de subgrupos de Sylow satisface $n_p \cong 1 \ (mod \ p), \quad n_p|M$*
4. *Todo $p-$subgrupo está contenido en un $p-$ Sylow*

Theorem. *Si tots els subgrups de Sylow de G son normals, llavors G es producte directe dels Sylows.*

3.4 Grupos abelianos

Theorem (Clasificación de grupos abelianos finitamente generados). .

Sea $G = \langle x_1, \ldots, x_n : M \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix} \rangle$ Por la forma normal de Smith sabemos que existen P, Q, D tal que $M = PDQ$ con coeficientes en el anillo.

$$D = diag(\alpha_i), \qquad \alpha_i = \frac{d_i(1)}{d_{i-1}(A)}, \qquad d_i(A) = gcd(menores \ de \ orden \ i)$$

4 Apéndice con Anillos, cuerpos y grupos

4.1 Anillos

Euclideos	$\mathbb{Z}, \quad \mathbb{Z}_p, \quad \mathbb{Z}[e^{i2\pi/3}](N(a+b\omega) = a^2+b^2-ab), \quad K[X]$
DIP pero no Euclideos	$\mathbb{Z}[\frac{1+\sqrt{-19}}{2}]$
UFD pero no DIP	$K[X,Y]$
Integro pero no UFD	$\mathbb{Z}[\sqrt{-5}]$