Anillos finitos locales

XXVII Escuela Venezolana de Matemáticas – EMALCA

Edgar Martínez-Moro

Sept. 2014

imUVa Instituto de Investigación en Matemáticas

Universidad de Valladolid

Estructura de los anillos finitos

Un anillo conmutativo A es local si tiene un único ideal maximal que denotaremos por $\mathfrak{m}$.

Las siguientes propiedades son equivalentes a la definición que acabamos de enunciar (siempre que $1 \neq 0$)

1. Si la suma de cualquier par elementos en A que no sean unidades no es tampoco una unidad.
2. Si $a \in A$, entonces a o bien $1 - a$ es una unidad.
3. Si una suma finita es una unidad, entonces también lo será alguno de sus sumandos.

Estructura de los anillos finitos

Un anillo conmutativo A es local si tiene un único ideal maximal que denotaremos por $\mathfrak{m}$.

Las siguientes propiedades son equivalentes a la definición que acabamos de enunciar (siempre que $1 \neq 0$)

1. Si la suma de cualquier par elementos en A que no sean unidades no es tampoco una unidad.
2. Si $a \in A$, entonces a o bien $1 - a$ es una unidad.
3. Si una suma finita es una unidad, entonces también lo será alguno de sus sumandos.

Ejemplo: Si $\mathbb{F}$ es un cuerpo y n es un entero positivo entonces el anillo cociente

$$A = \mathbb{F}[x]/\langle x^n \rangle$$

es local y su ideal maximal $\mathfrak{m}$ son aquellas clases representadas por polinomios con término constante nulo. Simplemente comprobando su definición se tiene que A no es un anillo de Galois.

El teorema chino de los restos es una técnica recurrente dentro del álgebra. Consideremos A un anillo y $\mathfrak{a}_1, \ldots, \mathfrak{a}_n$ ideales de A. Diremos que los ideales $\mathfrak{a}_i$ y $\mathfrak{a}_j$ con $i \neq j$ son coprimos si se cumple que $\mathfrak{a}_i + \mathfrak{a}_j = A$. Dado el siguiente homomorfismo de anillos

$$\phi : A \to A/\mathfrak{a}_1 \oplus \cdots \oplus A/\mathfrak{a}_n$$

donde $\phi(a) = (a + \mathfrak{a}_1, \ldots, a + \mathfrak{a}_n)$.

Las siguientes propiedades se pueden verificar fácilmente:

1. Si para cada par $i \neq j$ se tiene que $\mathfrak{a}_i$, $\mathfrak{a}_j$ son ideales coprimos entonces
$$\mathfrak{a}_1 \cap \cdots \cap \mathfrak{a}_n = \mathfrak{a}_1 \cdot \mathfrak{a}_2 \cdot \cdots \cdot \mathfrak{a}_n.$$
2. Si $\mathfrak{a}_i$, $\mathfrak{a}_j$ son ideales coprimos entonces también lo son sus potencias $\mathfrak{a}_i^m$, $\mathfrak{a}_j^m$ para $m = 1, 2, \ldots$.
3. El homomorfismo de anillos ϕ es inyectivo si y sólo si $\mathfrak{a}_1 \cap \cdots \cap \mathfrak{a}_n = \{0\}$.
4. El homomorfismo de anillos ϕ es sobreyectivo si y sólo si $\mathfrak{a}_i$, $\mathfrak{a}_j$ son coprimos si $i \neq j$.

Un elemento $e \in A$ de un anillo A diremos que es un idempotente si $e^2 = e$. Diremos que dos idempotentes e_1 y e_2 son ortogonales si $e_1 \cdot e_2 = 0$ y que e es un idempotente central si $e \cdot a = a \cdot e$ para todo elemento a del anillo A.

– Lema –

Un dominio de integridad finito es un cuerpo.

Un elemento $e \in A$ de un anillo A diremos que es un idempotente si $e^2 = e$. Diremos que dos idempotentes e_1 y e_2 son ortogonales si $e_1 \cdot e_2 = 0$ y que e es un idempotente central si $e \cdot a = a \cdot e$ para todo elemento a del anillo A.

– Lema –

Un dominio de integridad finito es un cuerpo.

– Proposición –

Si A es un anillo, las siguientes proposiciones son equivalentes:

1. A se puede expresar como una suma directa de anillos A_i con $i = 1, 2, \ldots, n$.
2. Existen idempotentes e_i con $i = 1, 2, \ldots, n$ centrales en el anillo A tales que

$$1 = \sum_{i=1}^{n} e_i \quad \text{and} \quad A_i \simeq e_i A. \tag{1}$$

3. A es suma directa de ideales $\mathfrak{a}_i \simeq A_i$ para $i = 1, 2, \ldots, n$.

– Teorema (Estructura) –

Sea A un anillo conmutativo finito. A descompone de manera única (salvo reordenamiento de los sumandos) como una suma directa de anillos locales.

– Proposición –

Sea $A = A_1 \oplus A_2 \oplus \cdots \oplus A_n$ la descomposición en anillos locales de un anillo finito conmutativo, entonces

1. $U(A) = U(A_1) \times U(A_2) \times \cdots \times U(A_n)$ y
2. el anillo de polinomios $A[x]$ factoriza

$$A[x] = \bigoplus_{i=1}^{n} A_i[x].$$

El anillo de polinomios $A[x]$

Durante esta sección el anillo A será siempre un anillo conmutativo finito local con ideal maximal $\mathfrak{m}$ y cuerpo de residuos $\mathbb{K} = A/\mathfrak{m}$. Denotaremos por μ la proyección natural

$$\mu : A[x] \to \mathbb{K}[x]$$

de donde el morfismo natural de A en $\mathbb{K}$ es simplemente la restricción de μ a los polinomios constantes.

– Teorema –

Sean A y B dos anillos tales que $A \subset B$. Entonces si $b \in B$ existe un polinomio mónico $f \in A[x]$ tal que $f(b) = 0$.

El anillo de polinomios $A[x]$

Durante esta sección el anillo A será siempre un anillo conmutativo finito local con ideal maximal $\mathfrak{m}$ y cuerpo de residuos $\mathbb{K} = A/\mathfrak{m}$. Denotaremos por μ la proyección natural

$$\mu : A[x] \to \mathbb{K}[x]$$

de donde el morfismo natural de A en $\mathbb{K}$ es simplemente la restricción de μ a los polinomios constantes.

– Teorema –

Sean A y B dos anillos tales que $A \subset B$. Entonces si $b \in B$ existe un polinomio mónico $f \in A[x]$ tal que $f(b) = 0$.

Sean $f, g \in A[x]$ dos polinomios sobre el anillo A.

1. Diremos que f es nilpotente si existe un entero n con $f^n = 0$.
2. f es una unidad si existe $g \in A[x]$ tal que $fg = 1$.
3. f es regular si f no es un divisor de 0.
4. f es primo si el ideal $\langle f \rangle$ es un ideal primo propio.
5. f es ireducible si no es una unidad y si $f = gh$ implica que, bien g es una unidad o bien h lo es.
6. f es primario si el ideal $\langle f \rangle$ es un ideal primario.
7. f y g están asociados si $\langle f \rangle = \langle g \rangle$.
8. f y g son coprimos si $\langle f \rangle + \langle g \rangle = A[x]$.

– Teorema –

Consideremos el polinomio $f(x) = a_0 + a_1 x + \cdots + a_n x^n \in A[x]$.

1. Los siguientes enunciados son equivalentes:
   - 1.1 f es una unidad,
   - 1.2 $\mu(f)$ es una unidad,
   - 1.3 a_0 es una unidad y $a_1, \ldots, a_n$ son nilpotentes.
2. Los siguientes enunciados son equivalentes:
   - 2.1 f es un polinomio nilpotente,
   - 2.2 $\mu(f) = 0$,
   - 2.3 $a_1, \ldots, a_n$ son nilpotentes,
   - 2.4 f es un divisor de 0,
   - 2.5 existe un elemento no nulo $a \in A$ con $af = 0$.

– Teorema (cont) –

3. Los siguientes enunciados son equivalentes:
   - 3.1 f es un polinomio regular,
   - 3.2 $\langle a_1, \ldots, a_n \rangle = A$,
   - 3.3 existe un índice i, $0 \leq i \leq n$ tal que a_i es una unidad,
   - 3.4 $\mu(f) \neq 0$.

Sea $\mathfrak{a}$ un ideal del anillo A, denotaremos por $\mathfrak{a}[x]$ al conjunto de polinomios de $A[x]$ dados por

$$\mathfrak{a}[x] = \{f(x) = a_0 + a_1x + \cdots + a_nx^n \in A[x] \mid a_i \in \mathfrak{a},\ i = 1, \ldots, n\}.$$

– Teorema –

Sea $\mathfrak{m}$ el ideal maximal del anillo A. Entonces se tiene que

1. Nilradical de $A[x]$.

$$\mathfrak{m}[x] = \bigcap\{\mathfrak{p} \mid \mathfrak{p} \text{ es un ideal primo de } A[x]\}.$$

2. Radical de Jacobson de $A[x]$.

$$\mathfrak{m}[x] = \{f \mid gf + 1 \text{ es una unidad para todo } g \in A[x]\}.$$

Sea $\mathfrak{a}$ un ideal del anillo A, denotaremos por $\mathfrak{a}[x]$ al conjunto de polinomios de $A[x]$ dados por

$$\mathfrak{a}[x] = \{f(x) = a_0 + a_1x + \cdots + a_nx^n \in A[x] \mid a_i \in \mathfrak{a},\ i = 1, \ldots, n\}.$$

– Teorema –

Sea $\mathfrak{m}$ el ideal maximal del anillo A. Entonces se tiene que

1. Nilradical de $A[x]$.

$$\mathfrak{m}[x] = \bigcap\{\mathfrak{p} \mid \mathfrak{p} \text{ es un ideal primo de } A[x]\}.$$

2. Radical de Jacobson de $A[x]$.

$$\mathfrak{m}[x] = \{f \mid gf + 1 \text{ es una unidad para todo } g \in A[x]\}.$$

Llamaremos a $\mathfrak{m}[x]$ el radical de $A[x]$ y lo denotaremos por $\mathrm{Rad}(A[x])$.

Sean f, g dos polinomios en el anillo $A[x]$. Diremos que f es un divisor de g si $\langle g \rangle \subset \langle f \rangle$. Diremos que es un divisor propio si la contención es extricta.

Llamaremos a $\mathfrak{m}[x]$ el radical de $A[x]$ y lo denotaremos por $\mathrm{Rad}(A[x])$.

Sean f, g dos polinomios en el anillo $A[x]$. Diremos que f es un divisor de g si $\langle g \rangle \subset \langle f \rangle$. Diremos que es un divisor propio si la contención es extricta.

– Teorema (Lema de Hensel) –

Sea $f \in A[x]$ un polinomio y

$$\mu(f) = \prod_{i=1}^{n} \bar{g}_i$$

donde los polinomios $\bar{g}_i$ con $i = 1, 2, \ldots, n$ son coprimos dos a dos en $\mathbb{K}[x]$. Entonces existen $g_i \in A[x]$, $i = 1, 2, \ldots, n$ tales que:

1. g_i, $i = 1, 2, \ldots, n$ son coprimos dos a dos,
2. $\mu(g_i) = \bar{g}_i$ para $i = 1, 2, \ldots, n$ y
3. $f = \prod_{i=1}^{n} g_i$.

– Lema –

Si f es un polinomio regular en el anillo $A[x]$ existen polinomios mónicos $f_i \in A[x]$, $i = 1, 2, \ldots$ tales que

$$\operatorname{gr}(f_i) = \operatorname{gr}(\mu(f)), \quad f_i \equiv f_{i+1} \mod \mathfrak{m}^j$$

y existen $g_i \in \mathfrak{m}[x]$ y una unidad $b_i \in A$ tales que

$$b_i f \equiv f_i + g_i f_i \mod \mathfrak{m}^j$$

– Teorema –

Si f es un polinomio regular de $A[x]$ entonces existe un unico polinomio mónico $f^\star$ tal que $\mu(f) = \mu(f^\star)$ y tal que si $a \in A$ entonces $f(a) = 0$ si y sólo si $f^\star(a) = 0$. Además existe una unidad $v \in A$ tal que $vf = f^\star$.

– Teorema (Polinomios regulares irreducibles) –

Sea $f \in A[x]$ un polinomio regular. Entonces

1. Si $\mu(f)$ es irreducible en $\mathbb{K}[x]$ entonces f también lo es.
2. Si f es un polinomio irreducible entonces $\mu(f) = \delta g^n$ con $\delta \in \mathbb{K}$ y g un polinomio mónico irreducible de $\mathbb{K}[x]$.
3. Si f pertenece al conjunto J entonces f es irreducible si y sólo si lo es $\mu(f)$.

– Lema –

Consideremos f un polinomio en $A[x]$ regular irreducible que esté contenido en el conjunto J. Entonces f es primo si y sólo si $\mathfrak{m} \subseteq \langle f \rangle$ donde $\mathfrak{m}$ es el ideal maximal del anillo A.

– Teorema (Caracterización de los cuerpos finitos) –

Sea A un anillo conmutativo finito y local. Los siguientes enunciados son equivalentes:

1. A es un cuerpo finito.
2. Cada polinomio de $A[x]$ irreducible y regular es también primo.
3. Existe al menos un polinomio irreducible y regular en el conjunto J que es primo.

Factorización en $A[x]$

A denota un anillo conmutativo finito y local con ideal maximal $\mathfrak{m}$. En general, para un anillo local A, el anillo de polinomios $A[x]$ no es un anillo de factorización única, por ejemplo en $\mathbb{Z}_{p^2}[x]$ tenemos que $x^2 = x \cdot x = (x - p) \cdot (x + p)$.

– Teorema (Factorización) –

Consideremos un polinomio regular en el anillo $A[x]$.

1. $f = \delta \prod_{i=1}^{n} g_i$, donde δ es una unidad y g_i con $i = 1, 2, \ldots, n$ son polinomios regulares primarios coprimos entre sí.
2. Si $f = \delta \prod_{i=1}^{n} g_i = \delta' \prod_{j=1}^{n'} h_j$, donde δ, δ' son unidades y g_i con $i = 1, 2, \ldots, n$, h_j con $j = 1, 2, \ldots, n'$, son polinomios regulares primarios coprimos entre sí dentro de cada serie. Entonces $n = n'$ y tras un posible reordenamiento $\langle g_i \rangle = \langle h_i \rangle$ para $i = 1, 2, \ldots, n$.

Diremos que un polinomio irreducible $\pi \in A[x]$ es básico irreducible si $\mu(\pi)$ es irreducible en $\mathbb{K}[x]$.

– Proposición –

Un polinomio $f \in A[x]$ es primario, regular no unidad si y sólo si es de la forma

$$f = \delta\pi^n + \beta$$

donde δ es una unidad, π es un polinomio básico irreducible, n es un entero positivo y β pertenece al ideal $\mathfrak{m}[x]$.

Diremos que un polinomio irreducible $\pi \in A[x]$ es básico irreducible si $\mu(\pi)$ es irreducible en $\mathbb{K}[x]$.

– Proposición –

Un polinomio $f \in A[x]$ es primario, regular no unidad si y sólo si es de la forma

$$f = \delta\pi^n + \beta$$

donde δ es una unidad, π es un polinomio básico irreducible, n es un entero positivo y β pertenece al ideal $\mathfrak{m}[x]$.

Estructura de los anillos locales

– Teorema (Estructura anillos locales) –

Sea A un anillo conmutativo local con característica p^n, ideal maximal $\mathfrak{m}$ y cuerpo de residuos $\mathbb{K} = A/\mathfrak{m}$. Sea $r = [\mathbb{K} : \mathbb{F}_p]$ y $\{m_1, m_2, \ldots, m_t\} \subset \mathfrak{m}$ un sistema de generadores minimal de $\mathfrak{m}$. Entonces existe un subanillo C de A tal que

1. $C \simeq GR(p^{nr}, p^n)$ es único y es la mayor extensión de Galois de $\mathbb{Z}_{p^n}$ en A.
2. A es una imagen mediante un homomorfismo de anillos del anillo de polinomios $C[x_1, x_2, \ldots, x_t]$.

El anillo de Galois C se denomina anillo de coeficientes de A.

Por lo tanto un anillo local A es de la forma

$$C[x_1, x_2, \ldots, x_t]/\mathfrak{q}$$

donde C es un anillo de Galois y $\mathfrak{q}$ es un ideal primario con $\mathfrak{q} \cap C = \{0\}$. Además el radical de $\mathfrak{q}$ es $\langle p, x_1, x_2, \ldots, x_t \rangle$ y finalmente como C es una imagen mediante un homomorfismo de $\mathbb{Z}_{p^n}$ podemos concluir que cualquier anillo local es una imagen, mediante un homomorfismo de anillos de $\mathbb{Z}_{p^n}[x_1, x_2, \ldots, x_t, x_{t+1}]$.

– Teorema –

Sea A un anillo local conmutativo con característica p^n. Si el conjunto $\{a_1, a_2, \ldots, a_s\}$ son generadores del grupo de unidades de A entonces el anillo A es una imagen mediante un homomorfismo de anillos del anillo de polinomios $\mathbb{Z}_{p^n}[x_1, x_2, \ldots, x_s]$.

Anillos de cadena

Un anillo de cadena es un un anillo local conmutativo con todos su ideales propios principales.

Sea A anillo principal local con característica p^n ideal maximal $\mathfrak{m}$ y cuerpo de residuos $\mathbb{K} = A/\mathfrak{m}$ y anillo de coeficientes el anillo de Galois $C = GR(p^{rn}, p^n)$.

Si tomamos un elemento $\theta \in \mathfrak{m} \setminus \mathfrak{m}^2$ entonces $\langle \theta \rangle = \mathfrak{m}$ y cada ideal de A es de la forma $\langle \theta^i \rangle$ para $i = 1, 2, \ldots, \beta - 1$ donde β es el índice de nilpotencia de $\mathfrak{m}$.

Anillos de cadena

Un anillo de cadena es un un anillo local conmutativo con todos su ideales propios principales.

Sea A anillo principal local con característica p^n ideal maximal $\mathfrak{m}$ y cuerpo de residuos $\mathbb{K} = A/\mathfrak{m}$ y anillo de coeficientes el anillo de Galois $C = GR(p^{rn}, p^n)$.

Si tomamos un elemento $\theta \in \mathfrak{m} \setminus \mathfrak{m}^2$ entonces $\langle \theta \rangle = \mathfrak{m}$ y cada ideal de A es de la forma $\langle \theta^i \rangle$ para $i = 1, 2, \ldots, \beta - 1$ donde β es el índice de nilpotencia de $\mathfrak{m}$.

– Lema –

Sea A un anillo de cadena, cualquier elemento de A es de la forma $u\theta^i$ con i único y la unidad u está unívocamente determinada módulo el ideal $\langle \theta^{\beta-i} \rangle$.

– Corolario –

Si $1 \leq i < j \leq \beta$ y $\theta^i c \in \langle \theta^j \rangle$ entonces $c \in \langle \theta^{j-i} \rangle$. En particular, si $\langle \theta^i \rangle \neq 0$ entonces $c \in \langle \theta^{\beta-i} \rangle$.

– Lema –

Sea A un anillo de cadena, cualquier elemento de A es de la forma $u\theta^i$ con i único y la unidad u está unívocamente determinada módulo el ideal $\langle \theta^{\beta-i} \rangle$.

– Corolario –

Si $1 \leq i < j \leq \beta$ y $\theta^i c \in \langle \theta^j \rangle$ entonces $c \in \langle \theta^{j-i} \rangle$. En particular, si $\langle \theta^i \rangle \neq 0$ entonces $c \in \langle \theta^{\beta-i} \rangle$.

– Lema –

Sea A un anillo de cadena y sea $V \subseteq A$ un conjunto de representantes de las clases de equivalencia de $A/\langle\theta\rangle$. Entonces:

1. Para cada $a \in A$ existen elementos únicos $a_0, \ldots, a_{\beta-1} \in V$ tales que

$$a = \sum_{i=0}^{\beta-1} a_i \cdot \theta^i.$$

2. $|V| = |A/\mathfrak{m}|$.
3. $|\langle\theta^j\rangle| = |A/\mathfrak{m}|^{\beta-j}$ con $0 \leq j \leq \beta - 1$.

– Lema –

Con la notación anterior existen enteros positivos s y t tales que:

1. $A = C \oplus C\theta \oplus \cdots \oplus C\theta^{s-1}$ como C-módulos.
2. $\theta^s = p(a_{s-1}\theta^{s-1} + \cdots + a_1\theta + a_0)$ donde $a_i \in C$ para $i = 1, 2, \ldots, s-1$ y a_0 es una unidad.
3. Como C-módulos

$$C\theta^i \simeq C,\ 1 \leq i \leq t-1 \quad , C\theta^i \simeq Cp,\ t \leq i \leq s-1.$$

4. $\beta = (n-1)s + t$, $1 \leq t \leq s$. Además si $n = 1$ se tiene que $s = t = \beta$.

Para el anillo de Galois C en el teorema anterior el polinomio

$$g(x) = x^s + p(a_{s-1}x^{s-1} + \cdots + a_1 x + a_0) \in C[x]$$

donde a_0 es una unidad se denomina polinomio de Eisenstein sobre C. El anillo $C[x]/\langle g(x)\rangle$ se denomina extensión de Eisenstein de C.

– Teorema (caracterización de los anillos de cadena –

Sea A un anillo de cadena con característica p^n ideal maximal $\mathfrak{m}$ con nilpotencia β y $r = [A/\mathfrak{m} : \mathbb{F}_p]$. Existen enteros no negativos t y s tales que $\beta = (n-1)s + t$, $1 \leq t \leq s$ y

$$A \simeq GR(p^{rn}, p^n)[x]/\langle g(x), p^{n-1}x^t \rangle$$

y $g(x)$ es un polinomio de Eisenstein de grado s sobre $GR(p^{rn}, p^n)$. El resultado recíproco también es cierto, cualquier anillo cociente de ese tipo es un anillo de cadena.

– Corolario –

En las condiciones del teorema anterior, si $(p, s) = 1$ se tiene que

$$A \simeq GR(p^{rn}, p^n)[x]/\langle x^s + p, p^{n-1}x^t \rangle.$$

En este caso el anillo A se denomina anillo de cadena puro.