Anillos de Galois

XXVII Escuela Venezolana de Matemáticas – EMALCA

Edgar Martínez-Moro

Sept. 2014

imUVa Instituto de Investigación en Matemáticas

Universidad de Valladolid

Definición y primeras propiedades

Un anillo asociativo A se llama anillo de Galois (denotado "GR" por sus siglas en inglés: *Galois Ring*) si es finito, conmutativo, con identidad y existe $d \in \mathbb{N}$ tal que el conjunto de divisores de cero de A es igual a dA.

Como ejemplos de anillos de Galois nos encontramos son los cuerpos finitos $\mathbb{F}_{p^r}$ y los anillos de residuos de enteros de orden potencia de primo $\mathbb{Z}_{p^n}$. En ambos casos basta con tomar $d = p$.

En la definición de anillo de Galois no es necesario imponer la conmutatividad del anillo, ya que ésta puede ser deducida del resto de las condiciones.

Definición y primeras propiedades

Un anillo asociativo A se llama anillo de Galois (denotado "GR" por sus siglas en inglés: *Galois Ring*) si es finito, conmutativo, con identidad y existe $d \in \mathbb{N}$ tal que el conjunto de divisores de cero de A es igual a dA.

Como ejemplos de anillos de Galois nos encontramos son los cuerpos finitos $\mathbb{F}_{p^r}$ y los anillos de residuos de enteros de orden potencia de primo $\mathbb{Z}_{p^n}$. En ambos casos basta con tomar $d = p$.

En la definición de anillo de Galois no es necesario imponer la conmutatividad del anillo, ya que ésta puede ser deducida del resto de las condiciones.

Definición y primeras propiedades

Un anillo asociativo A se llama anillo de Galois (denotado "GR" por sus siglas en inglés: *Galois Ring*) si es finito, conmutativo, con identidad y existe $d \in \mathbb{N}$ tal que el conjunto de divisores de cero de A es igual a dA.

Como ejemplos de anillos de Galois nos encontramos son los cuerpos finitos $\mathbb{F}_{p^r}$ y los anillos de residuos de enteros de orden potencia de primo $\mathbb{Z}_{p^n}$. En ambos casos basta con tomar $d = p$.

En la definición de anillo de Galois no es necesario imponer la conmutatividad del anillo, ya que ésta puede ser deducida del resto de las condiciones.

– Teorema –

Sea A un GR en el que el conjunto de divisores de cero es pA. Entonces se verifican las siguientes propiedades:

1. El conjunto $A^* = A \setminus pA$ es un grupo multiplicativo abeliano (el grupo de las unidades de A).
2. A es un anillo local con ideal maximal pA. El anillo cociente $\overline{A} = A/pA$ es un cuerpo finito $\mathbb{F}_q$ donde $q = p^r$ (para algún $r \in \mathbb{N}$). Es decir, p es un número primo.
3. La característica de A es igual a p^n, $n \in \mathbb{N}$.
4. El conjunto de ideales de A es la cadena estrictamente decreciente:

$$A = p^0 A \rhd p^1 A \rhd \cdots \rhd p^{n-1} A \rhd p^n A = 0.$$

– Teorema (cont) –

5. Para todo $t \in \{0, \ldots, n\}$ se verifica la igualdad:

$$|p^t A| = q^{n-t}.$$

En particular: $|A| = q^n$ y $|A^*| = (q-1)q^{n-1}$. Además, para todo $b \in p^t A \setminus p^{t+1}A$, y para todo $t \in \{0, \ldots, n-1\}$, se verifica:

$$Ab = bA = p^t A.$$

Existencia y unicidad

Sea A un GR de característica p^n y $\overline{A} = A/pA = \mathbb{F}_{p^r}$. Dado un polinomio $f(x) = \sum_{i=0}^{r} a_i x^i \in A[x]$ denotaremos por $\overline{f}(x)$ el polinomio $\sum_{i=0}^{r} \overline{a_i} x^i \in \overline{A}[x]$.

Si A es un GR, entonces un polinomio $g(x) \in A[x]$ se dice polinomio de Galois si es mónico y $\overline{g}(x) \in \overline{A}[x]$ es irreducible sobre $\overline{A}$.

La existencia de polinomios de Galois de cualquier grado sobre un anillo de Galois queda garantizada por la existencia de polinomios mónicos e irreducibles de cualquier grado sobre cuerpos finitos.

Existencia y unicidad

Sea A un GR de característica p^n y $\overline{A} = A/pA = \mathbb{F}_{p^r}$. Dado un polinomio $f(x) = \sum_{i=0}^{r} a_i x^i \in A[x]$ denotaremos por $\overline{f}(x)$ el polinomio $\sum_{i=0}^{r} \overline{a_i} x^i \in \overline{A}[x]$.

Si A es un GR, entonces un polinomio $g(x) \in A[x]$ se dice polinomio de Galois si es mónico y $\overline{g}(x) \in \overline{A}[x]$ es irreducible sobre $\overline{A}$.

La existencia de polinomios de Galois de cualquier grado sobre un anillo de Galois queda garantizada por la existencia de polinomios mónicos e irreducibles de cualquier grado sobre cuerpos finitos.

Existencia y unicidad

Sea A un GR de característica p^n y $\overline{A} = A/pA = \mathbb{F}_{p^r}$. Dado un polinomio $f(x) = \sum_{i=0}^{r} a_i x^i \in A[x]$ denotaremos por $\overline{f}(x)$ el polinomio $\sum_{i=0}^{r} \overline{a_i} x^i \in \overline{A}[x]$.

Si A es un GR, entonces un polinomio $g(x) \in A[x]$ se dice polinomio de Galois si es mónico y $\overline{g}(x) \in \overline{A}[x]$ es irreducible sobre $\overline{A}$.

La existencia de polinomios de Galois de cualquier grado sobre un anillo de Galois queda garantizada por la existencia de polinomios mónicos e irreducibles de cualquier grado sobre cuerpos finitos.

– Teorema –

Sea A un GR de característica p^n y q^n elementos ($q = p^r$), $m \in \mathbb{N}$ y $g(x) \in A[x]$ un polinomio de Galois de grado m. Entonces $S = A[x]/\langle g(x) \rangle$ es un GR de característica p^n y cardinal q^{mn}.

Si A es un subanillo de S y ambos son GR, entonces el cuerpo finito $\overline{A} = A/pA$ es un subcuerpo de $\overline{S} = S/pS$.

Si A y S son dos GR tales que $A \subseteq S$, con $[\overline{S} : \overline{A}] = m$, entonces diremos que S es una extensión de Galois de grado m de A (o que A es un subanillo de Galois de S) y denotaremos el grado de esta extensión como $[S : A]$.

Si A es un subanillo de S y ambos son GR, entonces el cuerpo finito $\overline{A} = A/pA$ es un subcuerpo de $\overline{S} = S/pS$.

Si A y S son dos GR tales que $A \subseteq S$, con $[\overline{S} : \overline{A}] = m$, entonces diremos que S es una extensión de Galois de grado m de A (o que A es un subanillo de Galois de S) y denotaremos el grado de esta extensión como $[S : A]$.

– Corolario –

Para todo anillo de Galois A y para todo $m \in \mathbb{N}$ existe una extensión de Galois de grado m de A.

– Corolario (Existencia) –

Para todo número primo p y para cualesquiera $r, n \in \mathbb{N}$, existe un anillo de Galois S de característica p^n y cardinal p^{rn} que es extensión de Galois de grado r de $\mathbb{Z}_{p^n}$.

– Corolario –

Para todo anillo de Galois A y para todo $m \in \mathbb{N}$ existe una extensión de Galois de grado m de A.

– Corolario (Existencia) –

Para todo número primo p y para cualesquiera $r, n \in \mathbb{N}$, existe un anillo de Galois S de característica p^n y cardinal p^{rn} que es extensión de Galois de grado r de $\mathbb{Z}_{p^n}$.

Si S es una extensión de Galois de A y $a \in S$, entonces llamamos extensión de A por a, y lo denotaremos $A[a]$, al subanillo de S generado por $A \cup \{a\}$. Claramente $A[a] = \{f(a) \mid f(x) \in A[x]\} \cong A[x]/\mathfrak{a}$ donde $\mathfrak{a}$ es el ideal anulador $\{f(x) \in A[x] \mid f(a) = 0\}$.

– Lema –

Sea S una extensión de Galois de un anillo de Galois A, $a \in S$ y $f(x) \in A[x]$ tal que $\overline{f}(\overline{a}) = \overline{0}$ y $\overline{f}'(\overline{a}) \neq \overline{0}$. Entonces existe un único $b \in S$, raíz de $f(x)$, tal que $\overline{b} = \overline{a}$.

Si S es una extensión de Galois de A y $a \in S$, entonces llamamos extensión de A por a, y lo denotaremos $A[a]$, al subanillo de S generado por $A \cup \{a\}$. Claramente $A[a] = \{f(a) \mid f(x) \in A[x]\} \cong A[x]/\mathfrak{a}$ donde $\mathfrak{a}$ es el ideal anulador $\{f(x) \in A[x] \mid f(a) = 0\}$.

– Lema –

Sea S una extensión de Galois de un anillo de Galois A, $a \in S$ y $f(x) \in A[x]$ tal que $\overline{f}(\overline{a}) = \overline{0}$ y $\overline{f}'(\overline{a}) \neq \overline{0}$. Entonces existe un único $b \in S$, raíz de $f(x)$, tal que $\overline{b} = \overline{a}$.

– Lema –

Sea S una extensión de Galois de grado m de un anillo de Galois A y $a \in S$ tal que $\overline{A}[\overline{a}] = \overline{S}$. Entonces

$$S = A[a] = \{f(a) \mid f(x) \in A[x],\ \mathrm{gr}(f(x)) < m\}.$$

– Teorema –

Sea S una extensión de Galois de grado m de A, un GR de característica p^n y cardinal p^{rn}. Sea $g(x) \in A[x]$ un polinomio de Galois de grado k. Entonces:

1. $g(x)$ tiene una raíz en S si y sólo si $k \mid m$.
2. Si $k \mid m$, entonces $g(x)$ posee exactamente k raíces $a_1, \ldots, a_k \in S$, distintas módulo pS, y

$$g(x) = (x - a_1) \ldots (x - a_k).$$

3. Para todo elemento $a \in S$ la igualdad $S = A[a]$ es cierta si y sólo si a es una raíz de un polinomio de Galois de grado m sobre A.

– Corolario –

Si S es una extensión de Galois de grado m de un anillo de Galois A entonces $S \cong A[x]/\langle g(x)\rangle$ donde $g(x) \in A[x]$ es un polinomio de Galois cualquiera de grado m. Además, S es un A-módulo libre de rango m con base $\{e, x, \ldots, x^{m-1}\}$. En particular, si S es un GR de característica p^n y cardinal p^{sn}, entonces $S \cong \mathbb{Z}_{p^n}[x]/\langle g(x)\rangle$ donde $g(x) \in \mathbb{Z}_{p^n}$ es un polinomio de Galois cualquiera de grado s.

– Corolario (Unicidad) –

Dos anillos de Galois son isomorfos si y sólo si tienen la misma característica y el mismo cardinal. Al único GR, salvo isomorfismo, de característica p^n y cardinal p^{rn} lo denotaremos $GR(p^{rn}, p^n)$.

Con la notación introducida $\mathbb{F}_{p^r} = GR(p^r, p)$, $\mathbb{Z}_{p^n} = GR(p^n, p^n)$ y, si $R = GR(q^n, p^n)$ $(q = p^r)$, entonces $\overline{R}$ es isomorfo a $\mathbb{F}_q$. En todo lo que resta de capítulo supondremos siempre que $q = p^r$, con $r \in \mathbb{N}$.

Si $A = GR(q^n, p^n)$, entonces para todo $t \in \{1, \ldots, n\}$ se tiene $A/p^t A = GR(q^t, p^t)$.

Conjunto Coordenado de Teichmüller

Si A es un GR, entonces un conjunto coordenado es un subconjunto $\Gamma \subseteq A$ tal que sus elementos forman un sistema completo de representantes módulo pA, esto es, $\overline{\Gamma} = \{\overline{a} \mid a \in \Gamma\} = \overline{A}$ y $|\Gamma| = |\overline{A}|$.

Ejemplo: Si $A = GR(p^n, p^n) = \mathbb{Z}_{p^n}$, entonces $\Gamma = \{0, 1, \ldots, p-1\}$ es un conjunto coordenado de A.

Conjunto Coordenado de Teichmüller

Si A es un GR, entonces un conjunto coordenado es un subconjunto $\Gamma \subseteq A$ tal que sus elementos forman un sistema completo de representantes módulo pA, esto es, $\overline{\Gamma} = \{\overline{a} \mid a \in \Gamma\} = \overline{A}$ y $|\Gamma| = |\overline{A}|$.

Ejemplo: Si $A = GR(p^n, p^n) = \mathbb{Z}_{p^n}$, entonces $\Gamma = \{0, 1, \ldots, p-1\}$ es un conjunto coordenado de A.

– Proposición –

Si A es un GR y $\Gamma \subseteq A$ es un conjunto coordenado, entonces para todo $a \in A$ existen elementos únicos $a_0, \ldots, a_{n-1} \in \Gamma$ tales que $a = \sum_{i=0}^{n-1} p^i a_i$.

En un anillo de Galois se pueden considerar diferentes conjuntos coordenados pero, entre todos los posibles, hay uno que tiene especial interés.

Un conjunto coordenado de un anillo de Galois A se dice conjunto coordenado de Teichmüller (TCS) si es cerrado para el producto.

– Proposición –

Si $A = GR(q^n, p^n)$, entonces $\Gamma(A) = \{a \in A \mid a^q = a\}$ es el único TCS de A.

En un anillo de Galois se pueden considerar diferentes conjuntos coordenados pero, entre todos los posibles, hay uno que tiene especial interés.

Un conjunto coordenado de un anillo de Galois A se dice conjunto coordenado de Teichmüller (TCS) si es cerrado para el producto.

– Proposición –

Si $A = GR(q^n, p^n)$, entonces $\Gamma(A) = \{a \in A \mid a^q = a\}$ es el único TCS de A.

Si $A = GR(q^n, p^n)$ entonces el epimorfismo canónico $A \to \overline{A}$ induce un isomorfismo multiplicativo $\Gamma(A) \to \overline{A}$.

Dado un anillo de Galois A con conjunto coordenado de Teichmüller $\Gamma(A)$ podemos considerar, para cada elemento $a \in A$, la descomposición p-ádica asociada a $\Gamma(A)$:

$$a = \gamma_0(a) + p\gamma_1(a) + \cdots + p^{n-1}\gamma_{n-1}(a)$$

donde $\gamma_i(a) \in \Gamma(A)$ para todo $i \in \{0, \ldots, n-1\}$.

Si A es un GR y $\Gamma(A)$ su TCS, entonces las aplicaciones $\gamma_i : A \to \Gamma(A)$ inducidas por la descomposición p-ádica asociada a $\Gamma(A)$ se llaman funciones coordenadas de A.

Si $A = GR(q^n, p^n)$ entonces el epimorfismo canónico $A \to \overline{A}$ induce un isomorfismo multiplicativo $\Gamma(A) \to \overline{A}$.

Dado un anillo de Galois A con conjunto coordenado de Teichmüller $\Gamma(A)$ podemos considerar, para cada elemento $a \in A$, la descomposición p-ádica asociada a $\Gamma(A)$:

$$a = \gamma_0(a) + p\gamma_1(a) + \cdots + p^{n-1}\gamma_{n-1}(a)$$

donde $\gamma_i(a) \in \Gamma(A)$ para todo $i \in \{0, \ldots, n-1\}$.

Si A es un GR y $\Gamma(A)$ su TCS, entonces las aplicaciones $\gamma_i : A \to \Gamma(A)$ inducidas por la descomposición p-ádica asociada a $\Gamma(A)$ se llaman funciones coordenadas de A.

– Proposición –

Si A es un GR y $\Gamma \subseteq A$ es un conjunto coordenado, entonces para todo $a \in A$ existen elementos únicos $a_0, \ldots, a_{n-1} \in \Gamma$ tales que $a = \sum_{i=0}^{n-1} p^i a_i$.

Ejemplo: Si $A = GR(p^n, p^n) = \mathbb{Z}_{p^n}$, con $n = 1$ ó $p = 2$, entonces el TCS de A es el conjunto $\Gamma(A) = \{0, 1, \ldots, p-1\}$. Si $n > 1$ y $p \neq 2$, entonces $\Gamma(A) \neq \{0, 1, \ldots, p-1\}$, ya que $(-1)^p = -1$ y, por tanto, $-1 \in \Gamma(A)$. En este caso $\Gamma(A) = \{0, 1, 2^{p^{n-1}}, \ldots, (p-1)^{p^{n-1}}\}$.

– Proposición –

Si A es un GR y $\Gamma \subseteq A$ es un conjunto coordenado, entonces para todo $a \in A$ existen elementos únicos $a_0, \ldots, a_{n-1} \in \Gamma$ tales que $a = \sum_{i=0}^{n-1} p^i a_i$.

Ejemplo: Si $A = GR(p^n, p^n) = \mathbb{Z}_{p^n}$, con $n = 1$ ó $p = 2$, entonces el TCS de A es el conjunto $\Gamma(A) = \{0, 1, \ldots, p-1\}$. Si $n > 1$ y $p \neq 2$, entonces $\Gamma(A) \neq \{0, 1, \ldots, p-1\}$, ya que $(-1)^p = -1$ y, por tanto, $-1 \in \Gamma(A)$. En este caso $\Gamma(A) = \{0, 1, 2^{p^{n-1}}, \ldots, (p-1)^{p^{n-1}}\}$.

Si $A = GR(q^n, p^n)$, entonces el conjunto coordenado de Teichmüller $\Gamma(A)$ no es, en general, un conjunto cerrado para la suma: basta notar que $\Gamma(\mathbb{Z}_{p^n})$, con $p \neq 2$, no es cerrado para la suma.

Si $\Gamma(A)$ es el TCS de un anillo de Galois A, entonces definimos la suma

$$\oplus : \Gamma(A) \times \Gamma(A) \to \Gamma(A)$$

como $a \oplus b = \gamma_0(a + b)$ para todo $a, b \in \Gamma(A)$.

Si $A = GR(q^n, p^n)$, entonces el conjunto coordenado de Teichmüller $\Gamma(A)$ no es, en general, un conjunto cerrado para la suma: basta notar que $\Gamma(\mathbb{Z}_{p^n})$, con $p \neq 2$, no es cerrado para la suma.

Si $\Gamma(A)$ es el TCS de un anillo de Galois A, entonces definimos la suma

$$\oplus : \Gamma(A) \times \Gamma(A) \to \Gamma(A)$$

como $a \oplus b = \gamma_0(a + b)$ para todo $a, b \in \Gamma(A)$.

– Proposición –

Si $A = GR(q^n, p^n)$ y $\Gamma(A) \subseteq A$ es su TCS, entonces $(\Gamma(A), \oplus, \cdot)$ es un cuerpo finito de q elementos y el epimorfismo canónico $\pi : \Gamma(A) \to \overline{A}$ es un isomorfismo de cuerpos.

Subanillos de Galois. Automorfismos

– Teorema –

Si $S = GR(p^{sn}, p^n)$ y $A = GR(p^{rn}, p^n) \subseteq S$ es un subanillo de Galois, entonces r divide a s. Recíprocamente, para cada divisor r de s, existe exactamente un subanillo de Galois de S de la forma $GR(p^{rn}, p^n)$.

Si S es una extensión de Galois de grado m de A, entonces el cuerpo $(\Gamma(S), \oplus, \cdot)$ es una extensión de Galois de grado m del cuerpo $(\Gamma(A), \oplus, \cdot)$.

Si $S = GR(p^{sn}, p^n)$, con $s, n > 1$, entonces existen subanillos de S que no son, necesariamente, de Galois. Por ejemplo, si $S_0 = GR(p^n, p^n)$ denota el subanillo generado por la identidad, entonces

$$A = \Gamma(S_0) + p\Gamma(S_0) + \cdots + p^{n-2}\Gamma(S_0) + p^{n-1}\Gamma(S)$$

es un subanillo propio de S, ya que $A = S_0 + p^{n-1}\Gamma(S)$, que no es de Galois, puesto que $|A| = p^{n-1}p^s$.

Si S es una extensión de Galois de grado m de A, entonces el cuerpo $(\Gamma(S), \oplus, \cdot)$ es una extensión de Galois de grado m del cuerpo $(\Gamma(A), \oplus, \cdot)$.

Si $S = GR(p^{sn}, p^n)$, con $s, n > 1$, entonces existen subanillos de S que no son, necesariamente, de Galois. Por ejemplo, si $S_0 = GR(p^n, p^n)$ denota el subanillo generado por la identidad, entonces

$$A = \Gamma(S_0) + p\Gamma(S_0) + \cdots + p^{n-2}\Gamma(S_0) + p^{n-1}\Gamma(S)$$

es un subanillo propio de S, ya que $A = S_0 + p^{n-1}\Gamma(S)$, que no es de Galois, puesto que $|A| = p^{n-1}p^s$.

– Teorema –

Si $A = GR(q^n, p^n)$, entonces:

1. Todo $\tau \in \mathrm{Aut}(A)$ estabiliza el TCS de A, es decir, $\tau(\Gamma(A)) = \Gamma(A)$. Además, la restricción $\tau|_{\Gamma(S)} = \widehat{\tau}$ es un automorfismo del cuerpo $(\Gamma(A), +, \oplus)$.
2. Para todo $\tau \in \mathrm{Aut}(A)$ existe $v \in \{0, \ldots, s-1\}$ tal que

$$\tau(a) = \gamma_0(a)^{p^v} + p\gamma_1(a)^{p^v} + \cdots + p^{n-1}\gamma_{n-1}(a)^{p^v}$$

   con $a \in A$.
3. La aplicación $\varphi : \mathrm{Aut}(A) \to \mathrm{Aut}(\Gamma(A))$, dada por $\varphi(\tau) = \widehat{\tau}$, es un isomorfismo de grupos y $\mathrm{Aut}(A)$ es un grupo cíclico de orden r.

– Corolario –

Si $A = GR(q^n, p^n)$ y $S = GR(q^{mn}, p^n)$ es una extensión de Galois de grado m suya, entonces el grupo $\mathrm{Aut}(S|A)$, de los automorfismos de S que dejan fijos los elementos del subanillo A, es isomorfo al grupo $\mathrm{Aut}(\Gamma(S)|\Gamma(A))$. Por tanto $\mathrm{Aut}(\Gamma(S)|\Gamma(A))$ es un grupo cíclico de orden m generado por el automorfismo

$$\tau(a) = \gamma_0(a)^q + p\gamma_1(a)^q + \cdots + p^{n-1}\gamma_{n-1}(a)^q$$

para todo $a \in S$.

Sea $S = GR(q^{mn}, p^n)$ una extensión de Galois de grado m de $A = GR(q^n, p^n)$. La función traza de la extension $S|A$ es la aplicación:

$$\mathrm{Tr}_A^S(a) = \sum_{\sigma \in \mathrm{Aut}(S|A)} \sigma(a).$$

– Proposición –

Si $S = GR(q^{mn}, p^n)$ es una extensión de Galois de grado m de $A = GR(q^n, p^n)$ y $\mathrm{Tr} = \mathrm{Tr}_A^S$ es la función traza de la extensión $S|A$, entonces $\mathrm{Tr} : S \to A$ es un epimorfismo de A-módulos.

Sea $S = GR(q^{mn}, p^n)$ una extensión de Galois de grado m de $A = GR(q^n, p^n)$. La función traza de la extension $S|A$ es la aplicación:

$$\mathrm{Tr}_A^S(a) = \sum_{\sigma \in \mathrm{Aut}(S|A)} \sigma(a).$$

– Proposición –

Si $S = GR(q^{mn}, p^n)$ es una extensión de Galois de grado m de $A = GR(q^n, p^n)$ y $\mathrm{Tr} = \mathrm{Tr}_A^S$ es la función traza de la extensión $S|A$, entonces $\mathrm{Tr} : S \to A$ es un epimorfismo de A-módulos.